Name: _____ Class: _____ Date: _____

Chapter 01 - Introduction to the Management of Information Security

1. The first step in solving problems is to gather facts and make assumptions.

a. True
b. False

ANSWER: False

2. Corruption of information can occur only while information is being stored.

a. True
b. False

ANSWER: False

3. The authorization process takes place before the authentication process.

a. True
b. False

ANSWER: False

4. 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

ANSWER: True

5. DoS attacks cannot be launched against routers.

a. True
b. False

ANSWER: False

6. "Shoulder spying" is used in public or semi-public settings when individuals gather information they are not authorized to have by looking over another individual's shoulder or viewing the information from a distance.

_____

ANSWER: False - surfing

7. When voltage levels lag (experience a momentary increase), the extra voltage can severely damage or destroy equipment. _____

ANSWER: False - spike

8. The macro virus infects the key operating system files located in a computer's start up sector.

_____

ANSWER: False - boot

9. The application of computing and network resources to try every possible combination of options of a password is called a dictionary attack. _____

ANSWER: False - brute force

10. The term phreaker is now commonly associated with an individual who cracks or removes software protection that is designed to prevent unauthorized duplication. _____

ANSWER: False - cracker

Name: _____ Class: _____ Date: _____

Chapter 01 - Introduction to the Management of Information Security

11. A(n) polymorphic threat is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for pre-configured signatures. _____
ANSWER: True

12. The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. _____
ANSWER: True

13. A device (or a software program on a computer) that can monitor data traveling on a network is known as a socket sniffer. _____
ANSWER: False - packet

14. One form of e-mail attack that is also a DoS attack is called a mail spoof, in which an attacker overwhelms the receiver with excessive quantities of e-mail. _____
ANSWER: False - bomb

15. Communications security involves the protection of which of the following?.
a. radio handsets
b. people, physical assets
c. the IT department
d. media, technology, and content
ANSWER: d

16. According to the C.I.A. triad, which of the following is a desirable characteristic for computer security?
a. accountability
b. availability
c. authorization
d. authentication
ANSWER: b

17. Which of the following is a C.I.A. characteristic that ensures that only those with sufficient privileges and a demonstrated need may access certain information?
a. Integrity
b. Availability
c. Authentication
d. Confidentiality
ANSWER: d

18. The use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections is an example of which process?
a. accountability
b. authorization
c. identification
d. authentication
ANSWER: d

19. What do audit logs that track user activity on an information system provide?
a. identification
b. authorization
c. accountability
d. authentication
ANSWER: c

20. Which of the following is the principle of management that develops, creates, and implements strategies for the accomplishment of objectives?

a. leading
b. controlling
c. organizing
d. planning

ANSWER: d

21. Which of the following is the principle of management dedicated to the structuring of resources to support the accomplishment of objectives?

a. organization
b. planning
c. controlling
d. leading

ANSWER: a

22. 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

ANSWER: d

23. Which of the following is the first step in the problem-solving process?

a. Analyze and compare the possible solutions
b. Develop possible solutions
c. Recognize and define the problem
d. Select, implement and evaluate a solution

ANSWER: c

24. Which of the following is NOT a step in the problem-solving process?

a. Select, implement and evaluate a solution
b. Analyze and compare possible solutions
c. Build support among management for the candidate solution
d. Gather facts and make assumptions

ANSWER: c

25. Which of the following is NOT a primary function of Information Security Management?

a. planning
b. protection
c. projects
d. performance

ANSWER: d

26. Which of the following functions of Information Security Management seeks to dictate certain behavior within the organization through a set of organizational guidelines?

a. planning
b. policy
c. programs
d. people

ANSWER: b

27. Which function of InfoSec Management encompasses security personnel as well as aspects of the SETA program?

a. protection
b. people

c. projects
d. policy

ANSWER: b

28. 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

ANSWER: c

29. _____ 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

ANSWER: d

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

ANSWER: c

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

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

ANSWER: b

32. “4-1-9” fraud is an example of a _____ attack.

a. social engineering
b. virus
c. worm
d. spam

ANSWER: a

33. Which type of attack involves sending a large number of connection or information requests to a target?

a. malicious code
b. denial-of-service (DoS)
c. brute force
d. spear fishing

ANSWER: b

34. Which of the following is not among the 'deadly sins of software security'?

a. Extortion sins
b. Implementation sins
c. Web application sins
d. Networking sins

ANSWER: a

Chapter 01 - Introduction to the Management of Information Security

35. 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

ANSWER: b

36. Blackmail threat of informational disclosure is an example of which threat category?

a. Espionage or trespass
b. Information extortion
c. Sabotage or vandalism
d. Compromises of intellectual property

ANSWER: b

37. 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

ANSWER: a

38. 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

ANSWER: b

39. Which of the following is a feature left behind by system designers or maintenance staff that allows quick access to a system at a later time by bypassing access controls?

a. brute force
b. DoS
c. back door
d. hoax

ANSWER: c

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

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

ANSWER: a

41. The three levels of planning are strategic planning, tactical planning, and _____ planning.

ANSWER: operational

42. The set of organizational guidelines that dictates certain behavior within the organization is called _____.

ANSWER: policy

43. Attempting to reverse-calculate a password is called _____.

ANSWER: cracking

44. ESD is the acronym for _____ discharge.

ANSWER: electrostatic

45. Duplication of software-based intellectual property is more commonly known as software _____.
ANSWER: piracy

46. A(n) _____ hacks the public telephone network to make free calls or disrupt services.
ANSWER: phreaker

47. A momentary low voltage is called a(n) _____.
ANSWER: sag

48. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, competitive _____.
ANSWER: intelligence

49. A(n) _____ is a potential weakness in an asset or its defensive control(s).
ANSWER: vulnerability

50. _____ is unsolicited commercial e-mail.
ANSWER: Spam

51. A virus or worm can have a payload that installs a(n) _____ door or trap door component in a system, which allows the attacker to access the system at will with special privileges.
ANSWER: back

52. A(n) _____ is an act against an asset that could result in a loss.
ANSWER: attack

53. A _____ overflow is an application error that occurs when the system can't handle the amount of data that is sent.
ANSWER: buffer

54. Explain the differences between a leader and a manager.
ANSWER: The distinctions between a leader and a manager arise in the execution of organizational tasks. A leader provides purpose, direction, and motivation to those that follow. By comparison, a manager administers the resources of the organization. He or she creates budgets, authorizes expenditures, and hires employees.

55. List and explain the critical characteristics of information as defined by the C.I.A. triad.
ANSWER: Confidentiality of information ensures that only those with sufficient privileges and a demonstrated need may access certain information. When unauthorized individuals or systems can view information, confidentiality is breached.
Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state.
Availability is the characteristic of information that enables user access to information without interference or obstruction and in a useable format.

56. List and explain the four principles of management under the contemporary or popular management theory. Briefly define each.

Chapter 01 - Introduction to the Management of Information Security

ANSWER: Popular management theory, which categorizes the principles of management into planning, organizing, leading, and controlling (POLC).
The process that develops, creates, and implements strategies for the accomplishment of objectives is called planning.
The management function dedicated to the structuring of resources to support the accomplishment of objectives is called organization.
Leadership includes supervising employee behavior, performance, attendance, and attitude. Leadership generally addresses the direction and motivation of the human resource.
Monitoring progress toward completion, and making necessary adjustments to achieve desired objectives, requires the exercise of control.

57. List the steps that can be used as a basic blueprint for solving organizational problems.

ANSWER:
1. Recognize and Define the Problem
2. Gather Facts and Make Assumptions
3. Develop Possible Solutions
4. Analyze and Compare Possible Solutions.
5. Select, Implement and Evaluate a Solution.

58. What are the three distinct groups of decision makers or communities of interest on an information security team?

ANSWER: Managers and professionals in the field of information security
Managers and professionals in the field of IT
Managers and professionals from the rest of the organization

59. List the specialized areas of security.

ANSWER:
Physical security
Operations security
Communications security
Network security

60. List the measures that are commonly used to protect the confidentiality of information.

ANSWER:
Information classification
Secure document (and data) storage
Application of general security policies
Education of information custodians and end users
Cryptography (encryption)

61. What is authentication? Provide some examples.

ANSWER: Authentication is the process by which a control establishes whether a user (or system) has the identity it claims to have. Examples include the use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections as well as the use of cryptographic hardware devices—for example, hardware tokens such as RSA's SecurID. Individual users may disclose a personal identification number (PIN) or a password to authenticate their identities to a computer system.

62. Discuss the planning element of information security.

ANSWER: Planning in InfoSec management is an extension of the basic planning model. Included in the InfoSec planning model are activities necessary to support the design, creation, and implementation of InfoSec strategies within the IT planning environment. The business strategy is translated into the IT strategy. Both the business strategy and the IT strategy are then used to develop the InfoSec strategy. For example, the CIO uses the IT objectives gleaned from the business unit plans to create the organization's IT strategy.

Chapter 01 - Introduction to the Management of Information Security

63. There are 12 general categories of threat to an organization's people, information, and systems. List at least six of the general categories of threat and identify at least one example of those listed.

ANSWER:

Compromises to intellectual property
Software attacks
Deviations in quality of service
Espionage or trespass
Forces of nature
Human error or failure
Information extortion
Missing, inadequate, or incomplete
Missing, inadequate, or incomplete controls
Sabotage or vandalism
Theft
Technical hardware failures or errors
Technical software failures or errors
Technological obsolescence