Practice Questions with Solutions

Chapter 1

1. What is the correct approach for addressing security and organization objectives?

   a. Security and organization objectives should be developed separately.

   b. Security should drive organization objectives.

   c. Security should support organization objectives.

   d. The site security officer should approve or reject organization objectives.

2. The statement, "Promote professionalism among information system security practitioners through the provisioning of professional certification and training" is an example of a/an:

   a. Mission statement

   b. Objective

   c. Goal

   d. Requirement

3. The two components of risk management are:

   a. Risk assessment and risk analysis

   b. Vulnerability assessment and risk treatment

   c. Risk assessment and risk mitigation

   d. Risk assessment and risk treatment

4. A security manager needs to perform a risk assessment on a critical business application in order to determine what additional controls may be needed to protect the application and its databases. The best approach to performing this risk assessment is:

   a. Perform a qualitative risk assessment only

   b. Perform a quantitative risk assessment only

   - **c. Perform a qualitative risk assessment first, then perform a quantitative risk assessment**
   - d. Perform a quantitative risk assessment, then perform a qualitative risk assessment

5. A qualitative risk assessment is used to identify:
   - a. Vulnerabilities, threats, and countermeasures
   - **b. Vulnerabilities, threats, threat probabilities, and countermeasures**
   - c. Assets, risks, and mitigation plans
   - d. Vulnerabilities and countermeasures

6. The impact of a specific threat is defined as:
   - a. The cost of recovering the asset
   - b. The cost required to protect the related asset
   - **c. The effect of the threat if it is realized**
   - d. The loss of revenue if it is realized

7. *Exposure factor* is defined as:
   - **a. The part of an asset's value that is likely to be lost by a particular threat**
   - b. The probability that the threat will be realized
   - c. The probability that a loss will occur in a year’s time
   - d. The cost of a single loss

8. A security manager is performing a quantitative risk assessment on a particular asset. The security manager wants to determine the quantitative loss for a single loss based on a particular threat. The correct way to calculate this is:
   - a. Divide the asset’s value by the exposure factor
   - b. Multiply the asset’s value times the annualized rate of occurrence
   - c. Multiply the asset’s value times the single loss expectancy
   - **d. Multiply the asset’s value times the exposure factor**

9. A security manager is performing a quantitative risk assessment on a particular asset. The security manager wants to estimate the yearly loss based on a particular threat. The correct way to calculate this is:

a. Multiply the single loss expectancy times the asset’s value

b. Multiply the asset’s value times the exposure factor

c. Multiply the asset’s value times the exposure factor times the single loss expectancy

d. Multiply the single loss expectancy times the annualized rate of occurrence

10. Annualized loss expectancy is defined as:

a. The annual estimate of loss of all assets based on all threats

b. The annual estimate of loss of an asset based on a single threat

c. The annual estimate of loss of an asset based on all threats

d. The annual estimate of loss of all assets based on a single threat

11. Annualized loss expectancy is calculated using which formula:

a. ALE = ARO x SLE

b. ALE = EF x SLE

c. ALE = ARO x AV

d. ALE = ARO / SLE

12. A risk manager has completed a risk analysis for an asset valued at $4000. Two threats were identified; the ALE for one threat is $400, and the ALE for the second threat is $500. What is the amount of loss that the organization should estimate for an entire year?

a. $450

b. $500

c. $900

d. $100

13. The options for risk treatment are:

a. Risk reduction, risk assumption, risk avoidance, and risk acceptance

b. Risk acceptance, risk reduction, risk transfer, and risk mitigation

c. Risk acceptance, risk reduction, and risk transfer

d. Risk acceptance, risk avoidance, risk reduction, and risk transfer

14. An organization recently completed a risk assessment. Based on the findings in the risk assessment, the organization chose to purchase insurance to cover possible losses. This approach is known as:

    a. Risk transfer

    b. Risk avoidance

    c. Risk acceptance

    d. Risk reduction

15. After completing a risk assessment, an organization was able to reduce the risk through the addition of detective and preventive controls. However, these controls did not remove all risk. What options does the organization have for treating the remaining risk?

    a. Accept, avoid, reduce, or transfer

    b. None—the organization must accept the risk

    c. The organization must either accept or transfer the risk

    d. Does not apply: remaining risk cannot be treated further

16. A security door has been designed so that it will ignore signals from the building’s door entry system in the event of a power failure. This is known as:

    a. Fail soft

    b. Fail open

    c. Fail closed

    d. Fail secure

17. CIA is known as:

    a. Confidentiality, Integrity, and Availability

    b. Computers, Information, and Assets

    c. Confidence In Applications

    d. Controls, Integrity, and Availability

18. An organization suffered a virus outbreak when malware was downloaded by an employee in a spam message. This outbreak might not have happened had the organization followed what security principle:

    a. Heterogeneity

b. Fortress

c. Integrity

d. Defense in depth

19. An organization has a strong, management-driven model of security-related activities such as policy, risk management, standards, and processes. This model is better known as:

a. Risk management

b. Security oversight

c. Security governance

d. Security control

20. The statement, “Information systems should be configured to require strong passwords,” is an example of a/an:

a. Security requirement

b. Security policy

c. Security objective

d. Security control

21. An organization wishes to purchase an application and is undergoing a formal procurement process to evaluate and select a product. What documentation should the organization use to make sure that the application selected has the appropriate security-related characteristics?

a. Security guidelines

b. Security policies

c. Security requirements

d. Functional requirements

22. A security manager is developing a data classification policy. What elements need to be in the policy?

a. Sensitivity levels, marking procedures, access procedures, and handling procedures

b. Labeling procedures, access procedures, and handling procedures

c. Sensitivity levels, access procedures, and handling procedures

d. Sensitivity levels and handling procedures

23. An employee with a previous criminal history was terminated. The former employee leaked several sensitive documents to the news media. To prevent this, the organization should have:

    a. Reviewed access logs

    b. Restricted the employee’s access to sensitive information

    c. Obtained a signed non-disclosure statement

    d. Performed a background verification prior to hiring the employee

24. An organization recently underwent an audit of its financial applications. The audit report stated that there were several segregation-of-duties issues that were related to IT support of the application. What does this mean?

    a. IT personnel should not have access to financial data.

    b. The duties of personnel are not formally defined.

    c. IT needs to begin the practice of job rotation.

    d. Individuals in IT have too many roles or privileges.

