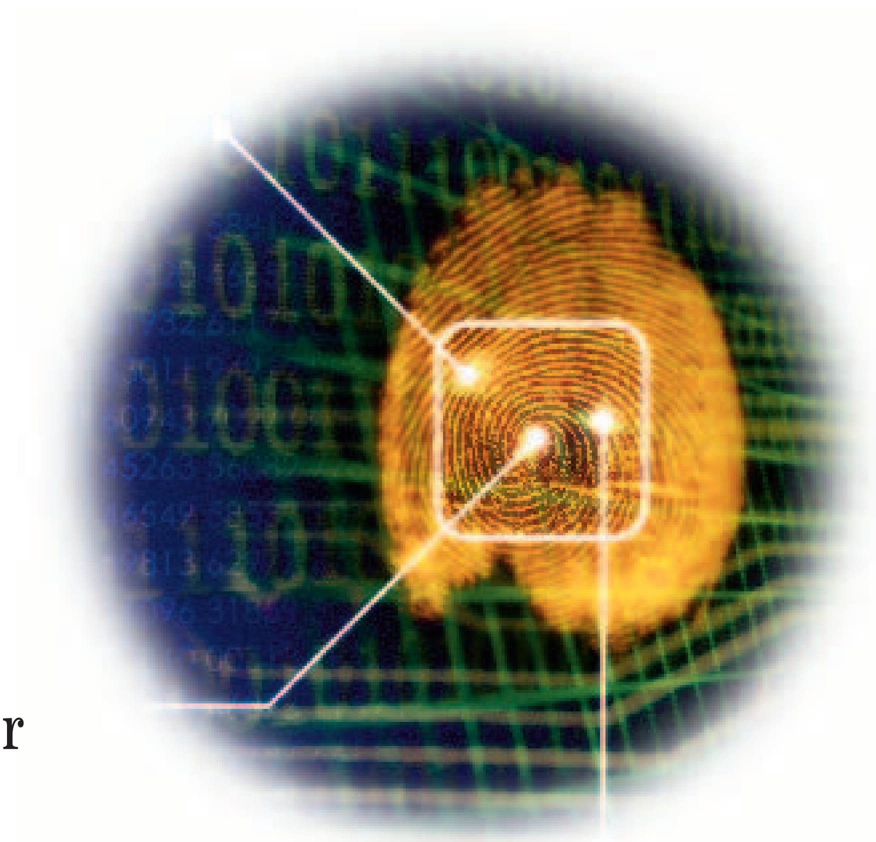
WILEY

TIMELY. PRACTICAL. RELIABLE.

Incident Response

Computer Forensics Toolkit



Douglas Schweitzer

Incident Response:
Computer Forensics Toolkit

Incident Response: Computer Forensics Toolkit

Douglas Schweitzer

WILEY

Wiley Publishing, Inc.

Incident Response: Computer Forensics Toolkit
Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

ISBN: 0-7645-2636-7

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

1O/RR/QU/QT/IN

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (800) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data on file with the publisher.

About the Author

Douglas Schweitzer is an Internet security specialist with Brainbench certifications in Internet security and ITAA Information Security Awareness. Douglas is a Certified Internet Webmaster Associate, and he holds A+, Network+, and i-Net+ certifications from the Computing Technology Industry Association. He has appeared as an Internet security guest speaker on several radio shows, including KYW Philadelphia, as well as on *Something You Should Know* and *Computer Talk America*, two nationally syndicated radio shows. He is also the author of *Securing the Network from Malicious Code: A Complete Guide to Defending Against Viruses, Worms, and Trojans* and *Internet Security Made Easy: A Plain-English Guide to Protecting Yourself and Your Company Online*.

Credits

ACQUISITIONS EDITOR
Katie Feltman

PROJECT EDITOR
Mark Enochs

TECHNICAL EDITOR
Russell Shumway

COPY EDITOR
Maarten Reilingh

EDITORIAL MANAGER
Mary Beth Wakefield

VICE PRESIDENT & EXECUTIVE GROUP PUBLISHER
Richard Swadley

VICE PRESIDENT AND EXECUTIVE PUBLISHER
Bob Ipsen

EXECUTIVE EDITOR
Carol Long

EXECUTIVE EDITORIAL DIRECTOR
Mary Bednarek

PROJECT COORDINATORS
Cindy Phipps, Bill Ramsey

GRAPHICS AND PRODUCTION SPECIALISTS
Beth Brooks, Sean Decker,
LeAndra Johnson, Stephanie Jumper,
Kristin McMullan, Heather Pope,
Julia Trippetti

QUALITY CONTROL TECHNICIANS
Carl W. Pierce, Robert Springer

PERMISSIONS EDITOR
Laura Moss

MEDIA DEVELOPMENT SPECIALIST
Travis Silvers

PROOFREADING
Kim Cofer

INDEXING
Virginia Bess

This book is dedicated in loving memory of Mirhan “Mike” Arian,
whose insight and camaraderie are forever missed.

Acknowledgments

This book would not have been possible without the combined efforts of some very talented people. I would first like to thank my agent, Carole McClendon of Waterside Productions for her assistance in again finding me a superb publisher. I would also like to thank the hard-working individuals at Wiley Publishing who helped to make this book a reality. Their enthusiasm and support were a continued shot in the arm. In particular, I would like to thank Acquisitions Editor, Katie Feltman for her confidence in me and for helping me to shape and hone the initial outline for the book. I am also grateful to Project Editor, Mark Enochs for all his suggestions. I would like to say thank you to my wife and best friend, Monique, for without her help, this book would not have been possible. I tip my hat to Russ Shumway who, as my technical editor, did a superb job ensuring that all my facts were correct and who suggested a number of additions that kept this book technically sound. Thanks, as well, to my sons Deran and Alex for their enduring patience with me while I spent many long hours writing.

Contents at a Glance

Contents

Introduction

On May 14, 1999, 54-year-old Sharon Guthrie drowned in the bathtub of her Wolsey, South Dakota home. An autopsy revealed that 10 to 20 capsules containing Temazepan were present in her body. The sleeping pills had been prescribed for her husband, the Reverend William Guthrie, pastor of the First Presbyterian Church in Wolsey. Despite his denials of any wrongdoing in connection with the death of his wife, police remained unconvinced of his innocence. Lacking any hard evidence in the case, police decided to engage the services of computer forensics expert, Judd Robbins. Several of the church computers frequently used by Rev. Guthrie were seized and frozen. After several days of examining the minister's files, Robbins eventually uncovered evidence that Guthrie had been searching the Internet for painless and surefire killing methods. Robbins also found detailed notes about sleeping pills and lethal household cleaning agents. On January 11, 2000, a 12-member jury convicted Guthrie of murder. Less than two weeks later, Circuit Judge Eugene Martin sentenced him to life imprisonment.

Computer Crime

Not every crime committed with a computer is a computer crime. If someone steals a telephone access code and makes a long-distance call, the code he has stolen is checked by a computer before the call is processed. Nevertheless, such a case is more appropriately treated as "toll fraud," not computer crime. It would, however qualify as cyber crime if the code was obtained as a result of hacking into a computer system. Although this example appears straightforward, many cases are not so neatly categorized. A bank employee who steals money from a cash drawer is embezzling. A bank employee who writes a computer program to randomly steal very small amounts from numerous accounts may also be embezzling, yet committing (and prosecuting) this offense may require a working knowledge of the bank's computer system. As a result, such a crime may reasonably be characterized as a computer offense.

According to the U.S. Department of Justice, computers generally play three distinct roles in a criminal case. First, a computer can be the target of an offense. This occurs when conduct is designed to take information without authorization from, or cause damage to, a computer or computer network. The Melissa and Explore.Zip.Worm viruses, along with hacks into the White House and other Web sites, are examples of this type of offense.

Second, a computer can be incidental to an offense yet still be significant in terms of law enforcement purposes. For example, drug traffickers may store transactional data (such as names, dates, and quantities) on computers, rather than in paper form.

Finally, a computer can be the tool used for committing an offense (such as fraud or the unlawful sale of prescription drugs over the Internet).

What Is Computer Forensics?

According to computer forensic expert Judd Robbins, “Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence.” The type of evidence gathered from a forensic examination can be useful in a wide variety of investigations:

- ✓ Civil litigations such as divorce, harassment, and discrimination cases
- ✓ Corporations seeking to acquire evidence in embezzlement, fraud, or intellectual property theft issues
- ✓ Individuals seeking evidence in age discrimination, wrongful termination, or sexual harassment claims
- ✓ Insurance company investigations where evidence is required relating to insurance fraud, wrongful death, workman’s compensation, and other cases involving insurance claims

Digital evidence may be sought in a wide array of computer-related crimes, and computer forensic examinations use a variety of methods for discovering data that resides in a computer system, or for recovering deleted, encrypted, or damaged file information. Any or all of this information can be of use in the processes of discovery, deposition, or litigation.

The Importance of Incident Response

Analyzing the aftermath of a computer intrusion takes far longer than it takes a perpetrator to commit the crime. It is often the speed of the response that determines the outcome; and the more prepared an organization is when an incident first occurs, the quicker it can respond in the incident’s wake. With the ever-increasing use of information technology (IT), organizations around the globe are facing the challenge of protecting valuable resources from a never-ending onslaught of threats. Computers, and the networks that connect them, process, store, and transmit information that is crucial for successful day-to-day operations and are therefore inviting targets for hackers and malicious code. The protection of critical IT resources requires not only adopting reasonable precautions for securing these systems and networks, but also the ability to respond quickly and efficiently when system and network security defenses have been breached.

Unfortunately, responding to computer security incidents is generally not an easy endeavor. Proper *incident response* requires technical knowledge, communication, and coordination among personnel in charge of the response process.

In information technology, *incident* refers to an adverse event in an information system and/or network or the threat of the occurrence of such an event. Examples of incidents include unauthorized use of another user’s account, unauthorized use of system privileges, and execution of malicious code that destroys data. Other adverse events include floods, fires, electrical outages, or excessive heat that results in system crashes. Adverse events such as natural disasters and power-related disruptions, though certainly undesirable incidents, are not generally within the scope of incident response teams and are better addressed by an organization's business continuity (contingency) plans. For the purpose of *incident response*, therefore, the term *incident* refers to an adverse event that is related to *information security*.

Similarly, an *event* is *any* observable occurrence in a system and/or network. Examples of events include the system boot sequence, a system crash, and data packet flooding within a network. Events are important because they often provide an indication that an incident is occurring. In reality, events caused by human error (for example, unintentionally deleting a critical directory and all files contained therein) are the most costly and disruptive. Events related to computer security, however, are attracting an increasing amount of attention within the computing community in general as well as within the federal government. Among other reasons, the unparalleled growth of networking and the abundance of malicious code available to perpetrators have resulted in greatly exposing more systems to the threat of unauthorized remote access.

Types of Incidents

According to the Federal Computer Incident Response Center (FedCIRC), the term *incident* encompasses the following general categories of adverse events:

- ✓ **Malicious code attacks.** Malicious code attacks include attacks by programs such as viruses, Trojan horse programs, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs to exclude unauthorized activity. Malicious code is particularly troublesome in that it is typically written in such a manner that it masquerades its presence, making it difficult to detect. Furthermore, self-replicating malicious code such as viruses and worms can replicate rapidly, thereby making containment especially challenging.
- ✓ **Unauthorized access.** Unauthorized access encompasses a range of incidents from improperly logging into a user's account (for example, when a hacker logs in to a legitimate user's account) to unauthorized access to files and directories stored on a system or storage media by obtaining superuser privileges. Unauthorized access may also entail accessing network data by planting an unauthorized sniffer program or device to capture all packets traversing the network at a particular point.
- ✓ **Unauthorized utilization of services.** It is not absolutely necessary to access another user's account to perpetrate an attack on the system or network. An intruder may also obtain access to information or plant Trojan horse programs by misusing available services. Examples include using the network file system (NFS) to mount the file system of a remote server machine or interdomain access mechanisms in Windows NT to access files and directories in another organization's domain.
- ✓ **Disruption of service.** Users rely on services provided by network and computing services. Those with malicious intent can disrupt these services in a variety of ways, including erasing critical programs, mail spamming (flooding a user account with electronic mail), and altering system functionality by installing Trojan horse programs.

- ✓ **Misuse.** Misuse occurs when someone uses a computing system for other than official purposes, such as when a legitimate user uses a government computer to store personal tax records.
- ✓ **Espionage.** Espionage is stealing information to subvert the interests of a corporation or government. Many of the cases of unauthorized access to U.S. government systems during Operation Desert Storm and Operation Desert Shield were the manifestation of espionage activity against the United States.
- ✓ **Hoaxes.** Hoaxes occur when false information about incidents or vulnerabilities is spread. In early 1995, for example, several users with Internet access distributed information about a so-called Good Times Virus, even though the virus did not exist.

It is unfortunate that despite the implementation of sophisticated firewalls, powerful intrusion detection systems, and antivirus software, computers and the networks that connect them may still be penetrated by hackers, crackers, and malicious code. When the unthinkable happens, responding to incidents and events is paramount. Because law enforcement agencies have heightened their interest in computer crimes, the capture and preservation of critical evidence via basic forensic methods are included in this book. Organizations require strategies for handling computer-security-related events effectively. Such strategy includes preparation, detection, and response. Adopting a hands-on approach, this book will arm readers with both the knowledge and the tools needed to mitigate risk and limit loss.

Who Should Read This Book?

While computer forensics is naturally of great concern to those in the law enforcement community, any computer user or owner who wants to understand how to acquire and handle potential digital evidence will benefit from reading this book. In addition, the incident response material presented in this book will be a tremendous advantage to network administrators, security personnel, and even executive officers who find it increasingly difficult to keep their organizational networks free from the debilitating and costly effects of hackers and malicious code despite the implementation of powerful security measures.

How to Read This Book

This book can be read as a complete introductory course in basic computer forensics and incident response. However, it is also meant to serve as both a guide and a tool; and many readers will already be somewhat familiar with the various subjects covered. Accordingly, each chapter is a complete stand-alone component that can be read whenever the reader deems it practical or convenient. As the reader, you probably specialize in one or more of the areas covered in this text. However, the information presented in this book should also provide additional knowledge and tools in other areas with which you may not yet be familiar.

Chapter 1

Computer Forensics and Incident Response Essentials

In This Chapter

- ✓ Catching the criminal: the basics of computer forensics
- ✓ Recognizing the signs of an incident
- ✓ The steps required to prepare for an incident
- ✓ Incident verification
- ✓ Preservation of key evidence
- ✓ Specific response measures
- ✓ Building a toolkit

THE *HI-TECH REVOLUTION* SWEEPING THE GLOBE in communications and information technology has truly made the world a smaller place. With effects on both our personal and professional lives, the United States is now investing more resources into the advancement of information technology than into the management or manufacture of consumer goods. The Internet has become so popular that it is now more commonplace to receive an e-mail message than a conventionally sent letter in daily correspondence. Current estimates put the worldwide Internet population at over 580 million strong and growing.

In this ever-evolving age of information technology, the requirements of law enforcement are shifting, as well. Some conventional crimes, especially those concerning finance and commerce, continue to become ever more technologically sophisticated. Paper trails have given way to electronic trails. Crimes relating to the theft and exploitation of data are detected daily. As evidenced in the murder of Sharon Guthrie, violent crime is also not immune to the use of the information technology. Remember, Rev. Guthrie was convicted based upon forensic evidence gleaned from his computer, namely the discovery of data indicating that he had visited Web sites that offered instructions for carrying out a murder using tranquilizers. It is not unheard of for those dealing in arms or drugs to store client names and contact information in databases on their computers.

Just as industry is gradually transforming from the manufacture of goods to the processing of information, criminal activity has to a great extent also converted from a largely physical dimension to a cyber dimension. Investigations once carried out in a more concrete, material manner now exist electronically, conducted online or through the examination of computer hardware and software.

Catching the Criminal: The Basics of Computer Forensics

Computer forensics is the science of acquiring, retrieving, preserving, and presenting data that has been processed electronically and stored on computer media. Computer forensic science is a relatively new discipline that has the potential to greatly affect specific types of investigations and prosecutions. As a greater number of people now make use of computers, more and more information of all kinds is being stored on them. This includes information that is of significant importance to an organization's clientele or that has a bearing on a civil or criminal case, such as evidence of financial fraud, embezzlement, wrongful employment termination, sexual harassment, theft, arson, workers compensation fraud, age or sex discrimination, child pornography, theft of trade secrets, or marital infidelity, to name a few.

Computer forensic science is different from the traditional forensic disciplines. To begin, the tools and techniques required are easily available to anyone seeking to conduct a computer forensic investigation. In contrast to traditional forensic analysis, there is commonly the requirement that computer examinations are performed at virtually any physical location, not just in a controlled environment. Rather than producing conclusions requiring expert interpretation, computer forensic science produces direct information and data that may play a significant role in the apprehension or conviction of cyber criminals.

The acquisition of digital evidence begins when information and/or physical items are collected or stored in anticipation of being examined. The term "evidence" implies that the collector of evidence is recognized by the courts and that the process of collecting is also understood to be a legal process, appropriate for evidence collection in the locality in which it is taking place. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee. The following are several important definitions the U.S. Federal Bureau of Investigation uses to delineate certain aspects of computer forensic science:

- ✓ **Data objects.** Objects or information of potential probative value that are associated with physical items. Data objects may occur in different file formats (for example, NTFS or FAT32) without alteration of the original information.
- ✓ **Digital evidence.** Information of probative value that is stored or transmitted in digital form.
- ✓ **Physical items.** Items on which data objects or information may be stored and/or through which data objects are transferred.
- ✓ **Original digital evidence.** Physical items and the data objects associated with such items at the time of acquisition or seizure.

- ✓ **Duplicate digital evidence.** An accurate digital reproduction of all data objects contained on an original physical item.

No investigation involving the review of documents, either in a criminal or corporate setting, is complete without the inclusion of properly handled computer evidence. Computer forensics ensures the preservation and authentication of computer data, which is fragile by nature and can be easily altered, erased, or subjected to claims of tampering if it is not properly handled. Additionally, computer forensics facilitates the recovery and analysis of deleted files and other forms of compelling information that are normally invisible to the user.

Unlike paper evidence, computer evidence often exists in digital data stored on the computer's storage media. The volume of information that can be stored on current computers is incredibly enormous. There are numerous types of storage media: floppy disks, hard disks, ZIP disks, magnetic tape, magneto-optical cartridges, CD-R, CD-RW, CD-ROM, DVD, as well as flash, CompactFlash, Smart Media, and Memory Stick storage devices.

A knowledgeable expert can facilitate the process of discovery by identifying other potential evidence that may later be included in legal proceedings. For example, during on-site premise inspections, in cases where computer disks are not actually seized or forensically copied, the forensics expert can quickly identify places to look, signs to look for, and point to additional, alternative sources for relevant evidence. These may take the form of earlier versions of data files (such as memos or spreadsheets that still exist on the computer's disk or on backup media) or as differently formatted versions of data, either created or treated by other application programs (for example, word processing, spreadsheet, e-mail, timeline, scheduling, or graphic applications).

As the world continues to move forward in the information age, the need for proper forensic analysis and well-planned incident response continues to increase. During his September 5, 2001 speech, "The Legal Aspects of Infrastructure Protection," at the INFOWARCON 2001 conference in Washington, D.C., Ronald Dick, Director of the National Infrastructure Protection Center, made the following statement:

> The NIPC, on behalf of each of its partner agencies, is firmly committed to the fundamental proposition that the investigation of cyber crimes and national security events must be achieved in a manner that protects the privacy rights of our citizens, which is an essential Constitutional right. We know that we can only be successful if we remain true to these core values.
>
> However, there is reason for concern that cyber intruders are gaining the ability to remain anonymous, regardless of their impact on human life and national security, and regardless of whether the government can make a showing that it should be able to get the information necessary to catch them. Quite simply, the balance described in the Constitution, which provides the government with the capacity to protect the public, is eroding. In its place, the privacy of criminals and foreign enemies is edging towards the absolute. If we continue down this path, no identifying information will be available when the government shows up, as specifically contemplated in the Fourth Amendment, with a warrant issued "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
>
> As a result of this shifting in the balance between privacy, public safety, and national security, the list of victims is growing and the World Wide Web is being referred to as the Wild Wild West. As time goes on, I find that more and more of the individuals I meet have firsthand knowledge of computer

> crime. Their own computers — not just computers of people they know — have been infected with a virus or worm, their company website has been defaced or its presence crippled by a denial of service attack, or their information systems have been infiltrated and their company's proprietary data has fallen into the hands of an unidentified intruder. Indeed, as time passes, amongst those that actively use computers, I meet fewer and fewer organizations that have proven immune to these growing threats. And, I suspect that the people in this room, and the groups you represent, are no different. If you don't think that you or your company has ever been affected by some form of cybercrime, either you just aren't aware of it, or you are a lucky member of a rapidly narrowing class. An annual computer crime survey conducted jointly between the Computer Security Institute and the FBI bears this out. In 1996, when we asked systems administrators if anybody had gained unauthorized access to their computers, less than half, 42 percent, answered yes. Last year, when asked the same question, well over half of the respondents, a full 70 percent, answered yes. And there lies the irony to the privacy debate. Law-abiding citizens are finding that their privacy is increasingly being intruded upon by criminals. Meanwhile, the criminals are gaining privacy. I've been the Director of the NIPC for a little over eight months now, having held a number of different management positions at the Center since arriving there in 1998. I have watched it grow and develop almost from its inception. Bear in mind that, just three years ago, infrastructure protection was relatively new ground for the Federal government. President Clinton issued Presidential Decision Directive 63 in May of 1998. It was a wake up call, which established a new framework for doing business. For the first time, the Federal government created an interagency entity, the National Infrastructure Protection Center — combining the United States law enforcement, military, and intelligence communities — to work directly with the private sector to achieve what many to this day say is impossible: The elimination of all vulnerabilities to our nation's critical infrastructures. Eliminating all of these vulnerabilities, stated the President, would necessarily require "flexible, evolutionary approaches" spanning both the public and private sectors, and protecting both domestic and international security.

Mr. Dick's concern that "Law-abiding citizens are finding that their privacy is increasingly being intruded upon by criminals while the criminals are gaining privacy" is echoed in both the public and private sectors. Nevertheless, apprehending cyber criminals and remaining within the confines of the law while doing so, remains imperative. Improper procedures in the gathering and handling of potential evidence may render that evidence inadmissible in a court of law. The USA Patriot Act of 2001 made significant changes to federal search and seizure laws.

x-ref

For more on the USA Patriot Act of 2001, see Chapter 2 and Appendix C.

While it is beyond the scope of this book to turn the reader into a forensics expert, the proper gathering of computer evidence can confirm or dispel concerns about whether an illegal incident has occurred. Such detective work can also document computer and network vulnerabilities after an incident has been verified. In addition, you may wish to obtain additional training before attempting some of techniques outlined in this book.

Recognizing the Signs of an Incident

The nearly unrelenting stream of security-related incidents has affected millions of computer systems and networks throughout the world and shows little sign of letting up. Table 1-1 shows a list of incidents that were reported to the Federal Computer Incident Response Center (FedCIRC) for the calendar year 2000. While incident response varies in approach depending upon each circumstance, the goals in all cases are predominantly the same.

In nearly every case, the focus is severalfold:

- ✓ Recover quickly and efficiently from the security incident.
- ✓ Minimize the impact caused by loss or theft of information (classified or unclassified) or by the disruption of critical computing services when an incident has occurred.
- ✓ Respond systematically, following proven procedures that will dramatically decrease the likelihood of reoccurrence.
- ✓ Balance operational and security requirements while remaining within a budgetary constraint.
- ✓ Deal with legal issues in an efficient manner. A plethora of legal issues surrounds the computer security arena. For example, the U.S. Department of Justice (as well as some federal and state laws) has declared it illegal to carry out certain monitoring techniques. By following proper protocols and procedures, those who conduct forensic examinations can be assured that legal statutes are not being violated.

Table 1-1 FedCIRC Incident Activity Summary for 2000

Count	Percentage	Type
155	26%	Root compromise
138	23%	Information request
113	19%	User compromise
70	11%	Reconnaissance
36	6%	Virus
35	5%	Denial of service
24	4%	Misuse of resources
24	4%	False alarm
9	1%	Unknown
7	1%	Deception

It is the general consensus among computer security experts that the vast majority of computer crimes are neither detected nor reported. To a certain extent, this is because many computer crimes are not overtly obvious. To use a simple analogy, when an item (especially an important one) is stolen, the owner readily detects this because the item is missing. However, if a hacker steals computer data by copying it, the original data remains, and is still accessible to the owner. There is a variety of ways incidents can occur and various manners in which they impact an organization.

Some common types of computer incidents include the following:

- ✓ Employee misuse of systems (for example, violations of Internet use policies)
- ✓ Malicious code (for example, viruses, worms, or Trojan horse programs)
- ✓ Intrusions or hacking
- ✓ Unauthorized electronic monitoring (sniffers, keyloggers, and so on)
- ✓ Web site defacement or vandalism
- ✓ Unauthorized access to confidential information
- ✓ Automated scanning tools and probes
- ✓ Insider sabotage (via espionage or disgruntled employees)

Unfortunately, there are no blanket solutions to prevent incidents from occurring, and the limited solutions that do exist are expensive and require an enormous amount of an organization's resources. The option of using weak incident response methods (or no methods at all) is, however, even more expensive and only compounds the damage that incidents cause. What's required is a long-term commitment to systematically prevent and respond to security incidents instead of just making short-term fixes for selected problems. Experience shows that most organizations do not think about how they will respond to a computer security incident until after they've been significantly victimized by one. They have not assessed (nor anticipated) the business risk of not having in place formal incident-detection and response mechanisms.

When it is not known that an intrusion (or an intrusion attempt) has occurred, it is difficult, sometimes impossible, to determine later that your systems have been compromised. If the information necessary to detect an intrusion is not being collected and reviewed, the organization cannot determine what sensitive data, systems, and networks are being attacked and what breaches in confidentiality, integrity, or availability have occurred. As a result of an inadequate ability to detect the signs of intrusion, the following may occur:

- ✓ You will not be able to detect such signs in a timely manner due to the absence of necessary warning mechanisms and review procedures.
- ✓ You will not be able to identify intrusions because of the absence of baseline information with which to compare your current operational state. Differences between a previous configuration and your current state can provide an indication that an intrusion has occurred.

- ✓ You will not be able to determine the full extent of an intrusion and the damage it has caused. You will also be unable to tell whether you have completely removed the presence of the intruder from your systems and networks. This will significantly impede, and even increase, your recovery time.
- ✓ Your organization may be subjected to legal action. Intruders can make use of systems they have compromised to launch attacks against other systems. If one of your systems is used in this fashion, you may be held liable for not exercising adequate due care with respect to security.
- ✓ Your organization may experience a tarnishing blow to its reputation.
- ✓ Your organization may suffer lost business opportunities.

Recognizing the signs of an incident while it is occurring is paramount to mitigating loss. Some signs that an incident has occurred are obvious. For example, a worker fails to scan a questionable e-mail attachment for the presence of malicious code and, after opening an attachment, finds that his or her computer is no longer operating properly. In this example of a malicious code incident, it can be inferred that the e-mail attachment contained some sort of malicious code or script, which affected an application or operating system.

Other incidents, such as network intrusions, are often harder to detect. Hackers are always seeking novel ways to infiltrate networked computer systems. They may attempt to breach a network's defenses from remote locations. In some cases, intruders resort to extreme measures, including attempts to physically infiltrate an organization to access information resources. Hackers often seek out vulnerabilities in the form of outdated or unpatched software.

Newly discovered vulnerabilities in operating systems, network services, and protocols are prime targets, and hackers usually take advantage of both. Intrusions and their resultant damage can be accomplished within seconds due to the development of powerful and sophisticated programs. Freely available at underground hacker Web sites, hackers use these powerful programs to crack passwords, bypass firewalls, and rapidly penetrate systems. The common approach to detecting intrusions is as follows:

- ✓ Observe your systems for unexpected behavior or anything suspicious.
- ✓ Investigate anything you consider to be unusual.
- ✓ If your investigation finds something that isn't explained by authorized activity, immediately initiate your intrusion response procedures (response procedures are covered later in this chapter).

Even if your organization has implemented security measures (such as firewalls), it is essential that you closely monitor your computer system for signs of intrusion. Monitoring can be complicated because intruders often hide their activities by modifying the systems they've broken into. An intrusion can already be underway and continue unnoticed because to users it appears that everything is operating normally (on the surface). The following checklist for Windows outlines important indications that your system may have been compromised, along with some helpful solutions:

✓ **Look for unusual or unauthorized user accounts or groups.** There are several ways to do this. You can use the User Manager tool in Windows NT or the Computer Management tool in Windows XP (see Figure 1-1) or the `net user`, `net group`, and `net localgroup` commands at the command line (DOS prompt). If the system does not require guest access, make sure that the built-in Guest account is disabled.

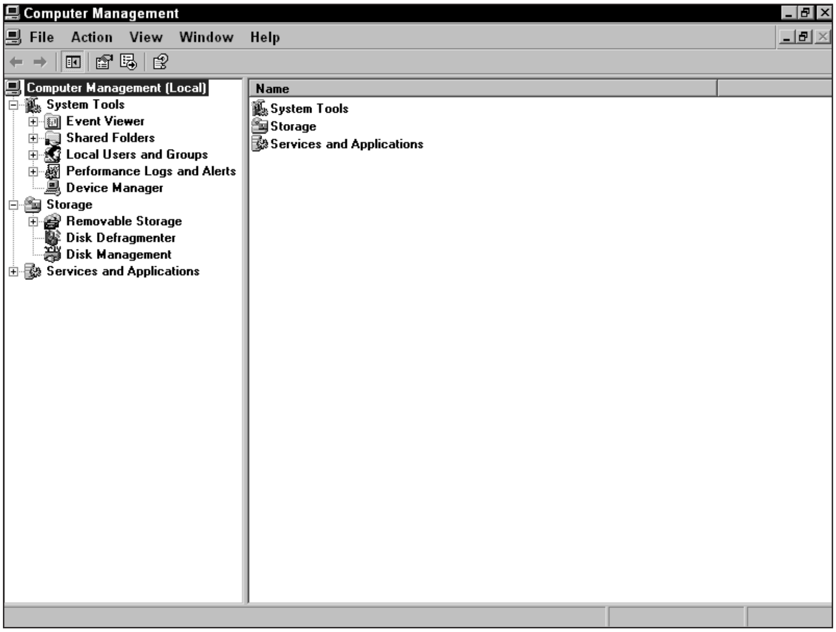


Figure 1-1: The Computer Management utility under Windows XP Professional

Disabling the Guest Account in Windows XP

To disable the guest account in Windows XP, follow these steps:

1. Click on the Start button.
2. From the pop-up menu, select the Control Panel option. This opens the Control Panel window.
3. In the Control Panel window, select User Accounts.
4. In the User Accounts window, select the "Change an account" option, or click on the Guest Account icon (if available) at the bottom of the User Accounts window.
5. Once open, the Guest Account has a toggle button that allows the user to turn the Guest account on or *off*.

✓ **Using the computer management tool, check all groups for invalid user membership.** In Windows NT, 2000, and XP, several of the default groups give unique privileges to the members of those groups. For example, while members of the Network Configuration Operators have limited administrative privileges to manage configuration of networking features, members of the Administrators group have the power to alter nearly any facet of the operating system.

tip

Besides the aforementioned built-in Windows management tool, another useful freeware auditing utility is DumpSec by SomarSoft. This security auditing program for Windows NT dumps the permissions (DACLs) and audit settings (SACLs) for the file system, Registry, printers, and shares in a concise and easy-to-read format making any holes in system security more readily apparent. For additional information or to download a copy of DumpSec visit `www.somarasoft.com`.

✓ **Check log files for connections from unusual locations or for any unusual activity.** All versions of Windows NT have a built-in Event Viewer that allows you to check for unusual logon entries, failures of services, or abnormal system restarts. Keep in mind that if your firewall, Web server, or router writes logs to a different location than the compromised system; you need to examine these logs as well.

x-ref

Configuring and examining log files are covered in detail in Chapter 3.

✓ **Search for invalid user rights.** To examine user rights use the User Manager tool under Policies → User Rights. There are more than two-dozen rights that can be assigned to users or groups. Normally the default configuration for these rights is secure.

✓ **Check to see if unauthorized applications are running.** There are several approaches hackers can take to start a backdoor program, therefore you may need to take one or more of the following precautions:

- **Examine the Windows Registry.** All versions of Windows come with a built-in Registry Editor (see Figure 1-2) that can be easily accessed by typing `regedit` at the command prompt. Several of the most common locations from which applications start through the Registry are illustrated in Table 1-2.

x-ref

Registry structure is covered in detail in Chapter 4.

- **Look for invalid services.** Some backdoor programs install themselves as a service that automatically starts when Windows first loads. Services can then run as any user with the Logon as Service user right. Check services that are started automatically and be sure that they are indispensable. The services executable file should also be scanned with an antivirus program to ensure that it has not been replaced with a Trojan horse or backdoor program. Logon rights control how security personnel are allowed access to the computer. These rights apply whether the access is from a keyboard or as a service that is activated when Windows loads. For each logon method, there exist two logon rights; one to permit logging on to the computer and another to deny logging on to the computer.

caution

Backdoor programs allow hackers to access your computer while it is connected to the Internet. They can steal passwords, log keystrokes, and even crash your computer. The intruder first must trick a user into running the program on the user's computer. This is usually accomplished by sending the file by e-mail message or via an instant messaging service.

What's Running on the System?

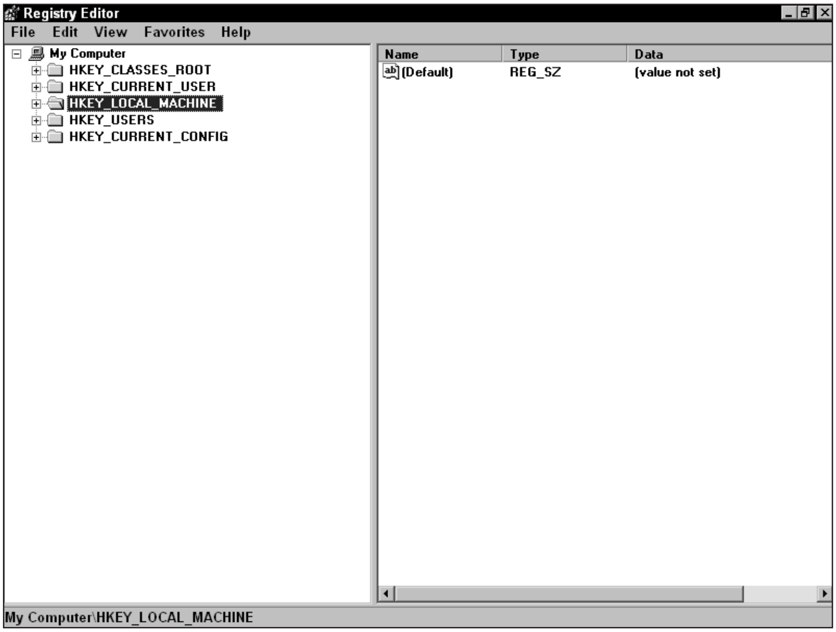
To observe which services are running on your Windows XP system, do the following:

1. From the Start menu, select Control Panel → Performance and Maintenance.
2. In the Performance and Maintenance window, select Administrative Tools.
3. Several icons appear; double-click Component Services.
4. Select Services Local from the drop-down list in the left pane. If you attempt to access Services too soon, you might encounter the message "Service Database is locked." This message means that some services are still loading or initializing in the background, so you can't get to the list of services just yet. If you wait a few seconds, you'll be able to bring up the dialog box.

In older versions of Windows NT there is another way to open this list:

1. From the Start menu, select Programs → Administrative Tools → Server Manager.
2. From Server Manager, select your computer, and then select the Computer → Services menu item.
3. If you possess the appropriate administrative privileges, you will even be able to see what services are running on remote computers, as well. Simply select the remote computer from Server Manager, and then select Computer → Services from the menu.

- **Monitor system startup folders.** You can examine all the shortcuts by selecting Start → Programs → Startup. There are two different startup folders, one for the local user and one for all users. When a user logs on, all of the applications in both the All Users folder and in the user's startup folder are started. Because of this it is important to check *all* of the startup folders for suspicious applications.



Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE

Figure 1-2: The Windows Registry Editor

Table 1-2 Common Program Startup Locations

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs

HKEY_LOCAL_MACHINE\System\ControlSet001\Control\Session Manager\KnownDLLs

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunOnceEx

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" line)

Continued

Table 1-2 Common Program Startup Locations *(Continued)*

`HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnce`

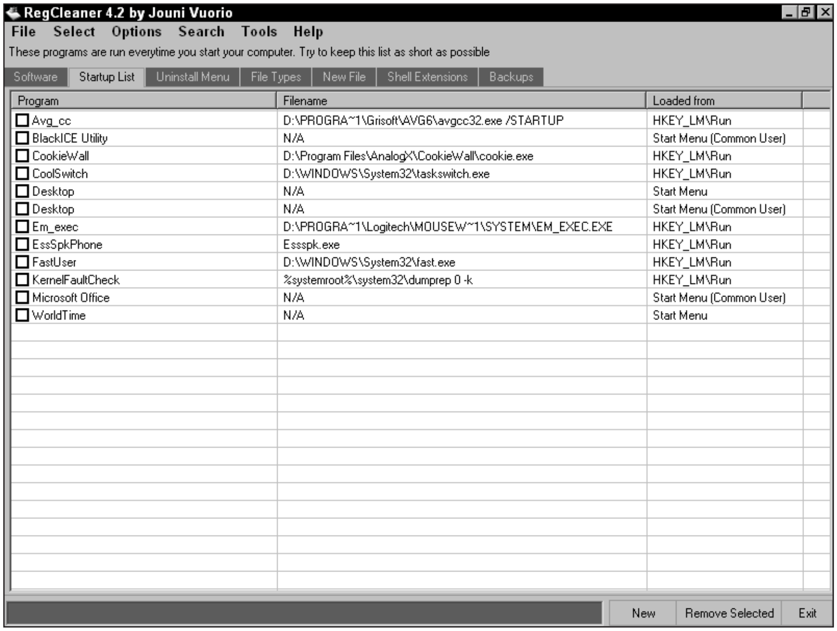
`HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\RunOnceEx`

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices`

`HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows ("run=" value)`

note

RegCleaner (see Figure 1-3), written by Jouni Vuorio, is a freeware program for Windows that is very useful in gathering important information about programs automatically launched at startup from the Windows Registry. If unwanted applications or services are present, this program also allows you to delete the appropriate Registry entry. Keep in mind that altering the Registry can be tricky. Deleting the wrong entry can render an application or the operating system unstable or inoperable. RegCleaner can be found at `www.vtoy.fi/jv16/index.shtml`.



These programs are run everytime you start your computer. Try to keep this list as short as possible

Program	Filename	Loaded from
□ Avg_cc	D:\PROGRA~1\Grisoft\AVG6\avgcc32.exe /STARTUP	HKEY_LM\Run
□ BlackICE Utility	N/A	Start Menu (Common User)
□ CookieWall	D:\Program Files\AnalogX\CookieWall\cookie.exe	HKEY_LM\Run
□ CoolSwitch	D:\WINDOWS\System32\taskswitch.exe	HKEY_LM\Run
□ Desktop	N/A	Start Menu
□ Desktop	N/A	Start Menu (Common User)
□ Em_exec	D:\PROGRA~1\Logitech\MOUSEW~1\SYSTEM\EM_EXEC.EXE	HKEY_LM\Run
□ EssSpkPhone	Essspk.exe	HKEY_LM\Run
□ FastUser	D:\WINDOWS\System32\fast.exe	HKEY_LM\Run
□ KernelFaultCheck	%systemroot%\system32\dumprep 0 -k	HKEY_LM\Run
□ Microsoft Office	N/A	Start Menu (Common User)
□ WorldTime	N/A	Start Menu

Figure 1-3: RegCleaner by Jouni Vuorio

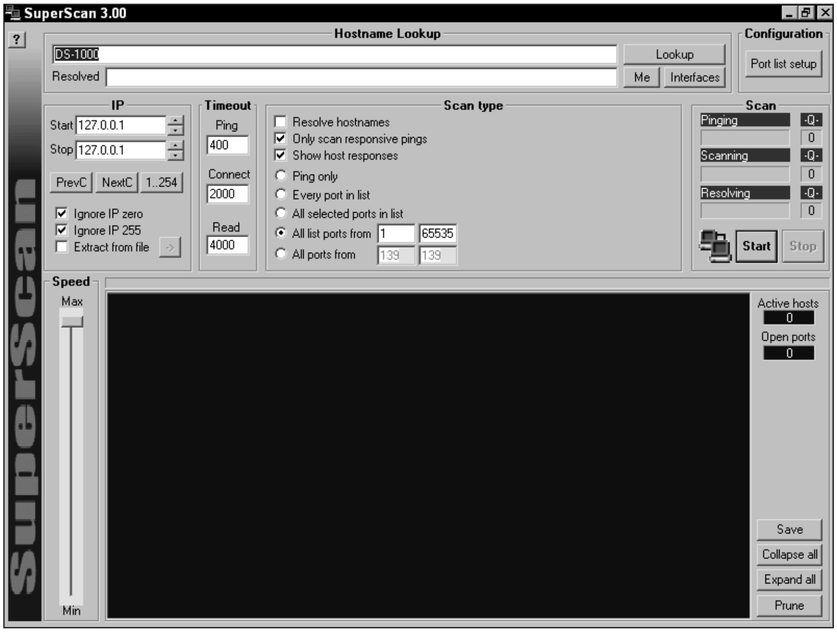
- ✓ **Inspect network configurations for unauthorized entries.** Look for invalid entries for settings like WINS, DNS, IP forwarding, and so on. These settings can be checked using the Network Properties tool or by using the `ipconfig /all` command at the command (DOS) prompt.

- ✓ **Check your systems program files for alterations.** Compare the versions on your systems with copies that you know have not been altered, such as those from your original installation media. Be cautious of trusting backups; they too may contain Trojan horses.

- ✓ **Check for unusual ports listening for connections from other hosts by using the `netstat -an` command at the command prompt.** Powerful third-party port-scanning programs like SuperScan by Foundstone, Inc. can also be used to scan for open or active TCP/UDP ports. SuperScan (see Figure 1-4) is a freeware program that can be found at `www.webattack.com`.

x-ref

For a comprehensive list of ports, see Appendix B.


SuperScan 3.00

Hostname Lookup
DS-1000
Resolved

IP
Start 127.0.0.1
Stop 127.0.0.1
☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout
Ping 400
Connect 2000
Read 4000

Scan type
☐ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
○ Every port in list
○ All selected ports in list
● All list ports from 1 65535
○ All ports from 139 139

Scan
Pinging 0
Scanning 0
Resolving 0

Active hosts 0
Open ports 0

Figure 1-4: SuperScan by Foundstone, Inc. can scan for open or active TCP/UDP ports.

note

Trojan horse programs are often engineered to mimic the same file size as the legitimate program they replace. As a result, just checking file properties and time-stamps associated with the applications is not sufficient for determining whether or not the legitimate programs have been replaced by a Trojan horse. A better alternative is to use Tripwire.

Tripwire is a Unix-based file-system-integrity-checking program that ensures the integrity of critical system files and directories by identifying all changes made to them. By using Tripwire for intrusion detection and damage assessment, you will be able to keep track of system changes which in turn can speed up the recovery from a system compromise by reducing the number of files you must restore to repair the system.

Using antivirus software aids in the detection of computer viruses, backdoor programs, and Trojan horse programs. However, bear in mind that since malicious programs are being created continuously, it is important to always keep your antivirus software up to date.

Preparing for Incidents

Prior to the early 1990s, threats to computer security (besides human errors) were mainly physical and environmental, consisting of physical damage and insider attacks, such as fire, water, or theft. These types of threats are understood fundamentally and are easily controlled through the use of traditional methods and contingency planning. Today, a new category of computer security threats has become equally as important to understand and control. These threats include transgressions by unauthorized intruders and users who exploit system vulnerabilities, computer viruses, worms, and Trojan horses. Several factors have contributed to the growing presence of these threats, such as the following:

- ✓ **Society's increased reliance on computers.** Today, nearly every organization, both public and private, relies on computers and networks for communication. Because of this increased reliance, many agencies would suffer great losses to productivity should their systems become unavailable. Due to system complexity, reliance on computer systems often presents unanticipated risks and vulnerabilities.
- ✓ **Malicious code.** Computer viruses, Internet mail worms, and Trojan horses in particular, continue to wreak havoc in personal computer security. As bad as this problem is at present, malicious code difficulties will only get worse. This is primarily a result of the proliferation of personal computers (with minimal built-in security controls), LANs, and a blatant disregard for safe computing practices. The number of variants and copycats of viruses has also increased and shows no signs of abating.
- ✓ **Wide area networks (WANs).** The use of WANs, linking governments, businesses, and educational institutions, continues to grow. An efficient response to a computer security incident is important for agencies linked via large networks such as an intranet or the Internet. Because of their interconnectivity, a compromise of one computer can affect

other systems that are connected to the network but are located in different organizations, resulting in possible legal or financial ramifications. Incident response teams are aware that intruder attempts to penetrate systems occur daily at numerous sites throughout the United States, yet many organizations remain unaware that their systems have been penetrated or have been used as springboards for attacks on other systems.

✓ **Reduced barriers to hacking.** Computing power is readily available, as is broadband connectivity. Hackers can download tools readily from the Internet, so relatively unskilled attackers can launch very sophisticated attacks.

Today, being prepared to handle a computer security incident has become a top priority for most system administrators. As businesses increase their online presence and their dependency on information systems' assets, the number of computer incidents also rises. These organizations are finally recognizing their need to adapt their security positions accordingly. This is accomplished in three stages.

First, organizations must develop and implement security plans and controls in a proactive effort. Second, they must work to ensure that their plans and controls are effective by continually reviewing and modifying them to guarantee that appropriate security is always in place. Finally, when controls are bypassed, either intentionally or unintentionally, organizations must be prepared to act quickly and effectively to minimize the impact of these lapses.

The prime objective of these security measures is to prevent an operational security problem from becoming a business problem that impacts revenue. Administrators and other users can obtain guidelines in this book to preplan a response to incidents and minimize any negative impact to a business. Waiting until an incident has occurred is naturally too late to begin planning how to address such an event. Incident response planning requires maintaining both administrative and technical roles. Each party must be familiar with the other's role, responsibilities, and capabilities.

Many computer security programs are not effective in dealing with newer and less-understood classes of threats to security. Traditional responses, such as risk analysis, contingency planning, and computer security reviews, have not been adequate in controlling incidents and preventing large-scale damage. Anecdotes abound wherein security incidents grow worse or where they have not been eradicated from a system. Consequently, some organizations spend far too much time reacting to recurring incidents, sacrificing convenience and productivity. Fearing unknown threats, some institutions have misguidedly restricted access to their systems and networks. What is needed instead therefore is a fundamentally different form of computer security response, a response that is able to quickly detect and react to incidents in a manner that is both efficient and cost-effective.

caution

A business should always make the effort to eradicate a security incident from the system immediately. For example, when companies fail to patch their e-mail programs for known and publicized flaws, they may get hit with a copycat virus that exploits the exact same flaw.

Having a computer security incident response capability means that an organization is prepared to detect and counter computer security incidents in a skilled and efficient manner. Such a capability is a combination of technically skilled people, policies, and techniques with the aim of constituting a proactive approach to handling computer security incidents. Having an incident response capability with traditional computer security elements can provide organization-wide protection from damaging incidents, saving the organization valuable resources and permitting it to take better advantage of the latest computer technology. Many businesses, organizations, and government agencies have implemented incident response capabilities with great success, generally focusing on the following areas:

- ✓ **Efficient response.** Efficiency is one of the most important aspects of a computer security incident response capability. Without an efficient capability, incident response is disorganized and ineffective, with the organization maintaining higher expenses and leaving vulnerabilities open and unprotected. For example, uneducated responses to small outbreaks of computer viruses can actually make their effects far worse, resulting in hundreds of computers being infected by the response team itself. A proper computer security incident response capability helps in the management of incident response expenses that are otherwise difficult to track, makes risk assessment more accurate, and improves user training and awareness with regard to computer security. Conversely, an inefficient incident response effort can perpetuate existing problems and even exacerbate them.
- ✓ **Centralization.** A security incident response capability must utilize centralized means for reporting and handling incidents. While this undoubtedly increases efficiency, it also permits a more accurate assessment of the incidents, such as whether they are related (in order to more quickly avert possible widespread damage). By virtue of centralization, incident response capability expenses and overhead can be kept down, and duplication of effort can be reduced (possibly eliminated entirely). Organizations may find a significant cost savings as a result.
- ✓ **Improved user awareness.** The benefits of an incident response capability include enhanced user awareness of threats and knowledge of appropriate controls. An incident response capability will help an organization identify vulnerabilities and issue computer security alerts. Information regarding security awareness can be disseminated throughout the organization by using a variety of mechanisms such as a company intranet, seminars, and training workshops. Such information greatly improves the users' ability to manage their systems efficiently and securely.

Developing a Computer Security Incident Response Capability

Because of the volume of business being done via the Internet, minimizing security vulnerabilities and maximizing the response to security incidents in an efficient and thorough manner can be critical to business continuity. Organizations often find, however, that they need not build this capability entirely from scratch. Many organizations will realize that they already possess the necessary building blocks for sufficient incident responses. These include help desks, central hotlines, and personnel with the requisite technical skills. The following are additional necessary features for a computer security incident response capability:

- ✓ **Structure.** There is no single structure for a computer security incident response capability. Depending on the organization's needs, this capability can take many forms. While centralization often presents the most cost-effective structure, some organizations find that a more widely distributed structure, despite some inevitable overlap, fits in best with existing structures. Very small organizations may find it practical to share an incident response capability with a larger organization. Hence, an incident response capability structure will vary depending on a variety of factors. Centralized reporting and centralization of effort, however, generally helps decrease operating costs and improve efficiency and security.
- ✓ **Alert mechanisms.** The incident response capability should include the capacity to quickly reach all users by sending an alert to a central mailing list, or, alternatively, telephone voice mail, messages via pagers or memorandums, or management contact lists.
- ✓ **Centralized reporting.** Effective incident response depends upon an organization's ability to quickly and conveniently communicate. Effective communications mechanisms include a central telephone hotline monitored on a 24-hour basis, a central e-mail messaging address, or a pager/cell phone arrangement. Users are more inclined to contact their computer security incident response personnel if the organization has made the communication straightforward (for example, users only have to remember one telephone number).
- ✓ **Personnel.** The organization should create a group of individuals that are responsible for handling incidents: a computer incident response team. Computer security incident response personnel must diagnose and/or understand technical problems, thus technical knowledge is a primary requirement for team members. Superior communications skills are equally important. Computer security incidents can generate emotionally charged situations; a skilled communicator must know how to resolve technical problems without fueling negative emotions or further complicating the situation. In addition, incident response personnel may spend much of their time communicating with affected users and managers, either directly or by preparing alert information, bulletins, and other guidance materials. It may be difficult, yet imperative, to find personnel who have the correct mix of technical, communications, and social skills.

The Computer Security Incident Response Team

Networks and IT resources remain persistently vulnerable to illegal and malicious activity and exploitation from both internal and external sources. The most common security threats are to network systems. Network security threats include impersonation, eavesdropping, denial of service, and packet replay/modification. Damage to IT systems from an intrusion into one or more computers can occur in a short period of time. It is essential that all organizations have procedures in place that can be activated without delay. The failure to report an intrusion to security personnel will impact (and potentially compromise) the security efforts of the rest of the organization as well as its customers.

To develop a complete incident response capability, all organizations need an incident response team. In the event of suspected computer crime or violations of user policies, the team should be engaged. Beforehand, the team should have written procedures for incident response, including what conditions warrant calling in local and/or federal law enforcement authorities. For example, inside violations of user policies may result in administrative actions such as employee suspension or termination of employment, while other, more serious computer crimes may warrant that law enforcement be contacted.

In either case, the incident response team must protect evidence. For policy violations and administrative actions, the following procedures may be sufficient. However, for more serious computer crimes, law enforcement authorities may instruct the incident team to wait for their arrival before taking action.

The actions required for securing a suspected computer incident scene include

- ✓ Securing the scene
- ✓ Documenting and labeling evidence
- ✓ Transporting the evidence
- ✓ Shutting down the computer(s)

The Incident Reporting Process

As mentioned earlier in this chapter, all organizations need to establish and implement an internal incident response capability. Intrusions are only one form of computer security incident. Remember, a computer security incident is any adverse event wherein some aspect of a computer system is threatened. This could include loss of data confidentiality, disruption of data integrity, and disruption or denial of service. The types of incidents are classified into low, medium, or high levels depending on their severity.

Low-level incidents are the least severe and should be resolved within one working day after the event occurs. These include

- ✓ Loss of passwords
- ✓ Suspected unauthorized sharing of accounts
- ✓ Misuse of computer hardware
- ✓ Unintentional computer actions
- ✓ Unsuccessful scans or probes

Mid-level incidents are more serious and should be handled the same day the event occurs (normally within two to four hours of the event). These include

- ✓ Property destruction related to a computer incident
- ✓ Illegal download of copyrighted music/unauthorized software
- ✓ Violation of special access
- ✓ Unauthorized use of a system for processing or storing personal data
- ✓ An act resulting from unfriendly employee termination
- ✓ Illegal building access
- ✓ Personal theft (moderate in value) related to a computer incident

High-level incidents are the most serious. Because of the gravity of these situations and the likelihood of damage resulting to the organization's bottom line, these types of incidents should be handled immediately. They include

- ✓ Property destruction related to a computer incident
- ✓ Child pornography
- ✓ Pornography
- ✓ Personal theft (higher in value than a mid-level incident) related to a computer incident
- ✓ Suspected computer break-in
- ✓ Denial of Service (DoS) attacks
- ✓ Illegal software download
- ✓ Malicious code (for example, viruses, worms, Trojan horses, and malicious scripts)
- ✓ Unauthorized use of a system for processing or storing of prohibited data
- ✓ Changes to system hardware, firmware (for example, BIOS), or software without the system owner's authorization
- ✓ Any violation of the law

Other types of incidents may include *isolated* cases of viruses or misuse of computer equipment, unintentional actions, and common, unsuccessful scans or probes. When faced with a security incident, an organization should be able to respond in a manner that both protects its own information and helps protect the information of others that might be affected by the incident.

Assessment and Containment

Every organization needs to develop internal reporting procedures that define the actions that must be taken in responding to and reporting computer security incidents. At a minimum, internal procedures should include the organization chain of authority or hierarchy and require the involvement of all of the organization's computer security personnel. These procedures also require the following:

- ✓ Preservation of evidence
- ✓ Assessment
- ✓ Containment and recovery actions
- ✓ Damage determination
- ✓ Report documentation
- ✓ Lessons learned
- ✓ Identification of corrective actions required by the organization's security programs

Organizations should distribute computer security procedures to all appropriate personnel responsible for identifying, reporting, or handling high-level incidents. Responsible parties should be instructed to read and become familiar with the incident reporting policy. Individuals assigned to incident handling or reporting may be organized into a response team that becomes active when a breach is identified.

All organizational networks must be monitored on an ongoing basis. It is not necessary to obtain and install intrusion detection devices or software for every server. Only the most critical locations need to have intrusion detection installed. As soon as suspicious activity is detected, qualified personnel designated to respond must be notified to take immediate action.

The upper-level management personnel authorized to take containment actions should assess the event and take appropriate action. This may include shutting down a system within a reasonable time after discovery of an intrusion to contain any future damage. In extreme instances, if the incident response team fails to adequately respond or if the problem is not contained in a timely manner (usually 12 hours), the organization's chief information officer (CIO) or designate may issue an order to bring the entire system down. Reporting directly to the CIO or upper-level management should occur in cases where a preliminary assessment indicates that significant damage to organizational resources may have occurred. Upon confirmation, the incident response actions must be implemented immediately. The unavailability of any official in the reporting chain should not delay the continuation of the incident notification or response process.

Recovery Operations

Every organization should prioritize those actions that support the smooth recovery of a compromised system. In no case should a compromised system, Web page, or application be returned to normal operation without the approval of the CIO or the person designated to be in charge of computer security. Computer security officers should reserve the right to further scrutinize the system to ensure that appropriate security is in place and continues to protect the organization. The organization should resume normal operation of the restored system only upon approval by the security team. Security personnel should usually request a 24-hour period for responding to the incident with the power to approve or disapprove the return of the system to normal operations.

Damage Analysis and Determination

A damage assessment of all computer security incidents is to be initiated immediately after containment and recovery actions have been carried out. Computer security officers should determine if the incident is confined to one system or to multiple systems and if there is any impact on outside organizations. The impact to each system should be analyzed to determine if control of the system has been compromised. All compromised systems should be disconnected from external communications immediately or as soon as possible. Control of a system is lost when an intruder obtains control of powerful root or system accounts with high-level administrative privileges. A determination should also be made if log files have been erased or compromised.

Shutdown Procedures while Preserving Evidence

Powering down a computer system in a manner that will not corrupt the integrity of existing files is a complicated computer security procedure. In the event of a suspected computer incident, great care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, merely opening a file changes it. In a legal sense, it is no longer the original evidence and at that point may be inadmissible in any subsequent legal or administrative proceedings.

Opening a file also alters the time and date it was last accessed. On the surface this may not seem an important issue; however, it could later become extremely important in the determination of who committed the violation and when it occurred. Isolation of the computer system is ideal, but if this cannot be accomplished due to operational requirements, no attempts should be made to recover or view files at the local level.

The isolation of a computer system so that evidence is not lost is of the utmost importance. Consideration must also be given to other storage media, handwritten notes, and documents found in the vicinity of the computer involved. These items can be of value in an ensuing investigation. Computer disks, CD-ROMs, tape storage media, and/or additional hard drives found in the area of the computer also must be isolated and protected.

No one, including the individual suspected of committing the alleged computer violation, should be allowed contact with the storage media or the computer involved in the security incident. Individuals with extensive computer experience can develop programs that, with a few keystrokes, can destroy all magnetic data on a hard drive.

Generally the type of operating system a company uses dictates the timing and the manner in which a computer is powered down. With some operating systems, merely pulling the power plug is the preferred method. With other systems, disconnecting the power supply without allowing the operating system to initiate internal shutdown could result in the loss of files or, in rare instances, a hard drive crash. Potential evidence may reside in typical storage areas such as the spreadsheet, database, or word processing files. However, potential evidence may also be in file slack (file slack is the unused space in a data cluster that's at the end of most files), erased files, and Windows swap files. Potential evidence in these locations is usually in the form of data fragments and can be easily overwritten by booting the computer and running the operating system.

For example, when the Windows operating system boots up (loads), it generates new files and opens existing files. This has the potential to overwrite and destroy data or possible evidence previously stored in the Windows swap file. To use another example, when word processing or other program files are opened and viewed, temporary files are created and overwritten by updated versions of files, making potential evidence stored in these locations subject to loss. According to the U.S. Department of Energy's First Responder's Manual, the following are the basic characteristics and procedures (broken down by operating system) that should be followed when an operating system shutdown is warranted.

MS-DOS OPERATING SYSTEM

Characteristics

- ✓ Text is on a solid background (usually black).
- ✓ The prompt contains a drive letter and uses backslashes.
- ✓ The prompt usually ends with a greater than sign (>).

Shutdown Procedures

- ✓ Photograph the screen and annotate any programs running.
- ✓ Pull the power cord from the wall.

WINDOWS 3.X OPERATING SYSTEM

Characteristics

- ✓ Program Manager
- ✓ Colored tile bar
- ✓ Standard menu options

Shutdown Procedures

- ✓ Photograph the screen and annotate any programs running.
- ✓ Pull the power cord from the wall.

WINDOWS NT 3.51 OPERATING SYSTEM

Characteristics

- ✓ Program Manager
- ✓ Colored tile bar
- ✓ Standard menu options
- ✓ Icons representing network computers and people

Shutdown Procedures

- ✓ Photograph the screen and annotate any programs running.
- ✓ Pull the power cord from the wall.

WINDOWS 95/98/NT 4.0/2000/XP OPERATING SYSTEM

Characteristics

- ✓ The Start button has a Windows symbol.

Shutdown Procedures

- ✓ Photograph the screen and annotate any programs running.
- ✓ Pull the power cord from the wall.

UNIX/LINUX OPERATING SYSTEM

Characteristics

- ✓ The Start button has a Unix/Linux version symbol.

Shutdown Procedures

- ✓ Photograph the screen and annotate any programs running.
- ✓ Right-click to the menu.
- ✓ From the menu, click Console.
  - The root user prompt is set to # sign. If not present, change user to root (type `su -`). At that point you are prompted for the root password. If the password is available, enter it. At the # sign, type `sync;sync;halt`, and the system will shut down. If you do not have the root password, pull the power cord from the wall.
  - If the # sign is displayed when at the console, type `id` and press Enter. If you see that your user ID is root, type `sync;sync;halt`, and press Enter. This will shut down the system. If your user ID is not root, pull the cord from the wall.

MAC OS OPERATING SYSTEM

Characteristics

- ✓ An Apple symbol in the upper left corner
- ✓ Small horizontal lines on the window's menu bar
- ✓ A single button in each corner of the window
- ✓ Trash icon

Shutdown Procedures

- ✓ Photograph the screen and annotate any programs running.
- ✓ Record the time from menu bar.

- Click Special.
- Click Shutdown.
- The window tells you it is safe to turn off the computer.
- Pull the power cord from the wall.

NIPC Recommendations for Victims

In addition to protecting your systems, the National Infrastructure Protection Center advises you to also consider taking the following actions to increase the chances of apprehending the perpetrator:

- Respond quickly. Contact law enforcement officials.

x-ref

For more on the pros and cons of dealing with law enforcement, see Chapter 2.

- If unsure of what actions to take, *do not* stop systems processes or tamper with files. This may destroy traces of an intrusion.
- Follow organizational policies/procedures. (Your organization should have a computer incident response capability/plan.)
- Use the telephone to communicate. Attacker(s) may be capable of monitoring e-mail traffic.
- Contact the incident response team for your organization. Quick technical expertise is crucial in preventing further damage and protecting potential evidence.
- Consider activating Caller Identification on incoming lines. This information may help in leading to the identification of the source/route of intrusion.
- Establish points of contact with general counsel, emergency response staff, and law enforcement officials. Preestablished contacts will help in a quick response effort.
- Make copies of files an intruder may have altered or left behind. If you have the technical expertise to copy files, this action will assist investigators in determining when and how the intrusion may have occurred.
- Identify a primary point of contact to handle potential evidence.
- Establish a chain-of-custody procedure that tracks who has been involved in handling the evidence and where it has been stored. Potential hardware/software evidence that is not properly controlled may lose its value.
- *Do not* contact the suspected perpetrator.

Building an Incident Response/Forensic Toolkit

There are two important issues when it comes to collecting digital evidence: authenticity and integrity. You need to be able to demonstrate that the evidence is what you say it is, came from where you say it came from, and has not been modified since you obtained it. How you collect and document evidence to preserve its authenticity and reliability depends on the circumstances and the computer systems you are dealing with. A dependable set of tools is invaluable for those in charge of incident response. A properly outfitted toolkit enables its owner to efficiently collect evidence for later analysis and should contain at a minimum the following basic elements:

- ✓ A tool to report any open TCP and UDP ports and map them to the owning process or application
- ✓ A tool to capture and analyze logs to identify and track who has gained access to a computer system
- ✓ A utility to make a bit-stream backup of a hard drive
- ✓ A tool to examine files on a disk drive for unauthorized activity
- ✓ A program used to document the CMOS System Time and Date on a computer seized as evidence
- ✓ A password-cracking utility
- ✓ A text-search utility that can scan DOS and Windows systems and locate targeted keywords and/or strings of text in computer-related investigations and computer security reviews
- ✓ A forensic binary data search tool that is used to identify targeted graphics file content and/or foreign language words and phrases stored in the form of computer data
- ✓ A tool to discover hidden files, such as NTFS Alternate Data Streams
- ✓ A data collection tool to capture file slack and unallocated (erased file) data

note

The previous list covers basic forensic tools and is not meant to be all-inclusive.

While there are a number of toolkits for Windows platforms, relatively few exist for the Unix or Linux operating systems. The Coroner's Toolkit (TCT), a software package that is the de-facto standard for collecting forensic evidence from Unix platforms and the plethora of forensic tools available for the Windows platform, are covered in detail in Chapter 7.

Chapter Summary

The Internet is the largest operating computer network in the world. Because it is largely a public network, threats may come from all corners of the globe. To protect themselves against the constant threat of hackers, crackers, and malicious code, organizations often make use of firewalls, antivirus software, and intrusion detection systems. Despite sophisticated defensive measures, however, computers and the networks that connect them are still subject to frequent attacks. As a result of this unfortunate fact, organizations and governments around the world must remain prepared to respond to a variety of threats by any computer security incident that circumvents security measures.

Key points covered in this chapter include

- ✓ The fundamentals and importance of computer forensics and incident response
- ✓ How to recognize the signs of a computer security incident
- ✓ How to verify that a computer security incident has occurred
- ✓ The basic steps all organizations should follow in preparation for responding to incidents
- ✓ How to verify that a security incident has occurred while preserving key evidence
- ✓ Specific types of response measures useful against modern day attacks
- ✓ The importance of building a forensic toolkit

Chapter 2

Addressing Law Enforcement Considerations

In This Chapter

- ✓ A look at the U.S. Constitution's Fourth Amendment
- ✓ A brief primer on the Freedom of Information Act
- ✓ The pros and cons of dealing with law enforcement
- ✓ Information-sharing issues in computer crime investigations
- ✓ The role of the National Infrastructure Protection Center (NIPC)
- ✓ Understanding disclosure and discovery
- ✓ A brief overview of federal computer crimes and laws

THERE IS A GROWING CONCERN that individuals, organizations, and governments around the globe are *increasingly* at risk when they choose to ignore the threats posed by hackers, intruders, and malicious code. The rash of malicious code outbreaks over the past several years are observable demonstrations of how an individual may cause widespread harm by infecting hundreds of thousands of computers within a matter of hours, and that he or she can locate targets even when vulnerabilities are well known, highly publicized, and could easily be protected. Whatever their motivation, the actions of these individuals are oftentimes impossible to distinguish from one another. From a law enforcement perspective, catching criminals, terrorists, and intelligence operatives has never been more difficult than in today's cyber environment.

In today's setting, attacks and intrusions are encrypted, broken into packets, and routed the world over, anonymously passing through Internet and telecommunications providers that are under no obligation to keep track of how their systems are used or, more importantly, how they may be misused. Law enforcement authorities must act carefully when conducting computer criminal investigations to catch the perpetrators while preserving the privacy rights and civil rights of others. This chapter focuses on the legal aspects concerning computer crimes and the role law enforcement plays in computer crime investigations.

A Look at the Fourth Amendment

The Fourth Amendment of the U.S. Constitution declares that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." In the early 1900s, the Supreme Court's philosophy regarding the Fourth Amendment was geared mainly toward the safeguarding of property. The Court's desire to protect property was evident in its 1928 decision in *Olmstead* v. *United States* [277 U.S. 438 (1928)].

In *Olmstead*, the Supreme Court held that the use of a wiretap to intercept a private telephone conversation was not a "search" for purposes of the Fourth Amendment. One of the grounds on which the Court justified its result was that there had been no physical intrusion into the person's home. Under *Olmstead*'s narrow view of the Fourth Amendment, the amendment was not applicable in the absence of physical intrusion. Thus, without trespass or seizure of any material object, surveillance was deemed beyond the scope of the Fourth Amendment as interpreted by the Olmstead case.

In the landmark 1967 Supreme Court ruling *Katz* v. *U.S.*, however, it was deemed that a search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. Charles Katz was arrested for illegal gambling after he used a public telephone to transmit "gambling information." The FBI had attached an electronic recording device onto the outside of the public phone booth that Katz habitually used. They argued that this constituted a legal action since they never actually entered the phone booth. The Court, however, ruled in favor of Katz, stating the Fourth Amendment allowed for the protection of a person and not just a person's property against illegal searches. Whatever a citizen "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

At the conclusion of the Katz case, the Court held that physical penetration of a constitutionally protected area is not necessary before a search and seizure can be held to violate the Fourth Amendment. According to the Court in *Katz*, "once it is recognized that the Fourth Amendment protects people — and not simply 'areas' — against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." Thus, although the government's activities in *Katz* involved no physical intrusion, they were found to have violated the privacy on which the petitioner justifiably relied and thus constituted "search and seizure" within the meaning of the Fourth Amendment.

Changing technology precipitated the shift from protection of property to protection of privacy, and in 1968, just one year after *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act, authorizing microphone surveillance or wiretapping for law enforcement purposes, and requiring a warrant, based on probable cause, prior to such surveillance or wiretapping.

The most basic Fourth Amendment question, as it relates to federal computer cases, asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers (or other electronic storage devices) under the individual's control. For example, do individuals have a reasonable expectation of privacy in the contents of their laptop computers, floppy disks, or pagers? If the answer is "yes," then the government ordinarily must obtain a warrant before it accesses the information stored therein.

On July 24, 2000, Kevin V. DiGregory, deputy assistant attorney general for the U.S. Department of Justice, made the following statement before the Subcommittee on the Constitution regarding the Fourth Amendment and its application in the information age:

> It is beyond dispute that the Fourth Amendment protects the rights of Americans while they work and play on the Internet just as it does in the physical world. The goal is a long-honored and noble one: to preserve our privacy while protecting the safety of our citizens. Our founding fathers recognized that in order for our democratic society to remain safe and our liberty intact, law enforcement must have the ability to investigate, apprehend and prosecute people for criminal conduct. At the same time, however, our founding fathers held in disdain the government's disregard and abuse of privacy in England. The founders of this nation adopted the Fourth Amendment to address the tension that can at times arise between privacy and public safety. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.
>
> Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. The Electronic Communications Privacy Act (ECPA) establishes a three-tier system by which the government can obtain stored information from electronic communication service providers. In general, the government needs a search warrant to obtain the content of unretrieved communications (like e-mail), a court order to obtain transactional records, and a subpoena to obtain information identifying the subscriber. See 18 U.S.C. §§ 2701–11.
>
> In addition, in order to obtain source and destination information in real time, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. See 18 U.S.C. 3121, et seq.
>
> Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510–22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.
>
> The safeguards for privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement, clarifying what is acceptable evidence gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in preserving privacy. When law enforcement investigates, successfully apprehends, and prosecutes a criminal who has stolen a citizen's personal information from a computer system, for example, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.
>
> As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emerging technologies that are changing the face of communications. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

According to the U.S. Department of Justice, to determine whether an individual has a reasonable expectation of privacy of information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if law enforcement would be prohibited from opening a closed container and examining its contents in the same situation (under the same circumstances).

note

While a "reasonable expectation of privacy" applies to law enforcement investigations, it does not offer any protection to individuals from searches by their employers, parents, and spouses.

A Brief Primer on the Freedom of Information Act

The U.S. Freedom of Information Act (FOIA) is a law ensuring public access to U.S. government records. Under the Freedom of Information Act all federal agencies are required to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions contained in the statute.

The FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Each state has its own public access laws that must be consulted prior to accessing to state and local records. While the FOIA has opened the door to the sharing of information between government and the private sector, it has also become one of the biggest roadblocks in getting the private sector to disclose cyber-crime information to government agencies such as the FBI.

In his March 2000 testimony before the Senate Subcommittee on Technology, Terrorism and Government Information, Harris N. Miller, president of the Information Technology Association of America, stated, "Companies worry that if information sharing with government really becomes a two-way street, FOIA requests for information they have provided to an agency could prove embarrassing and probably costly. Many in industry believe that freedom from FOIA concerns is the most formidable obstacle, and that an exemption for this type of information sharing is the only option."

Reporting Security Breaches to Law Enforcement

The reluctance of victims of network intrusions to report such intrusions to authorities poses a considerable threat to the future of network security. Upon finding a hacker in their system, for example, network administrators sometimes consider it sufficient to close the intruder's account and patch the vulnerability that originally allowed the hacker to gain entry. This is akin to kicking the hacker out, then locking the door. Unfortunately, this does little to help with overall security. Not only is the intruder free to attempt the same exploit on another company's network, he or she may have been savvy enough to leave behind a *backdoor* through which to return to the exploited system later, undetected. In addition, others with malicious intent may learn of the exploit through the hacker community and because of the lack of law enforcement response, join in compromising computer systems.

To believe that a hacker is motivated solely by the desire to show off computing prowess with no real intention to damage, steal, or defraud is naive. What may appear to be a simple hack with no real risk of damage can, in fact, be a part of a larger scheme to launch a very destructive attack against other sensitive machines. Intruders may compromise numerous systems, collecting them like trading cards. Some hackers use the "stolen" computers as springboards to launch attacks against other computers, shutting down the next victim, taking information from the system, and using the stolen data in extortion schemes, or to engage in countless other types of illegal conduct. With each compromise, the security of all networks is weakened. If victims do not report such incidents, law enforcement cannot provide an effective and appropriate response.

Industry experts claim that there is a wide variety of reasons for the reluctance to report computer security incidents. There is the perception on the part of some businesses that there is little upside to reporting network intrusions. According to Richard P. Salgado, Trial Attorney for the Computer Crime and Intellectual Property Section of the U.S Department of Justice, the rationale for not reporting an intrusion includes the following:

- ✓ "The victim company does not know which law enforcement entity to call. Surely, the victim reasons, the local or state police will not be able to comprehend the crime, and the FBI and Secret Service would have no interest in my system.
- ✓ If the victim company does report the intrusion to an appropriate agency, law enforcement will not act. Instead, the fact of the intrusion will become public knowledge, irreparably shaking investor confidence and driving current and potential customers to competitors who elect not to report intrusions.
- ✓ If law enforcement does act on the report and conducts an investigation, law enforcement will not find the intruder. In the process, however, the company will lose control of the investigation. Law enforcement agents will seize critical data and perhaps entire computers, damage equipment and files, compromise private information belonging to customers and vendors, and seriously jeopardize the normal operations of the company. Only competitors will benefit as customers flee and stock value drops.
- ✓ If law enforcement finds the intruder, the intruder likely will be a juvenile, reside in a foreign country, or both, and the prosecutor will decline or be unable to pursue the case.
- ✓ If the intruder is not a minor, the prosecutor will conclude that the amount of damage inflicted by the intruder is too small to justify prosecution.
- ✓ If law enforcement successfully prosecutes the intruder, the intruder will receive probation or at most insignificant jail time, only to use his or her hacker experience to find fame and a lucrative job in network security."

