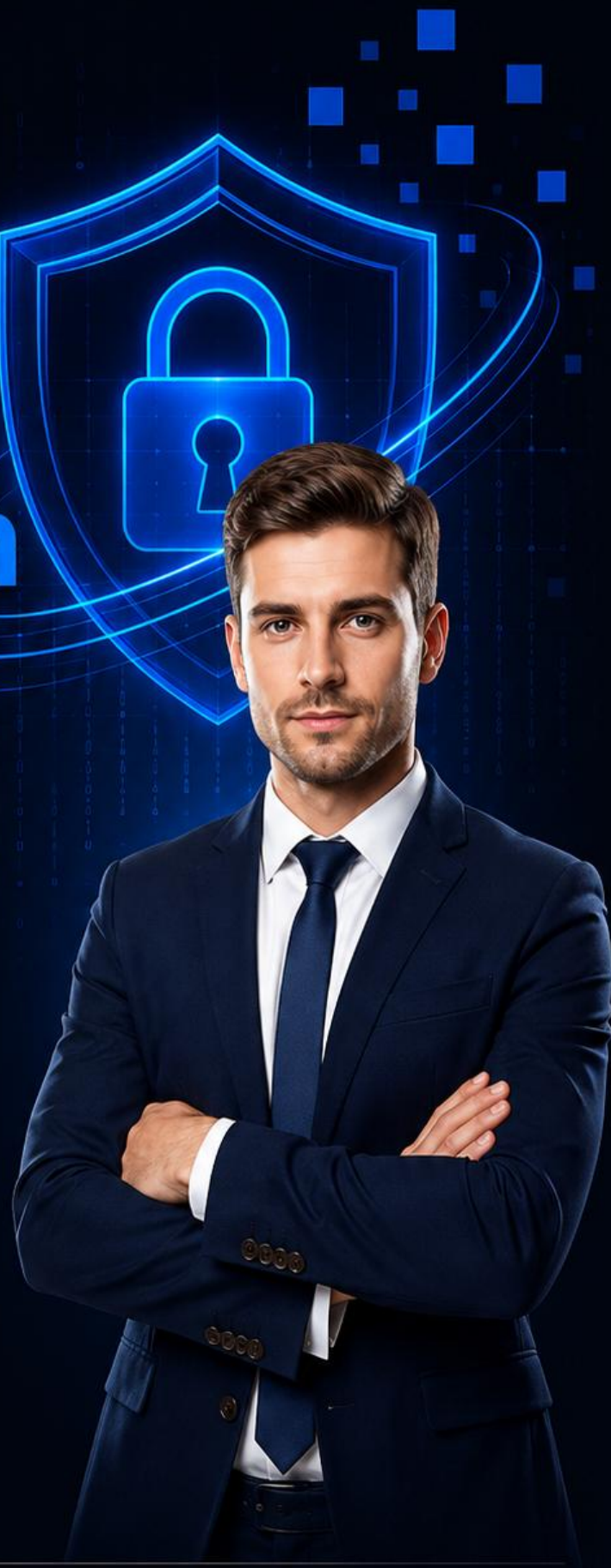
CyberHunt

ADVANCED PENETRATION TESTING

OSCP Preparation Program

Master real-world exploitation, privilege escalation, Active Directory compromise, and exam-level attack methodology. Built by practitioners. Proven by results.



- 100% Practical Training
- Exam-Oriented Methodology
- Manual Exploitation Focus
- Real-World Attack Simulation

5000+	95%	100+	24/7
Students Trained	Success Rate	Hiring Partners	Support

CyberHunt

Program Highlights

- 40-Hour Instructor-Led Training
- EC-Council Authorized Partner
- Practical Training on Latest Tools
- Telegram Group for Exam Support
- Learn from CEI Certified Trainers
- 98% Exam Pass Rate
- Post Training Support till Exam
- Access to Recorded Sessions
- Career Guidance & Mentorship

https://cyberhuntit.com/

CyberHunt

ABOUT COURSE

Offensive Security Certified Professional

The OSCP Preparation Program is an advanced, hands-on penetration testing training focused entirely on real-world exploitation skills. Unlike theory-heavy courses, every module is designed to mimic actual OSCP exam scenarios — ensuring you practice the exact way you will be tested.

This program prepares candidates for the OSCP exam while building strong practical penetration testing expertise required in enterprise environments. You will work through real machines, compromise real networks, and document your findings in a professional pentest report — all before exam day.

With a curriculum spanning web exploitation, buffer overflows, Active Directory attacks, and advanced pivoting, this is the most comprehensive OSCP prep available — covering every domain that Offensive Security tests.

