This chapter covers the following subjects:

- Vulnerabilities
- Threats
- Intruder Motivation
- Types of Attacks

CHAPTER 2

Attack Threats Defined and Detailed

This chapter discusses the potential network vulnerabilities and attacks that pose a threat to the network and provides you with a better understanding of the need for an effective network security policy.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 10-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 2-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 2-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Vulnerabilities	1, 5
Threats	10
Intruder Motivation	4, 6
Types of Attacks	2, 3, 7, 8, 9

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Your boss insists that it is fine to use his wife's name as his password, despite the fact that your security policy states that this is not a sufficient password. What weaknesses are revealed?
   a. This shows a lack of an effective security policy (policy weakness).
   b. This shows a technology weakness.
   c. This shows a protocol weakness.
   d. This shows a configuration weakness.
   e. This shows that your boss is an idiot.

2. You receive a call from a writer for a computer magazine. They are doing a survey of network security practices. What form of attack could this be?
   a. Reconnaissance
   b. Unauthorized access
   c. Data manipulation
   d. Denial of service
   e. None of the above

3. Walking past a programmer's desk, you see that he is using a network analyzer. What category of attack should you watch for?
   a. Reconnaissance
   b. Unauthorized access
   c. Data manipulation
   d. Denial of service
   e. None of the above

4. Looking at the logs, you notice that your manager has erased some system files from your NT system. What is the most likely motivation for this?
   a. Intruding for political purposes
   b. Intruding for profit
   c. Intruding through lack of knowledge
   d. Intruding for fun and pride
   e. Intruding for revenge

5. Your new engineer, who has very little experience working in your corporate environment, has added a new VPN concentrator onto the network. You have been too busy with another project to oversee the installation. What weakness do you need to be aware of concerning his implementation of this device?

   a. Lack of effective policy
   b. Technology weakness
   c. Lack of user knowledge
   d. Operating system weakness
   e. Configuration weakness

6. Statistically, what is the most likely launch site for an attack against your network?

   a. From poor configurations on the firewall
   b. From the Internet over FTP
   c. From the Internet through e-mail
   d. From within your network
   e. None of the above

7. Your accountant claims that all the electronic funds transfers from the previous day were incorrect. What category of attack could this be caused by?

   a. Reconnaissance
   b. Unauthorized access
   c. Denial of service
   d. Data manipulation
   e. None of the above

8. Your logs reveal that someone has attempted to gain access as the administrator of a server. What category of attack could this be?

   a. Reconnaissance
   b. Unauthorized access
   c. Denial of service
   d. Data manipulation
   e. None of the above

9. Your firewall and IDS logs indicate that a host on the Internet scanned all of your public address space looking of connections to TCP port 25. What type of attack does this indicate?

   a. Reconnaissance attack, vertical scan
   b. Reconnaissance attack, block scan
   c. Reconnaissance attack, horizontal scan
   d. Reconnaissance attack, DNS scan
   e. Reconnaissance attack, SMTP scan

10. True or False: A "script kiddie" that is scanning the Internet for "targets of opportunity" represents a structured threat to an organization?

   a. True
   b. False

The answers to the "Do I Know This Already?" quiz are found in the appendix. The suggested choices for your next step are as follows:

- **8 or less overall score**—Read the entire chapter. This includes the "Foundation Topics" and "Foundation Summary" sections and the "Q&A" section.
- **9 or 10 overall score**—If you want more review on these topics, skip to the "Foundation Summary" section and then go to the "Q&A" section. Otherwise, move on to the next chapter.

Foundation Topics

Computer systems have become a fundamental component of nearly every organization today. Large corporations and government organizations devote a tremendous amount of their assets to maintaining their networks, and even the smallest organization is likely to use a computer for maintaining their records and financial information. Because these systems are able to perform functions rapidly and accurately and because they make it very easy to facilitate communication between organizations, computer networks continue to grow and become more interconnected. Any organization that wants to provide some public access to their network maintains a connection to the Internet. This access does not come without certain risks. This chapter defines some of the risks to networks and explains how an ineffective security policy can further increase the chance of a network security breach.