25. An organization employs hundreds of office workers that use computers to perform their tasks. What is the best plan for informing employees about security issues?

    a. Include security policy in the employee handbook

    b. Perform security awareness training at the time of hire and annually thereafter

    c. Perform security awareness training at the time of hire

    d. Require employees to sign the corporate security policy

Chapter 2

26. An information system that processes sensitive information is configured to require a valid userid and strong password from any user. This process of accepting and validating this information is known as:

    a. Authentication

    b. Strong authentication

    c. Two-factor authentication

    d. Single sign-on

27. The reason that two-factor authentication is preferable over ordinary authentication is:

    a. Two-factor authentication is more difficult to crack

    b. It relies upon something the user knows

    c. It relies upon something that the user has

    d. Two-factor authentication uses stronger encryption algorithms

28. When an information system authenticates a user based on “what the user is,” this refers to the use of:

    a. Authorization based upon the user’s job title

    b. Role-based authentication

    c. Two-factor authentication

    d. Biometric authentication

29. In an information system that authenticates users based on userid and password, the primary reason for storing a hash of the password instead of storing the encrypted password is:

    a. No one, even system administrators, can derive the password

    b. Hashing algorithms are less CPU-intensive than encryption algorithms

    c. Hashed passwords require less storage space than encrypted passwords

    d. Support personnel can more easily reset a user’s password when it is hashed

30. The primary reason why users are told to use strong passwords is NOT:

    a. It is more difficult to “shoulder surf” a strong password because of the additional keystrokes

    b. Strong passwords are more difficult for others to guess

    c. Weak passwords are susceptible to dictionary attacks

    d. Passwords based on easily-discovered facts such as birthdays, spouse and pet names are easily guessed

31. One disadvantage of the use of digital certificates as a means for two-factor authentication is NOT:

    a. Digital certificates may not be portable across different types of machines

b. The password used to unlock the certificate may be weak and easily guessed

c. It may be possible to steal the certificate and use it on another computer

d. A digital certificate can theoretically be copied, unlike tokens and smart cards which are not easily cloned

32. A smart card is a good form of two-factor authentication because:

a. It contains a certificate on a microchip that is resistant to cloning or cracking

b. It can double as a proximity card for building entrance key card systems

c. It does not rely on internal power like a token

d. A smart card is portable and can be loaned to others

33. Organizations that implement two-factor authentication often do not adequately plan. One result of this is:

a. Some users will lose their tokens, smart cards, or USB keys

b. Some users will store their tokens, smart cards, or USB keys with their computers, thereby defeating one of the advantages of two-factor authentication

c. Users will have trouble understanding how to use two-factor authentication

d. The cost of implementation and support can easily exceed the cost of the product itself

34. Palm scan, fingerprint scan, and iris scan are forms of:

a. Strong authentication

b. Two-factor authentication

c. Biometric authentication

d. Single sign-on

35. A biometric authentication system that incorporates the results of newer scans into a user’s profile is less likely to:

a. Have a lower False Accept Rate

b. Reject future authentication attempts as the user's biometrics slowly change over time

c. Correctly identify and authenticate users

d. Reject an impostor

36. The use of retina scanning as a biometric authentication method has not gained favor because:

a. It is inconvenient to use retina scanning in a darkened room

b. Many users cannot hold their eye open long enough for a scan to complete

c. Users are uncomfortable holding their eye very near the biometric scanning device

d. The human retina changes significantly over time

37. Voice recognition as a biometric authentication method is difficult to measure because:

a. Many factors, including current health and respiration rate, make sampling difficult

b. Computers are not yet fast enough to adequately sample a voice print

c. Voice recognition does not handle accents well

d. Impatience changes voice patterns, which leads to increased False Reject Rates

38. Which of the following statements about Crossover Error Rate (CER) is true:

a. This is the point where the False Accept Rate falls below 50%

b. This is the point where the False Reject Rate falls below 50%

c. This is the point where False Reject Rate and False Accept Rate add to 100%

d. This is the point where False Reject Rate and False Accept Rate are equal

39. A security engineer has recently installed a biometric system, and needs to tune it. Currently the biometric system is rejecting too many valid, registered users. What adjustment does the security engineer need to make?

a. Increase the False Accept Rate

b. Reduce the False Accept Rate

c. Increase the False Reject Rate

d. Reduce the False Reject Rate

40. A security engineer is soliciting bids for a software product that will perform centralized authentication. The engineer has found two products so far: one that is based on LDAP and one that is based on TACACS. Which of the following statements is the best approach?

a. Select the LDAP-based product

b. Do not consider the TACACS-based product, consider the LDAP-based product, and continue looking for other products

c. Select the TACACS-based product

d. Consider the TACACS-based product, and continue looking for other products based on TACACS

41. Which of the following is NOT an authentication protocol:

a. Lightweight Directory Authentication Protocol

b. Diameter

c. RADIUS

d. Lightweight Directory Access Protocol

42. An intruder wishes to break in to an application in order to steal information stored there. Because the application utilizes strong authentication, what is the most likely approach the intruder will take?

a. Dictionary attack

b. Malicious code attack

c. Application bypass attack

d. Password guessing attack

43. Authentication, encryption, and ACLs are examples of:

a. Defense in depth

b. Detective controls

c. Administrative controls

d. Technical controls

44. The categories of controls are:

   a. Detective, deterrent, preventive, corrective, recovery, and compensating

   b. Detective, preventive, and deterrent

   c. Technical, logical, and physical

   d. Detective, preventive, recovery, and compensating

45. Video surveillance is an example of what type(s) of control:

   a. Detective and deterrent

   b. Detective only

   c. Deterrent only

   d. Preventive

46. Buffer overflow, SQL injection, and stack smashing are examples of:

   a. Vulnerabilities

   b. Exploits

   c. Input attacks

   d. Injection attacks

47. An organization is surplussing its old desktop computers. Being concerned with data remanence, what measures should the organization take first?

   a. Erase the hard drives

   b. Format the hard drives

   c. Activate its TEMPEST shielding

   d. Clear the computers' RAM

48. What is the best defense against social engineering?

   a. Spyware filters

   b. Firewalls

   c. Data leakage protection (DLP)

   d. Security awareness training

49. Signs, guards, guard dogs, and visible notices are examples of:

a. Administrative controls

b. Preventive controls

c. Deterrent controls

d. Detective controls

50. The reason preventive controls are preferred over detective controls is:

a. Preventive controls are less costly

b. Detective controls do not actually stop unwanted activity

c. Detective controls require more resources

d. Preventive controls are do not detect unwanted activity

Chapter 3

51. One reason an organization would consider a distributed application is:

a. Some components are easier to operate

b. Distributed applications have a simpler architecture than other types of applications

c. Some application components are owned and operated by other organizations

d. Distributed applications are easier to secure

52. All of the following are advantages of using self-signed SSL certificates EXCEPT:

a. Server authentication

b. Lower cost

c. Easier to create

d. More difficult to crack

53. The best defense against a NOP sled attack is:

a. Firewall

b. Anti-virus

c. The strcpy() function

d. Input boundary checking

54. The instructions contained with an object are known as its:

a. Class

b. Firmware

c. Code

d. Method

55. The purpose for putting a “canary” value in the stack is:

a. To detect a dictionary attack

b. To detect a stack smashing attack

c. To detect parameter tampering

d. To detect script injection

56. “Safe languages” and “safe libraries” are so-called because:

a. They automatically detect some forms of input attacks

b. They automatically detect parameter tampering

c. They automatically detect script injection

d. They automatically detect malware attacks

57. The following are characteristics of a computer virus EXCEPT:

a. Polymorphic

b. Downloadable

c. Self-propagating

d. Embedded in spam

58. Rootkits can be difficult to detect because:

a. They are encrypted

b. They are polymorphic

c. They reside in ROM instead of the hard drive

d. They use techniques to hide themselves

59. An attack on a DNS server to implant forged “A” records is characteristic of a:

a. **Pharming attack**

b. Phishing attack

c. Whaling attack

d. Spim attack

60. The purpose of digitally signing a Browser Helper Object (BHO) is:

a. **To prove its origin**

b. To prove that it is not malicious

c. To prove that it can be trusted

d. To prove that it was downloaded properly

61. An organization wants to prevent SQL and script injection attacks on its Internet web application. The organization should implement a/an:

