UNIT_3 Worksheet: Deliverable and Integration (MCQs)

Name: _____
Roll No.: _____
Date: _____

Multiple Choice Questions

1. What is the primary purpose of technical preparation before a penetration test?
A) To increase system downtime
B) To ensure tools, resources, and permissions are ready
C) To remove all security controls
D) To train end users
Answer: B

2. Technical preparation includes:
A) Selecting and configuring testing tools
B) Marketing planning
C) Employee recruitment
D) Budget auditing
Answer: A

3. Managing the engagement helps ensure that:
A) The assessment stays within scope and objectives
B) Systems remain vulnerable
C) Costs increase unnecessarily
D) Security policies are ignored
Answer: A

4. Reconnaissance is the process of:
A) Exploiting vulnerabilities
B) Gathering information about a target
C) Installing software
D) Encrypting files
Answer: B

5. Reconnaissance is often considered which phase of ethical hacking?
A) Final reporting
B) Initial information-gathering phase
C) Incident response
D) Risk mitigation
Answer: B

6. Social engineering attacks primarily target:
A) Network devices
B) Human behavior and trust
C) Databases only
D) Operating systems only
Answer: B

7. Which of the following is an example of social engineering?
A) Phishing email
B) Software patching
C) Data backup
D) Firewall configuration
Answer: A

8. Phishing is a technique used to:
A) Improve network performance
B) Trick users into revealing sensitive information
C) Encrypt data
D) Create backups
Answer: B

9. Physical security assessment evaluates:
A) Employee salaries
B) Protection of facilities and hardware assets
C) Software licenses
D) Programming skills
Answer: B

10. Which of the following is a physical security control?
A) Firewall
B) Antivirus
C) Access control card
D) Encryption software
Answer: C

11. Tailgating is a physical security threat where:
A) An unauthorized person follows an authorized person into a restricted area
B) A server crashes unexpectedly
C) Data is encrypted
D) Software is updated
Answer: A

12. Internet reconnaissance involves:
A) Gathering publicly available information from online sources
B) Installing malware
C) Deleting data
D) Replacing hardware
Answer: A

13. Which source is commonly used during internet reconnaissance?
A) Public websites
B) Social media platforms
C) Search engines
D) All of the above
Answer: D

14. Open Source Intelligence (OSINT) refers to:
A) Classified information gathering
B) Collection of publicly available information
C) Software development
D) Data encryption
Answer: B

15. Which search engine technique can help gather information about a target organization?
A) Google Dorking
B) Data Compression
C) Network Routing
D) Packet Filtering
Answer: A

16. Why is social engineering often successful?
A) It exploits human trust and emotions
B) It requires expensive equipment
C) It bypasses the internet
D) It removes firewalls automatically
Answer: A

17. During reconnaissance, information about employees may be gathered from:
A) Social networking sites
B) Public directories
C) Company websites
D) All of the above
Answer: D

18. Which of the following is NOT a reconnaissance activity?
A) Gathering domain information
B) Collecting employee details
C) Exploiting a vulnerability
D) Identifying network ranges
Answer: C

19. The objective of physical security testing is to:
A) Evaluate how well facilities prevent unauthorized access
B) Increase internet bandwidth
C) Develop applications
D) Install operating systems
Answer: A

20. What is the importance of engagement management during a security assessment?
A) It ensures legal, ethical, and operational compliance
B) It eliminates all security risks
C) It guarantees no vulnerabilities exist
D) It replaces security policies
Answer: A

21. Which of the following is an example of pretexting?
A) Creating a false identity to obtain information
B) Installing antivirus software
C) Updating a firewall
D) Encrypting files
Answer: A

22. Dumpster diving is associated with:
A) Social engineering and physical reconnaissance
B) Application development
C) Database management
D) Cloud deployment
Answer: A

23. Which activity is commonly performed during internet reconnaissance?
A) WHOIS lookup
B) Password reset
C) Data encryption
D) System formatting
Answer: A

24. Why should reconnaissance be performed carefully?
A) To avoid detection and gather accurate information
B) To damage systems
C) To increase network traffic
D) To bypass legal requirements
Answer: A

25. The information collected during reconnaissance is primarily used for:
A) Planning later stages of the security assessment
B) Employee evaluation
C) Financial auditing
D) Software installation
Answer: A

Score Sheet

Marks Obtained: _____ / 25

Instructor Signature: _____

Student Signature: _____