Vulnerabilities

To understand cyberattacks you must remember that computers, no matter how advanced, are still just machines that operate based on predetermined instruction sets. The operating systems and other software packages are just compiled instruction sets that the computer uses to transform input into output. A computer has no capability to determine the difference between authorized and unauthorized input unless this information is written into the instruction sets. Any point in a software package that enables a user to alter the software or gain access to a system (that was not specifically designed into the software) is called a *vulnerability*. In most cases, a cracker can gain access to a network or computer by exploiting a vulnerability if that user does not already have authorized access. (See the section "Internal Threats" later in this chapter.) It is possible to remotely connect to a computer on any of 65,535 ports. As hardware and software technology continues to advance, the "other side" continues to search for and discover new vulnerabilities. For this reason, most software manufacturers continue to produce patches for their products as vulnerabilities are discovered.

Self-Imposed Vulnerabilities

All networks contain a combination of public and private data. A properly implemented security scheme protects all of the data on the network yet allows some data to be accessed from outside entities, usually without the ability to change that data. One example of this may be the corporate website. Other data, such as payroll information, should not be made available to the public and should be restricted to only specific users within the organization. Network security, properly implemented, secures the corporate data, reduces the effectiveness of hacking attempts, and ensures that systems are used for their intended purposes. Networks designed to be freely available to the public need to be secured to ensure accuracy of the information and availability to the public if the network is to be useful. Additionally, properly securing a network ensures that the network is not used as an attack point against other networks.

Security attacks can become effective and damage networks for the following three main reasons:

- Lack of effective policy
- Configuration weakness
- Technology weakness

Lack of Effective Policy

Because a network security policy directs the administrators regarding how communications should be enabled and implemented, this is the basis for all security efforts. Security policies have weaknesses for a number of reasons, including the following:

- **Politics**—Politics within an organization can cause a lack of consistency within the policies or, worse, a lack of uniformly applying the policies. Many policies make so many exceptions for management and business owners that the policies become meaningless.
- **Lack of a written policy**—The lack of a written policy is essentially the same as not having any policy. Publishing and widely distributing the security policy prevents confusion about it within the organization.
- **Lack of continuity**—When personnel change too frequently, there is often a loosening in the care people take to ensure that policies are enforced. When a system administrator leaves a position, for example, all the passwords used by that administrator should be changed. In an organization that changes administrators several times each year, there is a natural reluctance to change the passwords because users knows they will be changed again very shortly due to administrator turnover.
- **Lack of disaster recovery planning**—A good disaster recovery plan must include contingencies for security breaches. The resulting confusion after a disaster can prevent forensic efforts from being successful because administrators are not careful in their recovery efforts.
- **Lack of patch management within the security policy**—A good security policy allows for frequent hardware and software upgrades. A detailed procedure for implementing new hardware and software ensures that security does not become forgotten while implementing new equipment.
- **Lack of monitoring**—Failure to monitor logs and intrusion detection systems appropriately exposes many organizations to attack without any knowledge that those attacks are occurring.
- **Lack of proper access controls**—Unauthorized network access is made easier when poorly designed access controls are implemented on the network. Improper password length, infrequent password changes, passwords written on notes attached to monitors, and freely shared passwords are items that have the potential to lead to security breaches.

Configuration Weakness

As network devices become increasingly complex, the knowledge base required to configure systems correctly grows. This can be more of an issue in smaller organizations where a single administrator is responsible for the LAN, WAN, servers, and workstations. Configuration weaknesses can be classified into one of the following:

