Chapter 1

Introduction to Computer Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Identify the top threats to a network: security breaches, denial of service attacks, and malware
- Assess the likelihood of an attack on your network
- Define key terms such as *cracker*, *sneaker*, *firewall*, and *authentication*
- Compare and contrast perimeter and layered approaches to network security
- Use online resources to secure your network

Introduction

It's hard to find a facet of modern life that does not involve a computer system, at least on some level. Online purchases, debit cards, and automatic bill pay are standard parts of modern life. Some retailers are using computerized automatic checkout. It is even likely that you have taken a class online, and you may even be using this textbook for a class you are currently taking online. You can, in fact, buy this book online. I personally purchase most of the books I read online.

Because so much of our business is transacted online, a great deal of personal information is stored in computers. Medical records, tax records, school records, and more are all stored in computer databases. This leads to some very important questions:

1. How is information safeguarded?
2. What are the vulnerabilities to these systems?
3. What steps are taken to ensure that these systems and data are safe?

FYI: Where Is the Internet Going?

Recently there have been more expansions to Internet technology and Internet use. Such expansions include increased transmission speeds, a wider use of wireless Internet, and the growing phenomenon of online education. Do you think that we will reach a point where all aspects of our lives have some Internet component? Have we already reached that point?

Recent news stories don't offer encouraging answers to these questions. The media gives a lot of attention to dramatic virus attacks, hackers, and other interesting Internet phenomena. Even the most technically naïve person cannot go more than a few weeks without hearing of some new virus or some hacking incident.

In spite of daily horror stories, however, many people (including some law enforcement professionals and trained computer professionals) lack an adequate understanding about the reality of these threats. Clearly the media will focus attention on the most dramatic computer security breaches, not necessarily giving an accurate picture of the most plausible threat scenarios. It is not uncommon to even encounter the occasional system administrator whose knowledge of computer security is inadequate.

This chapter outlines current dangers, describes the most common types of attacks on your personal computer and network, teaches you how to speak the lingo of both hackers and security professionals, and outlines the broad strokes of what it takes to secure your computer and your network.

In this book, you will learn how to secure both individual computers and entire networks. You will also find out how to secure data transmission, and you will complete an exercise to find out about your region's laws regarding computer security. Perhaps the most crucial discussion in this chapter is what attacks are commonly attempted and how they are perpetrated. In this first chapter we set the stage for the rest of the book by outlining what exactly the dangers are and introducing you to the terminology used by both network security professionals and hackers. All of these topics are explored more fully in subsequent chapters.

How Seriously Should You Take Threats to Network Security?

The first step in understanding computer and network security is to formulate a realistic assessment of the threats to those systems. You will need a clear picture of the dangers in order to adequately prepare a defense. There seem to be two extreme attitudes regarding computer security. The first group assumes there is no real threat. Subscribers to this belief feel that there is little real danger to computer systems, and that much of the negative news is simply unwarranted panic. They often believe taking only minimal security precautions should ensure the safety of their systems. The prevailing sentiment is, if our organization has not been attacked so far, we must be secure. If decision makers subscribe to this point of view, they tend to push a *reactive* approach to security. They will wait to address security issues until an incident occurs—the proverbial "closing the barn door after the horse has already gotten out." If you are fortunate, the incident will have only minor impact on your organization and will serve as a much needed wakeup call. If you are unfortunate, then your organization may face serious and possible catastrophic consequences. One major goal of this book is to encourage a proactive approach to security.

People who subscribe to the opposite viewpoint overestimate the dangers. They tend to assume that talented, numerous hackers are an imminent threat to your system. They may believe that any teenager with a laptop can traverse highly secure systems at will. Such a worldview makes excellent movie plots, but it is simply unrealistic. The reality is that many people who call themselves hackers are less knowledgeable than they think they are. These people have a low probability of being able to compromise any system that has implemented even moderate security precautions.

