Chapter 02
General Security Concepts

Multiple Choice Questions

1. *(p. 21)* _____ places the focus on the security processes and the actual data.
A. Computer security
B. Network security
C. Information assurance
D. Communications security

Difficulty: Easy

2. *(p. 21)* The term which refers to the attempt to gain unauthorized access to systems and computers used by a telephone company to operate its telephone network is a _____.
A. phone hacker
B. hacktivist
C. commh@ck3r
D. phreaker

Difficulty: Easy

3. *(p. 22)* Jane is in the finance department. Although she should not be able to open files or folders from the marketing department, she can and does. This a problem of _____.
A. confidentiality
B. integrity
C. availability
D. authentication
E. nonrepudiation

Difficulty: Easy

4. *(p. 22)* Jane is in the finance department. Although she should not be able to modify files or folders from the marketing department, she can, and does. This a problem of _____.
A. confidentiality
B. integrity
C. availability
D. authentication
E. nonrepudiation

Difficulty: Easy

5. *(p. 22)* Bob inadvertently disconnects the cable from the company file server. This creates a problem of _____.
A. confidentiality
B. integrity
C. availability
D. authentication
E. nonrepudiation

Difficulty: Easy

6. *(p. 22)* Joe sends a scathing e-mail to his boss regarding increased work hours. Joe tries to deny sending the e-mail, but is unable to due to the use of digital signatures. This is an example of _____.
A. confidentiality
B. integrity
C. availability
D. authentication
E. nonrepudiation

Difficulty: Easy

7. *(p. 22)* Ensuring that and individual is who they claim to be is the function of _____.
A. confidentiality
B. integrity
C. availability
D. authentication
E. nonrepudiation

Difficulty: Easy

8. *(p. 22-23)* The incident response team reviewed the security logs and discovered that the network had been breached, due to a misconfigured firewall. This is a failure of which element of the operational model of computer security?
A. Protection
B. Prevention
C. Detection
D. Response

Difficulty: Medium

9. *(p. 22)* The operational model of security is _____.
A. Prevention = Protection + (Detection + Response)
B. Prevention = Protection + (Detection x Response)
C. Protection = Prevention + (Detection + Response)
D. Protection = Prevention + (Detection x Response)

Difficulty: Easy

10. *(p. 22-23)* A newly purchased server with a defect catches fire and all data on the device is lost. A backup was never performed. This is a failure of which element of the operational model of computer security?
A. Protection
B. Prevention
C. Detection
D. Response

Difficulty: Medium

11. *(p. 22-23)* The IDS fails to alert on an intruder's ping sweep and port scan. This is a failure of which element of the operational model of computer security?
A. Protection
B. Prevention
C. Detection
D. Response

Difficulty: Medium

12. *(p. 24)* Ensuring that users have access only to the files they need to complete their tasks is an example of which principle?
A. Separation of duties
B. Implicit deny
C. Least privilege
D. Keep it simple

Difficulty: Easy

13. *(p. 25)* Requiring one employee to place an order and another employee to authorize the sale is an example of which principle?
A. Least privilege
B. Separation of duties
C. Implicit deny
D. Keep it simple

Difficulty: Easy

14. *(p. 25)* A list of web sites that can be visited is created. Only sites that are on the list are allowed to be accessed. This is an example of which principle?
A. Least privilege
B. Separation of duties
C. Implicit deny
D. Keep it simple

Difficulty: Easy

15. *(p. 30)* Reducing the number of services to the least number necessary for it to properly perform its functions is an example of which principle?
A. Least privilege
B. Separation of duties
C. Implicit deny
D. Keep it simple

Services are functions, not privileges. Having fewer services on a computer reduces the complexity of the configuration.

