UNIT_5 Worksheet: Deliverable and Integration (MCQs)

Name: _____
Roll No.: _____
Date: _____

Multiple Choice Questions

Deliverable

1. In an ethical hacking engagement, the deliverable is typically:
A) A software application
B) A security assessment report
C) A network device
D) A firewall configuration
Answer: B

2. The primary purpose of the deliverable is to:
A) Document findings and recommendations
B) Increase network traffic
C) Replace security staff
D) Install software updates
Answer: A

3. A well-prepared deliverable should be:
A) Clear, accurate, and actionable
B) Complex and confusing
C) Limited to technical details only
D) Free of recommendations
Answer: A

4. Which section of a security report provides a high-level overview for management?
A) Executive Summary
B) Appendix
C) References
D) Glossary
Answer: A

5. The document generated after testing should contain:
A) Findings and evidence
B) Risk assessments
C) Recommendations
D) All of the above
Answer: D

6. What is the importance of the overall structure of a report?
A) It improves readability and understanding
B) It increases vulnerabilities
C) It removes evidence
D) It avoids recommendations
Answer: A

7. Aligning findings means:
A) Relating vulnerabilities to business risks and objectives
B) Removing vulnerabilities from the report
C) Encrypting the report
D) Ignoring business requirements
Answer: A

8. Which of the following should be included for each finding?
A) Description of the vulnerability
B) Risk level
C) Recommendation
D) All of the above
Answer: D

9. Why is evidence included in a penetration testing report?
A) To support the validity of findings
B) To increase report size
C) To confuse readers
D) To replace recommendations
Answer: A

10. The presentation of findings should be:
A) Organized and understandable
B) Unstructured and lengthy
C) Hidden from management
D) Limited to screenshots only
Answer: A

Integration

11. Integration of results refers to:
A) Combining findings into the organization's security improvement process
B) Deleting assessment data
C) Purchasing new hardware
D) Installing operating systems
Answer: A

12. The integration summary provides:
A) A consolidated view of assessment outcomes
B) Employee attendance records
C) Software license information
D) Network diagrams only
Answer: A

13. Mitigation involves:
A) Reducing the likelihood or impact of identified risks
B) Increasing vulnerabilities
C) Ignoring security findings
D) Removing documentation
Answer: A

14. Which of the following is an example of mitigation?
A) Applying security patches
B) Strengthening passwords
C) Updating configurations
D) All of the above
Answer: D

15. Defense planning is the process of:
A) Developing strategies to protect systems and information assets
B) Eliminating documentation
C) Increasing attack opportunities
D) Ignoring threats
Answer: A

16. Incident management focuses on:
A) Detecting, responding to, and recovering from security incidents
B) Marketing products
C) Managing employee payroll
D) Designing websites
Answer: A

17. A security policy is best described as:
A) A set of rules and guidelines for protecting information assets
B) A software program
C) A hardware component
D) A financial report
Answer: A

18. Why should security findings be integrated into security policies?
A) To improve organizational security practices
B) To increase operational costs
C) To reduce system availability
D) To avoid compliance requirements
Answer: A

19. Which of the following is a goal of defense planning?
A) Prevent future attacks
B) Detect threats early
C) Improve response capabilities
D) All of the above
Answer: D

20. Effective incident management helps organizations:
A) Minimize damage from security incidents
B) Increase vulnerabilities
C) Eliminate all risks permanently
D) Ignore security alerts
Answer: A

21. The conclusion section of a security assessment report should:
A) Summarize findings and recommendations
B) Introduce new vulnerabilities only
C) Remove evidence from the report
D) Focus only on technical details
Answer: A

22. Which stakeholder is most likely to use the executive summary?
A) Senior Management
B) End Users Only
C) Customers Only
D) Vendors Only
Answer: A

23. A remediation plan is developed to:
A) Address identified vulnerabilities systematically
B) Increase attack surfaces
C) Delay corrective actions
D) Remove security controls
Answer: A

24. Which activity occurs after integrating assessment results?
A) Implementing security improvements
B) Ignoring recommendations
C) Deleting reports
D) Conducting unrelated audits
Answer: A

25. The ultimate purpose of the deliverable and integration phases is to:
A) Improve the organization's overall security posture
B) Increase system vulnerabilities
C) Reduce documentation quality
D) Eliminate security policies
Answer: A

Score Sheet

Marks Obtained: _____ / 25

Instructor Signature: _____

Student Signature: _____