# Offsec OSMR Course and Exam Review

Hello, in the past few months, I haven't been very active in the cyber security community because I've been studying Offsec's OSMR course. This course focuses on macOS internals and exploit development. The course is far more extensive than I had anticipated, and the content is entirely novel to me, which has required a significant investment of time. Fortunately, I recently passed the OSMR exam, and my hard work has paid off.



Compared to Offsec's other certifications, such as OSCP/OSEP/OSWE, OSMR is relatively new, with fewer certification holders and limited related insights and sharing available. Therefore, I want to share an additional OSMR review to help people who may be interested in it.

In the following sections, I will briefly introduce my motivations for studying this course, provide basic information about the course, discuss the exam, and share my personal evaluation.

# Motivation

I witnessed the initial release of the OSMR course and found it intriguing at the time, but I had no plans to enroll or study it. This was because Mac-related attacks and exploitation rarely came up in my daily work. However, a red team exercise centered around macOS made me realize the importance and appeal of Mac attacks and exploitation.

Before this, I had some experience using macOS but had only a superficial understanding of its internal. I assumed macOS was somewhat similar to Linux, and many concepts could be directly applied or adapted. However, during the Mac-focused red team exercise, my arrogance and ignorance were shattered. Before the exercise began, the team lead sent me some internal company resources on macOS security, introducing concepts like TCC, sandboxing, GateKeeper, SIP, and initial access methods on macOS. Many of these terms were entirely new to me, and simply browsing through the initial access methods highlighted how significantly macOS differs from Linux. It was evident I knew almost nothing about this operating system.

For the exercise, the client shipped us MacBooks used by their employees to simulate an assumed breach scenario. With access to the devices, local reconnaissance and review were naturally necessary, but I felt utterly at a loss. Fortunately, the team lead shared some links, such as guides on identifying and exploiting dylib hijacking. Although I have some findings in other phases of the red team exercise, I regret that I couldn’t contribute much to local reconnaissance and exploitation on macOS.

After this red team exercise, I resolved to study the OSMR course in the future. At the time, though, I was pursuing OSCE3, so it wasn’t part of my immediate plans. But now, with the support of my boss and employer, I’ve finally enrolled in the OSMR course.

