

Training: OffSec  
OffSec EXP-312 Advanced macOS Control Bypasses



## TRAINING GOALS:



Advanced 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. Learners who complete the course and pass the exam earn the OffSec macOS Researcher (OSMR) certification.

### Benefits

- Obtain a strong understanding of macOS Internals
- Learn how to bypass security controls implemented by macOS
- Exploit logic vulnerabilities to perform privilege escalation on macOS systems

### Who is this course for?

- Anyone who is interested in learning about macOS exploitation
- Pentesters looking to broaden their skill set to include macOS expertise
- Anyone committed to the defense or security of macOS systems
- Job roles like Penetration testers, Exploit developers, Security researcher, macOS defenders, and macOS application developers

## Exam

- The EXP-312 course and online lab prepares you for the OSMR certification
- 48-hour exam
- Proctored
- Learn more about the exam  
<https://help.offensive-security.com/hc/en-us/articles/4411099553172-OSMR-Exam-FAQ>

## What competencies will you gain?

- 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

## CONSPECT:

- macOS Control Bypasses: General Course Information
  - About The EXP-312 Course
  - Provided Materials
  - Overall Strategies for Approaching the Course
  - About the EXP-312 VPN Labs
  - About the OSMR Exam
  - Wrapping Up
- Virtual Machine Setup Guide
  - Creating VMs on Apple Silicon
  - Installing Xcode
  - Homebrew
  - Old and Other Software

- Third Party Software
- General System Settings
- Specific VM Instructions
- Introduction to macOS
  - macOS System Overview
  - High-Level OS Architecture
  - The Mach-O File Format
  - Objective-C Primer Wrapping Up
- macOS Binary Analysis Tools
  - Command Line Static Analysis Tools
  - Static Analysis with Hopper
  - Dynamic Analysis
  - The LLDB Debugger
  - Debugging with Hopper
  - Tracing Applications with DTrace
  - Wrapping Up
- The Art of Crafting Shellcodes
  - Writing Shellcode in ASM
  - Custom Shell Command Execution in Assembly
  - Making a Bind Shell in Assembly
  - Writing Shellcode in C
  - Wrapping Up
- Dylib Injection
  - DYLD\_INSERT\_LIBRARIES Injection in macOS
  - DYLIB Hijacking
  - Wrapping Up
- The Mach Microkernel
  - Mach Inter Process Communication (IPC) Concepts
  - Mach Special Ports
  - Injection via Mach Task Ports
  - BlockBlock Case Study - Injecting execv Shellcode
  - Injecting a Dylib
  - Wrapping Up
- Function Hooking on macOS
  - Function Interposing
  - Objective-C Method Swizzling

- Wrapping Up
- XPC Attacks About XPC
  - The Low Level C API: XPC Services
  - The Foundation Framework API
  - Attacking XPC Services
  - Apple's EvenBetterAuthorizationSample
  - CVE-2019-20057 - Proxyman Change Proxy Privileged Action Vulnerability
  - CVE-2020-0984 - Microsoft Auto Update Privilege Escalation Vulnerability
  - CVE-2019-8805 - Apple EndpointSecurity Framework Local Privilege Escalation
  - CVE-2020-9714 - Adobe Reader Update Local Privilege Escalation
  - Wrapping Up
- The macOS Sandbox Sandbox Internals
  - The Sandbox Profile Language (SBPL)
  - Sandbox Escapes
  - Case Study: QuickLook Plugin SB Escape
  - Case Study: Microsoft Word Sandbox Escape
  - Wrapping Up
- Bypassing Transparency, Consent, and Control (Privacy)
  - TCC Internals
  - CVE-2020-29621 - Full TCC Bypass via coreaudiod
  - Bypass TCC via Spotlight Importer Plugins
  - CVE-2020-24259 - Bypass TCC with Signal to Access Microphone
  - Gain Full Disk Access via Terminal
  - Wrapping Up
- GateKeeper Internals
  - File Quarantine
  - XProtect
  - GateKeeper
  - Wrapping Up
- Bypassing GateKeeper
  - CVE-2022-42821 GateKeeper Bypass Using AppleDouble Files
  - CVE-2021-30990 GateKeeper Bypass using Symbolic Links
  - Wrapping Up
- Symlink and Hardlink Attacks
  - The Filesystem Permission Model
  - Finding Bugs

- CVE-2020-3855 - macOS DiagnosticMessages File Overwrite Vulnerability
- CVE-2020-3762 - Adobe Reader macOS Installer Local Privilege Escalation
- CVE-2019-8802 - macOS Manpages Local Privilege Escalation
- Wrapping Up
- Getting Kernel Code Execution
  - KEXT Loading Restrictions
  - Sample KEXT
  - The KEXT Loading Process
  - CVE-2020-9939 - Unsigned KEXT Load Vulnerability
  - CVE-2021-1779 - Unsigned KEXT Load Vulnerability
  - Changes in Big Sur
  - Wrapping Up
- Injecting Code into Electron Applications
  - Setting up an Electron Development Environment
  - Creating a Simple Electron App
  - The Application
  - Environment Variable Injection
  - Debug Port Injection
  - Source Code Modification
  - Protecting Electron Applications
  - Wrapping Up
- Mount(ain) of Bugs (Archived)
  - The MAC Framework
  - The mount System Call
  - Disk Arbitration Service
  - CVE-2021-1784 - TCC Bypass Via Mounting Over com.apple.TCC
  - CVE-2021-30782 - TCC Bypass Via AppTranslocation Service
  - CVE-2021-26089 - Fortinet FortiClient Installer Local Privilege Escalation
  - CVE-2021-26089 - Exploitation
  - Wrapping Up
- The Art of Crafting Shellcodes (Apple Silicon Edition)
  - Writing Shellcode in ASM
  - Executing Custom Shell Commands in Assembly
  - Making a Bind Shell in Assembly
  - Writing Shellcode in C
  - Wrapping Up

- Mach IPC Exploitation
  - The Mach Interface Generator (MIG)
  - CVE-2022-22639 Exploitation Case Study
  - Wrapping Up
- Chaining Exploits on macOS Ventura
  - macOS Ventura Mitigations
  - Exploit Chain on macOS Ventura
  - Wrapping Up
- macOS Penetration Testing
  - Small Step For Man
  - The Jail
  - I am (g)root
  - CVE-2020-26893 - I Like To Move It, Move It
  - Private Documents - We Wants It, We Needs It
  - The Core
  - Wrapping Up

## REQUIREMENTS:

All learners are required to have:

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

## Difficulty level



## CERTIFICATE:

After passing the OSMR exam, candidates receive a title of OffSec macOS Researcher (OSMR).



## TRAINER:

Authorized OffSec Trainer

## ADDITIONAL INFORMATION:

Course is available as the e-learning product, in two subscription's models:

- Course & Cert Exam Bundle
- Learn One

	Most popular	Best value
	 <p><b>Course &amp; Cert Exam Bundle</b> <b>\$1649</b> One-time payment</p>	 <p><b>Learn One</b> <b>\$2599/year</b> Billed annually</p>
# of Courses	1	1
Days of lab access	90	365
# of Exam Attempts included	1	2
Fundamental content	N/A	Unlimited
<u>PEN-103</u> & 1 KLCP Exam	N/A	Included
<u>PEN-210</u> & 1 OSWP Exam	N/A	Included
<u>PG Practice</u>	N/A	Included