OSCP Domain Coverage

Exploitation & Web Attacks	30%
Enumeration & Recon	25%
Privilege Escalation	25%
Active Directory Attacks	15%
Pivoting & Tunneling	5%

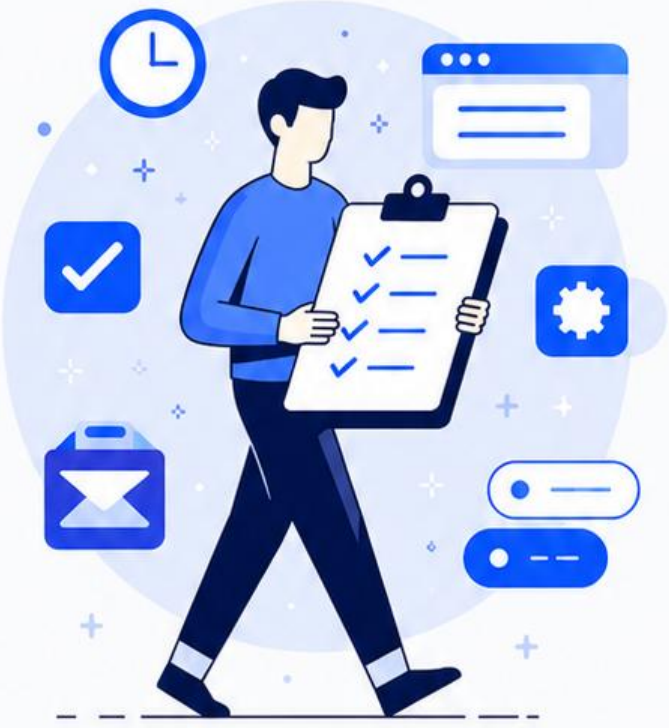
CyberHunt

Target Audience

- Security Analysts
- Ethical Hackers
- System Administrators
- Network Administrators
- Network and Security Engineers
- Cyber Security Managers
- Information Security Auditors
- Security Professionals

Pre-Requisites

- Basic understanding of network essentials and core concepts, including server and network components.



CyberHunt

Module-Wise Syllabus

Course Curriculum

Comprehensive OSCP-focused hands-on penetration testing training

01 Penetration Testing Methodology & Lab Setup

- OSCP Exam Structure & Strategy
- Kali Linux Advanced Usage
- VPN & Lab Environment Setup
- Enumeration-First Methodology
- Note-Taking & Documentation Strategy
- Tools Setup & Customization

Practical: Lab connectivity setup & methodology walkthrough.

02 Enumeration Mastery (Most Critical Phase)

- TCP/UDP Scanning Techniques
- Advanced Nmap Scanning
- Service Enumeration (SMB, FTP, HTTP, SSH, RDP)
- Web Enumeration & Directory Discovery
- Manual Enumeration Techniques
- Vulnerability Identification Without Automation

Practical: Multiple machines enumeration without hints.

03 Web Exploitation

- Manual SQL Injection & XSS
- File Upload Vulnerabilities
- Command Injection & LFI / RFI
- Authentication Bypass
- Web Shell Deployment
- Basic API Testing

Practical: Full compromise of web-based lab machines.

04 Buffer Overflow Exploitation

- Stack-Based Buffer Overflow Concepts
- Fuzzing Techniques & EIP Offset
- Bad Character Analysis
- Crafting Exploit with Python
- Generating Shellcode & Remote Shell

Practical: Complete manual buffer overflow exploitation.

05 Linux Privilege Escalation

- SUID Exploitation
- Misconfigured Cron Jobs & Writable Services
- Kernel Exploits & PATH Variable
- Capabilities Abuse
- Manual Enumeration Scripts

Practical: Root multiple Linux machines manually.

06 Windows Privilege Escalation

- Service Misconfigurations & Unquoted Paths
- DLL Hijacking & Token Impersonation
- Registry Exploitation
- Scheduled Task Abuse
- Manual Enumeration Techniques

Practical: Escalate to SYSTEM on Windows machines.

07 Active Directory Attacks

- AD Architecture & Kerberos Auth
- Kerberoasting & AS-REP Roasting
- Pass-the-Hash & Pass-the-Ticket
- NTLM Relay & Lateral Movement
- Domain Privilege Escalation

Practical: Full Active Directory Domain Compromise.

08 Pivoting & Tunneling

- Internal Network Enumeration
- SSH Tunneling & Port Forwarding
- ProxyChains & SOCKS Proxies
- Chisel Tunneling
- Accessing Internal Services

Practical: Multi-network pivoting lab scenario.