This does not mean that skillful hackers do not exist, of course. However, they must balance the costs (financial, time) against the rewards (ideological, monetary). "Good" hackers tend to target systems that yield the highest rewards. If a hacker doesn't perceive your system as beneficial to these goals, he is less likely to expend the resources to compromise your system. It is also important to understand that real intrusions into a network take time and effort. Hacking is not the dramatic process you see in movies. I often teach courses in hacking and penetration testing, and students are usually surprised to find that the process is actually a bit tedious and requires patience.

Both extremes of attitudes regarding the dangers to computer systems are inaccurate. It is certainly true that there are people who have the understanding of computer systems and the skills to compromise the security of many, if not most, systems. A number of people who call themselves hackers, though, are not as skilled as they claim to be. They have ascertained a few buzzwords from the Internet and may be convinced of their own digital supremacy, but they are not able to affect any real compromises to even a moderately secure system.

The truly talented hacker is no more common than the truly talented concert pianist. Consider how many people take piano lessons at some point in their lives. Now consider how many of those ever truly become virtuosos. The same is true of computer hackers. Keep in mind that even those who do possess the requisite skill need to be motivated to expend the time and effort to compromise your system.

A better way to assess the threat level to your system is to weigh the attractiveness of your system to potential intruders against the security measures in place.

Keep in mind, too, that the greatest external threat to any system is not hackers, but malware and denial of service attacks. Malware includes viruses, worms, Trojan horses, and logic bombs. And beyond the external attacks, there is the issue of internal problems due to malfeasance or simple ignorance.

Identifying Types of Threats

Most attacks can be categorized as one of six broad classes:

- **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.

- **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server… all the things you probably associate with the term *hacking*.
- **Denial of service (DoS) attacks:** These are designed to prevent legitimate access to your system.
- **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session hijacking:** These attacks are rather advanced, and involve an attacker attempting to take over a session.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

This section offers a broad description of each type of attack. Later chapters go into greater detail with each specific attack, how it is accomplished, and how to avoid it.

Malware

Malware is a generic term for software that has a malicious purpose. This section discusses three types of malware: viruses, Trojan horses, and spyware. Trojan horses and viruses are the most widely encountered.

According to Symantec (makers of Norton antivirus and other software products), a *virus* is "a small program that replicates and hides itself inside other programs, usually without your knowledge" (Symantec, 2003). A computer virus is similar to a biological virus; both are designed to replicate and spread. The most common method for spreading a virus is using the victim's email account to spread the virus to everyone in their address book. Some viruses don't actually harm the system itself, but *all* of them cause network slowdowns due to the heavy network traffic caused by the virus replication.

The *Trojan horse* gets its name from an ancient tale. The city of Troy was besieged for an extended period of time. The attackers could not gain entrance, so they constructed a huge wooden horse and one night left it in front of the gates of Troy. The next morning the residents of Troy saw the horse and assumed it to be a gift, so they rolled the wooden horse into the city. Unbeknownst to them, several soldiers where hidden inside the horse. That evening the soldiers left the horse, opened the city gates, and let their fellow attackers into the city. An electronic Trojan horse works the same way, appearing to be benign software but secretly downloading a virus or some other type of malware onto your computer from within.

Another category of malware currently on the rise is *spyware*. Spyware is simply software that literally spies on what you do on your computer. Spyware can be as simple as a *cookie*—a text file that your browser creates and stores on your hard drive—that a website you have visited downloads to your machine and uses to recognize you when you return to the site. However, that flat file can then be read by the website or by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked.

A *logic bomb* is software that lays dormant until some specific condition is met. That condition is usually a date and time. When the condition is met, then the software does some malicious act such as deleting files, altering system configuration, or perhaps releasing a virus.

Another form of spyware, called a *key logger*, records all of your keystrokes. Some key loggers also take periodic screenshots of your computer. Data is then either stored for later retrieval by the person who installed the key logger or is sent immediately back via email. We will discuss specific types of key loggers later in this book.

Compromising System Security

Next we will look at attacks that breach your system's security. This activity is what is commonly referred to as *hacking*, though that is not the term hackers themselves use. We will delve into appropriate terminology in just a few pages; however, it should be noted at this point that *cracking* is the appropriate word for intruding into a system without permission, usually with malevolent intent. Any attack that is designed to breach your security, either via some operating system flaw or any other means, can be classified as cracking.

