Ethical Hacking and Countermeasures

Version 6

Module LXVI

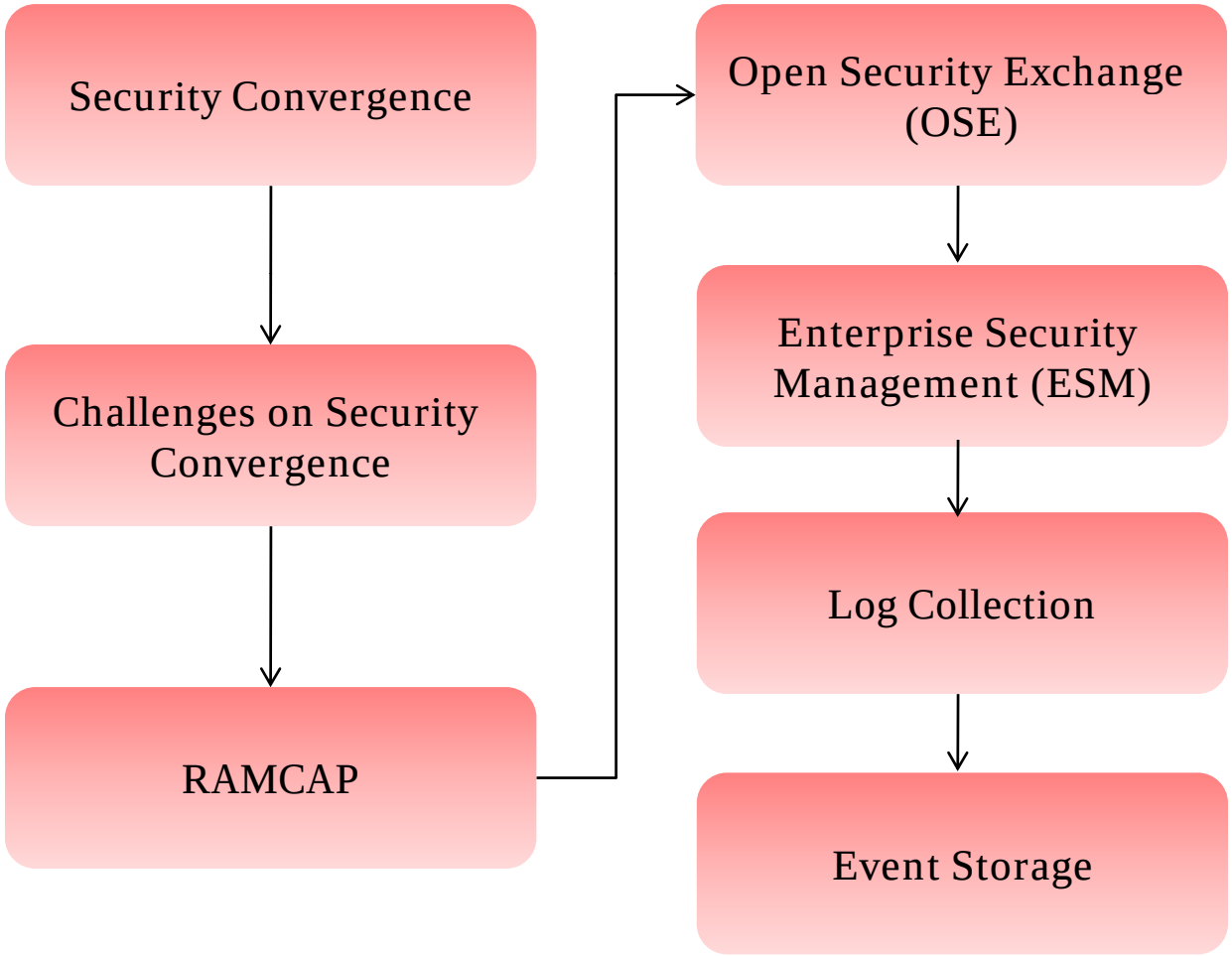
Security Convergence

Module Objective

This module with familiarize you with:

- Security Convergence
- Challenges on Security Convergence
- RAMCAP
- Open Security Exchange (OSE)
- Enterprise Security Management (ESM)
- Log Collection
- Event Storage

Module Flow



Security Convergence

Convergence is a process of reusing and blending various technologies to create new or improved capabilities and products

It is the integration of security functions and information into a common IP network

Security convergence can leverage technology to improve the performance of the security function both physically and logically

It is a three-pronged approach composed of technologies, security processes, and people

Challenges Confronting an Effective Security Convergence Policy

Understanding the challenges inherent in the original Internet design specifications

The ramifications of uncontrolled Internet growth and its effect on the administration policy

The security issues involved with the Transmission Control Protocol/Internet Protocol (TCP/IP)

Evolution of the Internet as a global platform for security solutions is expanding aggressively to accommodate convergence

Benefits of Using Risk Management in Planning IT Security Administration

Benefits for adopting a proactive and positive attitude towards IT security are:

- Better demonstration of IT security investment to the board
- More meaningful demonstration of business risk management to investors, especially the institutional investors that largely dictate stock prices
- Better demonstration of business risk management to customers
- Better employee awareness

RAMCAP

Risk Analysis and Management for Critical Asset Protection (RAMCAP) is a program initiated by Department of Homeland Security (DHS)

It is an innovative process for security policy based upon global risk assessment in collaboration with DHS

It promotes understanding of the various vulnerabilities that may lead attacker to select a particular target

It is composed of integrated steps to evaluate the threat potential, vulnerability, and possibility of a successful attack and its consequences

Open Security Exchange (OSE)

OSE integrates various components of the security infrastructure

It is a cross-industry forum dedicated to merge physical and IT security solutions across an enterprise

It provides the enterprise with increased operational efficiencies and intelligent security

It specifies Physical Security Bridge to IT Security (PHYSBITS) to assist in the integration of physical and IT security management

It provides technical integration on three levels:

- Common administration of users, privileges, and credentials
- Common strong authentication for accessing physical facilities and cyber systems through the use of dual-purpose credentials
- Common point of security management and event audit ability

CISO (Chief Information Security Officer)

CISO is typically focused on the issues involved with IT security and IT risk management

CISO focuses on information security strategy within an organization that includes:

- Information security mission development
- Information security office governance
- Information security policy development and management
- Information security training and awareness development
- Information security project portfolio development
- Supervision/management of ethical hackers and chief hacker officer

Elements of Building Secure Operations

Elements of fully secured enterprise operations include:

- A sound, comprehensive enterprise protection architecture augmented by a schema of well-documented, well-understood, and routinely practiced business processes
- A rigorous system for the detection, analysis of, and, when appropriate, alert to and protection from threats to enterprise operations and systems
- The ability to sustain continuity of operations during any conceivable threat
- Rapid recovery mechanisms to restore full operations once a threat is controlled
- The ability to analyze and apply forensics to determine what happens when an incident occurs and to incorporate lessons learned to improve future risk mitigation processes

Enterprise Security Management (ESM)

Enterprise Security Management (ESM) is a general term that has been applied to security event monitoring and analysis solutions

ESM is an enhancement and combination of:

- EEM Enterprise Event Management
- SIM Security Information Management
- SEM Security Event Management
- SIEM Security Information and Event Management

The focus of ESM is to allow an analyst to monitor an organization's infrastructure in real time, regardless of product, vendor, and version

ESM Deployment Strategies

ESM solutions can be deployed in standard, high-availability, and geographically dispersed configurations

ESM systems are designed to receive and process logs

Log collection appliances provide a solid solution for organizations to adopt an easy-to deploy appliance

In case there is no log aggregation strategy, it is possible to simply send logs directly from the point devices to the ESM manager

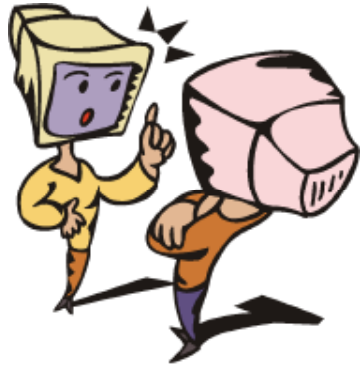
To move logs from point devices to the ESM manager, deploy log connectors at any natural aggregation points, such as device managers

Convergence of Network Operations and Security Operations

Network operation centers (NOCs) and Security operation centers (SOCs) are more focused on business impact than hardware and software impact

Separation of duties and checks and balances are important concepts to maintain when any groups converge

The NOC is concerned with keeping things moving efficiently and the SOC is concerned with security, rendered through analysis within the ESM



Log Collection

Log collection is important to increase operational efficiencies, reduce risk, and enhance an organization's security posture

A log collection mechanism needs to be scalable, extensible, and flexible

ESM solution needs to be able to process the raw log data and turn it into actionable information

Mechanism to collect logs is to simply send logs directly to the ESM manager for processing

The Log collectors installed on various operating systems listen for raw logs being sent to them, preprocess the logs, enrich them, and prepare them for transport

Log Normalization

In log normalization, each log data field is converted to a particular data representation and categorized consistently

Most common use of normalization is to store dates and times in a single format

Normalizing the data makes analysis and reporting much easier when multiple log formats are in use

In Normalization, the logs need to be parsed without deleting any information by default

Log parsing is the process of extracting data from a log so that the parsed values can be used as input for another logging process

Log Severity

Each log source may have a unique severity level assigned to it

The severity of what the point device discovered correlated with other logs, asset information, business relevance, and other factors can yield an overall priority score within most ESMs

Device severity captures the language used by the data source to describe its interpretation of the danger posed by a particular log

Connector severity is the translation of device severity into a normalized value

Log Time Correction

An important factor in log analysis is time

In an idealistic situation, everything would be synced with the Network Time Protocol (NTP) and the NTP device would get its time from a reliable source

Most ESM connectors are configurable to allow for time correction

Log Categorization

A methodology for describing logs, which enables analysts to understand the real significance of a particular log as reported from different devices is called categorization

Categorization can be applied to several other fields within a log besides the actual field expressing the content of the log

It includes detailing the log's behavior, which techniques it uses, its outcome, and various other categories

Event Storage

ESMs uses a variety of databases, mostly enterprise-level databases, due to its advanced features

For data management, backups, and data restoration, many ESM solutions divide the stored events into logical segments

Regardless of the data being stored offline or online, ESMs utilizes compression and indexing techniques to save space and reduce search times respectively

ESMs feature hashing of the database partitions to ensure that a tape loaded from several years ago has content that matches what was backed up

Discovering and Interacting with Patterns

Pattern discovery features are designed to identify patterns among events that an analyst may not have been specifically looking for

An analyst may desire to run a pattern discovery sweep across an hour, day, month, or more of the historic data in search of patterns

Interactive discovery reports are dynamic and allow an analyst or even a nontechnical individual to review and manipulate the data

Events can be displayed in various graphical representations, sections can be highlighted, and the output can be easily shared and reviewed among various individuals performing an investigation

Discovering and Interacting with Patterns: Data Sources

To detect fraudulent activity and anomalies in user's behavior, you need to analyze more than just intrusion detection system data

Similar to intrusion detection systems, Information Leak Prevention (ILP) products go through the content as it crosses the network

E-mail transactions generally are not analyzed in real time; they have been used as part of forensic investigations

Intelligent Platform Management Interface (IPMI) Standard

IPMI is a standard for monitoring and managing computer systems

They are out-of-band interfaces, meaning that even if a system is powered down, communication is still possible

IPMI standard consists of the following key information:

- Packet format
- Other communication mechanisms
- Sensor codes
- How to retrieve information

Summary

- Security convergence can leverage technology to improve the performance of the security function
- Security convergence is the identification of security risks and interdependencies between business functions and processes within the enterprise
- RAMCAP is an innovative process for security policy based upon global risk assessment in collaboration with DHS
- Enterprise Security Management (ESM) is a general term that has been applied to security event monitoring and analysis solutions
- IPMI is a standard for monitoring and managing computer systems