1. What is a passive measure that can be used to detect hacker attacks?
    a. Event logging
    b. Firewall reconfiguration
    c. Connection termination
    d. Process termination

2. What is another term for technical controls?
    a. Logical controls
    b. Access controls
    c. Detective controls
    d. Preventative controls

3. Which tool is an intrusion detection system (IDS)?
    a. Snort
    b. Nessus
    c. Tripwire
    d. Ethereal

4. Which authentication method checks the identity of both ends of the connection?
    a. Biometric authentication
    b. Mutual authentication
    c. CHAP authentication
    d. RADIUS authentication

5. Which methodology is used to analyze operating system exploitable weaknesses in a penetration testing project?
    a. Flaw hypothesis methodology
    b. Operating system fingerprint methodology
    c. Open Web application security Project methodology
    d. Vulnerability assessment and recovery methodology

6. Which protocol grants TGTs?
    a. ARP
    b. Kerberos
    c. L2TP
    d. Telnet

7. You have implemented a biometric system that analyzes signature dynamics. This biometric system is an example of which biometric category?
    a. Physiological
    b. Psychological
    c. Behavioral
    d. Biological

8. You have been given several suggestions for implementing the principle of least privilege. What is the best implementation of this principle?
    a. Complete administrative tasks at a computer that functions only as a server
    b. Issue the Run As command to execute administrative tasks during a regular user session
    c. Ensure that all services use the main administrative account execute their processes
    d. Issue a single account to each user, regardless of his job function

9. Users access your network using smart cards. Recently, hackers have uncovered the encryption key of a smartcard using reverse engineering. Which smart card attack was used?
    a. Microprobing
    b. Software attack
    c. Fault generation
    d. Side-channel attack

10. What is an example of a brute force attack?
    a. Sending multiple ICMP messages to a Web server
    b. Searching through a company's trash
    c. Using a program to guess passwords from a SAM file
    d. Gathering packets from a network connection

11. You have been asked to deploy a biometric system to protect your company's data center. Management is concerned that errors in the system will prevent users from accepting the system. Management stipulates that you must deploy the system with the lowest crossover error rate (CER). Identify one of the terms used in biometrics to determine CER?
    a. ACL
    b. EAR
    c. ERR
    d. FAR

12. Which password type is usually the easiest to remember?
    a. Pass phrase
    b. Static password
    c. Dynamic password
    d. Software generated password

13. Management of your company has recently become increasingly concerned with security. You have been asked to provide examples of controls that will help to prevent security breaches. Which control is an example of this?
    a. Backups
    b. Audit logs
    c. Job rotation
    d. Security policy

14. Which type of IPS monitoring requires that updates be regularly installed to ensure effectiveness?
    a. Network-based
    b. Anomaly-based
    c. Behavior-based
    d. Signature-based

15. Who is responsible for ensuring data integrity and security for an organization?
    a. Data owner
    b. Data custodian
    c. Security analyst
    d. Security administrator

16. Which security principle identifies sensitive data and ensures that unauthorized entities cannot access it?
    a. Availability
    b. Confidentiality
    c. Integrity
    d. Authentication

17. As a system administrator, you decide to implement audit trails to ensure that users are not violating policy during operation. What are you trying to determine?
    a. Identification
    b. Authorization
    c. Accountability
    d. Authentication

18. You are designing the access control for your organization's network. You need to ensure that access to network resources is restricted. Which criteria can be used to do this?
    a. Roles
    b. Groups
    c. Location
    d. Time of day
    e. Transaction type
    f. all of the above choices
    g. none of the choices

19. Which type of intrusion prevention system (IPS) watches for intrusions that match a known identity?
    a. Network-based
    b. Anomaly-based
    c. Behavior-based
    d. Signature based

20. Management has requested that active directory be implemented on your network. What is the function of this service?
    a. It is the directory service used on a Unix network
    b. It is the authentication service used on a Unix network
    c. It is the directory service used on a Windows server network
    d. It is the authentication service used on a Windows server network

21. Under MAC, which entity would exist as an object?
    a. A file
    b. A user
    c. A group
    d. A permission

22. What is the most important entity in a mandatory access control (MAC) environment?
    a. Security label
    b. Role-based controls
    c. Access control lists (ACLs)
    d. Owner determined controls

23. Because of the value of your company's data, your company has asked you to ensure data availability. You want to implement the techniques that can help to ensure data availability. Which mechanism should you implement?
    a. Auditing techniques
    b. Data recovery techniques
    c. Authentication techniques
    d. Access control techniques

24. Your organization uses a relational database to store customer contact information. You need to modify the schema of the relational database. Which component identifies this information?
    a. Query language (QL)
    b. Data control language (DCL)
    c. Data definition language (DDL)
    d. Data manipulation language (DML)

25. You need to ensure that data types and rules are enforced in the database. Which type of integrity should be enforced?
    a. Entity integrity
    b. Referential integrity
    c. Semantic integrity
    d. Cell suppression

26. Which type of malicious code is wrapped inside an otherwise benign program when the program is written?
    a. A Trojan horse
    b. A virus
    c. A worm
    d. A logic bomb

27. Which pair of processes should be separated from each other to manage the stability of the test environment?
    a. Testing and validity
    b. Validity and security
    c. Testing and development
    d. Validity and production

28. Which statement correctly defines the capability maturity model in the context of software development?
    a. It is a formal model based on the capacity of an organization to cater to projects
    b. It is a model based on conducting reviews and documenting the reviews in each phase of the software development cycle
    c. It is a model that describes the principles, procedures, and practices that should be followed by a developer in the software development cycle
    d. It is a model based on analyzing the risk and building prototypes and simulations during the various phases of the software development cycle

29. An organization's web site includes several Java applets. The Java applets include a security feature that limits the applet's access to certain areas of the web user's system. How does it do this?
    a. By using sandboxes
    b. By using object codes
    c. By using macro languages
    d. By using digital and trusted certificates

30. Which malicious software relies upon other applications to execute and infect the system?
    a. A virus
    b. A worm
    c. A logic bomb
    d. A Trojan horse

31. Which program translates one line of a code at a time instead of an entire section of a code?
    a. A compiler
    b. An interpreter
    c. An assembler
    d. An abstractor

32. You need to view windows events that are generated based on your auditing settings. Which log in event viewer should you view?
    a. Application
    b. Security
    c. System
    d. DNS

33. Which function is provided by remote procedure call (RPC)?
    a. It identifies components within a distributed computing environment (DCE)
    b. It provides code that can be transmitted across a network and executed remotely
    c. It provides an integrated file system that all users in the distributed environment can share
    d. It allows the execution of individual routines on remote computers across a network

34. Your company has an online transaction processing (OLTP) environment for customers. Management is concerned with the atomicity of the OLTP environment in its 24/7 environment. Which statement correctly defines management's concern?
    a. Transactions occur in isolation and do not interact with other transactions until the transaction is over
    b. Only complete transactions take place. If any part of the transaction fails, the changes made to a database are rolled back
    c. The changes are committed only if the transaction is verified on all systems, and the database cannot be rolled back after committing the changes
    d. Transactions are consistent throughout the different databases

35. Which statement correctly defines assurance procedures?
    a. Assurance procedures determine the modularity of the product
    b. Assurance procedures focus on the throughput and the performance of the system
    c. Assurance procedures focus on the applicability of the standard operating procedures
    d. Assurance procedures ensure that the control mechanisms implement the security policy of an information system

36. As a security administrator, you have recently learned of an issue with the web-based administrative interface on your Web server. You want to provide a countermeasure to prevent attacks via the administrative interface. All of the following are countermeasures to use in this scenario, EXCEPT:
    a. Remove the administrative interfaces from the Web server
    b. Use a stronger authentication technique on the Web server
    c. Control which systems are allowed to connect to and administer the Web server
    d. Hardcode the authentication credentials into the administrative interface links

