True / False

1. The Domain Name Service 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 sneaker.
   True—Companies may solicit the services of a sneaker to assess the company's vulnerabilities.

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 to review logs, records, and procedures.

8. Confidentiality, integrity, and availability are three pillars of 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.

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

Multiple Choice

1. In which type of hacking does the user block access from legitimate users without actually accessing the attacked system?
   a. Denial of service

b. Web attack
c. Session hijacking
d. None of the above

Answer A. A denial-of-service attack is probably the most common attack on the web.

2. Which type of hacking occurs due to user interaction with a website?
a. Denial of service
b. Web attack
c. Session hijacking
d. None of the above

Answer B. The most common purpose is to force the server to log the attacker onto the website. The most common type of web attack is SQL injection.

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. None of the above

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. White hat hackers are often hired by companies to do penetration tests.

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

Answer B. A black hat hacker might steal data, erase files, or deface websites.

6. A black hat hacker is also called a _____
a. Thief
b. Cracker
c. Sneaker
d. None of the above

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. There are many Internet tools that can be used to perform hacking tasks, and users of these tools who don't understand the target system are script kiddies.

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

Answer B. Anyone hired to assess the vulnerabilities of a system should be both technically proficient and ethical.

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

Answer A. A firewall can be a server, a router, or software running on a machine.

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 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 Advisor

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 Advisor

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 Advisor

Answer B. Information includes how a virus spreads, ways to recognize the virus, and, frequently, specific tools for cleaning an infected system.

Matching

a. Firewall
b. Proxy server
c. Denial-of-service attack
d. Malware
e. Sneaker
f. Availability

g. Auditing
h. Authentication
i. Phreaking
j. Social engineering

A. Barrier between a network and the outside world
B. Hides the internal network's IP address, and presents a single IP address to the outside world
C. Designed to prevent legitimate access to your system
D. Generic term for software that has a malicious purpose
E. Someone who legally breaks into a system to assess security deficiencies
F. Element of the CIA triangle that makes data readily available to authorized users
G. Process to review logs, records, and procedures to determine if it meets your standards
H. Process to determine if supplied credentials are authorized to access a network resource
I. Hacking that involves breaking into telephone systems
J. Technique for breaching a system's security by exploiting human nature rather than technology