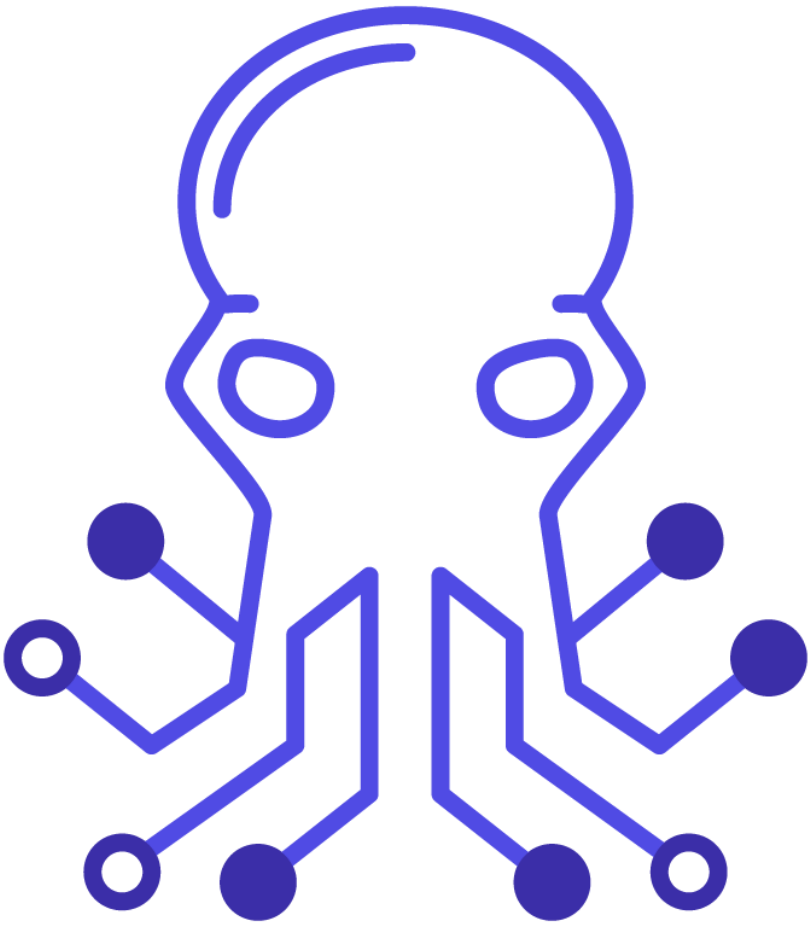
# macOS Control Bypasses

## Syllabus



1. **macOS Control Bypasses: General Course Information**
    a. About The EXP-312 Course
    b. Provided Materials
        EXP-312 Course Materials
        Access to the Internal VPN Lab Network
        The Offensive Security Student Forum
        Live Support
        OSMR Exam Attempt
    c. Overall Strategies for Approaching the Course
        Course Materials
        Course Exercises
    d. About the EXP-312 VPN Labs
        Control Panel
        Reverts
        Kali Virtual Machine
        Accessing the macOS Desktop
        Lab Behavior and Lab Restrictions
    e. About the OSMR Exam
    f. Wrapping Up
2. **Introduction to macOS**
    a. macOS System Overview
    b. High-Level OS Architecture
        Apple Proprietary File System (APFS)
        System Volume Protections
        Firmlinks
        Important Directories
        Property List Files
        Bundles
        The Application Bundle
        Other Bundles
        The dyld Shared Cache
    c. The Mach-O File Format
        Universal Binaries

Mach-O Structure
Mach-O Header
Load Commands
Mach-O Data

d. Objective-C Primer
    Defining Classes, Objects, and Calling Methods
    Setter and Getter Methods
    Instance Variables
    Putting it Together
    Protocols
    Basic Types, Classes
    Blocks
    Working with Files
e. Wrapping Up

