

CHAPTER 1: INTRODUCTION TO CYBER CRIME AND SECURITY

Multiple Choice:

1. Which of the following is NOT considered a type of threat to a computer system?

- A. Malware
- B. Intrusions
- C. Pop-ups
- D. Denial of Service (DoS) attacks

Answer: C **Reference:** Identifying Types of Threats **Difficulty:** easy

2. A generic term for a type of software that can harm a system is _____:

- A. malware.
- B. cookie.
- C. spyware.
- D. freeware.

Answer: A **Reference:** Identifying Types of Threats **Difficulty:** easy

3. What is the term for a small, dependent program that replicates itself in a system?

- A. Bomb
- B. Cookie
- C. Virus
- D. Worm

Answer: C **Reference:** Identifying Types of Threats **Difficulty:** easy

4. What is the main purpose of a cookie?

- A. To slowdown or shutdown a computer network
- B. To record keystrokes

- C. To protect a system from attack
- D. To identify users when they return to a particular Web site

Answer: D **Reference:** Identifying Types of Threats **Difficulty:** easy

5. Which of the following is an example of spyware?

- A. Worm
- B. Key logger
- C. Trojan horses
- D. Shareware

Answer: B **Reference:** Identifying Types of Threats **Difficulty:** moderate

6. _____ is the term for conning an individual into revealing secure information.

- A. Information engineering
- B. War-driving
- C. Mass mailing
- D. Social engineering

Answer: D **Reference:** Identifying Types of Threats **Difficulty:** easy

7. Which of the following is the most balanced reaction to threats on network security?

- A. Realistically assessing your system
- B. A reactive approach
- C. The belief that the danger from network attacks is vastly overestimated
- D. The belief that there are many imminent threats to your system

Answer: A **Reference:** How Seriously Should You Take Threats to Network Security? **Difficulty:** easy

8. Which of the following is NOT a component of perimeter security?

- A. Firewalls
- B. Password policies
- C. Proxy servers
- D. Event policies

Answer: D **Reference:** Network Security Paradigms **Difficulty:** moderate

9. Network security paradigms can be classified as each of the following EXCEPT:

- A. perimeter security.
- B. layered security.
- C. system security.
- D. proactive security.

Answer: C **Reference:** Network Security Paradigms **Difficulty:** moderate

10. The oldest piece of legislation in the United States that affects computer security is _____:

- A. Computer Security Act of 1987.
- B. Computer Crimes Act of Florida.
- C. OMB Circular A-130
- D. Health Insurance Portability and Accountability Act of 1996.

Answer: A **Reference:** How Do Legal Issues Impact Network Security? **Difficulty:** moderate

11. Which of the following is an example of a highly desirable hybrid security approach?

- A. A firewall, a proxy server, and password policies
- B. Layered security and a firewall
- C. Perimeter security, layered internal security, and intrusion detection
- D. An IDS and a password policy

Answer: C **Reference:** Network Security Paradigms **Difficulty:** moderate

12. This Web site includes detailed information on virus breakouts.

- A. Microsoft Security Advisor Web site
- B. SANS Institute Web site
- C. F-Secure Web site
- D. CERT Web site

Answer: C **Reference:** Online Security Resources **Difficulty:** moderate

Fill in the Blank:

13. The first step in understanding computer and network security is to formulate a(n) _____ of the threats to those systems.

Answer: realistic assessment **Reference:** How Seriously Should You Take Threats to Network Security?

Difficulty: moderate

14. Weighting the profile and the _____ of your system to potential intruders provides a balanced view in determining a threat level.

Answer: value **Reference:** How Seriously Should You Take Threats to Network Security? **Difficulty:** easy

15. A(n) _____ is the most common form of attack on individual as well as large organization networks.

Answer: worm **Reference:** Common Attacks on Your Network **Difficulty:** easy

16. The Bagel virus is an example of a(n) _____ virus that causes systems to crash.

Answer: mass-mailing **Reference:** Identifying Types of Threats **Difficulty:** easy

17. _____ is one common way to cause a system to crash and block legitimate users from accessing the system.

Answer: Denial of Service (DoS) **Reference:** Identifying Types of Threats **Difficulty:** easy

18. A(n) _____ is someone who calls himself a hacker, but lacks the expertise.

Answer: script kiddy **Reference:** Basic Security Terminology **Difficulty:** easy

19. Someone who is given permission by a corporation to hack their system is called a(n) _____.

Answer: sneaker **Reference:** Basic Security Terminology **Difficulty:** moderate

Matching:

20. Match the following terms to their meanings:

- | | |
|------------------|---|
| I. Virus | A. Text file that your browser creates and stores on your hard drive |
| II. Trojan horse | B. Seemingly benign software that secretly downloads a virus |
| III. Cookie | C. Small program that replicates and hides itself inside other programs |
| IV. Key logger | D. Form of spyware that records all keystrokes on the computer |

Answer: C B A D

Reference: Identifying Types of Threats

Difficulty: moderate

21. Match the following terms to their meanings:

- | | |
|------------------------|---|
| I. Social engineering | A. Attacks that include any attempt to gain unauthorized access to a system |
| II. Intrusions | B. Generic term for software that has a malicious purpose |
| III. Denial of Service | C. Designed to prevent legitimate access to a system |
| IV. Malware | D. Attacks a system by exploiting human nature rather than technology |

Answer: D A C B

Reference: Identifying Types of Threats

Difficulty: easy

22. Match the following terms to their meanings:

- | | |
|------------------|--|
| I. Hacking | A. Computer program used to identify the phone numbers that can successfully make a connection with a computer modem |
| II. Cracking | B. Act of breaking into a secure system |
| III. War-driving | C. Act of breaking into a secure system to steal and corrupt data |
| IV. War-dialing | D. Act of driving in a vehicle with a wireless laptop computer to exploit existing wireless networks |

Answer: B C D A

Reference: Identifying Types of Threats

Difficulty: moderate

23. Match the following terms to their meanings:

- | | |
|----------------------|---|
| I. White hat hacker | A. One who discovers a security weakness and causes harm to the system |
| II. Black hat hacker | B. One who exploits a computer system |
| III. Gray hat hacker | C. One who discovers a security weakness and reports it |
| IV. Hacker | D. One who abides by the law, but may be tempted to venture into illegal activity |

Answer: C A D B

Reference: Basic Security Terminology

Difficulty: easy

24. Match the following terms to their meanings:

- | | |
|---------------------------------|--|
| I. Firewall | A. System that monitors traffic, looking for suspicious activity |
| II. Proxy server | B. Barrier between a network and the outside world |
| III. Intrusion-detection system | C. Server that sits between a client application and a real server |
| IV. Security device | D. Hardware and software used to prevent breaches in security |

Answer: B A C D

Reference: Basic Security Terminology

Difficulty: easy

25. Match the following terms with the best description:

- | | |
|-----------------------|---|
| I. Proactive Security | A. A network with a firewall, proxy server, and a solid password policy |
| II. Phreaking | B. A segmented network with a firewall and a solid password policy |
| III. Layered Security | C. A network with and intrusion detection system (IDS) |
| IV. Authentication | D. Process of verifying user credentials when accessing a system |
| V. Perimeter Security | E. Process of reviewing event output |
| VI. Auditing | F. Process of accessing a telephone system |

Answer: C F B D A E **Reference:** Basic Security Terminology

Difficulty: easy