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

Validate

□□□ Offsec □□□□□□□□□ OSCP/OSEP/OSWE□OSMR □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ OSMR □□□□□□□□□□□□□□□□□

□□

□□□□ OSMR □□ Mac □□□□□□□□□□□□□□□□□□□□□□ Mac □□□□□□□□□□ Mac [

□□□□□□□ Mac □□□□□□□ Mac □□□□□□□□□□□□□ Mac □□□□□□ Linux□□□□□□□□□□□□□□□□□□□□□ Mac □□□□□□□□□□
breach □□□ dylib □□□□□□□□□□□□□□□□□□ Ma

□□□□□□□□□□□□□□□□□ OSMR□□□□□□□□□□ OSCE3□□ OSMR □□□

□□□□□□□

OSMR □□□ 300 □□□□□□

OSMR □ EXP□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ C □□□□□AMD64/ARM □□□□□□□□□□□□□DEBUG□□□□□□□

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

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Hi, I've noticed that last week most of the course content had been archived for the new "Apple Silicon" counterparts.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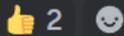
□□□□□□□□□□OSMR □□□□□□□□□□□□□□□ Mac □□□□□□□□□□□□□□□□□□□□ OSMR □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

> 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 □□□□□□□

□□□□

□□□□□□□□□□OSMR □□□□ 4 □□□□□□□□□□□□□□□□ 80 □□□□ 70 □□□□2 □□□□□□□□ 30 □□2 □□□□□□ 10 □□□□□□□□□□□□□□□□□

□□□□2 □ 30□ □□□□□□□□□□□□□□□□□□□ 47□□ 45 □□ + 24□□□□□□

Are there assignment dependencies in the exam?

Yes, the two mandatory assignments are dependent upon each other.

□□□□

□□□□□4 □□□□□□□□ 10 □□□□□□□□□ 2 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□OSMR □□□□□□□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□□□□□□□□Offsec □□□ CVE □□ Exploit□□□□□□□□□

In an effort to keep the exam experience equal for all learners, we request that you do not reveal the software being exploited in the OSMR exam, or share any exploitation steps and code publicly.

□□ Mac □□□□□□

□□□□

□□□□ OSCP/OSEP □□□□□□□OSMR □□□□□□□□□□□□□ VM□□□□□□□□□ lab□□□□□□□□□ exercise □ extra miles □□□□□□ VM □□□□□

□□□□

□□□□□□□ OSMR □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ Offsec □□□□□□□□□□□□

□□□□□□□□

□□□□□□□□□□□□□□□□□□□□ 14 □□□

□ OSED □□

□□ OSMR □ OSED □□ EXP □□

□□□□

1. □□□□□ C □□□□□□□□□□□□□□□□□DEBUG□□□□□□□□□□
2. □□□□□□□□□□□□□□□□□□□□□□□□
3. □□□□□□□□□□□□□□□□□□□□□□

□□□□

1. OSED □□□□□□□□□□□OSMR □□□□□□□□□
2. □□□□□OSED □□□□□□□□□□ C □□□□□□OSMR □□□ Objective-C □□□□□□

□□□□

□□□□□□□□□□ OSMR □□□□□ OSMR □□□

□□

1. □□□□□□□□□□□□□□
2. □□□□□□□□ Offsec □□□□□□□□□□
3. □□□□□□□□□□ Mac □□□□□□□□□

□□

1. □ VNC □□ lab □□□□□□□□□□□□https://www.nomachine.com/ □□□□
2. Offsec □□□□□□□□□□□□□