

OSCP / OSEP / OSDA Course & Certification Bundle by Offensive Security

90 days

Intermediate

90 days of course and lab access plus one exam attempt for one of the following advanced cybersecurity courses: PEN-200, PEN-300, SOC-200, WEB-200, WEB-300, EXP-301, EXP-312 + access to all Learn Fundamentals courses.

Platform Description:

OffSec's Learning Library offers courses and labs that enable students and professionals the ability to develop the try harder mindset and skills for a variety of cybersecurity and IT job roles.

Platform Features and Benefits:

90 Days of access to one of the following courses + 1 Exam Attempt + 90 Days Access to Course Labs for following courses:

- **PEN-200 (OSCP):** The industry-leading Penetration Testing with Kali Linux (PWK/PEN-200) course introduces penetration testing methodologies, tools and techniques via hands-on experience and is self-paced.
- **PEN-300 (OSEP):** This course builds on the knowledge and techniques taught in Penetration Testing with Kali Linux, teaching students to perform advanced penetration tests against mature organizations with an established security function and focuses on bypassing security mechanisms that are designed to block attacks.

- **SOC-200 (OSDA):** Learn the foundations of cybersecurity defense with Security Operations and Defensive Analysis (SOC-200), a course designed for job roles such as Security Operations Center (SOC) Analysts and Threat Hunters. Learners 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.
- **WEB-200 (OSWA):** This course teaches learners how to discover and exploit common web vulnerabilities and how to exfiltrate sensitive data from target web applications. Students that complete the course will obtain a wide variety of skill sets and competencies for web app assessments.
- **WEB-300 (OSWE):** Advanced Web Attacks and exploitation (WEB-300) is an advanced web application security course that teaches the skills needed to conduct white box web app penetration tests.
- **EXP-301 (OSED):** Windows User Mode Exploit Development (EXP-301) is beginner level course that teaches students the basics of modern exploit development. Despite being a fundamental course, it is at the 300 level because it relies on substantial knowledge of assembly and low level programming. It begins with basic buffer overflow attacks and builds into learning the skills needed to crack the critical security mitigations protecting enterprises.
- **EXP-312 (OSMR):** macOS Control Bypasses (EXP-312) is our first macOS security course. It's an offensive logical exploit development course for macOS, focusing on local privilege escalation and bypassing the operating system's defenses. EXP-312 is an advanced course that teaches the skills necessary to bypass security controls implemented by macOS, and exploit logic vulnerabilities to perform privilege escalation on macOS systems.

Who it's for:

With 90 days of access to OffSec lab course-specific lab environments and a chance to prove their mastery through, the OffSec Course and Cert Exam bundle is the ideal choice for any cybersecurity practitioner looking to fast track and showcase their cybersecurity knowledge.