Offsec OSMR

课程以及认证心得分享

大家好，最近几个月以来我在网络安全社区不是很活跃，因为我在学习 Offsec 的 OSMR 课程。这是一门有关 Mac OS
内部原理，以及漏洞利用开发的课程。课程的体量十分庞大，远远超出了我的预期，内容对于我来说也是十分
的新鲜，这使得我投入较多的时间。幸运的是，最近我通过了 OSMR 的考试，期间的努力学习得到了回报。







相对于 Offsec 的其他认证，例如 OSCP/OSEP/OSWE，OSMR
较新，认证持有者较少，因此相关的心得与分享也比较少。尤其是中文的 OSMR
心得，我目前尚未遇见，那么，我希望自己的分享能填补上这块空白。接下来，我会分别简要地介绍自己学习
的动机，课程基本信息，考试相关，以及个人评价。

动机

我有见证 OSMR 课程的首发，在当时觉得很新奇，但并没有报名和学习的想法。因为在平常的工作中，涉及 Mac 的攻击与利用几乎没有。但我在工作中的一次以 Mac 为主的红队项目让我意识到 Mac 攻击与利用的重要性，以及魅力。

在此之前，我有过 Mac 的使用经历，但对于 Mac 操作系统核心的了解很肤浅，觉得 Mac 在一些地方比较像 Linux，应该有挺多地方可以照搬和融会贯通吧。但在那次 Mac 为主的红队项目中，我的傲慢与无知被颠覆了。项目开始之前，领队发给了我一些公司内部的 Mac 安全的资料连接，介绍了 Mac 的一些安全机制，例如 TCC，沙箱， GateKeeper， SIP 等，以及在 Mac 上的初始访问的方法。光是这些名词我听都没听过，以及浏览了 Mac 上的初始访问方法，让我意识到 Mac 和 Linux 有着很大的不同，我对这个操作系统根本不了解。当时的客户给我们分别邮寄了员工会持有的 Mac 笔记本，以适配 assumed breach 的情景。既然有了设备，那么本地侦察和审计自然是需要做的，我有点手足无措。好在的是，我的领队给我发了一些链接，例如怎么寻找和利用 dylib 劫持。虽然我在其他的阶段有了一些发现，但就 Mac 设备的本地侦察和利用上面，很遗憾我没有帮到什么。

在这个红队项目之后，我决定以后会学习 OSMR。不过那时候我还在追求 OSCE3，因此不在近期的计划中。但如今，我也没什么借口了，在老板和雇主的支持下，我报名了 OSMR 课程。

课程基本信息

OSMR 是一门 300 系列的课程，因此显然具备一定的难度，更多信息，例如课程目录，可以查看 OSMR 官方页面: https://www.offsec.com/courses/exp-312/。

OSMR 是 EXP，即漏洞利用开发的分类。因此，尽管不是必须，掌握一些前置的技能很有帮助，例如 C 系编程语言， AMD64/ARM 汇编，脚本编写，逆向工程， DEBUG。缺乏这些技能的话，学习起来可能会比较痛苦，好在 OSED 为我打下了还不错的基础。关于是否需要持有物理 Mac 设备来学习，这个问题值得讨论一下。恰好在我考试前两天， OSMR 迎来了重大更新。在之前， OSMR 主要是基于 AMD64 架构的，但现在和以后，会逐渐完全迁移到 ARM 架构，而 AMD64 架构的内容被封存了。

