UNIT_2 Worksheet: Deliverable and Integration (MCQs)

Name: _____
Roll No.: _____
Date: _____

Multiple Choice Questions

1. What is the primary purpose of understanding business objectives before a security assessment?
A) To increase network traffic
B) To align security testing with organizational goals
C) To reduce employee salaries
D) To purchase new hardware
Answer: B

2. A security policy primarily provides:
A) Marketing guidelines
B) Rules and procedures for protecting information assets
C) Employee attendance records
D) Financial statements
Answer: B

3. Why should previous test results be reviewed before conducting a new security assessment?
A) To identify recurring vulnerabilities and measure improvements
B) To increase testing costs
C) To avoid documentation
D) To hire more employees
Answer: A

4. Business challenges may affect a security assessment by:
A) Defining constraints and priorities
B) Eliminating all risks
C) Preventing any testing
D) Increasing software licenses
Answer: A

5. A controlled attack is conducted to:
A) Damage systems intentionally
B) Evaluate security under managed conditions
C) Delete organizational data
D) Replace security staff
Answer: B

6. Inherent limitations refer to:
A) Restrictions naturally present in systems or environments
B) Government regulations only
C) Employee work schedules
D) Marketing policies
Answer: A

7. Imposed limitations are:
A) Restrictions defined by the client or organization
B) Hardware failures
C) Network outages
D) User errors
Answer: A

8. Why is timing important during a security assessment?
A) It determines employee salaries
B) It minimizes business disruption and maximizes effectiveness
C) It changes company policies
D) It eliminates vulnerabilities
Answer: B

9. Which attack type simulates an external threat actor?
A) External attack
B) Internal audit
C) Data backup
D) Patch management
Answer: A

10. The source point of an attack refers to:
A) The location from which the attack is initiated
B) The reporting format
C) The company headquarters
D) The software vendor
Answer: A

11. Required knowledge in penetration testing defines:
A) The amount of information provided to testers beforehand
B) Employee training schedules
C) Budget allocation
D) Legal penalties
Answer: A

12. A black-box test is characterized by:
A) Complete knowledge of the target environment
B) Partial knowledge of the target environment
C) No prior knowledge of the target environment
D) Knowledge of source code only
Answer: C

13. A white-box test provides testers with:
A) No information
B) Limited information
C) Full information about the target environment
D) Access to social media only
Answer: C

14. Multi-phased attacks involve:
A) A single attack step
B) Multiple stages carried out sequentially
C) No planning
D) Random activities
Answer: B

15. Teaming and attack structure help to:
A) Organize personnel and responsibilities effectively
B) Increase project costs
C) Avoid documentation
D) Replace management
Answer: A

16. An engagement planner is responsible for:
A) Defining scope, objectives, and resources for testing
B) Managing payroll
C) Designing websites
D) Purchasing software
Answer: A

17. The right security consultant should possess:
A) Relevant technical expertise and ethical standards
B) Marketing experience only
C) Accounting certification only
D) Sales experience only
Answer: A

18. The tester's primary responsibility is to:
A) Conduct security assessments within the agreed scope
B) Modify business policies
C) Approve budgets
D) Manage customer support
Answer: A

19. Logistics in penetration testing include:
A) Planning resources, schedules, and communication channels
B) Developing advertisements
C) Recruiting customers
D) Conducting interviews only
Answer: A

20. Intermediates in a security assessment are:
A) Third parties or systems involved in communication or testing activities
B) Final reports
C) Security patches
D) Backup servers only
Answer: A

21. Why may law enforcement involvement be necessary during a security assessment?
A) To ensure legal compliance and address incidents when required
B) To perform software updates
C) To monitor employee attendance
D) To reduce internet usage
Answer: A

22. Which document formally authorizes a penetration test?
A) Rules of Engagement
B) Employee Handbook
C) Sales Report
D) Inventory List
Answer: A

23. What is a key benefit of defining attack scope clearly?
A) Reduces misunderstandings and unauthorized activities
B) Increases vulnerabilities
C) Eliminates reporting requirements
D) Prevents risk assessment
Answer: A

24. Which attack type evaluates threats originating from inside the organization?
A) External Attack
B) Internal Attack
C) Remote Backup
D) Disaster Recovery
Answer: B

25. A successful controlled attack engagement should result in:
A) Identification of security weaknesses and recommendations
B) Permanent system damage
C) Loss of business data
D) Elimination of all future threats
Answer: A

Score Sheet

Marks Obtained: _____ / 25

Instructor Signature: _____

Student Signature: _____