Exam : SY0-101

Title : Security+

Ver : 12.14.06

QUESTION 1:

Who is responsible for establishing access permissions to network resources in the DAC access control model?

A. The system administrator.
B. The owner of the resource.
C. The system administrator and the owner of the resource.
D. The user requiring access to the resource.

Answer: B

Explanation:
The owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
Incorrect Answers:
A: The system administrator is responsible for access privileges in the MAC (Mandatory Access Control).
C: Only the owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
D: In no access control mechanism is the user that requires access allowed to establish access control permissions.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 11-12.

QUESTION 2:

Which access control system allows the owner of a resource to establish access permissions to that resource?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Answer: B

Explanation:
The owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
Incorrect Answers:
A: The system administrator is responsible for access privileges in the MAC (Mandatory Access Control).
C: Access control using the RBAC model is based on the role or responsibilities users

have in the organization.
D: The owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 3:

Which access control system allows the system administrator to establish access permissions to network resources?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Answer: A

Explanation:
The system administrator is responsible for access privileges in the MAC (Mandatory Access Control).
Incorrect Answers:
B: The owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
C: Access control using the RBAC model is based on the role or responsibilities users have in the organization.
D: The owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 4:

Who is responsible for establishing access permissions to network resources in the MAC access control model?

A. The system administrator.
B. The owner of the resource.
C. The system administrator and the owner of the resource.
D. The user requiring access to the resource.

Answer: A

Explanation:
The system administrator is responsible for access privileges in the MAC (Mandatory Access Control).
Incorrect Answers:
B: The owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
C: Only the owner of the resource is responsible for access privileges in the DAC (Discretionary Access Control).
D: In no access control mechanism is the user that requires access allowed to establish access control permissions.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 11-12.

QUESTION 5:

Which of the following access control models uses roles to determine access permissions?

A. MAC
B. DAC
C. RBAC
D. None of the above.

Answer: C

Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These usually reflect the organization's structure and can be implemented system wide.
Incorrect Answers:
A: Access control using the MAC model is based on predefined access privileges to a resource.
B: Access control using the DAC model is based on the owner of the resource allowing other users access to that resource.
D: Access control using the RBAC model is based on the role or responsibilities users have in the organization.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 6:

How is access control permissions established in the RBAC access control model?

A. The system administrator.
B. The owner of the resource.
C. The role or responsibilities users have in the organization.
D. None of the above.

Answer: C

Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These usually reflect the organization's structure and can be implemented system wide.
Incorrect Answers:
A: Access control using the MAC model is based on predefined access privileges established by the system administrator.
B: Access control using the DAC model is based on the owner of the resource allowing other users access to that resource.
D: Access control using the RBAC model is based on the role or responsibilities users have in the organization.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 7:

Which access control model uses Access Control Lists to identify the users who have permissions to a resource?

A. MAC
B. RBAC
C. DAC
D. None of the above.

Answer: C

Explanation:
The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
Incorrect Answers:
A: MAC model uses static relations. This is a predefined access privileges to a resource.

B:
RBAC uses the role or responsibilities users have in the organization rather than user permissions.
D: The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 8:

Which access control model uses static relations to identify the users who have permissions to a resource?

A. MAC
B. RBAC
C. DAC
D. None of the above.

Answer: A

Explanation:
MAC model uses static relations. This is a predefined access privileges to a resource.
Incorrect Answers:
B: RBAC uses the role or responsibilities users have in the organization rather than user permissions.
C: The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
D: MAC model uses static relations. This is a predefined access privileges to a resource.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 9:

Which access control model uses predefined access privileges control access to a resource?

A. MAC
B. RBAC

C. DAC
D. None of the above.

Answer: A

Explanation:
MAC model uses static relations. This is a predefined access privileges to a resource.
Incorrect Answers:
B: RBAC uses the role or responsibilities users have in the organization rather than user permissions.
C: The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
D: MAC model uses static relations. This is a predefined access privileges to a resource.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 10:

What does the DAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above.

Answer: C

Explanation:
The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
Incorrect Answers:
A: MAC model uses static relations. This is a predefined access privileges to a resource.
B: RBAC uses the role or responsibilities users have in the organization rather than user permissions.
D: The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 11:

What does the MAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above.

Answer: A

Explanation:
MAC model uses static relations. This is a predefined access privileges to a resource.
Incorrect Answers:
B: RBAC uses the role or responsibilities users have in the organization rather than user permissions.
C: The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
D: MAC model uses static relations. This is a predefined access privileges to a resource.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 12:

What does the RBAC access control model use to identify the users who have permissions to a resource?

A. Predefined access privileges.
B. The role or responsibilities users have in the organization
C. Access Control Lists
D. None of the above.

Answer: B

Explanation:
RBAC uses the role or responsibilities users have in the organization.
Incorrect Answers:
A: MAC model uses static relations. This is a predefined access privileges to a resource.

C: The DAC model allows the owner of a resource to control access privileges to that resource. This model uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
D: RBAC uses the role or responsibilities users have in the organization.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10, 668.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 13.

QUESTION 13:

Which of the following statements regarding access control models is FALSE?

A. The MAC model uses predefined access privileges to a resource to determine a user's access permissions to a resource.
B. The RBAC model uses the role or responsibilities users have in the organization to determine a user's access permissions to a resource.
C. In the DAC model a user's access permissions to a resource is mapped to the user's account.
D. The MAC model uses Access Control Lists (ACLs) to map a user's access permissions to a resource.

Answer: D

Explanation:
The DAC model, not the MAC model, uses Access Control Lists (ACLs) to map a user's to access permissions to a resource.
Incorrect Answers:
A, B, C: These are all true.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 11-12.

QUESTION 14:

Which of the following statements regarding the MAC access control models is TRUE?

A. The Mandatory Access Control (MAC) model is a dynamic model.
B. In the Mandatory Access Control (MAC) the owner of a resource establishes access privileges to that resource.
C. In the Mandatory Access Control (MAC) users cannot share resources dynamically.
D. The Mandatory Access Control (MAC) model is not restrictive.

Answer: C

Explanation:
Because the MAC model uses a predefined set of access privileges users cannot share resources dynamically.
Incorrect Answers:
A: The MAC model is a static, not a dynamic, model.
B: In the MAC the system administrator, not the owner of a resource, establishes access privileges to files on the system.
D: Because the MAC model uses a predefined set of access privileges, it can be very restrictive
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 11.

QUESTION 15:

Choose the mechanism that is NOT a valid access control mechanism.

A. DAC (Discretionary Access Control) list.
B. SAC (Subjective Access Control) list.
C. MAC (Mandatory Access Control) list.
D. RBAC (Role Based Access Control) list.

Answer: B

Explanation:
The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). There is no SAC (Subjective Access Control) list.
Incorrect Answers:
C: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). MAC is based on predefined access privileges to a resource.
A: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). DAC is based on the owner of the resource allowing other users access to that resource.
D: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). RBAC is based on the role or responsibilities users have in the organization.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION 16:

The DAC (Discretionary Access Control) model has an inherent flaw. Choose the option that describes this flaw.

A. The DAC (Discretionary Access Control) model uses only the identity of the user or specific process to control access to a resource. This creates a security loophole for Trojan horse attacks.
B. The DAC (Discretionary Access Control) model uses certificates to control access to resources. This creates an opportunity for attackers to use your certificates.
C. The DAC (Discretionary Access Control) model does not use the identity of a user to control access to resources. This allows anyone to use an account to access resources.
D. The DAC (Discretionary Access Control) model does not have any known security flaws.

Answer: A

Explanation:
The DAC model is more flexible than the MAC model. It allows the owner of a resource to control access privileges to that resource. Thus, access control is entirely at the digression of the owner, as is the resource that is shared. In other words, there are no security checks to ensure that malicious code is not made available for sharing.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p. 720.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 393.

QUESTION 17:

Choose the access control method which provides the most granular access to protected objects?

A. Capabilities
B. Access control lists
C. Permission bits
D. Profiles

Answer: B

Explanation:
Access control lists enable devices in your network to ignore requests from specified users or systems, or grant certain network capabilities to them. ACLs allow a stronger set of access controls to be established in your network. The basic process of ACL control allows the administrator to design and adapt the network to deal with specific security threats.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 13, 216, 219

QUESTION 18:

You work as the network administrator at Certkiller .com. The Certkiller .com network uses the RBAC (Role Based Access Control) model.
You must plan the security strategy for users to access resources on the Certkiller .com network. The types of resources you must control access to are mailboxes, and files and printers. Certkiller .com is divided into distinct departments and functions named Finance, Sales, Research and Development, and Production respectively. Each user has its own workstation, and accesses resources based on the department wherein he/she works.
You must determine which roles to create to support the RBAC (Role Based Access Control) model.
Which of the following roles should you create?

A. Create mailbox, and file and printer roles.
B. Create Finance, Sales, Research and Development, and Production roles.
C. Create user and workstation roles.
D. Create allow access and deny access roles.

Answer: B

Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These roles usually reflect the organization's structure, such as its division into different departments, each with its distinct role in the organization. Thus the RBAC model could be based on the different departments.
Incorrect Answers:
A: The RBAC model is based on user roles, not on resource roles such as file, printer, and mailbox roles. These resource roles might not reflect the different departments' access requirements to them.
C: The RBAC model is based on user roles, not on a division between users and machines. Grouping all users together does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.
D: By implementing allow access and deny access roles, we would create only two options: access to all resources or no access. This does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION 19:

On the topic of the DAC (Discretionary Access Control) model, choose the statement(s) which are TRUE.

A. All files that do not have a specified owner cannot be modified.
B. The system administrator is an owner of all objects.
C. The operating system is an owner of all objects.
D. All objects have an owner, and this owner has full control over that specific object.

Answer: D

Explanation:
The DAC model allows the owner of a resource to control access privileges to that resource. Thus, access control is entirely at the digression of the owner who has full control over the resource.
Incorrect Answers:
A: Each file does have an owner, which is the user that created the file, or the user to whom the creator of the file has transferred ownership.
B: The creator of the resource is the owner of that resource, not the administrator.
C: The creator of the resource is the owner of that resource, not the operating system.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 9-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION 20:

Choose the access control model that allows access control determinations to be performed based on the security labels associated with each user and each data item.

A. MACs (Mandatory Access Control) method
B. RBACs (Role Based Access Control) method
C. LBACs (List Based Access Control) method
D. DACs (Discretionary Access Control) method

Answer: A

Explanation:
Mandatory Access Control is a strict hierarchical model usually associated with governments. All objects are given security labels known as sensitivity labels and are

classified accordingly. Then all users are given specific security clearances as to what they are allowed to access.
Incorrect Answers:
B: RBAC is based on group membership, which would reflect both the role users fulfill in the organization and the structure of the organization.
C: LBAC is based on a list of users and the privileges they have been granted to an object. This list is usually created by the administrator.
D: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 13.

QUESTION 21:

Choose the terminology or concept which best describes a (Mandatory Access Control) model.

A. Lattice
B. Bell La-Padula
C. BIBA
D. Clark and Wilson

Answer: A

Explanation:
The word lattice is used to describe the upper and lower bounds of a user's access permission. In other words, a user's access differs at different levels. It describes a hierarchical model that is based on classifying data on sensitivity and categorizing it at different levels. Users must have the correct level of security clearances to access the data. This is the system that MAC is based on.
Incorrect Answers:
B: TheBell La-Padula model prevents a user from accessing information that has a higher security rating than that which the user is authorized to access. It also prevents information from being written to a lower level of security. Thus this model is based on classification which is used in MAC. However, it is not the best answer.
C: TheBIBA model is similar to the Bell La-Padula model but is more concerned with information integrity.
D: TheClark and Wilson model prevents the direct access of data. Data can only be accessed through applications that have predefined capabilities. This prevents unauthorized modification, errors, and fraud from occurring. This does not describe MAC.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 455, 267-269.

QUESTION 22:

Which of the following sequences is correct regarding the flow of the CHAP system?

A. Logon request, encrypts value response, server, challenge, compare encrypts results, authorize or fail
B. Logon request, challenge, encrypts value response, server, compare encrypted results, authorize or fail
C. Logon request, challenge, server, encrypts value response, compare encrypted results, authorize or fail
D. Logon request, server, encrypts value response, challenge, compare encrypted results, authorize or fail

Answer: B

Explanation:
The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14.

QUESTION 23:

Which authentication method does the following sequence: Logon request, encrypts value response, server, challenge, compare encrypts results, authorize or fail referred to?

A. Certificates
B. Security Tokens
C. CHAP
D. Kerberos

Answer: C

Explanation:
The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts

over.
Incorrect answers:
A: A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
B: If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.
D: The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-16.

QUESTION 24:

Which of the following statements is TRUE regarding the CHAP authentication system?

A. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
B. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed
C.
The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
D. The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over

Answer: D

Explanation:
The initiator sends a logon request from the client to the server. The server sends a

challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over
Incorrect Answers:
A: This is known as the Certificate system.
B: This is known as the Security Token system.
C: This is known as the Kerberos system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-16.

QUESTION 25:

Which of the following statements is TRUE regarding the Security Token system?

A. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.
B. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
C.
The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
D. The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over

Answer: A

Explanation:
The Security Token system functions in this manor. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.
Incorrect Answers:
B: This is known as the Certificate system.
C: This is known as the Kerberos system.
D: This is known as the CHAP system.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-16.

QUESTION 26:

Which of the following statements is TRUE regarding the Certificate system?

A. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a token every time a user or a session begins. At the completion of a session, the token is destroyed.
B. The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
C. The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over
D. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.

Answer: D

Explanation:
A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.
Incorrect answers:
A: This is known as the Security Token system.
B: This is known as the Kerberos system.
C: This is known as the CHAP system.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-16.

QUESTION 27:

Which of the following statements is TRUE regarding the Kerberos system?

A. If your token does not grant you access to certain information, that information will either not be displayed or your access will be denied. The authentication system creates a

token every time a user or a session begins. At the completion of a session, the token is destroyed.
B. The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network.
C.
The initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and if the information matches, the server grants authorization. If the response fails, the session fails and the request phase starts over
D. A certificate being handed from the server to the client once authentication has been established. If you have a pass, you can wander throughout the network. BUT limited access is allowed.

Answer: B

Explanation:
The authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process. The KDC authenticates the network. Principles can be users, programs, or systems. The KDC provides a ticket to the network. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another network
Incorrect answers:
A: This is known as the Security Token system.
C: This is known as the CHAP system.
D: This is known as the Certificate system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-16.

QUESTION 28:

Which of the following authentication systems make use of the KDC Key Distribution Center?

A. Certificates
B. Security Tokens
C. CHAP.
D. Kerberos.

Answer: D

Explanation:

The Kerberos authentication process uses a Key Distribution Center (KDC) to orchestrate the entire process.
Incorrect answers:
A, B, C: All make use of challenges.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-16.

QUESTION 29:

Which of the following methods of authentication makes use of hand scanners, fingerprints, retinal scanners or DNA structure to identify the user?

A. Smart Cards
B. Multi-Factor
C. Kerberos
D. Biometrics

Answer: D

Explanation:
Biometric devices use physical characteristics to identify the user. Multi-Factor could also be a factor but will require another authentication method in order for it to accept the user's login.
Incorrect answers:
A: A smart card is a type of badge or card that can allow access to multiple resources including buildings, parking lots, and computers.
B: When two or more of these access methods are included as a part of the authentication process, you are implementing a multi-factor system.
C: Kerberos is an authentication scheme that uses tickets (unique keys) embedded within messages.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-18.

QUESTION 30:

Which of the following authentication methods increases the security of the authentication process because it must be in your physical possession?

A. Smart Cards.
B. Kerberos.
C. CHAP.
D. Certificate.

Answer: A

Explanation:
The reader is connected to the workstation and validates against the security system but this system holds a risk if the card is not taken care of. A whole system can become useless if your smart card is lost or stolen.
Incorrect answers:
B: Kerberos makes use of a computer based Key Distribution Center.
C, D: Makes use of challenges.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-18.

QUESTION 31:

What is the first thing a computer system requires from a user for correct authentication?

A. Username and Password.
B. Smart card.
C. Certificate.
D. Security Token.

Answer: A

Explanation:
CHAP performs the handshake process when first establishing a connectin; and then at random intervals during the transaction session.
Incorrect answers:
B: Smart Cards make use of a pin number.
C: Certificates are required for verification only.
D: Security Tokens are only used once and are only created once a user logs in.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-18.

QUESTION 32:

Which of the following methods of authentication makes use of a card that is similar to a credit card?

A. CHAP
B. Certification
C. Biometrics
D. Smart Cards

Answer: D

Explanation:
A smart card is a type of badge or card that can allow access to multiple resources including buildings, parking lots, and computers.
Incorrect answers:
A: Makes use of challenges.
B: Makes use of challenges.
C: Makes use of physical characteristics such as fingerprints and DNA.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 14-19.

QUESTION 33:

Which of the following authentication methods scans unique physical attributes of a user to identify the user?

A. Smart Cards
B. Multi-Factor
C. Kerberos
D. Biometrics

Answer: D

Explanation:
Biometric devices use physical characteristics to identify the user. Multi-Factor could also be a factor but will require another authentication method in order for it to accept the user's login.
Incorrect answers:
A: A smart card is a type of badge or card that can allow access to multiple resources including buildings, parking lots, and computers.
B: When two or more of these access methods are included as a part of the authentication process, you are implementing a multi-factor system.
C: Kerberos is an authentication scheme that uses tickets (unique keys) embedded within messages.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 14-18.

QUESTION 34:

Which of the following is the MOST secure form of authentication?

A. Kerberos
B. Biometrics
C. Smart Cards

D. Username/password

Answer: B

Explanation:
Biometrics is the use of authenticating a user by scanning on of their unique physiological body parts. Just like in the movies, a user places their hand on a finger print scanner or they put their eyes against a retinal scanner. If the image matches what's on the database, it authenticates the user. Since a persons fingerprint, blood vessel print, or retinal image is unique the only way the system can authenticate is if the proper user is there. The only way an unauthorized user to get access is to physically kidnap the authorized user and force them through the system. For this reason, biometrics are the strongest (and the costliest) for of authentication.
Incorrect answers:
A: Kerberos are not as reliable as biometrics.
C: Smart Card authentication is one of the more secure forms of authentication but is not as secure as biometrics.
D: Usernames and passwords can be intercepted and are the least secure.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 18-19, 265

QUESTION 35:

Which of the following is the LEAST secure form of authentication?

A. Kerberos
B. Biometrics
C. Smart Cards
D. Username/password

Answer: D

Explanation:
Usernames and passwords can be intercepted and are the least secure.
Incorrect answers:
A: Kerberos are not as reliable as biometrics.
B: Biometrics is the use of authenticating a user by scanning on of their unique physiological body parts. For this reason, biometrics are the strongest (and the costliest) for of authentication.
C: Smart Card authentication is one of the more secure forms of authentication but is not as secure as biometrics.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 18-19, 265

QUESTION 36:

One of the below is considered as the MOST secure way of authentication, which is it?

A. Biometric
B. Password
C. Token
D. Ticket Granting

Answer: A

Explanation:
Biometric authentication systems take advantage of an individual's unique physical characteristics in order to authenticate that person's identity. Various forms of biometric authentication include face, voice, eye, hand, signature, and fingerprint, each have their own advantages and disadvantages. When combined with the use of a PIN it can provide two factors authentication.

QUESTION 37:

One of the below is an extremely critical attribute of a biometrics system, which is it?

A. Acceptability
B. Accuracy
C. Throughput
D. Reliability

Answer: B

QUESTION 38:

Which of the following uses unencrypted username and passwords?

A. PAP
B. CHAP
C. RADIUS
D. MS-CHAP

Answer: A
Password Authentication Protocol (PAP) uses username and password combinations but transmits the username and password in clear text.
Incorrect Answers:
B: Challenge Handshake Authentication Protocol (CHAP) does not use username and password combinations but uses a Shared Secret which is stored locally in clear text.

However, the Shared Secret is not transmitted over the network.
C: Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting service that uses username and password combinations but transmits the username and password in encrypted form.
D: Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) does not use username and password combinations but uses a Shared Secret which is stored locally in encrypted form.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 338-340.

QUESTION 39:

Which of the following uses encrypted username and passwords?

A. PAP
B. CHAP
C. RADIUS
D. MS-CHAP

Answer: C
Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting service that uses username and password combinations but transmits the username and password in encrypted form.
Incorrect Answers:
A: Password Authentication Protocol (PAP) uses username and password combinations but transmits the username and password in clear text.
B: Challenge Handshake Authentication Protocol (CHAP) does not use username and password combinations but uses a Shared Secret which is stored locally in clear text. However, the Shared Secret is not transmitted over the network.
D:
Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) does not use username and password combinations but uses a Shared Secret which is stored locally in encrypted form.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 338-340.

QUESTION 40:

Which of the following statements regarding authentication protocols is FALSE?

A. PAP is insecure because usernames and passwords are sent over the network in clear text.
B. CHAP is more secure than PAP because it encrypts usernames and passwords before they are sent over the network.

C. RADIUS is a client/server-based system that provides authentication, authorization, and accounting services for remote dial-up access.
D. MS-CHAP version 1 is capable of mutual authentication of both the client and the server.

Answer: D
MS-CHAP version 2 is capable of mutual authentication but MS-CHAP version 1 is not capable of mutual authentication.
Incorrect Answers:
A: Password Authentication Protocol (PAP) uses username and password combinations but transmits the username and password in clear text.
B: Challenge Handshake Authentication Protocol (CHAP) does not send username and password combinations but uses a Shared Secret which is stored locally in clear text.
D: Remote Authentication Dial-In User Service (RADIUS) is an authentication and accounting service for dial-up access.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 338-340.

QUESTION 41:

Choose the password generator that uses a challenge-response method for authentication.

A. Asynchronous password generator
B. Synchronous password generator
C. Cryptographic keys
D. Smart cards

Answer: B

Explanation:
An synchronous password generator, has an authentication server that generates a challenge (a large number or string) which is encrypted with the private key of the token device and has that token device's public key so it can verify authenticity of the request (which is independent from the time factor). That challenge can also include a hash of transmitted data, so not only can the authentication be assured; but also the data integrity.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION 42:

Which password management system best provides for a system with a large number of users?

A. Self service password reset management systems
B. Locally saved passwords management systems
C. multiple access methods management systems
D. synchronized passwords management systems

Answer: A

Explanation:
A self service password reset is a system where if an individual user forgets their password, they can reset it on their own (usually by answering a secret question on a web prompt, then receiving a new temporary password on a pre-specified email address) without having to call the help desk. For a system with many users, this will significantly reduce the help desk call volume.
Incorrect answers:
B: Locally saved password management systems are not designed for large networks and large amounts of users.
C: A multi-factor system is when two or more access methods are included as part of the authentication process. This would be impractical with a large number of users.
D: Synchronized password would pose a serious threat for any amount of users.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION 43:

Which of the following is a solution that you can implement to protect against an intercepted password?

A. Implement a VPN (Virtual Private Network).
B. Implement PPTP (Point-to-Point Tunneling Protocol).
C. Implement a one time password.
D. Implement complex password requirements.

Answer: C

Explanation:
A one time password is simply a password that has to be changed every time you log on; effectively making any intercepted password good for only the brief interval of time before the legitimate user happens to login themselves. So by chance, if someone were to intercept a password it would probably already be expired, or be on the verge of expiration within a matter of hours.
Incorrect Answers:
A: VPN tunnels through the Internet to establish a link between two remote private networks. However, these connections are not considered secure unless a tunneling protocol, such as PPTP, and an encryption protocol, such as IPSec is used.
B: PPTP is a tunneling protocol. It does not provide encryption which could mitigate

against interception.
D: Complex password requirements make the password more difficult to crack using brute force and dictionary attacks. However, it does not protect the password from being intercepted.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 22-26, 105-108.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.112-114

QUESTION 44:

Which definition best defines what a challenge-response session is?

A. A challenge-response session is a workstation or system that produces a random challenge string that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
B. A challenge-response session is a workstation or system that produces a random login ID that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
C. A challenge-response session is a special hardware device used to produce random text in a cryptography system.
D. A challenge-response session is the authentication mechanism in the workstation or system that does not determine whether the owner should be authenticated.

Answer: A

Explanation:
A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.
Incorrect Answers:
B: Challenge-response sessions do not generate random login IDs but random challenges.
C: Challenge-response sessions do not rely on special hardware devices to generate the challenge or the response. The computer system does this.
D: The purpose of authentication is to determine if the owner should be authenticated.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 20-21.
http://www.webopedia.com/TERM/C/challenge_response.html

QUESTION 45:

A very important capability or element must be deployed before the Kerberos

authentication system functions properly. What is it?

A. You must deploy dynamic IP (Internet Protocol) routing protocols for routers and servers.
B. You must deploy separate network segments for the realms.
C. You must deploy Token authentication devices.
D. You must deploy time synchronization services for clients and servers.

Answer: D

Explanation:
Time synchronization is crucial because Kerberos uses server and workstation time as part of the authentication process. Kerberos authentication uses a Key Distribution Center (KDC) to orchestrate the process. The KDC authenticates the principle (which can be a user, a program, or a system) and provides it with a ticket. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another principle. Kerberos is quickly becoming a common standard in network environments. Its only significant weakness is that the KDC can be a single point of failure. If the KDC goes down, the authentication process will stop.
Incorrect answers:
A: This is irrelevant.
B: Time synchronization is more important in Kerberos.
C: Tokens devices are not as essential to Kerberos as time synchronization is.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.17

QUESTION 46:

For which reason are clocks used in Kerberos authentication?

A. Clocks are used to ensure proper connections.
B. Clocks are used to ensure that tickets expire correctly.
C. Clocks are used to generate the seed value for the encryptions keys.
D. Clocks are used to both benchmark and specify the optimal encryption algorithm.

Answer: B

Explanation:
The actual verification of a client's identity is done by validating an authenticator. The authenticator contains the client's identity and a timestamp.
To insure that the authenticator is up-to-date and is not an old one that has been captured by an attacker, the timestamp in the authenticator is checked against the current time. If the timestamp is not close enough to the current time (typically within five minutes) then the authenticator is rejected as invalid. Thus, Kerberos requires your system clocks to be

loosely synchronized (the default is 5 minutes, but it can be adjusted in Version 5 to be whatever you want).
Incorrect answers:
A: Proper connections are not dependant on time synchronization.
C: Generating seed value for encryption keys are not time related.
D: You do not need time synchronization for benchmark and set optimal encryption algorithms.
References:
http://www.faqs.org/faqs/kerberos-faq/general/section-22.html

---

QUESTION 47:

Choose the important consideration tobear in mind on the Kerberos authentication system.

A. Kerberos authentication is at risk to man in the middle attacks.
B. Kerberos authentication tickets can be spoofed by hackers using replay attacks.
C. Kerberos authentication requires a centralized managed database of all user account and resource passwords.
D. Kerberos authentication uses clear text passwords.

Answer: C

Explanation:
If the key distribution centre is down, all of other systems dependent on those keys won't be able to function.
Incorrect answers:
A: This will not prevent Kerberos from functioning.
B: This will not prevent Kerberos from functioning.
D: Encryption is part of Kerberos. No passwords are sent in clear text.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.17

QUESTION 48:

You work as the security administrator at Certkiller .com. You must implement an authentication protocol that uses only encrypted passwords during the authentication process.
Choose the authentication protocol that accomplishes this.

A. PPTP (Point-to-Point Tunneling Protocol)
B. SMTP (Simple Mail Transfer Protocol)
C. Kerberos
D. CHAP (Challenge Handshake Authentication Protocol)

Answer: D

Explanation:
CHAP is commonly used to encrypt passwords. It provides for on-demand authentication within an ongoing data transmission, that is repeated at random intervals during a session. The challenge response uses a hashing function derived from the Message Digest 5 (MD5) algorithm.
Incorrect answers:
A: PPTP is a tunneling protocol. It does not provide encryption.
B: SMTP is a protocol for sending e-mail between SMTP servers.
C: Kerberos is an authentication scheme that uses tickets (unique keys) embedded within messages.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.112

QUESTION 49:

The CHAP (Challenge Handshake Authentication Protocol) sends a logon request from the client to the server, and the server sends a challenge back to the client. At which stage does the CHAP protocol perform the handshake process? Choose the best complete answer.

A. At the stage when the connection is established and at whichever time after the connection has been established.
B. At the stage when the connection is established and when the connection is disconnected.
C. At the stage when the connection is established.
D. At the stage when the connection is disconnected.

Answer: A

Explanation:
CHAP performs the handshake process when first establishing a connection; and then at random intervals during the transaction session.
Incorrect answers:
B: CHAP also challenges for a handshake during the connection.
C: CHAP also challenges for a handshake after the initial connection.
D: CHAP also challenges for a handshake during connections.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.15

QUESTION 50:

Choose the method of authentication which is the most COSTLY method.

A. Passwords
B. Tokens
C. Biometrics
D. Shared secrets

Answer: C

Explanation:
Biometrics
These technologies are becoming more reliable, and they will become widely used over the next few years. Many companies use smart cards as their primary method of access control. Implementations have been limited in many applications because of the high cost associated with these technologies.
Incorrect answers:
A, B, D: Passwords, tokens and shared secrets are in use in most companies since they are not as costly as biometrics.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 18-19, 265

QUESTION 51:

Which of the following are nonessential protocols and services?

A. Network News Transfer Protocol (NNTP)
B. TFTP (Trivial File Transfer Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

Answer: B

Explanation:
TFTP is a nonessential protocol.
Incorrect answers:
A, C, D: These are usually essential protocols.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp.20-21.

QUESTION 52:

Which of the following are nonessential protocols and services?

A. Mail
B. Web

C. NetBios services
D. Network News Transfer Protocol (NNTP)

Answer: C

Explanation:
NetBios is a nonessential protocol.
Incorrect answers:
A, B, D: These are usually essential protocols.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp.20-21.

QUESTION 53:

Which of the following protocols are not recommended due to them supplying passwords and information over the network?

A. Network News Transfer Protocol (NNTP)
B. SNMP (Simple Network Management Protocol).
C. Domain Name Service (DNS)
D. Internet Control Message Protocol (ICMP)

Answer: B

Explanation:
SNMP (Simple Network Management Protocol) is a nonessential protocol.
Incorrect answers:
A, C, D: These are usually essential protocols and are more secure.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp.20-21.

QUESTION 54:

Which of the following protocols are not recommended due to them supplying passwords and information over the network?

A. Network News Transfer Protocol (NNTP)
B. Internet Control Message Protocol (ICMP)
C. NetBios services
D. Network News Transfer Protocol (NNTP)

Answer: C

Explanation:

NetBios services are a nonessential protocol.
Incorrect answers:
A, B, D: These are usually essential protocols and are more safe and secure.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp.20-21.

QUESTION 55:

From the recommendations below, which is considered the best method for securing a web browser?

A. Do not upgrade web browsers because new versions have a tendency to contain more security flaws.
B. Disable all unused features of the web browser.
C. Only use a VPN (Virtual Private Network) connection to connect to the Internet.
D. Deploy a filtering policy for unknown and illegal websites that you do not want users to access.

Answer: B

Explanation:
Features that make web surfing more exciting like: ActiveX, Java, JavaScript, CGI scripts, and cookies all pose security concerns. Disabling them (which is as easy as setting your browser security level to High) is the best method of securing a web browser, since its simple, secure, and within every users reach.
Incorrect answers:
A: As newer versions one expects them to be better than the predecessors. However, this is not the best method to secure a web browser.
C: VPN tunnels through the Internet to establish a link between two remote private networks. However, these connections are not considered secure unless a tunneling protocol, such as PPTP, and an encryption protocol, such as IPSec is used.
D: This does not represent the best method for securing a web browser.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.112-114

QUESTION 56:

Choose the figure which represents the number of ports in the TCP/IP (Transmission Control Protocol/Internet Protocol) which are vulnerable to being scanned, attacked, and exploited.

A. 32 ports
B. 1,024 ports
C. 65,535 ports

D. 16,777,216 ports

Answer: C

Explanation:
Internet Control Message Protocol (ICMP) abuse and port scans represent known attack signatures. The Ping utility uses ICMP and is often used as a probing utility prior to an attack or may be the attack itself. If a host is being bombarded with ICMP echo requests or other ICMP traffic, this behavior should set off the IDS. Port scans are a more devious form of attack/reconnaissance used to discover information about a system. Port scanning is not an attack but is often a precursor to such activity. Port scans can be sequential, starting with port 1 and scanning to port 65535, or random. A knowledge-based IDS should recognize either type of scan and send an alert.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 7
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 67

QUESTION 57:

A DNS (Domain Name Service) server uses a specific port number. Choose this port number from the options.

A. Port 32
B. Port 1,024
C. Port 65,535
D. Port 16,777,216

Answer: B

Explanation:
Port 53 is used for Domain Name System (DNS) Name Queries
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Appendix B
http://www.iana.org/assignments/port-numbers

QUESTION 58:

Which of the following access attacks would involve listening in on someone's network?

A. Eavesdropping
B. Snooping
C. Interception

D. None of the above

Answer: A

Explanation:
Eavesdropping is the process of listening in or overhearing parts of a conversation.
Eavesdropping also includes attackers listening in on your network traffic.
Incorrect answers:
B: Snooping occurs when someone looks through your files in the hopes of finding something interesting.
C: a passive interception would involve someone who routinely monitors network traffic. Active interception might include putting a computer system between the sender and receiver to capture information as it is sent. From the perspective of interception, this process is a covert process.
D: There are only three types of access attacks and therefore must be one of the three.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 59:

Which of the following access attacks would involve looking through your files in the hopes of finding something interesting?

A. Interception
B. Snooping
C. Eavesdropping
D. None of the above

Answer: B

Explanation:
Snooping occurs when someone looks through your files in the hopes of finding something interesting.
Incorrect answers:
A
: a passive interception would involve someone who routinely monitors network traffic. Active interception might include putting a computer system between the sender and receiver to capture information as it is sent. From the perspective of interception, this process is a covert process
C: Eavesdropping is the process of listening in or overhearing parts of a conversation. Eavesdropping also includes attackers listening in on your network traffic.
D: There are only three types of access attacks and therefore must be one of the three.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 60:

Which of the following access attacks would involve putting a computer system between the sender and receiver to capture information?

A. Snooping
B. Eavesdropping
C. Interception
D. None of the above

Answer: C

Explanation:
A passive interception would involve someone who routinely monitors network traffic. Active interception might include putting a computer system between the sender and receiver to capture information as it is sent. From the perspective of interception, this process is a covert process
Incorrect answers:
A: Snooping occurs when someone looks through your files in the hopes of finding something interesting.
B: Eavesdropping is the process of listening in or overhearing parts of a conversation. Eavesdropping also includes attackers listening in on your network traffic.
D: There are only three types of access attacks and therefore must be one of the three.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 61:

Which of the following definitions would be correct regarding Eavesdropping?

A. Placing a computer system between the sender and receiver to capture information.
B. Someone looking through your files.
C. Listening or overhearing parts of a conversation
D. Involve someone who routinely monitors network traffic.

Answer: C

Explanation:
Eavesdropping is the process of listening in or overhearing parts of a conversation. Eavesdropping also includes attackers listening in on your network traffic.
Incorrect answers:
A: This access attack is known as Active Inception.
B: This access attack is known as Snooping
D: This access attack is known as Passive Inception.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 62:

Which of the following definitions would be correct regarding Snooping?

A. Involve someone who routinely monitors network traffic
B. Someone looking through your files.
C. Placing a computer system between the sender and receiver to capture information
D. Listening or overhearing parts of a conversation.

Answer: B

Explanation:
Snooping occurs when someone looks through your files in the hopes of finding something interesting
Incorrect answers:
A: This access attack is known as Passive Inception
C: This access attack is known as Eavesdropping
D: This access attack is known as Active Inception
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 63:

Which of the following definitions would be correct regarding Active Inception?

A. Someone looking through your files
B. Involve someone who routinely monitors network traffic
C. Listening or overhearing parts of a conversation
D. Placing a computer system between the sender and receiver to capture information.

Answer: D

Explanation:
Active interception might include putting a computer system between the sender and receiver to capture information as it is sent. From the perspective of interception, this process is a covert process.
Incorrect answers:
A: This access attack is known as Snooping
B: This access attack is known as Passive Inception
C: This access attack is known as Eavesdropping
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 64:

Which of the following definitions would be correct regarding Passive Inception?

A. Placing a computer system between the sender and receiver to capture information
B. Listening or overhearing parts of a conversation
C. Involve someone who routinely monitors network traffic
D. Someone looking through your files.

Answer: C

Explanation:
From the perspective of interception, this process is a covert process. A passive interception would involve someone who routinely monitors network traffic.
Incorrect answers:
A: This access attack is known as Active Inception
B: This access attack is known as Eavesdropping
D: This access attack is known as Snooping
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 65:

One of the below options are correct regarding the DoS (Denial of Service) attack?

A. Prevention access to resources by users authorized to use those resources.
B. Use of multiple computers to attack a single organization.
C. Placing a computer system between the sender and receiver to capture information
D. Listening or overhearing parts of a conversation.

Answer: A

Explanation:
Denial of service (DoS) attacks prevents access to resources by users authorized to use those resources. An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers. DoS attacks are very common on the Internet.
Incorrect answers:
B: This attack is known as the DDoS (Distributed Denial of Service)
C: This access attack is known as Active Inception
D: This access attack is known as Eavesdropping.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 66:

One of the below options are correct regarding the DDoS (Distributed Denial of Service) attack?

A. Listening or overhearing parts of a conversation
B. Placing a computer system between the sender and receiver to capture information
C. Use of multiple computers to attack a single organization
D. Prevention access to resources by users authorized to use those resources

Answer: C

Explanation:
A relatively new type of DoS attack called a Distributed Denial of Service Attack (DDoS) uses multiple computers to attack a single organization. These attacks exploit the inherent weaknesses of dedicated networks such as DSL and cable.
Incorrect answers:
A: This access attack is known as Eavesdropping
B: This access attack is known as Active Inception
D: This attack is known as the DoS (Denial of Service)
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 67:

Which of the following attacks would involve bringing down an e-commerce website to prevent or deny usage by legitimate customers?

A. DoS
B. Inception
C. DDoS
D. Eavesdropping

Answer: A

Explanation:
Denial of service (DoS) attacks prevents access to resources by users authorized to use those resources. An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers. DoS attacks are very common on the Internet.
Incorrect answers:
B: A passive interception would involve someone who routinely monitors network

traffic. Active interception might include putting a computer system between the sender and receiver to capture information as it is sent. From the perspective of interception, this process is a covert process.
C: A relatively new type of DoS attack called a Distributed Denial of Service Attack (DDoS) uses multiple computers to attack a single organization. These attacks exploit the inherent weaknesses of dedicated networks such as DSL and cable
D: Eavesdropping is the process of listening in or overhearing parts of a conversation. Eavesdropping also includes attackers listening in on your network traffic
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 68:

Which of the following attacks would involve multiple computers attacking a single organization?

A. Inception
B. Eavesdropping
C. DoS
D. DDoS

Answer: D

Explanation:
A relatively new type of DoS attack called a Distributed Denial of Service Attack (DDoS) uses multiple computers to attack a single organization. These attacks exploit the inherent weaknesses of dedicated networks such as DSL and cable.
Incorrect answers:
A
: A passive interception would involve someone who routinely monitors network traffic. Active interception might include putting a computer system between the sender and receiver to capture information as it is sent. From the perspective of interception, this process is a covert process.
B: Eavesdropping is the process of listening in or overhearing parts of a conversation. Eavesdropping also includes attackers listening in on your network traffic.
C: Denial of service (DoS) attacks prevents access to resources by users authorized to use those resources. An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers. DoS attacks are very common on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 51-52.

QUESTION 69:

Why do programmers make use of back doors?

A. For maintenance purposes
B. For observation purposes
C. For complicated operating systems
D. For all of the above mentioned

Answer: D

Explanation:
During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the code is running.
Incorrect answers:
A, B, C: These are vital points to think about for using back doors but are not true reasons to embark in the use of back doors. Not just any system can make use of back doors.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 53

QUESTION 70:

Which of the following common attacks would involve writing a fake logon program?

A. Back Door Attacks
B. Spoofing
C. Man In The Middle
D. Replay Attack

Answer: B

Explanation:
A spoofing attack is simply an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack. A very common spoofing attack that was popular for many years involved a programmer writing a fake logon program. This program would prompt the user for a user ID and password.
Incorrect answers:
A: During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the code is running. The back doors are stripped out of the code when it is moved to production.
C: This type of attack is also an access attack, but it can be used as the starting point for a modification attack. The method used in these attacks places a piece of software between a server and the user. The software intercepts and then sends the information to the

server. The server responds back to the software, thinking it is the legitimate client.
D: These attacks occur when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password information is sent between the client and the authentication system. The attacker can capture this information and replay it again later.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 54-57.

QUESTION 71:

Which of the following common attacks would allow them to examine operations inside the code while the code is running?

A. Replay Attack
B. Man In The Middle
C. Spoofing
D. Back Door Attacks

Answer: D

Explanation:
During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the code is running. The back doors are stripped out of the code when it is moved to production
Incorrect answers:
A: These attacks occur when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password information is sent between the client and the authentication system. The attacker can capture this information and replay it again later
B: This type of attack is also an access attack, but it can be used as the starting point for a modification attack. The method used in these attacks places a piece of software between a server and the user. The software intercepts and then sends the information to the server. The server responds back to the software, thinking it is the legitimate client.
C: A spoofing attack is simply an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack. A very common spoofing attack that was popular for many years involved a programmer writing a fake logon program. This program would prompt the user for a user ID and password.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 54-57.

QUESTION 72:

Which of the following common attacks would attack places a piece of software

between a server and the user?

A. Spoofing
B. Back Door Attacks
C. Man In The Middle
D. Replay Attack

Answer: C

Explanation:
A spoofing attack is simply an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack. A very common spoofing attack that was popular for many years involved a programmer writing a fake logon program. This program would prompt the user for a user ID and password
Incorrect answers:
A: This type of attack is also an access attack, but it can be used as the starting point for a modification attack. The method used in these attacks places a piece of software between a server and the user. The software intercepts and then sends the information to the server. The server responds back to the software, thinking it is the legitimate client
B: During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the code is running. The back doors are stripped out of the code when it is moved to production
C: These attacks occur when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password information is sent between the client and the authentication system. The attacker can capture this information and replay it again later.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 54-57.

QUESTION 73:

Which of the following common attacks would the attacker capture the user's login information and replay it again later?

A. Back Door Attacks
B. Replay Attack
C. Spoofing
D. Man In The Middle

Answer: C

Explanation:
These attacks occur when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password

information is sent between the client and the authentication system. The attacker can capture this information and replay it again later
Incorrect answers:
A: During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the code is running. The back doors are stripped out of the code when it is moved to production
B: This type of attack is also an access attack, but it can be used as the starting point for a modification attack. The method used in these attacks places a piece of software between a server and the user. The software intercepts and then sends the information to the server. The server responds back to the software, thinking it is the legitimate client
C: A spoofing attack is simply an attempt by someone or something to masquerade as someone else. This type of attack is usually considered an access attack. A very common spoofing attack that was popular for many years involved a programmer writing a fake logon program. This program would prompt the user for a user ID and password
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 54-57.

QUESTION 74:

Which of the following protocols suites are responsible for IP addressing?

A. ARP
B. IP
C. IGMP
D. ICMP

Answer: B

Explanation:
IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP.
Incorrect answers:
A
: ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address.
C: IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts.
D: ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 62-63.

QUESTION 75:

Which of the following protocol suite are responsible for resolving IP addressing?

A. IGMP
B. IP
C. ARP
D. ICMP

Answer: C

Explanation:
ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
Incorrect answers:
A: IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts.
B: IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP.
D: ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 62-63.

QUESTION 76:

Which of the following protocols suites are primarily responsible for managing IP multicast groups?

A. ARP
B. IP
C. ICMP
D. IGMP

Answer: D

Explanation:
IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts

Incorrect answers:
A: ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
B: IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP
C: ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 62-63.

QUESTION 77:

Which of the following protocol suites provides maintenance and reporting functions?

A. ICMP
B. IGMP
C. ARP
D. IP

Answer: A

Explanation:
ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Incorrect answers:
B: IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts
C: ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
D: IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 62-63.

QUESTION 78:

Which of the following definitions suits the protocols suite IP?

A. Responsible for IP addressing
B. Responsible for resolving IP addressing
C. Responsible for managing IP multicast groups
D. Provides maintenance and reporting functions

Answer: A

Explanation:
IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP
Incorrect answers:
B: ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
C: IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts
D: ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 62-63

QUESTION 79:

Which of the following definitions suits the protocols suite ARP?

A. Responsible for IP addressing
B. Responsible for resolving IP addressing
C. Responsible for managing IP multicast groups
D. Provides maintenance and reporting functions

Answer: B

Explanation:
ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
Incorrect answers:
A: IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP
C: IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts

D: ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 62-63

QUESTION 80:

Which of the following definitions suits the protocols suite IGMP?

A. Responsible for IP addressing
B. Responsible for resolving IP addressing
C. Responsible for managing IP multicast groups
D. Provides maintenance and reporting functions

Answer: C

Explanation:
IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts
Incorrect answers:
A: IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP also fragments and reassembles message packets. IP only routes information; it does not verify it for accuracy. Accuracy checking is the responsibility of TCP
B: ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
D: ICMP (Internet Control Management Protocol) provides maintenance and reporting functions. ICMP is the protocol used by the PING program.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 62-63

QUESTION 81:

Which of the following definitions suits the protocols suite ICMP?

A. Responsible for IP addressing
B. Responsible for resolving IP addressing
C. Responsible for managing IP multicast groups
D. Provides maintenance and reporting functions

Answer: D

Explanation:
ICMP (Internet Control Management Protocol) provides maintenance and reporting

functions. ICMP is the protocol used by the PING program
Incorrect answers:
A: IP (Internet Protocol) is a routable protocol, and it is responsible for IP addressing. IP verify it for accuracy. Accuracy
checking is the responsibility of TCP
B: ARP (Address Resolution Protocol) is responsible for resolving IP addresses to Network Interface layer addresses, including hardware addresses. ARP can resolve an IP address to a Media Access Control (MAC) address
C: IGMP (Internet Group Management Protocol) is responsible primarily for managing IP multicast groups. IP multicasts can send messages or packets to a specified group of hosts.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 62-63

QUESTION 82:

Which of the following options is the correct sequence for the TCP Three-Way Handshake?

A. Host A, SYN, SYN/ACK, ACK, Host B
B. Host A, ACK, SYN/ACK, Host B, SYN
C. Host A, SYN/ACK, ACK, SYN, Host B
D. Host A, ACK, SYN/ACK, SYN, Host B

Answer: A

Explanation:
A host called a client originates this connection. The client sends a TCP segment, or message, to the server. This client segment includes an Initial Sequence Number (ISN) for the connection and a window size. The server responds with a TCP segment that contains its Initial Sequence Number, and a window size indicating its buffer or window size. The client then sends back an acknowledgement of the server's sequence number.
Incorrect answers:
B, C, D: They are all incorrect sequences and would never work and therefore do not take part in the Three-Way Handshake.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 66.

QUESTION 83:

Which of the following attacks are being referred to if the attack involves the attacker gaining access to a host in the network and logically disconnecting it?

A. TCP/IP Hijacking

B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

Answer: A

Explanation:
TCP/IP hijacking, also called active sniffing, involves the attacker gaining access to a host in the network and logically disconnecting it from the network. The attacker then inserts another machine with the same IP address.
This happens quickly and gives the attacker access to the session and to all of the information on the original system. The server will not know this has occurred and will respond as if the client is trusted.
Incorrect answers:
B: UDP attack attacks either a maintenance protocol or a UDP service in order to overload services and initiate a DoS situation. UDP attacks can also exploit UDP protocols. UDP packets are not connection-oriented and do not require the synchronization process described in the previous section. UDP packets, however, are susceptible to interception, and UDP can be attacked
C
: ICMP attacks occur by triggering a response from the ICMP protocol when it responds to a seemingly legitimate maintenance request. ICMP supports maintenance and reporting in a TCP/IP network. ICMP is part of the IP level of the protocol suite. Several programs, including PING, use the ICMP protocol. Until fairly recently, ICMP was regarded as a benign protocol that was incapable of very much damage.
D: Smurf attacks are becoming common and can create pure havoc in a network. A smurf attack uses IP spoofing and broadcasting to send a PING to a group of hosts in a network. When a host is pinged, it sends back ICMP message traffic information indicating status to the originator. If a broadcast is sent to a network, all of the hosts will answer back to the ping. The result of this is an overload of the network and the target system
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 72-73.

QUESTION 84:

Which of the following protocols is used to transmit e-mail between the two e-mail servers?

A. Post Office Protocol, version 3 (POP3)
B. Simple Mail Transfer Protocol (SMTP)
C. Internet Control Message Protocol (ICMP)
D. Internet Message Access Protocol, version 4 (IMAP4)

Answer: B
SMTP (Simple Mail Transfer Protocol) is used for sending e-mail messages.

Incorrect Answers:
A, D: POP3 and IMAP4 transmit e-mail between the e-mail client and the e-mail server.
C: ICMP (Internet Control Message Protocol) is used for network management and control. It provides error testing and reporting for TCP/IP.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 78-79, 116, 207.

QUESTION 85:

Which of the following protocols is used to transmit e-mail between an e-mail client and an e-mail server?

A. Hypertext Transfer Protocol (HTTP)
B. Post Office Protocol, version 3 (POP3)
C. Simple Mail Transfer Protocol (SMTP)
D. Internet Control Message Protocol (ICMP)

Answer: B
POP3 and IMAP4 transmit e-mail between the e-mail client and the e-mail server.
Incorrect Answers:
A: HTTP is the protocol that is used by a web browser to communicate with web severs. It is not used for transmitting e-mail between the e-mail client and the e-mail server.
C: SMTP (Simple Mail Transfer Protocol) is used for transmitting e-mail messages from one e-mail server to another, not between the e-mail server and the e-mail client.
D: ICMP (Internet Control Message Protocol) is used for network management and control. It provides error testing and reporting for TCP/IP.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 78-79, 116, 207.

QUESTION 86:

Which of the following provides error reporting in TCP/IP?

A. NNTP
B. ICMP
C. IGMP
D. SNMP

Answer: B
ICMP (Internet Control Message Protocol) is used for network management and control. It provides error testing and reporting for TCP/IP.
Incorrect Answers:
A: NNTP (Network News Transfer Protocol) is used to access Usenet news servers. It does not provide error reporting.

C: IGMP (Internet Group Management Protocol) is used to manage IP multicast sessions. It does not provide error reporting.
D: SNMP (Simple Network Management Protocol) is a communications protocol that collects information about network devices, such as hubs, routers, and bridges. It does not provide error reporting.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 112-118.

QUESTION 87:

Which of the following is used to manage IP multicast sessions?

A. NNTP
B. ICMP
C. IGMP
D. SNMP

Answer: C
IGMP (Internet Group Management Protocol) is used to manage IP multicast sessions. It does not provide error reporting.
Incorrect Answers:
A: NNTP (Network News Transfer Protocol) is used to access Usenet news servers. It does not manage IP multicast sessions.
B: ICMP (Internet Control Message Protocol) is used for network management and control. It provides error testing and reporting for TCP/IP. It does not manage IP multicast sessions
D: SNMP (Simple Network Management Protocol) is a communications protocol that collects information about network devices, such as hubs, routers, and bridges. It does not manage IP multicast sessions.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 112-118.

QUESTION 88:

Which of the following protocols is used to transmit data between a web browser and a web server?

A. SSH
B. HTTP
C. SFTP
D. IMAP4

Answer: B
HTTP is the protocol that is used by a web browser to communicate with web severs.

Incorrect Answers:
A: The SSH protocol is used to establish a secure Telnet session over TCP/IP.
C: SFTP transmit data securely between tan FTP client and an FTP server.
D: IMAP4 transmit e-mail between the e-mail client and the e-mail server. It does not transmit data between a web browser and a web server.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 297.

QUESTION 89:

Which of the following is a secure alternative to Telnet?

A. SSH
B. HTTP
C. SFTP
D. IMAP4

Answer: A
Telnet is a terminal emulation protocol that provides a remote logon to another host over the network. The SSH protocol is used to establish a secure Telnet session over TCP/IP. It can thus be sued instead of Telnet.
Incorrect Answers:
B: HTTP is the protocol that is used by a web browser to communicate with web severs. This is not a function of Telnet.
C: SFTP transmit data securely between tan FTP client and an FTP server. This is not a function of Telnet.
D: IMAP4 transmit e-mail between the e-mail client and the e-mail server. This is not a function of Telnet.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 297.

QUESTION 90:

Which of the following provides remote logon over the Internet?

A. Telnet
B. SSH
C. PPP
D. IMAP4

Answer: C
The PPP protocol is used to establish a connection over point-to-point links such as dial-up and dedicated leased lines that are used to connect to the Internet.
Incorrect Answers:

A, B: Telnet is a terminal emulation protocol that provides a remote logon to another host over the network, not over the Internet. The SSH protocol is used to establish a secure Telnet session over TCP/IP. It can thus be sued instead of Telnet.
D: IMAP4 transmit e-mail between the e-mail client and the e-mail server. This is not a function of Telnet.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 297.

QUESTION 91:

Which of the following CANNOT be used for remote connections?

A. Telnet
B. SSH
C. PPP
D. IMAP4

Answer: D
IMAP4 transmit e-mail between the e-mail client and the e-mail server. This does not allow remote connections.
Incorrect Answers:
A, B: Telnet is a terminal emulation protocol that provides a remote logon to another host over the network, not over the Internet. The SSH protocol is used to establish a secure Telnet session over TCP/IP. It can thus be sued instead of Telnet.
C: The PPP protocol is used to establish a remote connection over point-to-point links such as dial-up and dedicated leased lines that are used to connect to the Internet.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 117, 297.

QUESTION 92:

Which of the following attacks are being referred to if packets are not connection-oriented and do not require the synchronization process?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

Answer: B

Explanation:
UDP attack attacks either a maintenance protocol or a UDP service in order to overload services and initiate a DoS situation. UDP attacks can also exploit UDP protocols. UDP

packets are not connection-oriented and do not require the synchronization process described in the previous section. UDP packets, however, are susceptible to interception, and UDP can be attacked
Incorrect answers:
A: TCP/IP hijacking, also called active sniffing, involves the attacker gaining access to a host in the network and logically disconnecting it from the network. The attacker then inserts another machine with the same IP address. This happens quickly and gives the attacker access to the session and to all of the information on the original system. The server will not know this has occurred and will respond as if the client is trusted.
C: ICMP attacks occur by triggering a response from the ICMP protocol when it responds to a seemingly legitimate maintenance request. ICMP supports maintenance and reporting in a TCP/IP network. ICMP is part of the IP level of the protocol suite. Several programs, including PING, use the ICMP protocol. Until fairly recently, ICMP was regarded as a benign protocol that was incapable of very much damage.
D: Smurf attacks are becoming common and can create pure havoc in a network. A smurf attack uses IP spoofing and broadcasting to send a PING to a group of hosts in a network. When a host is pinged, it sends back ICMP message traffic information indicating status to the originator. If a broadcast is sent to a network, all of the hosts will answer back to the ping. The result of this is an overload of the network and the target system
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 72-73.

QUESTION 93:

Which of the following attacks are being referred to if it was regarded as a benign protocol that was incapable of very much damage?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

Answer: C

Explanation:
ICMP attacks occur by triggering a response from the ICMP protocol when it responds to a seemingly legitimate maintenance request. ICMP supports maintenance and reporting in a TCP/IP network. ICMP is part of the IP level of the protocol suite. Several programs, including PING, use the ICMP protocol. Until fairly recently, ICMP was regarded as a benign protocol that was incapable of very much damage.
Incorrect answers:
A: TCP/IP hijacking, also called active sniffing, involves the attacker gaining access to a host in the network and logically disconnecting it from the network. The attacker then inserts another machine with the same IP address. This happens quickly and gives the attacker access to the session and to all of the information on the original system. The

server will not know this has occurred and will respond as if the client is trusted.
B: UDP attack attacks either a maintenance protocol or a UDP service in order to overload services and initiate a DoS situation. UDP attacks can also exploit UDP protocols. UDP packets are not connection-oriented and do not require the synchronization process described in the previous section. UDP packets, however, are susceptible to interception, and UDP can be attacked
D: Smurf attacks are becoming common and can create pure havoc in a network. A smurf attack uses IP spoofing and broadcasting to send a PING to a group of hosts in a network. When a host is pinged, it sends back ICMP message traffic information indicating status to the originator. If a broadcast is sent to a network, all of the hosts will answer back to the ping. The result of this is an overload of the network and the target system
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 72-73.

QUESTION 94:

Which of the following attacks uses IP spoofing and broadcasting to send a PING to a group of hosts in a network?

A. TCP/IP Hijacking
B. UDP Attack
C. ICMP Attacks
D. Smurf Attacks

Answer: D

Explanation:
Smurf attacks are becoming common and can create pure havoc in a network. A smurf attack uses IP spoofing and broadcasting to send a PING to a group of hosts in a network. When a host is pinged, it sends back ICMP message traffic information indicating status to the originator. If a broadcast is sent to a network, all of the hosts will answer back to the ping. The result of this is an overload of the network and the target system
Incorrect answers:
A: TCP/IP hijacking, also called active sniffing, involves the attacker gaining access to a host in the network and logically disconnecting it from the network. The attacker then inserts another machine with the same IP address. This happens quickly and gives the attacker access to the session and to all of the information on the original system. The server will not know this has occurred and will respond as if the client is trusted.
B: UDP attack attacks either a maintenance protocol or a UDP service in order to overload services and initiate a DoS situation. UDP attacks can also exploit UDP protocols. UDP packets are not connection-oriented and do not require the synchronization process described in the previous section. UDP packets, however, are susceptible to interception, and UDP can be attacked
C: ICMP attacks occur by triggering a response from the ICMP protocol when it responds to a seemingly legitimate maintenance request. ICMP supports maintenance and

reporting in a TCP/IP network. ICMP is part of the IP level of the protocol suite. Several programs, including PING, use the ICMP protocol. Until fairly recently, ICMP was regarded as a benign protocol that was incapable of very much damage.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 72-73.

QUESTION 95:

One of the below is a description for a password cracker, which one is it?

A. A program that can locate and read a password file.
B. A program that provides software registration passwords or keys.
C. A program that performs comparative analysis.
D. A program that obtains privileged access to the system.

Answer: C

Explanation:
In a dictionary crack, L0phtCrack encrypts (i.e., hashes) all the passwords in a dictionary file you specify and compares every result with the password hash. If L0phtCrack finds any matches, it knows the password is the dictionary word. L0phtCrack comes with a default dictionary file, words-english. You can download additional files from the Internet or create a custom file. In the Tools Options dialog box, you can choose to run the dictionary attack against the LANMAN password hash, the NT LAN Manager (NTLM) password hash, or both (which is the default).
In a hybrid crack, L0phtCrack extends the dictionary crack by appending numbers or symbols to each word in the dictionary file. For example, in addition to trying "Galileo," L0phtCrack also tries "Galileo24," "13Galileo," "?Galileo," "Galileo!," and so on. The default number of characters L0phtCrack tries is two, and you can change this number in the Tools Options dialog box.
In a brute-force crack, L0phtCrack tries every possible combination of characters in a character set. L0phtCrack offers four character sets, ranging from alpha only to all alphanumeric plus all symbol characters. You can choose a character set from the Character Set drop-down box in the Tools Options dialog box or type a custom character set in the Character Set drop-down box. L0phtCrack saves custom sets in files with an .lc extension. You can also specify a character set in the password file, as the example in Figure 2 shows.

QUESTION 96:

One of the below attacks focus on the cracking of passwords, which one is it?

A. SMURF
B. Spamming
C. Teardrop

D. Dictionary

Answer: D

Explanation:
Dictionaries may be used in a cracking program to determine passwords. A short dictionary attack involves trying a list of hundreds or thousands of words that are frequently chosen as passwords against several systems. Although most systems resist such attacks, some do not. In one case, one system in five yielded to a particular dictionary attack.

QUESTION 97:

Which of the below options would you consider as a program that constantly observes data traveling over a network?

A. Smurfer
B. Sniffer
C. Fragmenter
D. Spoofer

Answer: B

Explanation:
A sniffer is a program and/or device that monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect

---

QUESTION 98:

Choose the concept that represents the scenario where a string of data sent to a buffer is larger than the buffer is capable of handling.

A. Brute Force attack
B. Buffer overflows
C. Man in the middle attack
D. Blue Screen of Death attack
E. SYN flood attack
F. Spoofing attack

Answer: B

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave

the system sending the data with temporary access to privileged levels in the attacked system.
Incorrect answers:
A: A brute force attack is an attempt to guess passwords until a successful guess occurs.
C: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
D
: WinNuke or Blue Screen of Death is a Windows-based attack that affects only computers running Windows NT 3.51 or 4. It is caused by the way the Windows NT TCP/IP stack handles bad data in the TCP header.
Instead of returning an error code or rejecting the bad data, it sends NT to the Blue Screen of Death (BSOD). Figuratively speaking, the attack "nukes" the computer.
E: A SYN flood attack forces a victim system to use up one of its finite number of connections for each connection the initiator opens. Because these requests arrive so quickly, the victim system has no time to free dangling, incomplete connections before all its resources are consumed.
F: A spoofing attack is simply an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 135

QUESTION 99:

From the listing of attacks, choose the attack which exploits session initiation between a Transport Control Program (TCP) client and server within a network?

A. Buffer Overflow attack
B. SYN attack
C. Smurf attack
D. Birthday attack

Answer: B

Explanation:
SYN flood is a DoS attack in which the hacker sends a barrage of SYN packets. The receiving station tries to respond to each SYN request for a connection, thereby tying up all the resources. All incoming connections are rejected until all current connections can be established. Change this if you want but in the SYN flood the hacker sends a SYN packet to the receiving station with a spoofed return address of some broadcast address on their network. The receiving station sends out this SYN packets (pings the broadcast address) which causes multiple servers or stations to respond to the ping, thus overloading the originator of the ping (the receiving station). Therefore, the hacker may send only 1 SYN packet, whereas the network of the attacked station is actually what does the barrage of return packets and overloads the receiving station.
Incorrect answers:

A: Buffer overflow attacks, as the name implies, attempt to put more data (usually long input strings) into the buffer than it can hold.
C: A smurf attack is an attack caused by pinging a broadcast to a number of sites with a false "from" address. When the hosts all respond to the ping, they flood the false "from" site with echoes.
D: A birthday attack is a probability method of finding similar keys in MD5.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 530

QUESTION 100:

From the listing of attacks, which uses either improperly formatted MTUs (Maximum Transmission Unit) or the ICMP (Internet Control Message Protocol) to crash the targeted network computer?

A. A man in the middle attack
B. A smurf attack
C. A Ping of Death attack
D. TCP SYN (Transmission Control Protocol / Synchronized) attack

Answer: C

Explanation: The Ping of Death attack involved sending IP packets of a size greater than 65,535 bytes to the target computer. IP packets of this size are illegal, but applications can be built that are capable of creating them. Carefully programmed operating systems could detect and safely handle illegal IP packets, but some failed to do this.
Remember that MTU packets that are bigger than the maximum size the underlying layer can handle are fragmented into smaller packets, which are then reassembled by the receiver. For ethernet style devices, the MTU is typically 1500.
Incorrect Answers
A: A man in the middle attack allows a third party to intercept and replace components of the data stream.
B: The "smurf" attack, named after its exploit program, is one of the most recent in the category of network-level attacks against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses, all of it having a spoofed source address of a victim.
D:
In a TCP SYN attack a sender transmits a volume of connections that cannot be completed. This causes the connection queues to fill up, thereby denying service to legitimate TCP users.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 52

QUESTION 101:

From the listing of attacks, which analyzes how the operating system (OS) responds to specific network traffic, in an attempt to determine the operating system running in your networking environment?

A. Operating system scanning.
B. Reverse engineering.
C. Fingerprinting
D. Host hijacking.

Answer: C

Explanation:
Fingerprinting is the act of inspecting returned information from a server (ie. One method is ICMP Message quoting where the ICMP quotes back part of the original message with every ICMP error message. Each operating system will quote definite amount of message to the ICMP error messages. The peculiarity in the error messages received from various types of operating systems helps us in identifying the remote host's OS.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 67

QUESTION 102:

Which of the following correctly specifies what malicious port scanning attempts to determine?

A. Attempts to determine the computer name
B. Attempts to fingerprint the operating system
C. Attempts to determine the physical cabling topology of a network
D. Attempts to determine user IDs and passwords

Answer: B

Explanation:
Malicious port scanning is an attempt to find an unused port that the system won't acknowledge. Several programs now can use port scanning for advanced host detection and operating system fingerprinting. With knowledge of the operating system, the hacker can look up known vulnerabilities and exploits for that particular system.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 3

QUESTION 103:

One fingerprinting technique works by exploiting this piece of information:
Operating systems differ when it comes to the amount of information that is quoted when ICMP (Internet Control Message Protocol) errors occur.
Choose the fingerprinting technique that exploits this piece of information.

A. TCP (Transmission Control Protocol) options.
B. ICMP (Internet Control Message Protocol) error message quenching.
C. Fragmentation handling.
D. ICMP (Internet Control Message Protocol) message quoting.

Answer: D
ICMP Message quoting: The ICMP quotes back part of the original message with every ICMP error message. Each operating system will quote definite amount of message to the ICMP error messages. The peculiarity in the error messages received from various types of operating systems helps us in identifying the remote host's OS.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 70

QUESTION 104:

From the listing of attack types, which exploits poor programming techniques or lack of code review?

A. CGI (Common Gateway Interface) scripts
B. Birthday attacks
C. Buffer overflow attacks
D. Dictionary attacks

Answer: C

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system. This exploitation is usually a result of a programming error in the development of the software.
Incorrect answers:
A: CGI scripts were used to capture data from a user using simple forms. Vulnerabilities in CGI are its inherent ability to do what it is told. If a CGI script is written to wreak havoc (or carries extra code added to it by a miscreant) and it is executed, your systems will suffer.
B: A birthday attack is a probability method of finding similar keys in MD5.
D: A dictionary attack cycles through known words in a dictionary file, testing the user's password to see whether a match is made.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 135

QUESTION 105:

From the listing of attacks, choose the attack which misuses the TCP (Transmission Control Protocol) three-way handshake process, in an attempt to overload network servers, so that authorized users are denied access to network resources?

A. Man in the middle attack
B. Smurf attack
C. Teardrop attack
D. SYN (Synchronize) attack

Answer: D

Explanation:
SYN flood is a DoS attack in which the hacker sends a barrage of SYN packets. The receiving station tries to respond to each SYN request for a connection, thereby tying up all the resources. All incoming connections are rejected until all current connections can be established.
Incorrect answers:
A: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
B: A smurf attack is an attack caused by pinging a broadcast to a number of sites with a false "from" address. When the hosts all respond to the ping, they flood the false "from" site with echoes.
C: A teardrop attack is a DoS attack that uses large packets and odd offset values to confuse the receiver and help facilitate a crash.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 530

QUESTION 106:

From the list below, choose the exploit that can be considered a DoS attack because more traffic than what the node can handle is flooded to that node.

A. Ping of death
B. Buffer overflow
C. Logic bomb
D. Smurf attack

Answer: B

Explanation:

Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Incorrect answers:
A: The ping of death crashes a system by sending Internet Control Message Protocol (ICMP) packets that are larger than the system can handle.
C: A logic bomb is a special kind of virus or Trojan horse that is set to go off following a preset time interval, or following a pre-set combination of keyboard strokes. Some unethical advertisers use logic bombs to deliver the right pop-up advertisement following a keystroke, and some disgruntled employees set up logic bombs to go off to sabotage their company's computers if they feel termination is imminent.
D: A smurf attack uses IP spoofing and broadcasting to send a ping to a group of hosts in a network.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 135

QUESTION 107:

From the list below, choose the security breach that typically results in authorized users being unable to access the system. This security breach usually does not result in theft of data or any other form of security loss.

A. CRL
B. DoS
C. ACL
D. MD2

Answer: B

Explanation:
DOS attacks prevent access to resources by users authorized to use those resources. An attacker may attempt to bring down an e-commerce website to prevent or deny usage by legitimate customers.
Incorrect answers:
A: A Certificate Revocation List (CRL) is a list of digital certificate revocations that must be regularly downloaded to stay current.
C: An Access Control List (ACL) is a list of rights that an object has to resources in the network.
D: A Message Digest Algorithm (MDA) is an algorithm that creates a hash value. The hash value is also used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 53

QUESTION 108:

Which type of network attack are Loki, NetCaZ, Masters Paradise and NetBus examples of?

A. Brute force attack
B. Spoofing attack
C. Back door attack
D. Man in the middle attack

Answer: C

Explanation:
Since backdoor's are publicly marketed/distributed software applications, they are characterized by having a trade name.
Incorrect answers:
A: A brute force attack is an attempt to guess passwords until a successful guess occurs.
B: A spoofing attack is simply an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.
D: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.54

QUESTION 109:

TCP/IP (Transmission Control Protocol/Internet Protocol) session hijacking exploits a specific, inherent characteristic of the TCP/IP protocol. Which is it?

A. TCP/IP does not have an authentication mechanism, and allows a clear text password of 16 bytes.
B. TCP/IP allows packets to be tunneled to an alternate network.
C. TCP/IP does not have an authentication mechanism, and allows connectionless packets from whichever person.
D. TCP/IP allows a packet to be spoofed and added into a data stream, and in so doing allows commands to be executed on the remote host.

Answer: D

Explanation:
TCP/IP's connection orientated nature, and lack of natural security makes it easy to hijack a session by spoofing.
Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.69

QUESTION 110:

For which network attack can you implement these types of ingress/egress traffic filtering to reduce the likelihood of the attack occurring?
1. A packet arriving at the network must have a destination address from the internal network.
2. A packet arriving at the network must not have a source address of the internal network.
3. A packet arriving at the network or being sent from the network must not have a source address or destination address of a private address and must not have an address that is specified in RFC19lS reserved space.
4. A packet being sent from the network must have a source address from the internal network.
5. A packet being sent from the network must not have a destination address of the internal network.

A. SYN (Synchronize) flooding
B. Spoofing attacks
C. DoS (Denial of Service) attacks
D. Dictionary attacks

Answer: B

Explanation:
By having strict addressing filters, an adminstrator prevents a spoofed address from gaining access.
Incorrect answers:
A: A SYN flood forces a victim system to use up one of its finite number of connections for each connection the initiator opens.
C: Dos attacks can also be a result of SYN flooding.
D: A dictionary attack cycles through known words in a dictionary file, testing the user's password to see whether a match is made.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION 111:

From the list of attacks, which has to do with the misdirection of domain name resolution and Internet traffic?

A. DoS (Denial of Service) attacks
B. Spoofing attacks

C. Brute force attacks
D. Reverse DNS (Domain Name Service)

Answer: B

Explanation:
A spoofing attack is simply an attempt by someone or something masquerading as someone else.
Incorrect answers:
A: Denial of service(DoS) attacks prevent access to resources by users authorized to use those resources.
C: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period. It can be accomplished by applying every possible combination of characters that could be the key.
D: Reverse DNS involves using an IP address to find a domain name, rather than using a domain name to find an IP address (normal DNS). PTR records are used for the reverse lookup, and often this is used to authenticate incoming connections.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 56

QUESTION 112:

An attacker that launches an IP (Internet Protocol) spoofing attack against your network attempts to manipulate a specific field within an IP (Internet Protocol) packet. Which is it?

A. Version field.
B. Source address field.
C. Source port field.
D. Destination address field.

Answer: B

Explanation:
In IP Spoofing a hacker tries to gain access to a network by pretending his or her machine has the same network address as the internal network.
Incorrect answers:
The source port field is the port that is addressed on the destination.
The destination address field is the port to where data is being sent.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 515

QUESTION 113:

You work as the security administrator at Certkiller .com. While monitoring network traffic, you find that your domain name server is resolving the domain name to the incorrect IP (Internet Protocol) address. You discover that Internet traffic is being misdirected.
You immediately suspect that an intruder has launched a malicious attack against the network. Which type of network attack is in progress?

A. DoS (Denial of Service) attack
B. Spoofing attack
C. Brute force attack
D. Reverse DNS (Domain Name Service)

Answer: B

Explanation:
Spoofing is when you forge the source address of traffic, so it appears to come from somewhere else, preferably somewhere safe and trustworthy. Web spoofing is a process where someone creates a convincing copy of a legitimate website or a portion of the world wide web, so that when someone enters a site that they think is safe, they end up communicating directly with the hacker. To avoid this you should rely on certificates, IPSEC, and set up a filter to block internet traffic with an internal network address.
Incorrect answers:
A: Denial of service(DoS) attacks prevent access to resources by users authorized to use those resources.
C: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period. It can be accomplished by applying every possible combination of characters that could be the key.
D: Reverse DNS involves using an IP address to find a domain name, rather than using a domain name to find an IP address (normal DNS). PTR records are used for the reverse lookup, and often this is used to authenticate incoming connections.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 54

QUESTION 114:

You work as the security administrator at Certkiller .com. While monitoring network traffic, you find that an intruder has managed to access resources residing on your internal network.
You immediately attempt to find out where the attack is originating from. You discover that the source IP (Internet Protocol) addresses are originating from trusted networks
Which type of network attack is in progress?

A. Social engineering
B. TCP/IP (Transmission Control Protocol/Internet Protocol) hijacking

C. Smurfing
D. Spoofing attack

Answer: D

Explanation:
Spoofing is the process of trying to deceive, or to spoof, someone into believing that a source address is coming from somewhere else.
Incorrect answers:
A: Social engineering deals with the human aspect of gaining access and passwords.
B: TCP/IP hijacking requires an existing session.
C: Smurfing is a legitimate kind of DoS attack that does involve spoofing, however it doesn't match the above description.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 85-86.

QUESTION 115:

One type of network attack sends two different messages that use the same hash function to generate the same message digest. Which network attack does this?

A. Man in the middle attack.
B. Ciphertext only attack.
C. Birthday attack.
D. Brute force attack.

Answer: C

Explanation:
A birthday attack is based on the principle that amongst 23 people, the probability of 2 of them having the same birthday is greater the 50%. By that rational if an attacker examines the hashes of an entire organizations passwords, they'll come up with some common denominators.
Incorrect answers:
A: A man-in-the-middle attack is an attack that occurs when someone/thing that is trusted intercepts packets and retransmits them to another party.
B & D: Ciphertext can be used in brute force attacks as well. If the cryptographic formula is known, the attack can concentrate on breaking the cipher used more efficiently than pure guessing.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 312

QUESTION 116:

You can defend against a specific network attack by increasing the complexity and keyspace of a password. Which network attack is this?

A. Dictionary attack
B. Brute force attack
C. Inference
D. Frontal

Answer: B

Explanation:
A brute force attack is when a computer program try's EVERY single keystroke combination until it cracks the password. If you had a bike lock or a brief case with three combinations of numbers (0-9), there were 999 possible choices, so if you started at 000 and worked your way up you could attempt every number in about 20 minutes and eventually crack the lock. A computer keyboard has millions of possibilities, but since computers can enter thousands and even millions of keys a second, a brute force attack can be successful in a matter of hours. Each keyspace exponentially increases the possible answer choices, so passwords that are extremely short can be cracked within an hour but passwords beyond eight characters require time and computer resources that are usually beyond a brute force hackers patience and financial motives.
A dictionary attack is an attack that uses words from a database (dictionary) to test against passwords until a match is found. This is not a complexity issue.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 86

QUESTION 117:

You can defend against dictionary password cracks by enforcing a minimum length for passwords. What is the minimum recommended password length?

A. 6 characters in length.
B. 8 characters in length.
C. 10 characters in length.
D. 12 characters in length.

Answer: B

Explanation:
A dictionary attack is a preliminary brute force attempt at guessing a password. Dictionary attacks work on the principle that most people choose a simple word or phrase passwords can be hacked in a matter of hours. Since passwords become exponentially passwords can be hacked in a matter of hours. Since passwords become exponentially more difficult to crack with each character, passwords greater then 8 characters consume excessive time and resources to crack.

Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION 118:

You can defend against man in the middle attacks by implementing which of the following?

A. A virtual LAN (Local Area Network)
B. A GRE (Generic Route Encapsulation) tunnel IP-IP (Internet Protocol-within-Internet Protocol Encapsulation Protocol)
C. A PKI (Public Key Infrastructure)
D. An enforcement of badge system

Answer: C

Explanation:
PKI is a two-key system. Messages are encrypted with a public key. Messages are decrypted with a private key. If you want to send an encrypted message to someone, you would request their public key. You would encrypt the message using their public key and send it to them. They would then use their private key to decrypt the message.
Incorrect answers:
A
: This is a LAN that allows users on different switch ports to participate in their own network separate from, but still connected to, the other stations on the same or connected switch. Who is to say that the perpetrator is not one of the users in the private separate network?
B: PPTP encapsulates virtual network packets into PPP, which are, in turn, encapsulated into generic routing encapsulation (GRE) packets and transmitted in the form of IP datagrams between the parties. Meaning that after the tunnel is created data gets to be transferred, however, this does not prevent man in the middle attacks.
D: A smart card is a type of badge or card that gives you access to resources including buildings, parking lots, and computers. It contains information about your identity and access privileges. Each area or computer has a card scanner or a reader in which you insert your card. But this will not prevent man in the middle attacks.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 331

QUESTION 119:

You can defend against man in the middle attacks by implementing which of the following?

A. A firewall solution

B. Strong encryption
C. Strong authentication
D. Strong, hard-to-decipher passwords

Answer: B

Explanation:
Encryption makes the intercepted data unreadable to the interceptor.
Incorrect answers:
A: A firewall will not prevent a man in the middle attack.
C: Authentication only happens during logon and the attack could occur when already logged on. In some instances authentication is not present.
D: Passwords are usually only used when logging on. This is not a good enough defense.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 86

QUESTION 120:

You work as the security administrator at Certkiller .com. You have received instruction from the CIO to assess the company's vulnerability with regard to well-known network attacks.
All users of the Certkiller .com network have been issued with a token and 4-digit personal identification number (PIN), which they use to access their computers. The token works by performing off-line checking for the correct PIN.
Which type of network attack is Certkiller .com at risk to?

A. Birthday
B. Brute force
C. Man-in-the-middle
D. Smurf

Answer: B

Explanation: Brute force attacks are performed with tools that cycle through many possible character, number, and symbol combinations to guess a password. Since the token allows offline checking of PIN, the cracker can keep trying PINs until it is cracked.
Incorrect answers:
A: This type of attack is also an access attack, but it can be used as the starting point for a modification attack.
C: A man-in-the-middle attack is commonly used to gather information in transit between two hosts.
D: A smurf attack uses IP spoofing and broadcasting to send a ping to a group of hosts in a network.

Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter

---

QUESTION 121:

Which of the following definitions can be correctly fitted to the Polymorphic Virus?

A. Change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system.
B. It attaches itself to another file, such as a word processing document. It may also arrive as part of an e-mail for a free game, software, or other file. When activated and performs its task, it infects all of the word processing or template files. Consequently, every new file will carry the virus.
C. This virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the virus redirects commands around itself in order to avoid detection.
D. It attacks or bypasses the antivirus software installed on a computer. You can consider it as an anti-antivirus. It can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security

Answer: A

Explanation:
Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation.
Incorrect answers:
B: This virus is known as the Trojan Horse Virus
C: This virus is known as the Stealth Virus
D: This virus is known as the Retrovirus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 122:

Which of the following definitions can be correctly fitted to the Trojan Horse Virus?

A. Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation.

B. It attaches itself to another file, such as a word processing document. It may also arrive as part of an e-mail for a free game, software, or other file. When activated and performs its task, it infects all of the word processing or template files. Consequently, every new file will carry the virus.
C. This virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the virus redirects commands around itself in order to avoid detection.
D. It attacks or bypasses the antivirus software installed on a computer. You can consider it as an anti-antivirus. It can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security

Answer: B

Explanation:
A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files.
Incorrect answers:
A: This virus is known as the Polymorphic Virus
C: This virus is known as the Stealth Virus
D: This virus is known as the Retrovirus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 123:

Which of the following definitions can be correctly fitted to the Stealth Virus?
A.
Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation
B. It attaches itself to another file, such as a word processing document. It may also arrive as part of an e-mail for a free game, software, or other file. When activated and performs its task, it infects all of the word processing or template files. Consequently, every new file will carry the virus
C. This virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the virus redirects commands around itself in order to avoid detection
D. It attacks or bypasses the antivirus software installed on a computer. You can consider it as an anti-antivirus. It can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information

without your knowledge would leave you with a false sense of security

Answer: C

Explanation:
A stealth virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection
Incorrect answers:
A: This virus is known as the Polymorphic Virus
B: This virus is known as the Trojan Horse Virus
D: This virus is known as the Retrovirus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 124:

Which of the following definitions can be correctly fitted to the Retrovirus?
A.
Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation
B. It attaches itself to another file, such as a word processing document. It may also arrive as part of an e-mail for a free game, software, or other file. When activated and performs its task, it infects all of the word processing or template files. Consequently, every new file will carry the virus
C. This virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the virus redirects commands around itself in order to avoid detection
D. It attacks or bypasses the antivirus software installed on a computer. You can consider it as an anti-antivirus. It can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security

Answer: D

Explanation:
A retrovirus attacks or bypasses the antivirus software installed on a computer. You can consider a retrovirus as an anti-antivirus. Retroviruses can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense

of security. The virus may also directly attack an antivirus program to create bypasses for the virus.
Incorrect answers:
A: This virus is known as the Polymorphic Virus
B: This virus is known as the Trojan Horse Virus
C: This virus is known as the Stealth Virus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 125:

Which of the following definitions can be correctly fitted to the Multipartite Virus?

A. This virus attacks your system in multiple ways. This virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
B. This virus is designed to make itself difficult to detect or analyze. These viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C. This virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
D. This virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.

Answer: A

Explanation:
A Multipartite virus attacks your system in multiple ways. A multipartite virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue.
Incorrect answers:
B: This virus is known as the Armored Virus
C: This virus is known as the Companion Virus
D: This virus is known as the Phage Virus

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 126:

Which of the following definitions can be correctly fitted to the Armored Virus?

A. This virus attacks your system in multiple ways. This virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
B. This virus is designed to make itself difficult to detect or analyze. These viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C. This virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
D. This virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.

Answer: B

Explanation:
An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
Incorrect answers:
A: This virus is known as the Multipartite Virus
C: This virus is known as the Companion Virus
D: This virus is known as the Phage Virus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 127:

Which of the following definitions can be correctly fitted to the Companion Virus?

A. This virus attacks your system in multiple ways. This virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
B. This virus is designed to make itself difficult to detect or analyze. These viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C. This virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
D. This virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.

Answer: C

Explanation:
A companion virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
Incorrect answers:
A: This virus is known as the Multipartite Virus
B: This virus is known as the Armored Virus
D: This virus is known as the Phage Virus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 128:

Which of the following definitions can be correctly fitted to the Phage Virus?

A. This virus attacks your system in multiple ways. This virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
B. This virus is designed to make itself difficult to detect or analyze. These viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C. This virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
D. This virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.

Answer: D

Explanation:
A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.
Incorrect answers:
A: This virus is known as the Multipartite Virus
B: This virus is known as the Armored Virus
C: This virus is known as the Companion Virus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 129:

Which of the following definitions can be correctly fitted to the Macro Virus?

A. These programs in the document are called macros. A macro can tell your word processor to spellcheck your document automatically when it opens viruses can infect all of the documents on your system and spread to other systems using mail or other methods. Macro viruses are the fastest growing exploitation today
B. This virus is designed to make itself difficult to detect or analyze. These viruses will

cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C. This virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
D. This virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.

Answer: A

Explanation:
A macro virus exploits the enhancements made too many application programs. Programs such as Word or Excel allow programmers to expand the capability of the application. Word for example, supports a mini-BASIC programming language that allows files to be manipulated automatically. These programs in the document are called macros. A macro can tell your word processor to spellcheck your document automatically when it opens. Macro viruses can infect all of the documents on your system and spread to other systems using mail or other methods. Macro viruses are the fastest growing exploitation today.
Incorrect answers:
B: This virus is known as the Armored Virus
C: This virus is known as the Companion Virus
D: This virus is known as the Phage Virus
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81

QUESTION 130:

To which of the following viruses does the characteristic when the virus attacks your system, display a message on your computer, and delete files on your system form part of?

A. Polymorphic Virus
B. Trojan Horse Virus
C. Stealth Virus
D. Retrovirus

Answer: A

Explanation:
Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation.
Incorrect answers:
B: A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files.
C: A stealth virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection
D
: A retrovirus attacks or bypasses the antivirus software installed on a computer. You can consider a retrovirus as an anti-antivirus. Retroviruses can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security. The virus may also directly attack an antivirus program to create bypasses for the virus.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 131:

To which of the following viruses does the characteristic when the virus activates and performs its
task, it infects all of the word processing or template files form part of?

A. Polymorphic Virus
B. Trojan Horse Virus
C. Stealth Virus
D. Retrovirus

Answer: B

Explanation:
A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or

template files.
Incorrect answers:
A: Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation.
C: A stealth virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection
D: A retrovirus attacks or bypasses the antivirus software installed on a computer. You can consider a retrovirus as an anti-antivirus. Retroviruses can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security. The virus may also directly attack an antivirus program to create bypasses for the virus.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 132:

To which of the following viruses does the characteristic when the virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive, form part of?

A. Polymorphic Virus
B. Trojan Horse Virus
C. Stealth Virus
D. Retrovirus

Answer: C

Explanation:
A stealth virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection.
Incorrect answers:
A: Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as

mutation.
B: A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files
D: A retrovirus attacks or bypasses the antivirus software installed on a computer. You can consider a retrovirus as an anti-antivirus. Retroviruses can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security. The virus may also directly attack an antivirus program to create bypasses for the virus.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 133:

To which of the following viruses does the characteristic when the virus bypasses the antivirus software installed on a computer, form part of?

A. Polymorphic Virus
B. Trojan Horse Virus
C. Stealth Virus
D. Retrovirus

Answer: D

Explanation:
A retrovirus attacks or bypasses the antivirus software installed on a computer. You can consider a retrovirus as an anti-antivirus. Retroviruses can directly attack your antivirus software and potentially destroy the virus definition file of your antivirus software. Destroying this information without your knowledge would leave you with a false sense of security. The virus may also directly attack an antivirus program to create bypasses for the virus.
Incorrect answers:
A: Polymorphic viruses change form in order to avoid detection. These types of viruses attack your system, display a message on your computer, and delete files on your system. The virus will attempt to hide from your antivirus software. Frequently, the virus will encrypt parts of itself to avoid detection. When the virus does this, it is referred to as mutation.
B: A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files
C: A stealth virus will attempt to avoid detection by masking itself from applications. It may attach itself to the boot sector of the hard drive. When a system utility or program

runs, the stealth virus redirects commands around itself in order to avoid detection. An infected file may report a file size different from what is actually present in order to avoid detection.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 134:

To which of the following viruses does the characteristic when the virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus
D. Phage Virus

Answer: A

Explanation:
A Multipartite virus attacks your system in multiple ways. A multipartite virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue.
Incorrect answers:
B: An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C:
A companion virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program
D: A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 135:

To which of the following viruses does the characteristic when the virus is designed to make itself difficult to detect or analyze. These viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus
D. Phage Virus

Answer: B

Explanation:
An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program.
Incorrect answers:
A
: A Multipartite virus attacks your system in multiple ways. A multipartite virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
C: A companion virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program
D: A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 136:

To which of the following viruses does the characteristic when the virus attaches itself to legitimate programs and then creates a program with a different file

extension. This file may reside in the temporary directory of your system form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus
D. Phage Virus

Answer: C

Explanation:
A companion virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program.
Incorrect answers:
A: A Multipartite virus attacks your system in multiple ways. A multipartite virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
B: An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
D: A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 137:

To which of the following viruses does the characteristic when the virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected, form part of?

A. Multipartite Virus
B. Armored Virus
C. Companion Virus

D. Phage Virus

Answer: D

Explanation:
A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.
Incorrect answers:
A: A Multipartite virus attacks your system in multiple ways. A multipartite virus may attempt to infect your boot sector, infect all of your executable files, and destroy your applications files. The hope here is that you will not be able to correct all of the problems and will allow the infestation to continue
B: An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C: A companion virus attaches itself to legitimate programs and then creates a program with a different file extension. This file may reside in the temporary directory of your system. When the user types the name of the legitimate program, the companion virus executes instead of the real program. This effectively hides the virus from the user. Many of the viruses that are used to attack Windows systems make changes to program pointers in the Registry so that it points to the infected program. The infected program may perform its dirty deed and then start the real program
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 80-81.

QUESTION 138:

Choose the most effective method of preventing computer viruses from spreading throughout the network.
You should require root/administrator access to run programs and applications.
You should enable scanning of all e-mail attachments.
You should prevent the execution of .vbs files.
You should install a host based IDS (Intrusion Detection System)

Answer: B

Explanation:
Viruses get into your computer in one of three ways. They may enter your computer on a contaminated floppy or CD-ROM, through e-mail, or as a part of another program.
Incorrect answers:
A: This will pose a more serious risk.

C: Preventing the execution of .vbs files will not prevent virus infection.
D: Host based IDS installation is not as effective as scanning e-mail attachments.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 76

QUESTION 139:

You work as the security administrator at Certkiller .com. You want to educate your users on how they should respond to an e-mail message that contains a warning about a virus that could have accidentally been sent in the page. You want to inform users on the actions they should perform when the message suggests that the user delete a specific file when it appears on the user's computer.
What should you do next?

A. Users must check for the file and delete it immediately.
B. Users must check for the file, delete it immediately, and then copy the e-mail message to all distribution lists.
C. Users must immediately report the contents of the e-mail message to the security administrator.
D. Users must simply ignore the message because it is a virus hoax. Users need perform no actions.

Answer: C

Explanation:
In such a scenario the most rational answer is to tell your network administrator. Most network administrators don't have much to do most of the day, so they live for an opportunity like this.
Incorrect Answers:
A: Deleting the file wouldn't be good, because deleting a file doesn't necessarily eliminate a problem, as it could put it to your email trash folder, or to your recycle bin. This will give you a false sense of security, and work against the process of containment.
B: Copying the email to all distribution lists, is another mistake, because if indeed the email does contain a virus, you'll only spread it.
D: Ignoring the problem isn't a good problem, although virus hoaxes are common, all it takes is one real virus to cause a mini-disaster.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79

QUESTION 140:

You work as the security administrator at Certkiller .com. You must document the procedure for handling computer virus infections.
Choose the action which you should specify to perform when receiving an e-mail

message warning of the existence of a virus on the system if a specific executable file exists?

A. First investigate the e-mail message as a possible hoax with a trusted anti-virus vendor.
B. First search for and delete the virus file.
C. First broadcast a message to the all users to alert them of the presence of a virus.
D. First locate and download a patch to repair the file.

Answer: A

Explanation:
If a virus threat is for real, the major anti-virus players like Symantec, McAfee, or Sophos will know about it before you, and they will have details on their sites.
Incorrect answers:
B: Searching for and deleting a file is not only a waste of time with today's OS's complex directory systems, but its also ineffective. One can miss a file, the file could be hidden, the wrong file can be deleted, and worst of all: when you delete a file it doesn't really get completely deleted, instead it gets sent to a 'recycle bin.'
C: Broadcasting an alert and creating panic isn't the right thing to do, because it will waste bandwidth, and perhaps terrorizing the users is the original intent of the attack.
D: The act of locating and downloading a patch isn't just time consuming, but there's a chance that the patch itself could be the virus, or the process of resetting the computer could activate the virus.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79

QUESTION 141:

Choose the statement that best details the difference between a worm and a Trojan horse?

A. Worms are distributed through e-mail messages while Trojan horses do not.
B. Worms self replicate while Trojan horses do not.
C. Worms are a form of malicious code while Trojan horses are not.
D. There is no difference between a worm and a Trojan horse.

Answer: B

Explanation:
A worm is different from a virus. Worms reproduce themselves, are self-contained and do not need a host application to be transported. The Trojan horse program may be installed as part of an installation process. They do not reproduce or self replicate.
Incorrect answers:
A: The main difference between a worm and a Trojan horse is not the way they are being

spread, but rather the self replicating aspect of worms.
C: Both can be malicious.
D: There are differences of which the worms ability to replicate itself is the distinguishing factor.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 83, 85

QUESTION 142:

Choose the malicious code which can distribute itself without using having to attach to a host file.

A. A virus.
B. A Trojan horse.
C. A logic bomb.
D. A worm.

Answer: D

Explanation:
Worms are dangerous because they can enter a system by exploiting a 'hole' in an operating system. They don't' need a host file, and they don't need any user intervention to replicate by themselves. Some infamous worms were: Morris, Badtrans, Nimda, and Code Red.
Incorrect answers:
A: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
B: Trojan horses are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program.
C: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION 143:

One type of malicious code can record system keystrokes in a text file and then e-mail it to the source. This code can delete system logs when a backup is performed, and at five day intervals.
Which type of malicious code can perform these actions?

A. A virus.
B. A back door.
C. A logic bomb.
D. A worm.

Answer: C

Explanation:
A logic bomb is a special kind of virus or Trojan horse that is set to go off following a preset time interval, or following a pre-set combination of keyboard strokes. Some unethical advertisers use logic bombs to deliver the right pop-up advertisement following a keystroke, and some disgruntled employees set up logic bombs to go off to sabotage their company's computers if they feel termination is imminent.
Incorrect answers:
A: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
B. B: A back door is not an attack in its own right; it allows a user to enter a system from a different interface or with different credentials.
D: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION 144:

You work as the security administrator at Certkiller .com. A system administrator named Rory Allen has recently resigned from the company.
You delete the user ID of Rory and immediately notice that the system has started deleting files.
Which type of malicious code is present on the network?

A. A logic bomb
B. A virus
C. A Trojan horse
D. A worm

Answer: A

Explanation:
A Logic bomb is a virus or Trojan horse that is built to go off when a particular event occurs or a certain amount of time passes, in this case when the system administrator user ID was deleted.
Incorrect answers:

B: A virus is a piece of software designed to infect a computer system. A virus may also damage the data on your hard disk, destroy your operating system, and possibly spread to other systems.
C: Trojan horses are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program.
D: Designed to take advantage of holes in security, worms are similar in function and behavior to viruses, Trojan horses, and logic bombs-with the exception that they are self-replicating.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 80

QUESTION 145:

Choose the statement which best defines the characteristics of a computer virus.

A. A computer virus is a find mechanism, initiation mechanism and can propagate.
B. A computer virus is a learning mechanism, contamination mechanism and can exploit.
C. A computer virus is a search mechanism, connection mechanism and can integrate.
D. A computer virus is a replication mechanism, activation mechanism and has an objective.

Answer: D

Explanation:
Replication mechanism: To replicate a virus needs to attach itself to the right code, where it can replicate and spread past security systems into other systems.
Activation mechanism: Most viruses require the user to actually do something. During the 80's and early 90's most viruses were activated when you booted from a floppy disk, or inserted a new floppy disk into an infected drive. Nowadays most computer virus's come as email forwards, and they require the user to execute.
Objective: many viruses have no objective at all, but some have the objective to delete data, hog up memory, or crash the system.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

QUESTION 146:

Which of the following options best describe how a social engineering attack occurs?

A. You are attacked and robbed of the necessary information
B. You are e-mailed by your "manager" and he is out of town and forgot his password and you send him the necessary information
C. A family member told your "best friend" the password

D. A colleague spies on you in a quest to get your password and acquires it by reading as you type.

Answer: B

Explanation:
Another very common approach is initiated by a phone call or an e-mail from your software vendor, telling you that they have a critical fix that must be installed on your computer system. If this patch is not installed right away, your system will crash and you will lose all of your data. For some reason, you have changed your maintenance account password and they can't log on. Your systems operator gives the password to the person. Bingo! You have been hit again.
Incorrect answers:
A, C, D: These do not fall under a typical social engineering attack.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 87

QUESTION 147:

What type of attacker would normally be interested in acquiring the login password information?

A. A technician
B. A network professional
C. A con artist
D. A secretary

Answer: C

Explanation:
Only a con artist would want this information to attack the system and insert a virus.
Incorrect answers:
A, B, D: A these people wouldn't need that information from a specific user, and wouldn't attack by means of social engineering.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 87

QUESTION 148:

Which of the following attacks would involve acquiring information by means of e-mail or phone call?

A. Phage Virus
B. Armored Virus

C. Trojan horse.
D. Social engineering.

Answer: D

Explanation:
Another very common approach is initiated by a phone call or an e-mail from your software vendor, telling you that they have a critical fix that must be installed on your computer system. If this patch is not installed right away, your system will crash and you will lose all of your data. For some reason, you have changed your maintenance account password and they can't log on. Your systems operator gives the password to the person. Bingo! You have been hit again.
Incorrect answers:
A: A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system
B: An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program
C: A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 57, 87

QUESTION 149:

What would be the best method to steer clear of all social engineering attacks?

A. Don't tell anyone your password
B. Get qualified staff
C. Use a more complex method of authentication
D. All of the above

Answer: D

Explanation:
All of the above are great measures to effectively stay away from social engineering attacks.
Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p.83

QUESTION 150:

Which of the following attacks are low-tech?

A. Trojan Horse
B. Social engineering
C. Phage Virus
D. Armored Virus

Answer: B

Explanation:
Social Engineering is a low-tech attack due to it requiring minimal software and computer skills.
Incorrect answers:
A: A Trojan horse attaches itself to another file, such as a word processing document. Trojan horses may also arrive as part of an e-mail for a free game, software, or other file. When the Trojan horse activates and performs its task, it infects all of the word processing or template files.
C: A Phage virus modifies and alters other programs and databases. The virus infects all of these files. The only way to remove this virus is to reinstall the programs that are infected. If you miss even a single incident of this virus on the victim system, the process will start again and infect the system.
D: An armored virus is designed to make itself difficult to detect or analyze. Armored viruses will cover themselves with "protective code" that stops debuggers or disassemblers from examining critical elements of the virus. The virus may be written in such a way that some aspects of the programming act as a decoy to distract analysis while the actual code hides in other areas in the program.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p.83

QUESTION 151:

Which attack is not dependant on computer skills and software?

A. Trojan Horse
B. Social engineering
C. Phage Virus
D. Armored Virus

Answer: B

Explanation:
Social Engineering is normally carried through by con men and not really hacking professionals.
Incorrect answers:
A, C, D: These viruses are all carried through by means of high-tech software programs and trained computer hacking specialists.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p.57-83

QUESTION 152:

Which of the following options would be FALSE regarding the reason why social engineering attacks are so successful?

A. The lack of qualified staff
B. The minimal chance of the attack occurring
C. The fact that passwords are given away too easily
D. The attacker being part of the company

Answer: D

Explanation:
The attacker wouldn't be part of the company due to all employees owning their own passwords and if the attacker was to attack the company it wouldn't be a social engineering attack.
Incorrect answers:
A, B, C: These options form a large part of carrying through a social engineering attack.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p.83

QUESTION 153:

Which of the following options would be TRUE regarding the reason why social engineering attacks are so successful?

A. A highly qualified staff
B. The minimal chance of the attack occurring
C. The fact that passwords are not given away easily
D. The attacker being part of the company

Answer: B

Explanation:
There is such a slim chance that the social engineering attack that very often it is the last

known risk to the company and is therefore ignored until it happens to the company.
Incorrect answers:
A, B, C: These options do not form part of carrying through a social engineering attack and would make the attack more difficult to carry through.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p.83

QUESTION 154:

You are a respected worker at Certkiller .com and your boss realizes that you attacked the system but you deny and persist in proving your innocence. You then realize you had a visit from an old colleague that was fired some time back. This person acquired all the necessary information to perform the attack. What type of attack is this person performing?

A. Trojan Horse
B. Social engineering
C. Phage Virus
D. Armored Virus

Answer: B

Explanation:
This person is a con man and he/she is absorbing as much information as possible to access the company as an employee.
Incorrect answers:
A, C, D: These viruses are all carried through by means of high-tech software programs and trained computer hacking specialists they therefore requires no contact with one of the companies employees.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 87
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 155:

Why would Social Engineering be regarded as a low-tech attack method?

A. Due to it not requiring intricate software
B. Due to it requiring a Highly trained software professional
C. Due to it requiring authentication only
D. Due to it requiring only verbal contact with someone from the firm

Answer: D

Explanation:
Social Engineering requires nothing but human intelligence in order to carry through an attack. A skilled con man could acquire this information easily just by talking.
Incorrect answers:
A, B, C: Social engineering requires no such things.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 83

QUESTION 156:

Which of the following attacks could be the most successful when the security technology is properly implemented and configured?

A. Logical attacks
B. Physical attacks
C. Social Engineering attacks
D. Trojan Horse attacks

Answer: C

Explanation:
Social Engineering attacks - In computer security systems, this type of attack is usually the most successful, especially when the security technology is properly implemented and configured. Usually, these attacks rely on the faults in human beings. An example of a social engineering attack has a hacker impersonating a network service technician. The serviceman approaches a low-level employee and requests their password for network servicing purposes. With smartcards, this type of attack is a bit more difficult. Most people would not trust an impersonator wishing to have their smartcard and PIN for service purposes.

QUESTION 157:

Choose the more common method used by intruders to gain unauthorized access to a networking system.

A. A brute force attack.
B. Logging of keystrokes.
C. Trojan horse.
D. Social engineering.

Answer: D

Explanation:
Social engineering is a process where an attacker attempts to acquire information about

your network and system by talking to people in the organization. A social engineering attack may occur over the phone, by e-mail, or by a visit.
The answer is not written in the book, but the easiest way to gain information would be social engineering.
Incorrect answers:
A: A brute force attack is an attempt to guess passwords until a successful guess occurs. This type of attack usually occurs over a long period.
B: Logging of keystrokes involves being at the workstation itself.
C: Trojan horses are programs that enter a system or network under the guise of another program. A Trojan horse may be included as an attachment or as part of an installation program. This involves too much effort compared to social engineering.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 57, 87

QUESTION 158:

You work as the security administrator at Certkiller .com. You must implement measures to protect Certkiller .com against a social engineering attack.
Which option best describes the measures you should implement?

A. Enforce the security policy, user education, and limit available information.
B. Enforce the security policy, user education, and implementing a firewall solution.
C. Enforce the security policy, implementing a firewall solution, and incident response.
D. Enforce the security policy, incident response, and system logging.

Answer: A

Explanation:
A seems to be the best answer. The other answers involving objects and social engineering are verbal attacks.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.83

QUESTION 159:

Choose the attack or malicious code that entails the theft of network passwords without the intruder using software tools.

A. Trojan programs.
B. Social engineering attacks.
C. Sniffing.
D. Hacking.

Answer: B

Explanation:
Social engineering is any means of using people to seek out information. These people practice espionage to: break in without detection, disguise themselves in, trick others into giving them access, or trick others into giving them information.
Incorrect answers:
A: A Trojan is a software "code" used to infiltrate a network, like the installation of zombie software used for remote control attacks.
C: Sniffing is an application that captures all traffic traveling past a network interface attached to some network.
D: Hacking is both hardware and software based.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 2

QUESTION 160:

Choose the attack or malicious code that cannot be prevented or deterred solely through using technical measures.

A. Dictionary attacks.
B. Man in the middle attacks.
C. DoS (Denial of Service) attacks.
D. Social engineering.

Answer: D

Explanation:
Because of human rights laws, it is unlawful to use technology to directly control people's emotions and behaviors. For this reason social engineering attacks cannot be deterred through technical means.
Incorrect answers:
A: To prevent this type of attack you need to put technical measures in place that forces users to make use of difficult passwords.
B: In this attack, a third system is placed between two hosts (electronically) already communicating or currently in the process of setting up a communication channel. Positive mutual authentication between the end points of a given session is probably the best way to prevent these attacks. Certificates can be used for mutual authentication.
C: The Denial of service attack can be deterred through technical means because they make a target machine unavailable as the result of a buffer overrun and a crash. These DoS attacks are not application specific and can be prevented by a firewall.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION 161:

You work as the security administrator at Certkiller .com. You are busy auditing the Certkiller .com wireless network.
You find an unauthorized Access Point under the desk of a user named Amy Walsh. Amy works in the Finance department. You confront Amy about this. Amy denies any knowledge of the unauthorized Access Point. Amy informs you though that a new friend has recently visited her, and on numerous occasions, at the company premises.
Choose the type of attack that was launched against Certkiller .com.

A. A SYN flood attcks.
B. A (DDos) Distributed Denial of Service attack.
C. A man in the Middle attack.
D. A TCP flood attack.
E. IP Spoofing.
F. Social Engineering
G. A replay attack
H. Phone tag
I. A halloween attack

Answer: F

Explanation:
Social engineering is a process where an attacker attempts to acquire information about your network and system by talking to people in the organization. A social engineering attack may occur over the phone, be e-mail, or by a visit.
Incorrect answers:
A: A SYN flood, forces a victim system to use up one of its finite number of connections for each connection the initiator opens.
B: Distributed denial of service attacks are multicell attacks.
C: A man-in-the-middle attack is commonly used to gather information in transit between two hosts.
D: In this attack, the source system sends a flood of SYN requests and never sends the final ACK, creating a half-open TCP session.
E: In IP Spoofing a hacker can impersonate a valid service by sourcing traffic using the service's IP address or name.
G: A replay attack is similar in part to a man-in-the-middle attack. In this instance, an attacker intercepts traffic between two end points and retransmits or replays it later.
H: Phone tag is not the same as social engineering.
I: You are not a victim of a Halloween attack in this case.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 87
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter3

QUESTION 162:

Why do many web servers provide message auditing, as do logon, system, and applications?

A. To view what a particular party is doing
B. To view who is logged on
C. To check for unusual events
D. To check the volume of information on the system

Answer: C

Explanation:
This is done to ensure that the system is running ok and isn't being attacked.
Incorrect answers:
A, B, D: These options do not form part of this process.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 88.

QUESTION 163:

An Auditing system is necessary to prevent attacks on what part of the system?

A. The files.
B. The operating system.
C. The systems memory
D. None of the above

Answer: A

Explanation:
Files can be deleted, scrambled, modified, and administrators can be prevented from knowing what is happening in the site
Incorrect answers:
B, C, D: These options do not form part of this process.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 88

QUESTION 164:

Which of the following statements regarding system auditing is TRUE?

A. System audit files must be reviewed regularly for unusual events.
B. System audit files are not susceptible to access or modification attacks.

C. System audit files don't hold much information.
D. System audit files do not contain critical systems information that attackers can use to gather more detailed data about your network.

Answer: A

Explanation:
System audit files are no good if they are not periodically reviewed for unusual events.
Incorrect answers:
B: System audit files can be deleted, scrambled, modified, and administrators can be prevented from knowing what is happening in the site.
C: The amount and volume of information these files contain can be overwhelming
D: These files may also be susceptible to access or modification attacks. These files often contain critical systems information including resource sharing, security status, etc. The attacker may be able to use this information to gather more detailed data about your network.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 88

QUESTION 165:

Which of the following statements regarding system auditing is TRUE?

A. System audit files may be susceptible to access or modification attacks.
B. System audit files do not need to be reviewed for unusual events.
C. System audit files don't hold much information.
D. System audit files do not contain critical systems information that attackers can use to gather more detailed data about your network.

Answer: A

Explanation:
System audit files can be deleted, scrambled, modified, and administrators can be prevented from knowing what is happening in the site
Incorrect answers:
B: System audit files can be deleted, scrambled, modified, and administrators can be prevented from knowing what is happening in the site.
C: The amount and volume of information these files contain can be overwhelming
D: These files may also be susceptible to access or modification attacks. These files often contain critical systems information including resource sharing, security status, etc. The attacker may be able to use this information to gather more detailed data about your network.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 88

QUESTION 166:

Choose the network mapping tool (scanner) which uses ICMP (Internet Control Message Protocol).

A. A port scanner.
B. A map scanner.
C. A ping scanner.
D. A share scanner.

Answer: C

Explanation:
Ping confirms a connection by sending and receiving ICMP packets.
Incorrect answers:
A: Port scan is an automated procedure of initiating sessions on every specified TCP port to see whether the host replies.
B: Map scanning is mainly used to identify targets for attack.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Chapter 3

QUESTION 167:

Which of the following actions can an attacker perform when network services are enabled on a target system?

A. An attacker can install a rootkit on the target system.
B. An attacker can check the services file.
C. An attacker can enable logging on the target system.
D. An attacker can run a port scan against the target system.

Answer: D

Explanation:
A TCP/IP network makes many of the ports available to outside users through the router. These ports will respond in a predictable manner when queried. An attacker can systematically query a network to determine which services and ports are open. This process is called port scanning, and it can reveal a great deal about your network. Port scans can be performed both internally and externally. Many routers, unless configured appropriately, will let all the protocols pass through them.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 69

QUESTION 168:

One type of port scan can determine which ports are in a listening state on the network, and can then perform a two way handshake.
Which type of port scan can perform this set of actions?

A. A TCP (transmission Control Protocol) SYN (Synchronize) scan
B. A TCP (transmission Control Protocol) connect scan
C. A TCP (transmission Control Protocol) fin scan
D. A TCP (transmission Control Protocol) null scan

Answer: A

Explanation:
In SYN scanning, a TCP SYN packet is sent to the port(s) to be scanned. If the port responds with a TCP SYN ACK packet, then the port is listening. If it replies with a TCP RST packet, then it is not.
Incorrect answers:
B: TCP connect scans are used to identify potential targets and services. This type of scan utilizes the full TCP three-way handshake.
C: When a basic firewall or router blocks other TCP scans, the TCP FIN scan can be used. It is used to identify listening TCP ports based on a response, or lack of a response, to a finish (FIN) packet.
D: A TCP scan designed to penetrate firewalls and filtering routers is the TCP NULL scan. A NULL scan is similar to the XMAS scan in that TCP sequence numbers are zero, but the NULL scan passes no flags at all.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

QUESTION 169:

Which of the following would originally link UNIX systems together in a dial-up environment?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. VPN
D. RADIUS (Remote Authentication Dial-In User Service)

Answer: A

Explanation:
SLIP was originally designed to connect UNIX systems together in a dial-up environment, and it supports only serial communications. SLIP is a very simple protocol that is used to pass TCP/IP traffic. The protocol is not secure, nor is it efficient. Many

systems still support SLIP strictly for legacy systems.
Incorrect answers:
B: PPP has largely replaced SLIP. PPP offers multiple protocol support including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP does not provide data security, but it does provide authentication using CHAP.
C: VPNs are used to make connections between private networks across a public network, such as the Internet. These connections are not guaranteed to be secure unless a tunneling protocol, such as PPTP, and an encryption system, such as IPSec, is used. A wide range of options, including proprietary technologies, is available for VPN support.
D: RADIUS is a mechanism that allows authentication of dial-in and other network connections. A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether or not an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 170:

Which of the following has largely replaced SLIP?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. VPN
D. RADIUS (Remote Authentication Dial-In User Service)

Answer: B

Explanation:
PPP has largely replaced SLIP. PPP offers multiple protocol support including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP does not provide data security, but it does provide authentication using CHAP.
Incorrect answers:
A: SLIP was originally designed to connect UNIX systems together in a dial-up environment, and it supports only serial communications. SLIP is a very simple protocol that is used to pass TCP/IP traffic. The protocol is not secure, nor is it efficient. Many systems still support SLIP strictly for legacy systems.
C: VPNs are used to make connections between private networks across a public network, such as the Internet. These connections are not guaranteed to be secure unless a tunneling protocol, such as PPTP, and an encryption system, such as IPSec, is used. A wide range of options, including proprietary technologies, is available for VPN support.
D: RADIUS is a mechanism that allows authentication of dial-in and other network connections. A RADIUS server can be managed centrally, and the servers that allow

access to a network can verify with a RADIUS server whether or not an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 171:

Which of the following are used to make connections between private networks across a public network?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. VPN
D. RADIUS (Remote Authentication Dial-In User Service)

Answer: C

Explanation:
VPNs are used to make connections between private networks across a public network, such as the Internet. These connections are not guaranteed to be secure unless a tunneling protocol, such as PPTP, and an encryption system, such as IPSec, is used. A wide range of options, including proprietary technologies, is available for VPN support.
Incorrect answers:
A: SLIP was originally designed to connect UNIX systems together in a dial-up environment, and it supports only serial communications. SLIP is a very simple protocol that is used to pass TCP/IP traffic. The protocol is not secure, nor is it efficient. Many systems still support SLIP strictly for legacy systems.
B: PPP has largely replaced SLIP. PPP offers multiple protocol support including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP does not provide data security, but it does provide authentication using CHAP.
D: RADIUS is a mechanism that allows authentication of dial-in and other network connections. A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether or not an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 172:

Which of the following is a mechanism that allows authentication of dial-in and other network connections?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. VPN
D. RADIUS (Remote Authentication Dial-In User Service)

Answer: D

Explanation:
RADIUS is a mechanism that allows authentication of dial-in and other network connections. A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether or not an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.
Incorrect answers:
A: SLIP was originally designed to connect UNIX systems together in a dial-up environment, and it supports only serial communications. SLIP is a very simple protocol that is used to pass TCP/IP traffic. The protocol is not secure, nor is it efficient. Many systems still support SLIP strictly for legacy systems.
B: PPP has largely replaced SLIP. PPP offers multiple protocol support including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP does not provide data security, but it does provide authentication using CHAP.
C: VPNs are used to make connections between private networks across a public network, such as the Internet. These connections are not guaranteed to be secure unless a tunneling protocol, such as PPTP, and an encryption system, such as IPSec, is used. A wide range of options, including proprietary technologies, is available for VPN support.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 173:

Which of the following definitions fit correctly to SLIP (Serial Line Internet Protocol)?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. is a mechanism that allows authentication of dial-in and other network connections

Answer: A

Explanation:

SLIP was originally designed to connect UNIX systems together in a dial-up environment, and it supports only serial communications. SLIP is a very simple protocol that is used to pass TCP/IP traffic. The protocol is not secure, nor is it efficient. Many systems still support SLIP strictly for legacy systems
Incorrect answers:
B: This refers to PPP
C: This refers to VPN
D: This refers to RADIUS
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 174:

Which of the following definitions fit correctly to PPP (Point-to-Point Protocol)?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. is a mechanism that allows authentication of dial-in and other network connections

Answer: B

Explanation:
PPP has largely replaced SLIP. PPP offers multiple protocol support including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP does not provide data security, but it does provide authentication using CHAP.
Incorrect answers:
A: This refers to SLIP
C:This refers to VPN
D: This refers to RADIUS
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 175:

Which of the following definitions fit correctly to VPN?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such

as the Internet
D. is a mechanism that allows authentication of dial-in and other network connections

Answer: C

Explanation:
VPNs are used to make connections between private networks across a public network, such as the Internet. These connections are not guaranteed to be secure unless a tunneling protocol, such as PPTP, and an encryption system, such as IPSec, is used. A wide range of options, including proprietary technologies, is available for VPN support.
Incorrect answers:
A: This refers to SLIP
B:This refers to PPP
D: This refers to RADIUS
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 176:

Which of the following definitions fit correctly to RADIUS?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. is a mechanism that allows authentication of dial-in and other network connections

Answer: D

Explanation:
RADIUS is a mechanism that allows authentication of dial-in and other network connections. A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether or not an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.
Incorrect answers:
A: This refers to SLIP
B:This refers to PPP
C: This refers to VPN
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 177:

Which of the following would allow credentials to be accepted from multiple methods, including Kerberos?

A. SLIP (Serial Line Internet Protocol)
B. PPP (Point-to-Point Protocol)
C. TACACS (Terminal Access Controller Access Control System)
D. RADIUS (Remote Authentication Dial-In User Service)

Answer: C

Explanation:
Terminal Access Controller Access Control System (TACACS) is a client/server-oriented environment, and it operates in a similar manner to RADIUS. The most current method or level of TACACS is TACACS/+. TACACS/+ allows credentials to be accepted from multiple methods, including Kerberos.
Incorrect answers:
A: SLIP was originally designed to connect UNIX systems together in a dial-up environment, and it supports only serial communications. SLIP is a very simple protocol that is used to pass TCP/IP traffic. The protocol is not secure, nor is it efficient. Many systems still support SLIP strictly for legacy systems.
B: PPP has largely replaced SLIP. PPP offers multiple protocol support including AppleTalk, IPX, and DECnet. PPP works with POTS, Integrated Services Digital Network (ISDN), and other faster connections such as T1. PPP does not provide data security, but it does provide authentication using CHAP.
D: RADIUS is a mechanism that allows authentication of dial-in and other network connections. A RADIUS server can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether or not an incoming caller is authorized. In a large network with many connections, this allows a single server to perform all authentications.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 178:

Which of the following definitions fit correctly to TACACS?

A. Is an older protocol that was used in early remote access environments
B. Has largely replaced SLIP and offers multiple protocol support including AppleTalk, IPX, and DECnet
C. are used to make connections between private networks across a public network, such as the Internet
D. It allows credentials to be accepted from multiple methods, including Kerberos.

Answer: D

Explanation:
Terminal Access Controller Access Control System (TACACS) is a client/server-oriented environment, and it operates in a similar manner to RADIUS. The most current method or level of TACACS is TACACS/+. TACACS/+ allows credentials to be accepted from multiple methods, including Kerberos.
Incorrect answers:
A: This refers to SLIP
B:This refers to PPP
C: This refers to VPN
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 179:

Which of the following tunneling protocols supports encapsulation in a single point-to-point environment?

A. PPTP
B. L2F
C. L2TP
D. SSH

Answer: A

Explanation:
PPTP supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. Once the negotiation is performed, the channel is encrypted
Incorrect answers:
B: 2F was created by Cisco as a method of creating tunnels primarily for dial-up connections. L2F is similar in capability to PPP and should not be used over WANs. L2F does provide authentication, but it does not provide encryption
C: Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: the Layer Two Tunneling Protocol (L2TP). L2TP is a hybrid of PPTP and L2F. L2TP is primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP.
D: Secure Shell (SSH) is a tunneling protocol originally designed for UNIX systems. SSH uses encryption to establish a secure connection between two systems. SSH also provides security equivalent programs such as Telnet, FTP, and many of the other communications-oriented programs under UNIX
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 180:

Which of the following tunneling protocols was created by Cisco as a method of creating tunnels primarily for dial-up connections?

A. PPTP
B. L2F
C. L2TP
D. SSH

Answer: B

Explanation:
2F was created by Cisco as a method of creating tunnels primarily for dial-up connections. L2F is similar in capability to PPP and should not be used over WANs. L2F does provide authentication, but it does not provide encryption
Incorrect answers:
A: PPTP supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. Once the negotiation is performed, the channel is encrypted
C: Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: the Layer Two Tunneling Protocol (L2TP). L2TP is a hybrid of PPTP and L2F. L2TP is primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP.
D: Secure Shell (SSH) is a tunneling protocol originally designed for UNIX systems. SSH uses encryption to establish a secure connection between two systems. SSH also provides security equivalent programs such as Telnet, FTP, and many of the other communications-oriented programs under UNIX
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 181:

Which of the following tunneling protocols is primarily a point-to-point protocol?

A. PPTP
B. L2F
C. L2TP
D. SSH

Answer: C

Explanation:
Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: the Layer Two Tunneling Protocol (L2TP). L2TP is a hybrid of PPTP and L2F. L2TP is primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP
Incorrect answers:
A: PPTP supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. Once the negotiation is performed, the channel is encrypted
B: 2F was created by Cisco as a method of creating tunnels primarily for dial-up connections. L2F is similar in capability to PPP and should not be used over WANs. L2F does provide authentication, but it does not provide encryption.
D: Secure Shell (SSH) is a tunneling protocol originally designed for UNIX systems. SSH uses encryption to establish a secure connection between two systems. SSH also provides security equivalent programs such as Telnet, FTP, and many of the other communications-oriented programs under UNIX
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 182:

Which of the following is a tunneling protocol originally designed for UNIX systems?

A. PPTP
B. L2F
C. L2TP
D. SSH

Answer: D

Explanation:
Secure Shell (SSH) is a tunneling protocol originally designed for UNIX systems. SSH uses encryption to establish a secure connection between two systems. SSH also provides security equivalent programs such as Telnet, FTP, and many of the other communications-oriented programs under UNIX
Incorrect answers:
A: PPTP supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. Once the negotiation is performed, the channel is encrypted

B: L2F was created by Cisco as a method of creating tunnels primarily for dial-up connections. L2F is similar in capability to PPP and should not be used over WANs. L2F does provide authentication, but it does not provide encryption.
C: Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: the Layer Two Tunneling Protocol (L2TP). L2TP is a hybrid of PPTP and L2F. L2TP is primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 183:

Which of the following definitions fit correctly to PPTP?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is a tunneling protocol originally designed for UNIX systems.

Answer: A

Explanation:
PPTP supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. Once the negotiation is performed, the channel is encrypted.
Incorrect answers:
B: This refers to L2F
C:This refers to L2TP
D: This refers to SSH
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 184:

From the options, which is a VPN (Virtual Private Network) protocol that operates at the Network layer (Layer 3) of the OSI (Open Systems Interconnect) model?

A. PPP (Point-to-Point Protocol) protocol
B. SSL (Secure Sockets Layer) protocol
C. L2TP (Layer Two Tunneling Protocol) protocol
D. IPSec (Internet Protocol Security)

Answer: D

Explanation:
IPSec works at the network layer of the OSI layer model and is a key factor in VPNs.
Incorrect answers:
A: PPP is a full-duplex line protocol that supersedes SLIP (Serial Line Internet Protocol) often used in dial-up connections operating at layer 2.
B: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
C: L2TP is a tunneling protocol that adds functionality to PPP. This protocol was created by Microsoft and Cisco and is often used with virtual private networks (VPNs) operating at layer 2.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5, Lesson 2

QUESTION 185:

From the options, which is a tunneling protocol that can only work on IP networks because it requires IP connectivity?

A. IPX protocol
B. L2TP protocol
C. PPTP protocol
D. SSH

Answer: C

Explanation:
You can access a private network through the Internet or other public network by using a virtual private network (VPN) connection with the Point-to-Point Tunneling Protocol (PPTP). It was developed as an extension of the Point-to-Point Protocol (PPP), PPTP tunnels and/or encapsulates IP, IPX, or NetBEUI protocols inside of PPP datagrams. PPTP does not require a dial-up connection. It does, however, require IP connectivity between your computer and the server.
Incorrect answers:
A: IPX is a connectionless, routable network protocol based on the Xerox XNS architecture. It's the default protocol for versions of NetWare before NetWare 5 and operates at the Network layer of the OSI model and is responsible for addressing and routing packets to workstations or servers on other networks.
B: L2TP is an industry-standard Internet tunneling protocol with roughly the same functionality as the Point-to-Point Tunneling Protocol (PPTP). Like PPTP, L2TP encapsulates Point-to-Point Protocol (PPP) frames, which in turn encapsulate IP, IPX, or NetBEUI protocols
D: SSH is a replacement for rlogin in Unix/Linux that includes security. rlogin allowed

one host to establish a connection with another with no real security being employed SSH replaces it with slogin and digital certificates.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 122

QUESTION 186:

You work as the security administrator at Certkiller .com. You must open ports on your firewall to support L2TP (Layer Two Tunneling Protocol) and PPTP (Point-to-Point Tunneling Protocol) connections.
Which ports should you open to support both protocols?

A. Open TCP (Transmission Control Protocol) port 635, and open UDP (User Datagram Protocol) port 654
B. Open TCP (Transmission Control Protocol) port 749, and open UDP (User Datagram Protocol) port 781
C. Open TCP (transmission Control Protocol) port 1723), and open UDP (User Datagram Protocol) port 1701.
D. Open TCP (Transmission Control Protocol) port 1812 and open UDP (User Datagram Protocol) port 1813

Answer: C

Explanation:
L2TP uses UDP port 1701 while PPTP uses port 1723 and TCP for connections.
Incorrect answers:
A: TCP port 635 is used by RLZ Dbase and UDP port 654 is used by OADV.
B: TCP port 749 is used for Kerberos Admin, UDP port 781 is used by HP Performance data collector.
D: This is used by RADIUS accounting.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 120
http://www.iana.org/assignments/port-numbers

QUESTION 187:

From the list of protocols, which two are VPN (Virtual Private Network) tunneling protocols? Choose two protocols.

A. PPP (Point-to-Point Protocol).
B. SLIP (Serial Line Internet Protocol).
C. L2TP (Layer Two Tunneling Protocol).
D. SMTP (Simple Mail Transfer Protocol).
E. PPTP (Point-to-Point Tunneling Protocol).

Answer: C, E

Explanation:
PPTP and L2TP are both VPN tunneling protocols. L2TP is more sophisticated and gaining more popularity.
Incorrect answers:
A: PPP is an encapsulation protocol usually associated with ISDN.
B: SLIP is an old protocol used for direct serial line connections between two computers.
D: Simple Mail Transfer Protocol (SMTP) is a protocol for sending e-mail between SMTP servers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 120

QUESTION 188:

You work as the security administrator at Certkiller .com. You must configure the network to allow AH (Authentication Header) and ESP (Encapsulating Security Payload) tunnel-encapsulated IPSec (Internet Protocol Security) traffic to pass between a client and your firewall.
You open the L2TP (Layer Two Tunneling Protocol) and IKE (Internet Key Exchange) Transport layer ports on the perimeter router and on the firewall.
What else should you do to allow AH and ESP tunnel-encapsulated IPSec (Internet Protocol Security) traffic to pass between a client and your firewall?

A. Configure the perimeter router and firewall to allow inbound protocol number 51 for ESP encapsulated IPSec traffic
B. Configure the perimeter router and firewall to allow inbound protocol number 49 for ESP encapsulated IPSec traffic
C. Configure the perimeter router and firewall to allow inbound protocol numbers 50 and 51 for AH and ESP encapsulated IPSec traffic
D. Configure the perimeter router and firewall to allow inbound protocol numbers 52 and 53 for AH and ESP encapsulated IPSec traffic

Answer: C

Explanation:
The most secure firewall configuration is one in which the firewall permits only IKE and IPSec traffic to flow between the specific IP addresses of the peers. However, if these addresses are not static, or if there are many addresses, a less secure configuration might be required to permit IPSec and IKE traffic to flow between subnets.
When a firewall or filtering router exists between IPSec peers, it must be configured to forward IPSec traffic on UDP source and destination port 500, IP protocol 50 (ESP), or IP protocol 51 (AH).
Incorrect answers:

A: This alone will not allow traffic flow between a client and a firewall.
B: This option will not allow AH and ESP IPSec traffic between client and firewall.
D: Port 53 is used for DNS server lookups and SQL client name lookup.
References:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=

QUESTION 189:

You work as the security administrator at Certkiller .com. You must choose a technology or standard to both authenticate and encrypt IP (Internet Protocol) traffic.
Which should you use?

A. ESP (Encapsulating Security Payload)
B. S/MIME (Secure Multipurpose Internet Mail Extensions)
C. IPSec (Internet Protocol Security)
D. IPv2 (Internet Protocol version 2)

Answer: C
IPSec provides secure authentication and encryption of data and headers. IPSec can work in tunneling mode or transport mode. In tunneling mode, the data or payload and message headers are encrypted. Transport mode encrypts only the payload.
Incorrect answers:
A: ESP is a header used to provide a mix of security services in IPv4 and IPv6. ESP can be used alone or in combination with the IP Authentication Header (AH). But this is not enough to authenticate and encrypt IP traffic.
B: S/MIME is a standard used for encrypting e-mail not IP traffic.
D: IPv2 does not authenticate and encrypt IP traffic.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 127

QUESTION 190:

Choose the correct combination of VPN (Virtual Private Network) tunneling protocols.

A. IPSec (Internet Protocol Security), L2TP (Layer Two Tunneling Protocol), and SSL (Secure Sockets Layer)
B. IPSec (Internet Protocol Security), L2TP (Layer Two Tunneling Protocol), and PPP (Point-to-Point Protocol)
C. PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), and SSL (Secure Sockets Layer)
D. PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), and IPSec (Internet Protocol Security)

Answer: D

Explanation:
Tunneling refers creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually-agreed-upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network. It's obvious that L2TP and PPTP are tunneling protocols because the word tunneling is in the acronyms for their name, but IPSec is also considered a tunneling protocol because it creates a secure tunnel connection.
Incorrect answers:
A, C: SSL is not a tunneling protocol.
B: PPP is not a tunneling protocol.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 30-32

QUESTION 191:

From the list of options, which specifies the primary benefit of using RADIUS (Remote Authentication Dial-in User Service) for a multi-site VPN (Virtual Private Network) that supports a large number of remote users?

A. RADIUS (Remote Authentication Dial-in User Service) provides for a centralized user database.
B. RADIUS (Remote Authentication Dial-in User Service) provides for a decentralized user database.
C. No user database is required with RADIUS (Remote Authentication Dial-in User Service).
D. User database is replicated and stored locally on all remote systems.

Answer: A

Explanation:
Since RADIUS keeps its credentials and keys in a centralized database, it's ideal for a large population of remote users. RADIUS authenticates the dial-in user by means of a private symmetric key; and stores a user profile to grant user authorization.
Incorrect answers:
B: This is incorrect.
C: This is incorrect as a database is used in RADIUS.
D: There is no replication of user database as RADIUS gives you a single source for the authentication to take place.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 121-122

QUESTION 192:

You work as the security administrator at Certkiller .com. You must configure the firewall to support TACACS.
Which port(s) should you open on the firewall?

A. Port 21
B. Port 161
C. Port 53
D. Port 49

Answer: D

Explanation:
TACACS uses both TCP and UDP port 49.
Incorrect answers:
A: This port is used for FTP's control channel.
B: UDP port 161 is used by SNMP.
C: Port 53 is used for DNS.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 64
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION 193:

You work as the security administrator at Certkiller .com. You must configure the firewall to support SSH (Secure Shell).
Which port(s) should you open on the firewall?

A. Port 22
B. Port 69
C. Port 179
D. Port 17

Answer: A

Explanation:
SSH uses port 22 and TCP for connections.
Incorrect answers:
B: UDP port 69 is used for TFTP.
C, D: Port 17 is used for the quote of the day and port 179 is used for Border gateway protocol. SSH does not require the use of these ports for functionality.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 64,127
http://www.iana.org/assignments/port-numbers

QUESTION 194:

You work as the security administrator at Certkiller .com. You want to implement an alternative to using Telnet to establish secure connections between two systems. Which technology or standard should you use?

A. DES (Data Encryption Standard).
B. S-Telnet.
C. SSH (Secure Shell).
D. PKI (Public Key Infrastructure).

Answer: C

Explanation:
Secure Shell is like telnet in the sense that an administrator may enter commands into a remote server, except that it uses an encrypted and authenticated connection [(RSA) eryptography for connection and authentication; and IDEA, Blowfish,or DES for data stream encryption.] instead of Telnet's cleartext.
SSH is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent, programs for such Unix standards as Telnet, FTP, and many other communications-oriented programs. SSH is now available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other clear text-oriented programs in the Unix environment. SSH uses port 22 and TCP for connections.
Incorrect answers:
A: The Data Encryption Standard (DES) is a strong and efficient algorithm based on a 56-bit key. (Strong refers to the fact that it's hard to break.) DES has several modes that offer security and integrity. However, it has become a little dated as a result of advances in computer technology, and it's being replaced. For its time, it was one of the best standards available.
B: This cannot be used as an alternative to Telnet.
D: This is not an alternative to Telnet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 120

QUESTION 195:

What is the main reason why e-mail security concepts do not work?

A. The workers lack of interest in updating virus definitions

B. A lack of suitable software
C. The rate at which new viruses are being developed
D. Viruses are unstoppable

Answer: A

Explanation:
The software typically uses a virus definition file that is updated regularly by the manufacturer. Fortunately, these virus definition files are usually updated every two weeks or so. If these files are kept up to date, the computer system will be relatively secure. Unfortunately, most people don't keep them up to date. Users will exclaim that a new virus is out, because they just got it. Upon examination, you will discover that in most cases their virus definition file is months out of date.
Incorrect answers:
B: It cannot be blamed on the software because for virus there is a method of prevention.
C: This can be combated by updating your virus definitions regularly.
D: For every virus created the will be a method of prevention
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 64,130

QUESTION 196:

Which of the following network attacks cannot occur in an e-mail attack?

A. Dictionary attack
B. Trojan Horse
C. Phage Virus
D. Polymorphic Virus

Answer: A

Explanation:
A Dictionary attack involves guessing possible passwords for entering as another user. The attacker must have access to the network.
Incorrect answers:
B, C, D: These viruses are spread via e-mail.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 129

QUESTION 197:

When does your antivirus software scan your e-mails for possible viruses?

A. While receiving

B. While opening
C. While sending
D. All of the above

Answer: A

Explanation:
Your antivirus software should scan all your incoming mail before you can even read it.
Incorrect answers:
B, C, D: It is only necessary to scan your e-mails once and the antivirus software should pick up possible risks on receiving the mail.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 129

QUESTION 198:

Which of the following attacks are being referred to if someone is accessing your e-mail server and sending inflammatory information to others?

A. Trojan Horse.
B. Phage Virus.
C. Repudiation Attack.
D. Polymorphic Virus.

Answer: C

Explanation:
Repudiation attacks make data or information that is used invalid or misleading, which can be even worse. An example of a repudiation attack might be someone accessing your e-mail server and sending inflammatory information to others. This information can prove embarrassing to you or your company if this happens. Repudiation attacks are fairly easy to accomplish because most e-mail systems do not check outbound mail for validity. Repudiation attacks usually begin as access attacks.
Incorrect answers:
A, B, D: These attacks are not e-mail based.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 129

QUESTION 199:

What type of attack would involve a customer who claims that they never received a service for which they were billed. In this situation, the burden of proof is on the company to prove that the information used to generate the invoice is accurate?
This attack is done via e-mail.

A. Trojan Horse.
B. Phage Virus.
C. Repudiation Attack.
D. Polymorphic Virus.

Answer: C

Explanation:
A common type of repudiation attack would involve a customer who claims that they never received a service for which they were billed. In this situation, the burden of proof is on the company to prove that the information used to generate the invoice is accurate. If the data has been modified by an external attacker, accuracy verification of the information may be difficult.
Incorrect answers:
A, B, D: These attacks are not e-mail based.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 129.

QUESTION 200:

Which of the following protocols make use of port 25?

A. SMTP
B. FTP
C. Telnet
D. SNMP

Answer: A

Explanation:
Simple Mail Transfer Protocol makes use of this port for server to server communication.
Incorrect answers:
B: FTP makes use of port 20
C: Telnet makes use of port 23
D: SNMP makes use of port 162
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 201:

Which of the following protocols make use of port 110?

A. POP3

B. FTP
C. Telnet
D. SNMP

Answer: A

Explanation:
Post Office Protocol Version: 3 makes use of this port for client to server communication.
Incorrect answers:
B: FTP makes use of port 20
C: Telnet makes use of port 23
D: SNMP makes use of port 162
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 202:

Which of the following protocols make use of port 143?

A. IMAP4
B. FTP
C. Telnet
D. SNMP

Answer: A

Explanation:
Internet Message Access Protocol Version: 4 makes use of this port for client to server communication.
Incorrect answers:
B: FTP makes use of port 20
C: Telnet makes use of port 23
D: SNMP makes use of port 162
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 203:

Which of the following ports does SMTP use?

A. 25.
B. 20.
C. 23.
D. 162.

Answer: A

Explanation:
Simple Mail Transfer Protocol makes use of this port for server to server communication.
Incorrect answers:
B: FTP makes use of port 20
C: Telnet makes use of port 23
D: SNMP makes use of port 162
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 204:

Which of the following ports does POP3 use?

A. 110.
B. 20.
C. 23.
D. 162.

Answer: A

Explanation:
Post Office Protocol Version: 3 makes use of this port for client to server communication.
Incorrect answers:
B: FTP makes use of port 20
C: Telnet makes use of port 23
D: SNMP makes use of port 162
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 205:

Which of the following ports does IMAP4 use?

A. 143.
B. 20.
C. 23.
D. 162.

Answer: A

Explanation:

Internet Message Access Protocol Version: 4 makes use of this port for client to server communication.
Incorrect answers:
B: FTP makes use of port 20
C: Telnet makes use of port 23
D: SNMP makes use of port 162
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 206:

By which means do most network bound viruses spread?

A. E-mail.
B. Floppy
C. CD-Rom
D. Mass storage devices

Answer: A

Explanation:
E-mail is the reason for the high speed at which viruses are spread over the network.
Incorrect answers:
B, C, D: Removable storage such as floppy and CD's are not vital in a system and your antivirus software should reject the device immediately and prompt removal.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 67

QUESTION 207:

Which of the following options would be the primary firewall to protect you from e-mail viruses?

A. E-mail servers.
B. Antivirus software.
C. SMTP.
D. IMAP4.

Answer: A

Explanation:
E-mail servers detect the viruses in the messages received from various sources and send warnings to the recipient to warn him/her of the risky mail. This server has the necessary means to reject infected mail content. E-mail servers have their own virus scanners to

filter all the incoming mail before it reaches the server. An e-mail server is a middle man in the delivery of the message.
Incorrect answers:
B: Antivirus software only tackles the virus once it reaches the recipient therefore the recipient should have the latest virus definitions to stay immune.
C, D: This is a mail protocol and sole purpose is to form a platform on which mail is sent.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 273.

QUESTION 208:

Which of the following definitions should BEST suit the functions of an e-mail server?

A. Detect the viruses in the messages received from various sources and send warnings to the recipient to warn him/her of the risky mail.
B. Notify you that a message carries a virus.
C. Forms a platform on which messages are sent.
D. Makes use of a port used specifically for messages to be sent through.

Answer: A

Explanation:
E-mail servers detect the viruses in the messages received from various sources and send warnings to the recipient to warn him/her of the risky mail. This server has the necessary means to reject infected mail content. E-mail servers have their own virus scanners to filter all the incoming mail before it reaches the server. An e-mail server is a middle man in the delivery of the message.
Incorrect answers:
B: This is the function of antivirus software
C, D: These are messaging protocols.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 273.

QUESTION 209:

Which of the following would be the correct sequence for SSH?

A. E-mail client, SSH server, E-mail client, SSH Tunnel, SSH Server, E-mail server.
B. E-mail client, SSH Tunnel, SSH server, E-mail server.
C. E-mail client, SSH Tunnel, SSH server, E-mail client, E-mail server.
D. E-mail client, SSH server, SSH Tunnel, E-mail server, SSH server, E-mail client.

Answer: A

Explanation:
Secure Shell (SSH) is the tunneling protocol originally used on UNIX systems. SSH is now available for both UNIX and Windows environments. The handshake process between the client and server is similar to the process described in SSL. SSH is primarily intended for interactive terminal sessions. The first phase is a secure channel to negotiate the channel connection. The second phase is a secure channel used to establish the connection.
Incorrect answers:
B, C, D: These do not apply as any part of the SSH tunneling protocol.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 396.

QUESTION 210:

On which of the following should Anti-Virus software be installed to provide optimum protection on a network?

A. On all workstations connected to the Internet.
B. On all network servers.
C. On all workstations and servers.
D. On all terminals.

Answer: C
To provide optimum protection on the network, you should ensure that all systems, workstations and servers included, have Anti-Virus software in stalled on them.
Incorrect Answers:
A: Installing Anti-Virus software on only the workstations connected to the internet will leave the other workstations and servers vulnerable to LAN based viruses that can be introduced to the network through disk dives.
B: Installing
Anti-Virus software on only the servers will leave all workstations vulnerable to LAN based viruses that can be introduced to the network through disk dives and Internet based viruses.
D: Installing Anti-Virus software on only the terminals will leave the other workstations and servers vulnerable to Internet based viruses.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 392-394.

QUESTION 211:

Files with which of the following file extensions CANNOT be infected by a virus?

A. .txt
B. .com
C. .dll
D. .exe

Answer: A
Plain text documents cannot be infected by viruses.
Incorrect Answers:
B, C, D: Executable files such as .com, .exe and .dll files can be infected by viruses.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 392-394.

QUESTION 212:

Which of the following should be scanned for viruses?

A. Plain text documents.
B. Microsoft Word documents.
C. Executable files.
D. All of the above.

Answer: B, C
Incorrect Answers:
A: Plain text documents cannot be infected by viruses and do not need to be scanned.
D: Executable files such as .com, .exe and .dll files and Microsoft Word documents can be infected by viruses and should be scanned.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 392-394.

QUESTION 213:

Choose the primary disadvantage of using a third party mail relay.

A. Spammers can utilize the third party mail relay.
B. A third party mail relay limits access to specific users.
C. A third party mail relay restricts the types of e-mail that maybe sent.
D. A third party mail relay restricts spammers from gaining access.

Answer: A

Explanation:
Using a third party email relay can put you in an advantage of getting unnecessary spam. Anyone on the internet can relay an unsolicited email through an SMTP server, and the message will appear to be legitimate coming from the email server, and it makes it much

more difficult to trace the spammer.
Incorrect answers:
B: Relay actually lends itself to being exploited by unsolicited spammers.
C: This is not the main disadvantage of a relay.
D: The relay does not restrict spammers from gaining access.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 129

QUESTION 214:

Choose the option that correctly defines the purpose of S/MIME (Secure Multipurpose Internet Mail Extensions).

A. S/MIME is used to encrypt user names and profiles to ensure privacy.
B. S/MIME is used to encrypt messages and files.
C. S/MIME is used to encrypt network sessions acting as a VPN (Virtual Private Network) client.
D. S/MIME is used to automatically encrypt all outbound messages.

Answer: B

Explanation:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature data. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Incorrect answers:
A: S/MIME is meant to encrypt messages and files, not user names and profiles.
C: A VPN is a private network that provides security over an otherwise unsecure environment. This is not what S/MIME does.
D: It is not only outbound messages that are encrypted.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 330

QUESTION 215:

S/MIME requires the implementation of which of the following in order to operate?

A. A digital certificate.
B. A server side certificate.
C. A SSL (Secure Sockets Layer) certificate.
D. A public certificate.

Answer: A

Explanation:
What differentiates S/MIME from MIME is that it uses RSA asymmetric encryption and it relies on a digital certificate for authentication.
Incorrect answers:
B: You need a digital certificate and not a server side certificate.
C: This is not necessary for S/MIME.
D: You need a digital certificate with S/MIME instead.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 330

QUESTION 216:

A malformed MIME (Multipurpose Internet Mail Extensions) header can have a negative impact on the system. Choose the option that correctly details this.

A. Can lead to the creation of a back door, which will enable attackers to access the internal network.
B. Can create a virus that infects the computers of users.
C. Can result in the unauthorized disclosure of private information.
D. Can result in an e-mail server crashing.

Answer: D

Explanation:
Microsoft Exchange Server 5.0 & 5.5 had a vulnerability that made it suspect to crashes following a malformed MIME header. Patches have since been released.
Incorrect answers:
A: It does not create a backdoor. This is usually the result of a Trojan horse.
B: Viruses are not created due to malformed MIME.
C: This is not a result of malformed MIME.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 330

QUESTION 217:

Choose the standard typically used to encrypt e-mail messages.

A. S/MIME
B. BIND
C. DES
D. SSL

Answer: A

Explanation:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature data. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Incorrect answers:
B: BINDING allows zone transfers to be signed.
C: DES is a strong and efficient algorithm based on a 56-bit key. But it has been replaced.
D: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 368

QUESTION 218:

Choose the option that details one of the primary benefits of using S/MIME /Secure Multipurpose Internet Mail Extension)?

A. S/MIME allows users to send both encrypted and digitally signed e-mail messages.
B. S/MIME allows users to send anonymous e-mail messages.
C. S/MIME allows users to send e-mail messages with a return receipt.
D. S/MIME expedites the delivery of e-mail messages.

Answer: A

Explanation:
Secure MIME (S/MIME) is a standard used for encrypting e-mail. S/MIME can also contain signature data. S/MIME provides encryption, integrity, and authentication when used in conjunction with PKI.
Incorrect answers:
B
: S/MIME allows for digitally signed, more secure e-mail, anonymity is thus out of the question.
C: This is not an S/MIME benefit.
D: This is not the main benefit of S/MIME.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 368

QUESTION 219:

Choose the option that correctly specifies a likely negative technical impact of receiving large quantifies of spam,

A. DoS (Denial of Service).

B. Processor underutilization.
C. Reduction in hard drive space requirements.
D. Increased network throughput.

Answer: A

Explanation:
In systems where no email filters are set up, it is possible for some users to receive over a hundred unsolicited emails a day! If every user on a network received that much email, the human time necessary to sort through those emails will be Herculean. The system resources required to: process, download, and store such email can potentially reduce a network avalability to zero mthus denying service
Incorrect answers:
B: Processor underutilization usually occurs when the buffer overflows.
C: DoS will occur before you experience hard drive space reduction.
D: This is a secondary result of spamming.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 221

QUESTION 220:

On the topic of comparing viruses and hoaxes, which statement is TRUE? Choose the best TRUE statement.

A. Hoaxes can create as much damage as a real virus.
B. Hoaxes are harmless pranks and should be ignored.
C. Hoaxes can help educate users about a virus.
D. Hoaxes carry a malicious payload and can be destructive.

Answer: A

Explanation: Hoaxes do have the possibility of causing as much damage as viruses. Many hoaxes instruct the recipient to forward the message to everyone that they know and thus causes network congestion and heavy e-mail activity. Hoaxes also often instruct the user to delete files on their computer that may cause their computer or a program to quit functioning.
Incorrect answers:
B: Hoaxes are not harmless and can in fact cause a lot of damage.
C: It does not educate users.
D: This is false.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION 221:

Which of the following is the primary attribute associated with e-mail hoaxes?

A. E-mail hoaxes create unnecessary e-mail traffic and panic in non-technical users.
B. E-mail hoaxes take up large amounts of server disk space.
C. E-mail hoaxes can cause buffer overflows on the e-mail server.
D. E-mail hoaxes can encourage malicious users.

Answer: A

Explanation:
Although answer choices B,C,D have a degree of truth to them;the BEST answer is A. Email hoaxes often create unnecessary traffic because they ask users to forward an email to everyone in address book, and whether it is a computer virus or a blind, crippled, starving, cancer victim child suffering from Herpes it creates undue panic and emotion in the work setting.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION 222:

From the list of options, chose the primary attribute associated with e-mail hoaxes.

A. E-mail hoaxes create unnecessary e-mail traffic, as well as panic in users that are not technically inclined.
B. E-mail hoaxes consume large quantities of server disk space.
C. E-mail hoaxes can result in buffer overflows on the e-mail server.
D. E-mail hoaxes tend to encourage malicious users.

Answer: A

Explanation:
Although answer choices B,C,D have a degree of truth to them;the BEST answer is A. Email hoaxes often create unnecessary traffic because they ask users to forward an email to everyone in address book, and whether it is a computer virus or a blind, crippled, starving, cancer victim child suffering from Herpes it creates undue panic and emotion in the work setting.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 79

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION 223:

Choose the scheme or system used by PGP (Pretty Good Privacy) to encrypt data.

A. Asymmetric scheme
B. Symmetric scheme
C. Symmetric key distribution system
D. Asymmetric key distribution system

Answer: A

Explanation:
PGP is a shareware implementation of RSA encryption. Pretty Good Privacy (PGP) is a set of software tools that allows you to encrypt, decrypt, and digitally sign computer data and e-mail. PGP's encryption and decryption services are asymmetric.
Incorrect answers:
B, C, and D: Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A secret key-sometimes referred to as a private key-is a key that isn't disclosed to people who aren't authorized to use the encryption system. The disclosure of a private key breaches the security of the encryption system. If a key is lost or stolen, the entire process is breached. DES, 3DES, CAST, RC, Blowfish and IDEA Blowfish are all examples of encryption using a symmetric scheme.
Asymmetric algorithms use two keys to encrypt and decrypt data. These keys are referred to as the public key and the private key. The public key can be used by the sender to encrypt a message, and the private key can be used by the receiver to decrypt the message. As you may recall, symmetrical systems require the key to be private between the two parties. With asymmetric systems, each circuit has one key. RSA, Diffie-Hellman, ECC and El Gamal are examples of encryption using asymmetrical schemes.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 292-294
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION 224:

Choose the standard that relies on "Web of Trust" in its key management scheme.

A. Secure Multipurpose Internet Mail extensions (S/MIME)
B. Pretty Good Privacy (PGP)
C. MIME Object Security Services (MOSS)

D. Privacy Enhanced Mail (PEM)

Answer: B

Explanation:
"PGP does not use a hierarchy of CAs, or any type of formal trust certificates, but relies on a "web of trust" in its key management approach. Each user generates and distributes his or her public key, and users sign each other's public keys, which creates a community of users who trust each other. This is different than the CA approach where no one trusts each other, they only trust the CA.
Incorrect answers:
A: S/MIME contains signature data. It uses the PKCS #7 standard (Cryptographic Message Syntax Standard) and is the most widely supported standard used to secure e-mail communications.
C: MIME is the predecessor of S/MIME.
D: PEM is created with three digital signature algorithms.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 292-294
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 6, Lesson 1

QUESTION 225:

One of these concepts has a goal of verifying that an e-mail message received has not been tampered with while in transit. Which is it?

A. Authorization
B. Non-repudiation
C. Integrity
D. Cryptographic mapping

Answer: C

Explanation:
The goal of integrity is to verify that information being used is accurate and hasn't been tampered with. Integrity is coupled with accountability to ensure that data is accurate and that a final authority exists to verify this, if needed.
Incorrect answers:
A: Authorization has to do with an access to issue.
B: Non-repudiation The ability (by whatever means) to verify that data was seen by an intended party. It makes sure they received the data and can't repudiate (dispute) that it arrived.
D: Cryptographic mapping does not verify whether e-mail has been tampered with or not.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 286

QUESTION 226:

Choose the measure that best protects both the confidentiality and integrity of an e-mail message.

A. SHA-1 (Secure Hashing Algorithm 1)
B. IPSec (Internet Protocol Security)
C. Digital signature
D. S/MIME (Secure Multipurpose Internet Mail Extensions)

Answer: D

Explanation:
Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting e-mail.
S/MIME contains signature data. It uses the PKCS #7 standard (Cryptographic Message Syntax
Standard) and is the most widely supported standard used to secure e-mail communications.
Incorrect answers:
A: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol
B: IPSec is a set of protocols that enable encryption, authentication, and integrity over IP.
C: A digital signature is an electronic signature whose sole purpose is to authenticate the sender.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 330

QUESTION 227:

Which of the following statements regarding a firewall is TRUE?

A. A firewall protects hosts on a private network from attackers on a public network.
B. A firewall protects hosts on a public network from attackers on a private network.
C. A firewall protects hosts on a private network from virus attacks.
D. A firewall provides authentication services.

Answer: A
A firewall protects hosts on a private network from attackers on a public network by means of packet filtering, port filtering, or IP address filtering.
Incorrect Answers:

B: A firewall protects hosts on a private network from attackers on a public network rather than hosts on a public network from attackers on a private network.
C, D: A firewall provides packet filtering, port filtering, or IP address filtering. It does not provide authentication or anti-virus protection.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 331-343.

QUESTION 228:

Which of the following statements best describes a demilitarized zone (DMZ)?

A. A DMZ is a separate network segment that contains Internet accessible servers and is separated from the Internet and the rest of the private network by means of a firewall.
B. A DMZ is a separate DNS namespace reserved for Internet accessible servers and is protected by means of a firewall.
C. A DMZ is another term used to describe a private network that is protected by a firewall from attackers on a public network.
D. A DMZ is a bank of remote access servers that is protected by a firewall from attackers on a public network.

Answer: A
A DMZ is a separate network segment that contains Internet accessible servers such as access web servers, FTP servers, and mail-relay servers and is separated from the Internet and the rest of the private network by means of a firewall
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 331-343.

QUESTION 229:

Which of the following are NOT features of a firewall? (Choose all that apply)

A. Access control lists.
B. Dynamic packet filtering.
C. Virus protection.
D. Authentication.

Answer: C, D
A firewall provides packet filtering, port filtering, or IP address filtering. It does not provide authentication or anti-virus protection.
Incorrect Answers:
A, B: Access control lists and dynamic packet filtering are features of firewalls.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 331-343.

QUESTION 230:

Which of the following statements regarding a proxy server are TRUE? (Choose all that apply)

A. A proxy server is a type of firewall that completely separates packets from internal hosts and from external hosts.
B. A proxy server connects two dissimilar networks by providing Network Address Translation.
C. A proxy server operates at the lower layers of the OSI reference model.
D. A proxy server can cache frequently accessed Web pages and can increase network security by filtering out Web content that is considered insecure, such as executables, scripts, or viruses.

Answer: A, D
A proxy server caches web pages for future retrieval, allowing a user's request to be filled quicker and reducing Internet traffic. A proxy server also hides the IP addresses of all hosts on the internal network by replacing the private IP address of any requesting host with its own public IP address. Thus providing Network Address Translation.
Incorrect Answers:
A: A proxy server can provide Network Address Translation but it connects an LAN to the Internet, not to a dissimilar network.
C: A proxy server operates at the Application Layer of the OSI.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 134-13, 142-144.

QUESTION 231:

Which of the following CANNOT be performed by a proxy server?

A. Network Address Translation.
B. Web page caching.
C. Packet filtering.
D. Data encryption.

Answer: D
A proxy server does not provide data encryption.
Incorrect Answers:
A: A proxy server also hides the IP addresses of all hosts on the internal network by replacing the private IP address of any requesting host with its own public IP address. Thus providing Network Address Translation.
B: A proxy server caches web pages for future retrieval, allowing a user's request to be filled quicker and reducing Internet traffic.
C: A proxy server inspects the entire packet and can be configured to filter packets that

pass through it based on a number of criteria.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 134-13, 142-144.

QUESTION 232:

You work as a security administrator at Certkiller .com. You have installed a new firewall on the Certkiller .com network. A few days later Certkiller .com users complain that they can send outgoing e-mail but cannot receive any e-mail. What should you do?

A. Ensure that inbound traffic on port 25 is permitted on the firewall.
B. Ensure that outbound traffic on port 25 is permitted on the firewall.
C. Ensure that inbound traffic on port 110 is permitted on the firewall.
D. Ensure that outbound traffic on port 110 is permitted on the firewall.

Answer: C
The firewall is probably blocking inbound POP3 traffic which is used for email retrieval. POP3 uses port 110. Therefore we should ensure that inbound traffic on port 110 is permitted on the firewall.
Incorrect Answers:
A, B: SMTP uses port 25 to transfer email between email servers. However, the problem lies with clients sending email rather than servers transferring them.
D: Users can send email, therefore outbound POP3 traffic is not blocked on the firewall.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 134-13, 142-144.

QUESTION 233:

You work as a network administrator at Certkiller .com. The Certkiller .com network uses an IP proxy that provides Network Address Translation (NAT). You have implemented IPSec for all internet bound traffic; however, Internet access is now no longer possible. What should is the cause of this problem?

A. Network Address Translation (NAT) does not work with IPSec.
B. The IP proxy is blocking egress and ingress traffic on port 80.
C. The IP proxy is blocking egress and ingress traffic on port 1293.
D. The IP proxy is blocking egress and ingress traffic on port 8080.

Answer: A
Network Address Translation (NAT) is not compatible with IPSec because NAT changes the IP address in the IP header of each packet. IPSec does not allow this and drops the packet.
Incorrect Answers:

B: Port 80 is used for HTTP traffic. However, Internet access was possible before the switch t o IPSec. Therefore the problem does not lie with port blocking.
C: Port 1293 is used for IPSec traffic. If this port is blocked, IPSec traffic would not pass. However, the problem here is that Network Address Translation (NAT) changes the IP address in the IP header of each packet which is not permitted in IPSec.
D: Port 8080 is an alternate port for HTTP and is commonly used for proxy servers. However, the problem here is that Network Address Translation (NAT) changes the IP address in the IP header of each packet which is not permitted in IPSec.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 134-13, 142-144.

QUESTION 234:

Which of the following web vulnerabilities is being referred to when it is a programming language that allows access to system resources of the system running the script?

A. JavaScript.
B. Java Applets.
C. Signed Applets.
D. ActiveX

Answer: A

Explanation:
JavaScript is a programming language that allows access to system resources of the system running the script. These scripts can interface with all aspects of an operating system just like programming languages, such as the C language. This means that JavaScript scripts, when executed, can potentially damage systems or be used to send information to unauthorized persons.
Incorrect answers:
B: A Java applet is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they are becoming one of the most popular tools used for website development.
C: Signed applets are similar to Java applets-with one key difference. A signed applet does not run in the Java sandbox, and it has higher system access capabilities. Signed applets are not usually downloaded from the Internet. This type of applet is usually provided by in-house or custom-programming efforts. These applets can also include a digital signature to verify authenticity. If the applet is verified as authentic, it will be installed. Users should never download a signed applet unless they are sure that the provider is trusted.
D: ActiveX is a technology that was implemented by Microsoft. ActiveX allows customized controls, icons, and other features to increase the usability of web enabled

systems. ActiveX uses a method called authenticode for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server. ActiveX runs on the client.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 235:

Which of the following web vulnerabilities is being referred to when the client browser must have the ability to run Java applets in a virtual machine on the client?

A. JavaScript.
B. Java Applets.
C. Signed Applets.
D. ActiveX

Answer: B

Explanation:
A Java applet is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they are becoming one of the most popular tools used for website development.
Incorrect answers:
A: JavaScript is a programming language that allows access to system resources of the system running the script. These scripts can interface with all aspects of an operating system just like programming languages, such as the C language. This means that JavaScript scripts, when executed, can potentially damage systems or be used to send information to unauthorized persons.
C: Signed applets are similar to Java applets-with one key difference. A signed applet does not run in the Java sandbox, and it has higher system access capabilities. Signed applets are not usually downloaded from the Internet. This type of applet is usually provided by in-house or custom-programming efforts. These applets can also include a digital signature to verify authenticity. If the applet is verified as authentic, it will be installed. Users should never download a signed applet unless they are sure that the provider is trusted.
D: ActiveX is a technology that was implemented by Microsoft. ActiveX allows customized controls, icons, and other features to increase the usability of web enabled systems. ActiveX uses a method called authenticode for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server. ActiveX runs on the client.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 236:

Which of the following web vulnerabilities is being referred to when it can also include a digital signature to verify authenticity?

