Computer Security Fundamentals 5th edition William Chuck Easttom Test Bank

SKU: 9780137984954-TEST-BANK

Computer Security Fundamentals 5e
Chapter 1 Introduction to Computer Security

True / False

1. The Domain Name System is what translates human-readable domain names into IP addresses that computers and routers understand.
True

2. The type of hacking that involves breaking into telephone systems is called sneaking.
False—This type of hacking is called phreaking.

3. The technique for breaching a system's security by exploiting human nature rather than technology is war-driving.
False—This describes social engineering.

4. Malware is a generic term for software that has a malicious purpose.
True

5. Software that lays dormant until some specific condition is met is a Trojan horse.
False—This describes a logic bomb. Usually, the condition that is met is a date and time.

6. Someone who breaks into a system legally to assess security deficiencies is a penetration tester.
True

7. Auditing is the process to determine if a user's credentials are authorized to access a network resource.
False—This describes authentication. Auditing is the process of reviewing logs, records, and procedures.

8. Confidentiality, integrity, and availability are three pillars of security, called the CIA triangle.
True

9. The Health Insurance Portability and Accountability Act of 1996 requires government agencies to identify sensitive systems, conduct computer security training, and develop computer security plans.
False—This describes the Computer Security Act of 1987.

10. The SANS Institute website is a vast repository of security-related documentation.
True

Multiple Choice

1. Which type of hacking is designed to prevent legitimate access to a computer system?
    a. Denial of service
    b. Web attack
    c. Session hijacking
    d. DNS poisoning

Answer A.

2. Your company is instituting a new security awareness program. You are responsible for educating end users on a variety of threats, including social engineering. Which of the following best defines social engineering?
    a. Illegal copying of software
    b. Gathering information from discarded manuals and printouts
    c. Using people skills to obtain proprietary information
    d. Destruction or alteration of data

Answer C.

3. Which type of hacking occurs when the attacker monitors an authenticated session between the client and the server and takes over that session?
    a. Denial of service
    b. Web attack
    c. Session hijacking
    d. DNS poisoning

Answer C.

4. Someone who finds a flaw in a system and reports that flaw to the vendor of the system is a _____.
    a. White hat hacker
    b. Black hat hacker
    c. Gray hat hacker
    d. Red hat hacker

Answer A.

5. Someone who gains access to a system and causes harm is a _____?
    a. White hat hacker
    b. Black hat hacker
    c. Gray hat hacker
    d. Red hat hacker

Answer B.

6. A black hat hacker is also called a _____.

a. Thief
b. Cracker
c. Sneaker
d. Script kiddy

Answer B.

7. Someone who calls himself a hacker but lacks the expertise is a _____.
a. Script kiddy
b. Sneaker
c. White hat hacker
d. Black hat hacker

Answer A.

8. Someone who legally breaks into a system to assess security deficiencies is a _____.
a. Script kiddy
b. Penetration tester
c. Gray hat hacker
d. Black hat hacker

Answer B.

9. A(n) _____ is a basic security device that filters traffic and is a barrier between a network and the outside world or between a system and other systems.
a. Firewall
b. Proxy server
c. Intrusion detection system
d. Network monitor

Answer A.

10. A(n) _____ hides the internal network's IP address and presents a single IP address to the outside world.
a. Firewall
b. Proxy server
c. Intrusion detection system
d. Network monitor

Answer B.

11. Which one of these is NOT one of the three pillars of security in the CIA triangle?
a. Confidentiality
b. Integrity
c. Availability

d. Authentication

Answer D.

12. Which of these is the process to determine if the credentials given by a user or another system are authorized to access the network resource in question?

a. Confidentiality
b. Integrity
c. Availability
d. Authentication

Answer D.

13. Which of these is a repository of security-related documentation and also sponsors a number of security research projects?

a. Computer Emergency Response Team
b. F-Secure
c. SANS Institute
d. Microsoft Security Response Center

Answer C.

14. Which of these was the first computer incident-response team?

a. Computer Emergency Response Team
b. F-Secure
c. SANS Institute
d. Microsoft Security Response Center

Answer A.

15. Which of these is a repository for detailed information on virus outbreaks?

a. Computer Emergency Response Team
b. F-Secure
c. SANS Institute
d. Microsoft Security Response Center

Answer B.