OSCP (PEN-200) Offensive Security Certified Professional

Become a hands-on penetration tester who can compromise real networks and prove it under exam conditions.

Duration: 4 months | Prepares for: OffSec OSCP (PEN-200) | Format: Online or onsite, 1-on-1 or batch | Target exam: OSCP+ (PEN-200) | NUEXUS certificate on completion

OVERVIEW

This is an intensive, lab-heavy program built around OffSec's PEN-200 syllabus, the course behind the industry-respected OSCP certification. You learn offensive security the way it is actually practiced: enumerate a target, find a foothold, escalate privileges, and pivot deeper into a network, all in a live lab rather than through slides. Over roughly four months of mentor-led, hands-on sessions you build the manual tradecraft and the disciplined "try harder" methodology that OSCP is known for, and you finish exam-ready for the 24-hour practical assessment. It is delivered online from anywhere or onsite in Islamabad, in a batch or 1-on-1 format.

SKILLS YOU WILL GAIN

Information Gathering | Vulnerability Scanning | Web Application Attacks | SQL Injection | Client-Side Attacks | Locating & Fixing Public Exploits | Antivirus Evasion | Password Attacks | Windows Privilege Escalation | Linux Privilege Escalation | Port Redirection & SSH Tunneling | The Metasploit Framework | Active Directory Attacks | Lateral Movement | Report Writing

WHAT YOU WILL BE ABLE TO DO

- Run structured enumeration and reconnaissance against hosts, services, and web applications
- Find and exploit common vulnerabilities to gain an initial foothold, including web, service, and client-side attacks
- Perform privilege escalation on both Linux and Windows targets using manual techniques
- Pivot and move laterally through segmented networks, including exposure to Active Directory attack paths
- Adapt, fix, and use public exploits responsibly, and build simple tooling in Bash and Python
- Document your work in a clear, professional penetration test report as required by the OSCP exam

WHO IT IS FOR

- Aspiring penetration testers and red teamers who want a rigorous, practical entry into offensive security
- IT, network, or system administrators moving into a security or ethical hacking role
- SOC analysts and blue teamers who want to understand attacks from the attacker's side
- Security enthusiasts and CTF players ready to formalise their skills toward the OSCP
- Graduates and career changers targeting a recognised, hands-on offensive security credential

PREREQUISITES

- Solid comfort with the Linux command line and general networking (TCP/IP, ports, services, DNS)
- Basic scripting familiarity, for example Bash and a little Python, is strongly recommended
- A machine able to run Kali Linux (natively or in a VM) with a stable internet connection
- Persistence and self-discipline, since OSCP rewards methodical, independent problem solving

WHAT'S INCLUDED

- Mentor-led live sessions, online or onsite, in batch or 1-on-1
- Hands-on labs and real-world projects, not slides alone
- Recordings of your own sessions to revisit anytime
- Exam-aligned study material and practice questions
- Doubt-clearing and revision support through the program
- A verifiable NUEXUS completion certificate
- Career and next-step guidance after you finish

COURSE CURRICULUM

1 Penetration Testing Foundations and Methodology

- The penetration testing lifecycle and the OffSec approach
- Setting up and working effectively in Kali Linux
- Report-taking, note discipline, and organising findings
- Legal, ethical, and scoping fundamentals for engagements

2 Information Gathering and Enumeration

- Passive and active reconnaissance techniques
- Port scanning and service enumeration with Nmap
- Enumerating SMB, SMTP, SNMP, DNS, and other network services
- Building a target map and identifying attack surface

3 Vulnerability Scanning and Web Application Attacks

- Using and interpreting vulnerability scanners
- Cross-site scripting (XSS) and directory traversal
- SQL injection and command injection
- File inclusion and file upload vulnerabilities

4 Exploitation Fundamentals and Public Exploits

- Finding, reviewing, and adapting public exploits
- Fixing and compiling exploit code safely in the lab
- Introduction to buffer overflow concepts and memory corruption
- Using and understanding common Metasploit workflows

5 Client-Side and Password Attacks

- Client-side attack techniques and payload delivery
- Password cracking with tools such as Hashcat and John the Ripper
- Attacking network service authentication
- Working with credentials, hashes, and pass-the-hash concepts

6 Privilege Escalation: Linux and Windows

- Linux privilege escalation enumeration and techniques
- Windows privilege escalation enumeration and techniques
- Abusing misconfigurations, permissions, and scheduled tasks
- Kernel, service, and credential-based escalation paths

7 Tunnelling, Pivoting, and Port Redirection

- Port forwarding and redirection techniques
- SSH and tool-based tunnelling
- Pivoting through compromised hosts into internal networks
- Navigating segmented and firewalled environments

8 Active Directory Attacks

- Active Directory enumeration and mapping
- Attacking AD authentication and harvesting credentials
- Lateral movement across domain hosts
- Understanding common AD attack paths to domain compromise

9 The Complete Kill Chain and Exam Preparation

- Chaining enumeration, exploitation, and escalation end to end
- Working through practice machines and challenge labs
- Time management and methodology for the 24-hour exam
- Writing a professional penetration test report to OffSec standards

CAREER OUTCOMES

Penetration Tester · Red Team Operator · Offensive Security Engineer · Security Consultant · Exploit Developer

Entry	USD 60,000 to 90,000
Mid	USD 90,000 to 130,000
Senior	USD 130,000 to 170,000

Global averages from Glassdoor and PayScale, 2025. Actual pay varies by country, employer and experience.

CERTIFICATION PATH

NUEXUS training certificate

Issued by NUEXUS on course completion. Verifiable at nuexus.com/verify.

OffSec OSCP (PEN-200)

Earned by passing the official exam. Issued and verified by the certification body itself, not by NUEXUS.

Exam	OSCP+ (PEN-200)
Questions	3 standalone machines (60 points) plus a 3-machine Active Directory set (40 points)
Format	Fully hands-on, live-proctored exam plus a professional penetration-test report
Duration	23 hours 45 minutes of exam time, then 24 hours to submit the report
Passing score	70 out of 100 points (bonus points were removed in November 2024)
Delivery	OffSec proctored exam over a private VPN

An exam attempt comes with the official OffSec course and lab bundle, purchased separately from OffSec. Passing now earns the OSCP+ designation, which is valid for three years; the underlying OSCP does not expire. Even when NUEXUS arranges your exam voucher, the resulting certification is issued and verified by the certification body directly.