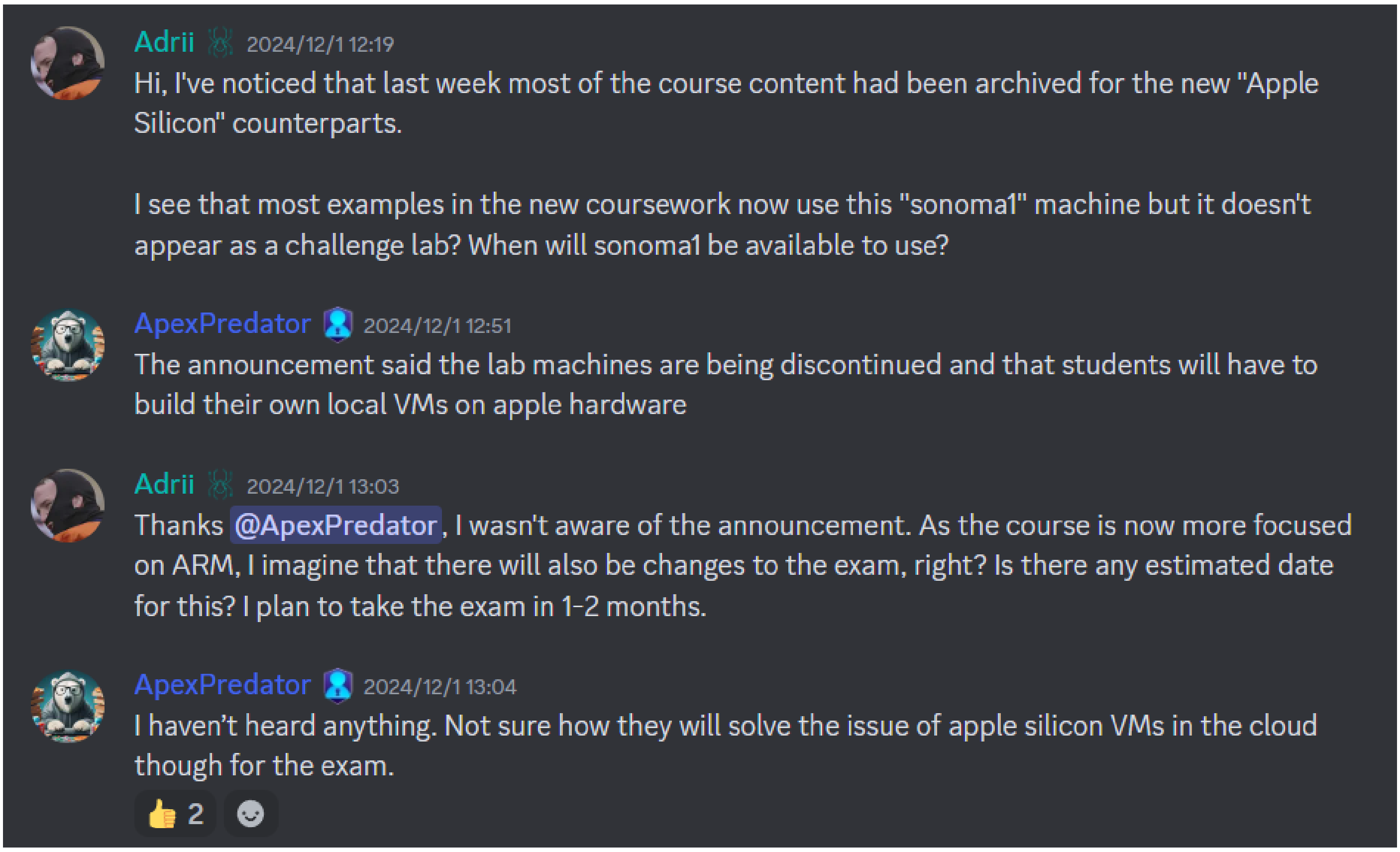
7	The Mach Microkernel (Apple Silicon)		December 01, 2024			☐
8	XPC Attacks (Apple Silicon)		December 04, 2024			☐
9	Function Hooking on macOS (Apple Silicon)		-			☐
10	The macOS Sandbox (Apple Silicon)		November 27, 2024			☐
11	Bypassing Transparency, Consent, and Control (Privacy) (Apple Silicon)		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

□□□ Offsec

□□□ Mac VM □□□□□□□□□□□□□□□□□ Mac VM □□□□□□□□□□□□□□□□□□□□□□

□□□□□□□□□□□□□□ **ARM □ Mac** □□□□□□□



正如我刚刚所称赞道的，OSMR 的内容十分与时俱进，这很重要，因为 Mac 的系统原理以及安全控制机制更新地比较勤快。自 OSMR 发布以来，教材内容已经得到了数次更新，以下这些内容是自首发以来新增加的章节。

```
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
```

如今，OSMR 教材的内容十分庞大，而且这些内容对于大多数人是很新奇的，因此会需要数月的投入时间。教材中所教的内容也比较难，需要花足够的时间来理解掌握，做笔记，以及形成自己的方法。从内容量和难度而言，OSMR 不愧是 300 级别的课程。