a. Intrusion detection system

b. Firewall

c. **Application firewall**

d. SSL certificate

62. A defense-in-depth strategy for anti-malware is recommended because:

a. **There are many malware attack vectors**

b. Anti-virus software is often troublesome on end user workstations

c. Malware can hide in SSL transmissions

d. Users can defeat anti-malware on their workstations

63. The primary advantage of the use of workstation-based anti-virus is:

a. Virus signature updates can be performed less often

b. Virus signature updates can be performed more often

c. The user can control its configuration

d. **This approach can defend against most, if not all, attack vectors**

64. The primary purpose of a firewall is:

a. To protect a server from malicious traffic

b. To block malicious code

c. **To control traffic between networks**

d. To create a DMZ network

65. The following are valid reasons to reduce the level of privilege for workstation users EXCEPT:

a. Decreased support costs because users are unable to change system configurations

b. **Decreased need for whole disk encryption**

c. Decreased impact from malware

d. Increased security because users are unable to tamper with security controls

66. A system administrator needs to harden a server. The most effective approach is:

a. Install security patches and install a firewall

b. Remove unneeded services, remove unneeded accounts, and configure a firewall

c. **Remove unneeded services, disable unused ports, and remove unneeded accounts**

d. Install security patches and remove unneeded services

67. The most effective countermeasures against input attacks are:

a. **Input field filtering, application firewall, application vulnerability scanning, and developer training**

b. Input field filtering, application firewall, and intrusion prevention system

c. Input field filtering, application firewall, intrusion detection system, and ethical hacking

d. Application firewall, intrusion detection system, and developer training

68. The term “object reuse” refers to:

a. A method used by malware to exploit weaknesses in running processes

b. The use of residual computing resources for other purposes

c. The ability to reuse application code

   d. Processes that can discover and use residual data associated with other processes

69. A security assessment discovered back doors in an application, and the security manager needs to develop a plan for detecting and removing back doors in the future. The most effective countermeasures that should be chosen are:

    a. Application firewalls

    b. Source code control

    c. Outside code reviews

    d. Peer code reviews

70. The best time to introduce security into an application is:

    a. Implementation

    b. Design

    c. Development

    d. Testing

71. A user, Bill, has posted a link on a web site that causes unsuspecting users to transfer money to Bill if they click the link. The link will only work for users who happen to be authenticated to the bank that is the target of the link. This is known as:

    a. Cross site request forgery

    b. Cross-site scripting

    c. Broken authentication

    d. Replay attack

72. What is the most effective countermeasure against script injection attacks?

    a. Stateful inspection firewall

    b. Disallow server-side scripting in the end user’s browser configuration

    c. Filter scripting characters in all input fields

    d. Disallow client-side scripting in the end user’s browser configuration

73. A database administrator (DBA) is responsible for carrying out security policy, which includes controlling which users have access to which data. The DBA has been asked to make just certain fields in some database tables visible to some new users. What is the best course of action for the DBA to take?

    a. Implement column-based access controls

    b. Export the table to a data warehouse, including only the fields that the users are permitted to see

    c. Clone the table, including only the fields that the users are permitted to see

    d. Create a view that contains only the fields that the users are permitted to see

74. The purpose of Data Control Language is:

    a. Define which users are able to view and manipulate data in a database

    b. Define data structures in a relational database

    c. Define data structures in an object-oriented database

    d. Retrieve, insert, delete and update data in a relational database

75. A list of all of the significant events that occur in an application is known as:

    a. Audit log

    b. Replay log

    c. Export file

    d. Data dump

Chapter 4

76. The primary reason for classifying disasters as natural or man-made is:

    a. To correctly determine their probable impact

    b. To correctly determine their probability of occurrence

    c. To classify different types of events to better understand them

    d. To determine which contingency plans need to be carried out

77. For the purpose of business continuity and disaster recovery planning, the definition of a "disaster" is:

    a. **Any event that impairs the ability of an organization to continue operating**

    b. Any natural event that impairs the ability of an organization to continue operating

    c. Any man-made event that impairs the ability of an organization to continue operating

    d. Any event that impairs the ability of an organization's IT systems to continue operating

78. The primary impact of a pandemic on an organization is:

    a. Significant disruptions of public utilities

    b. Significant disruptions of transportation systems

    c. Large numbers of casualties that reduce the demand for services

    d. **Long periods of employee absenteeism that impact the organization's ability to provide services**

79. The activity that is concerned with the continuation of business operations is:

    a. Emergency Response Procedures

    b. Disaster Recovery Planning

    c. **Business Continuity Planning**

    d. Business Impact Analysis

80. The main reason that a DRP project should have executive support and approval is:

    a. A DRP project is very expensive

    b. **A DRP project requires significant adjustments in the allocation of resources**

    c. A DRP project requires the redesign of all in-scope IT systems

    d. A DRP project requires the redesign of all in-scope business processes

81. An organization is about to start its first disaster recovery planning project. The project manager is responsible for choosing project team members. Which staff members should be chosen for this project?

a. The project should use outsourced technical experts

b. The least experienced team members

c. The most experienced team members

d. The project should use outsourced disaster recovery planning experts

82. At the beginning of a disaster recovery planning project, the project team will be compiling a list of all of the organization's most important business processes. This phase of the project is known as:

a. Business Impact Analysis

b. Risk Analysis

c. Business Process Analysis

d. Determination of maximum tolerable downtime (MTD)

83. In what sequence should a disaster recovery planning project be performed?

a. Business Impact Analysis, Maximum Tolerable Downtime, Recovery Point Objective, Recovery Time Objective, training, testing

b. Survey business processes, threat and risk analysis, develop recovery targets, criticality analysis

c. Project plan, risk assessment, statements of impact, criticality analysis, recovery targets, test recovery plans

d. Project plan, Business Impact Analysis, develop recovery plans, train personnel, test recovery plans

84. Benefits from disaster recovery and business continuity planning include all of the following EXCEPT:

a. Improved system resilience

b. Process improvements

c. Improved market advantage

d. Improved performance

85. The types of BCP and DRP tests are:

a. Document review, walkthrough, parallel test, cutover test

b. Document review, walkthrough, simulation, parallel test, cutover test

c. Document review, walkthrough, sanity test, parallel test, cutover test

d. Walkthrough, simulation, parallel test, cutover test, live test

86. The purpose of a cutover test is:

a. To determine the ability to perform live business transactions on backup systems instead of on production systems

b. To determine the ability for a recovery test to be interrupted

c. To determine the ability to perform live business transactions on production systems and backup systems at the same time

d. To determine the ability for the last minute substitution of a recovery team

87. The purpose of a parallel test is:

a. To determine the ability to perform live business transactions on backup systems instead of on production systems

b. To determine the ability for a recovery test to be interrupted

c. To determine the ability to perform live business transactions on production systems and backup systems at the same time

d. To determine the ability for the last minute substitution of a recovery team

88. The greatest risk related to a cutover test is:

a. If backup servers do not function correctly, the test will fail

b. A cutover test tests only the live load and not the switchover

c. A cutover test tests only the switchover and not the live load

d. If backup servers do not function correctly, critical business processes may fail

89. A project team has just completed building the organization’s business continuity plan. Which of the following tests should be performed first?

a. Walkthrough

b. Simulation

c. Parallel test

d. Cutover test

90. An organization that is building a disaster recovery capability needs to re-engineer its application servers to meet new recovery requirements of 40-hour RPO and 24-hour RTO. Which of the following approaches will best meet this objective?

