SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

ETHICAL HACKING

CONNAISSANCE . SCANNING
WEB . NETWORK . WIRELESS
LINUX . METASPLOIT . BURP

DURATION	LEVEL	MODULES	MODE
60 Hours	**Beginner to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A hands-on ethical hacking course taught entirely inside a controlled lab environment. The course follows the standard attack lifecycle — footprinting, scanning, enumeration, exploitation, privilege escalation, persistence and reporting — with each phase practised against deliberately vulnerable targets.

Learners maintain a lab of Kali Linux, Metasploitable, DVWA and Windows targets, and produce a written assessment report at the end.

WHO IT IS FOR

- IT and network administrators
- Security analysts and SOC trainees
- Developers who need attacker perspective
- Students preparing for CEH-style exams

PREREQUISITES

Networking fundamentals and basic Linux command line.

02 LEARNING OUTCOMES

01 Set up and isolate a legal testing lab.

02 Gather information on a target without touching it.

03 Scan and enumerate hosts, ports and services.

04 Exploit common vulnerabilities with Metasploit.

05 Escalate privileges on Linux and Windows hosts.

06 Test web applications against the OWASP Top 10.

07 Write a clear findings and remediation report.

03 MODULE STRUCTURE

8 MODULES

01 FOUNDATIONS AND LAW

Security concepts

Attacker types

Attack lifecycle

Rules of engagement

Indian IT Act and consent

Reporting duties

02 LAB SETUP

Virtualisation

Kali Linux

Vulnerable targets

Network isolation

Snapshots

LAB

BUILD THE PRACTICE LAB

03 RECONNAISSANCE

Passive footprinting

WHOIS and DNS

Google dorking

OSINT sources

Email and employee mapping

TOOLS

THEHARVESTER MALTEGO SHODAN

04 SCANNING AND ENUMERATION

- Host discovery
- Port scanning
- Service and version detection
- SMB and SNMP enumeration
- Vulnerability scanning

TOOLS

NMAP · NESSUS ESSENTIALS · NIKTO

05 SYSTEM EXPLOITATION

- Exploit selection
- Payloads
- Meterpreter
- Password attacks
- Privilege escalation
- Persistence

TOOLS

METASPLOIT · JOHN THE RIPPER · HYDRA

06 WEB APPLICATION ATTACKS

- SQL injection
- Cross-site scripting
- Broken authentication
- File upload flaws
- CSRF
- Access control

TOOLS

BURP SUITE · OWASP ZAP · SQLMAP

07 NETWORK AND WIRELESS

- Sniffing
- Man-in-the-middle
- ARP spoofing
- Wi-Fi attacks
- Denial of service concepts

TOOLS

WIRESHARK · AIRCRACK-NG · ETTERCAP

08 SOCIAL ENGINEERING AND REPORTING

Phishing simulation	Pretexting
Awareness controls	Evidence handling
Report structure	Remediation advice

PROJECT

FULL ASSESSMENT OF THE LAB NETWORK WITH REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

ETHICAL HACKER **SECURITY ANALYST** **PENETRATION TESTER (JUNIOR)** **VULNERABILITY ANALYST** **IT SECURITY ADMINISTRATOR**

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com