SAN660以及 GXPN 感受与心得，以及与 OSED 的对比

说起来，已经挺久没有写关于培训课程与认证的心得了，即便是通过 OSCE3 之后。在过去几天，我通过了 SEC660 课程所对应的认证 GXPN 的考试，因为我也是第一次接触 SANS 的课程与 GIAC 的认证，因此发表一些心得与感受，以及与 OSED 的对比。

课程基本信息

SEC660 (https://www.sans.org/cyber-security-courses/advanced-penetration-testing-exploits-ethical-hacking/)是 SANS 提供的高级渗透测试以及漏洞利用开发方向的课程，而 GXPN (https://www.giac.org/certifications/exploit-researcher-advanced-penetration-tester-gxpn/) 是 GIAC 提供的针对 SEC660 课程的认证。

价格

不包括考试凭证，单课程本身就 8500+ 美元，而考试凭证 979 美元。课程加上考试凭证，最终总计接近 10000 美元，十分感谢单位的报销，如果是个人购买，绝对不推荐的。

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

课程形式

根据排期现场上课，或者根据自己节奏自学，但价格几乎一致。报名后，SANS 会邮寄超过 1200 页的纸质教材，可以从网上下载 PDF 版本教材，访问在线 Lab，下载可本地部署的 VM 镜像等。我选择的是根据自己节奏自学，但现在看来会觉得现场上课更有氛围感。教材与 Lab 资源可以访问 4 个月。

知识领域

课程覆盖的知识领域还是很宽广的，内容很充足，量大管饱。有对网络协议的攻击与渗透，密码学攻击，Windows/Linux 后利用，限制性环境逃逸，基于 Python 的渗透工具开发，FUZZ 测试，PE 与 ELF 文件格式，32位 Linux 与 Windows 的 shellcode编写，Linux 32 位缓冲区溢出以及防护绕过(NX,ASLR,Canary等)，Linux 64 位缓冲区溢出 (篇幅不长)，Windows 32 位缓冲区溢出以及防护绕过(SEH,DEP等) 等。总的来说，主要是围绕着高级渗透测试与漏洞利用开发领域。

考试基本信息

上文所说，课程本身不包括考试凭证，如果想要获得认证，需要额外购买考试凭证，通过后方可获得 GXPN 认证。接下来，在不泄露具体考题的情况下说一下考试的相关事项。

考试预约

可以去线下的考试中心参与考试，或者在家使用特定的监考软件进行。这次，我选择的后者，但体验很令人失望和沮丧。同样是有监考的考试，GXPN 的考试体验比 Offsec 的考试体验还差得多。我觉得这次负面体验主要源于不够专业和熟练的监考官，他让考生注册阶段维持了接近一个小时。除此之外，还有 5 题结束考试的时候，在我自家网络没有问题的情况下，我遭遇了考试连接问题，被迫进行了第 2 次考生注册，第二个监考官也不是很熟练和专业，相同且无用的操作进行了多次。

考试形式

考试包含 60 题单选题，其中 55 题根据题目描述进行选择，5 题在网页端访问的 VM 上操作并得到要求的信息后进行选择，即操作题。虽然考试是选择题的形式，但实操性以及对课程内容的理解程度要求还是挺高的。我本想着这是选择题形式的考试，一开始有些轻视，但实际做起来发现有些汗流浃背。最后 5 题操作题不难，不需要像 OSED 那样写完整利用过程和一键脚本。

Exam Format

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

考试是开卷考试，但只能查阅携带的书本和纸面笔记，不能使用手机或者网页搜索等方式查询资料。大部分题目的答案可以在书中找到，所以一定要快速分析题目的考察知识点，以及出自教材的位置。题目的陷阱和兔子洞挺多，比较棘手，且没有很多能一眼看出答案的送分题。

过关标准

考试得分 67% 过关，即答对 2/3 的题目，考完就知道是否通过。在下文提到的模拟练习中，解答完一道题目就知道是否正确，但考试不会暗示你回答的正确与否。

模拟题

购买考试凭证附赠 2 套模拟练习，除了没有监考，以及实时告知考生解答的正确与否，其他与考试一模一样。这 2 次模拟练习可能会有重合的题目，均来自于题库，所以做完这 2 套后不建议额外购买模拟练习机会。官方声称模拟题中的题目不会出现在考试里，严格来说确实没有，但有不少解题思路一致但仅有数字不同的题目，所以做完 2 套模拟练习对考试肯定有帮助。至于难度，也是差不多。我的考试成绩介于 2 次模拟练习的成绩之间。

需要注意的是，模拟练习做完之后无法查看与回顾错题，所以遇到错题之后需要立即记录自己失误和薄弱的地方。

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

与 OSED 对比

SEC 660
虽然包含了漏洞利用开发方向，但覆盖知识不止于此。不过为了公平对比，这里只讨论就漏洞利用开发方向。

SEC 660 比 OSED 包括的内容更宽广，例如 Linux 32 位 shellcoding，Linux 下的缓冲区溢出， elf 文件格式等。但 OSED 在漏洞的案例的研究上更加深入，难度也更高。考试的话，也是 OSED
更难。如果已经通过了 OSED，再去学习 SEC660 会比较轻松，或者说提升比较有限。

个人评价

因为我在学习 SEC660 之前已经通过了 OSEP 与 OSED，所以学习 SEC660
课程还是比较轻松的，但这也意味着提升比较有限。我之前以为 GXPN 会包含 64 位的 Windows
缓冲区溢出，以及对 SEH/DEP/ASLR
之外的保护绕过技术，但实际上并没有涉及。以下是个人认为的优点与缺点。

优点

1. 除去性价比外， SEC660 的内容和品质真的很不错，讲解详细，内容量大管饱。
2. 知识比较全面，而且就漏洞利用开发方向，比 OSED 更广。
3. 这门课程不是面对新手的，或者说参与这门课的老手多多少少已经有过 CTF 经历。但如果先前没有 CTF 经历，学完这门课能直接上手一些方向。

缺点

1. 部分内容有些过时，或者在实际工作中没怎么用到过。
2. 就居家考试的体验而言，非常非常非常差。如果有下次，我还是去考试中心参加考试好了。

Revision #3
Created 2024-09-18 04:25:42 UTC by winslow Updated 2024-09-18 18:46:15 UTC by winslow