A. JavaScript.
B. Java Applets.
C. Signed Applets.
D. ActiveX

Answer: C

Explanation:
Signed applets are similar to Java applets-with one key difference. A signed applet does not run in the Java sandbox, and it has higher system access capabilities. Signed applets are not usually downloaded from the Internet. This type of applet is usually provided by in-house or custom-programming efforts. These applets can also include a digital signature to verify authenticity. If the applet is verified as authentic, it will be installed. Users should never download a signed applet unless they are sure that the provider is trusted.
Incorrect answers:
A: JavaScript is a programming language that allows access to system resources of the system running the script. These scripts can interface with all aspects of an operating system just like programming languages, such as the C language. This means that JavaScript scripts, when executed, can potentially damage systems or be used to send information to unauthorized persons.
B: A Java applet is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they are becoming one of the most popular tools used for website development.
D: ActiveX is a technology that was implemented by Microsoft. ActiveX allows customized controls, icons, and other features to increase the usability of web enabled systems. ActiveX uses a method called authenticode for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server. ActiveX runs on the client.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 237:

Which of the following web vulnerabilities is being referred to when it allows customized controls, icons, and other features to increase the usability of web enabled systems?

A. JavaScript.
B. Java Applets.
C. Signed Applets.
D. ActiveX

Answer: D

Explanation:
ActiveX is a technology that was implemented by Microsoft. ActiveX allows customized controls, icons, and other features to increase the usability of web enabled systems. ActiveX uses a method called authenticode for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server. ActiveX runs on the client.
Incorrect answers:
A: JavaScript is a programming language that allows access to system resources of the system running the script. These scripts can interface with all aspects of an operating system just like programming languages, such as the C language. This means that JavaScript scripts, when executed, can potentially damage systems or be used to send information to unauthorized persons.
B: A Java applet is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they are becoming one of the most popular tools used for website development.
C: Signed applets are similar to Java applets-with one key difference. A signed applet does not run in the Java sandbox, and it has higher system access capabilities. Signed applets are not usually downloaded from the Internet. This type of applet is usually provided by in-house or custom-programming efforts. These applets can also include a digital signature to verify authenticity. If the applet is verified as authentic, it will be installed. Users should never download a signed applet unless they are sure that the provider is trusted.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 238:

Which of the following web vulnerabilities is being referred to when it receives more data than it is programmed to accept?

A. Buffer Overflows.
B. Cookies.
C. CGI.
D. SMTP Relay

Answer: A

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Incorrect answers:
B: Cookies are text files that a browser maintains on the user's hard disk. A cookie will typically contain information about the user. Cookies are used to provide a persistent, customized web experience for each visit. A cookie can contain the history of a client to improve customer service.
C: Common Gateway Interface (CGI) is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. CGI scripts are not widely used in new systems and are being replaced by Java, ActiveX, and other technologies. The CGI script ran on the web server, and it interacted with the client browser.
D: SMTP relay is a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers. Initially, the SMTP relay function was intended to help bridge between systems. This capability allows e-mail connections between systems across the Internet to be made easily. Unfortunately, this feature has been used to generate a great deal of spam on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 239:

Which of the following web vulnerabilities is being referred to when it is used to provide a persistent, customized web experience for each visit?

A. Buffer Overflows.
B. Cookies.
C. CGI.
D. SMTP Relay

Answer: B

Explanation:
Cookies are text files that a browser maintains on the user's hard disk. A cookie will typically contain information about the user. Cookies are used to provide a persistent, customized web experience for each visit. A cookie can contain the history of a client to improve customer service.
Incorrect answers:
A: Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave

the system sending the data with temporary access to privileged levels in the attacked system.
C: Common Gateway Interface (CGI) is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. CGI scripts are not widely used in new systems and are being replaced by Java, ActiveX, and other technologies. The CGI script ran on the web server, and it interacted with the client browser.
D: SMTP relay is a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers. Initially, the SMTP relay function was intended to help bridge between systems. This capability allows e-mail connections between systems across the Internet to be made easily. Unfortunately, this feature has been used to generate a great deal of spam on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 240:

Which of the following web vulnerabilities is being referred to when it's an older form of scripting that was used extensively in early web systems?

A. Buffer Overflows.
B. Cookies.
C. CGI.
D. SMTP Relay

Answer: C

Explanation:
Common Gateway Interface (CGI) is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. CGI scripts are not widely used in new systems and are being replaced by Java, ActiveX, and other technologies. The CGI script ran on the web server, and it interacted with the client browser.
Incorrect answers:
A: Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
B: Cookies are text files that a browser maintains on the user's hard disk. A cookie will typically contain information about the user. Cookies are used to provide a persistent, customized web experience for each visit. A cookie can contain the history of a client to improve customer service.
D: SMTP relay is a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers. Initially, the SMTP relay function was intended to help bridge between systems. This capability allows e-mail connections between systems

across the Internet to be made easily. Unfortunately, this feature has been used to generate a great deal of spam on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 241:

Which of the following web vulnerabilities is being referred to when it has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers?

A. Buffer Overflows.
B. Cookies.
C. CGI.
D. SMTP Relay

Answer: D

Explanation:
SMTP relay is a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers. Initially, the SMTP relay function was intended to help bridge between systems. This capability allows e-mail connections between systems across the Internet to be made easily. Unfortunately, this feature has been used to generate a great deal of spam on the Internet.
Incorrect answers:
A: Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
B: Cookies are text files that a browser maintains on the user's hard disk. A cookie will typically contain information about the user. Cookies are used to provide a persistent, customized web experience for each visit. A cookie can contain the history of a client to improve customer service.
C: Common Gateway Interface (CGI) is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. CGI scripts are not widely used in new systems and are being replaced by Java, ActiveX, and other technologies. The CGI script ran on the web server, and it interacted with the client browser.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 242:

Which of the following definitions BEST suit JavaScript?

A. It is a programming language that allows access to system resources of the system running the script
B. The client browser must have the ability to run Java applets in a virtual machine on the client
C. It can also include a digital signature to verify authenticity
D. It allows customized controls, icons, and other features to increase the usability of web enabled systems

Answer: A

Explanation:
A Java applet is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they are becoming one of the most popular tools used for website development
Incorrect answers:
B: This refers to Java Applet
C: This refers to Signed Applet
D: This refers to ActiveX
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 243:

Which of the following definitions BEST suit Java Applet?

A. It is a programming language that allows access to system resources of the system running the script
B. The client browser must have the ability to run Java applets in a virtual machine on the client
C. It can also include a digital signature to verify authenticity
D. It allows customized controls, icons, and other features to increase the usability of web enabled systems

Answer: B

Explanation:
A Java applet is a small, self-contained Java script that is downloaded from a server to a client and then run from the browser. The client browser must have the ability to run Java applets in a virtual machine on the client. Java applets are used extensively in web servers today, and they are becoming one of the most popular tools used for website development.
Incorrect answers:

A: This refers to JavaScript
C: This refers to Signed Applet
D: This refers to ActiveX
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 244:

Which of the following definitions BEST suit Singed Applet?

A. It is a programming language that allows access to system resources of the system running the script
B. The client browser must have the ability to run Java applets in a virtual machine on the client
C. It can also include a digital signature to verify authenticity
D. It allows customized controls, icons, and other features to increase the usability of web enabled systems

Answer: C

Explanation:
Signed applets are similar to Java applets-with one key difference. A signed applet does not run in the Java sandbox, and it has higher system access capabilities. Signed applets are not usually downloaded from the Internet. This type of applet is usually provided by in-house or custom-programming efforts. These applets can also include a digital signature to verify authenticity. If the applet is verified as authentic, it will be installed. Users should never download a signed applet unless they are sure that the provider is trusted.
Incorrect answers:
A: This refers to JavaScript
B: This refers to Java Applet
D: This refers to ActiveX
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 245:

Which of the following definitions BEST suit ActiveX?

A. It is a programming language that allows access to system resources of the system running the script
B. The client browser must have the ability to run Java applets in a virtual machine on the client
C. It can also include a digital signature to verify authenticity

D. It allows customized controls, icons, and other features to increase the usability of web enabled systems

Answer: D

Explanation:
ActiveX is a technology that was implemented by Microsoft. ActiveX allows customized controls, icons, and other features to increase the usability of web enabled systems. ActiveX uses a method called authenticode for security. Authenticode is a type of certificate technology that allows ActiveX components to be validated by a server. ActiveX runs on the client.
Incorrect answers:
A: This refers to JavaScript
B: This refers to Java Applet
C: This refers to Singed Applet
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 246:

Which of the following definitions BEST suit Buffer Overflow?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.
C. It's an older form of scripting that was used extensively in early web systems
D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers

Answer: A

Explanation:
Buffer overflows occur when an application receives more data than it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system
Incorrect answers:
B: This refers to Cookies
C: This refers to CGI
D: This refers to SMTP Relay
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 247:

Which of the following definitions BEST suit Cookies?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.
C. It's an older form of scripting that was used extensively in early web systems
D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers

Answer: B

Explanation:
Cookies are text files that a browser maintains on the user's hard disk. A cookie will typically contain information about the user. Cookies are used to provide a persistent, customized web experience for each visit. A cookie can contain the history of a client to improve customer service.
Incorrect answers:
A: This refers to Buffer Overflow
C: This refers to CGI
D: This refers to SMTP Relay
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 248:

Which of the following definitions BEST suit CGI?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.
C. It's an older form of scripting that was used extensively in early web systems
D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers

Answer: C

Explanation:
Common Gateway Interface (CGI) is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. CGI scripts are not widely used in new systems and are being replaced by Java, ActiveX, and other technologies. The CGI script ran on the web server, and it interacted with the client browser.
Incorrect answers:
A: This refers to Buffer Overflow
B: This refers to Cookies
D: This refers to SMTP Relay
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 249:

Which of the following definitions BEST suit SMTP Relay?

A. It receives more data than it is programmed to accept.
B. It is used to provide a persistent, customized web experience for each visit.
C. It's an older form of scripting that was used extensively in early web systems
D. It has a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers

Answer: D

Explanation:
SMTP relay is a feature designed into many e-mail servers that allows them to forward e-mail to other e-mail servers. Initially, the SMTP relay function was intended to help bridge between systems. This capability allows e-mail connections between systems across the Internet to be made easily. Unfortunately, this feature has been used to generate a great deal of spam on the Internet.
Incorrect answers:
A: This refers to Buffer Overflow
B: This refers to Cookies
C: This refers to CGI
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 134-135

QUESTION 250:

Which of the following statements are true regarding FTP Connections?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection.

Answer: A

Explanation:
FTP has three separate functions. FTP is a protocol, a client, and a server. The client system runs a program called FTP. The server runs a service called FTP server. The FTP client and server communicate using the FTP protocol. The client requests a connection

to a server that runs the FTP service. The client and server communicate using a protocol that defines the command structure and interactions between the client and server.
Incorrect answers:
B: This refers to Blind FTP/Anonymous
C: This refers to FTP Secure
D: This refers to File Sharing
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 251:

Which of the following statements are true regarding Blind FTP/Anonymous?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection.

Answer: B

Explanation:
Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's e-mail address, and the password was anonymous. This honor system is still used in systems where public access to files is wanted. In this situation, the only security offered is what is configured by the operating system.
Incorrect answers:
A: This refers to FTP Connections
C: This refers to FTP Secure
D: This refers to File Sharing
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 252:

Which of the following statements are true regarding FTP Secure?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer

connection.

Answer: C

Explanation:
Secure FTP (S/FTP) is accomplished using a protocol called Secure Shell (SSH). As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server. SSH is available for UNIX and other systems that provide similar capabilities to FTP. SSH is a type of tunneling protocol that allows access to remote systems in a secure manner.
Incorrect answers:
A: This refers to FTP Connections
B: This refers to Blind FTP/Anonymous
D: This refers to File Sharing
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 253:

Which of the following statements are true regarding File Sharing?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection.

Answer: D

Explanation:
File sharing is accomplished by storing files on an assigned location on the server or workstation. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation. In an FTP connection, a file can be uploaded from a client using the PUT command. A download with FTP is accomplished using the GET command. Most modern servers and applications allow an application program to access shared files at the record level.
Incorrect answers:
A: This refers to FTP Connections
B: This refers to Blind FTP/Anonymous
C: This refers to FTP Secure
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 254:

Which one of the following File Transfer Protocol does the statement "FTP is a protocol, a client, and a server" refer to?

A. FTP Connections
B. Blind FTP/Anonymous
C. FTP Secure
D. File Sharing

Answer: A

Explanation:
FTP has three separate functions. FTP is a protocol, a client, and a server. The client system runs a program called FTP. The server runs a service called FTP server. The FTP client and server communicate using the FTP protocol. The client requests a connection to a server that runs the FTP service. The client and server communicate using a protocol that defines the command structure and interactions between the client and server.
Incorrect answers:
B
: Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's e-mail address, and the password was anonymous. This honor system is still used in systems where public access to files is wanted. In this situation, the only security offered is what is configured by the operating system
C: Secure FTP (S/FTP) is accomplished using a protocol called Secure Shell (SSH). As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server. SSH is available for UNIX and other systems that provide similar capabilities to FTP. SSH is a type of tunneling protocol that allows access to remote systems in a secure manner
D: File sharing is accomplished by storing files on an assigned location on the server or workstation. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation. In an FTP connection, a file can be uploaded from a client using the PUT command. A download with FTP is accomplished using the GET command. Most modern servers and applications allow an application program to access shared files at the record level
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 255:

Which one of the following File Transfer Protocol does the statement "Security was based on the honor system" refer to?

A. FTP Connections
B. Blind FTP/Anonymous
C. FTP Secure
D. File Sharing

Answer: B

Explanation:
Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's e-mail address, and the password was anonymous. This honor system is still used in systems where public access to files is wanted. In this situation, the only security offered is what is configured by the operating system.
Incorrect answers:
A: FTP has three separate functions. FTP is a protocol, a client, and a server. The client system runs a program called FTP. The server runs a service called FTP server. The FTP client and server communicate using the FTP protocol. The client requests a connection to a server that runs the FTP service. The client and server communicate using a protocol that defines the command structure and interactions between the client and server
C: Secure FTP (S/FTP) is accomplished using a protocol called Secure Shell (SSH). As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server. SSH is available for UNIX and other systems that provide similar capabilities to FTP. SSH is a type of tunneling protocol that allows access to remote systems in a secure manner
D: File sharing is accomplished by storing files on an assigned location on the server or workstation. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation. In an FTP connection, a file can be uploaded from a client using the PUT command. A download with FTP is accomplished using the GET command. Most modern servers and applications allow an application program to access shared files at the record level
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 256:

Which one of the following File Transfer Protocol does the statement "As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server" refer to?

A. FTP Connections
B. Blind FTP/Anonymous
C. FTP Secure
D. File Sharing

Answer: C

Explanation:
Secure FTP (S/FTP) is accomplished using a protocol called Secure Shell (SSH). As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server. SSH is available for UNIX and other systems that provide similar capabilities to FTP. SSH is a type of tunneling protocol that allows access to remote systems in a secure manner.
Incorrect answers:
A: FTP has three separate functions. FTP is a protocol, a client, and a server. The client system runs a program called FTP. The server runs a service called FTP server. The FTP client and server communicate using the FTP protocol. The client requests a connection to a server that runs the FTP service. The client and server communicate using a protocol that defines the command structure and interactions between the client and server
B: Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's e-mail address, and the password was anonymous. This honor system is still used in systems where public access to files is wanted. In this situation, the only security offered is what is configured by the operating system.
D: File sharing is accomplished by storing files on an assigned location on the server or workstation. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation. In an FTP connection, a file can be uploaded from a client using the PUT command. A download with FTP is accomplished using the GET command. Most modern servers and applications allow an application program to access shared files at the record level
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 257:

Which one of the following File Transfer Protocol does the statement "When files are stored on a workstation, the connection is referred to as a peer-to-peer connection" refer to?

A. FTP Connections
B. Blind FTP/Anonymous
C. FTP Secure
D. File Sharing

Answer: D

Explanation:
File sharing is accomplished by storing files on an assigned location on the server or

workstation. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation. In an FTP connection, a file can be uploaded from a client using the PUT command. A download with FTP is accomplished using the GET command. Most modern servers and applications allow an application program to access shared files at the record level.
Incorrect answers:
A: FTP has three separate functions. FTP is a protocol, a client, and a server. The client system runs a program called FTP. The server runs a service called FTP server. The FTP client and server communicate using the FTP protocol. The client requests a connection to a server that runs the FTP service. The client and server communicate using a protocol that defines the command structure and interactions between the client and server
B: Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's e-mail address, and the password was anonymous. This honor system is still used in systems where public access to files is wanted. In this situation, the only security offered is what is configured by the operating system.
C: Secure FTP (S/FTP) is accomplished using a protocol called Secure Shell (SSH). As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server. SSH is available for UNIX and other systems that provide similar capabilities to FTP. SSH is a type of tunneling protocol that allows access to remote systems in a secure manner
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 258:

Which one of the following File Transfer Protocol does the statement "The user ID and password are not encrypted and are subject to packet capture" refer to?

A. FTP Connections
B. Blind FTP/Anonymous
C. FTP Secure
D. Vulnerabilities and Sniffing

Answer: D

Explanation:
FTP has a major flaw. The user ID and password are not encrypted and are subject to packet capture. This creates a major security breach-especially if you are connecting to an FTP server across the Internet.
Incorrect answers:
A: FTP has three separate functions. FTP is a protocol, a client, and a server. The client system runs a program called FTP. The server runs a service called FTP server. The FTP client and server communicate using the FTP protocol. The client requests a connection

to a server that runs the FTP service. The client and server communicate using a protocol that defines the command structure and interactions between the client and server
B: Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's e-mail address, and the password was anonymous. This honor system is still used in systems where public access to files is wanted. In this situation, the only security offered is what is configured by the operating system.
C: Secure FTP (S/FTP) is accomplished using a protocol called Secure Shell (SSH). As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server. SSH is available for UNIX and other systems that provide similar capabilities to FTP. SSH is a type of tunneling protocol that allows access to remote systems in a secure manner
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 259:

You work as the security administrator at Certkiller .com. You have been instructed to perform the configuration which will allow only HTTP (Hypertext Transfer Protocol) traffic for outbound Internet connections. In addition to this requirement, only specific users must have permissions to browse the web.
Which solution should you use to enforce your requirements?

A. Implement a packet filtering firewall.
B. Implement a protocol analyzer.
C. Implement a proxy server.
D. Implement a stateful firewall.

Answer: C

Explanation:
A proxy server is a type of server that makes a single Internet connection and services requests on behalf of many users. It is a server that is situated between a client and a server; that intercessors requests. Proxy servers are used for two reasons;
* To filter requests, so a strict parent or company can prevent their kids or employees from viewing the wrong sties.
* The increase performance, so multiple users accessing the same information (like a school, or a library,) can fetch common information from the proxy server.
Incorrect answers:
A: A proxy server would be more suited to the needs of the company.
B: A protocol analyzer is not used to set permissions to allow only certain users access to browse the web.
D: A stateful firewall not only examine packets at the Network layer, but also gather information about the packet's communications session from all layers to determine whether a packet is valid in the context in which it is received. But this is all proxy-able.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 463

QUESTION 260:

You work as the security administrator at Certkiller .com. While monitoring e-mail traffic, you discover that your e-mail server is currently relaying e-mail for whichever e-mail server is requesting relaying. You find that this includes spam. Upon some in-depth investigation, you find the existence of /etc/mail/relay domains. You want to configure the relay domains file so as to prevent relaying for non-explicitly named domains.
What should you do next?

A. Move the .* entry to the end of the relay domains file.
Restart the e-mail system.
B. Move the .* entry to the start of the relay domains file.
Restart the e-mail system.
C. Delete the .* entry in the relay domains file.
Restart the e-mail system.
D. Delete the relay domains file from the /etc/mail folder.
Restart the e-mail system.

Answer: C

Explanation:
The symbol: *.* is known as a wild card mask, and just like in poker when a file matches a wild card anything goes. By deleting the wild card, it prevents ANY email server (including the SPAM servers) from relaying information.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 129-130

QUESTION 261:

One of these options best defines the main purpose of implementing an e-mail relay server. Which is it?

A. An e-mail relay server is used to block all spam. This results in the e-mail system functioning more efficiently, and without the additional load of spam.
B. An e-mail relay server is used to prevent inward bound viruses.
C. An e-mail relay server is used to protect the primary e-mail server and therefore assists in reducing the effects of viruses and port scan attacks.
D. An e-mail relay server is used to eliminate e-mail vulnerabilities, simply because all e-mail moves through the relay server first.

Answer: C

Explanation:
An email relay will essentially make your mail server invisible to the internet, so you can protect yourself from port scans, viruses, and arbitrary access.
Incorrect answers:
A: This is but one function of how it can be used.
B: This will not prevent viruses from entering the network.
D: It cannot eliminate vulnerabilities.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 129-130

QUESTION 262:

Choose the primary reason why you should configure your e-mail server to prevent e-mail relay.

A. Can result in untraceable, unwanted, unsolicited e-mail messages being sent.
B. Can result in an attacker gaining access to the server and eventually controlling the server.
C. Can result in confidential information in the e-mail boxes hosted on the server being read by using the relay.
D. Can result in an attacker using the open relay to gain control of nodes on other networks.

Answer: A

Explanation:
If someone can find a way to relay email through the relay server, they can send thousands of unsolicited emails a day without the recipients having a way to pinpoint the source.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 129-130

QUESTION 263:

An attacker can use a specific method to exploit the clear-text attribute of Instant-Messaging sessions. Which is it?

A. Packet sniffing.
B. Port scanning.
C. Cryptanalysis.
D. Reverse engineering.

Answer: A

Explanation:
Since only clear unencrypted text is being sent across the world through multitudes of WAN equipment and routerss,it is easy for someone to sniff your conversation and eavesdrop on every single word you type.
Incorrect answers:
B: Port scanning is when an attacker can systematically query your network to determine which services and ports are open.
C: This is the study and practice of finding weaknesses in ciphers.
D: Reverse engineering is the process of re-creating the functionality of an item by first deciding what the result is and then creating something from scratch that serves the same purpose.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 183-184

QUESTION 264:

You work as a security administrator at Certkiller .com. The Certkiller .com network must be configured to support e-mail communication using SMTP (Simple Mail Transfer Protocol).
Which ports must you open on the firewall to support SMTP connections?

A. Open TCP (Transmission Control Protocol) port 110 to inbound and outbound connections.
B. Open UDP (User Datagram Protocol) port 110 to inbound connections.
C. Open UDP (User Datagram Protocol) port 25 to inbound connections.
D. Open TCP (Transmission Control Protocol) port 25 to inbound and outbound connections.

Answer: D

Explanation:
TCP port 25 is reserved for SMTP while port 110 is for POP3.
Incorrect answers:
A, B, C: SMTP is a protocol for sending e-mail between SMTP servers. Whereas POP3 is the protocol used to download e-mail from an SMTP e-mail server to a network client.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 64

QUESTION 265:

During the SSL (Secure Sockets Layer) handshake process between a client and server, a specific number of steps are used. Choose the option that correctly defines

the number of steps used.

A. Five steps
B. Six steps
C. Seven steps
D. Eight steps

Answer: B

Explanation:
SSL establishes a stateful connection negotiated by a handshaking procedure between client and server. During this handshake, the client and server exchange the specifications for the cipher that will be used for that session. 1. The handshake begins when a browser connects to an SSL-enabled server, and asks the (2) server to send back its identification, a digital certificate that usually contains the server name, the trusted certifying authority, and the server public encryption key. The browser can contact the server of the trusted certifying authority and confirm that the certificate is authentic before proceeding.
The browser then presents a list of encryption algorithms and hashing functions (used to generate a number from another);(3) the server picks the strongest encryption that it also supports and notifies the client of the decision.
In order to generate the session keys used for the secure connection, the browser uses the server public key from the certificate to encrypt a random number and send it to the server. (4) The client can encrypt this data, but only the server can decrypt it: this is the one fact that makes the keys hidden from third parties, since only the server and the client have access to this data.
(5) The server replies with more random data (which doesn't have to be encrypted), and (6) then both parties use the selected hash functions on the random data to generate the session keys. This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the session keys.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4

QUESTION 266:

From the options below, which represents the first action performed by an SSL (Secure Sockets Layer) enabled server when a user clicks to browse a secure page?

A. The server uses its digital certificate to identify itself to the browser.
B. The server validates the user by checking the CRL (Certificate Revocation List).
C. The server requests the user to produce the CRL (Certificate Revocation List).
D. The server displays the page requested by the user on the browser, and then provides its IP (Internet Protocol) address for verification purposes.

Answer: A

Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key. The session is secure after this process.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION 267:

Choose the type of encryption used by SSL (Secure Sockets Layer).

A. Asymmetric key exchange.
B. Symmetric key exchange.
C. Public keys.
D. Secret encryption.

Answer: B

Explanation:
The Secure Sockets Layer (SSL) protocol uses both asymmetric and symmetric key exchange. It uses asymmetric keys for the SSL handshake. During the handshake, the master key is encrypted with the receivers public passes from the client to the server. The client and server make their own session keys using the master key. The session keys encrypt and decrypt data for the remainder of the session. Symmetric key exchange occurs during the exchange of the cipher specification, or encryption level.
Incorrect answers:
A: SSL makes use of symmetric key exchange not asymmetric keys.
C: Public keys are not necessarily symmetric and neither is it used in SSL.
D: Secret encryption does not mean symmetric key exchange which is used by SSL.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4

QUESTION 268:

SSL (Secure Socket Layer) establishes a stateful connection negotiated by a process performed between client and server.
Identify the protocol (steps) that allow for the following:
1. Client and server authentication.
2. MAC (Mandatory Access Control) and encryption algorithm negotiation.

3. Selection of cryptographic keys.

A. SSL (Secure Sockets Layer) alert protocol.
B. SSL (Secure Sockets Layer) change cipher spec protocol.
C. SSL (Secure Sockets Layer) record protocol.
D. SSL (Secure Sockets Layer) handshake protocol.

Answer: D

Explanation:
SSL Handshake Protocol
* runs before any application data is transmitted
* provides mutual authentication
* establishes secret encryption keys
* establishes secret MAC keys
Incorrect answers:
A: Handshake protocol occurs before alert protocol.
B: The change cipher spec protocol only occurs after the application protocol.
C: Record protocol encompasses the handshake, alert and change cipher spec protocols in SSL.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 178

QUESTION 269:

One of these protocols is used to encrypt traffic passed between a web browser and web server. Which is it?

A. IPSec (Internet Protocol Security)
B. HTTP (Hypertext Transfer Protocol)
C. SSL (Secure Sockets Layer)
D. VPN (Virtual Private Network)

Answer: C

Explanation:
The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines.
Incorrect answers:
A: IP Security (IPSec) is a security protocol that provides authentication and encryption across the Internet.
B: HTTP is the protocol used for communication between a web server and a web browser. Communication is not encryption.

D: A VPN is a system that uses the public Internet as a backbone for a private interconnection (network) between locations.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION 270:

Choose the protocol used by a web server to encrypt data.

A. TCP/IP (Transmission Control Protocol/Internet Protocol)
B. ActiveX
C. IPSec (Internet Protocol Security)
D. SSL (Secure Sockets Layer)

Answer: D

Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key. The session is secure after this process.
Incorrect answers:
A: TCP/IP) is the protocol suite developed by the DoD in conjunction with the Internet. It was designed as an internetworking protocol suite that could route information around network failures.
B: ActiveX is a technology implemented by Microsoft that allows customized controls, icons, and other features to increase the usability of web-enabled systems.
C: IP Security (IPSec) is a security protocol that provides authentication and encryption across the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION 271:

The SSL (Secure Sockets Layer) protocol offers session keys in two lengths or strengths. Which is it? Choose two correct answers.

A. 40-bit
B. 64-bit.
C. 128-bit.
D. 1,024-bit.

Answer:
A. C

Explanation:
SSL comes in two strengths, 40-bit and 128-bit, which refer to the length of the "session key" generated by every encrypted transaction. The longer the key, the more difficult it is to break the encryption code.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 4
http://wp.netscape.com/security/techbriefs/ssl.html

QUESTION 272:

From the list of protocols, which is used to secure web transactions?

A. S/MIME (Secure Multipurpose Internet Mail Extensions)
B. XML (Extensible Makeup Language)
C. SSL (Secure Sockets Layer)
D. SMTP (Simple Mail Transfer Protocol)

Answer: C

Explanation:
The Secure Socket Layer is used to establish a secure communication connection between two TCP-based machines. This protocol uses the handshake method. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key. The session is secure after this process.
Incorrect answers:
A: Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard used for encrypting e-mail.
B
: XML can be used to generate standard or fully customized content rich Web pages, documents, and applications. XML is used to provide widely accessible services and data to end users, exchange data among applications, and capture and represent data in a large variety of custom and standard formats.
D: SMTP is a protocol for sending e-mail between SMTP servers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 365

QUESTION 273:

One of the following options details the main advantage of why you should choose to use SSL (Secure Sockets Layer) over using HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer). Which is it?

A. SSL provides full application security for HTTP whereas HTTPS does not.
B. SSL supports additional Application layer protocols, for instance FTP (File Transfer Protocol) and NNTP (Network News Transport Protocol), whereas HTTPS does not.
C. SSL and HTTPS are transparent to the application.
D. SSL supports user authentication whereas HTTPS does not.

Answer: B

Explanation:
SSL on its own works at the session layer (layer 5) so it has more versatility in protocols that it supports.
Incorrect answers:
A: This is not the main advantage.
C: This is not an advantage when both have the same capability.
D: This is an advantage, but not the main difference and advantage between SSL and HTTPS.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION 274:

For a SSL (Secure Sockets Layer) connection to be automatically established between a web client and server, a specific element has to exist. Which is it?

A. Shared password.
B. Certificate signed by a trusted root CA (Certificate Authority).
C. Address on the same subnet.
D. Common operating system.

Answer: B

Explanation:
For an SSL connection to compete, the web client and server should have a trusted certificate to confirm authenticity.
A shared password, address on the same subnet, and a common operating system are ludicrous answers because they defy the reason why SSL exists.
Incorrect answers:
A: A shared password is not the way in which SSL allows a secure connection to be established.

C: An address on the same subnet does not necessarily mean an automatic connection.
D: A common operating system does not automatically mean a connection.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION 275:

SSLv3.0 (Secure Sockets Layer version 3.0) introduces a specific new capability with regard to security. Which is it?

A. The capability to act as a CA (Certificate Authority).
B. The capability to force client side authentication by using digital certificates.
C. The capability to use X.400 certificates.
D. The capability to protect data in transit by using 1024-bit symmetric encryption.

Answer: B

Explanation:
There are three versions of SSL out right now: SSL v.2, SSL v.3, and TLSv1 which is still going through standardization. SSL v.2 ensures encrypted data between client and serer. The server can authenticate the client, and the client can option to authenticate the server. SSL v.3 was enhanced for security and efficiency. It includes data compression, the ability of either the client or server requesting a renegotiation of the ciphers and shared key at any moment, and the use of certificate chains.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION 276:

You work as a security administrator at Certkiller .com. The Certkiller .com network must be configured to support SSL (Secure Sockets Layer).
Which ports must you open on the firewall to support SSL connections?

A. Open UDP (User Datagram Protocol) Transport layer protocol and port 80
B. Open TCP (Transmission Control Protocol) Transport layer protocol and port 80
C. Open TCP (Transmission Control Protocol) Transport layer protocol and port 443
D. Open UDP (User Datagram Protocol) Transport layer protocol and port 69

Answer: C

Explanation:
Secure Sockets Layer is secure, so it would be natural to assume that it uses the connection orientated TCP instead of UDP. Secondly, TCP port 80 is HTTP, which stands for (hyper text transfer protocol) TCP port 443 is HTTPS which stands for hyper

text transfer protocol over secure socket layer'
Incorrect answers:
A: UDP port 80 is meant for HTTP.
B: TCP port 80 is used for HTTP without the secure socket layer.
D: UDP port 69 is used for TFTP.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 2

QUESTION 277:

Choose the protocol or method that enables secure access to a web page, no matter what the browser type or vendor is.

A. Certificates with SSL (Secure Sockets Layer).
B. Integrated web with NOS (Network Operating System) security.
C. SSL (Secure Sockets Layer).
D. None of the above.

Answer: A

Explanation:
Regardless of whether or not you use Netscape Navigator or Microsoft Internet Explorer, if you come across a page with a security certificate and an SSL connection (most likely for banking, investments, or purchases) you will have secure access.
Incorrect answers:
B: Integrated web with NOS security do not guarantee secure access.
C: SSL only would be browser or vendor specific.
D: This is irrelevant.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION 278:

The SSL (Secure Sockets Layer) protocol operates between specific layers of the OSI (Open Systems Interconnection) reference model. Which is it? Choose all correct answers.

A. Application Layer.
B. Transport Layer
C. Network Layer
D. Data Link Layer
E. Physical Layer

Answer: A, B

Explanation:
SSL is associated with secure transactions (credit card purchases and online banking) over your web browser, so naturally it operates between the top two layers of the OSI model. SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
Incorrect answers:
C, D and E: The OSI model and SSL operates between the application layer and the transport layer not the Network, Data Link or Physical layers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128

QUESTION 279:

When compared to other messaging systems, which characteristic makes Instant Messaging particularly insecure?

A. The Instant Messaging messaging system is a peer-to-peer network that provides most organizations with practically no control over it.
B. Nearly all Instant Messaging clients are actually Trojan Horses.
C. The Instant Messaging messaging system is a centrally managed system that can be closely monitored.
D. Instant Messaging uses the insecure Internet as a transmission medium.

Answer: A

Explanation:

Answer: A seems to be the most correct of these answer.
Instant messaging is a form of immediate e-mail that takes place between two or more users. IM clients are often prone to hostile code (usually in the form of file transfers) and subject to social engineering attacks, wherein a hacker plays upon the culpability of a user to get what they need.
Incorrect answers:
B: Is incorrect because IM client are not Trojan Horses, but they can be compromised by Trojan Horses.
C: Is incorrect because the answer would make IM secure.
D: All IM messaging system that transverse the Internet uses it as a medium.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 21

QUESTION 280:

Choose the option that correctly details the greatest vulnerability of using Instant Messaging clients.

A. Results in theft of root user credentials.
B. Results in disconnection from the file server.
C. Results in malicious code being delivered by file transfer.
D. Results in slow Internet connections.
E. Results in loss of email privileges.
F. Results in Blue Screen of Death errors.

Answer: C

Explanation:
Instant Messaging (IM) enables users to communicate in real-time using text messages and to exchange files (pictures, music, and so on) with one another. Thus IM clients can also be compromised by malicious code, Trojan Horse programs, and traditional DoS attacks. IM clients are often prone to hostile code (usually in the form of file transfers) and subject to social engineering attacks, wherein a hacker plays upon the culpability of a user to get what they need.
Incorrect answers:
A: This is a result of spoofing.
B: This could result from a buffer overflow attack.
D: Slow internet connection could be ping of death attack results.
E: Loss of e-mail privileges is dependent on company policy.
F: Blue screen of Death errors is the result of a Winnuke attack.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 21

QUESTION 281:

Choose the option that correctly details the greatest flaw associated with an Instant Messaging messaging system.

A. Instant messaging is widely deployed and is therefore difficult to control and administer.
B. Instant messaging was created without consideration to security.
C. Instant messaging can easily be spoofed.
D. Instant messaging is created with file sharing enabled.

Answer: B

Explanation:
Instant messaging was created for speed and simplicity. They wanted a program that was feature rich, but not memory intensive so more people could be online more often. Since the text is unencrypted, it's very easy for someone to eavesdrop on a message, hijack the

conversation and send a virus that's disguised as an innocent graphic file.
Incorrect answers:
A: Other real time communication was designed with security in mind as well and is probable just as widely used.
C: A spoofing attack is an attempt by someone or something to masquerade as someone else. But in Instant Messaging this is not necessarily an attack. It could also be a safety measure.
D: Messaging is not necessarily file sharing.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 21

QUESTION 282:

Choose the attack that Instant Messaging is most vulnerable to.

A. DoS (Denial of Service) attacks.
B. Fraud attacks.
C. Stability.
D. Sniffing attacks.

Answer: D

Explanation:
Since instant messenger conversations are sent unencrypted (in clear-text) it's very easy for someone to use a sniffer on the line to eavesdrop on the entire conversation.
Incorrect answers:
A: DoS attacks are the result of flood attacks.
B: Fraud attacks do not usually result from Instant Messaging.
C: Stability? This is irrelevant in this case.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 21
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION 283:

Choose the privileges used to execute ActiveX control.

A. Current user account
B. Administrator account
C. Guest account
D. System account

Answer: A

Explanation:
When you are online and you execute an ActiveX control;the only thing that can control it, are the individual user settings of the current user.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 128

QUESTION 284:

Choose the function that is responsible for displaying an install dialog box for an ActiveX component

A. Browser setting of the user.
B. <script> meta tag.
C. Condition of the sandbox.
D. Negotiation between the client and the server.

Answer: A

Explanation:
ActiveX components are downloaded to the client hard disk, potentially allowing additional security breaches. Web browsers can be configured so that they require confirmation to accept an ActiveX control.
Incorrect answers:
B: This is not how ActiveX dialog boxes are installed.
C: The sandbox is a set of rules used when creating a Java applet that prevents certain functions when the applet is sent as part of a web page. This is not responsible for installing dialog boxes.
D: Negotiation between client and server is not how ActiveX dialog boxes are installed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 135

QUESTION 285:

From the options, which is used to prove where ActiveX controls originated from?

A. Encryption.
B. The location of ActiveX controls on the Web server.
C. SSL (Secure Sockets Layer) protocol.
D. Digital signatures.

Answer: D

Explanation:

ActiveX controls are digitally signed with an Authenticode signature, verified by a Certificate Authority. The controls are restricted by that signature only, not by the web browser settings.
Incorrect answers:
A: Encryption does not reveal origin.
B: Location of ActiveX controls on the Web server will not reveal where the controls originated from.
C: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 128,135
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 2

QUESTION 286:

Which scenario or element would typically cause a CGI (Common Gateway Interface) security issue?

A. The HTTP (Hypertext Transfer Protocol) protocol.
B. The compiler or interpreter which runs the CGI script.
C. The web browser.
D. The external data provided by the user.

Answer: D

Explanation:
Common Gateway Interface is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. The CGI script ran on the web server, and it interacted with the client browser. CGI is a doubtful choice in new applications because of its security issues, but it still widely used in older systems.
Although the answer is not given in the paragraph from the book, the answer would be D.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 136
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5

QUESTION 287:

You work as a network administrator at Certkiller .com. The Certkiller .com network contains a web server with CGI (Common Gateway Interface) scripts.
You want to configure permissions for the directories for public view.
Which permissions should you set?

A. Read permissions.
B. Execute permissions.
C. Read and Write permissions.
D. Read, Write, and Execute permissions.
E. Full Control permissions.

Answer: B

Explanation:
Common Gateway Interface is an older form of scripting that was used extensively in early web systems. CGI scripts could be used to capture data from a user using simple forms. The CGI script ran on the web server, and it interacted with the client browser. CGI is frowned upon in new applications because of its security issues, but it still widely used in older systems.
Incorrect answers:
A, C& D: CGI scripts are executed on the server and as such should have the execute permission in directories for public view.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 136, 217
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5

QUESTION 288:

Which of the following Directory Services does the statement that it is a standardized directory access protocol that allows queries to be made of directories refer to?

A. LDAP
B. Active Directory
C. X.500
D. eDirectory

Answer: A

Explanation:
LDAP Lightweight Directory Access Protocols (LDAP) is a standardized directory access protocol that allows queries to be made of directories (specifically, a pared down X.500-based directory). If a directory service supports LDAP, you can query that directory with an LDAP client, but it is the protocol. LDAP is growing in popularity and is being used extensively in online white and yellow pages.
Incorrect answers:
B: Active Directory Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. For Microsoft products, AD is the backbone for all security,

access, and network implementations from here on out. AD allows full control of resources by administrators. It is a proprietary directory service that provides services for other directory services, such as LDAP. AD functions are managed by one or more servers. These servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.
C: The X.500 standard was implemented by the International Telecommunications Union (ITU), an international standards group, for directory services in the late 1980s. The X.500 directory structure was the basis for later models of directory structure, such as LDAP. The major problem in the industry in implementing a full-blown X.500 structure revolved around the complexity of the implementation. Novell was one of the first manufacturers to implement X.500 in its NetWare NDS product.
D: eDirectory is the backbone for Novell networks. eDirectory stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server. eDirectory is an upgrade and replacement for NDS, and it has gained wide acceptance in the community.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 289:

Which of the following Directory Services does the statement that it is the backbone for all security, access, and network implementations from here on out refer to?

A. LDAP
B. Active Directory
C. X.500
D. eDirectory

Answer: B

Explanation:
Active Directory Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. For Microsoft products, AD is the backbone for all security, access, and network implementations from here on out. AD allows full control of resources by administrators. It is a proprietary directory service that provides services for other directory services, such as LDAP. AD functions are managed by one or more servers. These servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.
Incorrect answers:
A: LDAP Lightweight Directory Access Protocols (LDAP) is a standardized directory access protocol that allows queries to be made of directories (specifically, a pared down X.500-based directory). If a directory service supports LDAP, you can query that directory with an LDAP client, but it is the protocol. LDAP is growing in popularity and is being used extensively in online white and yellow pages.
C: The X.500 standard was implemented by the International Telecommunications Union

(ITU), an international standards group, for directory services in the late 1980s. The X.500 directory structure was the basis for later models of directory structure, such as LDAP. The major problem in the industry in implementing a full-blown X.500 structure revolved around the complexity of the implementation. Novell was one of the first manufacturers to implement X.500 in its NetWare NDS product.
D: eDirectory is the backbone for Novell networks. eDirectory stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server. eDirectory is an upgrade and replacement for NDS, and it has gained wide acceptance in the community.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 290:

Which of the following Directory Services does the statement that it was implemented by the International Telecommunications Union (ITU) refer to?

A. LDAP
B. Active Directory
C. X.500
D. eDirectory

Answer: C

Explanation:
The X.500 standard was implemented by the International Telecommunications Union (ITU), an international standards group, for directory services in the late 1980s. The X.500 directory structure was the basis for later models of directory structure, such as LDAP. The major problem in the industry in implementing a full-blown X.500 structure revolved around the complexity of the implementation. Novell was one of the first manufacturers to implement X.500 in its NetWare NDS product.
Incorrect answers:
A: LDAP Lightweight Directory Access Protocols (LDAP) is a standardized directory access protocol that allows queries to be made of directories (specifically, a pared down X.500-based directory). If a directory service supports LDAP, you can query that directory with an LDAP client, but it is the protocol. LDAP is growing in popularity and is being used extensively in online white and yellow pages.
B: Active Directory Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. For Microsoft products, AD is the backbone for all security, access, and network implementations from here on out. AD allows full control of resources by administrators. It is a proprietary directory service that provides services for other directory services, such as LDAP. AD functions are managed by one or more servers. These servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.
D: eDirectory is the backbone for Novell networks. eDirectory stores information on all

system resources, users, and any other relevant information about systems attached to a NetWare server. eDirectory is an upgrade and replacement for NDS, and it has gained wide acceptance in the community.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 291:

Which of the following Directory Services does the statement that it stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server refer to?

A. LDAP
B. Active Directory
C. X.500
D. eDirectory

Answer: D

Explanation:
eDirectory is the backbone for Novell networks. eDirectory stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server. eDirectory is an upgrade and replacement for NDS, and it has gained wide acceptance in the community.
Incorrect answers:
A: LDAP Lightweight Directory Access Protocols (LDAP) is a standardized directory access protocol that allows queries to be made of directories (specifically, a pared down X.500-based directory). If a directory service supports LDAP, you can query that directory with an LDAP client, but it is the protocol. LDAP is growing in popularity and is being used extensively in online white and yellow pages.
B: Active Directory Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. For Microsoft products, AD is the backbone for all security, access, and network implementations from here on out. AD allows full control of resources by administrators. It is a proprietary directory service that provides services for other directory services, such as LDAP. AD functions are managed by one or more servers. These servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.
C: The X.500 standard was implemented by the International Telecommunications Union (ITU), an international standards group, for directory services in the late 1980s. The X.500 directory structure was the basis for later models of directory structure, such as LDAP. The major problem in the industry in implementing a full-blown X.500 structure revolved around the complexity of the implementation. Novell was one of the first manufacturers to implement X.500 in its NetWare NDS product.
Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 292:

Which of the following definitions refers to LDAP?

A. It is a standardized directory access protocol that allows queries to be made of directories.
B. It is the backbone for all security, access, and network implementations from here on out.
C. It was implemented by the International Telecommunications Union (ITU).
D. It stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server.

Answer: A

Explanation:
LDAP Lightweight Directory Access Protocols (LDAP) is a standardized directory access protocol that allows queries to be made of directories (specifically, a pared down X.500-based directory). If a directory service supports LDAP, you can query that directory with an LDAP client, but it is the protocol. LDAP is growing in popularity and is being used extensively in online white and yellow pages.
Incorrect answers:
B: This refers to Active Directory
C: This refers to eDirectory
D: This refers to X.500
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 293:

Which of the following definitions refers to Active Directory?

A. It is a standardized directory access protocol that allows queries to be made of directories.
B. It is the backbone for all security, access, and network implementations from here on out.
C. It was implemented by the International Telecommunications Union (ITU).
D. It stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server.

Answer: B

Explanation:

Active Directory Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. For Microsoft products, AD is the backbone for all security, access, and network implementations from here on out. AD allows full control of resources by administrators. It is a proprietary directory service that provides services for other directory services, such as LDAP. AD functions are managed by one or more servers. These servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.
Incorrect answers:
A: This refers to LDAP
C: This refers to eDirectory
D: This refers to X.500
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 294:

Which of the following definitions refers to X.500?

A. It is a standardized directory access protocol that allows queries to be made of directories.
B. It is the backbone for all security, access, and network implementations from here on out.
C. It was implemented by the International Telecommunications Union (ITU).
D. It stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server.

Answer: C

Explanation:
The X.500 standard was implemented by the International Telecommunications Union (ITU), an international standards group, for directory services in the late 1980s. The X.500 directory structure was the basis for later models of directory structure, such as LDAP. The major problem in the industry in implementing a full-blown X.500 structure revolved around the complexity of the implementation. Novell was one of the first manufacturers to implement X.500 in its NetWare NDS product.
Incorrect answers:
A: This refers to LDAP
B: This refers to Active Directory
D: This refers to eDirectory
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 295:

Which of the following definitions refers to eDirectory?

A. It is a standardized directory access protocol that allows queries to be made of directories.
B. It is the backbone for all security, access, and network implementations from here on out.
C. It was implemented by the International Telecommunications Union (ITU).
D. It stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server.

Answer: D

Explanation:
eDirectory is the backbone for Novell networks. eDirectory stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server. eDirectory is an upgrade and replacement for NDS, and it has gained wide acceptance in the community.
Incorrect answers:
A: This refers to LDAP
B: This refers to Active Directory
C: This refers to X.500
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 296:

Which of the following Directory Services does the statement that it can identify an individual computer system on the Internet refer to?

A. DNS
B. Active Directory
C. X.500
D. eDirectory

Answer: A

Explanation:
DNS is one of the most popular directory services in use today. DNS can identify an individual computer system on the Internet. DNS, as you may recall, maps IP addresses to domain names and to individual systems..
Incorrect answers:
B: Active Directory Microsoft implemented a directory service called Active Directory (AD) with Windows 2000. For Microsoft products, AD is the backbone for all security, access, and network implementations from here on out. AD allows full control of resources by administrators. It is a proprietary directory service that provides services for

other directory services, such as LDAP. AD functions are managed by one or more servers. These servers are connected in a tree structure that allows information to be shared or controlled through the entire AD structure.
C: The X.500 standard was implemented by the International Telecommunications Union (ITU), an international standards group, for directory services in the late 1980s. The X.500 directory structure was the basis for later models of directory structure, such as LDAP. The major problem in the industry in implementing a full-blown X.500 structure revolved around the complexity of the implementation. Novell was one of the first manufacturers to implement X.500 in its NetWare NDS product.
D: eDirectory is the backbone for Novell networks. eDirectory stores information on all system resources, users, and any other relevant information about systems attached to a NetWare server. eDirectory is an upgrade and replacement for NDS, and it has gained wide acceptance in the community.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 297:

Which of the following definitions refers to DNS?

A. It is a standardized directory access protocol that allows queries to be made of directories.
B. It is the backbone for all security, access, and network implementations from here on out.
C. It was implemented by the International Telecommunications Union (ITU).
D. It can identify an individual computer system on the Internet.

Answer: D

Explanation:
DNS is one of the most popular directory services in use today. DNS can identify an individual computer system on the Internet. DNS, as you may recall, maps IP addresses to domain names and to individual systems.
Incorrect answers:
A: This refers to LDAP
B: This refers to Active Directory
C: This refers to X.500
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 243.

QUESTION 298:

Choose the mechanism (standard) that is similar to SSLv3 (Secure Sockets Layer version 3).

A. TLS (Transport Layer Security).
B. MPLS (Multi-Protocol Label Switching).
C. SASL (Simple Authentication and Security Layer).
D. MLS (Multi-Layer Switching).

Answer: A

Explanation:
Transport Layer Security is an end-to-end encryption protocol that is similar to and based on SSL version 3.0 except it uses stronger encryption, and not entirely interoperable. It is specified in ISO 10736 as part of the transport layer in a protocol stack;defined in RFC 2246.
Incorrect answers:
B: MPLS (Multi-Protocol Label Switching) is not similar to SSLv3.
C: Strong authentication over LDAP v3 is provided through Simple Authentication and Security Layer (SASL) communications defined in RFC 2222. This is not similar to SSLv3
D: Multi-Layer Switching is not the same as SSLv3.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION 299:

You work as the security administrator at Certkiller .com. The Certkiller .com network must be configured to allow LDAP (Lightweight Directory Access Protocol) traffic.
Which ports must you open on the firewall to allow LDAP traffic?

A. Open ports 389 and 636
B. Open ports 389 and 139
C. Open ports 636 and 137
D. Open ports 137 and 139

Answer: A

Explanation:
The 'well known' LDAP ports are 389 for LDAP and 636 for LDAP SSL.
Incorrect answers:
B: Port 139 is the NetBIOS session service port.
C: NetBIOS services occurs via ports 137, 138, and 139
D: Port 139 is the NetBIOS session service port.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda,

Sybex, 2004, p. 64
http://www.iana.org/assignments/port-numbers

QUESTION 300:

Choose the terminology that correctly refers to the start (top) of a LDAP (Lightweight Directory Access Protocol) directory.

A. Head
B. Root
C. Top
D. Tree

Answer: B

Explanation:
LDAP directories are arranged as trees. The top of the hierarchy is called the LDAP root. Below the topmost 'root' node, country information appears, followed by entries for companies, states or national organizations. Next comes entries for organizational units, such as branch offices and departments. Finally we locate individuals, which in X.500 and LDAP include people, shared resources such as printers, and documents. An LDAP directory server thus makes it possible for a corporate user to find the information resources she needs anywhere on the enterprise network.
Incorrect answers:
A: The top of the hierarchy is called the root and not the head.
C: This top is known as the root.
D: The whole directory is arranged as trees. And the top is called the root.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
http://www.intranetjournal.com/foundation/ldap.shtml

QUESTION 301:

Choose the terminology that correctly refers to the way in which the LDAP (Lightweight Directory Access Protocol) directory is structured.

A. As linked lists.
B. As trees.
C. As stacks.
D. As queues.

Answer: B

Explanation:
Directories are displayed best as directory trees, so naturally LDAP uses trees. LDAP is

based from an object-orientated access model built to directory enabled networking (DEN) standards.
The top of the hierarchy is called the LDAP root. The LDAP root server creates the hierarchy and the rest of the structure (and resources) branch out from that location.
LDAP uses objects to represent computers, user accounts, shared resources, services, and so on.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION 302:

Which of the following statements are true regarding Vulnerabilities and Sniffing?

A. FTP is a protocol, a client, and a server.
B. Security was based on the honor system.
C. As discussed earlier, SSH is a program that allows connections to be secured by encrypting the session between the client and the server.
D. The user ID and password are not encrypted and are subject to packet capture.

Answer: D

Explanation:
File sharing is accomplished by storing files on an assigned location on the server or workstation. When files are stored on a workstation, the connection is referred to as a peer-to-peer connection. The assigned location is typically a subdirectory located on one of the disk drives on the server or another workstation. In an FTP connection, a file can be uploaded from a client using the PUT command. A download with FTP is accomplished using the GET command. Most modern servers and applications allow an application program to access shared files at the record level.
Incorrect answers:
A: This refers to FTP Connections
B: This refers to Blind FTP/Anonymous
C: This refers to FTP Secure
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 135

QUESTION 303:

Which of the following definitions fit correctly to SSH?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol

D. It is a tunneling protocol originally designed for UNIX systems.

Answer: D

Explanation:
Secure Shell (SSH) is a tunneling protocol originally designed for UNIX systems. SSH uses encryption to establish a secure connection between two systems. SSH also provides security equivalent programs such as Telnet, FTP, and many of the other communications-oriented programs under UNIX.
Incorrect answers:
A: This refers to PPTP
B:This refers to L2F
C: This refers to L2TP
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 304:

Which of the following is not a tunneling protocol, but it is used in conjunction with tunneling protocols?

A. PPTP
B. L2F
C. L2TP
D. IPSec

Answer:

Explanation:
IPSec (Internet Protocol Security) is not a tunneling protocol, but it is used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, rather than dial-up connections. IPSec provides secure authentication and encryption of data and headers.
Incorrect answers:
A: PPTP supports encapsulation in a single point-to-point environment. PPTP encapsulates and encrypts PPP packets. This makes PPTP a favorite low-end protocol for networks. The negotiation between the two ends of a PPTP connection is done in the clear. Once the negotiation is performed, the channel is encrypted
B: L2F was created by Cisco as a method of creating tunnels primarily for dial-up connections. L2F is similar in capability to PPP and should not be used over WANs. L2F does provide authentication, but it does not provide encryption.
C: Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: the Layer Two Tunneling Protocol (L2TP). L2TP is a hybrid of PPTP and L2F. L2TP is primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX,

SNA, and IP.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 305:

Which of the following definitions fit correctly to IPSec?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is not a tunneling protocol, but it is used in conjunction with tunneling protocols.

Answer: D

Explanation:
IPSec (Internet Protocol Security) is not a tunneling protocol, but it is used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, rather than dial-up connections. IPSec provides secure authentication and encryption of data and headers.
Incorrect answers:
A: This refers to PPTP
B:This refers to L2F
C: This refers to L2TP
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 306:

Which of the following definitions fit correctly to L2F?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is a tunneling protocol originally designed for UNIX systems.

Answer: B

Explanation:
L2F was created by Cisco as a method of creating tunnels primarily for dial-up connections. L2F is similar in capability to PPP and should not be used over WANs. L2F does provide authentication, but it does not provide encryption.

Incorrect answers:
A: This refers to PPTP
C:This refers to L2TP
D: This refers to SSH
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 307:

Which of the following definitions fit correctly to L2TP?

A. It supports encapsulation in a single point-to-point environment
B. It was created by Cisco as a method of creating tunnels primarily for dial-up connections
C. It is primarily a point-to-point protocol
D. It is a tunneling protocol originally designed for UNIX systems.

Answer: C

Explanation:
Relatively recently, Microsoft and Cisco agreed to combine their respective tunneling protocols into one protocol: the Layer Two Tunneling Protocol (L2TP). L2TP is a hybrid of PPTP and L2F. L2TP is primarily a point-to-point protocol. L2TP supports multiple network protocols and can be used in networks besides TCP/IP. L2TP works over IPX, SNA, and IP.
Incorrect answers:
A: This refers to PPTP
B:This refers to L2F
D: This refers to SSH
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 122-125.

QUESTION 308:

Choose the protocol that is most vulnerable to packet sniffing attacks aimed at intercepting username and password information.

A. SSH (Secure Shell)
B. SSL (Secure Sockets Layer)
C. FTP (File Transfer Protocol)
D. HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)

Answer: C

Explanation:
FTP has a major flaw. The user ID and password are not encrypted and are subject to packet capture.
Incorrect answers:
A: Secure Shell (SSH) is a replacement for rlogin in Unix/Linux that includes security. rlogin allowed one host to establish a connection with another with no real security being employed ;SSH replaces it with slogin and digital certificates.
B: Secure Socket Layer (SSL) is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer.
D: Secure Hypertext Transfer Protocol (S-HTTP) is a protocol used for secure communications between a web server and a web browser.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 130

QUESTION 309:

You work as the security administrator at Certkiller .com. You must secure the FTP (File Transfer Protocol) server by allowing only authorized users access to it.
How will you accomplish this task?

A. Allow blind authentication.
B. Do not allow anonymous authentication.
C. Redirect FTP to a different port.
D. Provide the FTP server's address to only those users that must access it.

Answer: B

Explanation:
Early FTP servers did not offer security. Security was based on the honor system. Most logons to an FTP site used the anonymous logon. By convention, the logon ID was the user's email address, and the password was anonymous.
Incorrect answers:
A: Blind FTP is synonymous to anonymous FTP and allowing blind FTP is not the way to ensure that only authorized users access the FTP server.
C: Redirection will not prevent unauthorized access.
D: This is impractical as it will not prevent unauthorized access.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 137

QUESTION 310:

You work as the security administrator at Certkiller .com. You want to enable

anonymous FTP (File Transfer Protocol) read/write access.
Choose the important factor which you should consider and be aware of.

A. The upload and download directory for each user.
B. The detailed logging information for each user.
C. The storage and distribution of unlicensed software.
D. Less server connections and network bandwidth utilization.

Answer: C

Explanation:
Anonymous FTP is based on good faith. But if it used to take advantage of the non-secure logon, then answer C would seem to be the best answer.
Incorrect answers:
A: This is the legitimate use of an FTP site.
B
: You need to have a logon for any FTP (without anonymous access enabled) you want to access.
D: This is not the answer.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

QUESTION 311:

You work as the security administrator at Certkiller .com. You are investigating the consequences of networks attacks aimed at FTP servers.
Which of the following states the aim of a FTP (File Transfer Protocol) bounce attack?

A. The attack aims to exploit a buffer overflow vulnerability on the FTP server.
B. The attack aims to reboot the FTP server.
C. The attack aims to store and distribute malicious code.
D. The attack aims to establish a connection between the FTP server and another computer.

Answer: D

Explanation:
FTP bounce is a method that attackers use to protect their identity when scanning your network, by bouncing the scan off a vulnerable FTP server. In some implementations of FTP daemons, the PORT command can be misused to open a connection to a port of the attacker's choosing on a machine that the attacker could not have accessed directly.
Incorrect answers:
A: In an attack, the buffer overflow condition can be used to damage files, change data, acquire confidential information, or execute code on the target computer. The attacker

might even be able to gain full control over the target system.
B: Rebooting the server is not the aim of a FTP bounce attack.
C: The primary aim of a FTP bounce attack is to establish an illegitimate connection not storing and distributing malicious code. This is secondary.
References:
http://www.cert.org/advisories/CA-1997-27.html
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 1

QUESTION 312:

You work as the security administrator at Certkiller .com. The Certkiller .com network must be configured to allow FTP (File Transfer Protocol) traffic.
Which ports must you open on the firewall to allow FTP traffic?

A. Open ports 20 and 21.
B. Open ports 25 and 110.
C. Open ports 80 and 443.
D. Open ports 161 and 162.

Answer: A

Explanation:
In basic FTP operations, port 20 is the data port and port 21 is the command port.
Incorrect answers:
B: Port 25 is for SMTP. Port 110 is for POP3
C: Port 80 is used by HTTP (used for the World Wide Web) and port 443 for HTTPS (used for secure web connections)
D: Ports 161 and 162 are used for SNMP messages and traps respectively.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 64
http://www.iana.org/assignments/port-numbers

QUESTION 313:

Choose the ports that are used to access the FTP (File Transfer Protocol) protocol.

A. Ports 80 and 443.
B. Ports 20 and 21.
C. Ports 21 and 23.
D. Ports 20 and 80.

Answer: B

Explanation:

In basic FTP operations, port 20 is the data port and port 21 is the command port.
Incorrect answers:
A: Port 80 is used by HTTP (used for the World Wide Web) and port 443 for HTTPS (used for secure web connections)
C: Port 23 is used by Telnet.
D: Port 80 is used by HTTP.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 64
http://www.iana.org/assignments/port-numbers

QUESTION 314:

Which of the following Wireless standards has a maximum transmission speed of 54 Mbps? (Chose all that apply)

A. 802.11
B. 802.11a
C. 802.11b
D. 802.11g

Answer: B, D
IEEE 802.11a and IEEE 802.11g has transmission speeds of up to 54 Mbps.
Incorrect Answers:
A: IEEE 802.11, the original standard for wireless networks operates at a maximum speed of 2 Mbps.
C: IEEE 802.11b operates at a maximum speed of 11 Mbps.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, p. 66.

QUESTION 315:

Which of the following Wireless standards has a maximum transmission speed of 11 Mbps?

A. 802.11
B. 802.11a
C. 802.11b
D. 802.11g

Answer: C
IEEE 802.11b operates at a maximum speed of 11 Mbps.
Incorrect Answers:
A: IEEE 802.11, the original standard for wireless networks operates at a maximum speed of 2 Mbps.

B, D: IEEE 802.11a and IEEE 802.11g has transmission speeds of up to 54 Mbps.
Reference:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, p. 66.

QUESTION 316:

At what radio frequency does an IEEE 802.11g wireless network operate?

A. 2.4 GHz
B. 5.0 GHz
C. 5.4 GHz
D. 10 GHz

Answer: A
IEEE 802.11b and IEEE 802.11g uses the 2.4 GHz frequency band.
Incorrect Answers:
B: IEEE 802.11a uses the 5.0 GHz frequency band, not 802.11b.
C, D: NoIEEE wireless standard uses the 5.4 GHz or the 10 GHz frequency bands.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 249-252.

QUESTION 317:

At what radio frequency does an IEEE 802.11a wireless network operate?

A. 2.4 GHz
B. 5.0 GHz
C. 5.4 GHz
D. 10 GHz

Answer: B
IEEE 802.11a uses the 5 GHz frequency band.
Incorrect Answers:
A: IEEE 802.11b and IEEE 802.11g uses the 2.4 GHz frequency band frequency band.
C, D: No IEEE wireless standard uses the 5.4 GHz or the 10 GHz frequency bands.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 249-252.

QUESTION 318:

At what radio frequency does Bluetooth operate?

A. 2.4 GHz

B. 5.0 GHz
C. 5.4 GHz
D. 10 GHz

Answer: A
Bluetooth uses the 2.4 GHz frequency band.
Incorrect Answers:
B: IEEE 802.11a uses the 5.0 GHz frequency band.
C, D: Bluetooth does not use the 5.4 GHz or the 10 GHz frequency bands.
References:
David Groth and Toby Skandier, Network+ Study Guide (4th Edition), Sybex, Alameda CA, 2005, pp. 249-252.

QUESTION 319:

Which of the following characteristics form part of an IEEE (Institute of Electrical and Electronics Engineers) connection?

A. A low-power transmitter
B. A wireless device
C. An access point
D. All of the above

Answer: D

Explanation:
The primary method of connecting a wireless device to a network is with a wireless portal. A wireless access point is a low-power transmitter/receiver, also known as a transceiver, which is strategically placed for access. The portable device and the access point communicate using one of several communications protocols including IEEE 802.11 (also known as Wireless Ethernet).
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 109

QUESTION 320:

Which of the following is a hardware device that connects the digital signals from a computer to the analog telephone line?

A. Modem
B. Cell Phone
C. WLAN
D. PC

Answer: A

Explanation:
A modem is a hardware device that connects the digital signals from a computer to the analog telephone line. It allows these signals to be transmitted longer distances than are possible with digital signals. The word "modem" is an amalgam of the words "modulator" and "demodulator," which are the two functions that occur during transmission. Modems present a unique set of challenges from a security perspective.
Incorrect answers:
B: This device has its own means to connect to the internet
C: This device is used to connect computers
D: This device cannot connect to the internet without hardware such as a modem
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 114.

QUESTION 321:

By which of the following means do most cellular phones use?

A. Infrared
B. Radio Frequencies
C. Microwaves
D. None of the above

Answer: A

Explanation:
Infrared (IR) uses a type of radiation for communications. This infrared radiation allows a point-to-point connection to be made between two IR transceiver-equipped devices. IR is line of sight and is not secure, but the interception device must be either in position between the two connections or in an area where a reflection has occurred.
Incorrect answers:
B, C, D: These don't apply
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 114.

QUESTION 322:

Which of the following wireless communications technologies accomplishes communication by adding the data that is to be transmitted to a higher speed transmission?

A. DSSS
B. FHSS
C. ODFM

D. WTLS

Answer: A

Explanation:
DSSS accomplishes communication by adding the data that is to be transmitted to a higher speed transmission. The higher speed transmission contains redundant information to ensure data accuracy. Each packet can then be reconstructed in the event of a disruption.
Incorrect answers:
B: FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies. The changing or hopping is synchronized between both ends and appears to be a single transmission channel to both ends.
C: ODFM accomplishes communication by breaking the data into subsignals and transmitting them simultaneously. These transmissions occur on different frequencies or subbands.
D: WTLS provides reasonable security for mobile devices, and it is being widely implemented in wireless devices.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 177-179

QUESTION 323:

Which of the following wireless communications technologies accomplishes communication by hopping the transmission over a range of predefined frequencies?

A. DSSS
B. FHSS
C. ODFM
D. WTLS

Answer: B

Explanation:
FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies. The changing or hopping is synchronized between both ends and appears to be a single transmission channel to both ends.
Incorrect answers:
A: DSSS accomplishes communication by adding the data that is to be transmitted to a higher speed transmission. The higher speed transmission contains redundant information to ensure data accuracy. Each packet can then be reconstructed in the event of a disruption.
C: ODFM accomplishes communication by breaking the data into subsignals and transmitting them simultaneously. These transmissions occur on different frequencies or

subbands.
D: WTLS provides reasonable security for mobile devices, and it is being widely implemented in wireless devices.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 193.

QUESTION 324:

Which of the following wireless communications technologies accomplishes communication by breaking the data into subsignals and transmitting them simultaneously?

A. DSSS
B. FHSS
C. ODFM
D. WTLS

Answer: C

Explanation:
ODFM accomplishes communication by breaking the data into subsignals and transmitting them simultaneously. These transmissions occur on different frequencies or subbands.
Incorrect answers:
A: DSSS accomplishes communication by adding the data that is to be transmitted to a higher speed transmission. The higher speed transmission contains redundant information to ensure data accuracy. Each packet can then be reconstructed in the event of a disruption.
B: FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies. The changing or hopping is synchronized between both ends and appears to be a single transmission channel to both ends.
D: WTLS provides reasonable security for mobile devices, and it is being widely implemented in wireless devices.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 193.

QUESTION 325:

Which of the following statements best suits the wireless communication technology DSSS?

A. Accomplishes communication by adding the data that is to be transmitted to a higher speed transmission
B. Accomplishes communication by hopping the transmission over a range of predefined

frequencies
C. Accomplishes communication by breaking the data into subsignals and transmitting them simultaneously
D. Provides reasonable security for mobile devices, and it is being widely implemented in wireless devices

Answer: A

Explanation:
DSSS accomplishes communication by adding the data that is to be transmitted to a higher speed transmission. The higher speed transmission contains redundant information to ensure data accuracy. Each packet can then be reconstructed in the event of a disruption.
Incorrect answers:
B: This refers to FHSS.
C: This refers to ODFM.
D: This refers to WTLS.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 193.

QUESTION 326:

Which of the following statements best suits the wireless communication technology FHSS?

A. Accomplishes communication by adding the data that is to be transmitted to a higher speed transmission
B. Accomplishes communication by hopping the transmission over a range of predefined frequencies
C. Accomplishes communication by breaking the data into subsignals and transmitting them simultaneously
D. Provides reasonable security for mobile devices, and it is being widely implemented in wireless devices

Answer: B

Explanation:
FHSS accomplishes communication by hopping the transmission over a range of predefined frequencies. The changing or hopping is synchronized between both ends and appears to be a single transmission channel to both ends.
Incorrect answers:
A: This refers to DSSS.
C: This refers to ODFM.
D: This refers to WTLS.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 193.

QUESTION 327:

Which of the following statements best suits the wireless communication technology ODFM?

A. Accomplishes communication by adding the data that is to be transmitted to a higher speed transmission
B. Accomplishes communication by hopping the transmission over a range of predefined frequencies
C. Accomplishes communication by breaking the data into subsignals and transmitting them simultaneously
D. Provides reasonable security for mobile devices, and it is being widely implemented in wireless devices

Answer: C

Explanation:
ODFM accomplishes communication by breaking the data into subsignals and transmitting them simultaneously. These transmissions occur on different frequencies or subbands.
Incorrect answers:
A: This refers to DSSS.
B: This refers to FHSS.
D: This refers to WTLS.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 193

QUESTION 328:

From the options, which is commonly used by attackers to identify the existence of an 801.11b network?

A. War driving
B. Direct inward dialing
C. War dialing
D. Packet driving

Answer: A

Explanation:
War driving is the practice of literally driving around looking for free connectivity from Wi-Fi networks.

Incorrect Answers
B: Does not apply.
C: In war dialing combinations of numbers are tested to find network back doors via modem.
D: Does not apply.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 109

QUESTION 329:

You work as the security administrator at Certkiller .com. You want to prevent intruders from using access points on your wireless network?
Which solution should you implement?

A. ESP (Encapsulating Security Payload)
B. WEP (Wired Equivalent Privacy)
C. TLS (Transport Layer Security)
D. SSL (Secure Sockets Layer)

Answer: B

Explanation:
The 802.11 standard describes the communication that occurs in wireless local area networks (LANs). The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network ;this function isnot explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.
Incorrect answers:
A: ESP is a header used to provide a mix of security services in IPv4 and IPv6. ESP can be used alone or in combination with the IP Authentication Header (AH).
C: Transport Layer Security (TLS) is a protocol whose purpose is to verify that secure communications between a server and a client remain secure. Not exactly prevention of intruders.
D
: SSL is a protocol that secures messages by operating between the Application layer (HTTP) and the Transport layer. It does not prevent intruders from intruding.
References:
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

QUESTION 330:

You work as the security administrator at Certkiller .com. You want to implement a solution which will provide the following for handled devices in your wireless network:
1. Data privacy

2. Data integrity
3. Authentication
Which solution should you implement?

A. WEP (Wired Equivalent Privacy)
B. WAP (Wireless Application Protocol)
C. WSET (Wireless Secure Electronic Transaction)
D. WTLS (Wireless Transport Layer Security)

Answer: D

Explanation: Short for Wireless Transport Layer Security. WTLS is the security layer of the WAP, providing privacy, data integrity and authentication for WAP services.
Incorrect answers:
A: WEP is one of the most popular features available for a Wireless LAN. It is used to encrypt and decrypt data signals transmitted between Wireless LAN devices. In essence, WEP makes a wireless LAN link as secure as a wired link.
B: Wireless systems frequently use the Wireless Access Protocol (WAP) for network communications.
C: An electronic transaction is not the same as providing the means for secure communication insofar as privacy, data integrity and authentication is concerned.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 177-179

QUESTION 331:

WTLS (Wireless Transport Layer Security) provides security services between network devices or mechanisms. Which is it? Choose all that apply.

A. Web server.
B. Mobile device.
C. Wireless client.
D. Wireless network interface card.
E. WAP (Wireless Application Protocol) gateway

Answer: B, E

Explanation:
Since most wireless devices are low in: memory, processing power, and bandwidth capability creating a security mechanism is a difficult task. WTLS is the security layer of the Wireless Applications Protocol (WAP). WTLS provides authentication, encryption, and data integrity for wireless devices between a wireless device and the WAP gateway.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 177-178

QUESTION 332:

You work as the security administrator at Certkiller .com. You want to implement a solution which will provide a WLAN (Wireless Local Area Network) with the security typically associated with a wired LAN (Local Area Network):
Which solution should you implement?

A. WEP (Wired Equivalent Privacy)
B. ISSE (Information Systems Security Engineering)
C. ISDN (Integrated Services Digital Network)
D. VPN (Virtual Private Network)

Answer: A

Explanation:
Wired Equivalent Privacy is a wireless protocol designed to provide privacy equivalent to that of a wired network.
Incorrect answers:
B: This is not the method to supply security to a WLAN akin to a LAN.
C: ISDN is a telecommunications standard that is used to digitally send voice, data, and video signals over the same lines.
D: VPN is a system that uses the public Internet as a backbone for a private interconnection (network) between locations. This is not WLAN with the security levels akin to a LAN.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 372

QUESTION 333:

You work as the security administrator at Certkiller .com. You want to implement a solution which will secure the wireless network. The Certkiller .com wireless network environment uses access points as repeaters.
What should you do next to secure the wireless network?
Force users to use complex passwords.
Ensure that users are only using issued wireless cards.
Implement WEP (Wired Equivalent Privacy).
Force users to use Adhoc mode.

Answer: C

Explanation:
If every access point is secured to WEP standards, the entire range covered by the

wireless system will be encrypted to a security level that equals a conventional wired network, thus preventing sniffing and unauthorized 'drive by' access.
Incorrect answers:
A: Making use of complex passwords is not the same as repeaters.
B: Ensuring that wireless cards are used is not the same as providing security in the form of repeaters. This in fact might enhance the danger.
D
: Adhoc mode is the same as a point-to-point (ad-hoc or wireless bridge), a network created when two devices are brought within transmission range of each other. This is not the same as security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 186

QUESTION 334:

The Certkiller .com wireless network environment uses WEP (Wired Equivalent Privacy) to provide wireless security.
Choose the entity or entities that can authenticate to an access point.

A. Administrators only.
B. Anyone.
C. Only Certkiller .com users.
D. All Certkiller .com users that have the correct WEP (Wired Equivalent Privacy) key.

Answer: D

Explanation:
WEP relies on a secret key that is shared between a mobile station (eg. a laptop with a wireless Ethernet card) and an access point (ie. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. Server authentication requires the workstation to authenticate against the server (access point).
Incorrect answers:
A: This option should be more specific and mention from where the administrator operates from.
B: This is not true as this would make a farce of security.
C: Only users within the company are not correct since WEP applies to mobile users and the option should rather state users with the correct WEP key.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 117
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

QUESTION 335:

From the definitions, which correctly details the function of WEP (Wired Equivalent Privacy)?
WEP provides a WLAN (Wireless Local Area Network) with the level of security typically associated with a wired LAN (Local Area Network).
WEP provides a collision preventive method of media access for a WLAN (Wireless Local Area Network).
WEP provides a WLAN (Wireless Local Area Network) with a broader access area than that of a wired LAN (Local Area Network).
WEP makes it possible for radio frequencies to penetrate walls.

Answer: A

Explanation:
WEP is a security protocol for 802.11b (wireless) networks that attempts to establish the same security for them as would be present in a wired network. It is designed to provide privacy equivalent to that of a wired network.
Incorrect answers:
B: Providing collision prevention is not the purpose of WEP.
C: WEP is a security protocol, not a WLAN extender.
D: The purpose of WEP is not to allow radio frequencies to penetrate walls. That is just the way in which it is used.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 335

QUESTION 336:

Choose the structure which forms the basis of the WAP (Wireless Application Protocol) programming model.

A. Client, original server, WEP (Wired Equivalent Privacy) structure
B. Code design, code review, documentation structure
C. Client, original server, wireless interface card structure
D. Client, gateway, original server structure

Answer: D

Explanation:
Wireless networking is not unlike networking on cable. Computers can be connected to form a client/server network. Hubs and switches can be used to connect network segments and allow communications over a broader area.
WAP systems communicate using a WAP gateway system. The gateway converts information back and forth between HTTP and WAP, as well as encodes and decodes between the security protocols.
Incorrect answers:
A: There must be a gateway between client and server. WEP is intended to provide the

security for WAP.
B: This is not how WAP works.
C: The wireless interface card is not the same as a gateway.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 179

QUESTION 337:

Which of the following types of firewalls blocks ports?

A. Stateful Inspection Firewalls
B. Proxy Firewalls
C. Packet Filtering Firewalls
D. All of the above

Answer: C

Explanation:
Packet filtering firewalls passes or blocks traffic based on the type of application. This type of firewall decides whether to pass traffic based on the packet's addressing information and can also be based on IP addresses or ports.
Incorrect Answers:
A: With stateful inspection firewalls, information is retained through a state table which monitors the state of each communication connection. Stateful inspection firewalls works at the Network Layer to provide additional security through the evaluation of the IP header information.
B: A proxy firewall is an intermediary between your network and any other network. proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rules-based decisions about whether the request should be forwarded or refused.
D: C is the only correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.

QUESTION 338:

What is the rationale of implementing proxy firewalls in your network?

A. To monitor the state of network connections and retain information on network connections through a state table.
B. To provide services between the internal network and external network by processing requests from external networks.
C. To check traffic passing over a device and then either allow or deny traffic based on application type and port.

Answer: B

Explanation:
Proxy firewalls are implemented to provide services between the internal network and all external networks by processing requests received from external networks.
Incorrect Answers:
A: Stateful inspection firewalls monitor the state of network connections and retain information on network connections through a state table.
C: Packet filtering firewalls work by checking traffic passing over a device and allow or deny traffic based on application type and port.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.

QUESTION 339:

Which of the following types of firewalls monitors the state of all network connections, and tracks information on network connections?

A. Stateful Inspection Firewalls
B. Proxy Firewalls
C. Packet Filtering Firewalls
D. All of the above

Answer: A

Explanation:
With stateful inspection firewalls, information is retained through a state table. A stateful inspection firewall works at the Network Layer to provide an additional layer of security but it also monitors the state of each communication connection.
Incorrect Answers:
B: A proxy firewall is an intermediary between your network and any other network. proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rules-based decisions about whether the request should be forwarded or refused.
C: Packet filtering firewalls passes or blocks traffic based on the type of application. This type of firewall decides whether to pass it based on the packet's addressing information and can be based on IP addresses or ports.
D: Only stateful inspection firewalls tracks and retains information on each network connection, to provide an additional level of security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.

QUESTION 340:

If you need to implement a firewall solution that only watches TCP and UDP ports, and allows all traffic to be passed once a connection is established, what type of firewall would you implement?

A. Stateful Inspection Firewalls
B. Application filtering
C. Circuit-Level Firewall
D. None of the above

Answer: C

Explanation:
A circuit-level firewall works by monitoring and controlling TCP and UDP ports. Once a connection is established, the circuit-level firewall no longer monitors which data is being passed over the connection. All data is allowed because no further checking occurs on the contents of packets.
Incorrect Answers:
A: Withstateful inspection firewalls, should any attempt be made to perform an action that is non-standard for the specific protocol, that connection is immediately disconnected or dropped.
B: Application filtering monitors connections to check incoming e-mails for virus attachments.
D: A circuit-level firewall allows all traffic to be passed after the connection is allowed and established.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 341:

Which firewall type functions at the Network layer (layer 3) of Open System Interconnection (OSI) Reference Model?

