Romel Cabiling

Home

Home > My courses > Network Defense and Remote Access Configuration > 01 [Enter Module Title Here] > Lesson Proper for Week 1

# Lesson Proper for Week 1

NETWORK SECURITY FUNDAMENTALS

**Examining Network Security Fundamentals**

A variety of attackers might attempt network intrusions, causing loss of data, loss of privacy, and other consequences. You learn about these attackers in the following sections. These types of threats are becoming a concern for a growing number of corporate managers. More businesses are actively addressing information security, but many others have not taken steps to secure their systems from attack.

**Threats to Network Security**

When planning network security measures, knowing the types of attackers who might try to break into your network is important. This knowledge can help you anticipate threats and set up detection systems, firewalls, and other countermeasures to block attacks as effectively as possible. Similarly, understanding the motivation of attackers helps you prepare security controls:

- Status—Some attackers attempt to take over computer systems just for the thrill of it. They like to count the number of systems they have accessed as notches on their belt.
- Revenge—Disgruntled current or former employees might want to retaliate against an organization for policies or actions they consider wrong. They can sometimes gain entry through an undocumented account (back door) in the system.
- Financial gain—Other attackers have financial profit as their goal. Attackers who break into a network can gain access to financial accounts. They can steal individual or corporate credit card numbers and make unauthorized purchases. Just as often, attackers defraud people out of money with scams carried out via e-mail or other means.
- Industrial espionage—Proprietary information is often valuable enough that it can be sold to competing companies or other parties.

**Hackers**

A hacker is anyone who attempts to gain access to unauthorized resources on a network, usually by finding a way to circumvent passwords, firewalls, or other protective measures. Hackers seek to break into computers for different reasons:

- "Old school" hackers consider themselves seekers of knowledge; they operate on the theory that knowledge is power, regardless of how they come by that knowledge. They are not out to destroy or harm; they want to discover how things work and open any sources of knowledge they can find. They believe the Internet was intended to be an open environment, and that anything online can and should be available to anyone.
- Other less "ethical" crackers pursue destructive aims, such as the proliferation of viruses and worms, much like vandals.
- Some bored young people who are highly adept with computers try to gain control of as many systems as possible for the thrill of it. They enjoy disrupting systems and keeping them from working, and they tend to boast about their exploits online.
- Criminals and industrial spies might be interested in selling information to the top bidder or using it to influence potential victims. Some companies would certainly be interested in getting the plans for a new product from their competitors.
- The term script kiddie is often used to describe relatively unskilled programmers who spread viruses and other malicious scripts to exploit weaknesses in computer systems. Script kiddies lack the ability to create viruses or Trojan programs on their own, but they can usually find these programs online.
- Packet monkeys are primarily interested in blocking Web site activities through a distributed denial of service (DDoS) attack. In a DDoS attack, many computers are hijacked and used to flood the target with so many false requests that the server cannot process them all, and normal traffic is blocked. Packet monkeys might also want to deface Web sites by leaving messages that their friends can read.
- Hacktivists are computer attackers with political goals. Frequently they use denial of service attacks to shut down Web sites of organizations with whom they disagree. One of the best-known hacktivist groups, named Anonymous, has successfully shut down sites of the U.S. Federal Trade Commission to express its opposition to proposed laws that combat digital piracy. Anonymous has also shut down sites that belong to the State of Alabama in protest of immigration laws. After discovering that the Central Intelligence Agency (CIA) was investigating the group, Anonymous shut down some of the CIA's sites as well.

**Disgruntled Employees**

Disgruntled employees are usually unhappy over perceived injustices and want to exact revenge by stealing information. With the economic downturn, more current or former employees are stealing information for financial reasons. Often they give confidential information to new employers. When an employee is terminated, security measures should be taken immediately to ensure that the employee can no longer access the company network and telecommunications systems.

While most attacks come from outside a company, according to Cyber Security Watch, insider attacks are more costly to a victimized company and are becoming increasingly more sophisticated. Theft, data loss, and network damage can result from the malicious actions of current or former employees. The following are just a few examples:

- A logic bomb is malware designed to start at a specific time in the future or when a specified condition exists. At Fannie Mae, the Federal National Mortgage Association, a former engineer planted a logic bomb that could have shut the company down and cost millions by destroying all 4000 of the company's servers. Fortunately, the attack did not succeed. The former employee was sentenced to three years in jail.

