PEN-200: Penetration Testing with Kali Linux

Duration: 90 Days

Course Description:

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 will earn the OffSec Certified Professional (OSCP) penetration testing certification which requires holders to successfully attack and penetrate various live machines in a safe lab environment. The OSCP is considered to be more technical than other penetration testing certifications and is one of the few that requires evidence of practical pen testing skills.

Course Outlines:

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

- Learn to craft clear, actionable reports that detail security vulnerabilities, and potential impact, and provide step-by-step remediation guidance to help clients strengthen their security.

Information Gathering

- Employ advanced ethical hacking techniques and tools like Nmap and Shodan to meticulously map target systems, uncover potential entry points, and discover exploitable vulnerabilities.

Vulnerability Scanning

- Utilize powerful tools like Nessus and OpenVAS to systematically identify known vulnerabilities in networks, applications, and systems, streamlining your penetration testing process.

Introduction to Web Applications

- Gain a deep understanding of how web applications function, their underlying technologies, and the architectural weaknesses that give rise to common attack vectors.

Common Web Application Attacks

- Explore the techniques behind prevalent web attacks like cross-site scripting (XSS), injection flaws, and session hijacking, and learn essential mitigation strategies.

SQL Injection Attacks

- Master the art of manipulating databases via SQL injections to extract sensitive information, compromise backend systems, and escalate your privileges.

Client-Side Attacks

- Discover how to exploit vulnerabilities in web browsers, browser extensions, and client-side technologies like JavaScript to compromise user systems and gain unauthorized access.

Locating Public Exploits

- Learn where to find reliable public exploits, how to assess their applicability, and how to integrate them responsibly 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.