- **Misconfigured equipment**—A simple misconfiguration can cause severe security issues. Whether the error is caused through lack of knowledge or is just a typo, the consequences can still lead to an insecure network. Some areas that are susceptible to this are access lists, SNMP settings, and routing protocols.
- **Weak or exposed passwords**—Passwords that are too short, are easily guessed, or consist of common words make it easy for an intruder to gain access to resources. A "strong" password should consist of at least eight characters and should include upper- and lowercase, numbers, and special characters. Additionally, using the default password on administrator accounts is an especially poor practice. It is also important that users don't create a password that is too complex to remember. In such a scenario, the user will tend to write down the password, defeating the purpose for the password in the first place. One common method for creating and remembering passwords is the "vanity plate" method: Think of a word or phrase and convert it into the characters used on a vanity license plate, then change the case of a letter or two, and substitute one or more numbers for letters. Here is an example: In Virginia, for instance, a Honda owner is apparently not fond of mayonnaise. The Honda owner's license plate reads IH8 Mayo. You can drop in an underscore and an exclamation point and you get IH8_Mayo!. Not too fancy and very easy to remember.
- **Misconfigured Internet services**—Java applets, Java script, FTP security settings, and IP can all be configured in ways that are considered unsafe. Knowing exactly what services are required and what services are running ensures that Internet services do not create potential security breaches.
- **Using default settings**—The default settings on a great number of products were designed for assisting in the configuration of a device and placing it in a production environment. For example, the default filters for the Cisco 3000 Series VPN concentrators are insufficient protection for use in a production network. By default, there are no access lists limiting telnet access on routers; if telnet is enabled, you must ensure the access is limited to only authorized IP addresses (from your management network). These are just two examples of how the default settings are insufficient for production use.

Technology Weakness

All technologies have intrinsic weaknesses. These weaknesses can reside in the operating system, within the protocol, or within networking equipment. Each of these items is discussed further in the following sections:

- **Operating system weakness**—This was discussed earlier in this chapter under the heading "Vulnerabilities." Operating systems are simple, coded instructions written for the computer. If an intruder is able to inject additional instructions into the system by exploiting a vulnerability within the operating system, he or she may be able to affect how that system functions. It is extremely important to keep operating systems patched to reduce system vulnerabilities.
- **Protocol weakness**—Some protocols suites, such as TCP/IP, were designed without an emphasis on security aspects. Some of the security weaknesses of protocols are detailed in the following list:
  - Network File System (NFS) is used by Novell and UNIX servers. There are no provisions for authentication or encryption. Additionally, because NFS uses a random selection of ports, it can be difficult for an administrator to limit access.
  - The TCP/IP suite consists of ICMP, UDP, and TCP and has several inherent weaknesses. For example, the header and footer on an IP packet can be intercepted and modified without leaving evidence of the change. ICMP packets are routinely used in DoS attacks, as discussed later in this chapter.
  - AppleTalk is used by older Macintosh systems. Using this protocol raises a number of issues regarding security. Lack of encryption, a random port selection, and lack of authentication raise security concerns when using this protocol. MacOS now fully supports the TCP/IP suite and is not commonly used.
- **Application weaknesses**—Many applications are written without regard to security. The primary objective when developing applications is functionality. Service packs, upgrades, and patches are normally released by the application developer as vulnerabilities are identified. As technology continues to develop, however, security is becoming a greater priority and is now being written into newly created applications as they are designed.
- **Network equipment weakness**—Although all manufacturers strive to produce the best product possible, any system of sufficient complexity is prone to configuration errors or system design vulnerabilities. Additionally, all systems have their particular strengths and weaknesses. One product may be very efficient and secure when it processes a specific protocol or traffic for a specific application, for example, but may be weak or not support a different protocol or application. It is very important to focus on exactly what type of network traffic you need to support and ensure that you implement the correct device in the correct location on the network. Additionally, you should always test your systems to ensure that they perform their functions as expected. An administrator who knows the strengths and weaknesses of his equipment can overcome these shortcomings through the proper deployment and configuration of equipment.

Threats

Potential threats are divided into the following two categories, but their motivations fall into much larger categories, detailed in the section "Intruder Motivation," which follows:

- **Structured threats**—A structured threat is an organized effort to breach a specific target. This can be the most dangerous threat because of its organized nature. This is a preplanned attack by a person or group that is seeking a specific target.
- **Unstructured threat**—Unstructured threats are by far the most common. These are usually a result of scanning of the Internet by persons seeking targets of opportunity. Many different types of scanning files or "scripts" are available for download on the Internet and can be used to scan a host or network for vulnerabilities.

