

Notes

- [SAN660](#) [GXP](#) [N](#) [O](#) [S](#) [E](#) [D](#)
- [SEC660/GXP](#) Review And The Comparison With [OSED](#)
- [Offsec OSMR](#)
- [Offsec OSMR Course and Exam Review](#)

SANS SEC660 GXPN OSCE3

OSCE3 SEC660 GXPN SANS



SEC660 (<https://www.sans.org/cyber-security-courses/advanced-penetration-testing-exploits-ethical-hacking/>) SANS (<https://www.giac.org/certifications/exploit-researcher-advanced-penetration-tester-gxpn/>) GIAC SEC660



8500+ 979 10000

SANS HackFest Hollywood 2024

GXPN: GIAC Exploit Researcher and Advanced Penetration Tester
Universal City, CA, US

\$8,525 USD

GXPN Certification +\$979
OnDemand Bundle +\$979

*Prices exclude applicable local taxes

Event Details

In Person

Staff

Starts 30 Oct 2024 at 11:30 AM EDT (6 days)

Register for In Person

GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)

USD 979.00

1

USD 979.00



SANS 1200 PDF Lab VM



Windows/Linux Python FUZZ (NX,ASLR,Canary) Linux 64 () Windows 32 (SEH,DEP)



GXPN



GXPN Offsec



60 55 5 VM

Exam Format

- 1 proctored exam
- 60 questions
- 3 hours
- Minimum passing score of 67%



67% 2/3



2 2 2

Exam	Certification	Status	
GXPN Exam - ID	GIAC Exploit Researcher and Advanced Penetration Tester	✔ PASSED	Exam Summary
GXPN Exam - ID	GIAC Exploit Researcher and Advanced Penetration Tester	✔ PASSED	Exam Summary

OSED

SEC 660

SEC 660 OSED Linux 32 shellcodingLinux elf OSED



SEC660 OSEP OSED SEC660 GXPN 64 Windo



- 1. SEC660
- 2. OSED
- 3. CTF CTF



- 1.
- 2.

SEC660/GXPN Review And The Comparison With OSED

Hi folks, it's been quite a while since I last wrote review on training courses and certifications, even after passing OSCE3. In the past few days, I passed the GXPN exam, which is the certification exam of the SEC660 course. Since this was my first experience with a SANS course and a GIAC certification, I wanted to share some thoughts and impressions, as well as a comparison with OSED.

About The Course

SEC660 (<https://www.sans.org/cyber-security-courses/advanced-penetration-testing-exploits-ethical-hacking/>) is an advanced penetration testing and exploit development course offered by SANS, while GXPN (<https://www.giac.org/certifications/exploit-researcher-advanced-penetration-tester-gxpn/>) is the certification provided by GIAC specifically for the SEC660 course.

Price

The course alone, without the exam voucher, costs over \$8,500, and the exam voucher is \$979. Altogether, the course and exam total nearly \$10,000. I'm extremely grateful for my employer's reimbursement—this would definitely not be recommended for individual purchase.

SANS HackFest Hollywood 2024

GXPN: GIAC Exploit Researcher and Advanced Penetration Tester
Universal City, CA, US

\$8,525 USD



GXPN Certification +\$979
OnDemand Bundle +\$979

***Prices exclude applicable local taxes**

Event Details

In Person

 Staff

 Starts 30 Oct 2024 at 11:30 AM EDT (6 days) 

Register for
In Person

Course Format

You can either attend in-person classes according to the schedule or study at your own pace, but the price is nearly the same. After enrolling, SANS will send over 1,200 pages of printed materials, provide access to download the PDF version, access the online labs, and download locally deployable VM images. I opted for self-paced learning, but in hindsight, I feel that attending in-person classes would have provided a better atmosphere. The course materials and lab resources are accessible for 4 months.

Covered Topics

The course covers a wide range of knowledge areas, with rich and substantial content. It includes attacks and penetration on network protocols, cryptographic attacks, post-exploitation on Windows/Linux, escaping restrictive environments, developing Python-based penetration tools, fuzz testing, PE and ELF file formats, writing 32-bit shellcode for Linux and Windows, Linux 32-bit buffer overflows and protection bypasses (NX, ASLR, Canary, etc.), Linux 64-bit buffer overflows (though this section is brief), and Windows 32-bit buffer overflows and protection bypasses (SEH, DEP, etc.). Overall, the course focuses primarily on advanced penetration testing and exploit development.

About The Exam

As mentioned earlier, the course itself does not include the exam voucher. If you want to obtain the certification, you need to purchase the exam voucher separately. After passing the exam, you will receive the GXPN certification. Now, without revealing specific exam questions, let's discuss some relevant details about the exam.

Exam Reservation

You can take the exam at an exam center or at home using specific proctoring software. I chose the latter this time, but the experience was disappointing and frustrating. Even though it was a proctored exam, the GXPN exam experience was much worse than Offsec's. I believe the negative experience was mainly due to the unprofessional and inexperienced proctor. The registration process alone took nearly an hour.

In addition, when I had 5 questions left to complete the exam, I encountered connectivity issues despite my home internet being stable. This forced me to go through the registration process a

second time. The second proctor was also not very experienced, and they repeated the same ineffective procedures multiple times, which made the situation even more frustrating.