    a. Active/Passive server cluster with replication

    b. Tape backup and restore to a hot site

    c. Tape backup and restore to a cold site

    d. Server cluster with shared storage

91. The purpose of a server cluster includes all of the following EXCEPT:

    a. Improve an application's availability

    b. Increase an application's capacity

    c. Increase an application's data storage

    d. Provide fault tolerance

92. The purpose of off-site media storage is:

    a. To protect media from damage in the event of a disaster

    b. To protect media from theft

    c. To provide additional storage not available on-site

    d. To meet regulatory requirements for media protection

93. An organization that is performing a disaster recovery planning project has determined that it needs to have on-site electric power available for as long as ten days, in the event of an electric utility failure. The best approach for this requirement is:

    a. Uninterruptible power supply (UPS) and power distribution unit (PDU)

    b. Electric generator

    c. Uninterruptible power supply (UPS)

    d. Uninterruptible power supply (UPS) and electric generator

94. The first priority for disaster response should be:

    a. Backup media

    b. Paper records

c. Personnel safety

d. Remote access

95. Which of the following would NOT be on a list of parties to notify in the event of a disaster-related emergency:

a. Civil authorities

b. Utilities

c. Shareholders

d. Customers

96. Why is disaster recovery-related training a vital component in a DRP project?

a. The plan will be able to be certified

b. Recovery is performed by outside organizations

c. The personnel who are most familiar with systems may be unavailable during a disaster

d. Personnel may be unfamiliar with recovery procedures

97. Why is it important to understand the cost of downtime of critical business processes?

a. Management will be able to make decisions about the cost of mitigating controls and contingency plans

b. Management will be able to determine which processes are the most critical

c. Management will be able to establish a training budget

d. Management will be able to compare recovery costs with those in similar organizations

98. The definition of Recovery Point Objective (RPO) is:

a. The location of the recovery site

b. The maximum amount of downtime

c. The method used to recover backup data

d. The maximum amount of data loss

99. The definition of Recovery Time Objective (RTO) is:

a. The location of the recovery site

b. The maximum amount of downtime

c. The method used to recover backup data

d. The maximum amount of data loss

100. A DRP project team has determined that the RTO for a specific application shall be set to 180 minutes. Which option for a recovery system will best meet the application's recovery needs?

a. Hot standby systems and tape recovery

b. Server clustering and data replication

c. Warm standby systems and tape recovery

d. Cold site and tape recovery

Chapter 5

101. The process of transforming ciphertext to plaintext is known as:

a. Decryption

b. Encryption

c. Key recovery

d. Hashing

102. Which of the following statements is true about the Vernam cipher?

a. It is a polyalphabetic cipher

b. It is a running-key cipher

c. The encryption key is used for only one message

d. Another name for it is a one-time hash

103. What is the minimum key length for a one-time pad?

a. 128 bits

b. 64 bits

c. 56 bits

d. The length of the plaintext message

104. All of the following statements about the polyalphabetic cipher are true EXCEPT:

a. It is a form of one-time pad

b. It is resistant to frequency analysis attacks

c. It uses multiple substitution alphabets

d. It is a type of substitution cipher

105. A running-key cipher can be used when:

a. The plaintext is longer than the encryption key

b. The plaintext is shorter than the encryption key

c. The plaintext is streaming media

d. The plaintext is changing rapidly

106. In modulo arithmetic, when A – B < 0, then:

a. 26 is subtracted from the result

b. 100 is added to the result

c. 26 is added to the result

d. 32 is added to the result

107. A computer user is listening to an audio broadcast on the Internet through an SSL VPN. The type of encryption cipher used in this case is:

a. Block cipher

b. Stream cipher

c. Running key cipher

d. Vernam cipher

108. In an electronic codebook (ECB) cipher, each block of ciphertext:

a. Is used to encrypt the next block

b. Is used to encrypt the previous block

c. Is used to decrypt the next block

d. Is not used to encrypt the next block

109. The encryption mode where ciphertext output from each encrypted plaintext block in the encryption used for the next block is known as:

a. Cipher feedback

b. Output feedback

c. Cipher block chaining

d. Electronic codebook

110. Public key cryptography is another name for:

a. Secure Sockets Layer

b. Asymmetric cryptography

c. Symmetric key cryptography

d. Kerberos

111. Public key cryptography is so-named because:

a. It is the world standard for HTTPS

b. It works on all popular computer operating systems

c. It uses an encryption key that can be released to the public

d. The encryption algorithms reside in the public domain

112. A security manager is searching for an encryption algorithm to be used to encrypt data files containing sensitive information. Which of the following algorithms should NOT be considered:

a. FISH

b. Twofish

c. Blowfish

d. CAST

113. A particular encryption algorithm transforms plaintext to ciphertext by XORing the plaintext with the encryption key. This is known as:

a. Electronic codebook

b. Cipher block chaining

c. Block cipher

d. Stream cipher

114. Two parties that have never communicated before wish to send messages using symmetric encryption key cryptography. How should the parties begin?

a. The receiving party should send its public encryption key to the transmitting party.

b. Each party should exchange public encryption keys.

c. Each party should send the encryption key via the communications channel to the other party.

d. One party should transmit the encryption key via an out of band communications channel to the other party.

115. Two parties that have never communicated before wish to send messages using asymmetric key cryptography. How should the parties begin?

a. The receiving party should send its private encryption key to the transmitting party.

b. The transmitting party should send its private encryption key to the receiving party.

c. The receiving party should send its public encryption key to the transmitting party.

d. The transmitting party should send its public encryption key to the receiving party.

116. Two parties, Party A and Party B, regularly exchange messages using public key cryptography. One party, Party A, believes that its private encryption key has been compromised. What action should Party B take?

a. Request a new public key from Party A.

b. Request a new private key from Party A.

c. Send a new public key to Party A.

d. Send a new private key to Party A.

117. The Advanced Encryption Standard is another name for which cipher:

a. Digital Encryption Algorithm (DEA)

b. 3DES

c. Rijndael

d. International Data Encryption Algorithm (IDEA)

118. The Data Encryption Standard:

a. Is used by Secure Sockets Layer (SSL) encryption

b. Has been replaced by the International Data Encryption Algorithm (IDEA)

c. Uses a 64-bit encryption key

d. Uses a 56-bit encryption key

119. Two parties are exchanging messages using public key cryptography. Which of the following statements describes the proper procedure for transmitting an encrypted message?

a. The sender encrypts the message using the recipient’s public key, and the recipient decrypts the message using the recipient’s private key.

b. The sender encrypts the message using the sender’s public key, and the recipient decrypts the message using the recipient’s public key.

c. The sender encrypts the message using the sender’s private key, and the recipient decrypts the message using the recipient’s private key.

d. The sender encrypts the message using the sender’s public key, and the recipient decrypts the message using the sender’s public key.