Social engineering is a technique for breaching a system's security by exploiting human nature rather than technology. This was the path that the famous hacker Kevin Mitnick most often used. Social engineering uses standard con techniques to get users to give up the information needed to gain access to a target system (Lemos, 2000). The way this method works is rather simple: The perpetrator gets preliminary information about a target organization and leverages it to obtain additional information from the system's users.

Following is an example of social engineering in action. Armed with the name of a system administrator, you might call someone in the business's accounting department and claim to be one of the company's technical support personnel. Mentioning the system administrator's name would help validate that claim, allowing you to ask questions in an attempt to ascertain more details about the system's specifications. A savvy intruder might even get the accounting person to say a username and password. As you can see, this method is based on how well the prospective intruder can manipulate people and actually has little to do with computer skills.

The growing popularity of wireless networks gave rise to new kinds of attacks. One such activity is *war-driving*. This type of attack is an offshoot of *war-dialing*. With war-dialing, a hacker set up a computer to call phone numbers in sequence until another computer answered to try to gain entry to its system. War-driving is much the same concept, applied to locating vulnerable wireless networks. In this scenario, the hacker simply drives around trying to locate wireless networks (Poulsen, 2001). Many people forget that their wireless network signal often extends as much as 100 feet (thus, past walls). At the 2004 DefCon convention for hackers, there was a war-driving contest where contestants drove around the city trying to locate as many vulnerable wireless networks as they could (BlackBeetle, 2004).

Denial of Service Attacks

In a *denial of service* (DoS), the attacker does not actually access the system. Rather, he or she simply blocks access from legitimate users (CERT, 2003). One common way to do prevent legitimate service is to flood the targeted system with so many false connection requests, that the system cannot respond to legitimate requests. DoS is probably the most common attack on the Web.

Web Attacks

By their nature, web servers have to allow communications. Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands. The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

Session Hijacking

Session hijacking can be rather complex to perform. For that reason, it is not a very common form of attack. Simply put, the attacker monitors an authenticated session between the client machine and the server, and takes that session over. We will explore specific methods of how this is done later in this book.

DNS Poisoning

Most of your communication on the Internet will involve DNS, or Domain Name Service. DNS is what translates the domain names you and I understand (like www.ChuckEasttom.com) into IP addresses that computers and routers understand. DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an illicit site, often for the purpose of stealing personal information.

Assessing the Likelihood of an Attack on Your Network

How likely are these attacks? What are the real dangers facing you as an individual or your organization? What are the most likely attacks, and what are your vulnerabilities? Let’s take a look at what threats are out there and which ones are the most likely to cause you or your organization problems.

At one time, the most likely threat to individuals and large organizations was the computer virus. And it is still true that in any given month, several new virus outbreaks will be documented. This situation means that new viruses are being created all the time—and old ones are still out there. However, there are other very common attacks, such as spyware. Spyware is fast becoming as big a problem, even bigger than viruses.

After viruses, the most common attack is unauthorized usage of computer systems. Unauthorized usage includes everything from DoS attacks to outright intrusion of your system. It also includes internal employees misusing system resources. A recent survey by the Computer Security Institute of 223 computer professionals showed over $445 million in losses due to computer security breaches. In 75% of the cases, an Internet connection was the point of attack, while 33% of the professionals cited the location as their internal systems. A rather astonishing 78% of those surveyed detected employee abuse of systems/Internet (Computer Security Institute, 2002). This statistic means that in any organization, one of the chief dangers might be its own employees. A 2007 study by Jeffery Johnson and Zolt Ugray, of Utah State University, showed similar problems.

Basic Security Terminology

Before you embark on the rest of this chapter and this book, it is important to know some basic terminology. The security and hacking terms in this section are merely an introduction to computer security terminology, but they are an excellent starting point to help you prepare for learning more about computer security. Additional terms will be introduced throughout the text and listed in the Glossary at the end of this book.

The world of computer security takes its vocabulary from both the professional security community and the hacker community.

