MIS5206 **Your Name _____**
Week 13 **Date _____**

1. When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

   a) Use the IP address of an existing file server or domain controller
   b) Pause the scanning every few minutes to allow thresholds to reset
   c) Conduct the scans during evening hours when no one is logged-in
   d) Use multiple scanning tools since each tool has different characteristics

2. From a control perspective, the PRIMARY objective of classifying information assets is to:

   a) Establish guidelines for the level of access controls that should be assigned
   b) Ensure access controls are assigned to all information assets
   c) Assist management and auditors in risk assessment
   d) Identify which assets need to be insured against losses

3. Which of the following types of penetration tests simulates a real attack and is used to test incident handling and response capability of the target?

   a) Blind testing
   b) Targeted testing
   c) Double-blind testing
   d) External testing

4. Which of the following is a passive attack to a network?

   a) Message modification
   b) Masquerading
   c) Denial of service
   d) Traffic analysis

5. Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

   a) Overwriting the tapes
   b) Initializing the tape labels
   c) Degaussing the tapes
   d) Erasing the tapes

6. Which of the following wide area network (WAN) transmission techniques offers the BEST error and flow control procedures while transmitting data?

   a) Message switching
   b) Packet switching
   c) Circuit switching
   d) Virtual circuits

7. A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

   a) Introduce a secondary authentication method such as card swipe
   b) Apply role-based permissions within the application system
   c) Have users input the ID and password for each database transaction
   d) Set an expiration period for the database password embedded in the program

8. An IS Auditor has observed brute-force attacks on the administrator account. The BEST recommendation to prevent a successful brute force attack would be to:

   a) Increase the password length for the user
   b) Configure a session timeout mechanism
   c) Perform periodic vulnerability scans
   d) Configure a hard-to-guess username

9. A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?

   a) Audit logs are not enabled for the system
   b) A logon ID for the technical lead still exists
   c) Spyware is installed on the system
   d) A Trojan is installed on the system

10. Certification of an enterprise's public key by a recognized authority is essential because:

    a) The publicly available key might have been revoked
    b) Everyone has access to the enterprise's public key
    c) The enterprise's private key is not published
    d) The enterprise's public key may not be linked to the private key used

11. Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

    a) Install the vendor's security fix for the vulnerability
    b) Block the protocol traffic in the perimeter firewall
    c) Block the protocol traffic between internal network segments
    d) Stop the service until an appropriate security fix is installed

12. The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use

    a) Compression software to minimize transmission duration
    b) Functional or message acknowledgments
    c) A packet-filtering firewall to reroute messages
    d) Leased asynchronous transfer mode lines

13. Naming conventions for system resources are important for access control because they

    a) Ensure that resource names are not ambiguous
    b) Reduce the number of rules required to adequately protect resources
    c) Ensure that user access to resources is clearly and uniquely identified
    d) Ensure that internationally recognized names are used to protect resources

14. A hacker could obtain passwords without the use of computer tools or programs through the technique of

    a) Social engineering
    b) Sniffers
    c) Back doors
    d) Trojan horses

15. Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the Internet?

    a) Secure Sockets Layer (SSL) mode
    b) Tunnel mode with AH plus ESP
    c) Triple Data Encryption Standard (triple DES) encryption mode
    d) Transport mode with authentication header (AH) plus encapsulating security payload (ESP)

16. An IS auditor reviewing the operating system integrity of a server would PRIMARILY:

a) Verify that privileged programs or services cannot be invoked by user programs
b) Determine whether administrator accounts have proper password controls
c) Ensure that tile permissions are correct on configuration tiles
d) Verify that programs or services running on the server are from valid sources

17. An organization stores and transmits sensitive customer information within a secure wired network. IT has implemented an additional wireless local area network (WLAN) to support general-purpose staff computing needs. A few employees with WLAN access have legitimate business reasons for also accessing customer information. Which of the following represents the BEST control to ensure separation of the two networks?

a) Establish two physically separate networks
b) Implement virtual local area network (VLAN) segmentation
c) Install a dedicated router between the two networks
d) Install a firewall between the networks

18. 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 alter 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:

- Intrusion detection system (IDS)
- Vulnerability scan process
- Firewall rule set review
- Access control monitoring

19. What is the BEST way to verify that a digital signature is valid?

a) Verify that the sender's public key certificate is from a trusted certificate authority (CA)
b) Use a hash algorithm from the CA to determine whether the message has been tampered with
c) Verify the digital signature through a manual comparison of the hash value
d) Obtain the public key from the sender, and verify the digital signature

20. Which of the following Internet security threats could compromise integrity?

a) Theft of data from the client
b) Exposure of network configuration information
c) A Trojan horse browser
d) Eavesdropping on the net

21. Which of the following should concern an IS auditor when reviewing security in a client-server environment?

a) Protecting data using an encryption technique
b) Preventing unauthorized access using a diskless workstation
c) Enabling users to access and modify the database directly
d) Disabling floppy drives on the users' machines

22. A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

a) Dump the volatile storage data to a disk
b) Run the server in a fail-safe mode
c) Disconnect the web server from the network
d) Shut down the web server

23. An IS auditor at a bank is performing compliance testing and has discovered that one of the branches has virus signatures that have not been updated in over six months in this case, the IS auditor should recommend:

a) Security awareness and education regarding the importance of updating antivirus software
b) An automated process initiated from the main office to update antivirus software at each branch
c) Reconfiguration of the firewall to a most-restrictive policy and implementation of an intrusion prevention system (IPS)
d) That the branch re-certify the machines after the updates are installed

24. In Internet Protocol Security (IPSec), which of the following PRIMARILY provides data protection?

a) Semantic net
b) Encapsulated security payload (ESP)
c) Authentication header (AH)
d) Digital signature

25. 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) Denial-of-Service (DoS) attack
b) Spoofing
c) Port Scanning
d) A man in the middle attack

26. An employee has received a digital photo frame as a gift and has connected it to his/her work PC to transfer digital photos. The PRIMARY risk that this scenario introduces is that:

a) The photo frame storage media could be used to steal corporate data
b) The drivers for the photo frame may be incompatible and crash the user's PC
c) The employee may bring inappropriate photographs into the office
d) The photo frame could be infected with malware

27. Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

a) System analysis
b) Authorization of access to data
c) Application programming
d) Data administration

28. A new business application has been designed in a large, complex organization and the business owner has requested that the various reports be viewed on a "need to know" basis. Which of the following access control methods would be the BEST method to achieve this requirement?

a) Mandatory
b) Role based
c) Discretionary
d) Single Sign-On (SSO)

29. Certification of an enterprise's public key by a recognized authority is essential because:

a) The publicly available key might have been revoked
b) Everyone has access to the enterprise's public key
c) The enterprise's private key is not published
d) The enterprise's public key may not be linked to the private key used

30. When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

a) Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization
b) All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization
c) Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization
d) The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded