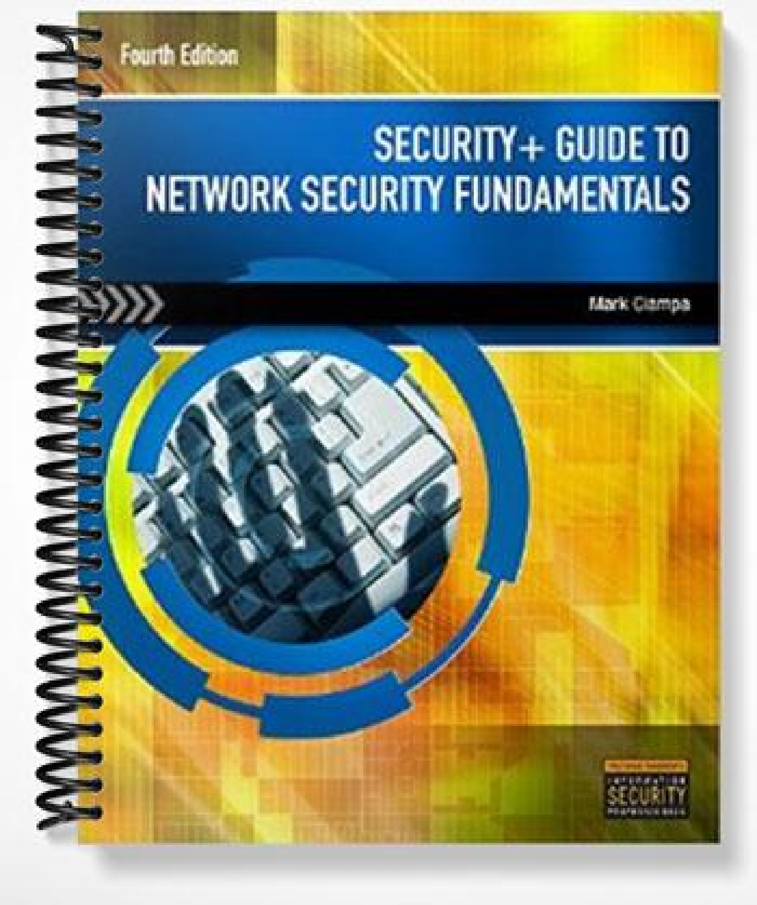
SOLUTIONS MANUAL



Chapter 2

Malware and Social Engineering Attacks

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

In this chapter, we will examine the threats and risks that a computer system faces today. It begins by looking at software-based attacks. Then, it considers attacks directed against the computer hardware. Finally, the chapter turns to the expanding world of virtualization and how virtualized environments are increasingly becoming the target of attackers.

Chapter Objectives

- Describe the differences between a virus and a worm
- List the types of malware that conceals its appearance
- Identify different kinds of malware that is designed for profit
- Describe the types of social engineering psychological attacks
- Explain physical social engineering attacks

Teaching Tips

Attacks Using Malware

1. Define malicious software, or malware, as software that enters a computer system without the owner's knowledge or consent. Malware is a general term that refers to a wide variety of damaging or annoying software.

2. Describe the three primary objectives of malware:
    a. To infect a computer system
    b. Conceal the malware's malicious actions
    c. Bring profit from the actions that it performs

Malware That Spreads

1. Define a virus as a program that secretly attaches to another document or program and executes when that document or program is opened.

2. Explain that once a virus infects a computer, it performs two separate tasks:
    a. Replicates itself by spreading to other computers
    b. Activates its malicious payload

3. Mention that viruses cause problems ranging from displaying an annoying message to erasing files from a hard drive or causing a computer to crash repeatedly. Use Figure 2-1 to illustrate your explanation.

4. Describe the following types of computer viruses:
    a. File infector virus
    b. Resident virus
    c. Boot virus
    d. Companion virus
    e. Macro virus

Teaching Tip	Because of the risk of macro viruses, users should be cautious of opening any e-mail attachment, because doing so could launch a macro virus.

5. Explain that metamorphic viruses avoid detection by altering how they appear. Polymorphic viruses also encrypt their contents differently each time.

6. Define a worm as a program designed to take advantage of a vulnerability in an application or an operating system in order to enter a system.

Teaching Tip	A worm uses a network to send copies of itself to other devices connected to the network.

7. Explain that worms are different from viruses in two regards:
    a. A worm can travel by itself
    b. A worm does not require any user action to begin its execution

8. Mention that some actions that worms perform include deleting files on the computer or allowing the computer to be remote-controlled by an attacker.

Malware That Conceals

1. Define a Trojan horse (or just Trojan) as a program advertised as performing one activity but actually doing something else.

2. Explain that Trojan horse programs are typically executable programs that contain hidden code that attack the computer system.

3. Define a rootkit as a set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.

4. Mention that the rootkit's goal is to hide the presence of other types of malicious software.

Teaching Tip	Originally the term "rootkit" referred to a set of modified and recompiled tools for the UNIX operating system. A root is the highest level of privilege available in UNIX, so a "rootkit" described programs that an attacker used to gain root privileges and to hide the malicious software.

