

 Beginner-Friendly **Live Bootcamp**

Think Like a Hacker

Hands-On Ethical Hacking Program

Start your cybersecurity journey
with guided practical labs.

Ashish Dhyani

10+ Years Experience

OSCP | CEH | Pentest+

Hands-on Ethical Hacking Practice

Nmap, Hydra & Wireshark exposure

OWASP, CVE & MITRE ATT&CK basics

AI-assisted ethical hacking

REGISTER NOW →



₹2000/-

₹99/- +TAXES

\$199

\$9

Only **30 Seats Left** at **This Price**

Why Attend?

Ethical hacking is one of the most important starting points for anyone who wants to understand how attackers think, how systems are tested, and how security weaknesses are identified before they are exploited. This bootcamp gives learners a structured introduction to ethical hacking concepts, penetration testing basics, reconnaissance, scanning, vulnerability assessment, web application attacks, password attacks, and social engineering risks.

Designed for beginners and early-stage cybersecurity learners, the program breaks down offensive security concepts in a clear and practical way. Participants will understand the ethical hacking methodology, common attack surfaces, basic tools, security testing approaches, and the role of responsible reporting in real-world cybersecurity assessments.

What Sets This Training Apart

Beginner-Friendly Ethical Hacking Start offensive security from the fundamentals	Web Attack Awareness Explore OWASP Top 10, SQL injection, and XSS basics
Structured Methodology Understand the full ethical hacking lifecycle from planning to reporting	Reconnaissance & Scanning Focus Understand how attackers identify exposed systems
Password & Social Engineering Coverage Learn common human and credential-based risks	Career-Focused Learning Earn 8 CPEs and build a strong foundation for ethical hacking roles

Key Takeaways

✓ Practice reconnaissance, scanning, and vulnerability assessment	✓ Build basic web and password testing skills
✓ Identify phishing and social engineering attack indicators	✓ Explore ethical hacking tools and AI-assisted analysis
✓ Learn OWASP, CVE, CVSS, Kill Chain, and MITRE	✓ Earn 8 CPE Credits

Meet the Expert



Ashish Dhyani

10+ Years of Experience

**Network+ | Security+ | Pentest+ | CEH | CND | ECSA | CCNA | ECDE | CPENT | LPT
OSCP**

Ashish Dhyani is an accomplished cybersecurity and network security professional, known for blending technical precision with practical application. He has delivered 30+ training programs annually, mentoring over 250 professionals worldwide in practical network defense, penetration testing, and exploit development.

Her specializations include:

- Internal & external vulnerability assessment and penetration testing (manual + tools).
- Cyber Threat Intelligence and Digital Forensics operations.
- Secure application and infrastructure design aligned with global standards.
- OSINT-based threat analysis and mitigation.
- Advanced red teaming, exploit development, and VAPT reporting.

Ashish's teaching style focuses on real-world threats, enabling participants to code, test, and defend with confidence.

Bootcamp Agenda

Day 1

Module 1: Ethical Hacking Fundamentals

- Cybersecurity and Information Security
- CIA Triad
- Threats, Vulnerabilities and Risk
- Ethical Hacking and Hacker Types
- Red Team, Blue Team and Purple Team
- Penetration Testing Basics
- Black-Box, White-Box and Gray-Box Testing

Module 2: AI-Assisted Ethical Hacking Methodology

- Ethical Hacking Methodology
- Cyber Kill Chain
- MITRE ATT&CK Introduction
- Role of AI in Ethical Hacking
- Responsible Use of AI in Security Testing

Practicals Covered

- Map reconnaissance, scanning and exploitation phases
- Map a sample attack to Cyber Kill Chain and MITRE ATT&CK
- Use AI to analyze findings

Tools Covered

SGPT, MITRE ATT&CK Navigator

Day 2

Module 3: Footprinting and Reconnaissance

- Passive and Active Reconnaissance
- OSINT Fundamentals
- Domain and DNS Information Gathering

Practicals Covered

- Perform WHOIS and DNS lookups
- Conduct search engine reconnaissance
- Identify website technologies and subdomains

Tools Covered

WHOIS, nslookup / dig, Wappalyzer, theHarvester

Module 4: Network Scanning

- IP Addressing Basics
- TCP, UDP, Ports and Services
- Host Discovery and Network Enumeration

Practicals Covered

- Discover live hosts
- Perform port scanning
- Identify services, versions and exposed ports

Tools Covered

Nmap, Netcat, Wireshark

Day 3

Module 5: Vulnerability Assessment

- Vulnerabilities and Exploits
- Security Misconfigurations and Missing Patches
- CVE and CVSS
- Vulnerability Prioritization

Practicals Covered

- Perform a basic vulnerability scan
- Analyze findings and related CVEs
- Interpret CVSS scores and prioritize vulnerabilities

Tools Covered

Nikto, Nmap NSE, NIST NVD

Module 6: Web Application Hacking

- Web Application Architecture
- HTTP Requests and Responses
- Parameters, Cookies and Sessions
- Authentication Basics
- OWASP Top 10 Introduction

Practicals Covered

- Inspect and modify HTTP requests
- Analyze cookies and sessions
- Demonstrate basic SQL Injection and XSS
- Identify authentication weaknesses

Tools Covered

Burp Suite, SQLMap

Day 4

Module 7: Password and System Hacking

- Password Security and Hashing
- Credential-Based Attacks
- Multi-Factor Authentication
- Privilege Escalation Basics

Practicals Covered

- Identify and analyze password hashes
- Demonstrate dictionary and brute-force concepts
- Review weak password policies and privilege escalation indicators

Tools Covered

Hashcat, John the Ripper, Hydra

Module 8: Social Engineering and Phishing

- Social Engineering Fundamentals
- Phishing and Spear Phishing
- Pretexting, Baiting and Impersonation
- Business Email Compromise
- Social Engineering Prevention

Practicals Covered

- Analyze sample phishing emails
- Inspect suspicious URLs and email headers
- Identify common social engineering indicators

Tools Covered

Zphisher, VirusTotal, URLScan.io

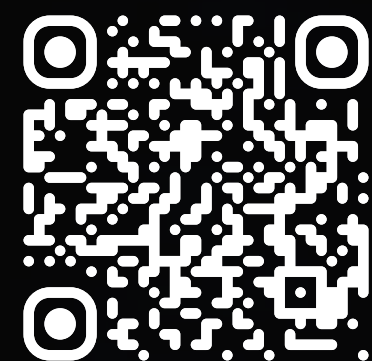


Get In Touch

 sales@infosectrain.com

 www.infosectrain.com

(A Brand of Azpirantz Technologies LLP)



Scan to Know More