MIS5206 **Your Name ________________________**
Week 11 **Date _________**

1. The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users may:

   a) Use this information to launch attacks
   b) Forward the security alert
   c) Implement individual solutions
   d) Fail to understand the threat

2. E-mail message authenticity and confidentiality is BEST achieved by signing the message using the

   a) Sender's private key and encrypting the message using the receiver's public key
   b) Sender's public key and encrypting the message using the receiver's private key
   c) Receiver's private key and encrypting the message using the sender's public key
   d) Receiver's public key and encrypting the message using the sender's private key

3. An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

   a) Run a low-level data wipe utility on all hard drives
   b) Erase all data file directories
   c) Format all hard drives
   d) Physical destruction of the hard drive

4. Which of the following anti-spam filtering techniques would BEST prevent a valid, variable-length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

   a) Heuristic (rule-based)
   b) Signature-based
   c) Pattern matching
   d) Bayesian (statistical)

5. Which of the following would be an indicator of the effectiveness of a computer security incident response team?

   a) Financial impact per security incident

b) Number of security vulnerabilities that were patched
c) Percentage of business applications that are being protected
d) Number of successful penetration tests

6. An organization has created a policy that defines the types of web sites that users are forbidden to access What IS the MOST effective technology to enforce this policy?

a) Stateful inspection firewall
b) Web content filter
c) Web cache server
d) Proxy server

7. When reviewing a digital certificate verification process, which of the following findings represents the MOST significant risk?

a) There is no registration authority (RA) for reporting key compromises
b) The certificate revocation list (CRL) is not current
c) Digital certificates contain a public key that is used to encrypt messages and verify digital signatures
d) Subscribers report key compromises to the certificate authority (CA)

8. The role of the certificate authority (CA) as a third party is to:

a) Provide secured communication and networking services based on certificates.
b) Host a repository of certificates with the corresponding public and secret keys issued by that CA
c) Act as a trusted intermediary between two communication partners.
d) Confirm the identity of the entity owning a certificate issued by that CA

9. For a discretionary access control to be effective, it must:

a) Operate within the context of mandatory access controls
b) Operate independently of mandatory access controls
c) Enable users to override mandatory access controls when necessary
d) Be specifically permitted by the security policy

10. At a hospital, medical personal carry handheld computer which contain patient health data. These handheld computers are synchronized with PCs which transfer data from a hospital database. Which of the following would be of the most importance?

a) The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss

b) The employee who deletes temporary tiles from the local PC, after usage, is authorized to maintain PCs
c) Timely synchronization is ensured by policies and procedures
d) The usage of the handheld computers is allowed by the hospital policy

11. A penetration test performed as part of evaluating network security:

a) Provides assurance that all vulnerabilities are discovered
b) Should be performed without warning the organization's management
c) Exploits the existing vulnerabilities to gain unauthorized access
d) Would not damage the information assets when performed at network perimeters

12. What should an organization do before providing an external agency physical access to its information processing facilities (lPFs)?

a) The processes of the external agency should be subjected to an IS audit by an independent agency
b) Employees of the external agency should be trained on the security procedures of the organization
c) Any access by an external agency should be limited to the demilitarized zone (DMZ)
d) The organization should conduct a risk assessment and design and implement appropriate controls

15. An organization is proposing to establish a wireless local area network (WLAN). Management asks the IS auditor to recommend security controls for the WLAN. Which of the following would be the MOST appropriate recommendation?

a) Physically secure wireless access points to prevent tampering
b) Use service set identifiers (SSIDs) that clearly identify the organization.
c) Encrypt traffic using the Wired Equivalent Privacy (WEP) mechanism.
d) Implement the Simple Network Management Protocol (SNMP) to allow active monitoring.

16. Which of the following encryption mechanisms is performed at the application layer of the open systems interconnection (OSI) model?

a) Secure sockets layer (SSL)
b) IP Security (lPSec)
c) Secure Shell (SSH)
d) Secure Hypertext Transfer Protocol (SHTTP)

17. A single sign-on (SSO) server is used to authenticate users to the network as the corporate identity system. The IS auditor has noticed that users may have

multiple IDs and that there is no enforced link between the human resources (HR) system and the identity authentication system. The IS auditor will MOST be concerned by which of the following?

a) User IDs are used in different applications
b) There is a lack of unique user IDs
c) Users may be assigned multiple system accounts
d) IDs are not using a single naming standard

18. Which of the following would MOST effectively enhance the security of a challenge-response based authentication system?

a) Selecting a more robust algorithm to generate challenge strings
b) Increasing the frequency of associated password changes
c) Increasing the length of authentication strings
d) Implementing measures to prevent session hijacking attacks

19. The MOST important difference between hashing and encryption is that hashing:

a) Is irreversible
b) Outputs the same length as the original message
c) Is concerned with integrity and security
d) Is the same at the sending and receiving end

20. Which of the following satisfies a two-factor user authentication?

a) Iris scanning plus finger print scanning
b) Terminal ID plus global positioning system (GPS)
c) A smart card requiring the user's personal identification number (PIN)
d) User ID along with password