Chapter: Chapter 15

Multiple Choice

1. The most common method used by attackers to breach security is ____.
A) masquerading
B) message modification
C) session hijacking
D) phishing

Ans: A
Section: 15.1
Difficulty: Medium

2. A code segment that misuses its environment is called ____.
A) a backdoor
B) a trap door
C) a worm
D) a Trojan horse

Ans: D
Section: 15.2.1
Difficulty: Medium

3. Worms ____.
A) use the spawn mechanism to ravage system performance
B) can shut down an entire network
C) continue to grow as the Internet expands
D) All of the above

Ans: D
Section: 15.3.1

Difficulty: Easy

4. A denial of service attack is ____.
A) aimed at gaining information
B) aimed at stealing resources
C) aimed at disrupting legitimate use of a system
D) generally not network based

Ans: C
Section: 15.3.3
Difficulty: Medium

5. In a paired-password system, ____.
A) the user specifies two passwords
B) the computer supplies one part of a password and the user enters the other part
C) passwords must contain equal amounts of numbers and digits paired together
D) two users must enter their own separate password to gain access to the system

Ans: B
Section: 15.5.4
Difficulty: Medium

6. A ____ virus changes each time it is installed to avoid detection by antivirus software.
A) polymorphic
B) tunneling
C) multipartite
D) stealth

Ans: A
Section: 15.2.5
Difficulty: Medium

7. ____ is a symmetric stream cipher.
A) DES

B) AES
C) RC4
D) twofish

Ans: C
Section: 15.4.1
Difficulty: Difficult

8. A ____ is a public key digitally signed by a trusted party.
A) key ring
B) digital certificate
C) message digest
D) digital key

Ans: B
Section: 15.4
Difficulty: Difficult

9. ____ layer security generally has been standardized on IPSec.
A) Network
B) Transport
C) Data-link
D) Application

Ans: A
Section: 15.4.2
Difficulty: Medium

10. Which of the following is true of SSL?
A) It provides security at the data-link layer.
B) It is a simple protocol with limited options.
C) It is commonly used for secure communication on the Internet.
D) It was designed by Microsoft.

Ans: C
Section: 15.4.3
Difficulty: Medium

Essay

11. What are the four levels of security measures that are necessary for system protection?

Ans: To protect a system, security measures must take places at four levels: physical (machine rooms, terminals, and workstations); human (user authorization, avoidance of social engineering); operating system (protection against accidental and purposeful security breaches); and network (leased, Internet, and wireless connections).
Section: 15.1
Difficulty: Medium

12. What is a trap door? Why is it problematic?

Ans: A trap door is an intentional hole left in software by the designer of a program or system. It can allow circumvention of security features for those who know about the hole. Trap doors pose a difficult problem because, to detect them, we have to analyze all the source code for all components of a system.
Section: 15.15.2.2
Difficulty: Medium

13. How does a virus differ from a worm?

Ans: A worm is structured as a complete, standalone program whereas a virus is a fragment of code embedded in a legitimate program.
Section: 15.3
Difficulty: Difficult

14. What is the most common way for an attacker outside of the system to gain unauthorized access to the target system?

Ans: The stack- or buffer-overflow attack is the most common way for an attacker outside the system to gain unauthorized access to a system. This attack exploits a bug in the software in order to overflow some portion of the program and cause the execution of unauthorized code.
Section: 15.2.4
Difficulty: Medium

15. What are the two main methods used for intrusion detection?

Ans: The two most common methods employed are signature-based detection and anomaly detection. In signature-based detection, system input or network traffic is examined for specific behavior patterns known to indicate attacks. In anomaly detection, one attempts, through various techniques, to detect anomalous behavior within computer systems.
Section: 15.6.3
Difficulty: Medium

16. What is port scanning and how is it typically launched?

Ans: Port scanning is not an attack but rather is a means for a cracker to detect a system's vulnerabilities to attack. Port scanning typically is automated, involving a tool that attempts to create a TCP/IP connection to a specific port or a range of ports. Because port scans are detectable, they are frequently launched from zombie systems.
Section: 15.3.2
Difficulty: Medium

17. What role do keys play in modern cryptography?

Ans: Modern cryptography is based on secrets called keys that are selectively distributed to computers in a network and used to process messages. Cryptography enables a recipient of a message to verify that the message was created by some computer possessing a certain key - the key is the source of the message. Similarly, a sender can encode its message so that only a computer with a certain key can decode the message, so that the key becomes the destination.
Section: 15.4
Difficulty: Difficult

18. What is the difference between symmetric and asymetric encryption?

Ans: In a symmetric encryption algorithm, the same key is used to encrypt and to decrypt. In an asymetric encryption algorithm, there are different encryption and decryption keys. Asymmetric encryption is based on mathematical functions instead of the transformations used in symmetric encryption, making it much more computationally expensive to execute.
Section: 15.4.1
Difficulty: Difficult

19. What are the two main varieties of authentication algorithms?

Ans: The first type of authentication algorithm, a message-authentication code (MAC), uses symmetric encryption. In MAC, a cryptographic checksum is generated from the message using a secret key. The second type of authentication algorithm, a digital-signature algorithm, uses a public and private key. The authenticators thus produced are called digital signatures.
Section: 15.4.1
Difficulty: Difficult

20. What is the practice of safe computing? Give two examples.

Ans: The best practice against computer viruses is prevention, or the practice of safe computing. Purchasing unopened software from vendors and avoiding free or pirated copies from public sources or disk exchange offer the safest route to preventing infection. Another defense is to avoid opening any e-mail attachments from unknown users.
Section: 15.6.4
Difficulty: Easy

True/False

21. It is easier to protect against malicious misuse than against accidental misuse.

Ans: False
Section: 15.1

Difficulty: Medium

22. Spyware is not considered a crime in most countries.

Ans: True
Section: 15.2.1
Difficulty: Medium

23. Biometric devices are currently too large and expensive to be used for normal computer authentication.

Ans: True
Section: 15.5.5
Difficulty: Easy

24. Tripwire can distinguish between an authorized and an unauthorized change.

Ans: False
Section: 15.6
Difficulty: Medium

25. Generally, it is impossible to prevent denial-of-service attacks.

Ans: True
Section: 15.3.3
Difficulty: Medium