Question Bank-VAPT

Unit 1

2-Markers

1. Define Vulnerability.
2. What is a Threat?
3. Explain the term “Exploit”.
4. What is Penetration Testing?
5. Define Patch Management.
6. What do you mean by Zero-Day Vulnerability?
7. Explain the term “False Positive”.
8. Define Security Controls.
9. What is CVSS?
10. Define Risk.

5-Markers

1. Explain any two vulnerability assessment tools in detail.
2. Describe the Vulnerability Assessment Lifecycle with suitable examples.
3. Explain the role and components of the Common Vulnerability Scoring System (CVSS).
4. Explain different types of vulnerabilities with suitable examples.
5. Describe the importance of Common Vulnerability Scoring System (CVSS).

Unit 2

2-Markers

1. Define VAPT methodology.
2. What is Black Box Testing?
3. Mention two techniques of Black Box Testing.
4. What is Boundary Value Analysis?
5. Define White Box Testing.
6. What is Statement Coverage in White Box Testing?
7. Define Gray Box Testing.
8. Mention two advantages of Gray Box Testing.
9. What is OWASP?
10. What is PTES?

5-Markers

1. Explain Black Box Testing Techniques with examples.
2. Discuss the key differences between OWASP and PTES frameworks.
3. Describe penetration testing phases with examples.
4. Explain PTES in brief.
5. Discuss OWASP testing methodology.

Unit 3

2-Markers

1. Define Network Penetration Testing.
2. Mention two types of Network Penetration Testing.
3. What is Reconnaissance?
4. Define Scanning in penetration testing.
5. What is SQL Injection?
6. Define Cross-Site Scripting (XSS).
7. What is CSRF?
8. What is Session Hijacking?
9. What do you understand by post-exploitation?
10. Name two tools used for exploitation in network penetration testing.

5-Markers

1. Describe reconnaissance methods and tools used for it.
2. Differentiate between SQL Injection and Cross-Site Scripting with examples.
3. Explain network penetration testing techniques with suitable examples.
4. Write a note on SQL Injection.
5. Write a note on exploitation frameworks and provide examples.

Unit 4

2-Markers

1. Define Vulnerability Assessment Report.
2. What is included in an Executive Summary of a VA Report?
3. What are Risk Ratings?
4. Define Risk Avoidance.
5. What is Risk Retention?
6. Mention two common challenges in interpreting VA reports.
7. Define Qualitative Risk Assessment.
8. What is Incident Response Management?
9. Define Incident Documentation.
10. Mention two containment strategies used in incident response.

5-Markers

1. Describe the phases involved in Incident Response Management.
2. Discuss in detail the steps involved in developing effective mitigation strategies post-assessment.
3. Describe the key aspects to consider while interpreting a vulnerability assessment report. Provide examples.
4. Explain how to interpret vulnerability assessment report.
5. Write a note on steps involved in post-assessment review.

Unit 5

2-Markers

1. Define ethical hacking.
2. Mention two principles of ethical hacking.
3. What is responsible disclosure?
4. What is GDPR?
5. Name two sector-specific cybersecurity regulations in India.
6. Define Intellectual Property in the context of VAPT.
7. Mention two professional certifications for ethical hackers.
8. Explain data privacy during testing.
9. What was the main issue in the Cambridge Analytica scandal?
10. Define the IT Act 2000.

5-Markers

1. Explain the responsible disclosure process of vulnerabilities.
2. Discuss the legal implications and compliance requirements involved in vulnerability assessments and penetration testing.
3. Explain the procedure and importance of responsible disclosure of vulnerabilities with suitable examples.
4. Explain the ethical considerations essential during vulnerability assessment and penetration testing.
5. Discuss the significance of compliance and legal frameworks in vulnerability assessments.