MIS5206 **Your Name _____**
Week 12 **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