- Ansir Khan, a former bank employee in Sheffield, England, attempted to steal $1.9 million after successfully stealing more than $1.1 million from the bank in April 2005 and May 2006. He extracted customer data and shared it with accomplices. He was sentenced to three years in jail.

- A former employee of United Way in Miami, Luis Robert Altamirano, accessed the United Way computer system a year after he left the organization. He deleted files and disabled the voicemail system. Altamirano pled guilty and was sentenced to 18 months in jail and fined $50,000 for computer fraud.

- Adeniyi Adeyemi, a contract employee of Bank of New York Mellon, stole the personal information of dozens of bank employees, mainly in the IT department. He used the information to open dummy financial accounts and receive funds stolen from the accounts of charities and nonprofit organizations.

### Terrorists

Until September 11, 2001, most people did not consider a terrorist attack on an information infrastructure (known as cyberterrorism) to be a likely threat. Since then, the threat posed by terrorists has been taken more seriously. A terrorist group might want to attack computer systems for several reasons: to make a political statement or accomplish a political goal, such as the release of a jailed comrade; cause damage to critical systems; or disrupt the target's financial stability. Attacking the World Trade Center certainly accomplished the latter goal, given the nature and location of the structures. Terrorists might also want simply to cause panic.

It might be hard to understand why a terrorist attack on computers would be considered a serious threat until you think about how many critical systems are controlled by computers. Consider the chaos that could result from a successful attack on a computer system that controls a nuclear power plant's reactors. The overall psychological effect could be just as detrimental as the infrastructure damage and even the loss of life.

### Government Operations

The shady world of international espionage is difficult to document, but it is becoming clear that a number of countries see computer operations as more than simply a spying technique; computer networks are a potential battleground. In 2010, a sophisticated malware program called Stuxnet was discovered. The Stuxnet worm was designed to attack Windows systems used in industrial and military settings. The goal was to infect the control systems of automated industrial processes. Security experts who analyzed Stuxnet concluded that it was probably the work of a government operation because of the complexity of the program and the amount of time and resources required to create and propagate it. Because Stuxnet was unusually prevalent in Iran, many observers believe that the United States and/or Israel were responsible for its creation and that it was intended to target Iran's nuclear industry.

Another focus of attention is the Chinese government, which is thought to be responsible for successful computer-based attacks on U.S. Department of Defense information systems as well as government, industrial, and military systems in Germany, France, and Britain.

### Malicious Code

In 2004, the MyDoom worm infected millions of computers in only a few days, costing $38.5 billion in cleanup, lost productivity, and other losses. MyDoom was believed to have been the fastest-spreading worm ever created. MyDoom is primarily transmitted via e-mail, with subject lines such as “Error,” “Mail Delivery System,” or “Mail Transaction Failed.” If the user opens the attachment, the worm resends itself to e-mail addresses in the user’s address book and local files. The first variant, MyDoom.A, contained a back door on port 3127/tcp and a denial of service attack on the SCO Group Web site that was timed to launch on February 1, 2004. The second variant, MyDoom.B, targeted the Microsoft Web site. It blocked access to Microsoft and some online antivirus sites, thus denying access to antivirus updates and virus-removal tools.

In 2008, a worm known as Conficker was discovered. This program attacked all Windows operating systems from Windows 2000 through Windows 7. An estimated 9 to 15 million computers were infected. In 2009, Microsoft offered a $250,000 reward for the identification of Conficker’s authors. Conficker was designed to create botnets: networks of tens of thousands of infected computers that belong to unsuspecting victims and can be controlled from a central station. As of this writing, the authors of Conficker have not been identified, but because the program was designed not to infect systems with a Ukrainian keyboard, it is thought that the worm was developed in Eastern Europe.

Information security has improved since MyDoom and Conficker, but new vulnerabilities always lurk right around the corner, and security professionals must stay one step ahead of attackers. The following sections review the types of malware you might encounter.

