ARMOURINFOSEC®

Hands-On Cyber Security Training · Indore, India

Certified Ethical Hacking & Penetration Testing

Course Syllabus

Master ethical hacking, penetration testing, vulnerability assessment, exploitation techniques, privilege escalation, malware analysis, network attacks, cryptography, and advanced offensive security methodologies using Kali Linux and real-world cybersecurity labs.

// COURSE INFORMATION

Course Information

DURATION	10 Months / 40 Weeks / 300 Hours
LEVEL	Beginner to Advanced
MODULES	16
FORMAT	Hands-on Labs / Hybrid (Online + Indore Classroom)

// COURSE OVERVIEW

Course Overview

The Advanced Ethical Hacking & Penetration Testing course is designed for aspiring ethical hackers, penetration testers, cybersecurity professionals, SOC analysts, red teamers, and security researchers who want practical offensive security skills. This course covers Kali Linux fundamentals, ethical hacking methodologies, footprinting, network scanning, enumeration, vulnerability assessment, exploitation, privilege escalation, buffer overflows, malware analysis, sniffing, social engineering, DoS attacks, cryptography, IDS/firewall evasion, and Metasploit framework mastery.

// LEARNING OBJECTIVES

Learning Objectives

- Conduct comprehensive penetration tests following industry methodologies
- Perform OSINT and reconnaissance using professional tools
- Scan and enumerate networks, services, and vulnerabilities
- Exploit vulnerabilities in networks, systems, and applications
- Conduct privilege escalation on Linux and Windows systems
- Develop and deploy buffer overflow exploits
- Master the Metasploit framework for exploitation and post-exploitation
- Evade security controls including IDS, firewalls, and honeypots
- Analyze malware and understand threat behavior

- Write professional penetration testing reports with remediation guidance
- Prepare for OSCP+, CEH, and CompTIA PenTest+ certifications

// PREREQUISITES
Prerequisites

- Basic networking knowledge (TCP/IP, DNS, HTTP)
- Familiarity with Linux and Windows operating systems
- Understanding of basic computer security concepts
- Laptop with 8GB+ RAM for lab environments

// MODULE BREAKDOWN
Module Breakdown

01 Kali Linux Fundamentals

- Kali Linux History and Introduction
- Installing Kali Linux
- Kali Linux GUI Desktops
- Kali Linux Commands
- Package Management
- Managing Repositories
- User Account Management
- File Permissions
- Network Configuration

02 Introduction to Penetration Testing & Ethical Hacking

- Hacking Concepts
- Ethical Hacking Principles
- Hacker Classes (White/Grey/Black Hat)
- Hacking Phases
- CIA Triad
- Defense in Depth
- Vulnerability Assessment
- Penetration Testing Methodology (PTES)
- Risk Management
- Red Team vs Blue Team vs Purple Team

03 Footprinting & Reconnaissance

- Search Engine Footprinting
- Website Footprinting
- Email Footprinting
- Google Hacking (Dorking)
- WHOIS Footprinting
- DNS Footprinting
- Social Engineering Recon
- Shodan

- GitHub Recon
- OSINT Framework
- Maltego

04 Scanning Networks

- Network Scanning Methodology
- Live Host Discovery
- Banner Grabbing
- Port Scanning Techniques
- Nmap Scanning Techniques
- NSE Scripts
- IDS Evasion During Scanning
- Vulnerability Scanning
- OpenVAS
- Nessus
- Nuclei

05 Proxies, VPNs & Tor

- Proxy Servers
- VPNs and VPN Protocols
- Jump Boxes
- SOCKS Proxies
- Proxy Chaining
- Tor Network
- Anonymous Browsing
- Operational Security for Pentesters

06 Tunneling Techniques

- HTTP Tunneling
- SSH Tunneling (Local, Remote, Dynamic)
- TCP/UDP Tunneling
- VPN Tunneling
- OpenVPN Configuration
- DNS Tunneling
- Pivoting Through Compromised Hosts

07 Enumeration

- DNS Enumeration
- SMB Enumeration
- FTP Enumeration
- SSH Enumeration
- SNMP Enumeration
- SMTP Enumeration
- NFS Enumeration
- MSSQL Enumeration
- MySQL Enumeration

- VNC Enumeration
- RDP Enumeration

08 System Hacking & Malware Threats

- Windows Security Architecture
- Password Cracking (Hashcat, Hydra, John the Ripper)
- Keyloggers
- Steganography
- Trojans and Backdoors
- Virus and Worm Concepts
- Malware Analysis Fundamentals
- Authentication Mechanisms
- Hashing Algorithms

09 Privilege Escalation

- Linux Privilege Escalation
- Windows Privilege Escalation
- SUID and SGID Exploitation
- Kernel Exploits
- Password Mining
- PATH Variable Abusing
- Cron Job Exploitation
- Service Exploitation
- Registry Exploits
- Startup Application Abuse

10 Buffer Overflow

- Stack Overflow Concepts
- Heap Overflow
- Format String Vulnerabilities
- Integer Overflow
- Exploitation Techniques
- ASLR (Address Space Layout Randomization)
- Stack Canaries
- Shellcode Development
- Mitigation Strategies

11 Advanced Exploitation & Metasploit Framework

- Metasploit Fundamentals
- Payloads and Exploits
- Meterpreter Sessions
- Msfvenom Payload Generation
- Exploit Writing Basics
- Vulnerability Scanning with Metasploit
- Persistence Mechanisms
- Session Hijacking

- Keylogging via Meterpreter
- Post-Exploitation Techniques

12 Evading IDS, Firewalls & Honeypots

- Firewall Evasion Techniques
- IDS Evasion Methods
- Honeypot Detection
- Fragmentation Attacks
- Obfuscation Techniques
- Session Splicing
- Snort IDS/IPS
- Detection and Countermeasures

13 Sniffing & MITM Attacks

- Packet Sniffing Concepts
- MAC Flooding
- ARP Poisoning
- DHCP Attacks
- DNS Poisoning and Spoofing
- Wireshark Packet Analysis
- Tcpdump Usage
- Network Packet Analysis
- MITM Attack Techniques
- SSL Stripping

14 Social Engineering

- Phishing Attacks
- Spear Phishing
- Shoulder Surfing
- Dumpster Diving
- Insider Threats
- Fake Security Applications
- Identity Theft
- Anti-Phishing Techniques
- Social Engineering Toolkit (SET)

15 Denial of Service (DoS/DDoS)

- DoS Attack Concepts
- DDoS Attack Types
- SYN Flooding
- ICMP Flooding
- Botnets
- Application-Layer Attacks
- Amplification Attacks
- Detection Techniques
- DDoS Protection and Mitigation

16 Cryptography

- Symmetric Encryption (AES, DES)
- Asymmetric Encryption (RSA, DSA)
- Hash Functions (MD5, SHA)
- SSL/TLS Protocols
- SSH Encryption
- PKI (Public Key Infrastructure)
- Digital Certificates
- Cryptographic Attacks
- Steganography Techniques

// TOOLS & HANDS-ON LABS

Tools & Hands-On Labs

- Dedicated Kali Linux attack machine
- Vulnerable target machines (Windows & Linux)
- Active Directory lab environment
- Network simulation with multiple subnets
- Buffer overflow practice targets
- Metasploit exploitation lab
- Packet capture and analysis environment
- 24/7 lab access during course duration

// TRAINING MODE

Training Mode

Every Armour Infosec course runs as a unified programme delivered in two parallel modes — the same curriculum, the same trainers, the same certification, regardless of how you join.

- ✓ Online Live Classes — real-time, instructor-led, fully interactive sessions
- ✓ On-Premise Classroom Training — in-person at our Indore centre (Sudama Nagar)
- ✓ Both modes run concurrently in every batch; switch between them as your schedule needs
- ✓ Same syllabus, lab access, and certification track for online and on-premise students

// CERTIFICATIONS & CAREER OUTCOMES

Certifications & Career Outcomes

This course aligns with industry-recognised certifications and prepares graduates for offensive-security, application-security, and infrastructure-security roles.

- OSCP+ (Offensive Security Certified Professional+) — Advanced Offensive Security Certification
- CEH (Certified Ethical Hacker)
- CompTIA PenTest+
- eJPT (eLearnSecurity Junior Penetration Tester)
- GPEN (GIAC Penetration Tester)

// ENROL WITH ARMOUR INFOSEC

Enrol With Armour Infosec

Reach out to discuss enrolment, batch schedule, and lab access. Our Indore training centre runs both in-person and live online cohorts with placement assistance.

PHONE	+91 99777 47168
EMAIL	info@armourinfosec.com
ADDRESS	674, Sudama Dwar, Narendra Tiwari Marg, Sudama Nagar, Indore, Madhya Pradesh 452009
WEBSITE	https://armourinfosec.com

Scan to View Course Online

https://www.armourinfosec.com/training/ethical-hacking/