PEN-200

OSCP+

Penetration Testing with Kali Linux

The Penetration Testing with Kali Linux (PEN-200) course is OffSec's essential training program for aspiring penetration testers. The course teaches learners how to identify and exploit real-world vulnerabilities across computers, networks, web applications, and basic cloud environments. Emphasizing hands-on, practical learning, PEN-200 provides the core technical skills and mindset required to simulate offensive security operations— and defend against them.

Introduction to CyberSecurity	Master the core concepts, technologies, and best practices that form the bedrock of cybersecurity, providing a solid foundation for your pen testing journey
Report Writing for Penetration Testers	Craft clear, actionable reports to detail security vulnerabilities, their potential impact, and step-by-step remediation guidance
Information Gathering	Use advanced ethical hacking techniques and tools like Nmap and Shodan to map target systems and discover exploitable vulnerabilities
Vulnerability Scanning	Use tools like Nessus and OpenVAS to identify known vulnerabilities in networks, applications, and systems to streamline your penetration testing process
Introduction to Web Applications	Learn how web applications function, what their underlying technologies are, and the architectural weaknesses that create common attack vectors
Common Web Application Attacks	Explore the techniques behind common web attacks, injection flaws, session hijacking, and the essential strategies to stop them
SQL Injection Attacks	Master the art of manipulating databases through SQL injections to extract sensitive information, compromise backend systems, and escalate your privileges
Client-Side Attacks	Exploit vulnerabilities in web browsers, browser extensions, and client-side technologies to compromise user systems and gain access
Locating Public Exploits	Find reliable public exploits, assess their significance, and responsibly integrate them into your security testing workflow
Fixing Exploits	Adapt and customize existing exploits, employ obfuscation techniques, and develop creative payloads to bypass defenses and successfully test target systems
Antivirus Evasion	Develop strategies and techniques to disguise exploits, obfuscate payloads, and evade detection by antivirus solutions to simulate real-world attacker behavior
Password Attacks	Uncover weak authentication practices using password cracking techniques like brute-force, dictionary attacks, and rainbow table methods to improve password security

Windows Privilege Escalation	Identify and exploit misconfigurations and vulnerabilities in Windows systems to gain admin-level access and more control within a network
Linux Privilege Escalation	Escalate your privileges and gain root-level access to fully compromised servers and critical infrastructure on Linux systems
Advanced Tunneling	Establish covert channels, pivot through networks, evade detection, and maintain persistence during penetration tests with sophisticated tunneling protocols and techniques
The Metasploit Framework	Use Metasploit's broad capabilities for exploit development, payload generations, and post-exploitation activities to streamline your penetration testing tasks
Active Directory: Introduction and Enumeration	Understand the structure of Active Directory, learn to enumerate users, groups, trusts, and sensitive configurations using tools like BloodHound and PowerView to identify attack paths
Attacking Active Directory Authentication	Exploit weaknesses in Active Directory authentication mechanisms (Kerberos, NTLM, etc) to compromise credentials and gain unauthorized access
Lateral Movement in Active Directory	Move laterally in Active Directory environments, expand your control, and achieve your penetration testing objectives with post-exploitation techniques and tools