120. A stream cipher encrypts data by XORing plaintext with the encryption key. How is the ciphertext converted back into plaintext?

a. XORing it with the encryption key

b. XORing it with the inverse of the encryption key

c. ANDing it with the encryption key

d. NANDing it with the encryption key

121. The purpose of digitally signing a message is to ensure:

a. Integrity of the sender

b. Confidentiality of the message

c. Authenticity of the sender

d. Confidentiality of the sender

122. The purpose of digitally signing a message is to ensure:

a. Integrity of the message

b. Confidentiality of the message

c. Integrity of the sender

d. Confidentiality of the sender

123. The purpose of the Diffie-Hellman key exchange protocol is:

a. To decrypt a symmetric encryption key

b. To encrypt a symmetric encryption key

c. To permit two parties who have never communicated to establish public encryption keys

d. To permit two parties who have never communicated to establish a secret encryption key

124. An attacker is attempting to learn the encryption key that is used to protect messages being sent between two parties. The attacker is able to create his own messages, get them encrypted by one of the parties, and can then examine the ciphertext for his message. This type of attack is known as:

a. Ciphertext only attack

b. Chosen ciphertext attack

c. Chosen plaintext attack

d. Man in the middle attack

125. Which is the best approach for two parties who wish to establish a means for confirming the confidentiality and integrity of messages that they exchange:

a. Digital signatures

b. Encryption and digital signatures

c. Key exchange

d. Encryption

Chapter 6

126. The categories of laws in the U.S. are:

a. Civil, criminal, administrative, and family

b. Intellectual, privacy, and computer crime

c. Criminal, civil, and administrative

d. Criminal, civil, and family

127. Trademarks, copyrights, and patents are all a part of:

a. Intellectual property law

b. Civil law

c. Administrative law

d. Private property law

128. An organization has developed a new type of printer. What approach should the organization take to protect this invention?

a. Trade secret

b. Copyright

c. Trademark

d. Patent

129. A financial services organization is required to protect information about its customers. Which of these laws requires this protection:

a. HIPAA

b. COPPA

c. CALEA

d. GLBA

130. A suspect has been forging credit cards with the purpose of stealing money from their owners through ATM withdrawals. Under which U.S. law is this suspect most likely to be prosecuted?

a. Computer Fraud and Abuse Act

b. Access Device Fraud

c. Computer Security Act

d. Sarbanes-Oxley Act

131. Which U.S. law gives law enforcement organizations greater powers to search telephone, e-mail, banking, and other records?

a. Patriot Act

b. Communications Assistance for Law Enforcement Act

c. Federal Information Security Management Act

d. Gramm-Leach-Bliley Act

132. The Payment Card Industry Data Security Standard (PCI DSS) requires encryption of credit card in which circumstances:

a. Stored in databases, stored in flat files, and transmitted over public and private networks

b. Stored in databases, and transmitted over public networks

c. Stored in databases, stored in flat files, and transmitted over public networks

d. Stored in databases, and transmitted over public and private networks

133. A security incident as defined as:

a. Unauthorized entry

b. Exposure of sensitive information

c. Theft of sensitive information

d. Violation of security policy

134. The phases of a comprehensive security incident plan are:

a. Declaration, triage, investigation, analysis, containment, recovery, debriefing

b. Investigation, analysis, containment, recovery, debriefing

c. Declaration, triage, containment, recovery, debriefing

d. Declaration, triage, investigation, analysis, documentation, containment, recovery, debriefing

135. A security manager has discovered that sensitive information stored on a server has been compromised. The organization is required by law to notify law enforcement. What should the security manager do first to preserve evidence on the server:

a. Disconnect power to the server

b. Back up the server

c. Shut down the server

d. Activate debug mode

136. All of the following statements about a security incident plan are correct EXCEPT:

a. The plan should be tested annually

b. The plan should be reviewed annually

c. The plan should be published annually

d. Training on plan procedures should be performed annually

137. The purpose of a security incident debrief is all of the following EXCEPT:

a. Review of log files

b. Review of technical architecture

c. Review of operational procedures

d. Review of technical controls

138. Why would a forensic examiner wish to examine a computer's surroundings during a forensic investigation?

a. Evaluate cleanliness

b. Interrogate the suspect

c. Search for DNA evidence

d. Search for any removable media and documents

139. A case of employee misconduct that is the subject of a forensic investigation will likely result in a court proceeding. What should included in the forensic investigation:

a. Legible notes on all activities

b. Law enforcement investigation

c. Chain of custody for all evidence

d. Dual custody for all evidence

140. The (ISC)² code of ethics includes all of the following EXCEPT:

a. Provide diligent and competent service to principals

b. Protect society and the infrastructure

c. Act honorably, honestly, justly, responsibly, and legally

d. Advance and protect the profession

141. A security manager has been asked to investigate employee behavior on the part of a senior manager. The investigation has shown that the subject has suffered a serious lapse in judgment and has violated the organization's code of conduct. The security manager has been asked to keep the results of the investigation a secret. How should the security manager respond?

a. Leak the results of the investigation to the media

b. Cover up the results of the investigation

c. Deliver the results of the investigation and recommendations for next steps to his superiors

d. Notify law enforcement

142. A forensics investigator has been asked to examine the workstation used by an employee who has been known to misbehave in the past. This investigation is related to more potential misconduct. What approach should the investigator take in this new investigation?

a. Approach this investigation objectively, without regard to the history of this employee's conduct

b. Approach this investigation subjectively, given the history of this employee's conduct

c. Assume the employee is guilty and search for evidence to support this

d. Assume the employee is innocent and search for evidence to refute this

143. The allegation that an employee has violated company policy by downloading child pornography onto a company workstation should result in:

a. Notification of affected customers

b. Termination of the employee

c. The declaration of a security incident

d. A forensic investigation and possible disciplinary action

144. An organization has developed its first-ever computer security incident response procedure. What type of test should be undertaken first?

a. Parallel test

b. Simulation

c. Walkthrough

d. Document review

145. An organization’s security incident management strategy consists of response procedures to be used when an incident occurs. What other measures should the organization undertake:

a. None

b. Develop proactive procedures to aid in incident prevention

c. Train selected personnel on incident response procedures

d. Partner with law enforcement on incident response procedures

146. The purpose of the containment step in a security incident response plan is:

a. To prevent the spread of the incident

b. To recover the affected system to its pre-incident state

c. To isolate the system

d. To collect evidence for possible disciplinary action or prosecution

147. The U.S. law that made sending unsolicited commercial e-mail illegal is:

a. STOP-SPAM

b. DMCA

c. Controlling The Assault of Non-Solicited Pornography and Marketing Act

d. Computer Security Act

148. The purpose of administrative laws in the U.S. is:

a. To define courtroom and law enforcement procedures

b. To define activities such as assault, arson, theft, burglary, bribery, and perjury

c. To define contract, tort, property, employment, and corporate law

d. To regulate the operation of U.S. government agencies

149. The U.S. Code defines:

a. Both criminal and civil laws

b. Administrative laws

c. Civil laws

d. Criminal laws

150. The type of intellectual property law that protects a written work is known as:

a. Copyright

b. Trademark

c. Patent

d. Service mark

Chapter 7

151. An employee in an organization is requesting access to more information than is required. This request should be denied on the basis of which principle:

a. Separation of duties

b. Least privilege

c. Need to know

d. Job rotation

152. Two separate employees are required to open a safe containing sensitive information. One employee has part of the safe combination, and a second employee has another part of the safe combination. This arrangement follows the principle of:

a. Split custody

b. Segregation of duties

c. Need to know

d. Least privilege

153. The information security officer in an organization has assigned various accounting department employees to various roles in the organization’s financial system, taking care to assign roles with the fewest possible functions. Roles have been assigned according to the principle of:

a. Need to know

b. Segregation of duties

c. Split custody

d. Least privilege

154. An organization has in its possession many types of business records that vary in sensitivity and handling requirements. No policy exists that defines how any of these records should be protected. This organization lacks:

a. Storage and handling procedures

b. Separation of duties

c. Data classification policy

d. Information security policy

155. The purpose of a periodic review of user access rights is:

a. To check whether employees have logged in to the system

b. To check for active accounts that belong to terminated employees

c. To determine password quality and expiration

d. To determine whether access control systems still function properly

156. The purpose of a password policy that requires a minimum number of days between password changes is:

a. To prevent a brute force attack against a password

b. To prevent an intruder from carrying out a dictionary attack against a password

c. To prevent someone from quickly cycling back to their familiar password

d. To prevent a second user from changing the password

157. The purpose of a password policy that locks an account after five unsuccessful login attempts is:

a. To prevent an intruder from carrying out a dictionary attack against a password

b. To prevent a second user from changing the password

c. To prevent someone from quickly cycling back to their familiar password

d. To prevent other individuals from logging in to the account

158. The purpose of backups includes all of the following EXCEPT:

a. Software malfunctions

b. Human error

c. Hardware malfunctions

d. Cluster failovers

159. The most effective way to confirm whether backups function properly is:

a. Confirming the presence of error messages in backup logs

b. Confirming the absence of error messages in backup logs

c. Testing the ability to backup data onto backup media

d. Testing the ability to restore data from backup media

160. An organization's data classification policy includes handling procedures for data at each level of sensitivity. The IT department backs up all data onto magnetic tape, resulting in tapes that contain data at all levels of sensitivity. How should these backup tapes be handled?

a. According to procedures for the lowest sensitivity level

b. According to procedures for the highest sensitivity level

c. According to procedures in between the lowest and highest sensitivity levels

d. Data handling procedures do not apply to backup media, only original media

161. All of the following methods for destroying data on hard disk drives are sufficient EXCEPT:

a. Reformatting

b. Degaussing

c. Shredding

d. Drilling

162. All of the following are valid reasons for backing up data EXCEPT:

a. Disaster

b. Software bugs that corrupt data

c. Replication

d. Sabotage

163. An organization’s IT manager is establishing a business relationship with an off-site media storage company, for storage of backup media. The storage company has a location 5 miles away from the organization’s data center, and another location that is 70 miles away. Why should one location be preferred over the other?

a. It makes no difference which facility is chosen

b. The closer location should be chosen, to facilitate periodic on-site inspections

c. The closer location should be chosen, to facilitate faster recovery

d. The farther location should be chosen, because it will not be affected by a regional disaster

164. An organization’s IT manager wants to discontinue the business relationship with an off-site media storage company, and instead store the organization’s backup tapes at his residence, which is closer to the organization’s data center. Should this plan be considered, and why:

a. This should not be considered because the media will have fewer physical safeguards

b. This should be considered because it will save money

c. This should be considered because it is closer to the organization’s data center

d. This should not be chosen because it is too closer to the organization’s data center

165. Why do the actions of system administrators need to be monitored more closely than other personnel?

a. Administrator actions can be more harmful and have a larger impact on the organization

b. Administrators are more likely to make mistakes

c. Administrators have access to all other users' passwords

d. Administrative interfaces have fewer safeguards

166. Which of the following is NOT a risk associated with remote access:

a. Risk associated with sensitive information is stored on a non-company-owned computer, out of the organization's control

b. A non-company-owned computer with inadequate anti-malware protection can introduce an infection through remote access

c. Anti-virus software on the remote computer will not be able to download virus definition updates

d. If a split tunnel is used, the remote computer may be more vulnerable to attack

167. A workstation that can remotely access the organization's network through a VPN and access the local LAN, all through the same physical network connection, is using:

a. Split tunneling

b. Split gateways

c. IPsec VPN software

d. SSL VPN software

168. What is the difference between *split tunneling* and *inverse split tunneling*:

a. Only inverse split tunneling can utilize a firewall

b. Only split tunneling can utilize a firewall

c. Split tunneling uses IPsec and SSL, while inverse split tunneling uses L2TP

d. In split tunneling, the default network is the LAN; in inverse split tunneling, the default network is the VPN

169. The primary advantage of the use of a central management console for anti-virus is:

a. Centralized virus detection

b. Centralized reporting

c. Consolidation of reporting and centralized signature file distribution

d. Centralized signature file distribution

170. The process of erasing magnetic media through the use of a strong magnetic field is known as:

a. Delousing

b. Degaussing

c. Shredding

d. Wiping

171. A security manager has instructed a system administrator to wipe files on a hard disk. This means that the administrator needs to:

a. Perform a low-level format on the hard disk

b. Use a degausser to re-align the magnetic storage material on the hard disk

c. Use a tool to overwrite files multiple times

d. Perform a high-level format on the hard disk

172. An organization has received notice of a lawsuit related to activities in its operations department. How should the organization respond:

a. Cease all purging activities until further notice

b. Alter retention schedules and begin purging the oldest information

c. Purge all information older than timelines specified in its retention schedule

d. Hire an outside organization to perform all purging activities

173. An organization has experienced several virus infections on its desktop workstations. Which of the following remedies would NOT be effective to reduce virus infections?

a. Install an anti-virus gateway web proxy server

b. Install anti-virus on its e-mail servers

c. Install anti-virus central management console

d. Install anti-virus on its web servers

174. An organization has been made a party in a civil lawsuit. The organization is required to search its electronic records for specific memoranda. This process is known as:

a. Subpoena

b. Search and seizure

c. Discovery

d. Electronic discovery

175. An organization's critical application is required to be continuously available, with only a few minutes' per month of downtime allowed. What measure should the organization implement to assure this level of availability?

a. Server clustering

b. Server clustering and data replication

c. Hot standby site

d. Data replication

Chapter 8

176. The use of key cards to control physical access to a work facility is a form of:

a. Both preventive and administrative control

b. Detective control

c. Both preventive and detective control

d. Preventive control

177. A security manager is concerned that lost key cards can be used by an intruder to gain entrance to a facility. What measure can be used to prevent this?

a. Implement PIN pads at card reader stations

b. Implement video surveillance at card reader stations

c. Implement man traps at card reader stations

d. Implement RFID sensors at card reader stations

178. Common biometric solutions that are suitable for building entrance control include:

a. Voice print and gait

b. Retina scan and hand print

c. Voice print and DNA

d. Fingerprint and hand print

179. A building access mechanism where only one person at a time may pass is called a:

a. Entrance trap

b. Step trap

c. Mantrap

d. Passtrap

180. An organization needs to build a wall or fence to keep out the most determined intruders. What should the organization build?

a. An eight-foot high fence or wall

b. An eight-foot high fence or wall with three stands of barbed wire

c. A twelve-foot high fence or wall

d. A six-foot high fence or wall with one strand of barbed wire

181. What controls can be used in combination with fences and walls to detect intruders?

a. Video surveillance

b. Motion detectors

c. Video surveillance and motion detectors

d. Visible notices

182. An organization that wishes to conduct covert video surveillance should consider using:

a. Hidden video cameras

b. Pan/tilt/zoom cameras

c. Night vision cameras

d. Weather-proof cameras

183. Which of the following is NOT a deterrent control:

a. Monitors showing video surveillance

b. Guard dogs

c. Surveillance notices

d. Mantrap

184. What is the minimum amount of lighting required to illuminate critical areas?

a. 6-foot-candles at a height of 12 feet

b. 2-foot-candles at a height of 12 feet

c. 4-foot-candles at a height of 8 feet

d. 2-foot-candles at a height of 8 feet

185. A security manager wants to implement barriers that will block the passage of vehicles but freely allow foot traffic. The control that should be implemented is:

a. Turnstiles

b. Bollards

c. Crash gates

d. Low walls

186. A secure facility needs to control incoming vehicle traffic and be able to stop determined attacks. What control should be implemented:

a. Crash gate

b. Guard post

c. Turnstile

d. Bollards

187. A security-minded organization is relocating its business office into a shared-tenant building. How should the entrance of personnel be controlled?

