Chapter 03 – Network and Computer Attacks

Notes

Overview

Chapter three describes different types of malicious software. Malicious software, sometimes referred to as malware, includes viruses, Trojan horses, and worms. You will learn about different types of malware and network attacks and how to protect their resources from them. Finally, the chapter explains the physical aspect of security and why it is essential for security and network professionals to pay attention to physical security.

Chapter Objectives

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

- Describe the different types of malicious software and what damage they can do
- Describe methods of protecting against malware attacks
- Describe the types of network attacks
- Identify physical security attacks and vulnerabilities

Tips

Malicious Software (Malware)

1. Malicious software is sometimes referred to as malware. Malware includes:
   a. Viruses
   b. Worms
   c. Trojan programs

Tip	Many users call all types of malware viruses. This is a misconception and you should understand the differences between the various types of malware.

2. The main goal of malware is making money. Malware was once targeted at Windows, Linux and other traditional OSs but today, it is written to target tablets, smartphones, and other Internet-connected devices.

Viruses

1. The following characteristics of a virus:
   a. Attaches itself to an executable file
   b. Does not stand on its own
   c. Needs a host program to replicate

Tip	Find more information about viruses and their types at https://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses.

2. See Figure 3-1 how a virus is attached to an e-mail.

3. Ransomware is a type of virus that locks a target system until a ransom is paid. It is a growing trend in viruses. See Table 3-1 for some viruses and their descriptions.

4. Antivirus solutions use virus signatures to identify and correct an infection. This is the reason why you should periodically update your virus signatures database.

Macro Viruses

1. A macro virus is a virus encoded as a macro in programs that support a macro language, such as Visual Basic for Applications (VBA).

2. A macro is a list of commands that can be executed. Although macros can be very helpful creating automatic processes for doing repetitive tasks, they can also be used for destructive purposes, such as deleting files. Many macros are configured to run as soon as a file is opened.

3. Macros are not a menace when used correctly. The main problem with macros is that even nonprogrammers can create macros with either good or bad purposes. You can easily find tutorials for creating macro viruses on many Web sites.

Worms

1. A worm, like a virus, replicates and propagates itself but without having to attach itself to a host.

2. Worms can rapidly replicate to multiple users on the same network or over the Internet. In theory, worms can infect every computer in the world over a short period of time.

Tip	To read an article about the most famous virus and worms of all time, visit: http://www.eweek.com/c/a/Security/The-Most-Famous-or-Infamous-Viruses-and-Worms-of-All-Time.

3. See Table 3-2 for common computer worms. In a search engine type in the name of a worm and investigate the resulting links.

Trojan Programs

1. Trojan programs infect your computer by disguising malicious content using apparently normal computer programs. Users are tricked to install and use these apparently normal programs. What users do not know is that at the same time, another program has been installed on the computer. This other program can be a rootkit or a backdoor. Rootkits and backdoors allow attackers to later return and regain access to the attacked computer.

2. Uou can help your network from being infected by Trojan programs using hardware firewalls, because many Trojan programs use uncommon ports for communication. Firewalls can detect such traffic and block it. However, this is not a complete solution, since there are Trojan programs that use common ports like TCP port 80 (HTTP) or UDP port 53 (DNS).

3. See Table 3-3 for some Trojan program examples and what ports they use.

Spyware

1. Spyware is used by attackers to collect information about their victims. When a spyware program is installed on a computer, it can send information from the infected computer to the attacker, including confidential financial data, passwords, PINs and any other stored data. Spyware programs can register every keystroke entered.

2. Users shouldn't assume physical security measures, such as locked doors, are enough to keep all intruders out.

Adware

1. Understand the similarities and differences between spyware and adware. Both can be installed without the user being aware of their presence. The main difference is that sometimes adware displays a banner that notifies users of its presence.

2. The main purpose of adware is to determine purchasing habits. Web browsers then display advertisements tailored to this user.

3. The biggest problem with adware is that it slows down the computer it's running on.

Tip	Find best practices for protecting against spyware and adware at http://www.sophos.com/virusinfo/bestpractice/.

Protecting Against Malware Attacks

1. Tools for protecting your network from malware attacks include:
   a. Antivirus software
   b. Education

2. See Figure 3-3 for antivirus software detecting a virus.

Educating Your Users

1. One simple but effective method to educate your users is to e-mail monthly security updates about viruses and other attacks.

2. Because many malware programs can be detected using antivirus solutions, it is very important that your users update the virus signature file as soon as it is available from the vendor. Unfortunately, antivirus solutions are not enough to detect and eradicate spyware and adware. You must install specialized software like SpyBot and Ad-Aware. Both are free solutions and should be downloaded from trusted sources.

