b526367 Ch01.qxd 3/21/03 3:37 PM Page 1

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 2

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 3

- ✓ **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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 4

> 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.

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 5

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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 6

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 7

- ✓ 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:

b526367 Ch01.qxd 3/21/03 3:37 PM Page 8

✓ **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.

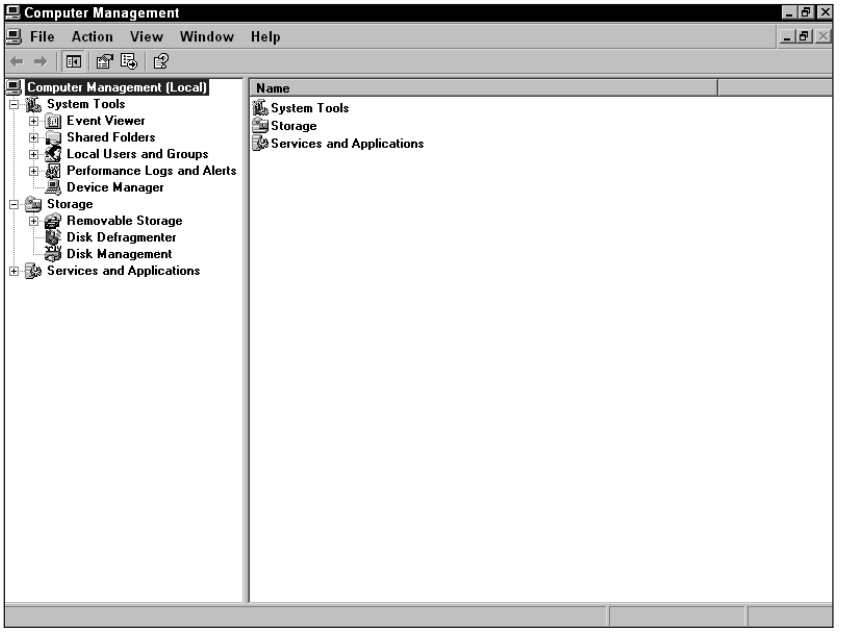

Figure 1-1: The Computer Management utility under Windows XP Professional

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*.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 9

- ✓ **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.

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.

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.

Registry structure is covered in detail in Chapter 4.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 10

- **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.

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 11

- **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.

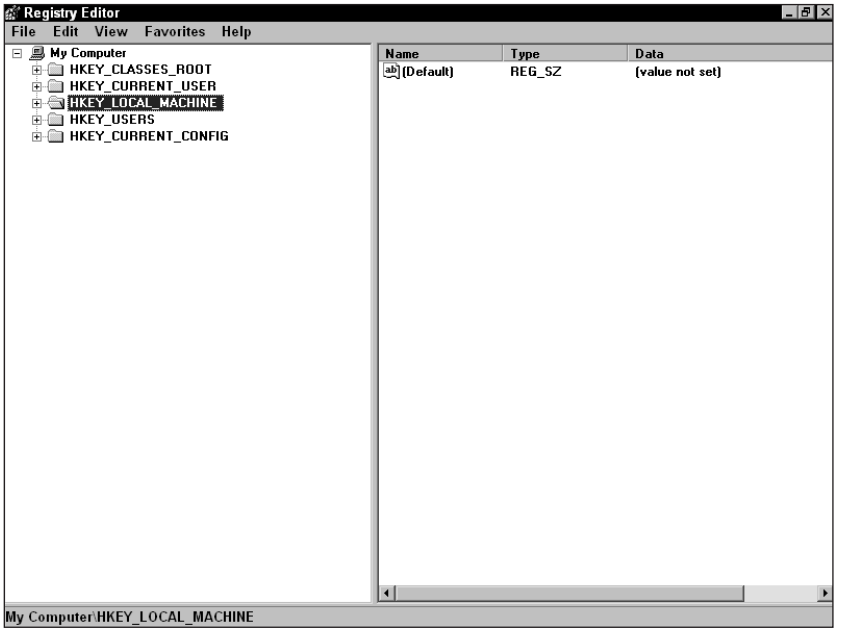

Figure 1-2: The Windows Registry Editor

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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 12

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)

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`.