a. One key card system that is jointly operated by all of the tenants

b. Separate key card systems that are operated by each tenant

c. Security guards to control who can enter the building

d. Video surveillance to monitor who enters the building

188. Which type of fire extinguisher is effective against flammable liquids:

a. Class C

b. Class K

c. Class A

d. Class B

189. The type of smoke detector that is designed to detect smoke before it is visible is:

a. Ionization

b. Optical

c. Ultraviolet

d. Radioactive

190. Provided it is permitted by local fire codes, which type of fire sprinkler system is most preferred for computer rooms?

a. Pre-action system

b. Deluge system

c. Wet pipe system

d. Foam water system

191. The advantage of a gaseous fire suppression system is:

a. It works by displacing oxygen in the room

b. It is hazardous to humans

c. It will not damage computing equipment

d. It is less expensive than sprinklers

192. The risks of excessive humidity in a computing facility include all of the following EXCEPT:

a. Static electricity

b. Corrosion

c. Condensation

d. Short circuits

193. Blackouts, brownouts, surges, and noise can all be remedied with:

a. Line conditioner

b. Power Distribution Unit (PDU)

c. Dual power supplies

d. UPS and electric generator

194. A computing facility experiences frequent brownouts but few, if any, blackouts. What should be implemented to mitigate this condition:

a. Line conditioner

b. Power Conditioning Unit (PDU)

c. Uninterruptible Power Supply (UPS)

d. Electric generator

195. The term “N+1” means:

a. The available electric power supply is at least double the current demand

b. Multiple components (N) have at least one (+1) independent backup component available

c. There is at least one (+1) backup HVAC unit in the event of failure or planned maintenance on another unit

d. Every server and network device utilizes a dual power supply

196. An organization is located in an area that experiences frequent power blackouts. What will the effect of an electric generator be in this circumstance?

a. The organization will have a continuous supply of electric power.

b. The organization will have to establish fuel supply contracts with at least two fuel suppliers.

c. Electric utility blackouts will result in short electric power outages for the organization.

d. An electric generator will be of no help in this situation.

197. Which of the following statements is TRUE about electric generators?

a. Generators require one-to-three minutes of startup time before they deliver electric power

b. Generators require an Uninterruptible Power Supply (UPS)

c. Generators require no startup time but deliver emergency electric power immediately on demand

d. Generators must be shut down to be refueled

198. The purpose of a fire extinguisher is:

a. The primary device used to fight accidental fires

b. The primary device to fight all fires until the fire department arrives

c. The primary device used to fight all fires

d. The primary device used to fight small fires

199. Controls to detect threats to equipment include:

a. Temperature sensors, humidity sensors, and water detectors

b. Temperature sensors, humidity sensors, and smoke detectors

c. Temperature sensors, humidity sensors, water detectors, gas detectors, and smoke detectors

d. Temperature sensors, humidity sensors, water detectors, and smoke detectors

200. The purpose of "secure siting" is:

a. To ensure that a site is reasonably free from natural hazards that could threaten ongoing business operations

b. To ensure that a site is reasonably free from hazards that could threaten ongoing business operations

c. To ensure that a site is free from all hazards that could threaten ongoing business operations

d. To ensure that a site is free from all man-made hazards that could threaten ongoing business operations

Chapter 9

201. The owners of files and directories on a file server are able to control which personnel may access those files and directories. The access control model that most closely resembles this is:

a. Role-based access control (RBAC)

b. Mandatory access control (MAC)

c. Discretionary access control (DAC)

d. Multilevel access

202. A resource server contains an access control system. When a user requests access to an object, the system examines the permission settings for the object and the permission settings for the user, and then makes a decision whether the user may access the object. The access control model that most closely resembles this is:

a. Mandatory access control (MAC)

b. Discretionary access control (DAC)

c. Non-interference

d. Role based access control (RBAC)

203. A security manager is setting up resource permissions in an application. The security manager has discovered that he can establish objects that contain access permissions, and then assign individual users to those objects. The access control model that most closely resembles this is:

a. Access matrix

b. Mandatory access control (MAC)

c. Discretionary access control (DAC)

d. Role based access control (RBAC)

204. An information system has multiple levels of security implemented, for both resources as well as users. In this system, a user cannot access resources below his level, and a user cannot create resources above his level. The access control model that most closely resembles this is:

a. Access matrix

b. Clark-Wilson

c. Biba

d. Bell-LaPadula

205. A security analyst has a system evaluation criteria manual called the “Orange Book”. This is a part of:

a. Common Criteria

b. Trusted Computer Security Evaluation Criteria (TCSEC)

c. Information Technology Security Evaluation Criteria (ITSEC)

d. ISO 15408

206. The Common Criteria supersedes which evaluation frameworks:

a. Neither TCSEC nor ITSEC

b. ITSEC

c. TCSEC and ITSEC

d. TCSEC

207. The TCSEC system evaluation criteria is used to address:

a. Confidentiality of information

b. Preventive and detective controls

c. Penetration testing

d. Intrusion prevention systems

208. The TCSEC system evaluation criteria is used to evaluate systems of what type:

a. E-Commerce

b. Public utilities

c. Banking

d. Military

209. A security manager wishes to objectively measure the maturity of security processes in his organization. Which model should be used for this evaluation?

a. SSE-CMM

b. SEI-CMM

c. Common Criteria

d. TCSEC

210. What is the purpose of the Software Engineering Institute Capability Maturity Model Integration (SEI CMMI)?

a. Objective assessment of the integrity of an organization’s application programs

b. Objective assessment of an organization’s systems engineering processes

c. Objective assessment of an organization’s business processes

d. Subjective assessment of an organization’s systems engineering processes

211. A security officer has declared that a new information system must be certified before it can be used. This means:

a. The system must be evaluated according to established evaluation criteria

b. A formal management decision is required before the system can be used

c. Penetration tests must be performed against the system

d. A code review must be performed against the system

212. An application has been certified against established evaluation criteria. This means:

a. A code review has been performed

b. The application can now be used

c. Formal management approval is required before it can be used

d. The application is already being used

213. DoD Information Assurance Certification and Accreditation Process (DIACAP):

a. Has been superseded by the Common Criteria

b. Is the process by which all U.S. federal information systems are certified and accredited

c. Has been superseded by DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process)

d. Is the process used to certify and accredit U.S. military information systems

214. The component in a computer where program instructions are executed is called the:

a. CPU

b. Bus

c. Front-side bus

d. Firmware

215. The purpose of the CPU’s Program Counter is:

a. To keep track of which instruction in memory is currently being worked on

b. To keep track of the number of instruction cycles the CPU has consumed on an individual program

c. To keep track of the starting address of a program

d. To track the version of the CPU’s microcode

216. The purpose of a CPU fetch operation is:

a. To retrieve data from memory

b. To retrieve an instruction from memory

c. To retrieve data from the hard disk drive

d. To retrieve data from the program counter

217. The component in a computer used for long-term storage is called:

a. Secondary storage

b. Main storage

c. Virtual memory

d. File system

218. A source code review uncovered the existence of instructions that permit the user to bypass security controls. What was discovered in the code review?