37. Which statement is true of network address hijacking?
    a. It is used for identifying the topology of the target network
    b. It uses ICMP messages to identify the systems and services that are up and running
    c. It allows the attacker to reroute data traffic from a network device to a personal computer
    d. It involves flooding the target system with malformed fragmented packets to disrupt operations

38. Which statement correctly describes Bind variables in structured query language (SQL)?
    a. Bind variables implement database security
    b. Bind variables are used to normalize a database
    c. Bind variables are used to replace values in SQL commands
    d. Bind variables are used to enhance the performance of the database

39. What is the BEST method to avoid buffer overflows?
    a. Run an audit trail
    b. Perform a check digit
    c. Perform a reasonable check
    d. Develop a well-written program

40. Management is concerned that attackers will attempt to access information in the database. They have asked you to implement database protection using bogus data in hopes that the bogus data will mislead attackers. Which technique is being requested?
    a. Partitioning
    b. Cell suppression
    c. Trusted front end
    d. Noise and perturbation

41. Which spyware technique inserts a dynamic link library into a running process's memory?
    a. SMTP open relay
    b. DLL injection
    c. Buffer overflow
    d. Cookies

42. Which statement correctly defines spamming attacks?
    a. Repeatedly sending e-mails
    b. Using ICMP oversized echo messages to flood the target computer
    c. Sending spoofed packets with the same source and destination address
    d. Sending multiple spoofed packets with the SYN flag set to the target host of an open port

43. Which option is NOT a reason to update the business continuity plan?
    a. Budget changes
    b. Personnel changes
    c. Infrastructure changes
    d. Organizational changes

44. Which entity is an example of a corrective control?
    a. Audit trails
    b. RAID
    c. Separation of duties
    d. Business continuity planning

45. Which business continuity plan (BCP) element exists to alleviate the risk of certain threats by providing monetary compensation in the event those threats occur?
    a. Insurance
    b. Business impact analysis (BIA)
    c. Reciprocal agreement
    d. Continuity of operations plan (COOP)

46. Which site is usually maintained within the company and requires no contract with an offsite vendor?
    a. Redundant site
    b. Hot site
    c. Warm site
    d. Cold site

47. The business continuity committee has developed the business impact analysis (BIA), identified the preventative controls that can be implemented, and develop the recovery strategies. Next, the committee should develop a contingency plan. All of the following teams should be included in this plan's development to aid in the execution of the final plan except?
    a. Restoration team
    b. Damage assessment team
    c. Salvage team
    d. Risk management team

48. Which alternate disaster recovery facility is the easiest to test?
    a. Hot site
    b. Warm site
    c. Cold site
    d. Reciprocal agreement site

49. What is covered by the last step of a business continuity plan?
    a. Testing the plan
    b. Analyzing risks
    c. Updating the plan
    d. Training personnel

50. What occurs during the reconstitution phases of a recovery?
    a. An organization transitions to a temporary alternate site
    b. An organization implements the recovery strategy
    c. An organization ensures that it's facility is fully restored at the alternate site
    d. An organization transitions back to its original site

51. Which plan ensures that a vital corporate position is filled in the event it is vacated during a disaster?
    a. Occupant emergency plan (0EP)
    b. Continuity of operations plan (C00P)
    c. Succession plan
    d. Reciprocal agreement

52. What is the primary consideration when choosing an alternate computing facility?
    a. Cost
    b. Location
    c. Amount of time facility needed
    d. Resources available

53. While completing the business impact analysis, the committee discovers that a human resources application relies on the following two servers: 1) a human resources server managed by the human resources Department, and 2) a database server managed by the IT department. What is this an example of?
    a. A preventative control
    b. A reciprocal agreement
    c. An interdependency
    d. A backup strategy

54. Your organization has just expanded its network to include another floor of the building where your offices are located. You have been asked to ensure that the new floor is included in the business continuity plan. What should you do?
    a. Complete a structured walk-through test
    b. Complete a simulation tests
    c. Complete a parallel test
    d. Update the business continuity plan to include the new floor and its functions

55. While developing the business continuity plan, your team must create a plan that ensures that normal operation can be resumed in a timely manner after an outage. Which element is your team creating?
    a. Vulnerability analysis
    b. Disaster recovery plan
    c. Business continuity plan
    d. Business impact analysis (BIA)

56. Which recovery site usually takes the longest to configure when needed?
    a. Hot site
    b. Warm site
    c. Cold site
    d. Redundant site

57. You administer a small corporate network. On Friday evening, after close of business, you performed a full backup of the hard disk of one of the company servers. On Monday evening, you performed a differential backup of the same server's hard disk, and on Tuesday, Wednesday, and Thursday evenings you performed incremental backups of the server's hard disk. Which files are recorded in the backup that you performed on Thursday?
    a. All the files on the hard disk
    b. All the files on the hard disk that were changed or created since the differential backup on Monday
    c. All the files on the hard disk that were changed or created since the incremental backup on Tuesday
    d. All the files on the hard disk that were changed or created since the incremental backup on Wednesday

58. What protects data on computer networks from power spikes?
    a. A heating system
    b. A key card
    c. A sprinkler
    d. A surge suppressor

59. The business continuity team is interviewing users to gather information about business units and their functions. Which part of the business continuity plan includes this analysis?
    a. Disaster recovery plan
    b. Contingency plan
    c. Business impact analysis (BIA)
    d. Occupant emergency plan (OEP)

60. During business continuity planning, you need to obtain the single loss expectancy (SLE) of the company's file server. Which formula should you use to determine this?
    a. Asset value times exposure factor (EF)
    b. Asset value times annualized rate of occurrence (ARO)
    c. Exposure factor (EF) times annualized rate of occurrence (ARO)
    d. Annualized loss expectancy (ALE) times annualized rate of occurrence (ARO)

61. Your company has a backup solution that performs a full backup each Saturday evening and an incremental backup all other evenings. A vital system crashes on Tuesday morning. How many backups will be needed to restore?
    a. One
    b. Two
    c. Three
    d. Four

62. Which term refers to how long a company can tolerate the outage of a certain asset, entity, or service?
    a. Business impact analysis
    b. Maximum tolerable downtime
    c. Maximum recovery time
    d. Mean time between failure
    e. Mean time to repair

63. During a recent natural disaster, the primary location for your organization was destroyed. To bring the alternate site online, you restored the most critical systems first. Now a new primary site is complete, and you need to ensure the site is brought online in an orderly fashion. What should you do first?
    a. Restore the most critical functions to the new primary site
    b. Restore the least critical functions to the new primary site
    c. Restore all independent functions to the new primary site
    d. Restore all interdependent functions to the new primary site

64. When is a disaster recovery plan implemented?
    a. After all systems are back online
    b. After the critical systems are back online
    c. After a disaster is declared
    d. When the company is in normal operation mode

65. Your organization has decided to implement the Diffie-Hellman asymmetric algorithm. Which statement is true of this algorithm's key exchange?
    a. Authorized users need not exchange secret keys
    b. Authorized users exchange public keys over a secure medium
    c. Authorized users exchange symmetric session keys over a nonsecure medium
    d. Unauthorized users exchange public keys over a nonsecure medium

66. What is a list of serial numbers of digital certificates that have not expired, but should be considered invalid?
    a. CA
    b. CRL
    c. KDC
    d. UDP

67. Which statement is NOT true of an RSA algorithm?
    a. RSA can prevent man in the middle attacks
    b. An RSA algorithm is an example of symmetric cryptography
    c. RSA encryption algorithms do not deal with discrete logarithms
    d. RSA is a public key algorithm that performs both encryption and authentication
    e. RSA uses public and private key signatures for integrity verification

68. Your organization signed a contract with the United States military. As part of this contract, all e-mail communication between your organization and the US military must be protected. Which e-mail standard must you use for this communication?
    a. Multipurpose Internet Mail extension (MIME)
    b. SMIME
    c. Message security protocol (MSP)
    d. Pretty good privacy (PGP)

