3-Month Cybersecurity and VAPT Training AI+ Syllabus

Master the fundamentals of cybersecurity, ethical hacking, and cutting-edge AI security techniques in this comprehensive 12-week intensive program.

From reconnaissance to advanced penetration testing, this syllabus will transform you into a skilled cybersecurity professional.

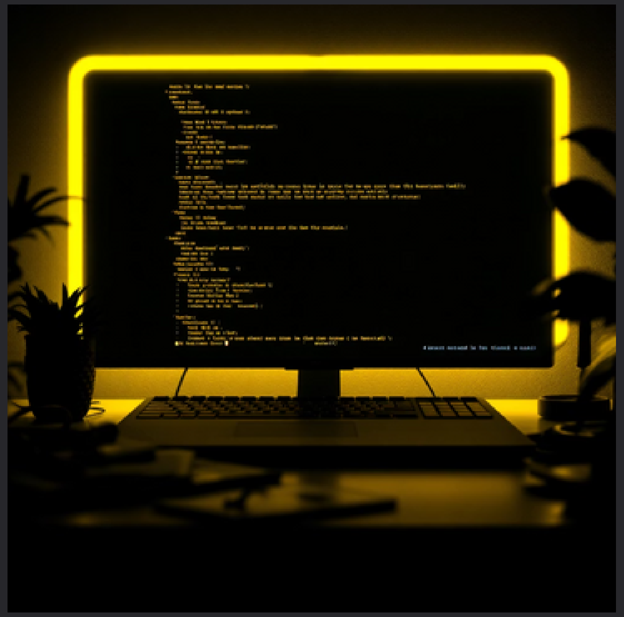
Month 1: Foundations

Week 1: Introduction to Cybersecurity & Ethical Hacking

- Cybersecurity basics: CIA triad, threat landscape, attack vectors
- Security domains (network, web, cloud, application, mobile)
- Lab setup: Kali Linux, Burp Suite, OWASP ZAP, Postman, VirtualBox/VMware
- Introduction to penetration testing lifecycle

Week 2: Reconnaissance & Footprinting

- Information Gathering & Reconnaissance
- Tools: Nmap, Maltego, Recon-ng
- Passive & Active Reconnaissance
- Lab: Perform OSINT on a test domain



Build your cybersecurity foundation with essential concepts and hands-on lab experience. Master the CIA triad principles while setting up your professional penetration testing environment with industry-standard tools.

Week 3: Scanning & Enumeration

- Scanning Networks
- Enumeration (SMB, SNMP, LDAP, DNS)
- Tools: Nmap scripting engine, Netcat, Nikto
- Lab: Enumerate open ports and services on a target VM

Week 4: System & Web Basics

- Vulnerability Analysis
- System Hacking (Password Attacks, Privilege Escalation, Keyloggers)
- Web Application Attacks basics (SQLi, XSS, CSRF)
- Lab: Exploit a vulnerable web app (DVWA / Juice Shop)

Progress from basic network scanning to advanced enumeration techniques. Learn to identify vulnerabilities in both system and web applications while gaining hands-on experience with real-world exploitation scenarios.

Month 2: API Security + VAPT + Bug Hunting

Week 5: API Security Basics

- What are APIs? REST vs SOAP vs GraphQL
- Common API vulnerabilities (OWASP API Security Top 10)
- Authentication & Authorization flaws (Broken Auth, JWT issues)
- Tools: Postman, Burp Suite extensions for API testing
- Lab: Test insecure APIs with intentional vulnerabilities

Week 6: VAPT Methodology – Part 1 (Web + API)

- Vulnerability Assessment vs Penetration Testing
- VAPT phases: Pre-engagement, Scanning, Exploitation, Reporting
- Web VAPT methodology (OWASP Top 10 focus)
- Lab: Conduct VAPT on a test web app & API endpoints

Focus Area: Master API security fundamentals and professional VAPT methodologies that are in high demand in today's cybersecurity landscape.

1

Week 7: VAPT Methodology – Part 2 (Network + Cloud)

- Network VAPT methodology (scanning, exploitation, pivoting)
- Cloud Security basics (AWS/Azure misconfigurations, S3 bucket exposure)
- Lab: Exploit misconfigured S3 bucket + escalate privileges in network pentest

2

Week 8: Bug Hunting Fundamentals

- Introduction to Bug Bounty platforms (HackerOne, Bugcrowd, Intigriti)
- How to read/write professional vulnerability reports
- Common real-world bug classes: IDOR, SSRF, RCE, Authentication flaws
- Lab: Find and report a bug in Juice Shop / HackTheBox Academy

Month 3: Advanced Topics + AI in Cybersecurity

Week 9: CEH Advanced Modules

- Malware Threats
- Sniffing (Wireshark, tcpdump)
- Social Engineering Attacks
- Denial of Service Attacks
- Lab: Packet sniffing & analyzing captured traffic

Week 10: Post-Exploitation + Bug Hunting (Intermediate)

- Lateral movement, privilege escalation
- Exploiting real-world web flaws (SSRF → RCE chains)
- Lab: Privilege escalation on Linux/Windows vulnerable machines

Master advanced penetration testing techniques including post-exploitation tactics and sophisticated attack chains. Develop expertise in packet analysis and social engineering while preparing for professional certifications.

1

Week 11: AI in Cybersecurity

- AI for threat detection & malware analysis
- Using ML for phishing detection (basic project: spam vs ham classifier)
- Adversarial AI: Evasion attacks against ML models
- AI-driven bug hunting (using GPT-powered payload generation, AI-assisted recon)
- Lab: Build a small ML model for anomaly detection in logs

2

Week 12: Capstone Project + Review

Choose your capstone project:

1. Perform end-to-end VAPT on a vulnerable web app + API and write a report
1. Bug hunting simulation: find and report at least 3 unique bugs
1. AI mini-project: Use ML to classify malicious vs benign traffic

> **"The future of cybersecurity lies at the intersection of human expertise and artificial intelligence."**

Career Roadmap

Recommended Certifications:

- CEH (Certified Ethical Hacker)
- OSCP (Offensive Security Certified Professional)
- API Security Specialist
- AI Security Research

Final Assessment

- Mock Bug Bounty assessment
- Professional VAPT simulation
- AI-powered security project presentation
- Course completion and certification pathway guidance