Salgado states further that while the preceding list of excuses may appear startling, barriers to reporting can be overcome by better-informed computer network owners and operators, and skillful investigatory and prosecutorial practices. The risk presented by failing to report intrusions is enormous. For the foreseeable future, computer networks are only going to become more complex, more interconnected, and therefore more vulnerable to intrusions. Networks are also going to command more importance in our private lives, our nation's defense, and the world's economy. For these reasons, it is imperative that organizations and individuals understand the importance of reporting intrusions.

One of the more noticeable benefits of cooperation between private sector organizations and law enforcement agencies is the faster distribution of information about threats and the ways to counter them. Conversely, organizations in the private sector sometimes find that calling in law enforcement to investigate a computer crime may lead to the following:

- ✓ Loss of privacy of their personal information
- ✓ Loss of consumer confidence
- ✓ Retaliatory attacks by the intruder
- ✓ A shutdown of the business as the law enforcement agents seize and review evidence

While there have been attempts to alleviate the aforementioned fears and foster cooperative ventures between law enforcement and the private sector, victims of computer intrusion are still hesitant to call in law enforcement when an intrusion has occurred. In her opening speech at the April 5, 2000 Cybercrime summit, Attorney General Janet Reno addressed these issues. Following is an excerpt from her speech:

> Law enforcement, like industry, has its duties, its tools and its constraints. As a prosecutor for almost 15 years in Miami, I can tell you that I know how intrusive a criminal investigation can be. I have heard from bankers long before they talked in terms of cyber tools about why they didn't report an embezzlement, why they didn't want to put up with a criminal investigation. I want your opinions, your suggestions about what we can do in law enforcement to design investigations that achieve the truth, that do it according to principles of the Constitution and do it with the least disruption to your undertakings. We ask industry to recognize that law enforcement has much to offer to make the Internet a secure place for their businesses and customers. But I also recognize that it is hard for government to attract a sufficient number of people who have both the technical and the legal expertise to deal with the critical issues that we face. I have been so proud of those in the Department of Justice who have done so much with limited resources, limited equipment. And we want to work with you to understand better how we can attract people, what we can do to retain them, how we can work with you in public-private partnerships to achieve new goals. Senior officials from the Department's Computer Crime Section meet regularly with representatives from Internet service providers, telecommunications carriers, and others through information industry group. The FBI's National Infrastructure Protection Center and its Computer Crime Squads have worked to develop the Infragard Program in communities around the country, to build relationships. And I think relationships is what it is all about. Until that FBI agent sits down with your security officer or deals one on one in terms of an investigation, people do not know each other. But when they have that experience, when you have a good working relationship, when you can build on a good experience, you learn so much about how we can work together. I would like to use

> this opportunity to make sure that we do that in the most effective way possible. We have also begun regular meetings with the Law Enforcement and Security Council of the Internet Alliance, an industry group that includes many of the largest ISPs. Industry and law enforcement have made sincere efforts to cooperate and have made real gains. Today's conference is another step in the right direction. We are not interested in a top-down approach. We do not know best. We know that people in the field, state and local law enforcement, industry can tell us what needs to be done. And we can provide a vantage point that can be helpful, as well. We do not want invasive government regulation or monitoring of the Internet. We must recognize that with overlapping areas of responsibility and control we can do so much if we define the particular function of each. The private sector in that regard should take the lead, I think, in protecting the security of private-sector computer systems. We must take the lead in protecting government systems. And we must share information about vulnerabilities so that we can each take steps to protect our systems against attack. Once the systems have been victimized, law enforcement must take the lead on investigating network and other computer crimes. We need to ensure that we have the technical and legal tools necessary to do it. We also want to ensure that we have the information and continued cooperation necessary to effectively investigate these cases. Always mindful that the victim is concerned about confidentiality, that the victim is concerned about the intrusion of the law enforcement process in their business, we need to design an approach that can be effective. These are the issues that we jointly face. This is an opportunity to speak directly, but even then we have another challenge. What happens when you learn information about a particular issue that if linked with ten other people or ten other businesses' information indicates a real threat to national security or a real threat to the Internet or a real threat to business? How can we develop the trust that will permit us to share information? If we share information how can we develop a process that will provide us a procedure for giving early warning to all concerned to avoid further injury to all concerned without interrupting or interfering with your business processes?

In her speech, Reno maintained that in order to balance constitutional rights such as privacy and freedom of speech with safety and security, a close relationship must be forged between law enforcement and private industry. As we've seen however, organizations are often reluctant to call in law enforcement because they fear the loss of confidential data or negative publicity. But, it is only when cyber crime is brought to the attention of law enforcement by businesses and other victims that effective measures can be taken to battle it.

Information Sharing Issues in Computer Crime Investigations

Individuals and organizations in the private sector are usually the first victims of malicious code and hackers. While this is an unfortunate fact, law enforcement agencies invariably benefit when the private sector shares its knowledge and experience with them. In fact, government agencies such as the Computer Crime and Intellectual Property Section of the U.S. Department of Justice (`www.cybercrime.gov`) and the National Infrastructure Protection Center (`www.nipc.gov`) routinely collect intelligence from industry in an effort to help solve computer crime cases and prevent future ones.

As mentioned earlier in this chapter, organizations are often concerned that information shared with the government might be made public. In his testimony of March 2000, Harris Miller also opined the following:

> Companies are understandably reluctant to share sensitive proprietary information about prevention practices, intrusions, and actual crimes with either government agencies or competitors. Information sharing is a risky proposition with less than clear benefits. No company wants information to surface that they have given in confidence that may jeopardize their market position, strategies, customer base, or capital investments. Nor would they risk voluntarily opening themselves up to bogus but costly and time-consuming litigation. Releasing information about security breaches or vulnerabilities in their systems presents just such risks. Negative publicity or exposure as a result of reports of information infrastructure violations could lead to threats to investor — or worse — consumer confidence in a company's products. Companies also fear revealing trade secrets to competitors, and are understandably reluctant to share such proprietary information. They also fear sharing this information, particularly with government, may lead to increased regulation of the industry or of Electronic Commerce in general.
>
> These concerns are relevant whether we are talking about inter-industry, cross-industry, or industry/government information sharing. Combine this with a historic lack of trust towards law enforcement, or a concern that company systems may become caught up in an investigation and thus lose production/development time, and many companies find it easier to keep quiet and absorb the pain inflicted by intrusions, even at substantial cost. I also would be remiss if I did not remind the committee of a company's need to protect individual customers' privacy. Industry fears that privacy breaches on innocent customers might inadvertently occur during investigations.
>
> Few high-tech companies are interested in being perceived by their customers as the active agents of law enforcement. Agencies, meanwhile, are often viewed as demanding this type of information from the private sector but giving little back in return. Let me be blunt. Information sharing cannot be a one-way street.

Under the Freedom of Information Act, information such as the extent of damages caused by a virus infection or hacker incident might well become public, damaging an organization's reputation, and aiding the competition as a side effect. By sharing details of an attack with law enforcement agencies, organizations could increase their odds of detecting and reducing the threats of cyber-criminal activity.

The current U.S. legal system makes it complicated and difficult to share information about intrusion cases before any arrests can be made. To address privacy concerns, information is to be safeguarded, classified, and protected, and everything possible should be done to make sure that the information gets only into the appropriate hands. Confidential data (such as personal financial and medical records) are routinely transferred across a series of information systems. There are many ways to safeguard this information and ensure that only those who need to know have access to it and then in only limited amounts.

The Role of the National Infrastructure Protection Center

The National Infrastructure Protection Center (NIPC) was established in the early part of 1998, with the purpose of serving as the U.S. government's center for threat assessment, warning, investigation, and response to threats or attacks against our critical information infrastructures. These infrastructures include banking, telecommunications, energy, water systems, government operations, and emergency services. Following is a list of the NIPC's functions as described on their Web site (`www.nipc.gov`):

- ✓ The NIPC is the national focal point for gathering information on threats to critical infrastructures as well as the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts.
- ✓ The NIPC includes investigators and analysts experienced in computer crimes and infrastructure protection. It is linked electronically to the rest of the federal government, including other warning and operation centers, as well as private sector Information Sharing and Analysis Centers (ISACs).
- ✓ The NIPC provides law enforcement and intelligence information and reports to relevant federal, state, and local agencies as well as private-sector ISACs. Before disseminating such information, the NIPC coordinates with the intelligence community to protect national security interests.
- ✓ When it detects an increased threat condition, the NIPC issues attack warnings and protective guidance to private-sector ISACs and the owners and operators of computer systems.

The NIPC combines the efforts of the law enforcement, intelligence, and the defense communities. By combining efforts, the NIPC can provide a unique response perspective to threat and incident information obtained from investigation, intelligence collection, foreign liaison, and private sector cooperation. This perspective ensures that all information is examined from a multidiscipline perspective.

While developing infrastructure protection capabilities, the NIPC has held firm to two guiding tenets. "First, the government can only respond effectively to threats by focusing on protecting assets against attack while simultaneously identifying, investigating, and responding to those who nonetheless would attempt or succeed in launching those attacks. And second, the government can only help protect this nation's most critical infrastructures by building and promoting a coalition of trust, one . . . amongst all government agencies, two . . . between the government and the private sector, three . . . amongst the different business interests within the private sector itself, and four . . . in concert with the greater international community." The focus of the NIPC is to develop the capacity to warn, investigate, and build partnerships, as well as initiate effective responses to computer security incidents.

Understanding Disclosure and Discovery

Computers and the vast array of networks that connect them have become indispensable to the smooth operation of businesses, government, and even our personal lives. Increasingly, disclosure and discovery involves data that is generated by computers, stored on computers, or can only be deciphered by computers. Disclosure and discovery are two different legal procedures. The process of discovery occurs during the period in which a court case is pending. Both plaintiff and defendant parties determine what the issues of their case are and what evidence exists that relates to the case. The rules of disclosure require that each party affirmatively disclose all facts and witnesses of which they are aware — whether helpful or harmful to their case — to the opposing party.

Electronic disclosure is the review and production of evidentiary material retrieved from electronic formats. This may include e-mail messages, word-processing documents, spreadsheets, databases, and presentations. Such data can be stored or found on portable media (for example, floppies, CDs, and tapes), hard drives, residual data (for example, deleted data), personal organizers (such as Palm Pilots), mobile telephones, and employee personal computers.

Paper is no longer the only source of documentary or text evidence. In fact, many of the documents created today exist *only* in electronic (digital) form. This has made paper disclosure almost archaic. Nevertheless, the disclosure and discovery of computer evidence in civil proceedings does present some unique problems that paper evidence would not. Among the most common difficulties are

- ✓ The location and volume of data
- ✓ The preservation of data subject to discovery
- ✓ Retrieving documents that have been deleted from the computers
- ✓ Retrieving embedded e-mail messages
- ✓ The conducting of an on-site inspection
- ✓ The need to contract expert assistance

In this ever-growing world of digital dependence, many e-mail messages and word-processing documents are never fully deleted. Instead, they continue to reside somewhere on the user's hard drive. By pressing Delete on your computer keyboard, you are not *actually* destroying the document. Nor are you throwing the document out when you place it in your computer's Recycle Bin or empty the Trash (Windows and Mac systems). Instead, you've simply deleted the "directions" the computer uses to find the data. The actual data remains until new data comes along and overwrites it.

x-ref

Chapter 6 covers data analysis and retrieval in detail.

Operating systems, data storage devices, and our ability to access remote data continue to evolve, forcing electronic disclosure procedures to evolve as well. The idea of addressing these issues and doing so correctly can quickly become daunting. It is important to realize however, that qualified professional help is available to assist in the electronic disclosure process. To better understand current disclosure law, following is Title 18, Part I, Chapter 121, Sec. 2702 of the Federal Criminal Code as it relates to disclosure of computer information:

Disclosure of Contents

(a) Prohibitions. Except as provided in subsection (b)

1. a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
2. a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
   - A. on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
   - B. solely for the purpose of providing storage or computer-processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and
3. a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph 1 or 2) to any governmental entity.

(b) Exceptions. A person or entity may divulge the contents of a communication

1. to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
2. as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
3. with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
4. to a person employed or authorized or whose facilities are used to forward such communication to its destination;
5. as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
6. to a law enforcement agency—

A. if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; or

B. if required by section 227 of the Crime Control Act of 1990 [42 U.S.C.A. S 13032]; or

C. if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

(c) Exceptions for disclosure of customer records. A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service, not including the contents of communications covered by subsection (a)(1) or (a)(2)

1. as otherwise authorized in section 2703;
2. with the lawful consent of the customer or subscriber;
3. as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
4. to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or
5. to any person other than a governmental entity.

Because of the universal widespread use of computers, computer-based discovery and disclosure has now become commonplace in civil litigation. While it does in many ways promise to simplify trial preparation and presentation, it is complicated, and as such it also has the potential to dramatically increase the costs connected with such litigation. Computer-based discovery and disclosure can be costly as a result of the manpower that must be contributed by hired experts in the field. Most observers believe that in spite of its costs, computer-based discovery will eventually overtake conventional discovery, as more and more information is routinely generated, transmitted, and stored on computers. Many of the costs associated with computer-based discovery can be avoided through proper management of the discovery process as well as the early detection of potential problems and their solutions.

Federal Computer Crimes and Laws

The FBI estimates that the vast majority of computer intrusions go undetected and those that are detected go unreported. The primary reason so few attacks are reported by organizations is the fear that employees, clients, and stockholders will lose faith in the organization if they admit that their systems have been attacked. Not all computer break-ins may be considered federal crimes.

In general, a computer crime breaks federal laws when it involves one of the following:

- ✓ The theft or compromise of national defense, foreign relations, atomic energy, or other restricted information
- ✓ A computer owned by a U.S. government department or agency

- ✓ A bank or most other types of financial institutions
- ✓ Interstate or foreign communications
- ✓ People or computers in other states or countries

In the United States, there are numerous federal laws protecting against attacks on computers, misuse of passwords, electronic invasions of privacy, and other cyber transgressions. One of the earliest pieces of legislation geared toward the cyber world was the Computer Fraud and Abuse Act of 1986. This central piece of legislation governs most common computer crimes, although many other laws may also be used to prosecute different types of computer crime. The act amended Title 18 of the United States Code §1030. This act was designed to complement the Electronic Communications Privacy Act of 1986, which served to outlaw the unauthorized interception of digital communications. The Computer Abuse Amendments Act of 1994 expanded the 1986 act to address the transmission of viruses and other harmful code. More recently, the USA Patriot Act of 2001 (covered later in this chapter) made additional sweeping changes to federal computer crime laws.

The Computer Fraud and Abuse Act of 1986

On October 16, 1986, President Reagan signed into law the Computer Fraud and Abuse Act, which received overwhelming support from the House, Senate, and the Justice Department. The act was approved with the intent of making clear the definitions of criminal fraud and abuse for federal computer crimes and was designed to help remove some of the legal ambiguities and obstacles to prosecuting computer-related crimes. It also established new felony offenses for the unauthorized access of "federal interest" computers and made the unauthorized trafficking in computer passwords a misdemeanor. Following is the text of the Computer Fraud and Abuse Act of 1986 act in its original form:

Computer Fraud and Abuse Act of 1986 (US) 18 USC 1030

(a) Whoever

1. knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;
2. intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

3. intentionally, without authorization to access any computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer;
4. knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;
5. intentionally accesses a Federal interest computer without authorization and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby—
   - A. causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or
   - B. modifies or impairs, or potentially modifies or impairs the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or
6. knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
   - A. such trafficking affects interstate or foreign commerce; or
   - B. such computer is used by or for the Government of the United States; shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
(c) The punishment for an offense under subsection (a) or (b) of this section is

1. (A) a fine under this title or imprisonment for not more than ten years or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and
2. (A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

3. (A) a fine under this title or imprisonment for not more than five years or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement, which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section—

1. the term “computer” means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device;
2. the term “Federal interest computer” means a computer—
   - A. exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution’s operation or the Government’s operation of such computer; or
   - B. which is one of two or more computers used in committing the offense, not all of which are located in the same State;
3. the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;
4. the term “financial institution” means—
   - A. an institution with deposits insured by the Federal Deposit Insurance Corporation;
   - B. the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
   - C. a credit union with accounts insured by the National Credit Union Administration;
   - D. a member of the Federal home loan bank system and any home loan bank;
   - E. any institution of the Farm Credit System under the Farm Credit Act of 1971;
   - F. a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and
   - G. the Securities Investor Protection Corporation;

5. the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
6. the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and
7. the term "department of the United States" means the legislative or judicial branch of the government or one of the executive departments enumerated in section 101 of title 5.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

As one can see, the legislation was carefully designed to address *only* federal and interstate computer crimes. This was born out of a concern that the act could violate individual state computer crime laws. According to the act, a federal interest computer, is "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government, and the conduct constituting the offense affects such use, or which is one of two or more computers used in committing the offense, not all of which are located in the same State." Financial institutions covered by the act specifically include federally insured banks, thrifts and credit unions; registered securities brokers; members of the Federal Home Loan Bank System, the Farm Credit Administration, and the Federal Reserve System. A felony conviction under the Computer Fraud and Abuse Act could result in a prison term of five years for a first offense and ten years for a second offense.

The Computer Fraud and Abuse Act of 1986 came about as the result of years of research and discussion among those in the legislative community. One of the principal reasons for the act's delay was the enormous difficulty in collecting testimony from computer crime victims. Organizations were (and continue to be) exceedingly hesitant to admit they had been victimized because they were apprehensive about having their vulnerabilities publicized.

The Computer Abuse Amendments Act of 1994

Back in the 1980s computer displays were largely text based with monochrome monitors. However the computer chip "wars" of the mid-1990s changed all that. The 1990s saw exponential advances in personal computer power and capability, allowing personal computers to handle even complex graphic applications. One important graphic application that changed the world of computers was the Web browser. With its point-and-click interface and ease of use, the Web browser helped usher in the Internet revolution.

With more and more individuals and organizations purchasing Internet-enabled computers and discovering and exploring the Internet, new legislation was required to keep up with the ever-changing computer landscape. Realizing the inadequacy of the Computer Fraud and Abuse Act of 1986, a new crime bill called the Computer Abuse Amendments Act of 1994 was signed into law. The amendments, which are an extension of the Computer Fraud and Abuse Act, significantly increase the chances of successfully prosecuting computer hackers by changing the standard from "intent" to cause harm to "reckless disregard" and by addressing the transmission of viruses and other harmful code. In addition, while previous laws protected only "federal interest computers" (machines belonging to a government agency or financial services firm), the new regulations cover computers "used in interstate commerce," meaning *any* PC connected to the Internet.

The USA Patriot Act of 2001

The tragic events of September 11, 2001 proved that the United States is not immune to terrorist attacks. This USA Patriot Act of 2001, also known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, was signed into law on October 26, 2001 by President George Bush. The act was quickly drafted by the Bush administration as part of the U.S. government's commitment to finding and eliminating terrorists. The legislation, which contains several provisions that directly affect information technology, originated with Attorney General John Ashcroft, who asked Congress for additional powers that he claimed were needed to fight terrorism in the wake of the events of September 11, 2001. Few amendments were made to Ashcroft's initial proposal to Congress, and the bill became law without any hearings or markup by a Congressional committee.

The USA Patriot Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence-gathering purposes. It vests the secretary of the treasury with regulatory powers to combat corruption of U.S. financial institutions for foreign money-laundering purposes. The act also seeks to further close U.S. borders to known foreign terrorists and to detain and remove those within U.S. borders, and recognizes new crimes, new penalties, and new procedural efficiencies for use against domestic and international terrorists. Although it is not without safeguards, critics contend that some of its provisions go too far. Although the USA Patriot Act grants many of the enhancements sought by the Department of Justice, others are concerned that it does not go far enough.

Among the USA Patriot Act's most important and sweeping provisions, are measures that

- ✓ Allow for indefinite detention of noncitizens who are not terrorists on minor visa violations if they cannot be deported because they are stateless, their country of origin refuses to accept them, or because they would face torture in their country of origin.
- ✓ Minimize judicial supervision of federal telephone and Internet surveillance by law enforcement authorities.
- ✓ Expand the ability of the government to conduct secret searches.
- ✓ Give the attorney general and the secretary of state the power to designate domestic groups as terrorist organizations and deport any noncitizen who belongs to them.
- ✓ Grant the FBI broad access to sensitive business records about individuals without having to show evidence of a crime.
- ✓ Lead to large-scale investigations of American citizens for "intelligence" purposes.

The USA Patriot Act amended more than 15 federal statutes, including the laws governing computer fraud and abuse, criminal procedure, wiretapping, foreign intelligence, and immigration.

These amendments expanded the authority of the FBI and other federal law enforcement agencies to gain access to business, medical, educational, and library records, including stored electronic data and communications. It also expanded the laws governing wiretaps and trap-and-trace phone devices to Internet and electronic communications. These enhanced surveillance procedures are the ones that pose the greatest challenge to privacy and confidentiality of electronic data.

x-ref

For a summary of important changes made by the USA Patriot Act of 2001 that relate to computer crime and electronic evidence, see Appendix C.

Chapter Summary

Over the past decade, computers and the Internet have come to play an integral part in many of our citizens' lives. Each day, millions of people throughout the world log on to the Internet where they surf the Web, send and receive e-mail messages, or conduct e-commerce transactions and activities. Unfortunately, wrongdoers too have not let the computer revolution pass them by. When committing their crimes, an increasing number of criminals now capitalize on the use of high-tech devices, such as pagers, cellular phones, laptop computers, and the Internet. For instance, the Internet can be used to quickly distribute viruses or to launch Denial of Service (DoS) attacks against vulnerable computer networks. It is not uncommon for drug or arms dealers to use computers to keep a database of their illicit transactions.

According to the U.S. Department of Justice in a July 2002 bulletin, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, "The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers. Electronic records, such as computer network logs, e-mails, word-processing files, and '.jpg' picture files, increasingly provide the government with important (and sometimes essential) evidence in criminal cases. The purpose of this publication is to provide federal law enforcement agents and prosecutors with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations."

Key points covered in this chapter include

- ✓ The Fourth Amendment and its role in computer crime investigations
- ✓ Why the Freedom of Information Act serves as a deterrent to reporting computer crimes
- ✓ The advantages and disadvantages of informing and involving law enforcement in cybercrime investigations
- ✓ The benefits and legal aspects of information sharing
- ✓ The function of the National Infrastructure Protection Center in combating cyber crime
- ✓ The importance of federal computer crime laws and their significance in forensic examinations
- ✓ Understanding disclosure and discovery in computer crime investigations

Chapter 3

Forensic Preparation and Preliminary Response

In This Chapter

- ✓ Preparing operating systems for data collection
- ✓ Enabling auditing and logging
- ✓ Using time synchronization and time-stamping
- ✓ Identifying network devices
- ✓ Collecting data from memory
- ✓ Imaging hard drives
- ✓ Following the chain of custody for memory collection
- ✓ Business continuity and contingency planning

RESPONDING TO COMPUTER SECURITY INCIDENTS IS, BY AND LARGE, NOT AN EASY MATTER. Effective incident response requires a blend of technical knowledge, communication, responsibility, and coordination among all of an organization's response staff. There are several distinct stages of response when addressing a computer security incident: *preparation, identification, containment, eradication, recovery,* and *follow-up*. Understanding the importance of each stage is critical to carrying out an efficient response. All personnel in an organization's hierarchy need to understand the process of responding so that they can work together to handle any unexpected aspects of incidents they may encounter. This chapter focuses on forensic preparation and preliminary response and its role in mitigating the effects of computer security incidents.

Preparing Operating Systems for Data Collection

After the BIOS, the operating system (OS) is the first software program you encounter when you turn on your computer. It allows applications (programs) to communicate with the computer and each other at a basic level. Every general-purpose computer requires some type of operating system that tells the computer how to operate and how to utilize other software and/or hardware that is installed on that computer. There are essentially two types of operating systems; those geared toward the home user and those geared toward businesses or power users. This chapter discusses the more powerful networking operating systems.

The most commonly used operating systems can be divided into three families: the Microsoft Windows family of operating systems, the Unix/Linux family of operating systems, and the Apple Macintosh operating systems. Each of these families offers versions of operating systems that are specifically geared toward networking, making them widely used by organizations around the world. In fact, Unix/Linux operating systems, considered some of the most secure systems, are designed specifically for networking. The high learning curve required to configure and maintain Unix/Linux-based computers, however, has kept them from being widely adopted.

Under the Microsoft family, Windows NT 4.0, 2000, and XP are commonly used network operating systems employed by organizational networks. Because they are easy to set up and use, and have the largest base of applications written for them, they are one of the most popular and widely used operating systems around the world. The Apple Macintosh operating system (currently in version OS X) is a Unix-based network operating system with many powerful networking and security features. However, due to certain architectural differences inherent with Apple hardware, Mac OS–based computers have not attained the popularity of Windows operating systems. (Mac OS is, however, considered by many to be better suited for organizations that use graphic-intense programs such as CAD/CAM.)

While all contemporary operating systems provide some measure of security, it is the network operating systems that possess the greatest security capabilities. They allow network administrators to specify access privileges to individual files, directories, and hardware devices. Through their extensive use of auditing and log files, network operating systems have the added appeal of capturing and preserving potential forensic evidence.

The Significance of Log Files

Log files have traditionally been the principal source for documenting events that have happened or are happening in operating systems. The purpose of logging is to capture and preserve significant events. For example, logging is useful in a case where an incident takes place and the administrator wants some idea of what has transpired. Sources of evidence that investigators may have at hand on a computer system include system logs, audit logs, application logs, network management logs, network traffic capture, and data regarding the state of the file system. Logs are traditionally regarded as the primary record or indication of transpired activity. With the progression from stand-alone PCs to networked systems, network logs have joined system logs to help improve the recording of ongoing computer activity.

Auditing and Logging Procedures

In order to analyze the security of computer systems and detect signs of unexpected and/or suspicious behavior, it is essential to collect all data generated by application, system, network, and user activities. Log files contain a wealth of information about past activities. System administrators should identify the various logging mechanisms and types of logs (for example, file access, system, network, and so on) as well as the type of data recorded within each log.

Since log files are sometimes the only evidence of suspicious activity, failure to enable the mechanisms to record this information and failure to use them to initiate alert mechanisms significantly lessens an organization's ability to detect intrusion attempts and to determine whether the attempts have met with success. Similarly, problems can result from not having the required procedures and mechanisms in place to analyze the log files that *have* been recorded.

Logs can help organizations by

- Alerting system administrators of any suspicious activity
- Determining the extent of any damage caused by an intruder's activity
- Helping to quickly recover systems
- Providing information or serving as evidence required for legal proceedings

Enabling Auditing and Logging on Windows NT

All versions of Windows NT (for example, 4.0, 2000, and XP) contain powerful built-in auditing features that allow you to determine who is accessing files on your system. Auditing provides a number of benefits including help with troubleshooting file access rights and detecting which user last accessed a particular file.

Unlike Unix or Linux, auditing is disabled by default when Windows NT is first installed on a computer. This means that numerous system events and user activities will *not* be recorded in the event logs. From an incident response perspective, the absence of such log records makes it difficult to identify any attempts to breach the security of a computer system. These event log records can also assist system administrators by allowing them to distinguish between failures in hardware or software, network intrusions, and errors in the configuration of user accounts.

note

In all versions of Windows, to enable auditing, you first need to be logged on as an administrative user. Only administrative users are permitted to modify key security and/or system settings. The procedure varies depending upon the version of Windows being used. Consult your Windows user manual for details regarding administrative account privileges for the version of Windows you use.

To enable auditing/logging in Windows NT 4.0, do the following:

1. From the Start menu, select Programs → Administrative Tools → User Manager.
2. From the User Manager Policies menu, select Audit, which activates the Audit Policy dialog screen.

3. Now enable the Audit These Events option and then select the following audit events:
    - In the Failure column, select all of the events.
    - In the Success column, select the following events: Logon and Logoff, User and Group Management, Security Policy Changes, Restart, Shutdown, and System.
4. Select OK to accept the Audit Policy. Now all the selected options will be written to the event log.

Like its predecessor NT 4.0, Windows 2000 disables each audit policy category by default, so the security log remains empty on a newly installed operating system.

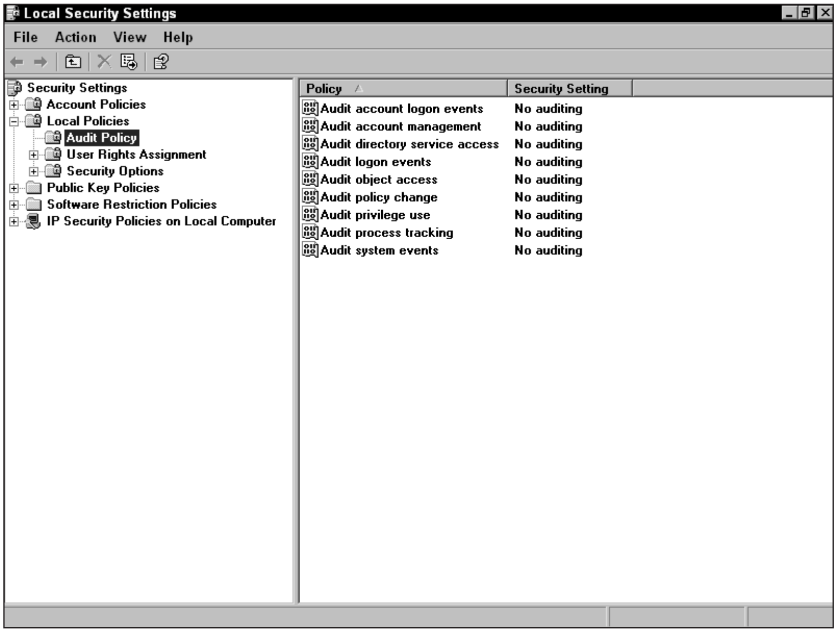
The general procedure to enable local auditing/logging in Windows 2000 is as follows:

1. Log on to Windows 2000 with an account that has full administrative rights.
2. From the Start menu, navigate to Administrative Tools → Local Security Policy. This opens the local security settings window.
3. In the left pane, double-click on Local Policies to expand it.
4. Now, double-click Audit Policy.
5. In the right pane, select the policy you wish to enable or disable by double-clicking it.
6. Select the desired Success and/or Fail check box.

The general procedure to enable local auditing/logging in Windows XP is as follows:

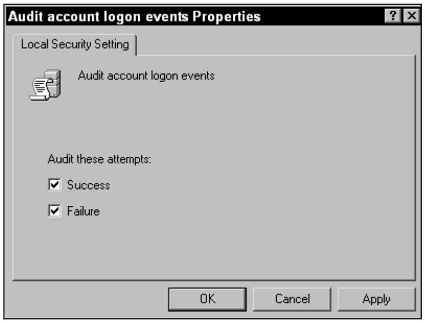
1. Log on as Administrator.
2. Click the Start button and select the Control Panel.
3. In the Control Panel, select Performance and Maintenance, then select Administrative Tools.
4. Double-click Local Security Policy shortcut to open and expand it.
5. In the left pane, select Audit Policy to display the individual policy settings, which will appear in the right pane. (See Figure 3-1.)
6. Double-click each setting in the right pane to enable auditing for each type of auditing desired. (See Figure 3-2.)

Remember, the most basic way to have intrusion detection in Windows is to enable auditing. This will alert you to changes in account policies, attempted password hacks, and unauthorized file access, as well as create log files that can later be used as evidence.



Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Figure 3-1: The Windows XP Pro Local Security Settings window



Audit account logon events

Audit these attempts:

☑ Success

☑ Failure

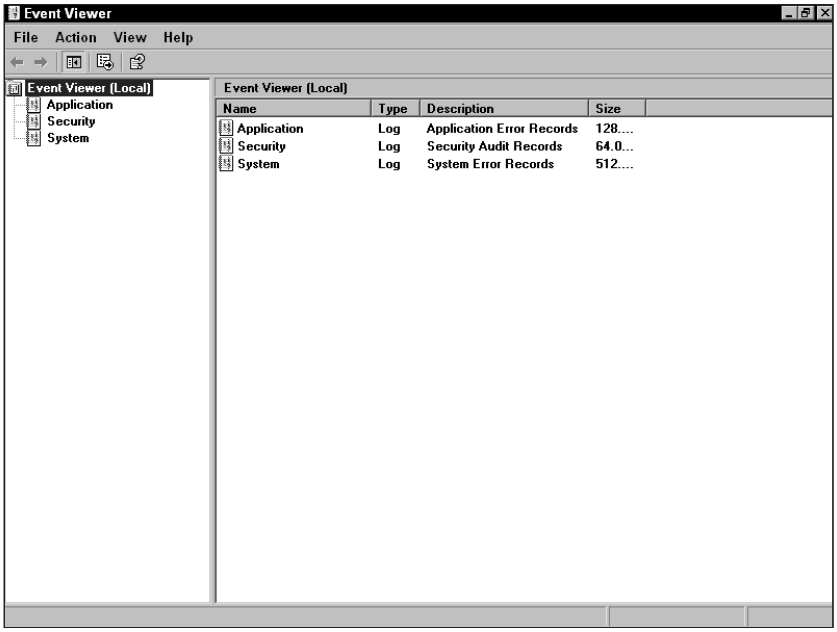
Figure 3-2: The Audit account logon events Properties dialog box in Windows XP Pro

A Quick Note about Auditing, Logging, and Log File Size

It is sometimes difficult to determine the exact amount of auditing and logging required. For instance, if a local hard drive (containing nonsensitive or public data) is accessed by many people over the course of a day then logging only the failed attempts might be sufficient. In fact, logging all attempts may possibly be disadvantageous because the resulting information could create so much activity in your log files that it would cause you to overlook important events. Conversely, if the data is classified and should only be accessed by a handful of users, you may want to track both failed attempts as well as successful ones.

Finally, because the default size of the Windows log file is only 512K, administrators with systems having moderate to high use may wish to increase the amount of data the log files may contain. While the exact procedure varies depending upon which version of Windows is being used, the general procedure is as follows:

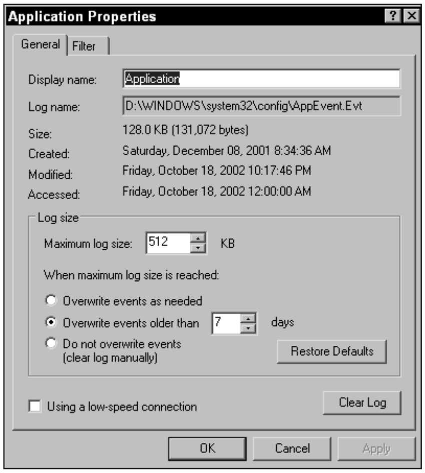
1. Click on Start → Control Panel → Performance and Maintenance.
2. Select Administrative Tools, then double-click on Event Viewer.
3. In the Event Viewer window, highlight the log that you wish to change (see Figure 3-3).
4. From the drop-down menu at the top, select Action → Properties.
5. In the Application Properties window, adjust the maximum log size accordingly by entering a new value in the "Maximum log size" field (see Figure 3-4).



Event Viewer (Local)

Name	Type	Description	Size
Application	Log	Application Error Records	128....
Security	Log	Security Audit Records	64.0...
System	Log	System Error Records	512....

Figure 3-3: The Windows XP Event Viewer



Display name: Application

Log name: D:\WINDOWS\system32\config\AppEvent.Evt

Size: 128.0 KB (131,072 bytes)

Created: Saturday, December 08, 2001 8:34:36 AM

Modified: Friday, October 18, 2002 10:17:46 PM

Accessed: Friday, October 18, 2002 12:00:00 AM

Log size

Maximum log size: 512 KB

When maximum log size is reached:

○ Overwrite events as needed

● Overwrite events older than 7 days

○ Do not overwrite events
(clear log manually)

□ Using a low-speed connection

Figure 3-4: The Windows XP Application Properties dialog box

Centralized Logging

Log files are usually the best source of information for determining if a system or network is experiencing a security compromise or other problem. With the proliferation of interoperable devices, it is not uncommon to find organizations using multiple computer network platforms such as Windows, Linux, or Novell NetWare. As a result, administrators often find it onerous to sift through the various operating system log files to gather evidence and look for the signs that indicate an incident has occurred. To make this process easier, centralized logging via the syslog protocol is often employed. Syslog support, which is included in Unix- and Linux-based systems, is an industry standard protocol used for capturing log information for devices on a network. Syslog is *not* included in Windows and Macintosh operating systems; however, there are third-party applications (covered later in this section) available to add this capability to your system.

The basic premise of centralized logging is to collect log data and send that data to a computer other than the one compromised. By doing this, the location of the log data is centralized and the integrity of that data remains protected. Centralized logging maintains a single centralized point of storage for log data, making it easier to back up, secure, and analyze. While a number of logging mechanisms exist for various computing platforms, the objective of a centralized logging mechanism is to support the most widely used and popular platforms. Cross-platform centralized logging software products from various vendors can be easily installed on an organization's network. The following two Windows-based centralized system-logging products are well suited to the task:

- ✓ **Kiwi Syslog Daemon** by Kiwi Enterprises is a freeware syslog daemon for the Windows platform. According to the manufacturer it receives, logs, displays, and forwards syslog messages received from hosts, such as routers, switches, Unix hosts, and any other syslog-enabled devices. Kiwi is online at `www.kiwisyslog.com`.
- ✓ **GFI LANguard Security Event Log Monitor** by GFI Software, Ltd. is a centralized security event log scanner that, according to its manufacturer, retrieves all event logs from servers and workstations and alerts the administrator of security breaches for immediate intrusion detection. By analyzing Windows NT/2000 event logs in real time, GFI LANguard Security Event Log Monitor can alert you to significant security events happening on your workstations and servers (for example, a user attempting to log on as an administrator, or a person being added to the administrator group). Because GFI LANguard analyzes the system event logs, rather than sniffing network traffic like traditional intrusion detection system (IDS) products do, it is not impaired by switches, IP traffic encryption, or high-speed data transfer. Find GFI at `www.gfi.com`.

Unfortunately, there will always be security flaws that can be exploited. While illegal entry and access to computer systems cannot always be completely prevented, such problems at least need to be recorded and tracked in an audit log for the purpose of revealing the security flaws in your systems and possibly identifying those (humans or computers) that have exploited these flaws. Information logging is of utmost importance in a properly secure setting. Logs by themselves, however, offer little if the files aren't being collected and reviewed.

tip

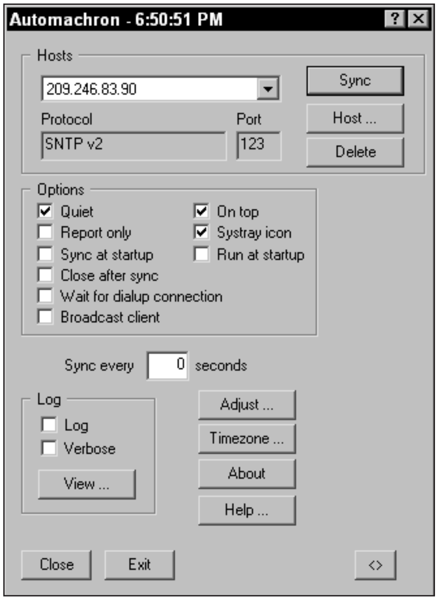
While file permissions protect log files from unprivileged alteration, you may also wish to protect log files from unauthorized alteration by having log files written to a CD-ROM or other read-only media.

Time Synchronization

While centralized logging can be beneficial for responding to security incidents, it also presents a unique problem. The more devices on the network, the more likely their times will not remain synchronized. This lack of synchronization may pose a difficulty for incident response. Automating the synchronization of system clocks saves substantial time during an incident response. Another benefit of synchronization is that the evidence is strengthened when the IDS and the host report the same event at the same time. If your organization conducts business across multiple time zones, use Greenwich Mean Time (GMT) to configure systems.

While a number of time synchronization mechanisms exist for various computer platforms, the objective of a centralized time-synchronization mechanism is to support the most platforms. For Internet protocol (IP)–based networks, Network Time Protocol is the one most commonly used. The Network Time Protocol (NTP) provides a mechanism to synchronize time on computers across the Internet. Unix, Linux, and most IP devices have built-in native support for the NTP protocol. While Windows does not, it can use NTP via such third-party freeware products as:

- ✓ **Automachron** by One Guy Coding, available at `www.oneguycoding.com/automachron/` (see Figure 3-5).
- ✓ The **NIST Internet Time Service** (ITS), available at `www.boulder.nist.gov/timefreq/service/its.htm`.
- ✓ **World Time** by PawPrint.net, available at `www.pawprint.net/wt/`.



Automachron - 6:50:51 PM

Hosts

209.246.83.90

Protocol: SNTP v2

Port: 123

Options

☑ Quiet
☐ Report only
☐ Sync at startup
☐ Close after sync
☐ Wait for dialup connection
☐ Broadcast client
☑ On top
☑ Systray icon
☐ Run at startup

Sync every 0 seconds

Log

☐ Log
☐ Verbose

Figure 3-5: Automachron time-synchronization program

note

In order to participate in the existing NTP synchronization network and obtain accurate, reliable time when using Unix or Linux, it is usually necessary to construct an appropriate configuration file, commonly known as ntp.conf. The exact syntax for this configuration file varies depending upon the timeserver with which you are trying to synchronize and the version of Unix/Linux you are using. Users are encouraged to consult with their Unix/Linux documentation for details.

Time-Stamping

One of the first things a hacker or network intruder will attempt is to modify their time of entry into a computer system. It is to the hacker's advantage to seek networks whose time clocks are not synchronized. In addition, by falsifying the date and time, a hacker can send a forensic investigator even further down a blind alley. There are two ways to avoid this problem:

- ✓ Be sure to synchronize the times of all network devices
- ✓ Ensure that the verification of time within your system cannot be distorted

Computer clocks are often comprised of low-cost oscillating circuits that can easily drift by several seconds per day. While this may not seem like a big deal, it can amount to several minutes over the course of a year. Synchronizing the times on all network devices adds a level of clock uniformity to all respective parts of the network. To prevent hacker attempts aimed at falsifying their entry time into a system, a network should employ a digital time-stamp that can be used at a later date to prove that an electronic document existed at the time stated on its time-stamp. To be reliable, the time-stamps must remain authentic, and the best way to ensure that a document has not been forged is to employ the services of a digital time-stamping service (DTS). While there are numerous companies that provide this type of service, two stand out as leaders in this emerging field.

- ✓ **Datum, Inc.** provides secure and auditable time-stamping technology for electronic transactions, time references for computer networks, and encryption engines for distribution and reception of confidential information. Find Datum online at `www.datum.com`.
- ✓ **Evertrust.net** markets and produces high-quality digital time-stamping solutions that help to protect the integrity of digital documentation. Look online at `www.evertrust.net`.

Identifying Network Devices

Organizations around the globe experience computer-security-related events (such as those caused by intrusions, attacks, and malicious code) on a regular basis. As a result, businesses find themselves scrambling to prevent attacks and intrusions wherever possible while monitoring and attempting to respond to critical security events. Part of the process of preliminary response to incidents is to quickly identify all network devices. This includes the auditing and mapping of computers, servers, hubs, switches, routers, and so on, as well as understanding their physical locations and configuration.

The network map is a graphical representation of the devices in a network. The network map is beneficial from an incident response standpoint because it helps to establish a baseline of your network for future comparison and helps you respond to security incidents by quickly locating any computers or devices subject to attack. Specifically a network map helps you to

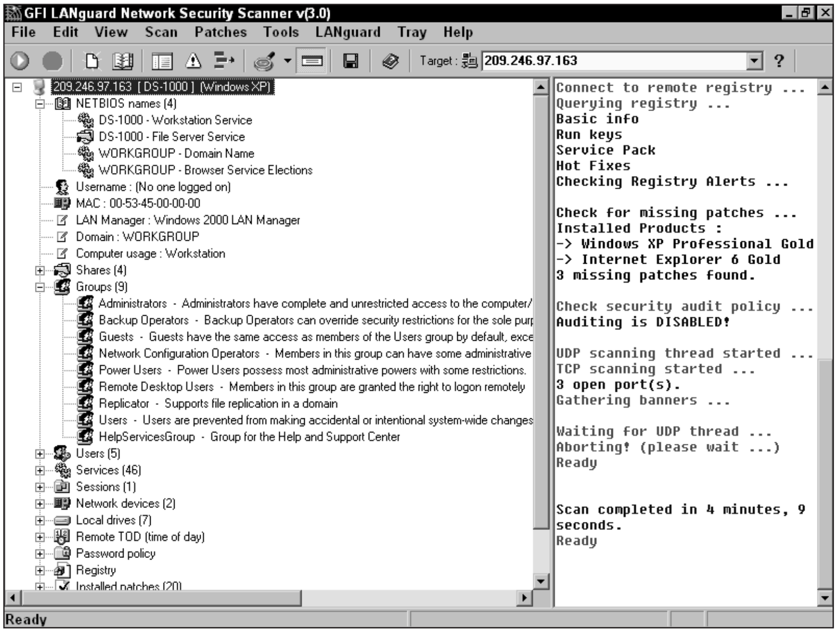
- ✓ Know exactly where each device is physically located
- ✓ Easily identify the users and applications that are affected by a problem
- ✓ Systematically search each part of your network for problems

In order to properly map your network you will need to know

- ✓ Which devices are on your network

- ✓ Which devices connect your network to the Internet
- ✓ How the devices are configured

During a computer security incident, the network map serves as both a reference and a blueprint. The map can be created by hand using any drawing or flow chart application. However, this can be both complicated and time-consuming. The better and preferred method is to use any one of the many software programs specifically designed for this task. One such program, the award-winning WhatsUP Gold by Ipswich, Inc. (`www.ipswitch.com`), is well suited to the task. Another program that can help in developing a network map is GFI LANguard Network Security Scanner (Figure 3-6) by GFI Software, Ltd. (`www.gfi.com`). Bear in mind that incident response is the process of successfully responding to an incident whether the objective is to just recover from the incident or to bring the perpetrators to prosecution. Having a network map can help an organization efficiently respond to computer security incidents by quickly providing information about the location and status of network devices.



```
209.246.97.163 [ DS-1000 ] (Windows XP)
  NETBIOS names (4)
    DS-1000 - Workstation Service
    DS-1000 - File Server Service
    WORKGROUP - Domain Name
    WORKGROUP - Browser Service Elections
  Username : (No one logged on)
  MAC : 00-53-45-00-00-00
  LAN Manager : Windows 2000 LAN Manager
  Domain : WORKGROUP
  Computer usage : Workstation
  Shares (4)
  Groups (9)
    Administrators - Administrators have complete and unrestricted access to the computer/
    Backup Operators - Backup Operators can override security restrictions for the sole purp
    Guests - Guests have the same access as members of the Users group by default, exce
    Network Configuration Operators - Members in this group can have some administrative
    Power Users - Power Users possess most administrative powers with some restrictions.
    Remote Desktop Users - Members in this group are granted the right to logon remotely
    Replicator - Supports file replication in a domain
    Users - Users are prevented from making accidental or intentional system-wide changes
    HelpServicesGroup - Group for the Help and Support Center
  Users (5)
  Services (46)
  Sessions (1)
  Network devices (2)
  Local drives (7)
  Remote TOD (time of day)
  Password policy
  Registry
  Installed patches (20)
```

```
Connect to remote registry ...
Querying registry ...
Basic info
Run keys
Service Pack
Hot Fixes
Checking Registry Alerts ...

Check for missing patches ...
Installed Products :
-> Windows XP Professional Gold
-> Internet Explorer 6 Gold
3 missing patches found.

Check security audit policy ...
Auditing is DISABLED!

UDP scanning thread started ...
TCP scanning started ...
3 open port(s).
Gathering banners ...

Waiting for UDP thread ...
Aborting! (please wait ...)
Ready


Scan completed in 4 minutes, 9
seconds.
Ready
```

Figure 3-6: GFI LANguard Network Security Scanner 3.0

Collecting Data from Memory

Computer memory comes in two forms, volatile and nonvolatile. Nonvolatile memory is mostly used in situations where the information stored needs to be maintained for extended periods of time. Examples of nonvolatile memory are the BIOS chips found on computer motherboards or the flash memory used by digital cameras. Since BIOS chips require special hardware to alter any information stored on them, it is unlikely that they will contain information related to a security incident. Thus, to a forensic investigator, preserving data stored on BIOS chips is not as important as preserving data stored in RAM.

Volatile memory presents a different position. Examples of volatile memory are the RAM (random access memory) chips used by all computers to load and store data generated by the operating system and applications. Any data stored on this type of memory is lost when the computer is powered off; with that lost data goes any potential evidence. Properly collected, data taken from volatile memory can be useful for apprehending an attacker and can yield useful, admissible evidence.

When collecting evidence you should proceed from the volatile to the less volatile. Here is a simple example of the order of volatility for a typical computer.

1. Memory
2. Temporary file systems
3. Disk
4. Physical configuration of the network

Memory is highest on the list because it is most volatile. Because evidence of an attack can easily slip away when memory is overwritten or deleted, one of the first steps to take is to perform a data dump. That is, the contents of the system memory should be printed or copied while it still resides in memory. When performed at the right time, this operation can capture and preserve potential evidence by documenting all the actions of any altered programming code that exists in memory. The information obtained from this process may also serve as evidence of how any malicious code operated on the system.

By default, Windows NT, like most networking operating systems, only generates a memory dump file upon a system crash. Fortunately, Windows 2000 and XP include a handy feature that allows you to manually cause the system to stop responding and to generate a memory dump file. It must first be configured to do so, however.

caution

Configuring Windows 2000 and XP to generate a memory dump file upon system crash requires you to edit the Windows Registry. An incorrect Registry entry may cause serious problems that may require you to reinstall your operating system. Use the Registry Editor carefully and with extreme caution. Before modifying the Registry, be sure to back it up. Furthermore, it is important that you understand the procedure for restoring the Registry in the event a problem does occur.

x-ref

Registry backup and restore procedures are covered in detail in Chapter 4.

To configure Windows 2000 to perform a manual memory dump, do the following:

1. Click on the Start button and select Run.
2. In the Open dialog box, type in the word **Regedit** to start the Registry Editor.
3. Expand the `HKEY_LOCAL_MACHINE` segment of the Registry to locate the following key:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters
   ```

4. On the Edit menu, click Add Value, and then add the following Registry values:

   ```
   Value Name: CrashOnCtrlScroll
   Data Type: REG_DWORD
   Value: 1
   ```

5. Close the Registry Editor.
6. Restart your computer for the changes to be applied.

After you restart the computer, you can generate a memory.dmp file on demand by simply holding down the right-Ctrl key and pressing the Scroll Lock key twice.

note

The preceding steps also work under Windows XP; however, the procedure for adding the `CrashOnCtrlScroll` Registry value is slightly different. At the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters` section, select Edit → New → DWORD Value. Name the value `CrashOnCtrlScroll`. Now double-click the newly created CrashOnCtrlScroll value to access the Edit DWORD value screen. Enter **1** in the value data space provided.

Selecting the Appropriate Memory Dump Options

Under the Windows operating system, there are three types of memory dumps that can be generated: complete memory dump, kernel memory dump, or small memory dump. For forensic examinations, it is best to choose the complete memory dump in order to capture the most information possible. Before manually triggering the dump, follow this general procedure:

1. Right-click My Computer, and then click Properties.
2. Click the Advanced tab, and then click the Startup and Recovery button.
3. Under Write Debugging Information, select the Complete Memory Dump option.

note

The location of the memory.dmp file varies slightly depending upon the location of the drive in which you have Windows installed and which version of Windows you are using. For Windows NT 4.0 and 2000, the default location is the directory `C:\WINNT`. For Windows XP the default directory is `C:\WINDOWS`. If you installed NT or XP in a directory other than `C`, you will need to substitute the appropriate drive letter for the location of your Windows directory such as `D:\WINNT` or `D:\WINDOWS`.

Using Dumpchk.exe to View the Windows memory.dmp File

The first thing you should do after creating a memory dump is verify that the integrity of the memory.dmp file is intact. Fortunately, Microsoft provides such a utility called Dumpchk, which is a command-line utility you can use to view the contents of a memory dump file and verify that it has been created correctly. Dumpchk can be found in the following locations:

- ✓ On the Windows NT 4.0 CD-ROM: `Support\Debug\<Platform>\Dumpchk.exe`.
- ✓ On the Windows 2000/XP CD-ROM: Install the Support Tools by running Setup.exe from the Support\Tools folder on the CD-ROM. By default, Dumpchk.exe is installed to the Program Files\Support Tools folder.

After locating the Dumpchk.exe on your Windows CD-ROM, copy the file to your default Windows directory (for example, `C:\WINNT` for NT and 2000, or `C:\WINDOWS` for XP). You can then run the Dumpchk utility directly from the command (DOS) prompt using the following syntax:

```
dumpchk.exe Memory.dmp
```

Performing Memory Dump on Unix Systems

Under Unix, the *sysdump* command is used to generate a system dump image of a live system's memory contents without disturbing normal functioning of the operating system. The system dump image is saved to a file for later analysis with the *crash* utility. Crash is an interactive Unix command used for examining a system image. Consult your Unix documentation for a complete list of crash commands.

To generate a system dump of a live system into the livedump file, type the following command:

```
/etc/sysdump –i /dev/mem –n /unix –o livedump
```

To use the crash utility to analyze the file, use this command:

```
/etc/crash –n livedump –d livedump
```

Once the memory dump file is created and its integrity verified, it needs to be properly preserved for future review by a computer forensic expert or legal authorities. Much of the information contained in a memory dump file is complex, requires an advanced knowledge of computer programming to understand, and is beyond the capability of the average computer user. However, the aforementioned procedures for collection can be quite beneficial when an organization wishes to capture and preserve memory-related computer evidence when performing a computer forensic investigation.

Remember the following when dealing with digital evidence obtained from a memory dump:

- ✓ All of the standard forensic and procedural principles must be applied.
- ✓ Upon seizing memory-related evidence, actions taken should not change that evidence.
- ✓ People who access original digital evidence should be trained for that purpose.
- ✓ All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- ✓ Individuals are responsible for all actions taken with respect to digital evidence while such evidence is in their possession.
- ✓ Any individual or group that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for complying with these principles.

With incident response and computer forensics, the safeguarding and protection of evidence is vital. A well-informed computer forensics professional should ensure that a subject computer system is carefully handled to ensure that

- ✓ No potential evidence is damaged, destroyed, or compromised in any way by the procedures used to investigate the computer.
- ✓ Extracted and possibly relevant evidence is properly handled and protected from later physical or magnetic damage.
- ✓ A continuing chain-of-custody is established and maintained.
- ✓ Business operations are affected for a limited amount of time, if at all.
- ✓ Any client-attorney information that is inadvertently acquired during a forensic exploration is ethically and legally respected and not divulged.

Imaging Hard Drives

The guiding tenet of computer forensics is to gather potential evidence that will be later analyzed and presented to a court of law to prove the presence of illegal activity. It is important when conducting a computer forensics examination that no alteration, damage, or corruption of data occurs. To perform a proper forensic analysis the first step is to collect computer evidence. Because there is some degree of volatility in the data stored on a hard drive, imaging is one of the first procedures to be carried out after the contents of the computer's memory have been copied and preserved.

As its name implies, hard-drive imaging provides a mirror image or a snapshot of the data contained on the hard drive. The snapshot is a perfect sector-by-sector copy of the drive, including all of the unused and partially overwritten spaces. The imaging process is nondestructive to the data and does not require the operating system to be turned on (booted). This ensures that the system is not altered in any way during the imaging process and thereby preserves its evidentiary value. Once an image is made, forensic examination is conducted using only the image (copy) and not the original hard drive.

The storage capacity of computer hard drives has grown exponentially over the past few years. As a result, hard drives are now capable of storing enormous amounts of data, making the process of imaging more complicated. The best approach for this task is to use a disk-imaging tool. The process of simply turning on the computer or utilizing a software utility like PowerQuest's Partition Magic to copy the original hard drive may potentially contaminate the evidence. The basic file-by-file copy does not capture all residual data (for example, deleted files, slack space, and swap files) necessary to perform a complete forensic analysis.

Choosing and using the right tool is imperative in a computer forensics investigation. According to the disk-imaging specifications published by the National Institute of Standards and Technology (NIST), the requirements of a top-level disk-imaging tool are as follows:

- ✓ The tool shall make a bit-stream duplicate or an image of an original disk or a disk partition on fixed or removable media.
- ✓ The tool shall not alter the original disk.
- ✓ The tool shall be able to access both IDE and SCSI disks.
- ✓ The tool shall be able to verify the integrity of a disk image file.
- ✓ The tool shall log input/output (I/O) errors.
- ✓ The tool's documentation shall be correct.

In addition, NIST mandates that the following requirements be met by all disk-imaging tools:

- ✓ The tool shall not alter the original.
- ✓ If there are no errors accessing the source media, then the tool shall create a bit-stream duplicate of the original.
- ✓ If there are I/O errors accessing the source media, then the tool shall create a qualified bit-stream duplicate. (A *qualified bit-stream duplicate* is defined to be a duplicate except in identified areas of the bit-stream.) The identified areas are replaced by values specified by the tool's documentation.
- ✓ The tool shall log I/O errors, including the type of error and location of the error.
- ✓ The tool shall be able to access disk drives through one or more of the following interfaces: direct access to the disk controller, Interrupt 13 BIOS interface, Interrupt 13 BIOS extended interface, ASPI SCSI interface, or Linux interface.
- ✓ Documentation shall be correct insofar as the mandatory and any implemented optional requirements are concerned. For example, if a user following the tool's documented procedures produces the expected result, then the documentation is deemed correct.

- ✓ The tool shall copy a source to a destination that is larger than or equal to the size of the source, and shall document the contents of the areas on the destination that are not part of the copy.
- ✓ The tool shall notify the user if the source is larger than the destination.

The following two disk-imaging tools are among the select few that currently meet the aforementioned stringent requirements as mandated by NIST:

- ✓ **Linux dd** is a freeware utility for any Linux system that can effectively image and copy every sector on all SCSI and IDE drives. This utility includes an MD5 mechanism, which can validate the data, and writes images to hard drive, tape, and any other removable media. Linux dd can be found at `www.redhat.com`.
- ✓ **SnapBack DatArrest**, by Columbia Data Products, Inc. (CDP), is a complete disk-imaging solution that is run from a single floppy disk. According to its manufacturer, it can acquire data at a rate of up to 300MB a minute, as well as back up DOS, Windows, Win95, WinNT, and Unix from the same disk, while providing a legal record of an exact "picture in time" of the computer's contents. It can even back up a self-destructive (booby-trapped) hard drive. Additional details and pricing can be found at `www.snapback.com`.

Following the Chain-of-Custody for Evidence Collection

Another vital concern when imaging a hard drive is to establish a chain-of-custody. The chain-of-custody tracks evidence from its original source to what is offered as evidence in court, demonstrating that the evidence collected is authentic. Chain-of-custody may be one of the most difficult issues faced by the forensic professional trying to introduce a digital image (of memory or a hard drive) as evidence in a criminal case. If a defendant alleges an image has been altered or could have been altered, the burden of proof falls upon the prosecution to prove otherwise. In many cases, the success of the argument hinges upon the procedures used to safeguard the security of the images.

For a proven chain-of-custody to occur

- ✓ The evidence is accounted for at all times.
- ✓ The passage of evidence from one party to the next is fully documented.
- ✓ The passage of evidence from one location to the next is fully documented.

The excerpt that follows, from the March 2001 *USA Bulletin* by Orin S. Kerr, Trial Attorney for the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, explains some of the important issues that can arise when the government seeks the admission of computer records under the Federal Rules of Evidence.

> **Computer Records and the Federal Rules of Evidence**
>
> Computer records can be altered easily, and opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. For example, in *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997), the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included detailed records of narcotics sales by three aliases: "Me" (Frost himself, presumably), "Gator" (the nickname of Frost's co-defendant Whitaker), and "Cruz" (the nickname of another dealer). After the government permitted Frost to help retrieve the evidence from his computer and declined to establish a formal chain of custody for the computer at trial, Whitaker argued that the files implicating him through his alias were not properly authenticated. Whitaker argued that "with a few rapid keystrokes, Frost could have easily added Whitaker's alias, 'Gator' to the printouts in order to finger Whitaker and to appear more helpful to the government." *Id.* at 602.
>
> The courts have responded with considerable skepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. *See Whitaker*, 127 F.3d at 602 (declining to disturb trial judge's ruling that computer records were admissible because allegation of tampering was "almost wild-eyed speculation . . . [without] evidence to support such a scenario"); *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); *United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."). *Id.* at 559. This is consistent with the rule used to establish the authenticity of other evidence such as narcotics. *See United States v. Allen*, 106 F.3d 695, 700 (6th Cir. 1997) ("Merely raising the possibility of tampering is insufficient to render evidence inadmissible."). Absent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility. *See Bonallo*, 858 F.2d at 1436.

The *USA Bulletin* further states, "The best evidence rule states that to prove the content of writing, recording, or photograph, the original writing, recording, or photograph is ordinarily required. See Fed. R. Evid. 1002. Agents and prosecutors occasionally express concern that a mere printout of a computer-stored electronic file may not be an 'original' for the purpose of the best evidence rule. After all, the original file is merely a collection of 0s and 1s. In contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes. Fortunately, the Federal Rules of Evidence have expressly addressed this concern. The Federal Rules state that [i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original."

The aforementioned bulletin refers to the Federal Rules of Evidence, which can be found at `www.cybercrime.gov` in the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. These rules govern the introduction of evidence in proceedings, both civil and criminal, in federal courts. While they do not apply to suits in state courts, the rules of many states have been closely modeled on these provisions. When it comes to chain-of-custody, authentication or identification is paramount. The standard for authenticating computer records is the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point been) in electronic form.

In summary, for digital images, the chain-of-custody should document the identity of the individuals who have had custody and control of the digital image file(s) from the point of capture to archiving. Once the file has been archived, the chain-of-custody should document the identity of the individuals who have custody and control of the archived image.

Business Continuity and Contingency Planning

Because nearly all organizations today rely on computers for the smooth operation of their daily functions, any event whether planned or unplanned, can bring business operations to a halt. If a disaster strikes and your company is unprepared, the consequences can be catastrophic and can range from prolonged system downtime to shutting down your business permanently. Planning insures your organization will be prepared to recover data and keep the business running after an IT-disabling disaster. The following is the National Institute of Standards and Technology IT contingency planning guide. While NIST publishes this guide for federal departments and agencies, organizations in the public and private sector will find it invaluable, as well.

The IT Contingency-Planning Process

To develop and maintain an effective IT contingency plan, organizations should use the following approach:

1. Develop the contingency-planning policy statement.
2. Conduct the business impact analysis (BIA).
3. Identify preventive controls.
4. Develop recovery strategies.
5. Develop an IT contingency plan.
6. Plan testing, training, and exercises.
7. Plan maintenance.

These steps represent key elements in a comprehensive IT contingency-planning capability. The responsibility for the planning process generally falls under the auspice of a position possibly titled contingency planning coordinator or contingency planner, who is typically a resource manager within the agency. The coordinator develops the strategy in cooperation with other resource managers associated with the system or the business processes supported by the system. The contingency planning coordinator also typically manages development and execution of the contingency plan. All major applications and general support systems should have a contingency plan.

1. DEVELOP THE CONTINGENCY-PLANNING POLICY STATEMENT

To be effective and ensure that personnel fully understand the agency's contingency-planning requirements, the contingency plan must be based on a clearly defined policy. The contingency-planning policy statement should define the agency's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning. To be successful, senior management, most likely the chief information officer (CIO), must support a contingency program. These officials should be included in the process to develop the program policy, structure, objectives, roles, and responsibilities. At a minimum, the contingency policy should comply with federal guidance contained in the documents listed in NIST SP 800-34; agencies should evaluate their respective IT systems, operations, and requirements to determine if additional contingency-planning requirements are necessary. Key policy elements are as follows:

- ✓ Roles and responsibilities
- ✓ Scope as applied to the type(s) of platform(s) and organization functions subject to contingency planning
- ✓ Resource requirements
- ✓ Training requirements
- ✓ Exercise and testing schedules
- ✓ Plan maintenance schedule
- ✓ Frequency of backups and storage of backup media

2. CONDUCT THE BUSINESS IMPACT ANALYSIS (BIA)

The BIA is a key step in the contingency-planning process, because it enables the contingency planning coordinator to fully characterize the system requirements, processes, and interdependencies as well as use this information to determine contingency requirements and priorities. The purpose of the BIA is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Key steps are listing critical IT resources, identifying disruption impacts and allowable outage times, and developing recovery priorities.

3. IDENTIFY PREVENTIVE CONTROLS

In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls. A variety of preventive controls is available, depending on system type and configuration; however, some common measures are listed here:

- ✓ Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls)
- ✓ Gasoline- or diesel-powered generators to provide long-term backup power
- ✓ Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor
- ✓ Fire suppression systems

- ✓ Fire and smoke detectors
- ✓ Water sensors in the computer room ceiling and floor
- ✓ Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- ✓ Heat-resistant and waterproof containers for backup media and vital nonelectronic records
- ✓ Emergency master system shutdown switch
- ✓ Offsite storage of backup media, nonelectronic records, and system documentation
- ✓ Technical security controls, such as cryptographic key management and least-privilege access controls
- ✓ Frequent, scheduled backups

4. DEVELOP RECOVERY STRATEGIES

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. Strategies should address disruption impacts and allowable outage times identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle.

The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system, and its operational requirements. Specific recovery methods may include commercial contracts with cold-, warm-, or hot-site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service-level agreements (SLAs) with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks (RAID), automatic failover, uninterruptible power supply (UPS), and mirrored systems should be considered when developing a system recovery strategy.

5. DEVELOP AN IT CONTINGENCY PLAN

IT contingency plan development is a critical step in the process of implementing a comprehensive contingency-planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan, the less scalable and versatile the approach. The information presented in NIST SP 800-34 is meant to be a guide; however, the plan format may be modified as needed to better meet the user's specific system, operational, and organization requirements.

In your approach, the contingency plan should comprise five main components: Supporting Information, Notification/Activation, Recovery, Reconstitution, and Plan Appendices. The first and last components provide essential information to ensure a comprehensive plan. The Notification/Activation, Recovery, and Reconstitution phases address specific actions that the organization should take following a system disruption or emergency.

- ✓ The Supporting Information component includes an introduction and concept-of-operations section that provides essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.
- ✓ The Notification/Activation phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification/Activation phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.
- ✓ The Recovery phase begins after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on contingency measures to execute temporary IT-processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery phase, the IT system will be operational and perform the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site. Teams with recovery responsibilities should understand and be able to perform these recovery strategies well enough that if the paper plan is unavailable during the initial stages of the event, they can still perform the necessary activities.
- ✓ In the Reconstitution phase, recovery activities are terminated, and normal operations are transferred back to the organization’s facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the contingency system should continue to operate. The Reconstitution phase should specify teams responsible for restoring or replacing both the site and the IT system.
- ✓ Contingency Plan Appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Appendices can include, but are not limited to contact information for contingency-planning team personnel; vendor contact information, including offsite storage and alternate site POCs; standard operating procedures and checklists for system recovery or processes; equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations; vendor agreements, reciprocal agreements with other organizations, and other vital records; description of, and directions to, the alternate site; and the BIA.

Plans should be formatted to provide quick and clear direction in the event those personnel unfamiliar with the plan or the systems are called on to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. Concise and well-formatted language reduces the likelihood of creating an overly complex or confusing plan.

6. PLAN TESTING, TRAINING, AND EXERCISES

Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each IT contingency plan element should be tested to confirm the effectiveness of individual recovery procedures and the overall plan. The following areas should be addressed in a contingency test:

- ✓ System recovery on an alternate platform from backup media
- ✓ Coordination among recovery teams
- ✓ Internal and external connectivity
- ✓ System performance using alternate equipment
- ✓ Restoration of normal operations
- ✓ Notification procedures

Training for personnel with contingency-plan responsibilities should complement testing. Training should be provided at least annually; new hires with plan responsibilities should receive training shortly after they are hired. Ultimately, contingency-plan personnel should be trained to the extent that that they are able to execute their respective recovery procedures without aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours after some disaster. Recovery personnel should be trained in the following plan elements:

- ✓ Purpose of the plan
- ✓ Cross-team coordination and communication
- ✓ Reporting procedures
- ✓ Security requirements
- ✓ Team-specific processes (Notification/Activation, Recovery, and Reconstitution phases)
- ✓ Individual responsibilities (Notification/Activation, Recovery, and Reconstitution phases)

7. PLAN MAINTENANCE

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change management process, to ensure new information is documented and contingency measures are revised if required. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews. Depending on the system type and criticality, it may be reasonable to evaluate plan contents and procedures more frequently.

Chapter Summary

Many organizations are not sufficiently prepared to deal with computer (or network) intrusions and are more likely to address the need to prepare and respond to incidents only *after* a breach has occurred. Even with sophisticated security and preventative measures in place, intrusions can — and do — happen. The best defense is a good offense. Organizations need a strategy — including preparation and plans for detection and response — to handling intrusions effectively. This chapter focuses on preparation, which includes selecting, installing, and becoming familiar with several tools and techniques that will assist you in the response process and help you collect and maintain data related to an intrusion.

Key points covered in this chapter include

- ✓ How to prepare operating systems to collect and preserve evidence via logging and auditing
- ✓ The benefits of time synchronization, time-stamping, and their role in strengthening an organization's incident response capability
- ✓ The importance of identifying and mapping network devices for incident response
- ✓ The procedures for collecting evidence from memory and the imaging of hard disks
- ✓ The importance of adhering to a chain-of-custody if any potential evidence is to be admissible in a court of law
- ✓ The criticality of business continuity planning in preparing for incident response

Chapter 4

Windows Registry, Recycle Bin, and Data Storage

In This Chapter

- ✓ An overview of the Windows Registry structure
- ✓ Collecting Registry data
- ✓ Registry editing and backup procedures
- ✓ Understanding Windows data storage
- ✓ The Windows File Allocation Table (FAT)
- ✓ Tracking and recovering deleted files through the Windows Recycle Bin
- ✓ Data storage using the Unix/Linux ext2 file system
- ✓ Recovering deleted files under ext2

WORLDWIDE, IT'S ESTIMATED THAT ABOUT 90 PERCENT OF PCS run one version or another of the Microsoft Windows operating system. In fact, the nearly ubiquitous nature of the Microsoft Windows operating systems was the focus of a much-publicized U.S. Department of Justice antitrust trial. With its user-friendly interface and widespread popularity, Windows continues to be the prime target for attacks by hackers and other intruders using malicious code. Recent studies indicate that unpatched and unprotected Windows-based computers that have been connected to the Internet are generally compromised in less than 72 hours.

Despite the use of powerful firewalls and sophisticated intrusion detection systems, even a protected system can become the victim of an attack. To be effective, today's incident response personnel must be trained in investigation techniques, incident response tactics, and the legal procedures for collecting evidence. One popular target for malicious intruders is the Windows Registry. Knowledgeable hackers can gain access to the Registry and manipulate user passwords, DNS settings, access rights, or other features that they may need in order to accomplish their objectives. To complicate matters more, the Windows Registry is large as well as dynamic, and the information in the Registry is diverse, making it difficult to monitor.

This chapter focuses on the roles the Windows Registry and data storage play in forensics investigation and incident response procedures. It provides incident handlers with the knowledge and tools needed to protect the Registry while successfully investigating and responding to computer incidents within their organizations.

The Windows Registry

The Windows Registry is a database where all the information about a computer is stored. The Registry is used to store

- ✓ Operating system configuration
- ✓ Application configuration information
- ✓ Hardware configuration information
- ✓ User security information
- ✓ Current user information

Everything from installed applications and Control Panel options to the colors displayed on the screen is stored in the Registry database. With Windows 9.x, the Registry is contained in two files (system.dat and user.dat) located in the Windows directory. Also located in the Windows directory are backup copies of the Registry called System.da0 and User.da0. With Windows NT/2000, the Registry files are referred to as *hives* and are stored in various directories within the NT operating system. Before the advent of Windows 95, Registry functions were performed by WIN.INI, SYSTEM.INI, and other .INI files that are associated with applications.

Registry Structure

The Registry has a hierarchal structure similar to the directory structure on the hard disk. Each main branch, denoted by a folder icon in the Registry Editor (a.k.a. REGEDIT, see Figure 4-1) is called a hive. Located within those hives are keys. Each key may contain other keys called subkeys along with their values. It is the values that contain the actual information that is stored within the Registry.

What follows is an overview of the six main Registry branches. Note that each branch contains a specific portion of the information stored in the Registry:

- ✓ `HKEY_CLASSES_ROOT`. This branch of the Registry contains file-association types, Object Linking and Embedding (OLE) information, and shortcut data. This key, along with the pointer to the `\Classes` subkey, provides backwards compatibility with Windows 3.X for OLE and DDE support.
- ✓ `HKEY_CURRENT_USER`. This branch points to the section of `HKEY_USERS` appropriate for the user currently logged into the PC.
- ✓ `HKEY_LOCAL_MACHINE`. This branch contains specific information about computer hardware, software, and other preferences for the local PC. This information is used for all users who log onto this computer.
- ✓ `HKEY_USERS`. This branch contains individual preferences for each user of the computer. Each user is represented by a security identifier (SID) subkey located under the main branch.

- ✓ HKEY_CURRENT_CONFIG. This branch links to HKEY_LOCAL_MACHINE\Config for machine-specific information.
- ✓ HKEY_DYN_DATA. This branch contains information that must be kept in RAM. Windows occasionally swaps information out to the hard drive, which updates system.dat or user.dat, but the information in HKEY_DYN_DATA remains in RAM. This branch does not appear in Windows XP or Windows 2000.

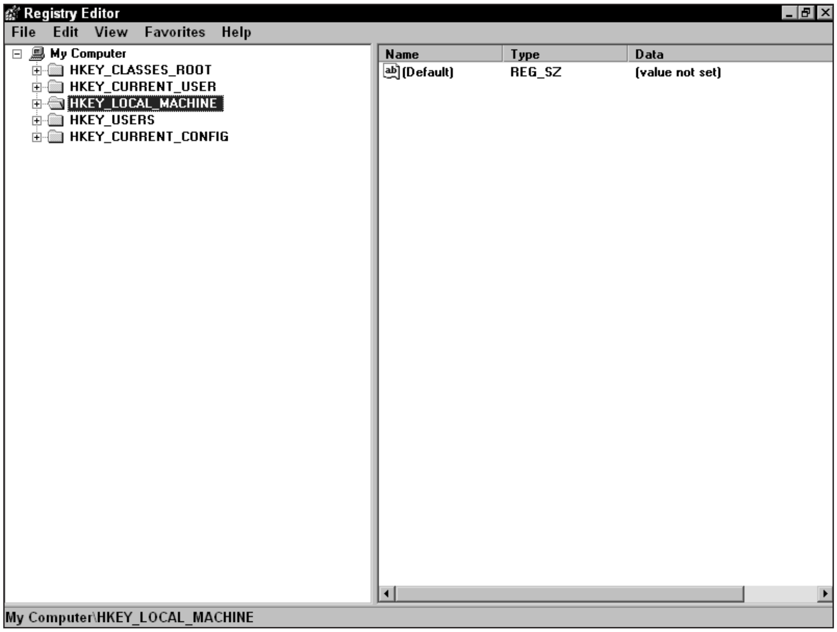
Within the Registry keys, there are five types of values. Following is a list of values along with a brief explanation of their functions:

- ✓ **String** or REG_SZ. This type is a standard string, used to represent human-readable text values.
- ✓ **Binary** or REG_BINARY. This type stores the value as raw binary data. Most hardware component information is stored as binary data and is displayed in the Registry Editor in hexadecimal format.
- ✓ **DWORD** or REG_DWORD. This type represents the data as a four-byte number and is commonly used for Boolean values, such as when 0 is disabled and 1 is enabled. Additionally, many parameters for device drivers and services are this type and can be displayed in binary, hexadecimal, and decimal format.
- ✓ **Multistring value** or REG_MULTI_SZ. This type is a multiple string used to represent values that contain lists or multiple values; each entry is separated by a NULL character.
- ✓ **Expandable string value** or REG_EXPAND_SZ. This type is an expandable data string, that is, a string containing a variable to be replaced when called by an application. For example, the string "%SystemRoot%" is replaced by the actual location of the directory containing the Windows NT system files.

Viewing and Editing the Registry

Before making any changes to the Registry, you should always back up the Registry first. Any mistakes or erroneous entries made when using the Registry Editor can cause Windows to behave erratically—or worse, you may find that Windows will not load at all. The Registry cannot be viewed or edited with a standard text editor. Because Registry data is stored in binary files, to view or edit the Registry, you must either use a program included with Windows called REGEDIT or a third-party program specifically designed for editing the Registry. Since REGEDIT is not listed on the Windows Start Menu, you must access it via a command (DOS) prompt or use the Run menu. To run this program, just click on Start, then Run, and then type **regedit** in the input field (see Figure 4-2) or type **regedit** at the command prompt when the Registry Editor starts. For more detailed information about editing the Registry, follow these steps while the Registry Editor is open:

1. At the top of the editor, select the Help menu, then Help Topics.
2. Select the Contents tab, then select Change Keys and Values.
3. Select the topic that you want.

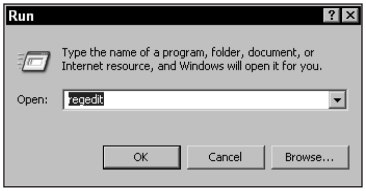


My Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Name	Type	Data
(Default)	REG_SZ	(value not set)

My Computer\HKEY_LOCAL_MACHINE

Figure 4-1: The Windows Registry Editor (REGEDIT)



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

Figure 4-2: Launching REGEDIT from the Windows Run dialog box

note

An alternative Registry Editor (REGEDT32.EXE) is available for use with Windows NT/2000. It includes some additional features not found in the standard version. Advanced features include the ability to view and modify security permissions, and the ability to create and modify the extended string values `REG_EXPAND_SZ & REG_MULTI_SZ`.

Collecting Registry Data

Many underground hacker Web sites emphasize the significance of the Windows Registry. Improper permissions or security settings can permit remote access to the Registry. Hackers can exploit this feature to compromise a system or to form the basis for adjusting file association and permissions to enable malicious code.

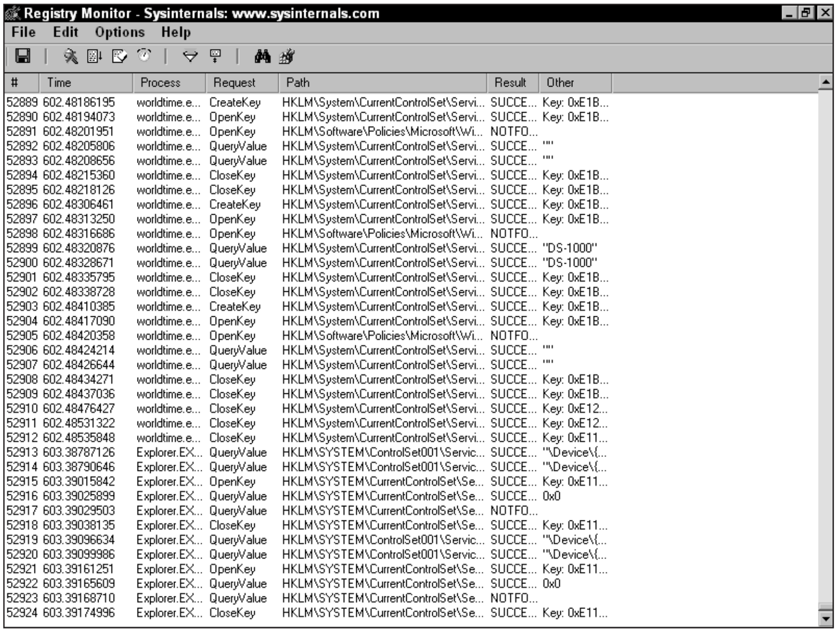
For example, a hacker might hide processes, files, and Registry keys. As described in Chapter 1, one simple method for loading an application at startup is to add an entry (key) to the following Registry hive:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run
```

While this is a common location for launching legitimate software applications, it can also be used by hackers or malicious coders to cause a dangerous application (like a Trojan horse or a keystroke logger) to be launched the next time the computer is started. While Registry data may be viewed through the built-in Windows Registry Editor (REGEDIT), most values in the Registry are read and updated only by the applications that use it.