### Viruses, Worms, and Trojan Programs

Although most users think of any type of virus, worm, or Trojan program as similar problems, they are completely different types of attacks. A virus is executable code that can replicate itself from one place to another surreptitiously and perform actions that range from benign to harmful. Viruses are spread by several methods, including running executable code, sharing disks or memory sticks, opening e-mail attachments, and viewing infected or malicious Web pages. Viruses can attach to other executables or replace them in order to spread or execute. Viruses require user intervention to run.

A worm creates files that copy themselves repeatedly and consume disk space. Worms do not require user intervention to be launched; they are self-propagating. Some worms can install back doors—a way of gaining unauthorized access to a computer or other resource, such as an unused port or terminal service, that makes it possible for attackers to gain control over the computer. A port is an area in random access memory (RAM) that is assigned a number (the port address) and is reserved for a program that runs in the background to listen for requests for the service it offers. Other worms can destroy data on a hard disk. Just like a cold or flu virus, computer viruses and worms can mutate or be altered to defeat antivirus software.

A Trojan program is also a harmful computer program, but one that appears to be something useful—a deception like the Trojan horse described in Greek legends. The difference between a virus and a Trojan program lies in how the malicious code is used. Viruses replicate and can potentially cause damage when they run on a user's computer. Trojan programs can also create a back door, which opens the system to additional attacks. The often hidden or obscure nature of a back door makes the attacker's activities difficult to detect.

Viruses, worms, and Trojan programs are a major security threat. They can damage files, enable attackers to control computers, and prevent applications from functioning correctly. When creating a network defense perimeter, you need to consider guarding against all three. Firewalls and intrusion-detection systems do not block malicious code on their own; you need to install anti-malware software or proxy servers that can be configured to filter out malicious code and delete it before it causes harm.

### Macro Viruses

A macro is a type of script that automates repetitive tasks in Microsoft Word or similar applications. When you run a macro, a series of actions are carried out automatically. Macros are a useful way to make some tasks perform more efficiently. Unfortunately, macro viruses perform the same functions as macros, but they tend to be harmful. For example, in March 1999, the Melissa macro virus caused Microsoft to shut down the company's entire e-mail service. Melissa spread rapidly and arrived as an attachment with the subject line "Important message from [name of someone]." The body text read, "Here is that document you asked for…don't show anyone else." If the recipient opened the attachment, the macro virus infected the computer and carried out a series of commands. Melissa was a fast-spreading virus, infecting more than 100,000 computers in the first few days. Macro viruses remain a threat today, but the good news is that the user must perform some action for the virus to be activated; therefore, educating users not to open the attachments is essential. Most modern operating systems and office suites do not automatically run macros, so the threat from macro viruses is reduced.