69. Which service is fulfilled by cryptography by ensuring that a sender cannot deny sending a message once it is transmitted?
    a. Confidentiality
    b. Authenticity
    c. Integrity
    d. Non-repudiation

70. Which service provided by a cryptosystem turns information into unintelligible data?
    a. Non-repudiation
    b. Authorization
    c. Cipher text
    d. Encryption

71. What identifies entries within an X.509 CRL?
    a. Digital certificates
    b. Private keys
    c. Public keys
    d. Serial numbers

72. You want to send a file to a coworker named Maria. You do not want to protect the file contents from being viewed; however, when Maria receives a file, you want her to be able to determine whether the contents of the file were altered during transit. Which protective measures should you use?
    a. A digital certificate
    b. A digital signature
    c. Symmetric message receipt
    d. Asymmetric encryption

73. Your organization uses the Kerberos protocol to authenticate users of the network. Which statement is true of the key distribution center (KDC) when this protocol is used?
    a. The KDC is only used to store secret keys
    b. The KDC is used to capture secret keys over the network
    c. The KDC is used to maintain and distribute public keys for each session
    d. The KDC is used to store, distribute, and maintain cryptographic session keys

74. Your organization is working with an international partner on a new and innovative product. All communication regarding this must be encrypted using a very strong symmetric algorithm. Which algorithm should you use?
    a. AES
    b. 3DES
    c. IDEA
    d. Blowfish

75. Which statement is true of the rijndael algorithm used in AES?
    a. Rijndael uses variable block lengths and variable key lengths
    b. Rijndael uses fixed block lengths and fixed key lengths
    c. Rijndael uses variable block lengths and fixed key lengths
    d. Rijndael uses fixed block lengths and variable key lengths

76. Your manager has asked you to ensure that the password files that are stored on the servers are not vulnerable to attacks. To which type of attack would these files be vulnerable?
    a. A dictionary attack
    b. A SYN flood attack
    c. A side channel attack
    d. A denial of service (DoS) attack

77. Your company hosts several public web sites on its Web Server. Some of the sites implement the secure sockets layer (SSL) protocol. Which statement is NOT true of this protocol?
    a. SSL is used to protect Internet transactions
    b. SSL version 2 provides client-side authentication
    c. SSL operates at the network layer of the OSI model
    d. SSL with TLS supports both server and client authentication
    e. TLS has two possible session key lengths: 128 bit and 256 bit

78. Your organization implements hybrid encryption to provide a high level of protection of your data. Which statement is true of this type of encryption?
    a. The secret key protects the encryption keys
    b. Public keys decrypt the secret key for distribution
    c. Asymmetric cryptography is used for secure key distribution
    d. The symmetric algorithm generates public and private keys

79. Recently, your organization has become increasingly concerned about hackers. You have been specifically tasked with preventing man in the middle attacks. Which protocol is NOT capable of preventing this type of attack?
    a. CHAP
    b. Secure shell (SSH)
    c. HTTP secure (HTTPS)
    d. Internet protocol security (IPSec)

80. Which hashing algorithm generates a 160 bit hashing value?
    a. Tiger
    b. HAVAL
    c. SHA
    d. MD5

81. You have implemented a public key infrastructure (PKI) to issue certificates to the computers on your organization's network. You must ensure that the certificates that have been validated are protected. What must be secured in a PKI to do this?
    a. The public key of the root CA
    b. The private key of the root CA
    c. The public key of a user's certificate
    d. The private key of a user's certificate

82. Which statement is NOT true of cross certification?
    a. Cross certification builds an overall PKI hierarchy
    b. Cross certification is primarily used to establish trust between different PKI's
    c. Cross certification checks the authenticity of the certificates in the certification path
    d. Cross certification allows users to validate each other's certificate when they are certified under different certification hierarchies

83. You have been specifically asks to implement a stream cipher for Wi-Fi. Which cryptographic algorithm could you use?
    a. RC4
    b. RC5
    c. TKIP
    d. MD5

84. The IT department manager informs you that your organization's network has been the victim of a ciphertext only attack. Which statement is true regarding this type of attack?
    a. A birthday attack is an example of a ciphertext only attack
    b. A ciphertext only attack is focused on discovering the encryption key
    c. It is very difficult for an attacker to gather the ciphertext in a network
    d. A ciphertext only attack is considered by hackers to be the easiest attack

85. You are engaged in a risk assessment for your organization's network. You have identified several risks. When you calculate the risks by using the quantitative method, you multiply the assets value by the exposure factor (EF). What is the result?
    a. Risk elimination
    b. Actual cost evaluation (ACV)
    c. Single loss expectancy (SLE)
    d. Annualized loss expectancy (ALE)

86. What is a potential opening in network security that a hacker can exploit to attack a network?
    a. An agent
    b. An event
    c. A target
    d. A vulnerability

87. As part of a new security initiative, your organization has decided that all employees must undergo security awareness training. What is the aim of this training?
    a. All employees must understand their security responsibilities
    b. All employees in the IT department should be able to handle security incidents
    c. All employees excluding top management should understand the legal implications of loss of information
    d. All employees in the IT department should be able to handle social engineering attacks

88. Which statement is true of risk?
    a. Risk is the probability of the exploitation of vulnerabilities by a threat agent
    b. Implementation of preventive controls is sufficient for risk mitigation
    c. A qualitative risk analysis should be preferred for assigning monetary values
    d. The risk of an internal security breach by employees is less than that posed by external threats

89. For which security objective(s) should system owners and data owners be accountable?
    a. Integrity
    b. Availability
    c. Confidentiality
    d. Integrity and availability
    e. Confidentiality and integrity
    f. Confidentiality and availability
    g. Availability, integrity, and confidentiality

90. The new security plan for your organization states that all data on your servers must be classified to ensure appropriate access controls are implemented. All of the following statements are true of information classification EXCEPT?
    a. A data owner must determine the information classification of an asset
    b. Data classification refers to assigning security labels of information assets
    c. A data custodian must determine the classification of an information asset
    d. The two primary classes of data classification deal with military institutions and commercial organizations

91. Of which control is WPA TKIP an example?
    a. Physical controls
    b. Technical controls
    c. Detective controls
    d. Administrative controls

92. You are designing the security awareness training plan for your organization. Several groups have been identified to receive customized training. Which group requires security training to ensure the programs produced by the company do not contain security problems?
    a. Administrators
    b. Developers
    c. Employees
    d. Executives

93. All of the following are controls which are integral parts of information security administration except?
    a. Information controls
    b. Physical controls
    c. Technical controls
    d. Administrative controls

94. You are the security manager for your organization. You are identifying potential security risks for your organization. Which technique would you NOT use?
    a. Interviewing
    b. Benchmarking
    c. Brainstorming
    d. Delphi technique

95. Your organization has decided that the organization needs to implement password policies for better security. Which password policy will NOT strengthen password security?
    a. Requiring users to use a minimum of eight characters in a password
    b. Requiring users to use symbols and numbers in their passwords
    c. Requiring users to use only alphabetic words as passwords
    d. Requiring users to periodically change their passwords

96. What is typically part of an information policy?
    a. Classification
    b. Authentication
    c. Acceptable use
    d. Employee termination procedure

97. What is a risk trigger?
    a. A risk response strategy
    b. A metric used to measure the impact of a risk
    c. An event that indicates that a risk has occurred or is about to occur
    d. An individual who is responsible for alerting the team when a given risk occurs

98. Your organization has decided that the organization needs to implement password policies for better security. Which password policy will likely REDUCE network security?
    a. Requiring users to increase the length of their passwords from six characters to eight characters
    b. Requiring users to use symbols such as the $ character and the % character in their passwords
    c. Requiring users to use easily remembered passwords
    d. Requiring users to change passwords in 60 days rather than 90 days

99. What is employed when user accounts are created by one employee and user permissions are configured by another employee?
    a. A collusion
    b. A two-man control
    c. Separation of duties
    d. Rotation of duties

