Chapter 2 Study Guide

Indicate whether the statement is true or false.

1. Organizations can use dictionaries to regulate password selection during the reset process and thus guard against easy-to-guess passwords.
   a. True
   b. False

2. With electronic information is stolen, the crime is readily apparent.
   a. True
   b. False

3. An act of theft performed by a hacker falls into the category of “theft,” but is also often accompanied by defacement actions to delay discovery and thus may also be placed within the category of “forces of nature.”
   a. True
   b. False

4. Information security safeguards the technology assets in use at the organization.
   a. True
   b. False

5. A worm requires that another program is running before it can begin functioning.
   a. True
   b. False

6. With the removal of copyright protection mechanisms, software can be easily distributed and installed.
   a. True
   b. False

7. Information security’s primary mission is to ensure that systems and their contents retain their confidentiality at any cost.
   a. True
   b. False

8. DoS attacks cannot be launched against routers.
   a. True
   b. False

9. A number of technical mechanisms—digital watermarks and embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to deter or prevent the theft of software intellectual property.
   a. True
   b. False

Chapter 2 Study Guide

10. Compared to Web site defacement, vandalism within a network is less malicious in intent and more public.
    a. True
    b. False

11. Expert hackers are extremely talented individuals who usually devote lots of time and energy to attempting to break into other people's information systems.
    a. True
    b. False

12. Forces of nature, force majeure, or acts of God can present some of the most dangerous threats, because they are usually occur with very little warning and are beyond the control of people.
    a. True
    b. False

13. A worm may be able to deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected.
    a. True
    b. False

14. Two watchdog organizations that investigate allegations of software abuse are SIIA and NSA.
    a. True
    b. False

15. A mail bomb is a form of DoS attack.
    a. True
    b. False

16. A sniffer program can reveal data transmitted on a network segment including passwords, the embedded and attached files—such as word-processing documents—and sensitive data transmitted to or from applications.
    a. True
    b. False

17. Attacks conducted by scripts are usually unpredictable.
    a. True
    b. False

18. Much human error or failure can be prevented with effective training and ongoing awareness activities.
    a. True
    b. False

19. As an organization grows it must often use more robust technology to replace the security technologies it may have outgrown.
    a. True
    b. False

Chapter 2 Study Guide

20. An advance-fee fraud attack involves the interception of cryptographic elements to determine keys and encryption algorithms.

a. True

b. False

Indicate the answer choice that best completes the statement or answers the question.

21. The _____ data file contains the hashed representation of the user's password.

a. SLA b. SNMP

c. FBI d. SAM

22. _____ are malware programs that hide their true nature, and reveal their designed behavior only when activated.

a. Viruses b. Worms

c. Spam d. Trojan horses

23. _____ are compromised systems that are directed remotely (usually by a transmitted command) by the attacker to participate in an attack.

a. Drones b. Helpers

c. Zombies d. Servants

24. In a _____ attack, the attacker sends a large number of connection or information requests to disrupt a target from a small number of sources.

a. denial-of-service b. distributed denial-of-service

c. virus d. spam

25. Acts of _____ can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

a. bypass b. theft

c. trespass d. security

26. "4-1-9" fraud is an example of a _____ attack.

a. social engineering b. virus

c. worm d. spam

27. A _____ is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

a. denial-of-service b. distributed denial-of-service

c. virus d. spam

28. Which of the following functions does information security perform for an organization?

a. Protecting the organization's ability to function.

b. Enabling the safe operation of applications implemented on the organization's IT systems.

c. Protecting the data the organization collects and uses.

d. All of the above.

Chapter 2 Study Guide

29. In the _____ attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network.

a. zombie-in-the-middle b. sniff-in-the-middle
c. server-in-the-middle d. man-in-the-middle

30. As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus _____.

a. false alarms b. polymorphisms
c. hoaxes d. urban legends

31. Hackers can be generalized into two skill groups: expert and _____.

a. novice b. journeyman
c. packet monkey d. professional

32. A short-term interruption in electrical power availability is known as a ____.

a. fault b. brownout
c. blackout d. lag

33. ____ is any technology that aids in gathering information about a person or organization without their knowledge.

a. A bot b. Spyware
c. Trojan d. Worm

34. Microsoft acknowledged that if you type a res:// URL (a Microsoft-devised type of URL) which is longer than _____ characters in Internet Explorer 4.0, the browser will crash.

a. 64 b. 128
c. 256 d. 512

35. One form of online vandalism is _____ operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

a. hacktivist b. phreak
c. hackcyber d. cyberhack

36. Human error or failure often can be prevented with training, ongoing awareness activities, and _____.

a. threats b. education
c. hugs d. paperwork

37. Which of the following is an example of a Trojan horse program?

a. Netsky b. MyDoom
c. Klez d. Happy99.exe

38. The _____ hijacking attack uses IP spoofing to enable an attacker to impersonate another entity on the network.

a. WWW b. TCP
c. FTP d. HTTP

Chapter 2 Study Guide

39. _____ is the premeditated, politically motivated attacks against information, computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents.

a. infoterrorism b. cyberterrorism

c. hacking d. cracking

40. Web hosting services are usually arranged with an agreement defining minimum service levels known as a(n) ____.

a. SSL b. SLA

c. MSL d. MIN