Hacker Slang

You probably have heard the term *hacker* used in movies and in news broadcasts. Most people use it to describe any person who breaks into a computer system. In the hacking community, however, a hacker is an expert on a particular system or systems, a person who simply wants to learn more about the system. Hackers feel that looking at a system's flaws is the best way to learn about that system. For example, someone well versed in the Linux operating system who works to understand that system by learning its weaknesses and flaws would be a hacker.

This process does often mean seeing if a flaw can be exploited to gain access to a system. This "exploiting" part of the process is where hackers differentiate themselves into three groups:

- A white hat hacker, upon finding some flaw in a system, will report the flaw to the vendor of that system. For example, if they were to discover some flaw in Red Hat Linux, they would then email the Red Hat company (probably anonymously) and explain exactly what the flaw is and how it was exploited. White hat hackers are often hired specifically by companies to do penetration tests. The EC Council even has a certification test for white hat hackers, the Certified Ethical Hacker test.

- A black hat hacker is the person normally depicted in the media. Once she gains access to a system, her goal is to cause some type of harm. She might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as crackers.

- A gray hat hacker is normally a law-abiding citizen, but in some cases will venture into illegal activities.

Regardless of how hackers view themselves, intruding on any system is illegal. This means that technically speaking all hackers, regardless of the color of the metaphorical hat they may wear, are in violation of the law. However, many people feel that white hat hackers actually perform a service by finding flaws and informing vendors before those flaws are exploited by less ethically inclined individuals.

Script Kiddies

A hacker is an expert in a given system, as with any profession it includes its share of frauds. So what is the term for someone who calls himself or herself a hacker but lacks the expertise? The most common term for this sort of person is *script kiddy* (Raymond, 1993). The name comes from the fact that the Internet is full of utilities and scripts that one can download to perform some hacking tasks. Many of these tools have an easy-to-use graphical user interface that allows someone with very little if any skill to operate the tool. A classic example is the Low Earth Orbit Ion Cannon tool for executing a DoS attack. Someone who downloads such a tool without really understanding the target system is considered a script kiddy. A significant number of the people you are likely to encounter who call themselves hackers are, in reality, mere script kiddies.

Ethical Hacking: Sneakers

When and why would someone give permission to another party to hack his system? The most common answer is in order to assess system vulnerabilities. This employee, commonly called a *sneaker*, legally breaks into a system in order to assess security deficiencies, such as portrayed in the 1992 film *Sneakers*, starring Robert Redford, Dan Aykroyd, and Sidney Poitier. More and more companies are soliciting the services of such individuals or firms to assess their vulnerabilities.

Anyone hired to assess the vulnerabilities of a system should be both technically proficient and ethical. Run a criminal background check, and avoid those people with problem pasts. There are plenty of legitimate security professionals available who know and understand hacker skills but have never committed security crimes. If you take the argument that hiring convicted hackers means hiring talented people to its logical conclusion, you could surmise that obviously the person in question is not as good a hacker as they would like to think, because they were caught.

Most importantly, giving a person with a criminal background access to your systems is on par with hiring a person with multiple DWI convictions to be your driver. In both cases, you are inviting problems and perhaps assuming significant civil liabilities.

Also some review of their qualifications is clearly in order. Just as there are people who claim to be highly skilled hackers yet are not, there are those who will claim to be skilled sneakers yet lack the skills truly needed. You would not want to inadvertently hire a script kiddy who thinks she is a sneaker. Such a person might then pronounce your system quite sound when, in fact, it was simply a lack of skills that prevented the script kiddy from successfully breaching your security. Later in this book, in

Chapter 11, "Network Scanning and Vulnerability Scanning," we discuss the basics of assessing a target system. In Chapter 11 we also discuss the qualifications you should seek in any consultant you might hire for this purpose.

Phreaking

One specialty type of hacking involves breaking into telephone systems. This subspecialty of hacking is referred to as *phreaking*. The *New Hacker's Dictionary* actually defines phreaking as "the action of using mischievous and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service" (Raymond, 2003). Phreaking requires a rather significant knowledge of telecommunications, and many phreakers have some professional experience working for a phone company or other telecommunications business. Often this type of activity is dependent upon specific technology required to compromise phone systems, more than simply knowing certain techniques.

