Training: OffSec
OffSec PEN-200 Penetration Testing with Kali Linux

OffSec | Learning Partner

TRAINING GOALS:



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, network security, web applications, and basic cloud environments. Emphasizing hands-on, practical learning, PEN-200 provides the core technical skills and mindset required to simulate offensive information security operations—and defend against them. It's a critical resource for those pursuing roles such as security analyst, security specialist, or certified ethical hacker.

PEN-200 covers a wide range of topics and attack techniques, including:

- Providing an introduction to cybersecurity and an effective learning strategy to help you get started
- Performing enumeration and information gathering, including vulnerability scanning
- Understanding encryption and cryptography
- Utilizing perimeter attacks in web security and client-side attacks, where we go into depth in the commonly seen vulnerabilities such as XSS, Command Injection, Directory Traversal, File Uploads, and SQL Injection. We also cover password attacks and touch on Anti-Virus Evasion
- Performing Windows and Linux privilege escalation and lateral movements, including pivoting and tunneling techniques
- Using Active Directory, attacking Active Directory authentication, and lateral movement in Active Directory
- Enumerating and attacking AWS cloud infrastructure
- Learning how to use commonly used tools and commands in penetration testing, such as Nmap,

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Metasploit, Burp Suite, Hydra, Nessus, sqlmap, and Shellter

PEN-200 is organized into 20+ modules. Most modules have companion videos for the visually inclined learners. Most modules have hands-on labs to help learners practice the concept and theory taught in that module. After mastering each of the techniques and skills taught in all modules, learners can move on to the 9 challenge labs to practice a combination of skills in one lab, mimicking the real-world penetration test engagement. To help learners get ready for their OSCP+ exam, three challenge labs are designed to closely replicate the OSCP+ exam environment.

Each participant in an authorized OffSec PEN-200 training held at Compendium CE receives a Learn One" license, which includes, among other benefits, a free OSCP+ exam voucher.

PEN-200 is suitable for those wishing to embark on a professional pen testing career, or wanting to learn skills possessed by pen testers. Before taking this course, we do suggest having hands-on practical knowledge of Linux and Windows administration, networking, and network scripting.

Objectives

After completing this course, learners will be able to:

- Master information gathering and enumeration techniques
- Conduct vulnerability scanning with Nessus and Nmap
- Perform web application and client-side attacks
- Execute Windows and Linux privilege escalation techniques
- Implement port redirection and SSH tunneling
- Analyze and attack Active Directory environments
- Utilize public exploit resources and adapt them for specific scenarios
- Evade antivirus detection
- Generate and debug shellcode for penetration testing
- Write detailed and effective penetration testing reports

Who is this course for?

- Infosec professionals transitioning into penetration testing
- Pentesters seeking one of the best pentesting certifications
- Those interested in pursuing a penetration tester career path
- Security professionals

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- Network administrators
- Other technology professionals

CONSPECT:

- Introduction to Cybersecurity
  - Master the core concepts, technologies, and best practices that form the bedrock of information security, 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 web security 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

- 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 security framework
- 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

REQUIREMENTS:

Penetration Testing with Kali Linux is a foundational course but still requires learners to have certain knowledge before attending the online class. A solid understanding of TCP/IP, networking, and reasonable Linux skills are required. Familiarity with Bash scripting along with basic Perl or Python is considered a plus.

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Compendium CE (course completion).

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

The PEN-200 course and online lab prepares you for the OSCP+ penetration testing certification. Learn more about the OSCP+ exam https://help.offsec.com/hc/en-us/articles/360040165632-OSCP-Exam-Guide

Each participant in an authorized OffSec PEN-200 training held at Compendium CE receives a Learn One" license, which includes, among other benefits, a free OSCP+ exam voucher.

TRAINER:

Authorized OffSec Trainer

ADDITIONAL INFORMATION:

The course includes a license "Learn One"

The license includes:

- One 200 or 300-level course
- 365 days of access
- 2 exam attempts
- Bonus KLCP and OSWP courses + exams
- 200+ Proving Grounds Practice labs

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007