SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

PENETRATION TESTING

OPING . EXPLOITATION . POST
ACTIVE DIRECTORY . WEB . A
ORTING . RETESTING . DEBR

DURATION	LEVEL	MODULES	MODE
70 Hours	**Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A professional penetration testing course covering methodology, exploitation depth and client reporting. The course works to a formal methodology — PTES and OWASP — from scoping and rules of engagement through exploitation, lateral movement and evidence collection. Active Directory attack paths and API testing are given full modules.

Assessment is a complete client-style report on a multi-host lab, defended in a debrief session.

WHO IT IS FOR

- Security analysts moving into offensive roles
- Ethical hacking course graduates
- SOC and blue team staff cross-training
- Consultants delivering assessments

PREREQUISITES

Ethical hacking fundamentals, networking, Linux and basic scripting.

02 LEARNING OUTCOMES

01 Scope an engagement and agree rules of engagement.

02 Enumerate and exploit hosts systematically.

03 Move laterally and escalate inside a domain.

04 Test web applications and APIs to OWASP standards.

05 Collect evidence without damaging systems.

06 Rate findings with CVSS and business impact.

07 Write and present a client-quality report.

03 MODULE STRUCTURE

8 MODULES

01 METHODOLOGY AND SCOPING

- PTES
- Scope and exclusions
- Time-boxing
- OWASP testing guide
- Legal agreements
- Client communication

02 INFRASTRUCTURE ENUMERATION

- Network mapping
- Credential discovery
- Service fingerprinting
- Attack surface documentation

TOOLS

NMAP · CRACKMAPEXEC · NETEXEC

03 EXPLOITATION

- Public exploits
- Payload handling
- Shell stabilisation
- Manual exploitation
- Antivirus considerations

TOOLS

METASPLOIT · MSFVENOM

04 POST-EXPLOITATION

- Local enumeration
- Credential dumping
- Persistence
- Privilege escalation
- Pivoting
- Cleanup

TOOLS

LINPEAS · WINPEAS · MIMIKATZ

05 ACTIVE DIRECTORY ATTACKS

- Domain enumeration
- AS-REP roasting
- ACL paths
- Kerberoasting
- Delegation abuse
- Domain persistence

TOOLS

BLOODHOUND · IMPACKET

06 WEB AND API TESTING

- Authentication flaws
- Business logic
- JWT handling
- Injection
- IDOR
- Rate limiting

TOOLS

BURP SUITE · POSTMAN

07 CLOUD AND CONTAINER NOTES

- Cloud misconfiguration
- Metadata services
- Secret exposure
- IAM abuse
- Container escapes

08 REPORTING AND DEBRIEF

- Evidence handling
- Executive summary
- Remediation plan
- CVSS scoring
- Technical detail
- Retest cycle

PROJECT

FULL PENETRATION TEST REPORT AND DEBRIEF

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

PENETRATION TESTER · RED TEAM OPERATOR · SECURITY CONSULTANT · APPLICATION SECURITY ANALYST · OFFENSIVE SECURITY ENGINEER

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com