OFFENSIVE SECURITY OSCP CERTIFICATION

PEN-200 Penetration Testing with Kali Linux

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

Additional Formats:

- Live in Person Training
(Inquire for pricing and booking)
- OffSec Academy
Virtual Instructor lead training

OFFENSIVE® security

Course Estimated time: 185 hours*

PEN-200, Penetration Testing with Kali Linux, is a unique penetration course course that combines traditional course materials with hands-on simulations, using a virtual lab environment. View the full syllabus for more details.

Topics Covered:

- Penetration Testing: What You Should Know
- Getting Comfortable with Kali Linux
- Command Line Fun
- Practical Tools
- Bash Scripting
- Passive Information Gathering
- Active Information Gathering
- Vulnerability Scanning
- Web Application Attacks
- Introduction to Buffer Overflows
- Windows Buffer Overflows
- Linux Buffer Overflows
- Client-Side Attacks
- Locating Public Exports
- Fixing Exploits
- File Transfers
- Antivirus Evasion
- Privilege Escalation
- Password Attacks
- Port Redirection and Tunneling
- Active Directory Attacks
- The Metasploit Framework
- PowerShell Empire
- Assembling The Pieces: Penetration Test Breakdown
- Trying Harder: The Lab

Course Prerequisites:

All students are required to have:

- Solid understanding of TCP/IP networking
- Reasonable Windows and Linux administration experience
- Familiarity of Bash scripting with basic Python or Pearl a plus

Competencies Gained:

- Using information gathering techniques to identify and enumerate targets running various operating systems.
- Writing basic scripts and tools to aid in the penetration testing process
- Analyzing, correcting, modifying, cross-compiling and porting public exploit code
- Conducting remote, local privilege escalation and client-side attacks
- Identifying and exploiting XSS, SQL injection and file inclusion vulnerabilities in web applications
- Leveraging tunneling techniques to pivot between networks
- Creative problem solving and lateral thinking skills

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

PEN-210 Offensive Security Wireless Attacks

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

Course Estimated time: 100 hours*

Like other Offensive Security courses, WiFu combines traditional course materials with hands-on practice within a virtual lab environment. The course covers the topics listed below in detail. Course topics can also be found in the syllabus.

Topics Covered:

- IEEE 802.11
- Wireless Networks
- Packets and Network Interaction
- Linux Wireless Stack and Drivers
- Aircrack-ng Essentials
- Cracking WEP and Connected Clients
- Cracking WEP via a Client
- Cracking Clientless WEP Networks
- Bypassing WEP Shared Key Authentication
- Cracking WPA/WPA2 PSK with Aircrack-ng
- Cracking WPA with JTR and Aircrack-ng
- Cracking WPA with coWPAtty
- Cracking WPA with Pyritt
- Additional Aircrack-ng Tools
- Wireless Reconnaissance Tools
- Understanding of how to implement different rouge access point attacks
- Familiarity with the BackTrack wireless tools

Course Prerequisites:

All students must have:

- Solid understanding of TCP/IP and the OSI model as well as familiarity with Linux.
- A modern laptop or desktop that can boot and run BackTrack
- Specific Hardware is required to complete course exercises

Recommended Wireless Network Routers

- D-Link DIR-601
- Netgear WNR1000v2

Recommended Wireless Cards

- Netgear WN111v2 USB
- ALFA Networks AWUD036H USB 500mW

Competencies Gained:

- Greater insight into wireless offensive security and expanded awareness of the need for real-world security solutions
- Implementing attacks against WEP and WPA encrypted network

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

PEN-300 Evasion Techniques and Breaching Defenses

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

Course Estimated time: 300 hours*

PEN-300, Evasion Techniques and Breaching Defenses, is an advanced course designed for OSCP-level penetration testers who want to develop their skills against hardened systems. Topics are covered below, or in the course syllabus.

Topics Covered:

- Operating System and Programming Theory
- Client Side Code Execution with Office
- Client Side Code Execution with Jscript
- Process Injection and Migration
- Introduction to Antivirus Evasion
- Advanced Antivirus Evasion
- Application Whitelisting
- Bypassing Network Filters
- Linux Post-Exploitation
- Kiosk Breakouts
- Windows Credentials
- Windows Lateral Movement
- Linux Lateral Movement
- Microsoft SQL Attacks
- Active Directory Exploitation
- Combining the Pieces
- Trying Harder: The Labs

Course Prerequisites:

We strongly suggest that students taking PEN-300 have either taken PWK and passed the OSCP certification or have equivalent knowledge and skills in the following areas:

- Working familiarity with Kali Linux command line
- Solid ability run enumerating targets to identify vulnerabilities
- Basic scripting abilities in Bash, Python and PowerShell
- Identifying and exploiting vulnerabilities like SQL injection, file inclusion and local privilege escalation
- Foundational understanding of Active Directory and knowledge of basic AD attacks
- Familiarity with C# programming is a plus

Competencies Gained:

- Preparation for more advanced field work
- Knowledge of breaching network perimeter defenses through clientside attacks, evading antivirus and allow listing technologies
- How to customize advanced attacks and chain them together web vulnerabilities

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

Course Estimated time:
150 hours*

OFFENSIVE SECURITY
OSWA CERTIFICATION

WEB-200 Web Attacks with Kali Linux

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

OFFENSIVE® security

WEB-200 (Web Attacks with Kali Linux) is Offensive Security's foundational web application assessment course. The course covers the topics below in detail.

Topics Covered:

- Tools for the Web Assessor
- Cross Site Scripting (XSS) Introduction and Discovery
- Cross Site Scripting (XSS) • Exploitation and Case Study
- Cross Origin Attacks
- Introduction to SQL
- SQL Injection (SQLi) and Case Study
- Directory Traversal
- XML External Entity (XXE) Processing
- Server Side Template Injection (SSTI)
- More Topics added monthly*

*The OffSec Training Library will be updated continuously with new Topics on an approximately monthly cadence. Not every course or content area will receive an update every month, but some course or content area will receive an update approximately monthly.

Course Prerequisites:

- All prerequisites for WEB-200 can be found within the Offsec Fundamentals Program, included with a Learn One or Learn Unlimited subscription
- Prerequisite Topics include:
  > PEN-100: Web Application Basics
  > PEN-100: Linux 1 & 2
  > PEN-100: Networking Basics

Competencies Gained:

- Students will obtain a wide variety of skill sets and competencies for Web App Assessments
- Students will learn foundational Black Box enumeration and exploitation techniques
- Students will leverage modern web exploitation techniques on modern applications

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

WEB-300 Advanced Web Attacks and Exploitation

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

Course Estimated time:
185 hours*

In **WEB-300**, you will learn white box web app pentesting methods. The bulk of your time will be spent analyzing source code, decompiling Java, debugging DLLs, manipulating requests and more, using tools like Burp Suite, dnSpy, JD-GUI, Visual Studio and the trusty text editor. For a more complete breakdown of the course topics view the full syllabus.

Topics Covered:

- Web security tools and methodologies
- Source code analysis
- Persistent cross-site scripting
- Session hijacking
- .NET deserialization
- Remote code execution
- Blind SQL Injections
- Data exfiltration
- Bypassing file upload restrictions and file extension filters
- PHP type juggling with loose comparisons
- PostgreSQL Extension and User Defined Functions
- Bypassing REGEX restrictions
- Magic hashes
- Bling SQL injection
- Bypassing character restrictions
- UDF reverse shells
- PostgreSQL large Objects
- DOM-based cross site scripting (black box)
- Server side template injection
- Weak random token generation
- XML external entity injection
- RCE via database functions
- OS command injection via WebSockets (black box)

Course Prerequisites:

All students are required to have:

- Comfort reading and writing at least one coding language (Java, .NET, JavaScript, Python, etc)
- Familiarity with Linux: file permissions, navigation, editing and running scripts
- Ability to write simple Python / Perl / PHP / Bash scripts
- Experience with web proxies such as Burp Suite and similar tools
- General understanding of web app attack vectors, theory and practice

