**MIS5206** **Your Name ________________________**

**Week 10** **Date _________**

1. What best describes a Trojan Horse?
   a) A fast spreading worm with a destructive payload
   b) Malicious code disguised as or inserted into a legitimate program
   c) A type of macro virus designed to attack Microsoft Office applications
   d) Malicious code inserted into a legitimate program that launches when a specific condition is met
   e)
2. When an attacker sends unsolicited communication, it is an example of:
   a) Spoofing
   a) Spamming
   b) Crackers
   c) Sniffers

3. Which access control technique allows security officers to specify access security policies based on an organization's structure?
   a) Lattice
   b) MAC
   c) DAC
   d) RBAC - role-based access control

4. What are three principals of identification and authentication?
   a) Something you are, something you have, something you control
   b) Something you know, something you are, something you control
   c) Something you know, something you are, something you have
   d) Something you have, something you control, something you know

5. Which technique monitors networks and computer systems for signs of intrusion or misuse?
   a) Bell-LaPadula
   b) MAC
   c) TACACS
   d) IDS - Intrusion Detection System

6. Which remote access protocol sends the user ID and password in clear text?
   a) CHAP
   b) PAP - Password Authentication Protocol
   c) Kerberos
   d) RADIUS

7. Background checks are what type of control?
   a) Physical
   b) Administrative

c) Logical
d) Technical

8. Which access control technique allows a resource owner to control other user's access to an object?
a) DAC – Distributed Access Control
b) RBAC
c) Lattice
d) MAC

9 A fence is what type of access control?
a) Administrative
b) Technical
c) Logical
d) Physical

10. What are three methods of performing centralized remote authentication access control?
a) TACACS, RADIUS, and DIAMETER
b) TACACS, RADIUS, and Kerboros
c) SESAME, RADIUS, and TACACS
d) RADIUS, SSO, and TACACS

Terminal access controller access control system
Remote Authentication Dial In User Service
DIAMETER name is a pun on the RADIUS protocol
Kerboros - strong authentication for client/server applications by using secret-key cryptography
SESAME - Secure European System for Applications in a Multi-vendor Environment

11. Which of the following access control models is most commonly used by firewalls?
a) Role-Based Access Control (RBAC)
b) Rule-Based Access Control (RBAC)
c) Discretionary Access Control (DAC)
d) Mandatory Access Control (MAC)

12. Which of the following allows attackers to break passwords?
a) Spamming
b) Sniffers
c) Crackers
d) Spoofing

13. Which access control model allows data owners to control access by modifying Access Control Lists which are enforced by the Operating System?
a) Discretionary Access Control (DAC)
b) Rule-Based Access Control (RBAC)

c) Mandatory Access Control (MAC)
d) Role-Based Access Control (RBAC)

14. Which access control technique is non discretionary?
    a) MAC
    b) DAC
    c) Lattice
    d) RBAC

15. Which hierarchical access control model is enforced by the operating system and can be difficult to implement?
    a) Mandatory Access Control (MAC)
    b) Role-Based Access Control (RBAC)
    c) Discretionary Access Control (DAC)
    d) Rule-Based Access Control (RBAC)

16. What type of access control alerts you when an access is violated?
    a) Deterrent
    b) Reactive
    c) Preventative
    d) Detective

17. Which of the following is a centralized access control methodology?
    a) RADIUS
    b) DAC
    c) MAC
    d) Lattice

18. Which of the following is a table that identifies user access rights for a particular system object?
    a) MAC
    b) DAC
    c) ACL - access control list
    d) Lattice

19. Which is an example of a decentralized access control methodology?
    a) PAP
    b) NIS - network information system
    c) RPC
    d) RADIUS

20. Kerberos certificates are susceptible to what kind of attack?
    a) Man-in-the-middle
    b) Social Engineering
    c) Denial of Service
    d) Replay

21. Which of the following is a knowledge-based authentication mechanism?
    a) Token
    b) Smart card
    c) Biometrics
    d) Password

22. Which of the following allows attackers to imitate a different user or system?
    a) Spamming
    b) Sniffers
    c) Crackers
    d) Spoofing

23. What type of access control avoids access violations?
    a) Reactive
    b) Preventative
    c) Deterrent
    d) Detective

24. Which example is not two factor authentication?
    a) Palm geometry and iris scan
    b) Token and password
    c) Iris scan and token
    d) Smart card and PIN

25. Which attack has victims believe they are communicating directly to their intended host when in reality all their messages are being intercepted?
    a) Replay
    b) Spoofing
    c) Man-in-the-middle
    d) Social engineering

26. Centralized access control provides remote users with all of the following properties except
    a) Authorization
    b) Authentication
    c) Accountability
    d) Availability

27. What is a type of attack that involves trying all possible combinations to break a code or password?
    a) Dictionary attack
    b) Brute force attack
    c) Word search attack
    d) Penetration attack