Intruder Motivation

Several motivations prompt someone to intrude on another's network. Although no text can list all the reasons that someone would choose to steal or corrupt data, some common themes become evident when looking at the motivations of previous intruders. To refine the discussion of intruder motivations, it is first necessary to define some terms. In the context of this chapter, the word *intruder* can be defined as someone who attempts to gain access to a network or computer system without authorization. Intruders can be further classified as *crackers*, *hackers*, or *script kiddies*:

- **Cracker**—Someone who uses an advanced knowledge of networking and the Internet to compromise network security without proper authorization. Crackers are usually thought of as having a malicious intent.
- **Hacker**—Someone who investigates the integrity or security of a network or operating system. Usually relying on advanced programming techniques, the hacker's motivations are not always malicious. The ethical hacker is a term used for security consultants; the hacker may be hired by a company to test an organization's current defenses and expose weaknesses.
- **Script kiddie**—This is a commonly used slang term for a novice hacker who relies heavily on publicly available scripts to test the security of a network and scan for vulnerabilities.

The reasons that someone attempts to access, alter, or disrupt a network are as different as the intruders themselves. Some of the most common motivations are discussed in the following sections.

Lack of Understanding of Computers or Networks

Sometimes a user initiates a security breach through a lack of understanding. For example, an uneducated user with administrative rights on a Windows NT system can easily remove or change critical settings, resulting in an unusable system. Having too much trust combined with a lack of understanding can be equally dangerous. It is not uncommon for an administrator to open up their

whole network to someone when access to a single machine is all that is required. A poorly trained administrator of a firewall can easily open connectivity to the point that the firewall becomes ineffective. Another possibility is that a temporary firewall opening becomes a permanent opening because there are no procedures in place to ensure that temporary openings are closed after the need for them has been removed. Although a good security policy can help prevent these examples, some security breaches occur without any malicious intent.

Intruding for Curiosity

Sometimes people are just curious regarding the data contained in a system or network. One incident typical of this type is a 14-year-old boy who broke into a credit card company's system to look around. When asked the reason for breaking into the system, he replied that simple curiosity was the motivation. Sometimes an employee, for example, may attempt to break into a payroll system just to see whether he or she is receiving pay in accordance with coworkers. Alternatively, an employee may be curious regarding the financial status of the company or wondering whether there is anything interesting within the personnel record. Despite the focus of the curiosity, the common theme among those intruding out of curiosity is that there is usually little or no damage to the data.

Intruding for Fun and Pride

Some intruders enjoy the challenge of being able to bypass security measures. Many times, the more sophisticated the security measures, the greater the challenge. Whether these intruders are hackers, crackers, or script kiddies, their motivation is fun, pride, or a combination of the two. When George Leigh Mallory was asked why he wanted to climb Mount Everest, his reply was, "Because it is there." This seems to be the motivation for a number of intruders. There are several bulletin boards and discussion groups where members list their latest conquests and the challenges posed to breaking into the systems. The members of these groups applaud successful attempts and provide guidance to those who are unsuccessful. These are good places for a security administrator to monitor for information on the latest techniques used for breaking into systems.

Intruding for Revenge

Revenge can be powerful motivation. Disgruntled or former employees who have a good understanding of the network and know what assets they want to target can cause substantial problems for an organization. It is always advisable to change passwords and disable accounts whenever key personnel leave the company and ensure that you monitor the network for attacks that target specific assets.

Intruding for Profit

Profit is another powerful motivator for breaking into systems. Credit card information, unauthorized bank transfers, and manipulation of billing information can be extremely profitable if successful. However, not all intrusions for profit are based on money. In November 2002, a prominent news

agency was accused of breaking into a Swedish company's computer system to steal data related to financial performance. The news agency was accused of obtaining this information to release it before the official announcement, thereby beating all the other news agencies to the story. At the time of this writing, there has been no determination whether this accusation has any merit. This example shows how profit may not always be directly related to transferring funds or obtaining credit card information. Of course, the theft of corporate secrets could provide a competitor with a significant advantage in the marketplace.