课程内容的呈现形式也很棒，有大量真实漏洞的分析，通过逆向工程对 Mac 系统机制的探索，以及在必要时化繁为简告知学生结论。

考试

因为 OSMR 课程的特别之处，OSMR 的考试也显得更加神秘。你可以在 https://help.offsec.com/hc/en-us/articles/4411099553172-OSMR-Exam-FAQ 查看官方关于考试的 QA，以及 https://help.offsec.com/hc/en-us/articles/4411107766804-EXP-312-Advanced-macOS-Control-Bypasses-OSMR-Exam-Guide 查看考试指南。在不透露具体细节的情况下，我分享一下 OSMR 考试相关的信息。

考试形式

正如官方考试指南所写，OSMR 考试一共 4 道题目，分别对应特定的任务，总计 80 分，其中 70 分过关。2 道必写题分别是 30 分，2 道可写题分别 10 分，也就是说想要通过，只能留一道可写题未完成。

此外，2 题 30分 的必写题是前后依赖的关系。考试时间是 47小时 45 分钟 + 24小时写报告。

Are there assignment dependencies in the exam?

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

考试难度

想要通过，4 题中仅能留有一道 10 分的可写题，而且 2 题必写题还是依赖关系，听起来是不是很苛刻和困难？但实际上，可能因为一些客观的限制，OSMR 考试并不困难。在我看来，决定考生能否通过的题目只有一题，只要能把这题做出来，就一定能通过。

也正因为如此，我觉得题目出得很巧妙和有趣。Offsec 所选择的软件，不仅具有能考察学习成果的漏洞，而且难度也控制地很合理。不过，别想着能在网络上找到相关的 CVE 或者 Exploit，老老实实地自己逆向发掘吧。

> 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.

题目很直接，没有兔子洞和陷阱，考试控制面板会有很详细的指示。有的题目甚至不严格需要 Mac 相关的知识。

备考练习

不同于 OSCP/OSEP 等其他课程，OSMR 课程除了学习教材时提供的 VM，没有额外的练习 lab。但教材里的一些 exercise 和 extra miles 可以通过在 VM 上安装提供的有漏洞的应用来获得更多练习机会。想要通过考试，extra miles 不是必须的，但对于理解内容和增加熟练度肯定会有帮助。

未来展望

因为之前提到 OSMR 的教材有了大更新，那么难免地，以后考试可能也会有相应的变化，等待 Offsec 对此的官方通知吧。

个人考试时间线

这次考试没有刻意留意时间节点。但最终 14
小时左右完成了所有题目以及报告的书写，其中包含了吃饭，休息，和睡觉的时间。因为我一边做题一边记笔
记，所以报告没有花很多时间。第一道必做题确实花了我一些时间，但并不是因为难，而是自己写的 EXP 中有一些语言用法上的小错误。

与 OSED 对比

因为 OSMR 和 OSED 都是 EXP 分类，因此经常会有人好奇两者的异同，我简单地做了个对比：

相同之处

1. 都有运用到 C 系语言编程，脚本编写，汇编代码， DEBUG，逆向工程等技能。
2. 对于理解各自所用的操作系统的机制都有所帮助
3. 对于各自领域的初学者，都有相当的难度。

不同之处

1. OSED 注重于内存损坏漏洞， OSMR 注重于逻辑漏洞。
2. 逆向方面， OSED 以阅读汇编代码以及 C 伪代码为主， OSMR 以阅读 Objective-C 伪代码为主。

个人评价

最后，分享一下自己对 OSMR 的评价。就 OSMR
内容和品质本身，我很满意，没有任何批评，但还是勉强分别讨论一下优点和不足：

优点

1. 内容品质高，章节量也很大
2. 内容比较新，而且 Offsec 有持续对其进行更新
3. 市面上极少数专注于 Mac 攻击与利用的课程

不足

1. 用 VNC 访问 lab 响应很慢，这点可以用 nomachine (https://www.nomachine.com/) 来优化。
2. Offsec 提供的配套练习比较有限

Revision #7
Created 2024-12-04 19:23:12 UTC by winslow
Updated 2024-12-05 00:16:35 UTC by winslow