A. Packet Filtering Firewalls
B. Application-Level Gateway
C. Circuit-Level Firewall
D. None of the above

Answer: A

Explanation:
Packet filtering firewalls function at the Network layer (layer 3) of the OSI Reference Model
Incorrect Answers:
B: AnApplication-level gateway works at the Application layer (layer 7) of the OSI Reference model.
C: A circuit level firewall works at the Session layer (layer 5) of the OSI Reference model.
D: Packet filtering firewalls work at the Network layer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 342:

What is the rationale of implementing packet filtering firewalls in your network?

A. To monitor the state of network connections and retain information on network connections through a state table.
B. To provide services between the internal network and external network by processing requests from external networks
C. To check traffic passing over a device and either allow or deny traffic based on application type and port.

Answer: C

Explanation:
Packet filtering firewalls passes or blocks traffic based on the type of application. This type of firewall decides whether to pass it based on the packet's addressing information and can be based on IP addresses or ports.
.
Incorrect Answers:
A: Stateful inspection firewalls monitor the state of network connections and retain information on network connections through a state table.
B: Proxy firewalls are implemented to provide services between the internal network and all external networks, by processing requests received from external networks.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.

QUESTION 343:

Which of the following statements regarding stateful inspection firewalls is FALSE?

A. Stateful inspection firewalls features combine the features of the circuit-level filtering, the packet filtering firewall and an application-level gateway.
B. Stateful inspection firewalls add an additional layer of security.
C. Stateful inspection firewalls monitor the state of connections, using a state table.
D. Stateful inspection firewalls work at the Network layer only to collect information on the packet's communication channel.

Answer: D

Explanation:
Stateful inspection firewalls work at all levels or layers of the network to collect information on the communication channel of a packet to determine whether a packet is firewalls can determine whether a packet is still valid with regard to the context in which it turned up.
Incorrect Answers:
A, B, C: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 344:

Which firewall type functions at the Session Layer of Open System Interconnection (OSI) Reference Model?

A. Packet Filtering Firewalls
B. Application-Level Gateway
C. Circuit-Level Firewall
D. None of the above

Answer: C

Explanation:
A circuit level firewall works at the Session layer (layer 5) of the OSI Reference model.
Incorrect Answers:
A: Packet filtering firewalls function at the Network layer (layer 3) of the OSI Reference Model.
B: Anapplication-level gateway works at the Application layer (layer 7) of the OSI Reference model.
D: C is the correct answer. A circuit level firewall works at the Session layer.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 345:

When designing a firewall solution, which policies should be considered in conjunction with the basic firewall types?

A. Network policy.
B. Service access policy.
C. Firewall design policy.
D. Authentication policy.
E. All of the above policy types

Answer: E

Explanation:
Network policy details general network issues with regard to application usage and solutions to lock down firewalls. Service access policy pertains to communication issues between the internal network and remote services accessible on the Internet. Firewall design policy deals with ways in which firewalls process traffic rules specified by the administrators. Authentication policies involve issues of defining secure user authentication methods.
Incorrect Answers:
A: B, C, and D are also part of the correct answer.
B: A, C, and D are also part of the correct answer.
C: A, B, and D are also part of the correct answer.
D: A, B, and C are also part of the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 346:

At which layer of the of Open System Interconnection (OSI) Reference Model does stateful inspection occur?

A. Network Layer
B. Session Layer

C. Application Layer
D. All layers of the network

Answer: D

Explanation:
Stateful inspection firewalls work at all levels or layers of the network to collect still valid with regard to the context in which it arrived.
Incorrect Answers:
A: Packet filtering firewalls function at the Network layer of the OSI Reference model
B: A circuit level firewall works at the Session layer (layer 5) of the OSI Reference model.
C: Anapplication-level gateway works at the Application layer (layer 7) of the OSI Reference model.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 347:

In which of the following policy types do you find rules that allow all traffic unless explicitly denied, or deny all traffic unless explicitly permitted?

A. Network policy
B. Service access policy
C. Firewall design policy
D. Authentication policy

Answer: C

Explanation:
Firewall design policy deals with ways in which firewalls process traffic filter rules specified by the administrators. Rules are defined that allow all traffic unless explicitly denied or deny all traffic unless explicitly permitted
Incorrect Answers:
A: Network policy details general network issues with regard to application usage and solutions to lock down firewalls.
B: Service access policy pertains to communication issues between the internal network and remote services accessible on the Internet.
D: Authentication policies involve issues of defining secure user authentication methods.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press,

Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 348:

Packet filter rules can accept or reject network packets based on which of the following criteria?

A. Source and destination IP address
B. TCP or UDP port
C. IP protocol ID
D. ICMP message type.
E. All of the above

Answer: E

Explanation:
A packet filtering firewall allows or denies packets based on network data packet fields: Source and destination IP address, TCP or UDP port, IP protocol ID and ICMP message type
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp.100-104.

QUESTION 349:

Which of the firewall types allow you to configure security devices with the rate of responses to requests to handle, and block any impending communications from suspicious hosts?

A. Packet Filtering Firewalls
B. Application-Level Gateway
C. Circuit-Level Firewall
D. None of the above

Answer: C

Explanation:
You can use a circuit-level firewall to configure security devices with the rate of responses to requests to process, block any impending communications from suspicious hosts, and specify that administrators should be alerted when security breaches occur
Incorrect Answers:

A: Packet filtering firewalls allow or blocks traffic based on the type of application. This type of firewall decides whether to pass traffic based on the packet's addressing information and can be based on IP addresses or ports.
B: Anapplication-level gateway works as a proxy server between the inside network perimeter and an external server to monitor and control external communications.
D: A circuit-level firewall solution is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 350:

Which of the following network devices is considered the simplest in a networking environment and most vulnerable to attacks, because they serve as central connectivity devices between hosts, where traffic sent to one port is sent to all other ports?

A. Hubs
B. Routers
C. Switches and bridges
D. All of the above

Answer: A

Explanation:
Hubs are network devices that allow many hosts to inter-communicate through the usage of physical ports. This makes hubs central connectivity devices and prone to being attacked. Traffic sent to one port is sent from all other ports. Hubs are considered highly unsecure because they enable flat network topologies.
Incorrect Answers:
B: Routers enable connectivity between two or more networks. Routers can connect multiple network segments into one network.
C: Switches and bridges are multiport devices that make switching and bridging decisions based on the media access control (MAC) address of each network interface. These devices are used to improve the efficiency of the network.
D: A is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 107.

QUESTION 351:

Which of the following statements are TRUE?

A. Network policy is further divided into high-level policy and low-level policy.
B. Application policy deals with communication between the internal network and external networks.
C. Low-level policy, a subcategory of network policy, deals with which applications can be used on the network.
D. Authentication policy deals with excluding the internal use of unauthorized external services as well as excluding the unauthorized external use of internal services.

Answer: A

Explanation:
Network policy is further divided into high-level policy and low-level policy. Low-level policy deals with how to place administrative controls on the network to lock down firewalls, and high-level policy deals with application usage.
Incorrect Answers:
B: Service access policy deals with communication between the internal network and external networks.
C: Low-level policy deals with how to place administrative controls on the network to lock down firewalls, and high-level policy deals with application usage.
D: Firewall solutions deal with excluding the internal use of unauthorized external services and excluding the unauthorized external use of internal services.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 352:

Which of the following statements on the security capabilities of switches are FALSE?

A. Switches improve network security because the usage of virtual circuits makes it not easily examinable through network monitoring tools.
B. Switches should be implemented if you have media contention problems.
C. Switches should not be considered as a replacement for conventional security devices.
D. Switching between two connections is always encrypted.
E. Switches only maintain limited routing information on systems residing in the internal network.

Answer: D

Explanation:
Switching between two connections is usually not encrypted. This is one of the reasons

why switching devices should not be regarded as replacements for the conventional security devices.
Incorrect Answers:
A, B, C, E: These statements are all TRUE.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 108.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 353:

Which of the following network devices have replaced the usage of multiport repeaters in the network, because they are typically prone to attack and enable unsecure networking environments?

A. Hubs
B. Routers
C. Switches
D. None of the above

Answer: C

Explanation:
Switches improve the efficiency of the network and can also protect your network from packet sniffers attempting to collect information on the network.
Incorrect Answers:
A: Hubs enable many hosts to inter-communicate through the usage of physical ports and are considered highly unsecure because they enable flat network topologies.
B: Routers enable connectivity between two or more networks. Routers can connect multiple network segments into one network.
D: C is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 107.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3

QUESTION 354:

Which of these network devices maintain tables that contain MAC address information and operate at Layer 2 of the OSI Reference Model?

A. Hubs

B. Switches and bridges
C. Routers
D. None of the above

Answer: B

Explanation:
Switches and bridges maintain MAC address information in their forwarding database, and also work at Layer 2.
Incorrect Answers:
A: Hubs provide central connectivity between hosts on the network.
C: Routers maintain ARP caches and routing tables that contain information on remote destination networks and connections.
D: B is the correct answer
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 107.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3

QUESTION 355:

Which of the following network devices can be configured to work as a packet-filtering firewall and also provide advanced firewall functions?

A. Hubs
B. Routers
C. Bridges
D. Switches

Answer: B

Explanation:
Routers can be configured to work as packet filtering firewalls. The more advanced series routers can provide advanced firewall functions as well.
Incorrect Answers:
A: Hubs are highly unsecure but do however enable you to set up port security. Port security can become problematic in environments where ports have to continuously be reconfigured.
C, D: Switches allow you to provide some protection from a user attempting to probe into the network but need additional security against more advanced threats. Switches can be configured for MAC filtering and port access control
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 107.

Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3

QUESTION 356:

Which of the following statements are TRUE as methods for securing routers?

A. Routers should be kept in locked rooms.
B. You should use complex passwords for administrative consoles.
C. Routers should be kept current with the latest available vendor security patches.
D. Configure access list entries to prevent unauthorized connections and routing of traffic.
E. Use monitoring equipment to protect connection points and devices.
F. All of the above

Answer: F

Explanation:
Each of the statements details methods for securing routers within your networking environment.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 357:

Which of the following network devices enable connectivity between two or more networks and can connect multiple network segments into one network?

A. Hubs
B. Routers
C. Bridges and switches
D. All of the above

Answer: B

Explanation:
Routers enable connectivity between two or more networks and can connect multiple network segments into one network.
Incorrect Answers:
A: Hubs or multiport repeaters allow many hosts to inter-communicate through the usage of physical ports and are considered highly unsecure because they enable flat network topologies.
C: Switches and bridges combine the features of routers and hubs to improve the

efficiency and performance of the network
D: B is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 107.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3

QUESTION 358:

Which of the following statements are TRUE as methods for securing switches?

A. Switches should be kept in locked rooms.
B. You should use complex passwords for administrative consoles.
C. Switches should be kept current with the latest available vendor security patches.
D. Use monitoring equipment to protect connection points and devices.
E. All of the above

Answer: E

Explanation:
Each of the statements details methods for securing switches within your networking environment.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 359:

Which of the following network devices is regarded as your first line of defense and should therefore be configured to only forward traffic which is authorized?

A. Hubs
B. Routers
C. Bridges and switches
D. All of the above

Answer: B

Explanation:
Routers are the first line of defense and should therefore be configured to forward only traffic that is authorized. Access entries can be specified to allow only authorized traffic and deny unauthorized traffic.
Incorrect Answers:

A: Hubs allow many hosts to inter-communicate through the usage of physical ports and are considered highly unsecure because they enable flat network topologies.
C: Switches and bridges combine the features of routers and hubs to improve the efficiency of the network
D: B is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 107.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3

QUESTION 360:

Which network device allows clients to use dial-up connections to access servers and internal networks?

A. Routers
B. Switches and bridges
C. Remote access servers
D. Modems

Answer: C

Explanation:
Remote access servers (RAS) allow clients to use dial-up connections to access servers and internal networks. RAS connections are achieved through dial-up and network technologies, including VPN (Virtual Private Network), DSL, and cable modems.
Incorrect Answers:
A: Routers enable connectivity between two or more networks and can connect multiple network segments into one network.
B: Switches and bridges are multiport devices that make switching and bridging decisions based on the media access control (MAC) address of each network interface.
D: Modems enable the digital signals from a computer to be connected to the analog telephone line. Modems are however being replaced by faster cable and DSL connections.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 110.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 361:

Which type of dial-up and network technology is prone to dial-tone attacks?

A. Dial-tone modems
B. Cable modems
C. DSL modems
D. None of the above

Answer: A

Explanation:
Dial-tone modems have low throughput and are fairly easy to flood with useless traffic, which means that dial-tone modems are easy targets for launching denial of service attacks.
Incorrect Answers:
B: Cable modems are not vulnerable to dial-tone modem attacks, but are however vulnerable to attack because Internet access is provided using a shared coaxial cable.
C: DSL modems, like cable modems are not vulnerable to dial-tone modem attacks.
D: Dial-tone modems are easy targets of dial-tone modem attacks.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 109 - 110.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 362:

Which of the following is NOT a typical method of securing remote access servers?

A. Implementing a strong authentication method or two-factor authentication.
B. Limiting which users are allowed to dial-in and limiting the dial-in hours.
C. Implementing account lockout and strict password policies.
D. Securing physical connections to network segments
E. Implementing a real-time alerting system.

Answer: D

Explanation:
All other methods are typical methods of securing remote access servers. Securing physical connections to network segments are typical for securing routers, switches, and bridges.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 363:

Which of the following dial-up and network technologies are used to enable remote access server connections?

A. DSL
B. VPN (Virtual Private Network)
C. Cable modems
D. ISDN
E. All of the above

Answer: E

Explanation:
DSL, VPNs, cable modems and ISDN are used to enable remote access connections, so that clients can use dial-up connections to access servers and internal networks.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 110.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 364:

Which of the following is your RAS environment always vulnerable to?

A. PBX vulnerabilities.
B. RAS software bugs and buffer overflows.
C. Social engineering.
D. All of the above.

Answer: D

Explanation:
The RAS environment is vulnerable to public PBX infrastructure vulnerabilities, RAS software bugs, buffer overflows, and social engineering. You should apply vendor security patches as soon as they are available to protect against RAS software bugs. Social engineering and the public PBX infrastructure is a common method used by intruders to access your RAS environment.
Incorrect Answers:
A: The RAS environment is also vulnerable to RAS software bugs, buffer overflows, and social engineering.
B:

The RAS environment is also vulnerable to RAS PBX vulnerabilities and social engineering.
C: The RAS environment is also vulnerable to RAS PBX vulnerabilities, and RAS software bugs and buffer overflows.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 365:

Which network device allows two-factor authentication to be implemented, based on the usage of smart cards?

A. Routers
B. Switches and bridges
C. Remote access servers
D. Modems

Answer: C

Explanation:
Remote access servers (RAS) connections can be secured through two-factor authentication. The user must have the physical card and a PIN to access the system.
Incorrect Answers:
A: Routers, being the first line of defense, are usually configured with access entries to allow only authorized traffic.
B: Switches and bridges are used to improve the efficiency of the network.
D: Modems enable the digital signals from a computer to be connected to the analog telephone line.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 110 - 114.

QUESTION 366:

For securing wireless networking environments, which of the following is an IEEE 802.11b defined method for user authentication?

A. Layer 2 Tunneling Protocol (L2TP)
B. IP Security (IPSec) protocol
C. Extensible Authentication Protocol over LANs (EAPOL)
D. Point-to-Point Tunneling Protocol (PPTP)

Answer: C

Explanation:
An IEEE 802.11b defined method for enabling user authentication in wireless networking environments is Extensible Authentication Protocol over LANs (EAPOL). EAPOL provides the means for vendors to supply a standard method for granting access to authorized wireless users. Wireless access points enable you to secure authentication. This is done by setting a specific access code on the wireless network interface card (NIC) and access point.
Incorrect Answers:
A: Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used by VPNs.
B: Internet Protocol Security (IPSec) is used by VPNs to provide secure tunnel communications between two VPN peers. VPNs use encryption and authentication to protect data passing within the tunnel.
D: Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol used by VPNs, based on the Point-to-Point Protocol (PPP).
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 112 - 114.

QUESTION 367:

Of the tunneling protocols listed below, which one provides authentication and encryption, and is regarded as the stronger security standard?

A. Layer 2 Tunneling Protocol (L2TP)
B. IP Security (IPSec) protocol
C. Extensible Authentication Protocol over LANs (EAPOL)
D. Point-to-Point Tunneling Protocol (PPTP)

Answer: B

Explanation:
IPSec provides data authentication and encryption services. In Transport mode, only the payload is encrypted. In Tunneling mode, both the payload and message headers are encrypted.
Incorrect Answers:
A: L2TP does not encrypt data and therefore does not provide data security.
C: Extensible Authentication Protocol over LANs (EAPOL) is used to secure wireless networks.
D: PPTP is weaker than IPSec because the negotiation between the two points of a PPTP connection is performed in clear text. Only after the negotiation is performed is data encrypted.
References:
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 368:

With regard to securing your PBX system, which of the following strategies does not apply?

A. You should block all toll numbers and limit long-distance calling.
B. Implement a PBX password change and audit policy.
C. Allow dial-in only and force callback to a preset number.
D. You should secure all maintenance ports.
E. Limit the number of entry points

Answer: C

Explanation:
Allowing dial-in only and forcing callback to a preset number are strategies for securing remote access servers (RAS).
Incorrect answers:
A, B, D, E: These are all methods for securing your PBX system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 110 - 112.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 369:

Which of the following protocols is not used in VPN tunneling communication, to secure the data being tunneled?

A. Layer 2 Tunneling Protocol (L2TP)
B. IP Security (IPSec) protocol
C. Extensible Authentication Protocol over LANs (EAPOL)
D. Point-to-Point Tunneling Protocol (PPTP)

Answer: C

Explanation:
Extensible Authentication Protocol over LANs (EAPOL) is used to secure wireless networks
Incorrect Answers:
A: Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used by VPNs.
B: Internet Protocol Security (IPSec) is used in VPNs to provide secure tunnel channels between two VPN peers.
D: Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol used by VPNs, and is based on the Point-to-Point Protocol (PPP).
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 112 - 114.

QUESTION 370:

Which type of technology runs on workstations or network devices to monitor and track network activity, and can be configured to raise an alarm when security breaches occur?

A. IP Security (IPSec) protocol
B. Packet filtering firewall
C. Intrusion Detection Systems (IDSs)
D. Circuit-level firewall

Answer: C

Explanation:
An Intrusion Detection Systems (IDSs) can run on network devices and on individual workstations. You can configure the IDS to monitor for suspicious network activity, check systems logs, perform stateful packet matching, and disconnect sessions that are violating your security policy.
Incorrect Answers:
A: IPSec provides data authentication and encryption services for securing VPNs. In Transport mode, only the payload is encrypted. In Tunneling mode, both the payload and message headers are encrypted.
B: Packet filtering firewalls allow or blocks traffic based on the type of application. This type of firewall decides whether to pass traffic based on the packet's addressing information and can be based on IP addresses or ports.
D: Circuit-level firewalls watch TCP and UDP ports and can be used to configure security devices with the rate of responses to requests to process, and to block any impending communications from suspicious hosts.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 114.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 371:

Blocking all toll numbers and limiting long-distance calling is a method of securing which systems or devices?

A. PBX system
B. Remote access server
C. Switches and bridges
D. Routers

Answer: A

Explanation:
You can secure your PBX system by blocking all toll numbers and limiting long-distance calling. Other methods include implementing a PBX password change and audit policy. You can also limit the number of entry points.
Incorrect Answers:
B: RAS connections can be secured through two-factor authentication. The user must have the physical card and a PIN to access the system.
C: Switches and bridges are used to improve the efficiency of the network.
D: Routers should be configured with access entries to allow only authorized traffic.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 114.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 372:

Of the protocols listed below, which can be used to transport TCP/IP traffic but is neither efficient nor secure?

A. Layer 2 Tunneling Protocol (L2TP)
B. Extensible Authentication Protocol over LANs (EAPOL)
C. Point-to-Point Tunneling Protocol (PPTP)
D. Serial Line Internet Protocol (SLIP)

Answer: D

Explanation:
SLIP has been replaced by the Point-to-Point Protocol (PPP) because it is neither efficient nor secure. SLIP is generally only supported by systems to provide support for legacy systems.
Incorrect Answers:
A: L2TP does not encrypt data and does not provide data security. It is though stronger than SLIP. PPP has replaced the usage of SLIP. L2TP is based on the PPP protocol.
B: Extensible Authentication Protocol over LANs (EAPOL) is used to secure wireless networks.
C: PPTP encrypts data after negotiation has occurred.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 118 - 120.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 373:

Which of the following configurations can be performed on an Intrusion Detection System (IDS)?

A. Configure the IDS to perform stateful packet matching and monitor for suspicious network activity
B. Configure the IDS to provide data authentication and encryption services for securing VPNs
C. Configure the IDS to allow or blocks traffic based on the type of application.
D. Configure the IDS to watch TCP and UDP ports and block any impending communications from suspicious hosts.

Answer: A

Explanation:
You can configure the IDS to monitor for suspicious network activity, check systems logs, perform stateful packet matching, and disconnect sessions that are violating your security policy.
Incorrect Answers:
B: IPSec provides data authentication and encryption services for securing VPNs.
C: Packet filtering firewalls allow or blocks traffic based on the type of application.
D: Circuit-level firewalls watch TCP and UDP ports and can be used to configure security devices with the rate of responses to requests to process, and to block any impending communications from suspicious hosts.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 114.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 374:

With regard to securing your PBX system, which of the following strategies is relevant?

A. You should block all toll numbers and limit long-distance calling.
B. Allow dial-in only and force callback to a preset number.
C. Limit which users are allowed to dial-in and limit the dial-in hours
D. Secure physical connections

Answer: A

Explanation:
Blocking all toll numbers and limiting long-distance calling is specific to securing the PBX system.

Incorrect answers:
B: Allowing dial-in only and forcing callback to a preset number are strategies for securing remote access servers (RAS).
C: Limiting which users are allowed to dial-in and limiting the dial-in hours is a strategy for securing remote access servers.
D: Securing physical connections is more specific for securing routers, switches and bridges.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 110 - 112.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 375:

Which type of technology can monitor and track system logs and network activity, and raise an alarm when security breaches occur?

A. IP Security (IPSec) protocol
B. Packet filtering firewall
C. Intrusion Detection Systems (IDSs)
D. Circuit-level firewall

Answer: C

Explanation:
An Intrusion Detection Systems (IDSs) can run on network devices and on individual workstations, and can be configured to check systems logs and raise an alarm when security breaches occur.
Incorrect Answers:
A: IPSec provides data authentication and encryption services for securing VPNs.
B: Packet filtering firewalls allow or blocks traffic based on the type of application. This type of firewall decides whether to pass traffic based on the packet's addressing information and can be based on IP addresses or ports.
D: Circuit-level firewalls watch TCP and UDP ports and can be used to configure security devices with the rate of responses to requests to process, and to block any impending communications from suspicious hosts.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 104 - 114.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 376:

Of the strategies listed below, which is not specific for securing modem dialing

software?

A. Monitor computers that have modems to check whether they have been compromised
B. Block toll numbers and limit long-distance calling
C. Check for software updates for computers that have modems.
D. Remove all unnecessary modems from computers.

Answer: B

Explanation:
Blocking toll numbers and limiting long-distance calling are strategies for securing PBX systems
Incorrect Answers:
A, C, D: These are strategies for securing modems.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 109 - 110.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 3

QUESTION 377:

Of the modes of operation listed below, specific to IDS systems, which one does not apply?

A. A passive IDS informs the administrator when an attack is underway and carries out a predefined action to protect the network from further attacks.
B. A host-based IDS runs on a host to monitor communications, system logs and file systems, and can detect suspicious activities.
C. A network IDS tracks network traffic to isolate suspicious traffic.
D. A misuse IDS works by detecting network traffic patterns that match any of the attack patterns contained in the attack pattern database.
E. An anomaly IDS system uses predefined norms to differentiate between acceptable traffic and suspicious traffic.

Answer: A

Explanation:
A passive IDS can only inform the administrator when an attack is underway. It cannot carry out a predefined action to protect the network from further attacks. An active IDS system can monitor attacks and perform a predefined action to prevent the intruder from performing further damage.
Incorrect Answers:
B, C, D, E: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex,

Alameda, 2004, p. 115.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 378:

When describing the features of an IDS system, which of the following statements are FALSE?

A. An IDS uses signature matching to identify attacks that are underway within the network
B. An IDS system can work together with a firewall to increase security.
C. An IDS works by preventing attacks before they occur and can also block unauthorized traffic from entering the network
D. An IDS can be set up to drop sessions that are violating security policy.

Answer: C

Explanation:
A firewall system works by preventing attacks before they occur and can block unauthorized traffic from entering the network. Firewall systems are the first line of defense. Should your first of defense be compromised, then an IDS system can monitor the network for suspicious activity and can also be configured to prevent an attack in progress from causing further damage.
Incorrect Answers:
A, B, D: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 115.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 379:

What is the rationale of implementing a host-based IDS system?

A. To monitor the network, inform the administrator when an attack is underway, and carry out a predefined action to protect the network from further attacks.
B. To run on a host in the network, to monitor communications, monitor system logs and file systems, and detect suspicious activities.
C. To track network traffic to isolate suspicious traffic.
D. To detect network traffic patterns that match any of the attack patterns contained in the attack pattern database.

Answer: B

Explanation:
Host-based IDS systems run on hosts in the networks. These IDS systems monitor communications, file systems, system logs to detect suspicious activities.
Incorrect Answers:
A: An active IDS system can inform the administrator when an attack is underway, and can carry out a predefined action to protect the network from further attacks.
C: A network IDS system tracks network traffic to isolate suspicious traffic.
D: A misuse IDS works by detecting network traffic patterns that match any of the attack patterns contained in the attack pattern database.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 115.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 380:

Of the statements listed below on active and passive IDS analysis, which is FALSE?

A. A passive IDS can inform the administrator when an attack
B. Active and passive IDS analysis involves detecting network traffic patterns that match known attack patterns.
C. An active IDS works by performing a predefined action to protect the network from further attacks.
D. Active and passive IDS analysis IDS monitor the network for attacks that are underway.

Answer: B

Explanation:
Misuse and anomaly analysis IDS systems monitor the network for traffic patterns that match known attack patterns
Incorrect Answers:
A, C, D: These statements are all TRUE.

QUESTION 381:

Which type of IDS system uses predefined norms to differentiate between acceptable traffic and suspicious traffic?

A. A passive IDS.
B. An active IDS.
C. A network IDS.
D. A misuse IDS
E. An anomaly IDS

Answer: E

Explanation:
An anomaly IDS system uses predefined norms to differentiate between acceptable traffic and suspicious traffic. All traffic patterns that fall outside of the norm triggers an action.
Incorrect Answers:
A: A passive IDS system monitors the network and can only inform the administrator when an attack.
B: An active IDS system can inform the administrator when an attack is underway, and can carry out a predefined action to protect the network from further attacks.
C: A network IDS system tracks network traffic to isolate suspicious traffic.
D: A misuse IDS works by detecting network traffic patterns that match any of the attack patterns contained in the attack pattern database.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 115.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 382:

Of the statements listed below on host and network IDS analysis, which is FALSE?

A. A host-based IDS runs on a host to monitor communications, system logs and file systems, and can detect suspicious activities.
B. A network IDS tracks network traffic to isolate suspicious traffic.
C. Host and network IDS analysis can prevent attacks before they occur and can block unauthorized traffic from entering the network
D. A host-based IDS or network IDS can work in conjunction with a firewall system to further enhance security.

Answer: C

Explanation:
Firewall solutions are the first line of defense and can prevent attacks before they occur. Firewalls can block unauthorized traffic from entering the network
Incorrect Answers:
A, B, D: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 115.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 383:

You work as the security administrator at Certkiller .com. You want to use a program that will perform the following functions:
1. Emphasize the vulnerabilities of servers on the Certkiller .comnetwork to various exploits.
2. Show how identifiedvulnerabilities can be mitigated.
Which program should you use?

A. Use an IDS (Intrusion Detection System).
B. Use a port scanner.
C. Use a vulnerability scanner.
D. Use a Trojan scanner.

Answer: C

Explanation:
A vulnerability assessment uses a set of tools to identify vulnerabilities in a network. It usually works by scanning the network for IP hosts and identifying the different services running on the computers on the network. Each service is then probed to test the service for its security against known vulnerabilities. These tools then reports the vulnerabilities it finds on each computer, their level of risk, and suggests methods for mitigating these risks.
Incorrect Answers:
A: Intrusion diction systems detect possible attacks by monitoring network behavior, scanning packet header information, and examining the contents of packets. It does not check for vulnerabilities.
B: Port scanning and sniffers are often used as part of vulnerability assessment; however, on their own, they do not report methods for mitigating against risks.
D: There is no such thing as a Trojan scanner.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 422.
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 301.

QUESTION 384:

You work as the security administrator at Certkiller .com. You want to examine traffic on the Certkiller .com network. You also want to ascertain which services are running on the network.
Which program should you use?

A. Use a sniffer.
B. Use an IDS (Intrusion Detection System).
C. Use a firewall.
D. Use a router.

Answer: A

Explanation:
Packet sniffers are used to capture, monitor and analyze network traffic. There legitimate purpose is to find traffic flow problems and bottlenecks. However, hackers use it to capture data, to use in replay attacks.
Incorrect Answers:
B: Intrusion diction systems detect possible attacks by monitoring network behavior, scanning packet header information, and examining the contents of packets. It does not check for vulnerabilities.
C: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network.
D: A router interconnects two discontiguous or dissimilar networks. It does not review traffic.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 422.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 67.

QUESTION 385:

You work as the security administrator at Certkiller .com. You want to secure your UNIX server to be less susceptible to attackers getting hold of user account passwords. You want to store encrypted passwords within a file that is only readable by root.
Which file should you use?

A. Passwd file
B. Shadow password file
C. Hosts.allow file
D. Hosts.deny file

Answer: B

Explanation:
The shadow password file is a UNIX file that contains password related user information, including the encrypted user passwords. This file is readable only by superuser and/or members of a specified group that has root access because the file is only readable by root.
Incorrect Answers:
A: The passwd file is a UNIX file used to store user information for each user on the system. This information includes the user's login name and an encrypted version of the user's password. Although the passwords are encrypted, the passwrd file has general read permission, so the file may be read by any authenticated users or process.

C, D: The hosts.allow and hosts.deny files are access control lists that control the systems that are allowed or denied specified services. The hosts are identified by their IP addresses or host names.
References:
Bozidar Levi, UNIX Administration - A Comprehensive Sourcebook for Effective Systems and Network Management, Boca Raton (FL), CRC Press, 2002, pp.170-171, 195-198, 364.

QUESTION 386:

From the statements, which is NOT a valid explanation for supporting the recommendation that only important services are provided by a specific host, and all unnecessary services be disabled?

A. An additional service increases the risk of compromising the host, other services running on the host, and clients of these services.
B. Different services could require different hardware and software, or a different administration approach.
C. When fewer services and applications are running on a host, less log entries and interactions between different services are expected. From a security approach, this assists in simplifying the analysis and maintenance of the system.
D. When a service does not use a well known port, firewalls are unable to disable access to this port, nor will an administrator be able to restrict access to this service.

Answer: B

Explanation:
All services are part of the operating system and do not require additional software. Furthermore, services are optimized to run on a computer that meets the minimum system requirements for the operating system. Therefore no additional hardware is required. However, additional hardware and software can be used to supplement certain services but this is not a requirement.
Incorrect Answers:
A: All unnecessary services should be disabled as each service running on a server has its own vulnerabilities that could be exploited.
C: Unnecessary services would generate unnecessary logging. Thus disabling unnecessary services will reduce logging.
D: Some firewalls, especially software based firewalls can only block well known ports. Thus, if an unnecessary service does not use a well known port, the firewall will not be able to control access to that port.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 115-117, 201-216.

QUESTION 387:

You work as the security administrator at Certkiller .com. You want to enhance network security. You examine a server on the Certkiller .com network and notice that a fairly large number of protocols are bound and active on each network interface card.
What should you do next?

A. Running unnecessary protocols do not pose a great risk and can be left active for compatibility reasons.
B. There are no unnecessary protocols on the majority of systems because protocols are selected during system installation.
C. All unnecessary protocols must be disabled on all server and client machines on a network because they pose great risk.
D. Configuring port filtering ACLs (Access Control List) at firewalls and routers is adequate to prevent malicious attacks on unnecessary protocols.

Answer: C

Explanation:
Leaving additional network services enabled may cause difficulties and can create vulnerabilities in your network. As much as possible, configure your network devices as restrictively as you can.
Incorrect Answers:
A: All unnecessary port or services should be disabled as each unnecessary port or services have its own vulnerabilities that can be exploited.
B: On most operating systems, a default protocol suite is installed during installation of the operating system. After the operating system is installed, the administrator should disable unnecessary protocols so as to harden the computer against attack.
D: Port filtering can block access to a port. However, protocols can be mapped to different ports.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 115-117, 201-216.

QUESTION 388:

What is the main primary reason why attackers frequently target a server in single server network environments?

A. Single servers contain application launch scripts.
B. Single servers store security policy settings.
C. Single servers store credentials for all systems and user credentials.
D. Single servers store master encryption keys.

Answer: C

Explanation:

In a single server environment, all user credentials are stored on one server. A successful attack on that server will thus give the attacker access to usernames, addresses, and password hashes for all network users.
Incorrect Answers:
A: A single server may contain launch scripts but this is not likely.
B: Each computer on a network, regardless if they are servers or workstations, will contain security policy settings.
D: Master encryption keys are only created in a PKI system. It is unlikely that a single server network will use a PKI system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 115-117, 201-216.

QUESTION 389:

You work as the security administrator at Certkiller .com. A network administrator has recently replaced a hub with a switch.
While using software to sniff packets from the network, you find that you only see communication between the network administrator's computers and servers on the Certkiller .com network. You do not see communication between network clients and the servers. You report the issue to the network administrator, who verifies that there is nothing wrong with the switch and its operation.
You must identify the most probable cause of the problem. Which is it?

A. Other than for broadcasts, switches do not forward traffic out all its associated ports.
B. The network administrator has configured the switch with a VLAN (Virtual Local Area Network) using all ports.
C. The software you are using to sniff packets from the network is incorrectly configured.
D. The Ethernet card of the software you are using to sniff packets from the network is problematic.

Answer: A

Explanation:
Switches were originally designed to segment networks to make communications more efficient. Unless traffic is sent to the broadcast address, a switch will not forward traffic out all ports. For this reason, sniffers cannot be used on a switched network.
Incorrect Answers:
B: VLANS can be implemented to segment a network using one switch. In this system, the ports a grouped into a virtual LAN. Thus VLANS are switched networks. Sniffers cannot be used on a switched network because they do not use broadcast addresses.
C: Sniffers cannot be used on a switched network, regardless of the software configuration.
D: Sniffers can be used only in the local segment. They cannot be used on a switched network because they do not use broadcast addresses.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 67, 114.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp. 78, 92.

QUESTION 390:

Prior to implementing a wireless solution, there is a specific action which you should perform. Choose this action from the available options.

A. Ad hoc mode must be enabled on all access points.
B. All users must have strong passwords.
C. You should only use Wi-Fi (Wireless Fidelity) equipment.
D. You should perform a thorough site survey first.

Answer: D

Explanation:
Geography and architecture can affect wireless availability and integrity. It would be crucial to perform a site survey first, to locate any geographical and architectural obstacles so they can be accommodated.
Incorrect Answers:
A: Ad hoc mode allows two wireless devices to communicate directly with each other without the need for a wireless access point.
B: Ensuringstrong passwords will improve authentication but will not prevent interception of packet.
C: Wireless solutions can consist of Wi-Fi devices and Bluetooth enabled devices.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 180.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 219.

QUESTION 391:

You work as the security administrator at Certkiller .com. You want to control the flow of packets traveling through routers.
Which security mechanism should you use?

A. Use ACL (Access Control List)
B. Use fault tolerance tables
C. Use OSPF (Open Shortest Path First) policy
D. Use packet locks

Answer: A

Explanation:

ACLs control access to resources based on user permissions or IP address. On a router, an ACL can allow or deny a machine access to a network based on the machine's IP address.
Incorrect Answers:
C:
OSPF policies can also be used to control the flow of packets traveling through routers. There are two OSPF policies: OSPF Accept Policies and OSPF Announce Policies. OSPF Accept Policies can be configured to prevent the forwarding of packets to external networks. OSPF Announce Policies can be prevent the advertising of external routes. However, these can only be applied to OSPF enabled routes.
B, D: There is not such thing as fault tolerance tables or packet locks.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 216.
http://www.rhyshaden.com/ospf.htm

QUESTION 392:

You work as the security administrator at Certkiller .com. You want to use IPSec in Tunnel mode to encrypt data.
Choose the option that defines which data will be encrypted.

A. The one time pad utilized in handshaking.
B. The message header and the message payload.
C. All e-mail messages and the hashing algorithm.
D. The message payload.

Answer: B

Explanation:
In IPSec the payload and the header are known as the ESP (Encapsulating Security Payload) and AH (Authentication Header).
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 112-114.

QUESTION 393:

You work as the security administrator at Certkiller .com. You want to implement a firewall solution.
Which step should you perform first to accomplish this?

A. Block all unwanted incoming traffic.
B. Block all unwanted outgoing traffic.
C. Develop and implement a firewall policy.
D. Protect the network from DDoS (Distributed Denial of Service) attacks.

Answer: C

Explanation:
A firewall is a hardware or software component that protects a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. The first step in implementing a firewall is to develop a firewall policy that defines how the firewall should filter traffic and the types of traffic that should be blocked or allowed.
Incorrect Answers:
A, B: The firewall policy should define which types of traffic and which ports should be permitted and which should be blocked.
D: There is no effective defense against a DDoS attack.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.100-104.

QUESTION 394:

You work as the security administrator at Certkiller .com. You want to define and configure the rules for a secure firewall implementation.
Which basic firewall strategy should you use?

A. Permit All.
B. Deny All.
C. Default Permit.
D. Default Deny.

Answer: D

Explanation:
A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. It should be configured to allow only explicitly permitted. All types of traffic and ports that are not explicitly permitted, should be denied by default.
A: A permit all policy would make a firewall obsolete as the purpose of a firewall is to block unwanted traffic.
B: A deny all policy will mean that no traffic is allowed through the firewall. This will effective prevent traffic between the trusted internal network and the external network.
C: A default permit policy would be a vulnerability as it means that ports and types of traffic that have not been explicitly allowed or blocked would be allowed to pass through the firewall.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.

QUESTION 395:

You work as the security administrator at Certkiller .com. You plan to implement a VPN (Virtual Private Network).
Which security consideration should you be aware of?

A. Intruders can intercept VPN traffic and then launch a man in the middle attack.
B. Captured data can be easily decrypted because there are only a finite number of encryption keys.
C. Tunneled data cannot be authenticated and authorized.
D. Firewalls cannot inspect traffic that is encrypted.

Answer: D

Explanation:
A firewall can't inspect traffic once it is channeled into a VPN. When a firewall sees a VPN channel, it considers it as already passing security checks. The firewall does not have the ability to see through the encrypted channel.
Incorrect Answers:
A: VPNtraffic is tunneled through the public network and cannot be intercepted.
B: Encrypted data cannot easily be decrypted.
C: A tunneled connection can be authenticated via RADIUS. Once connected, the normal network management systems can be used for authorization and accounting.
Reference:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.

QUESTION 396:

You work as the security administrator at Certkiller .com. You want to implement a strategy which will assist in limiting hostile sniffing on the LAN (Local Area Network).
What should you use?

A. Use an Ethernet switch.
B. Use an Ethernet hub.
C. Use a CSU/DSU (Channel Service Unit/Data Service Unit).
D. Use a firewall.

Answer: A

Explanation:
Switches were originally designed to segment networks to make communications more efficient. Unless traffic is sent to the broadcast address, a switch will not forward traffic out all ports. For this reason, sniffers cannot be used on a switched network.
Incorrect Answers:
B: An Ethernet hub transmits traffic out all ports. For this reason it does not prevent sniffing.
C: A CSU/DSU is a connection device for digital serial connections such as T1. It does not prevent sniffing.
D: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. However, a firewall does not prevent sniffing on the internal network.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.
David Groth and Toby Skandier, Network+ Study Guide, 4th Edition, San Francisco, Sybex, p 36.

QUESTION 397:

Choose the attack method or malicious code typically used by attackers to access a company's internal network through its remote access system.

A. A War dialer program.
B. Trojan horse.
C. DoS (Denial of Service) attack.
D. Worm.

Answer: A

Explanation:
A war dialer is a program that dials a block of telephone numbers in the attempt to fins a remote access computer to connect to. Although advances in telecom technology has made it easier to identify war dialers, war dialer remain a threat to remote access systems
Incorrect Answers:
B: A Trojan horse is a piece of malicious code that is included in a useful looking program. It is used to create backdoors into systems. This type of attack usually does not require remote access but an Internet connection.
C: A DoS attack attempts to affect the availability of network resources and serviced. This type of attack usually does not require remote access but an Internet connection.
D: A worm is a program that replicates itself by means of computer networks. It resides in active memory and is usually spread via e-mail.
References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 56, 71, 80, 82, 100, 202.

QUESTION 398:

You work as the security administrator at Certkiller .com. You want to implement a remote access solution that will enable mobile users to access the corporate Certkiller .com network. All mobile users will be using laptops that have Ethernet adapters to access shared files and e-mail on the corporate Certkiller .com network. Half of the laptops are equipped with modems.
What solution should you use?

A. Use ISDN (Integrated Services Digital Network).
B. Use Dial-up.
C. Use SSL (Secure Sockets Layer).
D. Use a VPN (Virtual Private Network) connection.

Answer: D

Explanation:
A VPN is a network connection that tunnels through a public network, providing the same level of security as a local connection. When the salesmen create a VPN connection, they will be required to authenticate to the VPN server. Once authenticated, they will virtual access to a private network that is safe, secure, and encrypted. However, their access to resources on the private network will be determined by their permissions on those resources.
Incorrect Answers:
A: ISDN is used mainly for Internet connectivity but can be used for remote access. However, this would require an ISDN modem.
B: Dial-up is a remote access method that requires the use of modems in both the remote access clients and the remote access server .Not all laptops have modems;therefore this option will not meet the needs of all laptop users.
C: SSL is a website technology used to secure communication between a browser and a web server. It is not used for remote access.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 105-108, 119, 258, 353.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 110, 112-114, 325.

QUESTION 399:

An
IDS (Intrusion Detection Systems) is made up of a number of components. Choose the two components usually found in an IDS.

A. A router.
B. A sensor.
C. A firewall
D. A console.

Answer: B D

Explanation:
An IDS has a number of components including a sensor and an analyzer. The sensor collects the data which is then passed on to the analyzer. The analyzer analyzes the data for suspicious activity. When suspicious activity is identified, an alert is sent to the operator either via e-mail or a console.
Incorrect Answers:
A: A router connects two networks, including two disparate networks.
C: A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. Afirewall is notpart of an IDS system however, an IDS can be used in conjunction with a firewall to increase security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.

QUESTION 400:

Which of the following details the primary advantage of implementing a multi-homed firewall?

A. A multi-homed firewall is relatively inexpensive to implement.
B. A multi-homed firewall's rules are easier to manage.
C. When a multi-homed firewall is compromised, only those systems residing in the DMZ (Demilitarized Zone) are vulnerable.
D. Attackers must get around two firewalls.

Answer: C

Explanation:
A firewall is a hardware or software component that to protect a private network from another, usually external and untrusted, network by use filters to control the network traffic that enters and/or leaves a network. A multi-homed firewall has two or more network cards. This allows for the distinction between multiple networks and allows for the creation of a demilitarized zone (DMZ). The DMZ hosts publicly accessible servers, such as web or FTP. The firewall provides secured but public access to the DMZ, while blocking access to the private network. If the multi-homed firewall is compromised, only the systems in the DMZ will be exposed.
Incorrect Answers:
A: A multi-homed firewall is simply a firewall that has multiple network cards. Network

cards are relatively inexpensive. However, this is not the main advantage of multi-homed firewalls. A firewall is a security device. Therefore, a multi-homed firewalls ability to create a distinction between different networks is more important.
B: A multi-homed firewall would require filters on all network cards, thus increasing the complexity of filtering while also increasing security.
D: It would not be possible for the attacker to circumvent the second firewall as it would be configured to block all traffic to the private network.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 76.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 100-104.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 331-341.

QUESTION 401:

Choose the option that specifies an element which is NOT typically included in security requirements for network servers.

A. The absence of vulnerabilities utilized by known forms of attack against network servers.
B. The capability to allow administrative functions to all network users.
C. The capability to deny access to data on the network server except to data that should be accessible.
D. The capability to disable unnecessary network services that are included in the operating system or server software.

Answer: B

Explanation:
Granting any user administrative privileges would allow any user full control over the system and would render that administrative account obsolete. This would not be a good security measure.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 259.

QUESTION 402:

From the options, choose the attack which an IDS (Intrusion Detection System) cannot detect.

A. DoS (Denial of Service) attack.
B. Vulnerability exploits.
C. Spoofed e-mail
D. Port scan attack

Answer: C

Explanation:
An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. E-mail messages are not network traffic, therefore spoofed emails will not be detected by the IDS.
Incorrect Answers:
A, B, D: An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. This includes DoS attacks, port scans, and vulnerability exploits.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION 403:

From the options, choose the disadvantage of implementing an IDS (Intrusion Detection System).

A. False positives.
B. Decrease in throughput.
C. Compatibility.
D. Administration.

Answer: A

Explanation:
An intrusion detection system (IDS) monitors inbound and outbound network traffic on a host or network in order to detect an attempted intrusion. Sometimes an IDS will mistake legitimate traffic for an intrusion. This is called a false positive.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 95.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 162-164, 173-174.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 422-432.

QUESTION 404:

Which of the following types of network cabling has a center conductor, an outer conductor , and an outer sheath; where the center conductor is used to carry data from point to point?

A. Coaxial cable.
B. STP (Shielded Twisted Pair) cable.
C. UTP (Unshielded Twisted Pair) cable.
D. Fiber-optic cable.

Answer: A

Explanation:
Coaxial cabling has a center conductor, an outer conductor, and an outer sheath. The center conductor is used to carry data from point to point. The center conductor has an insulator wrapped around it. A shield is found over the insulator, and a nonconductive sheath is found around the shielding. Coaxial cabling is probably one of the oldest network cabling used these days.
Incorrect answers:
B: UTP is the main cabling type used in LANs today, but has no shielding. There are seven types of UTP cable available.
C: STP is similar to UTP, with the differentiating factor being that STP is shielded. STP cabling has a single shield around all wire pairs. There are some STP versions that place shields over each pair of wires.
D: Fiber-optic uses light pulses for signal transmission. There is a glass cladding, plastic spacer, protective Kevlar fibers, and a protective outer sheath all outside of the fiber optic core.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 405:

Which of the following sabotage methods can bring down an entire bus topology coaxial network?

A. Cut wire
B. Severe electromagnetic interference (EMI).
C. Severe radio frequency interference (RFI).
D. Physical removal of a terminator
E. All of the above

Answer: E

Explanation:
Due to coaxial cable being popular in bus topologies, either of the above can result in the entire network being brought down. Both electromagnetic interference and radio

frequency interference have an impact on the reception of electronic transmissions and can cause sensitive electrical and electronic equipment to stop operating. Each end of a coaxial bus network has a terminator. By removing this terminator, you also end up with no communication occurring on the coaxial network.
Incorrect answers:
A: This is only part of the answer.
B: A, C, and D are also part of the answer.
C: A, B, and D are also part of the answer.
D: A, B, and C are also part of the answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 406:

Which of the following types of network cabling has no shielding?

A. Coaxial cable.
B. Unshielded Twisted Pair.
C. Shielded Twisted Pair.
D. Fiber optic cable.

Answer: B

Explanation:
While UTP is the main cabling type used in LANs today, it has no shielding.
Incorrect answers:
A: Coaxial cabling has a center conductor, an outer conductor, and an outer sheath. The center conductor has an insulator wrapped around it. A shield is found over the insulator, and a nonconductive sheath is found around the shielding.
C: STP cable has a single shield around all the pairs.
D:
Withfiber optic, there is a glass cladding, plastic spacer, protective Kevlar fibers, and a protective outer sheath all outside of the fiber optic core.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 407:

Which of the following types of network cables is less secure than coaxial cabling?

A. Twisted-pair cables.
B. Fiber optic cable.
C. All of the above

Answer: A

Explanation:
UTP has no shielding and STP only has a single shield around all pairs. Both UTP and STP cabling offer less security than coaxial cabling.
Incorrect answers:
B: Fiber optic cable is not affected by electromagnetic interference, and is considered the most secure cable. Fiber optic cabledoes not leak electrical signals either.
C: A is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 408:

Which of the following measures can be used to secure twisted-pair cable networks from eavesdropping?

A. Protect the physical cables.
B. Protect all central connectivity devices such as patch panels and hubs.
C. Protect all critical network segments that connect hubs and switches, and provide connectivity to routers and servers.
D. Check your network cable infrastructure regularly.
E. All of the above

Answer: E

Explanation:
To secure a twisted-pair network from eavesdropping, each of the above mentioned measures should be employed.
Incorrect answers:
A, B, C, D: These are all part of the complete correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex,

Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 409:

Which of the following network cable types is most vulnerable to electromagnetic interference (EMI) and radio frequency interference (RFI)?

A. Coaxial cable.
B. Unshielded Twisted Pair.
C. Shielded Twisted Pair.
D. Fiber optic cable.

Answer: B

Explanation:
Unshielded Twisted Pair (UTP) has a higher degree of vulnerability to radio frequency interference and electromagnetic interference than the other cabling types. This is due to UTP cables having no shielding.
Incorrect answers:
A: Coaxial cabling has a center conductor, an outer conductor, and an outer sheath. The center conductor has and insulator wrapped around it. A shield is found over the insulator, and a nonconductive sheath is found around the shielding
C: STP cabling has a single shield around all wire pairs. There are some STP versions that place shields over each pair of wires.
D: Fiber-optic uses light pulses for signal transmission. There is a glass cladding, plastic spacer, protective Kevlar fibers, and a protective outer sheath all outside of the fiber optic core.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 410:

Which of the following methods can be used to secure a coaxial network from eavesdropping?

A. Document and update the cable infrastructure being used within your network.
B. Set aside time to perform regular inspections on your cable infrastructure.

C. You should investigate all outages in a coaxial network.
D. Include all undocumented connections and hosts in your investigations.
E. All of the above

Answer: E

Explanation:
To secure coaxial network from eavesdropping, each of the above mentioned measures should be used. You can also further secure a coaxial network by placing network cable inside walls and by burying it underground.
Incorrect answers:
A, B, C, D: These are all part of the complete correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 411:

Which of the following network cable types is least vulnerable to electronic eavesdropping?

A. Coaxial cable.
B. Unshielded Twisted Pair.
C. Shielded Twisted Pair.
D. Fiber optic cable.

Answer: D

Explanation:
Because fiber-optic cable uses light pulses for signal transmission, fiber-optic cabling eliminates the tapping of electrical signals that can occur in twisted pair and coaxial cabling. Eavesdropping on traffic is much more difficult in fiber optic cable networks.
Incorrect answers:
A: Any connection within the coaxial network is vulnerable to eavesdropping. Intruders can tap into the coaxial cable at virtually any point on the coaxial network.
B: A UTP twisted-pair network can be compromised by eavesdropping through attaching a protocol analyzer to a twisted-pair connection point and by using escaping electromagnetic signals to eavesdrop on signals.
C: While STP cabling has a single shield around all wire pairs, a STP twisted-pair network is still vulnerable to eavesdropping. Intruders can attach a protocol analyzer to a twisted-pair connection point or use escaping electromagnetic signals to eavesdrop on signals.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 132 - 138.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3
3.3 Understand the concepts behind the various kinds of Security Topologies. (30 questions)

QUESTION 412:

Which of the following security zones is closest to the internal network of the company, and can also be considered as being internal to the company?

A. Internet
B. Intranet
C. Extranet
D. Perimeter network

Answer: B

Explanation:
An intranet is the private network of the company. Intranets are used by users that are internal to the company. An intranet belongs to and is controlled by the company
Incorrect answers:
A: The Internet is a global network that can be used by whichever person. The Internet connects computer and individual networks.
C: An extranet is the public area of the company network infrastructure that enables resources to be accessed by external users. An extranet is a semi-secure zone that allows partner access to specific resources.
D: Perimeter networks provide services to users located on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 413:

Which of the combinations here can be used to create an extranet?

A. Two intranets
B. Two perimeter networks

C. One intranet and one perimeter network
D. All of the above configurations

Answer: D

Explanation:
The rationale behind the above configurations is that the connected networks are used to share resources with partner organizations. If you use two perimeter networks to create an extranet, you can use one perimeter network to provide services to partner organizations, and the other perimeter network to provide services to the Internet
Incorrect answers:
A: A, B, and C are all correct.
B: A, B, and C are all correct.
C: A, B, and C are all correct.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 414:

For referring to an intranet, which of the following terms does not apply?

A. Internal network.
B. A demilitarized zone (DMZ)
C. Private network.
D. Local area network (LAN).
E. Trusted or protected network

Answer: B

Explanation:
A demilitarized zone (DMZ) or perimeter network provides a layer of privacy between the company infrastructure and the Internet. The demilitarized zone allows you to expose only those systems that must be known to the general public.
Incorrect answers:
A, C, D, E: All part of the complete, correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 415:

Choose the security zone that is a global network, which can be accessed by anybody?

A. Internet
B. Intranet
C. Extranet
D. Perimeter network

Answer: A

Explanation:
The Internet is a global network that can be used by whichever person. The Internet connects computer and individual networks.
Incorrect answers:
B: An intranet is the private network of the company. Intranets are used by users that are internal to the company. An intranet belongs to and is controlled by the company.
C: An extranet is the public area of the company network infrastructure that enables resources to be accessed by external users. An extranet is a semi-secure zone that allows partner access to specific resources.
D: Perimeter networks provide limited services to users located on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 416:

Which of the following security zones contain most of the company's private resources and network infrastructure equipment?

A. Internet
B. Intranet
C. Extranet
D. Perimeter network

Answer: B

Explanation:

An intranet is the private network of the company that contains most of the private resources and network infrastructure equipment of the company. Intranets are used by users that are internal to the company. An intranet belongs to and is controlled by the company.
Incorrect answers:
A: The Internet is a global network that can be used by whichever person. The Internet connects computer and individual networks.
C: An extranet is the public area of the company network infrastructure that enables resources to be accessed by external users. An extranet is a semi-secure zone that allows partner access to specific resources.
D: Perimeter networks provide limited services to users located on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 417:

Choose the security zone used to enable business partners to access specific resources.

A. Internet
B. Intranet
C. Extranet
D. Perimeter network

Answer: C

Explanation:
An extranet is the public area of the company network infrastructure that enables resources to be accessed by external users. An extranet is a semi-secure zone that allows partners of the organization to access specific resources.
Incorrect answers:
A: The Internet is a global network that can be used by whichever person. The Internet connects computer and individual networks.
B: An intranet is the private network of the company. Intranets are used by users that are internal to the company. An intranet belongs to and is controlled by the company.
D: Perimeter networks provide limited services to users located on the Internet.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 418:

Which of the following security topologies is a dual-homed device used to connect the outside network with the inside network. This would also be one of the first devices where public traffic arrives, and where specialized software defines which types of traffic are allowed to pass through?

A. Bastion host.
B. Screened host gateway.
C. Screened subnet gateway.
D. None of the above

Answer: A

Explanation:
A bastion host is a dual-homed device that connects the outside network with the secured intranet. A bastion host can be either a router running access lists, or a hardware device such as a Cisco PIX, or a PC running an operating system that supports traffic-filtering mechanisms. A dual-homed device has routing between its interfaces disabled. Instead, specialized software is used to define which types of traffic should be allowed through. All other traffic is excluded from passing through.
Incorrect answers:
B: A screened host gateway is a traffic filtering device that only accesses a specific application gateway within the network. Apart of this traffic, no traffic is allowed in/out of the screened host gateway.
C: A screened subnet gateway combines the architectures of the bastion host and screened host gateway to separate the secure network from the Internet. The screened subnet gateway creates a screened subnet, or DMZ between the secure network and the Internet.
D: A bastion host is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 419:

Security for the extranet security zone can include a number of strategies. Choose the one that does not apply.

A. Using VPN connections.
B. Regularly auditing all services

C. Use host-based firewalls for computers that contain confidential data
D. Removing all unnecessary services
E. Limiting the number of services provided

Answer: C

Explanation:
Using host-based firewalls for computers that contain confidential data is a strategy for securing the intranet security zone.
Incorrect answers:
A, B, D, E: These are all methods of securing the extranet security zone.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 420:

Of the technologies used to create a less vulnerable system, which technology can be implemented in a firewall, router, workstation or server computer; and translates the internal IP address range to an external IP address or address range?

A. Virtual local area network (VLAN)
B. Network address translation (NAT)
C. Tunneling
D. None of the above

Answer: B

Explanation:
NAT allows the organization to use publicly assigned IP addresses over the Internet that is different from its private IP addresses. In this way, NAT hides the private network from the public. The NAT server runs as a firewall for the network.
Incorrect answers:
A: VLANs enable you to segment one broadcast domain into two or multiple domains, and then restrict access to specific network resources. In this way, a VLAN allows you to hide segments of the network from other segments.
C: Tunneling or a virtual private network (VPN) is the method of creating a virtual dedicated connection between two systems or networks. Various tunneling protocols can be used to provide authentication, data integrity and encryption services.
D: NAT is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex,

Alameda, 2004, p. 29 - 31.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 421:

Which of the following security topologies creates a DMZ between the local area network and the Internet?

A. Bastion host.
B. Screened host gateway.
C. Screened subnet gateway.
D. None of the above

Answer: C

Explanation:
A screened subnet gateway combines the architectures of the bastion host and screened host gateway to separate the secure network from the Internet. The screened subnet gateway creates a screened subnet, or DMZ between the secure network and the Internet.
Incorrect answers:
A: A bastion host can be either a router running access lists, or hardware device such as a Cisco PIX, or a PC running an operating system that supports traffic-filtering mechanisms.
B: A screened host gateway is a traffic filtering device that only accesses a specific application gateway within the network. Apart of this traffic, no traffic is allowed in/out of the screened host gateway.
D: A screened subnet gateway is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 422:

Overloading NAT allows the organization to use publicly assigned IP addresses over the Internet that is different from its private IP addresses. To do this, which type of mapping is performed by Overloading NAT?

A. Performs a one-to-one mapping of an internal IP address to an external IP address
B. Maps multiple internal IP addresses to a range of external IP addresses.
C. Maps multiple internal IP addresses to one external IP address by employing a port-based mapping method.

Answer: C

Explanation:
Overloading NAT maps multiple internal IP addresses to one external IP address. PAT uses port-based mappings at a higher level up the OSI reference model.
Incorrect answers:
A: Static NAT performs a one-to-one mapping of an internal IP address to an external IP address.
B: Dynamic NAT maps multiple internal IP addresses to a range of external IP addresses.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 29 - 31.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 423:

Which technology allows you to segment or group users that have similar data sensitivity levels together and thereby increase security?

A. Virtual local area network (VLAN)
B. Network address translation (NAT)
C. Tunneling
D. None of the above

Answer: A

Explanation:
VLANs enable you to segment one broadcast domain into two or multiple domains, and then restrict access to specific network resources. VLANs allow administrators to segment or group users that have similar data sensitivity levels together and thereby increase security.
Incorrect answers:
B: NAT allows the organization to use publicly assigned IP addresses over the Internet that is different from its internal IP addresses. In this way, NAT hides the private network from the public.
C: Tunneling creates a virtual dedicated connection between two systems or networks. Various tunneling protocols can be used to provide authentication, data integrity and encryption services.
D: A VLAN is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 29 - 31.

Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 424:

Which type of NAT configuration maps a range of internal IP addresses to a range of external IP address?

A. Static NAT
B. Dynamic NAT
C. Overloading NAT

Answer: B

Explanation:
Dynamic NAT maps multiple internal IP addresses to a range of external IP addresses. The added benefit being that the mappings do change.
Incorrect answers:
A: Static NAT performs a one-to-one mapping of an internal IP address to an external IP address.
C: Overloading NAT maps multiple internal IP addresses to one external IP address. PAT uses port-based mappings.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 29 - 31.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 425:

Which security topology involves a packet-filtering device that is typically a router, which communicates only with a specific application gateway within the private network?

A. Bastion host.
B. Screened host gateway.
C. Screened subnet gateway.
D. None of the above

Answer: B

Explanation:

A screened host gateway is a packet filtering device that only accesses a specific application gateway within the network. Other than for this traffic, no traffic is allowed in/out of the screened host gateway.
Incorrect answers:
A: A bastion host can be either a router running access lists, or a hardware device such as a Cisco PIX, or a PC running an operating system that supports traffic-filtering mechanisms.
C
: A screened subnet gateway combines the architectures of the bastion host and screened host gateway to separate the secure network from the Internet. The screened subnet gateway creates a screened subnet, or DMZ between the secure network and the Internet.
D: A screened host gateway is the correct answer.
References:
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 426:

Which type of NAT configuration performs a one-to-one mapping of an internal IP address to an external IP address?

A. Static NAT
B. Dynamic NAT
C. Overloading NAT

Answer: A

Explanation:
Static NAT performs a one-to-one mapping of an internal IP address to an external IP address
Incorrect answers:
B: Dynamic NAT maps multiple internal IP addresses to a range of external IP addresses
C: Overloading NAT maps multiple internal IP addresses to one external IP address.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 29 - 31.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 427:

A compromise of which device could result in a VLAN being compromised?

A. Router

B. Switch
C. NAT server
D. None of the above

Answer: B

Explanation:
Switches are used to create VLANs. When a switch is compromised, the attacker could next compromise the VLANs created by the switch.
Incorrect answers:
A: Switches and not routers create VLANs.
C: A NAT server resides between the internal network and external network, and is used to map internal IP addresses to public IP addresses that can be routed on the Internet.
D: Switches create VLANs.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 428:

With reference to bastion hosts, which of following is FALSE?

A. A bastion host is a dual-homed device that connects the outside network to the internal network.
B. Specialized software on the bastion host determines which traffic to allow.
C. When the bastion host determines that a specific traffic flow is safe, it forwards the data to an application gateway for further handling.
D. Routing must be disabled on the two interfaces of the bastion host

Answer: C

Explanation:
A bastion host does not use an application gateway. An application is used in a screened host gateway configuration. Once a screened host gateway allows data, that data is passed to the application gateway for further processing.
Incorrect answers:
A, B, D: These statements are all TRUE.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 429:

Which of the following devices used in one of the three major types of security topologies, is a one-interface device?

A. Bastion host
B. Application gateway
C. Screened host gateway
D. Screened subnet gateway.

Answer: B

Explanation:
An application gateway is used in a screened host gateway configuration. The application gateway is a one-interface device to which the screened host gateway passes safe data.
Incorrect answers:
A: A bastion host is a dual-homed device, that is, a device with two interfaces.
C: A screened host gateway is also a device with two interfaces
D: A screened subnet gateway uses two screened host gateway devices to separate the internal network from the Internet.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 24 - 28.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 430:

Which type of NAT provides the most security benefits in hiding the internal network's addressing structure from the external network?

A. Static NAT
B. Dynamic NAT
C. Overloading NAT

Answer: C

Explanation:
While static NAT and dynamic NAT do hide internal IP addresses from the public, Overloading NAT uses port based mappings to ensure that the external structure is entirely different from the internal network structure.
Incorrect answers:
A: Static NAT offers less security than both Dynamic NAT and Overloading NAT.
B: Dynamic NAT offers more security than Static NAT because the external-to-internal address mappings can change, which makes it more difficult for attackers to find the addresses of hosts on the internal network. Overloading NAT does though provide better

security than Dynamic NAT.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 29 - 31.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 431:

On which of the following devices would you not implement NAT?

A. Router
B. Switch
C. Firewall
D. Server computer

Answer: B

Explanation:
NAT cannot be implemented on a switch. When it comes to security technologies, switches are used to create VLANs, and are not used to enable the NAT capability within your network.
Incorrect answers:
A, C, D: NAT can be implemented in a firewall, router, or a server computer. The NAT server resides between the internal network and the public network.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 29 - 31.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 3

QUESTION 432:

You work as the security administrator at Certkiller .com. Certkiller .com has headquarters in London and a branch office in Paris. You must ensure that a secure connection is established between the London headquarters and the Paris branch office over the public network.
You deploy IPSec (Internet Protocol Security) to achieve this goal. You must still configure the IPSec mode for the router at each location.
Which IPSec mode should you configure?

A. Secure moe

B. Tunnel mode
C. Transport mode
D. Data link mode

Answer: B

Explanation:
IPSec provides secure authentication and encryption of data and headers. IPSec can work in Tunneling mode or Transport mode. In Tunneling mode, the data or payload and message headers are encrypted. Transport mode encrypts only the payload.
Incorrect answers:
A: The mode that IPSec operate in is either transport- or tunnel mode.
C: Transport mode encrypts only the payload.
D: The mode that IPSec operate in is either transport- or tunnel mode.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 127

QUESTION 433:

You work as the security administrator at Certkiller .com. You must ensure that internal access to other parts of the network is controlled and restricted.
The solution which you implement to restrict network access must be hardware based. You also want to use the least amount of administrative effort to accomplish your task.
How will you accomplish the task?

A. Deploy firewalls between your subnets.
B. Deploy a VLAN (Virtual Local Area Network) Deploy.
C. Deploy a proxy server Deploy.
D. Deploy a VPN (Virtual Private Network).

Answer: B

Explanation:
Implement a VLAN (Virtual Local Area Network) to restrict network access is the best answer. VLAN's would restrict access only to their local VLAN, and this would require less administrative overhead than setting up firewalls at each subnet. They are also hardware based (at the switch and MAC level) Firewalls are used so that external users (outside the organization cannot get in), whereas VLAN's are used within an organization to provide security.
Incorrect answers:
A: Firewalls are used to keep external users from intruding. This is not the best solution under the circumstances.
C
: A proxy firewall can be thought of as an intermediary between your network and any

other network. Used to process requests from an outside network; the proxy firewall examines the data and makes rules-based decisions about whether the request should be forwarded or refused. The proxy intercepts all the packages and reprocesses them for use internally. This process includes hiding IP addresses. However, this is not a hardware based solution as is required by the question.
D: Implementing a VLAN is not what is required in this case as it is not hardware based.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, pp. 102, 112

QUESTION 434:

From the options, choose the VPN (Virtual Private Network) tunneling protocol.

A. AH (Authentication Header).
B. SSH (Secure Shell).
C. IPSec (Internet Protocol Security).
D. DES (Data Encryption Standard).

Answer: C

Explanation:
IPSec provides secure authentication and encryption of data and headers. IPSec can work in tunneling mode or transport mode. In tunneling mode, the data or payload and message headers are encrypted. Transport modes encrypt only the payload.
Incorrect answers:
A: Authentication Header (AH) is a header used to provide connectionless integrity and data origin authentication for IP datagrams, and used to provide protection against replays.
B: SSH is a replacement for rlogin in Unix/Linux that includes security.
D: DES is a block cipher algorithm used for encryption.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 127

QUESTION 435:

Which of the following best describes what tunneling is?

A. Tunneling is the process of utilizing the Internet as part of a private secure network.
B. Tunneling is the process of moving through three levels of firewalls.
C. Tunneling is the process of passing information over the Internet within the shortest time frame.
D. Tunneling is the process of creating a tunnel capable of capturing data.

Answer: A

Explanation:
Civil engineers build tunnels to allow one direction of traffic flow to be protected against another traffic flow. They will build a tunnel under a river, or underneath a highway. Network engineers use tunneling to protect a data flow from the elements of the internet. They tunnel by placing ordinary/non-secure IP packets into encrypted/secure IP packets.
Incorrect answers:
B: Tunneling is not meant to burrow through firewalls. It is meant to provide safe passage for ordinary non-secure packets into encrypted secure packets.
C: It is not a matter of time, but rather a matter of having a safe way of passing data packets.
D: The tunnel itself does not capture data.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 30

QUESTION 436:

Choose the option that best defines what tunneling is.

A. The process of encapsulating encrypted, secure IP packets within ordinary, non-secure IP packets.
B. The process of encapsulating ordinary, non-secure IP packets within encrypted, secure IP packets.
C. The process of encapsulating encrypted, secure IP packets within encrypted, non-secure IP packets.
D. The process of encapsulating ordinary, non-secure IP packets within ordinary, non-secure IP packets.

Answer: B

Explanation:
Tunneling refers to creating a virtual dedicated connection between two systems or networks. You create the tunnel between the two ends by encapsulating the data in a mutually-agreed-upon protocol for transmission. In most tunnels, the data passed through the tunnel appears at the other side as part of the network. Tunneling sends private data across a public network by placing (encapsulating) that data into other packets. Most tunnels are virtual private networks (VPNs).
Incorrect answers:
A: This is a vice versa description of tunneling.
C: This is not correct as ordinary non-secure data gets encapsulated inside of encrypted/secure IP packets.
D: This is not what tunneling dose; this is normal clear text messagin.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, pp. 30-32

QUESTION 437:

You work as the security administrator at Certkiller .com. You want to connect an IP (Internet Protocol) address scheme to the Internet, and need to determine whether NAT (Network Address Translation) is required.
Which address scheme will require NAT (Network Address Translation)?

A. 204.180.0.0/24
B. 172.16.0.0/24
C. 192.172.0.0/24
D. 172.48.0.0/24

Answer: B

Explanation:
The NAT server provides IP addresses to the hosts or systems in the network and tracks inbound and outbound traffic. A company that uses NAT presents a single connection to the network. This connection may be through a router or a NAT server. The only information that an intruder will be able to get is that the connection has a single address.
172.16.0.0 is a private IP address that can be NAT to a IP address.
Incorrect answers:
A, C, D: These addresses do not require NAT when connecting to the Internet. The private address ranges are:
10.0.0.0-10.255.255.255
172.16.0.0-172.31.255.255
192.168.0.0-192.168.255.255
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, p. 28

QUESTION 438:

Which concept correctly specifies the location where a system administrator would deploy a web server if that web server should be separated from other network servers?

A. A honey pot
B. A hybrid subnet
C. A DMZ (Demilitarized Zone)
D. A VLAN (Virtual Local Area Network)

Answer: C

Explanation:
A Demilitarized Zone is used by a company that wants to host its own Internet services

without sacrificing unauthorized access to its private network.
Incorrect answers:
A: A honey pot is a system designed to entice or entrap an attacker. Enticement means inviting or luring an attacker to the system. Entrapment is the process of encouraging an attacker to perform an act, even if they don't want to do it.
B: A Hybrid subnet is not meant for isolating a web server from the other servers on a network.
D: A virtual local area network (VLAN) allows you to create groups of users and systems and segment them on the network. This segmentation lets you hide segments of the network from other segments and thereby control access.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishing, Alameda, 2004, pp. 28, 185

QUESTION 439:

You work as the security administrator at Certkiller .com. You want to deploy a new web server named Certkiller -SR02 in the DMZ (Demilitarized Zone).
Certkiller -SR02 must be configured to provide the following services:
* SMTP (Simple Mail Transfer Protocol)
* HTTP (Hypertext Transfer Protocol)
* FTP (Pile Transfer Protocol)
* SSL (Secure Sockets Layer)
You must configure the firewall to allow traffic to be passed to and from Certkiller -SR02.
What ports should you open on the firewall?

A. Open ports 23, 21, 80, 119.
B. Open ports 21, 119, 443, 1250.
C. Open ports 21, 25, 80, 443,
D. Open ports 21, 80, 443, 110.

Answer: C

Explanation:
Port 80 is used by HTTP
Port 443 is used by HTTPS (HTTP over SSL)
Port 21 is used by FTP, and
Port 25 is used by SMTP
Incorrect answers:
A: Port 119 TCP is used by Network News Transfer Protocol (NNTP). Port 23 is used by Telnet. Ports 21 and 80 would be a necessity.
B: Ports 443 and 21 would be useful in setting up the web server. Port 119 TCP is used by Network News Transfer Protocol (NNTP). Port 1250 is used for swldy-sias.
D: Only port 110 would not be essential as it is used for POP version 3
Reference:

Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Appendix B
http://www.iana.org/assignments/port-numbers

QUESTION 440:

Choose the compoenent that you would locate in the DMZ (Demilitarized Zone).

A. Customer account database
B. User workstations
C. FTP (File Transfer Protocol) server
D. SQL (Structured Query Language) server

Answer: C

Explanation:
A DMZ is an area where you can place a public server for access by people you might not trust otherwise. By isolating a server in a DMZ, you can hide or remove access to other areas of your network.
A FTP server can be used by people from outside of your network and should be placed in the DMZ.
Incorrect answers:
A: The customers will not feel confident in your company as some of their confidential information will be exposed.
B: Staff workstations are not meant to be in a DMZ.
D: Your SQL based database server might hold confidential information that should not be open for scrutiny.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 26

QUESTION 441:

From the options, which explains the general standpoint behind a DMZ (Demilitarized Zone)?

A. All systems on the DMZ can be compromised because the DMZ can be accessed from the Internet.
B. No systems on the DMZ can be compromised because the DMZ cannot be accessed from the Internet.
C. Only those systems on the DMZ that can be accessed from the Internet can be compromised.
D. No systems on the DMZ can be compromised because the DMZ is completely secure and cannot be accessed from the Internet.

Answer: A

Explanation:
A DMZ (demilitarized zone) is an area in a network that allows restrictive access to untrusted users and isolates the internal network from access by external users and systems. It does so by using routers and firewalls to limit access to sensitive network resources.
Incorrect answers:
B: A demilitarized zone is accessible from the Internet.
C: This is partly true.
D: This is not correct.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 28

QUESTION 442:

Which of the following descriptions best describes an IDS?

A. Monitors network traffic and traffic patterns that could be indicative of attacks such as port scans and denial-of-service attacks.
B. Runs as software on a host computer system to monitor machine logs, system logs, and applications interactions.
C. Monitors the file structure of a system to determine if any system files were deleted or modified by an attacker.
D. A hardware device with software that monitors events in a system or network to identify when intrusions are taking place.
E. Works by parsing system log entries to isolate any system attacks.

Answer: D

Explanation:
An IDS system is a hardware device with software that monitors events in a system or network to identify when intrusions are taking place. The main types are a host-based IDS system and network IDS system. With a host-based IDS system, software runs on the host computer system to monitor machine logs, system logs, and how applications inter-operate. With a network IDS, the IDS checks for network traffic and traffic patterns that could be indicative of attacks such as port scan and denial-of-service attacks.
Incorrect answers:
A: A network IDS monitors network traffic and traffic patterns that could be indicative of attacks such as port scan and denial-of-service attacks.
B: A host-based IDS runs as software on a host computer system to monitor machine logs, system logs, and applications interactions
C: A system integrity verifier (SIV) monitors the file structure of a system to determine if any system files were deleted or modified by an attacker.
E: A log file monitor (LFM) parses system log entries to isolate any system attacks.
Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 443:

A misuse-detection IDS is mainly focused on which of the following?

A. Monitoring machine logs, system logs, and applications interactions on the host on which the IDS software is running
B. Monitoring events on the network to identify when intrusions are taking place.
C. Isolating attacks based on attack signatures and audit trails.
D. Monitoring the network to look for anomalies.

Answer: C

Explanation:
A misuse-detection IDS is mainly focused on isolating attacks based on attack signatures and audit trails.
Incorrect answers:
A: A host-based IDS runs as software on a host computer system to monitor machine logs, system logs, and applications interactions.
B: A network IDS monitors network traffic and traffic patterns that could be indicative of attacks such as port scan and denial-of-service attacks.
D: An anomaly-detection IDS monitors the network to look for anomalies.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 444:

Which of the following is a popular network IDS system?

A. Tripwire
B. Snort
C. SWATCH
D. None of the above

Answer: B

Explanation:
Snort is a popular network IDS system. Snort can isolate attacks such as any attempts at guessing the password to a network resource, port scanning, and denial of service (DoS) attacks.
Incorrect answers:
A: Tripwire is a popular system integrity verifier (SIV). Tripwire examine the file structure of a system to determine whether any system files were deleted or modified by an attacker
C: SWATCH is a log file monitor (LFM) for UNIX operating systems.
D: Snort is a popular network IDS system.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 445:

Of the reasons listed below, which is not a main reason for implementing a honeypot within your network environment?

A. To provide the means for administrators to collect information on hackers and attack techniques used to compromise systems, so that the appropriate measures can be implemented to secure the internal network.
B. To track and report specific events or network traffic that deviate from acceptable, standard work activity or network traffic patterns
C. To collect information on attackers who gain unauthorized access to the network; and then use the information to prosecute the guilty individuals.
D. To act as a decoy to hackers, or at least distract the hacker.

Answer: B

Explanation:
The main purpose of implementing an IDS system is to track and report specific events or network traffic that deviate from acceptable, standard work activity or network traffic patterns.
Incorrect answers:
A, C, D: Each of these is a reason why honeypots are implemented.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 172.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 446:

Which of the following intrusion detection technologies work by monitoring the file structure of a system to determine whether any system files were deleted or modified by an attacker?

A. Network IDS
B. Host-based IDS
C. System integrity verifier (SIV)
D. Log file monitor (LFM)

Answer: C

Explanation:
A system integrity verifier checks the file structure of a system to determine if any system files were deleted or modified by an attacker. Tripwire is a popular system integrity verifier (SIV).
Incorrect answers:
A: A network IDS monitors network traffic and traffic patterns that could be indicative of attacks such as port scan and denial-of-service attacks.
B: A host-based IDS runs as software on a host computer system to monitor machine logs, system logs, and application interactions.
D: A log file monitor (LFM) parses system log entries to isolate system attacks.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 447:

Which of the following IDS response methods should be used if you want the IDS to instruct the firewall to block sockets and ports that are sending offensive traffic?

A. Session termination
B. Deception
C. Network Configuration changes
D. Shunning

Answer: C

Explanation:
Network configuration changes is an active response that allows the IDS to instruct a firewall to close specific ports. The IDS can also instruct the firewall to not process requests from a specific IP address.
Incorrect answers:
A: An IDS can be configured to reset all open TCP connections, and restart processes that are not operating normally. Here, the response method would be session termination.
B: The aim of deception is to fool the attacker into thinking that he/she is being successful in their attack, while tracking his activity, and sending the attacker to a system that can be attacked/broken.
D: Shunning, a passive response, basically involves ignoring the attack because the specific attack will not work.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 448:

Which if the following technologies would you use if you need to implement a system that simulates a network of vulnerable devices, so that this network can be targeted by attackers?

A. A IDS
B. A circuit-level firewall
C. A honeypot
D. A system integrity verifier

Answer: C

Explanation:
A honey pot is the technology that you would implement if you need to have a decoy within your network, designed to attract hackers. A honeypot simulates a network of vulnerable devices, and have logging and tracing enabled. To attract hackers, a honeypot has its security level purposefully set quite low.
Incorrect answers:
A: An IDS system is a hardware device with software that monitors events in a system or network to identify when intrusions are taking place. The main types are a host-based IDS system and network IDS system.
B: A circuit-level firewall watches TCP and UDP ports, and can be used to configure security devices with the rate of responses to requests to process, and to block any impending communications from suspicious hosts.
D: A system integrity verifier (SIV) monitors the file structure of a system to determine

whether system files were deleted or modified by an attacker.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170, 172.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 449:

Which of the following security technologies cannot protect hosts from direct attacks, nor can they resolve security issues?

