CyberHunt

Advanced VAPT Expert Program

Master advanced offensive security and defensive strategies through real-world VAPT methodologies.

From reconnaissance to reporting—learn, exploit, secure, and protect.

Built by practitioners. Proven by results.

- 100% Practical Training
- Industry-Aligned Curriculum
- Advanced Hacking Methodologies
- Real-World Attack Simulation

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

ABOUT COURSE

Advanced VAPT Expert Program

Advanced VAPT Expert is a hands-on, real-time penetration testing program covering enterprise network security, web & API security, Active Directory exploitation, red teaming methodologies, and professional reporting aligned with global standards.

This program prepares candidates with the skills required to perform comprehensive vulnerability assessments and penetration tests across real enterprise environments. You will work through live attack scenarios, compromise real networks, and deliver executive-level pentest reports.

With a curriculum spanning advanced reconnaissance, web & API exploitation, Active Directory attacks, red team operations, and cloud security, this is the most comprehensive VAPT program available — covering every domain required by industry-leading security teams.

VAPT Domain Coverage

Web & API Security Testing	25%
Network Penetration Testing	20%
Active Directory Exploitation	20%
Privilege Escalation	15%
Red Team & Cloud Security	20%

CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.

CyberHunt

Module-Wise Syllabus
Course Curriculum

Comprehensive hands-on penetration testing training aligned with enterprise standards

01 Advanced Reconnaissance & OSINT

- Passive vs Active Reconnaissance
- Advanced Google Dorking
- WHOIS, ASN & DNS Enumeration
- Subdomain Enumeration (Manual + Automated)
- OSINT Framework Usage
- Shodan & Censys Recon
- Metadata Extraction
- Attack Surface Mapping
- Recon Automation Scripting

Practical: Reconnaissance of a live target domain and full attack surface mapping.

02 Advanced Network Penetration Testing

- TCP/IP Deep Dive for Pentesters
- Advanced Nmap Techniques
- Firewall & IDS/IPS Evasion
- SMB, FTP, SNMP Exploitation
- Service Exploitation
- Banner Grabbing & Version Detection
- Vulnerability Validation (Manual Testing)
- Exploit Research & CVE Mapping
- Exploitation using Metasploit
- Manual Exploitation Techniques

Practical: Compromise internal network services and escalate access.

03 Web Application Penetration Testing (Advanced)

- Web Application Architecture
- OWASP Top 10 – Deep Practical
- SQL Injection (Manual + Automated)
- XSS (Stored, Reflected, DOM-Based)
- CSRF Exploitation
- IDOR & Access Control Issues
- File Upload Vulnerabilities
- Authentication & Session Attacks
- Business Logic Vulnerabilities
- SSRF, XXE, Command Injection
- Web Shell Deployment

Practical: Complete manual web app pentest with vulnerability chaining.

04 API Security Testing

- API Architecture (REST, SOAP)
- API Recon & Endpoint Discovery
- Broken Object Level Authorization (BOLA)
- JWT Exploitation
- API Rate Limiting Bypass
- Parameter Tampering
- GraphQL Security Issues
- API Automation Testing using Tools

Practical: Full API security assessment of enterprise application.

05 Active Directory Exploitation

- AD Architecture & Components
- LDAP & Kerberos Concepts
- User & Group Enumeration
- Kerberoasting Attack
- AS-REP Roasting
- Pass-the-Hash Attack
- Pass-the-Ticket Attack
- NTLM Relay
- Golden Ticket & Silver Ticket
- BloodHound Analysis
- Lateral Movement Techniques

Practical: Complete AD Domain Compromise Simulation.

06 Privilege Escalation Mastery

- Service Misconfiguration (Windows)
- Unquoted Service Path
- Token Manipulation & DLL Hijacking
- Registry Exploitation
- SUID Exploitation (Linux)
- Cron Jobs Exploitation
- Kernel Exploits
- Misconfigured Permissions

Practical: Privilege escalation on both Windows & Linux machines.

07 Red Team Operations

- Red Team vs Pentesting
- Command & Control (C2) Concepts
- Payload Generation
- Phishing Simulation Basics
- AV Evasion Techniques
- Lateral Movement Strategy
- Data Exfiltration Techniques
- Persistence Mechanisms

Practical: Red Team Attack Simulation in Controlled Lab.

08 Cloud & Internal Network Pentesting

- AWS Misconfiguration Testing
- Azure Security Misconfigurations
- IAM Privilege Escalation
- Cloud Storage Exploitation
- Internal Network Segmentation Testing

Practical: Cloud Security Assessment Case Study.

09 Vulnerability Reporting & Client Communication

- Risk Rating (CVSS)
- Writing Executive Summary
- Technical Finding Documentation
- Proof of Concept Writing
- Remediation Recommendations
- Compliance Mapping
- Professional Pentest Report Creation

Practical: Submission of final enterprise-level penetration testing report.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!

For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on