**MIS5206** **Your Name _____**
**Week 14** **Date _____**

1. Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

   a) User from within could send a file to an unauthorized person
   b) Hacker may be able to use the FTP service to bypass the firewall
   c) FTP could significantly reduce the performance of a DMZ server
   d) FTP services could allow a user to download files from unauthorized sources

2. During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

   a) An unauthorized user may use the ID to gain access
   b) Passwords are easily guessed
   c) User access management is time consuming
   d) User accountability may not be established

3. What method might an IS auditor utilize to test wireless security at branch office locations?

   a) War dialing
   b) War driving
   c) Social engineering
   d) Password cracking

4. Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation Computers on the network that are located:

   a) At the backup site
   b) In employees homes
   c) At the Enterprise's remote offices
   d) On the enterprise's internal network

6. An organization's IT director has approved the installation of a wireless local area network (WLAN) access point in a conference room for a team of consultants to access the Internet with their laptop computers. The BEST control to protect the corporate servers from unauthorized access is to ensure that:

   a) Encryption is enabled on the access point.
   b) The conference room network is on a separate virtual local area network (VLAN)
   c) Antivirus signatures and patch levels are current on the consultants' laptops
   d) Default user IDs are disabled and strong passwords are set on the corporate servers

7. The review of router access control lists should be conducted during:

   a) An environmental review
   b) A network security review
   c) A business continuity review
   d) A data integrity review

8. Which of the following attacks targets the Secure Sockets Layer (SSL)?

   a) Man-in-the middle

b) Dictionary
c) Password sniffing
d) Phishing

9. Event log entries related to failed local administrator logon attempts are observed by the IS auditor. Which of the following is the MOST likely cause of multiple failed login attempts?

a) SYN flood attacks
b) Social engineering
c) Buffer overflow attacks
d) Malicious code attacks

10. ABC Inc. offers a number of services though its web site. During one day, senior executives of ABC Inc. were surprised to discover that sensitive data on their servers were being leaked to unauthorized individuals on the Internet. Post incident investigations revealed that ABC lnc.'s key servers were infected with a Trojan. The incident occurred after deployment of a newly acquired module from a software vendor, which was tested on test servers in accordance with functional specifications. The incident had gone unnoticed for a period of about four weeks. A potential cause of the leak may have been malware embedded in the new module. What approach might have detected this problem?

a) Encryption of server data
b) Updated antivirus software
c) Intrusion detection/intrusion prevention systems (lDS/IPSs)
d) Secure sockets layer (SSL)/transport layer security (TLS)

11. Receiving an electronic data interchange (EDI) transaction and passing it through the communication's interface stage usually requires:

a) Translating and unbundling transactions
b) Passing data to the appropriate application system
c) Routing verification procedures
d) Creating a point of receipt audit log

12. Which of the following is the MOST reliable sender authentication method?

a) Digital signatures
b) Asymmetric cryptography
c) Digital certificates
d) Message authentication code

13. Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

a) Implement column- and row-level permissions
b) Enhance user authentication via strong passwords
c) Organize the data warehouse into subject matter-specific databases
d) Log user access to the data warehouse

14. During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

a) An unauthorized user may use the ID to gain access
b) User access management is time consuming
c) User accountability is not established

d) Passwords are easily guessed

15. Which of the following is the BEST way to satisfy a two-factor user authentication?

a) A smart card requiring the user's personal identification number (PIN)
b) User ID along with password
c) Iris scanning plus fingerprint scanning
d) A magnetic card requiring the user's PIN

16. An organization has experienced a large amount of traffic being re-routed from its Voice-over IP (VoIP) packet network. The organization believes it is a victim of eavesdropping. Which of the following could result in eavesdropping of VoIP traffic?

a) Corruption of the address resolution protocol (ARP) cache in Ethernet switches
b) Use of a default administrator password on the analog phone switch
c) Deploying virtual local area networks (VLANs) without enabling encryption
d) End users having access to software tools such as packet sniffer applications

17. Which of the following would be considered an essential feature of a network management system?

a) A graphical interface to map the network topology
b) Capacity to Interact with the Internet to solve the problems
c) Connectivity to a help desk for advice on difficult issues
d) An export facility for piping data to spreadsheets