Exam Format

The exam consists of 60 multiple-choice questions, with 55 questions requiring selections based on the given descriptions and 5 questions being hands-on tasks. For the hands-on questions, you perform actions in a VM accessed via the web interface and select the correct answer based on the information obtained.

Although the exam is in multiple-choice format, it requires a high level of practical skills and a deep understanding of the course material. Initially, I underestimated the exam, thinking it would be straightforward due to the format, but once I started, I found myself sweating a bit. The final 5 hands-on questions were not particularly difficult, and unlike the OSED exam, they didn't require writing out a full exploit chain or an automated script.

Exam Format

- 1 proctored exam
- 60 questions
- 3 hours
- Minimum passing score of 67%

The exam is open book, but you are only allowed to refer to the books and paper notes you bring. You cannot use a phone, web searches, or any other online resources. Most of the answers can be found in the course materials, so it's crucial to quickly analyze the key concepts being tested and locate the relevant information in the textbooks. The questions contain plenty of traps and rabbit holes, making them quite tricky, and there aren't many straightforward, easy points where you can immediately identify the correct answer.

The exam duration is 3 hours, which is more than enough time. In both the two practice tests and the final exam, I finished in about 1.5 hours.

Passing Standard

To pass the exam, you need a score of 67%, meaning you must answer two-thirds of the questions correctly. After finishing the exam, you'll immediately know whether you passed. In the practice tests mentioned below, you get feedback on whether your answers are correct after each question, but in the actual exam, there is no indication of whether your answers are right or wrong.

Practice Test

When you purchase the exam voucher, it includes two practice tests. Apart from the lack of proctoring and the immediate feedback on whether your answers are correct, the practice tests are identical to the real exam. These two practice tests may contain overlapping questions, as they

both come from the same question pool. Therefore, after completing the two practice tests, it's not recommended to purchase additional practice tests.

While the official statement says that the questions from the practice tests won't appear in the actual exam, strictly speaking, this is true. However, there are quite a few questions that follow the same logic, with only different numbers. So, completing the two practice tests is definitely helpful for the actual exam. In terms of difficulty, they are similar. My exam score ended up being between my two practice test scores.

One important note: After finishing the practice tests, you won't be able to review the incorrect questions, so it's crucial to immediately record any mistakes or areas of weakness as you go through the practice tests.

Exam	Certification	Status	
GXPN Exam - ID	GIAC Exploit Researcher and Advanced Penetration Tester	✔ PASSED	Exam Summary
GXPN Exam - ID	GIAC Exploit Researcher and Advanced Penetration Tester	✔ PASSED	Exam Summary

Comparison with OSED

Although SEC660 includes exploit development, its scope extends beyond that. However, to make a fair comparison, I will focus only on the exploit development aspect.

SEC660 covers a broader range of topics compared to OSED, such as Linux 32-bit shellcoding, buffer overflows on Linux, the ELF file format, and more. However, OSED dives deeper into the case studies of vulnerabilities, and the challenges are more difficult. In terms of the exam, OSED is also more challenging.

If you have already passed OSED, studying SEC660 would be relatively easy. But at the same time, improvement in your skillset would be limited.

Final Review

Since I had already passed OSEP and OSED before studying SEC660, I found SEC660 relatively easy, but this also meant that my improvement was somewhat limited. I initially thought that GXPN would cover 64-bit Windows buffer overflows and bypass techniques beyond SEH/DEP/ASLR, but these were not included. Below are the pros and cons based on my personal experience.

Pros

- Aside from the cost-effectiveness, the content and quality of SEC660 are excellent. The explanations are detailed, and there's a large amount of material to absorb.
- The knowledge is comprehensive, and in the area of exploit development, it covers more ground than OSED.
- This course isn't for beginners; most participants likely have some CTF experience. However, if you do not have prior CTF experience, completing this course will give you hands-on knowledge in various areas.

Cons

- Some of the content is somewhat outdated or not frequently used in real-world work.
- The at-home exam experience was extremely poor. If I were to take it again, I'd definitely opt to take the exam at an exam center instead.

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>		
8	XPC Attacks (Apple Silicon)		December 04, 2024	<div><div></div></div>		
9	Function Hooking on macOS (Apple Silicon)		-	<div><div></div></div>	<div><div></div></div>	
10	The macOS Sandbox (Apple Silicon)		November 27, 2024	<div><div></div></div>		
11	Bypassing Transparency, Consent, and Control (Privacy) (Apple Silicon)		November 28, 2024	<div><div></div></div>		
12	GateKeeper Internals (Apple Silicon)		November 26, 2024	<div><div></div></div>		
13	Symlink and Hardlink Attacks (Apple Silicon)		November 27, 2024	<div><div></div></div>		
14	Injecting Code into Electron Applications (Apple Silicon)		November 26, 2024	<div><div></div></div>		
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

OSMR 4 80 70 2 30 2 10

2 30 47 45 + 24

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

Diagram illustrating the structure of a 64-bit instruction format:

- 4 bits (Opcode)
- 10 bits (Register)
- 2 bits (Shift)
- 32 bits (OSMR)
- 16 bits (Offsec)
- 16 bits (CVE)
- 2 bits (Exploit)

Mac

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

[illegible]

14

☐ OSMR ☐ OSED ☒ EXP

--	--	--	--

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

总结

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

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.



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



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.

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"/>

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.**



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 🗨️

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.