100. Which security management approach is recommended for an information security program?
    a. Top-down
    b. Bottom-up
    c. Integrated
    d. Differential

101. You identify a security risk that you do not have in-house skills to address. You decide to procure contract resources to mitigate this security risk. Which type of risk response strategy are you demonstrating?
    a. Avoidance
    b. Acceptance
    c. Mitigation
    d. Transference

102. What is the purpose of quantitative risk analysis?
    a. To generate an action plan in response to each identified risk
    b. To generate a prioritized list of risks that might adversely affect the project
    c. To determine the overall impact that specific risks posed to successful project completion
    d. To analyze the already prioritized risks in such a way as to give each a numerical rating

103. You are the security administrator for your company. You identify a security risk. You decide to continue with the current security plan. However, you develop a contingency plan for if the security risk occurs. Which type of risk response strategy are you demonstrating?
    a. Avoidance
    b. Acceptance
    c. Mitigation
    d. Transference

104. As you are designing your security awareness training, you list the different groups that require different training. Which group should receive security training that is part education and part marketing?
    a. Administrators
    b. Developers
    c. Employees
    d. Executives

105. Which role is a strategic role that helps to develop policies, standards, and guidelines and ensures the security elements are implemented properly?
    a. User
    b. Data owner
    c. Security administrator
    d. Security analyst

106. What does sending data across an insecure network, such as the Internet, primarily affect?
    a. Confidentiality and availability
    b. Integrity and availability
    c. Confidentiality and integrity
    d. Integrity and authenticity

107. What should be the role of management in developing an information security program?
    a. It should be minimal
    b. It is mandatory
    c. It is not required at all
    d. It is limited to the providing of funds

108. What would be a correct statement regarding ethics and laws?
    a. Ethics are always drawn from laws
    b. If something isn't illegal, then it is probably ethical
    c. Most laws are drawn from ethics
    d. Laws apply to everything in society that is right and wrong

109. Monitoring employee e-mail messages may be a useful tool for uncovering malicious activity. Which of the following is not something a company should do if they are going to carry out this type of monitoring?
    a. Inform users that this type of monitoring may take place
    b. Explain the ramifications of misuse of this resource to users
    c. Guarantee employee privacy
    d. Monitor all users consistently and fairly

110. Which of the following is an attack that uses tools to intercept electronic communications signals usually passively instead of actively?
    a. Masquerading
    b. Social engineering
    c. Sniffing
    d. Salami

111. What is the first step when investigating a computer crime?
    a. Photograph the area, computer, and contents on the screen
    b. Advise individuals in the area of their rights before evidence is collected
    c. Quickly look for planted logic bombs and Trojan horses to ensure damage cannot be done
    d. Power off the computer system

112. If senior executives are found liable for not properly protecting their company's assets and information systems, what type of law likely would apply in this situation?
    a. Criminal
    b. International
    c. Civil
    d. Common

113. During a trial, a company introduces documents that were created during the course of the investigation to show new evidence of wrongdoing. These documents would be classified as what type of evidence?
    a. Direct
    b. Conclusive
    c. Hearsay
    d. Corroborative

114. The investigation process of a computer crime is very similar to investigating many other types of crime. What is the “who" and "why" of a crime?
    a. Motivations
    b. Opportunities
    c. Means
    d. Capabilities

115. Typically, computer files are considered hearsay evidence. In which of the following scenarios would computer files be admissible?
    a. When the file clearly proves guilt
    b. When a forensic expert testifies that the evidence is trustworthy
    c. When the computer output is produced during the course of regular business
    d. It is never admissible

116. Which of the following is a true statement regarding warrants and seizure on an individual's property?
    a. Police do not have to have a warrant for most cases of property seizure
    b. A manager falls under the same restrictions as law enforcement agents if she follows the instruction of a law enforcement agent
    c. A manager without a warrant can seize the information on a computer at a company that contains suspected child pornography information if the manager was directed by a police officer to obtain this information
    d. If law enforcement has a warrant for a home computer in a case of suspected child pornography, they can also confiscate the computers at the homeowner's office

117. What is administrative law?
    a. Deals with violations of regulatory standards
    b. Deals with violent violation of individuals
    c. Deals with laws develop to protect the public
    d. Deals with commerce laws across borders

118. In many cases traditional laws do not adequately approach computer crimes and their ramifications. Which of the following is one way legal systems have changed to better allow these established rules to be used?
    a. The definition of property has been expanded to include intangible property, as in hard drives
    b. The definition of property has been expanded to include intangible property, as in electronic information
    c. The definition of property has been expanded to include tangible property, as in electronic information
    d. The definition of property has been expanded to include tangible property, as in secondary storage devices

119. Three main categories fall under common law. Which of the following is NOT one of them?
    a. Administrative law
    b. Civil law
    c. Criminal law
    d. Union law

120. Who usually blows the whistle on illegal software usage within companies?
   a. IT administrators
   b. CISSPs
   c. Disgruntled employees
   d. Managers

121. What type of attack is done with a protocol analyzer?
   a. Active
   b. Aggressive
   c. Masquerading
   d. Passive

122. Which of the following statements regarding trade secrets, copyright, patents, and trademark law is accurate?
   a. All countries follow a uniform standard for these areas
   b. A vendor with in a country should follow their own country's standards in these areas as the appropriate method to conduct their business
   c. Any vendor that is interested in doing business in a country outside of theirs should be aware of the differences in these specific areas, and take the necessary steps to properly protect their product
   d. A vendor can choose between his country's laws and practices or the foreign country in which they do business

123. Which of the Following Items Is Addressed in the $(ISC)^2$ Code of Ethics?
   a. Avoid conflicts of interest
   b. Avoid conducting the penetration tests
   c. Protect national security
   d. Protect individual rights

124. Which of the following acts was created to protect the privacy of medical information?
   a. US federal privacy act of 1974
   b. Computer fraud and abuse act
   c. HIPAA
   d. Gramm Leach Bliley act of 1999

125. A cashier who enters incorrect values in the cash register and keeps the remaining money has committed what kind of crime?
   a. Sniffing
   b. Social Engineering
   c. Masquerading
   d. Data diddling

126. An edict stating that all evidence be labeled with information about who secured it and who validated it is called _____
    a. CERT
    b. Chain of custody
    c. Direct evidence
    d. Incident response policy

127. Which of the following is addressed in the federal sentencing guidelines?
    a. Senior executives are not responsible for the computer and information security decisions they make and what actually takes place within their organizations
    b. Senior executives are responsible for the computer and information security decisions they make and what actually takes place within their organizations
    c. This act provides the necessary structure when dealing with espionage and further defines trade secrets to be technical, business, engineering, scientific, or financial
    d. This act requires federal agencies to identify computer systems that will contain sensitive information

128. Tricking an intruder into accessing the digital information in order to prosecute him is an example of what?
    a. Enticement
    b. Interrogation
    c. Entrapment
    d. Salami attack

129. There are different categories for evidence depending upon what form it is in and possibly how it was collected. Which of the following is considered supporting evidence?
    a. Best evidence
    b. Corroborative evidence
    c. Conclusive evidence
    d. Direct evidence

130. Which term refers to a hidden set of software instructions created by the developer as a matter of convenience?
    a. Covert channel
    b. Software patch
    c. Maintenance hook
    d. GUI

131. Don is a senior manager of a software development firm. He has just found out that a key contract was renewed, allowing the company to continue developing an application that was idle for several months. Excited to get started, Don begins work in the application privately, but cannot tell his staff until the news is announced publicly in a few days. However, as Don begins making changes in the software, various staff members notice changes in their connected systems, even though they work in a lower security level. What kind of model could be used to ensure this does not happen?
    a. Biba
    b. Bell-LaPadula
    c. Non-interference
    d. Clark Wilson

132. The concept that dictates that once an object is used it must be stripped of all of its data remnants is called _____
    a. Layering
    b. Object reuse
    c. Multi use
    d. Polymorphism

