SEC660/GXPN Review And The Comparison With OSED

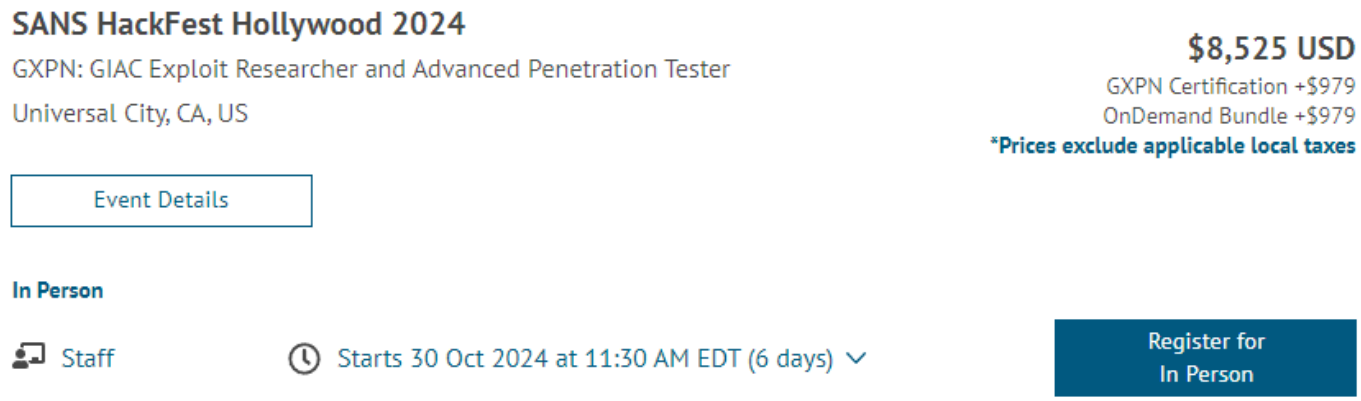
Hi folks, it's been quite a while since I last wrote review on training courses and certifications, even after passing OSCE3. In the past few days, I passed the GXPN exam, which is the certification exam of the SEC660 course. Since this was my first experience with a SANS course and a GIAC certification,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



GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	USD 979.00	1	**USD 979.00**

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.

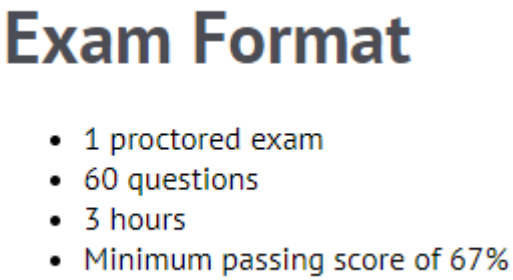
In addition, when I had 5 questions left to complete the exam, I encountered connectivity issues despite my home internet being stable. This forced me to go through the registration process a second time. The second proctor was also not very experienced, and they repeated the same

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.



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.



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.

Revision #4
Created 2024-09-18 18:47:28 UTC by winslow
Updated 2024-09-18 19:10:46 UTC by winslow