Professional Terms

Most hacker terminology, as you may have noticed, is concerned with the activity (phreaking) or the person performing the activity (sneaker). In contrast, security professional terminology describes defensive barrier devices, procedures, and policies. This is quite logical because hacking is an offensive activity centered on attackers and attack methodologies, whereas security is a defensive activity concerning itself with defensive barriers and procedures.

Security Devices

The most basic security device is the *firewall*. A firewall is a barrier between a network and the outside world. Sometimes a firewall takes the form of a standalone server, sometimes a router, and sometimes software running on a machine. Whatever its physical form, a firewall filters traffic entering and exiting the network. A *proxy server* is often used with a firewall to hide the internal network's IP address and present a single IP address (its own) to the outside world.

Firewalls and proxy servers guard the perimeter by analyzing traffic (at least inbound and in many cases outbound as well) and blocking traffic that has been disallowed by the administrator. These two safeguards are often augmented by an *intrusion-detection system* (IDS). An IDS simply monitors traffic, looking for suspicious activity that might indicate an attempted intrusion.

Security Activities

In addition to devices, we have activities. *Authentication* is the most basic security activity. It is merely the process of determining if the credentials given by a user or another system (such as a username and password) are authorized to access the network resource in question. When you log in with your username and password, the system will attempt to authenticate that username and password. If it is authenticated, you will be granted access.

Another crucial safeguard is *auditing*, which is the process of reviewing logs, records, and procedures to determine if these items meet standards. This activity will be mentioned in many places throughout this book and will be a definite focus in a few chapters.

The security and hacking terms that we have just covered are only an introduction to computer security terminology, but they provide an excellent starting point that will help you prepare for learning more about computer security. Additional terms will be introduced throughout the text as needed and compiled in the Glossary at the end of the book.

Concepts and Approaches

The approach you take toward security influences all subsequent security decisions and sets the tone for the entire organization's network security infrastructure. Before we delve into various network security paradigms, let us take a moment to examine a few concepts that should permeate your entire thinking about security.

The first concept is the *CIA triangle*. This does not refer to clandestine operating involving the Central Intelligence Agency; rather it is a reference to the three pillars of security: confidentiality, integrity, and availability. When you are thinking about security, your thought processes should always be guided by these three principles. First and foremost, are you keeping the data confidential? Does your approach help guarantee the integrity of data? And does your approach still make the data readily available to authorized users?

Another important concept to keep in mind is *least privileges*. This literally means that each user or service running on your network should have the least number of privileges/access required to do their job. No one should be granted access to anything unless it is absolutely required for their job. In military and intelligence circles this is referred to as "need to know."

Network security paradigms can be classified by either the scope of security measures taken (perimeter, layered) or how proactive the system is.

In a *perimeter security approach*, the bulk of security efforts are focused on the perimeter of the network. This focus might include firewalls, proxy servers, password policies, or any technology or procedure to make unauthorized access of the network less likely. Little or no effort is put into securing the systems within the network. In this approach the perimeter is secured, but the various systems within that perimeter are often vulnerable.

There are additional issues regarding perimeter security that include physical security. That can include fences, closed-circuit TV, guards, locks, and so on, depending on the security needs of your organization.

The perimeter approach is clearly flawed, so why do some companies use it? A small organization might use the perimeter approach if they have budget constraints or inexperienced network administrators. A perimeter method might be adequate for small organizations that do not store sensitive data, but it rarely works in a larger corporate setting.

A *layered security approach* is one in which not only is the perimeter secured, but individual systems within the network are also secured. All servers, workstations, routers, and hubs within the network are secure. One way to accomplish this is to divide the network into segments and secure each segment as if it were a separate network, so if the perimeter security is compromised, not all the internal systems are affected. This is the preferred method whenever possible.

You should also measure your security approach by how proactive/reactive it is. This is done by gauging how much of the system's security infrastructure and policies is dedicated to preventive measures and how much of the security system is designed to respond to attack. A passive security approach takes few or no steps to prevent an attack. A dynamic or proactive defense is one in which steps are taken to prevent attacks before they occur.

One example of this defense is the use of intrusion-detection systems (IDS), which work to detect attempts to circumvent security measures. These systems can tell a system administrator that an attempt to breach security has been made, even if that attempt is not successful. IDS can also be used to detect various techniques intruders use to assess a target system, thus alerting a network administrator to the potential for an attempted breach before the attempt is even initiated.

In the real world, network security is usually not completely in one paradigm or another; it is usually a hybrid approach. Networks generally include elements of both security paradigms. The two categories also combine. One can have a network that is predominantly passive but layered, or one that is primarily perimeter but proactive. It can be helpful to consider approaches to computer security along a Cartesian coordinate system, as illustrated in Figure 1.1, with the *x* axis representing the level of passive-active approaches and the *y* axis depicting the range from perimeter to layered defense.

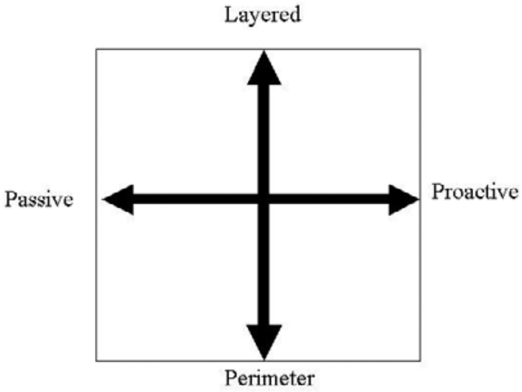

FIGURE 1.1 The security approach guide.

The most desirable hybrid approach is a layered paradigm that is dynamic, which is the upper-right quadrant of the figure.

How Do Legal Issues Impact Network Security?

An increasing number of legal issues affect how one approaches computer security. If your organization is a publicly traded company, a government agency, or does business with either one, there may be legal constraints regarding your network security. Even if your network is not legally bound to these security guidelines, it's useful to understand the various laws impacting computer security. You may choose to apply them to your own security standards.

One of the oldest pieces of legislation in the United States that affects computer security is the Computer Security Act of 1987 (100th Congress, 1987). It requires government agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. This law was a vague mandate ordering federal agencies in the United States to establish security measures, but did not specify any standards.

This legislation established a legal mandate to enact specific standards, paving the way for future guidelines and regulations. It also helped define terms, such as what information is considered "sensitive." This quote is found in the legislation itself:

> The term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. (100th Congress, 1987)

This definition of the word *sensitive* should be kept in mind because it is not just social security information or medical history that must be secured.

When considering what information needs to be secure, simply ask this question: Would the unauthorized access or modification of this information adversely affect your organization? If the answer is yes, then you must consider that information sensitive and in need of security precautions.

Another more specific federal law that applied to mandated security for government systems is OMB Circular A-130 (specifically, Appendix III). This document required that federal agencies establish security programs containing specified elements. It also described requirements for developing standards for computer systems and for records held by government agencies.

Most states have specific laws regarding computer security, such as legislation like the Computer Crimes Act of Florida, the Computer Crime Act of Alabama, and the Computer Crimes Act of Oklahoma. If you're responsible for network security, you might find yourself part of a criminal investigation. This could be an investigation into a hacking incident or employee misuse of computer resources. A list of computer crime laws (organized by state) can be found at http://law.findlaw.com/state-laws/computer-crimes/.

CAUTION

Privacy Laws

It is also critical to keep in mind that any law that governs privacy (such as the Health Insurance Portability and Accountability Act of 1996, HIPAA) also has a direct impact on computer security. If your system is compromised, and thus data that is covered under any privacy statute is compromised, you may need to prove that you exercised due diligence in protecting that data. If it can be shown that you did not take proper precautions, you might be found civilly liable.

Online Security Resources

As you read this book, and when you move out into the professional world, you will have frequent need for additional security resources. Appendix B includes a more complete list of resources, but this section highlights a few of the most important ones you may find useful now.