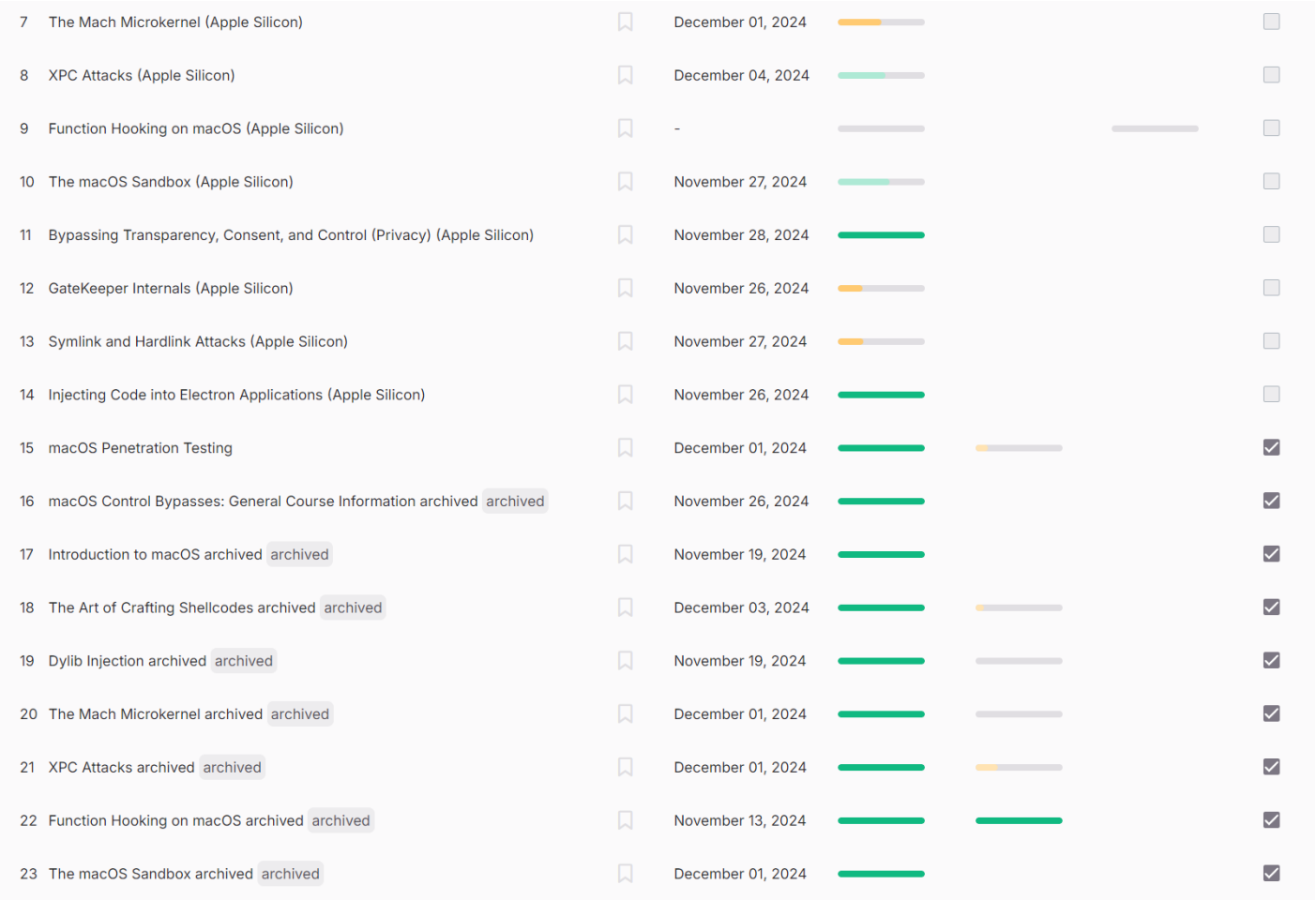
# Course Info

OSMR is a 300-level course, which clearly indicates a certain level of difficulty. For more details, such as the course syllabus, you can refer to the official OSMR page:

