PEN-200 - PENETRATION TESTING WITH KALI LINUX (PWK/OSCP)

Course Code: 840104

OffSec PEN-200 – Penetration Testing with Kali Linux

The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) 5 days course introduces penetration testing methodology, tools, and techniques in a hands-on, self-paced environment. Access PEN-200's first Learning Module for an overview of course structure, learning approach, and what the course covers.

Learners who complete the course and pass the exam after November 1, 2024 will earn the OffSec Certified Professional (OSCP & OSCP+) penetration testing certification which requires holders to successfully attack and penetrate various live machines in a safe lab environment. These certifications are considered to be more technical than other penetration testing certifications and is one of the few that requires evidence of practical pen testing skills. The OSCP is a lifetime certification and the OSCP+ expires after 3 years, representing learners' commitment to continuing education in the complex cybersecurity space.

What You'll Learn

Upon completing PEN-200 and successfully passing the OSCP exam, you'll have mastered core penetration testing methodologies, including:

- Information gathering and vulnerability scanning
- Exploit development and execution
- Privilege escalation (Windows and Linux)
- Web application attacks
- Active Directory exploitation

Who Needs to Attend

The PEN-200 course is ideal for security professionals seeking to enhance their ethical hacking skills and earn the industry-recognized OSCP pen testing certification. It's designed for individuals who have a solid foundation in networking and basic familiarity with Linux and Windows systems.

Prerequisites

While there are no formal prerequisites, it's strongly recommended that you have:

- A solid foundation in TCP/IP networking
- Basic scripting abilities (e.g., Bash, Python)
- Familiarity with Linux and Windows operating systems

Learners can also go through the OffSec Network Penetration Testing Essentials Learning Path to ensure they're ready for the course, included in Learn Fundamentals and Learn One subscription.

PEN-200 - PENETRATION TESTING WITH KALI LINUX (PWK/OSCP)

Course Code: 840104

VIRTUAL CLASSROOM LIVE	$8,845 CAD	5 Day

Virtual Classroom Live Outline

Penetration Testing with Kali Linux: General Course Introduction

- Welcome to PWK
- How to Approach the Course
- Summary of PWK Learning Modules

Introduction to Cybersecurity

- The Practice of Cybersecurity
- Threats and ThreatActors
- The CIA Triad
- Security Principles, Controls, and Strategies
- Cybersecurity Laws, Regulations, Standards, and Frameworks
- Career Opportunities in Cybersecurity

Effective Learning Strategies

- Learning Theory
- Unique Challenges to Learning Technical Skills
- OffSec Methodology
- Case Study: chmod -x chmod
- Tactics and Common Methods
- Advice and Suggestions on Exams
- Practical Steps

Report Writing for Penetration Testers

- Understanding Notetaking
- Writing Effective Technical Penetration Testing Reports

Information Gathering

- The Penetration Testing Lifecycle

- Passive Information Gathering
- Active Information Gathering

Vulnerability Scanning

- Vulnerability Scanning Theory
- Vulnerability Scanning with Nessus
- Vulnerability Scanning with Nmap

Introduction to Web Applications

- Web Application Assessment Methodology
- Web Application Assessment Tools
- Web Application Enumeration
- Cross-Site Scripting (XSS)

Common Web Application Attacks

- Directory Traversal
- File Inclusion Vulnerabilities
- File Upload Vulnerabilities
- Command Injection

SQL Injection Attacks

- SQL Theory and Database Types
- Manual SQL Exploitation
- Manual and Automated Code Execution

Client-Side Attacks

- Target Reconnaissance
- Exploiting Microsoft Office
- Abusing Windows Library Files

Locating Public Exploits

- Getting Started
- Online Exploit Resources
- Offline Exploit Resources
- Exploiting a Target

Fixing Exploits

- Fixing Memory Corruption Exploits
- Fixing Web Exploits

Antivirus Evasion

- Antivirus Evasion Software Key Components and Operations
- AV Evasion in Practice

Password Attacks

- Attacking Network Service Logins
- Password Cracking Fundamentals
- Working with Password Hashes

Windows Privilege Escalation

- Enumerating Windows
- Leveraging Windows Services
- Abusing other Windows Components

Linux Privilege Escalation

- Enumerating Linux
- Exposed Confidential Information
- Insecure File Permissions
- Insecure System Components

Port Redirections and SSH Tunneling

- Port Forwarding with *NIX Tools
- SSH Tunneling
- Port Forwarding with Windows Tools

Advanced Tunneling

- Tunneling Through Deep Packet Inspection

The Metasploit Framework

- Getting Familiar with Metasploit
- Using Metasploit Payloads
- Performing Post-Exploitation with Metasploit
- Automating Metasploit

Active Directory Introduction and Enumeration

- Active Directory Manual Enumeration
- Manual Enumeration Expanding our Repertoire
- Active Directory Automated Enumeration

Attacking Active Directory Authentication

- Performing Attacks on Active Directory Authentication
- Lateral Movement in Active Directory
- Active Directory Lateral Movement Techniques
- Active Directory Persistence

Assembling the Pieces

- Enumerating the Public Network
- Attacking WEBSRV1
- Gaining Access to the Internal Network
- Enumerating the Internal Network
- Attacking the Web Application on INTERNALSRV1
- Gaining Access to the Domain Controller

Virtual Classroom Live Labs

The Labs

- PWK Challenge Lab Overview
- Challenge Lab Details

- The OSCP -OSCP+ Exam Information

PEN-200 - PENETRATION TESTING WITH KALI LINUX (PWK/OSCP)

Course Code: 840104

PRIVATE GROUP TRAINING	5 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/18/2025 6:21:53 AM