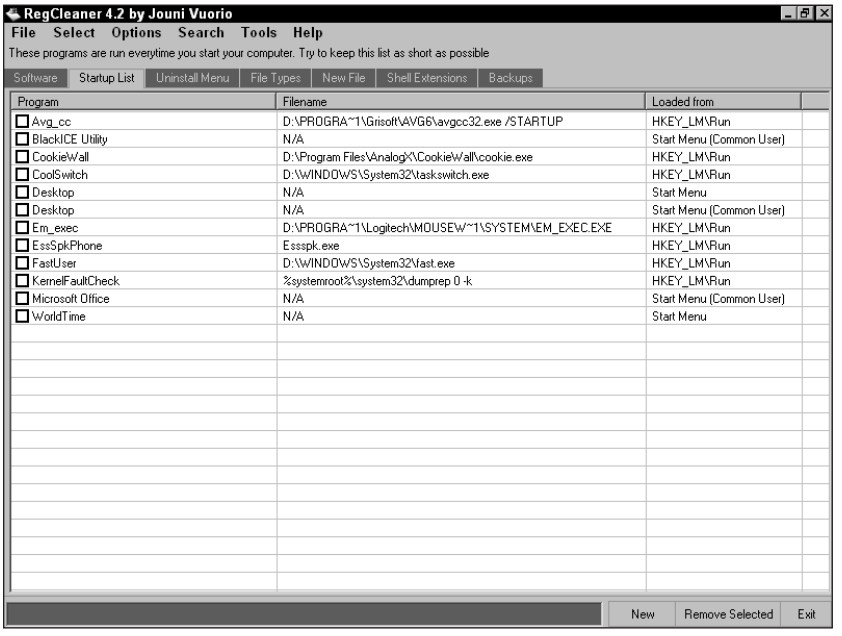

Figure 1-3: RegCleaner by Jouni Vuorio

b526367 Ch01.qxd 3/21/03 3:37 PM Page 13

- ✓ **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`.

For a comprehensive list of ports, see Appendix B.

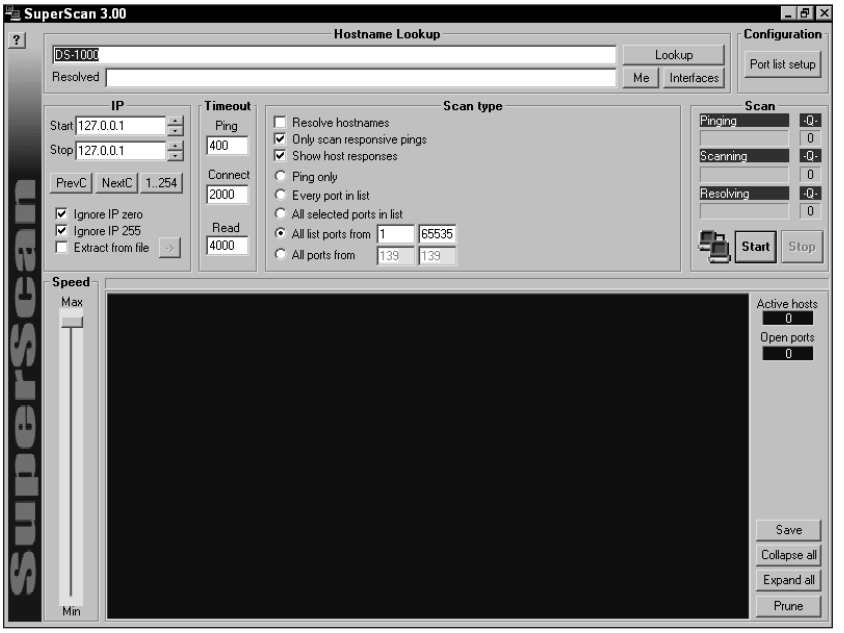

Figure 1-4: SuperScan by Foundstone, Inc. can scan for open or active TCP/UDP ports.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 14

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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 15

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.

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 16

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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 17

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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 18

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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 19

- ✓ 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:

b526367 Ch01.qxd 3/21/03 3:37 PM Page 20

- ✓ 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

b526367 Ch01.qxd 3/21/03 3:37 PM Page 21

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 22

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 23

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 24

- ✓ 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.

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 25

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

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.

b526367 Ch01.qxd 3/21/03 3:37 PM Page 26

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