### Other Threats to Network Security

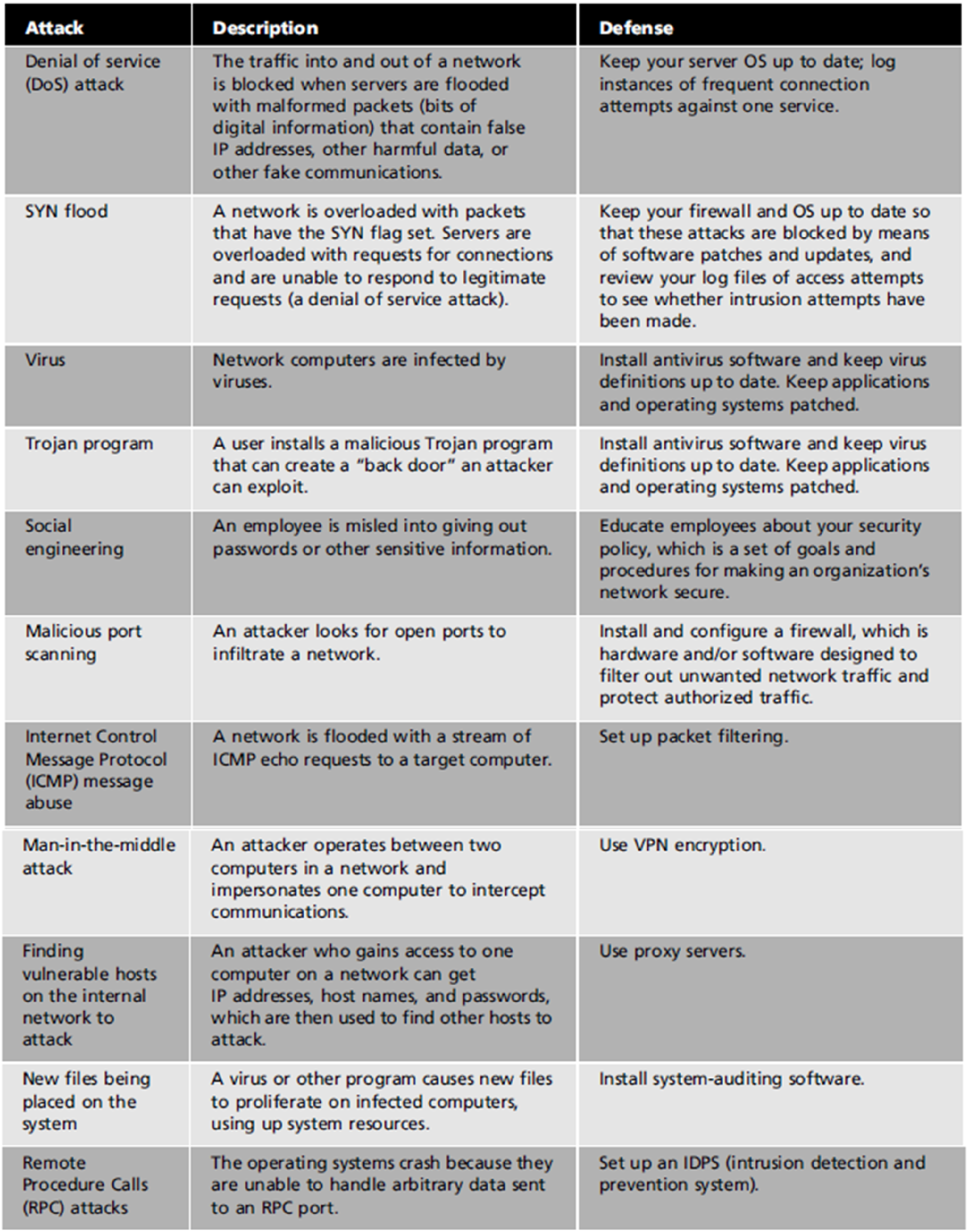
You cannot prepare for every possible risk to your systems. At best, you can maintain a secure environment for today's threats and have a comprehensive plan for integrating safeguards against tomorrow's threats into your defenses. The next threat might be infection by a new virus, exploitation of a recently discovered vulnerability, or an earthquake that destroys your facility. Many threats, such as natural disasters, cannot be mitigated entirely. Although you might have prepared for natural disasters by maintaining an alternate site complete with all necessary equipment, your primary site's network and equipment could still suffer devastating loss.

### Social Engineering: The People Factor

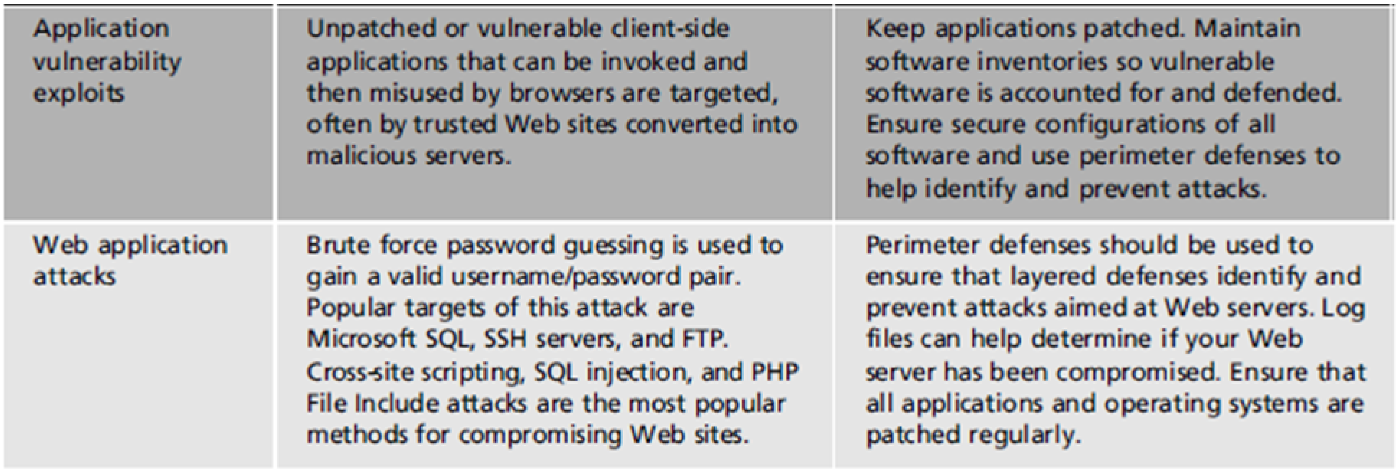
One common way that attackers gain access to an organization's resources cannot be prevented with hardware or software. The vulnerability in this case is well-meaning but gullible employees who attackers fool into giving out passwords or other access codes. To protect itself against personnel who do not observe accepted security practices or who willfully abuse them, an organization needs a strong and consistently enforced security policy and a rigorous training program. Security policies are discussed in Chapter 13.

