Penetration testing: Key Concepts

Duration- 16 hours

Module 1: Introduction to Penetration Testing and Methodologies

- Overview of penetration testing
- Types of penetration tests (network, application, wireless, etc.)
- Ethical and legal considerations

Module 2: Scoping and Engagement

- Defining objectives for a penetration test
- Rules of engagement and compliance requirements
- Scoping and resource allocation

Module 3: Open-Source Intelligence (OSINT)

- Introduction to OSINT and its importance in penetration testing
- Tools and techniques for OSINT

Module 4: Social Engineering Penetration Testing

- Types of social engineering attacks
- Techniques for simulating phishing and pretexting attacks
- Mitigation strategies

Module 5: Network Penetration Testing – External

- Understanding external attack surfaces
- Common vulnerabilities and misconfigurations
- Techniques for identifying and exploiting external vulnerabilities

Module 6: Web Application Penetration Testing

- OWASP Top 10 vulnerabilities
- Methods for identifying and exploiting web application weaknesses
- Overview of tools used for web application testing

Module 7: Network Penetration Testing – Internal and Perimeter Devices

- Internal attack strategies
- Lateral movement and pivoting basics
- Perimeter device vulnerabilities (firewalls, IDS/IPS)

Module 8: IoT and OT Penetration Testing

- Introduction to IoT security challenges
- Overview of OT and SCADA systems
- Key vulnerabilities and attack vectors

Module 9: Cloud Penetration Testing

- Cloud service models and associated risks
- Identifying misconfigurations and vulnerabilities in cloud environments

Module 10: Privilege Escalation and Defense Evasion

- Techniques for privilege escalation (Windows/Linux)
- Strategies for evading detection mechanisms

Module 11: Report Writing and Post-Test Actions

- Components of a professional penetration testing report
- Communicating findings to stakeholders
- Steps for remediation and follow-up actions