🔐 VAPT Course Curriculum

COURSE DURATION
45 DAYS

🟢 Module 1: Introduction to VAPT

- What is Vulnerability Assessment?
- What is Penetration Testing?
- Difference between VA and PT
- Importance of VAPT in cybersecurity
- Legal and ethical considerations (including scope & permission)

🟡 Module 2: Basics of Networking and Security

- OSI & TCP/IP models
- IP addressing, DNS, DHCP
- Common ports and protocols
- Firewalls, IDS/IPS
- Basics of Operating Systems (Windows/Linux)

🟠 Module 3: Methodologies and Standards

- OWASP Testing Guide
- PTES (Penetration Testing Execution Standard)
- NIST Framework

- OSSTMM Overview
- Bug bounty methodology (brief overview)

🔵 Module 4: Information Gathering (Reconnaissance)

- Passive vs Active Reconnaissance
- Tools: Whois, NSlookup, Maltego, Shodan, Google Dorking
- DNS enumeration
- Subdomain enumeration
- Email harvesting, metadata extraction

🟣 Module 5: Scanning and Enumeration

- Network Scanning using Nmap
- Banner Grabbing
- Service Enumeration
- Vulnerability Scanning: Nessus, OpenVAS, Nikto
- Identifying live hosts and services

🔴 Module 6: Vulnerability Assessment

- Understanding CVEs and CVSS scores
- Manual vulnerability analysis
- Automated tools (Nessus, Nexpose, OpenVAS)

- Report analysis and validation

🟤 Module 7: Exploitation (Penetration Testing)

- System Exploitation (Windows/Linux)
- Web Application Exploitation (OWASP Top 10: XSS, SQLi, LFI, RFI, etc.)
- Exploiting weak services (FTP, SMB, RDP, etc.)
- Tools: Metasploit, SQLMap, Burp Suite

⚫ Module 8: Post-Exploitation

- Privilege Escalation Techniques
- Persistence mechanisms
- Clearing logs and covering tracks (ethically, for learning only)
- Pivoting and lateral movement
- Data exfiltration techniques

⚪ Module 9: Web Application VAPT

- Manual Testing of Web Applications
- Web Vulnerabilities (OWASP Top 10 in depth)
- Tools: Burp Suite, OWASP ZAP
- Exploiting authentication, session management flaws

🟧 Module 10: Wireless and Network Penetration Testing

- Wireless standards (WEP, WPA, WPA2)
- Attacks: Evil Twin, Deauthentication
- Tools: Aircrack-ng, Wireshark, Bettercap

🟨 Module 11: Report Writing and Mitigation

- VAPT Report Structure
- Risk rating and impact analysis
- Executive summary and technical summary
- Remediation and mitigation suggestions

🟩 Module 12: Hands-On Projects and Labs

- Capture The Flag (CTF) exercises
- Simulated VAPT on vulnerable machines (DVWA, Metasploitable, TryHackMe, Hack The Box)
- Real-time report creation

📜 Certification Outcome:

- Prepare for CEH, OSCP, or company VAPT roles

- Become proficient in VAPT tools and methodologies
- Capable of handling client projects and internal audits