### Common Attacks and Defenses

Table 1-1 describes some of the common attacks you need to guard against and the defensive strategies you can use to defeat them. These concepts are discussed in more depth throughout the remainder of the book.



| Attack | Description | Defense |
|---|---|---|
| Denial of service (DoS) attack | The traffic into and out of a network is blocked when servers are flooded with malformed packets (bits of digital information) that contain false IP addresses, other harmful data, or other fake communications. | Keep your server OS up to date; log instances of frequent connection attempts against one service. |
| SYN flood | A network is overloaded with packets that have the SYN flag set. Servers are overloaded with requests for connections and are unable to respond to legitimate requests (a denial of service attack). | Keep your firewall and OS up to date so that these attacks are blocked by means of software patches and updates, and review your log files of access attempts to see whether intrusion attempts have been made. |
| Virus | Network computers are infected by viruses. | Install antivirus software and keep virus definitions up to date. Keep applications and operating systems patched. |
| Trojan program | A user installs a malicious Trojan program that can create a “back door” an attacker can exploit. | Install antivirus software and keep virus definitions up to date. Keep applications and operating systems patched. |
| Social engineering | An employee is misled into giving out passwords or other sensitive information. | Educate employees about your security policy, which is a set of goals and procedures for making an organization’s network secure. |
| Malicious port scanning | An attacker looks for open ports to infiltrate a network. | Install and configure a firewall, which is hardware and/or software designed to filter out unwanted network traffic and protect authorized traffic. |
| Internet Control Message Protocol (ICMP) message abuse | A network is flooded with a stream of ICMP echo requests to a target computer. | Set up packet filtering. |
| Man-in-the-middle attack | An attacker operates between two computers in a network and impersonates one computer to intercept communications. | Use VPN encryption. |
| Finding vulnerable hosts on the internal network to attack | An attacker who gains access to one computer on a network can get IP addresses, host names, and passwords, which are then used to find other hosts to attack. | Use proxy servers. |
| New files being placed on the system | A virus or other program causes new files to proliferate on infected computers, using up system resources. | Install system-auditing software. |
| Remote Procedure Calls (RPC) attacks | The operating systems crash because they are unable to handle arbitrary data sent to an RPC port. | Set up an IDPS (intrusion detection and prevention system). |



| | | |
|---|---|---|
| Application vulnerability exploits | Unpatched or vulnerable client-side applications that can be invoked and then misused by browsers are targeted, often by trusted Web sites converted into malicious servers. | Keep applications patched. Maintain software inventories so vulnerable software is accounted for and defended. Ensure secure configurations of all software and use perimeter defenses to help identify and prevent attacks. |
| Web application attacks | Brute force password guessing is used to gain a valid username/password pair. Popular targets of this attack are Microsoft SQL, SSH servers, and FTP. Cross-site scripting, SQL injection, and PHP File Include attacks are the most popular methods for compromising Web sites. | Perimeter defenses should be used to ensure that layered defenses identify and prevent attacks aimed at Web servers. Log files can help determine if your Web server has been compromised. Ensure that all applications and operating systems are patched regularly. |

Table 1-1 Common attacks and defenses

### Internet Security Concerns

As you probably know from your study of basic networking concepts and TCP/IP, a port number combined with a computer's IP address constitutes a network connection called a socket. Attackers commonly use software to try to identify sockets that respond to connection requests. The sockets that respond can be targeted to see whether they have been left open or have security vulnerabilities that can be exploited. Hypertext Transport Protocol (HTTP) Web services use port 80. HTTP is among the most commonly exploited services. In Hands-On Project 1-3, you use a port scanning tool to test the ports of a target computer.