18. An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

a) The data collected on attack methods
b) The information offered to outsiders on the honeypot
c) The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
d) The risk that the honeypot would be subject to a distributed denial-of-service attack

19. Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

a) Data Encryption Standard (DES)
b) Advanced Encryption Standard (AES)
c) Triple DES
d) RSA

20. Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability and integrity of data?

a) Secure Sockets Layer (SSL)
b) Intrusion detection system (IDS)
c) Public key infrastructure (PKI)
d) Virtual private network (VPN)

21. Which of the following is the MOST effective control when granting temporary access to vendors?

a) Vendor access corresponds to the service level agreement (SLA).
b) User accounts are created with expiration dates and are based on services provided
c) Administrator access is provided for a limited period

d) User IDs are deleted when the work is completed

22. Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

a) Simple Network Management Protocol
b) File Transfer Protocol (FTP)
c) Simple Mail Transfer Protocol (SMTP)
d) Telnet

23. While downloading software, a hash may be provided to:

a) Ensure that the software comes from a genuine source
b) Ensure that the software is the correct revision number
c) Ensure that the software has not been modified
d) Serve as a license key for paid users of the software

24. Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

a) Computation speed
b) Ability to support digital signatures
c) Simpler key distribution
d) Greater strength for a given key length

25. The logical exposure associated with the use of a checkpoint restart procedure is:

a) Denial of service
b) An asynchronous attack
c) Wiretapping
d) Computer shutdown

26. Due to a recent economic downturn, an IT organization has terminated several administrators and consolidated all IT administration at its central headquarters. During an IT audit, the auditor determines that the organization has implemented remote administration connectivity to each site using low-cost digital subscriber line (DSL) connections and an automated simple network management protocol (SNMP)-based monitoring system. What would be the GREATEST concern?

a) The authentication methods used for remote administration may be inadequate
b) Physical security at remote sites may not be adequate
c) Terminated employees may retain access to systems at remote sites
d) The connection to remote sites is not using a VPN for connectivity

27. The cryptographic hash sum of a message is recalculated by the message's receiver. This is to ensure:

a) The confidentiality of the message
b) Nonrepudiation by the sender
c) The authenticity of the message
d) The integrity of data transmitted by the sender

28. An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

a) The tools used to conduct the test
b) Certifications held by the IS auditor
c) Permission from the data owner of the server
d) An intrusion detection system (IDS) is enabled

29. Among the following controls, what is the BEST method to prevent inappropriate access to private and sensitive information through a business application?

a) Two-factor authentication access control
b) Encryption of authentication data
c) Role-based access control (RBAC)
d) Effective segregation of duties (SoD)

30. To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's

a) Public key and then encrypt the message with the receiver's private key
b) Private key and then encrypt the message with the receiver's public key
c) Public key and then encrypt the message with the receiver's public key
d) Private key and then encrypt the message with the receiver's private key

31. Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

a) Halon gas
b) Dry pipe sprinklers
c) Carbon dioxide gas
d) Wet-pipe sprinklers

32. In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

a) Appliances
b) Operating system-based
c) Host-based
d) Demilitarized

33. An IS auditor is reviewing an organization's controls over e-mail encryption. The company's policy states that all sent e-mail must be encrypted to protect the confidentiality of the message because the organization shares nonpublic information through e-mail. To ensure that personnel are complying with the policy, an IS auditor must be sure the message is encrypted with the sender's:

a) Private key and decrypted with the sender's public key
b) Private key and decrypted with the sender's private key
c) Private key and decrypted with the recipient's private key
d) Public key and decrypted with the recipient's private key

Encrypting with the public key and decrypting with the recipient's private key ensures message confidentiality.

34. To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

a) Online terminals are placed in restricted areas
b) ID cards are required to gain access to online terminals
c) Online access is terminated after a specified number of unsuccessful attempts
d) Online terminals are equipped with key locks

35. An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers-one filled with CO2, the other filled with Halon. Which of the following should be given the HIGHEST priority in the auditor's report?

a) The Halon extinguisher should be removed because Halon has a negative impact on the atmospheric ozone layer
b) Both Fire suppression systems present a risk of suffocation when used in a closed room
c) The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).
d) The documentation binders should be removed from the equipment room to reduce potential risks

36. The responsibility for authorizing access to a business application system belongs to the:

a) Data owner
b) IT security manager
c) Security administrator
d) Requestor's immediate supervisor

37. An IS auditor notes that the |intrusion detection system (IDS) log entries related to port scanning are not being analyzed This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

a) Denial of service
b) Replay
c) Social engineering
d) Buffer overflow

Prior to launching a denial-of-service attack, hackers often use automatic port scanning software to acquire information about the subject of their
attack. A replay attack is simply sending the same packet again. Social engineering exploits end-user vulnerabilities, and buffer overflow attacks
exploit poorly written code.

