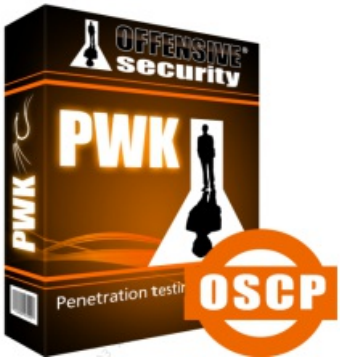
OSCP历程

原创

c2hhZG93 于 2021-12-08 00:12:22 发布 278 收藏 2
分类专栏： OSCP 文章标签： 安全

本文链接：https://blog.csdn.net/qq_34935231/article/details/121781213



Dear [redacted]

We are happy to inform you that you have successfully completed the Penetration Testing with Kali Linux certification exam and have obtained your Offensive Security Certified Professional (OSCP) certification.

Listed below is your name as it will appear on your printed certification. If any changes are required, please let us know right away at orders@offensive-security.com.

Message from Offensive Security

Thank you for verifying your delivery information. Your information has been successfully recorded and your certification will be shipped via DHL courier to the address provided.

Congratulations on achieving your certification!

Sincerely,

The Offensive Security Team

今天1点40，我收到了offensive发的邮件，通知我通过了oscp考试！现在总结下吧。

1、笔记很重要，教材一定要看，很多细节都在教材里面，遇到新知识一定要记笔记，每做一台靶机，之后一定要写报告，把你渗透的过程，思路，记录下来。因为当时你觉得可能记住了，但是做了几十台到考试前时候你发现什么都记不住，这时候就需要过一遍你的靶机writeup来回忆相关知识点。

2、官方靶机如果遇到不会的，没头绪的，可以上论坛，看看别人是怎么说的。如果一台靶机做了一天还是一点进展都没有，那就下一台吧，可能现在的知识点或者能力不足，需要继续提升一下再回来做。

3、bof一定要理解原理，badchars是考点，不过官方在12月2日发布，oscp考试要改革了，之前的25+25+20+20+10分的组合变成了20+20+20+40（域渗透），相对来说更难了，现在预约基本约不到了。

下面我来说说考试的经历：

我预约的是17点考试，因为当时我预约时候12月竟然5号之后全满了，17点也不错。请了2天假，第一天看看笔记，给kali做个快照备份下，第二天早上又把教材上的bof做了一遍，到了中午就开始紧张了，什么书都看不下去，在屋里转圈圈。终于熬到了考试前30分钟，我连上了监考系统。监考系统上面写着15分钟的时候登陆，但是提前30分钟就已经可以连上了。输入官方给你的os id与md5登陆监考系统，然后系统会测试你的摄像头功能，没问题的话浏览器会弹出一个插件，让你安装，这个是用来共享屏幕用的。官方推荐google浏览器。全部准备就绪后，监考会在聊天框里跟你说话，首先让你提供身份证件，拿护照给他看就行。记得在电脑里面存一张你护照的图片，如果摄像头看不清，监考会让你提供图片。核实完身份接下来监考会让你用摄像头照屋子的每个角落，任何电子产品都不要放在跟你一个屋子里，查完没问题了如果考试没开始他会让你等着，等到正式考试开始，收到exam的vpn，监考还有会让你执行trouble那个脚本，然后把生成的log复制粘贴进聊天框，然后就可以开始考试了。

我这边首先为了节约时间，除了bof那台机器，其他四台全部开启nmap扫描。然后开始做bof。这里面有个小插曲，因为第一次考试我也不知道，bof是有2台机器的，一台是调试机，一台是正式机，你可以在调试机里面编写你的bof脚本，但最后一定要攻击正式机来获得proof.txt，我傻傻的在调试机里面照proof找了40分钟。。。一个小时零20分钟，我完成了bof，然后看10分的题，20分钟搞定，当时还是比较开心的，然后做20分的题。web漏洞我很确定是哪个，但是就是无法反弹shell，我真的是把所有反弹shell的方式全都试了，就是无法反弹。后来休息了一下，好好想想会不会是防火墙或者网络策略限制了端口呢？于是我把反弹shell的端口改成了服务的端口，终于弹回来了。提权没什么难度，这台机器化了4小时。跟监考说了下，休息吃了点东西，回来继续干剩下那台20分的，上来我就掉rabbit hole里面去了，搞了半小时发现web根本打不进去，转换思路查看别的端口，终于发现了真正的漏洞，是文件共享的，成功得到ssh用户名密码，成功拿到local.txt，提权是内核提权，不多说了。打通了4台靶机，我花了7.5小时，拿到了25+20+20+10=75分，已经过了。但是网上好多人都是lab分数够，但是报告扣分导致没过，当时已经12点半了，直接睡了。

第二天早上起来，开始干那台25分的机器，没错，我又掉进rabbit hole里面去了，2个web service，花了4小时走了错误的路，发现实在攻不进去，意识到可能是漏洞错了，重新枚举，记住，官方的try harder不是让你在同一个地方一直尝试，而是多换角度去尝试，可以理解为try emun。最后终于在另一个web上发现了sql注入漏洞，查出用户名与密码，然后登陆web后台，上传木马，成功反弹shell，这时候已经7小时过去了，还有1小时就结束了，我决定不往下做了，检查了一下报告截图，提交了考试。最后我预估拿到了75+12.5=87.5分

休息了一下，开始写报告，趁热打铁，我采用的是官方报告模板，但是官方模板里面有很多没用的可以删掉哈，还有官方模板里面的人名是john，要改成你自己。

不得不说，官方现在评分速度也很快啊，2天就给我发了邮件，通知我考试过了，心里还是开心的但是没那么激动，700+小时的学习和练习，终于得到了回报。

哈哈，接下来计划是osep，加油吧，try harder！！！