3. Understand how firewall and IDSs can be used to protect network resources from malware attacks.

4. Using fear tactics to scare users into compliance is not the right approach. As a security tester, you cannot use fear to generate business. It is not only unethical, but against the OSSTMM's Rules of Engagement. As a security professional, you should promote awareness rather than instilling fear. Build upon their knowledge to explain security-related issues.

Intruder Attacks on Networks and Computers

1. Understand the following concepts:
    a. Attack
    b. Vulnerability
    c. Exploit
    d. Network security
    e. Computer security

Denial-of-Service Attacks

1. A Denial-of-Service (DoS) attack prevents legitimate users from accessing network resources. Some forms of DoS attacks do not involve computers. When attacks do involve computers, they do not attempt to access information on your network; instead, they cripple it so that the network is vulnerable to other types of attacks.

2. As a security professional you should not try to perform a DoS attack yourself. Instead, you simply need to prove that such attack can or cannot be carried out.

3. A Ping of Death attack is an attack that causes the victim computer to freeze and malfunction.

Distributed Denial-of-Service Attacks

1. A DoS attack can be enhanced to perform a distributed attack known as a Distributed Denial-of-Service (DDoS) attack. On this type of attack, several network devices are used simultaneously for attacking a particular target. Usually, attacking devices are not aware that they are part of a DDoS attack.

2. Loss of bandwidth and degradation of speed are symptoms of a DDoS attack.

3. An attacker might use a Dark DDOS attack as a smokescreen to distract network defenders while another stealthier and likely more damaging attack is occurring.

Buffer Overflow Attacks

1. Every input field on a program is associated with a buffer of a defined capacity. A buffer overflow attack happens when the attacker tries to accommodate more data than the predefined buffer capacity. Usually the exceeding data contains executable code that when executed, elevates the attackers permissions on the hosting system.

2. See Table 3-4 for some examples of well known buffer overflow vulnerabilities.

3. The best way to protect against this type of attack is to train your programming team to develop applications with security in mind. For example, programmers should never accept an input without first verifying its size against the buffer capacity.

Eavesdropping

1. An attacker will use eavesdropping tools (sniffing tools) in order to intercept confidential information or gather credentials that can be used to extend the attack.

2. To defend against eavesdropping, network equipment and applications should be forced to communicate only over encrypted protocols and utilize valid, trusted certificates.

Man-in-the-Middle

1. In a man-in-the-middle attack, attackers inject themselves between two parties or systems communicating with one another in order to manipulate messages being passed back and forth.

Network Session Hijacking

1. Session hijacking enables the attacker to join a TCP session and make both parties think he or she is the other party.

> ***Tip*** To read an article on how to help prevent session hijacking, click: https://technet.microsoft.com/en-us/magazine/2005.01.sessionhijacking.aspx.

Addressing Physical Security

Keyloggers

1. Keyloggers are software or hardware devices that can be used to capture keystrokes on a computer.

2. Software keyloggers behave like Trojan programs and can be detected with antivirus solutions.

3. Hardware-based keyloggers are devices that are placed between the keyboard and the actual computer. Random visual tests must be periodically conducted on your premises to detect unauthorized hardware installed on your computers and systems.

Behind Locked Doors

1. Good physical security policies with insufficient door locks will not protect a network. An average person can pick a deadbolt lock in less than five minutes (after a week or two of practice). Experienced hackers can pick the same lock in under 30 seconds.

2. Take the time to look for good deadbolt locks or some other strong door locking mechanism. Some companies implement a security card solution. Using security cards, you can deploy a system that keeps track of who enters and leaves the room and at what time. Also, security cards can give employees access to several doors with the same card, instead of having one key per door.

Additional Resources

1. The Morris Worm: http://limn.it/the-morris-worm/

2. MIT Guide to Lock Picking: http://www.lysator.liu.se/mit-guide/mit-guide.html

3. Macro virus stuff: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214550,00.html

4. Spybot S&D: http://www.safer-networking.org/en/index.html

5. Ad-aware: http://www.lavasoft.com/

Key Terms

- adware
- attack
- backdoor
- botnet
- buffer overflow attack
- computer security
- denial-of-service (DoS) attack
- distributed denial-of-service (DDoS) attack
- exploit
- keyloggers
- macro virus
- malware
- network security
- Ping of Death attack
- ransomware
- rootkit
- shell
- spyware
- Trojan program
- virus
- virus signature file
- vulnerability
- whitelisting
- worm
- zombies