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

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

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

The correct answer is C.
Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat tolife, and water is environmentally friendly. Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

2. 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

3. 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.

4. 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

5. 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

6. 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

7. 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.

8. 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

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. 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 (I double checked and this is right!)
d) Carbon dioxide-based tire extinguishers

17. 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

18. 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

19. 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

20. 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) D Physically destroy the hard disk
d) Low-level format the hard disk

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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)

27. 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

Yes, 28 and 29 are missing ☺

30. 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

31. 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

32. 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.

33. 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

34. 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

35. 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

36. 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

37. 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

38. 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

39. 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

40. 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