OffSec™
Partner Program

90-day Course and Certification Exam Bundle

The bundle includes 90-day access to any course listed here, a single exam attempt, and a certification badge awarded upon passing your exam.

PEN-200: Penetration Testing with Kali Linux

PEN-200 is a unique online penetration testing course that introduces learners to the latest pentesting methodologies, tools, and techniques via hands-on experience. It simulates a full penetration test by immersing the learners into a target-rich and vulnerable network environment. Learners who complete the PEN-200 course and the associated exam earn the Offensive Security Certified Professional (OSCP) certification.

PEN-300: Advanced Evasion Techniques and Breaching Defenses

PEN-300 builds on the knowledge and techniques taught in PEN-200, teaching learners to perform advanced penetration tests against mature organizations with an established security function and bypassing security mechanisms that are designed to block attacks. Learners who complete the course and pass the exam earn the Offensive Security Experienced Penetration Tester (OSEP) certification.

SOC-200: Foundational Security Operations and Defensive Analysis

SOC-200 is a course designed for job roles such as Security Operations Center (SOC) Analysts and Threat Hunters. Students gain hands-on experience with a SIEM, identifying and assessing a variety of live, end-to-end attacks against a number of different network architectures. Students who complete the course and pass the exam earn the Offensive Security Defence Analyst (OSDA) certification.

WEB-200: Foundational Web Application Assessments with Kali Linux

WEB-200 is our foundational web application security course that teaches learners how to discover and exploit common web vulnerabilities and how to exfiltrate sensitive data from target web applications. Learners who complete the course and pass the associated exam earn the Offensive Security Web Assessor (OSWA) certification, demonstrating their ability to leverage modern web exploitation techniques on modern applications.

WEB-300: Advanced Web Attacks and Exploitation

WEB-300 is a challenging course that will develop your team's skills in a white-box environment, performing deep analysis on decompiled web app source code, identifying and combining logical vulnerabilities to create a proof of concept on a web app, and exploiting vulnerabilities by chaining them into complex attacks. Learners who complete the course and pass the exam earn the Offensive Security Web Expert (OSWE) certification.

EXP-301: Windows User Mode Exploit Development

EXP-301 is an advanced course that introduces learners to modern 32-bit exploit development and reverse engineering techniques. Learners will obtain skills necessary to bypass DEP and ASLR security mitigations, create advanced custom ROP chains, write handmade Windows shellcode, and create read and write primitives by exploiting format string specifiers. Learners who complete the course and pass the exam earn the Offensive Security Exploit Developer (OSED) certification.

EXP-312 – Advanced macOS Control Bypasses

EXP-312 is OffSec's macOS security course, which aims to prepare learners for penetration testing, discovering and exploiting vulnerabilities in macOS environments. It's an offensive course, focusing on platform-independent logic vulnerabilities, privilege escalation, and bypassing the operating system's defenses. Learners who complete EXP-312 and pass the associated exam will earn the Offensive Security macOS Researcher (OSMR) certification.