Difficulty: Easy

16. *(p. 29)* A database server is put on the network by the for a project manager. No one is told it is there except for the project manager, so that he can work on it without worrying that other individuals will try to get to it. This is an example of which principle?
A. Layered defense
B. Job rotation
C. Diversity of defense
D. Security through obscurity

Difficulty: Easy

17. *(p. 28-29)* The network engineer suggests purchasing two firewalls from different companies so that a vulnerability affecting one type of firewall will not leave the entire network vulnerable. This is an example of which principle?
A. Layered defense
B. Job rotation
C. Diversity of defense
D. Security through obscurity

Difficulty: Easy

18. *(p. 26)* The database administrator falls ill and is not able to come to work for three weeks. No one else in the company knows how to administer the database server. This is a result of not following which principle?
A. Layered defense
B. Job rotation
C. Diversity of defense
D. Security through obscurity

Difficulty: Easy

19. *(p. 26-27)* The hacker was successful in breaching the firewall, the packet filtering router, and the internal firewall, but was quickly detected and unable to get past the workstation personal firewall. This is an example of what principle?
A. Layered security
B. Job rotation
C. Diversity of defense
D. Security through obscurity

Difficulty: Easy

20. *(p. 31)* Which of the following is not one of the three general methods used in authentication?
A. Something you have
B. Something you do
C. Something you are
D. Something you know

Difficulty: Easy

21. *(p. 33-34)* A person who tries to gradually obtain information necessary to compromise a network—by first appealing for help, and then, if necessary, by a more aggressive approach—is a(n) _____.
A. phreaker
B. social engineer
C. hacktivist
D. terrorist

Difficulty: Easy

22. *(p. 39)* John, who is in the development group, has admin passwords to both the development group files and the production group files. This might be a violation of which policy?
A. Due diligence
B. Due process
C. Need to know
D. Acceptable use

Difficulty: Easy

23. *(p. 38)* A company doing business online conducted all financial transactions over the Internet without any encryption. As a result, customer information such as credit card numbers, expiration dates, and the security codes found on the back of the credit cards was stolen. This is a violation of which policy?
A. Due diligence
B. Due process
C. Need to know
D. Acceptable use

Difficulty: Easy

24. *(p. 36-37)* Jane spends quite a bit of time on Facebook, and other social networking sites during work hours. This has resulted in reduced productivity. This is likely a violation of which policy?
A. Due diligence
B. E-mail policy
C. Need to know
D. Acceptable use

Difficulty: Easy

25. *(p. 38-39)* Rumors spread around the office that Mrs. Smith was stealing office supplies as well as talking badly about the senior management. This rumor eventually reached her boss, who then fired her. This is likely a violation of which policy?
A. Due diligence
B. Due process
C. Equal opportunity
D. Acceptable use

Difficulty: Easy

26. *(p. 40-42)* Background checks, drug testing, retirement, and termination are elements found in which type of policy?
A. Due diligence
B. Human resources
C. Equal opportunity
D. Privacy

Difficulty: Easy

27. *(p. 42-43)* Which of the following is a security model that addresses integrity?
A. Biba
B. Bell-LaPadula
C. Layered defense
D. Ring

Difficulty: Easy

28. *(p. 45)* Which of the following is a security model that uses transactions as the basis for its rules?
A. Biba
B. Bell-LaPadula
C. Layered defense
D. Clark-Wilson

Difficulty: Easy

29. *(p. 42-43)* The policies of the Biba model are
A. Ring (no read down) and Low-Water-Mark (no write up)
B. *-Property (no write down) and Simple Security Rule (no read up)
C. *-Property (no write up) and Simple Security Rule (no read down)
D. Ring (no read up) and Low-Water-Mark (no write down)

Difficulty: Easy

30. *(p. 42-43)* The policies of the Bell-LaPadula model are
A. Ring (no read down) and Low-Water-Mark (no write up)
B. *-Property (no write up) and Simple Security Rule (no read down)
C. Ring (no read up) and Low-Water-Mark (no write down)
D. *-Property (no write down) and Simple Security Rule (no read up)

Difficulty: Easy

True / False Questions

31. *(p. 21)* Computer security and information assurance are the same thing.
FALSE

Difficulty: Easy

32. *(p. 22)* The A in CIA refers to the term auditability.
FALSE

Difficulty: Easy

33. *(p. 22)* When files are modified by someone who is not authorized to do so, this is problem of confidentiality.
FALSE

Difficulty: Easy

34. *(p. 22)* Nonrepudiation means that the person who sends an e-mail will be unable to deny sending the e-mail.
TRUE

Difficulty: Easy

35. *(p. 22)* During the day, it takes an employee twice as long to retrieve files from the server that is under attack. The attack has resulted in a degradation of availability.
TRUE

If the employee is able to get the files, but it takes twice as long, it means that the employee can only get half as many files in a day.