09 Password Attacks

- Online vs Offline Attacks
- Brute Force & Wordlist Attacks
- Hash Cracking Techniques
- Password Spraying
- Credential Reuse Attacks

10 Report Writing & Exam Strategy

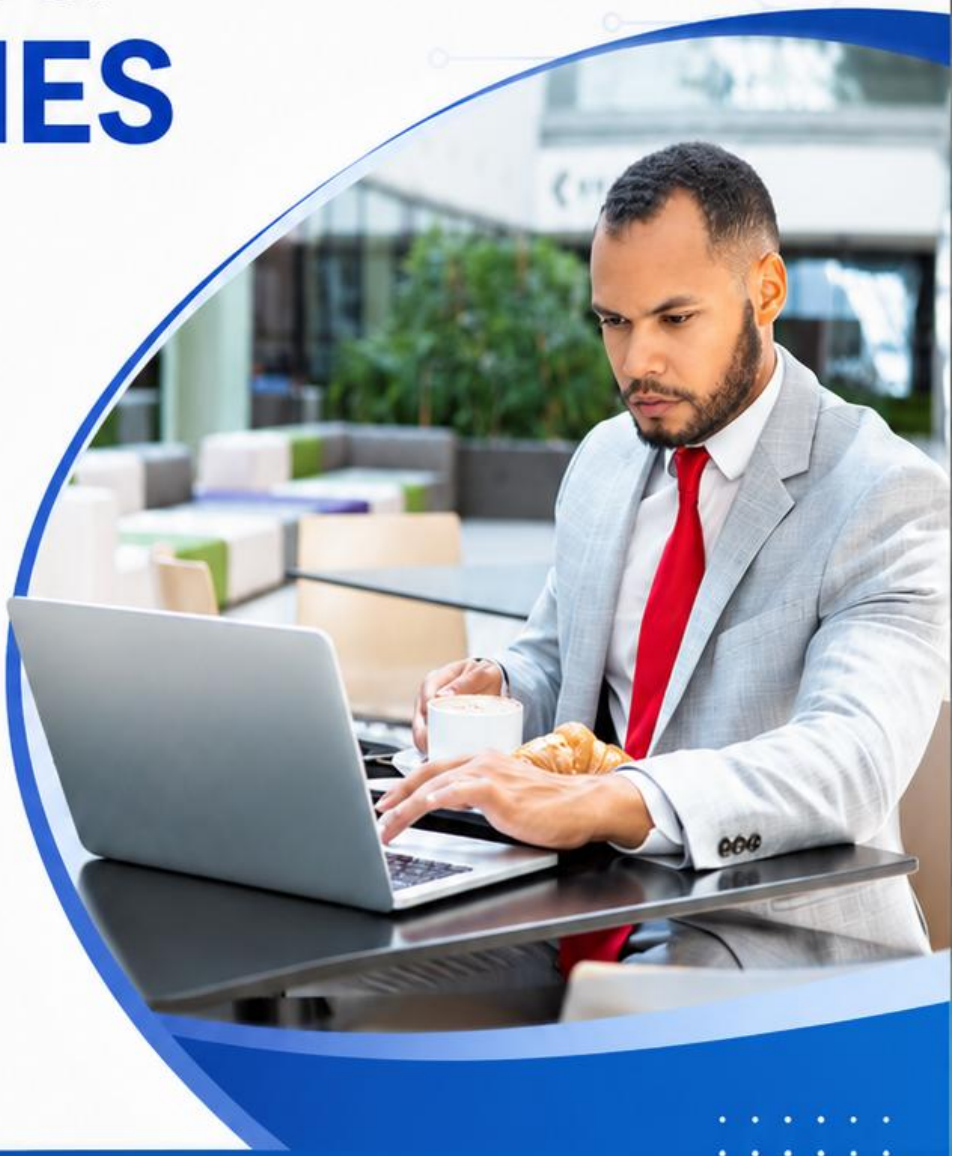
- OSCP Report Structure
- Writing Clear Proof of Concept
- Screenshot Documentation
- 24-Hour Exam Time Management
- Machine Prioritization & Attack Planning

Practical: Submit OSCP-style report for compromised machines.

CyberHunt

TRAINING ENQUIRIES

Have questions or need more information about our training programs? We're here to help!



For Training
+91 99599 06195
+91 93156 97737

Email
trainings@cyberhuntit.com

Website
www.cyberhuntit.com

Empowering Your Future
Industry-relevant training designed to upskill and empower you.

Follow us on