A. A circuit level firewall.
B. A IDS
C. A honeypot
D. A packet filtering firewall

Answer: C

Explanation:
A honeypot is merely a system that simulates a network of vulnerable devices. A honeypot has its security level purposefully set quite low, so as to draw attackers to it, and divert them from the private network.
Incorrect answers:
A: A circuit-level firewall watches TCP and UDP ports, and can be used to configure security devices with the rate of responses to requests to process, and to block any impending communications from suspicious hosts.
B: An IDS system is a hardware device with software that monitors events in a system or network to identify when intrusions are taking place.
D: Packet filtering firewalls allow or blocks traffic based on the type of application. This type of firewall decides whether to pass traffic based on the packet's addressing information and can be based on IP addresses or ports.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 450:

When using network monitoring systems to monitor workstations, which of the following elements should be reviewed because their information could indicate a

possible attack?

A. Audit log and system log
B. Hard disk space
C. Network counters
D. Network counters and access denied errors

Answer: D

Explanation:
Both network counters and access denied errors could indicate an attack in progress. When an attacker attempts to guess a password, a higher number of access denied errors are recorded.
Incorrect answers:
A: Audit logs are usually activated as part of your auditing policy, to track specific resource usage. System logs are used to track error messages on services that fail to start, track permission and file system changes, and track critical error messages.
B: Hard disk space should be regularly examined to identify workstations that could be failing to operate optimally, and log errors due to lack of resources.
C: Network counters is only part of the correct answer. You should also check access denied errors.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 451:

A passive response is the most common type of response to a number of intrusions. Which of the following is not a passive response strategy?

A. Logging
B. Notification
C. Deception
D. Shunning

Answer: C

Explanation:
Deception is an active response strategy. This response strategy attempts to send the attacker to the honeypot. The aim of deception is to fool attackers into thinking that they are being successful in the attack, while tracking their activity, and then sending the attackers to a system that can be attacked/broken.
Incorrect answers:
A: Logging is a passive response that involves gathering sufficient information on the

attack to assist administrators in implementing measures to divert it. Logging usually involves recording of events and the circumstances under which they occurred.
B: Notification is a passive response strategy that involves informing the designated administrator when a security related event occurred and communicating information on the event.
D: Shunning, a passive response, basically involves ignoring the attack because the specific attack will not work.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 167 - 170.

QUESTION 452:

When under attack, which of the following is least likely to run out of resources?

A. A honeypot
B. Production system
C. Firewall
D. IDS

Answer: A

Explanation:
Because honeypots are designed to be targeted by hackers, they usually do not run out of resources when under attack. This enables a honeypot to continue to log valuable information on the attack while it is being performed.
Incorrect answers:
B, C, D: Production systems, firewalls, and IDS systems usually no longer operate optimally when under attack. These systems tend to drop packets and eventually fail.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 102 - 104.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 453:

Which IDS response type(s) only collects information on the attack and reports it?

A. Active response method
B. Passive response method
C. Both of these response methods

Answer: B

Explanation:
The passive response type only collects sufficient information on the attack to assist administrators in implementing measures to divert it, and can also inform the designated administrator when a security related event occurred.
Incorrect answers:
A: An active response type can initiate an action based on the type of attack, to reduce the severity of the attack that is underway.
C: The correct answer is passive response.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 166 - 168.

QUESTION 454:

When discussing IDS systems, of the list of responses below, which is not an active response?

A. Session termination
B. Deception
C. Network Configuration changes
D. Shunning

Answer: D

Explanation:
Shunning is a passive response that basically involves ignoring the attack because the specific attack will not work.
Incorrect answers:
A: The session termination active response allows the IDS to reset all open TCP connections, and restart processes that are not operating normally.
B: The aim of deception (active response) is to fool the attacker into thinking that the attack is successful. Deception deals with tracking the intruder's activity, and then sending the attacker to a system, such as a honeypot, that can be attacked.
C: Network configuration changes (active response) is an active response where the IDS is enabled to instruct a firewall to close specific ports or to not process requests from a specific IP address.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 166 - 168.

QUESTION 455:

With reference to honeypots, which statement is FALSE?

A. Honeypots cannot protect hosts from direct attacks.

B. A honey pot is merely a system that simulates a network of vulnerable devices.
C. A honeypot has its security level purposefully set quite low.
D. Honeypots are usually more difficult to monitor than IDS systems and firewalls.

Answer: D

Explanation:
When compared to IDSs and firewalls, honeypots are usually easier to configure and monitor. In addition to this, IDSs and firewalls collect vast quantities of information while honeypots provide valuable information on only the specific attack.
Incorrect answers:
A, B, C: These statements are TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 456:

If you want the IDS to block a specific socket or port when it is under attack, which response method would you need to configure?

A. Session termination
B. Deception
C. Network Configuration changes
D. Shunning

Answer: C

Explanation:
Network configuration changes is an active response where the IDS is configured to instruct a firewall to close specific ports or to not process requests from a specific IP address. When the IDS detect that a port is under attack, it will inform the firewall to block traffic from that specific port.
Incorrect answers:
A: An IDS can also be configured to reset all open TCP connections, and restart processes that are not operating normally. This is what the session termination response method configures the IDS to do.
B: The aim of deception is to fool the attacker into thinking that it is being successful in its attack, while tracking his activity, and sending the attacker to a system that can be attacked/broken.
C: Shunning, a passive response, basically involves ignoring the attack because the specific attack will not work

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 166 - 168.

QUESTION 457:

Of the different IDS types and analysis methods, which of the following is considered the simplest IDS system to implement?

A. Pattern matching network-based IDS.
B. Stateful inspection network-based IDS.
C. Protocol decode analysis IDS.
D. Heuristic analysis IDS.

Answer: A

Explanation:
The pattern matching network-based IDSs is the simplest network-based IDS system that you can implement. The pattern matching network-based IDSs works by inspecting each packet and then compares it to the signature database. The signature database contains all known attack signatures.
Incorrect answers:
B: A stateful inspection network-based IDS is more intelligent that a pattern matching network-based IDS, simply because stateful inspection looks for signatures within data streams and not only at single packets.
C: A protocol decode analysis IDS improves on both pattern matching and stateful inspection network-based IDS. Protocol decode analysis applies protocol rules, defined in RFCs, in an attempt to find suspicious traffic. This essentially means that a protocol decode analysis IDS can look for irregularities in a packet's header field values and lengths.
D: The heuristic analysis IDS uses signatures like the pattern matching network-based IDSs, but it also implements threshold and frequency analysis. A heuristic analysis IDS can statistically analyze traffic to find suspicious traffic.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 458:

When defining methods to secure and monitor servers, which of the following statements are FALSE?

A. Servers should be secured in a locked room.
B. You should implement measures than prevent users from logging on interactively.
C. Monitor access to resources and services.
D. Use motion alarms and tracking equipment to better secure your servers.
E. Perform regular backups of your server configurations, service data, and all shared data.

Answer: D

Explanation:
To secure mobile devices, it is recommended that you use motion alarms and tracking equipment to better secure these devices.
Incorrect answers:
A, B, C, D These statements are all TRUE.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5

QUESTION 459:

Of the different IDS analysis methodologies, which is the most intricate to configure but also provides the most complex logic to monitor network activity and detect suspicious traffic, when compared to the other methodologies?

A. Pattern matching network-based IDS.
B. Stateful inspection network-based IDS.
C. Protocol decode analysis IDS.
D. Heuristic analysis IDS.

Answer: D

Explanation:
The heuristic analysis IDS system uses signatures like the pattern matching network-based IDSs, but it also implements threshold and frequency analysis. A heuristic analysis IDS can statistically analyze traffic to find suspicious traffic.
Incorrect answers:
A: The pattern matching network-based IDSs works by inspecting each packet and then compares it to the signature database. This is the simplest IDS method to use.
B: A stateful inspection network-based IDS is more intelligent that a pattern matching network-based IDSs, simply because stateful inspection looks for signatures within data streams and not only at single packets.
C: Protocol decode analysis IDS improves on both pattern matching and stateful inspection network-based IDS. Protocol decode analysis also applies protocol rules, defined in RFCs, in an attempt to find suspicious traffic. This essentially means that a protocol decode analysis IDS can look for irregularities in a packet's header field values and lengths.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 460:

With reference to locating honeypots, which of the following locations is the most dangerous placement strategy because an administrator has little control over it?

A. Inside the DMZ
B. Outside all firewalls.
C. Inside the private network
D. All of the above.

Answer: B

Explanation:
Placing the honeypot outside all firewalls means that administrators have little control over the decoy mechanism. It will be easy for attackers to use the decoy to initiate attacks.
Incorrect answers:
A: Placing the honeypot inside the DMZ means that the honeypot has a medium chance of drawing the attention of attackers because of firewall protection and invisibility.
C: Here, the decoy would probably not be attacked by external attackers. However, this placement provides some benefit to attacks being initiated from within the company.
D: B is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 461:

If you want to implement an IDS system that can check data streams for suspicious traffic, but is still relatively simple to configure, which would you implement?

A. Pattern matching network-based IDS.
B. Stateful inspection network-based IDS.
C. Protocol decode analysis IDS.

D. Heuristic analysis IDS.

Answer: B

Explanation:
A stateful inspection network-based IDS is more intelligent that a pattern matching network-based IDSs, simply because stateful inspection looks for signatures within data streams and not only at single packets. Other than for this, configuring stateful inspection network-based IDS is fairly simple because it is still a pattern matching IDS system.
Incorrect answers:
A: The pattern matching network-based IDSs is the simplest network-based IDS system that you can implement and is one of the simplest IDS systems to configure. The pattern matching network-based IDS cannot though look for signatures within data streams.
C: A protocol decode analysis IDS improves on both pattern matching and stateful inspection network-based IDS. Being a more complicated variation of pattern matching NIDS, protocol decode analysis is more intricate to configure than pattern matching and stateful inspection network-based IDS systems
D: While a heuristic analysis IDS can statistically analyze traffic to find suspicious traffic, to configure heuristic analysis network-based IDS and define all the thresholds to their optimal values does take quite some administrative effort.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 462:

Which of the following IDS analysis methods improves on both pattern matching and stateful inspection network-based IDS?

A. Protocol decode analysis IDS.
B. Heuristic analysis IDS.
C. Passive analysis IDS
D. None of the above

Answer: A

Explanation:
A protocol decode analysis IDS improves on both pattern matching and stateful inspection network-based IDS. Being a more complicated variation of pattern matching network IDS, protocol decode analysis is more intricate to configure than pattern matching network-based IDS and stateful inspection.
Incorrect answers:

B: While a heuristic analysis IDS can statistically analyze traffic to find suspicious traffic, to configure heuristic analysis network-based IDS and define all the thresholds to their optimal values does though take quite some administrative effort.
C: A passive analysis IDS system only watches traffic and can alert an administrator when suspicious activity is detected in network traffic. It can also record a communication session for later analysis.
D: A protocol decode analysis IDS is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 463:

When discussing the monitoring capabilities of a host-based IDS system, which of the statements best describes its capabilities?

A. A host-based IDS can monitor all network traffic, the ports used by the system or incoming connections, and it can monitor processes running on the system.
B. A host-based IDS can monitor network traffic specific to the host on which it is running, monitor checksums of important system files, the ports used by the system or incoming connections, and processes running on the system.
C. A host-based IDS can monitor network traffic specific to the host, checksums of important system files, ports used by the system or incoming connections, processes running on the system, and can include content filters and antivirus modules.
D. A host-based IDS can monitor network traffic specific to the host, checksums of important system files, ports used by the system or incoming connections, processes running on the system, and can include content filters.

Answer: C

Explanation:
This is the most correct answer. A host-based IDS system can only monitor traffic specific to the host on which it is running. It can also monitor checksums of important system files; ports used by the system or incoming connections, processes ruining on the system, and can include content filters and antivirus modules.
Incorrect answers:
A: This answer is incorrect, mainly because the host-based IDS system can only monitor traffic specific to the host on which it is running. It cannot monitor all network traffic.
B: This option does not include a host-based IDS system's capabilities to include content filters and antivirus modules that provide protection from viruses, client scripts, and spam attacks.
D: This option does not include the antivirus module.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 464:

A host-based IDS system can perform a number of monitoring and intrusion detection activities which a network IDS cannot. Choose the one that does not apply?

A. Can monitor system activity on the workstation
B. Can monitor workstation activity.
C. Can see information within encrypted tunnels.
D. Can monitor program installations.
E. Can monitor user logon/logoff events.

Answer: C

Explanation:
A host-based IDS system cannot see the information within the tunnel. This is due to end-to-end encryption only showing tunnel addressing and encapsulation information.
Incorrect answers:
A, B, D: These are all monitoring and intrusion detection activities that can be performed by a host-based IDS system, and not a network IDS.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 465:

Which of the following IDS analysis methods have the disadvantage of generating large volumes of false positive alerts and can flood the system with useless data, when the defined signatures are not specific enough?

A. Pattern matching network-based IDS.
B. Protocol decode analysis IDS.
C. Heuristic analysis IDS.
D. None of the above.

Answer: A

Explanation:
A pattern matching network-based IDSs uses highly specific signatures when monitoring the network to search for signatured patterns. When the signatures are not specific, the pattern matching process can cause large volumes of false positive alerts that eventually end up flooding the system.
Incorrect answers:
B: A protocol decode analysis IDS system applies protocol rules, defined in RFCs, in its attempt to find suspicious traffic. When signatures are accurately defined, fewer false positive alerts are reported.
C: A heuristic analysis IDS can statistically analyze traffic to find suspicious traffic. When signatures are accurately defined, and the threshold is specified appropriately, fewer false positive alerts are reported.
D: Pattern matching network-based IDS is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 466:

Of the intrusion detection capabilities listed below, which is FALSE for a network based IDS system?

A. A network based IDS system can monitor and report on all network traffic, based on where it is located.
B. A network based IDS system can see packet header information, which is invisible to host-based IDS systems.
C. A network based IDS system can detect dial-in intrusions and attempts to physically access the server.
D. A network based IDS system can detect attacks in progress, attack patterns within the network and malicious activities.

Answer: C

Explanation:
A host-based IDS, not network IDS system, can detect dial-in intrusions and attempts to physically access the server. These intrusions would typically not cross any network wires, and would therefore not be visible to network-based IDS systems.
Incorrect answers:
A, B, D: These statements are all TRUE

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 467:

When a network-based IDS detects a suspicious event, it can perform a number of actions. Which of the following does not apply?

A. Can pass an alarm to an administrative console or to a network management station through an SNMP trap.
B. Can transmit an email to the designated personnel directly or through a distribution group.
C. Can log the offending user off the system and disable the user account.
D. Can reset the suspect network connection and reconfigure a firewall.

Answer: C

Explanation:
A host-based IDS can log the offending user off the system and disable the user account.
Incorrect answers:
A, B, D: These are all actions which can be performed by a network-based IDS system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 468:

Of the intrusion detection capabilities listed below, which is FALSE for a host-based IDS system?

A. A host-based IDS system can monitor and report on all network traffic.
B. A host-based IDS system can detect dial-in intrusions and attempts to physically access the server.
C. A host-based IDS system provide better protection than a network IDS in terms of providing protection from external and from internal attacks.
D. A host-based IDS can monitor system files and running processes.

Answer: A

Explanation:
A host-based IDS only monitors network traffic, specific to the host on which it is running.
Incorrect answers:
B, C, D: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 469:

When a host-based IDS detects a suspicious event, it can perform a number of actions. Which of the following does not apply?

A. Can reset the suspect network connection and reconfigure a firewall.
B. Can pass an alarm to an administrative console or to a network management station through an SNMP trap.
C. Can store a record of the event in the log.
D. Can log the offending user off the system and also disable the user account.

Answer: A

Explanation:
A network-based IDS can reset the network connection and reconfigure a firewall.
Incorrect answers:
B, C, D: These are all actions which can be performed by a host-based IDS system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 470:

Which of the statements pertaining to heuristic analysis is FALSE?

A. A heuristic analysis IDS uses signatures like the pattern matching network-based IDS systems.

B. A heuristic analysis IDS implements threshold and frequency analysis.
C. This analysis method works on the assumption that a pattern could be detected a number of times before it is considered suspicious.
D. A heuristic analysis IDS can use less-specific signatures.
E. A heuristic analysis IDS can statistically analyze network traffic to find suspicious traffic.

Answer: D

Explanation:
A heuristic analysis IDS needs signatures to be accurately defined, and threshold values to be specified appropriately. This has the advantage of fewer false positive alerts being reported. Protocol decode analysis can use less-specific signatures.
Incorrect answers:
A, B, C, E: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 471:

With reference to locating honeypots, which of the following placement strategies provides some benefit for attacks being initiated from within the company network?

A. Inside the DMZ
B. Outside all firewalls.
C. Inside the private network
D. All of the above.

Answer: C

Explanation:
Here, the decoy would probably not be attacked by external attackers. However, it provides some benefit to attacks being initiated from within the company
Incorrect answers:
A: Placing the honeypot inside the DMZ means that the honeypot has a medium chance of drawing the attention of attackers because of firewall protection and invisibility.
B: Placing the honeypot outside all firewalls means that administrators have little control over the decoy mechanism. It will be easy for attackers to use the decoy to initiate attacks.
D: C is the correct answer.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 165 - 170.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 4, Lesson 5
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 472:

Into which category of systems would NetBus and Back Orifice fall?

A. Virus programs
B. Illicit servers
C. Spoofing tools
D. Allowable servers

Answer: B

Explanation:
Illicit servers are also known as 'backdoors.' They allow system access without using a security check.
An illicit server is an application/program that shouldn't be there but is operating on the network, and one that is commonly used to gain unauthorized control by allowing someone to bypass normal authentication. NetBus is one of the best-known examples of an illicit server.
Incorrect answers:
A: A virus is a program intended to damage a computer system. Sophisticated viruses are encrypted and hide in a computer and may not appear until the user performs a certain action or until a certain date. For example worms and phage viruses.
C: A spoofing attack is an attempt by someone or something to masquerade as someone else.
D: This is exactly the opposite of an illicit server.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 251

QUESTION 473:

Choose the three categories of active responses performed by intrusion detection.

A. Gather additional information, maintain the environment, perform an action against the intruder.
B. Gather additional information, change the environment, inform the manager of the intrusion.
C. Gather additional information, change the environment, perform an action against the intruder.

D. Drop any additional information, change the environment, perform an action against the intruder.

Answer: C

Explanation:
An active intrusion detection response is to begin taking action against the intruder as soon as the breach is detected. The principles are: detection (collect additional information), deflection (change the environment), and countermeasures (take action against the intruder).
So changing the environment to spoof the attacker and hide your valuable resources; and collecting details about the source of the intrusion and the type of intrusion to gather evidence for prosecution and future system hardening are all components of active intrusion detection.
Incorrect answers:
A: Maintaining the environment would be contradictory to the aim of the intrusion.
B: Only alerting the manager is not what intrusion detection is about.
D: It will not discard information.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide Second Edition, Sybex Publishing, Alameda, 2004, p. 115

QUESTION 474:

Choose the terminology used to refer to the situation when authorized access is perceived
as an intrusion or network attack.

A. False negative
B. False intrusion
C. False positive
D. False alarm

Answer: B

Explanation:
False intrusion is a false alarm, when there is no need of any alarm.
Incorrect answers:
A: This is a false negative acknowledgments of intrusion in an intrusion detection system, which means an intrusion has occurred but the IDS discarded related events or traces as false signals.
C: A false positive is a false affirmative acknowledgment of intrusion, which means an intrusion detection has incorrectly identified certain events or traces as signaling an attack or intrusion when no such attack or intrusion is underway. Thus, a false positive is a false alarm. A false positive is when legitimate traffic is picked up as an intruder.
D: False alarms can happen if the facility is in a remote location, wildlife and even the

wind can set off sound-based motion sensors. These alarms are comprised of microphones and monitoring chips that react when sound is produced in the monitored area, above a preset threshold (this is the area where adjustments can be made). These devices should be used in conjunction with other mechanisms, such as cameras, to help prevent reactions to normal events such as deer, dogs, cats, and the occasional stiff breeze.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 4

QUESTION 475:

You work as the security administrator at Certkiller .com. You are monitoring the Certkiller .com network and immediately notice that a security breach has recently occurred.
What should you do as your first countermeasure to the security breach?

A. Perform encryption
B. Perform authentication
C. Perform containment
D. Perform intrusion

Answer: C

Explanation:
When the hull of a ship ruptures, the crew seals the locks to contain the damage. When a population is exposed to a disease like SARS, those infected are quarantined to contain further infection. When a network's security is breached, it may take a while to fix the problem, and in the panic it's possible to actually spread the damage further, so the most important initial step is to contain the breach to minimize damage and ease reconstruction.
Incorrect answers:
A: Encryption should have been used as a preventative measure.
B: Authentication could have prevented a security breach.
D: Intrusion already occurred due to the security breach.
Reference:
Todd Bill, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 9

QUESTION 476:

Choose the planning element that should include a severed T1 line

A. Data recovery planning process.
B. Off site storage planning process.
C. Media destruction planning process.

D. Incident response planning process.

Answer: D

Explanation:
Telecommunications technology is developing to the point where all communications occur via data links to phone companies using standard data transmission technologies, such as T1 or T3. This means that both voice and data communications are occurring over the same network connection to a phone company or a provider. This allows a single connection for all communications to a single provider of these services. If someone intentionally severs a T1 cable you have a serious incident on your hands. An attack like this should be considered when planning incident response.
Incorrect answers:
A: Data recovery can be effected through backups and a severed T1 line would not be relevant.
B: Offsite storage would not be affected by a severed T1 line.
C: Media destruction is not reliant on a T1 line.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 111

QUESTION 477:

Choose the option that best defines what a security patch is?

A. It is a major, crucial update for an operating system or product for which it is intended, and consists of a collection of patches released to date since the operating system or product was shipped.
B. It is a fully tested hotfix, which addresses a new vulnerability, is mandatory for all users, and should be deployed as soon as possible.
C. It is a crucial update that should be deployed on each operating system installation as soon as possible.
D. It is a not fully tested software fix which addresses a specific issue(s) being experienced by certain customers.

Answer: B

Explanation:
A security patch is a fully tested hotfix that is released to address a new vulnerability. Security patches, unlike standard software hotfixes, have been fully tested. Another differentiating factor is that a security patch is mandatory for all users.
Incorrect answers:
A: A service pack is a major, crucial update for an operating system or product for which it is intended, and consists of a collection of patches released to date since the operating system or product was shipped.
C: A service pack can be thought of being a crucial update that should be deployed on

each operating system installation as soon as possible
D: A hotfix is a software fix, not fully tested, which addresses a specific issue(s) being experienced by certain customers
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 478:

Operating system hardening essentially means securing the operating system.
Which of the following is not a method, specific for securing the operating system?

A. Disable unnecessary programs, processes, and services and protocols.
B. Use encryption to protect the transfer of sensitive information, and ensure that encryption is enabled between the server and client.
C. Regularly check for vendor patches; and test and install all vendor patches.
D. You should disable promiscuous mode.
E. Consider using vulnerability scanners to assist you with identifying all potential security weaknesses.

Answer: B

Explanation:
Using encryption to protect the transfer of sensitive information, and ensuring that encryption is enabled between the server and client; and is a strategy for server application hardening - not specific for operating system hardening.
Incorrect answers:
A, C, D, E: These are all strategies for hardening the operating system.
Reference:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 479:

Firmware updates are usually produced by manufactures to address security issues with regard to processing logic or the operating system. To deploy any firmware update, you should perform a number of steps. Choose the one that does not apply.

A. Before you install any firmware update, first verify that it is authentic and not corrupted. To perform this authenticity check, you can verify the digital signature or checksum.
B. You do not need to perform a backup of the existing IOS image and running

configuration because this is a firmware update.
C. After you verify the authenticity of the firmware update, you can download the IOS image and place it on the network.
D. Perform the firmware update installation and download the new IOS image from the Trivial FTP (TFTP) server, File Transfer Protocol (FTP) server, or through NAS Change Proposal (NCP).

Answer: B

Explanation:
It is strongly recommended that you back up the existing IOS image and running configuration before you deploy any firmware update. If you are using TFTP, use the copy flash tftp command. To back up the running configuration, use the copy running-config tftp command.
Incorrect answers:
A, C, D: These steps are all part of the correct process to use, to deploy new firmware updates.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 480:

Choose the option that best defines what a hotfix is?

A. It is a major, crucial update for an operating system or product for which it is intended, and consists of a collection of patches released to date since the operating system or product was shipped.
B. It is a fully tested configuration, which addresses a new vulnerability, is mandatory for all users and should be deployed as soon as possible.
C. It is a crucial update that should be deployed on each operating system installation as soon as possible.
D. It is a not fully tested software fix which addresses a specific issue(s) being experienced by certain customers.

Answer: D

Explanation:
A hotfix is a not fully tested software fix which addresses a specific issue(s) being experienced by certain customers
Incorrect answers:
A: A service pack is a major, crucial update for an operating system or product for which it is intended, and consists of a collection of patches released to date, since the operating system or product was shipped.

B: A security patch is a fully tested hotfix that is released to address a new vulnerability. Security patches, unlike hotfixes, have been fully tested. Another differentiating factor is that a security patch is mandatory for all users.
C: A service pack is a crucial update that should be deployed on each operating system installation as soon as possible.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 481:

Of the three primary network protocols, which one is least secure?

A. NetBEUI
B. TCP/IP
C. IPX/SPX

Answer: A

Explanation:
The NetBEUI network protocol, developed by Microsoft for Windows networks, is the least secure between the three network protocols. This is due to NetBEUI not being designed to provide any of its own security capabilities. NetBEUI packets reveal information on system configuration, running services, and other information which an attacker can use to find ways to exploit the system. NetBEUI is less efficient than IPX/SPX or TCP/IP in large networking environments.
Incorrect answers:
B, C: The TCP/IP and IPX/SPX protocols are more efficient than NetBEUI in large networking environments. The current implementation of the TCP/IP protocol is relatively more secure than its earlier implementations.
References:
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 203 - 205.

QUESTION 482:

Which of the following is mandatory for all users, addresses a new vulnerability, and should be deployed as soon as possible?

A. A service pack
B. A security patch
C. A hotfix

D. A quick fix engineering (QFE).

Answer: B

Explanation:
A security patch is released to address a new vulnerability and is mandatory for all users.
Incorrect answers:
A: A service pack is a major, crucial update for an operating system or product for which it is intended, and consists of a collection of patches released to date since the operating system or product was shipped. A service pack might not address any vulnerability.
C: A hotfix might only address an issue, specific to certain customers only. A hotfix is therefore not mandatory for all users.
D: A quick fix engineering (QFE) is another name used to refer to a software hotfix.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 483:

Of the list of tools below, which is not a tool that collects security baseline-related information from Windows Management Instrumentation (WMI) or from sources other than WMI and Web-Based Enterprise Management (WBEM)?

A. MS Security Baseline Analyzer tool (MSBA).
B. MS Systems Management Server.
C. HFNetChk tool.
D. Snort.
E. Custom WMI scripting

Answer: D

Explanation:
Snort is a popular network IDS system. Snort can isolate attacks such as any attempts at guessing the password to a network resource, port scanning, and denial of service (DoS) attacks.
Incorrect answers:
A, B, C, E: These are all tools that collect security baseline-related information.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 484:

There are a number of methods by which you can harden the operating system.
From the list below, choose the appropriate answer.

A. Configure complex passwords for all user accounts, and also modify these passwords regularly.
B. Set account lockout policies.
C. Disable all unnecessary programs, processes, services and protocols, and modems.
D. Enable monitoring, logging, and intrusion detection techniques.
E. All of the above.

Answer: E

Explanation:
Each of the above mentioned options detail ways in which you can harden the operating system against external attacks.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 485:

For security patches, choose the FALSE statement.

A. Security patches can fix low-risk, moderate risk, or critical problems.
B. A security patch is mandatory for all users.
C. Because of their importance, security patches are usually fairly large in size.
D. A security patch can deal with client applications as well as subsystems integral to the workstations.

Answer: C

Explanation:
A service pack, and not security patch, is usually fairly large in size. This is due to a service pack containing all patches released to date since the operating system was shipped.
Incorrect answers:
A, B and D: These statements are all TRUE.
Reference:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 486:

Of the primary file systems listed below, which one offers the least security, and is especially unsecure in an Internet environment?

A. File Allocation Table (FAT)
B. New Technology File System (NTFS)
C. NetWare Storage Service (NSS)
D. Unix filesystem

Answer: A

Explanation:
The FAT file system offers the least security and is especially unsecure in an Internet environment. To address the security shortcomings of the FAT file system, Microsoft introduced the New Technology File System (NTFS) file system.
Incorrect answers:
B With the NTFS file system, security is built-in and very flexible; and files, directories, and volumes can have their own specific security defined. NTFS tracks security in Access Control Lists (ACLs). Each entry in the ACL can specify the access type granted. File encryption programs can also be used to encrypt data stored on the hard disk.
C
: The NSS file system enables control of each file resource residing on the NetWare server. The NSS file system provides security, high performance, large file storage capacities, and uses the NDS or eDirectory to provide authentication for access.
D: This is a hierarchical file system where each file, filesystem and subdirectory has complete granular access control.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 211- 212.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 487:

Which of the following network devices is your front line of defense?

A. Switches
B. Routers
C. Web and e-mail servers
D. DNS servers

Answer: B

Explanation:

Routers are the front line of defense against attacks being launched from outside the company network. You can configure and apply access control lists to the interfaces of routers to filter out unauthorized traffic. Through ACLs, you can design and change network security to counter specific security threats.
Incorrect answers:
A: Switches are used to create VLANs.
C: Web and e-mail servers are not a company's first line of defense against external attacks.
D: DNS servers provide name resolution services.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 215- 216.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 488:

Of the tools listed below, which is not used to scan the system for missing security patch information?

A. HFNetChk.
B. Windows Update.
C. Tripwire.
D. MBSA.

Answer: C

Explanation:
Tripwire is a popular system integrity verifier (SIV). Tripwire examines the file structure of a system to determine whether any system files were deleted or modified by an attacker.
Incorrect answers:
A, B, D: You can use HFNetChk, Windows Update, or MBSA to scan the system for missing security patch information.
Reference:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 489:

Which of the following file systems is the most intricate to implement because is needs you to define access-control hierarchies?

A. File Allocation Table (FAT)

B. New Technology File System (NTFS)
C. NetWare Storage Service (NSS)
D. Unix filesystem

Answer: D

Explanation:
While the Unix filesystem is a hierarchical file system where each file, filesystem and subdirectory has complete granular access control, it is dependent on the establishment of access-control hierarchies. This can turn into a time consuming effort, especially when the system is initially being configured.
Incorrect answers:
A: To address the security shortcomings of the FAT file system, Microsoft introduced the New Technology File System (NTFS) file system.
B With the NTFS file system, security is built-in and very flexible; and files, directories, and volumes can have their own specific security defined. NTFS tracks security in Access Control Lists (ACLs). Each entry in the ACL can specify the access type granted. Implementing NTFS is not dependent on the establishment of access-control hierarchies.
C: The NSS file system provides security, high performance, large file storage capacities, and uses the NDS or eDirectory to provide authentication for access. Implementing the NSS file system is not dependent on the establishment of access-control hierarchies.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 211- 212.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 490:

A number of factors need to be considered when you implement strategies to secure routers. Choose the factor that does not specifically relate to routers.

A. Physical security.
B. Router configuration security
C. Remote access security
D. Vulnerability scanning tools
E. Router interface security
F. Protocol security

Answer: D

Explanation:
Vulnerability scanning tools are usually used for application server hardening. There are vulnerability scanning tools designed for specific types of servers.
Incorrect answers:
A, B, C, E, F: Each of these factors should all be considered when implementing

strategies to harden and secure routers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 215- 216.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 491:

Which of these attacks, aimed at DNS servers, attempts to gather information on your network and network configuration?

A. DNS DoS attacks.
B. Network footprinting.
C. DNS cache poisoning
D. Compromising record integrity attacks

Answer: B

Explanation:
Because DNS servers usually store a vast quantity of information on the network and its configuration, they are also typically targeted by network footprinting attacks. Network footprinting is an attack that attempts to gather information on your network. To protect your DNS servers from network footprinting attacks, ensure that all information on the network, which gets stored in external DNS servers, are kept at a minimum.
Incorrect answers:
A: Most DoS attacks are aimed at DNS servers. This is a very real threat against DNS servers in todays networks because should the attack be successful, the system could become unusable. To protect your DNS servers from DoS attacks, ensure that all DNS server software and the operating system software are kept up to date with the latest security patches and service packs.
C: With the earlier implementations of DNS, DNS cache poisoning has been a very real threat. However, with the latest release of DNS, this attack has becomes rare. In DNS cache poisoning, a daemon caches DNS reply packets. The information obtained from the attack is typically used to launch break-in or man-in-the-middle attacks. While this attack has not been seen for a while, you still need to be aware of it.
D
: Here, an attacker inserts a false record in the primary DNS so that it will update or direct clients to the incorrect site. To prevent this from happening, ensure that authentication is required before any updates are made.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 492:

If you want to prevent the DHCP server from responding to requests from external users, which of the following ports should you block on the firewall?

A. TCP/UDP ports 137, 138, and 139
B. TCP/UDP port 67 and 68
C. TCP/UDP port 119
D. TCP port 110

Answer: B

Explanation:
If you want to ensure that the DHCP server does not respond to requests from external users, you should block TCP/UDP port 67 and 68 on the firewall.
Incorrect answers:
A: TCP/UDP ports 137, 138, and 139 are used by NetBIOS names and sessions.
C: Blocking TCP/UDP port 119 on the firewall prevents external users from accessing the private NNTP server.
D: POP3 clients use TCP port 110 to access the e-mail server.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 493:

Of the file systems listed below, which can track security in Access Control Lists (ACLs), and also provides file encryption programs to encrypt data stored on the hard disk?

A. File Allocation Table (FAT)
B. New Technology File System (NTFS)
C. NetWare Storage Service (NSS)
D. Unix filesystem

Answer: B

Explanation:
With the NTFS file system, security is built-in and very flexible; and files, directories, and volumes can have their own specific security defined. NTFS can track security in Access Control Lists (ACLs). Each entry in the ACL can specify the access type granted. File encryption programs can also be used to encrypt data stored on the hard disk.
Incorrect answers:
A: To address the security shortcomings of the FAT file system, Microsoft introduced the

New Technology File System (NTFS) file system.
C: The NSS file system enables control of each file resource residing on the NetWare server. The NSS file system provides security, high performance, large file storage capacities, and uses the NDS or eDirectory to provide authentication for access.
D: This is a hierarchical file system where each file, filesystem and subdirectory has complete granular access control.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 211- 212.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 494:

FTP servers can be used to serve both internal and external users. To secure your FTP servers, certain strategies can be used. Choose the FALSE statement?

A. You should limit access to your internal FTP servers.
B. To prevent your public FTP server from being used by attackers to compromise your internal network, place the public FTP server in the internal network so that it is protected by the firewall.
C. If you want to block FTP communications, you should block TCP port 20 and TCP port 21.
D. You should never allow unauthenticated write access.

Answer: B

Explanation:
To prevent your public FTP server from being used by attackers to compromise your internal network, you should place the public FTP server in the perimeter network. Should the public FTP server be compromised, your internal network will still be protected from being comprised through the public FTP server.
Incorrect answers:
A, C, D: These are all valid methods for securing FTP servers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p. 221
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 495:

Which of the following attacks is no longer as pertinent for DNS servers because the latest release of DNS includes measures to defend against the attack?

A. DNS DoS attacks.

B. Network footprinting.
C. DNS cache poisoning
D. Compromising record integrity attacks

Answer: C

Explanation:
With the earlier implementations of DNS, DNS cache poisoning has been a very real threat. However, with the latest release of DNS, this attack has becomes rare. In DNS cache poisoning, a daemon caches DNS reply packets. The information obtained from the attack is typically used to launch break-in or man-in-the-middle attacks. While this attack has not been seen for a while, you still need to be aware of it.
Incorrect answers:
A: Most DoS attacks are aimed at DNS servers. This is a very real threat against DNS servers in todays networks because should the attack be successful, the system could become unusable. To protect your DNS servers from DoS attacks, ensure that all DNS server software and the operating system software are up to date with all the latest security patches and service packs.
B: Because DNS servers usually store a vast quantity of information on the network and its configuration, they are also typically targeted by network footprinting. Network footprinting is an attack that attempts to gather information on your network. To protect your DNS servers from network footprinting attacks, ensure that all information on the network, which gets stored in external DNS servers are kept at a minimum.
D: Here, an attacker inserts a false record in the primary DNS server so that it will update or direct clients to the incorrect site. To prevent this from happening, ensure that authentication is required before any updates are made.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 496:

Of the primary file systems listed below, which uses NDS or eDirectory to provide authentication for access?

A. File Allocation Table (FAT)
B. New Technology File System (NTFS)
C. NetWare Storage Service (NSS)
D. Unix filesystem

Answer: C

Explanation:
The NSS file system provides security, high performance, large file storage capacities,

and uses the NDS or eDirectory to provide authentication for access.
Incorrect answers:
A: To address the security shortcomings of the FAT file system, Microsoft introduced the New Technology File System (NTFS) file system.
B With the NTFS file system, security is built-in and very flexible; and files, directories, and volumes can have their own specific security defined. NTFS can track security in Access Control Lists (ACLs). Each entry in the ACL can specify the access type granted. File encryption programs can also be used to encrypt data stored on the hard disk.
D: This is a hierarchical file system where each file, filesystem and subdirectory has complete granular access control.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 211- 212.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 497:

To secure file and printer shares from external attacks, which of the following ports should you block on the firewall?

A. TCP/UDP ports 137, 138, and 139 only
B. Network File System (NFS) TCP/UDP port 2049 only
C. TCP/UDP ports 137, 138
D. All of the above ports

Answer: D

Explanation:
Attackers can use NFS and SMB/NetBIOS file and printer shares to acquire the necessary information to access the private, internal network. To prevent attackers from accessing file and printer shares, you should block all the above-mentioned TCP/UDP ports on the firewall.
Incorrect answers:
A, B, C: These options present only part of the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 498:

To secure your DNS servers from network footprinting attempts, which of the following is most relevant?

A. Ensure that DNS server software and the operating system software are up to date.
B. Ensure that all information about the network, which gets stored in external DNS servers are kept at a minimum.
C. Ensure that authentication is required before any DNS updates are made.
D. None of the above.

Answer: B

Explanation:
To protect your DNS servers from network footprinting attacks, ensure that all information on the network, which gets stored in external DNS servers are kept at a minimum.
Incorrect answers:
A: To protect your DNS servers from DoS attacks, you need to ensure that DNS server software and the operating system software are up to date with the latest security patches and service packs.
C: To prevent an attacker from inserting a false record in the primary DNS server, you need to ensure that authentication is required before any updates are made.
D: B is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 499:

For hardening DNS servers, one of the methods listed below is FALSE. Choose the incorrect option.

A. The Windows 2000 DNS version implements DNS security. This assists in preventing DNS spoofing, and ensures that client systems access the proper DNS server.
B. You should use virtual private network (VPN) or Secure Shell (SSH) connections to secure information passing to and from the DNS server.
C.
Use a version of DNS that includes the correction for preventing DNS cache poisoning, or alternatively, obtain the relevant security patch to address this issue.
D. You should set up DNS servers so that they only perform zone transfers to specific secondary DNS servers.
E. For the perimeter network, use a separate DNS server. This server should not contain information which you do not want public users to access.

Answer: B

Explanation:
For FTP server activity and communication, is advised to use virtual private network

(VPN) or Secure Shell (SSH) connections. This is mainly due to the FTP protocol being weak in terms of security. For instance, when sending account and password information over the network, FTP sends it in an unencrypted format. This generally makes FTP one of the more frequently used mechanisms by hackers for attacking your internal network.
Incorrect answers:
A, C, D, E: Each one of these options describe a valid strategy to harden DNS servers.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 500:

NNTP is used to enable news clients to connect to NNTP servers. If you do not want persons external to the company to access the NNTP server, which of the following ports should you block on the firewall?

A. TCP/UDP ports 137, 138, and 139
B. NFS TCP/UDP port 2049
C. TCP/UDP port 119
D. TCP port 110
E. None of the above ports

Answer: C

Explanation:
If you do not want the NNTP server hosted on the internal network to be accessed by outside individuals, you should block TCP/UDP port 119 on the firewall.
Incorrect answers:
A: TCP/UDP ports 137, 138, and 139 are used by NetBIOS names and sessions
B: TCP/UDP port 2049 is used by NFS
D: POP3 clients use TCP port 110 to access the e-mail server.
E: C is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 501:

There are three different tiered models that you can choose between to implement and improve database security and system performance. In which tiered model do the database and the application exist on a single serer?

A. One-tier model
B. Two-tier model
C. Three-tier model
D. All of the above

Answer: A

Explanation:
The database and application reside on one system in a one-tier model. The one-tier model is usually used to host a stand-alone database.
Incorrect answers:
B: In a two-tier model, the application being run by the client PC accesses a database hosted on a different server.
C: In a three-tier model, a middle-tier server receives and verifies requests from clients, before passing it to the server on which the database resides. After the request is processed by the database server, the server passes the information back to the middle-tier server, who then passes the data to the client. The middle-tier server provides additional security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 226.

QUESTION 502:

Which of the following attacks is common for file and print servers, e-mail servers, and directory services?

A. Packet sniffing
B. Enumerating resources
C. DoS attacks
D. All of the above

Answer: A

Explanation:
The attack that is a threat to file and print servers, e-mail servers, and directory services, is packet sniffing. With file and print servers, attackers use packet sniffing to interpret the data of printer files and data files as these files are transported over the network. Packet sniffing is also used by attackers to target e-mail servers. E-mail is communicated between internal e-mail servers and e-mail clients. It is also transmitted between the Internet and other networks, and e-mail servers. Because e-mail passed between the e-mail server and e-mail clients are not encrypted by default, their data can be easily intercepted and read. Similarly, information passed over LDAP is not encrypted either. Attackers can use LDAP communications to acquire information about the internal network.
Incorrect answers:

B: This attack is typically aimed at file and print servers. Here, the attacker tries to connect to network resources through unauthenticated connections.
C: Of the three different network components listed in the question, DoS attacks are targeted at e-mail servers. Attackers attempt to send excessive e-mail communications over the network by attempting to get users to run viruses.
D: The correct answer is packet sniffing.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 503:

Blocking TCP/UDP port 119 on the firewall would result in preventing a certain type of public access to the internal network. Choose the correct option.

A. Prevent external users from accessing the private NNTP server.
B. Prevent the DHCP server from accidentally responding to requests from external users.
C. Prevent public users from accessing your internal Web servers.
D. Secures your file and print servers from external attacks.

Answer: A

Explanation:
Blocking TCP/UDP port 119 on the firewall assists in preventing external users from accessing the private NNTP server.
Incorrect answers:
B: If you want to ensure that the DHCP server does not respond to requests from external users, you should block TCP/UDP port 67 and 68 on the firewall.
C: Blocking TCP ports 80 and 443 would prevent public users from accessing your internal Web servers.
D: Blocking TCP/UDP ports 137, 138, and 139 secures your file and print servers from external attacks.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 504:

In which tiered model, used for providing additional database security, do the applications and database reside on different servers?

A. One-tier model
B. Two-tier model
C. Three-tier model
D. Two-tier and three-tier model

Answer: D

Explanation:
In the two-tier and three-tier model, the application being run by the client PC or system accesses a database hosted on a different server.
Incorrect answers:
A: In a one-tier model, the application being run by the client PC and the database being accessed reside on one server.
B: Both a two-tier and three-tier model has the application and the database residing on different servers.
C: Both a two-tier and three-tier model has the application and the database residing on different servers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 226.

QUESTION 505:

Blocking TCP ports 80 and 443 on the firewall would result in preventing a certain type of public access to the internal network. Choose the correct option

A. Prevent external users from accessing the private NNTP server.
B. Prevent the DHCP server from accidentally responding to requests from external users.
C. Prevent public users from accessing your internal Web servers.
D. Assist in securing your file and print servers from external attacks

Answer: C

Explanation:
Blocking TCP ports 80 and 443 would prevent public users from accessing your internal Web servers.
Incorrect answers:
A: Blocking TCP/UDP port 119 on the firewall prevents external users from accessing the private NNTP server.
B: If you want to ensure that the DHCP server does not respond to requests from external users, you should block TCP/UDP port 67 and 68 on the firewall.
D
: Blocking TCP/UDP ports 137, 138, and 139 assist in securing your file and print servers from external attacks.
References:

Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 506:

To harden your operating system, there are a number of strategies that you can use. Choose the one that is not specific for performing operating system or network operating system hardening?

A. Ensure that major and minor service pack revision numbers are the latest for the operating system that you are using.
B. It is recommended that you disable all unnecessary services on the network.
C. Make certain that administrative group membership is limited to only the specific persons that should be administrative group members.
D. Ensure that various static files cannot be requested through a URL.
E. You should rename local guest and administrator accounts.

Answer: D

Explanation:
All the other strategies pertain to operating system hardening. To harden your Web servers, you should ensure that various static files cannot be requested through a URL.
Incorrect answers:
A, B, C, E: Each strategy mentioned in these options pertain to operating system hardening.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 507:

Which of the following tiered models, used for providing additional database security, ensures the highest level of security?

A. One-tier model
B. Two-tier model
C. Three-tier model

Answer: C

Explanation:
In a three-tier model, a middle-tier server receives and verifies requests from clients,

before passing it to the server on which the database resides. After the request is processed by the database server, the server passes the information to the middle-tier server, who then passes the data to the client. The middle-tier server provides additional security.
Incorrect answers:
A: The database and application reside on one system in a one-tier model. The one-tier model is typical for hosting a stand-alone database.
B: In a two-tier model, the application being run by the client PC accesses a database hosted on a different server.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 226.

QUESTION 508:

You can secure your internal network by denying access to your internal Web servers? Which ports should you block at the firewall?

A. TCP/UDP ports 137, 138, and 139
B. TCP port 443
C. TCP/UDP port 119
D. TCP port 80

Answer: B, D

Explanation:
If you want prevent public users from accessing your internal Web servers, you should block TCP port 443 (HTTPS) and TCP port 80 (HTTP).
Incorrect answers:
A: TCP/UDP ports 137, 138, and 139 are used by NetBIOS names and sessions.
C: If you do not want the NNTP server hosted on the internal network to be accessed by outside individuals, you should block TCP/UDP port 119 on the firewall.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 509:

Blocking TCP/UDP port 67 and 68 on the firewall would result in preventing a certain type of public access to the internal network. Choose the correct option

A. Prevent external users from accessing the private NNTP server.
B. Prevent the DHCP server from accidentally responding to requests from external users.

C. Prevent public users from accessing your internal Web servers.
D. Assists in securing your file and print servers from external attacks.

Answer: B

Explanation:
If you want to ensure that the DHCP server does not respond to requests from external users, you should block TCP/UDP port 67 and 68 on the firewall.
Incorrect answers:
A: Blocking TCP/UDP port 119 on the firewall prevents external users from accessing the private NNTP server.
C: Blocking TCP ports 80 and 443 would prevent public users from accessing your internal Web servers.
D: Blocking TCP/UDP ports 137, 138, and 139 secures your file and print servers from external attacks.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 510:

Blocking TCP/UDP ports 20 and 21 on the firewall would result in preventing a certain type of public access to the internal network. Choose the correct option

A. Prevent external users from accessing the private NNTP server.
B. Prevent the DHCP server from accidentally responding to requests from external users.
C. Prevent public users from accessing your internal Web servers.
D. Prevent access to your internal FTP servers.

Answer: D

Explanation:
If you want to ensure that public users cannot access your internal FTP servers, then you should block TCP ports 20 and 21 on the firewall.
Incorrect answers:
A: Blocking TCP/UDP port 119 on the firewall prevents external users from accessing the private NNTP server.
B: If you want to ensure that the DHCP server does not respond to requests from external users, you should block TCP/UDP port 67 and 68 on the firewall.
C: Blocking TCP ports 80 and 443 would prevent public users from accessing your internal Web servers.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press,

Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 511:

Blocking TCP/UDP port 2049 on the firewall would result in preventing a certain type of public access to the internal network. Choose the correct option

A. Prevent external users from accessing the private NNTP server.
B. Prevent the DHCP server from accidentally responding to requests from external users.
C. Prevent public users from accessing your internal Web servers.
D. Prevent external access to your file and printer shares.
E. Prevent access to your internal FTP servers.

Answer: D

Explanation:
If you want to ensure that public users cannot access your internal file and printer shares, then you should block NFS TCP/UDP port 2049 on the firewall.
Incorrect answers:
A: Blocking TCP/UDP port 119 on the firewall prevents external users from accessing the private NNTP server.
D: If you want to ensure that the DHCP server does not respond to requests from external users, you should block TCP/UDP port 67 and 68 on the firewall
C: Blocking TCP ports 80 and 443 would prevent public users from accessing your internal Web servers.
E: Blocking TCP ports 20 and 21 would prevent public users from accessing your internal FTP servers.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 4

QUESTION 512:

From the list, which details the primary purpose of TCP (Transmission Control Protocol) wrappers?

A. To prevent IP (Internet Protocol) spoofing.
B. To control access to certain network services.
C. To encrypt TCP (Transmission Control Protocol) traffic.
D. To sniff TCP (Transmission Control Protocol) traffic for troubleshooting purposes.

Answer: B

Explanation:
TCP wrappers are an additional method of providing security against unwelcome visitors. In a Solaris environment there's a TCP daemon called
inted which responds to TCP/IP connections and initiates the right program to furnish the needs of that request. A TCP wrapper, wraps itself around this daemon with a tcpd program which logs the incoming request first, putting up an optional layer of access control that can allow or deny a request depending on where its from.
Incorrect answers:
A: Wrappers do not prevent IP spoofing.
C: Encryption is not a TCP wrapper's main function.
D: TCP wrappers' main purpose is not to perform sniffing in troubleshooting.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishers, 2004, p. 209

QUESTION 513:

Choose the characteristic that is NOT specific to the Directory Enabled Networking (DEN) standard.

A. DEN is mapped into the directory specified as part of the LDAP (Lightweight Directory Access Protocol).
B. DEN is inferior to SNMP (Simple Network Management Protocol).
C. DEN is an object oriented information model.
D. DEN is an industry standard that specifies how to structure and store information on the users, applications, and data of the network.

Answer: B

Explanation:
LDAP utilizes an object-oriented access model defined by the Directory Enabled Networking (DEN) standard, which is based on the Common Information Model (CIM) standard. Buffer overflow vulnerabilities, Format string vulnerabilities may result in unauthorized access to enact commands on the LDAP server or impair its normal operation, and improperly formatted requests may be used to create an effective denial of service (DoS) attack against the LDAP server, preventing it from responding to normal requests; are the valnerabilities of LDAP. However, it is certainly not inferior to SNMP.
Incorrect answers:
A: Mapping into a directory is part of DEN.
C: It does act as an object oriented information model.
D: This statement is true about directory enabled networking.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 5

QUESTION 514:

You work as the security administrator at Certkiller .com. You are monitoring the Certkiller .com network and immediately notice that TCP ports 25, 110, 143 and 389 are open.
You decide to restrict the number of open ports. You do not want to affect existing functionality and services. You have to take these factors into consideration for Certkiller .com users that work from home offices:
1. Users must be able to connect to the Certkiller .com network from their home offices.
2. Users must be able to send and receive e-mail messages over the Internet.
3. Users must be able to search the directory services database for user e-mail addresses.
4. Users must be able to search the directory services database for digital certificates.
5. Users must be able to use IMAPv.4 (Internet Message Access Protocol version 4) to read e-mail messages.
Currently, the directory services server and e-mail associated services run on a scanned server on the Certkiller .com network.
Which of the following ports can be filtered out to decrease unnecessary exposure?

A. Port 25
B. Port 110
C. Port 143
D. Port 389

Answer: B

Explanation:
Internet Message Access Protocol v4 uses port 143 and TCP for connections. POP3 uses port 110 and TCP for connections and therefore can be filtered out to decrease unnecessary exposure.
Incorrect answers:
A: SMTP makes use of port 25.
C: Port 143 is used for HTTPS.
D: LDAP (SSL) makes use of this port.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 130
http://www.iana.org/assignments/port-numbers

QUESTION 515:

You work as the security administrator at Certkiller .com. You must configure the firewall to allow SNMP traffic.

Which port should you open to allow SNMP traffic?

A. Port 21
B. Port 161
C. Port 53
D. Port 49

Answer: B

Explanation:
SNMP uses UDP port 161
Incorrect answers:
A: Port 21 is used for FTP.
C: DNS client to server lookup uses this port.
D: Port 49 is not used for SNMP traffic, it is used for Login Host Protocol (TACACS).
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 130
http://www.iana.org/assignments/port-numbers

QUESTION 516:

Choose the three elements of the SQL (Structured Query Language) security model.
Choose three answers.

A. Tables
B. Actions
C. Objects
D. Users

Answer: B, C, D

Explanation:
Objects are what the user constructs (ie: tables, columns, views, domains).
Actions are the operations performed on the objects. (ie: select, insert, delete, reference)
Users invoke the actions on the objects.
Incorrect answers:
A: A database is a collection of objects such as tables, views, and stored procedures. In other word, tables are user constructs.
Reference:
Kalen Delaney, Inside Microsoft SQL Server 2000, Microsoft Press, Redmond, 2000, Part 2, Chapter 3

QUESTION 517:

You work as the security administrator at Certkiller .com. You want to associates

users and groups to specific rights to use, read, write, modify, or execute objects on the networking system.
What should you use to accomplish your task?

A. Use a public key ring.
B. Use an ACL (Access Control List).
C. Use a digital signature.
D. Use a CRL (Certificate Revocation Lists).

Answer: B

Explanation:
An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Microsoft Windows NT/2000, Novell's NetWare, Digital's OpenVMS, and Unix-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.
Incorrect answers:
A: This is a two-key encryption system wherein messages are encrypted with a private key and decrypted with a public key.
C: This signature validates the integrity of the message and the sender.
D: A CRL is a list of digital certificate revocations that must be regularly downloaded to stay current.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 216
www.whatis.com

QUESTION 518:

You work as the security administrator at Certkiller .com. You want to implement a solution that will limit network exposure and vulnerability to port scan attacks.
What measure should you use?
Disable the ability to remotely scan the registry.
Ensure that all processes running for possible future use.
Close programs and processes that use TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ports.
Uninstall or disable programs or processes not required on the server.

Answer: D

Explanation:

Hackers perform port scans to find out which of the 65,535 ports are being used in hope of finding an application with a vulnerability. By uninstalling and disabling any program or processes that aren't really necessary, one greatly reduces the likelihood of an attack.
Incorrect answers:
A, B and C: Disabling all the unnecessary programs and processes is the best way of safeguarding yourself against vulnerabilities that can be exploited via port scans.
Reference:
Kirk Hausman, Diane Barrett, Martin Weiss, Security+ Exam Cram 2 (Exam SYO-101), Que Publishing, Indianapolis, 2003, Chapter 7
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 67

QUESTION 519:

You work as the security administrator at Certkiller .com. You want to implement a solution that will prevent unauthorized users from sending malicious e-mails from non-existent domains.
How will you accomplish the task?

A. On the e-mail server, enable DNS (Domain Name Service) reverse lookup.
B. On the e-mail server, enable DNS (Domain Name Service) forward lookup.
C. On the DNS (Domain Name Service) server, enable DNS (Domain Name Service) recursive queries.
D. On the DNS (Domain Name Service) server, enable DNS (Domain Name Service) reoccurring queries.

Answer: A

Explanation:
DNS reverse lookup takes a numbered IP address and converts it to a domain name. This is a very easy process, and there are free reverse DNS lookup services online. With reverse DNS a spammer won't be able to hide.
Incorrect answers:
B: In forward lookup zones, DNS servers map FQDNs to IP addresses. Forward lookup zones thus answer queries to resolve FQDNs to IP addresses. This will not prevent malicious users sending you e-mail from non-existent domains.
C
: As DNS servers make recursive queries on behalf of clients, they temporarily cache resource records. These cached records contain information acquired in the process of answering queries on behalf of a client. Later, when other clients place new queries that request information matching cached resource records, the DNS server can use the cached information to answer these queries. This is thus not a preventative measure.
D: There are no reoccurring queries on a DNS server.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION 520:

From the list of options, which defines what the purpose of implementing SSL (Secure Sockets Layer) is?
SSL secures communications with file and print servers.
SSL secures communications with RADIUS (Remote Authentication Dial-in User Service) servers.
SSL secures communications with AAA (Authentication, Authorization, and Administration) servers.
SSL secures communications with web servers

Answer: D

Explanation:
SSL is used to secure a connection between a web user and a web server for transactions like: banking, securities, and ecommerce.
Incorrect answers:
A, B and C: SSL is used for secure communications between a web browser and web servers not for file and print servers, RADIUS or AAA.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishers, 2004, p. 126

QUESTION 521:

From the list of attacks types, which is an attack frequently targeted at web servers?

A. Birthday attack.
B. Buffer overflow attack.
C. Spam attack.
D. Brute force attack.

Answer: B

Explanation:
Buffer overflow occur when an application receives more data that it is programmed to accept. This situation can cause an application to terminate. The termination may leave the system sending the data with temporary access to privileged levels in the attacked system.
Incorrect answers:
A: A birthday attack is a type of brute force attack and does not so common on your web server per se.
C: E-Mail servers are usually susceptible to spam attacks.
D: Brute force attacks work by trying to randomly guess a password repeatedly against a

known account ID. This is not a common web server attack.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishers, 2004, pp. 129,135

QUESTION 522:

You work as the security administrator at Certkiller .com. You plan to deploy a DNS (Domain Name) server on the Certkiller .com network. You must secure the DNS server by preventing a specific function from occurring between the DNS server and all untrusted nodes.
What function is it?

A. Prevent name resolutions.
B. Prevent reverse ARP (Address Resolution Protocol) requests.
C. Prevent system name resolutions.
D. Prevent zone transfers.

Answer: D

Explanation:
Users who can start zone transfers from your server can list all of the records in your zones.
Incorrect answers:
A: Name resolution is a function of DNS, you cannot prevent it.
B: IP address to MAC address resolution occurs through ARP Request and Reply messages. The reverse, MAC to IP resolution, uses Reverse ARP (RARP) Requests and Replies.
C: Name resolution is a function of DNS, you cannot prevent it.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION 523:

You work as a security administrator at Certkiller .com. You deploy the DNS (Domain Name Service) service on the Certkiller .com, and now need to secure the DNS server.
You want to limit the vulnerability of the primary DNS server by securing it from network intruders and DoS (Denial of Service) attacks.
How will you accomplish the task?

A. On the primary DNS server, disable the DNS cache function.
B. On the primary DNS server, ensure that expect for DNS, no application services are enabled.
C. On the primary DNS server, disable the DNS reverse lookup function.

D. Only allow encrypted zone transfers to occur to a secondary DNS server.

Answer: B

Explanation:
If a DNS server was only configured to handle DNS and nothing else, the only type of packets that could take up any resources will be domain name requests. Overwhelming an entire server's services with domain name requests alone is an engineering feat.
Incorrect answers:
A: This will cause the DNS server to be obsolete and as such is not an option.
C: This will interfere with the functioning of the DNS server.
D: This is not how you secure your DNS server against DoS attacks and hackers.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 8, Lesson 2

QUESTION 524:

From the options, which describes the best way to harden an application developed by a Certkiller .com application developer?
You should obtain and use an industry recommended hardening tool.
You should that security is prioritized throughout the entire development process.
You should attempt to attack the application to isolate vulnerabilities. Patches should be developed to fix all identified vulnerabilities.
You should that your auditing system is adequately sophisticated adequately detect and log all possible intrusions.

Answer: B

Explanation:
The Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex Publishers, Alameda, 2004, book discusses application hardening and refers this to the web, FTP, and E-mail servers. The question refers to programming new applications. Although I could not find any information in the book about programming hardening, I would say that answer B is the best choice out of the four answers.

QUESTION 525:

To which of the following Hashing Algorithms does the statement that it was designed to ensure the integrity of a message apply?

A. SHA.
B. MDA.
C. MD5.
D. None of the following.

Answer: A

Explanation:
The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. The SHA algorithm produces a 160-bit hash value. SHA has been updated; the new standard is SHA-1.
Incorrect answers:
B: The Message Digest Algorithm (MDA) is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD.
C: MD5 is the newest version of the algorithm. MD5 produces a 128-bit hash, but the algorithm is more complex than its predecessors and it offers greater security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 526:

To which of the following Hashing Algorithms does the statement that it uses a one-way hash apply?

A. SHA.
B. MDA.
C. MD5.
D. None of the following.

Answer: B

Explanation:
The Message Digest Algorithm (MDA) is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD.
Incorrect answers:
A: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. The SHA algorithm produces a 160-bit hash value. SHA has been updated; the new standard is SHA-1.
C: MD5 is the newest version of the algorithm. MD5 produces a 128-bit hash, but the algorithm is more complex than its predecessors and it offers greater security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 527:

To which of the following Hashing Algorithms does the statement that the algorithm is more complex than its predecessors and it offers greater security apply?

A. SHA.
B. MDA.
C. MD5.
D. None of the following.

Answer: C

Explanation:
MD5 is the newest version of the algorithm. MD5 produces a 128-bit hash, but the algorithm is more complex than its predecessors and it offers greater security.
Incorrect answers:
A: The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. The SHA algorithm produces a 160-bit hash value. SHA has been updated; the new standard is SHA-1.
B: The Message Digest Algorithm (MDA) is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 528:

Which of the following definitions apply to SHA?

A. It was designed to ensure the integrity of a message.
B. It uses a one-way hash.
C. The algorithm is more complex than its predecessors and it offers greater security.
D. The primary standard used in government and industry.

Answer: A

Explanation:
The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. The SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. The SHA algorithm produces a 160-bit hash value. SHA has been updated; the new standard is SHA-1.
Incorrect answers:
B: This refers to MDA.
C: This refers to MD5.
D: This does not form part of hashing.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 529:

Which of the following definitions apply to MDA?

A. It was designed to ensure the integrity of a message.
B. It uses a one-way hash.
C. The algorithm is more complex than its predecessors and it offers greater security.
D. The primary standard used in government and industry.

Answer: B

Explanation:
The Message Digest Algorithm (MDA) is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD.
Incorrect answers:
A: This refers to SHA.
C: This refers to MD5.
D: This does not form part of hashing.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 530:

Which of the following definitions apply to MDA?

A. It was designed to ensure the integrity of a message.
B. It uses a one-way hash.
C. The algorithm is more complex than its predecessors and it offers greater security.
D. The primary standard used in government and industry.

Answer: C

Explanation:
MD5 is the newest version of the algorithm. MD5 produces a 128-bit hash, but the algorithm is more complex than its predecessors and it offers greater security.
Incorrect answers:
A: This refers to SHA.
B: This refers to MDA.
D: This does not form part of hashing.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 531:

To which of the following Symmetric Algorithms does the statement that it the primary standard used in government and industry apply?

A. DES.
B. AES.
C. 3DES.
D. CAST.

Answer: A

Explanation:
The Data Encryption Standard (DES) has been used since the mid-1970s. This standard was the primary standard used in government and industry. It is a strong and efficient algorithm. Strong refers to the fact that it is hard to break. DES has several modes that offer security and integrity.
Incorrect answers:
B: Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemon and Vincent Rijmen. AES is now the current product used by U.S. governmental agencies. AES supports key sizes of 128, 192, and 256 bits.
C: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems. 3DES is more secure than DES.
D: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 532:

To which of the following Symmetric Algorithms does the statement that it supports key sizes of 128, 192, and 256 bits apply?

A. DES.
B. AES.
C. 3DES.
D. CAST.

Answer: B

Explanation:
Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemon and Vincent Rijmen. AES is now the current product used by U.S. governmental agencies. AES supports key sizes of 128, 192, and 256 bits.
Incorrect answers:
A: The Data Encryption Standard (DES) has been used since the mid-1970s. This standard was the primary standard used in government and industry. It is a strong and efficient algorithm. Strong refers to the fact that it is hard to break. DES has several modes that offer security and integrity.
C: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems. 3DES is more secure than DES.
D: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 533:

To which of the following Symmetric Algorithms does the statement that it is considerably harder to break than many other systems apply?

A. DES.
B. AES.
C. 3DES.
D. CAST.

Answer: C

Explanation:
Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems. 3DES is more secure than DES.
Incorrect answers:
A: The Data Encryption Standard (DES) has been used since the mid-1970s. This standard was the primary standard used in government and industry. It is a strong and efficient algorithm. Strong refers to the fact that it is hard to break. DES has several modes that offer security and integrity.
B: Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemon and Vincent Rijmen. AES is now the current product used by U.S. governmental agencies. AES supports key sizes of 128, 192, and 256 bits.

D: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.

QUESTION 534:

To which of the following Symmetric Algorithms does the statement that it is very fast and efficient apply?

A. DES.
B. AES.
C. 3DES.
D. CAST.

Answer: D

Explanation:
CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
Incorrect answers:
A:
The Data Encryption Standard (DES) has been used since the mid-1970s. This standard was the primary standard used in government and industry. It is a strong and efficient algorithm. Strong refers to the fact that it is hard to break. DES has several modes that offer security and integrity.
B: Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemon and Vincent Rijmen. AES is now the current product used by U.S. governmental agencies. AES supports key sizes of 128, 192, and 256 bits.
C: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems. 3DES is more secure than DES.

QUESTION 535:

Which of the following definitions apply to DES?

A. It the primary standard used in government and industry.
B. It supports key sizes of 128, 192, and 256 bits.
C. It is considerably harder to break than many other systems.
D. It is very fast and efficient.

Answer: A

Explanation:

The Data Encryption Standard (DES) has been used since the mid-1970s. This standard was the primary standard used in government and industry. It is a strong and efficient algorithm. Strong refers to the fact that it is hard to break. DES has several modes that offer security and integrity.
Incorrect answers:
B: This refers to AES.
C: This refers to 3DES.
D: This refers to CAST.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 536:

Which of the following definitions apply to AES?

A. It the primary standard used in government and industry.
B. It supports key sizes of 128, 192, and 256 bits.
C. It is considerably harder to break than many other systems.
D. It is very fast and efficient.

Answer: B

Explanation:
Advanced Encryption Standard (AES) has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemon and Vincent Rijmen. AES is now the current product used by U.S. governmental agencies. AES supports key sizes of 128, 192, and 256 bits.
Incorrect answers:
A: This refers to DES.
C: This refers to 3DES.
D: This refers to CAST.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 537:

Which of the following definitions apply to 3DES?

A. It the primary standard used in government and industry.
B. It supports key sizes of 128, 192, and 256 bits.
C. It is considerably harder to break than many other systems.
D. It is very fast and efficient.

Answer: C

Explanation:
Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems. 3DES is more secure than DES.
Incorrect answers:
A: This refers to DES.
B: This refers to AES.
D: This refers to CAST.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 538:

Which of the following definitions apply to CAST?

A. It the primary standard used in government and industry.
B. It supports key sizes of 128, 192, and 256 bits.
C. It is considerably harder to break than many other systems.
D. It is very fast and efficient.

Answer: D

Explanation:
CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
Incorrect answers:
A: This refers to DES.
B: This refers to AES.
C: This refers to 3DES.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 539:

To which of the following Symmetric Algorithms does the statement that it uses a key size of up to 2,048 bits. It is considered to be a strong system apply?

A. RC.
B. Blowfish.
C. IDEA.
D. CAST.

Answer: A

Explanation:
RC is an encryption family produced by RSA laboratories. RC stands for Ron's Code or Rivest's Cipher. Ron Rivest is the author of this algorithm. The current levels are RC5 and RC6. RC5 uses a key size of up to 2,048 bits. It is considered to be a strong system.
Incorrect answers:
B: Blowfish is an encryption system produced by Counterpane systems. The original author was Bruce Schneier. His next generation product Twofish was a finalist in the AES selection process. AES supports key lengths of up to 448 bits.
C: International Data Encryption Algorithm (IDEA) is an algorithm that uses a 128-bit key. This product is similar in speed and capability to DES, but it is more secure. IDEA is used in PGP. Pretty Good Privacy (PGP)
is a public domain encryption system used by many for e-mail. IDEA was developed by a Swiss consortium. Currently, ASCOM AG holds the right to market IDEA.
D: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 540:

To which of the following Symmetric Algorithms does the statement that it supports key lengths of up to 448 bits apply?

A. RC.
B. Blowfish.
C. IDEA.
D. CAST.

Answer: B

Explanation:
Blowfish is an encryption system produced by Counterpane systems. The original author was Bruce Schneier. His next generation product Twofish was a finalist in the AES selection process. AES supports key lengths of up to 448 bits.
Incorrect answers:
A: RC is an encryption family produced by RSA laboratories. RC stands for Ron's Code or Rivest's Cipher. Ron Rivest is the author of this algorithm. The current levels are RC5 and RC6. RC5 uses a key size of up to 2,048 bits. It is considered to be a strong system.
C: International Data Encryption Algorithm (IDEA) is an algorithm that uses a 128-bit key. This product is similar in speed and capability to DES, but it is more secure. IDEA is used in PGP. Pretty Good Privacy (PGP)
is a public domain encryption system used by many for e-mail. IDEA was developed by a

Swiss consortium. Currently, ASCOM AG holds the right to market IDEA.
D: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 541:

To which of the following Symmetric Algorithms does the statement that it is similar in speed and capability to DES, but it is more secure apply?

A. RC.
B. Blowfish.
C. IDEA.
D. CAST.

Answer: C

Explanation:
International Data Encryption Algorithm (IDEA) is an algorithm that uses a 128-bit key. This product is similar in speed and capability to DES, but it is more secure. IDEA is used in PGP. Pretty Good Privacy (PGP)
is a public domain encryption system used by many for e-mail. IDEA was developed by a Swiss consortium. Currently, ASCOM AG holds the right to market IDEA.
Incorrect answers:
A: RC is an encryption family produced by RSA laboratories. RC stands for Ron's Code or Rivest's Cipher. Ron Rivest is the author of this algorithm. The current levels are RC5 and RC6. RC5 uses a key size of up to 2,048 bits. It is considered to be a strong system.
B: Blowfish is an encryption system produced by Counterpane systems. The original author was Bruce Schneier. His next generation product Twofish was a finalist in the AES selection process. AES supports key lengths of up to 448 bits.
D: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares-hence the name. CAST is used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it is very fast and efficient.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 542:

Which of the following definitions apply to RC?

A. It uses a key size of up to 2,048 bits. It is considered to be a strong system.
B. It supports key lengths of up to 448 bits.

C. It is similar in speed and capability to DES, but it is more secure.
D. It is very fast and efficient.

Answer: A

Explanation:
RC is an encryption family produced by RSA laboratories. RC stands for Ron's Code or Rivest's Cipher. Ron Rivest is the author of this algorithm. The current levels are RC5 and RC6. RC5 uses a key size of up to 2,048 bits. It is considered to be a strong system.
Incorrect answers:
B: This refers to Blowfish.
C: This refers to IDEA.
D: This refers to CAST.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 543:

Which of the following definitions apply to Blowfish?

A. It uses a key size of up to 2,048 bits. It is considered to be a strong system.
B. It supports key lengths of up to 448 bits.
C. It is similar in speed and capability to DES, but it is more secure.
D. It is very fast and efficient.

Answer: B

Explanation:
Blowfish is an encryption system produced by Counterpane systems. The original author was Bruce Schneier. His next generation product Twofish was a finalist in the AES selection process. AES supports key lengths of up to 448 bits.
Incorrect answers:
A: This refers to RC.
C: This refers to IDEA.
D: This refers to CAST.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 544:

Which of the following definitions apply to IDEA?

A. It uses a key size of up to 2,048 bits. It is considered to be a strong system.
B. It supports key lengths of up to 448 bits.

C. It is similar in speed and capability to DES, but it is more secure.
D. It is very fast and efficient.

Answer: C

Explanation:
International Data Encryption Algorithm (IDEA) is an algorithm that uses a 128-bit key. This product is similar in speed and capability to DES, but it is more secure. IDEA is used in PGP. Pretty Good Privacy (PGP)
is a public domain encryption system used by many for e-mail. IDEA was developed by a Swiss consortium. Currently, ASCOM AG holds the right to market IDEA.
Incorrect answers:
A: This refers to RC.
B: This refers to Blowfish.
D: This refers to CAST.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 545:

To which of the following Asymmetric Algorithms does the statement that it is an early public key encryption system that uses large integer numbers as the basis of the process apply?

A. RSA.
B. Diffie-Hellman.
C. ECC.
D. El Gamal.

Answer: A

Explanation:
RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is a widely implemented, and it has become a de facto standard. RSA works for both encryption and digital signatures. RSA is used in many environments, including SSL. The RSA algorithm is an early public key encryption system that uses large integer numbers as the basis of the process.
Incorrect answers:
B: The Diffie-Hellman key exchange was conceptualized by Dr. W. Diffie and Dr. M. E. Hellman. They are considered the founders of the public/private key concept. This algorithm is used primarily to send keys across public networks. The process is not used to encrypt or decrypt messages; it used merely for the transmission of keys in a secure manner. The Diffie-Hellman process is one of the first implementations of a public/private key system. Their original work conceptualized splitting the key into two parts.

C:
The Elliptic Curve Cryptosystem (ECC) provides similar functionality to RS
A. ECC is
being implemented in smaller, less intelligent devices such as cell phones and wireless devices. ECC is smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. This process is less mathematically intensive than processes such as RSA.
D: El Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based on calculating logarithms. The process used is similar to the Diffie-Hellman key exchange and is based on the characteristics of logarithmic numbers and calculations. The El Gamal algorithm is also called DSA, and it was first published in 1985.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 324.

QUESTION 546:

To which of the following Asymmetric Algorithms does the statement that it is one of the first implementations of a public/private key system apply?

A. RSA.
B. Diffie-Hellman.
C. ECC.
D. El Gamal.

Answer: B

Explanation:
The Diffie-Hellman key exchange was conceptualized by Dr. W. Diffie and Dr. M. E. Hellman. They are considered the founders of the public/private key concept. This algorithm is used primarily to send keys across public networks. The process is not used to encrypt or decrypt messages; it used merely for the transmission of keys in a secure manner. The Diffie-Hellman process is one of the first implementations of a public/private key system. Their original work conceptualized splitting the key into two parts.
Incorrect answers:
A:
RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is a widely implemented, and it has become a de facto standard. RSA works for both encryption and digital signatures. RSA is used in many environments, including SSL. The RSA algorithm is an early public key encryption system that uses large integer numbers as the basis of the process.
C: The Elliptic Curve Cryptosystem (ECC) provides similar functionality to RS
A. ECC
is being implemented in smaller, less intelligent devices such as cell phones and wireless

devices. ECC is smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. This process is less mathematically intensive than processes such as RSA.
D: El Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based on calculating logarithms. The process used is similar to the Diffie-Hellman key exchange and is based on the characteristics of logarithmic numbers and calculations. The El Gamal algorithm is also called DSA, and it was first published in 1985.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 324.

QUESTION 547:

To which of the following Asymmetric Algorithms does the statement that it is based on encryption systems are based on the idea of using points on a curve to define the public/private key pair apply?

A. RSA.
B. Diffie-Hellman.
C. ECC.
D. El Gamal.

Answer: C

Explanation:
The Elliptic Curve Cryptosystem (ECC) provides similar functionality to RS
A. ECC is
being implemented in smaller, less intelligent devices such as cell phones and wireless devices. ECC is smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. This process is less mathematically intensive than processes such as RSA.
Incorrect answers:
A: RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is a widely implemented, and it has become a de facto standard. RSA works for both encryption and digital signatures. RSA is used in many environments, including SSL. The RSA algorithm is an early public key encryption system that uses large integer numbers as the basis of the process.
B: The Diffie-Hellman. key exchange was conceptualized by Dr. W. Diffie and Dr. M. E. Hellman. They are considered the founders of the public/private key concept. This algorithm is used primarily to send keys across public networks. The process is not used to encrypt or decrypt messages; it used merely for the transmission of keys in a secure manner. The Diffie-Hellman process is one of the first implementations of a public/private key system. Their original work conceptualized splitting the key into two parts.
D: El Gamal is an algorithm used for transmitting digital signatures and key exchanges.

The method is based on calculating logarithms. The process used is similar to the Diffie-Hellman key exchange and is based on the characteristics of logarithmic numbers and calculations. The El Gamal algorithm is also called DSA, and it was first published in 1985.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 324.

QUESTION 548:

To which of the following Asymmetric Algorithms does the statement that it is based on the key exchange and is based on the characteristics of logarithmic numbers and calculations apply?

A. RSA.
B. Diffie-Hellman.
C. ECC.
D. El Gamal.

Answer: D

Explanation:
El Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based on calculating logarithms. The process used is similar to the Diffie-Hellman key exchange and is based on the characteristics of logarithmic numbers and calculations. The El Gamal algorithm is also called DSA, and it was first published in 1985.
Incorrect answers:
A: RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is a widely implemented, and it has become a de facto standard. RSA works for both encryption and digital signatures. RSA is used in many environments, including SSL. The RSA algorithm is an early public key encryption system that uses large integer numbers as the basis of the process.
B: The Diffie-Hellman key exchange was conceptualized by Dr. W. Diffie and Dr. M. E. Hellman. They are considered the founders of the public/private key concept. This algorithm is used primarily to send keys across public networks. The process is not used to encrypt or decrypt messages; it used merely for the transmission of keys in a secure manner. The Diffie-Hellman process is one of the first implementations of a public/private key system. Their original work conceptualized splitting the key into two parts.
C: The Elliptic. Curve Cryptosystem (ECC) provides similar functionality to RS
A. ECC
is being implemented in smaller, less intelligent devices such as cell phones and wireless devices. ECC is smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. This process is less mathematically intensive than processes such as RSA.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 324.

QUESTION 549:

Which of the following definitions apply to RSA?

A. It is an early public key encryption system that uses large integer numbers as the basis of the process.
B. It is one of the first implementations of a public/private key system.
C. It is based on encryption systems are based on the idea of using points on a curve to define the public/private key pair.
D. It is based on the key exchange and is based on the characteristics of logarithmic numbers and calculations.

Answer: A

Explanation:
RSA is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman. RSA is a widely implemented, and it has become a de facto standard. RSA works for both encryption and digital signatures. RSA is used in many environments, including SSL.
The RSA algorithm is an early public key encryption system that uses large integer numbers as the basis of the process.
Incorrect answers:
B: This refers to Diffie-Hellman.
C: This refers to ECC.
D: This refers to El Gamal.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 550:

Which of the following definitions apply to Diffie-Hellman?

A. It is an early public key encryption system that uses large integer numbers as the basis of the process.
B. It is one of the first implementations of a public/private key system.
C. It is based on encryption systems are based on the idea of using points on a curve to define the public/private key pair.
D. It is based on the key exchange and is based on the characteristics of logarithmic numbers and calculations.

Answer: B

Explanation:
The Diffie-Hellman key exchange was conceptualized by Dr. W. Diffie and Dr. M. E. Hellman. They are considered the founders of the public/private key concept. This algorithm is used primarily to send keys across public networks. The process is not used to encrypt or decrypt messages; it used merely for the transmission of keys in a secure manner. The Diffie-Hellman process is one of the first implementations of a public/private key system. Their original work conceptualized splitting the key into two parts.
Incorrect answers:
A: This refers to RSA.
C: This refers to ECC.
D: This refers to El Gamal.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 551:

Which of the following definitions apply to ECC?

