K7 ACADEMY

VAPT Foundation Programme

Overview

The VAPT Foundation Programme is designed for beginners who wish to build practical skills in Vulnerability Assessment and Penetration Testing. Over 18 focused hours, you will set up your own hacking lab, learn networking and Linux essentials, perform real scanning and exploitation, and understand how attackers think – giving you the foundation for an offensive security career.

Mode	Duration	Level
Online/Offline Classes	18 Hours	Beginner

Who Should Enrol?

- Cybersecurity beginners and IT students seeking an offensive security entry point
- Developers & sysadmins wanting to understand how attacks work
- Bug bounty hunters starting their journey
- Anyone curious about ethical hacking who wants structured, hands-on training

Learning Outcomes

- Explain the difference between Vulnerability Assessment and Penetration Testing
- Set up a professional ethical hacking lab with Kali Linux and Metasploitable
- Analyse network traffic and identify protocol anomalies using Wireshark
- Perform active reconnaissance, port scanning, and service enumeration with Nmap
- Conduct OSINT and target footprinting using industry-standard tools
- Execute basic web application tests and identify OWASP Top 10 vulnerabilities
- Perform password attacks using John the Ripper and Hashcat
- Launch safe exploitations using Metasploit Framework
- Document findings and produce a basic penetration testing report

Modules

Module 1 – Introduction to Ethical Hacking & Career Roadmap

- What is VAPT? VA vs PT
- Types of Hackers
- Career Paths
- Lab Setup: Kali Linux, VirtualBox, Metasploitable
- Cyber Kill Chain basics
- Real-world attack demonstrations

Module 2 – Networks & Internet Basics

- OSI & TCP/IP
- Ports & Protocols
- DNS, DHCP, ARP
- Wireshark Packet Capture
- Hands-on packet analysis lab

Module 3 – Linux Fundamentals

- Linux commands
- Permissions
- Processes
- Basic Bash Scripting
- Linux file hunting practical

Module 4 – Web Technologies Primer

- HTTP Methods
- Cookies & Sessions
- Burp Suite Introduction
- SQL Basics
- OWASP Top 10 beginner labs

Module 5 – Password Attacks

- Hash Functions
- Dictionary vs Brute-force
- John the Ripper
- Hashcat Basics
- Weak password auditing practical

Module 6 – Scanning & Enumeration

- Nmap Scan Types
- NSE Scripts
- SMB Enumeration
- Live target scanning practical

Module 7 – Exploitation Basics

- Metasploit Basics
- Reverse Shell vs Bind Shell
- SearchSploit
- Safe exploitation lab

Module 8 – OSINT & Reconnaissance

- WHOIS
- Google Dorking
- theHarvester
- Maltego
- LinkedIn OSINT exercises
- Target footprinting assignment

Tools & Technologies Covered

Kali Linux
Primary pentesting OS

VirtualBox
Lab virtualisation

Metasploitable
Intentionally vulnerable target

Wireshark
Packet capture & analysis

Nmap
Port scanning & enumeration

Burp Suite CE
Web proxy & vulnerability testing

Metasploit
Exploitation framework

SearchSploit
Offline exploit lookup

John the Ripper
Password cracking

Hashcat
GPU password recovery

theHarvester
OSINT – emails & subdomains

Maltego CE
Visual intelligence mapping

Career Opportunities

Role

- Junior Penetration Tester
- Bug Bounty Hunter (Entry)
- Vulnerability Assessment Analyst
- IT Security Support Engineer
- Cyber Security Intern/Trainee

Certification & Assessment

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

K7 ACADEMY

www.k7academy.com

202607171