**3. macOS Binary Analysis Tools**

a. Command Line Static Analysis Tools
    codesign
    objdump
    jtool2
b. Static Analysis with Hopper
    Views in Hopper
    Navigating the Code
    External C Function Resolution
c. Dynamic Analysis
    macOS Debugging Rules
d. The LLDB Debugger
    Setting Breakpoints
    Disassembling with LLDB
    Reading and Writing Memory, and Registers
    Modifying Code During Debugging
e. Debugging with Hopper
    Setting Breakpoints
    Starting the Debugger
    Basic Controls and Functionality

Inspecting External Function Resolution

f. Tracing Applications with DTrace

Basic Terms

DTrace Example - Monitoring System Calls

DTrace Example - Monitoring Write Calls

DTrace Example - Creating Aggregation Info

DTrace Probes

System DTrace Scripts

g. Wrapping Up

**4. The Art of Crafting Shellcodes**

a. Writing Shellcode in ASM

Calling Conventions and Registers

System Call Numbering

Making Syscalls from Shellcode

b. Custom Shell Command Execution in Assembly

Planned Memory Layout

Putting Arguments on the Stack

Setting up the Syscall

Putting it Together

Analyzing the Shellcode with dtrace

Analyzing the Shellcode in a Debugger

c. Making a Bind Shell in Assembly

Creating a Socket

In the Darkness Bind Them

Listening on the Socket

Accepting Incoming Connections

Duplicating File Descriptors

Executing /bin/zsh

Putting the Bind Shell Together

d. Writing Shellcode in C

Writing execv Shellcode in C

Eliminating RIP Relative Addressing

Eliminating Calls into the __stub Section

Locating execv Pointer and Running the Code

e. Wrapping Up

5. **Dylib Injection**
    a. DYLD_INSERT_LIBRARIES Injection in macOS
        Performing an Injection
        Restrictions of DYLD_INSERT_LIBRARIES Injection
        Verifying Restrictions
    b. DYLIB Hijacking
        Dylib LOAD Commands
        Dylib Loading Process and Hijacking Scenarios
        Finding Vulnerable Applications
        Performing Dylib Hijacking
        Hijacking Dlopen
    c. Wrapping Up
6. **The Mach Microkernel**
    a. Mach Inter Process Communication (IPC) Concepts
    b. Mach Special Ports
    c. Injection via Mach Task Ports
        Getting the SEND Right
        Writing to Remote Process Memory
        Starting a Remote Thread
    d. BlockBlock Case Study - Injecting execv Shellcode
        The Vulnerability
        The BlockBlock Shellcode
        Finding the Process ID
        Putting it Together
    e. Injecting a Dylib
        Promoting Mach Thread to POSIX Thread
        The Shellcode
    f. Wrapping Up
7. **Function Hooking on macOS**
    a. Function Interposing
        Interposing printf
        Interposing ioctl Calls
    b. Objective-C Method Swizzling

The Objective-C Runtime

Objective-C Message Sending

Using the Runtime API

Hooking Objective-C Methods

Sniffing a KeePass Master Password

c. Wrapping Up

**8. XPC Attacks**

a. About XPC

b. The Low Level C API: XPC Services

c. The Foundation Framework API

d. Attacking XPC Services

Typical Issues in XPC Services

The API to Verify Client Signature Information

e. Apple's EvenBetterAuthorizationSample

Authorization Concepts

Authorization in EvenBetterAuthorizationSample

f. CVE-2019-20057 - Proxyman Change Proxy Privileged Action Vulnerability

CVE-2019-20057 - Root Cause Analysis

CVE-2019-20057 - Exploitation

g. CVE-2020-0984 - Microsoft Auto Update Privilege Escalation Vulnerability

CVE-2020-0984 - Root Cause Analysis

CVE-2020-0984 - Exploitation

h. CVE-2019-8805 - Apple EndpointSecurity Framework Local Privilege Escalation

CVE-2019-8805 - Root Cause Analysis

CVE-2019-8805 - Exploitation

i. CVE-2020-9714 - Adobe Reader Update Local Privilege Escalation

The Original Vulnerability and Exploit

Analyzing the Patch

CVE-2020-9714 - Exploitation

j. Wrapping Up

**9. The macOS Sandbox**

a. Sandbox Internals

Sandbox Containers

Entering the Sandbox

Disable Sandbox Through Interposing

b. The Sandbox Profile Language (SBPL)
    - SBPL Syntax
    - Writing Custom SBPL Profiles
    - System Sandbox Profiles
c. Sandbox Escapes
d. Case Study: QuickLook Plugin SB Escape
    - The QuickLook Vulnerability
    - Creating QuickLook Plugins
    - Escaping the Sandbox - QuickLook
e. Case Study: Microsoft Word Sandbox Escape
    - The Word Vulnerability
    - Escaping the Sandbox - Word
    - The Patch
f. Wrapping Up