A. It is an early public key encryption system that uses large integer numbers as the basis of the process.
B. It is one of the first implementations of a public/private key system.
C. It is based on encryption systems are based on the idea of using points on a curve to define the public/private key pair.
D. It is based on the key exchange and is based on the characteristics of logarithmic numbers and calculations.

Answer: C

Explanation:
The Elliptic Curve Cryptosystem (ECC) provides similar functionality to RS
A. ECC is
being implemented in smaller, less intelligent devices such as cell phones and wireless devices. ECC is smaller than RSA and requires less computing power. ECC encryption systems are based on the idea of using points on a curve to define the public/private key pair. This process is less mathematically intensive than processes such as RSA.
Incorrect answers:
A: This refers to RSA.
B: This refers to Diffie-Hellman.
D: This refers to El Gamal.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 552:

Which of the following definitions apply to El Gamal?

A. It is an early public key encryption system that uses large integer numbers as the basis of the process.
B. It is one of the first implementations of a public/private key system.
C. It is based on encryption systems are based on the idea of using points on a curve to define the public/private key pair.
D. It is based on the key exchange and is based on the characteristics of logarithmic numbers and calculations.

Answer: D

Explanation:
El Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based on calculating logarithms. The process used is similar to the Diffie-Hellman key exchange and is based on the characteristics of logarithmic numbers and calculations. The El Gamal algorithm is also called DSA, and it was first published in 1985.
Incorrect answers:
A: This refers to RSA.
B: This refers to Diffie-Hellman.
C: This refers to ECC.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 319-320

QUESTION 553:

You work as the security administrator at Certkiller .com. You want to protect passwords stored on the authentication server.
Which would be the best method to use?

A. Use clear text to store the passwords.
B. Use a hashing algorithm on the passwords.
C. Use asymmetric keys to encrypt the passwords
D. Use a public key to encrypt the passwords.

Answer: B

Explanation:
This seems to be the best choice out of the four answers. By hashing the passwords, they will be encrypted.
Incorrect answers:
A: Storing any password in clear text is foolhardy.

C, D: These methods do not represent the best ways to protect passwords that are stored on the authentication server.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 554:

On the topic of hashing and hash encryption, choose the TRUE statement.

A. Hashing uses 32 bits.
B. Hashing uses 64 bits.
C. Hashing uses 128 bits.
D. Hashing uses 256 bits.

Answer: C

Explanation:
Hashing produces a 128 bit message digest (hash), very fast, appropriate for medium security usage, e.g. MD4 and MD5. Only SHA-1, also a hash encryption produces a 160 bit message digest (hash), standard for the U.S. government, but slower than MD5.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 287-292
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 555:

Block Cipher provides a specific type of encryption. What is it?

A. Symmetric encryption.
B. Asymmetric encryption.
C. Both symmetric and asymmetric encryption.
D. None of the above.

Answer: A

Explanation:
There are two main types of symmetric ciphers: block ciphers and stream ciphers.
Incorrect answers:
B: Block cipher does not provide asymmetric encryption.
C: Only symmetric encryption is provided by Block cipher, not both.
C: Symmetric encryption is provided by Block cipher.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 556:

Which option correctly specifies what digital signatures can be used?

A. For encryption.
B. To authenticate asymmetric keys.
C. For symmetric key encryption.
D. For public key decryption.

Answer: B

Explanation:
Digital signatures are used to authenticate asymmetric keys.
Incorrect answers:
A: You do not necessary have to make use of digital signatures for encryption.
C: Symmetric key encryption does not require digital signatures.
D: Digital signatures are not used for Public key encryption.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 557:

When encrypting files, which option defines the purpose of using asymmetric algorithms?

A. For symmetric keys encryption.
B. For file contents encryption.
C. For certificates encryption.
D. For hash results encryption.

Answer: A

Explanation:
The asymmetric algorithms are used to encrypt two different keys; a public key and a private key.
Incorrect answers:
B: It is not the file contents that are encrypted by the asymmetric algorithm.

C: Certificates does not get encrypted in the asymmetric algorithm file encryption process.
D: Hash results are not encrypted in the file encryption process of asymmetric algorithms.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 558:

Non-repudiation is based on a specific key infrastructure system. What is it?

A. Symmetric systems.
B. Distributed trust.
C. Asymmetric systems.
D. User-centric systems.

Answer: C

Explanation:
Non-repudiation is unique to asymmetric systems, because the private key is exclusive to one party only.
Incorrect answers:
A: Symmetric systems are not non-repudiation based.
B: A distributed trust is not non-repudiation.
D: User-centric systems are not non-repudiation based.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Kirk Hausman, Diane Barrett, Martin Weiss, and Ed Tittel, Security+ Certification Exam Cram 2, Indianapolis, Que, 2003, pp. 182-183

QUESTION 559:

Choose the two symmetric-key algorithms used for encryption. Choose two that apply.

A. Stream cipher
B. Block cipher
C. Public keys
D. Secret keys

Answer: A, B

Explanation:
Symmetric key encryption comes in two categories:
* block cipher (encrypt a number of bits as a single unit)
* stream cipher (encrypts single bits of plain text one bit at a time)
Incorrect answers:
C: Public keys are used with asymmetric encryption algorithms.
D: Secret or Private keys are used in asymmetric encryption algorithms.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 560:

What type of encryption algorithm is Advanced Encryption Standard (AES) an example of?

A. WTLS
B. Symmetric
C. Multifactor
D. Asymmetric

Answer: B

Explanation:
Here are some of the common standard that use symmetric algorithm.
DES, AES has replaced DES as the current standard, and it uses the Rijindael algorithm, 3DES, CAST, RC, Blowfish and IDEA
Incorrect answers:
A: Wireless Transport Layer Security (WTLS) is the security layer of the Windows Application Protocol
C: When two or more access methods are included as part of the authentication process, you're implementing a multi-factor system. A system that uses smart cards and passwords is referred to as a two-factor authentication system.
D: Four popular asymmetric systems are in use today are RSA, Diffie-hellman, ECC and El Gamal
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 561:

You work as the security administrator at Certkiller .com. You want to use symmetric-key encryption to encrypt and decrypt data.
What number of keys do you need?

A. More than 3 keys
B. 2 keys
C. 1 key
D. No keys

Answer: C

Explanation:
Symmetrical Keys present a difficult challenge to both key management and security perspective. The loss or compromise of a symmetrical key compromises the entire system. Single key systems are entirely dependant on the privacy of the key. This key requires special handling and security. Make sure that symmetrical keys are never divulged. Symmetrical keys should be transmitted using secure out-of-band methods.
Incorrect answers:
A: You only need one key with symmetric encryption.
B: Two keys are used in asymmetric encryption.
D: At least a key is necessary to encrypt and decrypt.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 562:

On the topic of asymmetric cryptography, which statement is TRUE?

A. Authentication and encryption occurs without the exchange of private keys.
B. The fastest algorithm available is used to encrypt the secret key.
C. Each party has to be authenticated before encryption can occur.
D. Encryption is limited to a session key.

Answer: A

Explanation:
Asymmetric algorithm uses two keys to encrypt and decrypt data. These keys are referred to as the public and private key. The public key can be used by the sender to encrypt a message, and the private key can be used by the sender to encrypt a message, and the private key can be used by the receiver to decrypt the message.
Incorrect answers:

B: This is not a necessarily true with asymmetric cryptography. Any of the asymmetric algorithms can be used.
C: Asymmetric cryptography provides a method to validate an individual.
D: It is not limited to a session key.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1

QUESTION 563:

Cryptography is used to meet a specific security requirement within the digital signature procedure. What is it?

A. Confidentiality
B. Access control
C. Data integrity
D. Authentication

Answer: D

Explanation:
Authentication requires a user to provide some proof or credential that represents something they know, something they have, or something they are before allowing access to your company's resources.
Incorrect answers:
A: Because there is a public key and a private key, the public key can be provided to anyone that you want to send you encrypted information, but only you can decrypt that information. This helps ensure data confidentiality.
B
: Access Control is the means of giving or restricting user access to network resources. This is usually accomplished through the use of an ACL (Access Control List).
C: Data integrity refers to the level of confidence that data won't be jeopardized and will be kept secret. A digital signature validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress Publishing, 2002, p 513

QUESTION 564:

Choose the element encrypted by an asymmetric algorithm when a user digitally signs a document.

A. Secret passkeys.
B. File contents.
C. Certificates.
D. Hash results.

Answer: D

Explanation:
The digital signature is derived from a hash process known only by the originator. A digital signature validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
Incorrect answers:
A: Secret pass keys are not encrypted when using digital signatures in an asymmetric algorithm.
B: File content is not encrypted by an asymmetric algorithm when digital signatures are used.
C: The document is digitally signed and not the certificates.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 2925-298

QUESTION 565:

On the topic of symmetric cryptography, which component or process represents its main disadvantage?

A. Speed
B. Key distribution process
C. Weak algorithms
D. Memory management process

Answer: B

Explanation:
In symmetric encryption the message can be encrypted and decrypted using the same key.
Incorrect answers:
A: The algorithms used with symmetric encryption are relatively fast, so they impact

system performance less and are good for encrypting large amounts of data (for instance, data on a hard disk or data being transmitted across a remote access link).
C Symmetric algorithms are difficult to decipher without the correct algorithm; therefore they are not easy to break. Well-tested symmetric algorithms such as 3DES and AES are nearly impossible to decipher without the correct key.
D: Memory management does not fall into the disadvantages of symmetric cryptography category.
Reference:
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 3, Lesson 1
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 292-293

QUESTION 566:

File encryption using symmetric cryptography can be used to meet a specific security requirement. What is it?

A. Confidentiality
B. Access control
C. Data integrity
D. Authentication

Answer: A

Explanation:
"The first goal of cryptography is confidentiality". Since file encryption using symmetric cryptography is a form of cryptography, it would make sense it would meet the confidentiality requirement.
Incorrect answers:
B: Access Control is the means of giving or restricting user access to network resources. This is usually accomplished through the use of an ACL (Access Control List).
C: Data integrity refers to the level of confidence that data won't be jeopardized and will be kept secret. A digital signature validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
D: Authentication requires a user to provide some proof or credential that represents something they know, something they have, or something they are before allowing access to your company's resources.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress Publishing, 2002, p 513

QUESTION 567:

Choose the encryption method that works on the basis of the sender and receiver using different keys for encryption and decryption.

A. Symmetric encryption
B. Blowfish
C. Skipjack
D. Asymmetric encryption

Answer: D

Explanation: Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.
Incorrect Answers
A: In symmetric encryption the message can be encrypted and decrypted using the same key.
B: Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA.
C: Skipjack is the encryption algorithm contained in the Clipper chip, and was designed by the NSA.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 292-293

QUESTION 568:

On the topic of symmetric algorithm, choose the statement that specifically defines one of its attributes.

A. When compared to other cryptographic schemes, symmetric algorithms perform a fast transformation of data.
B. The size of the output data is fixed, irrespective of the size of the input data.
C. When compared to other cryptographic schemes, symmetric algorithms are somewhat slow in transforming data.
D. Symmetric algorithms contain a one way function, making it computationally infeasible for a different entity to calculate the input data from the output data.

Answer: A

Explanation:
Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A private key is simply a key that is not disclosed to people who are not authorized to use the encryption system. The disclosure of a private key breaches the

security of the encryption system.
By having the secret key, that would mean you will be authenticated to received the file or data that.
Incorrect answers:
B: This is not true as the size of data input determines the size of data output.
C: This is relative for all algorithms.
D: A symmetric algorithm requires both ends to have the same key and is thus not a one-way function.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 292-293

QUESTION 569:

A hashed password is vulnerable to which type of network attack?

A. Man in the middle attack.
B. Dictionary attack or brute force attack.
C. Reverse engineering.
D. DoS (Denial of Service) attack.

Answer: B

Explanation:
Here is how a hash is arrived at. Password:this ASCll Values t = 116, h = 104, i = 105, s = 115 (These values are multiplied by 2 to get the calculated number, which would be 232, 208, 210, 230. These numbers are added together then divided by 10. (232+208+210+230)/10. This gives you a hash of 80, but there are other number/ letter combinations that would give you this one way hash. So it cannot be used to crack the password.
A hashed password cannot be guessed, or reversed engineered. Hashing is a number used for data integrity also known as checksum, not encryption of password.
As you can see the hash value is just a single number. The hash value cannot be used to derive the meaning of the original message. But a password can still be guessed using adictionary or brute force.
Incorrect answers:
A
: If a hash was stolen off the wire using a man in the middle attack, it would do him no good. The reason is that the hash can represent several different words. The hash cannot be used to crack a password or message; it is used to verify or to store on a server as opposed to plain text.
C: Reverse engineering is the process of re-creating the functionality of an item by first deciding what the result is and then creating something from scratch that serves the same purpose. Hashed passwords will thus not be vulnerable.
D: Hashed passwords are not susceptible to DoS attacks.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 57

QUESTION 570:

Hashing is used to meet a specific security requirement within the digital signature procedure. What is it?

A. Non-repudiation.
B. Access control.
C. Data integrity.
D. Authentication.

Answer: C

Explanation:
Data integrity refers to the level of confidence that data won't be jeopardized and will be kept secret. A digital signature validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.
Incorrect answers:
A: Non-repudiation is the ability (by whatever means) to verify that data was seen by an intended party. It makes sure they received the data and can't repudiate (dispute) that it arrived.
B: Access Control is the means of giving or restricting user access to network resources. This is usually accomplished through the use of an ACL (Access Control List).
D: Authentication requires a user to provide some proof or credential that represents something they know, something they have, or something they are before allowing access to your company's resources.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 297-298
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1

QUESTION 571:

What would be the main reason for wanting confidentiality in your cryptography system?

A. Intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network
B. Involves providing assurance that a message was not modified during transmission
C. Is the process of verifying that the sender is who they say they are
D. The sender cannot deny the previous actions or message

Answer: A

Explanation:
A major reason to implement a cryptographic system is to ensure the confidentiality of the information being used. This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network.
Incorrect answers:
B: This refers to Integrity.
C: This refers to Authentication
D: This refers to Non-Repudiation
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 572:

What would be the main reason for wanting integrity in your cryptography system?

A. Intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network
B. Involves providing assurance that a message was not modified during transmission
C. Is the process of verifying that the sender is who they say they are
D. The sender cannot deny the previous actions or message

Answer: B

Explanation:
A major goal of a cryptographic system involves providing assurance that a message was not modified during transmission. This modification may render a message unintelligible or, even worse, inaccurate. Imagine the consequences if record alterations were not discovered in medical records involving drug prescriptions. If a message is tampered with, the encryption system should have a mechanism to indicate that the message has been corrupted or altered.
Incorrect answers:
A: This refers to Confidentiality.
C: This refers to Authentication.
D: This refers to Non-Repudiation.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 573:

What would be the main reason for wanting Authentication in your cryptography system?

A. Intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network
B. Involves providing assurance that a message was not modified during transmission
C. Is the process of verifying that the sender is who they say they are
D. The sender cannot deny the previous actions or message

Answer: C

Explanation:
Authentication is the process of verifying that the sender is who they say they are. This is very critical in many applications. A valid message from an invalid source is not authentic. One of the more common methods of verifying authenticity is the addition of a digital signature. Authenticity can be established using secret words that have been mutually agreed upon in advance.
Incorrect answers:
A: This refers to Confidentiality.
B: This refers to Integrity.
D: This refers to Non-Repudiation.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 574:

What would be the main reason for wanting Non-Repudiation in your cryptography system?

A. Intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network
B. Involves providing assurance that a message was not modified during transmission
C. Is the process of verifying that the sender is who they say they are
D. The sender cannot deny the previous actions or message

Answer: D

Explanation:
Non-repudiation means the sender cannot deny the previous actions or message. This can be achieved in a two-key system. If for example, you encrypted the message with a private key, the only way the message can decrypted properly is with the public key. This process has one serious problem: anybody can claim to be the legitimate receiver, and if they have access to this type of system, they can send you a public key.
Incorrect answers:
A: This refers to Confidentiality.
B: This refers to Integrity.
C: This refers to Authentication.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 575:

Which of the following cryptography services does the statement that it is intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network apply?

A. Confidentiality
B. Integrity
C. Authentication
D. Non-Repudiation

Answer: A

Explanation:
A major reason to implement a cryptographic system is to ensure the confidentiality of the information being used. This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network.
Incorrect answers:
B: A major goal of a cryptographic system involves providing assurance that a message was not modified during transmission. This modification may render a message unintelligible or, even worse, inaccurate. Imagine the consequences if record alterations were not discovered in medical records involving drug prescriptions. If a message is tampered with, the encryption system should have a mechanism to indicate that the message has been corrupted or altered.
C: Authentication is the process of verifying that the sender is who they say they are. This is very critical in many applications. A valid message from an invalid source is not authentic. One of the more common methods of verifying authenticity is the addition of a digital signature. Authenticity can be established using secret words that have been mutually agreed upon in advance.
D: Non-repudiation means the sender cannot deny the previous actions or message. This can be achieved in a two-key system. If for example, you encrypted the message with a private key, the only way the message can decrypted properly is with the public key. This process has one serious problem: anybody can claim to be the legitimate receiver, and if they have access to this type of system, they can send you a public key.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 576:

Which of the following cryptography services does the statement that it involves

providing assurance that a message was not modified during transmission apply?

A. Confidentiality
B. Integrity
C. Authentication
D. Non-Repudiation

Answer: B

Explanation:
A major goal of a cryptographic system involves providing assurance that a message was not modified during transmission. This modification may render a message unintelligible or, even worse, inaccurate. Imagine the consequences if record alterations were not discovered in medical records involving drug prescriptions. If a message is tampered with, the encryption system should have a mechanism to indicate that the message has been corrupted or altered.
Incorrect answers:
A: A major reason to implement a cryptographic system is to ensure the confidentiality of the information being used. This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network.
C: Authentication is the process of verifying that the sender is who they say they are. This is very critical in many applications. A valid message from an invalid source is not authentic. One of the more common methods of verifying authenticity is the addition of a digital signature. Authenticity can be established using secret words that have been mutually agreed upon in advance.
D: Non-repudiation means the sender cannot deny the previous actions or message. This can be achieved in a two-key system. If for example, you encrypted the message with a private key, the only way the message can decrypted properly is with the public key. This process has one serious problem: anybody can claim to be the legitimate receiver, and if they have access to this type of system, they can send you a public key.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 577:

Which of the following cryptography services does the statement that it is the process of verifying that the sender is who they say they are apply?

A. Confidentiality
B. Integrity
C. Authentication
D. Non-Repudiation

Answer: C

Explanation:
A major goal of a cryptographic system involves providing assurance that a message was not modified during transmission. This modification may render a message unintelligible or, even worse, inaccurate. Imagine the consequences if record alterations were not discovered in medical records involving drug prescriptions. If a message is tampered with, the encryption system should have a mechanism to indicate that the message has been corrupted or altered.
Incorrect answers:
A: A major reason to implement a cryptographic system is to ensure the confidentiality of the information being used. This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network.
B: Authentication is the process of verifying that the sender is who they say they are. This is very critical in many applications. A valid message from an invalid source is not authentic. One of the more common methods of verifying authenticity is the addition of a digital signature. Authenticity can be established using secret words that have been mutually agreed upon in advance.
D: Non-repudiation means the sender cannot deny the previous actions or message. This can be achieved in a two-key system. If for example, you encrypted the message with a private key, the only way the message can decrypted properly is with the public key. This process has one serious problem: anybody can claim to be the legitimate receiver, and if they have access to this type of system, they can send you a public key.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 578:

Which of the following cryptography services does the statement that it is the sender cannot deny the previous actions or message apply?

A. Confidentiality
B. Integrity
C. Authentication
D. Non-Repudiation

Answer: D

Explanation:
Non-repudiation means the sender cannot deny the previous actions or message. This can be achieved in a two-key system. If for example, you encrypted the message with a private key, the only way the message can decrypted properly is with the public key. This process has one serious problem: anybody can claim to be the legitimate receiver, and if they have access to this type of system, they can send you a public key.
Incorrect answers:

A: A major reason to implement a cryptographic system is to ensure the confidentiality of the information being used. This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network.
B: Authentication is the process of verifying that the sender is who they say they are. This is very critical in many applications. A valid message from an invalid source is not authentic. One of the more common methods of verifying authenticity is the addition of a digital signature. Authenticity can be established using secret words that have been mutually agreed upon in advance.
C: A major goal of a cryptographic system involves providing assurance that a message was not modified during transmission. This modification may render a message unintelligible or, even worse, inaccurate. Imagine the consequences if record alterations were not discovered in medical records involving drug prescriptions. If a message is tampered with, the encryption system should have a mechanism to indicate that the message has been corrupted or altered.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 579:

Which of the following cryptography services does the statement that it is the methods, processes, and mechanisms of preventing unauthorized access to the systems that do the cryptography apply?

A. Confidentiality
B. Integrity
C. Authentication
D. Access Control

Answer: D

Explanation:
Access control refers to the methods, processes, and mechanisms of preventing unauthorized access to the systems that do the cryptography. Keys are very vulnerable to theft, loss, and human security failings. A key component of access control involves both physical and operational security of these resources.
Incorrect answers:
A: A major reason to implement a cryptographic system is to ensure the confidentiality of the information being used. This confidentiality may be intended to prevent the unauthorized disclosure of information in a local network or to prevent the unauthorized disclosure of information across a network.
B: Authentication is the process of verifying that the sender is who they say they are. This is very critical in many applications. A valid message from an invalid source is not authentic. One of the more common methods of verifying authenticity is the addition of a digital signature. Authenticity can be established using secret words that have been

mutually agreed upon in advance.
C: A major goal of a cryptographic system involves providing assurance that a message was not modified during transmission. This modification may render a message unintelligible or, even worse, inaccurate. Imagine the consequences if record alterations were not discovered in medical records involving drug prescriptions. If a message is tampered with, the encryption system should have a mechanism to indicate that the message has been corrupted or altered.
Reference:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 580:

What would be the main reason for wanting access control in your cryptography system?

A. It is the methods, processes, and mechanisms of preventing unauthorized access to the systems that do the cryptography
B. Involves providing assurance that a message was not modified during transmission
C. Is the process of verifying that the sender is who they say they are
D. The sender cannot deny the previous actions or message

Answer: A

Explanation:
Access control refers to the methods, processes, and mechanisms of preventing unauthorized access to the systems that do the cryptography. Keys are very vulnerable to theft, loss, and human security failings. A key component of access control involves both physical and operational security of these resources.
Incorrect answers:
B: This refers to Integrity.
C: This refers to Authentication
D: This refers to Non-Repudiation
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 328-330.

QUESTION 581:

Which of the following statements best suit the government agency NSA?

A. Is responsible for creating codes, breaking codes, and coding systems for the U.S. government.
B. It was created in the early 1970s to help standardize and support Department of Defense (DoD) activities.
C.

Has been involved in developing and supporting standards for the U.S. government for over 100 years.
D. None of the above

Answer: A

Explanation:
Frequency analysis involves looking at blocks of an encrypted message to determine if any common patterns exist. Initially, the analyst does not try to break the code, but looks at the patterns in the message. In the English language, the letters E and T are very common.
Incorrect answers:
B: The National Security Agency/Central Security Service (NSA/CSS) is an independently functioning part of the NS
A. It was created in the early 1970s to help standardize and support Department of Defense (DoD) activities. The NSA/CSS supports all branches of the military. Each branch of the military used to have its own intelligence activities.
C: The National Institute of Standards and Technology (NIST) has been involved in developing and supporting standards for the U.S. government for over 100 years. NIST was formerly known as the National Bureau of Standards (NBS). NIST has become very involved in cryptography standards, systems, and technology in a variety of areas.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 582:

Which of the following statements best suit the government agency NSA/CSS?

A. Is responsible for creating codes, breaking codes, and coding systems for the U.S. government.
B. It was created in the early 1970s to help standardize and support Department of Defense (DoD) activities.
C. Has been involved in developing and supporting standards for the U.S. government for over 100 years.
D. None of the above

Answer: B

Explanation:
The National Security Agency/Central Security Service (NSA/CSS) is an independently functioning part of the NS
A. It was created in the early 1970s to help standardize and support Department of Defense (DoD) activities. The NSA/CSS supports all branches of the military. Each branch of the military used to have its own intelligence activities

Incorrect answers:
A: Frequency analysis involves looking at blocks of an encrypted message to determine if any common patterns exist. Initially, the analyst does not try to break the code, but looks at the patterns in the message. In the English language, the letters E and T are very common.
C: The National Institute of Standards and Technology (NIST) has been involved in developing and supporting standards for the U.S. government for over 100 years. NIST was formerly known as the National Bureau of Standards (NBS). NIST has become very involved in cryptography standards, systems, and technology in a variety of areas.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 583:

Which of the following statements best suit the government agency NIST?

A. Is responsible for creating codes, breaking codes, and coding systems for the U.S. government.
B. It was created in the early 1970s to help standardize and support Department of Defense (DoD) activities.
C. Has been involved in developing and supporting standards for the U.S. government for over 100 years.
D. None of the above

Answer: C

Explanation:
The National Institute of Standards and Technology (NIST) has been involved in developing and supporting standards for the U.S. government for over 100 years. NIST was formerly known as the National Bureau of Standards (NBS). NIST has become very involved in cryptography standards, systems, and technology in a variety of areas.
Incorrect answers:
A: Frequency analysis involves looking at blocks of an encrypted message to determine if any common patterns exist. Initially, the analyst does not try to break the code, but looks at the patterns in the message. In the English language, the letters E and T are very common.
B: The National Security Agency/Central Security Service (NSA/CSS) is an independently functioning part of the NS
A. It was created in the early 1970s to help
standardize and support Department of Defense (DoD) activities. The NSA/CSS supports all branches of the military. Each branch of the military used to have its own intelligence activities.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 584:

Which of the following statements best suit the association ABA?

A. Has been very involved in the security issues facing the banking and financial industries.
B. Is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers.
C. Is a professional group that is comprised primarily of Internet experts.
D. Is an association concerned with the interoperability, growth, and standardization of the World Wide Web

Answer: A

Explanation:
The American Bankers Association (ABA) has been very involved in the security issues facing the banking and financial industries. Banks need to communicate with each other in a secure manner. The ABA sponsors and supports several key initiatives regarding financial transactions.
Incorrect answers:
B: The Internet Engineering Task Force (IETF) is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers. The IETF is mainly interested in improving the Internet. It is also very interested in computer security issues. The IETF uses working groups to develop and propose standards.
C
: The Internet Society (ISOC) is a professional group that is comprised primarily of Internet experts. The ISOC oversees a number of committees and groups, including the IETF.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 585:

Which of the following statements best suit the association IETF?

A. Has been very involved in the security issues facing the banking and financial industries.
B. Is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers.
C. Is a professional group that is comprised primarily of Internet experts.
D. Is an association concerned with the interoperability, growth, and standardization of

the World Wide Web

Answer: B

Explanation:
The Internet Engineering Task Force (IETF) is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers. The IETF is mainly interested in improving the Internet. It is also very interested in computer security issues. The IETF uses working groups to develop and propose standards.
Incorrect answers:
A: The American Bankers Association (ABA) has been very involved in the security issues facing the banking and financial industries. Banks need to communicate with each other in a secure manner. The ABA sponsors and supports several key initiatives regarding financial transactions.
C: The Internet Society (ISOC) is a professional group that is comprised primarily of Internet experts. The ISOC oversees a number of committees and groups, including the IETF.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 586:

Which of the following statements best suit the association ISOC?

A. Has been very involved in the security issues facing the banking and financial industries.
B. Is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers.
C. Is a professional group that is comprised primarily of Internet experts.
D. Is an association concerned with the interoperability, growth, and standardization of the World Wide Web

Answer: C

Explanation:
The Internet Society (ISOC) is a professional group that is comprised primarily of Internet experts. The ISOC oversees a number of committees and groups, including the IETF.
Incorrect answers:
A: The American Bankers Association (ABA) has been very involved in the security issues facing the banking and financial industries. Banks need to communicate with each other in a secure manner. The ABA sponsors and supports several key initiatives

regarding financial transactions.
B: The Internet Engineering Task Force (IETF) is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers. The IETF is mainly interested in improving the Internet. It is also very interested in computer security issues. The IETF uses working groups to develop and propose standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 587:

Which of the following statements best suit the association W3C?

A. Has been very involved in the security issues facing the banking and financial industries.
B. Is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers.
C. Is a professional group that is comprised primarily of Internet experts.
D. Is an association concerned with the interoperability, growth, and standardization of the World Wide Web

Answer: D

Explanation:
The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
Incorrect answers:
B: The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards
C: The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 588:

Which of the following statements best suit the association ITU?

A. Has been involved in developing telecommunications and data communications standards for many years.
B. Is responsible for virtually all aspects of telecommunications and radio communications standards worldwide.
C. Is an international organization focused on technology and related standards.
D. Is an association concerned with the interoperability, growth, and standardization of the World Wide Web

Answer: B

Explanation:
The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards.
Incorrect answers:
A: The Comité Consultatif International Téléphonique et Télégraphique (CCITT) standards committee has been involved in developing telecommunications and data communications standards for many years. The functions performed by the CCITT have been taken over by the ITU, and CCITT standards are now managed by the ITU-T committee.
C: The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 589:

Which of the following statements best suit the association IEEE?

A. Has been involved in developing telecommunications and data communications standards for many years.
B.
Is responsible for virtually all aspects of telecommunications and radio communications standards worldwide.
C. Is an international organization focused on technology and related standards.

D. Is an association concerned with the interoperability, growth, and standardization of the World Wide Web

Answer: C

Explanation:
The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
Incorrect answers:
A: The Comité Consultatif International Téléphonique et Télégraphique (CCITT) standards committee has been involved in developing telecommunications and data communications standards for many years. The functions performed by the CCITT have been taken over by the ITU, and CCITT standards are now managed by the ITU-T committee.
B: The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 590:

Which of the following statements associations does the following statement that they have been involved in developing telecommunications and data communications standards for many years refer to?

A. CCITT.
B. ITU.
C. IEEE.
D. W3C.

Answer: A

Explanation:
The Comité Consultatif International Téléphonique et Télégraphique (CCITT) standards committee has been involved in developing telecommunications and data communications standards for many years. The functions performed by the CCITT have been taken over by the ITU, and CCITT standards are now managed by the ITU-T committee.

Incorrect answers:
B: The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards.
C: The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 591:

Which of the following statements associations does the following statement that they are responsible for virtually all aspects of telecommunications and radio communications standards worldwide refer to?

A. CCITT.
B. ITU.
C. IEEE.
D. W3C.

Answer: B

Explanation:
The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards.
Incorrect answers:
A: The Comité Consultatif International Téléphonique et Télégraphique (CCITT) standards committee has been involved in developing telecommunications and data communications standards for many years. The functions performed by the CCITT have been taken over by the ITU, and CCITT standards are now managed by the ITU-T committee.
C: The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the

interoperability, growth, and standardization of the World Wide Web.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 592:

Which of the following statements associations does the following statement that they are an international organization focused on technology and related standards refer to?

A. CCITT.
B. ITU.
C. IEEE.
D. W3C.

Answer: C

Explanation:
The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
Incorrect answers:
A: The Comité Consultatif International Téléphonique et Télégraphique (CCITT) standards committee has been involved in developing telecommunications and data communications standards for many years. The functions performed by the CCITT have been taken over by the ITU, and CCITT standards are now managed by the ITU-T committee.
B: The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 593:

Which of the following statements associations does the following statement that they are an association concerned with the interoperability, growth, and standardization of the World Wide Web refer to?

A. CCITT.
B. ITU.
C. IEEE.
D. W3C.

Answer: D

Explanation:
The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web.
Incorrect answers:
A: The Comité Consultatif International Téléphonique et Télégraphique (CCITT) standards committee has been involved in developing telecommunications and data communications standards for many years. The functions performed by the CCITT have been taken over by the ITU, and CCITT standards are now managed by the ITU-T committee.
B: The International Telecommunications Union (ITU) is responsible for virtually all aspects of telecommunications and radio communications standards worldwide. The ITU is broken into three main groups that are targeted at specific areas of concern. ITU-R is concerned with radio communication and spectrum management. ITU-T is concerned with telecommunication standards.
C: The Institute of Electrical and Electronics Engineers (IEEE) is an international organization focused on technology and related standards. The IEEE is organized into several working groups and standards committees. IEEE is very actively involved in the development of PKC, wireless, and networking protocols standards.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 594:

Which of the following statements associations does the following statement that they have been very involved in the security issues facing the banking and financial industries refer to?

A. ABA.
B. IETF.
C. ISOC.
D. W3C

Answer: A

Explanation:
The American Bankers Association (ABA) has been very involved in the security issues facing the banking and financial industries. Banks need to communicate with each other in a secure manner. The ABA sponsors and supports several key initiatives regarding

financial transactions.
Incorrect answers:
B
: The Internet Engineering Task Force (IETF) is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers. The IETF is mainly interested in improving the Internet. It is also very interested in computer security issues. The IETF uses working groups to develop and propose standards.
C: The Internet Society (ISOC) is a professional group that is comprised primarily of Internet experts. The ISOC oversees a number of committees and groups, including the IETF.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 595:

Which of the following statements associations does the following statement that they are an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers refer to?

A. ABA.
B. IETF.
C. ISOC.
D. W3C

Answer: B

Explanation:
The Internet Engineering Task Force (IETF) is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers. The IETF is mainly interested in improving the Internet. It is also very interested in computer security issues. The IETF uses working groups to develop and propose standards.
Incorrect answers:
A: The American Bankers Association (ABA) has been very involved in the security issues facing the banking and financial industries. Banks need to communicate with each other in a secure manner. The ABA sponsors and supports several key initiatives regarding financial transactions.
C
: The Internet Society (ISOC) is a professional group that is comprised primarily of Internet experts. The ISOC oversees a number of committees and groups, including the IETF.
D: The World Wide Web Consortium (W3C) is an association concerned with the

interoperability, growth, and standardization of the World Wide Web
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 596:

Which of the following statements associations does the following statement that they are a professional group that is comprised primarily of Internet experts refer to?

A. ABA.
B. IETF.
C. ISOC.
D. W3C

Answer: C

Explanation:
The Internet Society (ISOC) is a professional group that is comprised primarily of Internet experts. The ISOC oversees a number of committees and groups, including the IETF.
Incorrect answers:
A: The American Bankers Association (ABA) has been very involved in the security issues facing the banking and financial industries. Banks need to communicate with each other in a secure manner. The ABA sponsors and supports several key initiatives regarding financial transactions.
B: The Internet Engineering Task Force (IETF) is an international community of computer professionals, which includes network engineers, vendors, administrators, and researchers. The IETF is mainly interested in improving the Internet. It is also very interested in computer security issues. The IETF uses working groups to develop and propose standards.
D: The World Wide Web Consortium (W3C) is an association concerned with the interoperability, growth, and standardization of the World Wide Web
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 360.

QUESTION 597:

If you want to implement data integrity, which of the following should you use?

A. An asymmetric cipher
B. A digital certificate
C. A message digest
D. A symmetric cipher

Answer: C

Explanation:
The Message Digest Algorithm is another algorithm that creates a hash value. MDA uses a one-way hash. The hash value is used to help maintain integrity.
Incorrect answers:
A, D: A cipher is a method used to encode characters to hide their value. Ciphering is the process of using a cipher to encode a message.
B: A digital certificate is an electronic credential used to authenticate users.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 291-293

QUESTION 598:

What does IPSec (IP Security) offer to satisfy two specific security requirements?

A. Provides Secure Shell (SSH) to ensure data confidentiality.
B. Provides Password Authentication Protocol (PAP) to ensure user authentication.
C. Provides Authentication Header (AH) to ensure data integrity.
D. Provides Internet Protocol (IP) to ensure data integrity.
E. Provides Nonrepudiation Header (NH) to ensure identity integrity.
F. Provides Encapsulation Security Payload (ESP) to ensure data confidentiality.

Answer: C, F

Explanation:
IPSec is a security protocol that provides authentication and encryption across the Internet. IPSec can use AH or ESP.
Incorrect answers:
A, B, D and E: These are not provided by IPSec.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 120-121

QUESTION 599:

Choose the primary authentication method used.

A. Certificates.
B. Tokens.
C. Passwords.
D. Biometrics.

Answer: C

Explanation:
Password authentication is common on every operating system, and every restricted website. The sheer number of password authentication dwarves all the other options all put together. Passwords are easy to implement, users are accustomed to them, and the only equipment necessary is a keyboard.
Incorrect answers:
A: Certificates authentication is not as common as password authentication.
B: Tokens can be pricier than passwords and thus not a popular as passwords.
D: Biometric are too expensive and as such is not in such to the same scale as passwords.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 16
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1

QUESTION 600:

Which of the following statements specify the primary reason why token based authentication is not as easy to attack?

A. Tokens make use of digital certificates.
B. Tokens are devices that are physically owned.
C. Tokens can only be used once.
D. Only the designated owner can use a token

Answer: B

Explanation:
A token is a device that can be issued to a user for use in the authentication process. For example, there are token devices that, when enabled, synchronize with a server. Think of a token as a small piece of data that holds a sliver of information about the user. With a token being a physical possession it makes it hard to attack.
Tokens are difficult to duplicate and are generally tamper resistant. Some can be carried with you for use on any workstation, although others require appropriate hardware peripherals and software on a workstation. Although tokens offer reliable security, they can be costly and difficult to deploy in an enterprise environment.
Tokens can either provide a one-time-use password or store information about the user. The user information can be a certificate and a password, as with smart cards. Smart card technologies provide strong security through encryption as well as access control. Smart cards require a reader that is used when the authentication is required.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 16
Microsoft Corporation with Andy Ruth & Kurt Hudson, Security+ Certification Training Kit e-Book, Microsoft Press, Redmond, 2003, Chapter 7, Lesson 1

QUESTION 601:

You work as the security administrator at Certkiller .com. You want to implement an authentication method that will provide an additional layer of security when stored keys and passwords are not strong enough.
Which authentication type should you implement?

A. Mutual authentication.
B. Multi-factor authentication.
C. Biometric.
D. Certificate authentication.

Answer: B

Explanation:
Multi-Factor
When two or more of these access methods are included as a part of the authentication process, you are implementing a multi-factor system.
Incorrect answers:
A: Mutual authentication is when both the user and the resource authenticate to each other. But is is not an additional layer of security.
C: Biometrics does not represent an additional security layer.
D: Certificate authentication is not synonymous with the provision of an additional layer of security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 17, 244

QUESTION 602:

The single sign-on process addresses a specific authentication problem. What is it?

A. The issue of authorization through multiple servers.
B. The issue of multiple domains.
C. The issue of multi-factor authentication.
D. The issue of multiple usernames and passwords.

Answer: D

Explanation:
One of the big problems that larger systems must deal with is the need to access multiple systems or applications. This may require a user to remember multiple accounts and passwords. The purpose of a single sign-on (SSO) is to give users access to all the applications and systems they need when they log on with a single sign-on.
Incorrect answers:

A: Authorization through multiple servers is not what a single sign on is meant for.
B: Multiple domains are irrelevant in this case.
C: Multifactor authentication is when two or more access methods are included as part of the authentication process, you're implementing a multi-factor system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 17, 388

QUESTION 603:

Which of the following describes the main reason for implementing security measures and countermeasures?

A. To prevent unauthorized access, unauthorized data modification, and denial of authorized access.
B. To prevent interoperability of the framework, unauthorized data modification, and denial of authorized access.
C. To prevent potential discovery of access, interoperability of the framework, and denial of authorized access.
D. To prevent interoperability of the framework, unauthorized data modification, and unauthorized access.

Answer: A

Explanation:
Security measures and countermeasures are used for confidentiality, integrity, availability and accountability.
Incorrect answers:
B: Prevention of the interoperability of the framework is not a direct concern of security measures.
C: The prevention of potential discovery of access is not the primary purpose of technical security measures.
D: Interoperability of the framework is not a direct concern of security measures.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 308

QUESTION 604:

Which of the following describes the main reason for needing to control access to networks, systems, and data?

A. To preserve authenticity, confidentiality, integrity and availability.
B. To preserve integrity and availability.
C. To preserve confidentiality, integrity and availability.
D. To preserve authenticity, confidentiality and availability.

Answer: C

Explanation:
The design goals of a security topology must deal with issues of confidentiality, integrity, availability and accountability. You will often see the confidentiality, integrity and availability referred to as the CIA of network security. The accountability is equally important.
Incorrect answers:
A: Integrity, availability and confidentially can be preserved through access control. Authenticity can occur through many other methods.
B: It more for more than mere integrity and availability.
D: Integrity is another necessary factor that is missing from this option.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, p. 211

QUESTION 605:

To detect network attacks, intrusion detection systems monitor for, and detect specific conditions. Which two do most intrusion detection systems monitor for?

A. Patterns
B. Viruses
C. Signatures
D. Hackers
E. Malware

Answer: A, C

Explanation:
IDS can detect two types of traffic patterns. Misuse-Detection IDS is primarily focused on evaluating attacks based on attack signatures and audit trails. Anomaly-Detection IDS focuses on abnormal traffic patterns.
Incorrect answers:
B: They do not make use of viruses to detect attacks.
D: IDS cannot go and look for hackers to look for attacks. They need to look at patterns and signatures in order to detect a hacker.
E: IDS does not make use of malware to detect attacks.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex Publishing, 2004, pp. 115-117

QUESTION 606:

Which of the following statements best suit the PKI trust model Hierarchical?

A. In this trust model, the intermediate CAs only trust information that is provided from the root CA.
B. In this trust model, a peer-to-peer relationship exists between the root CAs.
C. This model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs.
D. This model can use the capabilities of any or all of the structures that have been discussed in the previous sections

Answer: A

Explanation:
In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
Incorrect answers:
B: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs.
C: The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure
D: A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments..
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 607:

Which of the following statements best suit the PKI trust model Bridge?

A. In this trust model, the intermediate CAs only trust information that is provided from the root CA.
B. In this trust model, a peer-to-peer relationship exists between the root CAs.
C. This model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs.
D. This model can use the capabilities of any or all of the structures that have been discussed in the previous sections

Answer: B

Explanation:
In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs.
Incorrect answers:
A
: In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs
that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
C: The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure
D: A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments..
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 608:

Which of the following statements best suit the PKI trust model Mesh?

A. In this trust model, the intermediate CAs only trust information that is provided from the root CA.
B. In this trust model, a peer-to-peer relationship exists between the root CAs.
C. This model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs.
D. This model can use the capabilities of any or all of the structures that have been discussed in the previous sections

Answer: C

Explanation:
The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure.

Incorrect answers:
A
: In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs
that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
B: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs
D: A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments..
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 609:

Which of the following statements best suit the PKI trust model Hybrid?

A. In this trust model, the intermediate CAs only trust information that is provided from the root CA.
B. In this trust model, a peer-to-peer relationship exists between the root CAs.
C. This model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs.
D. This model can use the capabilities of any or all of the structures that have been discussed in the previous sections

Answer: D

Explanation:
A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments.
Incorrect answers:
A
: In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs
that are in their hierarchy. This allows a high level of control at all levels of the

hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
B: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs
C: The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 610:

Which of the following PKI trust models does the statement that this trust model, the intermediate CAs only trust information that is provided from the root CA refer to?

A. Hierarchical.
B. Bridge.
C. Mesh.
D. Hybrid

Answer: A

Explanation:
In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
Incorrect answers:
B
: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs.
C: The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure
D: A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a

hybrid trust structure. The flexibility of this model also allows you to create hybrid environments.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 611:

Which of the following PKI trust models does the statement that this trust model, a peer-to-peer relationship exists between the root CAs refer to?

A. Hierarchical.
B. Bridge.
C. Mesh.
D. Hybrid

Answer: B

Explanation:
In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs.
Incorrect answers:
A
: In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs
that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
C: The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure
D: A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 612:

Which of the following PKI trust models does the statement that this model expands

the concepts of the bridge model by supporting multiple paths and multiple root CAs refer to?

A. Hierarchical.
B. Bridge.
C. Mesh.
D. Hybrid

Answer: C

Explanation:
The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure.
Incorrect answers:
A: In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs
that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
B: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs.
D: A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 613:

Which of the following PKI trust models does the statement that this model can use the capabilities of any or all of the structures that have been discussed in the previous sections refer to?

A. Hierarchical.
B. Bridge.
C. Mesh.
D. Hybrid

Answer: D

A hybrid structure can use the capabilities of any or all of the structures that have been discussed in the previous sections. You can be extremely flexible when you build a hybrid trust structure. The flexibility of this model also allows you to create hybrid environments.
Incorrect answers:
A: In a hierarchical trust model, the intermediate CAs only trust information that is provided from the root C
A. Additionally, the root CA will also trust intermediate CAs
that are in their hierarchy. This allows a high level of control at all levels of the hierarchical tree. This might be the most common implementation in a large organization that wants to extend its certificate processing capabilities.
B
: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. Each of the root CAs can communicate with each other, allowing crosscertification. This allows a certification process to be established between organizations or departments. Each of the intermediate CAs trusts only the CAs above and below it, but the CA structure can now be expanded without creating additional layers of CAs.
C: The mesh model expands the concepts of the bridge model by supporting multiple paths and multiple root CAs. It also has the ability to cross certify with the other root CAs in the mesh. This may also be referred to as a web structure.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 341-342.

QUESTION 614:

Which of the following are used to decrypt a message in a PKI system?

A. Private Key.
B. Public Key.
C. Shared secret.
D. Digital signature

Answer: A

Explanation:
PKI uses two keys. It uses a public key to encrypt messages and a private key to decrypted messages.
Incorrect Answers:
B: PKI uses a public key to encrypt messages.
C, D: PKI uses public and private keys not digital signature or shared secret.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 330-331.

QUESTION 615:

Which of the following are used to encrypt a message in a PKI system?

A. Private Key.
B. Public Key.
C. Shared secret.
D. Digital signature

Answer: B

Explanation:
PKI uses two keys. It uses a public key to encrypt messages and a private key to decrypted messages.
Incorrect Answers:
Incorrect Answers:
A: PKI uses a private key to decrypt messages.
C, D: PKI uses public and private keys not digital signature or shared secret.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 330-331.

QUESTION 616:

Which of the following statements would best describe a public key?

A. A public key is sent over the network and is used to decrypt a message.
B. A public key is not sent over the network and is used to decrypt a message.
C. A public key is sent over the network and is used to encrypt a message.
D. A public key is not sent over the network and is used to encrypt a message.

Answer: C

Explanation:
When you want to send an encrypted message to someone, you must request that person's public key which you would use to encrypt the message. You can then send the encrypted message to them and they would then use their private key to decrypt the message.
Incorrect Answers:
A, B, D:
When you want to send an encrypted message to someone, you must request that person's public key which you would use to encrypt the message. You can then send the encrypted message to them and they would then use their private key to decrypt the message.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 330-331.

QUESTION 617:

Which of the following statements would best describe a private key?

A. A private key is sent over the network and is used to decrypt a message.
B. A private key is not sent over the network and is used to decrypt a message.
C. A private key is sent over the network and is used to encrypt a message.
D. A private key is not sent over the network and is used to encrypt a message.

Answer: B

Explanation:
When you want to send an encrypted message to someone, you must request that person's public key which you would use to encrypt the message. You can then send the encrypted message to them and they would then use their private key to decrypt the message. The private key is never transmitted over the network.
Incorrect Answers:
A, C, D:When you want to send an encrypted message to someone, you must request that person's public key which you would use to encrypt the message. You can then send the encrypted message to them and they would then use their private key to decrypt the message. The private key is never transmitted over the network.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 330-331.

QUESTION 618:

Under which of the following sub headings should you write the encrypted value of the key with regards to a PKI certificate?

A. Public key.
B. Extensions.
C. Serial number.
D. Subject.

Answer: A

Explanation:
The most popular certificate used is the X.509 v3 certificate. The X.509 certificate is a standard certificate format supported by the International Telecommunications Union (ITU) and many other standards organizations. Adopting a standard certificate format is important for systems to be assured interoperability in a certificate-oriented environment.
Incorrect Answers:

B, C, D: These fall under other categories and do not apply.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp. 336.

QUESTION 619:

Which of the following options regarding PKI defines what certificates can do?

A. A certificate policy
B. A certificate practice statement
C. A certificate authority
D. Trust models

Answer: A

Explanation:
Certificate policies define what certificates can be used to do. A CA can potentially issue a number of different types of certificates; say, one for e-mail, one for e-commerce, and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
Incorrect Answers:
B: A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used
to enforce policy at the C
A. The CA will provide this information to users of the CA's
services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
C: A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
D: For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate..
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 620:

Which of the following options regarding PKI discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility?

A. A certificate policy
B. A certificate practice statement
C. A certificate authority
D. Trust models

Answer: B

Explanation:
A certificate practice statement (CPS) is a statement that the CA uses to issue certificates a number of different types of certificates; say, one for e-mail, one for e-commerce, and and implement the policies of the C
A. This is a detailed document that is used to enforce
policy at the C
A. The CA will provide this information to users of the CA's services.
These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
Incorrect Answers:
A: Certificate policies define what certificates can be used to do. A CA can potentially and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
C: A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
D: For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate..
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 621:

Which of the following options regarding PKI is an organization that is responsible

for maintaining certificates?

A. A certificate policy
B. A certificate practice statement
C. A certificate authority
D. Trust models

Answer: C

Explanation:
A certificate authority (CA) is an organization that is responsible for maintaining a number of different types of certificates; say, one for e-mail, one for e-commerce, and certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
Incorrect Answers:
A: Certificate policies define what certificates can be used to do. A CA can potentially and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
B: A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used
to enforce policy at the C
A. The CA will provide this information to users of the CA's
services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
D: For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate..
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 622:

Which of the following options regarding PKI requires something to work, the capabilities of CAs must be readily available to users?

A. A certificate policy
B. A certificate practice statement

C. A certificate authority
D. Trust models

Answer: D

Explanation:
For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate.
Incorrect Answers:
A: Certificate policies define what certificates can be used to do. A CA can potentially a number of different types of certificates; say, one for e-mail, one for e-commerce, and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
B: A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used
to enforce policy at the C
A. The CA will provide this information to users of the CA's
services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
C: A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 623:

Which of the following statements is correct regarding Certificate policies?

A. It defines what certificates can do
B. It discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility
C. It is an organization that is responsible for maintaining certificates
D. PKI requires something to work, the capabilities of CAs must be readily available to users.

Answer: A

Explanation:
Certificate policies define what certificates can be used to do. A CA can potentially issue a number of different types of certificates; say, one for e-mail, one for e-commerce, and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
Incorrect Answers:
B: A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used
to enforce policy at the C
A. The CA will provide this information to users of the CA's
services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
C: A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
D: For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 624:

Which of the following statements is correct regarding Certificate practice statements?

A. It defines what certificates can do
B. It discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility
C. It is an organization that is responsible for maintaining certificates
D. PKI requires something to work, the capabilities of CAs must be readily available to users.

Answer: B

Explanation:
A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used to enforce
policy at the C
A. The CA will provide this information to users of the CA's services.
These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
Incorrect Answers:
A: Certificate policies define what certificates can be used to do. A CA can potentially a number of different types of certificates; say, one for e-mail, one for e-commerce, and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
C: A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
D: For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 625:

Which of the following statements is correct regarding Certificate authority?

A. It defines what certificates can do
B. It discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility
C. It is an organization that is responsible for maintaining certificates
D. PKI requires something to work, the capabilities of CAs must be readily available to users.

Answer: C

Explanation:
A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really

nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
Incorrect Answers:
A: Certificate policies define what certificates can be used to do. A CA can potentially a number of different types of certificates; say, one for e-mail, one for e-commerce, and one for financial transactions. The policy might indicate that it is not to be used for signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
B: A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used
to enforce policy at the C
A. The CA will provide this information to users of the CA's
services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
D: For PKI to work, the capabilities of CAs must be readily available to users. The model that has been shown to this point is the simple trust model. This simple trust model may not work as PKI implementations get bigger. Conceptually, every computer user in the world would have a certificate.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 626:

Which of the following statements is correct regarding Trust Models?

A. It defines what certificates can do
B. It discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility
C. It is an organization that is responsible for maintaining certificates
D. PKI requires something to work, the capabilities of CAs must be readily available to users.

Answer: D

Explanation:
.
Incorrect Answers:
A: Certificate policies define what certificates can be used to do. A CA can potentially a number of different types of certificates; say, one for e-mail, one for e-commerce, and one for financial transactions. The policy might indicate that it is not to be used for

signing contracts or for purchasing equipment. Certificate policies affect how a certificate is issued and how it is used. A CA would have policies regarding the interoperability or certification of another CA site; the process of requiring interoperability is called cross certification. The organizations using the certificates also have the right to decide which types of certificates are used and for what purposes.
B: A certificate practice statement (CPS) is a statement that the CA uses to issue certificates and implement the policies of the C
A. This is a detailed document that is used
to enforce policy at the C
A. The CA will provide this information to users of the CA's
services. These statements should discuss how certificates are issued, what measures are taken to protect certificates, and the rules that CA users must follow in order to maintain their certificate eligibility. These policies should be readily available to CA users.
C: A certificate authority (CA) is an organization that is responsible for maintaining certificates. This includes issuing, revoking, and distributing them. A certificate is really nothing more than a mechanism that associates the public key with an individual. A certificate contains a great deal of information about the user.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 336-340.

QUESTION 627:

From the definitions, which best defines the primary reason for using digital certificates.

A. Digital certificates are used to bind a public key to the identity of the signer and recipient.
B. Digital certificates are used to bind a private key to the identity of the signer and recipient.
C. Digital certificates are used to bind a public key to the entity that has the associated private key.
D. Digital certificates are used to bind a private key to the entity that has the associated public key.

Answer: C

Explanation:
A digital certificate is the public key with an individual. It is issued by a certification authority (CA) and contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.
Incorrect Answers:

A, B: A certificate associates the public key with an individual. This has nothing to do with any intended recipient. Furthermore, a PKI system is based on the continued security of the user's private key. This key must never leave the possession of the owner.
D: A certificate associates the public key with an individual. The user's private key must never leave the possession of the owner.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 305.

QUESTION 628:

Before a CA (Certificate Authority) can issue a certificate to a user, a user must provide the CA with something. What is it?

A. The public key of the user.
B. The public key of the recipient.
C. The public keys of the user and recipient.
D. The public and private keys of the user and recipient.

Answer: A

Explanation:
A certificate associates the public key with an individual. Therefore the user must submit proof of identity and his or her public key.
Incorrect Answers:
B, C, D: A certificate associates the public key with an individual. This has nothing to do with any intended recipient. Furthermore, a PKI system is based on the continued security of the user's private key. This key must never leave the possession of the owner.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 305.

QUESTION 629:

Choose the recommended good practice for deploying a CA (Certificate Authority).

A. You should ensure that users are enrolled for policy based certificates.
B. You should define a CPS (Certificate Practice Statement).
C. You should register the CA with a subordinate CA.
D. You should always create a mirror CA for fault tolerance purposes.

Answer: B

Explanation:
A certificate practice statement (CPS) is legal document that describes how the CA (Certificate Authority) manages the certificates it issue.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 538-539.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 301.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 131.

QUESTION 630:

On the topic of X509 version 3 certificates, choose the option which is NOT a valid field.

A. Private key field.
B. Issuer field.
C. Serial number field.
D. Subject field.

Answer: A

Explanation:
The X.509 has a Version field, a Serial Number field, a Signature Algorithm Identifier field, an Issuer field, a Validity Period field, a Subject Name field, a Subject Public Key Information field, and an Extension Field. It does not have a private key field.
Incorrect Answers:
B: X.509 does have an Issuer field.
C: X.509 does have a Serial Number field.
D: X.509 does have a Subject Name field.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 304-305.

QUESTION 631:

On the topic X509 certificates, choose the option which describes the actual content of users' certificates.

A. Contents include the user's public key, object identifiers, and location of the user's electronic identity.
B. Contents include the user's private key, the CA (Certificate Authority) distinguished name, and the type of symmetric algorithm used for encryption.
C.
Contents include the user's public key, the certificate's serial number, and the certificate's

validity dates.
D. Contents include the user's public key, the serial number of the CA (Certificate Authority) certificate, and the CRL (Certificate Revocation List) entry point.

Answer: C

Explanation:
The X.509 has a Version field, a Serial Number field, a Signature Algorithm Identifier field, an Issuer field, a Validity Period field, a Subject Name field, a Subject Public Key Information field, and an Extension Field. It does not have a private key field.
Incorrect Answers:
A: X.509 does not have an Object Identifiers field or the location of user's electronic identity.
B: X.509 does not have a private key field.
D: X.509 does not have the serial number of the CA (Certificate Authority) certificate, and the CRL (Certificate Revocation List) entry point.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 304-305.
http://csrc.nist.gov/pki/panel/santosh/tsld002.htm

QUESTION 632:

The majority of certificates used for authentication purposes are based on which certificate standards?

A. ISO19278 certificates standard
B. X.500 certificates standard
C. RFC 1205 certificates standard
D. X.509 v3 certificates standard

Answer: D

Explanation:
The most widely used digital certificates standard is the X.509 version 3.
Incorrect Answers:
A: There is no ISO19278 certificate standard.
B: X.500 is a standard for hierarchical directory structures. LDAP is based on the X.500 standard.
C: RFC 1205 describes the IBM 5250 Telnet interface.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 224, 304-305.
http://www.faqs.org/rfcs/rfc1205.html

QUESTION 633:

On the Internet, a pop-up browser window validates the identity of the ActiveX developer. Choose the option which correctly specifies this.

A. Authenticode
B. A Web server certificate
C. A CA (Certificate Authority) certificate
D. A server certificate

Answer: A

Explanation:
Authenticode is based on certificate technology which allows ActiveX components to be validated by the web server.
Incorrect Answers:
B: A web server certificate allows a website to enable SSL communication.
C: A CA (Certificate Authority) certificate associates a public key with a CA, verifying the identity of the CA and the validity of the certificates that the CA issues.
D: A server certificate is used to validate the identity of a server to a client.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 128.
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 49, 283.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 21-22.

QUESTION 634:

Embedded root certificates within web browsers are a typical example of which trust model?

A. Bridge trust model.
B. Mesh trust model.
C. Hierarchy trust model.
D. Trust list.

Answer: D

Explanation:
Web browsers like Internet Explorer and Netscape Navigator are capable of abiding by a trust list; which is a list of sites that are confirmed to be safe and have their valid certificates embedded to prove it.
Incorrect Answers:
A: In a bridge trust model, a peer-to-peer relationship exists between the root CAs. This

enables cross-certification as it allows the root CAs to communicate with each other. This trust model allows a certification process to be established between organizations or departments.
B: The mesh trust model combines the bridge model and the hierarchical model, expanding the bridge model by supporting multiple paths and multiple root CAs. Each root CA can cross-certify with the other root CAs in the mesh.
C: In a hierarchical trust model a root CA provides the certification information for intermediate CAs, which only trust information provided by the root C
A. The
intermediate CAs issue certificates to other entities.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 306-310.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 134.

QUESTION 635:

From the options, choose all that indicate recommended scenarios for using smart card technology. Choose all correct answers.

A. Mobile telephones.
B. Satellite television access cards.
C. A PKI (Public Key Infrastructure) token card shared by multiple users.
D. Credit cards.

Answer: A, B, D

Explanation:
A smart card is a hardware device that can be used for authentication purposes, including authentication user access to mobile telephones, satellite television access cards, credit cards and token cards.
Incorrect Answers:
C: There is no such thing as a PKI token card. PKI uses software based certificates and keys, not cards.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 6, 17, 300-301.

QUESTION 636:

Which of the following is included in a CRL (Certificate Revocation List)?

A. Certificates that have had a limited validity period and have expired.
B. Certificates that are pending renewal.
C. Certificates that are considered invalid because they do not contain a valid CA (Certificate Authority) signature.

D. Certificates that have been disabled before their scheduled expiration.

Answer: D

Explanation:
The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked. This information is published in the CRL.
Incorrect Answers:
A, B: Only certificates that have been revoked are published in the CRL, not certificates that have expired or that are pending renewal.
C: Certificates would not be issued without a valid CA (Certificate Authority) signature.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 131-132.

QUESTION 637:

Choose the element which can be included in a digital certificate.

A. Private key of the CA (Certificate Authority).
B. Private key of the certificate holder.
C. Revocation information on the certificate.
D. Validity period of the certificate.

Answer: D

Explanation:
A digital certificate associates the public key with an individual. Therefore the user must submit proof of identity and his or her public key. The fields contained in a certificate include a Version field, a Serial Number field, a Signature Algorithm Identifier field, an Issuer field, a Validity Period field, a Subject Name field, a Subject Public Key Information field, and an Extension Field. It does not have a private key field.
Incorrect Answers:
A, B: A digital certificate does not contain any private key information. A PKI system is based on the continued security of the private keys. These key must never leave the possession of the owner. Furthermore, certificate's revocation information is published in a Certificate Revocation List (CRL).
C: Certificate's revocation information is published in a Certificate Revocation List (CRL), not in the digital certificate.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 272.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 131-132, 305.

QUESTION 638:

On the topic of CRLs (Certificate Revocation Lists), choose the TRUE statement.
A.
A CLR query that receives a response in near real time points to the usage of high-availability devices and mechanisms.
B. A CLR query that receives a response in near real time points to the usage of a fault tolerant database.
C. A CLR query that receives a response in near real time does not mean that fresh data is always returned.
D. A CLR query that receives a response in near real time points to a CA (Certificate Authority) that is providing near real time updates.

Answer: C

Explanation:
A certificate revocation list is a list kept by a certificate authority that lists off sites who's certificates have expired, or been revoked for security breaches. The problem with them is that, although it is possible to get an immediate response, the data that is on the list has up to a 24 hour update delay. For this reason Online Certificate Status Protocol (OCSP) is better.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 131-132.

QUESTION 639:

When a private key becomes happens to be compromised before the certificate's normal expiration date, what gets issued?

A. Certificate enrollment list
B. Certificate expiration list
C. Certificate revocation list
D. Certificate validation list

Answer: C

Explanation:
Certification revocation is the process of revoking a certification before it expires. A certificate may need to be revoked because it was stolen, an employee moved on to a new company, or someone has had their access revoked.
Incorrect Answers:
A, B, D:
There is not certificate enrollment list, certificate expiration list, or certificate validation list.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2002, pp 305-306.

QUESTION 640:

Which of the following standards defines the certificate formats and fields for public keys?

A. X.509.
B. SSL.
C. TLS.
D. ISAKMP.

Answer: A
The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
Incorrect Answers:
B: The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key
C: Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
D: The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 641:

Which of the following standards establishes a secure communication connection between two TCP-based machines?

A. X.509.
B. SSL.
C. TLS.
D. ISAKMP.

Answer: B

The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
Incorrect Answers:
A: The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
C: Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
D: The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 642:

Which of the following standards is a security protocol that combines SSL and other security protocols?

A. X.509.
B. SSL.
C. TLS.
D. ISAKMP.

Answer: C
Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
Incorrect Answers:
A: The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
B: The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
D: The Internet Security Association and Key Management Protocol (ISAKMP) defines

a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 643:

Which of the following standards defines a framework within which a VPN client and server can connect?

A. X.509.
B. SSL.
C. TLS.
D. ISAKMP.

Answer: D
The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems.
Incorrect Answers:
A: The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
B: The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
C: Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 644:

Which of the following statements best suits the PKI standard X.509?

A. It defines the certificate formats and fields for public keys
B. It establishes a secure communication connection between two TCP-based machines
C. It is a security protocol that combines SSL and other security protocols

D. It defines a framework within which a VPN client and server can connect

Answer: A
The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
Incorrect Answers:
B: The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
C: Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
D: The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 645:

Which of the following statements best suits the PKI standard SSL?

A. It defines the certificate formats and fields for public keys
B. It establishes a secure communication connection between two TCP-based machines
C. It is a security protocol that combines SSL and other security protocols
D. It defines a framework within which a VPN client and server can connect

Answer: B
The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
Incorrect Answers:
A: The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
C: Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near

future.
D: The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 646:

Which of the following statements best suits the PKI standard TLS?

A. It defines the certificate formats and fields for public keys
B. It establishes a secure communication connection between two TCP-based machines
C. It is a security protocol that combines SSL and other security protocols
D. It defines a framework within which a VPN client and server can connect

Answer: C
Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
Incorrect Answers:
A: The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
B: The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
D: The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 647:

Which of the following statements best suits the PKI standard ISAKMP?

A. It defines the certificate formats and fields for public keys
B. It establishes a secure communication connection between two TCP-based machines

C. It is a security protocol that combines SSL and other security protocols
D. It defines a framework within which a VPN client and server can connect

Answer: D
The Internet Security Association and Key Management Protocol (ISAKMP) defines a framework within which a VPN client and server can connect. ISAKMP allows the two ends to negotiate which encryption and hashing algorithms should be used between the systems.
Incorrect Answers:
A: The X.509 standard defines the certificate formats and fields for public keys. It also defines the procedures that should be used to distribute public keys. The X.509 version 2 certificates are still used as the primary method of issuing CRL certificates.
B: The Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. When a connection request is made to the server, the server sends a message back to the client indicating a secure connection is needed. The client then sends the server a certificate indicating the capabilities of the client. The server then evaluates the certificate and responds with a session key and an encrypted private key.
C: Transport Layer Security (TLS) is a security protocol that combines SSL and other security protocols. Many industry analysts predict that TLS will replace SSL in the near future.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 366-367.

QUESTION 648:

Which terminology refers to the defacto Information Technology evaluation criteria for the international community?

A. Common Criteria.
B. Global Criteria.
C. TCSEC (Trusted Computer System Evaluation Criteria).
D. ITSEC (Information Technology Security Evaluation Criteria).

Answer: A
The Common Criteria is the defacto IT (Information Technology) security evaluation criteria for the international community. Before the Common Criteria, different criteria were used in America and in Europe. The criterion used in the USA was called the Trusted Computer Systems Evaluation Criteria (TCSEC), or Orange Book, and was developed by the U.S. Department of Defense while the criterion used in Europe was the Information Technology Security Evaluation Criteria (ITSEC). The Common Criteria is the result of efforts to combine these two.
Incorrect Answers:
B: There is no such thing as a Global Criteria.
C: Prior to the Common Criteria, the Trusted Computer Systems Evaluation Criteria

(TCSEC), or Orange Book, was used in the USA and differed from the criteria used in Europe.
D: Prior to the Common Criteria, the Information Technology Security Evaluation Criteria (ITSEC) was used in Europe and differed from the criteria used in the USA.
References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 62.

QUESTION 649:

Which algorithm is used by AES (Advanced Encryption Standard)?
Rijndael algorithm.
Nagle algorithm.
Spanning Tree algorithm.
PKI algorithm.

Answer: A

Explanation:
AES uses the Rijindael algorithm.
Incorrect Answers:
B: There is no Nagle algorithm
C: Spanning Tree is used in routing it is not an algorithm.
D: The Public Key Infrastructure (PKI) is based on certificates and keys. It is not an algorithm.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 503-504.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 293.

QUESTION 650:

Which algorithm creates a 128-bit hash from a data input to verify data integrity from a remote user?

A. IPSec (Internal Protocol Security)
B. RSA (Rivest Shamir Adelman)
C. Blowfish
D. MD5 (Message Digest 5)

Answer: D

Explanation:
MD5 is take a variable length of data input and produces a hash that is always equal to128-bits, regardless of the length of the input data.

Incorrect Answers:
A: IPSec is not an algorithm.
B: The RSA algorithm is a public-key encryption system for both encryption and digital signatures.
C: Blowfish is a block cipher algorithm that uses a 64-bit block of data to create the hash.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 120.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 293.

QUESTION 651:

Which IETF (Internet Engineering Task Force) protocols make use of AH (Authentication Header) and ESP (Encapsulating Security Payload)?
SSL (Secure Sockets Layer).
IPSec (Internet Protocol Security).
HTTPS (Secure Hypertext Transfer Protocol).
SSH (Secure Shell).

Answer: B

Explanation:
IPSec is an IETF protocol, and it does use an AH and ESP. AH is used to provide data integrity while ESP is used to provide authenticity and integrity of the data payload.
Incorrect Answers:
A, C, D: SSL, HTTPS and SSH does not use AH and ESP. Only IPSec uses AH and ESP.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 120.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION 652:

Choose the standard that provides 160-bit encryption.

A. MD5
B. MD4
C. SHA-1
D. Blowfish

Answer: C
SHA-1 uses a 160-bit secret key.
Incorrect Answers:
A, B: MD-2, MD-4 and MD-5 provide 128-bit encryption.

D: Blowfish provides 64-bit encryption.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 511, 512.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 291, 293.

QUESTION 653:

Choose that option that best defines what the Diffie-Hellman algorithm provides.

A. The Diffie-Hellman algorithm provides access to digital certificate stores from a CA.
B. The Diffie-Hellman algorithm provides a secret key exchange over an insecure medium without any prior arrangements.
C. The Diffie-Hellman algorithm provides authentication without having to use hashing algorithms.
D. The Diffie-Hellman algorithm provides multiple protocols for key exchange negotiations.

Answer: B

Explanation:
Also known as an exponential key agreement, the Diffie-Hellman algorithm allows two sides to agree to an exclusive secret key between them, with no prior arrangements. When the keys are exchanged they are done so secretively, then verified to confirm it reaches the right recipient.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 507-508.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 295, 445.

QUESTION 654:

Which of the following processes is the most important and first step in the process of working with keys and certificates?

A. Key generation.
B. Key storage and distribution.
C. Key escrow.
D. Key expiration.

Answer: A

Explanation:
Key generation (creating the key) is an important first step in the process of working with

keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
Incorrect Answers:
B: Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
C: A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation
D: A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 655:

Which of the following processes is how keys are stored affects how they are distributed?

A. Key generation.
B. Key storage and distribution.
C. Key escrow.
D. Key expiration.

Answer: B

Explanation:
Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
Incorrect Answers:
A: Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
C: A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation

D: A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 656:

Which of the following processes stores keys for the purpose of law enforcement access?

A. Key generation.
B. Key storage and distribution.
C. Key escrow.
D. Key expiration.

Answer: C

Explanation:
A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation.
Incorrect Answers:
A: Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
B: Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
D: A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 657:

Which of the following processes has a date which identifies when a key is no longer valid?

A. Key generation.
B. Key storage and distribution.
C. Key escrow.
D. Key expiration.

Answer: D

Explanation:
A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
Incorrect Answers:
A: Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
B: Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
C: A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 658:

Which of the following statements suits the process of Key generation?

A. Is the most important and first step in the process of working with keys and certificates.
B. It is how keys are stored affects how they are distributed.
C. Stores keys for the purpose of law enforcement access.
D. It has a date which identifies when a key is no longer valid.

Answer: A

Explanation:
Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of

the system in use.
Incorrect Answers:
B: Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
C: A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation.
D: A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 659:

Which of the following statements suits the process of Key storage and distribution?

A. Is the most important and first step in the process of working with keys and certificates.
B. It is how keys are stored affects how they are distributed.
C. Stores keys for the purpose of law enforcement access.
D. It has a date which identifies when a key is no longer valid.

Answer: B

Explanation:
Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
Incorrect Answers:
A: Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
C: A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation.
D: A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or

certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 660:

Which of the following statements suits the process of Key escrow?

A. Is the most important and first step in the process of working with keys and certificates.
B. It is how keys are stored affects how they are distributed.
C. Stores keys for the purpose of law enforcement access.
D. It has a date which identifies when a key is no longer valid.

Answer: C

Explanation:
A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation.
Incorrect Answers:
A:
Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
B: Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
D: A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 661:

Which of the following statements suits the process of Key expiration?

A. Is the most important and first step in the process of working with keys and

certificates.
B. It is how keys are stored affects how they are distributed.
C. Stores keys for the purpose of law enforcement access.
D. It has a date which identifies when a key is no longer valid.

Answer: D

Explanation:
A key expiration date identifies when a key is no longer valid. Normally, a key is date stamped. This means that it becomes unusable after a specified date. A new key or certificate is normally issued before the expiration date. Keys with expiration dates work similarly to credit cards that expire.
Incorrect Answers:
A: Key generation (creating the key) is an important first step in the process of working with keys and certificates. Certificates are one of the primary methods used to deliver keys to end entities. Key length and the method used to create the key also affect the security of the system in use.
B:
Where and how keys are stored affects how they are distributed. Distributing keys is usually accomplished using a Key Distribution Center (KDC), as used in Kerberos, or by using a Key Exchange Algorithm (KEA), as in the case of PKI.
C: A key escrow system stores keys for the purpose of law enforcement access. If a criminal investigation is underway, law enforcement agents, with a search warrant, have the right to access and search records within the scope of the warrant. In general, the key archival system will provide the access needed. Key escrow is listed separately because the usage is peculiar to a law enforcement investigation.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 662:

Which of the following processes are being referred to when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur?

A. Key revocation.
B. Key suspension.
C. Recovering and archiving keys.
D. Renewing keys.

Answer: A

Explanation:
Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur.

Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
Incorrect Answers:
B: A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
C:
One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage
D: Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 663:

Which of the following processes are being referred to if an employee were to take a leave of absence, the employee's key is held in safety until his return?

A. Key revocation.
B. Key suspension.
C. Recovering and archiving keys.
D. Renewing keys.

Answer: B

Explanation:
A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
Incorrect Answers:
A: Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be

invalid or possibly compromised. The credit card analogy is applicable here too.
C:
One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage
D: Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 664:

Which of the following processes are being referred to if a key-based system is that older information, unless processed with a new key, may become inaccessible?

A. Key revocation.
B. Key suspension.
C. Recovering and archiving keys.
D. Renewing keys.

Answer: C

Explanation:
One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage.
Incorrect Answers:
A: Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
B: A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.

D: Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 665:

Which of the following processes are being referred to if a process of enabling a key for use after its scheduled expiration date?

A. Key revocation.
B. Key suspension.
C. Recovering and archiving keys.
D. Renewing keys.

Answer: D

Explanation:
Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover.
Incorrect Answers:
A: Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
B:
A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
C: One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 666:

Which of the following statements suits the process of Key revocation?

A. Keys compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur.
B. If an employee were to take a leave of absence, the employee's key is held in safety until his return.
C. If a key-based system is that older information, unless processed with a new key, may become inaccessible.
D. If a process of enabling a key for use after its scheduled expiration date.

Answer: A

Explanation:
Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
Incorrect Answers:
B:
A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
C: One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage.
D: Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 667:

Which of the following statements suits the process of Key suspension?

A. Keys compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur.
B. If an employee were to take a leave of absence, the employee's key is held in safety until his return.
C. If a key-based system is that older information, unless processed with a new key, may become inaccessible.
D. If a process of enabling a key for use after its scheduled expiration date.

Answer: B

Explanation:
A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
Incorrect Answers:
A: Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
C: One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage.
D: Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 668:

Which of the following statements suits the process of Recovering and archiving keys?

A. Keys compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur.
B. If an employee were to take a leave of absence, the employee's key is held in safety until his return.
C. If a key-based system is that older information, unless processed with a new key, may

become inaccessible.
D. If a process of enabling a key for use after its scheduled expiration date.

Answer: C

Explanation:
One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage.
Incorrect Answers:
A: Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
B: A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
D: Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 669:

Which of the following statements suits the process of Renewing keys?

A. Keys compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur.
B. If an employee were to take a leave of absence, the employee's key is held in safety until his return.
C. If a key-based system is that older information, unless processed with a new key, may become inaccessible.
D. If a process of enabling a key for use after its scheduled expiration date.

Answer: D

Explanation:

Key renewal defines the process of enabling a key for use after its scheduled expiration date. A key would be reissued for a certain time in this situation. This process is called a key rollover. In most cases, the rollover of keys is something that occurs for a given time frame. Many systems provide a way to renew existing keys, rather than a rollover.
Incorrect Answers:
A: Keys are revoked when they are compromised, the authentication process has malfunctioned, when people are transferred, and when many other security risks occur. Revoking a key keeps it from being misused. A revoked key must be assumed to be invalid or possibly compromised. The credit card analogy is applicable here too.
B: A key suspension is a temporary situation. If an employee were to take a leave of absence, the employee's key could be suspended until they came back to work. This temporary suspension would ensure that the key would not be usable during their absence. A suspension might also occur if a high number of failed authentications or other unusual activities were occurring.
C: One of the problems with a key-based system is that older information, unless processed with a new key, may become inaccessible. If for example, you have a two-year-old file on your system and it is still encrypted, will you remember which key was used to encrypt it two years ago? If you are like most people, you won't. If you can't decrypt the data, it is useless. To deal with this problem, archiving old keys is essential. This is most easily done on a server that offers secure storage.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2002, pp 373-386.

QUESTION 670:

Choose the type of encryption keys used to verify a digital signature.

A. The public key of the signer.
B. The private key of the signer.
C. The public key of the recipient.
D. The private key of the recipient.

Answer: A

Explanation:
A digital signature validates the authenticity of the message by verifying the source of the message. This is known as non-repudiation. The digital signature also ensures that the message was not altered in transit by using hashing. The sender or signer uses his or her private key to hash the message. Once the recipient receives the message he or she uses the signer's public key to verify the hash.
Incorrect Answers:
B: The signer's private key is used to sign the message. It never leaves the possession of the signer ; hence it is referred to as the private key
C, D: The same key pair must be used to validate the message. Since the signer uses his own private key to sign the message, the recipient must use the signer's public key to

verify it. The sender cannot use the recipient's key to sign the message as this would not prove the identity of the sender.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 515-516.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION 671:

Choose the entity that provides authenticated keying material for forming security associations through a secure process.

A. ISAKMP (Internet Security Association and Key Management Protocol)
B. ESP (Encapsulating Security Payload)
C. SSH (Secure Shell)
D. SKEME (Secure Key Exchange Mechanism)

Answer: A

Explanation:
IPSec uses (ISAKMP) as its security association manager. It is used to negotiate and provide authenticated keying material for security associations in a secured manner.
Incorrect Answers:
B: IPSec uses ESP to provide data encryption to ensure the authenticity and integrity of the data payload.
C:
SSH is used to secure access to remote systems and replaces the standard Telnet, rlogin, rsh, and rcp commands. It uses public key cryptography to provide session encryption.
D: There is not such thing as SKEME.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 118, 120, 121-122.

QUESTION 672:

On the topic of non-repudiation, which uses distinct key pairs to differentiate between confidentiality services and integrity services?

A. A discrete key pair.
B. A dual key pair.
C. Key escrow.
D. A foreign key.

Answer: B

Explanation:
Dual key pair support is critical for applications that utilize both encryption and digital signatures. An end user needs one key pair for encryption and another for digital signing so that the encryption key pair can be backed up without compromising the integrity of the user's digital signatures.
Incorrect Answers:
A: There is no such thing as a discrete key pair.
C: Key escrow is used for recovery purposes. It is a storage process by which copies of private keys and/or secret keys are retained by a centralized management system as a means of insurance or recovery in the event of a disaster.
D: A foreign key is used in relational databases to ensure the integrity of data in the database. It is not used to provide network security.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 553-554.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 138.
http://www.verisign.com/products-services/security-services/pki/pki-security/public-key-infrastructure/

QUESTION 673:

You want to ensure that an e-mail message can only be read by its intended recipient. What must be used to encrypt the e-mail message?