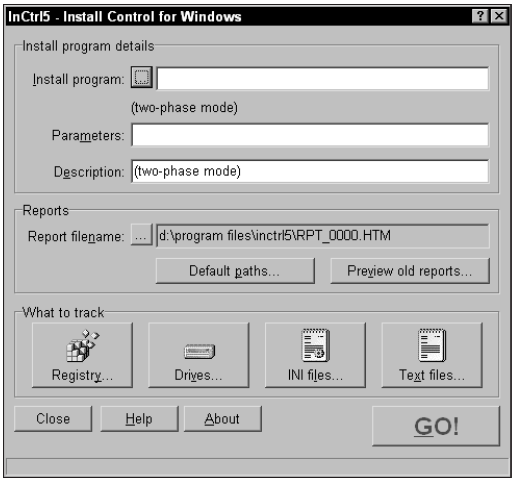
One of the first steps when gathering information on a compromised Windows computer is the collection of volatile data. Volatile data can be defined as active information temporarily reflecting the machine's current state. This includes the contents of registers, caches, physical and virtual memory as well as information about network connections, shares, running processes, disks, floppy disk drives, tape, CD/ROM, and printing activity. One useful tool for the collection of volatile Registry data is Regmon (see Figure 4-3), by Mark Russinovich and Bryce Cogswell. Regmon is a freeware utility that displays, captures, and logs all Registry activity in real time. Because it has the ability to monitor, capture, and log Registry activity, it is useful as both an incident-response and a forensic tool. For additional details or to download Regmon, visit www.sysinternals.com.

Another useful freeware tool for monitoring and logging changes to the Windows Registry is InCntrl5 (see Figure 4-4), written by Neil J. Rubenking. InCntrl5 monitors the changes made to Registry, drives, and .INI and text files of Windows-based computers. While it was primarily designed to track systemwide changes that occur when installing new software, it is also quite useful when conducting a forensic examination as it allows the examiner to compare changes made to a system both before and after a system compromise. InCntrl5 can be downloaded at www.extremetech.com.



```
#     Time          Process        Request     Path                                     Result     Other
52889 602.48186195  worldtime.e... CreateKey   HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52890 602.48194073  worldtime.e... OpenKey     HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52891 602.48201951  worldtime.e... OpenKey     HKLM\Software\Policies\Microsoft\Wi...  NOTFO...
52892 602.48205806  worldtime.e... QueryValue  HKLM\System\CurrentControlSet\Servi...  SUCCE...   ""
52893 602.48208656  worldtime.e... QueryValue  HKLM\System\CurrentControlSet\Servi...  SUCCE...   ""
52894 602.48215360  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52895 602.48218126  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52896 602.48306461  worldtime.e... CreateKey   HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52897 602.48313250  worldtime.e... OpenKey     HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52898 602.48316686  worldtime.e... OpenKey     HKLM\Software\Policies\Microsoft\Wi...  NOTFO...
52899 602.48320876  worldtime.e... QueryValue  HKLM\System\CurrentControlSet\Servi...  SUCCE...   "DS-1000"
52900 602.48328671  worldtime.e... QueryValue  HKLM\System\CurrentControlSet\Servi...  SUCCE...   "DS-1000"
52901 602.48335795  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52902 602.48338728  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52903 602.48410385  worldtime.e... CreateKey   HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52904 602.48417090  worldtime.e... OpenKey     HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52905 602.48420358  worldtime.e... OpenKey     HKLM\Software\Policies\Microsoft\Wi...  NOTFO...
52906 602.48424214  worldtime.e... QueryValue  HKLM\System\CurrentControlSet\Servi...  SUCCE...   ""
52907 602.48426644  worldtime.e... QueryValue  HKLM\System\CurrentControlSet\Servi...  SUCCE...   ""
52908 602.48434271  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52909 602.48437036  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE1B...
52910 602.48476427  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE12...
52911 602.48531322  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE12...
52912 602.48535848  worldtime.e... CloseKey    HKLM\System\CurrentControlSet\Servi...  SUCCE...   Key: 0xE11...
52913 603.38787126  Explorer.EX... QueryValue  HKLM\SYSTEM\ControlSet001\Servic...    SUCCE...   "\Device\{...
52914 603.38790646  Explorer.EX... QueryValue  HKLM\SYSTEM\ControlSet001\Servic...    SUCCE...   "\Device\{...
52915 603.39015842  Explorer.EX... OpenKey     HKLM\SYSTEM\CurrentControlSet\Se...     SUCCE...   Key: 0xE11...
52916 603.39025899  Explorer.EX... QueryValue  HKLM\SYSTEM\CurrentControlSet\Se...     SUCCE...   0x0
52917 603.39029503  Explorer.EX... QueryValue  HKLM\SYSTEM\CurrentControlSet\Se...     NOTFO...
52918 603.39038135  Explorer.EX... CloseKey    HKLM\SYSTEM\CurrentControlSet\Se...     SUCCE...   Key: 0xE11...
52919 603.39096634  Explorer.EX... QueryValue  HKLM\SYSTEM\ControlSet001\Servic...    SUCCE...   "\Device\{...
52920 603.39099986  Explorer.EX... QueryValue  HKLM\SYSTEM\ControlSet001\Servic...    SUCCE...   "\Device\{...
52921 603.39161251  Explorer.EX... OpenKey     HKLM\SYSTEM\CurrentControlSet\Se...     SUCCE...   Key: 0xE11...
52922 603.39165609  Explorer.EX... QueryValue  HKLM\SYSTEM\CurrentControlSet\Se...     SUCCE...   0x0
52923 603.39168710  Explorer.EX... QueryValue  HKLM\SYSTEM\CurrentControlSet\Se...     NOTFO...
52924 603.39174996  Explorer.EX... CloseKey    HKLM\SYSTEM\CurrentControlSet\Se...     SUCCE...   Key: 0xE11...
```

Figure 4-3: The Regmon utility



Install program:
(two-phase mode)
Parameters:
Description: (two-phase mode)

Report filename: d:\program files\inctrl5\RPT_0000.HTM

Figure 4-4: The InCntrl5 Utility

Registry Backup and Restore Procedures

The Registry is a critical operating system component. When it is corrupted, Windows does not load properly. Without it, Windows does not load at all. When a system has suffered a compromise, a backup of the Registry plays an important role in incident response. It is mandatory that appropriate precautions be taken to safeguard the essential data that is required for recovery in the event of any damage to a Windows system, especially its Registry. In addition, since hackers and malicious coders often target the Registry, a backup copy of an unadulterated Registry can be used as a baseline for comparison when conducting a forensic examination of an affected computer. The concept of backing up files is often disregarded and/or poorly understood among organizational computer users. Unfortunately, the consequences of not properly backing up files can put an organization out of business. The following are general backup procedures for Windows NT 4.0, 2000, and XP.

WINDOWS NT 4.0

Under Windows NT 4.0 there are two methods that that can be used in order to back up and restore the entire Registry. The first (and preferred) method is to use the built-in Windows NT Backup tool (Ntbackup.exe) and use the option to either back up or restore the Registry. This program, which is part of Windows NT 4.0, can be invoked by simply typing `ntbackup` in the Run command box in the Windows Start menu or at the command prompt. Bear in mind that to employ this method you need a functioning tape, Zip, or CD-RW drive to receive the backup.

The second backup method is to use RDISK with the `rdisk /s` command. Windows NT contains an RDISK utility that is used to extract essential data (from the Registry of a Windows NT system) required for recovery in the event that the Registry has become damaged. When used with the `/s` option, RDISK aids in recovery of user accounts, groups, policies, and access controls by extracting Security Account Manager (SAM) information. After using this procedure, the extracted data is initially written to files in a directory named repair, usually located in the `C:\WINNT\` directory.

note

The RDISK utility is not intended for making a complete backup of a Windows NT 4.0 Registry. The RDISK data files are only intended to contain the essential information needed for quick recovery, not the entire contents of the Registry. To perform a complete backup of the Windows NT 4.0 Registry, a more comprehensive utility tool (like Ntbackup.exe) or a third-party utility specifically designed for Registry backup should be used.

WINDOWS 2000

In order to make a backup of the entire Registry under Windows 2000, it is necessary to use the Windows 2000 Backup utility. While the backup utility is often used to create an Emergency Repair Disk (ERD), it can also be used to back up and restore the System State, which includes the Registry, the COM+ Class Registration database, and other critical files required for booting the computer.

The procedure for backing up the System State on a Windows 2000 computer is as follows:

1. Click Start, and then select Programs.
2. Navigate to Accessories, then System Tools.
3. Under System Tools, select the Backup program.
4. Under the Backup program, select (click on) the Backup tab.

Select the System State check box. (All of the components to be backed up are listed in the right pane. You cannot individually select each item.)

note

During the System State backup, you must select to back up the Winnt\Sysvol folder. This option is also required during the restoration process in order to have a working system volume (sysvol) after the recovery.

The procedure for restoring the System State from a backup on a Windows 2000 computer is as follows:

1. Click Start, and then select Programs.
2. Navigate to Accessories, then choose System Tools.
3. Under system tools, select the Backup program.
4. Under the Backup program, select the Restore tab.
5. From the Restore tab, select the appropriate backup media and System State to restore.

note

As with the System State backup procedure, during the restore operation, the Winnt\Sysvol folder must also be selected to be restored in order to have a working sysvol after the recovery process. Be sure that the advanced option to restore "junction points and data" is also selected prior to the restoration. This ensures that sysvol junction points are re-created.

6. In the Restore Files to box, select Original Location.
7. Click Start Restore.
8. After the restoration process is complete, restart the computer.

If you wish to restore the System State on a compromised or damaged system, it is best to perform the aforementioned steps while the computer is operating in Safe Mode. In order to start the computer in Safe Mode, follow these steps:

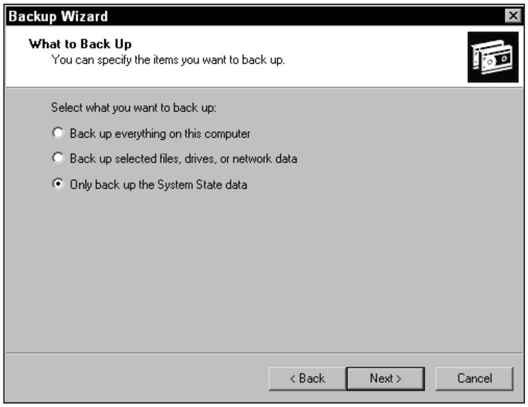
1. Power on the computer, and press the F8 key as soon as you see the Windows 2000 Boot menu.
2. Using the arrow keys on the keyboard, highlight the appropriate Safe Mode option, and then press Enter.
3. Windows will now boot up in Safe Mode.

WINDOWS XP

Like Windows 2000, to back up the System State (Registry, the COM+ Class Registration database, and critical boot files) under Windows XP, you need to employ the Backup utility.

The procedure for backing up the System State on a Windows XP computer is as follows:

1. Click Start, and then select All Programs.
2. Navigate to Accessories, then System Tools.
3. Under System Tools, select the Backup program.
4. By default, the Backup and Restore Wizard screen appears.
5. Select Advanced Mode, and then click the Backup Wizard Advanced button.
6. The Backup Wizard screen appears. Select Next.
7. In the What to Back Up panel, select the "Only back up the System State data" option (see Figure 4-5), and then select Next to choose the name and location for the backup files.
8. Click on Finish to complete the process.



Backup Wizard

What to Back Up

You can specify the items you want to back up.

Select what you want to back up:

○ Back up everything on this computer

○ Back up selected files, drives, or network data

● Only back up the System State data

Figure 4-5: The Windows XP Backup Wizard

The procedure for restoring the System State from a backup on a Windows XP computer is as follows:

1. Click Start, and then select All Programs.
2. Navigate to Accessories, then System Tools.
3. Under System Tools, select the Backup program.
4. By default, the Backup and Restore Wizard screen appears.
5. Select Advanced Mode, and then click the Restore Wizard Advanced button.

6. At the Welcome to Restore Wizard Screen, select Next.
7. Select the backup file you wish to restore, then select Restore to finish the process.

Registry Backup Programs (Shareware and Freeware)

The process of backing up the Registry varies among Windows versions. Rather than list them all, users interested in learning how to manually back up under their particular Windows version can find detailed instructions at `http://support.microsoft.com`.

Later versions of Windows have a built-in Restore utility that takes periodic snapshots of the Registry and other critical files and saves them in a special location. This allows users to roll back the OS configuration to a working copy in the event the Registry becomes corrupted or altered by malicious code. Fortunately, there are dozens of freeware and shareware utilities that can easily perform Registry backup and restoration with only a few mouse clicks. For those who are interested, the following are three Web sites that contain Registry backup and restoration freeware and shareware programs along with numerous other utilities:

- ✓ `http://freeware.intrastar.net/registry.htm`
- ✓ `www.webattack.com`
- ✓ `www.davecentral.com`

Understanding Data Storage

To understand forensic data recovery, it is important to first appreciate how and where data is stored. Nearly every desktop computer and server in use today contains one or more hard-disk drives. Unlike floppy disks and Zip disks, which contain a thin flexible plastic film to store data, hard-disk drives have a specially coated hard platter that stores the magnetic digital data. This is quite different from CD-ROM (for example, CD-R and CD-RW) discs, which store digital data as microscopic reflective and nonreflective spots along grooves on the disk.

The Hard Disk

The hard disk is one of the most important components of the modern day computer. The hard-disk drive holds the vast majority of the data stored in a computer. From an incident response standpoint, the hard drive must be protected because of the value of the data contained within it. From a forensic standpoint, the hard disk, because of the log files and data-storage nooks and crannies, can be a valuable source of potential evidence.

At one time, hard-disk drives were called Winchester drives. This term dates back to the early 1960s when IBM developed a high-speed hard-disk drive that had 30MB of fixed-platter storage and 30MB of removable-platter storage. The drive, called the 30-30, soon earned the moniker Winchester after the famous Winchester 30-30 rifle. The nickname Winchester had no technical value, it was simply so widely used that all high-speed hard drives were soon referred to as “Winchester” drives.

Hard disks store data on one or more metal oxide platters, each with two sides upon which data can be stored. The hard-disk platters are made of glass or aluminum. A typical hard drive contains several of these 3.5-inch platters, which can contain tens of billions of individual bits of data. Areal density has been the primary growth rate indicator for hard-drive capacity. The higher the areal density of a hard disk's platters, the more data bits that can be packed into each square inch of platter real estate. These platters, which spin at a rate of between 3,600 and 10,000 revolutions per minute, hold the magnetic charges that make up the data stored on the disks. A hard disk drive has one read/write head per platter, which is attached to an actuator arm. This head actually floats on a cushion of air generated by the rapidly spinning platters. The distance that the heads float is only about 1 to 2 micro-inches (one millionth of an inch) above the surface of the platters. Because of these extreme tolerances, the disk drive is sealed to prevent any dirt or dust from entering the drive.

All information contained on a hard-disk drive is stored in tracks, which are concentric circles placed on the surface of each platter, much like the annual rings of a tree. Since a hard-disk track would be too large for an operating system to manage as a continuous single unit, multiple tracks are used. The tracks are numbered, starting from zero, and they begin at the outside of the platter and increase (0, 1, 2, 3, and so on) toward the center. A modern hard disk has tens of thousands of tracks on each platter. Each track can hold many thousands of bytes of data. Even with multiple tracks, data storage still requires a tremendous amount of operating system resources to read and write data. It would be inefficient to make a track the smallest unit of storage on the disk, since this would mean small files would also occupy a large amount of disk space. Obviously having a small file occupy a large area of disk space is wasteful, and for that reason, disk tracks are further divided into even smaller numbered divisions known as sectors. Sectors are the basic unit of data storage on a hard disk.

The Floppy Disk

The floppy-disk drive was invented in 1967 by Alan Shugart while he was working as an engineer at IBM. It was one of Shugart's senior engineers, David Noble, who actually first proposed the concept of a flexible media disk protected by a plastic jacket with a fabric lining. This concept became a reality when the first floppy disk was created. Shugart left IBM in 1969 to work for Memorex and then later left Memorex in 1973 to form his own company, Shugart Associates, which designed and developed floppy-disk drives. The floppy-disk interface developed by his company was the basis for the floppy-disk drives still in use today. The first floppies were 8 inches in diameter and somewhat cumbersome.

By the mid-1970s advancements in technology permitted engineers to create a smaller 5.25-inch floppy disk with an initial capacity of 360K. By the mid-1980s floppy disks reached their current size of 3.5 inches; however, they only had an initial capacity of 720K. By the mid-1990s the standard 3.5-inch floppy disk reached its zenith at 2.88MB. As data storage requirements continued to grow, the capacity of the floppy disk followed suit. While the physical disk size has not changed much, the amount of data that a floppy disk can store has increased dramatically. Modern day super floppy disks like the LS-120 and the Iomega Zip Disk can now hold millions of bytes of data in the same size 3.5-inch diameter disk of the original floppy.

The inside of a standard floppy drive has many similarities to the inside of a hard drive. The majority of floppy drives have two read/write heads, meaning they are double-sided. One head is used to read and write data to the diskette while the other is used to erase a track before any data is written by the other head. As with a hard drive, the head mechanism is moved by an actuator. Using a design similar to that of early hard drives, a motor moves the heads in and out, giving them the ability to position themselves over any track on the disk to store and retrieve data.

The benefit of floppy disks is that they are portable, making it easy to transfer data from one computer to another. The drawback of floppy disks is that they are not a reliable medium for storing important files since dust, scratches, moisture, and magnetic fields can easily damage them.

From an incident response and forensic standpoint, the floppy disk plays an important role. One should never allow a suspect computer to boot from its hard drive or use its operating system to perform investigative tasks. Many times evidence is erased or altered during the normal boot process. In addition, you do not know what type of cleanup procedures are waiting in the boot process. When conducting a forensic investigation you should always boot from a floppy disk. Keep in mind that the computer's BIOS may first need to be modified via the BIOS setup program to allow the computer to boot from a floppy disk. This exact procedure varies depending upon the type of BIOS that was used in the manufacture of the computer's chipset. Once you are sure you can boot from the floppy drive, the hard drive can be examined.

tip

The BIOS setup program can normally be entered only during the boot process; however, some BIOSes permit entry into their setup program using a key combination at any time. One recent universal standard has begun to emerge; the use of the Del key to enter the setup program during the boot process. This appears to hold true for the two most popular BIOSes, AMI and Award, as well as several others. Older BIOSes can use a multitude of strange key combinations, including but not limited to: Esc, F1, F2, F10, Ctrl+Esc, Alt+Esc, Ctrl+Alt+Esc, Ctrl+Alt+Enter, Ins, and several others.

The CD-ROM

Compact Disc-Read Only Memory, better known as a CD-ROM, is a type of optical disc capable of storing enormous amounts of data. While the most common size for such discs is around 650 to 700MB, newer high-capacity CD-ROMs are capable of storing even more than that. A 700MB single CD-ROM has the storage capacity of around 700 floppy disks, enough storage to hold roughly 300,000 text pages. In 1978 Phillips and Sony Corporation joined forces in an endeavor to produce the current audio CD. Sony pushed for a 12-inch disc while Phillips wanted a smaller, more portable disc. With the details eventually ironed out, the current standard 4.72-inch (120mm) disc was announced in 1982. Legend has it that this size was chosen because it could contain Beethoven's Ninth Symphony in its entirety.

Since its introduction by Sony and Philips, the compact disc has had a remarkable impact on how people listen to music. CD-ROMs have affected how we watch movies, share photographs, and read books. The advantages of CDs include their small size, large data capacity, low manufacturing cost, and physical robustness. With the continued cooperation of Sony and Phillips, additional specifications were announced in the late 1980s that led to the use of the CD-ROM for the storage of computer data.

CD TECHNOLOGY

While identical in size and appearance to audio CDs, computer CDs are designed to store computer data in addition to audio data. CD-ROMs are made of a thin metallic film of aluminum alloy surrounded by polycarbonate. The metallic film is the part of the CD where the digital information is stored. The clear polycarbonate shell simply protects the film and provides rigidity to the disc. These CDs are single sided; all of the reading is done from the underside of the CD and a label is usually placed on the top.

Information stored on the metallic film of the CD can be read only by reflecting a low-power laser off the aluminum film. A special light receptor in the CD-ROM drive notes where light is reflected and where light is absent. The absence of reflected light is caused by small *pits* etched into the surface of the aluminum strata. Individual pits are only .12 microns (millionths of an inch) deep and are etched into the spiral track that traverses from the outside edge of the disc to its center (similar to old-style vinyl analog records). The absence of pits (the surface or high points) is referred to as *lands*. A low-power laser reads the pits and lands, which are converted by the CD-ROM drive into binary code (0s and 1s). This binary (native) computer code is the actual data used by the computer. Standard CD-ROM discs are read-only and cannot be altered or erased. This changed with the advent of CD-R and CD-RW formats.

CD-R AND CD-RW

CD-R is the abbreviation for CD-Recordable. Recordable CDs are also known as WORM (Write Once, Read Multiple) media, and they work in a fashion similar to a standard CD. The advantage of CD-R over other types of optical media is that data can be read from these discs with a standard CD player. The disadvantage is that discs can’t be reused once data has been written to them. A related technology called CD-Rewritable (CD-RW) allows you to erase discs and reuse them, but the CD-RW media doesn’t work in all CD players, particularly older ones. CD-Rewritable drives are able to write both CD-R and CD-RW discs.

One of the primary applications for CD-Recordable discs is archiving. By placing critical system information such as Registry backups or System State on a CD-R, you are ensuring that the material contained on the discs is authentic. When conducting a forensic investigation, CD-R discs are useful for the sheer volume of data they can hold and also because once data is written to them it cannot be altered or erased, helping preserve the chain-of-custody.

The Windows File Allocation Table

The File Allocation Table (FAT) tells the Windows operating system which sectors are used for certain files. In layman’s terms, the FAT is a table of contents that the operating system uses to locate files on a disk. Files change in size and end up being larger or smaller after data has been added or removed. When this happens, the data may not fit back in the exact same site on the hard drive. The too-large data is then broken up into chunks, and pieces are stored in various places around the hard drive. This redistribution is called fragmentation. The job of the FAT is to keep track of all files on the hard disk including these fragments. If the File Allocation Table is damaged or lost, then a disk is unreadable by the operating system. In file servers, the FAT data is sometimes kept in the computer RAM for quick access and is easily lost if the system crashes (as the result of a power failure, for example).

Today, FAT comes in three different versions:

- ✓ **FAT12.** The oldest and original type of FAT, it uses a 12-bit binary number to hold the cluster number. FAT12 can only be used on storage volumes of 16MB or less. It is therefore most suitable for very small volumes and is used on floppy disks and hard-disk partitions smaller than about 16MB. (The latter being rare today.)
- ✓ **FAT16.** Using a 16-bit binary number to hold cluster numbers, FAT16 is used by older systems and for small partitions on modern systems. A hard disk using FAT16 can only hold a maximum of 65,526 clusters. FAT16 is used for hard-disk volumes ranging in size from 16MB up to 2GB (two billion bytes). The Virtual File Allocation Table (VFAT) system, used by Windows 95 and later, is a variant of FAT16 that allows the operating system to circumvent the old 8.3 file-name limitation (for example, autoexec.bat where an eight-letter file name is followed by the DOS three-character extension) that plagued DOS and permits the use of file names up to 255 characters long.
- ✓ **FAT32.** The most recent version of FAT, FAT32 is supported by newer versions of Windows beginning with the Windows 95 SR2 release. FAT32 actually uses a 28-bit, not a 32-bit, binary cluster number. This is because the commonly used ATA hard-drive interface that accesses the data on a hard drive is limited to 28-bit addressing. However, 28 bits is still enough to permit enormous hard-disk volumes of up to 2TB (two trillion bytes) in size. In addition, FAT32 uses space more efficiently. FAT32 uses smaller clusters (for example, 4K clusters for drives up to 8GB in size), resulting in 10 to 15 percent more efficient use of disk space relative to large FAT drives.

The number of data bits used by the FAT file system is what gives it its name. Another important feature of the FAT file system is that FAT disks usually contain two copies of FAT (the second copy of FAT immediately follows the first one). In both FAT12 and FAT16 systems, all copies of FAT are kept in sync with each other, but only the first copy is ever read. Microsoft claims that the next copies of FAT are used when the first one is physically unusable, but this does not appear true for all versions of their operating systems. In FAT32 there exists a field in the BPB (BIOS Parameter Block) that tells the operating system which copy to use and whether to synchronize all copies. The BPB stores a lot of information about the volume itself, like its size, the number of bytes per sector, the number of sectors per cluster, and several other items of information. In summary, FAT32 uses the BPB to know how to deal with a FAT volume.

The Windows New Technology File System

With the advent of Windows NT, Microsoft replaced the aging FAT file system with a faster, more secure and robust way to provide disk and file access: the New Technology File System (NTFS). While Windows NT can use the older-style FAT file system, the NT file system provides a combination of performance, reliability, and compatibility not found in the FAT file system. It is designed to quickly and efficiently perform normal file operations such as read, write, and search. For very large applications, NTFS supports volume spanning. Volume spanning means that files and directories can be distributed across several physical hard-disk drives. One of the benefits of an NTFS is that it works on hard disks of any size. While there is a maximum physical size limit of the NT file system, that number is so large that it will be decades before hard-drive technology exceeds its capability.

At the heart of NTFS is the Master File Table or MFT. The MFT is analogous to the FAT file system's File Allocation Table because the MFT maps all the files and directories on the drive. The MFT is divided into discrete units known as records. In one or more MFT records, NTFS stores the *metadata*. The metadata is data that describes a file or directory's characteristics (security settings and other attributes such as read-only or hidden) and its location on the disk.

The Windows Recycle Bin

With the advent of Windows 95, Microsoft introduced to their operating system users the ability to place deleted files in a Recycle Bin for storage. The purpose of the Recycle Bin was to provide computer users with the ability to reclaim — at a later time — files that had been placed there. Whenever a file or folder is deleted, that item is sent to the Recycle Bin, and it remains on the hard disk until the Recycle Bin is emptied. Before the Recycle Bin is emptied, any files stored there can be restored to their original locations.

Note that files or folders deleted from floppy disks, Zip disks, or network servers are not stored in the Recycle Bin. When removable media items are deleted, Windows simply asks for a confirmation of the deletion. In addition, items deleted from within an application program (such as a word-processing program) may or may not be sent to the Windows Recycle Bin. So what happens when a user empties the Recycle Bin? Are the files or folders that they deleted gone for good? The following sections address how to track deleted files through the Windows Recycle Bin.

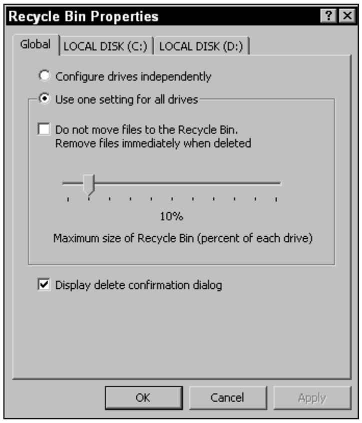
The Bin Is Empty, yet the Evidence Remains

All digital data stored on a computer — even when placed in the Recycle Bin — can be subject to subpoena at any moment. Before the widespread use of computers, criminals covered their tracks by using a shredder to destroy paper documents that contained incriminating evidence. Legitimate organizations and businesses also used shredders to limit and reduce the amount of classified information they accumulated. Today, paper shredding is no longer a viable solution for the plethora of digital documents that are created in our wired world. Since the vast majority of paper documents today originate from computers, shredding the paper copy does nothing to erase the digital copy stored on the computer's hard drive. In many investigations, the evidence needed to make or break a case still resides on the suspect's hard drive.

Digital evidence takes many forms, including sensitive word-processing documents, customer database lists, financial records, and e-mail messages, to name a few. Even when a user sends incriminating documents to the Recycle Bin and then empties it, the actual information (digital data) remains in its original place on the hard drive for a period of time — until the operating system overwrites the original location where the incriminating document was stored. Only the "map" that Windows uses to locate the data has been destroyed. In fact, computer forensic evidence of this nature was used during the high-profile impeachment hearings for President Bill Clinton when forensic computer experts recovered deleted data from Monica Lewinsky's home computer as well as "her" computer at the Pentagon. The file-system mechanics used by Windows to store, retrieve, and delete data are covered in detail later in this chapter.

Tracking Deleted Files Through the Windows Recycle Bin

When you delete a file or folder using Windows Explorer or My Computer, the file immediately appears in the Recycle Bin. As mentioned earlier, the file or folder remains in the Recycle Bin until the Recycle Bin is emptied or the file is restored. Older files are also automatically removed from the Recycle Bin when more recent files are deleted and when the contents of the older files in the Recycle Bin exceeds the maximum size allocated for the Recycle Bin properties. The Recycle Bin Properties box (see Figure 4-6) can be accessed by right-clicking the Recycle Bin icon on the Windows desktop.



○ Configure drives independently

● Use one setting for all drives

☐ Do not move files to the Recycle Bin.
Remove files immediately when deleted

10%
Maximum size of Recycle Bin (percent of each drive)

☑ Display delete confirmation dialog

Figure 4-6: The Recycle Bin Properties box in Windows XP Pro

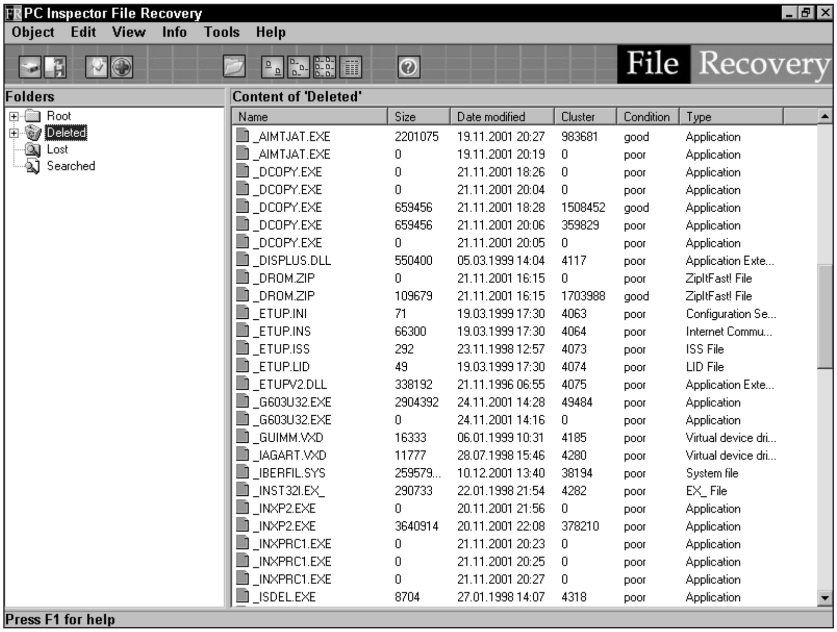
For each local hard disk on the user's computer, a hidden folder named Recycled is created. This folder contains files deleted using My Computer, Windows Explorer, and some Windows applications. The Windows OS keeps track of any files sent by the user to the Recycle Bin by generating temporary Info files. When a file or folder is deleted, the complete path, including the original file name, is stored in a special hidden file called Info in the Recycled folder. The deleted file is renamed, using the following syntax:

```
D<original drive letter of file><#>.<original extension>
```

As mentioned earlier in this section, each local hard drive has its own Recycled folder. Files deleted from many Windows applications are also moved to the Recycled folder on the drive from which they are deleted. Double-clicking the Recycle Bin icon displays the folder listing of all deleted files that are available for restoration. By right-clicking the file and choosing Restore, the original file is renamed and restored to its original name and location.

For those conducting a forensic investigation, Recycle Bin Info files serve as a window to the past by documenting a user's file deletion activities. The Windows OS contains numerous Recycle Bin Info files spread throughout hidden areas of the hard drive. Even after the Recycle Bin has been emptied, traces of the temporary Info files remain. By using readily available freeware programs like PC Inspector File Recovery by Convar Deutschland GMBH, an investigator can often determine when a user deleted particular files, even if those files were long since emptied from the Recycle Bin (see Figure 4-7). For more information about PC Inspector File Recovery or to download a copy, visit `www.convar.de`._

The previously mentioned Info file records help to tell stories about file histories and even a user's emotional state. As files automatically deleted by the OS do not leave a record in the Info file, an Info file record indicates that a user *knowingly* deleted a file in question. It is not uncommon to find files deleted during a certain time period, such as when the user may have felt that suspicion was focused upon him. A skilled computer forensic investigator is able to recover these Info files, which are often vital for creating a convincing case.



Content of 'Deleted'

Name	Size	Date modified	Cluster	Condition	Type
_AIMTJAT.EXE	2201075	19.11.2001 20:27	983681	good	Application
_AIMTJAT.EXE	0	19.11.2001 20:19	0	poor	Application
_DCOPY.EXE	0	21.11.2001 18:26	0	poor	Application
_DCOPY.EXE	0	21.11.2001 20:04	0	poor	Application
_DCOPY.EXE	659456	21.11.2001 18:28	1508452	good	Application
_DCOPY.EXE	659456	21.11.2001 20:06	359829	poor	Application
_DCOPY.EXE	0	21.11.2001 20:05	0	poor	Application
_DISPLUS.DLL	550400	05.03.1999 14:04	4117	poor	Application Exte...
_DROM.ZIP	0	21.11.2001 16:15	0	poor	ZipItFast! File
_DROM.ZIP	109679	21.11.2001 16:15	1703988	good	ZipItFast! File
_ETUP.INI	71	19.03.1999 17:30	4063	poor	Configuration Se...
_ETUP.INS	66300	19.03.1999 17:30	4064	poor	Internet Commu...
_ETUP.ISS	292	23.11.1998 12:57	4073	poor	ISS File
_ETUP.LID	49	19.03.1999 17:30	4074	poor	LID File
_ETUPV2.DLL	338192	21.11.1996 06:55	4075	poor	Application Exte...
_G603U32.EXE	2904392	24.11.2001 14:28	49484	poor	Application
_G603U32.EXE	0	24.11.2001 14:16	0	poor	Application
_GUIMM.VXD	16333	06.01.1999 10:31	4185	poor	Virtual device dri...
_IAGART.VXD	11777	28.07.1998 15:46	4280	poor	Virtual device dri...
_IBERFIL.SYS	259579...	10.12.2001 13:40	38194	poor	System file
INST32I.EX	290733	22.01.1998 21:54	4282	poor	EX_ File
_INXP2.EXE	0	20.11.2001 21:56	0	poor	Application
_INXP2.EXE	3640914	20.11.2001 22:08	378210	poor	Application
_INXPRC1.EXE	0	21.11.2001 20:23	0	poor	Application
_INXPRC1.EXE	0	21.11.2001 20:25	0	poor	Application
_INXPRC1.EXE	0	21.11.2001 20:27	0	poor	Application
_ISDEL.EXE	8704	27.01.1998 14:07	4318	poor	Application

Figure 4-7: PC Inspector File Recovery by Convar Deutschland GMGH showing recently deleted files

Recovering Deleted Data in Windows

As mentioned earlier, to understand how deleted files are recovered, you first need to have an understanding of how files are stored on a disk. With that behind us, the next step in recovering deleted data is to understand what happens when a user deletes a file under any one of the aforementioned Windows file systems. Regardless of the file system used by Windows, whenever a user deletes a file, the Windows operating system doesn't actually remove the file. Instead, the OS moves the file's directory entry (FAT entry) and information about the file's original location into a hidden folder that represents the Recycle Bin. The actual physical data isn't deleted or even moved, only the location of the directory (FAT entry) changes.

As mentioned earlier in this chapter, when the Recycle Bin is "full" — no longer able to hold deleted data — the oldest files are purged first. While it is possible to bypass the Recycle Bin by holding down the Shift key when deleting a file, the actual file data will yet remain. When files are deleted under the FAT file system, Windows modifies the deleted data's FAT entry by indicating that those entries are now available for reuse. Under NTFS, the process is similar. Only the file's directory entry, data clusters, and MFT entry are marked as available. The file's data remains, though, until the clusters are recycled to store some other file. In either case, once the disk clusters that were originally occupied by a deleted file have been overwritten by new data, the file is gone forever.

When computer files are created, their length varies depending upon the content of the data being stored. In DOS and Windows, files are stored in blocks of data of fixed length, called clusters. Since file sizes rarely match the size of one or multiple clusters perfectly, data storage space, known as file slack, exists from the end of one file to the end of the last cluster assigned to that file. Cluster sizes vary in length depending upon the operating and file systems involved. Larger cluster sizes mean more file slack and also more waste of storage space, particularly when Windows 95 is involved. However, this shortcoming can be useful for the computer forensics investigator since file slack can be a significant source of evidence.

File slack has the potential to contain randomly selected bytes of data from computer memory. This occurs because DOS/Windows normally stores data in 512-byte blocks known as sectors. Clusters are made up of groups or blocks of sectors. If there is not enough data stored to completely fill the last sector in a file, the DOS and Windows operating system will pad the remaining space with data taken from the computer's memory buffers. This randomly selected data from memory is called RAM slack since it is extracted from the random access memory of the computer. RAM slack may contain any information that has been created, downloaded, copied, viewed, or modified since the computer was last booted. If the computer has not been shut down for an extended period of time, the data stored in file slack can come from work sessions that occurred in the past. Because file slack potentially contains random data "borrowed" from the computer's memory, it is possible to identify network logon names, passwords, and other sensitive information associated with everyday computer usage. It is important not to forget that file slack can also exist on floppy disks, Zip disks, and other removable media devices.

Industrial-Strength Recovery Utility

While there are numerous freeware and shareware utilities available for data recovery, only a select few possess the qualities necessary to be used when conducting a computer forensic investigation. In addition to the previously mentioned PC Inspector File Recovery, another excellent data recovery utility is EasyRecovery Professional by Kroll Ontrack, Inc. According to its manufacturer, EasyRecovery Professional contains advanced data recovery capabilities that allow you to search and recover numerous file types. In addition, EasyRecovery Professional includes an Emergency Boot Diskette to help recover data from compromised systems that are no longer capable of loading Windows. For pricing and additional information, visit `www.ontrack.com`.

Unix/Linux Data Storage Using the ext2 File System

All operating systems use file systems, and all file systems perform the same basic functions. The fundamental goal of any file system is the organization of data and efficiently accessing that data. Accordingly, while file systems do share some common traits, they often differ in the way they store data. Unix has been around for several decades, making it one of the oldest operating systems, and Unix file systems are quite different from Windows file systems.

Ext2 is traditionally a Unix file system; however, it is also used by Linux. In ext2, data is stored on disks in blocks. The typical block size is small, around 4K in size. The file metadata (the data about the data) is stored in *inodes*. An inode stores all information about a file with the exception of its name. In ext2, the directories store file names and their associated inodes. Directories are stored as normal files on disk but marked as being a directory by the information contained in the inode. Directories are structured in the form of a hierarchical tree. Each directory can contain files and subdirectories. Directories are implemented as a special type of file. Actually, a directory is a file containing a list of entries. Each entry contains an inode number and a file name. The ext2 file system is able to manage very large hard drives. While the original version of ext2 was restricted to a maximal file-system size of 2GB, recent changes have raised this limit to 4TB. Accordingly, it is now possible to use big disks without the need to create many 2GB (or less) partitions. In addition to being able to handle larger hard drives, the ext2 file system also provides for the use of long file names. It uses variable length directory entries. Like FAT32, the maximum file-name size is 255 characters; however, it is possible to extend this limit to 1,012 characters, if needed.

File Deletion in ext2

In ext2, when a file is deleted, the complete inode information is preserved. Only its name is removed from the directory, and the time of the deletion in the inode is marked. In other words, only the association between the file name and the inode is removed. Because inode data and data blocks are not immediately overwritten, all the data needed to recover a file (with the exception of the file name) remains on disk. However, the ability to recover deleted files is limited since the deleted data can be overwritten at any point in time after its deletion. Once this happens, the data *is* gone permanently.

File Recovery in ext2

The first step toward file recovery in ext2 is to immediately unmount the file system on the hard disk drive where the deleted file was located. This helps minimize any risk of accidentally overwriting the deleted file while conducting the recovery process. The basic syntax or command to unmount a Unix or Linux device is `unmount /dev/devicename`.

note

Any data written to the file system containing the deleted file (either by you or by any other process running on your machine) has the potential to overwrite some of the data you hope to recover. If you are unable to unmount the file system because the deleted file was located on your root file system, for example, you may wish to consider removing the hard drive and reinstalling it into another Unix or Linux machine as a nonroot drive.

Using e2undel

The fundamental procedure for recovering data in ext2 involves finding the deleted data on the raw partition device and then making it visible again to the operating system. There are two ways to accomplish this. The first method is to remove the delete flag from the inodes of the deleted data. This approach is somewhat complicated because it requires some programming knowledge and the use of debugging tools. The preferred and safer process is to ferret out where the data lies in the partition, and then copy that data into a new file on another file system.

The best method for recovering deleted data under the ext2 file system is to use a handy freeware utility called e2undel. This handy program recovers the data of deleted files on computers using the ext2 file system. Among its features is a built-in library that allows you to recover deleted files by name. One of the biggest benefits of this utility is that it does not require an extensive knowledge of the ext2 file-system commands in order to use it. The basic syntax for recovering data using ex2undel is as follows:

```
e2undel -d device -s path [-a] [-t]
```

The following shows what the commands in the above line mean:

`-d` is the file system location where you wish to search for the deleted files (for example, `/dev/hd0` for the first partition on the primary IDE drive).

`-s` is the directory where you wish to save recovered files.

`-a` recovers all deleted files, not just those listed in the undel log file.

`-t` attempts to determine the type of deleted files without names (this option works only in conjunction with the `-a` command).

note

While the `-a` option should always be used, the `-t` option is not mandatory. For additional information about e2undel commands or to download a copy of this utility, visit `http://sourceforge.net/projects/e2undel`.

Chapter Summary

While most organizations employ firewalls and intrusion detection systems to protect their networks, they still fall victim to successful attacks by technologically savvy network intruders. In order to combat modern-day network marauders, network personnel must be trained in investigative techniques, incident response tactics, and the legal procedures for collecting evidence. Because Windows is the most widely used operating system, it is also the most popular target for hackers, crackers, and users of malicious code. Network attacks may come from either external sources or internal personnel. Two common targets are the Windows Registry and data storage systems. While network intruders often attempt to cover their tracks by deleting certain files, a number of methods and software tools are available to help in retrieving this ostensibly lost data.

Key points covered in this chapter include

- ✓ An overview of the Windows Registry and its role in incident response
- ✓ How to view, edit, preserve, and protect the Windows Registry data
- ✓ Overview of Windows and Unix/Linux data storage structures
- ✓ How to collect evidence from deleted files via the Windows Recycle Bin
- ✓ Procedures for recovering deleted data under FAT and ext2 file systems

Chapter 5

Analyzing and Detecting Malicious Code and Intruders

In This Chapter

- ✓ Analyzing abnormal system processes
- ✓ Detecting unusual or hidden files
- ✓ Locating rootkits and backdoors
- ✓ Detecting and preventing network sniffers

THE INTERNET HAS ALTERED THE WAY BUSINESS IS CONDUCTED. Nearly everything is accessible with the click of a mouse. While individuals and organizations use the Internet daily for e-mail messaging, e-commerce, or instant messaging, rarely do we consider the dangers posed by hackers, viruses, worms, and Trojan horses as we click away from Web site to Web site. We place trust in our computers and assume that they offer protection for our sensitive information. The largely unregulated Internet harbors numerous threats. While hackers, crackers, and law-abiding citizens all live together in the cyber world, the average Internet user is usually unaware of the presence of malevolent individuals. Malicious code in the form of viruses, worms, and Trojan horses traverses the Internet, exploiting flaws that exist in the operating systems and applications of many an innocent user.

Because of these cyber threats, individuals and organizations need to change the way they operate and manage their networks. Security training frequently is focused on basic security issues and not on responding to Internet threats. During typical user awareness training the specifics of e-mail message attachments (and their ability to hide malicious code or masquerade as legitimate documents or graphics files) are not addressed sufficiently. We cannot blame computer users for virus proliferation if they are thrust into a computerized environment without first having been exposed to some incident response basics. This chapter focuses on detecting, analyzing, and responding to threats posed by intruders and malicious coders.

System Processes

Simply put, a *process* is an executing program. Oftentimes a thread is confused with a process. Similar to a process, a *thread* is the unit of execution to which the operating system assigns processing time (a time slice), and it consists only of data flow and control. Threads provide a useful programming technique for dividing work into separate pieces. Thread execution is monitored and scheduled solely by the operating system, and every process is started with the execution of a single thread, usually called the primary thread. Even where there are multiple threads, they still use only the address space of a single process.

Every program running on a computer uses at least one process, consisting of the memory address (space) allocated to the process by the computer to run the program and the ability of the computer's OS to monitor the program throughout the execution process. In modern-day 32-bit multitasking operating systems, processes are managed for the most part as isolated entities so that if one process crashes, the others are generally not affected. The resources they use (memory, disk, I/O, and CPU time) are virtual in nature, meaning that every process has its own set of virtual resources, untouched by other processes. Even when several programs are running at the same time, each process has its own address space and flow of control. Thus, a process is a place to work and a way to keep track of what a program is doing.

Detecting Abnormal System Processes

Monitoring system processes can be both complicated and time-consuming. The ability to identify suspicious or abnormal processes first requires a thorough understanding of the types of processes one normally would expect to be executing on a system at a given time as well as how they should behave. However, due to the enormous number of processes running simultaneously and their constantly changing nature, it is nearly impossible for a single individual to monitor all of them continually. To make the job of monitoring system resources easier, some organizations divide system monitoring among several different personnel. Each individual is assigned a particular system resource to monitor.

The value of information that can be gathered from a periodic snapshot of currently executing processes is limited. Organizations may need to utilize a range of information gathering and monitoring mechanisms to assist in collecting and analyzing data associated with processes, and to alert incident response personnel to any suspicious activity.

In general, monitors should look for the following signs:

- ✓ Unusual resource utilization or process behavior
- ✓ Missing processes
- ✓ Added processes
- ✓ Processes that have unusual user identification associated with them (such as an ID belonging to someone not employed by an organization)

Abnormal system processes can be caused by

- ✓ Programs that log a user's keystrokes or monitor and steal passwords

- ✓ Malicious code (viruses, Internet worms, and Trojan horse applications)
- ✓ Spyware (software that transmits information back to a third party *without* notifying the user)

As mentioned in Chapter 1, log files should be checked for connections from unusual locations or for any unusual activity. All versions of Windows NT have a built-in Event Viewer that allows you to check for unusual logon entries, failures of services, or abnormal processes. Data collected from log files can help in the analysis of the process behavior.

These include the following:

- ✓ The process names and startup times
- ✓ The status of the process (for example, time duration, resources consumed, and so on)
- ✓ Which user executed the process
- ✓ The amount of system resources used (for example, CPU, memory, disk, and time) by specific processes over time
- ✓ System and user processes and services executing at any given time
- ✓ The method by which each process is normally started (for example by the system administrator, other users, other programs, or spawned from other processes) and what authorization and privileges have been assigned to those processes
- ✓ Hardware devices used by specific processes
- ✓ Files currently opened by specific processes

When reviewing operating system or network logs, look for the following:

- ✓ Processes consuming excessive resources (for example, memory, disk, or CPU time)
- ✓ Processes starting or running at unexpected times
- ✓ Unusual processes not the result of normal authorized activities (for example, packet sniffing, password cracking, and so on)
- ✓ Processes that prematurely terminate
- ✓ Previously inactive user accounts that suddenly begin to spawn processes and consume computer or network resources
- ✓ Unexpected or previously disabled processes, which may indicate that a hacker or intruder has installed his own version of a process or service
- ✓ A workstation or terminal that starts exhibiting abnormal input/output behavior
- ✓ Multiple processes with similar names (for example, when a computer virus runs Explorer.exe using a capital letter to disguise itself rather than the actual process, which is called explorer.exe by the operating system)
- ✓ An unusually large number of running processes

Using the Windows Task Manager to View Running Processes

The Windows Task Managerprovides information about programs and processes running on your computer. It also displays the most commonly used performance measures for any running processes. While the Task Manager is useful for monitoring key indicators of your computer's performance, it also permits you to quickly see the status of the programs and processes that are running and even terminate programs (when they freeze or stop responding). You may assess the activity of running processes using numerous parameters and viewing graphs and data on CPU and memory usage (see Figures 5-1, 5-2, and 5-3). The name of the Task Manager program is taskmgr.exe, and there are several manners in which to access the program. One way is to type `taskmgr` in the Run box on the Start menu or at the command (DOS) prompt to bring up the program. Another convenient access method is to create a shortcut link to the program directly on the Windows desktop. Finally, you may type Ctrl+Alt+Del (a.k.a. "the three finger salute") at any time while the operating system is running.

tip

To create a desktop shortcut to the taskmgr.exe program, you first need the location of this file in the Windows OS. The default location is `C:\winnt\system32` for Windows NT and 2000 and `c:\windows\system32` for Windows XP.

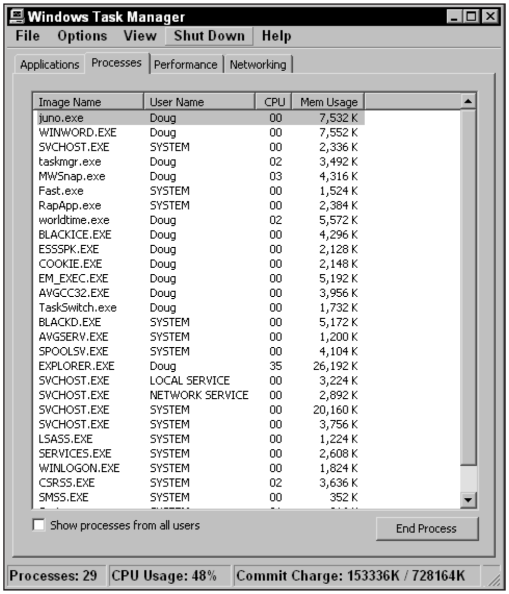
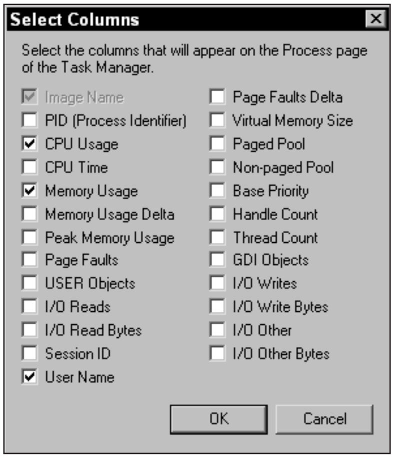

Windows Task Manager
File Options View Shut Down Help
Applications Processes Performance Networking
End Process

Image Name	User Name	CPU	Mem Usage
juno.exe	Doug	00	7,532 K
WINWORD.EXE	Doug	00	7,552 K
SVCHOST.EXE	SYSTEM	00	2,336 K
taskmgr.exe	Doug	02	3,492 K
MWSnap.exe	Doug	03	4,316 K
Fast.exe	SYSTEM	00	1,524 K
RapApp.exe	SYSTEM	00	2,384 K
worldtime.exe	Doug	02	5,572 K
BLACKICE.EXE	Doug	00	4,296 K
ESSSPK.EXE	Doug	00	2,128 K
COOKIE.EXE	Doug	00	2,148 K
EM_EXEC.EXE	Doug	00	5,192 K
AVGCC32.EXE	Doug	00	3,956 K
TaskSwitch.exe	Doug	00	1,732 K
BLACKD.EXE	SYSTEM	00	5,172 K
AVGSERV.EXE	SYSTEM	00	1,200 K
SPOOLSV.EXE	SYSTEM	00	4,104 K
EXPLORER.EXE	Doug	35	26,192 K
SVCHOST.EXE	LOCAL SERVICE	00	3,224 K
SVCHOST.EXE	NETWORK SERVICE	00	2,892 K
SVCHOST.EXE	SYSTEM	00	20,160 K
SVCHOST.EXE	SYSTEM	00	3,756 K
LSASS.EXE	SYSTEM	00	1,224 K
SERVICES.EXE	SYSTEM	00	2,608 K
WINLOGON.EXE	SYSTEM	00	1,824 K
CSRSS.EXE	SYSTEM	02	3,636 K
SMSS.EXE	SYSTEM	00	352 K

☐ Show processes from all users

Processes: 29 | CPU Usage: 48% | Commit Charge: 153336K / 728164K

Figure 5-1: The Windows XP Task Manager window showing all currently running processes

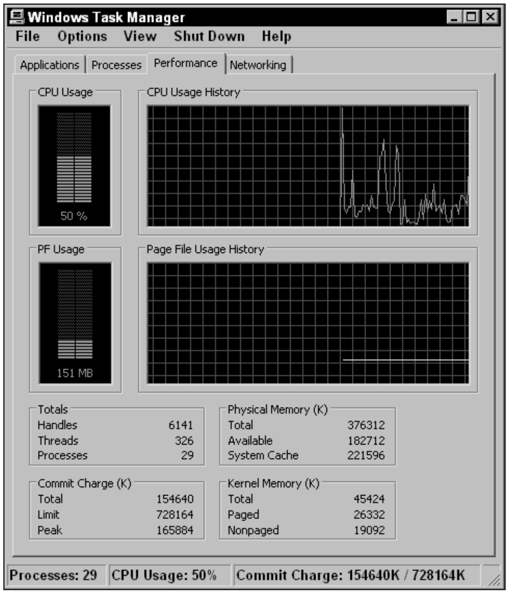


Select Columns

Select the columns that will appear on the Process page of the Task Manager.

☑ Image Name
☐ PID (Process Identifier)
☑ CPU Usage
☐ CPU Time
☑ Memory Usage
☐ Memory Usage Delta
☐ Peak Memory Usage
☐ Page Faults
☐ USER Objects
☐ I/O Reads
☐ I/O Read Bytes
☐ Session ID
☑ User Name
☐ Page Faults Delta
☐ Virtual Memory Size
☐ Paged Pool
☐ Non-paged Pool
☐ Base Priority
☐ Handle Count
☐ Thread Count
☐ GDI Objects
☐ I/O Writes
☐ I/O Write Bytes
☐ I/O Other
☐ I/O Other Bytes

Figure 5-2: The Select Columns box in Windows XP Task Manager



Totals	
Handles	6141
Threads	326
Processes	29

Physical Memory (K)	
Total	376312
Available	182712
System Cache	221596

Commit Charge (K)	
Total	154640
Limit	728164
Peak	165884

Kernel Memory (K)	
Total	45424
Paged	26332
Nonpaged	19092

Processes: 29 CPU Usage: 50% Commit Charge: 154640K / 728164K

Figure 5-3: Viewing CPU performance with Windows XP Task Manager

Default Processes in Windows NT, 2000, and XP

In order to detect errant or unauthorized processes using the Windows Task Manager, it is helpful to understand which processes run by default during normal system operations. There are a number of default processes that are automatically run by the Windows operating system (they vary depending upon which version of Windows is being used). The following is an alphabetical listing of some of the default processes that are commonly run under Windows NT/2000/XP, along with a brief explanation of their functions:

- ✓ **Csrss.exe.** Csrss or Client/Server Run-time Subsystem is an essential subsystem that must remain running at all times. Csrss provides text window support, shutdown, and hard-error handling to the Windows NT environment subsystems.
- ✓ **Explorer.exe.** This is the Graphical User Interface in which we see the familiar taskbar and desktop environment. Explorer lets users open documents and applications from various icons and Windows cascading menus.
- ✓ **Lsass.exe.** This process helps handle security administration on the local computer, including user access and permissions. This process is responsible for authenticating users for the Winlogon service and is shared by the Netlogon service.
- ✓ **Mstask.exe.** This is the task scheduler service. It is responsible for running tasks at times that are predetermined by the user.
- ✓ **Services.exe.** This is the Windows Services Control Manager, which is responsible for starting and stopping system services and works with other Windows machines on the network to maintain a current list of available resources.
- ✓ **Smss.exe.** Session Manager Subsystem is responsible for starting the user session. Smss is initiated by the system thread and is responsible for a range of actions, including launching the Winlogon and Win32 (Csrss.exe) processes and setting system variables.
- ✓ **Spoolsv.exe.** This is the Windows spooler service and is responsible for the management of spooled print and fax jobs.
- ✓ **Svchost.exe.** A generic process, which acts as a host for other processes running from DLLs; therefore, don't be surprised to see more than one entry for this process.
- ✓ **System.** This permits system kernel-mode threads to run as the System process.
- ✓ **System Idle Process.** This process is a single thread running on each processor. Its sole task is accounting for processor time when the system isn't processing other threads.

Process-Monitoring Programs

In the nonvirtual world, when a complex task must be carried out, tools are available to make the job easier. The same principal applies in the virtual world of computers. As mentioned earlier in this chapter, monitoring system processes can be time-consuming and complex. Most Unix operating systems ship with a command-line tool called `ps`. The `ps` command allows you to list what processes are being executed by the machine on which the command was entered. Administrators can use it along with the **`-ef`** option (for example, `ps -ef`) to get a full listing of all processes on the Unix system. While Windows NT, 2000, and XP come with Task Manager, they don't offer a significant level of detail about individual processes. Luckily, there are several programs available that can make the job of monitoring system processes less onerous. At the Sysinternals Web site (`www.sysinternals.com`) there is a downloadable suite of advanced freeware utilities called PsToolscoded by Mark Russinovich. It can assist in the monitoring and gathering of detailed information about system processes under the Windows operating system. The PsTools suite includes the following tools, which can be downloaded individually or as a package:

- ✓ **PsExec** executes processes remotely.
- ✓ **PsFile** shows files opened from a remote location.
- ✓ **PsGetSid** displays the SID (security identifier) of a computer or a user.
- ✓ **PsInfo** lists information about a system.
- ✓ **PsKill** terminates processes by name or process ID.
- ✓ **PsList** lists detailed information about processes.
- ✓ **PsLoggedOn** shows who's logged on locally and via resource sharing.
- ✓ **PsLogList** dumps event log records.
- ✓ **PsService** views and controls services.
- ✓ **PsShutdown** shuts down and optionally reboots a computer.
- ✓ **PsSuspend** suspends processes.
- ✓ **PsUptime** shows how long a system has been running since its last reboot.

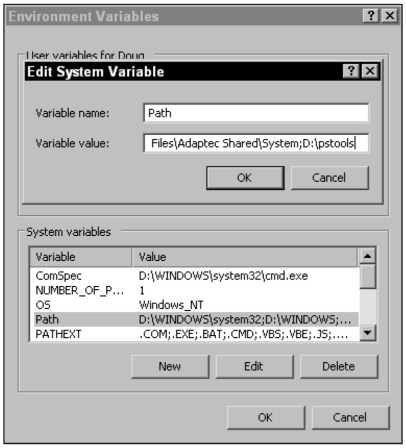
Since all of the PsTools are command-line tools, they must be run from a command (DOS) prompt. You will need to add the folder that they are stored in to your system's path in order to run them from any directory other than the directory or folder in which they were placed. By placing these tools in your Winnt directory (Windows NT/2000) or your Windows directory (Windows XP), they will automatically be included in your system's Path statement. If you wish to place these tools in their own directory (for example, `C:\PsTools`) yet still have Windows locate them automatically, perform the following steps.

Under Windows NT 4.0, do the following:

1. Right-click the My Computer icon.
2. Select Properties from the context menu.
3. Double-click the System icon.
4. Click the Environment tab.
5. Select Path from the list of system variables.
6. Edit the Path statement by adding the directory in which PsTools is stored.

Under Windows 2000, XP, do the following:

1. Right-click the My Computer icon. (In Windows XP, the My Computer Icon may be located in the Start menu.)
2. Select Properties from the context menu.
3. Select the Advanced tab.
4. Click the Environment Variables button.
5. From the System Variables window, highlight Path entry and then select Edit.
6. Add (append) the location of the PsTools directory to the list of directories in the Path by using a semicolon directly after the last statement in the Path, then adding the location of the PsTools Directory (see Figure 5-4).



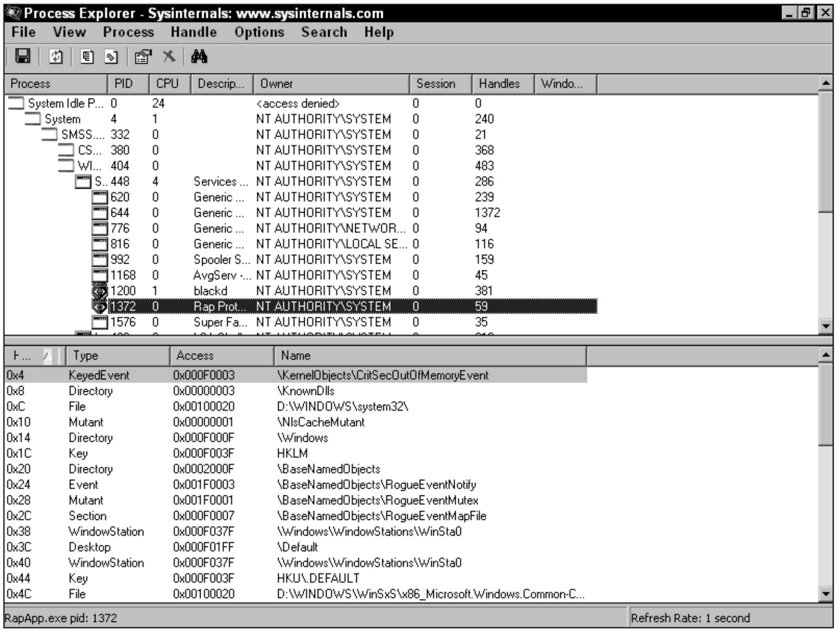
Variable name: Path

Variable value: Files\Adaptec Shared\System;D:\pstools

Variable	Value
ComSpec	D:\WINDOWS\system32\cmd.exe
NUMBER_OF_P…	1
OS	Windows_NT
Path	D:\WINDOWS\system32;D:\WINDOWS;…
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;….

Figure 5-4: Adding the location of the PsTools directory to your directories list via Windows XP Pro Environmental Variables editing utility

Another useful tool from the Sysinternal Web site is Process Explorer (see Figure 5-5) by Mark Russinovich. With this powerful point-and-click, Windows-based, freeware utility, you can find out who owns each process, and, for each of these processes, what files, Registry keys, and other objects are open. In addition, Process Explorer shows which DLLs have loaded and which handles opened with each process. This makes it a powerful tool for understanding the internal behavior of applications, as well as for tracking down handle leaks and DLL version mismatches.



Process	PID	CPU	Descrip...	Owner	Session	Handles	Windo...
System Idle P...	0	24		<access denied>	0	0	
System	4	1		NT AUTHORITY\SYSTEM	0	240	
SMSS....	332	0		NT AUTHORITY\SYSTEM	0	21	
CS...	380	0		NT AUTHORITY\SYSTEM	0	368	
WI...	404	0		NT AUTHORITY\SYSTEM	0	483	
S..	448	4	Services ...	NT AUTHORITY\SYSTEM	0	286	
	620	0	Generic ...	NT AUTHORITY\SYSTEM	0	239	
	644	0	Generic ...	NT AUTHORITY\SYSTEM	0	1372	
	776	0	Generic ...	NT AUTHORITY\NETWOR...	0	94	
	816	0	Generic ...	NT AUTHORITY\LOCAL SE...	0	116	
	992	0	Spooler S...	NT AUTHORITY\SYSTEM	0	159	
	1168	0	AvgServ -...	NT AUTHORITY\SYSTEM	0	45	
	1200	1	blackd	NT AUTHORITY\SYSTEM	0	381	
	1372	0	Rap Prot...	NT AUTHORITY\SYSTEM	0	59	
	1576	0	Super Fa...	NT AUTHORITY\SYSTEM	0	35	

H...	Type	Access	Name
0x4	KeyedEvent	0x000F0003	\KernelObjects\CritSecOutOfMemoryEvent
0x8	Directory	0x00000003	\KnownDlls
0xC	File	0x00100020	D:\WINDOWS\system32\
0x10	Mutant	0x00000001	\NlsCacheMutant
0x14	Directory	0x000F000F	\Windows
0x1C	Key	0x000F003F	HKLM
0x20	Directory	0x0002000F	\BaseNamedObjects
0x24	Event	0x001F0003	\BaseNamedObjects\RogueEventNotify
0x28	Mutant	0x001F0001	\BaseNamedObjects\RogueEventMutex
0x2C	Section	0x000F0007	\BaseNamedObjects\RogueEventMapFile
0x38	WindowStation	0x000F037F	\Windows\WindowStations\WinSta0
0x3C	Desktop	0x000F01FF	\Default
0x40	WindowStation	0x000F037F	\Windows\WindowStations\WinSta0
0x44	Key	0x000F003F	HKU\.DEFAULT
0x4C	File	0x00100020	D:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-C...

RapApp.exe pid: 1372

Refresh Rate: 1 second

Figure 5-5: Process Explorer 5.25

Unusual or Hidden Files

It is sometimes difficult to determine if a system has been compromised. It is important therefore to search periodically for any unusual or hidden files that may have bypassed intrusion detection and antivirus protection. Hidden files can be used to conceal hacker tools, malicious code, and sensitive information (for example, password-cracking programs, password files from other systems, and so on). A number of recently developed malicious programs have exploited the default behavior of Windows operating systems to hide file extensions. This behavior can be used to trick users into executing code by making a file appear to be something it is not. Multiple e-mail-borne viruses are known to exploit this vulnerability.

Viewing Hidden Files in Windows

Windows operating systems contain an option to “Hide file extensions for known file types.” The option is enabled by default, but a user may choose to disable this option in order to have file extensions displayed by Windows.

To show hidden files, folders, and filename extensions under Windows, perform the following steps.

For Windows NT, do the following:

1. Click the Start button, select Settings, then Control Panel.
2. From the View menu, select Options.
3. Click the View tab.
4. From the View tab, select “Show all files.”
5. Deselect the “Hide file extensions for known file types” option.
6. Click OK to complete the changes.

For Windows 2000, do the following:

1. Click the Start button, select Settings, then Control Panel.
2. From the Tools menu, select Folder Options.
3. Click the View tab.
4. Under “Hidden files and folders,” select “Show hidden files and folders.”
5. Deselect the “Hide file extensions for known file types” option.
6. Deselect “Hide protected operating system files.” (Note: Windows 2000 will display a dialog box asking for confirmation. Be sure to read and understand the information contained in the dialog, and then click Yes.)
7. Click OK to complete the changes.

For Windows XP, do the following:

1. Click the Start button, and select Control Panel.
2. From the Tools menu, select Folder Options.
3. Click the View tab.
4. Under “Hidden files and folders,” select “Show hidden files and folders.”
5. Deselect the “Hide file extensions for known file types” option.
6. Deselect “Hide protected operating system files.” (Note: Windows XP will display a dialog box asking for confirmation. Be sure to read and understand the information contained in the dialog, and then click Yes.)
7. Click OK to complete the changes.

tip

In all versions of Windows you can view hidden files at the command prompt by typing dir /ah.

Viewing Hidden Files under Unix/Linux

Even when using Unix or Linux, it is important to search the system for unusual or hidden files. Under Unix and Linux systems, these are files that start with a period and normally are not shown by the ls command. (The ls command lists all of the files and subdirectories you have in a given directory.) These files are often used by hackers to hide tools and password-cracking programs. A common technique used with Unix/Linux systems is to put a hidden directory or file in a user's account with an unusual name such as .. (dot-dot-space) or ..^G (dot-dot-control-G). Luckily, the built-in Find program in Unix can help seek out these types of concealed files. Here are two examples:

```
find / -name ".. " -print -xdev
find / -name ".*" -print -xdev
```

Another favorite hacker ploy is to exploit SUID root programs. (SUID root refers to Set User ID root.) SUID root allows the program to carry out functions that only system administrators with full root privileges would be permitted to perform. Programs that run as root have complete access to a Unix system, and SUID programs run as root regardless of who is executing them. Programs that run low-level networking routines and control functions such as graphical display, changing passwords, and logging in are all examples of programs that require a user with full root privileges to execute them. Intruders often leave behind SUID copies of /bin/sh or /bin/time to allow them to gain root access later. Find all SUID programs on your system and keep track of what they are. By doing so, you will be aware of any changes, which could indicate a potential intruder. Use the following command to find and print a list of all programs or files that are SUID root:

```
find / -type f -perm -4000 -print | mail root
```

You may also wish to browse through the list of all SUID programs and locate those that you seldom or never use. You can turn off (disable) the SUID bit using the chmod (change mode) command. Essentially, chmod refers to setting the access privileges for a file. To execute chmod on a file or directory, you must be its owner or a superuser with root privileges. The next step in controlling SUID root programs is to analyze which programs should not be SUID root or those that can be removed without impeding system functionality. The list of programs that should not be SUID root varies from system to system. In general, before turning off the SUID root, you should first determine the program's function and then decide if it is an essential program or if it must be SUID root.

note

A superuser account is a privileged account with unrestricted access to all files and commands. Many administrative tasks can only be performed by a superuser account. By convention, the username for the superuser account is root.

