CHAPTER 1: INTRODUCTION TO NETWORK SECURITY

Multiple Choice:

1. Which of the following is NOT a connectivity device used to connect machines on a network?

A. Hub

B. Switch

C. Proxy server

D. Network interface card

Answer: C **Reference:** The Basics of a Network **Difficulty:** Easy

2. Which is a technique used to provide false information about data packets?

A. Hacking

B. Spoofing

C. Phreaking

D. Social engineering

Answer: B **Reference:** Data Packets **Difficulty:** Easy

3. Encryption and virtual private networks are techniques used to secure which of the following?

A. Data

B. Firewalls

C. Proxy servers

D. Connection points

Answer: A **Reference:** What Does This Mean for Security **Difficulty:** Easy

4. Which is NOT one of the three broad classes of security threats?

A. Malicious software

B. Disclosing contents of private networks

C. Gaining unauthorized access into a system

D. Preventing or blocking access to a system

Answer: B **Reference:** Classification of Threats **Difficulty:** Easy

5. A text file that is downloaded to a computer by a Web site to provide information about the Web site and online access is called a:

A. cookie

B. key logger

C. script kiddy

D. Trojan horse.

Answer: A **Reference:** Classification of Threats **Difficulty:** Easy

6. Which term is generally used by hackers to refer to attempts at intrusion into a system without permission and usually for malevolent purposes?

A. Hacking

B. Cracking

C. Blocking

D. Social engineering.

Answer: B **Reference:** Classification of Threats **Difficulty:** Easy

7. An attack characterized by an explicit attempt by attackers to prevent legitimate users from accessing a system is called:

A. denial of service.

B. social engineering.

C. spoofing.

D. war-dialing.

Answer: A **Reference:** Classification of Threats **Difficulty:** Easy

8. Those who exploit systems for harm such as to erase files, change data, or deface Web sites are typically called:

A. white hat hackers

B. gray hat hackers

C. red hat hackers

D. black hat hackers

Answer: D **Reference:** Hacking Terminology **Difficulty:** Easy

9. The process of determining whether the credentials given by a user are authorized to access a particular network resource is called:

A. auditing

B. accessing

C. authorization

D. authentication

Answer: D **Reference:** Security Terminology **Difficulty:** Moderate

10. What is a technique used to determine if someone is trying to falsely deny that they performed a particular action?

A. Auditing

B. Sneaking

C. Non-repudiation

D. Access Control Authorization

Answer: C **Reference:** Security Terminology **Difficulty:** Moderate

11. The process of reviewing logs, records, and procedures to determine whether they meet appropriate standards is called:

A. auditing

B. filtering

C. sneaking

D. authenticating

Answer: A **Reference:** Security Terminology **Difficulty:** Easy

12. Which approach to security addresses both the system perimeter and individual systems within the network?

A. Perimeter security approach

B. Layered security approach

C. Dynamic security approach

D. Hybrid security approach

Answer: B **Reference:** Approaching Network Security **Difficulty:** Moderate

13. Which approach to security is proactive in addressing potential threats before they occur?

A. Passive security approach

B. Layered security approach

C. Dynamic security approach

D. Hybrid security approach

Answer: C **Reference:** Approaching Network Security **Difficulty:** Difficult

14. In addition to mandating federal agencies to establish security measures, the Computer Security Act of 1987 defined important terms such as:

A. sensitive information

B. unauthorized access

C. private information

D. security information

Answer: A **Reference:** Network Security and the Law **Difficulty:** Moderate

15. Which of the following maintains a repository for information on virus outbreaks and detailed information about specific viruses?

A. CERT

B. F-Secure Corporation

C. Microsoft Security Advisor

D. SANS Institute

Answer: B **Reference:** Security Resources **Difficulty:** Easy

Fill in the Blank:

16. A(n) _____ serves as a barrier to unauthorized communication between a network and the outside world.

Answer: firewall **Reference:** Basic Network Structure **Difficulty:** Easy

17. _____ is a type of attack where header information on data packets is changed to provide false information.

Answer: Spoofing **Reference:** Data Packets **Difficulty:** Easy

18. Another name for an ethical hacker operating legally and with permission is _____.

Answer: sneaker **Reference:** Hacking Terminology **Difficulty:** Easy

19. A category of software that keeps track of users' activities on a computer is called _____.

Answer: spyware **Reference:** Classifications of Threats **Difficulty:** Easy

20. A term used to describe calling numerous telephone numbers, usually sequentially, in hopes of reaching a computer to attempt to hack into is called _____.

Answer: war-dialing **Reference:** Classifications of Threats **Difficulty:** Easy

21. _____ refers to a process used to locate wireless networks that might be vulnerable to attack.

Answer: War-driving **Reference:** Classifications of Threats **Difficulty:** Easy

22. Flooding a system with many false connection attempts in an effort to prevent legitimate use is an example of a _____ attack.

Answer: denial of service **Reference:** Classifications of Threats **Difficulty:** Easy

23. The preferred paradigm, or approach to security, is a _____ approach.

Answer: layered **Reference:** Approaching Network Security **Difficulty:** Moderate

24. Since they are easier to perpetrate than intrusions, _____ attacks are the most common form of attack after viruses.

Answer: blocking **Reference:** Classifications of Threats **Difficulty:** Moderate

25. The first computer incident-response team was sponsored by _____ University.

Answer: Carnegie-Mellon **Reference:** Using Security Resources **Difficulty:** Moderate

Matching:

26. Match the following terms to their meanings:

I. Cracking	A. Breaking into a system to learn about its flaws or weaknesses
II. Hacking	B. Attacking a system using non-technological means
III. Phreaking	C. Attacking a telecommunications system for gain
IV. Key logging	D. Attacking a system to cause harm or for personal gain
V. Social engineering	E. Attacking a system with software or hardware that tracks system use

Answer: D, A, C, E, B **Reference:** Hacking Terminology **Difficulty:** Easy

27. Match the following terms to their meanings:

I. White hat	A. Hacker who downloads and uses utilities with little understanding
II. Gray hat	B. Hacker who gains access to systems to cause harm
III. Black hat	C. Hacker who conducts illegal activities for perceived ethical reasons
IV. Script kiddy	D. Hacker who legally breaks into systems to assess security deficiencies
V. Ethical hacker	E. Hacker who looks for and reports vulnerabilities so they can be fixed

Answer: E, C, B, A, D **Reference:** Hacking Terminology **Difficulty:** Moderate

28. Match the following approaches to security to their meanings:

I. Perimeter Security	A. Few steps or actions are taken to prevent an attack.

II. Layered Security B. Network access and individual systems within the network are protected.

III. Passive Security C. Paradigm combining best of several approaches.

IV. Dynamic Security D. Emphasis includes firewalls, proxy servers, password policies, and network access.

V. Hybrid Security E. Steps are taken to prevent an attack before it occurs.

Answer: D, B, A, E, C **Reference:** Approaching Network Security **Difficulty:** Moderate

29. Match the following terms to their meaning:

I. encryption A. affects legitimate access to a system

II. spoofing B. used to secure data in the event of interception

III. router C. used to shut down a machine or prevent access

IV. blocking D. used to connect subnetworks together

V. buffer overflow E. changing the header data to provide misleading information

Answer: B, E, D, A, C **Reference:** The Basics of a Network **Difficulty:** Moderate

30. Match the following terms to their meanings:

I. CERT A. Provides documentation on virtually every aspect of security

II. SANS B. One of the most respected incident-response teams in the industry

III. HPPA C. Governs how publicly traded companies store and report financial information

IV. F-Secure D. Maintains repository for information on viruses

V. Sarbanes-Oxley E. Governs privacy of medical records and their security

Answer: B, A, E, D, C **Reference:** Network Security and the Law **Difficulty:** Easy