A. The public key of the recipient.
B. The private key of the recipient.
C. The public key of the sender.
D. The private key of the sender.

Answer: A

Explanation:
Ensuring that only the intended recipient can read an e-mail message is referred to as authenticating the recipient. To authenticate the recipient in private/public key cryptography, the sender must use the recipient's public key to encrypt message. This forces authentication of the recipient as only the recipient can posses the corresponding private key to decrypt the message.
Incorrect Answers:
B: The sender cannot be in possession of the recipient's private key as a private key never leaves the possession of its owner. Therefore the sender cannot use the recipient's private key to encrypt the message.
C, D: The sender's private key can be used to hash the message so as to allow the recipient to use the sender's public key to verify the identity of the sender. This authenticates the sender, not the recipient.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 127.

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 515-516.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION 674:

The lifespan of a public key certificate and its connected keys are determined by a number of factors. What is it?
What two common methods can be used to maintain access to network servers?

A. ACL and PGP.
B. PIM and CRL.
C. CRL and OCSP.
D. RSA and MD2

Answer: C

Explanation:
CRL and OCSP are used in certificate revocation. This process begins when the CA is notified that a particular certificate needs to be revoked. The CA marks the certificate as revoked by publishing it in the certificate revocation list (CRL). The information is published in the CRL and becomes available using the Online Certificate Status Protocol (OCSP).
Incorrect Answers:
A: An access control list (ACL) is used to control access to network resources for authenticated users and does not require the implementation of a PKI while Pretty Good Privacy (PGP) is uses to provide security for e-mail messages.
B: Certificate revocation lists (CRLs) are used in PKI but not Protocol Independent Multicasting (PIM), which is a routing protocol.
D: RSA and MD5 are encryption algorithms used to encrypt data transmissions.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 124, 216, 292-292, 294, 305-306.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 128-135, 393, 540-541.

QUESTION 675:

The lifespan of a public key certificate and its connected keys are determined by a number of factors. What is it?

A. The value or importance of the information being protected.
B. The management fees.
C. The length of the asymmetric hash.
D. The data being openly available on the PKI system.

Answer: A
As with passwords, the longer a certificate key is used, the greater is the possibility that it would be compromised. Therefore certificates have an expiration date or lifespan. Upon reaching the expiration date, the certificate will no longer be valid.
Incorrect Answers:
B: Security should be of greater concern than cost.
C: Certificates have key lengths not hash lengths.
D: Data is not openly available on the PKI system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 344.

QUESTION 676:

Choose the terminology used to refer to a pervasive system whose services are implemented through using public key technologies.

A. Public key cryptography scheme.
B. Public key distribution authority.
C. Public key exchange.
D. Public key infrastructure.

Answer: D

Explanation:
The PKI is a system that provides for exchange of data over a network, by way of a secure asymmetric key system. The most popular companies that do this are VeriSign and Thwate.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 532-534.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 300-301.

QUESTION 677:

Choose the option that describes the main factor of centralized key management systems

A. All keys must be distributed securely and stored securely
B. All certificates must be made readily available.
C. Users must be able to publicly access the key repository.
D. Certificate contents must confidential.

Answer: A

Explanation:
If all the keys are stored in one place, under the watch of a limited number of people; the more a hacker will have to gain by infiltrating that particular key depository, and the more financial incentive he'll have to stage an elaborate attack, including social engineering to capitalize on the volume of a centralized facility.
Incorrect Answers:
B: Although certificates must be accessible to users who need to validate a owner of a certificates identity, this is not the primary concern of a PKI system. The security of the keys is more important. As soon as keys are compromised, the entire system fails.
C: Keys must be secure at all times. Making the key repository publicly accessible will compromise the keys stored there.
D: Certificates are used to identify a user's public key. This information cannot be kept confidential.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 532-534.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 300-301.

QUESTION 678:

If a recipient wants to verify a digital signature, what must be used in conjunction with the hash value?

A. The private key of the signer.
B. The private key of the receiver.
C. The public key of the signer.
D. The public key of the receiver.

Answer: C

Explanation:
A digital signature validates the authenticity of the message by verifying the source of the message. This is known as non-repudiation. The digital signature also ensures that the message was not altered in transit by using hashing. The sender or signer uses his or her private key to hash the message. Once the recipient receives the message he or she uses the signer's public key to verify the hash.
Incorrect Answers:
A: The signer's private key is used to sign the message. It never leaves the possession of the signer; hence it is referred to as the private key.
B, D: The same key pair must be used to validate the message. Since the signer uses his own private key to sign the message, the receiver must use the signer's public key to verify it. The sender cannot use the receiver's key to sign the message as this would not prove the identity of the sender.
References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 515-516.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 297.

QUESTION 679:

Which public key infrastructure model uses a CA (Certificate Authority) to issue and revoke certificates?

A. The managed model.
B. The distributed model.
C. The centralized model.
D. The standard model.

Answer: C

Explanation:
In centralized key management the certificate authority has complete control over the entire process. Many users aren't comfortable with someone else having access to their private keys, and don't feel personally secure with this solution.
Incorrect Answers:
A, B, D: The only PKI models are the centralized model and the hierarchical model.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 533-534.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 301-302.

QUESTION 680:

You work as the security administrator at Certkiller .com. You want to ensure that keys used in your cryptographic system, which are no longer needed, are destroyed. How should you dispose of these keys?

A. Keys should be stored and destroyed in a secure manner.
B. Keys deleted from storage.
C. Keys should be recycled.
D. Keys should be submitted to a key repository.

Answer: A

Explanation:
PKI keys should remain secure at all times. If a key is no longer required, it should be taken out of usage and stored securely, or it should be destroyed.
Incorrect Answers:

B: Deleting a key from the system's storage mechanism does not ensure that the key is secure. The key may still be on the user's computer where is would be vulnerable.
C: Keys are not recycled. They are issued to a specific user and are used to identify that user as the author of a document.
D: A key repository is an escrow system that is used to restore a key in case of a disaster. It does not ensure that the key will be taken out of use.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 342, 344-345.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 556, 560.

QUESTION 681:

Choose the type of keys stored within a digital certificate.

A. Public keys.
B. Private keys.
C. Hashing keys.
D. Session keys.

Answer: A

Explanation:
Digital certificates contain public keys, so that the public can verify authenticity.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 118, 121-122.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 227.

QUESTION 682:

A multiple barrier system implies that multiple physical barriers should be used to physically deter intruders from accessing the company premises. A minimum of three physical barriers should be used. Which physical barrier should be secured, monitored and protected by alarm systems?

A. External entrance to the building/perimeter.
B. Entrance to the computer center.
C. Entrance to the computer room
D. All of the above

Answer: D

Explanation:

Each of these physical barriers should be secured, monitored and protected by alarm systems. The perimeter should be protected by external walls, surveillance, and burglar alarms. Networking devices such as routers, and servers that contain mission-critical data should be stored in a secured computer center. The entrances to your computer center should be individually secured and monitored.
Incorrect Answers:
A, B, C: Each physical barrier should be secured and monitored.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 238 - 239.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 683:

Which type of security mechanism has bullet-proof glass, high-strength doors, and locks; and is designed to physically contain an unauthorized between its doors?

A. Mantrap.
B. Security zone.
C. Perimeter security.
D. None of the above.

Answer: A

Explanation:
A mantrap has bullet-proof glass, high-strength doors, and locks; and is designed to physically contain an unauthorized individual between its doors. The mantrap can hold an unauthorized individual between its doors until security officials can deal with the offender.
Incorrect Answers:
B: A security zone is an area within the company's building where access is controlled.
C: Perimeter security refers to implementing measures that prevent unauthorized access to the company premises and equipment.
D: Mantrap is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 237 - 239.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 684:

With regard to implementing physical barriers to secure the company premises and

network devices from intruders and theft, what is the minimum number of barriers that should be implemented?

A. One barrier system.
B. Two barrier system
C. Three barrier system
D. Four barrier system

Answer: C

Explanation:
A minimum of three physical barriers should be used to secure the company premises and network devices from intruders and theft. Each barrier should be secured, monitored and protected by alarm systems. In a three barrier system, securing the entrance to the building is the first barrier, securing the entrance to the computer center is the second barrier, and securing the entrance to the computer room is the third barrier.
Incorrect Answers:
A, B: The minimum recommended number of physical barriers to implement is three.
D: Implementing more than three physical barriers to secure your premises and networking equipment would provide more security.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 238 - 239.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 685:

Of the different motion detectors that can be used inside and outside the company's building, which only works well at non-daylight times when being used externally?

A. Light-based motion detectors.
B. Sound-based sensors.
C. Ultrasonic sensors.
D. Infrared and heat-based motion sensors.

Answer: D

Explanation:
Infrared and heat-based motion sensors only work at night. These sensors are usually used to monitor very small areas - windows, and doorways.
Incorrect Answers:
A: Light-based motion detectors generate a beam of light over the physical area that should be protected, and works with a photosensitive receiver. This visible light creates

the deterrent. When an object blocks the beam of light, an alarm will be sound.
B: Sound-based sensors are usually used inside a building.
C: Ultrasonic sensors send a small ultra-high frequency wave. Both the transmitter and receiver are usually in one device.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 686:

To control access to a secure area, a variety of lock types can be implemented to serve as a deterrent to intruders. Which lock type works on a punch code entry system?

A. Wireless systems.
B. Cipher lock type.
C. Swipe card lock type.
D. Biometric technologies.

Answer: D

Explanation:
Cipher locks work on a punch code entry system to keep unauthorized individuals from accessing the company premises and network devices.
Incorrect Answers:
A: Wireless systems use a card or token. A person wanting to enter the premises keeps the card or token to the receiver. The receiver then checks the information on the card and either allows or denies access.
C: With swipe cards, the individual has to insert or swipe a card to access the premises. Based on the information on the card, the door either opens, or remains shut.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 687:

Biometric authentication devices make use of different characteristics to identify individuals. Which biometric method involves the scanning and matching of a thumbprint or fingerprint?

A. Hand/palm geometry
B. Fingerprint matching
C. Voiceprint

A. Facial geometry

Answer: B

Explanation:
Fingerprint matching involves the scanning and matching of a thumbprint or fingerprint, and is the older biometric method used these days. Fingerprint scans are still popular these days because the fingerprints of an individual are unique
Incorrect Answers:
A: Hand/palm geometry involves a scan of the hand or palm shape of an individual. Unique hand shape characteristics such as length, thickness, and curvature of fingers are used to verify an individual's identity.
C: Voiceprint uses the voice of an individual to verify an individual's identity. This is one of the more complex biometric functions. A weakness of this method is that is easy to spoof with recordings.
D: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 688:

Which biometric method involves using the iris pattern of the eyeball for verification and identification of an individual?

A. Iris scan.
B. Retina scan.
C. Facial geometry
D. None of the above

Answer: A

Explanation:
The iris scan method uses the iris pattern of the eyeball to identify an individual. This biometric method is both easy to use and noninvasive.
Incorrect Answers:
B:

The retina scan uses the blood vessel pattern at the back of the eye to verify the identity of an individual. This method is more accurate than virtually any other biometric technology.
C: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.
D: The iris scan method is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 689:

Which of the following lock types provides the highest level of security and reliability when it comes to securing access and serving as a deterrent to intruders?

A. Wireless systems
B. Cipher lock type
C. Swipe card lock type
D. Biometric technologies

Answer: D

Explanation:
Biometric technologies provide the most secure form of authenticating identities of individuals because it uses a unique biological trait to identify a person.
Incorrect Answers:
A: Wireless systems use a card or token. A person wanting to enter the premises keeps the card or token to the receiver. The receiver then checks the information on the card and either allows or denies access.
B: Cipher locks work on a punch code entry system to keep unauthorized individuals from accessing the company premises and network devices.
C: With a swipe card, the individual has to insert or swipe a card to access the premises. Based on the information on the card, the door either opens, or remains close.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 690:

Which of the following biometric methods is considered a more complex biometric function, but is also easier to spoof than the other listed methods?

A. Hand/palm geometry
B. Fingerprint matching
C. Voice print
D. Facial geometry

Answer: C

Explanation:
Voiceprint uses the voice of an individual to verify an individual's identity. This is one of the more complex biometric functions. A weakness of this method is that is easier to spoof through recordings that the other biometric methods.
Incorrect Answers:
A: Hand/palm geometry involves a scan of the hand or palm shape of an individual. Unique hand shape characteristics such as length, thickness, and curvature of fingers are used to verify an individual's identity.
B: Fingerprint matching involves the scanning and matching of a thumbprint or fingerprint, and is the older biometric method used these days. Fingerprint scans are still popular because the fingerprints of an individual are unique.
D: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 691:

Which form of social engineering occurs when an intruder holds the door for an authorized individual after he/she opened it, and then slips in before the door closes?

A. Piggybacking.
B. Impersonation
C. Talking
D. None of the above

Answer: A

Explanation:
Piggybacking, impersonation, and talking are all forms of social engineering. Social engineering occurs when intruders gain access to the company's premises and network devices by exploiting the trusting instinct of authorized employees. Piggybacking occurs when an intruder holds the door for an authorized individual after he/she opened it, and then slips in before the door closes.
Incorrect Answers:
B: Impersonation occurs when an intruder masquerades as a repair technician, company guest, or maintenance worker in an attempt to gain access into the company's premises.
C: Talking is a form of social engineering where the intruder makes excuses such as losing his/her entry badge, leaving keys behind, or simply not understanding the access system to gain access to the building.
D: Piggybacking is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243 - 244.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 692:

Which one of the following biometric methods is one of the older, more poplar methods?

A. Hand/palm geometry
B. Fingerprint matching
C. Voice print
D. Facial geometry

Answer: B

Explanation:
Fingerprint matching involves the scanning and matching of a thumbprint or fingerprint, and is the older biometric method used these days. Fingerprint scans are still popular these days because the fingerprints of an individual remain unique.
Incorrect Answers:
A: Hand/palm geometry involves a scan of the hand or palm shape of an individual. Unique hand shape characteristics such as length, thickness, and curvature of fingers are used to verify an individual's identity.
C: Voiceprint uses the voice of an individual to verify an individual's identity. This is one of the more complex biometric functions. A weakness of this method is that is easy to spoof.
D: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 693:

Which of the following methods is a form of social engineering?

A. Piggybacking.
B. Impersonation
C. Talking
D. A and B
E. All of the above

Answer: E

Explanation:
Piggybacking, impersonation and talking are all forms of social engineering. Social engineering occurs when intruders gain access to the company's premises and network devices by exploiting the trusting instinct of people. Piggybacking occurs when an intruder holds the door for an authorized individual after he/she opened it, and then slips in before the door closes. Impersonation occurs when an intruder masquerades as a repair technician, company guest, or maintenance worker to attempt to gain access into the company's premises. Talking is a form of social engineering where the intruder makes excuses such as losing his/her entry badge, leaving keys behind, or simply not understanding the access system to gain access to the building.
Incorrect Answers:
A, B, C, D: These options only represent part of the complete answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243 - 244.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 694:

Power conditioner devices can include a number of the elements. Choose the correct option.

A. Filters.

B. Surge suppressors.
C. Temporary voltage regulation.
D. Capable of activating backup power supplies.
E. All of the above.

Answer: E

Explanation:
Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies, and can include filters, surge suppressors, and temporary voltage regulation.
Incorrect Answers:
A, B, C, D: These options present only part of the complete correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 695:

Which biometric method is considered the more accurate biometric technology?

A. Iris scan.
B. Retina scan.
C. Facial geometry
D. None of the above

Answer: B

Explanation:
The retina scan uses the blood vessel pattern at the back of the eye to verify the identity of an individual. This method is more accurate than virtually any other biometric technology. Here, an individual has to look into an infrared light that shines through the eyeball.
Incorrect Answers:
A: The iris scan method uses the iris pattern of the eyeball to identify an individual. This biometric method is both easy to use and noninvasive.
C: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.
D: The retina scan method is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.

Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 696:

Which method of social engineering occurs when an intruder masquerades as a repair technician, company guest, or maintenance worker to attempt to gain access into the company's premises?

A. Piggybacking.
B. Impersonation
C. Talking
D. None of the above

Answer: B

Explanation:
Impersonation occurs when intruder masquerades as a repair technician, company guest, or maintenance worker to attempt to gain access into the company's premises.
Incorrect Answers:
A: Piggybacking occurs when an intruder holds the door for an authorized individual after he/she opened it, and then slips in before the door closes.
C: Talking is a form of social engineering where the intruder makes excuses such as losing his/her entry badge, leaving keys behind, or simply not understanding the access system to gain access to the building.
D: Impersonation is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243 - 244.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 697:

Most of the fire suppression systems work on a concept where if any of three critical components of a fire are removed, a fire cannot be caused. Which of the following components is FALSE?

A. Heat and fuel
B. Oxygen
C. Water
D. Oxygen and water

Answer: C

Explanation:
The critical components of a fire are oxygen, heat, and fuel. When you remove any of these components, a fire cannot be caused. Water is not one of these components.
Incorrect Answers:
A: Heat and fuel are two critical components of a fire.
B: Oxygen is a one of the critical components of a fire.
D: While oxygen is a critical component of a fire, water is not.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 698:

Which type of power system product must you use if you need to provide a continuous power supply in power loss situations?

A. Power conditioners
B. Surge protectors
C. Backup power technologies
D. None of the above

Answer: C

Explanation:
Backup power systems are used when a continuous power supply is needed in power loss situations. Backup power systems are used either for short-term usage or long-term usage. Power generators are activated when a loss in power is detected. An Uninterruptible Power Supply (UPS) system is a backup power system that utilizes batteries to provide short-term power when a power loss is detected.
Incorrect Answers:
A: Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.
B: Surge protectors are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground.
D: Backup power systems is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex,

Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 699:

If you want to use the voice of an individual to verify identity, which biometric method would you have to implement?

A. Hand/palm geometry
B. Fingerprint matching
C. Voice print
D. Facial geometry

Answer: C

Explanation:
Voiceprint uses the voice of an individual to verify an individual's identity. This is one of the more complex biometric functions. A weakness of this method is that is easier to spoof through recordings.
Incorrect Answers:
A: The hand/palm geometry method involves a scan of the hand or palm shape of an individual. Unique hand shape characteristics such as length, thickness, and curvature of fingers are used to verify an individual's identity.
B: Fingerprint matching involves the scanning and matching of a thumbprint or fingerprint, and is the older biometric method used these days. Fingerprint scans are still popular these days because the fingerprints of an individual are unique.
D: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 700:

To keep the electrical service constant and to offer assistance for solving most electrical line problems, power system products can be used. Which type of power system product monitors and regulates the power in the building?

A. Power conditioners

B. Surge protectors
C. Backup power technologies
D. Uninterruptible Power Supply (UPS) system

Answer: A

Explanation:
Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.
Incorrect Answers:
B: Surge protectors are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground.
C: Backup power systems are used when a continuous power supply is needed in power loss situations. Backup power systems are used either for short-term usage or long-term usage. Power generators are activated when a loss in power is detected.
D: An Uninterruptible Power Supply (UPS) system is a backup power system that utilizes batteries to provide short-term power when a power loss is detected.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 701:

If you want to use the unique hand shape characteristics such as length, thickness, and curvature of fingers of an individual, to verify identity; which biometric method would you have to implement?

A. Hand/palm geometry
B. Fingerprint matching
C. Voice print
D. Facial geometry

Answer: A

Explanation:
The hand/palm geometry biometric method involves a scan of the hand or palm shape of an individual. Unique hand shape characteristics such as length, thickness, and curvature of fingers are used to verify an individual's identity
Incorrect Answers:
B: Fingerprint matching involves the scanning and matching of a thumbprint or

fingerprint. Fingerprint scans are still popular these days because the fingerprints of an individual are unique.
C: Voiceprint uses the voice of an individual to verify an individual's identity. This is one of the more complex biometric functions. A weakness of this method is that is easier to spoof using recordings.
D: Facial geometry identifies an individual by his/her facial characteristics. The weakness of this method is that it is not as accurate as fingerprint matching.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 243.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 702:

Which type of power system product consists of passive devices that are used to protect electrical components from spikes in the power line?

A. Power conditioners
B. Surge protectors
C. Backup power technologies
D. Uninterruptible Power Supply (UPS) system

Answer: B

Explanation:
Surge protectors are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground.
Incorrect Answers:
A: Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.
C: Backup power systems are used when a continuous power supply is needed in power loss situations. Backup power systems are used either for short-term usage or long-term usage. Power generators are activated when a loss in power is detected.
D: An Uninterruptible Power Supply (UPS) system is a backup power system that utilizes batteries to provide short-term power when a power loss is detected.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 703:

Which of the characteristics here are FALSE for a gas-based fire-suppression system?

A. Attempts to remove the oxygen component of a fire.
B. To remove oxygen, gas-based systems use carbon dioxide.
C. Can result in damage to energized electrical equipment - computers.
D. Can suffocate anybody that remains in the room.

Answer: C

Explanation:
Water-based fire-suppression systems can cause great damage to computers.
Incorrect Answers:
A, B, D: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 704:

When using surge protectors, what capability are you providing for with regard to power systems?

A. You want to ensure that the electrical service remains constant, and want the power in the building regulated and monitored.
B. You want to protect electrical components from spikes in the power line.
C. You want to provide for a continuous power supply in the event of power loss situations.
D. None of the above

Answer: B

Explanation:
Surge protectors are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground.
Incorrect Answers:

A: Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.
C: Backup power systems are used when a continuous power supply is needed in power loss situations. Backup power systems are used either for short-term usage or long-term usage. Power generators are activated when a loss in power is detected. An Uninterruptible Power Supply (UPS) system is a backup power system that utilizes batteries to provide short-term power when a power loss is detected.
D: B is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 705:

A water-based fire-suppression system attempts to remove two of the required critical components of a fire. Choose the correct combination.

A. Heat and fuel
B. Oxygen and heat
C. Fuel and heat
D. Oxygen and fuel

Answer: B

Explanation:
A water-based fire-suppression system attempts to remove two of the required critical components of a fire, namely oxygen and heat.
Incorrect Answers:
A, C, D: These options represent the incorrect combinations.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 706:

When using power conditioner devices, what capability are you providing for with regard to power systems?

A. You want to ensure that the electrical service remains constant, and want the power in the building regulated and monitored.
B. You want to protect electrical components from spikes in the power line
C. You want to provide for a continuous power supply in the event of power loss situations.
D. None of the above

Answer: A

Explanation:
Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.
Incorrect Answers:
B: Surge protectors are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground.
C:
Backup power systems are used when a continuous power supply is needed in power loss situations. Backup power systems are used either for short-term usage or long-term usage. Power generators are activated when a loss in power is detected. An Uninterruptible Power Supply (UPS) system is a backup power system that utilizes batteries to provide short-term power when a power loss is detected.
D: A is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 707:

A gas-based fire-suppression system attempts to remove one of the required critical components of a fire. Choose the correct answer.

A. Heat
B. Oxygen
C. Fuel
D. All of the above

Answer: B

Explanation:

A gas-based fire-suppression system attempts to remove one of the required critical components of a fire, namely oxygen.
Incorrect Answers:
A, C: A water-based fire-suppression system attempts to remove two of the required critical components of a fire, namely fuel and heat.
D: B is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 708:

When using backup power systems, what capability are you providing for with regard to power systems?

A. You want to ensure that the electrical service remains constant, and want the power in the building regulated and monitored.
B. You want to protect electrical components from spikes in the power line
C. You want to provide for a continuous power supply in the event of power loss situations.
D. None of the above

Answer: C

Explanation:
Backup power systems are used when a continuous power supply is needed in power loss situations. Backup power systems are used either for short-term usage or long-term usage. Power generators are activated when a loss in power is detected. An Uninterruptible Power Supply (UPS) system is a backup power system that utilizes batteries to provide short-term power when a power loss is detected.
Incorrect Answers:
A: Power conditioner devices assist in keeping the electrical service constant by monitoring and regulating the power in the building. These devices can activate backup power supplies.
B: Surge protectors are passive devices that are used to protect electrical components from spikes in the power line. Surge protectors usually utilize Metal Oxide Varistors (MOVs) to shunt the voltage spike to ground
D: C is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 249.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press,

Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 709:

Which of the characteristics here are FALSE for a water-based fire-suppression system?

A. Easy to maintain.
B. Can result in damage to energized electrical equipment - computers.
C. Reliable and inexpensive.
D. Requires sealed environments to operate.

Answer: D

Explanation:
Gas-based fire-suppression systems require sealed environments to operate
Incorrect Answers:
A, B, C: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 710:

Which type of fire can reoccur quite quickly if the voltage is not removed?

A. Wood and paper fire
B. Electrical fire
C. Flammable liquids fire.
D. Flammable metals fire.

Answer: B

Explanation:
An electrical fire can reoccur quite quickly if the voltage is not removed. This is one of the bigger concerns with regard to electrical fires.
Incorrect Answers:
A, C, D: An electrical fire has voltage as a factor.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex,

Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 711:

Which type of fire suppression system can put out fires that involve different types of fuel?

A. A water-based fire suppression system
B. A gas-based fire suppression system
C. Both of the above

Answer: B

Explanation:
A gas-based fire suppression system can put out fires that involve different types of fuel. This includes wood, oil, metals, fabric, electrical, and chemical.
Incorrect Answers:
A: A water-based fire suppression system attempts to remove heat and fuel from a fire.
C: A gas-based fire suppression system is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, p 251 - 253.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 712:

Choose the access control principle that requires each user to have the most restricted privileges.

A. Principle of control permissions.
B. Principle of least privilege.
C. Principle of hierarchical permissions.
D. Access control modes.

Answer: B

Explanation:
The principle of least privilege states that every user should be granted the most restrictive level of access that would allow them to perform their work, and no more.

Incorrect Answers:
A: Access control permissions are used to grant users access to network resources. They are not access control principles.
C: Thereare no hierarchical permissions, though there is a hierarchical trust model, which refers to security certificates and is not an access control principle.
D: Access control modes are the methods used to ensure that users can only access resources that they are authorized to access.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 451-452.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 265.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 6.

QUESTION 713:

The Bell La-Padula access control model is made up of four elements. What is it?

A. Subjects, objects, access modes, security levels.
B. Subjects, objects, roles, groups.
C. Read only, read/write, write only, read/write/delete.
D. Groups, roles, access modes, security levels.

Answer: A

Explanation:
The Bell La-Padula access control model is designed to prevent unauthorized access to classified information and prevents users from accessing information that has a higher security rating than they are authorized to access. The model also prevents information from being written to a lower level of security.
In this model, the entities in a computer system are divided into abstract sets of subjects and objects. The system is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a specific security policy. In order to determine whether or not a specific access mode is allowed, the clearance of a subject is compared to the classification of the object, and a determination is made as to whether the subject is authorized for the specific access mode. The clearance/classification scheme is expressed in terms of a lattice.
With Bell-LaPadula, users can only create content at or above their own security level and can only view content at or below their own security level.
Incorrect Answers:
B: The Bell La-Padula access control model uses security levels, not groups or roles.
C: The Bell La-Padula access control model uses security levels, not permissions.
D: The Bell La-Padula access control model uses subjects and objects, not groups and roles.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda,

Sybex, 2004, p 267.
http://en.wikipedia.org/wiki/Bell-LaPadula_model
http://www.itsecurity.com/dictionary/bell.htm

QUESTION 714:

RBAC (Role Based Access Control) defines a specific relation between users, roles and operations. Choose the option that defines this relation.

A. Multiple users, single role, single operation.
B. Multiple users, single role, multiple operations.
C. Single user, single role, single operation.
D. Multiple users, multiple roles, multiple operations.

Answer: D

Explanation:
Access control using the RBAC model is based on the role or responsibilities users have in the organization. These roles usually reflect the organization's structure, such as its division into different departments, each with its distinct role in the organization. Users with the same responsibility and who perform the same functions in an organization are grouped together in one role. Each role are allowed the level of access required to perform the operations that comprises their responsibility within the organization.
Incorrect Answers:
A, B, C: RBAC is based on multiple users, multiple roles and multiple operations. With a single role, all users will have the same access levels.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 6.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 13.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 10.

QUESTION 715:

You work as the security administrator at Certkiller .com. One morning you discover that the office window, which is next to the computer room, has been broken. You immediately inform the owner of that specific office about the broken window so that he can have the window repaired.
You decide to not follow up on the window being repaired because it is not your office window.
Based on these events, choose the option that defines the probability of a threat associated with the vulnerability taking place.

A. Should the broken window be repaired, the probability of the threat taking place will increase.

B. Should the broken window be repaired, the probability of the threat taking place will stay the same.
C. Should the broken window not be repaired, the probability of the threat taking place will decrease.
D. Should the broken window not be repaired, the probability of the threat taking place will increase.

Answer: D

Explanation:
If the window is not repaired, the threat that someone may use it to gain access will increase as more people become aware of the vulnerability.
Incorrect Answers:
A: Having the windows repaired would not increase the threat; instead, the threat will be reduced.
B: Having the windows repaired would reduce the threat. Thus the threat will not remain constant.
C: If the window is not repaired, the threat will increase as more people become aware of the vulnerability. It will not decrease.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 5.

QUESTION 716:

Choose the device that does not make use of smart cards.

A. CD players.
B. Cell phones.
C. Satellite cards.
D. Handheld computers.

Answer: A

Explanation:
CD players do not have security features and would not require the use of a Smart card.
Incorrect Answers:
B, D: Smart cards are usually used in mobile devices such as cell phones, hand held computers, and laptops. They are used to authenticate the user to the mobile device.
C: Satellite cards use smart card technology to authenticate the user.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 6, 17, 300-301.

QUESTION 717:

You work as the security administrator at Certkiller .com. Certkiller .com has headquarters in London and branch offices in Paris, Berlin, Milan and Madrid. The London headquarters and four branch offices are connected using fast links.
A new Certkiller .com security policy requires that each company premises must have security measures implemented. All employees must always wear their identification badges and all visitors are required to sign in.
You must ensure that all servers and networking devices are physically secure. You must implement the best security measures possible and at the lowest possible cost.
How will you accomplish the task?

A. Place all servers and networking devices in a single server room at the London headquarters premises. Implement the appropriate security measures to secure the server room.
B. Place most servers and networking devices in a single server room at the London headquarters premises, and deploy some servers at each branch office. Implement the appropriate security measures to secure the server rooms.
C. Decentralize servers and networking devices, and then implement the appropriate security measures to secure the server rooms.
D. Place all servers and networking devices in a single server room at the London headquarters premises. Controls are already in place to prevent visitors from just walking into the building.

Answer: A

Explanation:
Placing all the servers along with the networking devices in one room would allow us to implement physical security measures to one room. This will provide the best level of security at the lowest cost and is viable because all Certkiller branch offices are connected with fast links.
Incorrect Answers:
B, C, D: We want to keep the cost of physically securing the servers and vital components at a minimum. This means keeping the number of locations that require securing to a minimum. Placing all the servers and vital components in one room meet this requirement.

QUESTION 718:

Choose the option that does NOT define a method for improving the physical security of workstations.

A. Use lockable cases, keyboards and removable media drives.
B. Use key or password protected setup and configuration.
C. Use passwords required to boot.
D. Use strong passwords.

Answer: D

Explanation:
Physical security refers to the physical access to the device. Strong passwords will not prevent physical access to the device.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 258

QUESTION 719:

You work as the security administrator at Certkiller .com. You want to implement a fire protection plan for the server room.
What should be included in your plan?

A. Processes for an emergency shutdown of computer equipment.
B. A sprinkler system that surpasses local code requirements.
C. Rules for using non-flammable materials.
D. Fireproof doors that open easily when the alarm is raised.

Answer: A

Explanation:
If there is a fire, the smart thing to do would be to perform an emergency system shutdown. Equipment that gets shut down properly will be less likely to spread the fire, and equipment that is shut down properly is more likely to preserve its data.
Incorrect Answers:
B: A computer room would contain sensitive electronic equipment which would be damaged by a sprinkler system. Furthermore, the water from a sprinkler system could cause an electrical short that could lead to secondary fires, loss of equipment and loss of data.
C: Although the use of non flammable materials in the computer room would be a good idea, smoke or heat from a nearby fire could still damage equipment.
D: Although fireproof doors can be used to contain a fire to one side of the fireproof door, they will not protect equipment in the computer room if the fire originates in that room. Furthermore, to effective contain the fire to one side of the fireproof door, it should remain closed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 248, 251-253.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 154-155.

QUESTION 720:

Which backup type performs a full, complete backup of all files on a server or disk, with the end result being a complete archive of the system at the specific time when the backup was performed?

A. Full backup
B. Incremental backup
C. Differential backup
D. Full backup and Incremental backup

Answer: A

Explanation:
A full backup provides a complete backup of all files on a server or disk, with the end result being a complete archive of the system at the specific time when the backup was performed. While the backup is being run, the system should not be used.
Incorrect Answers:
B:
An incremental backup is a partial backup. This backup type only backs up the information which has changed since the last full backup or incremental backup was performed. Incremental backups are smaller than full backups, and are also the fastest backup type to perform.
C: A differential backup has some similarities to an incremental backup. This backup type only backs up those files that have been modified since the last full backup was performed, and also makes copies of files that have not changed since the last differential backup. Differential backups tend to grow as the week progresses and no new full backup have been performed.
D: Only a full backup makes a complete backup of all files on a server or disk when it is run.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 368-369.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 721:

When drawing up your disaster recovery plan (DRP), several alternate site options exist. Which DRP option provides an alternate site that is up and available 24 hours a day, seven days a week, has the advantage of a very quick return to business, as well as the ability to test a disaster recovery plan without affecting current operations?

A. A hot site
B. A warm site
C. A cold site.
D. All of the above

Answer: A

Explanation:
A hot site is an alternate site that is up and available 24 hours a day, seven days a week, has the advantage of a very quick return to business, as well as the ability to test a DRP without affecting current operations. When setting up a hot site, you should ensure that this site is sufficiently far from the corporate facility being mirrored so that it does not get affected by the same damages. A hot site usually mirrors the configuration of the corporate facility.
Incorrect Answers:
B: A warm site provides a cheaper, scaled-down version of a hot site. A warm site usually only contains the power, phone, network ports, and other basic services required. When a disaster occurs at the corporate facility, additional effort is needed to bring the computers, data, and resources to the warm site.
C: A cold site is usually only made up of empty office space, electricity, and bathrooms. A cold site still needs networking equipment and complete configuration before it can operate when a disaster strikes the corporate facilities. This alternate site option is the cheapest.
D: A hot site is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 722:

Which backup method takes data from a hard drive, moves it to another system, and can store up to 17GB of data?

A. Magnetic tape back up
B. Disk imaging/mirroring method.
C. CD-ROM burning.
D. DVD-ROM burning.
E. Direct offsite, over the Web

Answer: D

Explanation:
DVD-ROM burning is a method of taking data from a hard drive and moving it to another system. DVDs can store up to 17GB of data.
Incorrect Answers:
A: The magnetic tape backup method is the easiest and cheapest backup method, and can also be automated.
B: The disk imaging or mirroring method is more intricate than the magnetic tape method. With disk imaging, disk duplication occurs from one disk to another disk, or by

using software that images the entire contents of the drive and then produces a file for offsite storage.
C: CD-ROM burning is the simpler method of taking data from a hard drive, and moving it to a write-once or write-many CD-ROM system.
E: With direct offsite backups, the company has to subscribe to a backup service, which then backs up the critical servers and data of the company.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 723:

Which backup type tends to grow as the week progresses and no new full backups have been performed?

A. Full backup
B. Incremental backup
C. Differential backup
D. All of the above

Answer: C

Explanation:
Differential backups tend to grow as the week progresses and no new full backups have been performed. A differential backup has some similarities to an incremental backup. This backup type only backs up those files that have been modified since the last full backup was performed, and also makes copies of files that have not changed since the last differential backup.
Incorrect Answers:
A: A full backup provides a complete backup of all files on a server or disk, with the end result being a complete archive of the system at the specific time when the backup was performed. While the backup is being run, the system should not be used.
B: An incremental backup is a partial backup. This backup type only backs up the information which has changed since the last full backup or incremental backup was performed. Incremental backups are smaller than full backups, and are also the fastest backup type to perform.
D: Differential backup is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 368-369.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 724:

Which alternate site option provides a site that is a scaled down version of a site that is available 24 hours a day, seven days a week?

A. A hot site
B. A warm site
C. A cold site.
D. All of the above

Answer: B

Explanation:
A warm site provides a cheaper, scaled-down version of a hot site. A warm site usually only contains the power, phone, network ports, and other base services required. When a disaster occurs at the corporate facility, additional effort is needed to bring the computers, data, and resources to the warm site.
Incorrect Answers:
A: A hot site is an alternate site that is up and available 24 hours a day, seven days a week, has the advantage of a very quick return to business, as well as the ability to test a DRP without affecting current operations. When setting up a hot site, you should ensure that this site is sufficiently far from the corporate facility being mirrored so that it does not get affected by the same damages. A hot site usually mirrors the configuration of the corporate facility.
C:
A cold site is usually only made up of empty office space, electricity, and bathrooms. A cold site still needs networking equipment and complete configuration before it can operate when a disaster strikes the corporate facilities. This DRP option is the cheapest.
D: A warm site is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 725:

There are numerous methods that you can use to perform a backup. Which backup method is the easiest, cheapest and can also be automated?

A. Magnetic tape back up
B. Disk imaging/mirroring method.
C. CD-ROM burning.
D. DVD-ROM burning.
E. Direct offsite, over the Web

Answer: A

Explanation:
The magnetic tape backup method is the easiest, cheapest backup method, and can also be automated.
Incorrect Answers:
B: The disk imaging or mirroring method is more intricate than the magnetic tape method. With disk imaging, disk duplication occurs from either one disk to another disk, or by using software that images the entire contents of the drive and then produces a file for offsite storage.
C: CD-ROM burning is the simpler method of taking data from a hard drive, and moving it to a write-once or write-many CD-ROM system.
D: DVD-ROM burning is a method of taking data from a hard drive and moving it to another location for storage. DVDs can store up to 17GB of data.
E: With direct offsite backups, the company has to subscribe to a backup service, which then backs up the critical servers and data of the company.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 726:

Which backup type is the fastest backup type to perform?

A. Full backup
B. Incremental backup
C. Differential backup
D. Incremental and differential backup

Answer: B

Explanation:
Incremental backups are smaller than full backups, and are also the fastest backup type to perform. This backup type only backs up the information which has changed since the last full backup or incremental backup was performed.
Incorrect Answers:
A: A full backup provides a complete backup of all files on a server or disk, with the end result being a complete archive of the system at the specific time when the backup was performed. While the backup is being run, the system should not be used.
C: A differential backup has some similarities to an incremental backup. This backup type backs up those files that have been modified since the last full backup was performed, and also makes copies of files that have not changed since the last differential backup. Differential backups tend to grow as the week progresses and no new full

backups have been performed.
D: Only the incremental backup type is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 368-369.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 727:

Which alternate site represents a compromise between a very expensive site and a site which is not preconfigured?

A. A hot site
B. A warm site
C. A cold site.
D. All of the above

Answer: B

Explanation:
A warm site is an alternate site solution that exists between a hot site and a cold site. The warm alternate site provides a cheaper, scaled-down version of a hot site. A warm site usually only contains the power, phone, network ports, and other base services required. When a disaster occurs at the corporate facility, additional effort is needed to bring the computers, data, and resources to the warm site.
Incorrect Answers:
A: A hot site is an alternate site that is up and available 24 hours a day, seven days a week, has the advantage of a very quick return to business, as well as the ability to test a DRP without affecting current operations. When setting up a hot site, you should ensure that this site is sufficiently far from the corporate facility being mirrored so that it does not get affected by the same damages. A hot site usually mirrors the configuration of the corporate facility.
C: A cold site is usually only made up of empty office space, electricity, and bathrooms. A cold site still needs networking equipment and complete configuration before it can operate when a disaster strikes the corporate facilities. This DRP option is the cheapest
D: A warm site is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 728:

Which backup method carries out disk duplication from either one disk to another disk, or by using software that images the entire contents of the drive and then produces a file for offsite storage?

A. Magnetic tape back up
B. Disk imaging/mirroring method.
C. CD-ROM burning.
D. DVD-ROM burning.
E. Direct offsite, over the Web

Answer: B

Explanation:
The disk imaging or mirroring method is more intricate than the magnetic tape backup method. With disk imaging, disk duplication occurs from either one disk to another disk, or using by software that images the entire contents of the drive and then produces a file for offsite storage.
Incorrect Answers:
A: The magnetic tape backup method is the easiest, cheapest and can also be automated.
C: CD-ROM burning is the simpler method of taking data from a hard drive, and moving it to a write-once or write-many CD-ROM system.
D: DVD-ROM burning is a method of taking data from a hard drive and moving it to another location for storage. DVDs can store up to 17GB of data.
E: With direct offsite backups, the company has to subscribe to a backup service, which then backs up the critical servers and data of the company.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 729:

Which type of storage mechanism, used to store data, consists of partial or full backups that are stored at the computer center for immediate recovery purposes, if necessary?

A. Working copies
B. Onsite storage
C. Offsite storage
D. All of the above

Answer: A

Explanation:
Working copies are partial or full backups that are stored at the computer center for immediate recovery purposes, if necessary.
Incorrect Answers:
B: Onsite storage refers to a location on the site of the computer center, which the company uses to store data locally. Onsite storage containers are used to store backup media. These onsite storage containers are classed according to fire, moisture, and pressure resistance.
C: Offsite storage refers to a location not at the site of the computer center, which the company uses to store data. Offsite storage involves keeping of the backup media at a remote site.
D: Working copies is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 365-366.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1

QUESTION 730:

Which DRP option is usually only made up of empty office space, electricity, and bathrooms?

A. A hot site
B. A warm site
C. A cold site.
D. All of the above

Answer: C

Explanation:
A cold site is usually only made up of empty office space, electricity, and bathrooms. A cold site still needs networking equipment and complete configuration before it can operate when a disaster strikes the corporate facilities. This DRP option is the cheapest.
Incorrect Answers:
A: A hot site is an alternate site that is up and available 24 hours a day, seven days a week, has the advantage of a very quick return to business, as well as the ability to test a DRP without affecting current operations. When setting up a hot site, you should ensure that this site is sufficiently far from the corporate facility being mirrored so that it does not get affected by the same damages. A hot site usually mirrors the configuration of the corporate facility.
B: A warm site provides a cheaper, scaled-down version of a hot site. A warm site usually only contains the power, phone, network ports, and other base services required. When a disaster occurs at the corporate facility, additional effort is needed to bring the computers, data, and resources to the warm site.
D: A cold site is the correct answer.

References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 731:

Which backup method involves the company having to subscribe to a backup service, which then backs up the critical servers and data of the company?

A. Magnetic tape back up
B. Disk imaging/mirroring method.
C. CD-ROM burning.
D. DVD-ROM burning.
E. Direct offsite, over the Web

Answer: E

Explanation:
With direct offsite backups, the company has to subscribe to a backup service, which then backs up the critical servers and data of the company. This is one of the newer backup methods.
Incorrect Answers:
A: The magnetic tape backup method is the easiest, cheapest and can also be automated.
B:
The disk imaging or mirroring method is more intricate than the magnetic tape method. With disk imaging, disk duplication occurs from either one disk to another disk, or by using software that images the entire contents of the drive and then produces a file for offsite storage.
C: CD-ROM burning is the simpler method of taking data from a hard drive, and moving it to a write-once or write-many CD-ROM system.
D: DVD-ROM burning is a method of taking data from a hard drive and moving it to another location for storage. DVDs can store up to 17GB of data.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 732:

Which type of storage mechanism, used to store backup data, stores the backup media at a location on the site of the computer center?

A. Working copies

B. Onsite storage
C. Offsite storage
D. All of the above

Answer: B

Explanation:
Onsite storage refers to a location on the site of the computer center, which the company uses to store data locally. Onsite storage containers are used to store backup media. These onsite storage containers are classed according to fire, moisture, and pressure resistance.
Incorrect Answers:
A: Working copies are partial or full backups that are stored at the computer center for immediate recovery purposes, if necessary
C: Offsite storage refers to a location that is not at the site of the computer center, which the company uses to store data. Offsite storage involves keeping of the backup media at a remote site.
D: Onsite storage is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 365-366.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1

QUESTION 733:

Which of the following are reasons why information might need to be restored from backup copies?

A. Workstation and server failures
B. Accidental deletion
C. Virus infection
D. Natural disasters
E. Workstation and server failures, accidental deletion and virus infection
F. All of the above

Answer: F

Explanation:
Each option contains a valid reason why information might need to be restored from backup copies.
Incorrect Answers:
A, B, C, D, E: These options only present part of the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 734:

Which alternate site option is not immediately ready for use and needs the company to provide the equipment and network when a disaster occurs at the corporate facility?

A. A hot site
B. A warm site
C. A cold site.
D. All of the above

Answer: C

Explanation:
A cold site is usually only made up of empty office space, electricity, and bathrooms. A cold site still needs networking equipment and complete configuration before it can operate when a disaster strikes the corporate facilities. This DRP option is the cheapest
Incorrect Answers:
A: A hot site is an alternate site that is up and available 24 hours a day, seven days a week, has the advantage of a very quick return to business, as well as the ability to test a DRP without affecting current operations. When setting up a hot site, you should ensure that this site is sufficiently far from the corporate facility being mirrored so that it does not get affected by the same damages. A hot site usually mirrors the configuration of the corporate facility.
B: A warm site provides a cheaper, scaled-down version of a hot site. A warm site usually only contains the power, phone, network ports, and other base services required. When a disaster occurs at the corporate facility, additional effort is needed to bring the computers, data, and resources to the warm site.
D: A cold site is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 735:

You work as the security administrator at Certkiller .com. You must define the disaster recover plan.
Choose the systems that you should include in the disaster recover plan.

A. You must include all systems.
B. You must include systems identified by the board of directors.

C. You must include financial, sales, and human resources systems.
D. You must include systems identified through a formal risk analysis process.

Answer: D

Explanation:
A preliminary risk analysis is performed to identify business critical applications and functions. Once those functions have been identified and documented, a structured approach to disaster recovery is prepared for the organization.
Incorrect Answers:
A: It is not always necessary to recover all systems as workstations usually do not hold critical data. These systems can be rebuilt rather than recovered.
B: Critical systems should be included in the disaster recover plan rather than systems identified by the board of directors, the president or the owner.
C: Financial systems and human resources systems would probably be included as they are usually critical systems. However, this is not the best answer as other critical systems should also be included. These critical systems would be identified in a formal risk analysis process.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 693-695.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 156.

QUESTION 736:

If your server room is destroyed, which of the following is the initial process for resuming operations at the original site if you have an alternate site?

A. Start with the least critical process
B. Start with the most critical process.
C. Start with the process that is most costly to maintain at the alternate site.
D. Start with the process that has maximum visibility in the company.

Answer: A

Explanation:
If you already have the most critical components of your operation set up and running at an alternate site, you should begin relocation at the original site with the least critical process. That way, if something does go wrong at the original, or if following the disaster something wasn't fixed properly, you won't risk disrupting critical operations again.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 692-693.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 374-375.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 157-158.

QUESTION 737:

Which of the following are key components of business continuity?

A. Utilities
B. High availability and fault tolerance
C. Backups
D. Utilities, high availability and fault tolerance mechanisms
E. All of the above

Answer: E

Explanation:
Utilities consist of services such as electricity, water, mail, and natural gas that are essential aspects of business continuity. Where possible, you should include fallback measures that allow for interruptions in these services. High availability and fault-tolerance refers to implementing mechanisms such as redundant array of independent disks (RAID), fault-tolerant servers and clustered servers, which would ensure that your business can still continue to operate when a system failure occurs. One of the important methods of ensuring business continuity is to back up mission-critical servers and data. Data should be backed up regularly, and you should store a copy of your backup offsite.
Incorrect Answers:
A, B, C, D: These options present only part of the complete answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 357-360.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 738:

RAID technologies use multiple disks to provide fault tolerance. Which RAID level provides no fault tolerance though because when any drive fails, the entire logical drive cannot be used?

A. RAID Level 0
B. RAID Level 1
C. RAID Level 3
D. RAID Level 5

Answer: A,

Explanation:
RAID 0 provides no fault tolerance because when any drive array fails, the entire logical drive cannot be used. This RAID implementation is primarily used for performance purposes and not for providing data availability during hard disk failures.
Incorrect Answers:
B: RAID Level 1, disk mirroring, provides full redundancy. All data is stored on multiple disks which mean that when one disk fails, another disk continues to operate. This allows you to replace the failed disk, without interrupting business operation.
C: RAID Level 3, disk striping with a parity disk, uses RAID 0 with a separate disk that stores parity information. When a disk in the array fails, the system can continue to operate while the failed disk is being replaced. Parity information is a value that is based on the value of the specific data stored on each disk
D: RAID Level 5, disk striping with a parity disk, uses RAID 0 with parity information being stored over all the disks in the array, and not one dedicated disk. Here, when disk in the array to fails, the system continues to operate while the failed disk is being removed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 361-362.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 739:

Which of the methods listed here, is not a method for building fault tolerance into a server?

A. Deploying clustered servers that share client load and can continue to operate when one server in the cluster fails.
B. Adding a second power supply.
C. Adding a second CPU.
D. Performing regular backups of the server

Answer: D

Explanation:
Fault-tolerant servers and clustered servers ensure that your business can still continue to operate when a system failure occurs. One of the important methods of ensuring business continuity is to back up mission-critical servers and data. Data should be backed up regularly, and you should store a copy of your backup offsite.
Incorrect Answers:
A, B, C: These are all methods of building fault tolerance into a server.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex,

Alameda, 2004, pp 357-360.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 740:

Which RAID level provides full redundancy at the expense of doubling hard disk storage requirements?

A. RAID Level 0
B. RAID Level 1
C. RAID Level 3
D. RAID Level 5

Answer: B

Explanation:
RAID Level 1, disk mirroring, provides full redundancy. All data is stored on multiple disks which mean that when one disk fails, another disk continues to operate. This allows you to replace the failed disk, without interrupting business operation.
Incorrect Answers:
A: RAID 0 provides no fault tolerance though because when any drive array fails, the entire logical drive cannot be used. This RAID implementation is primarily used for performance purposes and not for providing data availability during hard disk failures.
C: RAID Level 3, disk striping with a parity disk, uses RAID 0 with a separate disk that stores parity information. Here, when a disk in the array to fails, the system continues to operate while the failed disk is being removed. Parity information is a value that is based on the value of the specific data stored on each disk
D: RAID Level 5, disk striping with a parity disk, uses RAID 0 with parity information being stored over all the disks in the array, and not one dedicated disk. When a disk in the array to fails, the system can continue to operate while the failed disk is being removed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 361-362.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 741:

High availability pertains to ensuring that your primary servers are available 99.999 percent of the time. Which of the following is NOT a method for ensuring high availability systems?

A. Implementing fault-tolerant systems
B. Performing regular backups of your servers.
C. Implementing redundant technologies.
D. Monitoring the system for intrusions.

Answer: D

Explanation:
Implementing fault-tolerant systems and redundant technologies, and performing regular backups of your servers are all solutions for ensuring high availability systems.
Monitoring the system for intrusions is a method of securing systems from attacks from unauthorized individuals.
Incorrect Answers:
A, B, C: Implementing fault-tolerant systems and redundant technologies, and performing regular backups of the servers are all solutions for ensuring high availability systems.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 357-360.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 742:

Which RAID level provides redundancy and stores parity information over all disks within the array?

A. RAID Level 1
B. RAID Level 3
C. RAID Level 5
D. None of the above

Answer: C

Explanation:
RAID Level 5, disk striping with a parity disk, uses RAID 0 with parity information being stored over all the disks in the array, and not one dedicated disk. When a disk in the array to fails, the system continues to operate while the failed disk is being removed.
Parity information is a value that is based on the value of the specific data stored on each disk.
Incorrect Answers:
A: RAID Level 1, disk mirroring, provides full redundancy. All data is stored on multiple disks which mean that when one disk fails, another disk continues to operate. This allows

you to replace the failed disk, without interrupting business operation.
B:
RAID Level 3, disk striping with a parity disk, uses RAID 0 with a separate disk that stores parity information. Here, when a disk in the array to fails, the system continues to operate, while the failed disk is being removed.
D: RAID Level 5 is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 361-362.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 743:

Which of the following, represents a fault-tolerant implementation where everything is N+1, and multiple computers are used to provide 100 percent availability of a single server?

A. Tandem.
B. Stratus.
C. HP.
D. All of the above.

Answer: D

Explanation:
Each of these options involve a fault-tolerant implementation where everything is N+1, and multiple computers are used to provide 100 percent availability of a single server
Incorrect Answers:
A, B, C: Each one of these options makes up a part of the complete answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 357-360.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 744:

Which of the following mechanisms can be used to provide power for only a few minutes during power outages?

A. Uninterrupted power supply (UPS).

B. A large array of batteries.
C. A backup generator that is connected into the electrical supply lines of the building.
D. All of the above.

Answer: A

Explanation:
A UPS can be used to provide power for only a few minutes during power outages. A UPS also serves the purpose of protecting servers and other network equipment from power spikes as well as power outages.
Incorrect Answers:
B, C: A large array of batteries or a backup generator represents solutions for ensuring that the business can operate in extended power failure situations. A backup generator usually has failover switches that allow the generator to start operating automatically when a power outage occurs.
D: A UPS is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 357-358.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 745:

Which RAID level provides redundancy and stores parity information on a dedicated disk?

A. RAID Level 1
B. RAID Level 3
C. RAID Level 5
D. None of the above

Answer: B

Explanation:
RAID Level 3, disk striping with a parity disk, uses RAID 0 with a separate disk that stores parity information. Here, when a disk in the array to fails, the system can continue to operate while the failed disk is being removed. Parity information is a value that is based on the value of the specific data stored on each disk.
Incorrect Answers:
A: RAID Level 1, disk mirroring, provides full redundancy. All data is stored on multiple disks which mean that when one disk fails, another disk continues to operate. This allows you to replace the failed disk, without interrupting business operation.
C: RAID Level 5, disk striping with a parity disk, uses RAID 0 with parity information

being stored over all the disks in the array, and not one dedicated disk.
D: RAID Level 3 is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 361-362.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 746:

Which of the following mechanisms usually has failover switches that allow the mechanism to operate automatically when a power outage occurs?

A. Uninterrupted power supply (UPS)
B. A large array of batteries
C. A backup generator
D. All of the above

Answer: C

Explanation:
A backup generator has failover switches that allow the generator to operate automatically when a power outage occurs.
Incorrect Answers:
A: An UPS can be used to provide power for only a few minutes during power outages. A UPS also serves the purpose of protecting servers and other network equipment from power spikes as well as power outages.
B: A large array of batteries is a solution for ensuring that the business can operate in extended power failure situations. However, backup generators are equipped with failover switches.
D: A backup generator is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Sybex, Alameda, 2004, pp 357-358.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 4
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 7

QUESTION 747:

Choose the option that describes acceptable and expected network behavior.

A. Traffic originating from or being sent to unexpected locations.

B. Non-standard packet and protocol violations.
C. Recurring, failed connection attempts.
D. Changes in network performance including variations in traffic load.

Answer: D

Explanation:
In any network there will always be variations of traffic load as this is dependent on usage patterns.
Incorrect Answers:
A: Traffic coming from or going to unexpected locations is not expected and not acceptable.
B: Non-standard or malformed packets/protocol violationsare suspicious traffic that may indicate an attempted network attack.
C: Repeated, failed connection attempts are suspicious traffic that may indicate unauthorized access attempts.

QUESTION 748:

You work as the security administrator at Certkiller .com. You must draw up a well defined business continuity plan.
Which elements must you include in your business continuity plan? Choose all options that apply.

A. Strategic planning and mitigation
B. Risk and risk analysis.
C. Business impact analysis
D. Budgeting
E. Integration and validation.
F. Auditing and maintenance.
G. Training.
H. Documentation and security labeling.

Answer: A, B, C, E, F, G

Explanation:
Business Continuity Planning is the process of implementing policies, controls, and procedures to counteract the effects of losses, outages, or failures of critical business processes.
Incorrect Answers:
D, H: Budgeting, and documentation and security labeling are usually not part of a business continuity plan
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 695-697.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda,

Sybex, 2004, pp 253-257.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 159-160.

QUESTION 749:

Which of the following is likely to arise from temperature fluctuations of between 60 and 90 degrees?

A. Electrostatic discharge.
B. Power outages.
C. Chip creep.
D. Poor air quality.

Answer: C

Explanation:
The expansion and contraction that occurs during the normal heating and cooling cycles of your system can cause chips and cards, over time, to inch loose from sockets or slots. This is referred to as chip creep.
Incorrect Answers:
A: High humidity levels, rather than fluctuations in temperature, can increase electrostatic discharge
B: Power outages are not caused by fluctuations in temperature.
D: Poor air quality can cause problems related to ESD and fluctuations in temperature. However, poor air quality does not result from fluctuations in temperature.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 588.

QUESTION 750:

Which of the following concepts consists of the rules and requirements which should be adhered to within an organization?

A. Policies
B. Standards
C. Guidelines
D. Procedures

Answer: A

Explanation:
A policy consists of the rules and requirements which should be adhered to within an organization. Policies usually cover a single area, and contain conditions of expected performance, and the consequences of non-compliance.
Incorrect Answers:

B: Standards detail rules and best practices that govern an organization and how business is conducted. Standards usually outline best practices for specific platforms, implementations, operating system versions; and must be complied with.
C: Guidelines are similar to standards, in that they too detail rules and best practices that govern an organization and how business is conducted. The difference is that guidelines are not mandatory. Guidelines are usually drawn up to streamline the implementation of security policy elements.
D: Procedures detail how policies should be implemented within the production environment. A procedure contains a list of the necessary steps to implement policy elements
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 751:

Which policy type addresses organizational and departmental business issues and has an impact on the security of an organization?

A. Business policies
B. Certificate policies.
C. Incident response policies.
D. Human resource policies.

Answer: A

Explanation:
Business policies addresses organizational and departmental business issues and have an impact on the security of an organization.
Incorrect Answers:
B: Certificate policies pertain to policies that detail rules for certificate issuing and usage.
C: Incident response policies specify the way in which an organization should respond to an incident.
D: Human resource policies deal with specifying standards and enforcing behaviors.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 752:

Which of the following is not a component of a security triad?

A. Confidentiality.
B. Integrity.
C. Fault tolerance.
D. Availability.

Answer: C

Explanation:
Fault tolerance is not a component of the security triad.
Incorrect Answers:
A, B, D: These are all components of a security triad.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 753:

If you are formulating policies that specify the way in which an organization should respond to an incident, which type of policy are you defining?

A. Business policies
B. Certificate policies.
C. Incident response policies.
D. Human resource policies.

Answer: C

Explanation:
Incident response policies specify the way in which an organization should respond to an incident.
Incorrect Answers:
A: Business policies address organizational and departmental business issues and have an impact on the security of an organization.
B: Certificate policies pertain to policies that detail rules for certificate issuing and usage.
D: Human resource policies deal with specifying standards and enforcing behaviors.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 754:

Which of the following personnel security policies specify the process of how new

personnel are hired, and detail processes for screening employees for new positions?

A. Hiring policies
B. Acceptable use policies
C. Ethics policies
D. Need to Know policies

Answer: A

Explanation:
Hiring policies specify the process of how new personnel are hired, and detail processes for screening employees for new positions.
Incorrect Answers:
B: Acceptable Use policies contain rules that define the acceptable manner in which computers and company information are used, as well as activities that are not allowed.
C: Ethics policies are policies that govern accepted organizational ethics.
D: Need to Know policies define that information should be limited to only those individuals who require it, so as to minimize unauthorized access of information.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 379 - 382
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 755:

Which of the following concepts outline best practices for specific platforms, implementations, operating system versions; and must be complied with?

A. Policies
B. Standards
C. Guidelines
D. Procedures

Answer: B

Explanation:
Standards detail rules and best practices that govern an organization and how business is conducted. Standards usually outline best practices for specific platforms, implementations, operating system versions; and must be complied with.
Incorrect Answers:
A: A policy consists of specifying the rules and requirements which should be adhered to within an organization. Policies usually cover a single area, and contain conditions of expected performance and consequences of non-compliance.

C: Guidelines are similar to standards, in that they too detail rules and best practices that govern an organization and how business is conducted. The difference is that guidelines are not mandatory. Guidelines are usually drawn up to streamline the implementation of security policy elements.
D: Procedures detail how policies should be implemented within the production environment. A procedure contains a list of the steps necessary to implement policy elements.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 756:

Which type of business policies describes rules that reduce the risk of fraud and other losses?

A. Separation of duties
B. Physical access control
C. Document destruction
D. None of the above

Answer: A

Explanation:
Separation of duties policies describes rules that reduce the risk of fraud and other losses. These policies should define more than one person for completing business critical tasks.
Incorrect Answers:
B: Physical access control policies limit issues such as unauthorized disclosure of information, unauthorized access to the company facilities, and data theft.
C: Document destruction policies detail the methods on how information that is no longer needed gets disposed.
D: Separation of duties policies is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 382 - 384
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1

QUESTION 757:

Choose the option that best describes the definition of certificate policies?

A. Addresses organizational and departmental business issues and have an impact on the security of an organization.

B. Sets up policies that detail rules for certificate issuing and usage.
C. Specifies the way in which an organization should respond to an incident.
D. Deals with specifying standards and enforcing behaviors.

Answer: B

Explanation:
Certificate policies pertain to policies that detail rules for certificate issuing and usage.
Incorrect Answers:
A: Business policies addresses organizational and departmental business issues and have an impact on the security of an organization.
C: Incident response policies specify the way in which an organization should respond to an incident.
D: Human resource policies deal with specifying standards and enforcing behaviors.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 758:

Which of the following policies details the responsibilities of individuals within the organization, and also details when the responsibilities of people in the organization will be audited?

A. Access control
B. Accountability
C. Authentication
D. Password

Answer: B

Explanation:
An accountability policy details the responsibilities of individuals within the organization, and also details when responsibilities of people in the organization will be audited.
Incorrect Answers:
A: Access control policy contains guidelines on the rights, privileges, and restrictions for using company equipment and assets.
C: An authentication policy details those methods, equipment, and parameters which are allowed for accessing the resources of the network.
D: A password policy details processes that describe how passwords are managed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 759:

Which component of a security triad deals with ensuring that information is not intentionally or unintentionally disclosed?

A. Confidentiality.
B. Integrity.
C. Fault tolerance.
D. Availability.

Answer: A

Explanation:
Confidentiality deals with ensuring that information is not intentionally or unintentionally disclosed.
Incorrect Answers:
B: Integrity deals with protecting against the unauthorized modifications to data.
C: Fault tolerance is not one of the three components of the security triad.
D: Availability deals with ensuring that any needed data is available when necessary.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 760:

Which of the following concepts detail rules and best practices that govern an organization and how business is conducted, but is not mandatory?

A. Policies
B. Standards
C. Guidelines
D. Procedures

Answer: C

Explanation:
Guidelines are similar to standards, in that they too detail rules and best practices that govern an organization and how business is conducted. The difference is that guidelines are not mandatory. Guidelines are usually drawn up to streamline the implementation of security policy elements.
Incorrect Answers:

A: A policy consists of specifying the rules and requirements which should be adhered to within an organization. Policies usually cover a single area, and contain conditions of expected performance and consequences of non-compliance.
B: Standards detail rules and best practices that govern an organization and how business is conducted. Standards usually outline best practices for specific platforms, implementations, operating system versions; and must be complied with.
D: Procedures detail how policies should be implemented within the production environment. A procedure contains a list of steps necessary to implement policy elements.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 761:

Which type of business policies detail the methods on how information that is no longer needed gets disposed?

A. Separation of duties
B. Physical access control
C. Document destruction
D. None of the above

Answer: C

Explanation:
Document destruction policies detail the methods on how information that is no longer needed gets disposed.
Incorrect Answers:
A: Separation of duties policies describes rules that reduce the risk of fraud and other losses. These policies should define more than one person for completing business critical tasks.
B: Physical access control policies limit issues such as unauthorized disclosure of information, unauthorized access to the company facilities, and data theft.
D: Document destruction policies is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 382 - 384
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1

QUESTION 762:

Which of the following personnel security policies define that information should be

limited to only those individuals who require it, so as to minimize unauthorized access of information?

A. Hiring policies
B. Acceptable use policies
C. Ethics policies
D. Need to Know policies

Answer: D

Explanation:
Need to Know policies define that information should be limited to only those individuals who require it, so as to minimize unauthorized access of information.
Incorrect Answers:
A: Hiring policies specify the process of how new personnel are hired, and detail processes for screening employees for new positions.
B: Acceptable Use policies contain rules that define the acceptable manner in which computers and company information is used, as well as activities that are not allowed.
C: Ethics policies are policies that govern accepted organizational ethics.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 379 - 382
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 763:

Which type of policies must clearly define which information can be disclosed, what information cannot be disclosed, and what types of information employees are provided?

A. Privacy policy
B. Firewall policy
C. Violations reporting policy
D. Network maintenance policy

Answer: A

Explanation:
Privacy policy must clearly define which information can be disclosed, what information cannot be disclosed, and what types of information employees are provided.
Incorrect Answers:
B: Firewall policy defines which type of data is allowed, and which type of data is not allowed to move over the firewall.

C: A violations reporting policy defines violations, such as privacy issues, usage of equipment; and details how violations are to be reported.
D: Network maintenance policy defines how maintenance personnel are allowed to access and deal with the equipment of the company, specifies the extent to which external maintenance can be utilized, and specifies whether remote maintenance is allowed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 764:

Which component of a security triad deals with protecting against unauthorized modifications to data?

A. Confidentiality.
B. Integrity.
C. Fault tolerance.
D. Availability.

Answer: B

Explanation:
Integrity deals with protecting against the unauthorized modifications to data.
Incorrect Answers:
A: Confidentiality deals with ensuring that information is not intentionally or unintentionally disclosed.
C: Fault tolerance is not one of the three components of the security triad.
D: Availability deals with ensuring that any needed data is available when necessary.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 765:

Which of the following detail how policies should be implemented within the production environment?

A. Policies
B. Standards
C. Guidelines
D. Procedures

Answer: D

Explanation:
Procedures detail how policies should be implemented within the production environment. A procedure contains a list of the steps necessary to implement policy elements.
Incorrect Answers:
A: A policy consists of specifying the rules and requirements which should be adhered to within an organization. Policies usually cover a single area, and contain conditions of expected performance and consequences of non-compliance.
B: Standards detail rules and best practices that govern an organization and how business is conducted. Standards usually outline best practices for specific platforms, implementations, operating system versions; and must be complied with
C: Guidelines are similar to standards, in that they too detail rules and best practices that govern an organization and how business is conducted. The difference is that guidelines are not mandatory. Guidelines are usually drawn up to streamline the implementation of security policy elements.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 766:

Which of the following policies details processes that describe how passwords are managed?

A. Access control
B. Accountability
C. Authentication
D. Password

Answer: D

Explanation:
A password policy details processes that describe how passwords are managed.
Incorrect Answers:
A: Access control policy contains guidelines on the rights, privileges, and restrictions for using company equipment and assets.
B: An accountability policy details the responsibilities of individuals within the organization, and also details when responsibilities of people in the organization will be audited.
C An authentication policy details those methods, equipment, and parameters which are allowed for accessing the resources of the network.

References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 767:

Business policies deals with organizational and departmental business issues, and consists of three main areas. Choose the correct answer?

A. Separation of duties
B. Physical access control
C. Document destruction
D. All of the above

Answer: D

Explanation:
Separation of duties, physical access control, and document destruction are the three main areas of business policy.
Incorrect Answers:
A: Separation of duties policies describes rules that reduce the risk of fraud and other losses. These policies should define more than one person for completing the business critical tasks.
B: Physical access control policies limit issues such as unauthorized disclosure of information, unauthorized access to the company facilities, and data theft.
C: Document destruction policies detail the methods on how information that is no longer needed gets disposed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 382 - 384
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1

QUESTION 768:

Choose the option that best describes the definition of human resource policies.

A. Addresses organizational and departmental business issues and have an impact on the security of an organization
B. Sets up policies that detail rules for certificate issuing and usage.
C. Specifies the way in which an organization should respond to an incident.
D. Deals with specifying standards and enforcing behaviors.

Answer: D

Explanation:
Human resource policies deal with specifying standards and enforcing behaviors.
Incorrect Answers:
A: Business policy addresses organizational and departmental business issues and has an impact on the security of an organization.
B: Certificate policies pertain to policies that detail rules for certificate issuing and usage.
C: Incident response policies specify the way in which an organization should respond to an incident.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 769:

Which of the following contain conditions of expected performance and consequences of non-compliance?

A. Policies
B. Standards
C. Guidelines
D. Procedures

Answer: A

Explanation:
A policy consists of specifying the rules and requirements which should be adhered to within an organization. Policies usually cover a single area, and contain conditions of expected performance and consequences of non-compliance.
Incorrect Answers:
B: Standards detail rules and best practices that govern an organization and how business is conducted. Standards usually outline best practices for specific platforms,
C: Guidelines are similar to standards, in that they too detail rules and best practices that govern an organization and how business is conducted. The difference is that guidelines are not mandatory. Guidelines are usually drawn up to streamline the implementation of security policy elements.
D: Procedures detail how policies should be implemented within the production environment. A procedure contains a list of steps necessary to implement policy elements.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 770:

Which component of a security triad deals with ensuring that any needed data is available when necessary?

A. Confidentiality.
B. Integrity.
C. Fault tolerance.
D. Availability.

Answer: D

Explanation:
Availability deals with ensuring that any needed data is available when necessary.
Incorrect Answers:
A: Confidentiality deals with ensuring that information is not intentionally or unintentionally disclosed
B: Integrity deals with protecting against the unauthorized modifications to data.
C: Fault tolerance is not one of the three components of the security triad.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 771:

Which type of policies must clearly define which type of data is allowed and which type of data is not allowed to move over the firewall?

A. Privacy policy
B. Firewall policy
C. Violations reporting policy
D. Network maintenance policy

Answer: B

Explanation:
Firewall policy defines which type of data is allowed and which type of data is not allowed to move over the firewall.
Incorrect Answers:
A: Privacy policy clearly defines which information can be disclosed, what information cannot be disclosed, and what types of information employees are provided.
C: A violations reporting policy defines violations, such as privacy issues, usage of implementations, operating system versions; and must be complied with

D: Network maintenance policy defines how maintenance personnel are allowed to access and deal with the equipment of the company, specifies the extent to which external maintenance can be utilized, and specifies whether remote maintenance is allowed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 772:

Which type of Service Level Agreement (SLA) deals with specifying bandwidth and connection availability guarantees?

A. ISP SLA
B. LAN SLA
C. Data center SLA
D. Hardware SLA
E. Application service provider SLA.

Answer: A

Explanation:
An ISP SLA deals with specifying bandwidth and connection availability guarantees.
Incorrect Answers:
B: A LAN SLA specifies the availability of LAN connectivity devices as well as the acceptable response times for resolving issues.
C: A data center SLA details availability of the data of the organization, and includes elements such as backup frequency, recovery times, and system guarantees of those systems that store company data.
D: A hardware SLA details issues such as repairing, replacing, or restoring computers and other hardware within a predetermined time frame.
E: An application service provider SLA deals with the hosting of a specific application or service. The SLA details issues such as availability, server up time, and recovery times.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 773:

Which of the following elements, included in password policy, definesthe time duration for which a locked out account remains locked out?

A. Account lockout duration
B. Password complexity
C. Account lockout threshold
D. Password expiration

Answer: A

Explanation:
Account lockout duration defines the time duration for which a locked out account remains locked out.
Incorrect Answers:
B: Password complexity defines the types of characters which users must utilize for passwords.
C: Account lockout threshold defines the number of incorrect logon attempts permitted, before an account is locked out.
D: Password expiration defines the duration of time a password is valid, before it has to be changed to another value.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 774:

Which type of business policies involve limiting issues such as unauthorized disclosure of information, unauthorized access to the company facilities, and data theft?

A. Separation of duties
B. Physical access control
C. Document destruction
D. None of the above

Answer: B

Explanation:
Physical access control policies limit issues such as unauthorized disclosure of information, unauthorized access to the company facilities, and data theft.
Incorrect Answers:
A: Separation of duties policies describes rules that reduce the risk of fraud and other losses. These policies should define more than one person for completing the business critical tasks.
C: Document destruction policies detail the methods on how information that is no longer needed gets disposed.
D: Physical access control policies is the correct answer.

References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 382 - 384
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1

QUESTION 775:

Which of the following policies details those methods, equipment, and parameters which are allowed for accessing the resources of the network?

A. Access control
B. Accountability
C. Authentication
D. Password

Answer: C

Explanation:
An authentication policy details those methods, equipment, and parameters which are allowed for accessing the resources of the network
Incorrect Answers:
A: Access control policy contains guidelines on the rights, privileges, and restrictions for using company equipment and assets.
B: An accountability policy details the responsibilities of individuals within the organization, and also details when responsibilities of people in the organization will be audited.
D: A password policy details processes that describe how passwords are managed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 776:

Which type of Service Level Agreement (SLA) deals with specifying the availability of LAN connectivity devices as well as the acceptable response times for resolving issues?

A. ISP SLA
B. LAN SLA
C. Data center SLA
D. Hardware SLA
E. Application service provider SLA.

Answer: B

Explanation:
A LAN SLA specifies the availability of LAN connectivity devices as well as the acceptable response times for resolving issues.
Incorrect Answers:
A: An ISP SLA deals with specifying bandwidth and connection availability guarantees.
C: A data center SLA details availability of the data of the organization, and includes elements such as backup frequency, recovery times, and system guarantees of those systems that store company data.
D: A hardware SLA details issues such as repairing, replacing, or restoring computers and other hardware within a predetermined time frame.
E: An application service provider SLA deals with the hosting of a specific application or service. The SLA details issues such as availability, server up time, and recovery times.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 777:

Which type of policies defines violations, such as privacy issues, usage of equipment; and details how violations are to be reported?

A. Privacy policy
B. Firewall policy
C. Violations reporting policy
D. Network maintenance policy

Answer: C

Explanation:
A violations reporting policy defines violations, such as privacy issues, usage of equipment; and details how violations are to be reported.
Incorrect Answers:
A: Privacy policy clearly defines which information can be disclosed, what information cannot be disclosed, and what types of information employees are provided.
B: Firewall policy defines which type of data is allowed and not allowed to move over the firewall.
D: Network maintenance policy defines how maintenance personnel are allowed to access and deal with the equipment of the company, specifies the extent to which external maintenance can be utilized, and specifies whether remote maintenance is allowed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press,

Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 778:

Which of the following statements regarding password policy is FALSE?

A. Specifies the minimum acceptable password length.
B. Specifies the types of characters that must be used for passwords.
C. Specifies the time duration for which a password can be used, before it must be changed.
D. Specifies the number of correct logon attempts permitted, prior to an account being locked out of the system.

Answer: D

Explanation:
Password policies specifies the number of INCORRECT logon attempts permitted, prior to an account being locked out of the system
Incorrect Answers:
A, B, C: These statements are all TRUE.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 779:

Which of the following personnel security policies detail processes for terminating employment of employees, and should specify that the appropriate personnel be informed so that the necessary accounts can be disabled and systems be backed up?

A. Acceptable use policies
B. Ethics policies
C. Need to Know policies
D. Termination policies

Answer: D

Explanation:
Termination policies detail processes for terminating employment of employees, and should specify that the appropriate personnel be informed so that the necessary accounts can be disabled and systems be backed up.
Incorrect Answers:

A: Acceptable Use policies contain rules that define the acceptable manner in which computers and company information is used, as well as activities that are not allowed.
B: Ethics policies are policies that govern accepted organizational ethics.
C: Need to Know policies define that information should be limited to only those individuals who require it, so as to minimize unauthorized access of information.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 379 - 382
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 780:

Which type of Service Level Agreement (SLA) details availability of the data of the organization, and includes elements such as backup frequency, recovery times, and system guarantees of those systems that store company data?

A. ISP SLA
B. LAN SLA
C. Data center SLA
D. Hardware SLA
E. Application service provider SLA.

Answer: C

Explanation:
A data center SLA details availability of the data of the organization, and includes elements such as backup frequency, recovery times, and system guarantees of those systems that store company data.
Incorrect Answers:
A: An ISP SLA deals with specifying bandwidth and connection availability guarantees.
B: A LAN SLA specifies the availability of LAN connectivity devices as well as the acceptable response times for resolving issues.
D: A hardware SLA details issues such as repairing, replacing, or restoring computers and other hardware within a predetermined time frame.
E: An application service provider SLA deals with the hosting of a specific application or service. This SLA details issues such as availability, server up time, and recovery times.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 781:

Which of the following activities can violate security policy, and can lead to an incident?

A. All system changes performed without the consent of the owner to hardware, software, and firmware.
B. Unauthorized processing, modification and deletion of data.
C. DoS attacks which disable the computer system, routers, and any other type of network device.
D. Unauthorized access attempts to access computer systems and private data.
E. All of the above

Answer: E

Explanation:
Each option details a method or activity that can violate security policy and lead to an incident.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 386
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 782:

Which of the following methods, based on the separation of duties principle, involves provisioning of at least two people for a task to enhance security, and also ensures that multiple people are trained for each task?

A. Cross training
B. Job rotation
C. Mandatory vacations
D. None of the above

Answer: A

Explanation:
Cross training is a method that involves the provisioning of at least two people for a task to enhance security, and also ensure that multiple people are trained for each task.
Incorrect Answers:
B: Job rotation is method that assists in ensuring that an employee does not abuse power. Job rotation works on the basis of moving employees from one job responsibility to another job responsibility.

C: With mandatory vacations, an employee is removed from the working environment for a specific duration of time, which allows auditors the necessary time to examine the activities of the specific employee.
D: Cross training is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 783:

Which type of policies defines how maintenance personnel are allowed to access and deal with the equipment of the company, specifies the extent to which external maintenance can be utilized, and specifies whether remote maintenance is allowed?

A. Privacy policy
B. Firewall policy
C. Violations reporting policy
D. Network maintenance policy

Answer: D

Explanation:
Network maintenance policy defines how maintenance personnel are allowed to access and deal with the equipment of the company, specifies the extent to which external maintenance can be utilized, and specifies whether remote maintenance is allowed.
Incorrect Answers:
A: Privacy policy clearly defines which information can be disclosed, what information cannot be disclosed, and what types of information employees are provided.
B:
Firewall policy defines which type of data is allowed, and which type of data is not allowed to move over the firewall.
C: A violations reporting policy defines violations, such as privacy issues, usage of equipment; and details how violations are to be reported.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 784:

Which type of policies defines the levels of care which should be used to maintain the confidentiality of private data?

A. Separation of duties
B. Physical access control
C. Document destruction
D. Due care policies

Answer: D

Explanation:
Due care policies defines the levels of care which should be used to maintain the confidentiality of private data. These policies define how information must be handled.
Incorrect Answers:
A: Separation of duties policies describes rules that reduce the risk of fraud and other losses. These policies should define more than one person for completing business critical tasks.
B: Physical access control policies limit issues such as unauthorized disclosure of information, unauthorized access to the company facilities, and data theft.
C: Document destruction policies detail the methods on how information that is no longer needed gets disposed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 382 - 384
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1

QUESTION 785:

Which of the following policies detail guidelines on the rights, privileges, and restrictions for using company equipment and assets?