CERT

The *Computer Emergency Response Team* (CERT, www.cert.org) is sponsored by Carnegie-Mellon University. CERT was the first computer incident-response team, and it is still one of the most respected in the industry. Anyone interested in network security should visit the site routinely. On the website you will find a wealth of documentation, including guidelines for security policies, cutting-edge security research, and more.

Microsoft Security Advisor

Because so many computers today run Microsoft operating systems, another good resource is the Microsoft Security Advisor website: www.microsoft.com/security/default.mspx. This site is a portal to all Microsoft security information, tools, and updates. If you use any Microsoft software, then it is advised that you visit this website regularly.

F-Secure

The F-Secure corporation maintains a website at www.f-secure.com. This site is, among other things, a repository for detailed information on virus outbreaks. Here you will not only find notifications about a particular virus but you will also find detailed information about the virus. This information includes how the virus spreads, ways to recognize the virus, and frequently, specific tools for cleaning an infected system of a particular virus.

SANS Institute

The SANS Institute website (www.sans.org) is a vast repository of security-related documentation. On this site you will find detailed documentation on virtually every aspect of computer security you can imagine. The SANS Institute also sponsors a number of security research projects and publishes information about those projects on their website.

Summary

Network security is a complex and constantly evolving field. Practitioners must stay on top of new threats and solutions and be proactive in assessing risk and protecting their networks. The first step to understanding network security is to become acquainted with the actual threats posed to a network. Without a realistic idea of what threats might affect your systems, you will be unable to effectively protect them. It is also critical that you acquire a basic understanding of the terminology used by both security professionals and those who would seek to compromise your security.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. One extreme viewpoint about computer security is what?

   A. The federal government will handle security.

   B. Microsoft will handle security.

   C. There are no imminent dangers to your system.

   D. There is no danger if you use Linux.

2. Before you can formulate a defense for a network you need what?

   A. Appropriate security certifications

   B. A clear picture of the dangers to be defended against

   C. To finish this textbook

   D. The help of an outside consultant

3. Which of the following is not one of the three major classes of threats?

   A. Attempts to intrude on the system

   B. Online auction fraud

   C. Denial of service attacks

   D. A computer virus

4. What is a computer virus?

   A. Any program that is downloaded to your system without your permission

   B. Any program that self-replicates

   C. Any program that causes harm to your system

   D. Any program that can change your Windows Registry

5. What is spyware?

   A. Any software that monitors your system

   B. Only software that logs keystrokes

   C. Any software used to gather intelligence

   D. Only software that monitors what websites you visit

6. What is a sneaker?

   A. A person who hacks a system without being caught

   B. A person who hacks a system by faking a legitimate password

   C. A person who hacks a system to test its vulnerabilities

   D. A person who is an amateur hacker

7. What is the term for hacking a phone system?

   A. Telco-hacking

   B. Hacking

   C. Cracking

   D. Phreaking

8. What is malware?

   A. Software that has some malicious purpose

   B. Software that is not functioning properly

   C. Software that damages your system

   D. Software that is not properly configured for your system

9. What is war-driving?

   A. Driving and seeking a computer job

   B. Driving while using a wireless connection to hack

   C. Driving looking for wireless networks to hack

   D. Driving and seeking rival hackers

10. When a hacking technique uses persuasion and deception to get a person to provide information to help them compromise security, this is referred to as what?

    A. Social engineering

    B. Conning

    C. Human intel

    D. Soft hacking

11. What is the most common threat on the Internet?

    A. Auction fraud

    B. Hackers

    C. Computer viruses

    D. Illegal software

12. What are the three approaches to security?

    A. Perimeter, layered, hybrid

    B. High security, medium security, low security

    C. Internal, external, and hybrid

    D. Perimeter, complete, none

13. An intrusion-detection system is an example of which of the following?

    A. Proactive security

    B. Perimeter security

    C. Hybrid security

    D. Good security practices

14. Which of the following is the most basic security activity?

    A. Authentication

    B. Firewalls

    C. Password protection

    D. Auditing

15. The most desirable approach to security is one that is which of the following?

    A. Perimeter and dynamic

    B. Layered and dynamic

    C. Perimeter and static

    D. Layered and static

16. According to a recent survey of 223 computer professionals prepared by the Computer Security Institute, which of the following was cited as an issue by more of the respondents?