133. A computer's hard drive, floppy disks, or CD-ROM is called _____
    a. Primary storage
    b. Virtual memory
    c. Real storage
    d. Secondary storage

134. The ability for a computer to perform I/O functions is the key factor in its effectiveness. When proper I/O levels cannot be maintained, a system may malfunction and operations freeze. Which one of the core security principles does this affect most?
    a. Integrity
    b. Availability
    c. Confidentiality
    d. Consistency

135. What is the main reason why an application would be developed using the Brewer-Nash model?
    a. To provide varying degrees confidentiality and integrity
    b. To ensure that unauthorized subjects cannot make modifications
    c. To ensure conflicts of interest are minimized through dynamic access control
    d. To ensure that the integrity on an object at a higher level is not compromised

136. What is the result of combining RAM and secondary storage?
    a. Virtual storage
    b. Real storage
    c. Primary storage
    d. Combo storage

137. Which of the following computer components dictates when data is processed by the system's processor?
    a. Control unit
    b. Registers
    c. ALU
    d. Ring 0

138. Computers have many methods for protecting themselves. One security measure is an abstract machine that ensures all subjects have adequate permission to access objects. This concept ensures objects will not be harmed by untrusted subjects. What is this security control called?
    a. Security kernel
    b. Trusted computer base
    c. Reference monitor
    d. Security domain

139. Which security model specifies that commands and activities performed at one security level should not be seen or affect subjects or objects at a different security level?
    a. Biba model
    b. Information flow model
    c. Security separation model
    d. Noninterference model

140. Which of the following provides the highest security when it comes to memory?
    a. Memory mapping
    b. Hardware segmentation
    c. Virtual machines
    d. Protection rings

141. Companies should follow certain steps in selecting and implementing a new computer product. Which of the following sequences is ordered correctly?
    a. Evaluation, accreditation, certification
    b. Evaluation, certification, accreditation
    c. Certification, evaluation, accreditation
    d. Certification, accreditation, evaluation

142. Operating systems that provide multilevel security and mandatory access control are based on which model?
    a. Brewer-Nash
    b. Biba
    c. Clark-Wilson
    d. Bell-LaPadula

143. Data is stored in a variety of ways. Sometimes it is stored based on convenience and sometimes on necessity. Sequential storage means that data saved on a medium must be accessed in the same order in which it was saved. Which of the media types below is a sequential storage device?
    a. CD-ROM
    b. WSB drive
    c. Magnetic tape
    d. Hard drive

144. There are several types of components that fall within the trusted computing base (TCB). Which of the following would not be within the security perimeter?
    a. Firmware on motherboard
    b. Applications
    c. Protective hardware components
    d. Reference monitor and security kernel

145. A company has performed the following steps when buying a new operating system: 1) analyzed common criteria evaluation report on the product; 2) purchased the product after comparing other alternatives; and 3) properly certified the product within the internal network. What is the next step that needs to happen before the process is complete?
    a. Software debugging
    b. Contingency planning
    c. Accreditation
    d. Establish access control policies

146. Many of the security architecture models (Bell-LaPadula, Biba, Clark Wilson) are very high level constructs and provide abstracts for software designers to use as a map to meet specific security goals. Which of the following models address more granular activities, as in all subjects and objects should be created securely?
    a. Harrison-Ruzzo-Ullman model
    b. Brewer Nash
    c. Information flow
    d. Graham Denning model

147. Which of the following best describes TCSEC?
    a. A criteria to validate the security and assurance provided in products
    b. The red book
    c. European assurance evaluation criteria
    d. A penetration testing method

148. Tim is an entry-level customer service representative working with a client on a service escalation. After working through several issues, the customer asks him if he can verify the annual service charge and opt-out provisions of his contract. Tim unhappily responds he only has access to technical and operations data and cannot access contract information. He says he must transfer the customer to customer service. What type of control is described in this example?
    a. Clipping level
    b. Least privilege
    c. Operations security
    d. ACL

149. Pretending to be another person in order to gain privileges is an example of what kind of attack?
    a. Scavenging
    b. Spoofing
    c. Keystroke logging
    d. Man in the middle

150. The three main types of operational controls are technical, administrative, and physical. There or several mechanisms for each of these types that provide different services. What service does passwords, ACL's, and ID badges all provide?
    a. Deterrent
    b. Correction
    c. Prevention
    d. Compensation

151. In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?
    a. A blacklist of companies that have their mail server relays configured to allow traffic only to their specified domain name
    b. A blacklist of companies that have their mail server relays configured to be wide open
    c. Mail relay, which is a technique of bouncing e-mail from internal to external mail servers continuously
    d. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally

152. What is configuration management used for in many different environments?
    a. Controlling changes in testing procedures
    b. Controlling testing environments and documentation of testing
    c. Ensuring changes in design and its verification process, testing, and implementation
    d. Controlling changes in design and its verification of process, testing, and implementation

153. Which of the following ensures that security is not compromised when a system crashes or a component failure occurs?
    a. Trusted recovery
    b. Hot swappable
    c. Redundancy
    d. Secure boot

154. Which of the following controls are used to amend a situation after an attack has occurred or a vulnerability has been identified?
    a. Deterrent
    b. Corrective
    c. Preventive
    d. Recovery

155. Max has just finished developing a new software feature that the network provisioners have been requesting for some time. Anxious to get this to the group, Max installs the patch on a production system. The next day he is summoned to his boss's office who is very angry. His boss says, "You didn't submit a request, get approval, document anything, or do proper testing." What procedure is Max's boss referring to?
    a. Sanitization
    b. Due care
    c. Change control
    d. Operational assurance

156. A device used to ensure facsimile security so that transmissions are NOT sent in cleartext is called a _____
    a. Firewall
    b. Fax encryptor
    c. Security policy
    d. TCB

157. Which is NOT true regarding "authorization creep?"
    a. Typically occurs when employees transfer to new departments or change positions
    b. Violates "least privilege"
    c. Enforces the need to know concept
    d. Tendency of users to request additional privileges but seldom ask for it to be taken away

158. What role should accountability play in the access to media and auditing portion of a company's operations security strategy policies?
    a. None. Accountability is managed by corporate security policies, not at the operator level
    b. Accountability is the other side of the coin of auditing. If a user is properly authorized, any violations or errors he makes can be traced back to him if auditing is in place
    c. Accountability means that the creator of the company's access policy bears final accountability for any improper access
    d. Accountability means that the entire IT department, as creator of the company's access policy, bears final accountability for any improper accesses

159. Which of the following is NOT a correct way in which an operating system responds to a failure?
    a. System reboot
    b. Emergency system restart
    c. System cold start
    d. Not starting

160. Which of the following works as a transfer agent?
    a. SET
    b. IP
    c. SMTP
    d. ASCII

161. There should be one role or committee that is responsible for enforcing and maintaining the change control process within a company. Which of the following functions is NOT the responsibility of this group?
    a. To properly modify the change control process depending upon the logic of the change that was requested
    b. To provide formal approval or rejection of the change to the requester
    c. To enforce strict, consistent companywide procedures
    d. To provide clear instructions to all employees on how to initiate a change request

162. Which of the following is NOT considered a countermeasure to port scanning and operating system fingerprinting?
   a. Allow access at the perimeter network to all internal ports
   b. Remove as many banners as possible within operating systems and applications
   c. Use TCP wrappers on vulnerable services that have to be available
   d. Disable unnecessary ports and services

163. Similar activities are carried out by hackers and security professionals performing an assessment. Identifying assets in a victims network is called_____
   a. Port scanning
   b. TCP wrapping
   c. Fingerprinting
   d. Man in the middle

164. What is Nessus used for?
   a. To identify vulnerabilities within a network
   b. To open network security holes
   c. To re-amplify a signal
   d. To track network connections

165. A reservationist at a travel agency is allowed to commit two mistakes per month without consequence. An automated system tracks these errors and alerts appropriate personnel when this limit is exceeded. What is the limit referred to as?
   a. Clipping level
   b. Maximum fault tolerance
   c. Proximate causation
   d. Due care

166. Operations departments should back up data in all of the following situations EXCEPT which of the following?
   a. Once per year
   b. Before a reorganization
   c. After a system upgrade
   d. For authorized on-demand requests

167. Generating strong magnetic fields to erase the content on a type of media is called _____
   a. Sniffing
   b. Degaussing
   c. Wiretapping
   d. Magnetizing

168. Which of the following refers to the data left on the media after the media has been erased?
    a. Semi-hidden
    b. Dregs
    c. Sticky bits
    d. Remanence

169. The estimated lifetime of a device or the estimated timeframe until a component within a device gives out is called _____
    a. UPS
    b. MTTB
    c. MTTR
    d. MTBF

170. A company with highly combustible materials is trying to determine which sprinkler system type to purchase. They are not concerned with false alarms, but instead are insistent that the system be effective at extinguishing large and rapidly growing fires extremely fast. Which would be the best sprinkler system for this company?
    a. Wet pipe
    b. Deluge
    c. Dry pipe
    d. Pre-action

171. What does a company need to investigate to ensure that the availability of production systems are not negatively affected for a long period of time if a new system goes down?
    a. NDA and MTTR
    b. SLAs and MTTR
    c. MTBF and NDA
    d. MTTR and TCSEC

172. Companies that offer mission-critical services to their customers have to make contingencies for potential power failures. An uninterruptible power supply (UPS) is a common alternative that companies select in situations where even one second of power interruption is unacceptable, the UPS can take over the load as soon as power is lost. These UPS types have primary power continually running through them and are activated immediately if the primary source fails. What are these systems called?
    a. Standby UPS
    b. Inline UPS
    c. Ghost UPS
    d. Generator

173. What is the last line of defense in a physical security sense?
   a. People
   b. Interior barriers
   c. Exterior barriers
   d. Walls

174. Several types of fire detectors are available on the market. Which of the following detect a fire by identifying changes in a stream of light waves?
   a. Optical detector
   b. Thermometer detector
   c. Heat activated detector
   d. Flame activated detector

175. Physical security components combat all of the following main risks except _____
   a. SYN flood
   b. Physical damage
   c. Theft
   d. Fire

176. Which of the following items is NOT considered a preventive physical control?
   a. Fencing
   b. Access logs
   c. Security guards
   d. Security dogs

177. Internal partitions should NOT be used in which of the following instances?
   a. To provide protection of a sensitive area
   b. To create storage rooms for nonsensitive material
   c. To create different work areas
   d. To create barriers between areas

178. Which of the following should be used to suppress the fuel supply of a fire of common combustibles?
   a. Soda Acid
   b. CO2
   c. Halon
   d. Freon

179. The classes of fire are determined by their level of combustibility. Of the materials below, which does NOT have a Class A rating?
   a. Wood
   b. Rubber
   c. Oil-based paint
   d. Paper

180. A physical security mechanism consisting of a small area with two doors used to "hold" an individual until his identity can be verified is called a _____

a. Turnstile
b. Holding area
c. Mantrap
d. Man in the middle

181. How does an acoustical seismic device detect an intruder?
a. Change in vibration
b. Change in magnetic field
c. Change in microwaves within room
d. Breakage of foil strip in window

182. A secured computing room should have all of the following characteristics except _____
a. No more than two doorways
b. Walls that extend from the true flooring to the true ceiling
c. Comfortable sitting areas around workstations
d. Strict physical access controls

183. Which one of the following characteristics is NOT true of an ideal data processing room?
a. Humidity level of 50%
b. Carpeting
c. Room temperature around 72°F
d. Independent HVAC and ventilation systems

184. What is Plenum space?
a. Open space above drop ceilings and below raised floors
b. The screened subnet area within the DMZ
c. The unprotected area around the security perimeter fence
d. a VPN tunnel

185. Due to some recent after-hours altercations in a nearby parking lot, Jim's company is installing new lights at the location to improve security. Jim is in charge of physical security and has done the research on lighting requirements in critical areas. One of the requirements Jim found was something called "two foot-candles at eight feet." What does this mean?
a. Lights must be placed 2 feet apart
b. The area being lit must be illuminated 2 feet high and 2 feet out
c. This is an illumination metric used for lighting
d. Each lit area must be within 2 feet of the next lit area

186. Jonathan's workstation is overloaded with electrical connections into a small number of outlets. He is daisy chaining power strips in order to service all of his equipment. One problem that always remains is excessive line noise and power fluctuation. He needs to address the problem but does not have a great deal of money budgeted for it. Which of the solutions below would be LEAST favorable for this specific issue?
    a. Surge protector
    b. Line conditioners
    c. Redistribute cords to other outlets
    d. UPS

187. Low levels of humidity result in static electricity. High levels of humidity create a host of problems as well. Which of the following issues pertaining to high levels of humidity is the most concerning to a security professional?
    a. Excessive moisture in the air is not an optimum condition for employees who spend their days in a computer room
    b. High humidity levels put strain on HVAC systems, which can cause security concerns
    c. High humidity levels can damage or destroy computer parts
    d. High humidity levels make the possibility of fire more likely

188. Sometimes basic fencing does not provide the level of protection a company requires. Which of the following combines the functions of intrusion detection systems and fencing?
    a. PIDAS
    b. PERIMETER
    c. Closed-circuit TV
    d. Acoustical seismic detection system

189. Different organizations have different physical security protection requirements, thus they need different types of controls and countermeasures. Which of the following is NOT a legitimate justification for using security guards at a facility?
    a. They are one of the best deterrence for potential intruders
    b. They are flexible and can be positioned randomly
    c. They provide judgment and understanding of different situations
    d. They are cheaper than most automated detection systems

190. Which of the following water sprinkler systems sounds an alarm and delays water release?
    a. Wet pipe system
    b. Pre-action system
    c. Deluge system
    d. Dry pipe system

191. Any of the following actions can be taken to prevent static electricity except which one?
    a. Install carpet
    b. Use antistatic bands when working in computer systems
    c. Install antistatic flooring
    d. Ensure proper grounding

192. Which protocol is described as a "best effort delivery" protocol?
    a. TCP
    b. SMTP
    c. UDP
    d. ARP

193. Which of the following can provide up to 45 Mbps of bandwidth?
    a. BRI
    b. T3
    c. T1
    d. M1

194. Which of the following is a LAN transmission technology that is susceptible to collisions and provides a mechanism for retransmission?
    a. Ethernet
    b. Token Ring
    c. ATM
    d. FDDI

195. Why are network sniffers dangerous to an environment?
    a. They can be used to launch active attacks
    b. Their presence can cause many false positives
    c. Their presence and activities are not detectable
    d. They can access sensitive data within applications

196. Which firewall makes access decisions based only on addresses and port numbers in the header?
    a. Circuit based proxy
    b. Application based proxy
    c. Stateful
    d. Dual homed

197. ARP broadcasts messages on the LAN to find what?
    a. IP address
    b. MAC address
    c. Router
    d. Hostname

198. Which of the following TCP protocols typically works on ports 20 and 21?
   a. Telnet
   b. Hypertext transfer protocol (HTTP)
   c. File transfer protocol (F TP)
   d. Simple network management protocol (SNMP)

199. A WAN technology that uses 53 bytes cells and has low delay levels is called what?
   a. ATM
   b. Frame relay
   c. X.25
   d. SMDS

200. Which of the following devices typically works at the application layer and acts as a protocol translator for different environments?
   a. Switch
   b. Gateway
   c. Bridge
   d. Router

201. What device works at the physical layer to boost electrical signals between network segments?
   a. Switch
   b. Router
   c. Repeater
   d. Gateway

202. Which statement is not true of a dedicated line?
   a. More secure than using public networks
   b. Connects two locations
   c. Inflexible and expensive
   d. Uses packet switching technology

