Multiple Choice Questions

1. Which component of the CIA triad ensures that changes to data are reversible if made in error?
   a. a) Confidentiality
   b. b) Integrity
   c. c) Availability
   d. d) Accountability
2. What is the primary purpose of reconnaissance in ethical hacking?
   a. a) Exploiting vulnerabilities
   b. b) Gathering target information
   c. c) Covering tracks
   d. d) Installing backdoors
3. Which of the following best describes the role of non-repudiation in information security?
   a. a) Ensuring data availability
   b. b) Preventing unauthorized data modification
   c. c) Providing proof of data origin
   d. d) Ensuring data redundancy
4. What distinguishes passive footprinting from active footprinting?
   a. a) Passive footprinting targets applications, while active targets networks.
   b. b) Passive footprinting involves indirect methods, while active involves direct interaction.
   c. c) Passive footprinting is automated, while active requires manual effort.
   d. d) Passive footprinting focuses on vulnerability exploitation.
5. Which tool is commonly used for DNS footprinting?
   a. a) Nessus
   b. b) nslookup
   c. c) Metasploit
   d. d) Wireshark
6. What is a key objective of using theHarvester in footprinting?
   a. a) Identifying open ports on a target system
   b. b) Collecting information like emails and subdomains
   c. c) Detecting network intrusions
   d. d) Exploiting vulnerabilities in web servers
7. What scanning technique uses FIN, URG, and PSH flags to identify closed ports?
   a. a) SYN Scan

    b. b) Full Connect Scan
    c. c) Xmas Scan
    d. d) UDP Scan

8. What is the primary role of a vulnerability scanner like Nessus?
    a. a) Exploiting vulnerabilities
    b. b) Scanning for malware
    c. c) Identifying known security weaknesses
    d. d) Cracking passwords
9. Which of the following is NOT a stage of the Cyber Kill Chain?
    a. a) Weaponization
    b. b) Installation
    c. c) Exploitation
    d. d) Data Reconciliation
10. Which of the following would be considered a compensating control?
    a. a) Using a backup power supply
    b. b) Enabling multifactor authentication
    c. c) Implementing a firewall
    d. d) Creating detailed access logs
11. How does traceroute contribute to network footprinting?
    a. a) By identifying vulnerable software versions
    b. b) By revealing the path packets take through the network
    c. c) By scanning for open ports
    d. d) By enumerating DNS records
12. What is the purpose of WHOIS lookups in footprinting?
    a. a) Identifying active hosts in a subnet
    b. b) Obtaining domain registration details
    c. c) Detecting open ports on a system
    d. d) Exploiting weak credentials
13. What type of scan sends SYN packets but does not complete the handshake?
    a. a) Full Connect Scan
    b. b) Stealth Scan
    c. c) Xmas Scan
    d. d) ACK Scan
14. Which of the following is an example of a deterrent security control?
    a. a) Installing an IDS
    b. b) Enforcing strict access controls
    c. c) Placing warning signs on server rooms
    d. d) Configuring regular data backups

15. What kind of vulnerabilities does DNS poisoning exploit?
    a. a) Misconfigured firewalls
    b. b) Caching mechanisms in DNS resolvers
    c. c) Weak encryption algorithms
    d. d) Authentication protocols
16. In what way does the Cyber Kill Chain’s "Weaponization" stage differ from "Delivery"?
    a. a) Weaponization involves deploying the attack payload, while Delivery identifies the target.
    b. b) Weaponization creates the attack payload, while Delivery transmits it to the target.
    c. c) Weaponization identifies vulnerabilities, while Delivery exploits them.
    d. d) Weaponization installs the payload, while Delivery secures the target.
17. What is the difference between vulnerability scanning and penetration testing?
    a. a) Vulnerability scanning identifies weaknesses, while penetration testing exploits them.
    b. b) Vulnerability scanning uses manual methods, while penetration testing is automated.
    c. c) Vulnerability scanning targets networks, while penetration testing targets applications.
    d. d) Vulnerability scanning is destructive, while penetration testing is not.
18. Which of these tools is primarily used for subdomain enumeration?
    a. a) Sublist3r
    b. b) hping
    c. c) Nikto
    d. d) Masscan
19. How does defense in depth enhance organizational security?
    a. a) By employing a single robust control
    b. b) By using multiple overlapping controls
    c. c) By automating threat detection
    d. d) By minimizing operational costs
20. What is the key difference between reconnaissance and scanning?
    a. a) Reconnaissance focuses on exploiting systems, while scanning focuses on mitigation.
    b. b) Reconnaissance is passive, while scanning involves active interactions.
    c. c) Reconnaissance uses network tools, while scanning uses application tools.
    d. d) Reconnaissance identifies vulnerabilities, while scanning resolves them.