Difficulty: Easy

36. *(p. 22)* Authentication means that the person who sends and e-mail will be unable to deny sending the e-mail.
FALSE

Difficulty: Easy

37. *(p. 22)* Auditability refers to whether a control can be verified as functioning or not.
TRUE

Difficulty: Easy

38. *(p. 22)* The formula for the operational model of computer security is Prevention = Protection + (Detection + Response)
FALSE

Difficulty: Easy

39. *(p. 23)* Access controls, firewalls, and encryption are technologies used for prevention.
TRUE

Difficulty: Easy

40. *(p. 23)* Audit logs, intrusion detection systems, and honeypots are technologies used for detection.
TRUE

Difficulty: Easy

41. *(p. 23)* Backups, incident response teams, and computer forensics are response technologies.
TRUE

Difficulty: Easy

42. *(p. 23)* Bob works in a small office with a network of computers. Bob, along with all the other employees, is responsible for securing his own computer on the network. This is an example of network security.
FALSE

Difficulty: Easy

43. *(p. 23)* Network security places the emphasis on controlling access to external resources from internal entities.
FALSE

Difficulty: Easy

44. *(p. 24)* Operating systems and applications all implement rights and permissions the same way.
FALSE

Difficulty: Easy

45. *(p. 25)* All applications, scripts, and batch files run in the same security context of the user who is logged in at the time.
TRUE

Difficulty: Easy

46. *(p. 25)* The concept of separation of duties applies to networks, but is inappropriate for physical environments.
FALSE

Difficulty: Easy

47. *(p. 27)* Making the effort to compromise a system more costly than the value of accomplishing it is the goal of security.
TRUE

Difficulty: Easy

48. *(p. 31)* Three means of establishing auditability: something you know, something you have, or something you are.
FALSE

Difficulty: Easy

49. *(p. 35)* A security procedure is a high-level statement produced by senior management that outlines both what security means to the organization and the organization's goals for security.
FALSE

Difficulty: Easy

50. *(p. 42)* The objective of the Bell-LaPadula security model is integrity.
FALSE

Difficulty: Easy

Fill in the Blank Questions

51. *(p. 34)* Gathering seemingly unimportant information and then combining it to discover potentially sensitive information is known as _____.
data aggregation

Difficulty: Medium

52. *(p. 22)* _____ is the condition that a control can be verified as functioning.
Auditability

Difficulty: Medium

53. *(p. 31)* Ensuring that an individual is who they claim to be before allowing them to access information they are authorized to access is _____.
authentication

Difficulty: Medium

54. *(p. 31)* The ability to manage whether a subject can interact with an object is called _____.
access control

Difficulty: Medium

55. *(p. 22)* To ensure that only those individuals who have authority to view a piece of information may do so is called _____.
confidentiality

Difficulty: Medium

56. *(p. 22)* Ensuring that changes made to the data are only done by users who are authorized to do so protects the data's _____.
integrity

Difficulty: Medium

57. *(p. 22)* _____ ensures that the data, or the system itself, is available for use when the authorized user wants it.
Availability

Difficulty: Medium

58. *(p. 22)* _____ deals with the ability to verify that a message has been sent and received and that the sender can be identified and verified.
Nonrepudiation

Difficulty: Medium

59. *(p. 23)* _____ security takes a granular view of security by focusing on protecting each computer and device individually instead of addressing protection of the network as a whole.
Host

Difficulty: Medium

60. *(p. 23)* _____ security places the emphasis on controlling access to internal computers from external entities.
Network

Difficulty: Medium

Essay Questions

61. *(p. 22)* In the context of information security, what does the acronym CIA stand for? Explain each term.

The goal of computer security has been threefold: confidentiality, integrity, and availability—the "CIA" of security. The purpose of *confidentiality* is to ensure that only those individuals who have the authority to view a piece of information may do so. No unauthorized individual should ever be able to view data they are not entitled to access. *Integrity* is a related concept but deals with the generation and modification of data. Only authorized individuals should be able to create or change (or delete) information. The goal of *availability* is to ensure that the data, or the system itself, is available for use when the authorized user wants it.

Difficulty: Hard

62. *(p. 23-30)* During a job interview you are asked to explain in what ways you would secure the company's information if you were hired. Using any three principles of security from the chapter, describe how you would secure their information.

