VAPT – Vulnerability Assessment s Penetration Testing Professional Course

Complete Job-Oriented Training Program (Beginner to Advanced)

Course Objectives

By the end of this course, students will be able to:

- Understand security concepts, vulnerabilities C modern attack vectors
- Perform Vulnerability Assessment and Penetration Testing across platforms
- Conduct manual C automated exploitation of security flaws
- Perform Web, Network C Mobile Application Pentesting
- Generate professional security reports C remediation guidelines
- Prepare for Cyber Security interviews C certification pathways

---

Detailed Course Curriculum

Module 1: Introduction to Cyber Security s VAPT

- What is Information Security, Cyber Security, and Ethical Hacking
- Difference between VA C PT
- Real-world security breach case studies
- Security Testing Methodologies
- Phases of a Penetration Test
- Rules of Engagement C legal considerations

Module 2: Networking Fundamentals for Pentesters

- Networking Basics C OSI / TCP-IP Model
- Ports C Protocols
- DNS, DHCP, VPN, NAT, Firewalls C Proxy

Module 3: Linux s Essential Tools

- Linux commands for security testing
- Using Kali Linux for pentesting
- Tools installation C management
- Scripting basics (Bash C Python for Automation)

Module 4: Reconnaissance s Information Gathering

- Active vs Passive Recon
- WHOIS C DNS reconnaissance
- Subdomain discovery techniques
- Metadata C email footprinting
- Network scanning with Nmap
- Banner grabbing C service detection

Module 5: Vulnerability Assessment

- Understanding CVE / CVSS / CIA Triads
- Vulnerability Assessment Methodology
- Scanning using Nessus, OpenVAS, Nikto, Nmap NSE, Nessus
- Reading vulnerability scan reports

Module 6: Penetration Testing Methodology

- Manual vs Automated testing
- Exploiting common vulnerabilities
- Remediation C recommendation analysis

Module 7: Web Application Penetration Testing

Includes Complete OWASP Top 10

Additional Web Security Attacks

- XSS (Persistence/Non-persistence/Blind)
- INJECTION ATTACKS (SQL, HTML, HHI)
- Directory Traversal
- File Upload attacks C Web Shell Deployment
- Rate-limit bypass C authentication abuse
- Session Hijacking
- CSRF
- CMS vulnerabilities (Wordpress/xmlrpc/)
- Source Code Review/File disclosure
- Image Mata data issues
- Business logic vulnerabilities (OTP Bypass/Payment Bypass)

Tools Covered

Burp Suite Pro, Zap Proxy, Nmap, Assetfinder, SQLMap, Nessus

Module 8: Mobile Application Security

Android s iOS Pentesting

- Mobile architecture C testing environment setup
- Components of Android Application
- IOS Application code Analysis
- APK Decompiling, Reverse Engineering
- Mobile OWASP Top 10
- Mobexler, APK Tool, MobSF, JADX-GUI

Module 9: Network Penetration Testing

- Internal C External network testing
- Man-in-the-Middle Attacks
- Directory Traversal Pentesting
- Network C Port Scanning
- Exploit the open ports

Module 10: Cryptography and Steganography

- Types of Cryptography
- Hashing
- Encrypted email communications
- Encryption and Decryption techniques – Live Practical
- Data Hiding Analysis by Stag techniques

Module 11: Web server Security

- Web Server Fundamentals
- Robots.txt
- Web Server Vulnerability Assessment by nikto
- Web server bruteforcing for directory listing issues
- Dirb & Dirbuster tool in kali Linux for webserver Pen testing

---

Module 12: Report Writing s Documentation

- Professional pentest report structure
- POC writing C screenshot standards
- Risk rating methodology C mitigation guidelines
- Executive summary vs technical detail writing

Module 13: Interview Preparation s Career Guidance

- Common VAPT C Cyber Security interview questions
- Scenario-based interview practice
- Resume building for security jobs
- Freelancing C Bug Bounty career guidance
- CEH / OSCP / eJPT / eWPT certification roadmap

Practical Assignments s Real-world Projects

- Live Pentesting projects
- Capture The Flag challenges
- Final Assessment Project C Review

Training Outcomes

Students completing the program will:

✓ Perform real-world VAPT independently

✓ Identify, exploit C report security vulnerabilities

✓ Be job-ready for Security Analyst / Pentester / VAPT roles

✓ Start participating in Bug Bounty programs