A. Access control
B. Accountability
C. Authentication
D. Password

Answer: A

Explanation:
Access control policy contains guidelines on the rights, privileges, and restrictions for using company equipment and assets.
Incorrect Answers:
B: An accountability policy details the responsibilities of individuals within the organization, and also details when responsibilities of people in the organization will be audited.
C: An authentication policy details those methods, equipment, and parameters which are allowed for accessing the resources of the network.
D: A password policy details processes that describe how passwords are managed.

References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 786:

Which of the following elements, included in password policy, definesthe number of incorrect logon attempts permitted, before an account is locked out?

A. Account lockout duration
B. Password complexity
C. Account lockout threshold
D. Password expiration

Answer: C

Explanation:
Account lockout threshold defines the number of incorrect logon attempts permitted, before an account is locked out.
Incorrect Answers:
A: Account lockout duration defines the time duration for which a locked out account remains locked out.
B: Password complexity defines the types of characters which users must utilize for passwords.
D: Password expiration defines the duration of time a password remains valid, before it has to be changed to a different value.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 787:

Which of the rules listed here are FALSE for implementing effective password policies for users?

A. Users should never share passwords.
B. Passwords should not be obvious or predictable.
C. A password should at least be four characters in length.
D. An effective password consists of a combination of alphabetic, numeric, and special characters.
E. All of the above are TRUE.

Answer: C

Explanation:
An effective password consists of at least SEVEN characters, and this should be a combination of alphabetic, numeric, and special characters.
Incorrect Answers:
A, B, D: These statements are all TRUE.
E: All statements are not TRUE, because C is incorrect.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 788:

Which type of Service Level Agreement (SLA) deals with hosting of a specific application or service?

A. ISP SLA
B. LAN SLA
C. Data center SLA
D. Hardware SLA
E. Application service provider SLA.

Answer: E

Explanation:
An application service provider SLA deals with the hosting of a specific application or service. This SLA details issues such as availability, server up time, and recovery times.
Incorrect Answers:
A: An ISP SLA deals with specifying bandwidth and connection availability guarantees.
B: A LAN SLA specifies the availability of LAN connectivity devices as well as the acceptable response times for resolving issues.
C: A data center SLA details availability of the data of the organization, and includes elements such as backup frequency, recovery times, and system guarantees of those systems that store company data.
D: A hardware SLA details issues such as repairing, replacing, or restoring computers and other hardware within a predetermined time frame.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 789:

Which of the following methods, based on the separation of duties principle, works on the basis of moving employees from one job responsibility to another job responsibility?

A. Cross training
B. Job rotation
C. Mandatory vacations
D. None of the above

Answer: B

Explanation:
Job rotation is method that assists in ensuring that an employee does not abuse power. Job rotation works on the basis of moving employees from one job responsibility to another job responsibility.
Incorrect Answers:
A: Cross training is a method that involves provisioning of at least two people for a task to enhance security and ensure that multiple people are trained for each task.
C: With mandatory vacations, an employee is removed from the working environment for a specific duration of time, which allows auditors the necessary time to examine the activities of the specific employee.
D: Job rotation is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 8

QUESTION 790:

The level of security of a network can be reduced when certain conditions prevail. Which one can reduce network security?

A. Passwords must be greater than eight characters in length and should minimally contain one non-alpha character.
B.
Passwords are configured to expire at regular intervals. Users must then choose new passwords which have never been used before.
C. Complex passwords which users are unable to remotely change are randomly selected by the administrator and then passed to these users.
D. After a predefined number of failed logon attempts, the server will lock out the specific user account. The administrator must manually enable all locked out accounts.

Answer: C

Explanation:
If a user gets a difficult password that they can't remember, there's a certain chance that they will forget the password or compromise security by writing down their password on a Post It note on their keyboard. Since the user won' be able to reset the password themselves they'll have to make regular trips to help desk for a new password, and with regular disgruntled users getting emotional over passwords, the risk of social engineering increases.
Incorrect Answers:
A: Strong passwords with long password lengths and complex character sets will improve network security as it will make it more difficult for a hacker to crack a user's password.
B: A password lifetime policy will increase network security by reducing the opportunity for a hacker to guess a user's password.
D: An account lockout policy will improve network security by locking out a user account after a set number of failed logon attempts. A number of failed logon attempts would indicate a possible attempt to crack an account's password.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 76-77, 647-648.

QUESTION 791:

You work as the security administrator at Certkiller .com. You have noticed that when users leave their work areas, they fully display confidential information on their monitors. You want to advise users on what they should do when they need to leave their workstations unattended for a short time period.
Which advice should you pass to users?

A. Because the monitor is in a designated area within the Certkiller .com premises, users can merely leave their work areas.
B. Advise users to turn off their monitors.
C. Advise users to wait for the screen saver to activate before leaving their work areas unattended.
D. You should consult the security policy on how to secure confidential data.

Answer: C

Explanation:
A user can ensure that sensitive material on his monitor is not accessible by unauthorized users by waiting for the screensaver to come on before leaving the area. However, the screen saver should be password protected.
Incorrect Answers:
A: If you leave the computer unattended a social engineer could walk by, and view your sensitive material.

B: If you turn off your monitor, they can easily turn it back on.
D: A policy for securing sensitive data usually refers to the secure storage of data.

QUESTION 792:

You plan to update the user security policy. Whom should the new updated user security policy be distributed and made available to?

A. All security administrators.
B. All auditors.
C. All users.
D. All staff.

Answer: D

Explanation:
A user security policy would affect all employees at a company. In addition, all employees will have to be aware of the new policy so as to adhere to it. Thus, the new user security policy should be made available to the whole staff.
This question requires a distinction between network users, which are all users of a network, including administrators and would be akin to all staff, and a default network group called Users which do not have administrative privileges.
Incorrect Answers:
A: A user security policy would affect all employees at a company. In addition, all employees will have to be aware of the new policy so as to adhere to it. Thus, the new user security policy should be made available to the whole staff and not just the security administrator.
B: A user security policy would affect all employees at a company. In addition, all employees will have to be aware of the new policy so as to adhere to it. Thus, the new user security policy should be made available to the whole staff and not just the auditors.
C: In this scenario, users should refer to all network users, which is akin to all staff members, rather than the default network group called Users, which do not have administrative privileges.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 271.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 163.

QUESTION 793:

Choose the option that contains the typically ignored component of security management.

A. Security awareness
B. Intrusion detection
C. Risk assessment

D. Vulnerability control

Answer: A

Explanation:
Security awareness and education are critical to the success of a security effort. Security awareness and education include explaining policies, standards, procedures, and guidelines to both users and management. However, security awareness is the most overlooked element of security management.
Incorrect Answers:
B, C, D: Security awareness rather than intrusion diction, risk assessment, and vulnerability control is the most overlooked element of security management.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 174-175.

QUESTION 794:

You work as the security administrator at Certkiller .com. A Certkiller .com employee named Rory Allen works in the Sales department. Rory must be issued with a laptop computer. Rory will be using the laptop computer to remotely connect to and access the Certkiller .com newtwork.
Rory must not be allowed to install unauthorized software on this laptop computer.
What should you do to achieve your goal?

A. You should update the company security policy so that no users are issued laptop computers. This will prevent this issue.
B. Rory should be informed on what can and cannot be installed on his laptop computer.
C. You should ensure that the hard disk is read only.
D. Use biometrics to authenticate Rory before allowing software to be installed.

Answer: B

Explanation:
Countless employees have compromised their business applications by installing computer games, and pornographic movies. To avoid such a problem all you have to do is to get employees to agree to an acceptable use policy so they can know before hand what activities they are allowed and what activities they are not allowed.
Incorrect Answers:
A: Not giving the user a laptop could be counter productive as it would mean that the employee would not be able to work remotely.
C: Should the hard disk be made read only, the user would only be able to access files on the system. He or she would not be able to make changes to the files and thus would not be able to accomplish their tasks
D: Biometrics and authentication do not control authorization and thus cannot be used to control what a user is and is not allowed.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 381.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 163.

QUESTION 795:

You work as the security administrator at Certkiller .com. You are defining a SLA (Service Level Agreement). You want to ensure the availability of server based resources over guaranteed server performance levels.
What must you include in the SLA to achieve this objective?

A. Network
B. Hosting
C. Application
D. Security

Answer: B

Explanation:
In the hosting business, every company aims for 100% availability in their service level agreements, and usually offer concessions for times of reduced availability. Sadly, these agreements have exceptions which include: scheduled network maintenance, hardware maintenance, software maintenance, virus attacks, hacker attacks, force majeure, labour actions, war, insurrections, sabotage, and past due accounts on your part.
Incorrect Answers:
A, C: In a network an application server, availability as well as performance would be required as these would be productivity issues.
D: In most case a company would want to implement its own security.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 649-650.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 376-378.

QUESTION 796:

Computer forensics experts use specific guidelines to gather and analyze data while minimizing data loss.
What guidelines do they use?

A. Evidence
B. Chain of custody
C. Chain of command
D. Incident response

Answer: B

Explanation:
The chain of custody documents the history of evidence that has been collected from the moment evidence is discovered through to the presentation of the evidence in court.
Incorrect Answers:
A: Evidence collected during the investigation of the crime is used as proof in determining possible guilt. However, for evidence to be presentable in court, the forensic expert must be able to show that the evidence was handled egitimately, that the evidence was properly preserved, and that the evidence was collected properly. The chain of custody is used to accomplish this.
C: A chain of command indicated the hierarchical organization of a company. It is not relevant to the preservation of evidence.
D: Incident response refers to the process of identifying, investigating, repairing, documenting, and adjusting procedures to prevent the reoccurrence of an incident. It does not refer to the collection and analysis of data by forensic experts.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 602-609.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 385, 406-409.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 101-102, 170-171.

QUESTION 797:

You work as the security administrator at Certkiller .com. You want to reduce the current vulnerability from dumpster diving.
How will you accomplish the task?

A. Employ additional security staff.
B. Destroy all paper and other media that are no longer required.
C. Install expensive surveillance equipment.
D. Remove the contents of the trash can on a regular basis.

Answer: B

Explanation:
Dumpster diving is the process of scavenging through trash in a search for clues trash for clues to users' passwords and other sensitive information. The secure disposal and destruction of waste can prevent dumpster diving. This includes the shredding and incineration of printed material, and the incineration, crushing, or magnetic destruction of storage media.
Incorrect Answers:
A, C: Additional security staff and surveillance equipment will not be able to prevent dumpster diving once the trash has been removed from the site.
D: Emptying the trash can frequently will not prevent dumpster diving at the location

where the trash is taken to. Thus the vulnerability would remain.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 49.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 165.

QUESTION 798:

Choose the items which an intruder wants to find by going through disposed garbage. Choose all options that apply.

A. Process lists.
B. Boot sectors.
C. Old password information.
D. Virtual memory.
E. Network diagrams or drawings.
F. IP (Internet Protocol) address lists.

Answer: C, E, F

Explanation:
During dumpster diving, a potential attacker would search for clues about the network. These would include network diagrams, IP address lists, user passwords, etc.
Incorrect Answers:
A: Process lists are of little use to an attacker and would not be something an attacker would search for during dumpster diving.
B: Boot sectors are of little use to an attacker and would not be something an attacker would search for during dumpster diving.
D: Virtual memory is space on a hard disk drive that is used when system RAM is full. It is erased as soon as the application that required the data held in virtual memory is closed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 49.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 165.
David Groth and Dan Newland, et al, A+ Complete Study Guide, Second Edition, San Francisco, 2001, pp 455-456, 569-570, 839.

QUESTION 799:

Choose the items that an intruder would ignore when going through disposed garbage. Choose all options that apply.

A. IP (Internet Protocol) address lists.
B. Network diagrams or drawing.
C. Old password information.
D. System access requests.

Answer: D

Explanation:
During dumpster diving, a potential attacker would search for clues about the network. These would include network diagrams, IP address lists, user passwords, etc. However, system access requests would not reveal much information. They are a card that an employee fills that requests the types of resources they want access to, and the privileges they want. All a hacker can learn from them is that from the moment the request was dated, that particular user did not have those privileges
Incorrect Answers:
A: An IP address would be of value to a potential hacker as it gives them an indication of the network being used. It also gives them the address of a system to attack.
B:
Aconfiguration or system map is of value to a potential hacker because they can help the hacker 'blueprint' the network structure.
C: Old passwords would be of value to a potential hacker because they give the hacker an indication of how strong the password is, including the password length, the character sets used, and possibility the password lifetime.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 49.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 72.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 165.

QUESTION 800:

You work as the security administrator at Certkiller .com. You want to reduce the likelihood of Certkiller .com employees misusing Certkiller .com e-mail.
How will you accomplish the task?

A. Create and enforce ACLs (Access Control List).
B. Create and enforce network security policy.
C. Implement a strong authentication method.
D. Encrypt all company e-mail messages.

Answer: B

Explanation:
E-mail usage cannot effectively be controlled by mechanism such as permissions as users

often require access to e-mail to perform their job functions. Thus, the user needs to take responsibility for their use of the company's e-mail system. The best way to accomplish this would be though a usage policy, which is one of the elements of a network security policy.
Incorrect Answers:
A: Access control lists define the permissions users have to network resources such as files, folders, printers and computers. It does not control the use of a company's e-mail system.
C:
Strong authentication would control user access to the network system or to a server. It does not control e-mail usage. Furthermore, users would probably require access to e-mail in their job functions thus users would need to be authenticated to the e-mail server. Once authenticated, the system has no further control over the use of the e-mail system.
D: E-mail encryption is on a per user basis. Each user would need to encrypt his or her e-mail. Thus the user can still misuse the company's e-mail system by sending unencrypted e-mail messages.

QUESTION 801:

A sound company security policy should define a specific element. What is it?

A. The assets of the organization.
B. Attacks planned against the company.
C. How the company evaluates the others in security audits.
D. The weaknesses in systems of competitor companies.

Answer: A
A security policy is concerned with the protection of company assets, including systems, data, networks, and staff.
Incorrect Answers:
B: It is most unlikely that an organization would be aware of attacks that are planned against it. Further more, a security policy would define procedures that are to be followed in response to an attack rather than the attack itself.
C, D: A security policy is not concerned with the security levels at a rival organization and is comparative.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 9.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 635

QUESTION 802:

Which access control method is centrally controlled and managed, where all access capabilities are predefined and users have no influence on permissions, nor can

users share information that has not been previously defined by administrators?

A. Mandatory Access Control (MAC) method
B. Discretionary Access Control (DAC) method
C. Role-Based Access Control (RBAC)
D. All of the above

Answer: A

Explanation:
The MAC method enforces a rigid model of security. The MAC access method is centrally controlled and managed, where all access capabilities are predefined and users have no influence on permissions, nor can they share information that has not been previously established by administrators. Here, administrators make all necessary changes.
Incorrect Answers:
B: The Discretionary Access Control (DAC) method enables users to set permissions when necessary, but within the specific guidelines of the broader MAC guidelines. This method allows users to have some level of flexibility with regard to the manner in which information is accessed. While the DAC method allows greater flexibility than the MAC method, the risk of unauthorized disclosure of information is increased.
C: The Role-Based Access Control (RBAC) method focuses on group management and not on users, by implementing access according to job function or responsibility. In this method, users have one or multiple roles that allow access to specific information. Administrators usually group users and then assign MAC permissions based on the role in the company.
D: Mandatory Access Control (MAC) is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 392-393.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter

---

QUESTION 803:

Which security management model works on the basis that security-specific responsibilities are delegated between employees at different locations?

A. Centralized security management model.
B. Decentralized security management model.
C. Both of the above.
D. None of the above.

Answer: B

Explanation:
A decentralized security management model works on the basis that security-specific responsibilities are delegated between employees at different locations. While decentralized management is less secure than centralized security, it provides greater scalability.
Incorrect Answers:
A: The centralized security management model works on the basis that all new privilege assignments and privilege assignment modifications made to existing privileges are performed through one governing group. This management model has the benefit of greater security than the decentralized security management model, but at the expense of scalability.
C: Decentralized security management model is the correct answer.
D: Decentralized security management model is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 804:

Which auditing method verifies that the organization has the necessary procedures, policies and mechanisms for dealing with emergencies and catastrophes?

A. Escalation audits.
B. Usage audits.
C. Privilege audits.
D. All of the above.

Answer: A

Explanation:
Escalation audits verify that the organization has the necessary procedures, policies and mechanisms for dealing with emergencies and catastrophes. This type of auditing can assist in ensuring that an organization's procedures are operating correctly.
Incorrect Answers:
B: Usage audits assist with ensuring that all computer systems and software are being used appropriately.
C: Privilege audits assist in ensuring that all user accounts, groups, and roles are correctly defined, and assigned correctly as well.
D: Escalation audits is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 390 - 392.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 805:

Which of the following statements is FALSE for role-based access control?

A. Access control is not managed on an individual user basis, but on a group basis.
B. Access control is a combination of mandatory and discretionary methods.
C. Group members cannot pass on rights and privileges to other users.
D. Users are grouped according to common access needs and job function.

Answer: C

Explanation:
After users are placed into groups, those group members are allowed to pass on rights and privileges to other users
Incorrect Answers:
A, B, D: These statements are TRUE
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 392-393.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter

---

QUESTION 806:

Which of the following is based on granting users access to all the systems, applications and resources they need, when they start a computer session?

A. Principle of single sign-on (SSO).
B. Role-Based Access Control (RBAC) method.
C. Centralized privilege management.
D. None of the above.

Answer: A

Explanation:
The principle of single sign-on (SSO) is based on granting users access to all the systems, applications and resources they need, when they start a computer session. The SSO capability is usually provided by a directory service, with a digital certificate being used to authenticate the user. Once authenticated, the user is granted access to the appropriate systems and resources.
Incorrect Answers:
B: Role-Based Access Control (RBAC) is an access control method where users have

one or multiple roles that allow access to specific information. Administrators usually group users and then assign MAC permissions based on the role in the company.
C: Centralized privilege management is one of the features provided by the principle of single sign-on. Centralized system management allows administrators to gain expertise on planning and controlling access rights and privileges.
D: The principle of single sign-on (SSO) is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 388 - 389.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter

---

QUESTION 807:

When configuring auditing for your systems, which of the following should be monitored?

A. Monitor successful attempts and failed attempts to access resources.
B. Monitor failed attempts to exercise privileges and access resources.
C. Monitor successful and failed attempts to access resources, and successful and failed attempts to exercise privileges.
D. Monitor successful attempts and failed attempts to exercise privileges.
E. Monitor successful attempts and failed attempts to access resources, and failed attempts to exercise privileges.

Answer: C

Explanation:
You should monitor successful and failed attempts to access resources, and successful and failed attempts to exercise privileges.
Incorrect Answers:
A, B, D, E: These statements do not include the complete answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 390 - 392.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 808:

Which access control method allowsusers to have some level of flexibility on how information is accessed, but at the expense of increasing the risk of unauthorized disclosure of information?

A. Mandatory Access Control (MAC) method
B. Discretionary Access Control (DAC) method
C. Role-Based Access Control (RBAC) method.
D. All of the above

Answer: B

Explanation:
The Discretionary Access Control (DAC) method enables users to set permissions when necessary, but within the specific guidelines of the broader MAC guidelines. This method allows users to have some level of flexibility with regard to the manner in which information is accessed. While the DAC method allows greater flexibility than the MAC method, the risk of unauthorized disclosure is increased.
Incorrect Answers:
A: The Mandatory Access Control (MAC) is centrally controlled and managed, where all access capabilities are predefined and users have no influence on permissions, nor can they share information that has not been previously established by administrators. Here, administrators make all necessary changes. The MAC method enforces a rigid model of security.
C: The Role-Based Access Control (RBAC) method focuses on group management and not on users, by implementing access according to job function or responsibility. In this method, users have one or multiple roles that allow access to specific information. Administrators usually group users and then assign MAC permissions based on the role in the company.
D: Discretionary Access Control (DAC) is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 392-393.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter

---

QUESTION 809:

Monitoring changes to the current security policy represents the best way to audit which element?

A. Privilege
B. Usage
C. Privilege escalation
D. All of the above.

Answer: A

Explanation:

The best way in which to monitor privilege is to monitor changes to the current security policy.
Incorrect Answers:
B, C, D: These are incorrect options.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 390 - 392.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 810:

Which security management model works on the basis that all new privilege assignments and privilege assignment modifications made to existing privileges are performed through one governing group?

A. Centralized security management model.
B. Decentralized security management model.
C. Both of the above.
D. None of the above.

Answer: A

Explanation:
The centralized security management model works on the basis that all new privilege assignments and privilege assignment modifications made to existing privileges are performed through one governing group. This management model has the benefit of greater security than the decentralized security management model, but at the expense of scalability.
Incorrect Answers:
B: A decentralized security management model works on the basis that security-specific responsibilities are delegated between employees at different locations. While decentralized management is less secure than centralized security, it provides greater scalability.
C: Centralized security management model is the correct answer.
D: Centralized security management model is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 811:

Which access control method would you need to implement if you want to use a group management approach to defining access to company resources and data, so that you can define access according to job function or responsibility?

A. Mandatory Access Control (MAC) method
B. Discretionary Access Control (DAC) method
C. Role-Based Access Control (RBAC) method.
D. All of the above

Answer: C

Explanation:
The Role-Based Access Control (RBAC) method focuses on group management and not on users, by implementing access according to job function or responsibility. In this method, users have one or multiple roles that allow access to specific information. Administrators usually group users and then assign MAC permissions based on the role in the company.
Incorrect Answers:
A: The Mandatory Access Control (MAC) is centrally controlled and managed, where all access capabilities are predefined and users have no influence on permissions, nor can they share information that has not been previously established by administrators. Here, administrators make all necessary changes. The MAC method enforces a rigid model of security.
B:
The Discretionary Access Control (DAC) method enables users to set permissions when necessary, but within the specific guidelines of the broader MAC guidelines. This method allows users to have some level of flexibility with regard to the manner in which information is accessed. While the DAC method allows greater flexibility than the MAC method, the risk of unauthorized disclosure is increased.
D: Role-Based Access Control (RBAC) is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 392-393.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter

---

QUESTION 812:

Which of the following environments are using the principle of single sign-on to grant users access for accessing resources?

A. Novell eDirectory.
B. Kerberos.
C. Microsoft Active Directory.
D. All of the above.

Answer: D

Explanation:
Each of these environments uses the principle of single sign-on to grant users access for accessing resources.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 388 - 389.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 813:

Which auditing method assists in ensuring that all user account, groups, and roles are correctly defined and assigned correctly?

A. Escalation audits.
B. Usage audits.
C. Privilege audits.
D. All of the above.

Answer: C

Explanation:
Privilege audits assist in ensuring that all user accounts, groups, and roles are correctly defined and assigned.
Incorrect Answers:
A: Escalation audits verify that the organization has the necessary procedures, policies and mechanisms for dealing with emergencies and catastrophes. This type of auditing can assist in ensuring that an organization's procedures are operating correctly.
B: Usage audits assist with ensuring that all computer systems and software are being used appropriately.
D: Privilege audits is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 390 - 392.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 814:

On the subject of security management models, identify the statement that is TRUE?

A. While a centralized security management model is less secure than decentralized security, it provides greater scalability
B. While a decentralized management model has the benefit of greater security, it provides less scalability than a centralized security management.
C.
Decentralized security involves the process of assigning all new privileges through multiple governing groups, located at different location.
D. The centralized security management model works well in small networks.

Answer: C

Explanation:
Decentralized security involves the process of assigning all new privileges through multiple governing groups, located at different location. In this model, security-specific responsibilities are delegated between employees at different locations.
Incorrect Answers:
A: While a decentralized security management model is less secure than centralized security, it provides greater scalability
B: While a centralized management model has the benefit of greater security, it provides less scalability than a decentralized security management.
D: The decentralized security management model works well in small networks.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 815:

Which of the following is FALSE for the MAC access method?

A. Users are allowed to change permissions or rights that are associated with objects.
B. Enforces a rigid model of security.
C. Security breaches are easy to identify, investigate and correct.
D. All statements are TRUE.

Answer: A

Explanation:
With the MAC access method, administrators, and not users are allowed to change permissions or rights that are associated with objects.
Incorrect Answers:
B, C: These statements are TRUE

C: All statements are not TRUE, because option A is FALSE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 392-393.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter

---

QUESTION 816:

Which auditing method assists with ensuring that all computer systems and software are being used appropriately?

A. Escalation audits.
B. Usage audits.
C. Privilege audits.
D. All of the above.

Answer: B

Explanation:
Usage audits assist with ensuring that all computer systems and software are being used appropriately.
Incorrect Answers:
A: Escalation audits verify that the organization has the necessary procedures, policies and mechanisms for dealing with emergencies and catastrophes. This type of auditing can assist in ensuring that an organization's procedures are operating correctly.
C: Privilege audits assist in ensuring that all user accounts, groups, and roles are correctly defined and assigned correctly.
D: Usage audits is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 390 - 392.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 9, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 817:

From the options, which details a specific advantage of implementing a single sign-on technology?

A. Users must log on twice at all times.
B. You can configure system wide permissions.
C. Multiple applications can be installed.

D. Multiple directories can be browsed.

Answer: D

Explanation:
A single sign-on allows a user to authenticate one to the system, allowing them to access all of the applications and systems they have permissions to without requiring them to authenticate to each resource.
Incorrect Answers:
A: A single sign-on allows a user to authenticate one to the system, not twice.
B: Thesingle sign-on is an authentication process, which allows users to log on to the system. It is not an authorization system. An authorization system uses permissions to determine which resources an authenticated user is able to access, and their levels of access.
C: Thesingle sign-on is an authentication process, which allows users to log on to the system. It does not provide authenticated users with permissions to perform operations.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 388-389.

QUESTION 818:

Which of the following coorectly specifies where user accounts and passwords are stored in a decentralized privilege management environment?

A. User accounts and passwords are stored on a central authentication server.
B. User accounts and passwords are stored on each individual server.
C. User accounts and passwords are stored on no more than two servers.
D.
User accounts and passwords are stored on a server configured for decentralized management.

Answer: B

Explanation:
In a decentralized management system, user accounts and passwords stored on each server throughout the network.
Incorrect Answers:
A, D: A single server cannot be configured for decentralized management as management would then be centralized on one server.
C: In a decentralized management system, user accounts and passwords stored on each server in the network. Depending on the size of the network, this would probably be more than two servers.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 389.

QUESTION 819:

You work as the security administrator at Certkiller .com. One morning you discover that clients can no longer navigate web sites which have been created for them.
What is the most likely cause of the issue?

A. The incorrect permissions have been assigned for the web sites.
B. The server is located in a DMZ (Demilitarized Zone).
C. IP (Internet Protocol) filtering has been enabled for the web sites.
D. The server has a heavy processing load.

Answer: A

Explanation:
By having the authority to access the controlled sites, you will be allowed to navigate them. If they are not configured correctly or you do not have the correct access privileges, you will not be allowed to navigate that site.
Incorrect Answers:
B: A DMZ is a security zone that is separated from the internal network by one or more firewalls. However, servers in the DMZ is accessible from the internal network and from the internet.
C: Sites that have IP filtering will prevent access to that site rather. However, users are not able to navigate the site. We can therefore assume that they can access the site.
D: Heavy traffic would make it difficult to navigate the site as bandwidth usage would be high. However, site navigation would be slow rather than impossible.
References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, pp. 365-366.

QUESTION 820:

When reviewing audit trails, what makes unique user IDs especially important?

A. Unique user IDs cannot be modified easily.
B. Unique user IDs establishes individual accountability.
C. Unique user IDs show which files and data were changed.
D. Unique user IDs triggers corrective controls.

Answer: B

Explanation:
Each user account has a unique user ID associated with it. These IDs uniquely identify an authenticated user, allowing you to track user activity once the user has logged on to the system. Thus, the user can be held accountable for his or her actions.
Incorrect Answers:

A: User IDs cannot easily be altered. However, this does not explain their usefulness in audit trails.
C: User IDs do not show which files were changed, but which user account was used to change a file.
D: User IDs do not trigger corrective controls. They uniquely identify a user account.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 14.

QUESTION 821:

You work as the security administrator at Certkiller .com. One morning you discover that a user named Mia Hamm has used her user account to log on to a network server. Mia has then executed a program and been able to perform operations which only a network administrator or security administrator should be able to. What type of attack has occurred?

A. Trojan horse.
B. Privilege escalation attack.
C. Subseven back door.
D. Security policy removal.

Answer: B

Explanation:
A user obtaining access to a resource they would not normally be able to access. This is done inadvertently by running a program with SUID (Set User ID) or SGID (Set Group ID) permissions - or by temporarily becoming another user.
Incorrect Answers:
A: A Trojan horse is a malicious program that may be included as an attachment or as part of a useful installation program. It can be used to create a back door or replace a valid program during installation.
C: A back door is a program or configuration that is designed to allow unauthenticated access to a system. These can be legitimate applications such as Symantec's PC Anywhere, or malicious code such as SubSeven or T0rnkit.
D: Removing a security policy would not provide a user with more privileges as permissions and privileges needs to be explicitly granted.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 80, 388.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 30, 169.
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 80.

QUESTION 822:

Which of the following statements best defines what chain of custody is?

A. Describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally.
B. Represents a well-documented log that shows who collected the evidence and had access to each piece of evidence.
C. Is a policy that outlines how the organization handles and responds to a computer security incident.
D. Defines the procedure of trying to determine the very basic situation that resulted in the computer security incident.

Answer: B

Explanation:
Chain of custody represents a well-documented log which shows who collected evidence and had access to each piece of evidence. It is a log that contains the history of evidence which was collected and should include each event that was discovered.
Incorrect Answers:
A: Computer forensics describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally. Collected evidence has to be preserved to maintain its legal usability.
C: An incidence response policy is a policy that outlines how the organization handles and responds to a computer security incident.
D: Root cause analysis refers to the procedure of trying to determine the very basic situation that resulted in the computer security incident.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 404.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 823:

The concept of forensic analysis involves a standard approach or process. Choose the correct combination of steps for this process.

A. Acquire the evidence.
B. Authenticate the evidence.
C. Analyze the evidence
D. Collect the evidence and analyze the evidence.
E. A, B, C

Answer: E

Explanation:
The process of forensic analysis is a three part process that involves the following steps:
1. Acquire the evidence, 2. Authenticate the evidence, and 3. Analyze the evidence
Incorrect Answers:
A, B, C, D: These options only present part of the complete, correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 405 - 406.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 824:

When evidence is used in court, a number of factors must be TRUE for the actual data. Choose the option that is FALSE.

A. The data must be legally usable or admissible in court, and must represent a complete copy.
B. The data must have been modified while it was being collected, documented, and maintained or stored; so that is current.
C. The data must have been secured from when evidence gathering commenced, to the point at which it is in court.
D. The data must have been collected through a reliable procedure.

Answer: B

Explanation:
The data must NOT have been modified while it was being collected, documented, and maintained or stored. The chain of custody should contain a history of evidence which was collected.
Incorrect Answers:
A, C, D: These options are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 406 - 407.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 825:

Forensic investigations and response actions should define the actions for dealing with a number of situations. Which of the following actions should you perform when an attack is in progress? Choose all options that apply.

A. You should maintain connectivity for a possible return of the attacker.
B. You should maintain connectivity so that you can continuously collect data on the attack
C. You should remove all affected systems immediately.
D. You should remove the affected systems for immediate evidence collection and to recover the system.

Answer: B, C

Explanation:
While an attack is ongoing, you should maintain connectivity for continued data collection on the attack and also remove all affected systems immediately.
Incorrect Answers:
A, D: These are actions which are typically performed once the attack has ended.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 826:

Keeping all relevant information on the attack or intrusion and using a previously defined procedure to secure and assess all relevant information on the attack, both onsite and offsite is the processes that describes which of the following?

A. Collecting evidence
B. Authenticating evidence
C. Preserving evidence
D. All of the above

Answer: C

Explanation:
Preserving evidence is the process that involves keeping all relevant information on the attack of intrusion and using a previously defined procedure to secure and access all relevant information on the attack, both onsite and offsite.
Incorrect Answers:
A: Collecting evidence involves automatic and manual methods of gathering evidence of an intrusion. You can use a network sniffer to collect evidence. You can also collect relevant data from sources such as the hard disk, RAM, system cache.
B: Authenticating evidence is the process which proves that the evidence presented is in

fact the evidence which was collected. Here, encryption and time stamping is usually used to both preserve and authenticate collected data.
D: Preserving evidence is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 408 - 409.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 827:

Which of the following is a definition of computer forensics?

A. Describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally.
B. Represents a well-documented log which shows who collected the evidence and had access to each piece of evidence.
C. Is a policy that outlines how the organization handles and responds to a computer security incident.
D. Defines the procedure of trying to determine the very basic situation that resulted in the computer security incident.

Answer: A

Explanation:
Computer forensics describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally. Collected evidence has to be preserved to maintain its legal usability.
Incorrect Answers:
B: Chain of custody represents a well-documented log which shows who collected the evidence and had access to each piece of evidence. It is a log that contains the history of evidence which was collected and should include each event that was discovered.
C: An incidence response policy is a policy that outlines how the organization handles and responds to a computer security incident.
D: Root cause analysis refers to the procedure of trying to determine the very basic situation that resulted in the computer security incident.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 404.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 828:

Automatic collection of evidence involves the collection of evidence using a number of tools. Choose the option that is FALSE?

A. Intrusion detection systems (IDSs).
B. Monitoring tools.
C. Specialized tools that collect evidence from hard drives, system cache, CPU caches, RAM and virtual memory.
D. Network data analysis tools.

Answer: C

Explanation:
Because of the nature of hard drives, system cache, CPU caches, RAM and virtual memory; investigating and collecting evidence from these components is usually done manually. Running monitoring tools on these system components is not automated. There is however specialized tools which you can use, to assist you in collecting data in an orderly manner, so that it is legally useable.
Incorrect Answers:
A, B, D: These are all methods which are used to automatically acquire evidence.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 405.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 829:

Which of the following tools is NOT a computer forensic tool or a provider that offers computer forensic tools?

A. EnCase
B. ASR Data
C. Tripwire
D. Foundstone

Answer: C

Explanation:
Tripwire is a popular system integrity verifier (SIV). Tripwire examine the file structure

of a system to determine whether any system files were deleted or modified by an attacker
Incorrect Answers:
A: EnCase is a forensic tool from Guidance Software.
B: ASR Data is a provider of forensic tools for Macintosh and Linux.
D: Foundstone is a provider of forensic tools for Microsoft Windows systems.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3

QUESTION 830:

Which of the following concepts pertain to the process which proves that evidence presented is in fact the evidence which was collected?

A. Collecting evidence
B. Authenticating evidence
C. Preserving evidence
D. All of the above

Answer: B

Explanation:
Authenticating evidence is the process which proves that evidence presented is in fact the evidence which was collected. Here, methods such as encryption and time stamping are usually used to both preserve and authenticate collected data.
Incorrect Answers:
A: Collecting evidence involves the automatic and manual methods of gathering evidence of an intrusion. You can use a network sniffer to collect evidence and collect the relevant data from sources such as the hard disk, RAM, system cache.
C: Preserving evidence is the process that involves keeping all relevant information on the attack of intrusion and using a previously defined procedure to secure and access all relevant information on the attack, both onsite and offsite.
D: Authenticating evidence is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 408 - 409.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 831:

Forensic investigations and response actions should define the actions for dealing with a number of situations. Which of the following actions should you perform

once an attack is over? Choose all options that apply.

A. You should maintain connectivity for a possible return of the attacker
B. You should maintain connectivity so that you can continuously collect data on the attack
C. You should remove all affected systems immediately.
D. You should remove the affected systems for immediate evidence collection and to recover the system.

Answer: A, D

Explanation:
Once the attack is over, you should continue to maintain connectivity for the possible return of the attacker. You should also remove the affected systems for immediate evidence collection and to recover the system.
Incorrect Answers:
B, C: These are actions typically performed while the attack is being performed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 832:

On the topic of an incidence response policy, choose the statement that is TRUE.

A. Describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally.
B. Represents a well-documented log which shows who collected the evidence and had access to each piece of evidence.
C. Represents the rules that outlines how the organization handles and responds to a computer security incident.
D. Defines the procedure of trying to determine the very basic situation that resulted in the computer security incident.

Answer: C

Explanation:
An incidence response policy is a policy that outlines how the organization handles and responds to a computer security incident.
Incorrect Answers:
A: Computer forensics describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally. Collected evidence has to be

preserved to maintain its legal usability.
B: Chain of custody represents a well-documented log which shows who collected the evidence and had access to each piece of evidence. It is a log that contains the history of evidence which was collected and should include each event that was discovered.
D: Root cause analysis refers to the procedure of trying to determine the very basic situation that resulted in the computer security incident
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 404.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 833:

Which of the following types of data collection involves using specialized software to collectevidence from hard drives, system cache, CPU caches, RAM and virtual memory?

A. Automatic data collection.
B. Intrusion detection.
C. Manual data collection.
D. All of the above.

Answer: C
Because of the nature of hard drives, system cache, CPU caches, RAM and virtual memory; investigating and collecting evidence from these components is usually done manually. Running monitoring tools on these system components is not automated. There is however specialized tools which you can use, to assist you in collecting data in an orderly manner, so that it is legally useable.
Incorrect Answers:
A, B: Automatic data collection occurs when the collection of evidence takes place using a number of tools, of which intrusion detection systems is one.
D: Manual data collection is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 405.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 834:

To preserve evidence, you need to adhere to a number of rules. Choose the one that

does not fit.

A. Document and keep all relevant information on the attack of intrusion until the investigation is over.
B. Store all preserved information on the attack both onsite and offsite.
C. Use a previously defined procedure to secure and access all relevant information on the attack, both onsite and offsite.
D. All information on the attack should be preserved while the investigation is being performed, and until legal action has been pursued.

Answer: A
On the topic of preserving evidence, you need to retain and secure all information on the attack while the investigation is being performed, and until legal action has been pursued
Incorrect Answers:
B, C, D: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 405.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 835:

On the topic of root cause analysis, choose the statement that is TRUE.

A. Describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally.
B. Represents a well-documented log which shows who collected the evidence and had access to each piece of evidence.
C. Represents the rules that outlines how the organization handles and responds to a computer security incident.
D. Defines the procedure of trying to determine the very basic situation that resulted in the computer security incident.

Answer: D

Explanation:
Root cause analysis refers to the procedure of trying to determine the very basic situation that resulted in the computer security incident.
Incorrect Answers:
A: Computer forensics describes the process of investigating and analyzing computer system security incidents, to determine how the incident occurred and to collect and document all probable evidence that can be used legally. Collected evidence has to be

preserved to maintain its legal usability.
B:
Chain of custody represents a well-documented log which shows who collected the evidence and had access to each piece of evidence. It is a log that contains the history of evidence which was collected and should include each event that was discovered.
C: An incidence response policy is a policy that outlines how the organization handles and responds to a computer security incident.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 404.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 836:

When should you remove all systems that were affected by an attack, for immediate evidence collection and system recovery purposes?

A. When an attack is in progress.
B. When an attack is over.
C. When an attack is being performed and also when it is over.

Answer: B

Explanation:
Once the attack is over, you should continue to maintain connectivity for a possible return of the attacker. You should also remove the affected systems for immediate evidence collection and to recover the system.
Incorrect Answers:
A: When an attack is in progress, you should remove all affected systems immediately, and maintain connectivity so that you can continuously collect data on the attack.
C: When an attack is over is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9

QUESTION 837:

Which of the following concepts involve using a network sniffer to acquire evidence, and gathering the relevant data on intrusions from sources such as the hard disk, RAM, system cache?

A. Collecting evidence
B. Authenticating evidence
C. Preserving evidence
D. All of the above

Answer: A

Explanation:
Collecting evidence involves the automatic and manual methods of gathering evidence of an intrusion. You can use a network sniffer to collect evidence and collect the relevant data from sources such as the hard disk, RAM, system cache.
Incorrect Answers:
B: Authenticating evidence is the process which proves that evidence presented is in fact the evidence which was collected. Here, methods such as encryption and time stamping are usually used to both preserve and authenticate collected data.
C: Preserving evidence is the process that involves keeping all relevant information on the attack of intrusion and using a previously defined procedure to secure and access all relevant information on the attack, both onsite and offsite.
D: Collecting evidence is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 408 - 409.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 11, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 838:

You work as the security administrator at Certkiller .com. You have become aware of a hacker accessing confidential company data from over the network.
Which of the following actions should you perform? Choose all correct answers.

A. Prevent members of the organization from entering the server room.
B. Prevent members of the incident response team from entering the server room.
C. Shut down the server to prevent the hacker from accessing more data.
D. Detach the network cable from the server to prevent the hacker from accessing more data.

Answer: A, D

Explanation:
You would want to prevent to possible contamination of evidence. This would be best achieved by preventing people other than the incident response team from entering the room. You could disconnect the network cable to prevent the hacker from gaining further data as this will not corrupt evidence.

Incorrect Answers:
B: When an incident occurs, the first thing that should be done is to document what is going on and notify the incident response team.
C: Shutting down the server would corrupt any evidence that is stored in RAM. This would result in a loss of evidence.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 101-102.

QUESTION 839:

You work as the security administrator at Certkiller .com. A hacker has recently accessed confidential company data from over the network. You have just secured the crime scene and now want to preserve evidence.
What should you do next? Choose all correct options.

A. Take photographs of all information being displayed on all monitors that was used to access the confidential data.
B. Document all messages being displayed by the computer.
C. Shut down the computer to prevent any other attacks that could end up changing your data.
D.
Collect all malfunctioning devices, and materials and equipment used in the crime scene for transport to another location.

Answer: A, B

Explanation:
When an incident occurs, the first thing that should be done is to document what is going on and notify the incident response team. You could document what is the incident by photographing information displayed on the monitors or by writing down messages displayed by the computer.
Incorrect Answers:
C: Shutting down the server would corrupt any evidence that is stored in RAM. This would result in a loss of evidence.
D: You should not touch or remove anything from the scene until the incident response team arrives.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 172-177, 385-386.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 101-102.

QUESTION 840:

Which of the following is a definition of a threat agent?

A. The probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
B. Anything that can result in the loss of an asset
C. The process of evaluating threats and vulnerabilities, and how these affect assets.
D. The security policies and procedures, firewalls, and all other mechanisms that can be implemented, based on the level of a risk to a specific asset.

Answer: B

Explanation:
A threat or threat agent refers to anything which can result in the loss of an asset.
Incorrect Answers:
A:
A risk is the probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
C: Risk assessment is the process of evaluating threats and vulnerabilities, and how these affect assets.
D: Security controls refers to security policies and procedures, firewalls, and all other mechanisms that can be implemented, based on the level of a risk to a specific asset.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 841:

Calculating risk involves a number of assessments which are then multiplied to determine the risk. Choose the correct combination of factors that should be assessed.

A. Threat and Vulnerability
B. Vulnerability and Impact
C. Threat and Impact
D. Threat and Vulnerability and Impact

Answer: D

Explanation:
Calculating risk involves assessing threats, vulnerability, and impact. When an assessments factor is zero, risk is zero.
Incorrect Answers:
A, B, C: These options present only part of the complete answer.

References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 842:

When it comes to assessing the impact of a specific threat compromising the assets of a company, you can use a multipoint scale. Which of the following would a high rating (5) indicate?

A. Minor damage.
B. Loss of the organization to operate.
C. Loss of data.
D. Denial of service.

Answer: B

Explanation:
A high rating on a multipoint scale would indicate the loss of the organization to operate or critical business damages.
Incorrect Answers:
A: Minor damage is indicated by a low rating (1).
C, D: Loss of data and a successful denial of service attack are usually indicated by a medium rating (3 - 4).
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 843:

Which of the following threats, specifically affects the hard drive and can lead to a loss of the actual drive, data and productivity? Choose all correct options.

A. Equipment or hardware failures.
B. Users deleting files.
C. Power outages.
D. Administrators performing incorrect configuration changes.

Answer: A, C

Explanation:
Common threats to hard drives are hardware failures and power outages.

Incorrect Answers:
B: Users deleting files is a threat more relevant for data of the organization.
D: Administrators performing incorrect configuration changes is usually a threat for database applications.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 844:

Internal and external threats to the network and data can be grouped into distinct categories. Into which category would earthquakes, fires, thunderstorms and floods fall?

A. Environmental threats
B. Natural threats
C. Human threats
D. All of the above

Answer: B

Explanation:
Earthquakes, fires, thunderstorms and floods are all examples of natural threats.
Incorrect Answers:
A: Environmental threats include conditions such as long-term power outages, chemical spills and pollutants that can harm the organization's assets.
C: Human threats involve human actions that can end up causing damages to the organization's assets.
D: Natural threats is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 845:

Which of the following is a definition of a risk?

A. The probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
B. Anything that can result in the loss of an asset.

C. The process of evaluating threats and vulnerabilities, and how these affect assets.
D. The security policies and procedures, firewalls, and all other mechanisms that can be implemented, based on the level of a risk to a specific asset.

Answer: A

Explanation:
A risk is the probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
Incorrect Answers:
B: A threat or threat agent refers to anything which can result in the loss of an asset.
C: Risk assessment is the process of evaluating of threats and vulnerabilities, and how these affect assets.
D: Security controls refers to security policies and procedures, firewalls, and all other mechanisms that can be implemented, based on the level of a risk to a specific asset.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 846:

Choose the FALSE statement?

A. A vulnerability can be a weakness in an asset.
B. A vulnerability can be a weakness in the environment in which an asset is located
C. A vulnerability can potentially cause harm to an asset
D. A vulnerability can be a weakness in configuration of an asset

Answer: C

Explanation:
A threat can potentially cause harm to an asset.
Incorrect Answers:
A, B, D: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 847:

In terms of assessing and prioritizing risks, which concept refers to the probability of an event occurring within a year?

A. Single loss expectancy (SLE)
B. Annualized rate of occurrence (ARO)
C. Annual loss expectancy (ALE).
D. All of the above.

Answer: B

Explanation:
The annualized rate of occurrence (ARO) signifies the probability of an event occurring within a year. This conclusion is usually based on referencing historical data.
Incorrect Answers:
A, C: Single loss expectancy and Annual loss expectancy (ALE) are monetary values assigned to data to reflect loss.
D: Annualized rate of occurrence (ARO) is the correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 848:

Into which category of threats would conditions such as long-term power outages and chemical spills fall?

A. Environmental threats
B. Natural threats
C. Human threats
D. All of the above

Answer: A

Explanation:
Environmental threats are conditions such as long-term power outages, chemical spills and pollutants that can harm the organization's assets.
Incorrect Answers:
B: Earthquakes, fires, thunderstorms and floods are all examples of natural threats.
C: Human threats involve human actions that can end up causing damages to the organization's assets.
D: Environmental threats is the correct answer.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 849:

Which of the following is a definition of risk assessment?

A. The probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
B. Anything that can result in the loss of an asset
C. The process of evaluating threats and vulnerabilities, and how these affect assets.
D. The security policies and procedures, firewalls, and all other mechanisms that can be implemented, based on the level of a risk to a specific asset.

Answer: C

Explanation:
Risk assessment is the process of evaluating of threats and vulnerabilities, and how these affect assets.
Incorrect Answers:
A: A risk is the probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
B: A threat or threat agent refers to anything which can result in the loss of an asset.
D: Security controls refers to security policies and procedures, firewalls, and all other mechanisms that can be implemented, based on the level of a risk to a specific asset.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 850:

Which of the following vulnerabilities does not directly affect the data of an organization?

A. An administrative mistake.
B. Lack of antivirus software.
C. Important information known only by the IT manager.
D. Misconfigured software.

Answer: C

Explanation:
Important information known only by the IT manager usually has an associated risk of loss of expertise to the IT Manager asset of the company.
Incorrect Answers:
A, B, D: All of these vulnerabilities have a direct impact on loss of data of the organization.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 851:

Which of the following would typically be involved in identifying and valuing assets?

A. IT Manager
B. Accountants
C. Security administrators
D. All of the above.

Answer: B

Explanation:
Because of assets having a depreciation value, accountants are usually involved in identifying and valuing assets.
Incorrect Answers:
A, C: The IT manager and security administrators should know how to identify assets. They should also be aware of how valuable each asset is to the organization.
D: Accountants is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 852:

Into which category of threats would situations such human actions that can end up causing damages to the organization's assets fall?

A. Environmental threats
B. Natural threats
C. Human threats
D. All of the above

Answer: C

Explanation:
Human threats involve human actions that can end up causing damages to the organization's assets
Incorrect Answers:
A: Environmental threats are conditions such as long-term power outages, chemical spills and pollutants that can harm the organization's assets.
B: Earthquakes, fires, thunderstorms and floods are all examples of natural threats.
D: Human threats is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 853:

What is a vulnerability?

A. The probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
B. Anything that can result in the loss of an asset
C. A weakness in an asset, or the configuration of an asset, or environment in which it is located.
D. The process of evaluating threats and vulnerabilities, and how these affect assets.

Answer: C

Explanation:
A vulnerability refers to a weakness in an asset, or the configuration of an asset, or environment in which it is located.
Incorrect Answers:
A: A risk is the probability of a specific threat resulting in a vulnerability that will end up causing some form of damage to a company's asset.
B: A threat or threat agent refers to anything which can result in the loss of an asset.
D: Risk assessment is the process of evaluating of threats, vulnerabilities, and how these affect assets. A risk is the probability of a specific threat resulting in a vulnerability that

will end up causing some form of damage to a company's asset.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 32 - 33.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 2
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 854:

You work as the security administrator at Certkiller .com. You must define new asset protection policies for Certkiller .com. Assets must be weighted on a scale of importance, ranging from 1 to 10, with 10 being the highest level of importance.
You have to comply with the following weights:
* Internet connectivity has a weight of 8.
* Servers have a weight of 9.
* Software has a weight of 3.
* Staff has a weight of 6.
* Workstations have a weight of 7.
Using these weights as the basis, which order should you use to create the new policies?

A. Internet policy, server security, workstation security policy, personnel safety policy, software policy.
B. Server security policy, Internet policy, workstation security policy, software policy, personnel safety policy.
C. Software policy, personnel safety policy, workstation security policy, Internet policy, server security policy.
D. Server security policy, Internet policy, workstation security policy, personnel safety policy, software policy.

Answer: D

Explanation:
You should generate policies for the most important assets first. In this scenario, servers have the highest importance, followed by Internet connectivity, workstations, personnel and then software.
Incorrect Answers:
A: Policies should be generated for the most important assets first. In this scenario, servers have a higher level of importance than Internet connectivity. Thus, a server security policy should be generated before an Internet plicy.
B: Policies should be generated for the most important assets first. In this scenario, personnel has a higher importance than software. Thus policies for personnel should be generated before policies for software.
C: Policies should be generated for the most important assets first, not for the least

important assets. In this scenario, servers have the highest importance, followed by Internet connectivity, workstations, personnel and then software.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 791-792.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION 855:

Choose the option that defines why you would implement security policies, procedures, and settings after you have identified risks that an organization's assets are exposed to?

A. To eliminate all threats that could affect business continuity.
B. To manage the risks so as to minimize any problems that could arise because of them.
C. To implement security measures to the extent that each risk to which an asset may be exposed is addressed.
D. To ignore as much risks as possible so as to minimize company costs.

Answer: B

Explanation:
The purpose of risk analysis is to prepare for the possibility of risks occurring so as to minimize the effect of such events and recovering from them.
Incorrect Answers:
A: Some environmental threats can be minimized but not eliminated.
C: Implementing countermeasure against all risks, especially environmental risks such as earthquakes and hurricanes, would require a large amount of capital and may not make economic sense.
D: If risks are to be ignored, then there is no need for a risk analysis.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 33-35.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION 856:

Choose the option that contains a fundamental risk management assumption.

A. Computers are only completely secure after you have installed all vendor patches.
B. Computers are only completely secure when it has an effective password.
C. Computers can never be completely secure.
D. Computers are only completely secure when one user uses it.

Answer: C

Explanation:
There is no way to bullet proof a computer's security. There are too many variables to consider.
Incorrect Answers:
A: Vendor patches are reactive attempt to fix vulnerabilities. They are not proactive. Thus other as yet unknown vulnerabilities might remain.
B: Passwords can be cracked, guessed or spoofed.
D: Computers can never be secure, regardless of the how many people use it.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 33-35.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION 857:

From the list of options, which stipulates the primary reason why any organization would perform risk analysis?

A. The organization wants to identify vulnerabilities to its systems.
B. The organization wants to quantify the impact of potential threats in relation to loss of business continuity costs.
C. The organization wants to determine the costs of implementing counter measures.
D. The organization wants to delegate responsibility.

Answer: B

Explanation:
The purpose of risk analysis is to prepare for the possibility of risks occurring so as to minimize the effect of such events, as well as the cost involved in recovering from them.
Incorrect Answers:
A: Identifying which vulnerabilities a system may be exposed to is one aspect of risk analysis. Risk analysis is also concerned with environmental risks, the costs of recovering from an event and the impact an event might have should it occur.
C: Identifying cost to implement counter measures is one aspect of risk analysis. Risk analysis is also concerned with environmental risks, vulnerabilities, and the impact an event might have should it occur.
D: Risk analysis in not concerned with delegating responsibility.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 33-35.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 172.

QUESTION 858:

What is the best reason for including business impact analysis in the business continuity planning process?

A. To test the authenticity of data obtained from risk analysis.
B. To agree formally, on maximum acceptable downtime levels.
C. To create the structure for drawing up tests so that you can determine the effectiveness of your business continuity plans.
D. To meet all documentation requirements of the insurance companies being used to cover the risks of system and data important for business continuity.

Answer: B

Explanation:
An impact analysis is when you plan out a worst case disaster scenario and illustrate just how much business a commpany can lose; then estimate the price of the best solution. From there you start compromising, with a cost factor analysis to factor out how much a solution and its risk reduction benefits would cost versus the probability of lost business and peace of mind. During which the company formally decides how much downtime they can afford to lose, and ends up implementing a solution accordingly.
Incorrect Answers:
A: A risk analysis is the second component of a business continuity plan. It is concerned with the probability of asset loss while a business impact analysis is concerned with critical business processes.
C, D: A business impact analysis is a component of a business continuity plan. It is concerned with critical business processes.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 253-254.

QUESTION 859:

Which of the following conditions is a valid reason why after backing up data on a server, that data could still be at risk?

A. When the recovery processes have not been tested.
B. When all users have not logged off while you have run the backup job.
C. When the backup media is moved offsite.
D. When an administrator discovers that a failure occurred when the backup job was run.

Answer: A

Explanation:
Recovery is equally as important a step as the original backup. Sadly, most system administrators make the assumption that their recovery will work flawlessly and fail to test their recovery procedures.
Incorrect Answers:
B: Reliable backups and recovery can be performed, regardless of whether users are logged on.

C: Keeping backup media on an off-site location is a good security precaution incase a natural disaster occurs.
D: If a failure occurs during the backup, then the data was always at risk. The failure would prevent the backup from being created; hence we cannot then speak of the data still being at risk as we have not moved beyond that.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 690-696.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp 363-368.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 156.

QUESTION 860:

Missing audit log entries could have serious consequences. What could be impacted most by missing audit log entries?

A. Capability of recovering destroyed data.
B. Capability of legally prosecuting a hacker.
C. Capability of assessing system vulnerabilities.
D. Capability of creating reliable system backups.

Answer: B
Audit logs play an important role in audit trails. They allow administrators to identify the user account used to perpetrate an attack and possibly prosecute the guilty party. Should the audit logs be lost or altered, thie will not be possible.
Incorrect Answers:
A, D: Auditlogs are not used for data backup or recovery purposes.
C: Auditlogs are used in audit trains, not in risk analysis.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 27-28, .
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, pp 101, 102.

QUESTION 861:

You work as the security administrator at Certkiller .com. You want to reduce vulnerabilities on your web server.
Which measure could you implement to accomplish your goal?

A. For all inbound connections, use a packet sniffing technology.
B. Ensure that the most recent vendor updates and patches are applied to the web server.
C. Enable auditing on the web server, and then assess the audit log entries.
D. Ensure that all inbound DNS (Domain Naming Service) requests are blocked.

Answer: B

Explanation:
Web servers must be accessible to internet users. Therefore it is not possible to protect them by using traditional techniques such as IP filtering or placing them behind firewalls. The best way to protect such servers is by ensuring that the latest security updates and patches are installed on the servers. These updates and patches are provided by the operating system vendor.
Incorrect Answers:
A: Depending on the amount of traffic that a web server could receive, the use of packet sniffing would require great overhead.
C: Auditing a web server is not really practical given the amount of audited data that would be collected.
D: The web server should need to be accessible to the Internet. Blocking incoming DNS requests to the server would make it impossible for users to access the server.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp 245, 478.
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 217.
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 108.

QUESTION 862:

Choose the method which will assist in ensuring that implemented security controls do not end up turning into vulnerabilities.

A. You should use security controls that are designed and implemented by the system vendor.
B. You should test the security controls.
C. You should implement the security controls at the application layer.
D. You should use security controls that can use multiple factors of authentication.

Answer: B

Explanation:
Any security controls, which include firewalls IDS systems, should be tested to ensure that they meet the organizations requirements. Untested security controls which may have been incorrectly configured would represent a potential vulnerability.
Incorrect Answers:
A, C: The vendor that designs and implements the security control, or the OSI layer at which the security control operates, will not lead to a vulnerability.
D: Multifactorauthentication is more secure and would not create a vulnerability.
References:
Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p 249.

QUESTION 863:

Choose the stage when you should test the system for vulnerabilities and try to defeat passwords, encryption and access lists.

A. Penetration testing.
B. Control testing.
C. Audit planning
D. Discovery testing.

Answer: A

Explanation:
Penetration testing is similar to system scanning and vulnerability scanning. It is used to determine if all known security vulnerabilities have been correctly addressed by producing an audit report listing all of the vulnerabilities of the system.
Incorrect Answers:
B, D: There is no such thing as control testing or discovery testing.
C: Audit planning is not related to vulnerability testing. Auditing is used to trace the user that violates a system while vulnerability testing is used to ensure that violations via known vulnerabilities do not occur.
References:
James Michael Stewart, Security+ Fast Pass, San Francisco, Sybex, 2004, p 33.

QUESTION 864:

Which method is most effective for testing the network for security vulnerabilities, and to determine existing security holes?

A. Perform a vulnerability assessment.
B. Perform a port scan.
C. Use sniffer software.
D. Install and then monitor an IDS (Intrusion Detection System)

Answer: A

Explanation:
A vulnerability assessment is a set of tools that are used to identify vulnerabilities in a network. It usually works by scanning the network for IP hosts and identifying the different services running on the hosts. Each service then probed to test the service for its security against known vulnerabilities.
Incorrect Answers:
B, C: Port scanning and sniffers are often used as part of a vulnerability assessment, however, on their own, they do not expose all known vulnerabilities.
D: An IDS does not detect vulnerabilities. It used known patterns of attacks and deviations from normal network behavior to identify possible attacks.

References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 301.

QUESTION 865:

What phrase can be used to refer to a company that has a security vulnerability assessment performed on the systems it uses?

A. The site is secure and cannot be hacked.
B. The company is committed to protect its data and customers.
C. The company is showing insecurity.
D. The company is showing an unnecessary fear of being attacked.

Answer: B

Explanation:
If a company relies on a system for its day to day business; they owe it to their shareholders and customers to protect their data. Usually the more important the comapany, the more incentive there is for on attack; so vulnerability assessment isn't a form of insecurity. Any site is vulnerable to a hacker, so vulnerability assessments are rarely done in vain.
Incorrect Answers:
A: It is not possible to create a hack proof system. It is only possible to ensure that known vulnerabilities are not used to hack a system. No precautions can be taken against as yet unknown vulnerabilities.
C, D: In today's interconnected networks, the threat of hackers is real. Taking precaution against hackers does not constitute a needless fear or insecurity on the part of the organization.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 11.

QUESTION 866:

Which of the following correctly defines when privileged accounts are most vulnerable?

A. Directly after successful remote login has been performed.
B. Directly after a privileged user has been terminated.
C. Directly after a default installation has been performed.
D. Directly after a full system backup has been performed.

Answer: B

Explanation:

When a disgruntled administrator is fired the system is most vulnerable until the fired administrator's user account is deleted. While his or her account is still operable, the fired administrator could login remotely and wreck havoc to the system.
Incorrect Answers:
A: Remote login is normal in a network environment. They do pose a security risk but there should be secure authentication methods in place for these logins.
C: Permissions must be explicitly granted. If permissions are not granted, then there are no permissions. During the default installation, the Administrator's account is the one with the most default permissions. These accounts are usually renamed to increase their security. However, this account is still protected by a password which the administrator enters during the installation.
D: Permissions must be explicitly granted. If permissions are not granted, then there are no permissions. No permissions are granted during backup and once the backup is restored, the permissions are retained.
References:
Mitch Tulloch, Microsoft Encyclopedia of Security, Redmond, Microsoft Press, 2003, p. 401.

QUESTION 867:

Which of the following concepts is a marketing strategy to promote the security stance and programs of the organization?

A. Security training
B. Security education
C. Security awareness
D. All of the above

Answer: C

Explanation:
Security awareness is a marketing strategy that promotes the security stance and programs of the organization.
Incorrect Answers:
A: Security training refers to various methods that are used to increase the involvement of users with regard to security and teach them how to perform certain functions.
B: Security education is an ongoing endeavor, aimed at researching and increasing security awareness and implementing security best practices.
D: Security awareness is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 868:

When providing security education, you should customize your programs to address different roles within the organization. Choose the correct combination of roles.

A. All staff, management
B. Management, technical staff
C. All staff, management, technical staff
D. Technical staff, all staff

Answer: C
When providing security education, you should customize your programs to specifically address different roles within the organization: All staff, Management, and Technical staff. Each of the above mentioned roles within the organization would have security concerns. For instance, everyone in the organization must understand the organization's security policies and procedures. All employees should be aware of the security measures and resources that deal with security breaches. Managers on the other hand would be more concerned with enforcing security policies and procedures, knowing which departments are impacted by which security policies, and the precise mechanisms at hand to deal with loss of productivity issues. Technical staff needs to be well educated on the different security methodologies and the various systems that can be implemented to control and enforce security.
Incorrect Answers:
A, B, D: These options present only part of the complete answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 869:

Which of the following methods represent effective security training?

A. Security websites
B. News servers
C. Logon access banners
D. Hands-on classroom training

Answer: D

Explanation:
Hands-on classroom training, aimed at those users which need to be educated on a

specific security task, is one of the more effective methods of security training.
Incorrect Answers:
A, B, C: Security websites, news servers, and logon access banners are usually included in security awareness programs which are aimed at the entire organization.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 870:

When providing security education, which of the following represents the goal of the program?

A. To make certain that users read all distributed security awareness messages.
B. To assist users in understanding threats, prevention mechanisms, and enforcement.
C. To show users how to encrypt mission-critical information.
D. All of the above

Answer: B
The purpose of security education should be an effort that assists users in understanding threats aimed at the organization and its assets, prevention mechanisms, and enforcement.
Incorrect Answers:
A: Security awareness involves using innovative methods to ensure that users continue to read distributed security awareness messages
C: Showing users how to encrypt mission-critical information is usually encompassed in security training for specific users. Usually, not all employees of the organization need to know how to encrypt mission-critical information
D: B is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 871:

Which of the following uses various methods to increase the involvement of users with regard to security and teach them how to perform certain functions?

A. Security training

B. Security education
C. Security awareness
D. All of the above

Answer: A

Explanation:
Security training refers to various methods that are used to increase the involvement of users with regard to security and teach them how to perform certain functions.
Incorrect Answers:
B: Security education is an ongoing endeavor, aimed at researching and increasing security awareness and implementing security best practices.
C: Security awareness a marketing strategy that promotes the security stance and programs of the organization.
D: Security training is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 872:

Which of the following roles within an organization must understand the organization's security policies and procedures, and also be aware of available security measures and resources that deal with security breaches?

A. All staff
B. Technical staff
C. Management
D. All of the above

Answer: A
Everyone must understand the organization's security policies and procedures. All users should also be aware of the security measures and resources in effect that deal with security breaches.
Incorrect Answers:
B: Technical staff needs to be well educated on the different security methodologies and the various systems that can be implemented to control and enforce security.
C: Managers are more concerned with enforcing security policies and procedures, knowing which departments are impacted by which security policies, and the precise mechanisms at hand to deal with loss of productivity issues.
D: All staff is the correct answer.
References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 873:

When communicating your security policies to new employers, which of these methods are not particularly favored?

A. Hands-on training
B. Handing the security document to the new employee and ensuring that it is signed before allowing him/her to access your systems.
C. Including the new employee in all security lectures and demonstrations.
D. Ensuring that the new employee is handed all new security newsletters.
E. Granting the employee access to the news servers so that he/she has access to all new published security articles.

Answer: B
Handing the security document to the new employee and ensuring that it is signed before allowing him/her to access your systems could be perceived as being aggressive. Forcing new employees to take in a pile of documents as soon as possible, and having them sign acceptance thereof, does not guarantee that your employees have taken in its content. More likely than not, your new employees will be intimated into signing the document, for fear of not being employed.
Incorrect Answers:
A, C, D, E: All new employees should be included in each of these.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 874:

Which of the following roles within an organization is concerned with knowing which departments are impacted by which security policies, and the precise mechanisms at hand to deal with loss of productivity issues?

A. All staff
B. Technical staff
C. Management

D. All of the above

Answer: C
Managers on are generally more concerned with enforcing security policies and procedures, knowing which departments are impacted by which security policies, and the precise mechanisms at hand to deal with loss of productivity issues.
Incorrect Answers:
A: Everyone must understand the organization's security policies and procedures and should be aware of the security measures and resources in effect that deal with security breaches.
B: Technical staff needs to be well educated on the different security methodologies and the various systems that can be implemented to control and enforce security.
D: Management is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 875:

Your security awareness program should encompass a number of security topics. Choose the option that is FALSE.

A. The security policies and practices of the organization.
B. Account and password selection policies.
C. Methods used by vendors to implement security in their products.
D. The role of various individuals within the organization.
E. Methods of preventing social engineering.

Answer: C
The methods used by vendors to implement security in their products is not usually part of the security awareness program, aimed at the entire organization. Rather, this is an issue that should be addressed to security administrators, network administrators and program developers.
Incorrect Answers:
A, B, D, E: These statements are all TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 876:

Which of the following roles needs to be well educated on the different security methodologies and the various systems that can be implemented to control and enforce security?

A. All staff
B. Technical staff
C. Management
D. All of the above

Answer: B
Technical staff needs to be well educated on the different security methodologies and the various systems that can be implemented to control and enforce security.
Incorrect Answers:
A: Everyone must understand the organization's security policies and procedures. They should also be aware of the security measures and resources in effect that deal with security breaches.
C: Managers are usually more concerned with enforcing security policies and procedures, knowing which departments are impacted by which security policies, and the precise mechanisms at hand to deal with loss of productivity issues.
D: Technical staff is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 416 - 419.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 3
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter9.

QUESTION 877:

Which of the following sets the ground rules for protecting the resources and assets of the organization?

A. Standards
B. Guidelines
C. Both of the above
D. None of the above

Answer: A

Explanation:
Standards set the ground rules for protecting the resources and assets of the organization.
Standards are rules which detail a specific result. Each standard must be complied with.
Incorrect Answers:

B: Guidelines differ to standards in that they do not need to be strictly complied with. Unlike standards, guidelines provision for professional judgment when faced with a situation.
C: Standards is the correct answer.
D: Standards is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 878:

Which of the following policies deal with defining how information is classified?

A. Notification policies.
B. Information classification policies.
C. Information destruction policies.
D. Information retention and storage policies.

Answer: B

Explanation:
Information classification policies deal with defining how information is classified. These policies are usually useful in assisting employees to understand the requirements of how information is used as well as data confidentiality.
Incorrect Answers:
A: Notification policies specify who should be contacted when information classifications need to be verified, when information is updated, and when changes are performed.
C: Information destruction policies specify the manner in which data should be destroyed when it is no longer needed.
D: Information retention and storage policies define how information is stored and for how long it should be retained/stored.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410 - 411.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 879:

Data classification deals with setting standards for how information is classified and evaluated. Which classification of data can end up significantly affecting business operations and can cause a financial loss if compromised?

A. Private information
B. Secret information
C. Confidential information
D. Public information

Answer: B

Explanation:
When secret information is compromised, the organization could be so badly affected that it ceases to operate, or it loses out financially. It is recommended that you encrypt secret information when it is both stored and sent over the network. You should also only allow staff who should access secret information, access to those systems hosting the information.
Incorrect Answers:
A: When private information is compromised, an organization usually ends up with its reputation, clients and employees tarnished. Users should not be able to access private information on public terminals.
C:
Confidential information could also possibly hinder business operations and lead to some financial loss. You should only allow staff who should access confidential information, access to those systems hosting the information.
D: Public information can be freely accessed, transmitted and distributed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 880:

Which of the following best describes configuration management policies?

A. To define which information should be backed up.
B. To define which information is backed up and how this is done.
C. To inform you on what is occurring on systems.
D. To specify procedures that define how hardware and software systems are modified, upgraded and retired.

Answer: D

Explanation:
Configuration management policies specify procedures that define how hardware and

software systems are modified, upgraded and retired.
Incorrect Answers:
A: A backup policy defines what should be backed up, as well as how any identified information is backed up.
B: The backup policy of the organization has a two-fold purpose: It should define what information needs to be backed up, and how the identified information is backed up.
C: Systems logs inform you on what is occurring on system.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410 - 412.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 881:

Which of the following can be used to ensure that required tasks are being performed regularly, and can also be used to track the assets of the organization?

A. System logs
B. Inventories
C. System architecture documentation
D. All of the above

Answer: A

Explanation:
Systems logs inform you on what is occurring on system. Logs can be used to ensure that required tasks are being performed regularly, and can also be used to track the assets of the organization.
Incorrect Answers:
B: Inventories can be used to verify the existence and availability of physical assets and software assets. You can use products such as CA Unicenter for asset management and inventory purposes. You should also perform regular inventories of classified information.
C: System architecture refers to hardware and software infrastructure of your systems. System architecture documents contain information on system architecture and configuration.
D: System logs is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 412 - 413.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 882:

On the topic of destroying information, choose the option that is FALSE?

A. Sensitive information must be shredded when no longer needed to reduce the possibility of it being used.
B. Erasing files on a computer removes the information from disk.
C. Disk drives must be zeroed out when computers are retired.
D. Magnetic media should be degaussed.

Answer: B

Explanation:
Erasing files on a computer does not mean that the information is automatically always removed from disk. You should use a utility to completely wipe the disk clean, and destroy all information.
Incorrect Answers:
A, C, D: These statements are TRUE.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410 - 411.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 883:

Data classification deals with setting standards for how information is classified and evaluated. Which classification of data should only those staff that need to access the data, be allowed to?

A. Private information
B. Secret information
C. Confidential information
D. All of the above

Answer: D

Explanation:
You should only allow staff who should access secret information, access to those systems hosting the information. You should only allow staff who should access confidential information, access to those systems hosting the information. The same is

true for private information.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 884:

Which of the following policies specify who should be contacted when information classifications need to be verified, and when information is updated?

A. Notification policies.
B. Information classification policies.
C. Information destruction policies.
D. Information retention and storage policies.

Answer: A

Explanation:
Notification policies specify who should be contacted when information classifications need to be verified, when information is updated, and when changes are performed.
Incorrect Answers:
B: Information classification policies deal with defining how information is classified. These policies are usually useful in assisting employees to understand the requirements of how information is used, as well as data confidentiality.
C: Information destruction policies specify the manner in which data should be destroyed, that is, when it is no longer needed.
D: Information retention and storage policies define how information is stored and for how long it should be retained/stored.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410 - 411.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 885:

Which of the following provisions for professional judgment when faced with a situation?

A. Standards
B. Guidelines
C. Both of the above

D. None of the above

Answer: B

Explanation:
Guidelines differ to standards in that they do not need to be strictly complied with. Unlike standards, guidelines provision for professional judgment when faced with a situation.
Incorrect Answers:
A: Standards set the ground rules for protecting the resources and assets of the organization. Standards are rules which detail a specific result. Each standard must be complied with.
C: Guidelines is the correct answer.
D: Guidelines is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 886:

What is the purpose of a backup policy?

A. To define which information should be backed up.
B. To define which information is backed up and how this is done.
C. To inform you on what is occurring on systems.
D. To specify procedures that defines how hardware and software systems are retired.

Answer: B

Explanation:
A backup policy of the organization has a two-fold purpose: It should define what information needs to be backed up, and how the identified information is backed up.
Incorrect Answers:
A: The backup policy also defines how any identified information is backed up.
C: Systems logs inform you on what is occurring on system
D: Configuration management policies specify procedures that define how hardware and software systems are modified, upgraded and retired.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 412.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 887:

Data classification deals with setting standards for how information is classified and evaluated. Which classification of data COULD end up affecting business operations if compromised?

A. Private information
B. Secret information
C. Confidential information
D. Public information

Answer: C

Explanation:
Confidential information could possibly hinder business operations and lead to some financial loss. You should only allow staff who should access confidential information, access to those systems hosting the information.
Incorrect Answers:
A: When private information is compromised, an organization usually ends up with its reputation, clients and employees tarnished. Users should not be able to access private information on public terminals.
B: When secret information is compromised, the organization could be so badly affected that it ceases to operate, or it loses out financially. It is recommended that you encrypt secret information when it is both stored and sent over the network. You should also only allow staff who should access secret information, access to those systems hosting the information.
D: Public information can be freely accessed, transmitted and distributed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 888:

Choose the option that best describes the purpose of information retention and storage policies?

A. Specifies who should be contacted when information classifications need to be verified, when information is updated, and when changes are performed.
B. Deals with defining how information is classified.
C. Specifies the manner in which data should be destroyed when it is no longer needed.
D. Defines how information is stored and for how long it should be retained or stored.

Answer: D

Explanation:
Information retention and storage policies define how information is stored and for how long it should be retained or stored.
Incorrect Answers:
A: Notification policies specify who should be contacted when information classifications need to be verified, when information is updated, and when changes are performed.
B: Information classification policies deal with defining how information is classified. These policies are useful in assisting employees to understand the requirements of how information is used as well as data confidentiality.
C:
Information destruction policies specify the manner in which data should be destroyed when it is no longer needed.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410 - 411.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 889:

Which of the following items for each system should be included in your system architecture documentation?

A. Operating system configuration, Hardware configuration, and Network configuration
B. Operating system configuration, Network configuration, and Applications.
C. Operating system configuration, Hardware configuration, and Applications.
D. Operating system configuration, Hardware configuration, Network configuration, and Applications

Answer: D

Explanation:
Your system architecture documentation should include Operating system configuration, Hardware configuration, Network configuration, and Applications information for each system.
Incorrect Answers:
A, B, C: These options present only part of the complete, correct answer.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 890:

Choose the option that verifies the physical existence of an organization's assets and as well as its availability.

A. System logs
B. Inventories
C. System architecture documentation
D. All of the above

Answer: B

Explanation:
Inventories can be used to verify the existence and availability of physical assets and software assets. You can use products such as CA Unicenter for asset management and inventory purposes. You should perform regular inventories of classified information.
Incorrect Answers:
A: Systems logs inform you on what is occurring on system. Logs can be used to ensure that required tasks are being performed on a regularly, and can also be used to track the assets of the organization.
C: System architecture documents contain information on system architecture and configuration.
D: Inventories is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 412 - 413.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 891:

Data classification deals with setting standards for how information is classified and evaluated. Which classification of data could cause an organization's reputation and its clients to be tarnished if compromised?

A. Private information
B. Secret information
C. Confidential information
D. Public information

Answer: A

Explanation:
When private information is compromised, an organization usually ends up with its reputation, clients and employees tarnished. Users should not be able to access private information on public terminals.
Incorrect Answers:
B: When secret information is compromised, the organization could be so badly affected that it ceases to operate, or it loses out financially. It is recommended that you encrypt secret information when it is both stored and sent over the network. You should also only allow staff who should access secret information, access to those systems hosting the information.
C: Confidential information could also possibly hinder business operations and lead to some financial loss. You should only allow staff who should access confidential information, access to those systems hosting the information.
D: Public information can be freely accessed, transmitted and distributed.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 892:

What is a backup of information?

A. A policy that defines which information is backed up and how this is done.
B. A set of data that is regularly removed from the system because it is not needed any longer.
C. A copy of a set of data that can be restored.
D. All of the above

Answer: C

Explanation:
A backup of information is a copy of a set of data that can be restored.
Incorrect Answers:
A: A backup policy of the organization defines what information needs to be backed up, and how the identified information is backed up.
B: An archive is a set of data that is regularly removed from the system because it is not needed any longer.
D: Option C is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 412.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.

Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 893:

Choose the option that best describes the purpose of information destruction policies?

A. Specifies who should be contacted when information classifications need to be verified, when information is updated, and when changes are performed.
B. Deals with defining how information is classified.
C. Specifies the manner in which data should be destroyed when it is no longer needed.
D. Defines how information is stored and for how long it should be retained or stored.

Answer: C

Explanation:
Information destruction policies specify the manner in which data should be destroyed when it is no longer needed.
Incorrect Answers:
A: Notification policies specify who should be contacted when information classifications need to be verified, when information is updated, and when changes are performed.
B: Information classification policies deal with defining how information is classified. These policies are useful in assisting employees to understand the requirements of how information is used as well as data confidentiality.
D: Information retention and storage policies define how information is stored and for how long it should be retained/stored.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 410 - 411.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 894:

Which of the following contains detailed information on system architecture and configuration?

A. System logs
B. Inventories
C. System architecture documentation
D. All of the above

Answer: C

Explanation:
System architecture refers to hardware and software infrastructure of your systems. System architecture documents contain information on system architecture and configuration. Your system architecture documentation should include Operating system configuration, Hardware configuration, Network configuration, and Applications information for each system
Incorrect Answers:
A: Systems logs inform you on what is occurring on system. Logs can be used to ensure that required tasks are being performed regularly, and can also be used to track the assets of the organization.
B: Inventories can be used to verify the existence and availability of physical assets and software assets. You can use products such as CA Unicenter for asset management and inventory purposes. You should perform regular inventories of classified information.
D: System architecture documentation is the correct answer.
References:
Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 412 - 413.
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.

QUESTION 895:

Data classification deals with setting standards for how information is classified and evaluated. Which classification of data can be freely accessed, transmitted and distributed?

A. Private information
B. Secret information
C. Confidential information
D. Public information

Answer: D

Explanation:
Public information can be freely accessed, transmitted and distributed.
Incorrect Answers:
A: When private information is compromised, an organization usually ends up with its reputation, clients and employees tarnished. Users should not be able to access private information on public terminals.
B: When secret information is compromised, the organization could be so badly affected that it ceases to operate, or it loses out financially. It is recommended that you encrypt secret information when it is both stored and sent over the network. You should also only

allow staff who should access secret information, access to those systems hosting the information.
C: Confidential information could also possibly hinder business operations and lead to some financial loss. You should only allow staff who should access confidential information, access to those systems hosting the information.
References:
Andy Ruth and Kurt Hudson, Security+ Certification Training Kit, Microsoft Press, Redmond, 2003, Chapter 10, Lesson 1.
Todd Bill, The Security+ Training Guide, QUE Publishing, Indianapolis, 2003, Chapter 9.