K7 ACADEMY

Applied VAPT & Offensive Security Programme

Overview

The Applied VAPT & Offensive Security Programme is a comprehensive advanced course for security professionals who want to operate at a Red Team and professional pentesting level. Across 42 hours you will master advanced recon, web application exploitation, Active Directory attacks, Linux privilege escalation, wireless attacks, social engineering, malware creation and AV evasion, cloud and container security, post-exploitation frameworks, and professional report writing — all culminating in a full enterprise VAPT simulation.

Mode	Duration	Level
Online/Offline Classes	42 Hours	Intermediate to Advanced

Who Should Enrol?

- VAPT Foundation Programme graduates ready for advanced content
- Junior Pentesters aiming to move into senior or Red Team roles
- Security Engineers wanting offensive depth for better defence
- Bug Bounty Hunters targeting high-severity and chained vulnerabilities
- SOC Analysts who want to understand attacker tradecraft from the inside

Learning Outcomes

- Perform advanced recon using Shodan, Censys, and automated attack surface mapping
- Exploit advanced web vulnerabilities: SQLi, XSS, JWT attacks, GraphQL, API flaws
- Bypass WAF protections and conduct full bug bounty methodology
- Execute Active Directory attacks — Kerberoasting, DCSync, Golden/Silver Tickets
- Escalate privileges on Linux systems via SUID, Cron, kernel, and PATH exploitation
- Conduct wireless attacks — WPA2/3 cracking, PMKID, and Evil Twin campaigns
- Build and deploy custom payloads and evade AV/EDR detections
- Analyse and sandbox malware — static and dynamic analysis
- Identify and exploit AWS, Azure, Docker, and Kubernetes misconfigurations
- Operate post-exploitation frameworks and perform lateral movement
- Write professional, executive, and technical VAPT reports with CVSS scoring
- Deliver a full enterprise VAPT simulation from recon to final report

Modules

Module 1 — Advanced Recon & Enumeration

- Advanced Nmap & NSE
- Subdomain Enumeration
- OSINT & Attack Surface Mapping
- Shodan & Censys
- Real-world recon methodology
- Attack surface reduction concepts

Module 2 — Advanced Web Application Pentesting

- OWASP Top 10
- SQL Injection Advanced
- XSS Advanced
- JWT Attacks
- GraphQL Security
- API Security Testing
- WAF Bypass Concepts
- Bug bounty workflow
- Advanced Burp Suite methodology

Module 3 — Network Penetration Testing

- SMB Exploitation
- Hydra & Password Attacks
- Pivoting & Tunneling
- Pass-the-Hash
- IPv6 Attacks

Module 4 — Windows & Active Directory Attacks

- BloodHound
- Kerberoasting
- AS-REP Roasting
- DCSync
- Golden Ticket & Silver Ticket
- LSASS Credential Access
- UAC Bypass Concepts
- AD attack path mapping
- Privilege escalation lab scenarios

Module 5 — Linux Exploitation & Privilege Escalation

- SUID Exploitation
- Cron Job Hijacking
- Kernel Exploits
- PATH Hijacking

Module 6 — Wireless & Social Engineering

- WPA2/WPA3 Attacks
- PMKID Attack
- Evil Twin Attack
- GoPhish
- SET Toolkit
- Real phishing campaign simulation

Module 7 — Malware & AV Evasion

- msfvenom Payloads
- Static Malware Analysis
- Dynamic Malware Analysis
- AV/EDR Evasion
- Process Hollowing
- Reflective DLL Injection
- Safe malware sandboxing
- Android APK Payload Generation

Module 8 — Cloud & Container Security

- AWS Misconfigurations
- Azure Misconfigurations
- Docker Security
- Kubernetes Security
- Cloud IAM abuse scenarios
- Container escape practical

Module 9 — Reporting & Professional Practice

- Executive Summary Writing
- Technical Reporting
- CVSS Scoring
- Retesting Methodology
- Professional evidence documentation

Module 10 — Post-Exploitation, Persistence & Lateral Movement

- Post-Exploitation Frameworks (Cobalt Strike Concepts, Sliver)
- Persistence Mechanisms (Registry, Scheduled Tasks, Services)
- Lateral Movement Techniques (WMI, PsExec, SMB)
- Command & Control (C2) Concepts
- Data Exfiltration Techniques
- OPSEC for Pentesters
- Hands-on lab: Full attack chain simulation

Module 11 — Final Capstone Project

- Full enterprise VAPT simulation
- Recon → Exploit → Report workflow

Tools & Technologies Covered

Kali Linux
Primary offensive security OS

Nmap/NSE
Advanced scanning & enumeration

Amass/Subfinder
Subdomain & OSINT enumeration

Shodan/Censys
Internet-wide asset discovery

Burp Suite Pro
Advanced web application testing

SQLMap
Automated SQL injection

Metasploit
Exploitation & post-exploitation

BloodHound
AD attack path visualisation

Impacket
AD protocol exploitation suite

Mimikatz
Credential extraction

Aircrack-ng
Wireless password cracking

GoPhish
Phishing campaign platform

SET Toolkit
Social engineering attacks

msfvenom
Custom payload generation

Chisel/Ligolo
Tunneling & pivoting

CVSS Calculator
Vulnerability severity scoring

ANY.RUN/Cuckoo
Malware dynamic sandboxing

Hydra
Network password brute-forcing

Career Opportunities

Role

- Penetration Tester
- Red Team Operator
- Web Application Pentester
- Active Directory Specialist
- Cloud Security Pentester
- Bug Bounty Hunter (Advanced)
- Malware Analyst/RE
- Senior VAPT Consultant

Certification & Assessment

- Module-wise Quizzes
- Lab Submission Reports — graded hands-on exercises
- Final Certification Exam — Passing Score: 70%

K7 ACADEMY

www.k7academy.com

202607163