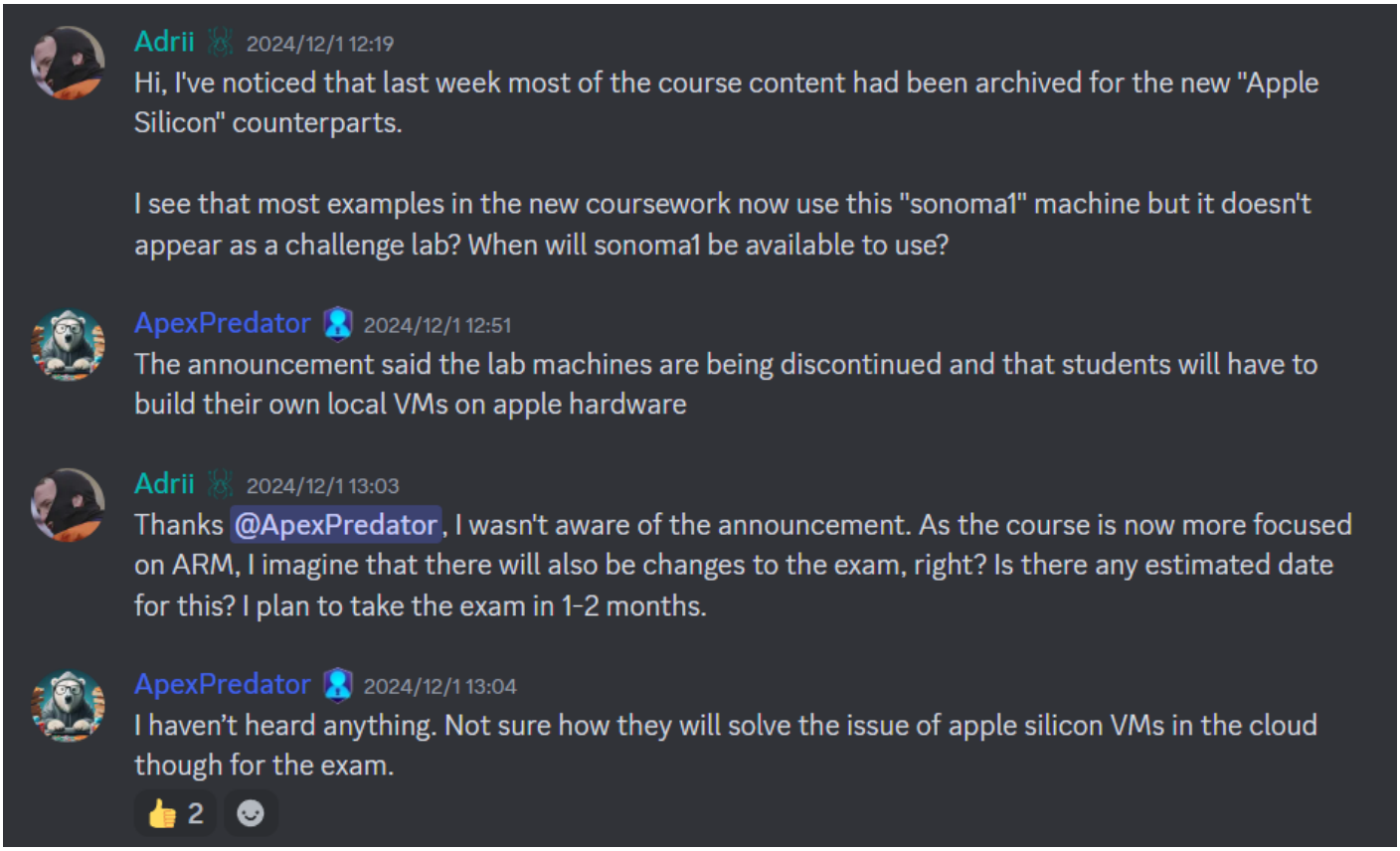
https://www.offsec.com/courses/exp-312/.

OSMR falls under the EXP category, focusing on exploit development. While not mandatory, having some prerequisite skills can be highly beneficial, such as knowledge of C programming, AMD64/ARM assembly, scripting, reverse engineering, and debugging. Without these skills, the learning process may be quite challenging. Fortunately, my prior experience with OSED provided me with a solid foundation.

One common question is whether owning a physical Mac device is necessary for the course. Interestingly, just two days before my exam, OSMR underwent a major content update. Previously, the course was primarily based on the AMD64 architecture, but moving forward, it will gradually transition entirely to the ARM architecture, with AMD64 content archived.




I am very pleased with this significant update, as it reflects the course's commitment to staying up-to-date with current trends. The content is cutting-edge, but this architectural shift, combined with infrastructure limitations, means that while students previously could use an Offsec-provided macOS VM for practice, they will now need to set up their own macOS ARM VM for learning. Therefore, the answer to this question is: **yes, you now need an ARM-based Mac device for the course**.




As I mentioned earlier, the OSMR course content is highly contemporary, which is crucial since macOS system internals and security controls are updated quite frequently. Since the course's launch, the training materials have been updated several times, and new chapters have been added to reflect these changes.

- 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

Currently, the OSMR training materials are extensive, and most of the content is novel for many learners, requiring months of dedicated study. The material is challenging and demands sufficient time to understand and master, take notes, and develop your own methodologies. In terms of content volume and difficulty, OSMR truly lives up to its status as a 300-level course.

The presentation of the course content is also excellent. It includes extensive analyses of real-world vulnerabilities, explorations of macOS mechanisms through reverse engineering, and concise conclusions to simplify complex topics when necessary.