5. Explain that rootkits function by replacing operating system commands with modified versions that are specifically designed to ignore malicious activity in order to escape detection.

6. Mention that detecting a rootkit can be difficult. Removing a rootkit from an infected computer is extremely difficult. You need to reformat the hard drive and reinstall the operating system.

7. Define a logic bomb as a computer program or a part of a program that lies dormant until it is triggered by a specific logical event. Once triggered, the program can perform any number of malicious activities. Use Table 2-1 to describe the most famous logic bombs.

8. Mention that logic bombs are extremely difficult to detect before they are triggered.

9. Define privilege escalation as exploiting a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining.

10. Describe the following types of privilege escalation:
    a. When a user with a lower privilege uses privilege escalation to access functions reserved for higher privilege users
    b. When a user with restricted privileges accesses the different restricted functions of a similar user

Teaching Tip	Privilege escalation has been discovered in Microsoft Windows, Cisco software, antivirus software, Apple Mac OS X, Microsoft Internet Information Services, and Linux.

Quick Quiz 1

1. A(n) ____ is a program that secretly attaches itself to a legitimate “carrier,” such as a document or program, and then executes when that document is opened or program is launched.
   Answer: computer virus

2. A(n) ____ is a set of software tools used by an intruder to break into a computer, obtain special privileges to perform unauthorized functions, and then hide all traces of its existence.
   Answer: rootkit

3. A(n) ____ is a computer program or a part of a program that lies dormant until it is triggered by a specific logical event, such as a certain date reached on the system calendar or a drop below a previous level of a person’s rank in an organization.
   Answer: logic bomb

4. ____ is exploiting a vulnerability in software to gain access to resources that the user would normally be restricted from obtaining.
   Answer: Privilege escalation

Malware that Profits

1. Define spam as unsolicited e-mail.

2. Mention that spam is a lucrative business. Describe the costs involved for spamming:
   a. E-mail address
   b. Equipment and Internet connection

Teaching Tip	The profit from spamming can be substantial. If a spammer sent spam to six million users for a product with a sale price of $50 that cost only $5 to make, and if only 0.001 percent of the recipients responded and bought the product (a typical response rate), the spammer would make over $270,000 in profit.

3. Mention that text-based spam messages can easily by trapped by spam filters.

4. Explain that image spam uses graphical images of text in order to circumvent text-based spam filters. It includes nonsense text so that it appears the e-mail message is legitimate. Use Figure 2-2 to illustrate your explanation.

5. Explain that in addition to sending a single graphical image, spammers also use other techniques, such as the following:
   a. GIF Layering (See Figure 2-3)
   b. Word Splitting (See Figure 2-4)
   c. Geometric variance (See Figure 2-5)

6. Explain that image spam cannot be easily filtered based on the content of the message. To detect image spam, one approach is to examine the context of the message and create a profile, asking questions such as:
   a. Who sent the message?
   b. What is known about the sender?
   c. Where does the user go if she responds to this e-mail?
   d. What is the nature of the message content?
   e. How is the message technically constructed?

7. Define spyware as a general term used for describing software that imposes upon a user’s privacy or security.

8. Mention that the Antispyware Coalition defines spyware as technologies that are deployed without the user’s consent and impair the user’s control over:
   a. Material changes that affect their user experience, privacy, or system security
   b. Use of their system resources, including what programs are installed on their computers
   c. Collection, use, and distribution of their personal or other sensitive information

9. Describe the two characteristics that make spyware very treacherous:
    a. Spyware creators are motivated by profit. Because of this, spyware in many instances is more intrusive than viruses, harder to detect, and more difficult to remove
    b. Spyware is not always easy to identify

10. Use Table 2-2 to explain the effects of spyware.

11. Mention that spyware is very widespread. Although attackers use several different spyware tools, the two most common are adware and keyloggers.

Teaching Tip	Read more about spyware at: http://en.wikipedia.org/wiki/Spyware.

12. Define adware a software program that delivers advertising content in a manner that is unexpected and unwanted by the user.

13. Explain that adware can be a security risk. Many adware programs perform a tracking function, which monitors and tracks a user's activities and then sends a log of these activities to third parties without the user's authorization or knowledge.

14. Define a keylogger as a small hardware device or a program that monitors each keystroke a user types on the computer's keyboard. As the user types, the keystrokes are collected and saved as text**.**

15. Explain that as a hardware device, a keylogger is a small device inserted between the keyboard connector and computer keyboard port. Use Figure 2-6 to illustrate your explanation.

16. Define software keyloggers as programs that silently capture all keystrokes, including passwords and sensitive information. They hide themselves so that they cannot be easily detected even if a user is searching for them. Use Figure 2-7 to illustrate your explanation.

Teaching Tip	Keyloggers are frequently found on public access computers, such as those in a library or a student computing lab. Users should not use these computers to perform any actions that require entering sensitive data.

