UNIT_4 Worksheet: Deliverable and Integration (MCQs)

Name: _____
Roll No.: _____
Date: _____

Multiple Choice Questions

Enumeration

1. What is the primary purpose of enumeration in ethical hacking?
A) To destroy data
B) To gather detailed information about systems and services
C) To create malware
D) To install applications
Answer: B

2. Enumeration is typically performed after:
A) Reporting
B) Reconnaissance
C) Exploitation
D) Recovery
Answer: B

3. Which of the following is commonly identified during enumeration?
A) User accounts
B) Network shares
C) Running services
D) All of the above
Answer: D

4. Enumeration techniques are used to:
A) Obtain detailed information from discovered targets
B) Increase internet speed
C) Manage employee records
D) Design applications
Answer: A

5. A soft objective in enumeration focuses on:
A) Gathering information without disrupting services
B) Exploiting vulnerabilities immediately
C) Deleting system logs
D) Crashing servers
Answer: A

6. "Looking Around" during enumeration refers to:
A) Collecting information without actively attacking the target
B) Installing malware
C) Modifying system files
D) Performing denial-of-service attacks
Answer: A

7. Which activity would be considered an attack rather than simple enumeration?
A) Identifying open ports
B) Listing user accounts
C) Exploiting a vulnerability
D) Discovering shared resources
Answer: C

8. Which of the following is an element of enumeration?
A) User identification
B) Service discovery
C) Resource identification
D) All of the above
Answer: D

9. Why is enumeration important before exploitation?
A) It provides information needed for planning attacks
B) It increases system performance
C) It reduces storage requirements
D) It creates backups
Answer: A

10. Preparing for the next phase means:
A) Using collected information to guide exploitation activities
B) Deleting gathered information
C) Installing operating systems
D) Rebooting systems
Answer: A

Exploitation

11. Exploitation refers to:
A) Gathering public information
B) Taking advantage of identified vulnerabilities
C) Creating security policies
D) Updating software
Answer: B

12. Intuitive testing relies primarily on:
A) Experience, judgment, and creativity of the tester
B) Automated backups
C) Employee interviews
D) Accounting records
Answer: A

13. Evasion techniques are used to:
A) Avoid detection by security mechanisms
B) Improve hardware performance
C) Increase storage capacity
D) Generate reports
Answer: A

14. In cybersecurity, a threat is:
A) A potential danger to systems or information
B) A software update
C) A backup copy
D) A security policy
Answer: A

15. Why are operating systems important during exploitation?
A) Vulnerabilities often depend on the operating system being used
B) They increase network speed
C) They eliminate threats automatically
D) They prevent enumeration
Answer: A

16. Password crackers are tools used to:
A) Recover or test password strength
B) Encrypt files
C) Monitor network traffic only
D) Create user accounts
Answer: A

17. A rootkit is primarily designed to:
A) Hide unauthorized access or malicious activity
B) Improve system performance
C) Create backups
D) Manage databases
Answer: A

18. Application exploitation targets:
A) Software applications and their vulnerabilities
B) Physical buildings
C) Electrical systems
D) Human resources departments
Answer: A

19. War dialing is a technique used to:
A) Scan telephone numbers for connected modems or systems
B) Increase wireless speed
C) Encrypt communications
D) Create user accounts
Answer: A

20. Network exploitation focuses on:
A) Weaknesses in network infrastructure and protocols
B) Office management
C) Employee attendance
D) Inventory control
Answer: A

21. Which of the following is considered a network service?
A) DNS
B) HTTP
C) FTP
D) All of the above
Answer: D

22. Services running on unnecessary ports can:
A) Increase the attack surface
B) Eliminate vulnerabilities
C) Improve security automatically
D) Prevent enumeration
Answer: A

23. Areas of concern during exploitation include:
A) Weak passwords
B) Misconfigured services
C) Unpatched systems
D) All of the above
Answer: D

24. Which activity is most likely to occur during exploitation?
A) Attempting to gain unauthorized access using identified weaknesses
B) Writing security policies
C) Conducting employee training
D) Performing data backups
Answer: A

25. The ultimate goal of exploitation in ethical hacking is to:
A) Demonstrate the impact of vulnerabilities and improve security
B) Cause permanent damage
C) Steal confidential data
D) Disable business operations
Answer: A

Score Sheet

Marks Obtained: _____ / 25

Instructor Signature: _____

Student Signature: _____