-------- Academy

Presents,

OSCP Online Course

Industry-Recognized | Expert-Led Training | Online Support

------- Academy

At ------- Academy, we provide world-class training to help professionals learn from **Offensive Security Certified Professional (OSCP) Course**, a globally recognized certified course for cybersecurity leadership roles.

Industry-Recognized Certifications: Globally accepted OSCP credential

Expert-Led Training: Learn from certified OSCP professionals

Hands-on Labs & Real-World Scenarios: Practical exposure to security management

Resume Building & Career Guidance: Helping you land top cybersecurity leadership roles

Flexible Learning Options: Live sessions, self-paced modules, and hands-on exercises

OSCP
(Offensive Security Certified Professional)

------ Academy’s OSCP course offers in-depth, hands-on training in ethical hacking and penetration testing techniques. Perfect for aspiring cybersecurity professionals aiming to validate their skills with one of the industry's most respected certifications.

Course Information

Course Duration : 12-16 Weeks (Flexible Based on Student Progress)

Mode : Theory + Hands-on Lab Exercises + Assignments

Course Outline - 1

Week 1: Introduction to Ethical Hacking & Penetration Testing

Lecture Topics:

- What is Ethical Hacking?
- Understanding Penetration Testing
- OSCP Certification Overview
- Legal & Ethical Considerations (Rules of Engagement, GDPR, Cyber Laws)
- Penetration Testing Methodologies (PTES, OSSTMM)

Practical Exercises:

- Setting up a Kali Linux Attack Machine
- Creating a Lab Environment with Virtual Machines (Windows & Linux)
- Understanding Offensive Security's PWK Labs

Assignments:

- Research and list five ethical hacking frameworks
- Install and configure VirtualBox/VMware with Kali Linux

Week 2: Information Gathering & Reconnaissance

Lecture Topics:

- Introduction to OSINT (Open-Source Intelligence)
- Active vs. Passive Reconnaissance
- WHOIS Lookup, Subdomain Enumeration
- DNS Reconnaissance & Zone Transfers
- Banner Grabbing & Service Enumeration

Practical Exercises:

- Using whois, nslookup, dig for domain reconnaissance
- Subdomain enumeration using Sublist3r & Amass
- Banner grabbing with Netcat, Telnet, Nmap

Assignments:

- Perform reconnaissance on a given domain
- Identify open ports and services using Nmap

Course Outline - 2

Week 3: Scanning & Enumeration

Lecture Topics:

- Network Scanning Techniques
- Service & Version Detection
- Identifying Open Ports & Running Services
- Web Application Enumeration
- SMB, SNMP & FTP Enumeration

Practical Exercises:

- Performing network scans using Nmap (SYN, UDP, Aggressive)
- Identifying services using Nmap scripting engine (NSE)
- Enumerating SMB & FTP shares

Assignments:

- Scan and enumerate a target machine
- Create a detailed scan report with identified vulnerabilities

Week 4: Vulnerability Assessment & Exploitation Basics

Lecture Topics:

- Understanding CVEs & CVSS Scores
- Using Exploit Databases (ExploitDB, Metasploit)
- Introduction to Exploiting Misconfigurations
- Manual vs. Automated Exploitation

Practical Exercises:

- Using searchsploit to find exploits
- Scanning for vulnerabilities with Nikto & OpenVAS
- Exploiting a simple web vulnerability (SQL Injection or LFI)

Assignments:

- Research recent CVEs and their impact
- Exploit a vulnerable web application using SQLi

Course Outline - 3

Week 5: Exploitation – Web Applications

Lecture Topics:

- Web Application Security Basics
- Exploiting SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Local File Inclusion (LFI) & Remote File Inclusion (RFI)

Practical Exercises:

- SQL Injection using sqlmap
- Exploiting XSS using BeeF
- Exploiting LFI/RFI vulnerabilities

Assignments:

- Perform SQLi on a test application
- Write a report on how XSS can be weaponized

Week 6: Exploitation – Network Services

Lecture Topics:

- Exploiting SMB, FTP, SSH
- Exploiting Misconfigured Network Services
- Brute Force Attacks & Weak Passwords

Practical Exercises:

- Exploiting SMB using EternalBlue (Metasploit)
- Brute forcing SSH passwords with Hydra
- Exploiting FTP misconfigurations

Assignments:

- Identify a network service vulnerability
- Exploit an SSH misconfiguration

Course Outline - 7

Final Week: OSCP Exam Preparation & Report Writing

Lecture Topics:

- Time Management for OSCP Exam
- How to Approach the 24-Hour Exam
- Report Writing Guidelines

Practical Exercises:

- Simulating an OSCP-style exam
- Writing a professional penetration testing report

Key Learning Outcomes

- Penetration Testing – Follow structured methods to exploit systems.
- Recon & Scanning – Identify weaknesses through active discovery.
- Exploitation – Exploit real-world Windows and Linux flaws.
- Privilege Escalation – Gain higher access on compromised systems.
- Post-Exploitation – Extract data and hide activities.
- Buffer Overflows – Understand basic exploit development.
- Reporting – Document and present key findings.
- Time Management – Work efficiently under exam pressure.

Skills Covered

- Network service vulnerability exploitation
- Custom buffer overflow development
- Web application attack techniques
- Linux privilege escalation methods
- Windows Active Directory exploitation
- Post-exploitation persistence and cleanup

Training Features

- Network service vulnerability exploitation
- Custom buffer overflow development
- Web application attack techniques
- Linux privilege escalation methods
- Windows Active Directory exploitation
- Post-exploitation persistence and cleanup

Who should enroll?

- **Cybersecurity professionals looking to advance into security leadership**
- **IT security managers, risk analysts, and network security engineers**
- **IT professionals preparing to learn about offensive security.**

Pre-Requisites for course

- At least five years of experience in cybersecurity (or four years with a degree)
- Knowledge of security principles, networking, and risk management

Career Opportunities

- Chief Information Security Officer (CISO)
- Security Architect
- IT Risk Manager
- Security Consultant

Join ------- Academy Today!

Take the first step toward becoming a certified cybersecurity professional.

Email: info@-------academy.com

Phone: +91-----274739

Website: www.-------academy.com

Disclaimer: ------ Academy provides training programs to help students prepare for industry-recognized certification exams. We are not an official training partner of CompTIA, (ISC)², EC-Council, or any other certification body. All certification names, logos, and trademarks belong to their respective owners. Certification exams must be taken through the official certification provider.