The exact syntax for removing SUID root varies depending upon which files you wish to modify. Assuming that you want to remove the SUID bit on `/usr/bin/passwd`, the syntax is

```
chmod -s / usr/bin/passwd
```

The guiding tenet common with SUID root programs is to limit them to only those that are necessary. System administrators are encouraged to examine the function of each program to determine whether it needs to be set as SUID root or not.

Rootkits and Backdoors

The maxim asserts, “It takes a thief to catch a thief.” The same can be said of hackers. To catch a hacker, one must have a general understanding of the tools and techniques hackers employ to overcome users and systems. One of the most widely used hacker tools to accomplish this objective is the rootkit. A rootkit is used to accomplish the following functions:

- Prevent logging of activity
- Establish backdoors for reentry
- Hide or remove evidence of initial entry
- Hide specific contents of files
- Hide files and directories
- Gather intelligence (for example, usernames and passwords)

A rootkit comes by its name not because the toolbox is composed of tools to *crack* root, but instead because it is comprised of tools to *maintain* or keep root. Under both Unix and Linux, root is the highest privilege granted. Users with root privileges have access to all aspects of the operating system because root access implies complete control of a machine.

Rootkits are used by intruders to hide and secure their presence on a computer system. While there are rootkits available for the Windows operating system, Windows rootkits are currently not as widespread as their Unix counterparts and are usually detected by any reputable antivirus software. Under Unix and Linux, network administrators generally trust the `ps` command to display a list of all system processes and the `ls` command to list all files located on a hard drive directory. A rootkit generally contains a suite of hacker utilities, such as log clean-up scripts and network packet sniffers. In addition, rootkits contain specialized replacements of core Unix and Linux utilities, such as `netstat`, `ifconfig`, `ps`, and `ls`. Even though hackers must first gain access to victim systems before they can install their rootkits, their ease-of-use, widespread availability, and the amount of destruction they are able to cause make rootkits a serious threat for computer network administrators. Inevitably, most computer systems will be infiltrated by an intruder or infected by some type of malicious code. The following U.S. Department of Justice public press release demonstrates that even government agencies like NASA are not immune to rootkit exploits:

> December 1, 2000
>
> <u>News Release</u>
>
> **Hacker Pleads Guilty in New York City to Hacking into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California**
>
> MARY JO WHITE, the United States Attorney for the Southern District of New York, announced that RAYMOND TORRICELLI, a/k/a "Rolex," a member of a hacker group known as "#conflict," pled guilty today in Manhattan federal court to charges of breaking into two computers owned and maintained by the National Aeronautics and Space Administration's Jet Propulsion Laboratory ("JPL"), located in Pasadena California.
>
> According to a previously filed Complaint, TORRICELLI used one of those computers to host an Internet chat-room and installed programs designed to obtain usernames and passwords from the other computer.
>
> In pleading to a five-count Information, TORRICELLI admitted that, in 1998, he was a computer hacker, and a member of a hacking organization known as "#conflict." TORRICELLI admitted that, operating from his residence in New Rochelle, he used his personal computer to run programs designed to search the Internet, and seek out computers which were vulnerable to intrusion; once such computers were located, TORRICELLI's computer would then obtain unauthorized access to the computers by uploading a program known as "rootkit." According to the Complaint, "rootkit" is a program which, when run on a computer, allows a hacker to gain complete access to all of a computer's functions without having been granted these privileges by the authorized users of that computer.
>
> According to the Information and Complaint, one of the computers TORRICELLI accessed was used by NASA to perform satellite design and mission analysis concerning future space missions; another was used by JPL's Communications Ground Systems Section as an e-mail and internal Web server. After gaining this unauthorized access to computers, he intruded and loading "rootkit," TORRICELLI under his alias "Rolex," used many of the computers to host chat-room discussions.
>
> In his plea allocution, TORRICELLI admitted that, in these discussions, he invited other chat participants to visit a Web site which would enable them to view pornographic images, and that he earned $0.18 for each visit a person made to that Web site. According to the Complaint, TORRICELLI earned approximately $300 to $400 per week from this activity.
>
> TORRICELLI also pled guilty to intercepting usernames and passwords traversing the computer networks of a computer owned by San Jose State University, and to possession of stolen passwords and usernames which he used to gain free Internet access, or to gain unauthorized access to still more computers. TORRICELLI admitted, as part of his plea allocution, that he when he obtained passwords which were encrypted, he would use a password-cracking program known as "John-the-Ripper" to decrypt the passwords.
>
> In addition, TORRICELLI pled guilty to possessing stolen credit card numbers. As part of his plea, TORRICELLI admitted that he used one such credit card number to purchase long distance telephone service. As alleged in the Complaint, TORRICELLI obtained these credit card numbers from other individuals and stored them on his computer.

> As described in the Complaint, much of the evidence obtained against TORRICELLI was obtained through a search of his personal computer. According to the Complaint, in addition to thousands of stolen passwords and numerous credit card numbers, investigators found transcripts of chat-room discussions in which TORRICELLI and members of "#conflict" discuss, among other things, (1) breaking into other computers (a practice known as "hacking"); (2) obtaining credit card numbers belonging to other persons and using those numbers to make unauthorized purchases (a practice known as "carding"); and (3) using their computers to electronically alter the results of the annual MTV Movie Awards.
>
> Chief United States District Judge MICHAEL B. MUKASEY set sentencing in the case for March 7, 2001, at 9:15 A.M. At sentencing, TORRICELLI faces up to 10 years in prison and a $250,000 fine each on the credit card fraud and password possession charges; 5 years in prison and a $250,000 fine on the password interception charge; and 1 year in prison and a $100,000 fine on each of the charges involving his unauthorized access of the two NASA computers.
>
> Ms. WHITE praised the investigative efforts of the National Aeronautics and Space Administration, Office of the Inspector General, Computer Crimes Division; the New Rochelle, New York, Police Department; and the Federal Bureau of Investigation.
>
> Ms. WHITE stated: "The Internet is not a safe haven for criminals. As this case demonstrates, hackers who use the Internet to commit credit card fraud, steal private passwords and usernames, and gain access to restricted Government computers, thereby damaging those computers, are not harmless pranksters — they are criminals, and will be dealt with vigorously."

In a written statement to the court, Torricelli said he broke into NASA computers known as HEIDI.JPL.NASA.GOV between April 17 and 25, 1998 with a rootkit tool that could give him root access to all files on that computer. At the time the rootkit was installed, Torricelli stated, "I did not know that it was being installed on computers belonging to NASA; I did know it was being installed on computers that I was not authorized to access."

On September 5, 2001, Raymond Torricelli was sentenced to four months in prison and four months of home confinement. In addition, Torricelli was ordered to pay $4,400 in restitution to NASA.

Detecting the Presence of a Rootkit

Entry of a computer system by an intruder may leave traces of evidence via various log file messages. Most rootkits include utilities that automatically remove any suspicious or incriminating messages from the log files. One of the more common indicators that a rootkit has been used is when one or more of the core system utilities that worked flawlessly in the past suddenly begins to behave erratically because intruders have replaced these utilities with rootkit versions designed to hide their malicious activities. For instance, a command-line switch to `netstat` or `ps`, which you used to use without a problem every day, might start returning an error message. The utility with which they replaced the original one might be of a different version or could have been compiled with different options, and as a result, it does not have the same features as the original.

Rootkit detection is vital, yet it can be one of the more daunting tasks a system administrator undertakes. Rootkits fall under the category of malicious code and are detected much in the same manner as viruses, worms, or Trojans are. In fact, most rootkits contain Trojan horse backdoor components that allow them to regain entry at a later date. A careful and sophisticated hacker will not leave any evidence to find. Others may leave traces that can be picked up, but only by those familiar with operating system details and network layout.

With hard-disk drives becoming larger and operating systems more complex, it is not uncommon to have tens of thousands of files and numerous processes running. This can make locating or detecting a rootkit analogous to finding a needle in a haystack. As mentioned earlier in this chapter, the majority of modern-day rootkits merely replace standard utilities with "specialized" versions. Furthermore, rootkit installations often forge time-stamp and file-size information in an effort to prevent system administrators from visually confirming the integrity of the utilities via the Unix/Linux `ls` command.

MANUAL INSPECTION

One way to detect the presence of a rootkit is via manual inspection, which is typically carried out using the `strings` command. The `strings` utility, which is standard on all modern Unix/Linux platforms, merely displays the readable portions of a binary file. The `strings` utility looks for printable strings in regular files and writes those strings to standard printer output. A string is any sequence of four or more printable characters that end with a new-line or a null character. For the experienced systems administrator, the `strings` command can produce readable data such as the names of files where intruder passwords are kept, library versions with which the rootkit was compiled, and other information that does not normally correlate with the original data in the target file. The exact syntax used with the `strings` command varies depending upon which version of Unix or Linux is used. In general, the syntax for the `strings` command is as follows:

```
strings [ -a ] [ - ] [ -o ] [ -t (d) (o) (x) ] [ -n  ] [ File name etc... ]
```

For a listing of the flags used, see Table 5-1.

Table 5-1 Flags Used in the Unix/Linux Strings Command

`-a` or `-`	This flag searches the entire file (not just the data section) for printable strings.
`-n (`*`number`*`)`	This flag is identical to the `-number` flag and specifies a minimum string length other than the default of four characters. The maximum value of a string length is 4,096.
`-o`	This flag is identical to the `-t o` flag and lists each string preceded by its octal offset in the file.
`-t (`*`format`*`)`	This flag lists each string preceded by its offset from the start of the file. The format is dependent on the character used as the format variable, some of which are listed below: `d` writes the offset in decimal format. `o` writes the offset in octal format.

Continued

Table 5-1 Flags Used in the Unix/Linux Strings Command *(Continued)*

	`x` writes the offset in hexadecimal format.
	Note: When the `-o` and the `-t` format flags are defined more than once on a command line, the last flag specified controls the behavior of the `strings` command.
`-number`	This flag specifies a minimum string length other than the default of four characters. The maximum value of a string length is 4,096. This flag is identical to the `-n (`*`number`*`)` flag.
`file`	This flag identifies the file to be searched.

ROOTKIT DETECTION PROGRAMS

Chkrootkit is a collection of small freeware utilities used to detect the presence of known rootkits on a Linux system. Although it is possible to find stand-alone detection scripts for almost all rootkits, Chkrootkit differentiates itself by its ability to detect a large number of *different* rootkits using a single application. In addition to detecting known rootkit signatures, Chkrootkit also runs some generic tests that might aid in discovering rootkits that are not actually supported by the application. For additional information or to download a copy, visit `www.chkrootkit.org`.

For Windows- and Unix-based systems, Intact by Pedestal Software (`www.pedestalsoftware.com`) can help detect the presence of a rootkit as well as other system breaches. Intact detects rootkits by monitoring changes in computer systems. Specifically, the program takes a snapshot of system objects and then compares the snapshot to the active system in real time. By reporting unexpected changes, Intact detects unauthorized intrusions; effects of viruses, Trojan horses, rogue installation programs, file corruption, and security alterations; and changes to auditing settings. As you've seen earlier in this book, changes, additions, and/or deletions are often evidence that a compromise of a system's integrity has occurred.

Detecting the Presence of a Backdoor

Attackers often install backdoors in a system so that they may easily reenter that system later. Hidden logon IDs and passwords may be placed on a system by legitimate hardware or software manufacturers as a way for their technicians to gain access for repairs or maintenance. Hackers sometimes use these hidden logon IDs and passwords or use Trojan horses to establish illegal and unauthorized logon IDs and passwords on computer systems. While backdoors can be installed for accessing a variety of services, those that provide interactive access are of particular interest concerning network security.

The backdoor for most intruders provides three main functions:

1. Getting back into the system with the least amount of visibility. Most backdoors provide a way to avoid being logged, and many times a machine may appear to have no one online even while an intruder is using it.
2. Getting back into a machine even if the administrator tries to secure it (for example, by changing all the passwords).
3. Permitting the hacker to regain entry into the system in the least amount of time. Most intruders seek to get back into the machine easily, without having to redo all the work of exploiting a hole to gain access.

Using a backdoor to reenter a system is a popular technique used by hackers. Because backdoor tools are available at hacker Web sites, even juvenile hackers use them to gain entry. Using a backdoor is a threat to information infrastructure and a crime that the U.S. government takes seriously. How the government considers that threat is evidenced by the following U.S. Department of Justice press release:

> September 21, 2000
>
> **JUVENILE COMPUTER HACKER SENTENCED TO SIX MONTHS IN DETENTION FACILITY**
>
> **Case marks first time a juvenile hacker sentenced to serve time**
>
> WASHINGTON, D.C. — The Justice Department announced today that a 16-year-old from Miami has pleaded guilty and been sentenced to six months in a detention facility for two acts of juvenile delinquency. Under adult statutes, those acts would have been violations of federal wiretap and computer abuse laws for intercepting electronic communications on military computer networks and for illegally obtaining information from NASA computer networks.
>
> "Breaking into someone else's property, whether it is a robbery or a computer intrusion, is a serious crime," said Attorney General Janet Reno. "This case, which marks the first time a juvenile hacker will serve time in a detention facility, shows that we take computer intrusion seriously and are working with our law enforcement partners to aggressively fight this problem."
>
> The juvenile, who is known on the Internet as "c0mrade," admitted today in U.S. District Court in Miami that he was responsible for computer intrusions from August 23, 1999, to October 27, 1999, into a military computer network used by the Defense Threat Reduction Agency (DTRA). DTRA is an agency of the Department of Defense charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons.
>
> In pleading guilty, "c0mrade" also admitted that he gained unauthorized access to a computer server, known as a "router," located in Dulles, Va., and installed a concealed means of access or "backdoor" on the server. The program intercepted more than 3,300 electronic messages to and from DTRA staff. It also intercepted at least 19 user names and passwords of computer accounts of DTRA employees, including at least ten usernames and passwords on military computers.
>
> "The Department of Defense takes seriously any threats against its information infrastructure," said Joseph A. McMillan, Special Agent in Charge of the DOD Mid Atlantic Field Office. "Any segments

> of society, be they adults or juveniles, which are intent on threatening DOD's information infrastructure, should be aware that steps will be taken to identify and thoroughly investigate their activities and seek the necessary judicial actions."
>
> In addition to the computer intrusions at DOD, on June 29 and 30, 1999, "c0mrade" illegally accessed a total of 13 NASA computers located at the Marshall Space Flight Center, Huntsville, Ala., using two different ISPs to originate the attacks. As part of his unauthorized access, he obtained and downloaded proprietary software from NASA valued at approximately $1.7 million. The software supported the International Space Station's (ISS) physical environment, including control of the temperature and humidity within the living space.
>
> As a result of the intrusions and data theft, the NASA computer systems were shut down for 21 days in July 1999. This shutdown resulted in a delivery delay of program software costing NASA approximately $41,000 in contractor labor and computer equipment replacement costs.
>
> In addition to serving six months in a detention facility, as conditions of his guilty plea, "c0mrade" will write letters of apology to the Department of Defense and NASA and has agreed to the public disclosure of information about the case."

As disturbing as the preceding press release is, it doesn't reflect another alarming characteristic of backdoors. Backdoors are, by design, difficult to detect. A common scheme for masking their presence is to run a server for a standard service (such as TELNET, for example) but on an undistinguished port rather than the well-known port associated with the service, or perhaps on a well-known port associated with a different service.

DETECTING BACKDOORS

A good number of backdoors are implemented by a type of malicious code called a Trojan horse. In fact many rootkits contain "Trojanized" versions of commonly used programs and system utilities. Two popular Trojan horse applications are BackOrifice and SubSeven, with both operating as a server on the system they infect. This server opens a backdoor, making access from the outside possible, and this permits the infected system to be accessed by hackers who can then do virtually anything on a system, including stealing or deleting files. Some of the capabilities possessed by backdoor Trojans are listed here:

- ✓ Upload or download files
- ✓ Move, copy, rename, or delete files
- ✓ Erase hard drives and other data disks
- ✓ Execute programs
- ✓ See your screen as you see it
- ✓ Log key presses (even the entry of hidden passwords)
- ✓ Open, close, and move windows
- ✓ Move the mouse cursor
- ✓ See all open connections to and from your computer
- ✓ Close connections

There are numerous backdoor Trojans circulating in the wild. While most are detected by antivirus products, it proves helpful to know a little about each of them. Following is a short list of backdoor Trojans:

- ✓ **BackOrifice/BackOrifice 2000(BO2K).** Back Orifice (or BO2K) is probably the most advanced Trojan in circulation and requires a steep learning curve, making it the most difficult to put in place.
- ✓ **Back Construction.** This very rare backdoor lets the hacker have access to a system's hard disks. It always runs on port 5400, so it is advised that users simply block that port on their firewalls.
- ✓ **Barok.** This Trojan gathers dialup passwords and sends them to the hacker. The simple way to defend against the Barok: Don't select the option "Always remember my password" in password boxes.
- ✓ **Blade Runner.** This sophisticated Trojan is geared more toward the abilities of savvy system crackers as it contains components that are beyond the skills of average hackers.
- ✓ **Cyn.** This particular Trojan is similar in form and features to the SubSeven; however it includes an additional feature that allows a hacker to reset the system CMOS.
- ✓ **Deepthroat.** Deepthroat is a simple-to-use Trojan and has almost as many options as the SubSeven.
- ✓ **Girlfriend.** There isn't much to distinguish this Trojan, as it contains the standard features common to most Trojan backdoors. Most respectable firewalls can block Girlfriend.
- ✓ **Hack'a'Tack.** This easy-to-use and colorful remote-control Trojan is actually quite rare. Since this Trojan always runs on port 31787, it is relatively easy to defend against by just blocking access to port 31787 at the firewall.
- ✓ **SchoolBus.** This common Trojan is powerful despite its simplicity. It even boasts a built-in scanner and operates using port 54321 by default.
- ✓ **SubSeven (a.k.a. Backdoor-G).** With its small learning curve and numerous features, SubSeven is probably the most popular (from the hacker's standpoint) and powerful Trojan horse. The SubSeven Trojan can be configured to inform someone when the computer it has infected connects to the Internet. The hacker (who infected the system with the SubSeven) is then provided with information he or she may use against the system or organization.

Given that backdoors are accessed from a remote location outside an organization's network, detecting them is achieved by monitoring connections to various system ports. Since firewalls are supposed to monitor and limit port activities, they are the natural choice for detecting the presence of a backdoor. However, since Trojan horse applications often masquerade as legitimate applications, using a firewall does not guarantee that the presence of a backdoor will be detected.

Appendix B provides a list of the ports commonly used by rootkits and backdoor Trojans.

Since most reputable antivirus products are able to detect any one of the aforementioned Trojan horse applications, they are considered mandatory for Internet security. Antivirus software is not without faults, however. Most antivirus products rely on users to regularly update their *viral signatures* to aid in the detection of backdoor Trojans (or any malicious code for that matter). Computer viruses are made up of strings of self-replicating code, which is called its binary signature. Antivirus software works by comparing the binary signatures of any incoming files against any *known* viral binary signatures stored in its database in order to determine if that code looks suspect or dangerous.

For more on viral signatures, check out another book I wrote, *Securing the Network from Malicious Code: A Complete Guide to Defending Against Viruses, Worms, and Trojans* (2002, Wiley).

Unfortunately, they sometimes fail to detect new variants for which a signature is not yet available. A more effective means to determine if a Trojan or backdoor has been installed on a system is to gather specific information from the infected system itself. There are several freeware tools that can be employed to collect this information. Here are some personal favorites:

- **Fport.exe.** Fport is a Windows-only utility by Foundstone, Inc. Fport not only reports all open TCP/IP and UDP ports, but also traces them back to the owning application. While this same information could be obtained by using the Windows `netstat -an` command, it goes a step further by tracing those ports to running processes with the process ID, name, and path. Fport can be used to quickly identify unknown open ports and their associated applications. For additional information or to download a copy at no cost, visit `www.foundstone.com`.
- **Superscan.** Also by Foundstone, Inc., SuperScan is a powerful TCP port scanner, pinger, and hostname resolver. This program is extremely fast and versatile and can connect to any open ports discovered using built-in user-specified helper applications.
- **Nmap.** Nmap (Network Mapper) is an open-source utility useful for exploring network connections and security auditing. Nmap determines what hosts are available on the network as well as which ports they are using. Nmap runs on most types of computers using Unix and Linux operating systems. It comes in both console and graphical versions. Nmap is free software, available with full source code under the terms of the GNU General Public License (GPL) at `www.insecure.org/nmap`.

- ✓ **Listdlls.exe.** ListDLLs, a Windows freeware utility by Mark Russinovich, is able to display the full path names of loaded modules — not just their base names. In addition, ListDLLs flag loaded DLLs that have different version numbers than their corresponding on-disk files (which occurs when the file is updated after a program loads the DLL), and can illustrate which DLLs have been relocated because they are not loaded at their base address. This handy utility can be downloaded at `www.sysinternals.com`.

DETECTING BACKDOORS WITH THE NETSTAT COMMAND

The `netstat` command is a useful tool for checking network configuration and activity. By using `netstat`, you can find out which ports on your computer are open, which in turn helps determine if your computer has been infected by a Trojan horse. The `netstat` command lists all the open connections to and from your PC.

Unix, Linux, and Windows all support the `netstat` command. To use it under Windows, open a command (DOS) prompt and enter the command **`netstat -a`**, which lists all open connections going to and from your PC. If you discover any connection that you don't recognize, you need to track down the process that is using that connection. You can use a handy freeware program called TCPView to do this. TCPView is a Windows program that provides detailed listings of all TCP and UDP endpoints (for example, clients, servers, and so on) on your system, including the local and remote addresses and the state of TCP connections.

On Windows NT, 2000, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides additional information than can be achieved when using the built-in netstat program that comes with Windows. TCPView can be downloaded at `www.sysinternals.com`. As with Windows, under Unix or Linux when you execute the `netstat -a` command, you see a listing of all the connections along with their listening ports.

Removing Rootkits and Trojans

Once it's been discovered that a computer is infected by a rootkit or backdoor Trojan, removal of the offending program is the next logical step. Due to the flood of rootkits and backdoor Trojans in the wild, it is impossible to list the removal procedures for them all; however, the general guidelines for removal are as follows.

The steps necessary for removing a Trojan:

1. Identify the Trojan horse file on your system hard disk.
2. Find out how it is being initiated (for example, via Registry, Startup Folder, and so on) and take the action(s) necessary to prevent it from being restarted after a reboot.
3. Reboot your machine and delete the Trojan horse.

The basic steps involved in recovering from a rootkit are:

1. Isolate the affected machine. (Disconnect it from the network and/or Internet.)
2. Determine the severity of the compromise. (Are other networked computers also infected?)
3. Begin the cleanup by reinstalling the operating system and applications from a trusted (clean) backup.

> **tip**
>
> Oftentimes, backdoor Trojans can be detected by simply updating your antivirus software signatures.

Detecting and Defending Against Network Sniffers

A network packet sniffer is a utility that monitors and logs network activity to a file by sniffing traffic but without modifying the network's packets in any way. In the early days of computing, sniffers were hardware devices that were physically connected to the network. Now sniffing is done by software, bringing network sniffing to anyone who wishes to perform this task. Hacker Web sites are rife with sniffers that manage to run on any OS platform. In fact, it is common for a hacker or cracker to employ a network sniffer to capture usernames and password data, which is passed unencrypted (in cleartext, a plain ASCII format that can be read in Notepad, for example) over the network.

Unfortunately, nearly every rootkit includes utilities for sniffing network traffic. One disturbingly powerful aspect of packet sniffers is their ability to place the hosting machine's network adapter into *promiscuous mode*. Network adapters running in promiscuous mode receive not only the data directed to the machine hosting the sniffing software, but also *all* other data traffic on the physically connected local network. This capability allows packet sniffers to be used as potent spying tools.

Detecting network sniffers is tricky but not impossible. Under Unix and Linux, the `ifconfig` command allows the privileged administrator (superuser) to determine whether any interfaces are in promiscuous mode. Any interface running in promiscuous mode is listening to all network traffic, a key indicator that a network sniffer is being used. To check your interfaces using `ifconfig`, just type **`ifconfig -a`** and look for the string `PROMISC`. If this string is present, your interface is in promiscuous mode, and you need to probe further, using built-in tools such as the `ps` utility to identify the offending process. For Windows-based systems, a handy freeware tool called PromiscDetect can be used to quickly detect any adapters running in promiscuous mode. PromiscDetect is a command-line tool that can be downloaded at `www.ntsecurity.nu/toolbox/promiscdetect/` and works on Windows NT 4.0-, 2000-, and XP-based systems.

In light of the fact that a promiscuous sniffer can only sniff the data traffic being shared on its segment of the local area network, promiscuous sniffing can be prevented by using network switches rather than standard network hubs.

A standard Ethernet hub operates by retransmitting any data it receives to all computers also connected to the hub. In such an environment packets meant for one machine are received by all the other machines, as well. This is different from a switch that can identify the specific computer on the LAN segment for which any received data is destined. A switch retransmits any received data only on the LAN segment containing the intended receiver. In other words, a switch is an "intelligent" device that sends packets to the destined computer only and does not broadcast it to all the machines on the network, as is done on Ethernet hubs. When switches are used instead of hubs, each machine occupies its own LAN segment, and that segment only carries data traffic intended for that machine. Such LAN segmentation renders promiscuous-mode packet sniffers completely ineffective in cases where the sniffer is not connected to the same network.

Chapter Summary

Because the cyber threats that come from individuals and malicious code are constantly changing, organizations need to alter the way they approach the protection of their networks. Unfortunately, security training is frequently focused on the more localized and basic security issues and not on the response to outside threats, such as hackers and malicious coders. Rootkits are one of the tools used by intruders to hide and secure their presence on your system, and backdoors, one of the components of a rootkit, are used by hackers to regain entry into a system. Often, an intruder achieves complete cloaking capability by relying on an administrator to trust the output of various system programs. For example, when a rootkit is properly installed, the administrator will not be able to tell the difference between the original and the modified versions, making them difficult to detect. This chapter focused on the tools, techniques, and basic methodologies that can be used by system administrators to detect the presence of rootkits, backdoors, and network sniffers.

Key points covered in this chapter include

- ✓ The role of system processes and their importance in detecting hidden programs
- ✓ How to detect unusual and hidden files, which are often the sign of a system compromise
- ✓ The tools and techniques for detecting and eliminating rootkits and backdoors
- ✓ The threats posed by network sniffers and how to detect and eliminate them

Chapter 6

Retrieving and Analyzing Clues

In This Chapter

- ✓ Performing keyword searches to develop evidence
- ✓ Locating and examining the Windows swap file for evidence
- ✓ Locating and retrieving e-mail evidence
- ✓ Recovering evidence from Web browser cache
- ✓ Viewing the Web browser history
- ✓ The importance of Windows print spooler files or enhanced metafiles (EMF)
- ✓ Locating hidden data and passwords on computers

IN THE PAST, THE VAST MAJORITY OF CRIMES WERE SOLVED USING EVIDENCE, such as fingerprints, footprints, paper documents, and other tangible items, extracted from the crime scene. While these types of evidence continue to provide law enforcement with important facts, technology has now added another element for examination: digital evidence. More information can sometimes be gained from the analysis of a computer and its contents than from a fingerprint. As in the case of the Sharon Guthrie murder mentioned in the Introduction of this book, sometimes the story of a crime may be told through the recovery of files forgotten or thought to have been deleted. Fortunately, law enforcement and legal professionals are quickly beginning to recognize that computer forensics provides vital evidence and may possibly hold the key to solving certain crimes. With a greater importance now being placed on digital evidence, it has become crucial that the evidence be handled and examined properly.

As computers become more widespread in the corporate environment, employers must safeguard critical business information. A major concern today is the possibility that data could be damaged, destroyed, or stolen by a disgruntled employee. If there is a computer at the crime scene, there is a good chance that valuable evidence is stored on that computer. An ever-growing proportion of criminal activity, including white-collar crime, is being committed with the aid of computers. There is no doubt that the collection of evidence is both a time-consuming and complex process. This chapter centers on the tools and procedures for retrieving and analyzing digital clues.

note

Before conducting a search of any computer, you should first review the legal procedures for searching and seizing computers and obtaining electronic evidence. In the U.S. this can be found at `www.cybercrime.gov`. Without proper training, you may inadvertently destroy critical evidence. In addition, you may also be held criminally or civilly liable for your actions if you do the search without proper authority.

Performing Keyword Searches

Analysis of data involves a variety of techniques. One method used to uncover targeted information is the keyword search. For example, a computer forensic investigation is sometimes performed to try to determine if a specific computer has been used to post inappropriate or offensive messages. This review may include re-creating an employee's Internet usage, recovering deleted Internet files, and performing keyword searches for information that appears in the offending messages. These methods can be effective even when the individual has made an attempt to cover his or her electronic tracks. Keyword searches are used for the following purposes:

- ✓ To locate occurrences of words or strings of text in data stored in files or slack and unallocated file space
- ✓ Internal audits to identify violations of corporate policy
- ✓ To find evidence in corporate, civil, and criminal investigations, which involve computer-related evidence
- ✓ To find embedded text in formatted word-processing documents or fragments of such documents

Due to the enormous size of the modern hard disk, it is exceedingly difficult to manually assess every file stored on the drive. Consequently, forensic text search tools are available to help quickly and easily ferret out relevant evidence. Using automated software, keywords can be used in the search of all types of computer storage media including hard-disk drives, floppy/removable disks, and CD-RW discs. When performing a keyword search, the word list should be kept as short as possible and using common words or words that are a part of other words should be avoided. In such cases, the words should be surrounded with spaces. For example, the word "copyright" is embedded in virtually every executable file within Windows. If you search on it, you will get literally thousands of hits.

Industrial Strength Keyword-Searching Programs

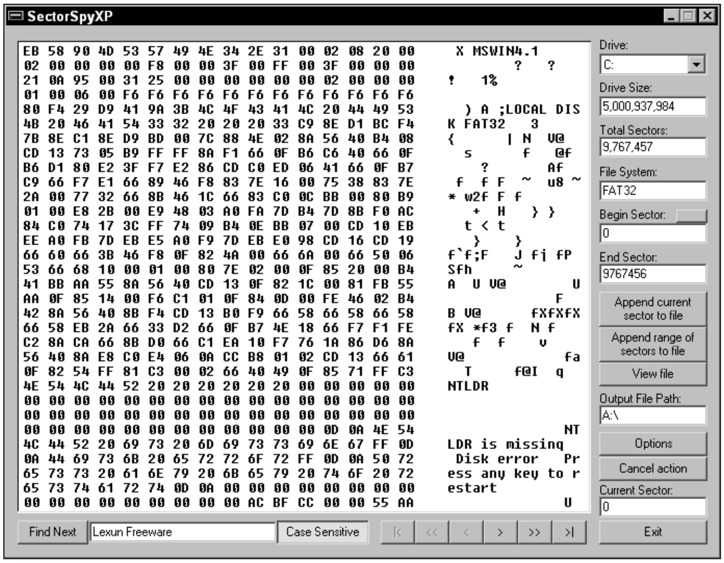
There are several programs available for Unix, Linux, and Windows that automate the task of a keyword search. Unfortunately, the commercial versions of these products are somewhat expensive and often include numerous other features (forensic suite) in addition to their ability to perform basic keyword searches. Here are some examples:

- ✓ **The Forensic Toolkit** by AccessData Corporation ($595)
- ✓ **Encase** by Guidance Software, Inc. ($1,995–$2,495)
- ✓ **Maresware Suite** by Mares and Company, LLC ($325–$950)

Freeware Keyword Search Tools

Luckily, there are several powerful freeware utilities that will suffice for the vast majority of organizations or individuals who carry out the task of a forensic keyword search. While they don't contain some of the additional features of the commercial versions, when they are combined with some of the other forensic freeware tools mentioned throughout this book, they help to quickly build a powerful toolkit that can collect and preserve potential digital evidence. Here are three of my personal favorites for the Windows platform:

- ✓ **BinText** by Foundstone, Inc. (currently in Version 3.0) is a small, fast, and powerful text extractor. BinText can extract text from any kind of file, such as plain text, Unicode, and resource strings. In addition, this handy utility provides both detailed information for each item by using an optional (advanced) view mode and keyword filtering to help prevent any unwanted text from being listed. The gathered list can be searched and saved to a separate file either as a plain text file or in a tabular format. For more information or to download a copy, visit `www.foundstone.com`.
- ✓ **Disk Investigator** by Kevin Soloway (`www.theabsolute.net/sware/`) is another forensic freeware utility than can gather a variety of information from a user's hard disk. Disk Investigator helps discover all that is "hidden" on a computer hard disk, aids in locating sensitive data with search-viewing functions, and displays the drive's true contents. By bypassing the operating system and directly reading raw drive sectors, Disk Investigator helps the user search files and clusters for specific keywords or content.
- ✓ **SectorSpyXP** by Nick McCamy of Lexun Freeware (see Figure 6-1) is a powerful computer forensic tool that can be used by law enforcement or anyone wishing to search for and retrieve evidence left on computer hard drives and diskettes. While not as powerful or flexible as EnCase (the leading tool for such purposes), SectorSpyXP is still quite powerful and *free.* SectorSpyXP examines all data on a hard drive or diskette at the sector level and even contains detailed documentation on how to use it to perform a keyword search to find and retrieve incriminating evidence. It can be used to retrieve lost information, text that has been deleted and removed from the Recycle Bin, and even information not found by other file-retrieval programs. This program works on Windows 2000 and XP operating systems. For additional information about SectorSpyXP, including links to Web sites where you may download a copy, visit `http://home.carolina.rr.com/lexunfreeware`.



```
EB 58 90 4D 53 57 49 4E 34 2E 31 00 02 08 20 00     X MSWIN4.1
02 00 00 00 00 F8 00 00 3F 00 FF 00 3F 00 00 00            ?   ?
21 0A 95 00 31 25 00 00 00 00 00 00 02 00 00 00    !   1%
01 00 06 00 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6 F6
80 F4 29 D9 41 9A 3B 4C 4F 43 41 4C 20 44 49 53      ) A ;LOCAL DIS
4B 20 46 41 54 33 32 20 20 20 33 C9 8E D1 BC F4    K FAT32   3
7B 8E C1 8E D9 BD 00 7C 88 4E 02 8A 56 40 B4 08    {       | N  V@
CD 13 73 05 B9 FF FF 8A F1 66 0F B6 C6 40 66 0F      s      f   @f
B6 D1 80 E2 3F F7 E2 86 CD C0 ED 06 41 66 0F B7        ?        Af
C9 66 F7 E1 66 89 46 F8 83 7E 16 00 75 38 83 7E     f   f F   ~  u8 ~
2A 00 77 32 66 8B 46 1C 66 83 C0 0C BB 00 80 B9    * w2f F f
01 00 E8 2B 00 E9 48 03 A0 FA 7D B4 7D 8B F0 AC       +  H    } }
84 C0 74 17 3C FF 74 09 B4 0E BB 07 00 CD 10 EB      t < t
EE A0 FB 7D EB E5 A0 F9 7D EB E0 98 CD 16 CD 19        }     }
66 60 66 3B 46 F8 0F 82 4A 00 66 6A 00 66 50 06    f`f;F    J fj fP
53 66 68 10 00 01 00 80 7E 02 00 0F 85 20 00 B4    Sfh        ~
41 BB AA 55 8A 56 40 CD 13 0F 82 1C 00 81 FB 55    A  U V@          U
AA 0F 85 14 00 F6 C1 01 0F 84 0D 00 FE 46 02 B4                    F
42 8A 56 40 8B F4 CD 13 B0 F9 66 58 66 58 66 58    B V@       fXfXfX
66 58 EB 2A 66 33 D2 66 0F B7 4E 18 66 F7 F1 FE    fX *f3 f   N f
C2 8A CA 66 8B D0 66 C1 EA 10 F7 76 1A 86 D6 8A       f  f     v
56 40 8A E8 C0 E4 06 0A CC B8 01 02 CD 13 66 61    V@                fa
0F 82 54 FF 81 C3 00 02 66 40 49 0F 85 71 FF C3       T      f@I   q
4E 54 4C 44 52 20 20 20 20 20 20 00 00 00 00 00    NTLDR
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 0D 0A 4E 54                  NT
4C 44 52 20 69 73 20 6D 69 73 73 69 6E 67 FF 0D    LDR is missing
0A 44 69 73 6B 20 65 72 72 6F 72 FF 0D 0A 50 72     Disk error   Pr
65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 72    ess any key to r
65 73 74 61 72 74 0D 0A 00 00 00 00 00 00 00 00    estart
00 00 00 00 00 00 00 00 00 AC BF CC 00 00 55 AA                   U
```

Drive: C:

Drive Size: 5,000,937,984

Total Sectors: 9,767,457

File System: FAT32

Begin Sector: 0

End Sector: 9767456

Output File Path: A:\

Current Sector: 0

Find Next: Lexun Freeware

Figure 6-1: SectorSpyXP

Using SectorSpyXP to Perform a Keyword Search

SectorSpyXP retrieves information and writes it to a text file called the evidence file (or the data recovery file for those not using the program forensically). The name of the evidence file is always SectorSpyXP.txt and is written to a drive A disk (floppy disk) as the default.

You do not have to write to the floppy disk, however. If you are analyzing a floppy disk in drive A, then you must write the data to another drive. Alternatively, you may not be concerned with contaminating the hard drives you are working with, in which case you could write to the hard drives instead of to a diskette.

When SectorSpyXP is launched, it immediately looks on drive A for a disk with a key on it. If a disk is not found or the key is not found, SectorSpyXP assumes you want the evidence file to be written to drive A. If you do not want to write to a floppy diskette in drive A, follow the directions in the following section.

WRITING THE EVIDENCE FILE TO A LOCATION OTHER THAN DRIVE A

To write the evidence files to a location other than a disk on drive A, you must create a simple text file (it must be called SectorSpyXPFilePath.txt) that contains the path name for the location where you would like the evidence file to be written. This is the key that SectorSpyXP seeks when it is launched. Follow these simple steps:

1. Create a text file called SectorSpyXPFilePath.txt.
2. On the first line, type the full path name for the location where you would like the evidence files to be written. *Example 1:* If you want the file to be located in the root directory of drive D, you would type `D:\`. *Example 2:* If you want the file to be located in `D:\My Evidence File`, you would type **`D:\My Evidence File\`**.

3. Always remember to put the last \ at the end of the path name.
4. Do not include the name of the text file.
5. Save the file and copy it to a floppy disk.
6. Make sure the floppy disk is inserted when you start up SectorSpyXP.
7. You may remove the floppy disk once you've started SectorSpyXP. You cannot change the evidence file path name without restarting SectorSpyXP.

note

If you are analyzing a floppy disk, you do not want to write the evidence file to it. Follow the directions above to write the evidence file to another location. Insert the disk with the SectorSpyXPFilePath.txt key file, and then start up SectorSpyXP. Remove the disk and replace it with the one you wish to analyze.

USING SECTORSPYXP TO SEARCH FOR SPECIFIC INFORMATION

When using SectorSpyXP, there are two methods you can use to search for specific information.

METHOD 1 Type in the text you would like to search for and click the Find Next button (for the example shown in Figure 6-1, the search text is "Lexun Freeware"). Find Next finds the first occurrence of "Lexun Freeware" within a sector, starting at the currently displayed sector, and highlights the text in red. It does not highlight subsequent occurrences of "Lexun Freeware" within the same sector. When you click Find Next again, it looks for the first occurrence of "Lexun Freeware" within the next sector. This avoids having to repeatedly click Find Next when the text "Lexun Freeware" exists many times within a sector. Explained in another way, Find Next seeks the first occurrence of "Lexun Freeware" within the next sector that it encounters and stops looking for "Lexun Freeware" in the current sector once it has found the first occurrence of it. Note that you may search only in the forward direction.

The Case Sensitive button, of course, determines if the search text is case sensitive or not. In our example, the Case Sensitive button is pressed, and searches for "Lexun Freeware" succeed only if any capitalization (or lack thereof) matches exactly. For example, "Lexun freeware" would not be a hit in this example, but it would be if the Case Sensitive button was not pressed.

METHOD 2 A search can be made for a list of keywords that have been entered in a text file by following this procedure:

1. Create a text file called findnextlist.txt, and within that file, type keywords, one per line.
   For example:
   keyword1
   keyword2
   keyword3
2. Place that file where the evidence file will be written.
3. To use the list in searches, type `findnextlist` in the Find Next edit box as described in Method 1.
4. SectorSpyXP stops and displays any one of the keywords it finds.

General Guidelines for Hard Drive Examination

There are several ways to go about searching a suspect's hard drive for incriminating keyword evidence. One method is to leave the hard drive in the suspect's computer and, using a program like BinText or SectorSpy, search the suspected hard drive for certain keywords (evidence). This method is not without its faults, however. Evidence could be erased or altered during the normal boot process of the computer.

While you could boot the computer using a special boot floppy disk or even a bootable CD-ROM, you would then need to purchase one of the more complicated DOS-based forensic utilities like Text Search Plus or DiskSearch Pro by New Technologies, Inc. (`www.forensics-intl.com`) to perform the keyword search. Unfortunately, these utilities are only provided to law enforcement or government personnel. The free, albeit slightly more complicated, alternative is to remove the suspect's hard drive and make a copy or clone by placing that hard drive into another computer with a hard drive or partition big enough to contain an exact clone of the original hard drive.

note

Hard-disk removal is also necessary when a suspect's computer has a boot-sector password initiated in the BIOS, preventing the computer from booting via floppy disk, CD-ROM, or hard disk.

If done properly (as outlined in Chapter 3), the cloned or imaged drive will be a sector-by-sector copy (as mandated by NIST) of the original hard drive. This preserves the state of the original hard drive, while allowing detailed forensic examination of the data contained in the reproduction using either the BinText or SectorSpy programs.

tip

For individuals or organizations wishing to make a fast clone or copy of a hard drive partition for their own personal or an organization's internal purposes, a handy utility called DrvClonerXP is available from Lexun Freeware at `http://home.carolina.rr.com/lexunfreeware`.

Once the copy or clone of a suspect's hard drive has been made, the original should not be touched. Always study the secondary copies. Any changes made to originals affect the outcome of analysis later done to copies. Make sure you don't run any data extraction or copy programs that have the potential to modify the access times of files such as tar (Unix/Linux) and xcopy (DOS/Windows). Finally, be sure to remove any external opportunities for change and in general analyze the evidence only after it's been collected.

x-ref

Collecting and preserving evidence are covered in greater detail in Chapter 7.

Examining the Windows Swap File

The Windows swap file (pagefile under Windows NT/2000/XP) is space on a hard disk reserved for the operating system to do what's called *paging*. Under conditions where the physical memory (RAM) is no longer available (such as when several programs are running at the same time), Windows will take the oldest unused pages (each page consisting of a 4K chunk of data) from memory and move them to virtual memory. Any new data pages from the program you're using can then be kept in physical memory. This process is often referred to as *swapping*, hence the term *swap file*. The swap file is essentially nothing more than a single large file containing perhaps thousands of these pages.

Physical memory is an easy concept to grasp since it's the amount of RAM actually installed on your system. Virtual memory, however, has nothing to do with the amount of physical memory installed but is the amount of memory that the operating system and the applications you're running *perceive* to be available via paging.

The swap file is important when conducting a forensic investigation since a large volume of data can exist within the swap file of which the computer user has no knowledge. Windows swap files can provide the computer forensics specialist with investigative leads that might not otherwise be discovered. Windows swap files can be dynamic (temporary) or permanent, depending on the version of Windows involved and the settings selected by the computer user or system administrator.

Permanent swap files are more important to a computer forensics specialist since their size remains static and they retain their data for longer periods of time than do dynamic swap files. Permanent swap files can hold enormous amounts of data. Because of the vast amounts of data they may contain, they should be sought out early by the computer forensics specialist in any examination (as potential evidence relating to past use of the subject computer). Windows swap files may contain easily recognized data such as credit card numbers, telephone numbers, passwords, and fragments of English language text.

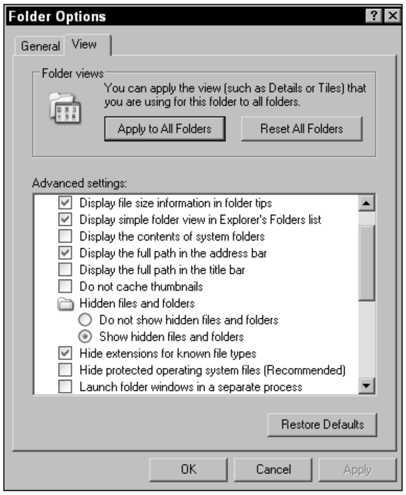
Whenever a computer is run, the potential exists for information in the Windows swap file to be overwritten. The swap file may prove valuable from an evidence perspective since fragments of Windows work sessions may remain in the Windows swap file. The Windows swap file acts as a huge data buffer, and many times entire documents end up in this file. Accordingly, careful analysis of the swap file can result in the discovery of valuable evidence when Windows is involved.

Locating the Windows Swap File

Under most installations of Windows, the default location for the swap file is in the root directory on the drive where Windows is installed, usually in drive C. However, since the Windows OS can be installed in other hard disk partitions (for example, D, E, and so on) and because the swap file may have been moved from its default setting by the user, the exact location of the swap file may vary. As a rule, the swap file is normally located on the root directory of the partition where Windows is installed. Under Windows 95/98/ME the swap file is called win386.swp, and in Windows NT/2000/XP it is called pagefile.sys. If you are unsure of the location of the swap/page file, you can always perform a search for it using the Windows search utility located in the Start menu.

Since pagefile.sys is a hidden system file, you must first make sure that Windows has been set up to view hidden files and not to hide protected operating system files. These options can be found in the Folder Options dialog box (see Figure 6-2) using the procedures that were outlined in

Chapter 5. Once Windows has been set up to view hidden system files, you simply start the Search utility and type the name of the swap file for which you wish to search (for example, `pagefile.sys`) and allow Windows to locate it for you (see Figure 6-3).



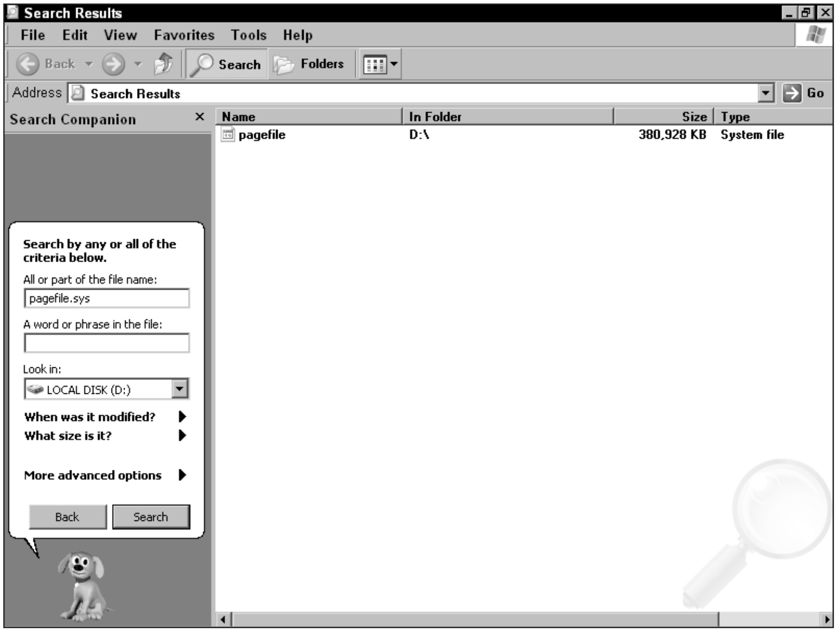
Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- ☑ Display file size information in folder tips
- ☑ Display simple folder view in Explorer's Folders list
- □ Display the contents of system folders
- ☑ Display the full path in the address bar
- □ Display the full path in the title bar
- □ Do not cache thumbnails
- Hidden files and folders
  - ○ Do not show hidden files and folders
  - ● Show hidden files and folders
- ☑ Hide extensions for known file types
- □ Hide protected operating system files (Recommended)
- □ Launch folder windows in a separate process

Figure 6-2: The Windows XP Folder Options box



Name	In Folder	Size	Type
pagefile	D:\	380,928 KB	System file

Search by any or all of the criteria below.

All or part of the file name: pagefile.sys

A word or phrase in the file:

Look in: LOCAL DISK (D:)

Figure 6-3: The Windows XP Search utility

Viewing the Contents of the Swap/Page File

Unfortunately, viewing the contents of a swap/page file is no easy task. The swap/page file is composed of thousands of individual 4K-pages of data. The chief drawback is that you cannot view the contents of the swap file while the operating system is loaded. More importantly, once the computer is rebooted and the OS starts, it deletes the old swap file and allocates a new one because the file is perceived as a *transient* or temporary file. For this reason, a proper image of the hard disk (as described in Chapter 3) must be performed before the suspected computer is rebooted. You can preserve the state of the swap file by first powering down the computer, then rebooting it using a boot floppy disk or bootable CD-ROM. In fact, many of the better forensic suites include utilities for booting the suspected computer without requiring that you load the operating system and compromise the integrity of any potential evidence contained in the swap file.

Swap files can be viewed like any other files with popular software utilities like Norton Commander or Norton DiskEdit or any binary editor. The problem is that swap files can be very large, with some over 200MB in size. In addition, they contain mostly binary information, which is not readable. Looking for leads in the swap file by viewing it with standard binary editing utilities is tedious and will most likely be unfruitful because of the volume of data involved. In order to unravel the contents of the swap files, more productive, specialized tools are needed such as EnCase (`www.guidancesoftware.com`) or Filter_1 by New Technologies, Inc. (`www.forensics-intl.com`) so that the numerous fragments of page file data can be extracted and assembled. Such tools can save significant amounts of time in identifying all sorts of leads from the contents of the Windows swap file. Unfortunately, these tools may be overly expensive for the casual user and may require special training, as well. This makes swap-file analysis better left to trained law enforcement or forensic specialists.

tip

Specific keywords or strings of readable text stored in the Windows Swap File can be located with tools like SectorSpy, as mentioned earlier in this chapter.

E-Mail as Evidence

Before the invention of the telephone, letter writing was the primary means for communication across large geographical distances. Today, people commit a good deal of revealing material to written text in the form of electronic mail (e-mail) messages. Whether the messages involve terrorists, crooked CEOs, or local drug dealers, the overabundance of e-mail messages and electronic files that circulate the globe or become stored in computers represents a treasure trove of evidence for the forensic investigator or law enforcement official.

E-mail messages sent or received on an employer's computer system are subject to discovery and review by law enforcement officials in criminal investigations; however, proper procedures must be carefully followed under the Federal Rules of Evidence. (In fact, much of the evidence that the Justice Department presented to the court with regard to Microsoft's anticompetitive activities was based on intra-company e-mail messages that officials within the company sent to each other.)

When searching for e-mail evidence, the most important rule to remember is that privacy laws still apply, and the legal aspects are complicated. E-mail messages that have not yet been sent may become evidence from a suspect's computer if there are valid grounds to search for them. Incoming e-mail messages, however, are treated in a different manner. They must first be downloaded by the recipient from a mail server (whether located at the ISP or on an organization's local server) before they can be accessed as evidence and used against the recipient. To view or remove them from the mail server *before* the recipient has downloaded them violates federal law, even when a valid reason exists to conduct a search. Federal law strictly prohibits a third party from accessing e-mail messages before they've been downloaded from a server. Conversely, several recent court cases have upheld that checking e-mail *after* transmission is legal, since it is viewed as similar to searching through a file in an employee's drawer.

note

It is strongly advised that you consult with legal counsel before undertaking any search.

x-ref

For more on the Federal Rules of Evidence, see Appendix D.

Locating E-Mail

As we saw in Chapter 4, deleting something doesn't mean it has been permanently erased. When you delete an e-mail message, you're really just telling your computer that the space the e-mail once occupied is now available to be overwritten by new data. However, with hard drive sizes now reaching mammoth proportions, it may take months or even years before deleted data has been completely overwritten by any new data. Even when files are overwritten, fragments of documents can continue to exist (sometimes in several places on a computer) due to fragmentation of the data stored on hard drives.

Fragmentation occurs when a data file changes size and then doesn't fit back into the area of a hard disk from where it was retrieved. When hard drive data has become larger, such as when you add text to a word-processing document, some of it will be saved in its original location while data that does not fit there is saved elsewhere. Therefore, if you do a lot of file creation — copying, deleting, and overwriting — files tend to get divided into pieces in order to fill in all the empty spaces of a hard disk.

The use of e-mail messaging as important (and possibly damning) evidence made worldwide headlines when Kenneth Starr released supporting evidence in his investigation of President Clinton that included deleted e-mail messages retrieved from Monica Lewinsky's computer. Many users continue to think of e-mail messaging as private and secure, as long as it doesn't leave their company's internal communications (or their personal home) network. There have been countless incidents of employees circulating e-mail messages consisting of off-color jokes, racial slurs, defamatory remarks, gender-related remarks, age-related remarks, and other inappropriate content that have subjected them and their employers to liability as a result.

Given the nearly universal use of e-mail messaging as the communication tool of choice within most organizations, it is not surprising that many investigators specifically focus on e-mail during the discovery process. However, e-mail poses the forensic investigator with several challenges.

- ✓ E-mail messages often have attachments, which may also contain vital evidence.
- ✓ E-mail messages can be found in a number of different places, such as the sender's e-mail Inbox/Outbox, on a network server's mailbox, or in backup media.
- ✓ The high volume of e-mail messages often necessitates the use of keywords to focus a review.

Because of these challenges, locating e-mail messages and attachments, if any, for use as evidence depends on whether the e-mail message was sent, received, or deleted. If the message has not been deleted, locating it is of course not difficult. While individual programs vary, most e-mail message programs include the following storage locations:

- ✓ **Inbox.** Storage for e-mail messages once they have been received
- ✓ **Outbox.** Storage for e-mail messages that have been sent to their destination or recipient
- ✓ **Draft.** Storage for unfinished e-mail messages that have not yet been placed in the Outbox for delivery
- ✓ **Sent Messages.** A copy of all messages that have been sent to a recipient, stored by the e-mail client for future reference

Retrieving Deleted E-Mail

It is unfortunate that most organizations treat e-mail messages quite differently than they do other office documents and internal memorandums. Instead of archiving messages, users tend to treat e-mail messages like throw-away Post-It notes that are read and discarded with little afterthought. The majority of e-mail messages are deleted immediately after the recipient has finished reading or responding to them. There is something (a perceived impermanence) about the electronic medium that causes people to make informal comments they would not put to paper. Users tend to be more careless about retaining e-mails simply because they do not think of them as real documents.

Due to the high costs involved in e-mail retention, many organizations fail to archive or back up old e-mail messages. If you suspect a user has recently deleted an incriminating e-mail message, finding that message can be as simple as looking in the deleted e-mail folder within the user's e-mail application. The exact procedure varies depending on which e-mail software is being used. In general, when a user deletes e-mail from his or her e-mail client, you can usually recover it for several days after the deletion occurred. The e-mail message isn't completely deleted but only moved to the Deleted Items folder. Until this folder is permanently emptied, you can move items back from it into your Inbox or any other folder in the Move Items dialog box (see Figure 6-4).

To restore a deleted e-mail message under Outlook or Outlook Express (XP), follow these steps:

1. Start the Outlook or Outlook Express e-mail program.
2. Select the Deleted Items folder (Outlook) or Deleted Items Shortcut (Outlook XP) from the window on the left.
3. Right-click the deleted e-mail message, then select "Move to folder" on the drop-down menu.
4. From the list of folders in the Move Items box, select the folder where you would like the deleted e-mail message to be moved.

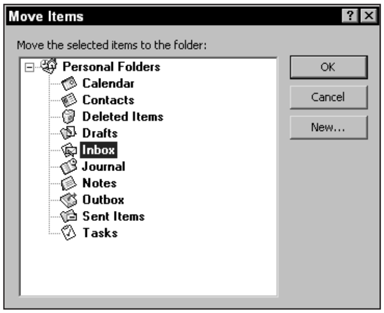


Figure 6-4: The Move Items box in Microsoft Outlook for Windows XP Pro.

note

The ability to retrieve deleted data becomes more complicated once the e-mail message has been permanently deleted. Once this has occurred, you need to use the data recovery procedures outlined in Chapter 4 and/or use programs such as SectorSpy or Disk Investigator to perform a keyword search to attempt to recover any specific e-mail text.

Recovering Evidence from the Web Browser

Most Web browsers store copies of recently visited Web pages. The Web cache is your Web browser's way of saving you time when you download Web pages. Many Internet users appreciate having a fast download of Web pages they visit often, particularly if they use a slower dial-up type of Internet connection. Web browser caching involves storing information viewed from Web pages that might include links, pictures (images), and Web page text on your computer. By storing items in cache, information contained in Web pages that were previously viewed load faster when accessed subsequently, because they have already been loaded once and stored in the browser cache. For example, when a user requests a Web page that he or she has visited before, the browser first looks in the cache; if it finds that page there, it loads the cached page rather than connecting to the Web to download a new one. Web caches reveal a lot about which Web sites a user has visited. Most contemporary Web browsers (for example, Internet Explorer and Netscape Navigator) perform Web caching.

Locating Browser History Evidence

Another way Internet users may inadvertently reveal their surfing habits is via the auto-completion feature found in some of the newer Web browsers. The URL line at the top of the browser contains a drop-down list box of recently visited sites and auto-completes partially entered Web addresses for you. As a user selects a URL or begins to type one in, the URLs visited by the user in the past appear. In addition, most browsers keep a history of all the URLs that a user has browsed. The length of time that files remain in the history can be adjusted by the user. Under Windows XP for example, the default setting places the limit at only the past 20 days; however, this can be modified by the user to as few as 0 days or as long as 99 days. You can trace a user's surfing habits by viewing the browser's history list. Following are the steps for two popular Web browsers.

For Netscape Navigator, follow these steps:

1. Open the Communicator menu.
2. Select Tools, then History.
3. To view a particular Web page, double-click on its line within the list.

tip

You can sort the history list by clicking one of the categories (for example, Location, Title, and so on) in ascending, descending, or alphabetical order.

For Internet Explorer, there are several ways to locate Web sites and pages you've recently viewed. To find recently viewed pages, follow these steps:

1. On the toolbar, click the History button. A History bar appears on the left, containing links for Web sites and pages visited in previous days and weeks.
2. Under the History bar, click on a day or week to expand the list.
3. Select a Web site folder by clicking it; this displays individual pages.
4. Next, click the page icon to display the Web page.

note

The following procedures will only display the history for the currently logged on user and if you boot the computer via the operating system. This will not work if you've mounted the image disk as a secondary hard drive (the recommended method to avoid changing the data during the examination process).

tip

To sort or search the History bar, click the arrow next to the View button at the top of the History bar.

Locating Web Cache Evidence

The Web browser cache contains data that can tell a forensic investigator a lot about a user's surfing habits. For example, in *United States* v. *Tucker*, 150 F.Supp.2d 1263 (D. Utah 2001), a conviction was largely supported by evidence found in the form of Internet cache files that the defendant's browser saved to his hard drive when he viewed them on various Web sites. As stated earlier in this section, all contemporary Web browsers employ a caching scheme to speed up the loading of frequently viewed Web pages. In Netscape Navigator and Internet Explorer, Web pages are stored in a special folder on the user's hard drive; however, Navigator also uses memory (RAM) to further enhance the caching scheme. In Navigator, the user can control both the amount of memory (RAM) allocated to storing pages in memory as well as the location and the amount of hard drive space used for caching. In Explorer you can only adjust the amount of hard disk space. Following are the steps used to manage cache settings for both of these popular browsers.

To manage Netscape Navigator cache settings, follow these steps:

1. Start the Web browser.
2. Select Edit in the Toolbar menu and choose Preferences.
3. Under the Category section on the left-hand side, click the + to expand the Advanced Settings.
4. Click Cache at the top of the Advanced Settings list.
5. You will now see the Cache Management screen, including the location where cache files are to be found on the computer's hard drive.

tip

After determining the exact location of the hard drive cache file, navigate to the cache folder to view its contents or copy the files to a disk for forensic review.

To manage Microsoft Internet Explorer (6.0) cache settings, follow these steps:

1. Start the Web browser.
2. Select Tools on the Explorer toolbar, and then select Internet Options to display the Internet Options screen. (You can also right-click on the Internet Explorer icon in your Start menu and select Properties.)

3. Under the General tab, select the Settings button under Temporary Internet Files. (By default, Explorer stores cached pages on your hard drive in a folder called Temporary Internet Files.)
4. Select View Files to display the contents of the Web cache.

As with many aspects of computer forensics, freeware tools are available that can simplify otherwise complicated tasks. When it comes to the viewing of browser cache files under Windows, one of my favorite freeware tools is CacheMonitor II by David M. Pochron of Enigmatic Software. CacheMonitor displays the contents of the entire browser cache in a convenient list window, including changes to the cached files in the Status column (in the monitor). Another nice feature of this program is that it allows you to easily export the entire contents of the cache (in text format) for preservation to removable media such as a Zip disk or CD-R disc. This handy freeware tool can be downloaded at `www.mindspring.com/~dpoch/enigmatic/cachemonitor2.html` and at several freeware Web sites.

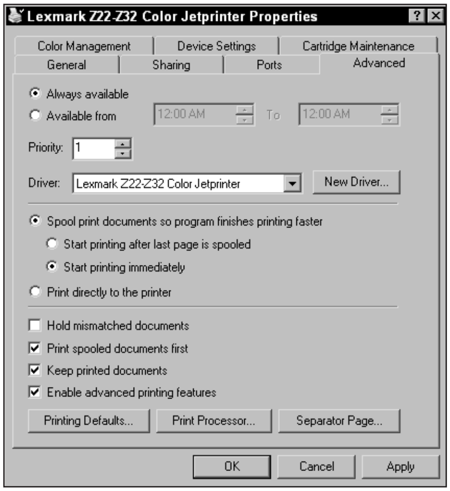
Print Spooler Files

On December 13, 1999, Michael Craig Dickman was taken into custody by the FBI and the San Diego Police Department shortly after the 5:00 p.m. robbery of the Bank of America located in La Jolla. Dickman, a former biotech executive dubbed the Gap-Toothed Bandit by the local media, created demand notes on his word processor by printing the demand notes (without ever saving them as files onto his computer). However, skilled examiners from the San Diego Regional Computer Forensics Laboratory were able to recover the demand notes in the form of deleted EMF files from the hard drive of Dickman’s laptop computer. This evidence played a central role in securing the Gap-Toothed Bandit’s conviction.

Printing under Windows involves a process called “spooling” whereby the OS creates a temporary copy of the file to be printed, known as an enhanced metafile (EMF). Whenever you print a document, Windows first creates a copy of that file (EMF) on the hard disk and then sends that copy to the printer. Even if the user never saves the document, that printer version temporarily resides on the disk. After printing is complete, the EMF files are normally deleted by Windows, a process invisible to the user. Since these are deleted files, you need to follow the procedures and use the tools covered in Chapter 4 to recover them.

Under certain conditions, users may have the Windows print spooler option set to retain and not automatically delete print spool files. The general procedure to determine if Windows XP has been set to retain print spooler files is as follows:

1. Click the Windows Start button and navigate to Printers and Faxes.
2. In Printers and Faxes, right-click on the Printer Icon with the check mark (this is the default printer) and select Properties.
3. If “Keep printed documents” is selected in the Printer Properties screen (see Figure 6-5), then Windows is set to save print spooler files.



Lexmark Z22-Z32 Color Jetprinter Properties

● Always available
○ Available from 12:00 AM To 12:00 AM

Priority: 1

Driver: Lexmark Z22-Z32 Color Jetprinter

● Spool print documents so program finishes printing faster
○ Start printing after last page is spooled
● Start printing immediately
○ Print directly to the printer

□ Hold mismatched documents
☑ Print spooled documents first
☑ Keep printed documents
☑ Enable advanced printing features

Figure 6-5: Retaining print spooler files in the printer's Properties box

Under these circumstances, a simple search of the user's hard drive for *.emf files (using the built-in Windows search utility) will find, display, and even let you copy print spooler EMF files to removable media for preservation and/or later analysis.

Locating Hidden Data

Sometime during a computer crime investigation, a forensic examiner will attempt to uncover files that have been intentionally hidden by a perpetrator. It's easy for criminals to hide cybercrime evidence and other pertinent information within a computer. Letters, spreadsheets, pictures, and other potential evidence can be encrypted, zipped, and/or password-protected using a variety of freeware programs. Cyber criminals have even been known to manipulate file extensions to help disguise a file's true attributes.

Steganography

Steganography is the practice of hiding a message or file within another message or file known as a carrier file. Steganography is a way to hide a message in such a way that anyone can see it but only a select few know what to look for to successfully decode or receive the hidden message. Steganographers can hide a message or image in any one of the following:

- ✓ Another image
- ✓ An audio file
- ✓ A video or movie file

In addition, an audio or video file can be hidden inside another media file such as a large graphic file. Steganography differs from cryptography in that while cryptography works to mask the content of a message, steganography works to mask the very existence of the message itself. Unfortunately, most steganographic methods in use today are invisible to the observer's senses, and there are currently few tools available to the public to detect the use of steganography. If you suspect that a perpetrator has hidden a text file, image, or other content within an image, a handy freeware program does exist that can help you detect if that file is using steganography. The automated tool, Stegdetect, is capable of detecting several different steganographic methods used to embed hidden information in JPEG images. Stegdetect can be found at `www.outguess.org/detection.php` with versions available for Unix/Linux and Windows.

Password-Protected Compressed Data

There are times during an investigation when a computer forensic examiner will come across files that the user has compressed and password-protected. There are numerous reasons this could occur, such as when employees suddenly leave the organization without unprotecting the files they've left behind. Password-protected Zip files are easy to make since there are numerous programs available on the Internet (many are freeware) that allow an individual to compress documents or files. This allows the document or files to take up far less space on the hard drive and even reduces the time it takes to transmit that document across the Internet, a boon to slower Internet connections. Some zipped files can be prepared so that they automatically unzip (decompress) after the user just clicks on the compressed files icon. That way the recipient doesn't need any special software to decompress the file after it is received. In addition, the document or file can have password protection applied to it so that when a user tries to unzip the file, he or she needs to supply the appropriate password or the file does not successfully decompress.

When a document or file is encountered that requires entering a password before it can be decompressed, there are several options. You can call in a company that specializes in password cracking and recovery, or you may attempt to crack the password yourself by using any one of the many commercial or freeware Zip password-cracking utilities available on the Internet.

Two companies that specialize in this burgeoning field are:

- ✓ **Password Crackers, Inc.** (`www.pwcrack.com`)
- ✓ **Discount Password Recovery** (`www.discountpasswordrecovery.com`)

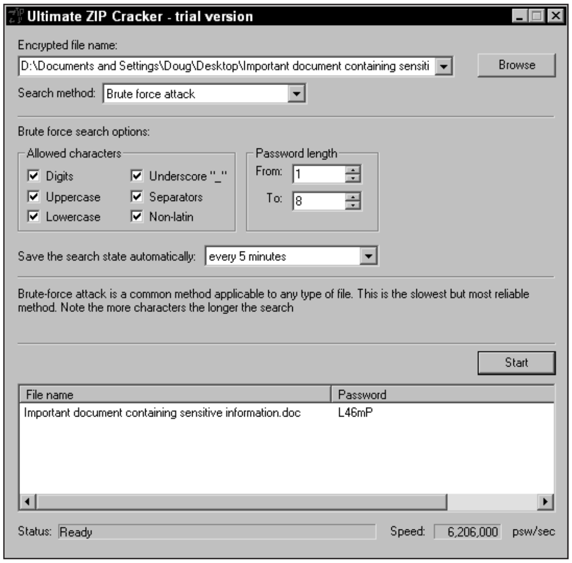
If you wish to try cracking the password yourself, hundreds of shareware/freeware programs are available. The following programs are among the most popular:

- ✓ **ZIP Password Finder** by ASTONSOFT (`www.astonsoft.com`)
- ✓ **Cain & Abel v2.5 beta20 for Windows NT/2000/XP** (`www.oxit.it`)
- ✓ **Ultimate ZIP Cracker** by VDG Software (`www.vdgsoftware.com`)

Example Using Ultimate ZIP Cracker

Let’s say you are performing a forensic examination of a user’s hard disk and encounter a zipped document or even a Word or Excel document that requires a password (to extract and view). Using ZIP Cracker, follow these steps:

1. Start ZIP Cracker by double-clicking the program’s icon.
2. Locate the document or file you wish to have password-recovered (cracked) by using ZIP Cracker’s built-in file browser. In our example, the document is called Introduction.zip and is located on the Desktop. The file is a password-protected zipped Word document (see Figure 6-6) that was compressed using ZipItFast! 2.0, from MicroSmarts Enterprise.
3. The Password Recover Wizard starts and offers a series of suggestions on how to speed up the password recovery procedure. You can either choose to follow the program’s suggestions, or skip them and go directly to cracking the password. In the test, I use the case-sensitive, alphanumeric password “L46mP,” and it took this program just over two minutes to crack it on my PC.



Encrypted file name: D:\Documents and Settings\Doug\Desktop\Important document containing sensiti

Search method: Brute force attack

Brute force search options:

Allowed characters

☑ Digits ☑ Underscore "_"
☑ Uppercase ☑ Separators
☑ Lowercase ☑ Non-latin

Password length

From: 1

To: 8

Save the search state automatically: every 5 minutes

Brute-force attack is a common method applicable to any type of file. This is the slowest but most reliable method. Note the more characters the longer the search

File name	Password
Important document containing sensitive information.doc	L46mP

Status: Ready Speed: 6,206,000 psw/sec

Figure 6-6: Using ZIP Cracker to bypass a password

One important point to remember is that password cracking can be a time-consuming endeavor, particularly if the passwords are over five characters in length. Some criminals follow the rules of strong passwords by using a mixture of upper- and lowercase letters as well as alphanumeric characters. Companies that specialize in password recovery have powerful computers that use sophisticated software and can usually recover a password in a fraction of the time that one could with any one of these freeware/shareware programs.

Chapter Summary

Computer forensics frequently involves the use of computer technology to uncover electronic evidence. The ability to retrieve sought-after information is increasingly important, as many business and financial records now exist only in electronic format. Using computer forensic tools and techniques, an investigator can uncover many different types of data, even password-protected documents and deleted files, hidden on computers. Electronic discovery involves analyzing a suspect's computer systems and storage media to locate such evidence as old e-mail messages, hidden files, and deleted files and documents. Computer forensic investigators also can break passwords as part of their investigations. The key is being able to gain access to the necessary electronic media and having the know-how to uncover the relevant evidence once you have the equipment.

Key points covered in this chapter include

- ✓ Understanding the tools and techniques for performing a keyword search
- ✓ The relevance of the Windows swap file when conducting a forensic investigation
- ✓ How to locate and preserve e-mail evidence
- ✓ How to recover data from a Web browser cache
- ✓ How to review and preserve Web browser history files
- ✓ How to extract information from print spooler files even when documents were not saved by the user
- ✓ How to locate and recover hidden and password-protected data

Chapter 7

Procedures for Collecting and Preserving Evidence

In This Chapter

- ✓ Collecting evidence after system compromise
- ✓ Understanding volatility of evidence
- ✓ Creating a real mode boot disk
- ✓ Using packet sniffers to gather evidence
- ✓ Building a forensic toolkit
- ✓ Following the chain of custody
- ✓ The admissibility of evidence

IT IS IMPORTANT TO REMEMBER ONE OF THE BASIC PRINCIPLES OF THE U.S. LEGAL SYSTEM; that without evidence of a crime, there is no crime. Actions taken at the crime scene at the onset of an investigation may play a critical role in the resolution of a case. Careful, thorough investigation is critical to ensure that potential physical evidence is not tainted or destroyed or that possible witnesses are not overlooked. It is of paramount importance that utmost care is taken in the collection and preservation of evidence.

Incident investigations are carried out to discover the cause(s) of an incident. If the investigation is done soundly, it points out crucial information for preventing the event from happening again. To achieve this, investigators must maintain the skills and knowledge to plan and conduct an effective investigation. Even under the best of circumstances, evidence may be difficult to collect. When the evidence is in electronic format, the investigator faces another layer of complexity; such evidence has none of the permanence of conventional evidence and is even more difficult to form into easily explainable evidence. This chapter focuses on the basic procedures of evidence collection and preservation.

Postcompromise Evidence Collection

Electronic evidence may be costly to collect in terms of both man-hours and system downtime. The processes can be time-consuming and complicated. Affected systems may be unavailable for normal use for an extended time while analysis and data collection is performed. There are two simple reasons for this: accountability and prevention. The attacker is responsible for the damage done, and the only way to bring him or her to justice or to seek remuneration is with adequate evidence to demonstrate that the attack was the result of his or her action.

The victim, on the other hand, has a responsibility to the general public. Information gathered after a compromise can be examined and used by others to prevent further attacks. Victims may also have a legal obligation to perform an analysis of evidence collected, for instance if the attack on their system was part of a larger attack committed against several different companies' systems. When the time arrives to begin the collection of evidence, the first rule that must be followed is to not hurry. Anxiety levels are certain to be high, and a knee-jerk reaction will cause people to look for answers as rapidly as possible. However, if the investigator rushes through the data collection procedures, evidence may be overlooked, tainted, or lost. A mistake in collecting and preserving the evidence is often irreversible.

Legal Requirements for Collecting Electronic Evidence

When collecting evidence after a crime has been committed, certain legal constraints must be followed if evidence is to be admissible in a court of law. As these requirements are vast, complex, and vary from country to country, it is beyond the scope of this book to elucidate them all; however, this chapter covers those that are common to most investigations.

An obstacle to be overcome when collecting evidence is maintaining the privacy rights of system users. Users of corporate networks forfeit their rights to privacy when the organization or system administrator institutes use of a logon banner on their network. The logon banner establishes that user activities will be monitored for the duration of time that they use the system. The banner cautions users that should they be found to have acted in violation of the organization's security policy while using the network, they will be subject to legal action. When the organization has not incorporated such a banner, stipulating the organization's expectations of users, prosecuting even known transgressions may be impossible. Guilty defendants have been cleared of charges simply because they had been given no overt notice of the organization's prohibition of improper system/network usage. On the other hand, the user's right to privacy has led some individuals who have been monitored *without being given prior notice* to make legal claims against their employers.

Installing a logon banner for Windows NT 4.0 can be accomplished using the REGEDIT program. Implementing a logon message involves editing two related keys. Remember, editing the Registry involves some risk. It is best to first back up the Registry using the Registry backup procedures covered in Chapter 4.