38. What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

a) The VPN logon could be spoofed
b) Traffic could be sniffed and decrypted
c) Malicious code could be spread across the network
d) The VPN gateway could be compromised

39. Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

a) Processing power
b) Volume of data
c) Key distribution
d) Complexity of the algorithm

40. During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

a) An unauthorized user may use the ID to gain access
b) User access management is time consuming
c) Passwords are easily guessed
d) User accountability may not be established

41. Which of the following is the BEST control to prevent the deletion of audit logs by unauthorized individuals in an organization?

a) Actions on log tiles should be tracked in another log
b) Only select personnel should have rights to view or delete audit logs
c) Write access to audit logs should be disabled
d) Backups of audit logs should be performed periodically

42. Which of the following is the BEST control to implement in order to mitigate the risk of an insider attack?

a) Ensure that a comprehensive incident response plan has been put into place
b) Log all user activity for critical systems
c) Perform a criminal background check on all employees or contractors
d) Limit access to what is required for an individual's job duties

43. The information security policy that states that "each individual must have their badge read at every controlled door" addresses which of the following attack methods?

a) Piggybacking
b) Dumpster diving
c) Impersonation
d) Shoulder surfing

44. Which of the following message services provides the STRONGEST evidence that a specific action has occurred?

a) Proof of delivery
b) Nonrepudiation
c) Proof of submission
d) Message origin authentication

Yes, these other methods provide some proof – non-repudiation is the strongest proof

45. An IS auditor performing a review of a firewall upgrade project discovered that several ports were left open that were not required for business purposes. It was determined that the ports were opened for a test server that was no longer being used. What is the BEST control to recommend so that this situation will not recur?

a) Firewall rule changes should happen only if the changes are properly documented.
b) Test servers should never be connected via the production firewall.

c) IT management should engage a third-party to review the firewall rules and to conduct a penetration test on a quarterly basis
d) The security administrator should perform periodic reviews to validate firewall rules

46. Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

a) Wet-pipe sprinkler system
b) Dry-pipe sprinkler system
c) FM-200 system
d) Carbon dioxide-based tire extinguishers

47. Which of the following will reduce the incidence of forgotten passwords while accessing multiple applications and maintaining the integrity of identification management controls?

a) Reducing the strength of passwords
b) Having a single sign-on (SSO)
c) Having two-factor authentication
d) Allowing the use of previous passwords

48. An organization is developing a new web-based application to process orders from customers. Which of the following security measures should be taken to protect this application from hackers?

a) Ensure that ports 80 and 443 are blocked at the firewall
b) Inspect tile and access permissions on all servers to ensure that all tiles have read-only access
c) Perform a web application security review
d) Make sure that only the IP addresses of existing customers are allowed through the firewall

49. Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

a) Registration authority
b) Certificate authority (CA)
c) Certification relocation list (CRL)
d) Certification practice statement

50. A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

a) Rewrite the hard disk with random Os and 1s
b) Demagnetize the hard disk
c) Physically destroy the hard disk
d) Low-level format the hard disk

51. An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

a) Increase the frequency for data replication between the different department systems to ensure timely updates
b) Centralize all request processing in one department to avoid parallel processing of the same request

c) Change the application architecture so that common data are held in just one shared database for all departments
d) Implement reconciliation controls to detect duplicates before orders are processed in the systems

52. During a review of intrusion detection logs, an IS auditor notices traffic coming from the Internet, which appears to originate from the internal IP address of the company payroll server. Which of the following malicious activities would MOST likely cause this type of result?

a) A denial-of-service (DoS) attack
b) Spoofing
c) Port scanning
d) A man-in-the-middle attack