17. Define a botnet as hundreds, thousands, or even tens of thousands of zombie computers that are under the control of an attacker.

18. Define a zombie as an infected computer with a program that will allow the attacker to remotely control it.

19. Explain that attackers use Internet Relay Chat (IRC) to remotely control the zombies. An attacker is knows as a bot herder.

20. Use Table 2-3 to describe the uses of botnets.

Social Engineering Attacks

1. Mention that social engineering is a means of gathering information for an attack by relying on the weaknesses of individuals.

Psychological Approaches

1. Explain that social engineering relies on an attacker's clever manipulation of human nature in order to persuade the victim to provide information or take actions.

2. Explain that basic methods of persuasion include ingratiation (flattery or insincerity), conformity (everyone else is doing it), and friendliness.

3. Mention that social engineering psychological approaches often involve impersonation, phishing, spam, and hoaxes.

Teaching Tip	Conformity is a group-based behavior, yet it can be used on an individual by convincing the victim that everyone else has been giving the attacker the requested information. This type of attack is successful because it is used as a way to diffuse the responsibility of the employee cooperating and alleviates the stress on the employee.

Physical Procedures

1. Define dumpster diving as an attack that involves digging through trash receptacles to find information that can be useful in an attack.

2. Explain that a weakness of automated access control systems is that they cannot control how many people enter the building when access is allowed; once an authorized person opens the door, then virtually any number of individuals can follow behind and also enter the building or area. This type of attack is known as tailgating.

3. Use Table 2-5 to describe some of the materials that may be found by dumpster diving.

Quick Quiz 2

1. ____ is a general term used for describing software that imposes upon a user's privacy or security.
   Answer: Spyware

2. ____ is a software program that delivers advertising content in a manner that is unexpected and unwanted by the user.

Answer: Adware

3. A(n) ____ is either a small hardware device or a program that monitors each keystroke a user types on the computer's keyboard.
Answer: keylogger

4. _____ is a form of tailgating that involves the tailgater colluding with an authorized person.
Answer: Piggybacking

Class Discussion Topics

1. Describe and compare the main types of spyware.

2. Why is spam so difficult to eradicate?

Additional Projects

1. Have students do some research to find software and hardware that can be used to hack into a computer system. Ask them to summarize their research in a short paper.

2. Ask your students to read more about hybrid threats, such as those that are part of the TDSS, Zeus or other complex threat platforms.

Additional Resources

1. Tdss rootkit silently owns the net
http://www.prevx.com/blog/139/Tdss-rootkit-silently-owns-the-net.html

2. Adware
www.webopedia.com/TERM/A/adware.html

3. Rootkit
http://www.webopedia.com/TERM/R/rootkit.html

4. Social Engineering Education
http://www.social-engineer.org/

5. Avoiding Social Engineering and Phishing Attacks
http://www.us-cert.gov/cas/tips/ST04-014.html

Key Terms

- **adware** A software program that delivers advertising content in a manner that is unexpected and unwanted by the user.
- **backdoor** Software code that gives access to a program or a service that circumvents normal security protections.
- **botnet** A logical computer network of zombies under the control of an attacker.
- **computer virus** (**virus**) A malicious computer code that, like its biological counterpart, reproduces itself on the same computer.
- **dumpster diving** The act of digging through trash receptacles to find information that can be useful in an attack.
- **hoax** A false warning.
- **impersonation** An attack that creates a fictitious character and then plays out the role of that person on a victim.
- **keylogger** Captures and stores each keystroke that a user types on the computer's keyboard.
- **logic bomb** Computer code that lies dormant until it is triggered by a specific logical event.
- **malware** Software that enters a computer system without the user's knowledge or consent and then performs an unwanted—and usually harmful—action.
- **pharming** A phishing attack that automatically redirects the user to a fake site.
- **phishing** Sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate enterprise in an attempt to trick the user into surrendering private information.
- **rootkit** A set of software tools used by an attacker to hide the actions or presence of other types of malicious software.
- **shoulder surfing** Watching an authorized user enter a security code on a keypad.
- **social engineering** A means of gathering information for an attack by relying on the weaknesses of individuals.
- **spam** Unsolicited e-mail.
- **spear phishing** A phishing attack that targets only specific users.
- **spim** A variation of spam, which targets instant messaging users instead of e-mail users.
- **spyware** A general term used to describe software that spies on users by gathering information without consent, thus violating their privacy.
- **tailgating** The act of unauthorized individuals entering a restricted-access building by following an authorized user.
- **Trojan horse** (**Trojan**) An executable program advertised as performing one activity, but actually does something else (or it may perform both the advertised and malicious activities).
- **vishing** A phishing attack that uses a telephone call instead of using e-mail.
- **whaling** A phishing attack that targets only wealthy individuals.
- **word splitting** Horizontally separating words so that they can still be read by the human eye.
- **worm** A malicious program designed to take advantage of a vulnerability in an application or an operating system in order to enter a computer and then self-replicate to other computers.