# Exam

Due to the unique nature of the OSMR course, its exam also carries an air of mystery. You can refer to the official FAQ about the exam at https://help.offsec.com/hc/en-us/articles/4411099553172-OSMR-Exam-FAQ and the exam guide at https://help.offsec.com/hc/en-us/articles/4411107766804-EXP-312-Advanced-macOS-Control-Bypasses-OSMR-Exam-Guide.

Without revealing specific details, I will share some general information about the OSMR exam.

## Exam Format

As stated in the official exam guide, the OSMR exam consists of 4 tasks, each corresponding to specific objectives, with a total score of 80 points, and a passing score of 70. There are 2 mandatory tasks worth 30 points each and 2 optional tasks worth 10 points each. This means that to pass, you can only leave one optional task incomplete.

Additionally, the two mandatory 30-point tasks are interdependent, requiring progress in one to complete the other. The exam duration is 47 hours and 45 minutes, followed by an additional 24 hours to submit the report.

> **Are there assignment dependencies in the exam?**
>
> Yes, the two mandatory assignments are dependent upon each other.

## Exam Difficulty

To pass, you can only leave one optional 10-point task incomplete, and with the two mandatory tasks being interdependent, it might sound harsh and challenging. However, in practice, due to some objective factors and limitations, the OSMR exam isn’t as difficult as it seems. In my opinion, passing the exam hinges on solving just one critical task—if you can accomplish that, you're almost guaranteed to pass.

This is precisely why I find the exam design clever and engaging. The software selected by Offsec not only includes vulnerabilities that effectively assess learning outcomes but also maintains a well-balanced level of difficulty. That said, don’t expect to find relevant CVE or exploits online—diligently reverse engineer the software to uncover vulnerabilities and attack paths yourself.

> 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.

The tasks are straightforward, with no rabbit holes or traps. The exam control panel provides detailed guidance, and some tasks don’t even strictly require macOS-specific knowledge.

### Exam Preparation

Unlike other courses such as OSCP or OSEP, the OSMR course does not provide additional practice labs beyond the VM included with the study materials. However, some exercises and extra miles in the materials allow you to practice further by installing the provided vulnerable applications on the VM. While completing the extra miles is not mandatory for passing the exam, they certainly help in understanding the content and improving proficiency.

### Possible Changes In the Future

Given the significant updates to the OSMR materials, it’s likely that future exams might also see corresponding changes. Let’s wait for Offsec’s official announcements on this.

### Personal Exam Timeline

I didn’t intentionally track the time during the exam, but I completed all the tasks and the report in about 14 hours, including time for meals, breaks, and sleep. Since I took notes while solving the tasks, I didn’t spend much additional time on the report. The first mandatory task did take me some time, but not because it was difficult. The delay was due to minor issues in the exploit I wrote, such as syntax errors and mistakes in selecting the appropriate classes and methods.

## Comparison with OSED

Since both OSMR and OSED fall under the EXP category, people often wonder about their similarities and differences. Here’s a simple comparison:

### Similarities

- Both involve the use of C-family programming languages, scripting, assembly code, debugging, and reverse engineering skills.
- Both help deepen the understanding of the respective operating system internal.
- Both present considerable difficulty for beginners in their respective fields.

### Differences

- OSED focuses on memory corruption vulnerabilities, while OSMR emphasizes logic vulnerabilities.

- In terms of reverse engineering, OSED primarily involves reading assembly code and C pseudocode, whereas OSMR focuses on reading Objective-C pseudocode.

# Personal Evaluation

Finally, here’s my evaluation of OSMR. Regarding the course content and quality, I am very satisfied and have no real criticisms. That said, here are some pros and cons for discussion:

## Pros

- High-quality content with extensive material.
- The content is up-to-date, and Offsec continues to update it regularly.
- One of the very few courses on the market that focuses on macOS attacks and exploitation.

## Cons

- Accessing the lab via VNC is slow, but this can be improved by using NoMachine ( https://www.nomachine.com/).
- The practice exercises provided by Offsec are relatively limited.

---

Revision #2
Created 5 December 2024 03:22:08 by winslow
Updated 5 December 2024 03:49:01 by winslow