Competencies Gained:

- Performing advanced web app source code auditing
- Analyzing code, writing scripts and exploiting web vulnerabilities
- Implementing multi-step chained attacks using multiple vulnerabilities
- Using creative and lateral thinking to determine innovative ways of exploiting web vulnerabilities

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

OFFENSIVE SECURITY
OSED CERTIFICATION

EXP-301 Windows User Mode Exploit Development

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

Course Estimated time: 350 hours*

EXP-301 is an intermediate course that teaches the skills necessary to bypass DEP and ASLR security mitigations, create advanced custom ROP chains, reverse-engineer a network protocol and even create read and write primitives by exploiting format string specifiers. View the full syllabus.

Topics Covered:

- Operating System and Programming Theory
- WinDbg tutorial
- Stack buffer overflows
- Exploiting SEH overflows
- Intro to IDA Pro
- Overcoming space restrictions: Egghunters
- Shellcode from scratch
- Reverse-engineering bugs
- Stack overflows and DEP/ASLR bypass
- Format string specifier attacks
- Custom ROP chains and ROP payload decoders

Course Prerequisites:

All students should have the following prerequisite skills before starting the course:

- Familiarity with debuggers (ImmunityDBG, OllyDBG)
- Familiarity with basic exploitation concepts on 32-bit
- Familiarity with writing Python 3 code
- The following optional skills are recommended:
    - Ability to read and understand C code at a basic level
    - Ability to read and understand 32-bit Assembly code at a basic level
- The prerequisite skills can be obtained by taking our Penetration Testing with Kali Linux course.

Competencies Gained:

- Using WinDbg
- Writing your own shellcode
- Bypassing basic security mitigations, including DEP and ASLR
- Exploiting format string specifiers
- The necessary foundations for finding bugs in binary applications to create custom exploits

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

OFFENSIVE SECURITY
OSMR CERTIFICATION

EXP-312 macOS Control Bypasses

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

OFFENSIVE® security

Course Estimated time:
150 hours*

EXP-312 (macOS Control Bypasses) is an offensive logical exploit development course for macOS, focusing on local privilege escalation and bypassing the operating system's defenses. It's an intermediate course that teaches the skills necessary to bypass security controls implemented by macOS, and exploit logic vulnerabilities to perform privilege escalation on macOS systems.

Topics Covered:

- Introduction to macOS internals
- Debugging, Tracing   Hopper
- Shellcoding in macOS
- Dylib Injection
- Mach and Mach injection
- Hooking
- XPC exploitation
- Sandbox escape
- Attacking privacy (TCC)
- Symlink attacks
- Kernel code execution
- macOS Pentesting

Course Prerequisites:

- C programming knowledge
- Normal user experience with macOS
- Basic familiarity with 64-bit assembly and debugging
- Understanding of basic exploitation concepts

Competencies Gained:

- Obtain a strong understanding of macOS internals
- Learn the basics of Mach messaging
- Learn how to bypass Transparency, Content and Control (TCC) protections
- Learn how to escape the Sandbox
- Perform symbolic link attacks
- Leverage process injection techniques
- Exploit XPC for privilege escalation
- Perform hooking based attacks
- Write Shellcode for macOS
- Bypass kernel code-signing protection

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

OFFENSIVE SECURITY
OSDA CERTIFICATION

SOC-200 Security Operations and Defensive Analysis

Course Includes the Following:

- Course Materials
- Active Student Forums
- Access to Home Lab Setup

Learn One

- One course
- 365 days of lab access
- Two exam attempts
- Plus exclusive content

Learn Unlimited

- All courses
- 365 days of lab access
- Unlimited exam attempts
- Plus exclusive content

OFFENSIVE® security

Course Estimated time: 150 hours*

SOC-200 (Security Operations and Defensive Analysis) is Offensive Security's foundational security operations course.

This new course teaches students the mindset required to assess and respond to security incidents. Topics covered are below.

Topics Covered:

- Attacker Methodology
- Introduction
- Windows Endpoint Introduction
- Windows Server Side Attacks
- Windows Client Side Attacks
- Windows Privilege Escalation
- Linux Endpoint Introduction
- Linux Server Side Attacks
- Linux Privilege Escalation
- More Topics added monthly*

*The OffSec Training Library will be updated continuously with new Topics on an approximately monthly cadence. Not every course or content area will receive an update every month, but some course or content area will receive an update approximately monthly.

Course Prerequisites:

- All prerequisites for SOC-200 can be found within the Offsec Fundamentals Program, included with a Learn One or Learn Unlimited subscription
- Prerequisite Topics include:
  > PEN-100: Linux Basics 1 & 2
  > PEN-100: Windows Basics 1 & 2
  > PEN-100: Networking Basics

Competencies Gained:

- Students will get hands on experience investigating malicious activity
- Students will learn about attack surfaces and how they can be reduced
- Students will develop a working knowledge of security operations and best practices

*Time estimates are based on OffSec averages and could vary by individual skill and experience.

Learn Fundamentals

NEW Subscription for 100-Level Content

Introducing Learn Fundamentals OffSec's entry-level, or beginner, training plan. Get annual access to all 100-level content (PEN-100, WEB-100, and SOC-100) with new learning tracks and reporting features coming soon!

Fundamentals not only provides access to all 100-level courses, but will also offer Assessments and Badges upon successful completion.

Additionally, Learn Fundamentals includes access to PEN-103 (Kali Linux Revealed) and PEN-210 (Wireless Attacks).

TOPICS Included in Fundamentals

New Topics are continuously added to Fundamentals. These are just a sample few of what is available for students. Core Topics apply to each Fundamentals course, while the courses also have specific Topics that pertain to the subject at hand.

WORKFLOW for Learn Fundamentals

LEARN
Choose from a growing library of 100-level tracks and Topics to develop your skills for a variety of job roles

APPLY
Use hands-on exercises with lab machines to reinforce what you learn and track progress toward your goals

ASSESS
Test yourself with hands-on Assessments to check your progress towards gaining critical prerequisites for 200-level Courses

PROVE
Earn OffSec Badges to demonstrate your learnings and show-off your knowledge, skills, and abilities

Example Topics:

ALL

- Linux Basics I & II
- Networking Fundamentals
- Troubleshooting 101
- *More coming soon!*

WEB-100

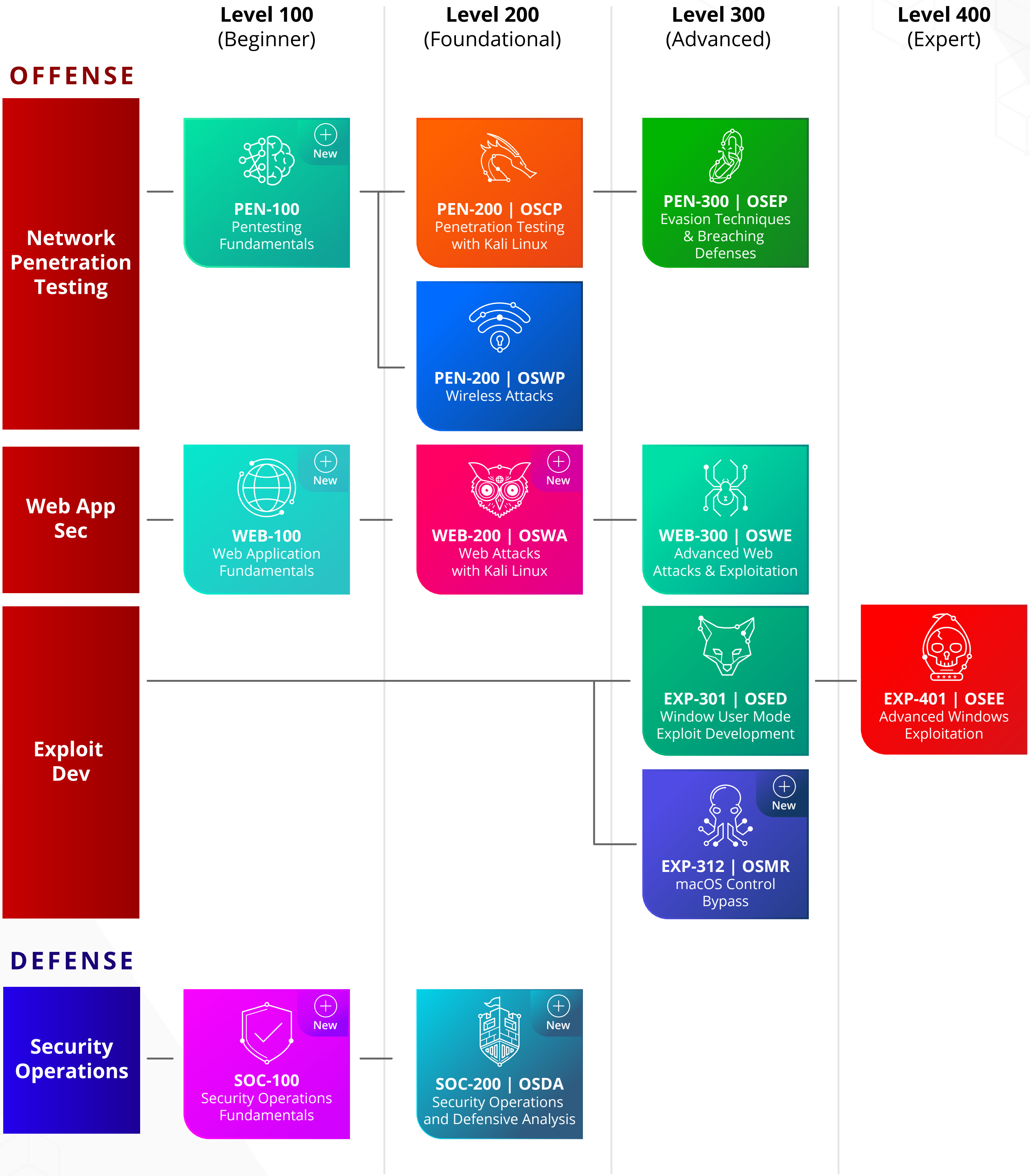
- Web Attacker Methodology
- Introduction to Secure Coding
- Input Validation
- *More coming soon!*

PEN-100

- Introduction to Cryptography
- Web Application Basics
- Working with Shells
- *More coming soon!*

SOC-100

- Enterprise Network Architecture
- SOC Management Processes
- Windows Logging
- *More coming soon!*



Level 100 (Beginner)

Level 200 (Foundational)

Level 300 (Advanced)

Level 400 (Expert)

OFFENSE

Network Penetration Testing

- **PEN-100** Pentesting Fundamentals (New)
- **PEN-200 | OSCP** Penetration Testing with Kali Linux
- **PEN-200 | OSWP** Wireless Attacks
- **PEN-300 | OSEP** Evasion Techniques & Breaching Defenses

Web App Sec

- **WEB-100** Web Application Fundamentals (New)
- **WEB-200 | OSWA** Web Attacks with Kali Linux (New)
- **WEB-300 | OSWE** Advanced Web Attacks & Exploitation

Exploit Dev

- **EXP-301 | OSED** Window User Mode Exploit Development
- **EXP-312 | OSMR** macOS Control Bypass (New)
- **EXP-401 | OSEE** Advanced Windows Exploitation

DEFENSE

Security Operations

- **SOC-100** Security Operations Fundamentals (New)
- **SOC-200 | OSDA** Security Operations and Defensive Analysis (New)

OSEP + OSWE + OSED = OSCE³ (New Cert)

Course Syntax

Track	Course Level	Operating System
PENtesting	**100 -** Beginner	**0 -** Multiple OS
WEB App Security	**200 -** Foundational	**1 -** Windows
EXPloit Dev	**300 -** Advanced	**2 -** macOS
DEFensive	**400 -** Expert	**3 -** Linux