203. All computers are connected to a central device in which of the following topologies?
   a. Star
   b. Bus
   c. Mesh
   d. Tree

204. When a router modifies a private IP address of a computer into a registered IP address to send out through an external link, it is performing _____
   a. Network address translation
   b. Polling
   c. Address resolution protocol
   d. Multiplexing

205. Which of the following is a real threat in wireless communication?
   a. Encryption is not available in wireless technologies
   b. Users cannot be authenticated as they move from one AP to another
   c. No data integrity can be performed as users move from one AP to another
   d. Wardriving can uncover traffic, AP and station location

206. A breach is, generally, an impermissible use or disclosure that compromises the security or privacy of the protected information. What must you do to determine if a data breach must be reported?
   a. Verify the breach in log history
   b. Examine existing laws and regulations
   c. Check with law enforcement such as the FBI
   d. Follow procedures in your DRP

207. A DDoS attack occurs when a hacker has deposited remote-controlled agents, zombies, or bots onto numerous secondary victims and then uses the deployed bots as a single entity to attack a primary target. What class of computer crime would this be reported as?
   a. Computer incidental crime
   b. Computer-resisted crime
   c. Computer-targeted crime
   d. Computer due care crime

208. Intellectual property is an intangible (you can't touch it) asset that is the result of creativity (the use of intellect). Which of the following U.S. laws or regulations protects intellectual proper for up to 70 years?
   a. Patent law
   b. Digital Rights Management
   c. Trademark law
   d. Copyright law

209. ISC2 code of ethics is important for a CISSP and strict adherence to this Code is a condition of certification. Which of the following would you consider to be least important?
   a. Provide diligent and competent service to principals (employers)
   b. Advance and protect the profession
   c. Act honorably, honestly, justly, responsibly, and legally
   d. Protect society, the commonwealth (nation), and the infrastructure

210. Compliance is ensuring that your organization's policies follow guidelines, specifications, legislation, or regulations, including local, state, federal, and industry-accepted regulations. In which area is compliance most important?
    a. Legislative and regulatory
    b. Payment Card Industry
    c. Privacy of your employee's information
    d. Guidelines for due care and due diligence.

211. There have been some recent changes in best practices and standards. Which of the following could be considered a new stress for the CISSP exam?
    a. Asset valuation for risk management
    b. Plan Do Check Act
    c. Continuous improvement
    d. Employment candidate screening

212. Threat modeling is a systematic approach used to understand how different threats could be realized and how a successful compromise could take place. After determining and diagramming potential attacks what would typically be done next.
    a. Perform a reduction analysis
    b. Develop new policies
    c. Prepare a Gantt chart
    d. Identifying threats and threat agents

213. A data owner is an important role in the enterprise. The owner controls the process of defining IT service levels, supporting the review of controls, and authorizing the enforcement of security controls to protect the specified information assets of the organization. Data Owners are also responsible for determining the data's sensitivity or classification levels. To whom is the data owner typically accountable?
    a. Auditors
    b. Board of Directors
    c. Data Custodian
    d. CISO

214. A policy is high level documents which directs how things should be done. Policies are developed by management to clearly transmit the rules, guiding strategy and philosophy of management to all employees An early step in developing any good policy is _____ .
    a. Defining procedures
    b. Polyinstantiation
    c. Evaluation of lessons learned
    d. Scoping

215. A multi-level security model allows a computer system to process information with different sensitivities (i.e., at different security levels). It may permit simultaneous access by users with different security clearances and need-to-know. The formal model which provides for No Write Down is _____ .
    a. Brewer Nash
    b. Biba
    c. Bell LaPadula
    d. Clark Wilson

216. Hashing is often used in forensic analysis. It is used to verify that an exact copy of the original media has been made for examination. Hashes can also help in finding or eliminating some specific files. During forensic analysis which algorithm would you recommend be used for determining accurate copies?
    a. SHA1
    b. MD5
    c. Quantum
    d. SHA2

217. Chain of custody is a document that indicates various details about evidence across its life cycle. It begins with the time and place of discovery and identifies who discovered the evidence, who secured it, who collected it, who transported it, who protected it while in storage, and who analyzed it. Where would be the typical place a hard drive being store for evidence be placed?
    a. BitLocker
    b. Vault
    c. Safe
    d. Faraday Cage

218. NIST developed the Risk Management Framework (RMF) to provide a more flexible, dynamic, approach for effective management of information system-related security risk in highly diverse environments and throughout the system development life cycle. The RMF identifies six steps that provide a disciplined and structured process for managing mission/business risk associated with the operation and use. What is the second step of the RMF?
    a. Perform a Business Impact Analysis
    b. Categorize the information system
    c. Assess the security controls
    d. Select an initial set of baseline security controls

219. Mary is developing an application for use in her company domain. She intends to use an RSA key exchange then switch to faster AES algorithm to transfer large amounts of data securely. What will be needed to secure the session key?
    a. Sender's Private Key
    b. Recipient's X509 Digital Certificate
    c. Sender's Public Key
    d. Pseudo Random Number Generator

220. Physical security controls are your first line of defense and should be designed so that the breach of any one will not compromise the physical security of the organization. CCTV cameras, mantraps, lighting, guards, dogs, and locks are but a few of the layers of physical security. Which area would it be most appropriate to install physical detective and deterrent controls to protect Ethernet appliances?
    a. Faraday Barrier
    b. Wiring Closet
    c. Plenum Space
    d. HVAC

221. Many networking protocols operate at a single level of the OSI model. A few such as ATM and DNP3 are said to operate at multiple levels. Where would you expect to find DNP3 used?
    a. To tie together APIs on an authentication system
    b. In core routers on the Internet
    c. In conjunction with routers running OSPF
    d. In a SCADA or ICS systems

222. IEEE 802.11i is a security amendment for the IEEE 802.11 wireless standard. It defines two new security protocols, Temporal Key Integrity Protocol (TKIP) for symmetric key generation and the use of_____ .
    a. AES for strong encryption
    b. A mandatory RADIUS server for strong authentication
    c. RC4 as a strong replacement for WEP
    d. Digital signatures for non-repudiation

223. Which type of law deals with grievances or wrongs against individuals or companies that result in damages or loss.
    a. Intellectual property
    b. Criminal
    c. Tort
    d. Regulatory

224. A distributed network is a type of computer network that is spread over different networks typically in different locations. If you were using this type of system a good way to speed access to large files would be to implement which of the following?
    a. Proxy for web caching
    b. Reverse proxy for load balancing
    c. Content Distribution Network
    d. Private cloud for IaaS

225. Virtual machine is software enabling several operating systems to run simultaneously run on a single PC without interfering with each other. A hypervisor in virtualized systems can be thought of as an operating system for operating systems. You are thinking of trying virtualization for some hosts in your DMZ. What would be a best practice?
   a. Setup a Bastion Host as a decoy
   b. Install an IDPS to monitor for incidents
   c. Use a type 2 hypervisor with Linux to host guest OSs
   d. Use a type 1 hypervisor to host guest OSs

226. Physical separation (decoupling) of the network control plane of packets from the data plane (hardware) is typically accomplished by _____ .
   a. Software Defined Networking
   b. Platform as a Service (PaaS)
   c. Software Defined Storage
   d. Implementing PVLANs

227. Federated Identity Management (FIM) is a model that enables companies to allow registered users of their domain to access information from other domains in a smooth way. A federation can be best defined as _____ .
   a. Security Assertion Markup
   b. An alliance
   c. Single Sign On (SSO)
   d. An authentication system

228. Everyone should understand their responsibilities for achieving adequate information security and for managing information system-related security risks. Step three of the RMF stresses the need to assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly. A common assessment of the network by your administrators is called a _____ .
   a. Business Impact Analysis
   b. Pen Test
   c. Vulnerability Scan
   d. Port Scan