    A. Internal systems

    B. Employee abuse

    C. Routers

    D. Internet connection

17. Which of the following type of privacy law affects computer security?

    A. Any state privacy law

    B. Any privacy law applicable to your organization

    C. Any privacy law

    D. Any federal privacy law

18. The first computer incident-response team is affiliated with what university?

    A. Massachusetts Institute of Technology

    B. Carnegie-Mellon University

    C. Harvard University

    D. California Technical University

19. Which of the following is the best definition of the term *sensitive information*?

    A. Any information that has impact on national security

    B. Any information that is worth more than $1,000

    C. Any information that if accessed by unauthorized personnel could damage your organization in any way

    D. Any information that is protected by any privacy laws

20. Which of the following is a major resource for detailed information on a computer virus?

    A. The MIT Virus Library

    B. The Microsoft Virus Library

    C. The F-Secure Virus Library

    D. The National Virus Repository

EXERCISES

EXERCISE 1.1: How Many Virus Attacks Have Occurred This Month?

1. Using some website resource, such as www.f-secure.com, look up recent computer virus outbreaks.
2. How many virus outbreaks have occurred in the past 7 days?
3. Write down how many outbreaks there have been in the past 30 days, 90 days, and 1 year.
4. Are virus attacks increasing in frequency?

EXERCISE 1.2: Learning about Cookies as Spyware

1. Get an idea of what kind of information cookies store. You might find the following websites helpful:

   http://computercops.biz/article3911.html

   www.ctc-solutions.co.uk/internet_security_2.html

   www.howstuffworks.com/cookie1.htm

2. Write a brief essay explaining in what way cookies can invade privacy.

EXERCISE 1.3: Hacker Terminology

1. Use the *Hacker's Dictionary* at www.hackersdictionary.com/html/index.html to define the following hacker terms:

   A. Alpha geek

   B. Grok

   C. Red Book

   D. Wank

EXERCISE 1.4: Using Security Resources

1. Using one of the preferred web resources listed in this chapter, find three policy or procedure documents from that resource.

2. List the documents you selected.

3. Write a brief essay explaining why those particular documents are important to your organization's security.

EXERCISE 1.5: Learning About the Law

1. Using the Web, journals, books, or other resources, find out if your state or territory has any laws specific to computer security. You might find the following websites helpful:

   www.usdoj.gov/criminal/cybercrime/cclaws.html

   www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html

   www.ncsl.org/programs/lis/cip/viruslaws.htm

   www.cybercrime.gov/

2. List three laws that you find, with a brief description of each. The list can be a simple one, noting the pertinent laws in your region. Describe each one with one or two sentences.

PROJECTS

PROJECT 1.1: Learning About a Virus

1. Using web resources from Appendix B and sites such as www.f-secure.com, find a virus that has been released in the past 6 months.
2. Research how the virus spread and the damage it caused.
3. Write a brief (half to one page) paper on this virus. Explain how the virus worked, how it spread, and any other essential information you can find.

PROJECT 1.2: Considering the Law (a group project)

Write a description of a computer law that you would like to have passed, along with specifications as to its implementation, enforcement, and justification.

PROJECT 1.3: Recommending Security

1. Using the Web, journals, or books, locate security recommendations from any reputable source, such as the SANS Institute. Any of the sites mentioned in the "Online Security Resources" section of this chapter would be a good choice.
2. List five of those recommendations.
3. Explain why you agree or disagree with each one.

Case Study

In this case study we will consider a network administrator for a small, family-oriented video store. The store is not part of a chain of stores and has a very limited security budget. It has five machines for employees to use to check out movies and one server on which to keep centralized records. That server is in the manager's office. The administrator takes the following security precautions:

1. Each machine is upgraded to Windows XP, with the personal firewall turned on.
2. Antivirus software was installed on all machines.
3. A tape backup is added to the server, and tapes are kept in a file cabinet in the manager's office.
4. Internet access to employee machines is removed.

Now consider these questions:

1. What did these actions accomplish?
2. What additional actions might you recommend?