**10. Bypassing Transparency, Consent, and Control (Privacy)**

a. TCC Internals
    - The Consent Databases
    - User Intent
    - Managing TCC
    - TCC Summary
b. CVE-2020-29621 - Full TCC Bypass via coreaudiod
    - CVE-2020-29621 Vulnerability Analysis
    - The Private TCC API
    - . CVE-2020-29621 Exploitation
c. Bypass TCC via Spotlight Importer Plugins
    - The Spotlight Service
    - Vulnerability Analysis
    - Exploitation
d. CVE-2020-24259 - Bypass TCC with Signal to Access Microphone
    - CVE-2020-24259 Vulnerability Analysis
    - CVE-2020-24259 Exploitation
e. Gain Full Disk Access via Terminal
f. Wrapping Up

**11. Symlink and Hardlink Attacks**

a. The Filesystem Permission Model
    - The POSIX Model
    - Flag Modifiers
    - The Sticky Bit
    - Access Control Lists
    - The macOS Sandbox

b. Finding Bugs
    - Static Analysis
    - Dynamic Analysis
    - Exploitable Conditions

c. CVE-2020-3855 - macOS DiagnosticMessages File Overwrite Vulnerability

d. CVE-2020-3762 - Adobe Reader macOS Installer Local Privilege Escalation

e. CVE-2019-8802 - macOS Manpages Local Privilege Escalation

f. Wrapping Up

**12. Getting Kernel Code Execution**

a. KEXT Loading Restrictions

b. Sample KEXT

c. The KEXT Loading Process
    - Initiating KEXT Load Requests
    - Entering kextd
    - KEXT Staging
    - KEXT Authentication and syspolicyd
    - Loading the KEXT, Entering XNU

d. CVE-2020-9939 - Unsigned KEXT Load Vulnerability
    - The Vulnerability and the Exploit Plan
    - Staging a KEXT with Symlink
    - The Insecure Location Problem
    - The Race to the Kernel
    - Disabling SIP

e. CVE-2021-1779 - Unsigned KEXT Load Vulnerability
    - The Patch
    - Bypassing Code Signing
    - Forget the Race, Meet Interactive Mode

f. Changes in Big Sur
g. Wrapping Up

**13. Injecting Code into Electron Applications**

a. Setting up an Electron Development Environment
b. Creating a Simple Electron App
    Typical Contents of Electron Applications
c. The Application
d. Environment Variable Injection
e. Debug Port Injection
f. Source Code Modification
g. Protecting Electron Applications
h. Wrapping Up

**14. Mount(ain) of Bugs**

a. The MAC Framework
b. The mount System Call
c. Disk Arbitration Service
d. CVE-2021-1784 - TCC Bypass Via Mounting Over com.apple.TCC
    CVE-2021-1784 - Exploitation
e. CVE-2021-30782 - TCC Bypass Via AppTranslocation Service
    CVE-2021-30782 - Exploitation
f. 16.6. CVE-2021-26089 - Fortinet FortiClient Installer Local Privilege Escalation
    CVE-2021-26089 - Exploitation
g. Wrapping Up

**15. macOS Penetration Testing**

a. Small Step For Man
b. The Jail
    Prison Break
    Let's Persist
c. I am (g)root
    Searching for Low-Hanging Fruit?
d. CVE-2020-26893 - I Like To Move It, Move It
    Periodic Scripts
    PAM Modules
    This is the Way

e. Private Documents - We Wants It, We Needs It
CVE-2020-9934 - HOME Relocation
f. The Core
g. Wrapping Up