Introduction to Network Security Threats

Terms you'll need to understand:

- ✓ Denial of service (DoS)
- ✓ Distributed denial of service (DDoS)
- ✓ Reconnaissance attacks
- ✓ Access attacks
- ✓ Internal threats
- ✓ External threats
- ✓ Unstructured threats
- ✓ Structured threats
- ✓ Cisco Secure Access Control Server (CSACS)
- ✓ Cisco Secure Scanner

Techniques you'll need to master:

- ✓ Security policy
- ✓ Types of attacks
- ✓ Cisco security wheel

Introduction to security involves discussing the types of threats we face in our secure environments. Policies and processes help us protect our secure environments from threats in this ever-changing world of security. This chapter introduces a basic understanding of the types of threats we face and the policies and processes necessary for maintaining secure environments.

Network Security Threats

Data communications networks have served the academic, corporate, and government sectors for many years; however, the concept of security within these networks has only recently become a high priority. As data becomes readily available by connecting networks to public media or even other internal networks, the vulnerability of data to attacks and threats becomes apparent. Several distinct types of threats have emerged, and the network security community has developed new ways to protect us from these threats.

Types of Security Threats

Several types of threats exist in secure environments, but most of them can be classified into the following four main categories:

- Internal threats
- External threats
- Unstructured threats
- Structured threats

Internal Threats

Internal threats are more widespread than most people realize. These threats typically come from users who have legitimate access to the computers or networks they want to harm. Disgruntled or former employees whose privileged access has not been promptly terminated can cause a considerable amount of damage to a system. Lastly, these internal threats can be some of the most difficult to monitor and defend against.

Results of surveys conducted by the Computer Security Institute (CSI) revealed that 70% of organizations polled admitted to security breaches, 60% of which came from within the organizations themselves (internal threats).

External Threats

External threats originate from individuals who are operating outside an organization's network. The individuals typically do not have authorized access to the network but use remote access channels such as dial-up or Internet connections to attempt security breaches. This threat is difficult to protect against and is always present when external access is provided by the company. If no Internet access or dial-up capabilities exist, you are safe from true external threats.

Unstructured Threats

Unstructured threats are caused by individuals commonly known as *script kiddies* who use prebuilt tools, programs, or scripts readily available on the Internet to launch their attacks. Script kiddies can be compared to kids joy riding in a car; their actions are motivated more by excitement than by any calculated thought or knowledge. If their tools fail to give them access to the networks they desire, they typically move on to another target, rapidly losing interest. Script kiddies might seem harmless, but the damage they can cause makes them potentially very dangerous. In most cases, unstructured threats are performed by individuals lacking an understanding of how their actions can impact themselves or the target network.

Structured Threats

By contrast, *structured* threats are performed by individuals who are fully aware of what they intend to do and who use programs and tools to attack networks or computers. The attackers have the ability to modify their tools as required and the skills to develop their own new methods of attack against unknown vendor vulnerabilities. Structured attackers can be driven by certain goals, including credit card number theft, software code theft, or intentional damage to a competitor's Web site and internal networks. In addition to their tools, these attackers also have the patience needed to penetrate the networks, using meticulously self-created programs or even social engineering tactics. Competitors, law enforcement, or other agencies might hire the services of structured attackers to acquire information, test security, or cause damage to specific networks.

Social engineering is a means of collecting information from people by fooling them; it's also known as *people hacking*. A typical example of this is calling or sending an email message to a corporate user, posing as a manager or an administrator, to extract information such as a user's password.

Three Types of Attacks

There are several types of attacks on networks. Some aim to gain information or access to restricted locations, whereas others focus on bringing down computers. These attacks are categorized into three main types:

- Reconnaissance attacks
- Access attacks
- Denial-of-service attacks

Reconnaissance Attacks

A *reconnaissance* attack is a form of information gathering from a network or computer system. Hackers might start mapping out a network using tools such as ping sweepers to locate active computers. Additional information, such as operating systems in use and available open ports, can be acquired through port scanners and Simple Network Management Protocol (SNMP). Reconnaissance attacks usually occur prior to a denial-of-service (DoS) or access attack.

Access Attacks

The *access* attacks involve collecting or obtaining access to data or networks that usually are not available to the individual. These attacks can come in several forms, including unauthorized data retrieval, unauthorized system access, and unauthorized privilege escalation. This form of attack can be accomplished in several ways; however, two common hacking tools used to gain access are password hacking programs and Trojan horses. The types of access attacks are described in the following list:

- *Unauthorized data retrieval*—The process of reading, writing, and possibly deleting normally inaccessible information
- *Unauthorized system access*—The process of gaining access to a system by exploiting a weakness in the operating system
- *Unauthorized privilege escalation*—The process in which a low-level user tries to gain a higher level of access such as administrator-level privileges

A *Trojan horse* is an impostor that hides inside an email message or another program. When the email is opened or the program launched, the Trojan horse is released, causing unlimited possible problems. This type of attacking mechanism (which Cisco might reference as a *virus*, on the exam) can delete files, steal passwords, give access to remote systems, or even download more Trojan horses and viruses.