53. A human resources (HR) company offers free public wireless Internet access to its guests, after authenticating with a generic user ID and password. The generic ID and password are requested from the reception desk. Which of the following controls BEST addresses the situation?

a) The password for the wireless network is changed on a weekly basis
b) A stateful inspection firewall is used between the public wireless and company networks
c) The public wireless network is physically segregated from the company network
d) An intrusion detection system (IDS) is deployed within the wireless network

54. Which of the following provides the MOST relevant information for proactively strengthening security settings?

a) Bastion host
b) Honeypot
c) Intrusion detection system (IDS)
d) Intrusion prevention system

55. The MOST likely explanation for a successful social engineering attack is:

a) That computers make logic errors
b) That people make judgment errors
c) The computer knowledge of the attackers
d) The technological sophistication of the attack method

56. Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

a) Encrypts the information transmitted over the network
b) Makes other users' certificates available to applications
c) Facilitates the implementation of a password policy
d) Stores certificate revocation lists (CRLs)

57. Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

a) Policies that require instant dismissal if such devices are found
b) Software for tracking and managing USB storage devices
c) Administratively disabling the USB port
d) Searching personnel for USB storage devices at the facility's entrance

58. An IS auditor noticed that newly hired employees were sharing passwords while logging on to an application system, which is against company policy. Which of the following would be the MOST effective method to control this problem?

a) Providing security awareness training to users
b) Assigning responsibility to the department head
c) Training IT personnel
d) Terminate Employees who use USB drives against company policy

59. An online stock trading Firm is in the process of implementing a system to provide secure e-mail exchange with its customers. What is the BEST option to ensure confidentiality, integrity and nonrepudiation?

a) Symmetric key encryption
b) Digital signatures
c) Message digest algorithms
d) Digital certificates

60. Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

a) Computation speed
b) Simpler key distribution
c) Greater strength for a given key length
d) Ability to support digital signatures

61. Which of the following types of transmission media provide the BEST security against unauthorized access?

a) Copper wire
b) Twisted pair
c) Fiber optic cables
d) Coaxial cables

62. Which of the following is the MOST effective control for restricting access to unauthorized Internet sites in an organization?

a) Routing outbound Internet traffic through a content-filtering proxy server
b) Routing inbound Internet traffic through a reverse proxy sewer
c) Implementing a firewall with appropriate access rules
d) Deploying client software utilities that block inappropriate content

A content-filtering proxy server will effectively monitor user access to Internet sites and block access to unauthorized web sites.

63. During an IS audit the IS auditor discovers that a wireless network |s used within the enterprise s headquarters What is the FIRST thing that the auditor should check?

a) The signal strength outside of the building
b) The configuration settings
c) The number of clients connected
d) The IP address allocation mechanism

64. Which of the following is the MOST effective control over visitor access to a data center?

a) Visitors are escorted
b) Visitor badges are required
c) Visitors sign in
d) Visitors are spot checked by operators

65. Which of the following would prevent unauthorized changes to information stored in a server's log?

a) Write-protecting the directory containing the system log
b) Writing a duplicate log to another sewer
c) Daily printing of the system log
d) Storing the system log in write-once media

66. Applying a digital signature to data traveling in a network provides:

a) Confidentiality and integrity
b) Security and nonrepudiation
c) Integrity and nonrepudiation
d) Confidentiality and nonrepudiation

67. In a client-server architecture, a domain name service (DNS) is MOST important because it provides the

a) The address of the domain server
b) Resolution service for the name/address
c) IP addresses for the Internet
d) Domain name of the system

68. Which of the following would MOST effectively reduce social engineering incidents?

a) Security awareness training
b) Increased physical security measures
c) E-mail monitoring policy
d) Intrusion detection systems

69. An IT executive of an insurance company asked an external auditor to evaluate the user IDs for emergency access (tire call ID). The IS auditor found that tire call accounts are granted without a predetermined expiration date. What should the IS auditor recommend?

a) Review of the access control privilege authorization process
b) Implementation of an identity management system (IMS)
c) Enhancement of procedures to audit changes made to sensitive customer data
d) Granting of tire call accounts only to managers

70. After reviewing its business processes, a large organization is deploying a new web application based on a Voice-over IP (VoIP) technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

a) Fine-grained access control
b) Role-based access control (RBAC)
c) Access control lists
d) Network service access control