To edit the keys in NT 4.0, do the following:

1. Run Registry Editor (Regedt32.exe).
2. Go to the following key in the Registry: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`.
3. Edit the Value Name by typing **LegalNoticeCaption**. (This contains the caption text for the dialog box, which will be presented to the user.)
4. Edit the Value Name by typing **LegalNoticeText**. (This contains the text, which will appear within the dialog box.)
5. Exit the Registry Editor and restart the computer for the change to take effect.

Windows 2000/XP does not use the LegalNoticeCaption or LegalNoticeText Registry settings. Instead, you need to use the Local Security Policy console to set a legal notice as shown in the following steps:

1. Click Start, then Settings, then Control Panel.
2. Double-click on Performance and Maintenance (XP only), then Administrative Tools, Local Security Settings, Local Policies, and Security Options.
3. Set Message text to be seen by users attempting to log on.
4. Set Message title for users attempting to log on under Interactive Logon.
5. Log off then log back on to test.

Unix/Linux Login Banners

The logon banners for Unix/Linux operating systems vary depending on the particular version being used. For many contemporary systems (for example, Sun or Linux), creating the file `/etc/issue` in the root directory containing the banner text causes the banner text to be displayed before the console login and before all interactive logins, such as `telnet`, `rsh`, and `rlogin`. The `/etc/issue` file is a plain-text file used in Unix and Linux in order to insert information about the system and have that information displayed at user logon. Since it is a plain-text file, it can also be used to create a logon banner and can be customized to your own taste. Linux systems use two such files, `/etc/issue` for console logins and `/etc/issue.net` for `telnet` logins, so be sure to place the banner text in both.

For other Linux systems (that do not respond to the `/etc/issue` file), put the banner text in the file `/etc/motd`. The contents of this file are displayed by the global `/etc/.login` and the `/etc/profile` files, depending on which shell you start (`sh` or `csh`), immediately after a successful login. Displaying the `/etc/motd` file immediately after login is also an option for the Secure Shell daemon (`sshd`), and this can be set in the `/usr/local/etc/sshd` config file. For machines that do not use any of these methods for displaying banners, consult the manual pages for each service to see if there is a banner mechanism available.

When creating a logon banner, care must be taken when formulating its text. The banner must be correctly worded in order to be valid. The following is a U.S. Department of Justice–approved sample message that can be used in a logon banner:

```
**WARNING**WARNING**WARNING**WARNING**WARNING**WARNING
This is a {Organization Name Here} computer system, which may be accessed and
used only for business by authorized personnel. Unauthorized access or use of
this computer system may subject violators to criminal, civil, and/or
administrative action.
Any information on this computer system may be intercepted, recorded, read,
copied, and disclosed by and to authorized personnel for official purposes,
including criminal investigations. Access or use of this computer system by
any person, whether authorized or unauthorized, constitutes consent to these
terms.
**WARNING**WARNING**WARNING**WARNING**WARNING**WARNING
```

Expectation of privacy is not based upon specific facts and circumstances, but upon whether the expectation of privacy is one which society in general recognizes. Policies of the organization may remove any expectation of privacy. For example, if the organization's workplace policy states that an employee's desk (or computer) can be searched at any time or if a copy of the key to the desk is kept by management, then there is no reasonable expectation of privacy.

An employer-issued computer is a part of the workplace because, although it is primarily used by the employee, it is owned and under the control of the employer. The computer remains part of the workplace even when the employee has placed personal information on it and also when the employee's employment is terminated. Although the employee may have some degree of expectation of privacy, a public employer may search the contents of an employee's computer without a warrant when confronted with an alleged violation of its Acceptable Usage Policy (AUP) provided the search is reasonable at its inception and in its scope, and it is work-related. When a workplace search is not work-related, any attempt to acquire evidence of criminal activity or a search of an employee's personal property at the workplace without consent requires a warrant.

The Fourth Amendment to the U.S. Constitution governs the issue of privacy. One pivotal court case that addresses the issue of workplace privacy is *O'Connor* v. *Ortega*, 480 U.S. 709 (1987) in which the United States Supreme Court held that the public employer's search of the employee's office was reasonable at its inception because its purpose was to find evidence of the employee's alleged misconduct and to retrieve work-related materials. As an employee of a state hospital, Dr. Ortega had the primary responsibility of training physicians in the psychiatric residency program. Hospital officials became worried about a lack of decorum in his management of the program, mainly due to charges against him concerning sexual harassment of female hospital employees and inappropriate disciplinary action against a resident. Pending an investigation of these complaints, Dr. Ortega was placed on administrative leave. While on leave, hospital officials searched his office and seized personal items from his desk and file cabinets that were later used in administrative proceedings resulting in his discharge from the hospital. Dr. Ortega filed an action against hospital officials in Federal District Court under 42 U.S.C. 1983, alleging that the search of his office violated the Fourth Amendment. The Hospital maintained the search was justified in order to protect state property and to investigate charges of Dr. Ortega's misconduct. Dr. Ortega argued the search violated his Fourth Amendment rights, as it was an attempt to discover and collect evidence to be used against him in an administrative proceeding.

Furthermore, Justice O'Connor, joined by Chief Justice Rehnquist, Justice White, and Justice Powell, concluded that:

> Searches and seizures by government employers or supervisors of the private property of their employees are subject to Fourth Amendment restraints. An expectation of privacy in one's place of work is based upon societal expectations that have deep roots in the history of the Amendment. However, the operational realities of the workplace may make some public employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. Because the record does not reveal the extent to which hospital officials may have had work-related reasons to enter respondent's office, the Court of Appeals should have remanded the matter to the District Court for its further determination. However, a majority of this Court agrees with the determination of the Court of Appeals that respondent had a reasonable expectation of privacy in his

> office. Regardless of any expectation of privacy in the office itself, the undisputed evidence supports the conclusion that respondent had a reasonable expectation of privacy at least in his desk and file cabinets.

Once you are certain that all legal procedures have been adequately covered, the next step is to actually collect the evidence. Following are general steps that should be followed for evidence collection:

note

The 4th Amendment constraints apply only to government organizations and their agents. There is no 4th Amendment restriction on private organizations. They may, however, be governed by state or local privacy laws. Expectation of privacy is a concept that applies (in the legal sense) only to 4th Amendment issues.

The Order of Collection

If evidence collection is done correctly and in an orderly fashion, it is much more useful in apprehending the attacker and as such stands a much greater chance of being admissible in the event of a prosecution. Collection order should be conducted following these basic steps:

1. **Find the evidence.** Figure out where the evidence you are seeking is being stored on the system. Making a checklist can help you in the collection process, and you can use it to double-check that everything you are looking for is there.
2. **Determine data relevance.** As you uncover evidence, you must decide what parts of it are relevant to the case at hand. To be safe, you should overcollect rather than exclude possible evidence. Keep in mind, however, that you need to work fast; don't waste time collecting information that will be of no use to your case.
3. **Rank volatility.** Once you've determined which items to collect, you must decide in which order to gather them. The main determining factor is that items that are most likely to be volatile (those items that can degrade or become unusable) should be collected first. Using and sticking to the order once you've established it ensures that the loss of usable (for example, uncorrupted) evidence remains minimal. Begin with the items you've ranked as most volatile and follow with those categorized as less so. (Volatility is explored in more detail in the next section.)
4. **Eliminate outside interference.** It is crucial that you avoid altering original data because it is far easier to prevent tampering than it is to rectify the consequences of tampering. As only unaltered data may be entered as evidence, utmost care must be taken to thwart any possible outside contamination. Knowledgeable attackers have been known to install a *dead-man switch*, which can delete evidence once a computer is disconnected from the network or from the Internet.
5. **Collect the evidence.** You may now begin the collection process. Use all the tools you have available for this task. As you gather evidence, continue to examine the items

you've already collected, as new pieces you collect may influence what you consider worthy information. You may come to realize that you've overlooked something. Now is the time to get it.

6. **Document everything.** Your method of collecting the evidence you present may be called into question later, so be sure to maintain a record of everything that you've done in the collection process. Timestamps, digital signatures, and signed statements will serve you well later; include all the substantiation you can.

Understanding Volatility of Evidence

In order to solve a computer crime or system breach effectively, you need to examine the system more as a detective than as a computer user. Solving computer crimes has much in common with its physical crime-solving counterpart. You generally don't have a lot of time to solve a mystery. Evidence vanishes over time, either as the result of normal system activity or as the result of acts by users. Likewise, every step that *you* take may destroy information, so whatever steps you take must be right the first time, or valuable information can be lost. As stated earlier, you must uphold the Fourth Amendment's protection of a user's right to privacy. It is imperative that you do not collect information in areas that you do not normally have reason to access (such as personal files) unless you have notified the user (for example, via a logon banner) that all information stored on the computer is subject to seizure at all times or if you have sufficient reason to believe that a valid security incident is occurring or has occurred.

In general, computer evidence needs to be

- ✓ **Admissible.** The evidence must conform to certain legal rules before it can be put before a court. This is covered later in this chapter.
- ✓ **Authentic.** It must be possible to positively tie the evidentiary material to the incident by showing that the evidence relates to the incident in a relevant way.
- ✓ **Complete.** It must tell the whole story and not just one particular perspective. Not only should you collect evidence that can prove the attacker's actions, but also evidence that could prove his or her *innocence*.
- ✓ **Reliable.** There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- ✓ **Believable and understandable.** The evidence must be readily believable and understandable by a court of law. There's no point in presenting the output of a memory dump if a jury will have no idea what it means.

Volatile evidence is evidence that can quickly disappear or is only temporary in nature. This type of evidence needs to be collected before the machine is disconnected from the network and powered down. When collecting evidence you should proceed from the most volatile to the least volatile. The following is an example of the *order of volatility* for a typical system.

- ✓ **Memory** (physical and virtual)
- ✓ **Running Processes** (SPOOLSV.exe, EXPLORER.exe, and so on)
- ✓ **Network State** (connections and anything running in promiscuous mode)
- ✓ **Permanent Storage Systems** (hard disks, floppies, tapes, and CD-RWs/ROMs)

It's all too easy to inadvertently destroy volatile evidence. When you are in the process of collecting volatile evidence, always remember to take the following precautions:

- ✓ Do not power down the system until you have completed all the evidence collection procedures for volatile evidence. Much evidence may be lost when a system is powered down, and the attacker may have altered the startup and shutdown scripts and services to destroy evidence.
- ✓ Don't trust the programs on the system. Intruders have been known to replace system commands. Run your evidence-gathering programs from appropriately protected media (see the next section, "Creating a Real-Mode Forensics Boot Disk").
- ✓ Don't run programs that modify the access time of all files on the system (for example, tar or xcopy).
- ✓ When removing outside interference, keep in mind that simply disconnecting from the network may trigger a dead-man switch that can detect when the computer is disconnected from the network and quickly delete evidence.

Creating a Real-Mode Forensics Boot Disk

When conducting a forensic examination of a Windows-based system, it is best to boot the computer with a controlled boot disk, which can control the initial booting process so that the operating system cannot start writing to the disk. Some operating systems begin writing to the drive during the boot process, changing disk access times and possibly overwriting data that may be pertinent to your case. In fact, the simple act of booting a Windows-based computer will update hundreds of files, leaving potential evidence compromised or destroyed, and therefore no longer available for use as evidence. During a forensic examination, all access of the original storage media is normally performed at a low level, frequently at a real-mode or DOS level. The reason for this as mentioned earlier in this section is that all versions of Windows (Windows 95/98/Me/NT/2000/XP) directly write to any other fixed drive media on a computer during the normal boot process. These writes occur even when the original media is located on a secondary drive on the computer. Most forensic examiners use a real-mode boot disk.

A controlled boot disk boots a computer into real mode. Real mode limits the processor to 1MB of memory and provides no memory management or memory protection features. The phrase is often used to describe device drivers that only operate in this mode. MS-DOS runs in real mode. This is in contrast to protected mode, which lets the PC access the largest possible amount of memory. In protected mode, different parts of memory are assigned to different programs. This way, memory is protected in the sense that only the operating system will allow access to it. All modern-day operating systems operate in this mode. A true real-mode boot disk will start a computer in its most basic state (the DOS level) and does not load any advanced protected mode device drivers. This helps to preserve the state of the operating system. Once loaded via the real-mode boot disk, forensic utilities may then be run in DOS (real) mode to collect evidence.

Many forensic toolkits such as The Forensic Toolkit v2.0 by Foundstone, Inc. (`www.foundstone.com`) are small enough for the entire forensic suite of utilities to be placed on a single boot floppy. After booting a Windows NT machine from the boot floppy disk, appropriate tools can be run directly off the floppy, helping the investigator to collect and preserve evidence.

The Skinny on the FAT

FAT is an abbreviation for File Allocation Table. There are several different types of file allocation tables, such as FAT12, FAT16, FAT32, and NTFS. Each FAT has its own limitations and capabilities. FAT12-formatted disks only recognize DOS partition sizes up to 32MB. Prior to MS-DOS 3.30, this was all that existed. MS-DOS 3.30 through MS-DOS 7.00 supported FAT16, which supports partitions up to 2GB in size. With MS-DOS 7.10 and 8.00, FAT32 support was introduced. FAT32 partitions can be up to 2TB in size. Windows 2000 (NT 5.0) was the first version of Windows to support all versions of the Microsoft file systems natively. Windows 2000 supports FAT12, FAT16, FAT32, and NTFS as does all versions of Windows XP. MS-DOS 7.00 through 8.00 were never released as a stand-alone unit but instead were integrated into the Windows 9x series. MS-DOS 7.00 is integrated into Windows 95 Original Release and Windows 95 OSR 1.0. MS-DOS 7.10 is integrated into Windows 95 OSR 2.0 through Windows 98 Second Edition. MS-DOS 8.00 is integrated into Windows Millennium.

Creating a Windows Real-Mode Boot Disk

The three basic files that must be on a real-mode disk to make it bootable are:

- ✓ IO.SYS
- ✓ MSDOS.SYS
- ✓ COMMAND.COM

These files must reside in the disk's boot sector, or the disk will not be bootable. The most common way of creating a boot disk is by typing `SYS A:` at the command prompt to transfer the operating system boot files to the floppy disk's boot sector in drive A:. However there is another slightly more complicated way to create a bootdisk.

1. First you boot Windows to the DOS prompt, and insert a blank, formatted floppy disk into drive A:.
2. Now at the command prompt, type the following lines, hitting Enter at the end of each line:

```
attrib io.sys -r -h -s
copy io.sys a:
```

```
attrib io.sys +r +h +s
attrib a:\io.sys +r +h +s
attrib msdos.sys -r -h -s
copy msdos.sys a:
attrib msdos.sys +r +h +s
attrib a:\msdos.sys +r +h +s
attrib command.com -r -s
copy command.com a:
attrib command.com +r +s
attrib a:\command.com +r +s
```

Once completed, the floppy boot disk you created can be used to start a computer in real mode (DOS) allowing you to conduct a forensic examination of the computer's hard drive using any utilities you may have placed on the floppy disk.

Creating a Linux Boot Disk

There may be occasions when a forensic examination needs to be conducted on a computer that uses the Linux operating system. In order to create a Linux boot disk, perform the following steps:

1. Start the Linux OS, and log in as *root user*.
2. Check the kernel version of the Linux OS. At the prompt, type `uname -r`.

note

The kernel version will display and should look something like this: `2.4.12`.

3. Insert a blank (empty) floppy disk into the floppy drive. (Under Linux drive A is called `fd0`.)
4. At the prompt, type `mkbootdisk --device /dev/fd0 2.4.12`.

note

The example here uses kernel version 2.4.12; however, you will need to substitute your kernel version as determined in step 2.

5. You should have a boot disk within about one minute. All previous data on the floppy will be erased.

Keep in mind that this boot floppy disk is intended primarily to allow you to get access to the Linux partitions from which you need to recover data or information and will allow you access to the Linux partitions *only*.

Using Packet Sniffers to Gather Evidence

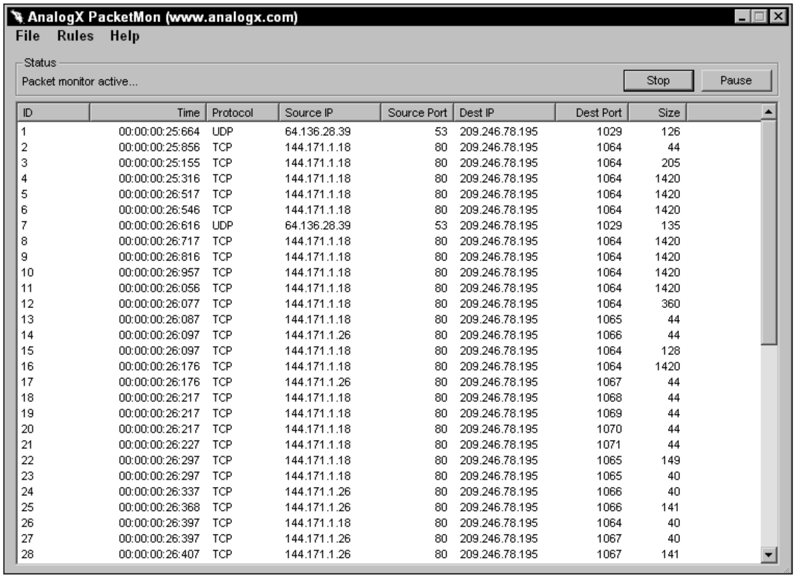
Computer investigations sometimes warrant the capture of live data as it travels in real time across an organization's computer network. To capture network data, special software or hardware is needed. Capturing and viewing these data packets or datagrams as they traverse a network is known as *packet sniffing,* and the programs designed for this purpose are called packet sniffers, protocol analyzers, or network analyzers. A packet sniffer is analogous to a phone wiretap, only this wiretap plugs into computer networks and eavesdrops on the network traffic.

Sniffing became popular with Ethernet, which is known as a *shared medium* network commonly used in organizational networks. Because Ethernet sends data by broadcasting all data packets to all machines connected to the local network, it is unnecessary to receive packets that were intended for other machines. In other words, traffic on an Ethernet network segment bypasses all the hosts that are attached to that segment. Ethernet interfaces support a feature commonly called *promiscuous mode,* in which the interface *listens* to network traffic promiscuously. The Ethernet hardware commonly found in computers have a special filter that prevents the host machine from *seeing* traffic addressed to other computers. Sniffing programs essentially circumvent the filter, and thus can see everyone's traffic. Running a sniffer on a network is an excellent way of collecting evidence of computer abuse or as an intrusion detection system to check for suspicious network activity. The FBI's controversial Carnivore system, which is installed at ISP facilities to collect evidence, is one example of a network sniffer. For the computer crime investigator, there are many sniffers from which to choose. The following is a small sampling of some popular network sniffers:

- ✓ **Snort.** Snort is an open-source (freeware) network intrusion detection system for Unix and Linux systems, and it is capable of performing real-time traffic analysis and packet logging on IP networks. While it excels as an intrusion detection system, it can also be used as a straight packet sniffer. For additional information or to download a copy, visit `www.snort.org`.
- ✓ **NGSSniff.** NGSSniff is a small, easy-to-use network packet capture and analysis program. It requires Windows 2000 or XP to operate and allows users to capture, save, and analyze traffic on their network. This small packet sniffer can be downloaded at `www.nextgenss.com/products/ngssniff.html`.
- ✓ **Ethereal.** Ethereal is a freeware network protocol analyzer with versions for both the Unix and Windows operating systems. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the captured data, viewing summary and detail information for each packet. It can be downloaded from `www.ethereal.com`.

- ✓ **AnalogX PacketMon.** AnalogX PacketMon, available for Windows 2000/XP only, allows you to capture IP packets that pass through a network interface even if they originate from a remote computer on the network. Once the packet is captured, you can use the built-in viewer to examine the header as well as the contents. You can even export the results into a standard ASCII text file for viewing with your favorite text-editing program. AnalogX PacketMon can be downloaded from `www.analogx.com`.

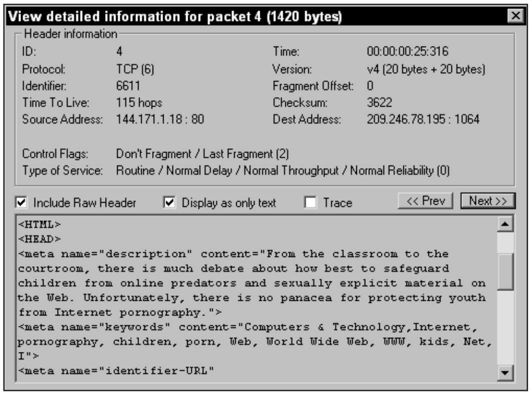
Once they are captured, you can easily search for specific strings of readable text in any packets by using the search capability that is built into many packet-capturing programs. For example, let's say you suspect a worker of visiting inappropriate Web sites violating the company's Internet policy. If that worker is savvy enough to erase temporary Internet files and delete all entries in the browser history, it would be difficult to gather sufficient evidence. While you could use a program like PC Inspector File Recover to uncover the deleted data, an easier and quicker method would be to capture and preserve network packets in real time. Using a program like AnalogX PacketMon, for example (see Figure 7-1), you can scan through each individual captured packet looking for signs of incriminating strings of text (see Figure 7-2). In addition, many of the aforementioned packet sniffers can be configured so that when the software sees a packet that fits certain criteria, it will log (preserve) that data to a file. The most popular use of packet sniffing by forensic investigators is for capturing packets that contain key words that are of benefit to the investigation.



Status
Packet monitor active...

ID	Time	Protocol	Source IP	Source Port	Dest IP	Dest Port	Size
1	00:00:00:25:664	UDP	64.136.28.39	53	209.246.78.195	1029	126
2	00:00:00:25:856	TCP	144.171.1.18	80	209.246.78.195	1064	44
3	00:00:00:25:155	TCP	144.171.1.18	80	209.246.78.195	1064	205
4	00:00:00:25:316	TCP	144.171.1.18	80	209.246.78.195	1064	1420
5	00:00:00:26:517	TCP	144.171.1.18	80	209.246.78.195	1064	1420
6	00:00:00:26:546	TCP	144.171.1.18	80	209.246.78.195	1064	1420
7	00:00:00:26:616	UDP	64.136.28.39	53	209.246.78.195	1029	135
8	00:00:00:26:717	TCP	144.171.1.18	80	209.246.78.195	1064	1420
9	00:00:00:26:816	TCP	144.171.1.18	80	209.246.78.195	1064	1420
10	00:00:00:26:957	TCP	144.171.1.18	80	209.246.78.195	1064	1420
11	00:00:00:26:056	TCP	144.171.1.18	80	209.246.78.195	1064	1420
12	00:00:00:26:077	TCP	144.171.1.18	80	209.246.78.195	1064	360
13	00:00:00:26:087	TCP	144.171.1.18	80	209.246.78.195	1065	44
14	00:00:00:26:097	TCP	144.171.1.26	80	209.246.78.195	1066	44
15	00:00:00:26:097	TCP	144.171.1.18	80	209.246.78.195	1064	128
16	00:00:00:26:176	TCP	144.171.1.18	80	209.246.78.195	1064	1420
17	00:00:00:26:176	TCP	144.171.1.26	80	209.246.78.195	1067	44
18	00:00:00:26:217	TCP	144.171.1.18	80	209.246.78.195	1068	44
19	00:00:00:26:217	TCP	144.171.1.18	80	209.246.78.195	1069	44
20	00:00:00:26:217	TCP	144.171.1.18	80	209.246.78.195	1070	44
21	00:00:00:26:227	TCP	144.171.1.18	80	209.246.78.195	1071	44
22	00:00:00:26:297	TCP	144.171.1.18	80	209.246.78.195	1065	149
23	00:00:00:26:297	TCP	144.171.1.18	80	209.246.78.195	1065	40
24	00:00:00:26:337	TCP	144.171.1.26	80	209.246.78.195	1066	40
25	00:00:00:26:368	TCP	144.171.1.26	80	209.246.78.195	1066	141
26	00:00:00:26:397	TCP	144.171.1.18	80	209.246.78.195	1064	40
27	00:00:00:26:397	TCP	144.171.1.26	80	209.246.78.195	1067	40
28	00:00:00:26:407	TCP	144.171.1.26	80	209.246.78.195	1067	141

Figure 7-1: Analog X PacketMon capturing packets on TCP/IP network



View detailed information for packet 4 (1420 bytes)

Header information

```
ID:               4                    Time:             00:00:00:25:316
Protocol:         TCP (6)              Version:          v4 (20 bytes + 20 bytes)
Identifier:       6611                 Fragment Offset:  0
Time To Live:     115 hops             Checksum:         3622
Source Address:   144.171.1.18 : 80    Dest Address:     209.246.78.195 : 1064

Control Flags:    Don't Fragment / Last Fragment (2)
Type of Service:  Routine / Normal Delay / Normal Throughput / Normal Reliability (0)
```

☑ Include Raw Header ☑ Display as only text □ Trace

```
<HTML>
<HEAD>
<meta name="description" content="From the classroom to the
courtroom, there is much debate about how best to safeguard
children from online predators and sexually explicit material on
the Web. Unfortunately, there is no panacea for protecting youth
from Internet pornography.">
<meta name="keywords" content="Computers & Technology,Internet,
pornography, children, porn, Web, World Wide Web, WWW, kids, Net,
I">
<meta name="identifier-URL"
```

Figure 7-2: Output of captured packet showing HTML data

Building a Forensic Toolkit

The essential component of any computer crime investigation is the collection of specialized software tools (toolkit) that can extract and provide detailed information about the computer or network you are examining. Toolkits come in two types: one that you assemble yourself and a prefabricated one that you download or purchase as a suite from any one of many forensic software vendors. During a computer investigation, there are times when you will be required to monitor traffic, sniff data, and even crack passwords. An incident response/forensic toolkit should contain the appropriate programs to perform each of these tasks. In addition, prefabricated toolkits usually contain *all* the necessary tools to duplicate, capture, and/or analyze system files and data stored on the disk.

Those who wish to use a prefabricated forensic toolkit can use the Forensic Toolkit by AccessData (`www.accessdata.com`) or the Corporate Evidence Processing Suite by New Technologies, Inc. (`www.forensics-intl.com`). Those who wish to assemble their own custom toolkit may do so using a combination of freeware and/or shareware utilities. The following are the types of tools (specific examples of these tool types are given throughout this book) you may wish to include when conducting a basic computer forensic examination:

- ✓ A tool to capture network traffic for analysis (for example, a network sniffer)
- ✓ A utility to create disk images or clones at the bit level
- ✓ A tool to crack passwords
- ✓ A tool that reports open TCP/IP ports and then maps them back to their owning process
- ✓ A tool to recover deleted (erased) data
- ✓ A utility to back up and edit the Windows Registry
- ✓ A utility to display all file system activity in real time
- ✓ A tool to analyze file properties

- ✓ A monitoring tool that displays all Registry activity in real time
- ✓ A utility that displays any network shares including local and remote
- ✓ A monitoring tool that displays logons, logoffs, and privilege usage
- ✓ A tool that displays open files, object processes, Registry keys, DLLs, and owners of object processes

note

The preceding list is intended only as an example and is by no means all-inclusive.

In addition, when selecting tools, there are a few guidelines to follow:

- ✓ Command-line tools are best here; avoid tools that use a Windows (GUI) interface.
- ✓ Create several floppy disks containing your most important data collection tools.
- ✓ Use tested tools that you know work.

The Coroner's Toolkit (TCT)

The Coroner's Toolkit (TCT), written by Dan Farmer and Wietse Venema, is a collection of forensic programs that is used for the examination and analysis of a Unix system after a system compromise. TCT includes an assortment of utilities for examining and collecting data from a computer. The main parts of the toolkit are Grave-robber (a data-gathering program), lazarus (a data reconstruction program), and mactime (a file system time-stamp reporter). (Go to `www.porcupine.org/forensics/tct.html` and/or `www.fish.com/tct/` for more information.)

Additional programs included in TCT are:

- ✓ **file.** This program attempts to determine the content type of a file.
- ✓ **icat.** This program copies (cat(1)) files by inode number.
- ✓ **ils.** This program lists file system inode information.
- ✓ **lastcomm.** A portable `lastcomm` command that displays information in reverse chronological order about all previously executed commands.
- ✓ **major_minor.** This program is used internally by TCT and emits two PERL routines, `dev_major()` and `dev_minor()`, that take a device number as returned by `stat()` and then breaks the number up into the device major and minor number, respectively.
- ✓ **md5.** This is the RSA MD5 digital signature tool.

- ✓ **pcat.** This program copies the address space of a running process.
- ✓ **reconfig.** This program tries to find all the appropriate files on the current system.
- ✓ **strip_tct_home.** This program is used internally by TCT and strips out a variable from various files.

Using Grave-robber

Grave-robber is TCT's main data collection tool. There are several command options available to the user when using Grave-robber that can specify what type of information Grave-robber should collect and where to save the information once it has been collected. For simplicity's sake, the following examples will run Grave-robber in both default configuration and with commands to collect the maximum amount of data. Grave-robber is a powerful tool and can perform the following tasks:

- ✓ Collect inode data from unallocated areas of the file system
- ✓ Record `stat()` information on all files
- ✓ Record `md5` checksums of all files
- ✓ Save open files that have been unlinked since the system compromise
- ✓ Save certain files defined in TCT configuration files
- ✓ Save information from system utilities
- ✓ Record information from the `/dev` directory
- ✓ Gather information such as `ssh` keys and `rhosts` and `host.equiv` files

Running Grave-robber

Although the Grave-robber tool does not require root privileges to run, it should be run under root in order to retrieve root and other processes for further analysis. Start Grave-robber to collect the default set of data by typing as follows:

- ✓ Issuing the following command executes Grave-robber in its default format:

  ```
  # /grave-robber
  ```

- ✓ If you want to gather the maximum amount of data, you also need to provide option `-E`, as shown here:

  ```
  # /grave-robber -d -E -v /
  ```

- ✓ In this line, option `-d` directs the tool to use the actual directory (`/tct-data`) as the location (directory) to store all output. Option `-v` directs the tool to create a more verbose (detailed) explanation of its progress. The last argument, `/`, controls which directory is used as the starting point for any disk analysis.

note

The preceding two lines assume you are already at the directory (or floppy disk) where the Graverobber program is located.

Learning to use all of TCT's tools correctly requires a great deal of time and effort. You must carefully review all documentation and test all components before using them so that you understand and take full advantage of all their features.

Following the Chain-of-Custody

It is important to ensure at all times that the personnel conducting a computer investigation understand and adhere to proper evidence-collecting procedures. This includes following a chain-of-custody to ensure the evidence collected is trustworthy for use in a possible legal case. The chain-of-custody is a record of evidence-handling from the time of seizure to the time evidence is presented in a court of law. The chain-of-custody process is used to maintain and document the chronological history of the evidence. Documents should include the name or initials of the individual(s) collecting the evidence, each person or entity subsequently having custody of it, the dates the items were collected or transferred, the victim's or suspect's name, and a brief description of the item. Without a proper chain-of-custody, it is difficult if not impossible to maintain that relevant evidence was not altered or placed on the computer after the seizure. The courts and the public still consider electronic media fragile and susceptible to unexplainable changes.

Since the chain-of-custody is so important in forensic investigations, it is best to have two forensics investigators assigned to each incident each step of the way. Specifically, having one person document what the other is doing and how they are doing it provides a detailed and accurate record of the handling of the evidence. It is important to include in the documentation the times and dates that steps were taken, as well as the names of those involved.

If nothing else, by having comprehensive documentation, you should be able to disprove any claims of mishandling. In addition, detailed documentation can provide a good point of reference for jogging the memories of the forensic examiners when the duration of the examination becomes lengthy.

Keep written notes as you work, and provide as much information as you can on the following:

- ✓ The current date and time (include appropriate time zone)
- ✓ Broken hardware or any significant problems
- ✓ Notes on the evidence found, which will go into your final report in more detail. These would essentially be notes that anyone could pick up and, at a glance, know exactly where you left off in your assessment of the seized computer and media.

- ✓ Special techniques (for example, sniffers, password crackers, and so on.) used above and beyond normal processes.
- ✓ Outside sources used (for example, third-party companies or products that helped to provide assistance and information)

In addition, it is important that the notebook used to record information be of the type that does not permit any pages to be removed. You will need to record the who, what, where, when, and how of the investigation process. Since this notebook is an essential component in maintaining the chain-of-custody, any information recorded must be as detailed as possible. Items to be recorded in the notebook should include the following:

- ✓ The names of all personnel involved in the investigation including a list of administrators responsible for the routine maintenance of systems
- ✓ A record of all applications running on the suspect's computer
- ✓ A list of who had access to the collected evidence including date and time of access, as well as the date and time of any actions taken by those with access. In addition, the clock of the affected system must be compared with the actual current time and any discrepancies must be noted with the system clock *left unchanged*. Adjustment of the clock may subsequently be considered data tampering, leaving the resultant evidence inadmissible.
- ✓ Details of the initial assessment leading to the formal investigation
- ✓ Circumstances surrounding the suspected incident including who initially reported the suspected incident along with date and time
- ✓ A complete list of all computer systems included in the investigation along with system specifications
- ✓ A printed copy of any organizational policies and logon banners that relate to accessing and using computer systems
- ✓ A comprehensive list of steps used to collect and analyze evidence

The Admissibility of Evidence

The personal computer revolution has created new challenges to law enforcement regarding the manner in which evidence of a crime is seized, analyzed, and presented in court. Before a computer record can be used as evidence, it must first be proven to be authentic. The standard for authenticating computer records is similar to authenticating other types of records. The extent of authentication does not differ simply because a record happens to be in a digital format. A complete guide to offering computer records as evidence is beyond the scope of this book. However, the following sections outline some of the more important issues that can arise when seeking the admission of computer evidence.

Authentication

Over the past few years, the personal computer has become a powerful tool used in the perpetration of nearly all types of criminal activity. The atrocious acts of September 11, 2001 proved that criminal and terrorist activity can easily be coordinated on a worldwide scale using encrypted Internet communications, concealed from government and law enforcement officials. The use of a computer to create and store information often leaves behind electronic "fingerprints" that can in fact make or break a criminal case. Fortunately for law-enforcement computer-evidence specialists, personal computers were not designed to be secure. As a result, passwords, time- and date-stamps, and other forensically valuable information are written to various locations on computer hard disk drives during normal operating system activity.

Unfortunately, computer records can be easily modified, and defense attorneys often claim that computer records lack authenticity because they may have been tampered with or changed *after* they were created. Authentication of computer evidence has thus far been governed by laws in existence long before computer use became so widespread. Authentication of computer evidence poses unique problems in cases involving computer-related crime. You must be able to prove that you did not alter any of the evidence after the computer came into your possession. Such proof will help you rebut allegations that you changed or altered the original evidence.

When duplicating and storing data captured from a suspect's computer, the authenticity of the original data must be retained with a proven method to ensure that the copied data is identical to the original. The best way to authenticate data evidence is through the use of mathematical checksums, which are a popular and legally accepted way to check the validity of the copy from the original data. Checksums are advanced mathematical algorithms, applied to the information stored on a drive or file, which generate a unique numerical output. The result is that a comparison may be made between the original and the copy. Identical checksums between the original and a copy show that an exact copy has been produced. It is impossible to change the information on the drive without changing the checksums.

The majority of law-enforcement computer-forensic specialists rely upon authentication via mathematical checksums to verify that restored bit-stream mirror images of a computer disk drive and relevant files exactly match the contents of the original computer. Such comparisons help resolve questions that might be raised during litigation about the accuracy and authenticity of the restored mirror image. They also protect the computer-forensic specialist from any allegations that data was altered or planted by law enforcement officials or other involved parties during the processing of the computer evidence.

The hard disk drive should always be imaged using a specialized bit-stream backup product. Computer forensic utilities like those offered by Guidance Software (`www.guidancesoftware.com`), X-Ways Software (`www.sf-soft.de`), and New Technologies (`www.forensics-intl.com`) offer bit-stream hard-drive-imaging software that provide the necessary mathematical authentication of copied data, allowing that data to be used as evidence in a court of law.

Issues regarding authentication of computer records are usually in the form of disputes over the accuracy of documents retrieved from computers. According to the Federal Rules of Evidence, the proponent of computer-generated evidence should produce evidence "describing the process or system used to produce the evidence" and "showing that the process produces an accurate result."

There are three phases where errors can be introduced regarding authentication of evidence:

1. When data is entered into the computer
2. When the computer processes the data
3. When the data generated by the computer is evaluated

The most important rule in analyzing computer evidence is to never use the suspect's computer to view data. Instead, you should always use a separate computer to view or analyze a copy of the data. Another important rule to follow in the retrieval and/or analysis of computer data is to make sure a *clean* (forensically sterile) designated computer is used. Otherwise, you might encounter the argument that data on the computer used for analysis has contaminated the data seized from the suspect. When possible, you should not examine the target computer directly. It is best to first make a copy of the disk and then perform all examinations against the copy because the act of looking at the disk may modify it by changing file dates and times.

note

The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. When performing a hard drive image, it is best to use a reputable product.

The Frye Test

The most common test for the admissibility of computer evidence is the Frye test, which originated from the Court of Appeals of the District of Columbia in a decision rejecting the admissibility of a systolic blood pressure deception test (a forerunner of the polygraph test). The court stated that admission of this novel technique was dependent on its acceptance by the scientific community. Because that test was not "sufficiently established to have gained general acceptance in the particular field in which it belongs," the court rejected the defendant's claim and affirmed his murder conviction. Although the Frye test is no longer used in federal courts, it still is being used in various forms in state courts.

The Best Evidence Rule

According to the U.S. Department of Justice, the best evidence rule states, "To prove the content of a writing, recording, or photograph, the 'original' writing, recording, or photograph is ordinarily required." Fortunately, the Federal Rules of Evidence have expressly addressed this concern. This rule provides that "to prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." The Federal Rules, while maintaining the same central policy of the best evidence rule, have made it acceptable to introduce into the courtroom a broad selection of many forms of electronic evidence. Questions of admissibility do not concern whether the data introduced is on a hard drive, a duplicate floppy disk, or a printout of either one. The court is instead interested in whether the original data is authentic and whether any copies presented are accurate. As a result, any authenticated printout of computer data is always considered as meeting the requirements of the best evidence rule.

Public records — if they've been produced through normal business activities *and* if they've been established as authentic — are admissible as evidence in U.S. state and federal court systems, even when those records are produced by automated systems.

x-ref

For more on the Federal Rules of Evidence, turn to Appendix D.

The Permissible Time Period for Examining Seized Computers

Despite applying the best efforts to analyze seized computers quickly, the forensic examination of those computers may sometimes take months to complete because computers are able to store such enormous amounts of data. As a result, suspects whose computers have been seized may be deprived of their computer hardware for extended periods. Even the Fourth Amendment, however, doesn't impose any specific limitation or restrictions on the duration that seized evidence may be retained in order to conduct a forensic examination.

A few judges have nevertheless begun to take a different view. In recent years, several judges have refused to sign search warrants authorizing the seizure of computers unless the forensic examination is anticipated to be conducted relatively quickly, such as within 30 days. In extreme cases, some judges have imposed time limits as short as seven days, and several have forced specific time limitations when legal authorities apply for a warrant to seize computers from operating businesses.

Evidence Preservation

Preservation of evidence is the key concern of any criminal investigation, and computer evidence is certainly no exception. Destructive Trojan horse programs, for example, can permanently destroy computer evidence in a matter of seconds. Because electronic evidence can be altered without a trace, original copies of evidentiary data should be placed in secure storage. Imaged evidence must be stored into appropriate media or reliable mass storage such as optical media.

Because they are fast and reliable and offer a long life span, CD-R discs can be used as mass storage media. In five to ten years time, floppy or proprietary media, like Zip disks, may no longer be widely available. In addition, data stored on magnetic media disks tends to degrade over time. This means that evidence could at some point fail to be recoverable. Since computer crime cases may take several years to come to trial, secure storage media and space to store the original evidence is vitally important to avoid any contamination or alteration of data.

The investigator must be sure to preserve all systems logs, including those that are current and any logs that were archived previously. Subsequent comparison of these logs might even uncover the presence of previously undetected incidents. Logs can offer proof of the type of intrusion made to the system as well as the source of the intrusion and its ultimate destination.

Chapter Summary

In this ever-changing, high-tech world, the collection and preservation of evidence of a computer crime can be a tedious task. Some of the most common reasons for improper evidence collection are lack of written policies, lack of incident response training, and a broken chain-of-custody. Establishing reliability and authenticity depends on the accuracy of the process used to produce the record, the source of information in the record, and the method and time of its preparation. This chapter reviews the basic procedures for collecting and preserving computer-related evidence.

Key points covered in this chapter include

- ✓ The general legal requirements for performing evidence collection
- ✓ The collection order of volatile computer evidence
- ✓ How to create a real-mode boot disk and its role in computer forensics
- ✓ The benefits of using a packet sniffer to collect evidence
- ✓ How to construct a computer forensic toolkit
- ✓ Why the chain-of-custody can make or break a computer crime investigation
- ✓ The importance of evidence preservation

Chapter 8

Incident Containment and Eradication of Vulnerabilities

In This Chapter

- ✓ Overview of quarantine and containment procedures
- ✓ Severing network and Internet connections
- ✓ Understanding the risks of network and file sharing
- ✓ Recognizing the trust model
- ✓ Changing passwords
- ✓ Security awareness using multimedia documentation strategies
- ✓ Eradication of vulnerabilities

COMPUTER SECURITY INCIDENT HANDLING CAN BE DIVIDED INTO SIX GENERAL PHASES: preparation, identification, containment, eradication, recovery, and follow-up. Appreciating what can go wrong in each of these phases will help you respond quickly and efficiently to each incident. As we've already established, responding to computer security incidents is generally not an easy endeavor. Incident response requires a blend of technical knowledge, communication, and coordination among the personnel who respond to the incident. Even the incidents themselves are becoming increasingly more complex. New security vulnerabilities that expose systems and networks to unauthorized access or deny service are constantly being discovered.

With ever-increasing demands for timely processing of greater volumes of information comes an increased threat of information-system disruption. In some instances, interruptions of only a few hours are unacceptable. The impact resulting from an inability to process data must be assessed, and actions should be taken to assure the availability of those systems considered essential to an organization's normal operation. Those in management are obliged to identify critical computer applications and develop contingency plans so that the probability of loss of data processing and telecommunications support is minimized.

The aftereffects of an incident are frequently debilitating, requiring weeks or even months before the integrity of compromised systems is reestablished. In addition, if the perpetrator is caught and prosecution sought, it's reasonable to anticipate that the defense will do everything in its power to cast a shadow of uncertainty and unreliability over the prosecution. For this reason, a clear and effective incident-handling methodology must be in place, particularly when law enforcement is going to be brought in. This chapter focuses on the containment and eradication phases of the incident response model.

Quarantine and Containment

During this phase, the goal is to limit the scope and magnitude of an incident to prevent the incident from causing more damage. This stage of responding to incidents involves limiting the extent and enormity of an incident. Because so many incidents observed today involve the use of malicious code, incidents can spread rapidly, resulting in widespread damage and the compromise of a great deal of sensitive information. It is not unusual to find that every unprotected workstation connected to a LAN has been infected when there is a virus outbreak. The Nimda Worm affected over one million computers in a period of just three days. Total infection doubled before it was contained. Containment should be initiated immediately upon detection or suspicion that a security incident is in progress. The following steps should be taken in the containment phase:

- ✓ Survey the situation and extent of damages.
- ✓ Be discreet and avoid looking for the attacker using obvious methods.
- ✓ Avoid using potentially compromised applications since intruder(s) may have installed or hidden Trojan horses or similar malicious code in place of system files.
- ✓ Back up the system and Registry (Windows). It is important to obtain a full backup of the system in order to acquire evidence of illegal activity. Back up to new (unused) media and store backup tapes in a secure location.
- ✓ Determine the risk of continuing operations (covered in the next section).
- ✓ Change passwords on compromised systems and on all systems that regularly interact with the compromised systems.

note

Password procedures are covered in detail later in this chapter.

Determine the Risk of Continuing Operations

Should the system be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so that activity on the system can be monitored? The answer depends on the type and magnitude of the incident. In the case of an innocuous or nuisance-type virus, it may only be necessary to run your antivirus scanner to detect and eradicate any viruses without having to shut down the infected system entirely. However, if the system contains classified or sensitive information, or if critical programs risk becoming corrupted, it is generally advised that the system be shut down or is at least temporarily disconnected from the network. On the other hand, if there is a reasonably good chance that a perpetrator can be identified and caught by letting a system continue to run as normal, that tactic may be considered. Allowing a system to run in these circumstances, however, must be weighed against the risk of disrupting or compromising data. Again, work within your organizational chain of command in order to reach this type of critical decision.

Preserving Integrity

Information has integrity when both it and the systems that have manipulated it are deemed trustworthy. For systems to be trustworthy, errors must have been (and continue to be) curtailed at every possible juncture. This includes inaccuracies that are the result of both intentional exploitation as well as those that stem from inadvertent mishandling.

Audit Mechanisms

When atypical activity is detected on your organization's computer system, security personnel should be alerted to it by system audit mechanisms. Unusual activity may be in the form of repeated (unsuccessful) attempts to gain access to the system. The audit mechanism can be set to make its notification after a predetermined number of failed attempts have been made to access the system. The audit mechanism will sound different alarms depending upon the degree and significance of the security incident or system compromise.

User-Detected Technical Vulnerabilities

Most of the currently known technical vulnerabilities in applications and operating systems were initially discovered by end users. Vulnerabilities are often discovered when these users attempt to run a program or change system configurations. If a technical vulnerability that can be used to undermine system or network security is discovered, immediately document that vulnerability. In addition, record information about the vulnerability using a vulnerability reporting form, making sure that the following is made clear:

- ✓ What the vulnerability is
- ✓ How the vulnerability can defeat security mechanisms
- ✓ How to exploit the vulnerability (including special conditions under which the vulnerability occurs)

The following is an example of a "Vulnerability Reporting Form" used by the U.S. military. It is not intended as an all-inclusive example, but it can be used as a template for constructing your own form suitable for your organization's specific needs:

Vulnerability Reporting Form

A. General Information:

1. Report Date: ____
2. Name: ____
3. Organization: ____
4. Electronic Mail Address: __________________________________
5. Phone Number: ____
6. Hardware/Software:
    - a. List hardware and system configuration:
      ____
      ____
      ____
    - b. Software Description:
      (1) Operating system (include release number): _____________
      ____
      (2) Describe any unique attributes — primarily, locally modified special security properties: ____
      ____
      ____

B. Describe the nature and effect of the vulnerability in as general terms as possible:
____
____
____

C. Description of Technical Vulnerability:

1. A scenario that describes specific conditions to demonstrate the weakness or design deficiency. The description should sufficiently describe the conditions so that the weakness or design deficiency can be repeated without further information. This scenario may include source or object code.
   ____
   ____
   ____
2. Describe the specific impact or effect of the weakness or design deficiency in terms of the following: (1) denial of service, (2) alteration of information, and/or (3) compromising of data. Cite specific examples as appropriate.
   ____
   ____
   ____

D. Suggested Fixes: Describe any code or procedures you may have discovered that when implemented may reduce the impact of the defined technical vulnerability.

____

____

____

E. Additional Information:

1. System Specifics:
   - a. Location: ____
   - b. Owner: ____
   - c. Network connections: __________________________________
   - d. Account or Serial Number(s): ____________________________
2. System use and highest classification of data on system:

   ____

   ____
3. Additional clarifying information: ____________________________

   ____

   ____

The next decision during quarantine and containment concerns the operational status of the compromised system itself. Should the system be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operating condition so that activity on it can be monitored? The answer depends on the type and magnitude of the incident. In the case of a nondestructive (for example, nuisance) type of virus, it is almost certainly best to use up-to-date antivirus software to quickly eradicate that virus without shutting the infected system down. If the system contains sensitive data, that information may be at risk, and it is generally best to shut the system down (or at least temporarily disconnect it from the network or Internet).

Severing Network and Internet Connections

Intruders are always looking for novel ways to break into systems. We have all seen or heard accounts of how hackers break into computer systems and steal or destroy sensitive information. They enthusiastically develop and employ sophisticated programs to rapidly penetrate systems. Accordingly, intrusions and the damage they cause are often achieved in a matter of just seconds.

When protecting a network against hackers, crackers, and threats posed by malicious code, your primary tools are intrusion detection systems, firewalls, antivirus software, backups, and well-educated users. However, when a system administrator believes that his or her system *has* nevertheless been compromised, one of the recommended actions is to disconnect the computer from the network, preventing further access by the hacker. This is particularly useful with serious computer security incidents. A serious computer security incident can be defined as the type of incident that jeopardizes the integrity, privacy, and/or availability of other computers and networks.

Examples of serious computer security incidents include break-ins where privileged accounts (for example, Unix root accounts or NT Administrator accounts) are used without authorization, incidents where network traffic is monitored without authorization, and incidents where computers or networks are either the source or the target of a Denial of Service attack. In addition, if a serious virus is suspected, such as a fast-spreading worm or dangerous Trojan horse, you should immediately disconnect the infected computer from the network. If the computer is connected to the network via an Ethernet connection, simply removing the Ethernet cable from the Ethernet wall socket will immediately sever the connection. If you use dial-in via a modem, remove the cable connecting the modem to the telephone socket. Users should then refrain from using the computer for Internet/e-mail access until that computer has been scanned with up-to-date antivirus software and you are sure it is no longer infected by malicious code.

After severing the connection, you can then examine log file information for connection and login attempts, and compare any original (vendor provided) applications to those currently residing on the system. This allows you to detect if any files have been modified by the hacker, perhaps for use as a backdoor to permit later access to the network to perform malevolent deeds.

Network and File-Sharing Issues

When a computer is part of a network or has a full-time connection to the Internet, such as via a T-1, DSL, or cable modem, you should disconnect the computer from the network and the Internet once malicious code has been discovered. The foremost reason for this is that many of the more dangerous types of malicious code — worms and Trojan horses — can use Windows network shares to proliferate. Using network shares for proliferation is not a novel concept for malicious code. The infamous Klez worm of 2002 was notorious for exploiting network shares and caused the National Infrastructure Protection Agency (NIPC) to issue the following warning:

> **Propagation of the W32/Klez.h@mm Worm and Variants**
> **April 26, 2002**
> The National Infrastructure Protection Center (NIPC) continues to monitor a mass-mailing worm called Klez.h. The NIPC is issuing this alert due to information received from industry partners, combined with the striking number of infections reported in the wild during the last forty-eight hours. Klez.h spoofs an e-mail address found on the intended victim's system and may appear to have been sent from a familiar party. It has over 100 randomly selected subject lines and uses several different file attachment names when attaching itself. The worm also masquerades as a "Klez.E immunity tool" with the subject line "Worm Klez.E Immunity." The worm also attempts to disable common antivirus scanning programs such as McAfee, Antivir, Norton, Scan, AVConsol, F-Secure, Sophos, and others.
>
> Klez.h also infects the victim machine with the Elkern virus, which may be detected as NGVCK.a. The Elkern virus randomly infects executable files on the local machine and network shares and replaces the contents of these files with random characters to maintain the original file size. This will cause most systems to crash and at the very least destroy critical operating system files.
>
> Users are strongly encouraged to update their antivirus signatures and visit the following Microsoft Web sites for the appropriate patches for Outlook and Internet Explorer 5.x:
>
> `www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp`, or `http://support.microsoft.com/default.aspx?scid=kb;en-us;Q262631`.

If you have shared files or folders, disable them. Once you have completed the removal procedure, if you later decide to reenable file sharing, it is advised that you do not share the root of drive C but instead, share specific individual folders. These shared folders must be password-protected with a secure password.

Configuring Windows File Sharing for Maximum Security

If you simply do not need to share files on your computer or share files on anyone else's computer, you should remove Windows file sharing. If you must retain the Client for Microsoft Networks component, you should still disable file and printer sharing so your computer does not make known its disk drive contents to anyone else on your local network (LAN) or on the Internet. This allows you to use files on another computer or server, but it does not allow others to use files on your computer.

The following steps explain how to configure file sharing for maximum security and assume that Windows is installed in its default location, the C drive. If Windows is installed in a different location, such as drive D, you must substitute that particular drive letter location when using these steps.

For Windows NT/2000, perform the following steps:

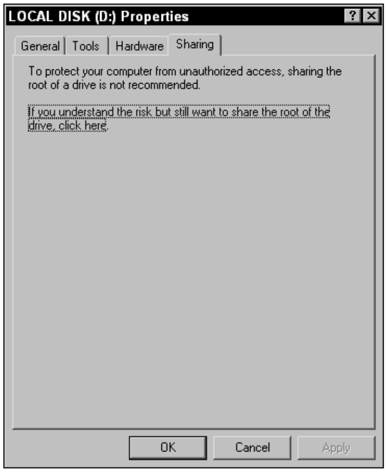
1. Double-click on My Computer.
2. Right-click on drive C, then select the Sharing option under the drop-down menu.
3. Check the Share name. The drive will normally be shared as C$, which is the default share required for system administration. If you click the Permissions button, you should see the message "This has been shared for Administrative purposes. The permissions cannot be shared."
4. Click on the drop-down menu for the Share name to determine if the drive is shared with any other names.
5. If the drive is not shared with any other names, then you need not proceed any further. If the drive is shared with a name other than the default C$, then you have to either remove or modify any specific folders you do not wish to share by following Steps 6 through 8.
6. Select a specific folder and right-click on it, then select "Do not share this folder."
7. If you do not want to completely remove a shared resource, you can increase security by selecting Permissions and then modify the settings so that only certain users and/or groups may write to it.
8. For each shared file or folder, individually check permissions to verify that only required users have write access.

For those who are comfortable using the command line under Windows NT, 2000, or XP, there is an alternate option for deleting Windows shares. At the command (DOS) prompt, type `net share`. The resulting output returns a list of all the shares currently present on the hard drive. Note that the default share names like C$, Admin$, and IPCS$ should be ignored. However, any other shares in the list may be deleted by using the following syntax: `net share sharename /delete`.

Windows XP File Sharing

By default, file sharing is disabled under Windows XP. However, to check for the presence of any shared files or folders, follow these steps:

1. Click the Start button, and then double-click My Computer.
2. Right-click on the C drive, and then select Sharing and Security from the drop-down menu.
3. Click on the link "If you understand the risk but still want to share the root of the drive, click here" (see Figure 8-1).
4. In the Network Sharing and Security portion of the window, look to see if either one of the two radio boxes is checked. To disable sharing, simply uncheck both of them.
5. Close the Sharing and Security dialog box.
6. With My Computer still open, double-click on the Shared Documents folder (see Figure 8-2). If it contains any shortcuts to files or folders and you do not want them shared, simply delete them by right-clicking on them and selecting Delete from the drop-down menu.



To protect your computer from unauthorized access, sharing the root of a drive is not recommended.

If you understand the risk but still want to share the root of the drive, click here.

Figure 8-1: The Sharing tab of Disk Properties for Windows XP Pro

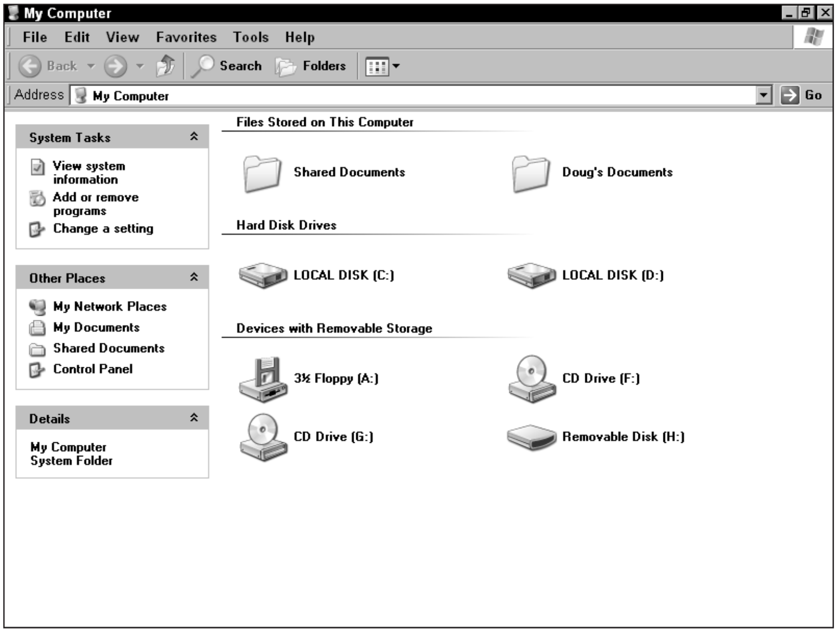
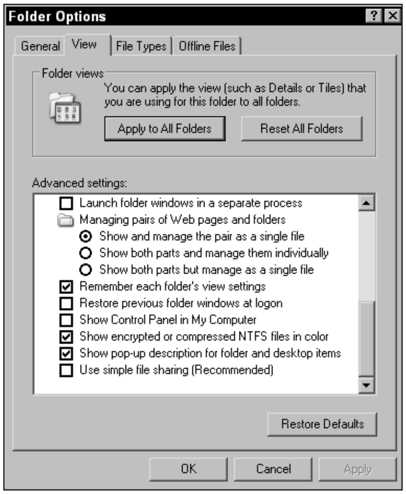


Figure 8-2: Windows XP Pro Shared Documents folder under My Computer

Windows XP Simple File Sharing

By default, the Simple File Sharing feature is activated in Windows XP Professional. While easier to use than navigating the advanced file sharing options, this feature is best suited for members of a smaller workgroup rather than members of a domain, which is typically used in large corporate networks. If you wish to utilize Windows XP's advanced file sharing capabilities, you need to disable Simple File Sharing for increased security and control. To do this, follow these steps:

1. Click on Start, then select My Computer.
2. Under the Tools menu at the top of the window, select Folder Options.
3. Under Folder Options, select View.
4. Scroll to the very bottom of the list of advanced settings and deselect the "Use simple file sharing" option (see Figure 8-3).
5. Click OK.



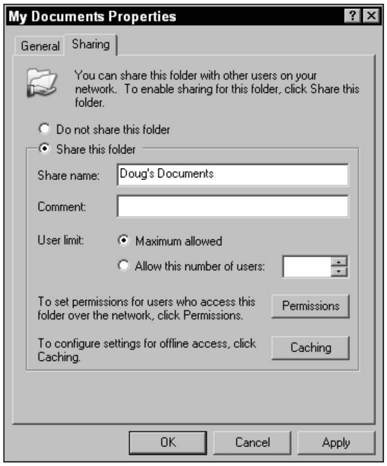
You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

- ☐ Launch folder windows in a separate process
- Managing pairs of Web pages and folders
  - ● Show and manage the pair as a single file
  - ○ Show both parts and manage them individually
  - ○ Show both parts but manage as a single file
- ☑ Remember each folder's view settings
- ☐ Restore previous folder windows at logon
- ☐ Show Control Panel in My Computer
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- ☐ Use simple file sharing (Recommended)

Figure 8-3: Windows XP Pro Folder Options

Once Simple File Sharing has been disabled, you can modify the specific sharing options for any folder located under My Computer by doing the following:

1. Right-click on the folder, and then select Sharing and Security from the drop-down menu.
2. Select the Sharing tab, then select the “Share this folder” option, and enter a share name. In this example, the folder is called Doug’s Documents (see Figure 8-4).
3. You may add a comment (if desired), which describes the share and appears in My Network Places on other computers.
4. You may leave the “User limit” option alone. On XP professional, the default maximum limit is 10.
5. Click on the Permissions button (See the “Creating Access Control Lists” section below) and proceed to make any adjustments you wish regarding how this folder is shared with other users (see Figure 8-5).



My Documents Properties

General | Sharing

You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Doug's Documents

Comment:

User limit: ● Maximum allowed

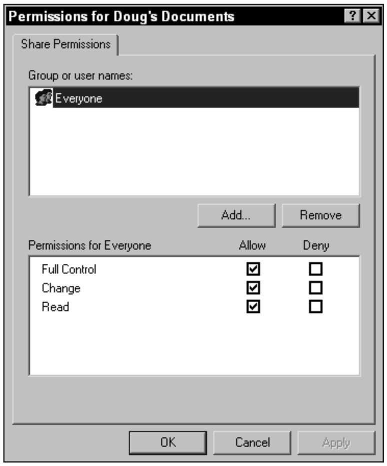
○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions. [Permissions]

To configure settings for offline access, click Caching. [Caching]

[OK] [Cancel] [Apply]

Figure 8-4: The Sharing tab under My Documents Properties of Windows XP Pro



Permissions for Doug's Documents

Share Permissions

Group or user names:

Everyone

[Add...] [Remove]

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

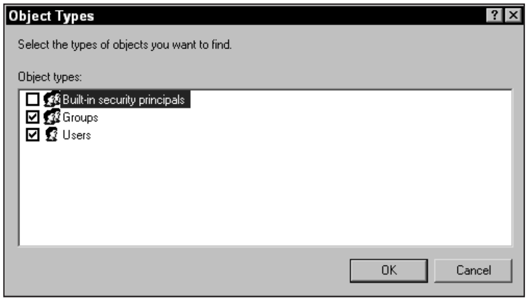
[OK] [Cancel] [Apply]

Figure 8-5: Share Permissions tab under My Documents Properties of Windows XP Pro

Creating Access Control Lists

When modifying file sharing under Windows XP, you will notice that, by default, the Everyone group has the Full Control option checked. This means that *all* users can read, write, and even delete files. From a security standpoint, this is not acceptable. Instead, access control lists should be set up to specify who has access and to what. To do this under Windows XP, follow these steps:

1. With the Permissions window open, click the Add button, and then choose Object Types.
2. Deselect the "Built-in security principals" option and the Groups option (see Figure 8-6), since you wish to view Users only.
3. Click OK, then choose Advanced, and click Find Now.
4. Click on the users who should have access to this share (see Figure 8-7).
5. Click OK, and the users are added. You may repeat this to add additional users.
6. When done, click OK.



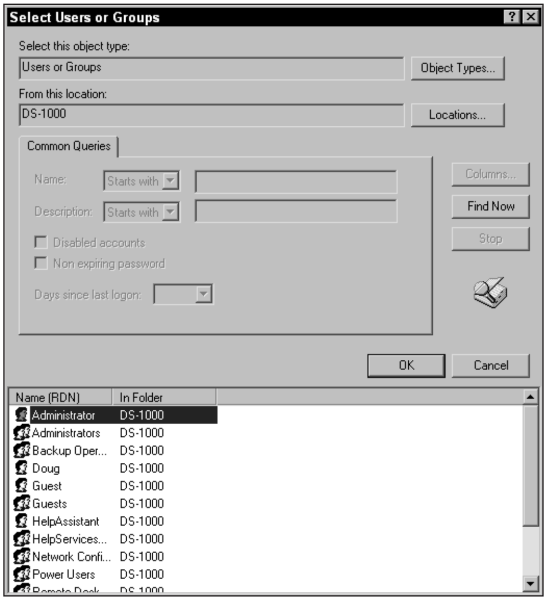
Object Types

Select the types of objects you want to find.

Object types:

□ Built-in security principals
☑ Groups
☑ Users

Figure 8-6: Object Types window under Windows XP Pro



Select Users or Groups

Select this object type: Users or Groups

From this location: DS-1000

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts
□ Non expiring password

Days since last logon:

Name (RDN)	In Folder
Administrator	DS-1000
Administrators	DS-1000
Backup Oper...	DS-1000
Doug	DS-1000
Guest	DS-1000
Guests	DS-1000
HelpAssistant	DS-1000
HelpServices...	DS-1000
Network Confi...	DS-1000
Power Users	DS-1000
Remote Desk...	DS-1000

Figure 8-7: Select Users or Groups window under Windows XP Pro

note

By default, any new users added have read-only access. If you want them to have read/write access, then click the Change box. You will need to do this for each user by selecting each user in the list, and then specify Change permission. To prevent Guest access to this share, you must remove the Everyone group. Select it, and click the Remove button.

Disabling File and Print Sharing under Windows 95/98/Me

In situations where you have a stand-alone computer connected to the Internet, it is often advised that you disable file and print sharing to prevent any unauthorized access to the computer via the Internet. To disable file and print sharing, follow these steps:

1. On the Windows desktop, right-click the Network Neighborhood icon and select Properties.
2. Click on the Configuration tab, and then select Client for Microsoft Networks.
3. Click on File and Print Sharing.
4. Deselect both boxes, and then select OK.

If you do not wish to disable file and print sharing, follow these steps:

1. On the Windows desktop, double-click the My Computer icon.
2. Right-click on drive C, and then select the Sharing option.
3. If you see sharing, then follow Steps 5 through 8.
4. If Shared is checked, then you do not need to proceed any further.
5. If Not Shared is checked, then it is recommended that you enable this option by checking Shared.
6. If you must share this hard drive volume, then under Access Type, check either Read-Only or Depends on Password.
7. You can create separate passwords for read-only and full access. Give the Full Access Password only to those who require it.
8. For any other shared files and folders, make sure the Access Type is appropriately set.

Recognizing the Trust Model

Trust is an essential part of any relationship. The guiding principle of security presumes that a trust model exists that defines the trusted relationships between all the components involved. A trust model is a means for helping to recognize and visualize varying degrees of confidence, intentionally or unintentionally granted to individuals, based upon the risks associated with granting confidence. Having a complete trust model provides a greater awareness of the risks posed by vulnerabilities and threats. The information provided by a trust model will allow your organization to assess its vulnerabilities and threats and find solutions to either mitigate that risk or choose to accept it.

Traditionally, stand-alone computers and small networks rely on some type of user authentication and access control to provide security. Authentication is accomplished via a control mechanism, which verifies the identity of a system user. Once identified, that user is permitted to use, change, or view certain computer resources. Currently, several different approaches are being used in the attempt to reliably authenticate users. These include passwords, digital signatures, smart cards, and biometrics, to name a few.

The Trust Model in Computer Operations

Modern-day information security relies on trust relationships to operate. However, with trust comes the risk that trust will be violated. In order to combat this possibility, trust mechanisms must be implemented to ensure the dependability of trust. Following are some of the ways trust mechanisms can be implemented in the computer environment.

User ID and Password Trust

In most organizations when a user is given access to a computer account, he or she is assigned a user ID and a password to access that account. Along with the user ID and password are certain trusts that the user inherits, which grant access to resources on the computer. Without a user ID and passwords, no trust is given because the computer has no other way of identifying the user. The user ID and password are analogous to a key that opens the door allowing entry. The chief risk associated with user IDs and passwords is that IDs and passwords can be lost, stolen, or exploited (cracked). Organizations can mitigate these risks by instituting and following sound password policies and practices. This can be accomplished by applying the guidelines found in "Password Protection 101" published by the National Infrastructure Protection Center.

> **Password Protection 101**
>
> Every year thousands of computers are illegally accessed because of weak passwords. How many users are guilty of any of the following things:
>
> - Writing down a password on a sticky note placed on or near your computer.
> - Using a word found in a dictionary. That's right, a dictionary. Any dictionary!
> - Using a word from a dictionary followed by 2 numbers.
> - Using the names of people, places, pets, or other common items.
> - Sharing your password with someone else.
> - Using the same password for more than one account, and for an extended period of time.
> - Using the default password provided by the vendor.
>
> Chances are, if you are anything like the majority of computer users, you answered yes to one or more of the above questions. The problem is, hackers are aware of these problems as well and target those who don't take the correct precautions.
>
> **Why Is There a Problem?**
>
> Passwords are one of the first lines of defense that users have to protect their systems. Unfortunately, people are not accustomed to remembering difficult passwords consisting of numbers and weird characters. The ever-increasing number of passwords required to work in today's world only makes this

> problem worse. Many people have compensated for this problem by writing down their password and keeping that information in an unsecured area, like stuck to a computer screen.
>
> One of the first things a hacker will attempt to do against a system is run a program that will attempt to guess the correct password of the target machine. These programs can contain entire dictionaries from several different languages. In addition to words found in dictionaries, these programs often contain words from popular culture such as science fiction movies and novels.
>
> Hackers like to attack people's weaknesses. One of the major weaknesses is the reluctance to remember several, long, difficult to guess words such as passwords. Therefore, once one is chosen, the likelihood that the same password is used for several accounts is very high. This is similar to the problem with default passwords because users have a tendency to keep the same password for a long period of time, thereby allowing the attacker that much more time to gain access to a system.
>
> **What You Can Do?**
>
> Remembering long passwords can be difficult, but there are some basic techniques users can employ to lessen the pain. First, choose a phrase that you will remember. As an example, we will use the phrase "The pearl in the river." You can then take a number that you are familiar with, such as a birthday. For this example we will use 7/4/01. Next, you can take the first letter of your phrase and interlace it with the chosen date to make something similar to t7p4i0t1r. This method creates a password that won't be found in any dictionary and is unique to the person who created it.
>
> It is important to remember though, that any password can be guessed if given enough time. Therefore, it is important to change your password within the amount of time it would take an attacker to guess it. For example, with the previous password it may take an attacker 60 days on a very fast computer to guess what it is. In order to ensure your system's safety then, a user must change their password before those 60 days come to an end.
>
> While password security is a very important deterrent to hackers gaining access to your system, it is only one component to the "defense in depth" principle. What this means, is passwords need to be used along with other measures such as updated antivirus software and a personal firewall such as Zone Alarm.

Remember that the first line of defense in computer system trust is the protection of passwords and user IDs.

note

With the increase in computing power, it takes less time than ever to guess passwords. Therefore, strong passwords need to be combined with account lockouts (lock the account after some number of incorrect guesses) or the attacker can eventually guess it.

Operating System Trust

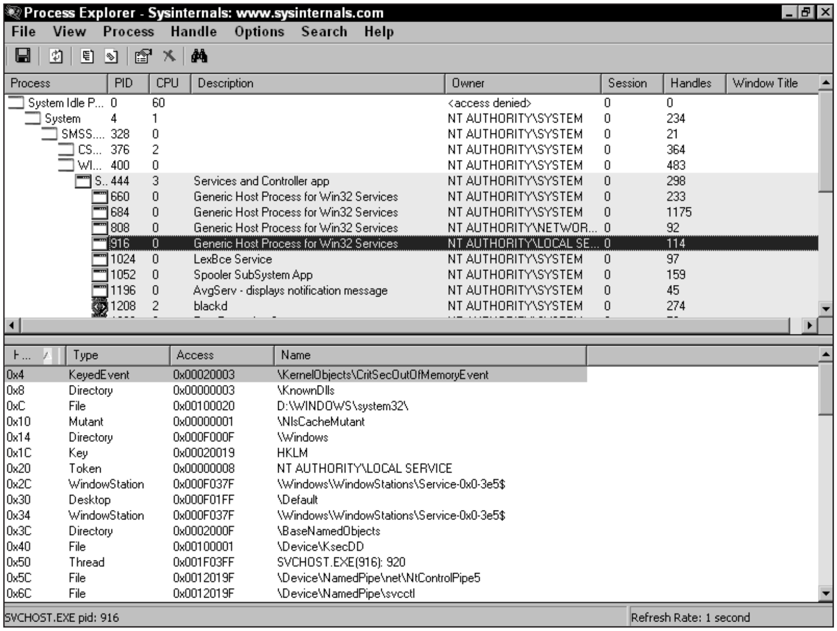
Operating system trust is one of the most complex types of trust because the operating system performs so many functions, including data sharing, network communications, and authentication when users log on. When an operating system is initially installed and configured, certain services are enabled by default. In Unix systems, for example, Trivial File Transfer Protocol (TFTP) and echo are two default services that permit complete trust by running as root. With Windows NT, certain Web services and the File Transfer Protocol (FTP) are enabled by default.

Unfortunately, system administrators are often unaware that unneeded services — which can be exploited by hackers — are left running on the system, leaving them vulnerable to attack.

The easiest way to mitigate these operating system risks is to minimize the amount of services you run, for example, by only running the services that are needed on your workstations and servers. The Code Red Bug, for example, successfully overwhelmed many networks because employees had installed Web services on their individual workstations. While there will be occasions when certain individuals may be required to run Web servers on their workstations for development and testing, more often than not, these Web server services provide little function other than creating a potential jump-off point for a worm or other hostile attack. For those in charge of managing large numbers of workstations, it becomes an onerous task to eliminate select services from each and every workstation.

While reducing the amount of services running on a computer limits functionality, it does harden the system in terms of security. Hardening your servers and workstations is just a first step in preventing hackers from breaking into a computer system by limiting what the attacker is able to exploit and utilize. While some services — such as the WWW service on a Web server — are required, it is important to also keep abreast of the updates, patches, and hot fixes on *all* services.

On Windows-based computers, you can easily detect running services by using a program like Process Explorer. With Process Explorer up and running, select the Options → Highlight Services menu item. You can then click on any of the highlighted services to see service details, which appear in the lower pane of Process Explorer (see Figure 8-8). Process Explorer can be downloaded from `www.sysinternals.com`.



Process	PID	CPU	Description	Owner	Session	Handles	Window Title
System Idle P...	0	60		<access denied>	0	0	
System	4	1		NT AUTHORITY\SYSTEM	0	234	
SMSS....	328	0		NT AUTHORITY\SYSTEM	0	21	
CS...	376	2		NT AUTHORITY\SYSTEM	0	364	
WI...	400	0		NT AUTHORITY\SYSTEM	0	483	
S..	444	3	Services and Controller app	NT AUTHORITY\SYSTEM	0	298	
	660	0	Generic Host Process for Win32 Services	NT AUTHORITY\SYSTEM	0	233	
	684	0	Generic Host Process for Win32 Services	NT AUTHORITY\SYSTEM	0	1175	
	808	0	Generic Host Process for Win32 Services	NT AUTHORITY\NETWOR...	0	92	
	916	0	Generic Host Process for Win32 Services	NT AUTHORITY\LOCAL SE...	0	114	
	1024	0	LexBce Service	NT AUTHORITY\SYSTEM	0	97	
	1052	0	Spooler SubSystem App	NT AUTHORITY\SYSTEM	0	159	
	1196	0	AvgServ - displays notification message	NT AUTHORITY\SYSTEM	0	45	
	1208	2	blackd	NT AUTHORITY\SYSTEM	0	274	

H...	Type	Access	Name
0x4	KeyedEvent	0x00020003	\KernelObjects\CritSecOutOfMemoryEvent
0x8	Directory	0x00000003	\KnownDlls
0xC	File	0x00100020	D:\WINDOWS\system32\
0x10	Mutant	0x00000001	\NlsCacheMutant
0x14	Directory	0x000F000F	\Windows
0x1C	Key	0x00020019	HKLM
0x20	Token	0x00000008	NT AUTHORITY\LOCAL SERVICE
0x2C	WindowStation	0x000F037F	\Windows\WindowStations\Service-0x0-3e5$
0x30	Desktop	0x000F01FF	\Default
0x34	WindowStation	0x000F037F	\Windows\WindowStations\Service-0x0-3e5$
0x3C	Directory	0x0002000F	\BaseNamedObjects
0x40	File	0x00100001	\Device\KsecDD
0x50	Thread	0x001F03FF	SVCHOST.EXE(916): 920
0x5C	File	0x0012019F	\Device\NamedPipe\net\NtControlPipe5
0x6C	File	0x0012019F	\Device\NamedPipe\svcctl

SVCHOST.EXE pid: 916

Refresh Rate: 1 second

Figure 8-8: Process Explorer by Mark Russinovich

The Trust Model and Identity Theft

It is estimated that identity theft has become the fastest-growing financial crime in America and perhaps the fastest-growing crime of any kind in our society. Identity theft has been referred to by some as the crime of the new millennium. It can be accomplished anonymously, often easily, by a variety of means, and its impact upon the victim can be devastating. Identity theft is simply the theft of identity information such as a name, date of birth, Social Security number (SSN), or a credit card number. The Federal Trade Commission (FTC) reports that its Consumer Sentinel Web site — which provides law enforcement with access to more than 300,000 complaints about all types of consumer fraud — has received more complaints about identity theft and fraud than any other category of consumer fraud.

