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. Kerberos authentication
    d. RADIUS authentication

5. Which methodology is used to analyze operating system vulnerabilities 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. Your company has decided to allow users to dial into the network from remote locations. Because security is a major concern for your company, you must implement a system that provides centralized remote user authentication, authorization, and accounting. Which technology should you implement?
    a. VPN
    b. DMZ
    c. RADIUS
    d. Single sign-on

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

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

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

18. As a system administrator, you decide to implement audit trails to ensure that users are not performing unauthorized functions. What are you trying to determine?
    a. Identification
    b. Authorization
    c. Accountability
    d. Authentication

19. 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

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

21. 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 Novell network
    b. It is the authentication service used on a Novell network
    c. It is the directory service used on a Windows server 2003 network
    d. It is the authentication service used on a Windows server 2003 network

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

23. 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

24. 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 mechanisms should you implement?
    a. Auditing techniques
    b. Data recovery techniques
    c. Authentication techniques
    d. Access control techniques

25. Your manager has instructed you to use the syskey utility in your Windows server 2003 domain. What is the function of this utility?
    a. To generate one-time passwords
    b. To encrypt the UNIX password file
    c. To add complexity to the password encryption process in a UNIX system
    d. To encrypt the Windows security accounts management (SAM) database

26. 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)

27. 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

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

29. 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

30. 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 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

31. 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

32. Which type of virus is specifically designed to infect programs as they are loaded into memory?
    a. Boot sector replication
    b. Companion
    c. Nonresident
    d. Resident

33. 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

34. 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. And abstractor

35. Which type of virus installs itself under the antivirus system and intercepts any calls that the antivirus system makes to the operating system?
    a. Script virus
    b. Meme virus
    c. Boot sector virus
    d. Tunneling virus

36. You need to view 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

37. 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

38. Your company has an online transaction processing (OLTP) environment for customers. Management is concerned with the atomicity of the OLTP environment and a 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

39. You have configured auditing for several security events on your Windows server 2003 network. The event viewer logs are backed up on a daily basis. You configure the following settings for the security log: 1) The maximum event log size setting is set to 70, 400 KB, 2) The Audit: Shut down system immediately if unable to log security events setting is enabled, and 3) The Do not overwrite events setting is enabled. A few weeks later, the computer mysteriously shuts down. You discovered that the security event log settings are causing the problem. You could do all of the following except which to correct the problem?
    a. Configure automatic log rotation
    b. Disable the Audit: Shut down system immediately if unable to log security events setting
    c. Enable the Overwrite events as needed setting
    d. Decrease the size of the security log

40. Which statement correctly defines an application control?
    a. It is a mechanism to control user access to resources
    b. It determines controls that are functioning with in an operating system
    c. It ensures that valid transactions are processed accurately and only wants
    d. It ensures that a system performs with a high throughput without any time lag

41. Recently, your organization's website was attacked. The graphics and text on the home page were modified by the attacker. Of which type of threat is this an example?
    a. Financial fraud
    b. Privileged access
    c. Vandalism
    d. Theft of intellectual property

42. 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

43. 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

44. 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

45. Which statement is correct for database security?
    a. Data identification language implements security on data components
    b. Data manipulation language (DML) implements access control through authorization
    c. Bind variables provide access control through implementing granular restrictions
    d. Data control language (DCL) implements security through access control and granular restrictions

46. 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

47. 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. Execute a well-written program

48. 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

49. 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

50. Which statement correctly defines spamming attacks?
    a. Repeatedly sending identical e-mails to a specific address
    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

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

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

53. Which role is considered the leader of the business continuity plan committee and is responsible for the overall success of the business continuity plan?
    a. IT manager
    b. Security manager
    c. Disaster recovery manager
    d. Business continuity coordinator

54. During the business impact analysis (BIA), the business continuity committee identifies a server that has a maximum tolerable downtime (MTD) of 48 hours. Into which maximum tolerable downtime (MTD) category should the system be placed?
    a. Critical
    b. Urgent
    c. Important
    d. Normal
    e. Nonessential

55. 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)

