Vulnerability Assessment and Penetration Testing (VAPT) Syllabus

1 Month Duration

Module 1: Introduction to Cybersecurity and VAPT

Duration: 2 days

- Overview of Cybersecurity
- What is Vulnerability Assessment and Penetration Testing (VAPT)?
- Importance of VAPT in the cybersecurity lifecycle
- VAPT vs. vulnerability scanning
- Phases of Penetration Testing: Reconnaissance, Scanning, Exploitation, Post-exploitation
- Ethical hacking principles and legal aspects

Module 2: Networking and System Fundamentals for VAPT

Duration: 4 days

- OSI and TCP/IP Models
- IP addressing, subnetting, and network protocols
- Understanding common network services: HTTP, FTP, DNS, SSH, etc.
- Basic networking devices and configurations
- Operating System fundamentals: Windows & Linux (command line usage, file systems, etc.)
- Importance of system hardening in VAPT

Module 3: Information Gathering and Reconnaissance

Duration: 4 days

- Reconnaissance: Active vs. Passive Information Gathering
- Tools for information gathering: WHOIS, DNS interrogation, Google Dorking
- Footprinting: IP enumeration, Domain name information, Network range identification
- Banner grabbing and version detection
- Tools: Nmap, Netcat, and online reconnaissance tools
- Social engineering in VAPT: Methods and Mitigation

Module 4: Vulnerability Assessment (Scanning & Identification)

Duration: 4 days

- Vulnerability scanning vs. penetration testing
- Common vulnerability scanners: Nessus, OpenVAS, Nexpose
- Interpreting scan results: False positives, severity ratings
- Manual vulnerability detection techniques

- Finding misconfigurations, outdated software, and weak security settings
- Vulnerability databases: CVE, Exploit-DB
- Risk analysis: Determining the criticality of vulnerabilities

Module 5: Penetration Testing Techniques and Exploitation

Duration: 5 days

- Exploit development process: Researching vulnerabilities, exploiting systems
- Tools for exploitation: Metasploit, Social-Engineer Toolkit (SET), and custom exploit development
- Gaining access through various attack vectors (Web Apps, OS, Network, etc.)
- SQL Injection, Cross-Site Scripting (XSS), and other common web application attacks
- Password cracking: Brute force, dictionary, and rainbow table attacks
- Exploiting misconfigurations (unencrypted protocols, exposed services)
- Pivoting within a network: Lateral movement techniques

Module 6: Post-Exploitation and Privilege Escalation

Duration: 4 days

- Post-exploitation: What to do after initial access
- Privilege escalation on Windows and Linux systems (exploiting sudo, kernel vulnerabilities, etc.)
- Maintaining access: Backdoors, rootkits, and persistent shells
- Data exfiltration: Techniques for extracting sensitive data
- Covering tracks: Log manipulation, deleting traces
- Remote Access Trojans (RATs) and Trojans in VAPT
- Tools: Meterpreter, Mimikatz, Empire, PowerShell Empire

Module 7: Web Application Penetration Testing

Duration: 4 days

- OWASP Top 10 vulnerabilities (SQLi, XSS, CSRF, etc.)
- Web application penetration testing methodology
- Testing for SQL Injection, Command Injection, Cross-Site Scripting (XSS), and File Inclusion
- Bypassing authentication: Session hijacking, login bypass
- Web application firewalls (WAFs) and evasion techniques
- Burp Suite: Scanning, intercepting traffic, and exploiting vulnerabilities
- Tools: Burp Suite, Nikto, Gobuster

Module 8: Report Writing, Remediation, and Conclusion

Duration: 3 days

- Importance of effective reporting in VAPT
- Writing professional vulnerability reports: Executive summary, risk analysis, technical details

- Remediation strategies: How to fix the discovered vulnerabilities
- Explaining vulnerabilities in layman's terms for non-technical stakeholders
- Final project: Performing a VAPT on a simulated environment (Lab Setup)
- Presentation and discussion of findings

Practical Sessions and Final Project (Ongoing throughout the month)
- Conducting live vulnerability assessments and penetration tests on test systems
- Working with a variety of tools in real-world scenarios
- Collaborating in teams for advanced attack simulations
- Final project: Simulate a full VAPT cycle (from reconnaissance to reporting) on a predefined target