Having a trust model or method for assuring identity is an excellent method of solving the problem of identity theft. In fact, a trust model is essential to any security infrastructure. A security infrastructure built on security credentials addresses the problems of fraud and identity theft when security credentials are identified and authenticated.

Computer Security Awareness

It's been said, "The only secure computer system is one that's unplugged or turned off." Since it is not realistic to leave computers off all of the time, employees — and all other users — need to understand the risks to systems and prepare themselves to guard against them. A sound computer-security-awareness program educates organizational computer users about the potential threats facing the company's information infrastructure. With this knowledge, employees are better prepared to recognize potential security problems. Once the problem has been identified, employees should be familiar with the proper reporting procedures, including the chain of command. Since security can be likened to a moving target, security awareness must remain an ongoing event. Since security threats and vulnerabilities are capricious in nature, security must always be prepared and include an automatic response. A good guideline to follow is Section 5 of the Computer Security Act of 1997, which mandates the following security training for federal agencies:

> **SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.**
>
> **(a)** In General. — Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be
>
> 1. provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or
> 2. provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

> **(b)** Training Objectives.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed
>
> **1.** to enhance employees' awareness of the threats to and vulnerability of computer systems; and
>
> **2.** to encourage the use of improved computer security practices.
>
> **(c)** Regulations.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

Security awareness may be presented in many forms, such as logon banners that remind computer users about security each time they start their computers to audio and video documentation. Whatever methods are employed, the main objective is to enhance continued employee awareness of the threats to and vulnerability of computer systems; and to encourage the use of improved computer security practices within the organization.

Multimedia Documentation Strategies

With the events of September 11, 2001 still fresh in our memories, we are reminded that security awareness has never been more important. People are undoubtedly the most challenging facets of security that any organization has to face. The organization must convince all computer users that information security is everyone's responsibility and not just that of the system administrators. Users must be convinced that they can be directly or indirectly affected by a security compromise.

As mentioned earlier in this chapter, security is a complex moving target. As the world gradually becomes more network-dependent, it is essential that computer-security-awareness programs that benefit *all* computer users be developed and implemented. Once this objective is achieved, users can quickly recognize and react to information security breaches. Without this awareness, users remain naive to computer security threats.

When it comes to computer security awareness, videos can be one of the most effective methods for communication. However, they come with a price. The cost of producing your own video can reach several thousand dollars per minute of finished product. For organizations with large IT security budgets, this may not seem like an excessive expense. For smaller, more budget-constricted organizations, however, there is an alternative. Numerous third-party vendors sell ready-made computer security videos that may be suitable for a wide variety of organizations. Such videos generally cost significantly less than the costs associated with producing in-house proprietary security videos.

Following are two vendors that produce excellent security awareness products, including various posters, audio tapes, videos, and CD-ROMs.

- ✓ **Commonwealth Films:** `www.commonwealthfilms.com`
- ✓ **Native Intelligence, Inc.:** `www.nativeintelligence.com/awareness/index.asp`

Bear in mind that since you are able to reuse the video, a computer security-related video would be an outstanding tool in your security awareness program.

The Eradication Phase

The next priority — after containing damage from a computer security incident — is to remove the cause of the incident. Hackers and crackers relentlessly seek out security vulnerabilities in new or existing software, especially where the software vendor hasn't developed a patch or where the organization has failed to download an available fix (which would have eliminated the vulnerability). The eradication phase ensures that the problem is eliminated and vulnerabilities that allow reentry to the system are eliminated, as well. In the case of a virus incident, you should remove the virus from all systems and media (e.g., floppy disks, backup media) by using one or more proven commercial virus eradication applications. If there are flaws in the operating system or applications for which there are updates, they should be patched immediately.

Remember, many network intruders leave remnants (backdoor Trojans, spyware, and so on) that can prove difficult to locate. Your organization should *first* concentrate on the eradication of any malicious code (for example, Trojan horses, worms, and so on), close any unneeded open ports, and *later* concentrate on the more benign dangers (for example, hoax/nuisance viruses) especially when they don't present a serious enough risk to justify the cost of eradication. Use information gathered during the containment procedures to collect additional information. If a single attack method cannot be determined, list and rank the possibilities.

Harden Your Defenses

Implement appropriate protection techniques by adding firewalls, router filters, intrusion detection systems, and/or moving the system to a new IP address. In extreme cases, your organization might find it beneficial to migrate workstations or servers to a more robust and secure operating system such as Linux or Unix. You should also remove all unnecessary applications and default accounts to close potential points of unauthorized access. Certainly, you should never forget the human element. Social-engineering attacks focus on bypassing the most sophisticated security tools available by targeting the weakest link of the security chain, the human link. Social engineering is the science of getting people to comply with your wishes. Focusing on the human link ensures that no computer security system is needlessly subjected to social-engineering attacks.

Perform Analysis of Vulnerabilities

Use a vulnerability analysis tool to scan for vulnerable systems that are connected to affected systems. Security personnel routinely audit their systems with the same scanners and sniffers (tools) that hackers and crackers use to compromise networks. A more aggressive approach to vulnerability analysis involves penetration testing. Penetration testing looks at organizational security from an external vantage point. Port and vulnerability scanners are the basic tools of both the attacker probing for misconfigured or unpatched services, and for the system administrator trying to find and plug holes before they *are* exploited. For Unix or Linux operating systems, numerous vulnerability scanners are available, Here are several:

- ✓ **Nessus** by Renaud Deraison is a freeware software security scanner that audits a specified network remotely and determines whether hackers could compromise or exploit it in some fashion. For additional information or to download a copy, visit `www.nessus.org`.

- ✓ **SAINT** by SAINT Corporation is an acronym for the "Security Administrator's Integrated Network Tool" and is used to scan Unix/Linux computer systems to uncover potential areas of weakness and then recommend fixes. Among some of its many features, SAINT vulnerability assessment can detect and repair potential weak points in your network's security before they can be exploited by intruders. In addition, SAINT can anticipate and prevent common system vulnerabilities and demonstrate that your organization's computers systems are in compliance with current data privacy regulations, such as the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and Children's Online Privacy Protection Act (COPPA). For information on pricing or to download a free trial copy, visit `www.saintcorporation.com`.
- ✓ **GFI LANguard Network Security Scanner (N.S.S.)** allows you to not only scan your network but allows you to do it from a hacker's point of view. It can identify all network-connected computers gathering their NetBIOS information, open ports, and network shares to name just one of its many features. LANguard Network Scanner can also display installed program patches (a.k.a. hot fixes) and scan for known security issues. If any security issues are found, this program will provide a Web link to additional information. N.S.S. contains a large database of common vulnerabilities, including CGI, FTP, and Registry exploits. This program allows the user to customize the database, add custom criteria, and even specify alert flags based on user preferences. With the information from LANguard N.S.S., your organization can proactively secure its network by shutting down unnecessary ports and shares. This program will also produce convenient HTML-based reports for distribution across the Internet or a company intranet, if needed. Even for the nonprofessional, this program provides in-depth information about the LAN. While the freeware version has some advanced features disabled (like scheduled scans, a report generator, and result comparison deployment), it is still well suited for the majority of users. For additional information or to download a copy, visit `www.gfi.com`.
- ✓ **The Microsoft Baseline Security Analyzer (MBSA)** is a software-based utility that allows users to scan Windows-based computers for common security problems such as a software misconfiguration or the failure to apply updates and patches.

Chapter Summary

The repercussions of a computer security incident often require a significant amount of time and peoplepower before the integrity of compromised systems can be reestablished. The primary goal of incident response is to first limit the effects of a computer security incident and then to quickly restore business continuity. Immediate decisions must be made regarding a number of issues, such as whether to shut down a system, disconnect a system from the network, or simply monitor the system for suspicious activity. Incident containment and eradication of vulnerabilities are two important, critical phases of an organization's overall incident response plan.

Key points covered in this chapter include

- ✓ A brief overview of computer security incident quarantine and containment procedures
- ✓ The pros and cons of severing network and Internet connections during the containment phase of the incident response model
- ✓ An overview of the risks of using network and file shares under Windows-based networks, including steps on how to mitigate those risks
- ✓ The importance of understating the computer security trust model and its role in an organization's overall incident response plan
- ✓ Proper password procedures and the importance of frequent password changes
- ✓ How to foster company-wide security awareness using multimedia documentation strategies
- ✓ An overview of steps involved in eradicating computer security vulnerabilities

Chapter 9

Disaster Recovery and Follow-Up

In This Chapter

- ✓ Understanding disaster recovery planning
- ✓ The importance of incident recordkeeping
- ✓ UPS and backup procedures
- ✓ Post-incident monitoring of systems
- ✓ Anticipating further attacks

WITH THEIR INCREASED RELIANCE ON THE INTERNET, organizations around the globe routinely face threats from hackers, crackers, computer viruses, and network worms, which often exploit a variety of weaknesses in computer systems and cause significant damage. Due to the rise in connectivity brought about by the Internet, damage caused by seemingly isolated computer security incidents can rapidly spread to other Internet-enabled computer systems, causing widespread financial losses. A disaster recovery plan should be tailored to fit your organization's exposure to risk and should provide concrete information and procedures to guide decisions and operations in times of crisis.

Disaster recovery procedures should include the following:

- ✓ Restoring the system after compromise. Once a compromise has been eradicated, the next logical step is to restore the system to its precompromise fully operational state.
- ✓ Validating the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal operating condition.
- ✓ Deciding when to restore operations. Management may decide to leave the system offline while operating system upgrades and patches are installed.
- ✓ Monitoring the systems. Once the system is back online, continue to monitor for backdoors that may have eluded detection.

Knowing how to react properly in an emergency is critical to making decisions that will minimize resultant damage and quickly restore operations. In their December 7, 2001 Highlights Bulletin, the National Infrastructure Protection Agency posted the following:

> September 11, 2001
>
> **Terrorist Incidents Lessons Learned: New Approaches Needed for Disaster Recovery and Business Continuity Planning**
>
> Three major themes can be noted in the many articles in which technical professionals have been discussing the impacts of the September 11 incidents.
>
> **Emerging Lessons**
>
> First, the disaster recovery plans of most organizations tend to focus on information system availability ("up-time") issues. Second, the evolving understanding of the scope of the impacts has resulted in a fundamental reassessment by both private sector and government organizations of the meaning of "worst-case scenario." Third, and most important, there appears to be an emerging synthesis of the two first themes: the incidents have resulted in an increasing awareness of the need for business continuity plans and disaster recovery plans to complement each other.
>
> **Financial Services Infrastructure**
>
> Many large financial service organizations quickly restored their information systems at alternate sites. The systems demonstrated stability under high transaction volumes as markets reopened and business resumed. Factors contributing to successful resumption of operations include investments in real-time data backup and full hot site capabilities, frequent disaster plan testing and updates, lessons learned during Y2K remediation and other plans for critical functions such as NASDAQ's decimalization conversion plan.
>
> **Traditional Disaster Recovery Services Pushed to New Limits**
>
> Companies offering disaster recovery services have reported record numbers of organizations submitting disaster alerts and disaster declarations. Furthermore, in many cases the nature of the services required is also significantly broader than in previous disasters such as Hurricane Floyd in 1999 and the 1993 World Trade Center attack.
>
> **Need to Reevaluate Risk Issues**
>
> During the last 15–20 years, focus on cost-cutting and productivity increases has contributed to consolidation of organizational operations, information, people, processes, and supply chain relationships. The September 11 incidents show these trends present new potentials for failures that have not been reflected in many disaster recovery and business continuity plans. Additionally, the incidents also point out risk factors related to close proximity to other "high value targets" and cross-infrastructure dependencies on telecommunications, power, and transportation.
>
> **Critical Infrastructure and Enterprise Network Implications**
>
> The basic principles of emergency readiness have been used for decades and can continue to be a basis for addressing new challenges. However, two new planning approaches need to be addressed. First, the scope of disaster recovery planning must be broadened beyond its traditional focus on primarily operational issues to include backup security measures as well. Second, business continuity planning combined with disaster recovery planning needs to be approached as an enterprise-wide business operation requirement.

In this bulletin, the NIPC stresses the need to have disaster recovery and business continuity procedures that complement each other. No matter how many precautions are employed and enforced, most people in the field of computer security would agree that there are no completely secure computers. When the unthinkable happens, a well-designed disaster recovery plan describes the preparation and action required to effectively respond to the disaster, assigns and/or delegates responsibilities, and even describes the procedures for testing and maintaining the plan. In addition, a disaster recovery plan needs to be frequently tested and updated to reflect current hardware, software, procedures, critical applications, and personnel. The type and extent of testing adopted by an organization will depend on the following factors:

- ✓ Cost of executing the test plan
- ✓ Budget availability
- ✓ Complexity of information system and components

Disaster Recovery Planning

The best approach to disaster recovery focuses primarily on planning and prevention. The aim of disaster recovery planning is to enable an organization to endure a disaster and to reestablish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time. Therefore, the goals of the business continuity plan should be to as follows:

- ✓ Identify flaws and vulnerabilities and implement a disaster prevention program
- ✓ Minimize disruptions to business operations
- ✓ Facilitate recovery tasks
- ✓ Reduce the complexity of the recovery effort

In today's business climate, any long-term computer disruptions have a dramatic impact on an organization's bottom line. Recovery strategies should therefore incorporate both information technology assets and management personnel who have responsibility for protecting those assets. In addition, organizations need to train their employees to execute recovery plans by doing the following:

- ✓ Making employees aware of the need for a disaster recovery/business resumption plan
- ✓ Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency
- ✓ Training all personnel with responsibilities identified in the plan to perform the disaster recovery and business continuity procedures
- ✓ Providing the opportunity for recovery teams to practice their disaster recovery and business continuity skills

Developing a Disaster Recovery Plan

All successful disaster recovery plans begin with a business impact analysis to determine what functions are absolutely essential to the organization. Anyone who is reasonably objective can evaluate which of the organization's processes or functions are critical and decide which ones should be recovered first when a recovery situation presents itself. Less important areas can be recovered after all the vital elements are functioning adequately.

Individuals responsible for the critical system applications of your organization should develop and perform regularly scheduled procedures for backing up important data and computer programs. Disaster recovery backups should be located in a safe place away from the facility's building. The successful recovery of application systems is totally dependent on the accuracy — and currency — of the backup data available to recover it.

There is no single disaster recovery plan that will apply to all organizations. Instead, these plans must be tailored to your organization's particular needs. It would be impossible to cover every possible scenario; however, all disaster recovery plans should encompass the following key points:

- ✓ Provide management with an understanding of all the resources needed to develop and maintain an effective disaster recovery plan. In addition, the organization should have the committed support from all group members (for example, management or IT personnel) to help support and participate in the effort.
- ✓ Assemble an incident response team that includes representatives from every key division of the organization.
- ✓ Define recovery requirements from the perspective of business functions.
- ✓ Identify the risks. Every risk must be identified along with what steps would be necessary to thwart it happening in the first place. Avoiding a crisis is likely cheaper than repairing it after the fact. All disaster plans must start with a focus on prevention.
- ✓ Document the impact of an extended loss to operations and key business functions. It is impossible for a disaster recovery plan to justify each expense included in every business process and application in the recovery process. The organization should therefore inventory and prioritize critical business processes.
- ✓ Select recovery teams to oversee the disaster recovery process and ensure that the required proper balance is maintained for disaster recovery plan development.
- ✓ Develop a contingency plan that is understandable, easy to use, and easy to maintain by all organization members.
- ✓ Define how contingency planning considerations are to be incorporated in your ongoing business planning. System development procedures must also be defined in order for the plans to remain viable.

For those wishing to construct their own computer disaster recovery plan, the following contingency and disaster recovery plan guidelines from the Virginia Community College System demonstrate the steps required to create a computer disaster recovery plan. These guidelines are not meant to be all-inclusive but rather should be used as a template:

Sample Contingency Disaster Recovery Plan

State the purpose of the disaster recovery plan.

I. ASSUMPTIONS

List and describe the things that could be assumed from the plan. The list of assumptions will not be all-inclusive. Some assumptions could be:

1. All resources and staff can be made available as soon as possible.
2. All members of the disaster recovery teams have the most current copies of the disaster recovery plan.
3. Users will continue to operate via a manual mode.
4. Backups will be made available as soon as possible.

II. DATA PROCESSING/BUSINESS ENVIRONMENT

Provide a detailed description of your business and/or data processing environment.

III. WHEN A DISASTER IS RECOGNIZED

State the course of actions that should occur when a disaster is recognized. The following is an example:

> In the event of a disaster, the disaster planning coordinator should be contacted. The coordinator should contact the emergency management team. The emergency management team should go to the area of the disaster, assess the damage and provide the coordinator with the results of the assessment as soon as possible. The disaster planning coordinator should decide which other teams to contact depending on the type and severity of the disaster. Disaster recovery operations should not begin until the coordinator has designated the plan of operation.

IV. DISASTER RECOVERY TEAMS

Organize disaster recovery teams to handle different functions during the period from which the disaster is first reported until full recovery is completed. Depending on the size of your site, the size of each of your teams may vary as well as the number of teams. Each team is responsible for *developing a set of actions* to be followed to facilitate an orderly recovery from a disaster.

A. **Disaster Planning Coordinator**

   Determine who the disaster recovery coordinator should be. List the responsibilities of the disaster recovery coordinator. Some responsibilities could be to

   1. Serve as the primary contact and coordinate the recovery effort.
   2. Contact all support personnel involved in the recovery effort.
   3. Provide all support personnel with a copy of the plan.

4. Contact the management personnel.
5. Maintain the disaster recovery plan.

B. **Emergency Management Team**

Determine who the members of the emergency management team will be. List the responsibilities of the emergency management team. Some responsibilities could be to

1. Assess the damage.
2. Provide a detail status of the disaster to the disaster planning coordinator as soon as possible.
3. Contact all vendors, contractors, or external resources necessary to restore services to the damaged areas.
4. Provide a general status of the disaster to college personnel.
5. Determine the priorities. There should be a minimal accepted time frame the college will function with degraded operations before the backup plan is implemented.
6. Ensure all needed support staff has been contacted to provide assistance.
7. Determine a general time frame for when all services will be restored.

C. **Technical Support Team**

Determine who the members of the technical support team will be. List the responsibilities of the technical support team. Some responsibilities could be to

1. Determine what computer hardware/software has been damaged.
2. Review the risk assessment analysis and business impact analysis and determine what the critical/noncritical applications are and to determine who is responsible for each application.
3. List procedures to create a new environment for the hardware or for the purchase of new hardware (give actual procedures).
4. List procedures to restore critical software/applications (give actual procedures).
5. List procedures to restore noncritical software/applications (give actual procedures).
6. Contact application owners to determine their role in the recovery process.

D. **Special Projects Team**

Determine who the members of the special projects team will be. List the responsibilities of the special project team. Some responsibilities could be to

1. Provide transportation to/from backup facilities.
2. Make any necessary telephone calls.
3. Order supplies, complete necessary paper work, and provide assistance as required to all support groups.

E. **Customer Support Team**

Determine who the members of the customer support team will be. List the responsibilities of the customer support team. Some responsibilities could be to

1. Notify computer customers of the disaster and give them a time frame for recovery.
2. Help customers develop manual procedures to accomplish work if resources are unavailable for a long duration of time.
3. Have customers list the priority of their day-to-day work.

V. EMERGENCY RESPONSE PROCEDURES

List the emergency response procedures appropriate to any incident or activity, which may endanger lives, property, or the capability to perform essential functions.

VI. EMERGENCY TELEPHONE LIST

Make a list of the emergency services telephone numbers in your area; for example, fire and police service, air-condition service, security service, and so on. In addition, list all the names and telephone numbers (work and home) of all the members of the disaster recovery teams. You can also list the telephone numbers of any hardware and/or software vendors as well as any other important telephone numbers.

VII. MAINTAINING THE PLAN

This should be the responsibility of the Disaster Planning Coordinator. List the steps the coordinator should take to maintain this plan. Some steps could be to

1. Develop a timetable to test the plan (at least once a year).
2. Keep the plan updated with the most recent information.
3. Make sure the plan is safeguarded at the office and a copy is on file at a secured off-site location.

Electronic Recordkeeping

Computers produce electronic records, including numeric, graphic, and text information, which may be stored on any storage medium capable of being read by a computer. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks.

The creation of electronic records is dependent on the software applications, hardware, operating system, media, and file formats that make up the type of computer system used. The personnel in your organization who are responsible for records should be concerned with — and help other employees understand — the methods used to create your records and the documentation of the system that created the records in order to ensure the ability to retrieve, read, and use those records in the future.

Each electronic storage medium can be classified into two types, magnetic media and optical media. Each type has certain benefits and drawbacks. For example, information stored on magnetic media (for example, hard and floppy disks) is more prone to corruption by outside sources (such as strong magnetic fields). Optical media (such as CD-ROMs) are not prone to magnetic corruption but can be damaged by deep surface scratches that prevent the laser from reading the data stored on the disc.

Examples of commonly used storage media include

- ✓ Hard disks
- ✓ 3.5-inch floppy disks
- ✓ Zip disks
- ✓ CD-ROMs (for example, CD-R, CD-RW, and DVD)
- ✓ Flash memory
- ✓ Tape cartridges

The above are just a few of the many types of electronic storage media currently in use. Storage technology is always evolving; new media and formats are constantly being developed and introduced. Users, network administrators, and security management personnel should jointly and periodically reevaluate electronic media suitable for business or archival purposes. Each storage medium has a different life span. Because of this, recorded data may need to be transferred to a new type of storage medium or format to extend its preserved life.

The proper selection of software, media, and file formats to be used for creating electronic records ensures that those records are adequately readable, retrievable, and duplicated until such time as they are no longer needed. Instructions for retrieval or preservation must be documented in a manner to ensure long-term usage. This should include physical attributes of the records, hardware, and software platforms required to retrieve the records.

Implementing and maintaining an effective records security program should incorporate the following:

- ✓ Ensure that only authorized personnel have access to electronic records
- ✓ Provide for backup and recovery of records to protect against information loss
- ✓ Ensure that appropriate personnel are trained to protect sensitive or classified electronic records
- ✓ Minimize the risk of unauthorized alteration or erasure of electronic records

Authentication of Electronic Records

Authentication is confirmation that the record is accurate and complete. All records requiring authentication must be dated and signed, initialed, stamped, or otherwise attested. Usually, paper records can easily be authenticated because most forms of hard copy record authentication are visible on the front of the record. Methods for the authentication of electronic records, however, are more diverse. These methods include, but are not limited to, the following:

- ✓ A hard copy of a document that accompanies the electronic media containing information about the electronic record that can be used for identifying, retrieving, or indexing
- ✓ Attaching an authentication label to the media
- ✓ Linking a digital signature to the electronic file or document

Electronic Records as Evidence

As mentioned in Chapter 2, electronic records may be admitted as evidence for use in court proceedings only when a strict chain-of-custody is followed. Organizations should implement the following procedures to improve the legal admissibility of electronic records:

- ✓ Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.
- ✓ Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions.
- ✓ Identify the electronic media on which records are stored throughout their life cycle, and the maximum time that records remain on each type of storage medium.
- ✓ Coordinate all of the foregoing with appropriate senior management staff and legal counsel.

Records Security

Those who create malicious code are finding more effective ways to circumvent such security measures as antivirus programs, intrusion detection systems, and firewalls. To make matters worse, new forms of malicious code are beginning to appear that ensure that attachments need not be opened in order to infect a computer. In addition, viruses, worms, and Trojan horses can search out the most damaging information (for example, files containing words such as “confidential,” “private,” “privileged,” “clinical,” or “password”) to send out to selected e-mail addresses found in the infected computer’s memory or to predetermined e-mail addresses.

When it comes to information security, the more levels of protection your organization employs, the tougher it is for a hacker, cracker, or malicious agent to compromise your system or steal critical data. For example, you may find it beneficial to keep critical or sensitive data in encrypted form on a removable medium (for example, floppy, Zip, or CD-RW disk), rather than on the system hard drive. This permits you to keep the media stored safely in a secure area. Using antivirus programs with frequently updated virus definitions, installing an appropriate firewall, keeping sensitive data on floppies, disconnecting the computer when it is not in use, using sophisticated password systems and encryption, and applying other, similar approaches all contribute to preventing sensitive data from being compromised. Additionally, your organization should implement and maintain an effective records security program that incorporates the following:

- ✓ Ensure that only authorized personnel have access to electronic records.
- ✓ Minimize the risk of unauthorized modification or erasure of electronic records by storing sensitive data on removable media.
- ✓ Ensure that appropriate personnel are trained to protect sensitive or classified electronic records.
- ✓ Provide for backup and recovery of records to protect against information loss.
- ✓ Ensure that electronic records security is included in your organization's overall information security plans.

The Uninterruptible Power Supply

It's a fact of life: electronic devices (computer systems included) are sometimes subject to electrical power disturbances. Computer hardware can be subjected to damage when a power surge or voltage spike occurs in its external alternating current (AC) power source. In addition to hardware damage, data loss can also occur when there is a sudden drop in voltage (power sag), or when a complete blackout occurs. These power disruptions may also cause the CPU and peripherals to face intermittent problems such as keyboard lockups, hardware performance degradation, or complete loss of data.

An uninterruptible power supply (UPS) is an important part of an incident response plan because it acts as a comprehensive power delivery system. In the event of a power failure, a generator may not supply the uninterrupted power required to maintain your computer system operation. A UPS is essentially a battery that sits between a computer and the AC electrical power; the AC keeps it charged and running, and the UPS supplies even, stable power to your computer when its external AC power fails.

How UPS Works

There are two different types of systems in use today: a continuous UPS and a standby UPS. The standby UPS is designed so that the source of power normally used is the primary power source or (AC) outlet power. The secondary power source, the UPS battery, only kicks in if the primary source of power is disrupted. In other words, the AC power from the wall is always one of these sources, and the battery contained within the UPS is the other. A switch is employed to control which of these sources powers the equipment at a given time. The switch changes from the primary source to the secondary only when it detects that the primary power has gone out. It switches back from the secondary power source to the primary when it detects that the primary power source has returned.

In a continuous UPS, the computer is always running off battery power, with the battery continuously being recharged by an external AC power source. The benefit of this type of UPS is that there is no switchover necessary. This setup provides a stable and constant supply of power.

Standby UPS systems are commonly found in the small-office/home-office (SOHO) environment because they cost far less than the continuous type of UPS. While more costly than the standby type, the continuous UPS does provide extremely clean, stable power and as such is more likely to be used with critical applications.

UPS Benefits

Regardless of which type of UPS is employed, when a sudden loss of AC power occurs, the battery in the UPS will supply power long enough for your personnel to save and close files, and to properly power down their computers. UPS protection ensures that equipment will not be damaged and that valuable data and personalized settings will be preserved. Many UPS system have audible alarms that alert users to changes in the operating environment and battery conditions. In addition, some UPS systems offer unattended safe shutdown of many operating systems in the event a power failure occurs while the computer or server is unattended, for example at night or on weekends.

Purchasing a UPS

Before purchasing a UPS, you must first decide on the level of protection required to meet your organization's specific needs. A UPS should be able to supply power to the computer long enough to facilitate a smooth and orderly shutdown, thus avoiding the normal file corruption and other problems associated with a sudden interruption in service. In general, a UPS should provide power for at least 10 to 20 minutes to allow users enough time to save their work and terminate running programs. Since the majority of power problems last only a short duration, UPS protection should eliminate loss of service for the majority of the electrical problems encountered in most office environments. The size of the UPS you need depends on the amount of power your computer consumes. If you have a standard desktop computer with only one internal hard drive, a small UPS (such as the popular APC Back-UPS 300) should suffice. For a computer or server with several hard drives or numerous peripherals, a larger UPS will be required. For more information on UPS performance and sizing, visit the American Power Conversion Corporation UPS selector Web site at `www.apcc.com/template/size/apc` for further details.

Understanding Data Backup Procedures

Data backup is something everybody needs to do but many of us neglect to do regularly. When disaster strikes, a backup may be the only hope of retrieving some original data. Several antivirus and Internet security products automatically back up critical data and some even place that data on protected areas of the user's hard drive. However, some hackers are so sophisticated that even the best security measures may not be sufficient to thwart an attack. When a savvy hacker succeeds at destroying data, well-planned regular backups can save a great amount of time, money, and aggravation. Critical data should be backed up more frequently, perhaps daily or even more often for vitally important data. Noncritical data can be backed up less frequently; a weekly or monthly backup would be sufficient if the bulk of the data doesn't change frequently.

The three types of backups commonly used are as follows:

- ✓ **Normal:** Normal backups copy all selected files and then mark all the files as backed up. The advantage to this type of backup is that it allows you to quickly restore files with a minimal amount of data loss because all current files are on the backup. The drawback to this type of backup is that it is very time-consuming.
- ✓ **Differential:** Differential backups copy only files that have been added or changed since the last differential backup was performed but do *not* mark the files as backed up. Restoring files only requires that you start with the last full backup, then move directly on to the last differential backup. The advantage to this type of backup is that it is faster, while the disadvantage is that it requires longer file restoration because files are not in one continuous piece.
- ✓ **Incremental:** Very similar to differential backups, incremental backups copy only files that were added or changed since the last full or incremental backup. Conversely, unlike differential backups, they *do* mark the files as backed up. To restore files one only needs to start with the last full backup, then perform the increments in their respective order. The advantage to this type of backup is that it consumes the least amount of time and space.

Creating a Backup Plan

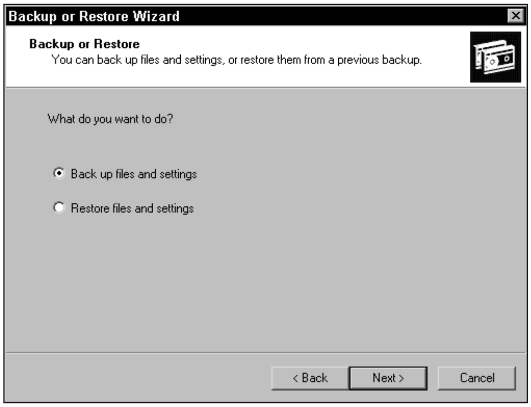
It is important that your organization designate one person as coordinator and record keeper of all backups. A backup plan should be created, put in writing, and kept with the organization's security policies and procedures documentation. The following items should be included in the backup plan:

- ✓ The name of the backup coordinator and/or record keeper
- ✓ The type of data requiring backup
- ✓ The frequency of data backups
- ✓ The location of on-site data storage
- ✓ The location of offsite data storage
- ✓ The method used for backing up data along with a checklist of procedures

Data Backup Tools

Numerous tools are available for individuals and organizations to make the process of backing up data easy and painless. Nearly all backup software programs provide for this process to be carried out automatically. The use of automation ensures that performing regular data backups is not put off or forgotten. For users of Unix or Linux, many freeware programs with this automated feature are available at `www.storagemountain.com`. For Macintosh users, freeware backup software can be found at `www.versiontracker.com`. Windows users, for the most part, need to look no further since backup software is provided with the Windows operating system. While the built-in Windows backup program may lack some of the advanced features of more sophisticated third-party backup products, it has enough functionality to make it very useful to individuals and organizations alike.

The backup programs provided by later versions of Windows — like 2000 and XP — have dramatically improved over earlier versions. In Windows XP for example, the built-in backup software is located in the System Tools folder under Accessories in the Start menu. For other Windows versions, users need to check their manuals for the exact location of the backup program. Once activated, the Backup and Restore Wizard queries the user as to whether a backup or restoration of data is desired (see Figure 9-1). The next screen prompts users to select which files on their computer they wish to back up (see Figure 9-2). There are several options here. However, if users select the last option, “Let me choose what to back up,” they are then provided with a screen that requires them to select which files they wish to back up (see Figure 9-3). After selecting the appropriate files, users are then prompted to choose a destination for their backup data (see Figure 9-4). In this illustration, the recipient of the backup data is an Iomega ZIP drive. Backups can be written to other media types, as well, such as a tape drive or a CD-R disk.



Backup or Restore

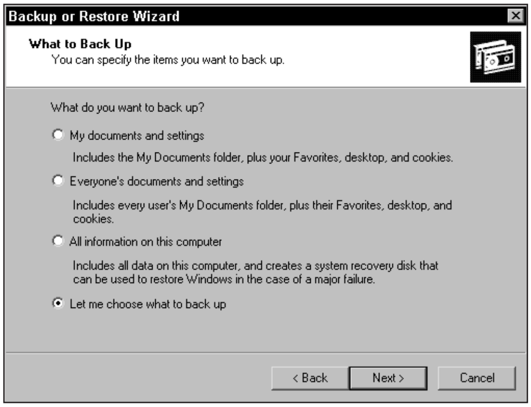
You can back up files and settings, or restore them from a previous backup.

What do you want to do?

● Back up files and settings

○ Restore files and settings

Figure 9-1: The Backup or Restore Wizard under Windows XP Pro



What to Back Up

You can specify the items you want to back up.

What do you want to back up?

○ My documents and settings

Includes the My Documents folder, plus your Favorites, desktop, and cookies.

○ Everyone's documents and settings

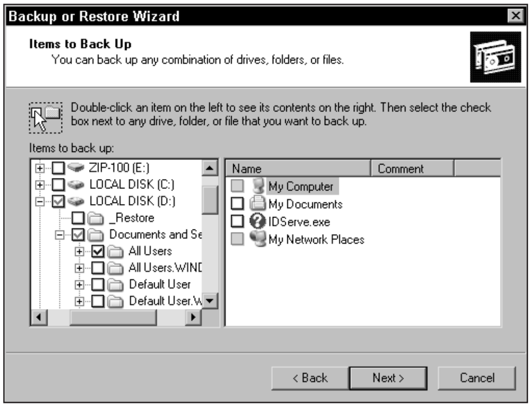
Includes every user's My Documents folder, plus their Favorites, desktop, and cookies.

○ All information on this computer

Includes all data on this computer, and creates a system recovery disk that can be used to restore Windows in the case of a major failure.

● Let me choose what to back up

Figure 9-2: Specifying what you want backed up using the Backup and Restore Wizard for Windows XP Pro



Backup or Restore Wizard

Items to Back Up

You can back up any combination of drives, folders, or files.

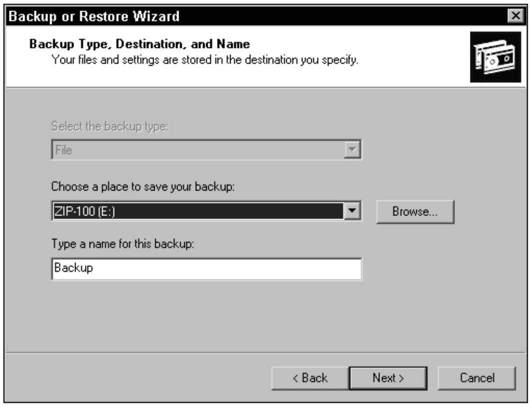
Double-click an item on the left to see its contents on the right. Then select the check box next to any drive, folder, or file that you want to back up.

Items to back up:

- □ ZIP-100 (E:)
- □ LOCAL DISK (C:)
- ☑ LOCAL DISK (D:)
  - □ _Restore
  - ☑ Documents and Se
    - ☑ All Users
    - □ All Users.WINE
    - □ Default User
    - □ Default User.W

Name	Comment
□ My Computer	
□ My Documents	
□ IDServe.exe	
□ My Network Places	

Figure 9-3: Backing up combinations under the Backup and Restore Wizard for Windows XP Pro



Backup or Restore Wizard

Backup Type, Destination, and Name

Your files and settings are stored in the destination you specify.

Select the backup type: File

Choose a place to save your backup: ZIP-100 (E:)

Type a name for this backup: Backup

Figure 9-4: Choosing the destination for saving your backup under the Backup and Restore Wizard for Windows XP Pro

Post-Incident Monitoring and Analysis

Learning from mistakes is an essential component of incident response. Do not wait until the next attack occurs to learn from a previous attack. It is important to take the time after each incident to see if any procedures, processes, tools, techniques, and configurations need to be modified or improved.

In the wake of a computer security incident, several actions should take place. These actions can be summarized as follows:

- ✓ Validate the attack has subsided
- ✓ Examine files and logs for details of the attack

- ✓ Determine if legal action is warranted or possible
- ✓ Reevaluate or modify overall computer network security

After an incident has been resolved, a *postmortem* should be conducted so that the organization can learn from the experience and, if necessary, update its procedures. The following types of incident information should be examined:

- ✓ How the incident started
- ✓ Which vulnerabilities or flaws were exploited
- ✓ How access was gained
- ✓ How the organization became aware of the incident
- ✓ How the incident was eventually resolved
- ✓ Whether existing incident response procedures were adequate or require updating

As a result of a post-incident analysis, computer security personnel may need to issue alerts or warnings to all organization employees about actions to take to reduce vulnerabilities that were exploited during the incident. The organization may also need to update any computer operations manuals to reflect new procedures. In addition, computer security personnel should use a post-incident analysis to ascertain its impact on the organization in handling and resolving the incident.

Anticipating Future Attacks

Each day organizations around the globe face the daunting challenge of protecting the integrity, confidentiality, and availability of their digital assets. The vulnerability of a corporation's digital assets remains a growing concern. Properly anticipating and planning for unforeseen disruptions to business operations is increasingly important in remaining competitive in today's business environment. From hackers breaking in and sabotaging systems to malicious code destroying and deleting critical data, disruptions can cost companies millions of dollars in losses. Being aware of the different methods used by hackers attempting to infiltrate an organization's network will allow those in charge of information security to better anticipate and defend against such attacks.

It's an unfortunate fact that for years hackers have been exploiting security weaknesses of Internet-connected computers. The Internet is a public network and the number of worldwide users with access to the Internet is staggering. Current estimates put the global Internet population at over 500 million. Since anyone with an Internet connection has the potential to be a hacker or cracker, cyberspace can be a dangerous place. Hackers now have more tools available than ever before. With the number of reported attacks increasing daily, the need to anticipate future attacks has never been more critical.

Fortunately, not all computer attacks are successful. In fact, many hacking attempts are performed simply to "acquire" information about a computer system — to scan for weaknesses or vulnerabilities or in preparation for a future attack. Employing the tools of the trade or by using social engineering, hackers can install backdoors or guess passwords to surreptitiously gain illegal entry into an Internet-connected system. In extreme cases, attacks have caused entire systems and networks to crash, denied computer service to legitimate users, or resulted in the theft of large sums of money. The following press release from the U.S. Department of Justice shows just how easy it is for hackers located halfway around the globe to access and defraud, in this instance, online monetary exchange systems.

> October 4, 2002 U.S. Department of Justice
> United States Attorney
> Western District of Washington
>
> **RUSSIAN COMPUTER HACKER SENTENCED TO THREE YEARS IN PRISON**
>
> John McKay, United States Attorney for the Western District of Washington, and Charles E. Mandigo, Special Agent in Charge, Seattle Division, Federal Bureau of Investigation, announced today that Chief United States District Judge John C. Coughenour has sentenced VASILIY GORSHKOV, age 27, of Chelyabinsk, Russia, to serve 36 months in prison for his convictions at trial last year on 20 counts of conspiracy, various computer crimes, and fraud committed against Speakeasy Network of Seattle, Washington; Nara Bank of Los Angeles, California; Central National Bank of Waco, Texas; and the online credit card payment company PayPal of Palo Alto, California. GORSHKOV also was ordered to pay restitution of nearly $700,000 for the losses he caused to Speakeasy and PayPal.
>
> According to evidence presented at trial and other court records:
>
> GORSHKOV was one of two men from Chelyabinsk, Russia, who were persuaded to travel to the United States as part of an FBI undercover operation. The operation arose out of a nationwide FBI investigation into Russian computer intrusions that were directed at Internet Service Providers, e-commerce sites, and online banks in the United States. The hackers used their unauthorized access to the victims' computers to steal credit card information and other personal financial information, and then often tried to extort money from the victims with threats to expose the sensitive data to the public or damage the victims' computers. The hackers also defrauded PayPal through a scheme in which stolen credit cards were used to generate cash and to pay for computer parts purchased from vendors in the United States. The FBI's undercover operation was established to entice persons responsible for these crimes to come to U.S. territory.
>
> As part of the operation, the FBI created a start-up computer security company named "Invita" in Seattle, Washington. Posing as Invita personnel, the FBI communicated with GORSHKOV and the other man, Alexey Ivanov, by e-mail and telephone during the summer and fall of 2000. The men agreed to a face-to-face meeting in Seattle. As a prelude to their trip to the United States, the FBI arranged a computer network for the two men to hack into and demonstrate their hacking skills. The men successfully broke into the test network.
>
> GORSHKOV and Ivanov arrived in Seattle, Washington, on November 10, 2000, and a meeting was held at the office of Invita. Unbeknownst to the Russian men, the participants in the meeting were undercover FBI agents and the meeting was recorded on audio and video tape. During the meeting, GORSHKOV discussed their hacking prowess and took responsibility for various hacking incidents and activities. GORSHKOV shrugged off any concern about the FBI, explaining that the FBI could not get them in Russia. When asked about their access to credit cards, GORSHKOV declined to talk about it while they were in the United States and added that "this kind of question is better discussed in Russia."
>
> At the conclusion of the Invita undercover meeting, the two men were arrested. Ivanov was transported to the District of Connecticut to face charges for a computer intrusion at the Online

> Information Bureau of Vernon, Connecticut. GORSHKOV and Ivanov were charged in the Western District of Washington with conspiracy and 19 additional crimes involving Speakeasy, Nara Bank, Central National Bank — Waco, and PayPal.
>
> A few days after the two men were arrested, the FBI obtained access via the Internet to two of the men's computers in Russia. The FBI copied voluminous data from the accounts of GORSHKOV and Ivanov and examined the data pursuant to a search warrant issued by a United States Magistrate Judge. GORSHKOV's pretrial challenge to the FBI's copying and search of the Russian data was denied by Chief Judge Coughenour in a written order dated May 23, 2001.
>
> The data copied from the Russian computers provided a wealth of evidence of the men's computer hacking and fraud. They had large databases of credit card information that was stolen from Internet Service Providers like Lightrealm of Kirkland, Washington. More than 50,000 credit cards were found on the two Russian computers. The Russian computers also contained stolen bank account and other personal financial information of customers of online banking at Nara Bank and Central National Bank — Waco.
>
> The data from the Russian computers revealed that the conspirators had gained unauthorized control over numerous computers — including computers of a school district in St. Clair County, Michigan — and then used those compromised computers to commit a massive fraud involving PayPal and the online auction company e-Bay. The fraud scheme consisted of using computer programs to establish thousands of anonymous e-mail accounts at e-mail web sites like Hotmail, Yahoo!, and MyOwnEmail. GORSHKOV's programs then created associated accounts at PayPal with random identities and stolen credit cards. Additional computer programs allowed the conspirators to control and manipulate e-Bay auctions so that they could act as both seller and winning bidder in the same auction and then effectively pay themselves with stolen credit cards.
>
> The case was investigated by FBI Special Agents Marty Prewett and Michael Schuler, who were awarded the Director's Annual Award for Outstanding Criminal Investigation by the Director of the FBI for their work on the case.

Any number of flaws or weaknesses can leave computer systems vulnerable to attack. Remember, they are most vulnerable in the following situations:

- ✓ Inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords.
- ✓ Weak passwords are chosen that can be easily guessed.
- ✓ An identified system or network security weakness goes uncorrected.
- ✓ Intentionally designed malicious threats install software programs that compromise or damage information and systems.

Attackers employ a variety of different methods to exploit vulnerable computer systems. Here are some examples:

- ✓ **Password cracking.** A technique in which attackers try to guess or steal passwords to obtain access to computer systems

- ✓ **Sendmail.** A common type of attack in which the attacker installs malicious code in an electronic mail message that adds a password into the system's password file, thereby giving the attacker total system privileges
- ✓ **Packet sniffing.** A technique in which attackers surreptitiously insert a software program that captures passwords and user identifications

Once access has been gained, hackers use the computer system as though they were legitimate, authorized users. Employing a variety of techniques, hackers often attempt to cover their tracks to avoid detection and then steal information both from the systems compromised as well as the systems connected to them.

Chapter Summary

No single disaster recovery plan will fit every organization's needs. Disaster recovery plans should be tailored to fit your organization's security requirements and exposure to risk. Since disaster recovery plans provide detailed information and well-defined procedures, they act as blueprints to guide critical decisions and operations in times of emergency. Disaster recovery procedures can include any number of events including post-compromise restoration, validation, and monitoring of network computer systems. Knowing how to react properly in an emergency is critical to making quick decisions that mitigate damage and quickly restore operations.

Key points covered in this chapter include

- ✓ The benefits of advanced planning when preparing a disaster recovery plan
- ✓ The importance of incident recordkeeping and its overall role in an organization's business continuity planning
- ✓ Why uninterruptible power supply (UPS) and backup procedures are indispensable to an organization's disaster and business continuity plan
- ✓ How examining previous attacks can help shape future incident response and business continuity planning
- ✓ Why anticipating and planning for unforeseen disruptions to business operations helps organizations remain competitive in today's business climate

Chapter 10

Responding to Different Types of Incidents

In This Chapter

- ✓ Responding to hacker or cracker attacks
- ✓ Responding to malicious code attacks
- ✓ Handling inappropriate use
- ✓ Recognizing and managing incidents involving sexual harassment
- ✓ Understanding industrial espionage
- ✓ Defending against insider attacks

PREPARING TO HANDLE A COMPUTER SECURITY INCIDENT HAS NOW BECOME A TOP PRIORITY for many computer system administrators. With virus attacks and stories of hackers abounding, organizations are becoming more diligent about protecting their information assets than ever before. As organizations increase their Internet presence and dependency on information technology assets, the number of computer incidents will rise. After an incident occurs is, of course, too late to begin planning how to address the situation. A computer security incident can occur at any time of the day or night, although most hacker/cracker incidents occur during off-hours when hackers do not expect system managers to be tending their flock. In contrast, worm and virus incidents can occur any time of the day. Thus, time and distance considerations in responding to incidents are very important. This chapter focuses on various types of common computer security incidents and the basic procedures to contain and mitigate their damage.

Responding to Hacker Incidents

Hacker incidents require a somewhat different response than do virus incidents. Some hackers are highly skilled, employ sophisticated techniques, and will go to great lengths to avoid being detected. To complicate matters further, a hacker can also be someone working for an organization (an insider) engaging in after-hours illegal activity, such as unauthorized access to sensitive information or perhaps password cracking. Whether they originate from the inside or outside, all hacker incidents need to be addressed as real threats to organizational computer systems.

Hacking incidents can be divided into three general categories:

- ✓ Those involving attempts to gain access to a system
- ✓ Active, or live, sessions on a system
- ✓ Events discovered after the fact

Of the three, an active hacker session is the most severe and must be dealt with as soon as possible. There are two basic methods for handling an active hacking incident. The first method is to quickly lock the hacker out of the system. To do this, you must first identify the hacker's point of entry into the system. Here are some common entry points that hackers look for when seeking to gain a way in:

- ✓ **Port access.** It is common for Internet applications to be configured to listen on a predefined port for incoming connections. Hackers routinely use port scanners to look for open TCP/IP ports as a possible means to gain entry. They can use these open ports to connect to your system and gain access to your data. The more ports that are open on a system, the greater the likelihood of intrusion.
- ✓ **Internet access.** Hackers often write simple scripts that randomly generate and ping large groups of IP addresses, looking for computers or servers that respond. The response is called a *ping acknowledgement* and is a standard feature of the popular ping utility. Once an IP address responds, the hacker will then attempt to gain access to the server via a common protocol called TELNET. TELNET is the main Internet protocol for creating a connection with a remote machine. It gives the user the opportunity to be on one computer system and do work on another, which may be across the street or thousands of miles away. When users log in to a TELNET server, they usually type an account name and password. Hackers can log TELNET sessions and possibly configure the TELNET program to record username and password combinations.
- ✓ **Trojan horse.** Trojan horses are a bit different from viruses. They're transmitted the same ways as viruses, but they don't replicate nor do they make themselves obvious. Instead, they sit quietly on your Internet-connected computer system and generate open ports. Hackers trawl for computers that have been infected by Trojan horses and then use them to gain access to those systems. BackOrifice and NetBus are examples of well-known Trojan horses.

The second method is to allow the hacker to continue his or her attack while you attempt to collect potential information that could lead to identification and possible criminal conviction of the hacker. One method for identifying the source of an attack(s) is by carefully examining system log files and active network connections. Be sure to make copies of all audit trail information. Capture system process and status information in a separate file, and then store that file in a safe place. Programs like Process Explorer, by Mark Russinovich (`www.sysinternals.com`), are excellent for this task.

Identify the Hacker

Once the source of the attacks has been identified, the next step is attempting to obtain the identity of the hacker or cracker. In his May 2001 bulletin "Tracking a Computer Hacker," Daniel A. Morris, Assistant United States Attorney Computer and Telecommunications Coordinator for the District of Nebraska states the following:

> Clues to the identity of a hacker often exist in cyberspace and in the real world if the investigator knows where to look. Computer systems of interest to hackers usually keep track of all authorized and unauthorized access attempts. Records, called computer logs, provide useful and often critical clues that a trained agent or computer specialist can use as the starting point to trace the route taken from computer to computer through the worldwide web, to discover the one computer out of the millions in the world from which an intrusion was conducted.
>
> All computers using the Internet are assigned a different numeric Internet Protocol (IP) address while online, similar to country, city, street, and number addresses for houses. Unless the hacker alters the victim's logs once he or she gains unauthorized access, the victim's logs should list the precise computer address from which unauthorized access was gained. That address may not be the hacker's own computer, but instead another computer that the hacker has hijacked or an account that he owns on a third party's computer, as discussed in more detail below.
>
> Lookup tools are available online to identify the owner of the network through which an attack was launched. To see how this works, see `www.arin.net`, operated by the American Registry of Internet Numbers.
>
> **Obstacles to Identifying the Hacker**
>
> Because of the make-up of the Internet, it is sometimes difficult for law enforcement officers to discover the identity of a hacker.
>
> 1. A hacker might hide or "spoof" his Internet Protocol (IP) address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. Subpoenas and court orders to each bounce point may be necessary to identify the hacker.
> 2. Some victims don't keep logs or don't discover a hacker's activities until it is too late to obtain records from the hacker's Internet Service Provider (ISP). A victim who has no record of the IP address of the computer from which unauthorized access was gained limits law enforcement officers to traditional investigative techniques, which alone may be inadequate to identify the hacker.
> 3. Some ISPs don't keep records or don't keep them long enough to be of help to law enforcement officers. When the investigator determines the identity of an ISP from which records will be needed, the prosecutor should send a retention letter under 18 U.S.C. § 2703(f) requiring the ISP to preserve the records while a court order or other process is being obtained.
> 4. Some computer hackers alter the logs upon gaining unauthorized access, thereby hiding the evidence of their crimes.

5. Some leads go through foreign countries, not all of which consider hacking a crime. Treaties, conventions, and agreements are in place with some countries, and there are "24/7" contacts in dozens of countries around the world who can be contacted for help. When a lead points to a foreign country, the investigator should contact a CTC or CCIPS attorney at `www.cybercrime.gov`.

Some of the information investigators need to track a hacker might be readily available to the general public on the Internet. No special restrictions apply to an investigator's access to and use of such information — in the same way that information available in a public library can be used by investigators without special authorization. Common search engines such as `www.dogpile.com`, `www.lycos.com`, `www.excite.com`, `www.google.com`, or `www.netscape.com` may be used to find information about a username or nickname of the person or group claiming credit for a computer intrusion.

Active Hacker Incidents

Active hacker incidents include any live or current hacker activity or commands initiated by an unauthorized individual. Examples of active hacker activity include the following:

- ✓ Active rlogin (remote login)
- ✓ Active TELNET session (terminal emulation)
- ✓ Active FTP session (file transfer protocol session)
- ✓ Successful callback attempts

As mentioned earlier in this chapter, when active hacker activity is discovered, one of two decisions must be made. Your organization can either allow the activity to continue while you gather evidence or sever the hacker's access thereby effectively locking the hacker out of the system. Since a hacker can cause a significant amount of damage in a very short time, it is critical that a quick reaction be taken when responding to active hacker attacks. If a decision is made to remove that hacker from the system, the following steps should be taken:

- ✓ **Lock out the hacker.** Kill all active or running processes that the hacker is using and remove any files or programs that he or she may have left on the system. Change passwords on any accounts accessed by the hacker/cracker and be sure to keep a log of all actions taken.
- ✓ **Restore the system.** Restore the system to a normal state, and restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Also, install patches for other vulnerabilities of which the hacker may not have taken advantage, and inform the appropriate people. All actions taken to restore the system to a normal state should be documented in the logbook for this incident.

- ✓ **Notify authorities.** Once the incident has been contained and the hacker removed from the system, the next step is to contact the appropriate authorities. Several agencies (see Table 10-1) can be called upon once an incident has occurred and been detected.
- ✓ **Follow-up.** After the investigation is complete, a report describing the incident should be written and distributed to all incident response and security personnel. It should include all actions that were taken by the organization in response to the incident.

Table 10-1 Computer Crime Contact Information (U.S. Dept. of Justice)

Type of crime	Appropriate federal investigative law enforcement agencies
Computer intrusion (hacking)	**FBI local office**
	NIPC Online reporting: www.nipc.gov Tel: 202-323-3205 Toll-free: 888-585-9078 E-mail: `nipc.watch@fbi.gov`
	U.S. Secret Service local office
Password trafficking	**FBI local office**
	NIPC Online reporting: www.nipc.gov Tel: 202-323-3205 Toll-free: 888-585-9078 E-mail: `nipc.watch@fbi.gov`
	U.S. Secret Service local office
Copyright (software, movie, and sound recording) piracy	**FBI local office**
	If imported, **U.S. Customs Service** Local office Toll-free: 800-BE-ALERT or 800-232-2538
Theft of trade secrets	**FBI local office**

Continued

Table 10-1 Computer Crime Contact Information (U.S. Dept. of Justice) *(Continued)*

Type of crime	Appropriate federal investigative law enforcement agencies
Trademark counterfeiting	**FBI local office**
	If imported, **U.S. Customs Service** Local office Toll-free: 800-BE-ALERT or 800-232-2538
Counterfeiting of currency	**U.S. Secret Service local office**
	FBI local office
Child pornography or exploitation	**FBI local office**
	If imported, **U.S. Customs Service** Local office Toll-free: 800-BE-ALERT or 800-232-2538
ContinuedChild exploitation and Internet fraud matters that have a mail nexus	**U.S. Postal Inspection Service local office**
Internet fraud	**The Internet Fraud Complaint Center**
	FBI local office
	U.S. Secret Service local office
	Federal Trade Commission
	If securities fraud, **Securities and Exchange Commission**
Internet harassment	**FBI local office**
Internet bomb threats	**FBI local office**
	ATF local office
Trafficking in explosive or incendiary devices or firearms over the Internet	**FBI local office** **ATF local office**

Monitoring Hacker Activity

There is no single procedure for monitoring the activity of a hacker. Each incident needs to be handled on an individual basis. Once the decision has been made to cease monitoring a hacker's activities and instead have the hacker removed from the system(s), the aforementioned procedures for removing the hacker should be followed.

Previous Incidents

Occasionally, there are cases where a computer security incident is discovered after the fact. When this happens, there is not always a lot of evidence available to identify who infiltrated the system or how they gained access to the system. When an employee discovers that someone successfully hacked into the organization's computer system, he or she should notify incident response team personnel within one working day.

Follow-Up

After the investigation is complete, a report describing the incident and actions that were taken should be written and distributed to all computer security personnel in your organization.

Responding to Malicious Code Incidents

While malicious code presents itself in several differing forms (for example, viruses, worms, or Trojan horses), the key procedures for handling them are nearly the same — for example, system isolation and the need for a quick response. A computer virus is a small program written to modify or change the way a computer operates. In general, a computer virus must meet two requirements:

- ✓ It must be self-executing.
- ✓ It must self-replicate.

Some viruses are designed to disrupt normal computer operations by damaging applications, deleting files, or, in extreme cases, reformatting the hard disk. Others are better classified as nuisances and are not designed to cause any real lasting harm. Instead of causing damage, benign viruses simply replicate themselves and make themselves known by presenting users with audio, video, or text messages. Even these so-called "harmless" viruses, however, can create problems for an organization's network by occupying computer memory used by legitimate programs and slowing down system operations.

Trojan Horses

While they are more sophisticated than a simple computer virus, Trojan horses are destructive programs that masquerade as harmless applications. Unlike viruses, Trojan horses do not self-replicate; however, they can be equally caustic. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead *introduces* viruses onto your computer.

Internet Worms

Computer worms pose a serious threat to the Internet, because they are self-replicating and self-sustaining programs — often transmitted via e-mail messages — that infect vulnerable systems, sometimes with disastrous results, other times with minimal impact. Their automatic nature makes them powerful, fast-spreading, and destructive. A worm is comparable to a virus in many aspects, except that it is a self-contained program that is able to rapidly spread functional copies of itself — or its segments — to other computer systems over networks without depending upon other programs to host its code. Viruses, on the other hand, typically need to attach themselves to host programs in order to spread.

Isolate the System and Notify Appropriate Staff

Once a computer virus, worm, or Trojan horse is discovered, the infected computer(s) must be isolated from the remaining network computers as soon as possible. When a worm is suspected, a decision must be made to disconnect the LAN from the Internet. Isolation is one simple method for quickly halting the spread of a worm. Systems suspected of being infected should not be powered off or rebooted. This is because some viruses infect a computer's boot sector and thereby may destroy some or all of the hard disk data if the system is rebooted. Additionally, rebooting a system could destroy needed information or evidence. Finally, notify incident response personnel as soon as any malicious code is detected. If unable to reach them, contact any backup personnel.

Contain the Virus, Worm, or Trojan Horse

All suspicious processes should now be halted and removed from the system. Make a full backup of the system and store that backup in a safe place. The tapes should be carefully labeled so unsuspecting people will not use them in the future. After that, remove all suspected infected files or malicious code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until computers have been cleaned to prevent further spread.

Inoculate the System

Once the malicious code has been contained, your next step is to use up-to-date antivirus software to remove remaining virus code. In addition, you should update and patch operating systems and applications against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been quickly stopped, then the task of assessing the damage is not especially difficult. However, if the malicious code was successful and caused significant damage, it may then be best to restore the system from backup tapes. Once the system is brought back into a safe mode, then any patches or fixes should be implemented and tested.

Return Systems to Normal Operating Mode

Prior to bringing systems back into normal function, all users should be notified that the systems are returning to a fully operational state. It is recommended that all users change their passwords. Before restoring connectivity to the Internet, verify that all affected parties have successfully eradicated the problem and inoculated their systems.

Handling Inappropriate Use

The orderly and smooth operation of an organization's computer network relies upon the proper conduct of the users who must adhere to strict computer use guidelines. In general, this requires efficient, ethical, and legal utilization of the network resources. In other words, all computing resources must be used in an ethical and responsible manner. Use of information technology resources can be broadly categorized as acceptable, tolerable, or prohibited:

- ✓ **Acceptable use** of information technology resources is legal use consistent with the organization's acceptable computer use policies.
- ✓ **Tolerable use** is legal use for other purposes that do not impinge on the organization's acceptable use policy.
- ✓ **Prohibited use** is illegal use and all other use that is neither acceptable nor tolerable.

The following guidelines are intended to help organizations understand and respond to various levels of inappropriate computer use.

- ✓ **Nuisance.** These offenses generally show a lack of consideration of other computer users, but do not threaten privacy or computer integrity or violate any ethical principles. In other words, the individual simply showed poor judgment. The organization should respond by issuing the user a verbal, e-mail, or hardcopy warning that his or her actions were not acceptable.
- ✓ **Questionable Ethics.** These offenses often involve violations where the ethics of actions are in question or when a person's privacy or computer integrity was violated. The organization could respond by suspending the user's account or computer access until a formal session with an Information Technology staff member has been attended. A copy of the organization's Internet access policy should be handed to the user with the specific area or offense highlighted.
- ✓ **Criminal.** This is when a user commits an offense that requires investigation by local, state, or federal law enforcement. Any user committing a criminal offense should forfeit all rights to the organization's computer privileges. Any and all information requested by local, state, or federal law enforcement must be provided. If the user is found guilty of the offense(s) under investigation, his or her employment with your organization should be terminated.

Types of Harassment

The U.S. courts define two categories of sexual harassment, quid pro quo sexual harassment and hostile environment sexual harassment. Quid pro quo occurs when the victim suffers concrete, physical, or economic consequences; for example, an employee being fired, demoted, or failing to receive a promotion for rejecting the sexual harassment. The second type, hostile environment sexual harassment, occurs when there have been unwelcome advances that have been sufficiently "severe or pervasive" so as to alter the terms and conditions of employment, even in the absence of any monetary or economic consequences.

Incidents Involving Sexual Harassment

Nearly every workplace today conducts some element of its business operations through the use of computers. While computers aid in workplace efficiency, widespread computer use also gives rise to a whole new set of workplace concerns.

Sexual harassment is unwanted attention of a sexual nature by a person or persons who knowingly or should have reasonably known that the attention is unwelcome to the recipient or recipients. Sexual harassment includes unwelcome advances, requests for sexual favors, or any other unwelcome conduct of a sexual nature (including those via e-mail, instant messaging, and so on). These actions may be in the form of:

- ✓ Repeated offensive sexual flirtations, advances, or propositions
- ✓ Comments of a sexual nature about an individual's body
- ✓ Uninvited physical contact such as touching, hugging, patting, or pinching
- ✓ Suggestive behavior
- ✓ Prolonged staring or leering at a person
- ✓ Jokes containing sexual content in front of people who find them offensive
- ✓ Offensive phone calls
- ✓ Offensive e-mail messages
- ✓ Display of sexually suggestive objects or pictures
- ✓ Offensive reading material

Most people think that sexual harassment involves interpersonal relationships in the workplace. Nevertheless, sexual harassment also covers uses of electronic technology, including e-mail correspondence. Electronic mail usage continues to grow and expand. E-mail messaging is particularly prevalent in the workplace, where most major employers have e-mail systems. This persistent use of e-mail messaging, coupled with the perception that e-mail is temporary, confidential, and informal, results in some shocking and amazing e-mail messages being sent in the workplace. The same holds true for instant messaging. Instant messaging is a type of communications service that enables a user to conduct a private chat with another individual. Typically, the instant messaging system alerts a user whenever somebody on the user's contact list is online. A user can then initiate a chat session with that particular individual. This type of communication constantly searches the Internet or company intranet looking for persons on the contact list. The rapid growth in instant messaging is causing equally rapid growth in risk for any business with employees who use it. Instant messaging, or IM, is another way for employees to get into trouble by posting offensive or inappropriate messages or even as a means to sexually harass another individual.

In 1998, the U.S. Supreme Court increased the liability faced by employers for incidents involving sexual harassment. Two landmark 1998 Supreme Court decisions (one involving the use of e-mail messaging) addressed the issue of an employer's responsibility when one or more supervisors conducts him or herself outside the scope of the employee's authority and creates a sexually hostile work environment for another employee. In these two decisions, the Supreme Court clarified that "An employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee. When no tangible employment action is taken, a defending employer may raise an affirmative defense to liability or damages, subject to proof by preponderance of the evidence. No affirmative defense is available, however, when the supervisor's harassment culminates in a tangible employment action, such as discharge, demotion, or undesirable reassignment."

The court also gave employers a newfound incentive to implement clear and effective sexual harassment guidelines, holding that "while proof that an employer had promulgated an anti-harassment policy with complaint procedure is not necessary in every instance as a matter of law, the need for a stated policy suitable to the employment circumstances may appropriately be addressed in any case when litigating the first element of the defense. And while proof that an employee failed to fulfill the corresponding obligation of reasonable care to avoid harm is not limited to showing any unreasonable failure to use any complaint procedure provided by the employer, a demonstration of such failure will normally suffice to satisfy the employer's burden under the second element of the defense."

Essentially, the Supreme Court stated that the *employer* is responsible for the actions of the employee, even when the employer is unaware of that employee's inappropriate and/or illegal behavior. An employer can no longer claim that they did not know about the sexual harassment because the victim did not inform them, nor can they claim that they were unaware of the perpetrator's behavior. Obviously, your organization must therefore take all possible actions, using available resources — hardware, software, personnel, and so on — to ensure that employees remain in compliance of company policies.

Avoiding Sexual Harassment Lawsuits

Today, in almost every profession, men and women are required to share the same workplace environment. As a result, sexual harassment has become a mounting problem that needs to be addressed seriously. In order to prevent potential sexual harassment litigation issues, organizations must develop, prominently post in central locations, and strongly enforce guidelines that detail what is considered appropriate workplace behavior.

If your organization does not currently have a sexual harassment policy, you should create/obtain one as soon a possible. The organization's sexual harassment policy should communicate that the organization has adopted a "zero tolerance" approach toward sexual harassment. In addition, it should be reviewed by an attorney who specializes in discrimination and labor laws.

Once complete, be sure it is distributed — and redistributed after updating — to all employees either as a handbook or in memo form. You may also wish to have each employee sign it to acknowledge that they've received and have read the policy. The policy, as well as the complaint procedure, should be written in a way that will be understood by all employees in the organization's workforce. Many organizations have employees who are not fluent in the English language. Under this circumstance it may be necessary to have your sexual harassment policy translated or communicated to them in their native language. If feasible, the organization should provide training to all employees to ensure that they understand their rights and responsibilities.

A sexual harassment policy should provide several different avenues for employees to file sexual harassment complaints. They might include:

- ✓ The ability to contact their supervisor
- ✓ A special hotline
- ✓ The ability to contact the human resource department

In addition, the employee should have the option of talking with a male or female organization representative. The organization should ensure that supervisors and managers understand their responsibilities under the organization's anti-harassment policy and complaint procedure. Periodic training of those individuals can help achieve that result. Such training should explain the types of conduct that violate the employer's anti-harassment policy, the seriousness of the policy, the responsibilities of supervisors and managers when they learn of alleged harassment, and the prohibition against retaliation.

Guidelines for Developing a Sexual Harassment Policy

In general, it is the responsibility of employers to establish, publicize, and enforce anti-harassment policies and complaint procedures. As stated by the Supreme Court, "Title VII is designed to encourage the creation of anti-harassment policies and effective grievance mechanisms" (Ellerth, 118 S. Ct. at 2270). While the Court noted that this "is not necessary in every instance as a matter of law," failure to do so will make it difficult for an employer to prove that it exercised reasonable care to prevent and correct harassment.

According to the U.S. Equal Employment Opportunity Commission (EEOC), an anti-harassment policy and complaint procedure should contain, at a minimum, the following elements:

- A clear explanation of prohibited conduct
- Assurance that employees who make complaints of harassment or provide information related to such complaints will be protected against retaliation
- A clearly described complaint process that provides accessible avenues of complaint
- Assurance that the employer will protect the confidentiality of harassment complaints to the extent possible
- A complaint process that provides a prompt, thorough, and impartial investigation
- Assurance that the employer will take immediate and appropriate corrective action when it determines that harassment has occurred

In order to clarify some of the preceding elements, the EEOC offers the following explanations:

Prohibition Against Harassment

An employer's policy should make clear that it will not tolerate harassment based on sex (with or without sexual conduct), race, color, religion, national origin, age, disability, and protected activity (i.e., opposition to prohibited discrimination or participation in the statutory complaint process). This prohibition should cover harassment by anyone in the workplace — supervisors, co-workers, or non-employees. Management should convey the seriousness of the prohibition. One way to do that is for the mandate to "come from the top," i.e., from upper management.

The policy should encourage employees to report harassment before it becomes severe or pervasive. While isolated incidents of harassment generally do not violate federal law, a pattern of such incidents may be unlawful. Therefore, to discharge its duty of preventive care, the employer must make clear to employees that it will stop harassment before it rises to the level of a violation of federal law.

Protection Against Retaliation

An employer should make clear that it will not tolerate adverse treatment of employees because they report harassment or provide information related to such complaints. An anti-harassment policy and complaint procedure will not be effective without such an assurance.

Management should undertake whatever measures are necessary to ensure that retaliation does not occur. For example, when management investigates a complaint of harassment, the official who interviews the parties and witnesses should remind these individuals about the prohibition against retaliation. Management also should scrutinize employment decisions affecting the complainant and witnesses during and after the investigation to ensure that such decisions are not based on retaliatory motives.

Effective Complaint Process

An employer's harassment complaint procedure should be designed to encourage victims to come forward. To that end, it should clearly explain the process and ensure that there are no unreasonable obstacles to complaints. A complaint procedure should not be rigid, since that could defeat the goal of preventing and correcting harassment. When an employee complains to management about alleged harassment, the employer is obligated to investigate the allegation, regardless of whether it conforms to a particular format, or is made in writing.

The complaint procedure should provide accessible points of contact for the initial complaint. A complaint process is not effective if employees are always required to complain first to their supervisors about alleged harassment, since the supervisor may be a harasser. Moreover, reasonable care in preventing and correcting harassment requires an employer to instruct all supervisors to report complaints of harassment to appropriate officials.

It is advisable for an employer to designate at least one official outside an employee's chain of command to take complaints of harassment. For example, if the employer has an office of human resources, one or more officials in that office could be authorized to take complaints. Allowing an employee to bypass his or her chain of command provides additional assurance that the complaint will be handled in an impartial manner, since an employee who reports harassment by his or her supervisor may feel that officials within the chain of command will more readily believe the supervisor's version of events.

It also is important for an employer's anti-harassment policy and complaint procedure to contain information about the time frames for filing charges of unlawful harassment with the EEOC or state fair employment practice agencies and to explain that the deadline runs from the last date of unlawful harassment, not from the date that the complaint to the employer is resolved. While a prompt complaint process should make it feasible for an employee to delay deciding whether to file a charge until the complaint to the employer is resolved, he or she is not required to do so.

Confidentiality

An employer should make clear to employees that it will protect the confidentiality of harassment allegations to the extent possible. An employer cannot guarantee complete confidentiality, since it cannot conduct an effective investigation without revealing certain information to the alleged harasser and potential witnesses. However, information about the allegation of harassment should be shared only with those who need to know about it. Records relating to harassment complaints should be kept confidential on the same basis.

A conflict between an employee's desire for confidentiality and the employer's duty to investigate may arise if an employee informs a supervisor about alleged harassment, but asks him or her to keep the matter confidential and take no action. Inaction by the supervisor in such circumstances could lead to employer liability. While it may seem reasonable to let the employee determine whether to pursue a complaint, the employer must discharge its duty to prevent and correct harassment. One mechanism to help avoid such conflicts would be for the employer to set up an informational phone line which employees can use to discuss questions or concerns about harassment on an anonymous basis.

> **Effective Investigative Process**
>
> An employer should set up a mechanism for a prompt, thorough, and impartial investigation into alleged harassment. As soon as management learns about alleged harassment, it should determine whether a detailed fact-finding investigation is necessary. For example, if the alleged harasser does not deny the accusation, there would be no need to interview witnesses, and the employer could immediately determine appropriate corrective action.
>
> If a fact-finding investigation is necessary, it should be launched immediately. The amount of time that it will take to complete the investigation will depend on the particular circumstances. If, for example, multiple individuals were allegedly harassed, then it will take longer to interview the parties and witnesses.
>
> It may be necessary to undertake intermediate measures before completing the investigation to ensure that further harassment does not occur. Examples of such measures are making scheduling changes so as to avoid contact between the parties; transferring the alleged harasser; or placing the alleged harasser on non-disciplinary leave with pay pending the conclusion of the investigation. The complainant should not be involuntarily transferred or otherwise burdened, since such measures could constitute unlawful retaliation.
>
> The employer should ensure that the individual who conducts the investigation will objectively gather and consider the relevant facts. The alleged harasser should not have supervisory authority over the individual who conducts the investigation and should not have any direct or indirect control over the investigation. Whoever conducts the investigation should be well trained in the skills that are required for interviewing witnesses and evaluating credibility.

Preventing Workers from Viewing Inappropriate Material

It's an unfortunate fact that workers can lose their jobs because of how they use the Internet at work. It is important that every organization make certain that all employees understand and follow all Internet access and acceptable use (IAP/AUP) polices. Regardless what the company's policy permits, it's wise to always use proper conduct online. In addition, language in e-mails should always remain professional.

INTERNET ACCESS /ACCEPTABLE USE POLICIES

Internet access or acceptable use policies (IAP/AUP) are becoming increasingly common. An IAP/AUP outlines what is considered appropriate and inappropriate Internet use at the workplace. They often state that employees cannot send or receive personal e-mail messages through their addresses at work. In addition, they may confine personal surfing to a worker's lunch hour or breaks. Keep in mind there are two types of online activity, Internet access and the use of e-mail messaging. Make sure your employees understand all of the parameters of your organization's IAP/AUP. Many businesses are becoming more restrictive regarding the use of personal e-mail messages, because they don't want the organization to become associated with the transmission of any questionable materials.

USING CONTENT FILTERS

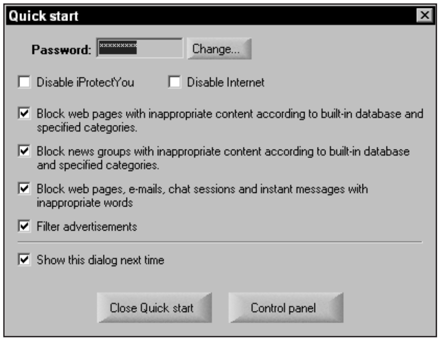
A content filter is a software program that either permits or blocks access to Internet content depending upon whether or not the content meets a predetermined set of criteria. Some filters only scan for certain prohibited keywords. Others may permit computer use only during specified time intervals or perhaps limit the amount of total time spent online by individual users.