The answer may include any three of the following:

Least privilege-This states that a subject (user, application, or process) should have only the necessary rights and privileges to perform its task with no additional permissions.
Separation of duties-This concept ensures that for any given task, more than one individual needs to be involved. This security concept is successful because no single individual can abuse the system for his or her own gain.
Implicit deny-If a particular situation is not covered by any of the rules, access cannot be granted.
Job rotation-This is the concept of the rotation of individuals through different tasks and duties in the organization's IT department.
Layered security-Different access controls and the utilization of various tools and devices are implanted within a security system on multiple levels.
Diversity of defense-A concept that involves making different layers of security dissimilar from each other in order to deter attacks; it complements the layered security principle.
Security through obscurity-This concept states that security is effective if the environment and protection mechanisms are confusing or supposedly not generally known.
Keep it simple-This concept implements the practice of keeping security processes and tools simple and elegant.

Difficulty: Hard

63. *(p. 32-40)* During a job interview you are asked to explain in what ways you would secure the company's information if you were hired. Using any three security policies from the chapter, describe how you would secure their information.

The answer may include any three of the following:

Acceptable use policy-This outlines what the organization considers to be the appropriate use of company resources, such as computer systems, e-mail, Internet usage, and networks.
Classification of information policy-This is the protection of the information processed and stored on computer systems and the network, which is a key component of IT security.
Due process policy-This concerns the guarantee of an individual's rights as outlined by the Constitution and Bill of Rights. Due process guarantees fundamental fairness, justice, and liberty in relation to an individual's rights.
Due care-This is the standard of care a reasonable person is expected to exercise in all situations.
Due diligence-This is the standard of care a business is expected to exercise in preparation for a business transaction.
Need to know policy-This concerns two security principles as guiding philosophies to an organization's security. These two principles are the need to know security principle and the least privilege security principle.
Disposal and destruction policy-This is an outline of the necessary methods of destroying discarded important or sensitive information so individuals from outside the company cannot access it after it is discarded.

Difficulty: Hard

64. *(p. 40-42)* Your boss is concerned with information security issues concerning new employees and employees who leave the company and would like your recommendations. Describe what human resources policies should be in place.

Hiring and promotions-It is becoming common for organizations to run background checks on prospective employees and to check the references prospective employees supply. Frequently, organizations require drug testing, check for any past criminal activity, verify claimed educational credentials, and confirm reported work history. For highly sensitive environments, special security background investigations can also be required.
Periodic reviews by supervisory personnel, additional drug checks, and monitoring of activity during work-If the organization chooses to implement any of these reviews, the company must specify them in the organization's policies, and prospective employees should be made aware of these policies before being hired.
Retirement, separation, or termination of an employee-When an employee decides to leave a company, generally as a result of a new job offer, continued access to sensitive information should be carefully considered. If the employee is leaving as a result of hard feelings toward the company, it might be wise to quickly revoke her access privileges. If she is leaving as a result of a better job offer, you may decide to allow her to transfer her projects gracefully to other employees, but the decision should be considered very carefully, especially if the new company is a competitor.
Mandatory vacations-From a security standpoint, an employee who never takes time off might be involved in nefarious activity, such as fraud or embezzlement, and might be afraid that if they leave on vacation, the organization will discover their illicit activities. As a result, requiring employees to use their vacation time through a policy of mandatory vacations can be a security protection mechanism.

Difficulty: Hard

65. *(p. 42-44)* Describe the Bell-LaPadula and Biba security models and the policies they use to protect information.

The *Bell-LaPadula* security model employs both mandatory and discretionary access control mechanisms when implementing its two basic security principles. The first of these principles is called the *Simple Security Rule*, which states that no subject (such as a user or a program) can read information from an object (such as a file) with a security classification higher than that possessed by the subject itself. This means that the system must prevent a user with only a Secret clearance, for example, from reading a document labeled Top Secret. This rule is often referred to as the "no-read-up" rule. The second security principle enforced by the Bell-LaPadula security model is known as the **-property* (pronounced "star property"). This principle states that a subject can write to an object only if its security classification is less than or equal to the object's security classification.
The *Biba* security model implements a hybrid of the Ring and Low-Water-Mark policies. Biba's model, in many respects, is the opposite of the Bell-LaPadula model in that what it enforces are "no-read-down" and "no-write-up" policies. It also implements a third rule that prevents subjects from executing higher-level programs. The Biba security model thus addresses the problems mentioned with both the Ring and Low-Water-Mark policies.

Difficulty: Hard