Intruding for Political Purposes

The fact that economies depend largely upon electronic transactions makes those economies vulnerable to disruptions by an attacker. Cyber-warfare does exist and can pose a real threat to any economy. If disruption of an economy is desired, doing so through electronic means may become the chosen method due to a number of factors. Among these factors are the ability to launch an attack from virtually any location, low equipment cost, low cost of connectivity, and a lack of sufficient protection. In November 2002, a number of the primary DNS servers on the Internet were attacked through a distributed denial-of-service (DDoS) attack and were rendered inoperable for a number of hours. Although we cannot guess the motivation for this attack, a more sophisticated version could dramatically affect Internet traffic and disrupt many organizations that communicate via the Internet. Another more common political motivation is known as *hactivism*, which is the act of targeting an organization and defacing their websites for political purposes.

Types of Attacks

Before discussing the characteristics of specific attacks, it's necessary to categorize the different types of attacks. Attacks are defined by the goal of the attack rather than the motivation of the attacker. There are three major types of network attacks, each with its own specific goal:

- **Reconnaissance attacks**—An attack designed not to inflict immediate damage to a system or network but only to map out the network to discover which address ranges are used, which systems are running, and which services are on those systems. One must "access" a system or network to some degree to perform reconnaissance, but normally one does not cause any damage at that time.
- **Access attacks**—An attack designed to exploit a vulnerability and to gain access to a system on a network. Once access is gained, the user can do the following:
  - Retrieve, alter, or destroy data
  - Add, remove, or change network resources, including user access
  - Install other exploits that can be used at a later date to gain access to the network
- **DoS attacks**—A DoS attack is designed solely to cause an interruption to a computer or network.

Reconnaissance Attacks

The term *reconnaissance* attack is misleading. The goal of this type of attack is actually to perform reconnaissance of a computer or network, and the goal of the reconnaissance is to determine the makeup of the targeted computer or network and to search for and map any vulnerabilities. A reconnaissance attack can be an indicator of the potential for other more invasive attacks. Many reconnaissance attacks have been written into scripts that enable novice hackers or script kiddies to launch attacks on networks with a few mouse clicks. The following list identifies the more common reconnaissance attacks:

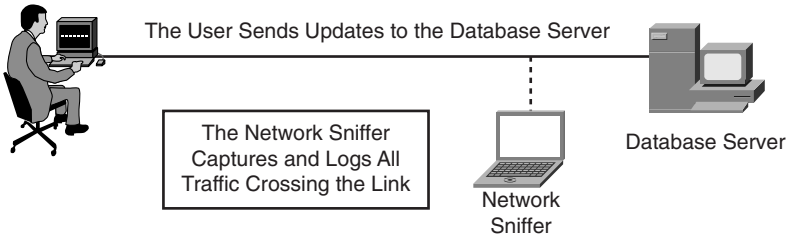
- **DNS whois queries**—A whois query of the DNS provides the unauthorized user with such information as what address space is assigned to a particular domain and who owns that domain.
- **Ping sweep**—The output from a ping sweep can tell the unauthorized user the number of hosts that are active on the network.
- **Vertical scans**—Vertical scans scan the service ports of a single host and request different services at each port. This method enables the unauthorized user to determine which type of operating system is running and what services are running on the computer.
- **Horizontal scans**—Horizontal scans scan an address range for a specific port or service. A very common horizontal scan is the FTP sweep. This is scanning a network segment looking for replies to connection attempts on port 21.
- **Block scan**—A block scan is a combination of the vertical and horizontal scans. In other words, it scans a network segment and attempts connections on multiple ports of each host on that segment.