There are numerous products available that offer Internet content filtering. Two popular content-filtering programs are Net Nanny by BioNet Systems, LLC (www.netnanny.com) and CyberPatrol by Surf Patrol plc (www.cyberpatrol.com). Each offers numerous content filtering features, such as

- ✓ Black listed URLs (URLs that are not permitted)
- ✓ White listed URLs (URLs that are allowed)
- ✓ The ability to create and manage custom lists
- ✓ Support for the latest Internet browsers from Microsoft and Netscape
- ✓ Expanded filter support for Web-capable e-mail clients
- ✓ The ability to filter inbound and outbound data

In addition to the aforementioned programs, a freeware program called iProtectYou performs many of the same functions (see Figures 10-1 and 10-2). Produced by SoftForYou (www.softforyou.com), this handy program allows for the blocking of e-mail messages, chat sessions, and instant messages that contain inappropriate words. In addition, it can restrict Internet time to a predetermined schedule and allows you to have control over which Web sites can be accessed and which programs are allowed Internet access. Options include setting levels of sensitivity, requesting detailed log files of Web and application activity, and making time-sensitive settings. Your organization can specify separate patterns, keywords, or blocks for Web sites, newsgroups, and advertising, and edit the list of inappropriate words. The program arrives with a large built-in list of prescreened, undesirable sites and keywords.

There are numerous reasons why organizations employ the use of content filters. Increasingly, organizations are finding that creating Internet Acceptable Use Policy guidelines and informing all organizational staff of that policy may not be sufficient to protect management from criminal prosecution should illegal or inappropriate material be found on company computers. Other organizations simply prefer having the peace of mind of knowing that no inappropriate material is allowed or viewed by anyone on their networks.



Quick start

Password: *********

□ Disable iProtectYou □ Disable Internet

☑ Block web pages with inappropriate content according to built-in database and specified categories.

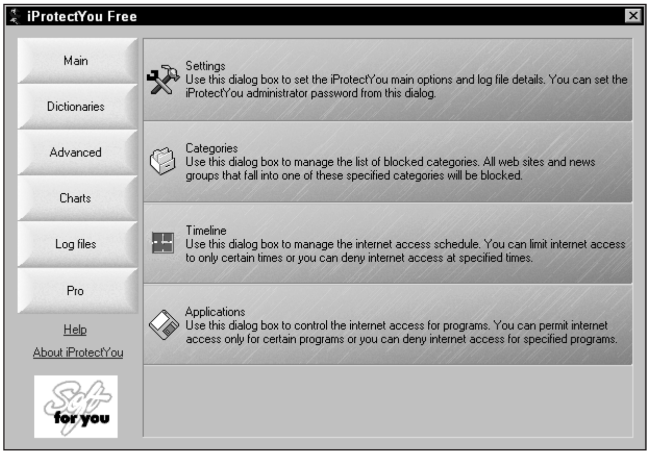
☑ Block news groups with inappropriate content according to built-in database and specified categories.

☑ Block web pages, e-mails, chat sessions and instant messages with inappropriate words

☑ Filter advertisements

☑ Show this dialog next time

Figure 10-1: iProtectYou Quick start screen



Settings
Use this dialog box to set the iProtectYou main options and log file details. You can set the iProtectYou administrator password from this dialog.

Categories
Use this dialog box to manage the list of blocked categories. All web sites and news groups that fall into one of these specified categories will be blocked.

Timeline
Use this dialog box to manage the internet access schedule. You can limit internet access to only certain times or you can deny internet access at specified times.

Applications
Use this dialog box to control the internet access for programs. You can permit internet access only for certain programs or you can deny internet access for specified programs.

Figure 10-2: iProtectYou Control Panel and associated options

note

While beneficial, content filters can sometimes pose problems by preventing legitimate searches from occurring. For example, a content filter might stop a Web page from loading because it contained the word "hardcore" even when not used in a sexual context.

Industrial Espionage

Industrial espionage is an extension of the competitive intelligence gathering seen among corporations and other organizations, even national governments. The reasons for taking part in industrial espionage range from a desire to gain superiority and dominance in a particular industry to seeking to simply achieve a better level of security within one's own organization. Monetary gain is another strong motivation for organizations and knowledgeable individuals to engage in industrial espionage.

Those conducting industrial espionage through transgression into computer systems and networks — cyber spies — often have substantial monetary backing from businesses and even governments. As opposed to run-of-the-mill joyriding hackers, these cyber spies often have at their disposal state of the art equipment and even personnel wherever and whenever they might need it.

The Internet and networked computer systems have facilitated the occupation of these cyber spies, regardless if they are working from within or from without the systems they are attacking. Networked computer security systems may be breached — and spied upon — from sites anywhere in the world, including sites within the organization itself. (More about insider attacks is included in the next section.) Unlike the spies of even the recent past, today's spy needs only to be present in a cyber sense, not necessarily in a physical sense.

Regardless of from where the attack comes, the high-tech gear used today sometimes leaves organizations unaware that their system has been penetrated without authorization. Even when an organization does know its computer system has been compromised, they may not be able to quantify how much, if any, revenue was lost as a result. When material items have been stolen (disks, documents, and so on) those offenses are sometimes only reported as robberies or burglaries, with the value of the information lost not realized and not included in the tally.

Organizations must remember that former employees, both those who leave on good terms and those who are disgruntled, may remain a threat to system security. Whether they are fueled by a desire for revenge, they are approached by a third party with monetary incentive, or they're starting their own business in the same industry, former employees may have enough knowledge to seriously impact your organization's assets, productivity, and even client confidentiality.

Former employees are not the sole risk to your organization's computer system security. Security incidents may arise from current employees, as well. Temporary personnel, subcontractors, and longstanding company employees all may have enough access to privileged and valuable organization information. Some employees deliberately reveal classified information (again, for profit or out of malice); however, others might reveal such information inadvertently. Those engaged in industrial espionage have been known to pose as in-house technicians and request passwords in order to do their job maintaining or repairing a company computer. Misguided employees willingly help by relaying such information. Sometimes, employees simply give out information — such as passwords — after receiving an official or important sounding phone call requesting it.

Defending Against Insider Attacks

Computer and network security threats can come from both outside or inside an organization. Outside threats, as we have seen, can be the hackers or crackers located halfway around the globe. However, a closer and more common network threat may originate from just in the next office in the form of a malevolent or disgruntled employee. The job of those in charge of information security is to detect suspicious activity and find weak links in the organization's computer network. This is analogous to when a security guard tests a door or window to make sure that it is locked. While a firewall can prevent hackers, crackers, and script kiddies (less knowledgeable, nascent hackers) from getting in, firewalls do not protect against seemingly legitimate users that are *already* inside the firewall.

With networked computers, anyone has the potential to access information contained within the entire network. While security personnel routinely focus on outside attacks, the stark reality is that your network is more likely to be compromised by people located inside your organization. Typical insider strategies include stealing or guessing a system administrator password and then giving themselves access to resources to which they are not entitled, such as payroll, accounting records, or proprietary material. This type of computer crime was evidenced in the fall of 2000 when Cisco Systems, Inc. employee Peter Morch (while still employed at Cisco Systems), intentionally exceeded his authorized access to the computer systems of Cisco Systems. According to his guilty plea with the U.S. Department of Justice, Mr. Morch, in order to obtain proprietary information that he knew he was not authorized to have, logged into the computer system both as an administrator and under his own username from a workstation belonging to another Cisco software engineer. He did this because the other engineer's computer had a writable CD drive capable of "burning" CDs. Mr. Morch admitted that he burned a number of CDs on the other employee's computer, using writable CDs that he obtained from the shelf above his computer monitor, and obtained material that included Cisco proprietary materials relating to both released Cisco products and then-ongoing developmental projects.

note

The use of strong passwords can help prevent the insider — and others — from guessing passwords.

The organization's security personnel must be diligent in the way they manage and monitor the logging of networked systems. Security personnel routinely face the time-consuming task of collecting, analyzing, and deciphering multiple systems' log files. Even simple carelessness might be the cause of a security breach. This could happen in a number of ways, such as when a system administrator forgets to log out of a management console, when someone brings an infected laptop into the office from home, or via a security hole created by a misconfigured wireless access point.

Fortunately, most of the more advanced intrusion detection systems, like Tripwire and CyberCop, focus on both external and internal attacks. Because insider attacks can come from so many potential directions, these products tackle the insider problem using a variety of approaches.

Since the best defense is a good offense, vulnerability scanning is one of the best ways for an organization to find and plug security holes in their network. Vulnerability scanning is beneficial for preventing both external and internal attacks. Two popular network vulnerability scanners used today are SAINT and ISS Internet Scanner:

- ✓ **SAINT.** SAINT is the Security Administrator's Integrated Network Tool. In its default mode, it gathers as much information about remote hosts and networks as possible. The information gathered includes the presence of various network information services, which are potential security flaws. These flaws often appear in the form of incorrectly configured network services, well-known bugs in system or network utilities, or weak policy configuration settings.
- ✓ **ISS Internet Scanner.** Those in charge of their organization's network security often choose ISS Internet Scanner for analyzing their network's vulnerabilities. ISS Internet Scanner focuses on the single most important aspect of organizational network risk management: the identification and correction of technical vulnerabilities. Internet Scanner performs scheduled and selective probes of your network's communication services, operating systems, key applications, and routers in search of those vulnerabilities most often used by unscrupulous threats (to probe, investigate, and attack your network). Internet Scanner then analyzes your vulnerability conditions and provides your organization with a series of corrective actions.

It's an unfortunate fact that most devastating security incidents originate from within your own organization. Proactive security scanning provides a meaningful assessment of your organization's system security against known threats. Security scanning can offer suggestions for effective countermeasures, further improving security. Proactive scanning can also lead to faster detection of, and perhaps reduced damages to, breached systems. With vulnerability scanning conducted at regular intervals, your organization can be made aware of potential security vulnerabilities as they occur.

Chapter Summary

The old adage states that an ounce of prevention is worth a pound of cure. Computer security is no exception to this maxim. Whenever possible, you want to take a proactive stance and prevent security incidents from happening in the first place. Unfortunately, we do not live in a perfect world. It is virtually impossible to prevent *all* security incidents. However, when a security incident does come about, you need to ensure that its impact is minimal. There are various response measures your organization can take to minimize the number and impact of security incidents that do take place. This chapter focused on understanding various types of computer security incidents faced by organizations and the basic procedures for responding to those incidents and limiting their impact.

Key points covered in this chapter include

- ✓ Basic procedures for responding to hacker, cracker, and malicious code attacks
- ✓ How to recognize and handle inappropriate computer use
- ✓ Procedures for recognizing and managing incidents involving sexual harassment
- ✓ The legal aspects of industrial espionage
- ✓ How to look for and defend against insider attacks

Chapter 11

Assessing System Security to Prevent Further Attacks

In This Chapter

- ✓ Assessment of security policies and procedures
- ✓ Developing security policy checklists
- ✓ An overview of the security audit process
- ✓ The basic steps to workstation and server audits
- ✓ The benefits of penetration testing
- ✓ Understanding HIPAA compliance issues
- ✓ The Honeynet Project

THE COMPUTER NETWORK IS A KEY TOOL IN TODAY'S BUSINESS WORLD. However, with hackers, crackers, and malicious code abounding, the need for increased security awareness and countermeasures has become imperative. Computer criminals come in many varieties, from hackers to coworkers. Many company security officers believe that the weakest link in the computer security chain is the employee — either disgruntled or simply lazy.

One critical component of incident response is the audit trail. Auditing helps define events that permit security managers to determine exactly what has happened in their network. When a system is breached, the system administrator needs to know what has happened to repair the breach and formulate a plan to prevent future attacks. The hardest part of responding to a network breach is tracing the criminal and assessing damages. A comprehensive security audit evaluates your organization's network and operating practices to ensure that your systems are secure from both internal and external threats. A security audit of the network should include the following:

- ✓ Assessment of current security policies, procedures, and practices
- ✓ A vulnerability assessment
- ✓ Penetration testing
- ✓ Visual inspection of the network's physical security

Security audits can help your organization develop a comprehensive report suitable for both management and technical staff. Such a report should include the following information:

- ✓ A list of vulnerabilities found, including the risk and probability of malicious users, hackers, customers, and business partners exploiting these flaws
- ✓ Recommendations given for patching and repairing of vulnerabilities
- ✓ A list of possible causes of the vulnerabilities
- ✓ Recommendations for preventing such vulnerabilities from arising in the future

In short, security audits help your organization minimize the risk of unscheduled outages, damage or destruction of your information assets, financial losses, and the other detrimental effects of security breaches. This chapter focuses on audit process and procedures, HIPAA compliance issues, the benefit of penetration testing and their role under incident response planning. The chapter concludes with how the lessons learned from the Honeynet Project are helping to shape the future of incident response.

Assessment of Security Policies and Procedures

Security measures are most effective when developed from well-planned, comprehensive, and broadly communicated organizational policies. The need for increased computer security is driving organizations to acquire and deploy innovative security solutions for their computer networks. Unfortunately, many organizations lack a policy structure to back up the technical security systems they deploy. While many have implemented various security policies, these policies are often incomplete or outdated.

Your organization's computer security policy should have the following goals:

- ✓ Establish policies to protect your organization's networks and computer systems from abuse and inappropriate use.
- ✓ Establish methods that will aid in the identification and prevention of abuse of the organization's networks and computer systems.
- ✓ Provide an effective method for responding to questions and complaints regarding abuses — real or unconfirmed — of the organization's networks and computer system.
- ✓ Establish procedures that will protect your professional reputation while allowing you to meet the organization's responsibilities (legal and ethical) regarding the computer system's Internet connection.

A well-designed information security policy is the key to the success of any information security-related actions. Since policies have a profound impact on all security efforts, they should be well developed, enforced, maintained, and periodically audited. Policies need periodic review to ensure that they continue to reflect your organization's overall security strategy. A weak policy can leave a company vulnerable to all kinds of human errors, from selecting a too-easily-guessed password to installing software that may cause security gaps.

When assessing a security policy, be sure to include the following:

- ✓ An explanation of the reason for the policy
- ✓ The effective date of the policy as well as the date it expires
- ✓ A listing of those who: (a) authorized the policy, (b) constructed the policy, (c) approved the policy, (d) will maintain the policy, and (e) will enforce the policy
- ✓ A listing of the personnel and staff that will be affected by the policy
- ✓ An outline of the actions the organization expects of its users
- ✓ The methods that will be used to enforce the policy
- ✓ The regulations and laws upon which the policy is based (including the in-house regulations of your organization)
- ✓ Which information assets must be protected
- ✓ The methods and procedures that personnel are to follow for reporting security violations (whether real or unsubstantiated)

Rapid advancements in information technology require that your organization's security policies be frequently reviewed. The frequency of those policy audits depends on the organization's security needs as well as the technological knowledge of your personnel. Generally, however, each new technological change has the potential to require a corresponding policy change. As a result, a good rule of thumb is to review all organizational policies (security or otherwise) at least annually.

Developing Security Policy Checklists

Auditing a security policy is designed to cope with the tendency on the part of human beings to occasionally make mistakes. In the wake of those mistakes, the need for organizations to conduct regular monitoring and reviewing becomes exceedingly important. Additionally, new vulnerabilities are being found constantly, and it may become overly difficult for an organization to stay on top of those vulnerabilities without outside assistance.

One of the ways to manage an audit is by using audit checklists, which are most beneficial when initiated as part of a larger plan to develop and implement your security policy throughout the organization. Customized checklists are a good idea if you want to maximize the effectiveness of any given guideline.

Policy Audit Checklist — Sample

The following checklist addresses ways to customize a security policy to your organization's specific needs:

- ✓ Have a broad range of employees within the organization — representative of a variety of positions and job levels — been involved in developing the security policy?
- ✓ Has the policy been drafted in a manner that can be understood and followed by all staff members?
- ✓ Has staff been informed of their security roles and responsibilities in writing?
- ✓ Have the needs and expectations of your organization been communicated to your personnel both initially and in an ongoing manner?
- ✓ Have your personnel received security training specifically tailored to the needs of their position?
- ✓ Are all new employees sufficiently trained regarding their security roles, responsibilities, and expectations?
- ✓ Are appropriate opportunities provided for personnel to voice security concerns and ask questions about security policies and procedures?
- ✓ Is adequate time provided for reading and reviewing security agreements before employees and outsiders are required to sign and submit them?
- ✓ Have your policy developers reviewed the policies (security-related practices) of other organizations in the same line of work or those with whom you will conduct business? Cooperation at this juncture ensures that all the engaged parties will be satisfied with future transactions.
- ✓ Has news of your organization's commitment to security been shared with the public?
- ✓ Have policy goals and objectives been translated into organizational security rules that are designed to modify staff behavior?
- ✓ Has an administrator been specifically appointed to be responsible for your organization's security?
- ✓ Are these security regulations enforced equally at all levels of your organization?
- ✓ Have security issues been included as a part of employee performance reviews?
- ✓ Are outsiders (for example, repair technicians and outside organizations) required to sign a contract acknowledging that they are aware of their responsibilities and that they will abide by your organization's security rules and regulations?
- ✓ Are security policies reviewed — and if need be, revised — at least on an annual basis?

An Overview of the Computer Security Audit Process

The purpose of a computer security audit is to provide a detailed analysis of the effectiveness of your organization's current security measures. The information obtained during the audit process will help you to prioritize and fix problem areas, minimizing the risk of unforeseen outages, damage or theft of sensitive information assets, damage to your reputation, and financial loss. Anytime a system is modified or reconfigured, security holes may be opened, allowing the network to become vulnerable to attack. Even when there have been no changes made to your organization's network, you may still fall victim to an attack that exploits a newly discovered vulnerability, confirming that even static systems require periodic auditing.

When developing a security policy for your organization, be sure to include details on how you will test your network(s). Once the initial security audit has been completed, any deficiencies found need to be quickly fixed. In addition, your security policy should detail how you will ensure that *new* flaws or security holes will be handled.

The following steps outline the basic six-step computer security audit process:

- ✓ **Analysis of vulnerabilities.** Determine the adequacy of your organization's security measures, identify security deficiencies, and evaluate the effectiveness of your existing security measures. The analysis should include the risk and likelihood of malicious coders, hackers, and insiders exploiting these flaws.
- ✓ **Network assessment and infrastructure analysis.** Examine hardware devices, intrusion detection systems, routers, and firewalls for vulnerabilities that could leave you open to intrusions.
- ✓ **Risk assessment.** List the safeguards you already have in place for protecting against potential threats by assessing their relative significance in terms of potential loss for all areas of your system. The results from this assessment can be used to determine which areas need the most attention first.
- ✓ **Access and policy assessment.** Examine each user's availability and access to computer system resources. Be sure to include a review of password policies, backup policies, Internet access policy, network security policy, remote access policy, desktop policy, server platform policy, application security policy, personal Internet-based accounts, and in general, the guidelines for the development and implementation of policy standards throughout your organization.
- ✓ **Physical security.** Examine physical computer assets for protection from vandalism, unauthorized access, and tampering. Include a review of all the organization's computer hardware and associated equipment, such as workstations, servers, terminals, routers, switches, removable storage media, hard copies of documentation, and support facilities.
- ✓ **Findings and recommendations report.** Include all of the findings resulting from the analysis and assessments performed as well as recommendations for implementing countermeasures to any of the vulnerabilities discovered during the security audit.

Auditing Workstations and Servers

Security is a serious issue in modern-day computing with threats that affect everyone. Audits on workstations and servers assess how these critical information assets are performing and help to analyze where additional attention is required. As many organizations strive for growth in the global marketplace, they are increasingly seeking to use computer-generated information to leverage a competitive advantage. Auditing can help correct workstation and server deficiencies while providing a useful planning tool for future system enhancements.

Analyzing Workstations

When conducting your organization's computer network assessment, be sure to examine individual workstations for the following:

- ✓ Has the user enabled a workstation screen lock?
- ✓ Has a BIOS password been implemented?
- ✓ Is sensitive data stored on a workstation in a secure manner?
- ✓ Have all unused or unnecessary networking protocols been removed?
- ✓ Are unnecessary services, such as IIS (Microsoft's Internet Information Server), prevented from running on the workstation?
- ✓ Is virus protection installed, updated, and running?
- ✓ Are any unnecessary files and folders precluded from being shared on the workstation?
- ✓ Has the operating system been updated and patched against known vulnerabilities?
- ✓ Is there a procedure to automate the frequent backup of data?

Analyzing Network Servers

In addition, be sure to also examine network servers for the following:

- ✓ Have the servers been located in a secure area that prevents unauthorized access?
- ✓ Has a BIOS password been implemented?
- ✓ Has all sensitive data been stored on an NTFS partition?
- ✓ Have all default accounts been disabled?
- ✓ Has the system administrator unbound unnecessary or unused protocols, such as IPX/SPX, NetBIOS, and so on?
- ✓ Have unnecessary services — such as SMTP, NTP, and FTP — been removed or disabled?
- ✓ Is virus protection software installed and regularly updated?
- ✓ Have any shared folders been given unique permissions for any individual users?
- ✓ Have service packs and security patches been installed when available?
- ✓ Is your network administrator on the organization's security mailing list (so as to be reminded to apply fixes and upgrades in a timely manner)?
- ✓ Are full backups made on a frequent, regular basis?

- ✓ Has your network administrator created and securely stored emergency repair disks?
- ✓ Has auditing and account logging been turned on?
- ✓ Are security event logs reviewed on a regular basis?
- ✓ Has the auto-run feature been disabled for CD-ROM use?
- ✓ Are audit logs being monitored?
- ✓ Has the server's real-time clock been synchronized to a central timeserver?
- ✓ Have password-cracking tools been used to detect weak or easily guessed passwords?
- ✓ Has a host-based intrusion detection system (IDS) been employed?
- ✓ Have floppy disk drives been disabled?
- ✓ Has auditing been enabled for the backup and restoration of data?
- ✓ Has anonymous logon been disabled or restricted?
- ✓ Have NetBIOS null sessions been disabled? (See detailed procedure below.)
- ✓ Has the administrator account been renamed?
- ✓ If appropriate, has the SAM password database been encrypted with 128-bit encryption? (Use syskey.exe for NT4.0.)
- ✓ Have procedures and guidelines been established for responding to incidents?

How to Disable NetBIOS Null Sessions

The null session is one of the most frequently used exploits in Windows hacking. Null sessions are unauthenticated connections (not using a username or password) to the Windows NT/2000/XP system. The null session is so common that it is listed as the number five Windows vulnerability on the SANS/FBI Top 20 list (see `www.sans.org/top20/#W5`). The IraqiWorm (a.k.a. Iraq_oil.exe) of December 2002 was an example of how malicious code can be used to exploit Windows NT–based computers with anonymous null sessions fully enabled or with weak (or null) passwords used on privileged accounts. The IraqiWorm propagated by exploiting Windows NT–based hosts, which had the following weak security configurations:

- ✓ Anonymous null sessions fully enabled
- ✓ Weak (or null) passwords on privileged user accounts

Null sessions take advantage of flaws in the structure of the Common Internet File System/ Server Messaging Block (CIFS/SMB). You can establish a null session with a Windows NT/2000/XP host by simply logging on with a null username and password. Using a null connection allows you to gather important information from the host, such as the following:

- ✓ A list of users and groups
- ✓ A list of computers on the network

- ✓ A list of file shares available
- ✓ A list of users and host Security Identifiers (SIDs)

In other words, null sessions enable an unauthenticated user to get a list of valid user accounts *and* the groups to which those users belong. Access to such information greatly simplifies a brute-force password attack against user accounts. The best defense against this type of attack is to disable NetBIOS null sessions within the Windows OS itself. The following steps show you how.

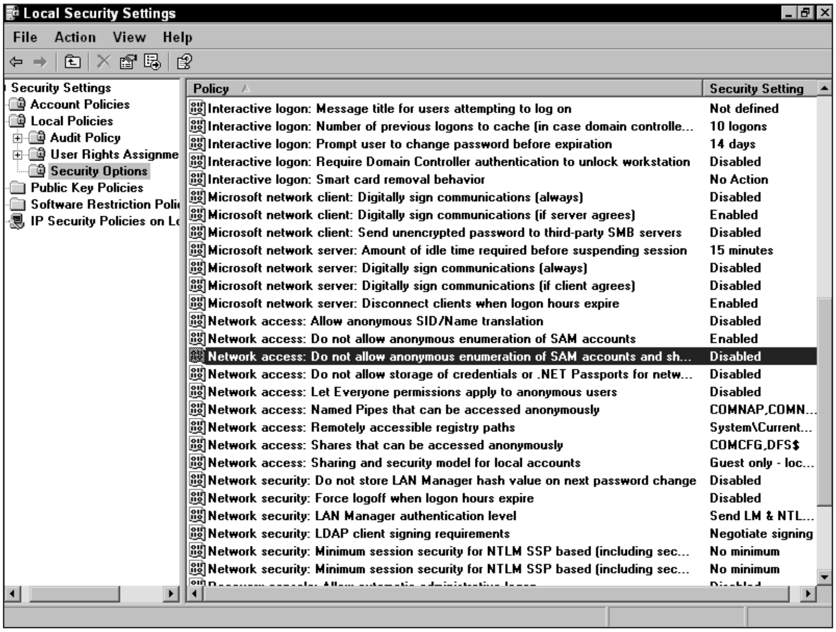
FOR WINDOWS XP

To disable NetBIOS null sessions within Windows XP, do the following:

1. Click on the Start button and navigate to the Control Panel.
2. In the Control Panel, click on Performance and Maintenance.
3. Click on the Administrative Tools icon.
4. Double-click on Local Security Settings.
5. Expand the Local Policies folder in the left pane, then highlight the Security Options folder.
6. In the Security Options folder (see Figure 11-1), make sure the following two policies are enabled:

   Network Access: Do not allow anonymous enumeration of SAM accounts

   Network Access: Do not allow anonymous enumeration of SAM accounts and shares



Policy	Security Setting
Interactive logon: Message title for users attempting to log on	Not defined
Interactive logon: Number of previous logons to cache (in case domain controlle...	10 logons
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and sh...	Disabled
Network access: Do not allow storage of credentials or .NET Passports for netw...	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	COMNAP,COMN...
Network access: Remotely accessible registry paths	System\Current...
Network access: Shares that can be accessed anonymously	COMCFG,DFS$
Network access: Sharing and security model for local accounts	Guest only - loc...
Network security: Do not store LAN Manager hash value on next password change	Disabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send LM & NTL...
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including sec...	No minimum
Network security: Minimum session security for NTLM SSP based (including sec...	No minimum
Recovery console: Allow automatic administrative logon	Disabled

Figure 11-1: The Security Options folder within Windows XP Professional’s Local Policies folder

FOR WINDOWS 2000

To disable NetBIOS null sessions within Windows 2000, do the following:

1. Click on the Start button and navigate to the Control Panel.
2. In the Control Panel, double-click the Local Security Settings.
3. Navigate to Local Policies.
4. Open the Security Options folder.
5. Select "Additional restrictions of anonymous connections" in the Policy pane on the right.
6. From the pull-down menu labeled "Local policy setting," select "No access without explicit anonymous permissions."
7. Click OK.

FOR WINDOWS NT

Unfortunately, in Windows NT 4.0, you will need to edit the Registry in order to disable NetBIOS null sessions. Following the Registry editing and backup procedures outlined in Chapter 4, edit the following Registry key as follows:

```
HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/LSA/RestrictAnonymous=1
```

Blocking the following ports at the router or firewall can also help defend against NetBIOS null-session attacks:

Port number	Port protocol	Port description
135	TCP	DCE/RPC Portmapper
137	TCP/UDP	NetBIOS Name Service
138	TCP/UDP	NetBIOS Datagram Service
139	TCP	NetBIOS Session Service
445	TCP	Microsoft-DS (Windows 2000 CIFS/SMB)

Penetration Testing

Penetration testing is the process of analyzing, probing, and identifying security vulnerabilities in a network to the extent to which they might be exploited by outside parties. By simulating a real-world malicious attack, you can quickly know if your network is secure or not. Penetration testing is an important and necessary tool for determining the status of the current security policies and procedures of your organization because it can:

- ✓ Create the foundation for building a secure and protected environment in which to conduct business
- ✓ Discover any weaknesses in your network allowing your organization to address them before a malicious attacker can exploit them
- ✓ Profile the weaknesses based on risk levels, severity, and the skill required to carry out exploits
- ✓ Identify vulnerabilities, including any misconfiguration, that can be exploited by a remote attacker
- ✓ Provide specific recommendations to strengthen your security and to mitigate the risks discovered

Hackers routinely spend their time searching computer systems for security holes in the form of vulnerabilities. These security holes can be caused by a number of issues, such as misconfiguration and/or programming flaws. To protect your organization's computer systems from hackers, crackers, script kiddies, and malicious code, you need to check for known vulnerabilities and exploits within your networks' systems. Vulnerabilities can be comprised of bugs, application backdoors, or spyware (computer code used to monitor, log, or thwart activity on a computer system unbeknownst to its user(s)) that have entered applications or operating systems in the form of malicious code.

When it comes to network security, there is no better way to find weaknesses than by performing penetration testing on a regular basis. There are compelling reasons to perform penetration testing regularly:

- ✓ New exploits are released almost daily.
- ✓ Patches and updates to software and hardware are frequently released.
- ✓ With OS and application upgrades, the possibility of a new breach being introduced may occur.

In-House vs. Outsourcing

To perform a penetration test, organizations have only two choices: either perform the penetration test in-house or outsource the task to a security company that specializes in such testing.

There are only two circumstances where the penetration testing should be conducted in-house. The first reason would be if there are monetary or budgetary considerations. The second reason would be in extreme situations where the security of your data is so vital and/or classified that outside individuals can have no knowledge of it.

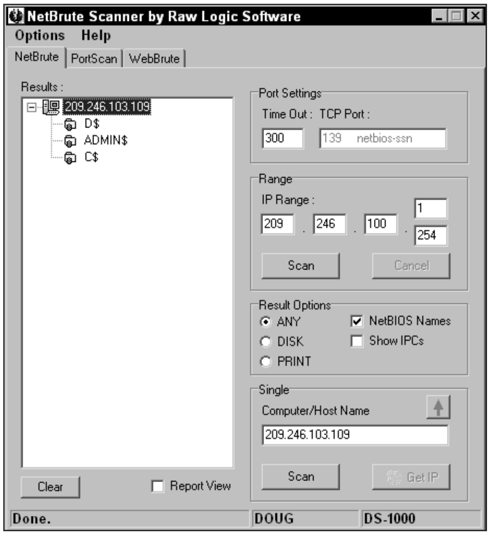
Penetration-Testing Software for In-House Audits

As one could expect, there are literally dozens of products available that allow an organization to perform an in-house penetration test of their network(s). A quick search on the Internet proves this point. For Windows-based systems, products like iNETPATROL and LANPATROL by Network Security Systems (`www.netsecuritysys.com`) and VIGILANTe.com SecureScan NX (`www.vigilante.com`) are popular. For Unix-/Linux-based systems, Nessus (`www.nessus.org`) and Security Administrator Tool for Analyzing Networks (SATAN) (`www.porcupine.org/satan`) have been used for years to conduct in-house penetration tests and network audits.

If your budget is extremely limited, a handy freeware product is available called NetBrute Scanner by Raw Logic Software (`www.rawlogic.com`), which can perform three different penetration tests on your Windows-based computers. NetBrute allows you to scan a single computer — or multiple IP addresses — for available Windows File and Print Sharing resources (see Figure 11-2). This is probably one of the most dangerous and easily exploited security holes, and it is not uncommon for novice users to have their printers or their entire hard drive shared without being aware of it. This utility helps you to zero in on these resources, so you can secure them with a firewall or inform your users about how to properly configure their shares with tighter security.

PortScan (see Figure 11-3), which is included in NetBrute, allows you to scan a single computer or multiple IP addresses for available Internet services. This allows you to identify which TCP ports need to be blocked by your firewall, if you wish to secure them. Alternatively, it allows you to identify unused services that are running, so they can be stopped.

WebBrute (see Figure 11-4), also part of NetBrute, allows you to scan your Web directories that are protected with HTTP authentication, testing the security strength of your users' passwords. This allows you to better enforce your password maintenance policies to ensure that users are not using easily guessed passwords, or passwords that match their username.



Results :
209.246.103.109
D$
ADMIN$
C$

Port Settings
Time Out : 300
TCP Port : 139 netbios-ssn

Range
IP Range : 209 . 246 . 100 . 1 / 254

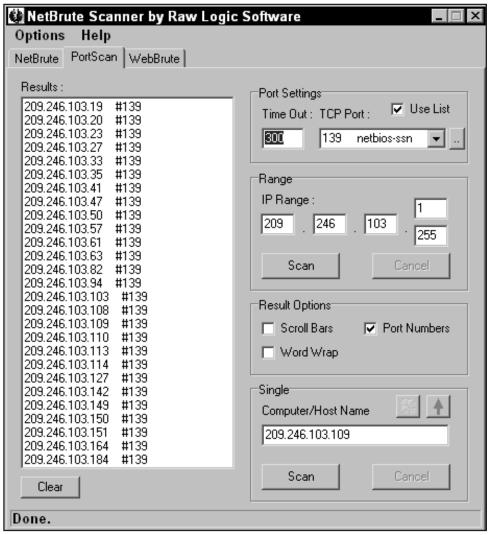
Result Options
● ANY
○ DISK
○ PRINT
☑ NetBIOS Names
☐ Show IPCs

Single
Computer/Host Name: 209.246.103.109

☐ Report View

Done. DOUG DS-1000

Figure 11-2: Scanning for available Windows File and Print Sharing resources for a host on an IP network



Results :

```
209.246.103.19   #139
209.246.103.20   #139
209.246.103.23   #139
209.246.103.27   #139
209.246.103.33   #139
209.246.103.35   #139
209.246.103.41   #139
209.246.103.47   #139
209.246.103.50   #139
209.246.103.57   #139
209.246.103.61   #139
209.246.103.63   #139
209.246.103.82   #139
209.246.103.94   #139
209.246.103.103   #139
209.246.103.108   #139
209.246.103.109   #139
209.246.103.110   #139
209.246.103.113   #139
209.246.103.114   #139
209.246.103.127   #139
209.246.103.142   #139
209.246.103.149   #139
209.246.103.150   #139
209.246.103.151   #139
209.246.103.164   #139
209.246.103.184   #139
```

Port Settings
Time Out : 300
TCP Port : 139 netbios-ssn
☑ Use List

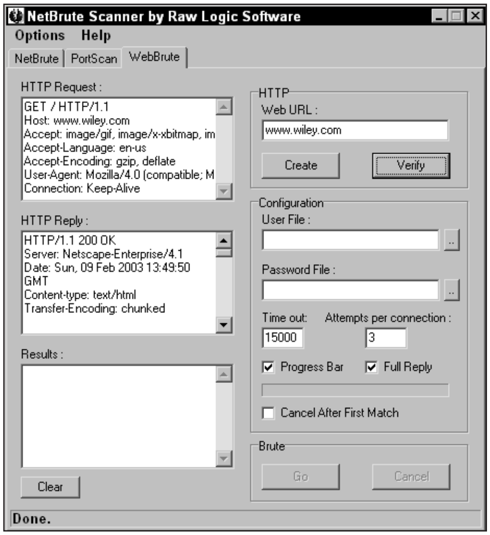
Range
IP Range : 209 . 246 . 103 . 1 – 255

Result Options
☐ Scroll Bars ☑ Port Numbers
☐ Word Wrap

Single
Computer/Host Name: 209.246.103.109

Done.

Figure 11-3: PortScan allows you to scan a single computer or multiple IP addresses for available Internet services.



HTTP Request :

```
GET / HTTP/1.1
Host: www.wiley.com
Accept: image/gif, image/x-xbitmap, im
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; M
Connection: Keep-Alive
```

HTTP Reply :

```
HTTP/1.1 200 OK
Server: Netscape-Enterprise/4.1
Date: Sun, 09 Feb 2003 13:49:50
GMT
Content-type: text/html
Transfer-Encoding: chunked
```

Results :

HTTP
Web URL : www.wiley.com

Configuration
User File :
Password File :
Time out: 15000
Attempts per connection : 3
☑ Progress Bar ☑ Full Reply
☐ Cancel After First Match

Brute

Done.

Figure 11-4: WebBrute allows you to scan your Web directories that are protected with HTTP authentication, testing the security strength of your users' passwords.

Third-Party Penetration Testing

It takes a true expert to realize the full extent of a hacker's work. Contracting with an outside third party to perform penetration testing does not require that an organization relinquish control of the complete testing process. For example, when using a third party for penetration testing, you can choose to give them as little or as much information about your network as you like.

Organizations typically choose to outsource penetration testing for several reasons:

- To determine the degree of system vulnerabilities that might not be detected through the use of in-house audits
- As a prelude to restructuring the organization's security system and for enhancing the perceived value of the organization's reputation
- To show customers how safely they can perform e-commerce transactions over the Internet

The biggest benefit to outsourcing penetration testing is the use of a no-knowledge attack. The no-knowledge attack, when performed by testers who have no factual information about the target location, is designed to provide the most realistic penetration test possible and usually includes gathering a significant amount of information about the target system before launching an attack.

It is almost always best if a third party performs this type of exercise because internal security personnel are too knowledgeable about their organization's environment to be sufficiently objective. A full-knowledge attack, on the other hand, is performed with testers having exceeding amounts of information about targeted environments. Such testing is designed to simulate an attacker who has intimate knowledge of the target organization's systems — such as a real employee.

Only trained and experienced professionals should carry out penetration testing. While third-party testing can often provide objective results, organizations sometimes become the victim of hackers who will use a simulation to find vulnerabilities for their own purposes. To combat this, some organizations try to insulate themselves against unscrupulous penetration testers by having their security staff monitor the penetration-testing procedures.

When searching for a third-party provider for penetration/vulnerability testing, it is best to use a well-established organization with a known good track record. Following is a short list of several popular providers:

- En Garde Systems, Inc. (`www.engarde.com/`)
- Red Hat, Inc. (`www.redhat.com/services/focus/security/testing.html`)
- ITSecure (`www.itsecure.com.au/`)
- VIGILANTe (`www.vigilante.com/`)

x-ref

For more on third-party vendors who provide penetration/vulnerability testing, check out the Information Security Magazine's list of vendors at `www.infosecuritymag.com/vendor_links.shtml`.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996. While the act contains numerous provisions relating to healthcare and the portability of benefits, it also contains provisions requiring the security of confidential and personal medical record data stored and transmitted by entities such as health plans, healthcare clearinghouses, and healthcare providers, all of which are required to use the HIPAA security standards to develop and maintain the security of all electronic individual health information. An entity that is one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations.

An important aspect as it relates to incident response is the HIPAA Administrative Simplification provision. This provision requires covered entities that maintain or transmit "Patient Identifiable Data" to develop and implement formal policies, procedures, and practices that safeguard the integrity, confidentiality, and availability of their electronic data. The security standards include numerous requirements under the following four general categories:

- ✓ **Procedures to guard the integrity, confidentiality, and availability of data.** These are documented, formal practices for selecting and carrying out security measures to protect data as well as the conduct of personnel in relation to the protection of data.
- ✓ **Physical safeguards.** These relate to the protection of your organization's computer systems, buildings, and equipment from fire and other natural and environmental hazards as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.
- ✓ **Technical security services.** These include the processes that are put in place to protect and to control and monitor information access.
- ✓ **Technical security mechanisms.** These include the processes that are put in place and carried out to prevent unauthorized access to data transmitted over your organization's network.

The preceding procedures should be adapted to the individual needs of your organization. They need not necessarily be presented in the same format or broken down into four categories.

x-ref

The final guidelines for HIPAA are located at `www.cms.gov`.

HIPAA Compliance

The Centers for Medicare & Medicaid Services (CMS) are responsible for implementing various provisions of HIPAA. The Administrative Simplification provisions of the Health Insurance

Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers and offer the following guidelines addressing the security and privacy of health data for covered entities:

ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

A. Certification Each organization would be required to evaluate its computer system(s) or network design(s) to certify that the appropriate security has been implemented. This evaluation could be performed internally or by an external accrediting agency.

We are, at this time, soliciting input on appropriate mechanisms to permit independent assessment of compliance. We would be particularly interested in input from those engaging in health care electronic data interchange (EDI), as well as independent certification and auditing organizations addressing issues of documentary evidence of steps taken for compliance; need for, or desirability of, independent verification, validation, and testing of system changes; and certifications required for off-the-shelf products used to meet the requirements of this regulation.

We also solicit comments on the extent to which obtaining external certification would create an undue burden on small or rural providers.

B. Chain of Trust Partner Agreement If data are processed through a third party, the parties would be required to enter into a chain of trust partner agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple two-party contracts may be involved in moving information from the originating party to the ultimate receiving party. For example, a provider may contract with a clearinghouse to transmit claims to the clearinghouse; the clearinghouse, in turn, may contract with another clearinghouse or with a payer for the further transmittal of those claims. These agreements are important so that the same level of security will be maintained at all links in the chain when information moves from one organization to another.

C. Contingency Plan We would require a contingency plan to be in effect for responding to system emergencies. The organization would be required to perform periodic backups of data, have available critical facilities for continuing operations in the event of an emergency, and have disaster recovery procedures in place. To satisfy the requirement, the plan would include the following:

- ✓ Applications and data criticality analysis
- ✓ A data backup plan
- ✓ A disaster recovery plan
- ✓ An emergency mode operation plan
- ✓ Testing and revision procedures

D. Formal Mechanism for Processing Records There would be a formal mechanism for processing records, that is, documented policies and procedures for the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information. This is important to limit the inadvertent loss or disclosure of secure information because of process issues.

E. Information Access Control An entity would be required to establish and maintain formal, documented policies and procedures for granting different levels of access to health care information. To satisfy this requirement, the following features would be provided:

- ✓ Access authorization policies and procedures
- ✓ Access establishment policies and procedures
- ✓ Access modification policies and procedures

Access control is also discussed later in this document in the personnel security requirement and under the physical safeguards, technical security services, and technical security mechanisms categories.

F. Internal Audit There would be a requirement for an ongoing internal audit process, which is the in-house review of the records of system activity (for example, logins, file accesses, and security incidents) maintained by an entity. This is important to enable the organization to identify potential security violations.

G. Personnel Security There would be a requirement that all personnel with access to health information must be authorized to do so after receiving appropriate clearances. This is important to prevent unnecessary or inadvertent access to secure information. The personnel security requirement would require entities to meet the following conditions:

- ✓ Assure supervision of personnel performing technical systems maintenance activities by authorized, knowledgeable persons.
- ✓ Maintain access authorization records.
- ✓ Ensure that operating, and in some cases, maintenance personnel have proper access.
- ✓ Employ personnel clearance procedures.
- ✓ Employ personnel security policy/procedures.
- ✓ Ensure that system users, including technical maintenance personnel, are trained in system security.

H. Security Configuration Management The organization would be required to implement measures, practices, and procedures for the security of information systems. These would be coordinated and integrated with other system configuration management practices in order to create and manage system integrity. This integration process is important to ensure that routine changes to system hardware and/or software do not contribute to or create security weaknesses. This requirement would include the following:

- ✓ Documentation
- ✓ Hardware/software installation and maintenance review and testing for security features
- ✓ Inventory procedures
- ✓ Security testing
- ✓ Virus checking

I. Security Incident Procedures There would be a requirement to implement accurate and current security incident procedures. These are formal, documented instructions for reporting security breaches, so that security violations are reported and handled promptly. These instructions would include the following:

- ✓ Report procedures
- ✓ Response procedures

J. Security Management Process A process for security management would be required. This involves creating, administering, and overseeing policies to ensure the prevention, detection, containment, and correction of security breaches. We would require the organization to have a formal security management process in place to address the full range of security issues. Security management includes the following mandatory implementation features:

- ✓ Risk analysis
- ✓ Risk management
- ✓ A sanction policy
- ✓ A security policy

K. Termination Procedures There would be a requirement to implement termination procedures, which are formal, documented instructions, including appropriate security measures, for the ending of an employee's employment or an internal/external user's access. These procedures are important to prevent the possibility of unauthorized access to secure data by those who are no longer authorized to access the data. Termination procedures would include the following mandatory implementation features:

- ✓ Changing combination locks
- ✓ Removal from access lists
- ✓ Removal of user account(s)
- ✓ Turning in of keys, tokens, or cards that allow access

L. Training This proposed rule would require security training for all staff regarding the vulnerabilities of the health information in an entity's possession and procedures which must be followed to ensure the protection of that information. This is important because employees need to understand their security responsibilities and make security a part of their day-to-day activities. The implementation features that would be required to be incorporated follow:

- ✓ Awareness training for all personnel, including management (this is also included as a requirement under physical safeguards)
- ✓ Periodic security reminders
- ✓ User education concerning virus protection
- ✓ User education in importance of monitoring login success/failure, and how to report discrepancies
- ✓ User education in password management

The Honeynet Project

We've all heard the expression: you can catch more flies with honey than with vinegar, the premise being that it's easier to attract and catch the things we want rather than to chase them down and catch them. While this same principle applies to honeypots, the purpose of the Honeynet Project is slightly different.

Founded in April 1999 by Lance Spitzner, a former officer in the Army's Rapid Deployment Force, the Honeynet Project is a nonprofit research group of 30 security professionals dedicated to information security. With no income or revenue, all Honeynet Project research is carried out strictly on a volunteer basis. The objective of the project is to study the tools, tactics, and motives of the blackhat (hacker) community and share these lessons with the security community at large.

Traditionally, honey*pots* are single computer systems used to lure aggressors toward an easy-to-attack target. Honey*nets*, on the other hand, are not actually designed to lure hackers. Instead, honeynets are collections of computers designed to let hackers break into a false network while allowing investigators to watch their every move. Designed for research, they are used to assist security experts in better understanding the workings of the blackhat community.

The Honeynet Project is valuable because data collected by the honeynet helps us better predict attack trends and find new hacker tools that are out in the wild. When a new attack method or tool is discovered, those involved in the Honeynet Project notify security alert organizations, such as the Computer Emergency Response Team (CERT) or the System Administration, Networking, and Security Institute (SANS). These organizations help disseminate this important data by releasing publications, which in turn raises security awareness of the threats and vulnerabilities that exist on the Internet.

Chapter Summary

The U.S. government estimates that recovery costs from reported cyber attacks in 2001 alone was $13 billion nationwide. The best means for avoiding these costs is to protect critical information assets and resources. Security audits are designed to find vulnerable areas where hackers, crackers, and insiders can gain unauthorized access to your computer systems. A comprehensive security audit evaluates your organization's network and operating practices to ensure that your systems are secure from both internal and external threats. Detecting vulnerabilities and intrusions through security audits helps determine if security infrastructures, policies, and procedures continue to provide the level of protection required by their organizations. Some industries — such as governmental and healthcare institutions — are already required to undergo comprehensive security audits that check traditional security on systems. This chapter focused on understanding such basic auditing procedures as the assessment of current security policies, procedures, and practices; vulnerability assessment; and penetration testing.

Key points covered in this chapter include

- ✓ The procedures for assessment of security policies and procedures and how computer security audits help mitigate risks to information assets
- ✓ How to develop and implement security policy checklists
- ✓ An overview of the security audit process and its role in incident response
- ✓ The basic steps to conduct workstation and server audits and their importance in the overall computer security process
- ✓ The pros and cons of in-house penetration testing and when and why outsourcing is sometimes superior
- ✓ Understanding HIPAA compliance issues for covered entities and how they relate to incident response preparation
- ✓ A brief overview of the Honeynet Project

Chapter 12

Pulling It All Together

In This Chapter

- ✓ Analyzing real-world attacks
- ✓ Lessons learned from others
- ✓ Where to go for up-to-date information
- ✓ Future trends in security technology

ON FEBRUARY 7, 2000, THE NIPC RECEIVED REPORTS THAT YAHOO had experienced a Denial of Service attack. In the days that followed, several other companies (including Cable News Network, eBay, Amazon.com, Buy.com, and ZDNET) also reported Denial of Service outages to the NIPC and FBI field offices. Unfortunately, the attackers used *spoofed* IP addresses, meaning that the address that appeared on the target's log was not the true address of the system that sent the messages. In addition, many of the victims had not kept complete network logs. These DoS attacks resulted in millions of dollars in lost revenue. The corporate sector, the media, and even government agencies were left exasperated.

A Denial of Service (DoS) attack is not a virus (as some people assume) but a method used by hackers to prevent or deny legitimate users access to a computer. DoS attacks are typically executed using specially designed tools that flood a computer with so many requests for data that the computer ceases to function and cannot provide information to legitimate users. The attack effectively shuts down the affected computer, hence the Denial of Service moniker. An analogy would be someone launching an automated program to have hundreds of phone calls placed *simultaneously* to an organization's switchboard. Coping efforts on the part of the organization's staff would be overcome in no time, and many callers would receive busy signals due to the high volume of telephone traffic.

Analyzing Real-World Attacks

It was in the fall of 1999 that the NIPC first began receiving reports about a new set of exploits or attack tools collectively called Distributed Denial of Service (or DDoS) tools. DDoS variants include tools known as Trinoo, Tribal Flood Net (TFN), TFN2K, and Stacheldraht (German for "barbed wire"). These tools essentially work as follows: Hackers gain unauthorized access to a computer system(s) and place software code on it that transforms that system into a master (also called a handler). The hackers also invade and then place malicious code onto other networks, making those systems become agents (also known as zombies, daemons, or slaves). Each master is capable of controlling multiple agents. In both instances, the network owners normally are not aware that dangerous tools have been placed (and reside) on their systems, thus becoming third-party victims to the intended crime.

Notes Michael Vatis, director of the NIPC, "The 'Masters' are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents, activating their DDoS ability. The agents then generate numerous requests to connect with the attack's ultimate target(s), typically using a fictitious or 'spoofed' IP (Internet Protocol) address, thus providing a falsified identity as to the source of the request. The agents act in unison to generate a high volume of traffic from several sources. This type of attack is referred to as a SYN flood, as the SYN is the initial effort by the sending computer to make a connection with the destination computer. Due to the volume of SYN requests the destination computer becomes overwhelmed in its efforts to acknowledge and complete a transaction with the sending computers, degrading or denying its ability to complete service with legitimate customers — hence the term 'Denial of Service.' These attacks are especially damaging when they are coordinated from multiple sites — hence the term 'Distributed Denial of Service.'"

While the DDoS attacks were costly, the most disturbing element was that they caught much of computer security industry by surprise simply because they were somewhat unexpected and the industry was not prepared. Being prepared and acting quickly are the hallmark of a sound incident response program.

Even computer security companies are not immune to attacks. At 2:00 a.m., January 11, 2002, the GRC.com Web site (home of Gibson Research Corporation) was knocked off the Internet by a new type of attack called a Distributed Reflected Denial of Service attack or DRDoS. According to GRC's president, Steve Gibson, "Perhaps the most startling aspect of this attack was that the apparent source was hundreds of the Internet's 'core routers,' web servers belonging to yahoo.com, and even a machine with an IP resolving to 'gary7.nsa.gov.' We appeared to be under attack by hundreds of very powerful and well-connected machines."

As the sophistication of malicious hackers grows and as the available supply of insecure and readily compromised Internet-connected host machines skyrockets, bandwidth-consuming Distributed Denial of Service (DDoS) attacks become more commonplace. This is due to the unfortunate fact that powerful, remote Internet attack tools are now finding their way into the hands of adolescents or *script kiddies* who use their disruptive power with little thought for, or remorse about, the consequences.

While Denial of Service attacks are just one type of threat faced by organizations conducting e-commerce, numerous other threats reside much closer to home in the form of the disgruntled or malicious employee. The following recent public press release is an example of one such attack.

December 17, 2002 U.S. Department of Justice
United States Attorney
District of New Jersey
Disgruntled UBS PaineWebber Employee Charged with
Allegedly Unleashing "Logic Bomb" on Company Computers

NEWARK—A disgruntled computer systems administrator for UBS PaineWebber was charged today with using a "logic bomb" to cause more than $3 million in damage to the company's computer network, and with securities fraud for his failed plan to drive down the company's stock with activation of the logic bomb, U.S. Attorney Christopher J. Christie announced.

Roger Duronio, 60, of Bogota, N.J., was charged today on a two-count Indictment returned by a federal grand jury, according to Assistant U.S. Attorney William Devaney.

The Indictment alleges that Duronio, who worked at PaineWebber's offices in Weehawken, N.J., planted the logic bomb in some 1,000 of PaineWebber's approximately 1,500 networked computers in branch offices around the country. Duronio, who repeatedly expressed dissatisfaction with his salary and bonuses at Paine Webber resigned from the company on Feb. 22, 2002. The logic bomb Duronio allegedly planted was activated on March 4, 2002.

In anticipation that the stock price of UBS PaineWebber's parent company, UBS, A.G., would decline in response to damage caused by the logic bomb, Duronio also purchased more than $21,000 of "put option" contracts for UBS, A.G.'s stock, according to the charging document. A put option is a type of security that increases in value when the stock price drops. Market conditions at the time suggest there was no such impact on the UBS, A.G. stock price.

PaineWebber promptly reported what had happened to government investigators and the U.S. Attorney's Office, and has been helpful and cooperative in the investigation by the U.S. Secret Service's Electronic Crimes Task Force.

Duronio is scheduled to make an initial appearance in court at 2:00 before U.S. Magistrate Judge Madeline Cox Arleo.

"Cybercrime against financial institutions is a significant issue," Christie said. "Although the damage was contained in this case, the potential for catastrophic damage in other cases is always there. We will prosecute cyber criminals and put them in prison."

The Indictment alleges that, from about November 2001 to February, Duronio constructed the logic bomb computer program. On March 4, as planned, Duronio's program activated and began deleting files on over 1,000 of UBS PaineWebber's computers. It cost PaineWebber more than $3 million to assess and repair the damage, according to the Indictment.

As one of the company's computer systems administrators, Duronio had responsibility for, and access to, the entire UBS PaineWebber computer network, according to the Indictment. He also had access to the network from his home computer via secure Internet access.

Duronio is charged in Count One of the Indictment with securities fraud, which carries a maximum penalty of 10 years in federal prison and a $1 million fine. He is charged in Count Two with Fraud and Related Activity In Connection with Computers. That charge carries a maximum prison sentence of 10 years and a fine of $250,000 or, alternatively, two times the gain made by the defendant or the loss suffered by the victim.

In February and March 2002, according to the Indictment, Duronio spent approximately $21,762 when purchasing 318 put-option contracts for the stock of UBS A.G., all due to expire on March 15. A "put-option" contract is a security that gives the purchaser the right to sell 100 shares of stock in a company for a fixed per-share price at a specified date. The lower the stock price falls, the more valuable the put-option contract becomes. If the contract is sold on or before the expiration date with the stock at or below a specified "strike price," a profit is earned.

It's a regrettable fact that essentially any Internet-connected computer can become the target of an attack from any point across the globe. The following public press release demonstrates that even the U.S. military can fall victim to a malicious hacker attack from a foreign land.

> **November 12, 2002 U.S. Department of Justice**
> **United States Attorney**
> **Eastern District of Virginia**
> **2100 Jameison Avenue**
> **Alexandria, VA 22314**
> **London, England Hacker Indicted Under Computer Fraud**
> **and Abuse Act for Accessing Military Computers**
> Paul J. McNulty, United States Attorney for the Eastern District of Virginia, announced that Gary McKinnon, of London, England, was indicted in Alexandria today by a federal grand jury on seven counts of computer fraud and related activity. McKinnon faces on each count a maximum sentence of 10 years of imprisonment and a $250,000 fine. The United States intends to formally request that the United Kingdom extradite McKinnon.
>
> According to the indictment, between March of 2001 and March of 2002, Gary McKinnon accessed and damaged without authorization 92 computers belonging to the United States Army, Navy, Air Force, Department of Defense, and NASA, and 6 computers belonging to a number of private businesses. One count charges McKinnon with accessing and damaging without authorization a computer used by the military for national defense and security. Other computers hacked by McKinnon include computers located at military bases throughout the United States and the Pentagon. The indictment alleges that Gary McKinnon scanned a large number of computers in the .mil network, was able to access the computers and obtained administrative privileges. Once he was able to access the computers, McKinnon installed a remote administration tool, a number of hacker tools, copied password files and other files, deleted a number of user accounts, and deleted critical system files. Once inside a network, McKinnon would then use the hacked computer to find additional military and NASA victims. Ultimately, McKinnon caused a network in the Washington D.C. area to shut down, resulting in the total loss of Internet access and e-mail service to approximately 2,000 users for three days.
>
> The estimated loss to the various military organizations, NASA, and the private businesses is approximately $900,000.
>
> The case was indicted as the result of a 17-month investigation by the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU), NASA Office of the Inspector General, Naval Criminal Investigative Service, 902nd Military Intelligence Group-Information Warfare Branch, Defense Criminal Investigative Service, the Air Force Office of Special Investigations, and the United Kingdom's National High Tech Crime Unit. Also assisting in the investigation were the U.S. Army Computer Emergency Response Team located at Fort Belvoir, VA., the Army Regional Computer Emergency Response Team at Fort Huachuca, the Naval Computer Incident Response Team, and the Department of Defense Computer Emergency Response Team.

Security Lessons Learned from Others

It is often said that wisdom is learning from the mistakes of others so that you don't repeat them yourself. This certainly holds true for computer security and incident response. When teaching incident response, examples of real-world failures are an effective method of demonstration and act as a cautionary warning to future computer security personnel. By reviewing some common information-security mistakes, for example, incident response personnel can refine security policies to correct shortcomings. Here are some common mistakes:

- ✓ Installing unnecessary programs and services
- ✓ Opening e-mail message attachments from unknown people
- ✓ Not keeping current on software patches, especially security-related ones
- ✓ Not installing antivirus software and keeping its virus patterns current
- ✓ Lack of adequate training to administer the system
- ✓ Not deploying encryption or intrusion detection systems
- ✓ Inadequate handling of sensitive data
- ✓ Sharing passwords or using weak passwords
- ✓ Propagating chain mail and virus hoaxes

Lessons Learned from the Code Red Worm

In July 2001, another Internet worm made headlines. Known as Code Red, this worm was malicious code that infected one machine and then propagated over a network attempting to infect others, exploiting a known vulnerability in Microsoft's Internet Information Server (IIS) software. Although the worm could be defeated by patching the vulnerability and rebooting, it had a secondary, unexpected — and damaging — side effect. Some of the infected networks became saturated with Web traffic and experienced significant slowdowns. The worm also revealed a number of flaws in certain types of networking equipment, particularly those that allow management through a Web interface. Many networking devices simply failed in the face of the Code Red buffer overflow.

It is important to understand and remember that when exceptions are made in security policies, they can have serious consequences. For example, if an organization designs a complete network security system and installs a firewall to block unauthorized incoming connections, but then allows Internet Web queries to bypass the firewall and reach an unpatched IIS Web server, the entire security design becomes undermined. The lesson learned here is that traditional firewalls don't help when you deliberately open up a security hole on your Web server and circumvent your perimeter protection.

While many Web servers performed fairly well in the face of the Code Red attack, the most disappointing characteristic of the Code Red incidents was the failure of the system administrator community to address the problem in a timely manner. Despite numerous warnings, many administrators failed to apply available patches to their systems. There may have been two reasons for this. It is possible that many computers were running without any system administrator present or that some system administrators were just ignoring the plethora of security warnings.

Increased capabilities of malicious code packages have resulted in more devastating impacts. Several other trends were also made apparent during 2001. One of the most significant was the incorporation of the capabilities of worms, Trojan horses (backdoors), and viruses all combined into a single powerful package. Malicious code attacks during 2001 also included techniques for propagating more rapidly than ever before. The brief interval between the Code Red worm and the release of the Nimda worm continued the long-established trend of malicious code packages being modified based on lessons learned from previous malevolent attacks. This resulted in even more advanced malicious code packages.

Lessons Learned from Hackers

The lessons learned from intrusions tend to focus on how the intruder got in and what types of vulnerabilities were exploited. Because of its widespread use, Windows-based computer systems are the primary target for many types of attacks, particularly with Trojan horse programs like Netbus, SubSeven, and BackOrifice. As noted in the previous section, most of these systems were compromised long before anyone realized that anything was amiss. Most system administrators became aware of Trojan horse or backdoor programs only after authorized users complained about poor system performance and the cause of the high system utilization was traced back to one of these unauthorized programs. Another lesson learned is that hacker activity — or hacktivity — normally increases during times of political tension. This argument is reinforced by the following advisory from the National Infrastructure Protection Center (NIPC), which warns of the increased threat of hacker activity due to increased tensions between the U.S. and Iraq.

> **Encourages Heightened Cyber Security as Iraq - US Tensions Increase**
> **February 11, 2003**
>
> The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq.
>
> Recent experience has shown that during a time of increased international tension, illegal cyber activity: spamming, web defacements, denial of service attacks, etc., often escalates. This activity can originate within another country, which is party to the tension. It can be state sponsored or encouraged, or come from domestic organizations or individuals independently. Additionally, sympathetic individuals and organizations worldwide tend to conduct hacking activity, which they view as somehow contributing to the cause. As tensions rise, it is prudent to be aware of, and prepare for this type of illegal activity.
>
> **Attacks may have one of several motivations:**
>
> - Political activism targeting Iraq or those sympathetic to Iraq by self-described “patriot” hackers.
> - Political activism or disruptive attacks targeting United States systems by those opposed to any potential conflict with Iraq.
> - Criminal activity masquerading or using the current crisis to further personal goals.
>
> Regardless of the motivation, the NIPC reiterates such activity is illegal and punishable as a felony. The U.S. Government does not condone so-called “patriotic hacking” on its behalf. Further, even Apatriotic hackers@ can be fooled into launching attacks against their own interests by exploiting malicious code that purports to attack the other side when in fact it is designed to attack the interests of the side sending it. In this and other ways Apatriotic hackers@ risk becoming tools of their enemy.
>
> During times of potentially increased cyber disruption, owners/operators of computers and networked systems should review their defensive postures and procedures and stress the importance of increased vigilance in system monitoring. Computer users and System Administrators can limit potential problems through the use of “security best practices” procedures. Some of the most basic and effective measures that can be taken are:

> - Increase user awareness
> - Update antivirus software
> - Stop potentially hostile/suspicious attachments at the e-mail server
> - Utilize filtering to maximize security
> - Establish policies and procedures for responding and recovery
>
> All users should be aware that malicious code (e.g., worms and viruses) can be introduced to spread rapidly by using patriotic or otherwise catchy titles, encouraging users to click on a document, picture, word, etc., which automatically spreads the damaging code. For additional security checklists, please refer to the following sites:
>
> `www.cert.org/security-improvement`
> `www.unixtools.com/securecheck`
> `www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp`
> `www.sans.org/topten.htm`
>
> The NIPC encourages recipients of this advisory to report computer intrusions and/or other crime to federal, state, or local law enforcement, their local FBI office at `http://www.nipc.gov/incident/cirr.htm`, and other appropriate authorities. Recipients may report incidents online to `http://www.nipc.gov/incident/cirr.htm`. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206 or `nipc.watch@fbi.gov`.

It is important to remember that your organization should always treat information assets as it would treat any other valuable asset. Just as you would not walk away from your desk leaving cash or other valuables unattended, you should take care to similarly protect your information assets. Always remember to take the following precautions:

- ✓ **Protect your computer equipment.** Keep it in a secure environment. Be sure to keep food, drink, and cigarette smoke away from it at all times. In addition, know where fire suppression equipment is located, and learn how to use it.
- ✓ **Protect your area.** Keep unauthorized people away from sensitive computer equipment and information and remember to question any strangers in your area.
- ✓ **Protect your password.** Never write it down or give it to anyone. In addition, do not use names, numbers, or dates that can be personally identified with you. Remember not only to change it often, but also to change it immediately if you think it has been compromised.
- ✓ **Protect your files.** Don't allow unauthorized access to your files and data, and remember to *never* leave your equipment unattended with your password activated; always sign off!
- ✓ **Protect against malicious code.** Don't use unauthorized software, and back up your critical files before implementing *any* new software.
- ✓ **Lock up storage media that contains sensitive data.** If the data or information is sensitive or critical to your organization, always be sure to lock it up in a secure location.
- ✓ **Back up your data.** Keep duplicates of your sensitive data in a safe place, out of your immediate area, and remember to back up data as often as necessary.
- ✓ **Report security violations.** Tell your system administrator or network security manager if you see any unauthorized changes to your data. Immediately report any loss of data or programs, whether automated or hard copy.

Whether security incidents come from computer viruses, hacker attacks, or computer mischief initiated by disgruntled employees, appropriate response demands that your organization continue operations while reversing damages, investigating causes, communicating with customers, and even launching investigations and seeking legal recourse. While the basic principles of emergency readiness have been used for decades — and will continue to be the basis for addressing new challenges — two new planning approaches must also be addressed. First, the scope of disaster recovery planning must be broadened beyond its traditional focus on primarily operational issues to include backup security measures, as well. Second, business continuity planning combined with disaster recovery planning needs to be approached as a corporate-wide business operation requirement.

Where to Go for Up-to-Date Information

The Internet is growing at an incredible rate with, experts say, hundreds of new sites popping up each day. It is possible for anyone to set up a Web site, placing information on it that they claim is credible; however, it is difficult to substantiate such claims and ascertain that the information posted is up-to-date and accurate. There are a vast number of resources available via the Internet. Business enterprises, organizations, educational institutions, communities, and individuals all serve as information providers for the electronic Internet community. This sharing of resources and information is an example of cooperation between the public, private, and governmental sectors of society and has encouraged extensive professional and personal communications throughout the world.

Savvy members of the electronic Internet community, however, are aware that there are few, if any, quality controls for the information that is made available. Accurate and reliable data may share a computer screen with data that is inaccurate, unreliable, or false and deliberately misleading. In addition, the differences between the types of data may be imperceptible, especially for those who are not expert in the topic at hand. Because the Internet does not fall under the responsibility of any one organization or institution, it is unlikely that any universal quality controls will be established in the near future. In light of this lack of a single governing body, Internet users must be prepared to become critically skilled consumers of the information they find and reap.

When it comes to computer forensics and incident response, several credible Web sites are available that *do* provide accurate and up-to-date information. Following is a short list of Web sites offering up-to-date computer security, incident response, and forensic information.

- ✓ **The CERT Coordination Center (CERT/CC) (`www.cert.org`).** Functioning as a hub of Internet security expertise, the CERT Coordination Center is located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The information provided at this site ranges from protecting systems against potential problems to reacting to current problems to predicting future problems. Their work centers around the handling of computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing information and training to help improve computer security.
- ✓ **The Forum of Incident Response and Security Teams (FIRST) (`www.first.org`).** Bringing together a range of computer security incident response teams from various government, commercial, and educational institutions, FIRST aims to encourage the

cooperation and coordination of incident prevention. In addition, FIRST promotes rapid reaction to incidents by encouraging information sharing among members of the Internet and computer security community at large.

- ✓ **The National Infrastructure Protection Center (NIPC) (`www.nipc.gov`).** Serving as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity, the NIPC provides timely warnings of international threats, comprehensive analysis, and law enforcement investigation and response. According to its Web site, the mission of the NIPC is to
  - "Detect, deter, assess, warn, respond, and investigate unlawful acts involving computer and information technologies and unlawful acts, both physical and cyber, that threaten or target our critical infrastructures
  - Manage computer intrusion investigations
  - Support law enforcement, counterterrorism, and foreign counterintelligence
  - Missions related to cyber crimes and intrusion
  - Support national security authorities when unlawful acts go beyond crime and are foreign-sponsored attacks on United States interests
  - Coordinate training for cyber investigators and infrastructure protectors in government and the private sector"
- ✓ **The SANS Institute (`www.sans.org`).** Consisting of security professionals, auditors, as well as system and network administrators, the mission of the SANS Institute is to share the lessons they have learned and find solutions to the challenges faced by the computer security community at large. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who provide hundreds of man-hours each year investigating and teaching to help the entire information security community.
- ✓ **The Computer Crime and Intellectual Property Section (CCIPS) (`www.cybercrime.gov`).** A division of the U.S. Department of Justice, CCIPS consists of lawyers who focus entirely on the issues raised by computer and intellectual property crime. CCIPS attorneys help
  - Advise federal prosecutors and law enforcement agents
  - Comment on and propose legislation
  - Coordinate international efforts to combat computer crime
  - Litigate cases
  - Train law enforcement groups

  Other areas of expertise possessed by CCIPS attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations, and intellectual property crimes.

- ✓ **The Computer Security Resource Center (CSRC)** (`www.csrc.nist.gov`). As a division of the National Institute of Standards and Technology, CSRC's mission, per its Web site, is to help improve computer security by
  - "Raising awareness of IT risks, vulnerabilities, and protection requirements, particularly for new and emerging technologies
  - Researching, studying, and advising agencies of IT vulnerabilities, and devising techniques for the cost-effective security and privacy of sensitive federal systems
  - Developing standards, metrics, tests, and validation programs: to promote, measure, and validate security in systems and services; to educate consumers; and to establish minimum security requirements for federal systems
  - Developing guidance to increase secure IT planning, implementation, management, and operation"

Future Trends in Security Technology

As society has become increasingly dependent on computers for creating, conveying, and storing essential documents and data, the amount of unauthorized theft of sensitive information stored in and transmitted from computers has increased correspondingly. As a result, current trends in security technology are aimed at the improvement of existing security systems, focusing on new security requirements and/or customer satisfaction. Examples of this are intrusion detection systems (IDSs) and firewalls. With constant enhancements, IDSs and firewalls are being continually improved to yield less false positives while improving their stability and overall reliability. In addition, the movement toward integrating several computer security devices — such as IDSs and firewalls — is also beginning to appear.

Another area of computer security that is certain to show great advancements is the enhancement of security for wireless technologies. Wireless access is quickly broadening network reach by providing convenient, inexpensive access, particularly in hard-to-wire locations. As networks expand beyond physical boundaries, wireless computer users struggle to retain control over network usage, privacy, and security. Fortunately, the wireless industry has responded with innovative security techniques, such as Rapid Re-keying, Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES) protocol, helping to deliver a more effective security toolset to the wireless community.

The ability to react quickly to security incidents when they occur is the key component and most essential part of an overall security plan. Future trends in computer security will certainly address this subject and may include an increase in the outsourcing of security services. This is mainly a result of the increased complexity in security management and the increased risk and severity of security threats faced by organizations today. In the future, strong authentication will also play a key role and may even act as the foundation for flexible and secure monetary systems. The field of computer security is evolving continuously, and it is common to see more questions than there are solutions.

Chapter Summary

As a result of the aftermath of September 11, society has now begun to take strong interest in security awareness and terrorism. Individuals and organizations are realizing that having in place basic infrastructures and standard processes for vulnerability management, crisis management, and incident handling are a *necessity* for mitigating risk, damage, and business interruption. Overall, basic security awareness and computer security has improved drastically when compared with the security policies in place only a few years ago. Response times — to attacks, emergencies, and serious new remote vulnerabilities — have improved measurably, particularly in business enterprises and large organizations. However, experience reminds us that hackers, crackers, and malicious code will continue to proliferate on the Internet of the future, and they will use sophisticated and novel methods of attack. This will force the computer security community to counteract by developing new tools and methods to combat those threats and capture evidence to prosecute cyber criminals.

Key points covered in this chapter include

- ✓ The analysis of several real-world attack methods and how a lack of preparation and failure to update and patch vulnerable systems can have devastating effects
- ✓ How lessons learned from others can help shape future incident response procedures and computer security in general
- ✓ Popular Web sites where up-to-date information can be found regarding computer security incidents and forensics
- ✓ An overview of some future trends in information security technology

Appendix A

What's on the CD-ROM

This appendix provides you with information on the contents of the CD that accompanies this book. For the latest and greatest information, please refer to the README file located at the root of the CD. Here is what you will find:

- ✓ System requirements
- ✓ Using the CD with Windows and Linux
- ✓ What's on the CD
- ✓ Troubleshooting

System Requirements

Make sure that your computer meets the minimum system requirements listed in this section. If your computer doesn't match up to most of these requirements, you may have a problem using the contents of the CD.

For Windows 9*x*, Windows 2000, Windows NT4 (with SP 4 or later), Windows Me, or Windows XP:

- ✓ PC with a Pentium processor running at 120 MHz or faster
- ✓ At least 32MB of total RAM installed on your computer; for best performance, at least 64MB is recommended
- ✓ Free disk space of at least 50MB for installation of all utilities
- ✓ Ethernet network interface card (NIC) or modem with a speed of at least 28,800 bps
- ✓ A CD-ROM drive

For Linux:

- ✓ PC with a Pentium processor running at 90 MHz or faster
- ✓ At least 32MB of total RAM installed on your computer; for best performance, at least 64MB is recommended
- ✓ Ethernet network interface card (NIC) or modem with a speed of at least 28,800 bps
- ✓ A CD-ROM drive

Using the CD with Windows

To install the items from the CD to your hard drive, follow these steps:

1. Insert the CD into your computer's CD-ROM drive.
2. A window appears with the following options: Install, Explore, eBook, and Exit.

   Install: Gives you the option to install the supplied software and/or the author-created samples on the CD-ROM.

   Explore: Enables you to view the contents of the CD-ROM in its directory structure.

   eBook: Enables you to view an electronic version of the book.

   Exit: Closes the auto-run window.

If you do not have auto-run enabled, or if the auto-run window does not appear, follow these steps to access the CD:

1. Click Start → Run.
2. In the dialog box that appears, type `d:\setup.exe`, where *d* is the letter of your CD-ROM drive. This brings up the auto-run window described in the preceding set of steps.
3. Choose the Install, Explore, eBook, or Exit option from the menu. (See Step 2 in the preceding list for a description of these options.)

Using the CD with Linux

To install the items from the CD to your hard drive, follow these steps:

1. Log in as root.
2. Insert the CD into your computer's CD-ROM drive.
3. If your computer has Auto-Mount enabled, wait for the CD to mount. Otherwise, follow these steps:

   a. Command line instructions:

      At the command prompt type:

      ```
      mount /dev/cdrom /mnt/cdrom
      ```

      (This mounts the `cdrom` device to the `mnt/cdrom` directory. If your device has a different name, change `cdrom` to that device name — for instance, `cdrom1`.)

b. Graphical: Right-click the CD-ROM icon on the desktop and choose Mount CD-ROM. This mounts your CD-ROM.