229. An IDS/IPS can implement signature-based and/or anomaly based intrusion detection. Anomaly detection in the IDS/IPS can identify unusual and abnormal patterns of activity against an established baseline. To verify this system is working properly it is desirable to check the response to _____ .
   a. Fuzzing
   b. XML injection
   c. Code review
   d. Synthetic Transactions

230. A CISSP is expected to be capable of establishing and maintaining security awareness and training to help in the prevention of _____.
   a. Social Engineering Attacks
   b. Lack of Due Care and Diligence
   c. Privilege Escalation
   d. Escalation from an Incident to a Disaster

231. Computer forensics techniques are used to search, preserve and analyze information on computer systems to find potential evidence for a trial. If you are defending against a tort what would your forensics be focused on if encrypted credit card information has been stolen and used even though you had effective controls in place?
   a. E Discovery
   b. Criminal Investigation
   c. Operational Investigation
   d. Steganography

232. Which of the following involves people with the requisite experience and education evaluating threat scenarios and rating the, potential loss and severity of each threat based on their experience
   a. Data Mining
   b. Qualitative risk analysis
   c. Risk assessment
   d. Risk management

233. What are the assessment results produced by the application of an assessment procedure to a system called?
   a. Plan of Action and Milestones
   b. Assessment Findings
   c. Risk Assessment
   d. Vulnerability Assessment

234. Thresholds of acceptable user errors and suspicious activities which can trigger and alert are called.
   a. Critical path analysis
   b. Remote journaling
   c. Clipping levels
   d. TOC/TOU

235. Java security employs a(n) _____ so an applet is restricted and fairly safe.
   a. ActiveX
   b. Sandbox
   c. Artificial neural network
   d. Deadlock situation

236. The crossover error rate (CER) _____.
   a. May be hidden by a stealth virus
   b. Is hidden for out-of-band communication
   c. Is concealed in a Trojan horse program
   d. Is the point at which FRR and FAR are equal

237. This IP address A address of 2002:0000:0000:3210:0800:200C:00CF:1234 could be shortened to _____ .
   a. 2002::321:8:200C:CF:1234
   b. 2002::3210:0800:200C:00CF:1234
   c. 2002::3210:800:200C:CF:1234
   d. 2002::3210:8:200C:CF:1234

238. A firewall can either be software configured on a computer system or a network appliance. Both are designed to block unauthorized access while permitting authorized communications. The firewall which dynamically open ports is called a _____.
   a. Proxy
   b. Stateful
   c. Stateless
   d. Packet Filter

239. An IPSec _____ defines how two entities have negotiated and agreed to utilize security services to communicate securely.
   a. Oakley negotiation
   b. Tunnel negotiation
   c. Security Association (SA)
   d. SAML (Security Association Markup Language)

240. Unauthorized access points created by programmers as a rescue option or malicious programs inserted by an attacker that allows an unauthorized entity to gain access into a system or program are called.
   a. Remote Access Tool
   b. Back Door
   c. Cracked Door
   d. Trojan Horse

241. Sending messages to Bluetooth-capable devices without the permission of the owner/user is a prank called_____.
   a. Blue Boffing
   b. Blue Snarfing
   c. Blue Fishing
   d. Blue Jacking

242. Which of the following is a proactive, long term, plan regarding the ability of critical business functions to continue in operation even in the face of serious threats.
   a. Incident Response Plan
   b. Disaster Recovery Plan
   c. Business Continuity Plan
   d. Business Resumption Plan

243. What is the process of storing copies of private keys by a certificate authority called?
   a. Key Continuity
   b. Key Journaling
   c. Key Escrow
   d. Software Escrow

244. A trusted authority in a network that generates asymmetric key pairs, issues and manages security credentials, publishes a CRL and more is a _____ .
   a. Online Certificate Status Authority
   b. Registration Authority
   c. Certification Authority
   d. Certificate Authority

245. Cloud computing can be defined as virtual servers, resources, applications services or anything you consume over the Internet. Which system offers a capability to the consumer to provision processing, storage, networks, and other fundamental computing resources?
   a. MaaS
   b. PaaS
   c. IaaS
   d. SaaS

246. *Common Criteria* (CC) was developed as an international IT evaluation criterion. Common Criteria is designed around Trusted Computing Base (TCB). EALs provide a specific level of confidence in the security functions of the system being analyzed. Which level would be most appropriate for a high security environment?
   a. EAL Level 1
   b. EAL Level 2
   c. EAL Level 4
   d. EAL Level 5

247. One way to exfiltrate data is using a secret communication path that allows data transfer in a way that violates the security policy. Such a path is called a _____ .

a. Tunnel
b. Overt Channel
c. Secure Channel
d. Covert Channel

248. Server side attacks an issue when users go to the Internet. One common issue is a form of malicious code injection attack where an attacker is able to compromise a web server and inject their own malicious code into the content sent to other visitors. This is commonly called _____ .

a. XML Injection
b. Cross Site Scripting
c. Buffer Overflow
d. Cross-site Request Forgery

249. Data remanence is data (remaining magnetism) that persists beyond means such as formatting used to delete it. This residual information may cause inadvertent disclosure of sensitive information. The best way to insure data remanence is not an issue is to _____ .

a. Destroy the circuit board of the drives
b. Smash the old hard drives
c. Degauss old hard drives
d. Overwrite old drives three times

250. Lots of testing is needed during software development. Separation of duties is followed so one programmer can serve as a check on others. Which test is commonly carried out after changes to validate and verify the code?

a. Acceptance testing
b. Regression testing
c. Integration testing
d. Unit testing

Final Practice Exam Answer Key

1	A	43	A	85	C	127	B	169	D	211	C
2	A	44	D	86	D	128	C	170	B	212	A
3	A	45	A	87	A	129	B	171	B	213	D
4	B	46	A	88	A	130	C	172	B	214	D
5	A	47	D	89	G	131	C	173	A	~~215~~	~~B~~
6	B	48	A	90	C	132	B	174	A	216	D
7	C	49	C	91	B	133	D	175	A	217	B
8	B	50	D	92	B	134	B	176	B	218	D
9	C	51	C	93	A	135	C	177	A	219	B
10	C	52	B	94	B	136	A	178	A	220	B
11	D	53	C	95	C	137	A	179	C	221	D
12	A	54	D	96	A	138	C	180	C	222	A
13	D	55	B	97	C	139	D	181	A	223	C
14	D	56	C	98	C	140	B	182	C	224	C
15	B	57	D	99	C	141	B	183	B	225	D
16	B	58	D	100	A	142	D	184	A	226	A
17	C	59	C	101	D	143	C	185	C	227	B
18	F	60	A	102	D	144	B	186	D	228	C
19	D	61	C	103	B	145	C	187	C	229	D
20	C	62	B	104	D	146	D	188	A	230	A
21	A	63	B	105	D	147	A	189	D	231	C
22	A	64	C	106	C	148	B	190	B	232	B
23	B	65	C	107	B	149	B	191	A	233	B
24	C	66	B	108	C	150	C	192	C	234	C
25	C	67	B	109	C	151	B	193	B	235	B
26	A	68	C	110	C	152	D	194	A	236	D
27	C	69	D	111	A	153	A	195	C	237	C
28	C	70	D	112	C	154	B	196	A	238	B
29	A	71	D	113	C	155	C	197	B	239	C
30	A	72	B	114	A	156	B	198	C	240	B
31	B	73	D	115	C	157	C	199	A	241	D
32	B	74	A	116	B	158	B	200	B	242	C
33	D	75	A	117	A	159	D	201	C	243	C
34	B	76	A	118	B	160	C	202	D	244	D
35	D	77	C	119	D	161	A	203	A	245	C
36	D	78	C	120	C	162	A	204	A	246	D
37	C	79	A	121	D	163	C	205	D	247	D
38	D	80	C	122	C	164	A	206	B	248	B
39	D	81	B	123	A	165	A	207	C	249	C
40	D	82	C	124	C	166	A	208	D	250	B
41	B	83	A	125	D	167	B	209	B		
42	A	84	B	126	B	168	D	210	A		