Cybersecurity VAPT Mastery Program - 2025 Edition

“From Hacker Mindset to Professional Pentester”

Objective: To give learners a strong foundation in hacking mindsets, methodologies, laws, and tools preparing them for practical VAPT in later modules.

Module 1 - Introduction to Ethical Hacking

1. **What is Ethical Hacking?**
   - Definition of ethical hacking vs. malicious hacking
   - Real-world examples of white hat hacking saving companies
   - Importance of VAPT in modern cybersecurity
2. **Types of Hackers:**
   - White Hat
   - Black Hat
   - Grey Hat
   - Red Team vs. Blue Team vs. Purple Team
   - Bug Bounty Hackers
3. **Terminology and Concepts:**
   - Key terms: vulnerability, exploit, payload, privilege escalation, backdoor, etc.
   - Introduction to common tools (e.g., Nmap, Metasploit, Wireshark) without deep technical details yet.
   - Attack surfaces and vectors.
4. **Mindset and Skills of an Ethical Hacker:**
   - Analytical thinking, problem-solving, and curiosity.
   - Importance of continuous learning in cybersecurity.
   - Overview of certifications (e.g., CEH, OSCP) and career paths.
5. **Ethical Hacking Methodology:**
   - Phases of ethical hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks.
   - Overview of penetration testing methodologies (e.g., OWASP, NIST, PTES).
   - Importance of a structured approach and documentation.

Module 2: Setting Up Ethical Hacking Environment & Introduction to VAPT

- What is VAPT and Why is VAPT Needed?
- Career Opportunities, Job Roles and Salary Range in VAPT (as of 2025)
- Types of VAPT & Certifications That Help in VAPT
- Setting Up VMware/VirtualBox and Installing OS(Linux, Ubuntu, Mint etc.)
- Setting Up Tools (Burpsuite, Acunetix etc.)

Module 3: Web Application Penetration Testing

Objective: Equip students with foundational knowledge and practical skills for identifying and exploiting web application vulnerabilities using real-world tools, OWASP Top 10, and CVEs.

1. **Understanding the Web:**
   - How the web works (HTTP, HTTPS, DNS, URL structure)
   - Web technologies overview: HTML, JavaScript, PHP, SQL, etc.
   - Client-side vs. server-side.
   - Frontend, backend, DB layers
   - Sessions, cookies, headers
2. **OWASP Top 10 (2023-2025 Focus)**
   - What is the OWASP Top 10?
   - Why Do Industries Follow OWASP Top 10?
   - OWASP Top 10 Web Application Security Risks
   - Understanding CVSS (Common Vulnerability Scoring System)
3. **Web Reconnaissance & Enumeration**
   - Passive recon (Google dorking, Wayback, Github leaks)
   - Active recon (Subdomain enum, DNS brute-force)
   - Tools: Amass, Subfinder, httprobe, httpx, theHarvester
   - Favicon hash hunting
   - Fingerprinting web servers and technologies (Wappalyzer, What Web)
4. **Important Tools and Their Use in Real Industries**
   - Burp Suite
   - Nmap
   - Nuclei
   - Metasploit
   - Wireshark
   - Acunetix
5. **Vulnerability Discovery Techniques & Exploiting Web Vulnerabilities (Hands-On)**
   - Manual Web Application Testing Workflow
   - Fuzzing and Input Discovery
   - Automated Scanning Techniques
   - OWASP Top 10 Vulnerability Identification
   - Technology Stack Fingerprinting & Exploitation
   - Exploring High Impact Vulnerabilities
   - Vulnerability Chaining for Maximum Impact
   - Zero-Day and End-Day Vulnerabilities
   - Reporting and Documentation
   - Real-World Context with Case Studies
   - Recommended Resources

Module 4: Network Penetration Testing

1. **Understanding Network Architecture & Basics Of Network**
   - LAN, WAN, DMZ, VPN, VLAN, firewalls
   - Network based attack surfaces
   - TCP/IP Protocol
   - Vpn and Vps
   - Ports and Protocol
2. **Network Reconnaissance**
   - Passive vs active recon
   - Nmap basics and advanced scans
   - OS and service detection
3. **Enumeration Techniques**
   - SMB, SNMP, LDAP, NetBIOS
   - Usergroup/domain info gathering
4. **Exploiting Network Services**
   - Common misconfigurations
   - Public exploits (EternalBlue, PrintNightmare, MS17-010)
   - Exploit frameworks (Metasploit, RCE scripts)
5. **Password Attacks**
   - Brute-force and spraying
   - NTLMv2 relay and capture
   - Cracking with Hashcat, John the Ripper
6. **Post Exploitation & Privilege Escalation**
   - Gaining persistence
   - Pivoting through internal network
   - Data exfiltration techniques
7. **Reporting, Risk Categorization & Case Studies**
   - Writing technical and business reports
   - Mapping findings to MITRE ATT&CK and CVSS
   - Real-world internal assessments and findings
   - Lateral movement and domain compromise

Module 5: Mobile Application Penetration Testing (Android)

1. **Introduction to Mobile App Security**
   - Mobile attack surface overview
   - OWASP Mobile Top 10 (2023-2025 updated)
   - Android vs iOS architecture & security models
2. **Mobile App Setup & Environment**
   - Setting up Android Emulator / Genymotion / Virtual devices
   - Using physical rooted/jailbroken devices
   - Tools: adb, Frida, objection, MobSF, apktool, jadx
3. **Static Analysis (SAST)**
   - APK decompiling & reversing with jadx / apktool
   - Understanding app components (Activities, Intents, Services)
   - Searching for hardcoded secrets, API keys, credentials
4. **Dynamic Analysis (DAST)**
   - Runtime hooking with Frida / objection
   - API endpoint analysis using Burp Suite / MITM Proxy
   - Debugging with Logcat / iOS Console / Frida traces
5. **Common Vulnerabilities in Mobile Apps**
   - Insecure storage (Shared Preferences, SQLite, Keychain)
   - Insecure communication (HTTP, SSL, pinning bypass)
   - Insecure authentication & authorization (JWT, OAuth flaws)
   - Reverse engineering & code tampering
   - Deep link abuse & insecure IPC
   - Improper implementation of root/jailbreak detection
6. **Bypassing Security Controls**
   - SSL pinning bypass (Frida, Burp's Mobile Assistant)
   - Root detection bypass
   - Debugger detection bypass
   - App repackaging
7. **Reporting Mobile App Bugs and Case Studies**
   - CVSS scoring for mobile
   - Responsible disclosure methods
   - Proof of concept for mobile flaws
   - Real world mobile app vulnerabilities reported on HackerOne/Bugcrowd

Note: At the midpoint of this course, you'll step beyond labs into the real-world VAPT environment. You'll directly interact with experienced penetration testers, security analysts, and engineers to gain insights into how real assessments are performed in production environments. This hands-on exposure bridges the gap between tools and true consulting - giving you an edge no traditional course offers.

"We don't teach checklists - we train cyber warriors."