Access Attacks

As the name implies, the goal of an access attack is to gain access to a computer or a network. Having gained access, the user can perform many different functions. These functions can be broken into three distinct categories:

- **Interception**—If the unauthorized user is able to capture traffic going from the source to the destination, that user can store that data for later use. The data could be anything that is crossing the network segment that is connected to the sniffer and could include confidential data such as personnel records, payroll, or research and development projects. If network management data is crossing the network, it is possible to acquire passwords for specific components and take control of that equipment. The methods used for intercepting traffic vary but usually require physical connectivity with the network. Upgrading from hub to switching technology greatly reduces the amount of traffic that can be captured by a network sniffer. The most effective way to protect your sensitive data is to save it in an encrypted format or to send it via an encrypted connection. This prevents the intruder from being able to read the data. Figure 2-1 depicts how interception may occur.

Figure 2-1 *Interceptions Can Occur if Data Is Sent in an Unencrypted Format*



- **Modification**—Having access, the unauthorized user can now alter the resource. This not only includes altering file content, it also includes system configurations, unauthorized system access, and unauthorized privilege escalation. Unauthorized system access is completed by exploiting a vulnerability in either the operating system or another software package running on that system. *Unauthorized privilege escalation* refers to a user with a low level but authorized account attempting to gain higher-level or more privileged user account information to increase the unauthorized user's privilege level. This enables the intruder to have greater control of the target system or network.
- **Fabrication**—With access to the target system or network, the unauthorized user can create false objects and introduce them into the environment. This could include altering data or inserting packaged exploits such as a virus, a worm, or a Trojan horse that can continue to attack the network from within.
  - **Virus**—Computer viruses range from annoying to destructive. They consist of computer code that attaches itself to other software running on the computer. This way, each time the attached software opens the virus reproduces and can continue to grow until it wreaks havoc on the infected computer.
  - **Worm**—A worm is a virus that exploits vulnerabilities on networked systems to replicate itself. A worm scans a network looking for a computer with a specific vulnerability. When it finds a host, it copies itself to that system and begins scanning from there as well.
  - **Trojan horse**—A Trojan horse is a program that usually claims to perform one function (such as a game) but does something completely different (such as corrupting data on your hard disk). Many different types of Trojan horses get attached to systems, and the effects of these programs range from a minor irritation for the user to total destruction of the computer file system. Trojan horses are sometimes used to exploit systems by creating user accounts on systems that enable unauthorized users to gain access or upgrade their privilege level. Some Trojan horses capture data from the host system and send it back to a location where it can be accessed by the attacker. Others enable the attacker to take control of the system and enlist it in a DDoS attack; this is a very common use of the Trojan horse.

DoS Attacks

A DoS attack is designed to deny user access to computers or networks. These attacks usually target specific services and attempt to overwhelm them by making numerous requests concurrently. If a system is not protected and cannot react to a DoS attack, it can be very easy to overwhelm that system by running scripts that generate multiple requests. It is possible to greatly increase the magnitude of a DoS attack by launching the attack from multiple systems against a single target. This practice is referred to as a *distributed denial-of-service* (DDoS) attack. The use of Trojan horses in a DDoS was discussed in the previous section.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your SECUR exam, a well-prepared candidate should at a minimum know all the details in each "Foundation Summary" before going to take the exam.

Vulnerabilities

A vulnerability is anything that can be exploited to gain access to or gain control of a host or network.

Self-Imposed Vulnerabilities

An organization can create its own vulnerabilities by not ensuring that the following issues are resolved through process or procedure:

- The lack of a effective and consistent security policy due to any of the following conditions:
  - **Politics**—Politics within an organization can cause a lack of consistency within the policies or a lack of uniform application of policies.
  - **Lack of a written policy**—The lack of a written policy is essentially the same as not having any policy.
  - **Lack of continuity**—When personnel change too frequently, there is often a loosening in the care people take to ensure that policies are enforced.
  - **Lack of disaster recovery planning**—The resultant confusion after a disaster often results in virtually all security efforts being dropped if the administrators are not careful in their recovery efforts.
  - **Lack of upgrade plans within the security policy**—A detailed procedure for implementing new hardware and software ensures that security does not become forgotten while implementing new equipment.
  - **Lack of monitoring**—Failure to monitor logs and intrusion detection systems appropriately exposes many organizations to constant attack without any knowledge that those attacks are occurring.
  - **Lack of proper access controls**—Improper password length, infrequent password changes, passwords written on notes attached to monitors, and freely shared passwords are all items that can lead to security breaches.

