PEN-200 - Penetration Testing with Kali Linux (PWK/OSCP)

Durée: 5 Jours **Réf de cours: GK840104** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) 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.
Upd April 2025

Public visé:

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. Its designed for individuals who have a solid foundation in networking and basic familiarity with Linux and Windows systems.

Objectifs pédagogiques:

- Upon completing PEN-200 and successfully passing the OSCP exam, youll 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

Pré-requis:

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.

Self-Directed Training Overview

The Pre-Course work provides students with the knowledge required to develop skills, abilities, and attitudes required to master the penetration testing techniques demonstrated during the ILT. Students will complete assignments inside the OffSec and partner vendor portals. Additionally, students will be provided videos to review and be expected to practice penetration test skill development tasks.

Test et certification

Contenu:

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

Trying Harder: The Labs

- PWK Challenge Lab Overview
- Challenge Lab Details
- The OSCP Exam Information

Méthodes pédagogiques :

Official course book provided to participants. Course materials in english

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement