VAPT & Ethical Hacking Curriculum

Become a Certified Cybersecurity Professional

The VAPT (Vulnerability Assessment & Penetration Testing) & Ethical Hacking Program is designed to provide real-world cybersecurity skills through intensive hands-on labs, real attack simulations, and professional penetration testing methodologies.

This program prepares students for careers such as Ethical Hacker, Penetration Tester, Security Analyst, and Cybersecurity Consultant.

Program Highlights

✓ 4 Months Intensive Training
✓ Real-Time Hacking Labs
✓ Industry Standard Tools
✓ Live Attack Simulation
✓ Resume Building & Interview Preparation
✓ Capstone Security Project
✓ Certification on Completion
✓ Placement Assistance

AimNxt School of Tech Leaders

Course Curriculum

Networking Fundamentals & Lab Setup

- OSI Model & TCP/IP Architecture
- IP Addressing & Subnetting
- Network Protocol Analysis
- Port Scanning Techniques
- Network Mapping & Discovery

Hands-on Tools:

Wireshark, Nmap, Netdiscover, Kali Linux

Linux for Hackers

- Linux Command Line Essentials
- File Permissions & User Management
- Process & Network Monitoring
- Bash Scripting for Automation
- Linux Privilege Escalation Techniques

Windows Internals & Active Directory

- Windows Architecture & Security Components
- PowerShell for Security Testing
- Active Directory Setup & Configuration
- Windows Authentication Mechanisms
- Windows Privilege Escalation Attacks

Tools Covered:

Mimikatz, Hashcat, PowerView

Web Technologies & OWASP Top 10

- HTTP Protocol Deep Dive
- Web Application Architecture
- Client-Side Technologies (JavaScript, Cookies, DOM)
- Server-Side Technologies (PHP & Backend Logic)
- OWASP Top 10 Security Vulnerabilities

Hands-on Tools:

Burp Suite, DVWA, bWAPP

AimNxt School of Tech Leaders

Information Gathering & Reconnaissance

- Passive Reconnaissance (OSINT)
- DNS Enumeration Techniques
- Subdomain Discovery
- Active Network Reconnaissance
- Web Application Recon

Tools Covered:

theHarvester, Maltego, Amass, Sublist3r, Gobuster

Vulnerability Assessment & Scanning

- Vulnerability Assessment Fundamentals
- CVE & CVSS Analysis
- Automated Vulnerability Scanning
- Manual Vulnerability Validation
- Web Application Security Scanning

Tools Covered:

Nessus, OpenVAS, OWASP ZAP, Nikto, WPScan

Web Security – Injection Attacks

- SQL Injection (Basic & Advanced)
- Command Injection Attacks
- XML External Entity (XXE) Attacks
- Template Injection (SSTI)
- Remote Code Execution

Web Security – Authentication & Authorization

- Broken Authentication Attacks
- Session Management Vulnerabilities
- Password Cracking Techniques
- Multi-Factor Authentication Bypass
- Authorization & Access Control Issues

Client-Side Attacks & Logic Flaws

- Cross-Site Scripting (XSS)
- Advanced XSS Techniques
- Cross-Site Request Forgery (CSRF)
- CORS & PostMessage Exploitation
- Business Logic Vulnerabilities

AimNxt School of Tech Leaders

Network Exploitation & Post-Exploitation

- Metasploit Framework
- Exploiting Network Services (SMB, FTP, SSH, RDP)
- Windows Post-Exploitation
- Linux Post-Exploitation
- Lateral Movement & Network Pivoting

Active Directory Attacks

- Active Directory Enumeration
- Kerberos Attacks (Kerberoasting)
- NTLM Relay Attacks
- Domain Privilege Escalation
- Domain Persistence Techniques

Wireless Security & IoT

- Wireless Network Fundamentals
- WiFi Attacks & Handshake Capture
- Wireless Reconnaissance
- Bluetooth & RFID Security
- IoT Security Testing

Mobile Application Security

- Mobile Security Fundamentals
- Android Application Analysis
- Android Runtime Security Testing
- Mobile API Security Testing
- iOS Security Basics

Cloud Security & API Testing

- Cloud Security Fundamentals
- AWS Security Testing
- Azure Security Testing
- REST API Security Testing
- GraphQL & WebSocket Security

AimNxt School of Tech Leaders

Report Writing & Professional Skills

- Professional Penetration Testing Reports
- Vulnerability Documentation
- Executive Summary Writing
- Remediation & Security Recommendations
- GitHub Portfolio & LinkedIn Profile Building

Capstone Project

Students will conduct a complete real-world penetration testing engagement including:

- Reconnaissance & Target Mapping
- Vulnerability Identification
- Exploitation & Privilege Escalation
- Post-Exploitation Activities
- Professional Security Report & Presentation

Tools Covered in Training

- Kali Linux
- Nmap
- Wireshark
- Burp Suite
- Metasploit
- Nessus
- OpenVAS
- Hashcat
- John The Ripper
- SQLMap
- Gobuster
- Amass

Career Opportunities

After completing this program, you can apply for roles such as:

- Ethical Hacker
- Penetration Tester
- SOC Analyst
- Cybersecurity Analyst
- Security Consultant
- Vulnerability Analyst

Program Details

Course Duration: 4 Months
Training Mode: Online / Offline / Hybrid
Certification: Course Completion Certificate
Placement Assistance: Yes

Who Can Join?

- Students (B.Tech, Degree, Diploma)
- IT Professionals
- Networking Engineers
- Cybersecurity Enthusiasts
- Anyone interested in Ethical Hacking