- Configuration weakness within a organization can result in significant vulnerability exposure.
  - **Misconfigured equipment**—A simple misconfiguration can cause severe security issues.
  - **Insufficient passwords**—Passwords that are too short, are easily guessed, or consist of common words, especially when transmitted over the Internet, are cause for concern.
  - **Misconfigured Internet services**—Knowing exactly which services are required and which services are running ensures that Internet services do not create potential security breaches.
  - **Using default settings**—The default settings on a great number of products are designed to assist in their configuration and are placed in a production environment.
- All technologies have intrinsic weaknesses. These weaknesses can reside in the operating system, within the protocol, or within networking equipment.
  - All operating systems have weaknesses. You must take proper measures to make these systems as secure as possible.
  - Certain protocols can be exploited because of the way they were written and the functionality that was written into the protocol.
- Although all manufacturers strive to make the best product possible, any system of sufficient complexity is prone to human and mechanical errors. Additionally, all systems have their particular strengths and weaknesses. Knowing the nuances of your particular equipment is the best way of overcoming technology weaknesses.

Threats

There are two different types of threats to computer networks:

- Structured threats are an organized effort to attack a specific target.
- Unstructured threats are not organized and do not target a specific host, network, or organization.

Intruder Motivation

- There are three different names for potential intruders, categorized by their skill level and intent:
  - **Cracker**—More advanced and usually part of a structured threat
  - **Hacker**—Can be involved in both structured and unstructured threats.
  - **Script kiddie**—Novice hacker using script files that perform most of the scanning and hacking functions

- The motivations for intruders vary but generally fit into one of the following categories:
  - Intruding through lack of knowledge
  - Intruding for curiosity
  - Intruding for fun and pride
  - Intruding for revenge
  - Intruding for profit
  - Intruding for political purposes

Types of Attacks

There are three major types of network attacks, each with its own specific goal:

- **Reconnaissance attacks**—An attack designed to gather information about a system or a network. The goal is to map the network, identify the systems and services, and to identify vulnerabilities that can be exploited at a later time.
- **Access attacks**—An attack designed to exploit a vulnerability and to gain access to a system on a network. After access has been gained, the user can do the following:
  - Retrieve, alter, or destroy data
  - Add, remove, or change network resources, including user access
  - Install other exploits that can be used at a later date to gain access to the network
- **DoS attacks**—A DoS attack is designed solely to cause an interruption to a computer or network.

Q&A

As mentioned in the section, "How to Use This Book," in the Introduction to this book, you have two choices for review questions. The questions that follow next give you a bigger challenge than the exam itself by using an open-ended question format. By reviewing now with this more difficult question format, you can exercise your memory better and prove your conceptual and factual knowledge of this chapter. The answers to these questions are found in the appendix.

For more practice with exam-like question formats, including questions using a router simulator and multiple choice questions, use the exam engine on the CD-ROM.

1. An application that is supposed to monitor your network and alert you in the event of an outage is being considered by your manager. You begin testing the product and discover that it requires a management connection to every network component (each requiring a password) but maintains these nonencrypted (clear-text) connections. This would require that the system send clear-text passwords to every network component that you want to manage. Would you consider this product for you network and why?
2. How many TCP ports can a system communicate over if no ports are blocked and a service is listening on every available port?
3. What are three "self-imposed vulnerabilities"?
4. Can a system misconfiguration be a security vulnerability?
5. Why would you not want to install security devices using the default settings?
6. How does NFS make network connections and why can it be difficult to secure?
7. Why is it difficult to determine whether IP traffic is spoofed?
8. What is a structured threat?
9. Which type of threat is more common: structured or unstructured?
10. Why should your security administrator be well trained and very familiar with the product that she is using?
11. What is the goal of a reconnaissance attack?
12. What is a "vertical scan"?
13. What is a "worm"?
14. What is a DDoS attack?