

Offsec OSMR

Offsec OSMR Mac OS



This is to acknowledge that
 Shen
is certified as an
OSMR
(OffSec macOS Researcher)
and successfully completed all requirements and criteria for
said certification through examination administered by OffSec.
This certification was earned on
December 4, 2024



Offsec OSCP/OSEP/OSWE OSMR OSMR



OSMR Mac Mac Mac

Mac Mac Mac Linux Mac
breach dylib M
OSMR OSCE3 OSMR




OSMR 300 <https://www.offsec.com/course/exp-312/>

OSMR EXP C AMD64/ARM DEBUG

7	The Mach Microkernel (Apple Silicon)		December 01, 2024	<div><div></div></div>		<input type="checkbox"/>
8	XPC Attacks (Apple Silicon)		December 04, 2024	<div><div></div></div>		<input type="checkbox"/>
9	Function Hooking on macOS (Apple Silicon)		-	<div><div></div></div>	<div><div></div></div>	<input type="checkbox"/>
10	The macOS Sandbox (Apple Silicon)		November 27, 2024	<div><div></div></div>		<input type="checkbox"/>
11	Bypassing Transparency, Consent, and Control (Privacy) (Apple Silicon)		November 28, 2024	<div><div></div></div>		<input type="checkbox"/>
12	GateKeeper Internals (Apple Silicon)		November 26, 2024	<div><div></div></div>		<input type="checkbox"/>
13	Symlink and Hardlink Attacks (Apple Silicon)		November 27, 2024	<div><div></div></div>		<input type="checkbox"/>
14	Injecting Code into Electron Applications (Apple Silicon)		November 26, 2024	<div><div></div></div>		<input type="checkbox"/>
15	macOS Penetration Testing		December 01, 2024	<div><div></div></div>	<div><div></div></div>	<input checked="" type="checkbox"/>
16	macOS Control Bypasses: General Course Information archived archived		November 26, 2024	<div><div></div></div>		<input checked="" type="checkbox"/>
17	Introduction to macOS archived archived		November 19, 2024	<div><div></div></div>		<input checked="" type="checkbox"/>
18	The Art of Crafting Shellcodes archived archived		December 03, 2024	<div><div></div></div>	<div><div></div></div>	<input checked="" type="checkbox"/>
19	Dylib Injection archived archived		November 19, 2024	<div><div></div></div>	<div><div></div></div>	<input checked="" type="checkbox"/>
20	The Mach Microkernel archived archived		December 01, 2024	<div><div></div></div>	<div><div></div></div>	<input checked="" type="checkbox"/>
21	XPC Attacks archived archived		December 01, 2024	<div><div></div></div>	<div><div></div></div>	<input checked="" type="checkbox"/>
22	Function Hooking on macOS archived archived		November 13, 2024	<div><div></div></div>	<div><div></div></div>	<input checked="" type="checkbox"/>
23	The macOS Sandbox archived archived		December 01, 2024	<div><div></div></div>		<input checked="" type="checkbox"/>

OSMR ARM Mac Offsec Mac VM




Adrii

2024/12/1 12:19

Hi, I've noticed that last week most of the course content had been archived for the new "Apple Silicon" counterparts.


I see that most examples in the new coursework now use this "sonoma1" machine but it doesn't appear as a challenge lab? When will sonoma1 be available to use?



ApexPredator

2024/12/1 12:51


The announcement said the lab machines are being discontinued and that students will have to build their own local VMs on apple hardware



Adrii

2024/12/1 13:03



Thanks @ApexPredator, I wasn't aware of the announcement. As the course is now more focused on ARM, I imagine that there will also be changes to the exam, right? Is there any estimated date for this? I plan to take the exam in 1-2 months.



ApexPredator

2024/12/1 13:04

I haven't heard anything. Not sure how they will solve the issue of apple silicon VMs in the cloud though for the exam.

 2 

OSMR Mac OSMR

The Art of Crafting Shellcodes (Apple Silicon Edition)
GateKeeper Internals
Bypassing GateKeeper
Injecting Code into Electron Applications archived
Mach IPC Exploitation
Chaining Exploits on macOS Ventura

OSMR

Mac



OSMR <https://help.offsec.com/hc/en-us/articles/4411099553172-OSMR-Exam-FAQ> (
<https://help.offsec.com/hc/en-us/articles/4411107766804-EXP-312-Advanced-macOS-Control-Bypasses-OSMR-Exam-Guide> OSMR

1. 使用 C 语言编写 DEBUG 程序
2. 使用汇编语言编写
3. 使用 Python 编写

工具

1. OSED 使用 OSMR 工具
2. 使用 OSED 工具 C 语言 OSMR 工具 Objective-C 工具

环境

使用 OSMR 工具 OSMR 工具

步骤

1. 使用工具
2. 使用 Offsec 工具
3. 使用 Mac 工具

资源

1. VNC 工具 lab 工具 <https://www.nomachine.com/> 工具
2. Offsec 工具

Revision #7

Created 4 December 2024 19:23:12 by winslow

Updated 5 December 2024 00:16:35 by winslow