4. Browse the CD and follow the individual installation instructions for the products listed below.

5. To remove the CD from your CD-ROM drive, follow these steps:

a. Command line instructions:

At the command prompt type:

```
umount /mnt/cdrom
```

b. Graphical: Right-click the CD-ROM icon on the desktop and choose UMount CD-ROM. This unmounts your CD-ROM.

What's on the CD

The following sections provide a summary of the software and other materials you'll find on the CD.

Author Checklists

Following are the checklists outlining the basic steps and procedures for data collection, evidence preservation, and incident response. More checklists can be found on the CD.

DEVELOPING A COMPUTER SECURITY INCIDENT RESPONSE

❑ Define your organization's overall incident response structure.

❑ Develop and implement alert mechanisms that permit quick action.

❑ Establish a centralized reporting structure.

❑ Appoint and train incident response personnel.

PREPARING SYSTEMS FOR DATA COLLECTION

❑ Enable logging and auditing on all workstations and servers.

❑ Make all workstations and servers time-synchronized with a reliable and accurate Internet timeserver, such as `www.time.nist.gov`.

❑ Use time-stamping and ensure that the verification of time stamps within your system cannot be modified or distorted.

❑ Identify network devices by creating a network map to serve as a baseline and graphical representation of the devices on your network for future reference.

DETECTING MALICIOUS CODE AND INTRUDERS

- ❑ Analyze any abnormal system processes using the Windows Task Manager or third-party tools like Process Explorer.
- ❑ Detect unusual or hidden files by modifying Windows to display certain hidden file types.
- ❑ Locate rootkits and backdoors in Unix and Linux by using third-party programs like Intact by Pedestal Software or via manual inspection.
- ❑ Scan for backdoors and network sniffers using the `netstat -n` and `ifconfig -a` commands.

RETRIEVING AND ANALYZING CLUES

- ❑ Perform keyword searches using third-party tools like Disk Investigator or BinTex.
- ❑ Locate and examine the Windows swap file for evidence. Under Windows 95/98/ME, the swap file is called win386.swp, and in Windows NT/2000/XP, it is called pagefile.sys.
- ❑ Locate and retrieve e-mail evidence. E-mail messages can be found in a number of different places, such as the sender's e-mail inbox/outbox, a network server's mailbox, or backup media.
- ❑ Recover evidence from Web browser cache and history. Web caches reveal a lot about which Web sites a user has visited. Most contemporary Web browsers (for example, Internet Explorer and Netscape Navigator) perform Web caching and maintain browsing history.
- ❑ Gather evidence from the Windows print spooler (EMF) files. Even if a user never saved a word-processing document, temporary versions of word-processing documents sometimes remain on the hard drive.
- ❑ Locate data in hidden or masked file extensions. Be sure to scan for evidence hidden in steganographic images and password-protected compressed files.

BASIC PROCEDURES FOR COLLECTING AND PRESERVING EVIDENCE

- ❑ Understand volatility of evidence. Some evidence, such as data in the computer's RAM, only exists while the computer is powered on.
- ❑ Create a real-mode boot disk, because the simple act of turning on the computer can destroy potential evidence. By using a special real-mode boot disk, a forensic investigation can be conducted without booting the computer via the hard drive.
- ❑ Use packet sniffers to gather evidence. Computer investigations sometimes warrant the capture of "live" data as it travels in real time across an organization's computer network.

❑ Build a forensic toolkit. Essential to any computer investigation, toolkits come in two types; those you assemble yourself and pre-fabricated ones that you download or purchase as a suite from any one of many forensic software vendors.

❑ Follow a chain-of-custody. The chain-of-custody is a record of evidence handling from the time of seizure to the time evidence is presented in a court of law.

❑ Ensure the admissibility of evidence collected via authentication. Before a computer record can be used as evidence, it must first be proven to be authentic.

INCIDENT CONTAINMENT AND ERADICATION OF VULNERABILITIES

❑ Contain the incident. The goal is to limit the scope and magnitude of an incident to prevent the incident from causing more damage.

❑ Determine the risk of continuing operations. If the system contains classified or sensitive information or if critical programs risk becoming corrupted, it is generally advised that the system be shut down or at least temporarily disconnected from the network.

❑ Sever network and Internet connections. For example, if a serious virus is suspected, such as a fast-spreading worm or dangerous Trojan horse, you should immediately disconnect the infected computer from the network.

❑ Understand the risks of using network and file shares. Many viruses and worms will use network file shares as a means to propagate across a network.

❑ Establish a trust model. A trust model is a means for helping to recognize and visualize varying degrees of confidence, intentionally or unintentionally granted to individuals, based upon the risks associated with granting confidence.

❑ Periodically change passwords. Passwords are one of the first lines of defense that users have to protect their systems. Changing them frequently or after a system compromise is mandatory.

❑ Promote security awareness by using multimedia documentation strategies that can be easily or periodically distributed to all organizational members.

DISASTER RECOVERY AND FOLLOW-UP

❑ Develop a Disaster Recovery Plan. Knowing how to react properly in an emergency is critical to making decisions that will minimize resultant damage and quickly restore operations.

❑ Develop incident recordkeeping procedures. The methods used to create your records are to be documented to ensure the ability to retrieve, read, and use those records in the future.

❑ Utilize an Uninterruptible Power Supply (UPS). In the event of a power failure, a generator may not supply the uninterrupted power required to maintain your computer system operation or to perform an orderly shutdown of a workstation or server.

- ❑ Perform regular backups. When disaster strikes, a backup may be the only hope of retrieving original data.
- ❑ After an incident, monitor systems for unusual or suspicious activity. In addition, a *post-mortem* examination should be conducted so that the organization can learn from the experience and, if necessary, update its procedures.
- ❑ Anticipate and plan for future attacks. Properly anticipating and planning for unforeseen disruptions to business operations is important for remaining competitive.

Software

The CD contains the following shareware, freeware, and trialware/demo programs for Windows and Linux platforms. As basic tools for conducting an in-house computer forensic investigation, these programs help you collect, preserve, and analyze computer-related evidence.

- ✓ **Autopsy Forensic Browser** (trialware) is a graphical interface to the command-line digital forensic analysis tools in The @stake Sleuth Kit (TASK). Together, TASK and Autopsy provide many of the same features as commercial digital forensics tools for the analysis of Windows and Unix file systems (NTFS, FAT, FFS, EXT2FS, and EXT3FS). For additional information, visit `www.atstake.com/research/tools/autopsy/`.
- ✓ **ByteBack,** by Tech Assist, Inc., is a professional data-recovery and computer-investigative utility demo. Some of its main features are the ability to clone or image a disk using a physical sector copy of most media types to like media (clone) or to a compressed file (image). ByteBack can automatically repair partitions and boot records of FAT12, FAT16, FAT32 and NTFS volumes and offers individual file recovery for these environments. ByteBack contains a powerful sector editor for working with raw data. For more information, visit `www.toolsthatwork.com/byte.shtml`.
- ✓ **Cain & Abel** is a password-recovery tool for Microsoft operating systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary and brute-force attacks, decoding scrambled passwords, revealing password boxes, and analyzing routing protocols. For additional information, visit `www.oxid.it/projects.html`.
- ✓ **Kiwi Syslog Daemon** is a freeware Syslog Daemon for Windows. It receives, logs, displays, and forwards syslog messages from hosts, such as routers, switches, Unix hosts, and any other syslog-enabled device. For additional information, visit `www.kiwisyslog.com`.
- ✓ **MaresWare Suite** (trialware) provides a set of tools for investigating computer records plus data analysis capabilities. This bundled suite of over 40 separate programs allows you to accomplish a variety of tasks and gives you the control to conduct an inquiry or analysis in the way you want. For additional information, visit `www.dmares.com/maresware/suite.htm`.

- ✓ **PDA Seizure** (demoware), by Paraben, is a comprehensive tool that allows PDA data to be acquired, viewed, and reported on, all within a Windows environment. For more information, visit `www.paraben-forensics.com/pda.html`.
- ✓ **ProDiscover DFT** (demoware), by Technology Pathways, offers forensics examiners an integrated Windows application for the collection, analysis, management, and reporting of computer disk evidence at an affordable price. Features include the ability to generate a bit-stream copy disk to new disk, recover deleted files contained in slack space, and display data contained in Windows NT/2000 Alternate Data Streams. Since this product is frequently updated, visit `www.techpathways.com` for product updates and additional information.
- ✓ **RegCleaner** is an easy-to-use freeware program that allows the user to detect and remove old and obsolete Registry entries. Features include the ability to remove file types, old software entries, and unused DLL files. For additional information, visit `www.vtoy.fi/jv16/shtml/regcleaner.shtml`.
- ✓ **The @stake Sleuth Kit (TASK)** open-source software allows an investigator to examine the file systems of a computer in a nonintrusive fashion. TASK is a collection of Unix-based command-line tools that can analyze NTFS, FAT, FFS, EXT2FS, and EXT3FS file systems. TASK reads and processes the file system structures and therefore does not require operating system support for the file systems. These can be used during incident response on live systems to bypass the kernel and view files that are being hidden by rootkits. For additional information, visit `www.atstake.com/research/tools/task/`.
- ✓ **Ultimate Zip Cracker** (trialware), by VDG Software, is designed for recovering the lost passwords for several file types such as: MS-Word documents (*.DOC) in Office 97–XP, MS-Excel documents (*.XLS) in Office 97–XP, and ZIP archives created by PKZIP, WinZip, and many others. The program utilizes a Password Wizard and provides easy step-by-step password recovery. For more information, please visit `www.vdgsoftware.com/uzc.html`.

Additional shareware, freeware, and trialware/demo computer forensics programs for Windows and Linux platforms are listed below.

Product Name	Company Name	Type of software	URL
Advanced Password Recovery software	ElcomSoft Co. Ltd.	shareware	www.elcomsoft.com
Automachron	One Guy Coding	freeware	www.oneguycoding.com/automachron
Blindwrite suite	Vso-software	demo	www.blindwrite.com
Conversions Plus	DataViz, Inc.	trial	www.dataviz.com

Continued

(Continued)

Product Name	Company Name	Type of software	URL
Detective	Tech Assist, Inc.	demo	www.toolsthatwork.com
dtSearch Desktop	dtSearch Corporation	evaluation	www.dtsearch.com
Email Examiner	Paraben Corporation	demo	www.paraben-forensics.com
Emulator Personal Edition	Paragon Technologie GmbH	demo	www.paragon-gmbh.com
F.I.R.E.	DMZ Services, Inc.	demo	www.dmzs.com
LADS	Frank Heyne Software	freeware	www.heysoft.de/index.htm
LC4	Atstake Limited	trial	www.atstake.com/research/lc/application/lc4setup.exe
Linux dd	Red Hat Software, Inc.	freeware	www.redhat.com
Nmap	Fyodor	freeware	www.insecure.org/nmap/index.html#download
OfficeRecovery Enterprise	Recoveronix Ltd.	demo	www.officerecovery.com
pdd	Paraben Corporation	demo	www.paraben-forensics.com
PLAC	unknown	freeware	http://sourceforge.net/projects/plac
TRINUX	unknown	freeware	http://trinux.sourceforge.net
UniAccess	ComAxis Technology	demo	www.comaxis.com
WinHex	X-Ways Software Technology	shareware	www.x-ways.com

For descriptions of the products listed above, please see the Read Me file on the CD.

Shareware programs are fully functional trial versions of copyrighted programs. If you like particular programs, register with their authors for a nominal fee and receive licenses, enhanced versions, and technical support. *Freeware programs* are copyrighted games, applications, and utilities that are free for personal use. Unlike shareware, these programs do not require a fee or provide technical support. *GNU software* is governed by its own license, which is included inside the folder of the GNU product. See the GNU license for more details.

Trial, demo, or evaluation versions are usually limited either by time or functionality (such as being unable to save projects). Some trial versions are very sensitive to system date changes. If you alter your computer’s date, the programs will “time out” and will no longer be functional.

eBook version of *Incident Response: Computer Forensics Toolkit*

The complete text of this book is on the CD in Adobe's Portable Document Format (PDF). With attacks on Internet Web sites and networks abounding, computer users are regularly reminded of these occurrences. Organizations and businesses conducting operations via the Internet often have their networks infiltrated without their knowledge. As long as there is an Internet, there will also be cyber criminals. As quickly as those in the computer security industry formulate sophisticated counteractive devices, attempts to thwart them will follow from equally sophisticated hackers. Becoming wary and remaining watchful will serve to greatly inhibit cyber attacks on organizational, business, and home user systems. The purpose of this book is to provide both the information and the tools for this task in one easy-to-read format. It will enable anyone to effectively respond to incidents while simultaneously collecting and preserving key evidence.

You can read and search through the file with the Adobe Acrobat Reader (also included on the CD). Adobe Acrobat Reader is free software for the viewing of Portable Document Format (PDF) files and is supported by nearly all major operating system platforms.

Troubleshooting

If you have difficulty installing or using any of the materials on the companion CD, try the following solutions:

- ✓ **Turn off any antivirus software that you may have running.** Installers sometimes mimic virus activity and can make your computer incorrectly believe that it is being infected by a virus. (Be sure to turn the antivirus software back on later.)
- ✓ **Close all running programs.** The more programs you're running, the less memory there is available to other programs. Installers also typically update files and programs; if you keep other programs running, installation may not work properly.
- ✓ **Reference the ReadMe.** Please refer to the README file located at the root of the CD-ROM for the latest product information at the time of publication.

If you still have trouble with the CD, please call the Customer Care phone number: (800) 762-2974. Outside the United States, call 1 (317) 572-3994. You can also contact Customer Service by e-mail at `techsupdum@wiley.com`. Wiley Publishing, Inc. will provide technical support only for installation and other general quality control items; for technical support on the applications themselves, consult the program's vendor or author.

Appendix B

Commonly Attacked Ports

The following table shows examples of commonly attacked ports exploited by hackers and Trojan horses. If you find probes directed against ports normally not used, it may be someone trying to connect to a Trojan inside your network. Please note that some Trojans can be configured to use any port and that the ones illustrated here are merely the default port numbers used. Knowledge of these commonly attacked ports helps make it easier to track down the cause of a security intrusion and to help guard against future attacks.

Port #	Protocol	Type of attack
0	ICMP	Click attack
8	ICMP	Ping attack
9	UDP	Chargen
19	UDP	Chargen
21	TCP	FTP service, Dolly Trojan
23	TCP	TELNET service
25	TCP	SMTP, AntiGen
31	TCP	Agent 31, Hacker's Paradise
41	TCP	Deep Throat
53	TCP	DNS
58	TCP	DM Setup
69	TCP	W32.Evala.Worm
70	TCP	W32.Evala.Worm
79	TCP	Firehotcker
80	TCP	Executor

Continued

Port #	Protocol	Type of attack
90	TCP	Hidden Port 2.0
110	TCP	ProMail Trojan
113	TCP	Kazimas
119	TCP	Happy99
121	TCP	Jammer Killah
129	TCP	Password Generator Protocol
135	TCP/UDP	NetBIOS remote procedure call
137	TCP/UDP	NetBIOS name (DoS attack)
138	TCP/UDP	NetBIOS datagram
139	TCP UDP	NetBIOS session (DoS attack)
146	TCP	Infector 1.3
421	TCP	TCP Wrappers
456	TCP	Hacker's Paradise
531	TCP	Rasmin
555	TCP	Stealth Spy, Phaze, 7-11 Trojan
666	TCP	Attack FTP
777	TCP	AIM Spy application
901	TCP	Backdoor.Devil
902	TCP	Backdoor.Devil
911	TCP	Dark Shadow
999	TCP	Deep Throat
1000	TCP	Der Spaeher
1001	TCP	Silencer, WebEx
1011	TCP	Dolly Trojan
1012	TCP	Dolly Trojan
1015	TCP	Dolly Trojan
1024	TCP	NetSpy
1025	UDP	Maverick's Matrix 1.2–2.0

Port #	Protocol	Type of attack
1027	TCP	ICQ
1029	TCP	ICQ
1032	TCP	ICQ
1033	TCP	NetSpy
1034	TCP	Backdoor.Systec
1042	TCP	Bla Trojan
1045	TCP	Rasmin
1090	TCP	Xtreme
1170	TCP	Voice Streaming Audio
1207	TCP	SoftWar
1214	TCP	KaZaa File Sharing (not a Trojan)
1234	TCP	Ultors Trojan
1243	TCP	SubSeven
1245	TCP	VooDoo Doll
1269	TCP	Maverick's Matrix
1349	UDP	BackOrifice DLL Comm
1394	TCP	GoFriller, Backdoor G-1
1492	TCP	FTP99CMP
1505	TCP/UDP	FunkProxy
1509	TCP	Psyber Streaming server
1533	TCP	Backdoor.Miffice
1600	TCP	Shivka-Burka
1604	TCP/UDP	ICA Browser
1722	TCP/UDP	Backdoor.NetControle
1807	TCP	SpySender
1981	TCP	Shockrave
1999	TCP	BackDoor

Continued

Port #	Protocol	Type of attack
2000	TCP/UDP	BackDoor.Fearic
2001	TCP	Trojan Cow
2002	TCP	TransScout
2003	TCP	TransScout
2004	TCP	TransScout
2005	TCP	TransScout
2023	TCP	Ripper
2090	TCP	Backdoor.Expjan
2115	TCP	Bugs
2140	TCP/UDP	Deep Throat
2155	TCP	Illusion Mailer
2283	TCP	HLV Rat5
2565	TCP	Striker
2583	TCP	WinCrash
2716	TCP	The Prayer 1.2–1.3
2721	TCP	Phase Zero
2801	TCP	Phineas Phucker
2989	UDP	Rat
3024	TCP	WinCrash
3028	TCP	Ring Zero
3129	TCP	Master’s Paradise
3150	TCP/UDP	Deep Throat
3256	TCP	W32.HLLW.Dax
3332	TCP	Q0 BackDoor
3410	TCP	OptixPro.12
3456	TCP/UDP	Backdoor.Fearic
3459	TCP	Eclipse 2000
3700	TCP	Portal of Doom

Port #	Protocol	Type of attack
3737	TCP	Backdoor.helios
3791	TCP	Eclypse
3801	UDP	Eclypse
4092	TCP	WinCrash
4100	TCP	Watchguard Firebox admin DoS Expl
4128	TCP	Backdoor.rcserv
4567	TCP	File Nail
4590	TCP	ICQ Trojan
5000	TCP	Sokets de Trois v1./Bubbel
5001	TCP	Sokets de Trois v1./Bubbel
5011	TCP	Ootlt
5031	TCP	Net Metropolitan 1.0
5032	TCP	Net Metropolitan 1.04
5152	TCP	Backdoor.laphex.client
5321	TCP	Firehotcker
5400	TCP	Blade Runner
5401	TCP	Blade Runner
5402	TCP	Blade Runner
5503	UDP	Remote Shell Trojan
5512	TCP	Xtcp
5521	TCP	Illusion Mailer
5550	TCP	Xtcp
5555	TCP	ServeMe
5556	TCP	BO Facil
5557	TCP	BO Facil
5558	TCP	Backdoor.Easyserv
5569	TCP	Robo-Hack

Continued

Port #	Protocol	Type of attack
5637	TCP	PC Crasher
5638	TCP	PC Crasher
5714	TCP	WinCrash
5741	TCP	WinCrash
5742	TCP	WinCrash
6000	TCP	The Thing 1.6
6112	TCP/UDP	Battle.net Game (not a Trojan)
6346	TCP	Gnutella clone (not a Trojan)
6400	TCP	The Thing
6667	TCP	Sub-7 Trojan (new ICQ notification)
6669	TCP	Vampyre
6670	TCP	Deep Throat
6671	TCP	Deep Throat
6711	TCP	SubSeven, Backdoor.G
6712	TCP	SubSeven
6713	TCP	SubSeven
6723	TCP	Mstream attack-handler
6771	TCP	Deep Throat
6776	TCP	SubSeven, Backdoor.G
6838	UDP	Mstream Agent-handler
6912	TCP	Sh*t Heap
6939	TCP	Indoctrination
6969	TCP	Backdoor.Sparta.B
6970	TCP	Gate Crasher
7000	TCP	Remote Grab
7028	TCP/UDP	Unknown Trojan
7300	TCP	Net Monitor
7301	TCP	Net Monitor

Port #	Protocol	Type of attack
7306	TCP	Net Monitor
7307	TCP	Net Monitor
7308	TCP	Net Monitor
7410	TCP	Backdoor.phoenix
7597	TCP	QaZ (Remote Access Trojan)
7614	TCP	Backdoor.GRM
7789	TCP	ICKiller
7983	UDP	MStream handler-agent
8012	TCP	Backdoor.Ptakks.b
8080	TCP	Ring Zero
8787	TCP/UDP	BackOrifice 2000
8811	TCP/UDP	Backdoor.Fearic
8879	TCP/UDP	BackOrifice 2000
8888	TCP	W32.Axatak
8889	TCP	W32.Axatak
9325	UDP	MStream Agent-handler
9400	TCP	InCommand
9696	TCP	Backdoor.gholame
9697	TCP	Backdoor.gholame
9872	TCP	Portal of Doom
9873	TCP	Portal of Doom
9874	TCP	Portal of Doom
9875	TCP	Portal of Doom
9876	TCP	Cyber Attacker
9878	TCP	Trans Scout
9989	TCP	iNi-Killer
9999	TCP	The Prayer 1.2–1.3

Continued

Port #	Protocol	Type of attack
10008	TCP	Cheese worm
10067	TCP/UDP	Portal of Doom
10167	TCP/UDP	Portal of Doom
10498	UDP	Mstream handler-agent
10520	TCP	Acid Shivers
10607	TCP	Coma
10666	TCP	Ambush
11000	TCP	Senna Spy
11050	TCP	Host Control
11223	TCP	Progenic Trojan
11831	TCP	Latinus Server
12076	TCP	GJamer
12223	TCP	Hack'99, KeyLogger
12345	TCP	Netbus, Ultor's Trojan
12346	TCP	Netbus
12361	TCP	Whack-a-Mole
12362	TCP	Whack-a-Mole
12456	TCP	NetBus
12631	TCP	WhackJob
12701	TCP	Eclypse 2000
12754	TCP	Mstream attack-handler
13000	TCP	Senna Spy
13700	TCP	Kuang2 the Virus
15104	TCP	Mstream attack-handler
15432	TCP	Backdoor.Cyn
16322	TCP	Backdoor.Lastdoor
16484	TCP	Mosucker
16959	TCP	SubSeven DEFCON8 2.1 Backdoor

Port #	Protocol	Type of attack
16969	TCP	Priority
17300	TCP	Kuang2 The Virus
18753	UDP	Shaft handler to Agent
20000	TCP	Millennium
20001	TCP	Millennium
20034	TCP	NetBus 2 Pro
20203	TCP	Logged!
20331	TCP	Bla Trojan
20432	TCP	Shaft Client to handlers
20433	TCP	Shaft Agent to handlers
20480	TCP	Trojan.Adnap
21554	TCP/UDP	GirlFriend
22222	TCP	Prosiak
22784	TCP	Backdoor-ADM
23476	TCP	Donald Dick
23477	TCP	Donald Dick
26274	TCP/UDP	Delta Source
27374	UDP	Sub-7 2.1
27379	TCP	Backdoor.optix.04
27444	UDP	Trin00/TFN2K
27573	TCP/UDP	Sub-7 2.1
27665	TCP	Trin00 DoS Attack
29559	TCP	Latinus Server
29891	TCP	The Unexplained
29999	TCP	Backdoor.Antilam.20
30029	TCP	AOL Trojan
30100	TCP	NetSphere

Continued

Port #	Protocol	Type of attack
30101	TCP	NetSphere
30102	TCP	NetSphere
30133	TCP	NetSphere Final
30303	TCP	Sockets de Troie
30999	TCP	Kuang2
31335	UDP	Trin00 DoS Attack
31336	TCP	BO-Whack
31337	TCP	Netpatch
31337	UDP	BackOrifice (BO)
31338	TCP	NetSpy DK
31338	UDP	Deep BO
31339	TCP	NetSpy DK
31666	TCP	BOWhack
31785	TCP	Hack'a'Tack
31787	UDP	Hack'a'Tack
31789	UDP	Hack'a'Tack
31790	UDP	Hack'a'Tack
31791	UDP	Hack'a'Tack
32418	TCP	Acid Battery
33270	TCP	Trinity Trojan
33333	TCP	Prosiak
33390	UDP	Unknown Trojan
33911	TCP	Spirit 2001 a
34324	TCP	BigGluck, TN
37651	TCP	Yet Another Trojan
40412	TCP	The Spy
40421	TCP	Agent, Master's of Paradise
40422	TCP	Master's Paradise
40423	TCP	Master's Paradise

Port #	Protocol	Type of attack
40425	TCP	Master’s Paradise
40426	TCP	Master’s Paradise
43210	TCP	Master’s Paradise
47252	TCP	Delta Source
47262	UDP	Delta Source
47891	TCP	Backdoor.antilam.20
49301	UDP	OnLine keyLogger
50505	TCP	Sockets de Trois v2.
50776	TCP	Fore
51234	TCP	Backdoor.Cyn
53001	TCP	Remote Windows Shutdown
54320	TCP	BackOrifice 2000
54320	UDP	BackOrifice
54321	TCP	School Bus, BackOrifice
54321	UDP	BackOrifice 2000
56565	TCP	Backdoor.Osirdoor
57341	TCP/UDP	NetRaider Trojan
58008	TCP	BackDoor.Tron
58009	TCP	BackDoor.Tron
59211	TCP	BackDoor.DuckToy
60000	TCP	Deep Throat
61000	TCP	Backdoor.mite
61348	TCP	Bunker-Hill Trojan
61466	TCP	Telecommando
61603	TCP	Bunker-Hill Trojan
63485	TCP	Bunker-Hill Trojan
65000	TCP	Stacheldraht, Devil
65535	TCP	Adore Worm/Linux

Appendix C

Field Guidance on USA Patriot Act 2001

On October 26, 2001, President Bush signed the USA Patriot Act (USAPA) into law. This new law has given sweeping new powers to both domestic law enforcement and international intelligence agencies and has eliminated the checks and balances that previously gave courts the opportunity to ensure that these powers were not abused. Following is the U.S. Department of Justice's field guidance relating to Computer Crime and Electronic Evidence collection under the USA Patriot Act of 2001.

Computer Crime and Intellectual Property Section (CCIPS) Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001

Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations

Previous law: Under previous law, investigators could not obtain a wiretap order to intercept wire communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). For example, in several investigations, hackers have stolen teleconferencing services from a telephone company and used this mode of communication to plan and execute hacking attacks.

Amendment: Section 202 amends 18 U.S.C. § 2516(1) — the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications — by adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses.

This provision will sunset December 31, 2005.

Section 209 Obtaining Voice-Mail and Other Stored Voice Communications

Previous law: Under previous law, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal's home.

Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

Moreover, in large part, the statutory framework envisions a world in which technology-mediated voice communications (such as telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might co-exist in a single transaction, it did not anticipate the convergence of these two kinds of communications typical of today's telecommunications networks. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an ISP by means of a search warrant (as required under 18 U.S.C. § 2703(a)) had no way of knowing whether the inbox messages include voice attachments (i.e., wire communications) which could not be compelled using a search warrant.

Amendment: Section 209 of the Act alters the way in which the wiretap statute and ECPA apply to stored voice communications. The amendments delete "electronic storage" of wire communications from the definition of "wire communication" in section 2510 and insert language in section 2703 to ensure that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

This provision will sunset December 31, 2005.

Section 210 Scope of Subpoenas for Electronic Evidence

Previous law: Subsection 2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer's name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer's true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity.

Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included “local and long-distance telephone toll-billing records,” but did not include parallel terms for communications on computer networks, such as “records of session times and durations.” Similarly, the previous list allowed the government to use a subpoena to obtain the customer’s “telephone number or other subscriber number or identity,” but did not define what that phrase meant in the context of Internet communications.

Amendment: Amendments to section 2703(c) update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes “records of session times and durations,” as well as “any temporarily assigned network address.” In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

Moreover, the amendments clarify that investigators may use a subpoena to obtain the “means and source of payment” that a customer uses to pay for his or her account with a communications provider, “including any credit card or bank account number” 18 U.S.C. §2703(c)(2)(F). While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users’ biographical information. (This section is not subject to the sunset provision in section 224 of the Act).

Section 211 Clarifying the Scope of the Cable Act

Previous law: The law contains two different sets of rules regarding privacy protection of communications and their disclosure to law enforcement: one governing cable service (the “Cable Act”) (47 U.S.C. § 551), and the other applying to the use of telephone service and Internet access (the wiretap statute, 18 U.S.C. § 2510 et seq.; ECPA, 18 U.S.C. § 2701 et seq.; and the pen register and trap and trace statute (the “pen/trap” statute), 18 U.S.C. § 3121 et seq.).

Prior to the amendments in Section 211 of the Act, the Cable Act set out an extremely restrictive system of rules governing law enforcement access to most records possessed by a cable company. For example, the Cable Act did not allow the use of subpoenas or even search warrants to obtain such records. Instead, the cable company had to provide prior notice to the customer (even if he or she were the target of the investigation), and the government had to allow the customer to appear in court with an attorney and then justify to the court the investigative need to obtain the records. The court could then order disclosure of the records only if it found by “clear and convincing evidence”—a standard greater than probable cause or even a preponderance of the evidence—that the subscriber was “reasonably suspected” of engaging in criminal activity. This procedure was completely unworkable for virtually any criminal investigation.

The legal regime created by the Cable Act caused grave difficulties in criminal investigations because today, unlike in 1984 when Congress passed the Cable Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. In recent years, some cable companies have refused to accept subpoenas and court orders pursuant to the pen/trap statute and ECPA, noting the seeming inconsistency of these statutes with the Cable Act’s harsh restrictions. See In re Application of United States, 36 F. Supp. 2d 430 (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) for records from cable company providing Internet service). Treating identical records differently depending on the technology used to access the Internet made little sense. Moreover, these complications at times delayed or ended important investigations.

Amendment: Section 211 of the Act amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services — such as telephone and Internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programming a customer chooses to purchase, such as particular premium channels or "pay-per-view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can use legal process under ECPA to compel the provider to disclose only those customer records relating to Internet service. (This section is not subject to the sunset provision in Section 224 of the Act.)

Section 212 Emergency Disclosures by Communications Providers

Previous law: Previous law relating to voluntary disclosures by communication service providers was inadequate in two respects. First, it contained no special provision allowing providers to disclose customer records or communications in emergencies. If, for example, an Internet service provider ("ISP") independently learned that one of its customers was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the account information to law enforcement could save lives. Since providing this information did not fall within one of the statutory exceptions, however, an ISP making such a disclosure could be sued civilly.

Second, prior to the Act, the law did not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber's login records) to law enforcement for purposes of self-protection, even though providers could disclose the content of communications for this reason. See 18 U.S.C. § 2702(b)(5), 2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. *United States* v. *Auler*, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing *United States* v. *Freeman*, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter, providers must have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime to law enforcement.

Amendment: Section 212 corrects both of these inadequacies in previous law. Section 212 amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers.

The amendments in Section 212 of the Act also change ECPA to allow providers to disclose information to protect their rights and property. It accomplishes this change by two related sets of amendments. First, amendments to sections 2702 and 2703 of title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers do have the statutory authority to disclose non-content records to protect their rights and property. All of these changes will sunset December 31, 2005.

Section 216 Pen Register and Trap and Trace Statute

The pen register and trap and trace statute (the "pen/trap" statute) governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider. The following sections discuss these provisions in greater detail. (This section is not subject to the sunset provision in Section 224 of the Act).

A. USING PEN/TRAP ORDERS TO TRACE COMMUNICATIONS ON COMPUTER NETWORKS

Previous law: When Congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks. Although numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute's telephone-specific language.

Amendment: Section 216 of the Act amends sections 3121, 3123, 3124, and 3127 of title 18 to clarify that the pen/trap statute applies to a broad variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, amendments to section 3123(b)(1)(C) now allow applicants for pen/trap orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information — all "dialing, routing, addressing, and signaling information" — utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Further, because the pen register or trap and trace "device" often cannot be physically "attached" to the target facility, Section 216 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap and trace device to be "attached or applied" to the target facility. Likewise, Section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

B. NATIONWIDE EFFECT OF PEN/TRAP ORDERS

Previous law: Under previous law, a court could only authorize the installation of a pen/trap device "within the jurisdiction of the court." Because of deregulation in the telecommunications industry, however, a single communication may be carried by many providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a string of providers located throughout the country — each requiring a separate order.

Moreover, since, under previous law, a court could only authorize the installation of a pen/trap device within its own jurisdiction, when one provider indicated that the source of a communication was a different carrier in another district, a second order in the new district became necessary. This order had to be acquired by a supporting prosecutor in the new district from a local federal judge — neither of whom had any other interest in the case. Indeed, in one case investigators needed three separate orders to trace a hacker's communications. This duplicative process of obtaining a separate order for each link in the communications chain has delayed or — given the difficulty of real-time tracing — completely thwarted important investigations.

Amendment: Section 216 of the Act divides section 3123 of title 18 into two separate provisions. New subsection (a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

The amendments in Section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

Consistent with the change above, Section 216 of the Act modifies section 3123(b)(1)(C) of title 18 to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal pen/trap orders, an amendment to section 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

C. REPORTS FOR USE OF LAW ENFORCEMENT PEN/TRAP DEVICES ON COMPUTER NETWORKS

Section 216 of the Act also contains an additional requirement for the use of pen/trap devices in a narrow class of cases. Generally, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, the provider itself should be able to collect the needed information and provide it to law enforcement. In certain rare cases, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI's DCS1000) to collect the information. In these infrequent cases, the amendments in section 216 require the law enforcement agency to provide the following information to the court under seal within thirty days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. 18 U.S.C. § 3123(a)(3).

Section 217 Intercepting the Communications of Computer Trespassers

Previous law: Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a "wire or electronic communication" according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a "bizarre result," in which a "computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims." Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Amendment: To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser's communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth, section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of "computer trespasser." Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18 without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers — both because they are authorized users and because they have an existing contractual relationship with the provider. These provisions will sunset December 31, 2005.

Section 220 Nationwide Search Warrants for E-Mail

Previous law: Section 2703(a) requires the government to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. Because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained be "within the district" of the issuing court, however, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations.

Amendment: Section 220 of the Act amends section 2703(a) of title 18 (and parallel provisions elsewhere in section 2703) to allow investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d). This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located. This provision will sunset December 31, 2005.

Section 814 Deterrence and Prevention of Cyberterrorism

Section 814 makes a number of changes to improve 18 U.S.C. § 1030, the Computer Fraud and Abuse Act. This section increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the mens rea required for such offenses to make explicit that a hacker need only intend damage, not a particular type of damage; adds a new offense for damaging computers used for national security or criminal justice; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold.

The following discussion analyzes these and other provisions in more detail.

A. SECTION 1030(C)—RAISING THE MAXIMUM PENALTY FOR HACKERS THAT DAMAGE PROTECTED COMPUTERS AND ELIMINATING MANDATORY MINIMUMS

Previous law: Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years. Certain offenders, however, can cause such severe damage to protected computers that this five-year maximum did not adequately take into account the seriousness of their crimes. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times that amount.

In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

Amendment: Section 814 of the Act raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders. 18 U.S.C. § 1030(c)(4). Congress chose, however, to eliminate all mandatory minimum guidelines sentencing for section 1030 violations.

B. SUBSECTION 1030(C)(2)(C) AND (E)(8)—HACKERS NEED ONLY INTEND TO CAUSE DAMAGE, NOT A PARTICULAR CONSEQUENCE OR DEGREE OF DAMAGE

Previous law: Under previous law, in order to violate subsections (a)(5)(A), an offender had to "intentionally [cause] damage without authorization." Section 1030 defined "damage" as impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least $5,000; (2) modified or impairs medical treatment; (3) caused physical injury; or (4) threatened public health or safety.

The question repeatedly arose, however, whether an offender must intend the $5,000 loss or other special harm, or whether a violation occurs if the person only intends to damage the computer, that in fact ends up causing the $5,000 loss or harming the individuals. It appears that Congress never intended that the language contained in the definition of "damage" would create additional elements of proof of the actor's mental state. Moreover, in most cases, it would be almost impossible to prove this additional intent.

Amendment: Section 814 of the Act restructures the statute to make clear that an individual need only intend to damage the computer or the information on it, and not a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8) (emphasis supplied). Under this clarified structure, in order for the government to prove a violation of 1030(a)(5), it must show that the actor caused damage to a protected computer (with one of the listed mental states), and that the actor's conduct caused either loss exceeding $5,000, impairment of medical records, harm to a person, or threat to public safety. 18 U.S.C. § 1030(a)(5)(B).

C. SECTION 1030(C) — AGGREGATING THE DAMAGE CAUSED BY A HACKER'S ENTIRE COURSE OF CONDUCT

Previous law: Previous law was unclear about whether the government could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional threshold of $5,000 in loss. For example, an individual could unlawfully access five computers on a network on ten different dates — as part of a related course of conduct — but cause only $1,000 loss to each computer during each intrusion. If previous law were interpreted not to allow aggregation, then that person would not have committed a federal crime at all since he or she had not caused over $5,000 to any particular computer.

Amendment: Under the amendments in Section 814 of the Act, the government may now aggregate "loss resulting from a related course of conduct affecting one or more other protected computers" that occurs within a one year period in proving the $5,000 jurisdictional threshold for damaging a protected computer. 18 U.S.C. § 1030(a)(5)(B)(i).

D. 1030(C)(2)(C) — NEW OFFENSE FOR DAMAGING COMPUTERS USED FOR NATIONAL SECURITY AND CRIMINAL JUSTICE

Previous law: Section 1030 previously had no special provision that would enhance punishment for hackers who damage computers used in furtherance of the administration of justice, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over $5,000 loss (or meet one of the other special requirements). Yet these systems serve critical functions and merit felony prosecutions even where the damage is relatively slight. Indeed, attacks on computers used in the national defense that occur during periods of active military engagement are particularly serious — even if they do not cause extensive damage or disrupt the war-fighting capabilities of the military — because they divert time and attention away from the military's proper objectives. Similarly, disruption of court computer systems and data could seriously impair the integrity of the criminal justice system.

Amendment: Amendments in Section 814 of the Act create section 1030(a)(5)(B)(v) to solve this inadequacy. Under this provision, a hacker violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over $5,000.

E. SUBSECTION 1030(E)(2) — EXPANDING THE DEFINITION OF "PROTECTED COMPUTER" TO INCLUDE COMPUTERS IN FOREIGN COUNTRIES

Previous law: Before the amendments in Section 814 of the Act, section 1030 of title 18 defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). The definition did not explicitly include computers outside the United States.

Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Amendment: Section 814 of the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.

In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.

F. SUBSECTION 1030(E)(10) — COUNTING STATE CONVICTIONS AS "PRIOR OFFENSES"

Previous law: Under previous law, the court at sentencing could, of course, consider the offender's prior convictions for State computer crime offenses. State convictions, however, did not trigger the recidivist sentencing provisions of section 1030, which double the maximum penalties available under the statute.

Amendment: Section 814 of the Act alters the definition of "conviction" so that it includes convictions for serious computer hacking crimes under State law — i.e., State felonies where an element of the offense is "unauthorized access, or exceeding authorized access, to a computer." 18 U.S.C. § 1030(e)(10).

G. SUBSECTION 1030(E)(11) — DEFINITION OF "LOSS"

Previous law: Calculating "loss" is important where the government seeks to prove that an individual caused over $5,000 loss in order to meet the jurisdictional requirements found in 1030(a)(5)(B)(i). Yet prior to the amendments in Section 814 of the Act, section 1030 of title 18 had no definition of "loss." The only court to address the scope of the definition of loss adopted an inclusive reading of what costs the government may include. In *United States* v. *Middleton*, 231 F.3d 1207, 1210–11 (9th Cir. 2000), the court held that the definition of loss includes a wide range of harms typically suffered by the victims of computer crimes, including costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of interruption of service.

Amendments: Amendments in Section 814 codify the appropriately broad definition of loss adopted in Middleton. 18 U.S.C. § 1030(e)(11).

Section 815 Additional Defense to Civil Actions Relating to Preserving Records in Response to Government Requests

Section 815 added to an existing defense to a cause for damages for violations of the Electronic Communications Privacy Act, Chapter 121 of Title 18. Under prior law it was a defense to such a cause of action to rely in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. This amendment makes clear that the "statutory authorization" defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. § 2703(f).

Section 816 Development and Support of Cybersecurity Forensic Capabilities

Section 816 requires the Attorney General to establish such regional computer forensic laboratories as he considers appropriate, and to provide support for existing computer forensic laboratories, to enable them to provide certain forensic and training capabilities. The provision also authorizes the spending of money to support those laboratories.

Appendix D

Computer Records and the Federal Rules of Evidence

This article (USA Bulletin, March 2001, by Orin S. Kerr, Trial Attorney) explains some of the important issues that can arise when the government seeks the admission of computer records under the Federal Rules of Evidence. The material here is an excerpt of a larger DOJ manual entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," which is available on the Internet at `www.cybercrime.gov/searchmanual.htm`.

Computer Crime and Intellectual Property Section

Most federal courts that have evaluated the admissibility of computer records have focused on computer records as potential hearsay. The courts generally have admitted computer records upon a showing that the records fall within the business records exception, Fed. R. Evid. 803(6):

Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

See, e.g., United States v. Cestnik, 36 F.3d 904, 909–10 (10th Cir. 1994); United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991); United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990); United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988); Capital Marine Supply v. M/V Roland Thomas II, 719 F.2d 104, 106 (5th Cir. 1983). Applying this test, the courts have indicated that computer records generally can be admitted as business records if they were kept pursuant to a routine procedure for motives that tend to assure their accuracy.

However, the federal courts are likely to move away from this "one size fits all" approach as they become more comfortable and familiar with computer records. Like paper records, computer records are not monolithic: the evidentiary issues raised by their admission should depend on what kind of computer records a proponent seeks to have admitted. For example, computer records that contain text often can be divided into two categories: computer-generated records, and records that are merely computer-stored. See People v. Holowko, 486 N.E.2d 877, 878–79 (Ill. 1985). The difference hinges upon whether a person or a machine created the records' contents. Computer-stored records refer to documents that contain the writings of some person or persons and happen to be in electronic form. E-mail messages, word-processing files, and Internet chat room messages provide common examples. As with any other testimony or documentary evidence containing human statements, computer-stored records must comply with the hearsay rule. If the records are admitted to prove the truth of the matter they assert, the offeror of the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy, see Advisory Committee Notes to Proposed Rule 801 (1972), and the records must be authentic.

In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Login records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. Unlike computer-stored records, computer-generated records do not contain human "statements," but only the output of a computer program designed to process input following a defined algorithm. Of course, a computer program can direct a computer to generate a record that mimics a human statement: an e-mail program can announce "You've got mail!" when mail arrives in an inbox, and an ATM receipt can state that $100 was deposited in an account at 2:25 pm. However, the fact that a computer, rather than a human being, has created the record alters the evidentiary issues that the computer-generated records present. See, e.g., 2 J. Strong, McCormick on Evidence §294, at 286 (4th ed. 1992). The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity). See id.; Richard O. Lempert & Steven A. Saltzburg, A Modern Approach to Evidence 370 (2d ed. 1983); Holowko, 486 N.E.2d at 878–79.

Finally, a third category of computer records exists: some computer records are both computer-generated and computer-stored. For example, a suspect in a fraud case might use a spreadsheet program to process financial figures relating to the fraudulent scheme. A computer record containing the output of the program would derive from both human statements (the suspect's input to the spreadsheet program) and computer processing (the mathematical operations of the spreadsheet program). Accordingly, the record combines the evidentiary concerns raised by computer-stored and computer-generated records. The party seeking the admission of the record should address both the hearsay issues implicated by the original input and the authenticity issues raised by the computer processing.

As the federal courts develop a more nuanced appreciation of the distinctions to be made between different kinds of computer records, they are likely to see that the admission of computer records generally raises two distinct issues. First, the government must establish the authenticity of all computer records by providing "evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Second, if the computer records are computer-stored records that contain human statements, the government must show that those human statements are not inadmissible hearsay.

A. Authentication

Before a party may move for admission of a computer record or any other evidence, the proponent must show that it is authentic. That is, the government must offer evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims." Fed. R. Evid. 901(a). See United States v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998).

The standard for authenticating computer records is the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. See United States v. DeGeorgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969); United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982). But see United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in dicta that "the complex nature of computer storage calls for a more comprehensive foundation"). For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) (citing cases). Instead, the witness simply must have first-hand knowledge of the relevant facts to which he or she testifies. See generally United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997) (FBI agent who was present when the defendant's computer was seized can authenticate seized files) United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); Moore, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).

Challenges to the authenticity of computer records often take one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created. Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author.

1. AUTHENTICITY AND THE ALTERATION OF COMPUTER RECORDS

Computer records can be altered easily, and opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. For example, in United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997), the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included detailed records of narcotics sales by three aliases: "Me" (Frost himself, presumably), "Gator" (the nickname of Frost's co-defendant Whitaker), and "Cruz" (the nickname of another dealer). After the government permitted Frost to help retrieve the evidence from his computer and declined to establish a formal chain of custody for the computer at trial, Whitaker argued that the files implicating him through his alias were not properly authenticated. Whitaker argued that "with a few rapid keystrokes, Frost could have easily added Whitaker's alias, "Gator" to the printouts in order to finger Whitaker and to appear more helpful to the government." Id. at 602.

The courts have responded with considerable skepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. See Whitaker, 127 F.3d at 602 (declining to disturb trial judge's ruling that computer records were admissible because allegation of tampering was "almost wild-eyed speculation . . . [without] evidence to support such a scenario"); United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."). Id. at 559. This is consistent with the rule used to establish the authenticity of other evidence such as narcotics. See United States v. Allen, 106 F.3d 695, 700 (6th Cir. 1997) ("Merely raising the possibility of tampering is insufficient to render evidence inadmissible."). Absent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility. See Bonallo, 858 F.2d at 1436.

2. ESTABLISHING THE RELIABILITY OF COMPUTER PROGRAMS

The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. If the program's output is inaccurate, the record may not be "what its proponent claims" according to Fed. R. Evid. 901.

Defendants in criminal trials often attempt to challenge the authenticity of computer-generated records by challenging the reliability of the programs. See, e.g., United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir. 1970); United States v. Liebert, 519 F.2d 542, 547–48 (3d Cir. 1975). The courts have indicated that the government can overcome this challenge so long as "the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof[.]" United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990). See also Liebert, 519 F.2d at 547; DeGeorgia, 420 F.2d. at 893 n.11. Compare Fed. R. Evid. 901(b)(9) (indicating that matters created according to a process or system can be authenticated with "[e]vidence describing a process or system used . . . and showing that the process or system produces an accurate result"). In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. See, e.g., United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) ("[T]he ordinary business circumstances described suggest trustworthiness, . . . at least where absolutely nothing in the record in any way implies the lack thereof.") (computerized tax records held by the IRS); Briscoe, 896 F.2d at 1494 (computerized telephone records held by Illinois Bell). When the computer program is not used on a regular basis and the government cannot establish reliability based on reliance in the ordinary course of business, the government may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests. Dioguardi, 428 F.2d at 1038. Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from . . . the operation of the computer program" affect only the weight of the evidence, not its admissibility. United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988).

Prosecutors may note the conceptual overlap between establishing the authenticity of a computer-generated record and establishing the trustworthiness of a computer record for the business record exception to the hearsay rule. In fact, federal courts that evaluate the authenticity of computer-generated records often assume that the records contain hearsay, and then apply the business records exception. See, e.g., United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (applying business records exception to telephone records generated "automatically" by a computer); United States v. Vela, 673 F.2d 86, 89–90 (5th Cir. 1982) (same). As discussed later in this article, this analysis is technically incorrect in many cases: computer records generated entirely by computers cannot contain hearsay and cannot qualify for the business records exception because they do not contain human "statements." See Part B, infra. As a practical matter, however, prosecutors who lay a foundation to establish a computer-generated record as a business record will also lay the foundation to establish the record's authenticity. Evidence that a computer program is sufficiently trustworthy so that its results qualify as business records according to Fed. R. Evid. 803(6) also establishes the authenticity of the record. Compare United States v. Saputski, 496 F.2d 140, 142 (9th Cir. 1974).

3. IDENTIFYING THE AUTHOR OF COMPUTER-STORED RECORDS

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records consist of a long string of zeros and ones that do not necessarily identify their author. This is a particular problem with Internet communications, which offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous e-mails, and Internet Relay Chat channels permit users to communicate without disclosing their real names. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the authenticity of the record by challenging the identity of its author.

Circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record. For example, in United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998), prosecutors sought to show that the defendant had conversed with an undercover FBI agent in an Internet chat room devoted to child pornography. The government offered a printout of an Internet chat conversation between the agent and an individual identified as "Stavron," and sought to show that "Stavron" was the defendant. The district court admitted the printout in evidence at trial. On appeal following his conviction, Simpson argued that "because the government could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice," the printout had not been authenticated and should have been excluded. Id. at 1249.

The Tenth Circuit rejected this argument, noting the considerable circumstantial evidence that "Stavron" was the defendant. See id. at 1250. For example, "Stavron" had told the undercover agent that his real name was "B. Simpson," gave a home address that matched Simpson's, and appeared to be accessing the Internet from an account registered to Simpson. Further, the police found records in Simpson's home that listed the name, address, and phone number that the undercover agent had sent to "Stavron." Accordingly, the government had provided evidence sufficient to support a finding that the defendant was "Stavron," and the printout was properly authenticated. See id. at 1250. See also United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000) (concluding that district court properly admitted chat room log printouts in circumstances similar to those in Simpson). But see United States v. Jackson, 208 F.3d 638 (7th Cir. 2000) (concluding that web postings purporting to be statements made by white supremacist groups were properly excluded on authentication grounds absent evidence that the postings were actually posted by the groups).

B. Hearsay

Federal courts have often assumed that all computer records contain hearsay. A more nuanced view suggests that in fact only a portion of computer records contain hearsay. When a computer record contains the assertions of a person, whether or not processed by a computer, the record can contain hearsay. In such cases, the government must fit the record within a hearsay exception such as the business records exception, Fed. R. Evid. 803(6). When a computer record contains only computer-generated data untouched by human hands, however, the record cannot contain hearsay. In such cases, the government must establish the authenticity of the record, but does not need to establish that a hearsay exception applies for the records to be admissible.

1. INAPPLICABILITY OF THE HEARSAY RULES TO COMPUTER-GENERATED RECORDS

The hearsay rules exist to prevent unreliable out-of-court statements by human declarants from improperly influencing the outcomes of trials. Because people can misinterpret or misrepresent their experiences, the hearsay rules express a strong preference for testing human assertions in court, where the declarant can be placed on the stand and subjected to cross-examination. See Ohio v. Roberts, 448 U.S. 56, 62–66 (1980). This rationale does not apply when an animal or a machine makes an assertion: beeping machines and barking dogs cannot be called to the witness stand for cross-examination at trial. The Federal Rules have adopted this logic. By definition, an assertion cannot contain hearsay if it was not made by a human being. Can we just use the word person? See Fed. R. Evid. 801(a) ("A 'statement' is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion.") (emphasis added); Fed. R. Evid. 801(b) ("A declarant is a person who makes a statement.") (emphasis added).

As several courts and commentators have noted, this limitation on the hearsay rules necessarily means that computer-generated records untouched by human hands cannot contain hearsay. One state supreme court articulated the distinction in an early case involving the use of automated telephone records:

The printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out-of-court declarants. Nor can we say that this printout itself is a "statement" constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. Of concern is the possibility that a witness may consciously or unconsciously misrepresent what the declarant told him or that the declarant may consciously or unconsciously misrepresent a fact or occurrence. With a machine, however, there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly.

State v. Armstead, 432 So.2d 837, 840 (La. 1983). See also People v. Holowko, 486 N.E.2d 877, 878–79 (Ill. 1985) (automated trap and trace records); United States v. Duncan, 30 M.J. 1284, 1287–89 (N-M.C.M.R. 1990) (computerized records of ATM transactions); 2 J. Strong, McCormick on Evidence §294, at 286 (4th ed.1992); Richard O. Lempert & Stephen A. Saltzburg, A Modern Approach to Evidence 370 (2d ed. 1983). Cf. United States v. Fernandez-Roque, 703 F.2d 808, 812 n.2 (5th Cir. 1983) (rejecting hearsay objection to admission of automated telephone records because "the fact that these calls occurred is not a hearsay statement."). Accordingly, a properly authenticated computer-generated record is admissible. See Lempert & Saltzburg, at 370.

The insight that computer-generated records cannot contain hearsay is important because courts that assume the existence of hearsay may wrongfully exclude computer-generated evidence if a hearsay exception does not apply. For example, in United States v. Blackburn, 992 F.2d 666 (7th Cir. 1993), a bank robber left his eyeglasses behind in an abandoned stolen car. The prosecution's evidence against the defendant included a computer printout from a machine that tests the curvature of eyeglass lenses. The printout revealed that the prescription of the eyeglasses found in the stolen car exactly matched the defendant's. At trial, the district court assumed that the computer printout was hearsay, but concluded that the printout was an admissible business record according to Fed. R. Evid. 803(6). On appeal following conviction, the Seventh Circuit also assumed that the printout contained hearsay, but agreed with the defendant that the printout could not be admitted as a business record: the [computer-generated] report in this case was not kept in the course of a regularly conducted business activity, but rather was specially prepared at the behest of the FBI and with the knowledge that any information it supplied would be used in an ongoing criminal investigation. . . . In finding this report inadmissible under Rule 803(6), we adhere to the well-established rule that documents made in anticipation of litigation are inadmissible under the business records exception. Id. at 670. See also Fed. R. Evid. 803(6) (stating that business records must be "made . . . by, or transmitted by, a person").

Fortunately, the Blackburn court ultimately affirmed the conviction, concluding that the computer printout was sufficiently reliable that it could have been admitted under the residual hearsay exception, Rule 803(24). See id. at 672. However, instead of flirting with the idea of excluding the printouts because Rule 803(6) did not apply, the court should have asked whether the computer printout from the lens-testing machine contained hearsay at all. This question would have revealed that the computer-generated printout could not be excluded on hearsay grounds because it contained no human "statements."

2. APPLICABILITY OF THE HEARSAY RULES TO COMPUTER-STORED RECORDS

Computer-stored records that contain human statements must satisfy an exception to the hearsay rule if they are offered for the truth of the matter asserted. Before a court will admit the records, the court must establish that the statements contained in the record were made in circumstances that tend to ensure their trustworthiness. See, e.g., Jackson, 208 F.3d at 637 (concluding that postings from the websites of white supremacist groups contained hearsay, and rejecting the argument that the postings were the business records of the ISPs that hosted the sites).

As discussed earlier in this article, courts generally permit computer-stored records to be admitted as business records according to Fed. R. Evid. 803(6). Different circuits have articulated slightly different standards for the admissibility of computer-stored business records. Some courts simply apply the direct language of Fed. R. Evid. 803(6). See e.g., United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991); United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988). Other circuits have articulated doctrinal tests specifically for computer records that largely (but not exactly) track the requirements of Rule 803(6). See, e.g., United States v. Cestnik, 36 F.3d 904, 909–10 (10th Cir. 1994) ("Computer business records are admissible if (1) they are kept pursuant to a routine procedure designed to assure their accuracy; (2) they are created for motives that tend to assure accuracy (e.g., not including those prepared for litigation); and (3) they are not themselves mere accumulations of hearsay.") (quoting Capital Marine Supply v. M/V Roland Thomas II, 719 F.2d 104, 106 (5th Cir. 1983)); United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990) (computer-stored records are admissible business records if they "are kept in the course of regularly conducted business activity, and [that it] was the regular practice of that business activity to make records, as shown by the testimony of the custodian or other qualified witness.") (quoting United States v. Chappell, 698 F.2d 308, 311 (7th Cir. 1983)). Notably, the printout itself may be produced in anticipation of litigation without running afoul of the business records exception. The requirement that the record be kept "in the course of a regularly conducted business activity" refers to the underlying data, not the actual printout of that data. See United States v. Sanders, 749 F.2d 195, 198 (5th Cir. 1984).

From a practical perspective, the procedure for admitting a computer-stored record pursuant to the business records exception is the same as admitting any other business record. Consider an e-mail harassment case. To help establish that the defendant was the sender of the harassing messages, the prosecution may seek the introduction of records from the sender's ISP showing that the defendant was the registered owner of the account from which the e-mails were sent. Ordinarily, this will require testimony from an employee of the ISP ("the custodian or other qualified witness") that the ISP regularly maintains customer account records for billing and other purposes, and that the records to be offered for admission are such records that were made at or near the time of the events they describe in the regular course of the ISP's business. Again, the key is establishing that the computer system from which the record was obtained is maintained in the ordinary course of business, and that it is a regular practice of the business to rely upon those records for their accuracy.

The business record exception is the most common hearsay exception applied to computer records. Of course, other hearsay exceptions may be applicable in appropriate cases. See, e.g., Hughes v. United States, 953 F.2d 531, 540 (9th Cir. 1992) (concluding that computerized IRS forms are admissible as public records under Fed. R. Evid. 803(8)).

C. Other Issues

The authentication requirement and the hearsay rule usually provide the most significant hurdles that prosecutors will encounter when seeking the admission of computer records. However, some agents and prosecutors have occasionally considered two additional issues: the application of the best evidence rule to computer records, and whether computer printouts are "summaries" that must comply with Fed. R. Evid. 1006.

1. THE BEST EVIDENCE RULE

The best evidence rule states that to prove the content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required. See Fed. R. Evid. 1002. Agents and prosecutors occasionally express concern that a mere printout of a computer-stored electronic file may not be an "original" for the purpose of the best evidence rule. After all, the original file is merely a collection of 0's and 1's. In contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes.

Fortunately, the Federal Rules of Evidence have expressly addressed this concern. The Federal Rules state that [i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original" Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. See Doe v. United States, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality. While strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout. Advisory Committee Notes, Proposed Federal Rule of Evidence 1001(3) (1972).

2. COMPUTER PRINTOUTS AS "SUMMARIES"

Federal Rule of Evidence 1006 permits parties to offer summaries of voluminous evidence in the form of "a chart, summary, or calculation" subject to certain restrictions. Agents and prosecutors occasionally ask whether a computer printout is necessarily a "summary" of evidence that must comply with Fed. R. Evid. 1006. In general, the answer is no. See Sanders, 749 F.2d at 199; Catabran, 836 F.2d at 456–57; United States v. Russo, 480 F.2d 1228, 1240–41 (6th Cir. 1973). Of course, if the computer printout is merely a summary of other admissible evidence, Rule 1006 will apply just as it does to other summaries of evidence.

About the Author: Orin S. Kerr is a Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice.

Appendix E

Glossary

Audit Examination and/or assessment of actions and records to ensure compliance with policies and operational procedures. If problems are found, recommendations are made to change policies or procedures.

Audit Trail A chronological record showing who has accessed a computer system and what operations were performed during specific time periods. This typically includes file access, user login, and whether any actual or attempted security violations have occurred.

Authentication The process of verifying that an individual or data really is who or what it is proclaimed to be. It is often used as a prerequisite for permitting access to resources in a system.

Backdoor A hole in the security of a computer system deliberately left in place by authorized programmers or repair personnel, but these can also be left behind by malicious intruders to get back into a system after having breached it once. Synonymous to a trap door, which is a hidden software or hardware apparatus used to circumvent security mechanisms.

Backup A copy of files and programs made to facilitate recovery of lost or corrupted data, if necessary.

Breach Any prohibited penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Business Continuity Plan (BCP) A predetermined set of procedures or directives that describe how an organization's business functions will continue during and after a system disruption.

Chain-of-Custody Protection of evidence by all individuals with access to ensure against loss, breakage, alteration, or unauthorized handling. This includes accurately identifying, securing, and dating all evidence.

Compromise Invasion of a system by skirting its security.

Compromise of Integrity The unauthorized alteration of authenticated information.

Computer Incident Response Team A group of technical investigators and security engineers that responds to and investigates computer security incidents.

Computer Security Incident An adverse event wherein some aspect of a computer system is threatened for example, loss of data confidentiality, disruption of data or system integrity, and disruption or denial of availability.

Copy The result or action of reading electronic data from a source, leaving that data unchanged, and writing the same data elsewhere on a medium that may differ from the source.

Cracker An individual who intentionally breaches computer security (usually by using a password-cracking tool) to infiltrate a computer or network, most often with malicious intent.

Damage Intentional or accidental modification, destruction, or removal of information from a computer system. Such damage to information may result in injury to an organization's reputation and/or financial losses.

Database A collection of information data consisting of at least one file, usually stored in one location, which may be available to several users simultaneously for various applications.

Denial of Service (DoS) The inability to use system resources due to unavailability stemming from a variety of causes for example, infiltrations by hackers, the flooding of IP addresses from external messages, and network worms.

Disaster Recovery Plan A plan (in written form) outlining steps and procedures to be followed in the event of a major hardware or software failure or destruction of facilities (unlike the Business Continuity Plan, which focuses primarily on maintaining and regaining normal business operations).

Discoverable Data Electronic data that can be obtained by an opponent in a litigation process.

Distributed Denial of Service (DDoS) Denial of Service attempts involving multiple Internet-connected systems launching or being used in attacks against one or more target systems.

Electronic Records Information stored in a format that can only be read and processed by a computer.

Encryption A technique for scrambling data to prevent unauthorized users from reading or tampering with that data. The data can include messages, files, folders, or disks, and only those with a password or key can decrypt and use the data.

Enhanced Metafile (EMF) In the Windows operating system, the 32-bit spool file format used in printing. The EMF format was created to solve the deficiencies of the original Windows Metafile format in printing graphics from sophisticated graphics programs.

Event A discernible episode or phase of a computer incident investigation that can be documented, verified, and analyzed.

Event Viewer In Windows NT, a utility used to display event logs. With Event Viewer, users can monitor events recorded in the Application, Security, and System logs.

Exploit To use a program or technique to take advantage of vulnerabilities or flaws in hardware or software.

File Allocation Table An MS-DOS file system located in the boot sector of the disk that stores the addresses of all files contained on a disk.

File Sharing The sharing of computer data, usually within a network, with users having varying degrees of access privileges. Users may be able to view, write to, modify, or print information to or from the shared file.

Firewall Hardware and software devices designed to thwart unauthorized connections to or from a computer (or network). Firewalls enforce an organization's network access policies by examining and evaluating Internet connections as they pass through the firewall.

Forensic Analysis The examination of materials and information to determine their vital features to discover evidence in a manner that is admissible in a court of law.

Hacker An individual (usually a proficient programmer) who is skilled at penetrating computer systems, often applying a variety of methods to do so.

Hoax Usually transmitted through e-mail, a hoax contains a message to send the alert to as many others as possible. Though they are not viruses, hoaxes may cause work disruption through false scares or provoke a Denial of Service through their proliferation by overloading the e-mail system.

Honeypot A lure set up to trap hackers and users with malicious intent as they attempt to gain entry into a computer system.

Incident An adverse computer security event or series of events that affects the organization's computer security and/or its ability to do business.

Incident Handling The action or actions taken to resolve a computer security incident.

Incident Oversight The ongoing surveillance of networks and systems to uncover deficiencies in security and take action before incidents can occur.

Incident Reporting The formal acknowledgement that a computer security incident has been detected.

Incident Response The process of analyzing a security incident how it was able to occur and how to prevent similar incidents from occurring in the future.

Incident Response Plan A documented plan of action directives and procedures for identifying, countering, and mitigating the damages resulting from malicious attacks against an organization's computer systems.

Intruder A person who is the perpetrator of a computer security incident often referred to as hackers or crackers (see "Hacker" above). An intruder is a vandal who may be operating from within the boundaries of an organization or attacking it from the outside.

Intrusion Unauthorized, inappropriate, and/or illegal activity by perpetrators either inside or outside an organization that can be deemed a system penetration.

Intrusion Detection System A security mechanism that monitors and analyzes system events to provide near real-time warnings to unauthorized access to system resources or to archive log and traffic information for later analysis.

Level of Consequence The impact an incident has on an organization, including loss of data, negative consequences to the organization (for example, damage to reputation), and the magnitude of damage that must be corrected.

Local Area Network (LAN) A group of computers and other network devices that exist in a limited area such as a single building. These devices are connected by a special communications link that permits any device to interact with any other device over the network.

Login The act of connecting to a computer system (or network) by a user, usually after entering a password and user ID.

Malicious Code Programming code designed to damage a computer system or data contained on a system. It is traditionally classified into three categories: viruses, worms, and Trojan horses, based upon the behavior of the code.

Media Various formats used for recording electronic data, including disks, film, computer tapes, and paper.

Mission-Critical Application An application that is vital to an organization's ability to carry out required operations.

Misuse The use or exploitation of a computer by an unsanctioned user (either an insider or intruder).

Need-to-Know Basis The need for access to, knowledge of, or possession of sensitive information in order to carry out required, authorized duties.

Network Port Scanning The process of probing selected service port numbers (for example, NetBIOS -139, FTP -21, and so on) over an IP network with the purpose of identifying available network services on that system. Network port scanning is an information-gathering process often helpful for troubleshooting system problems or tightening system security, but it's often performed as a prelude to an attack.

New Technology File System (NTFS) The file system used with the Windows NT operating system for storing and retrieving files on a hard disk.

Packet Sniffer A program or device that captures and analyzes data that travels between networked computers.

Password A unique sequence of characters that a user types as an authentication code to gain access to computers and/or sensitive files.

Penetration Testing The attempt to discern the level of security that is protecting a system or network. Such testing includes trying to evade security measures using the same tools and techniques that a potential attacker might use. Penetration testing may be used by a company to identify and correct security weaknesses.

Physical Security The procedures used by an organization to ensure that material (physical) resources are protected from both deliberate and unintentional threats.

Port A connecting point (gateway or portal) between a computer and another device. Identified by numbers ranging from zero to 65,536, ports enable the establishment of a session between a host and a Web server for network services. Popular services have reserved port numbers: TELNET is at port 23, and HTTP is at port 80, for example. Ports are usually targeted for attack by hackers and Trojan horses in order to gain access to a computer system.

Print Spooler File The print spooler is an executable file that manages the printing process and is responsible for scheduling the print job for printing.

Promiscuous Mode When an Ethernet interface reads all information regardless of its destination. This is the opposite of normal mode, when the interface reads packets destined for itself only.

Recordkeeping Managing records electronic or otherwise beginning with their inception (or receipt) through their distribution, processing, and storage to their final destination.

Registry In the Windows operating system, the site where information is kept.

Risk Assessment Determining the efficacy of the security procedures provided for a system or network. Risk assessment evaluates the likelihood of threats occurring and attempts to estimate the degree of losses that may be expected by the organization.

Rootkit A collection of software tools that permits a hacker to set up a backdoor into a computer system. Rootkits collect information about other systems on the network while disguising the fact that the system is compromised. Rootkits are a classic example of Trojan horse software and are available for a wide range of operating systems.

SATAN (Security Administrator Tool for Analyzing Networks) A freeware program that remotely probes networks to identify weaknesses in system security.

Script Kiddies Inexperienced, sometimes immature, rookie hackers with little training in malicious code writing and execution who nevertheless seek out and exploit computer security vulnerabilities, often using well-known, easy-to-find scripts and programs.

Security Audit An authorized investigation of a computer system to identify its inadequacies and vulnerabilities.

Security Policies An organization's documented set of laws, regulations, and directives that standardizes how the organization controls, guards, and distributes sensitive data.

Slack File Space The empty data storage space that exists from the end of a computer file to the end of the last cluster assigned to that file.

Social Engineering A hacking technique that relies on weaknesses in people rather than software with the aim of tricking people into revealing passwords or other information that compromises a target system's security.

Steganography The hiding of a covert message within an ordinary message that is decoded at its destination by the recipient. That the message contains an inserted hidden message remains unknown to (and therefore undetected by) anyone viewing it who has not been made aware of its presence.

Suspicious Activity Network traffic patterns that lie outside the usual definitions of standard traffic and which might indicate unauthorized activity on the network.

Swap File Space on a hard disk that is used to extend a computer's memory. Files not used recently are temporarily stored on the hard disk, leaving room for new files.

Threat A condition or event that has the potential to cause harm to an organization, its personnel, or its property, including computer system resources. Threats include the damage, disclosure, or alteration of data, as well as Denial of Service attacks, fraud, and other abuses. Network security threats include impersonation of authorized personnel, eavesdropping, Denial of Service, and packet modification.

Traceroute A Unix/Linux tool that traces (identifies) the route taken by data packets as they traverse (hop) across a network connection between two hosts and displays the time and location of the route taken to reach the destination computer. In Windows, this same utility is known as tracert.

Trojan Horse A useful and seemingly innocent program containing additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data. A Trojan horse performs some unexpected or unauthorized (usually malicious) actions, such as displaying messages, erasing files, or formatting a disk. A Trojan horse doesn't infect other host files, thus cleaning is not necessary.

Unallocated File Space Space left behind from an erased file, which may still harbor data. Unallocated file space may contain a number of files valuable to a forensic investigation such as intact files, remnants of files, subdirectories, and temporary files created and deleted by computer applications and the operating system.

Vendor Producer of hardware or software applications that are associated with computer technology (routers, operating systems, computers, and switches, for example).

Virus A malicious, self-replicating (or in some instances, executable) program with the potential to leave a computer or entire network inoperable. A virus attaches itself and spreads to files, programs, e-mail messages, and other storage media and may drain system resources (disk space, connections, and memory) and modify or wipe out files or display messages.

Vulnerability A flaw in a computer or network that leaves it susceptible to potential exploitation such as via unauthorized use or access. Vulnerabilities include, but are not limited to, weaknesses in security procedures, administrative or internal controls, or physical configuration, or features or bugs that enable an attacker to bypass security measures.

Vulnerability Scanning The practice of scanning for and identifying known vulnerabilities of computing systems on a computer network. Since vulnerability scanning is an information-gathering process, when performed by unknown individuals it is considered a prelude to attack.

Web Cache Web caching is a technique to improve Web browser performance by storing frequently requested Web pages, images, and other Web objects in a special location on the user's hard drive for faster access. On subsequent requests for the same object, the cache delivers the object from its storage rather than passing the request on to the origin server.

Worm A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or e-mail attachments.

Index

Wiley Publishing, Inc.
End-User License Agreement

READ THIS. You should carefully read these terms and conditions before opening the software packet(s) included with this book "Book". This is a license agreement "Agreement" between you and Wiley Publishing, Inc. "WPI". By opening the accompanying software packet(s), you acknowledge that you have read and accept the following terms and conditions. If you do not agree and do not want to be bound by such terms and conditions, promptly return the Book and the unopened software packet(s) to the place you obtained them for a full refund.

1. **License Grant.** WPI grants to you (either an individual or entity) a nonexclusive license to use one copy of the enclosed software program(s) (collectively, the "Software," solely for your own personal or business purposes on a single computer (whether a standard computer or a workstation component of a multi-user network). The Software is in use on a computer when it is loaded into temporary memory (RAM) or installed into permanent memory (hard disk, CD-ROM, or other storage device). WPI reserves all rights not expressly granted herein.

2. **Ownership.** WPI is the owner of all right, title, and interest, including copyright, in and to the compilation of the Software recorded on the disk(s) or CD-ROM "Software Media". Copyright to the individual programs recorded on the Software Media is owned by the author or other authorized copyright owner of each program. Ownership of the Software and all proprietary rights relating thereto remain with WPI and its licensers.

3. **Restrictions On Use and Transfer.**

   (a) You may only (i) make one copy of the Software for backup or archival purposes, or (ii) transfer the Software to a single hard disk, provided that you keep the original for backup or archival purposes. You may not (i) rent or lease the Software, (ii) copy or reproduce the Software through a LAN or other network system or through any computer subscriber system or bulletin-board system, or (iii) modify, adapt, or create derivative works based on the Software.

   (b) You may not reverse engineer, decompile, or disassemble the Software. You may transfer the Software and user documentation on a permanent basis, provided that the transferee agrees to accept the terms and conditions of this Agreement and you retain no copies. If the Software is an update or has been updated, any transfer must include the most recent update and all prior versions.

4. **Restrictions on Use of Individual Programs.** You must follow the individual requirements and restrictions detailed for each individual program in the About the CD-ROM appendix of this Book. These limitations are also contained in the individual license agreements recorded on the Software Media. These limitations may include a requirement that after using the program for a specified period of time, the user must pay a registration fee or discontinue use. By opening the Software packet(s), you will be agreeing to abide by the licenses and restrictions for these individual programs that are detailed in the About the CD-ROM appendix and on the Software Media. None of the material on this Software Media or listed in this Book may ever be redistributed, in original or modified form, for commercial purposes.

5. **Limited Warranty.**

   (a) WPI warrants that the Software and Software Media are free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of purchase of this Book. If WPI receives notification within the warranty period of defects in materials or workmanship, WPI will replace the defective Software Media.

   (b) WPI AND THE AUTHOR OF THE BOOK DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE PROGRAMS, THE SOURCE CODE CONTAINED THEREIN, AND/OR THE TECHNIQUES DESCRIBED IN THIS BOOK. WPI DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE.

   (c) This limited warranty gives you specific legal rights, and you may have other rights that vary from jurisdiction to jurisdiction.

6. **Remedies.**

   (a) WPI's entire liability and your exclusive remedy for defects in materials and workmanship shall be limited to replacement of the Software Media, which may be returned to WPI with a copy of your receipt at the following address: Software Media Fulfillment Department, Attn.: Incident Response: Computer Forensics Toolkit, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, or call 1-800-762-2974. Please allow four to six weeks for delivery. This Limited Warranty is void if failure of the Software Media has resulted from accident, abuse, or misapplication. Any replacement Software Media will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

   (b) In no event shall WPI or the author be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the Book or the Software, even if WPI has been advised of the possibility of such damages.

   (c) Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation or exclusion may not apply to you.

7. **U.S. Government Restricted Rights.** Use, duplication, or disclosure of the Software for or on behalf of the United States of America, its agencies and/or instrumentalities "U.S. Government" is subject to restrictions as stated in paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, or subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR supplement, as applicable.

8. **General.** This Agreement constitutes the entire understanding of the parties and revokes and supersedes all prior agreements, oral or written, between them and may not be modified or amended except in a writing signed by both parties hereto that specifically refers to this Agreement. This Agreement shall take precedence over any other documents that may be in conflict herewith. If any one or more provisions contained in this Agreement are held by any court or tribunal to be invalid, illegal, or otherwise unenforceable, each and every other provision shall remain in full force and effect.

GNU General Public License

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software — to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms and Conditions for Copying, Distribution and Modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS