Chapter 1 Study Guide

Indicate whether the statement is true or false.

1. The possession of information is the quality or state of having value for some purpose or end.
    a. True
    b. False

2. The physical design is the blueprint for the desired solution.
    a. True
    b. False

3. An e-mail virus involves sending an e-mail message with a modified field.
    a. True
    b. False

4. When a computer is the subject of an attack, it is the entity being attacked.
    a. True
    b. False

5. To achieve balance — that is, to operate an information system that satisfies the user and the security professional — the security level must allow reasonable access, yet protect against threats.
    a. True
    b. False

6. The implementation phase is the longest and most expensive phase of the systems development life cycle (SDLC).
    a. True
    b. False

7. Many states have implemented legislation making certain computer-related activities illegal.
    a. True
    b. False

8. Information security can be an absolute.
    a. True
    b. False

9. Hardware is often the most valuable asset possessed by an organization and it is the main target of intentional attacks.
    a. True
    b. False

10. The value of information comes from the characteristics it possesses.
    a. True
    b. False

Chapter 1 Study Guide

11. Using a methodology increases the probability of success.
    a. True
    b. False

12. A data custodian works directly with data owners and is responsible for the storage, maintenance, and protection of the information.
    a. True
    b. False

13. Applications systems developed within the framework of the traditional SDLC are designed to anticipate a software attack that requires some degree of application reconstruction.
    a. True
    b. False

14. The roles of information security professionals are almost always aligned with the goals and mission of the information security community of interest.
    a. True
    b. False

15. The bottom-up approach to information security has a higher probability of success than the top-down approach.
    a. True
    b. False

16. The investigation phase of the SecSDLC begins with a directive from upper management.
    a. True
    b. False

17. A breach of possession always results in a breach of confidentiality.
    a. True
    b. False

18. A champion is a project manager, who may be a departmental line manager or staff unit manager, and has expertise in project management and information security technical requirements.
    a. True
    b. False

19. Network security focuses on the protection of the details of a particular operation or series of activities.
    a. True
    b. False

20. During the early years of computing, the primary threats to security were physical theft of equipment, espionage against the products of the systems, and sabotage.
    a. True
    b. False

Chapter 1 Study Guide

21. A methodology for the design and implementation of an information system that is a formal development strategy is referred to as a __________.

a. systems design   b. development life project
c. systems development life cycle   d. systems schema

22. Which of the following phases is often considered the longest and most expensive phase of the systems development life cycle?

a. investigation   b. logical design
c. implementation   d. maintenance and change

23. During the __________ phase, specific technologies are selected to support the alternatives identified and evaluated in the prior phases.

a. investigation   b. implementation
c. analysis   d. physical design

24. An information system is the entire set of __________, people, procedures, and networks that make possible the use of information resources in the organization.

a. software   b. hardware
c. data   d. All of the above

25. The famous study entitled "Protection Analysis: Final Report" focused on a project undertaken by ARPA to understand and detect __________ in operating systems security.

a. Bugs   b. Vulnerabilities
c. Malware   d. Maintenance hooks

26. A type of SDLC where each phase has results that flow into the next phase is called the __________ model.

a. pitfall   b. SA&D
c. waterfall   d. Method 7

27. The ____ is the individual primarily responsible for the assessment, management, and implementation of information security in the organization.

a. ISO   b. CIO
c. CISO   d. CTO

28. __________ security addresses the issues necessary to protect the tangible items, objects, or areas of an organization from unauthorized access and misuse.

a. Physical   b. Personal
c. Object   d. Standard

29. Organizations are moving toward more __________-focused development approaches, seeking to improve not only the functionality of the systems they have in place, but consumer confidence in their product.

a. security   b. reliability
c. accessibility   d. availability

Chapter 1 Study Guide

30. A variation of n SDLC that can be used to implement information security solutions in an organizations with little or no formal security in place is the __________.

a. SecDSLC b. SecSDLC
c. LCSecD d. CLSecD

31. __________ has become a widely accepted evaluation standard for training and education related to the security of information systems.

a. NIST SP 800-12 b. NSTISSI No. 4011
c. IEEE 802.11(g) d. ISO 17788

32. A computer is the __________ of an attack when it is used to conduct an attack against another computer.

a. subject b. object
c. target d. facilitator

33. Which of the following is a valid type of role when it comes to data ownership?

a. Data owners b. Data custodians
c. Data users d. All of the above

34. In file hashing, a file is read by a special algorithm that uses the value of the bits in the file to compute a single number called the __________ value.

a. result b. smashing
c. hash d. code

35. __________ was the first operating system to integrate security as its core functions.

a. UNIX b. DOS
c. MULTICS d. ARPANET

36. __________ of information is the quality or state of being genuine or original.

a. Authenticity b. Spoofing
c. Confidentiality d. Authorization

37. A server would experience a __________ attack when a hacker compromises it to acquire information from it from a remote location using a network connection.

a. indirect b. direct
c. software d. hardware

38. People with the primary responsibility for administering the systems that house the information used by the organization perform the ____ role.

a. Security policy developers b. Security professionals
c. System administrators d. End users

39. Part of the logical design phase of the SecSDLC is planning for partial or catastrophic loss. ____ dictates what immediate steps are taken when an attack occurs.

a. Continuity planning b. Incident response
c. Disaster recovery d. Security response

Chapter 1 Study Guide

40. __________ is a network project that preceded the Internet.
a. NIST b. ARPANET
c. FIPS d. DES