a. Feature

b. Bot

c. Logic bomb

d. Back door

219. A security manager needs to be able to regularly determine when operating system files change. What kind of tool is needed for this task?

a. Event logging

b. Intrusion detection tool

c. File system integrity monitoring tool

d. Log analysis tool

220. A hidden means of communication between two systems has been discovered. This is known as:

a. Side channel

b. Covert channel

c. Steganography

d. Bot

221. Process management, resource management, access management, and event management are examples of:

a. Security processes

b. Functions of a database management system

c. Functions of an operating system

d. Types of operating systems

222. The innermost portion of an operating system is known as:

a. Kernel

b. Core

c. Ring 0

d. Process 0

223. A security manager wishes all new laptops purchased by his organization to include a security cryptoprocessor. What hardware should be required?

a. Floating point co-processor

b. Smart card reader

c. Fingerprint reader

d. Trusted Platform Module (TPM)

224. Where is firmware primarily stored on a computer system?

a. Trusted Platform Module

b. Read-only memory

c. Master boot record

d. File system

225. A computer running the Windows operating system has nearly exhausted available physical memory for active processes. In order to avoid exhausting all available memory, what should the operating system begin doing?

a. Swapping

b. Paging

c. Killing old processes

d. Running the garbage collector

Chapter 10

226. A network engineer who is examining telecommunications circuits has found one that is labeled as a DS-1. What is the maximum throughput that may be expected from this circuit?

a. Approximately 7,000k chars/sec

b. Approximately 56k bits/sec

c. Approximately 170k chars/sec

d. Approximately 1,544M bits/sec

227. The size of packets in an ATM networks is:

a. 53 bytes

b. 1500 bytes

c. 1544 bytes

d. Variable, from 64 to 1500 bytes

228. Digital subscriber line (DSL) service:

a. Utilizes existing cable service and communicates on a different frequency

b. Has been superseded by ISDN

c. Has been superseded by satellite communications

d. Utilizes existing telephone services and communicates on a different frequency

229. An IT manager wishes to connect several branch offices to the headquarters office for voice and data communications. What packet switched service should the IT manager consider?

a. ATM

b. DSL

c. MPLS

d. Frame Relay

230. A building facilities manager is overseeing the construction of a new office building for the organization. What type of cabling should be used for voice and data communication:

a. 10BASE2 thinnet

b. Category 6 twisted pair

c. Category 5e twisted pair

d. 10BASE5 thicknet

231. Which of the following statements about Ethernet MAC addresses is TRUE:

a. The MAC address is assigned using the DHCP protocol

b. The first 3 bits designates the manufacturer of the device

c. The first 3 bytes designates the manufacturer of the device

d. The last 3 bytes designates the manufacturer of the device

232. A systems engineer is designing a system that consists of a central computer and attached peripherals. For fastest throughput, which of the following technologies should be used for communication with peripheral devices:

a. USB 2.0

b. Firewire 400

c. USB 1.1

d. IDE

233. An Ethernet network that consists of a central Ethernet switch with cabling running to each station is best described as a:

a. Logical and physical star

b. Logical ring and physical star

c. Logical star and physical bus

d. Logical bus and physical star

234. The practical range for Bluetooth is:

a. 100m

b. 300m

c. 30m

d. 10m

235. “Please do not touch Steve’s pet alligator” is:

a. A memory aid for the names of the service types in a TCP/IP network

b. A memory aid for the names of the layers in the OSI network model

c. A memory aid for the names of the layers in the TCP/IP network model

d. A memory aid for the names of the address types in an Ethernet network

236. An organization is about to occupy an existing office building. The network manager has examined all of the network cabling and has observed that most of it has been labeled “Category 3”. What is the fastest network technology that can be used on this cabling?

a. 10Mbit/s Ethernet

b. 100Mbit/s Ethernet

c. 1000Mbit/s Ethernet

d. 10Gbit/s Ethernet

237. All of the following statements about the OSI network model are true EXCEPT:

a. No commercial network product that contains all of the components of the OSI model have ever been built

b. The OSI network model uses encapsulation to build communication packets

c. TCP/IP is an implementation of the OSI network model

d. The OSI network model is a model of a network protocol stack

238. Examples of TCP/IP link layer technologies include:

a. FTP, TELNET, DNS, HTTP, SMTP

b. IP, IPsec

c. TCP, UDP, ICMP

d. Ethernet, ATM, Frame Relay, Wi-Fi

239. On a TCP/IP network, a station's IP address is 10.0.25.200, the subnet mask is 255.255.252.0, and the default gateway is 10.0.25.1. How will the station send a packet to another station whose IP address is 10.0.24.10?

a. It will send the packet directly to the station

b. It will send the packet to the default gateway at 10.0.25.1

c. It will send a Proxy ARP packet to find the IP address of another default gateway

d. It cannot send a packet to the station

240. How many Class C networks can be created in a Class B network:

a. 254

b. 1,024

c. 16,535

d. 16,534

241. The layers in the OSI model are:

a. Link, internet transport, session, application

b. Link, internet, transport, application

c. Physical, data link, network, transport, session, presentation, application

d. Physical, network transport, session, application

242. A computer has just been rebooted. An application program has started, and the application program needs to send an FTP packet to a server at IP address 10.14.250.200. What is the first packet that the computer will send on the network to accomplish this:

a. ARP

b. Whois

c. FTP

d. Rlogin

243. Two computers are communicating on a wide area network over a UDP port. One computer is sending the contents of a large file to the other computer. Network congestion has caused some packets to be delayed. What will the TCP/IP network drivers do about the packet delay?

a. The receiving computer will request that the file transfer be restarted

b. The network drivers will assemble the packets into the proper order

c. The receiving computer will request the sending computer to re-transmit the delayed packets

d. Nothing

244. A station on a network is sending hundreds of SYN packets to a destination computer. What is the sending computer doing?

a. Sending the contents of a large file to the destination computer

b. Attempting to establish a TCP connection with the destination computer

c. Attacking the destination computer with a SYN flood

d. Transmitting streaming audio or video to the destination computer

245. The purpose of the NTP protocol is:

a. Transfer the contents of a file

b. Synchronization of computer clocks to a reference clock

c. A signaling protocol used for Voice over IP

d. Share file systems over a network

246. A systems engineer has discovered that a web server supports only 56-bit SSL connections. What can the systems engineer deduce from this?

a. Web communications with this server are highly secure

b. The server does not support remote administration

c. Web communications with this server are not secure

d. The server is running the Windows operating system

247. A network manager wishes to simplify management of all of the network devices in the organization through centralized authentication. Which of the following available authentication protocols should the network manager choose:

a. RADIUS

b. TACACS

c. OSPF

d. IPsec

248. A stateful packet filtering firewall protects a web server. Which of the following is true:

a. The firewall will authenticate all users to the web server

b. The firewall will detect but not block application level attacks

c. The firewall will block application level attacks

d. The firewall will not block application level attacks

249. Someone is sending ICMP echo requests to a network's broadcast address. What is this person doing?

a. Pinging the default gateway

b. Pinging the router

c. Conducting a Ping of Death attack

d. Conducting a Smurf attack

250. All of the following statements about the TCP protocol are true EXCEPT:

a. Correct order of delivery is guaranteed

b. Connectionless

c. Connection oriented

d. Missing packets will be retransmitted