### E-Mail and Communications

For a home user who regularly surfs the Web, uses e-mail, and engages in instant messaging, a firewall's primary job is to keep viruses from infecting the system and to prevent Trojan programs from being installed and creating back door openings. Personal firewall programs, such as Comodo Internet Security, come with an antivirus program that alerts users to an e-mail attachment or a file containing a known virus.

### Scripting

A widespread network intrusion that is increasing in frequency and severity is the use of scripts—executable code attached to e-mail messages or downloaded files that infiltrates a system. It can be difficult for a firewall or intrusion-detection system (IDS) to block all such files; specialty firewalls and other programs should be integrated with existing security systems to keep scripts from infecting a network.

A specialty e-mail firewall can monitor and control certain types of content that pass into and out of a network. These firewalls can be configured to filter out pornographic content, junk e-mail, and malicious code. M86 MailMarshal Secure Email Gateway by M86 Security, for instance, scans the content of each e-mail message before it reaches the recipient.

E-mail filtering programs, however, introduce privacy issues that need to be balanced against an organization's need for protection—a trade-off that applies to almost all aspects of network security, not just e-mail messages. Another problem you might encounter with the glut of available security software is redundant program functions that are incompatible. For example, Windows Firewall is included in Windows 7;

if you run it and another personal firewall program at the same time, you may have problems with your connection and desirable programs or communications being blocked.

**Always-On Connectivity**

The proliferation of affordable high-speed connections, such as cable and DSL, brings up special security concerns for network administrators. Computers that use always-on connections are easier to locate and attack because their IP addresses remain the same as long as they are connected to the Internet—which might be days at a time if computers are left on overnight or over a weekend. Some users pay extra for static IP addresses that never change and that enable them to run easily found Web servers or other services. Static IP addresses, however, make it easier for attackers to locate a computer and scan it for open ports.

Another problem could occur when remote users want to connect to an organization's internal network. Remote users include employees who are on the road, contractors who work at home, and business partners. As the Internet grew in popularity, more home computers started using modems. These connections were usually made through temporary dial-up connections that used protocols such as Point-to-Point Protocol (PPP). Today, however, it is increasingly likely that remote users connect to a network through an always-on DSL or cable modem connection, which means they might be connected to a network for hours at a time.

Always-on connections effectively extend the boundaries of your corporate network, and you should secure them as you would any part of your network perimeter. At the very least, your network security policy should specify that remote users have their computers equipped with firewall and antivirus protection software. While a written policy may be helpful, more and more organizations are using technology to enforce such remote access policies and allow administrators to block internal network access to remote systems that have not met security requirements. After all, if attackers can break into a remote user's computer while the user is connected to your network through a virtual private network (VPN) or other connection, your network becomes vulnerable as well.

◀ Preliminary Activity for Week 1

Jump to...

Analysis, Application, and Exploration For Week 1 ▶

Navigation

Home

Dashboard

Site pages

My courses

Capstone Project 2

Network Defense and Remote Access Configuration

Participants

General

01 [Enter Module Title Here]

Preliminary Activity for Week 1

**Lesson Proper for Week 1**

Analysis, Application, and Exploration For Week 1

Generalization for Week 1

Evaluation for Week 1

Assignment for Week 1

02 [Enter Module Title Here]

03 [Enter Module Title Here]

04 [Enter Module Title Here]

05 [Enter Module Title Here]

OJT/Practicum 2

Seminars and Tours

Courses

## Fair Warning

**NOTICE**: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

**PROSECUTION**: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION**: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

## Activities

Assignments

Forums

Quizzes

Resources