Denial-of-Service Attacks

Hackers use *denial-of-service (DoS)* attacks when trying to disable, slow down, or corrupt a network, thus denying service to the network's intended users. Even though the hacker might not actually have a valid user account on the network computers, if network access is achieved, the hacker can launch an attack. This attack typically floods the targeted computer or network with traffic with the intention to disable it.

Distributed DoS (DDoS) attacks combine the power of multiple attacking computers, which focus their attacks on a single receiving computer or network. Because DDoS attacks can come from so many computers in different geographical areas, administrators have extreme difficulty repelling such attacks. For example, if a single computer pings a Web server, little stress is placed on the server. However, if 10,000 computers are pinging a Web server all at the same time, the server can be so busy responding to the ping requests that users accessing a Web page time out and never receive the page. These types of attacks are some of the most feared by network administrators because blocking all the attacking computers without blocking legitimate users is very difficult.

Denial-of-service and distributed DoS attacks send large amounts of useless traffic into a network to disable or cripple a server or network.

The Secure Network

Obtaining a secure network is not a destination, but a never-ending quest to provide the best protection while the environment is constantly changing. A secure system today could be a very insecure system tomorrow, as hackers discover new vulnerabilities and security holes. Security policies and processes help set rules and guidelines to assist in acquiring and maintaining the most secure network environment possible.

The Security Policy

The security policy is the core document or set of procedures used to describe how an organization's information, data, and services will be protected. The policy supports the organization's primary security objectives, as defined by who will be allowed access, who will be denied access, and what explicitly the policy aims to protect. Lastly, this document should define roles, responsibilities, and managed expectations and provide guidelines in the event of a security breach or noncompliance.

RFC 2196, "Site Security Handbook," states, "A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."

The Security Process

Security requires an ongoing process of evaluation and adaptation. What works today might not be secure enough tomorrow. Cisco has created the security wheel to represent graphically the continuously evolving process of security. This process entails securing, monitoring, testing, and improving the security policy and technical changes necessary to protect the environment. Figure 2.1 shows the Cisco security wheel.

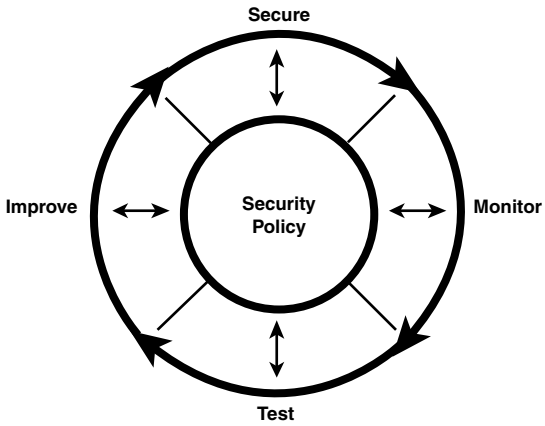

Figure 2.1 The Cisco security wheel.

The Cisco Security Wheel contains four basic steps to help visually display the process needed to maintain a secure environment. These steps are listed here:

1. Securing the environment
2. Monitoring the environment for violations and attacks
3. Testing the security of the environment
4. Improving the security policy

Step 1: Securing the Environment

Securing the environment involves the implementation of various tools addressing different points of vulnerability. Authentication systems, such as One-Time-Passwords (OTP) support and Cisco Secure Access Control Server (CSACS), aid protection by allowing only authenticated users into the environment. Encryption techniques can be used to disguise data traveling across insecure media; virtual private network (VPN) tunnels encrypted using Internet Protocol Security (IPSec) are a good example of this. Implementing firewalls, which filter incoming and outgoing traffic, can provide another layer of protection between a corporate inside network and outside intruders. Systems with known security holes should be kept up-to-date through the use of vulnerability patching. Physical security, which is often overlooked, involves keeping equipment secure behind locked doors. For example, if an intruder can physically access Cisco equipment, he can employ password-breaking procedures and have his way with your systems.

Step 2: Monitoring the Environment for Violations and Attacks

Monitoring for violations plays a critical role in determining how effective the secured environment is in supporting the security policy requirements. Using intrusion detection systems, such as Cisco Secure Intrusion Detection Systems (CSIDS), can provide an excellent solution for monitoring and blocking unwanted traffic. In addition, logging information such as user access and modifications to system settings can be recorded. Because the recording of log files can accumulate large amounts of raw data, you should store this data in a separate location, such as the Syslog server.

Step 3: Testing the Security of the Environment

After establishing your secure environment and security monitors, testing your environment is the only way you can ensure that your security measures are upholding your policy. Also, testing helps find new security holes in the environment before hackers find them. Cisco Secure Scanner is a tool you can use to test and identify such security holes.

Step 4: Improving the Security Policy

Improving the security policy within a varying and highly unpredictable external environment is an ongoing job. Continuously monitoring, testing, and identifying flaws and attacks against the network are imperative in refining and tuning the security policy. Vulnerability reports enable administrators to maintain an awareness of new potential attacks and should be considered during this step.

This chapter introduced the types of security threats that can be present against your networks. The security policy can be used to help you document what in your company needs protecting and how you will go about protecting that data. Cisco's security wheel demonstrates the ever-evolving enhancements you need to make to your security policy to keep you on the leading edge of protection and monitoring.