56. 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

57. One member of the business continuity plan committee has identified several governmental regulations that will affect the business continuity plan for several computers. Which step of the business continuity process identifies this type of data?
    a. Conduct the business impact analysis
    b. Develop recovery strategies
    c. Test the plan, and conduct training
    d. Develop the contingency plan

58. 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

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

60. 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

61. What occurs during the reconstitution phase 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

62. 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. Executive succession plan
    d. Reciprocal agreement

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

64. 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

65. 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

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

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

68. 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

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

70. 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)

71. 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)

72. 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 Monday morning. How many backups will be needed to be restored?
    a. One
    b. Two
    c. Three
    d. Four

73. Which term refers to the amount of time 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

74. 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

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

76. Your organization has decided 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 secret keys over a nonsecure medium
    d. Unauthorized users exchange public keys over a nonsecure medium

77. 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

78. Which statement is NOT true of cryptanalysis?
    a. It is used to test the strength of an algorithm
    b. It is a tool used to develop a secure cryptosystem
    c. It is used to forge coded signals that will be accepted as authentic
    d. It is a process of attempting reverse engineering of a cryptosystem

79. 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

80. 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. Privacy enhanced Mail (PEM)
    c. Message security protocol (MSP)
    d. Pretty good privacy (PGP)

81. 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

82. Which service provided by a cryptosystem turns information into unintelligible data?
    a. Non-repudiation
    b. Authorization
    c. Integrity
    d. Confidentiality

83. You are the security administrator for an organization. Management decides that all communication on the network should be encrypted using the data encryption standard (DES) algorithm. Which statement is true of this algorithm?
    a. The effective key size of DES 64 bits
    b. A triple DES (3DES) algorithm uses 48 rounds of computation
    c. A DES algorithm uses 32 rounds of computation
    d. A 56 bit DES encryption is 256 times more secure than a 40 bit DES encryption

84. Your organization has decided to implement a website for customers to purchase your organization's products. The website will use the SET protocol. Which statement is true of this protocol?
    a. SET uses 3DES for symmetric key exchange
    b. SET works at the network layer of the OSI model
    c. SET uses digital signatures and digital certificates to conduct and verify an electronic transaction
    d. SET automatically transmits a user's credit card information to a CA when an online purchase is made

85. What is contained within an X.509 CRL?
    a. Digital certificates
    b. Private keys
    c. Public keys
    d. Serial numbers

86. You want to send a file to a coworker named Maria. You do not want 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 encryption
    d. Asymmetric encryption

87. 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

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

89. Which statement is true of the rijndael algorithm?
    a. Rijndael uses variable block lengths and variable key lengths
    b. Rijndael uses fixed block lengths and pics to key lengths
    c. Rijndael uses variable block lengths and fixed key lengths
    d. Rijndael uses fixed block lengths and variable key lengths

90. 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

91. Your company hosts several public web sites on its Web Server. Some of the sites implement these 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. SSL has two possible session key lengths: 40 bit and 128 bit

92. 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

93. While developing your organization's website, the web developer needs to ensure that certain messages are transmitted securely. Which technology would be the best choice for this purpose?
    a. HTTP
    b. HTTPS
    c. S–HTTP
    d. SET

94. 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. Remote shell (rsh)
    b. Secure shell (SSH)
    c. HTTP secure (HTTPS)
    d. Internet protocol security (IPSec)

95. Which hashing algorithm uses a 192 bit hashing value and was developed for 64-bit systems?
    a. Tiger
    b. HAVAL
    c. SHA
    d. MD5

96. Which statement is NOT true of the operation modes of the data encryption standard (DES) algorithm?
    a. Electronic codebook (ECB) mode operation is best suited for database encryption
    b. ECB is the easiest and fastest DES mode that can be used
    c. ECB repeatedly uses produced ciphertext to encipher a message consisting of blocks
    d. cipher block chaining (CBC) and cipher feedback (CFB) mode are best used for authentication

97. 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

98. 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

99. You have been specifically asks to implement a stream cipher. Which cryptographic algorithm could you use?
    a. RC4
    b. RC5
    c. RC6
    d. MD5

100. 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