登录

OSCP经验分享

happytree / 2017-11-15 13:11:00 / 浏览数 29702 技术文章 技术文章 顶(6) 踩(0)

一、OSCP简介

安全技术类的证书有很多，像是CEH, Security+, CISSP等等。除了众多侧重于笔试的安全认证，OSCP(Offensive Security Certified Professional)是为数不多得到国际认可的安全实战类认证。

> OSCP认证，是一个专门针对Kali Linux渗透测试培训课程的专业认证。该认证机构声称，OSCP认证是一个区别于所有其它认证的考试，考试全程采取手动操作的方式，而不设笔试环节。
> 认证条件：无
> 考试：OSCP的认证考试也是另类的存在，考生拥有24小时的时间（实际是23小时45分钟）去完成考试，具体如何分配时间由考生自己决定。题目是5台主机（随机抽取
> 考试费用约为：$ 800 美元（30天实验室访问+认证）
> 相关链接：
> 概述
> 培训材料

CISSP每年需要提交教育学分，考试费用、年度维护费也比较高。OSCP认证是长期有效的。考一个还算是比较值得的。
博主也说明一点，拥有OSCP证书不代表你具备多么高超的渗透测试能力或经验。但是通过OSCP培训，确实可以给你建立出比较清晰的渗透测试思维。■■■■■■■这套渗透测试方法论，是公开的，博主确实也看到很多从业多年的渗透测试人员，有自己总结的一套方法论。比如可以参考《Penetration Testing》这本书:https://book.douban.com/subject/25883745/

所以这个证书或培训，主要还是看个人的需要啦。

二、经验分享

1、关于OSCP

- OSCP认证阶段分为：线上培训Lab■■、线上考试Exam■■（2个阶段 / 环境）
- 官网是https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/
- 参加OSCP认证，必须参加他们的线上课程。详情可见线上课程大纲：https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf
  线上课程Lab■■按天数分为3种（最小是30天）
  - Course + 30 days lab（有保持渗透测试训练的安全人员，可以考虑买最少的，毕竟价格还是很贵的）
  - Course + 60 days lab
  - Course + 90 days lab
- 如果你不是很有把握必过的话，30天Lab环境是不够做完练习题、10台Lab机器报告、50多台Lab环境机器提权的。
- 官网价格表：https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/ 搜“OSCP COST”
- 培训资料
  - PDF
    - 大纲：https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf
    - 里面有练习题
  - Video
  - Lab环境
    - 分为4个子网（Public、Development、IT、Admin）
    - 一开始学生是进入的与Public连通的Student网络
    - Lab环境是学员共用的，所以大家的操作会有很小的影响，至少博主没有遇到什么很不文明的行为
    - 50多台主机，有些主机可能拥有多个网卡（会有不同的用处哦～）
    - 学生目标是尽可能取得所有主机上的root/system权限
    - 攻击路径思路，其实比较自由，可能多条路径拿到root/system权限。时间足够的话，可以尝试多条路径。（但是价格太贵了，感兴趣的可以到后面博主提到的模
  - Exam环境（大约2天时间完成）
    - 5台主机（目标23小时45分攻破）
    - ■■■■■■■■■■■■■■■■■■■■■■■■■■■■0■■（重考又要交钱，仔细点省点钱哈）
    - 24小时完成一份英文报告
    - 考试成绩是实战Got Proof File，加上■■■■■■■■■■■■■■■■■■■■■■■■■。总共达到70分以上算通过
  - Forum & IRC
    - 上面会有一些小小的提示，Lab环境有一些机器比较难，博主看了下其他学员的对话，才找到思路。
    - 看他们的对话，感觉他们都好可爱。有些没有思路在上面询问的，有些有思路了在那儿Dance Dance的。
    - 另外一个很重要的一点建议，最好可以先看下论坛里面官方提供的一台机器的教学帖子。思路、方法、工具，写的非常详细，而且还用多种方式进行攻击，算是做of 100的样板吧。（不过在Lab环境里面，金钱和时间上都不允许这么做啊，有兴趣的可以到博主后面提到的模拟练习环境玩）
  - Revert

    - 先回滚再进行攻击，以免其他学员的操作影响到你。
    - 每天有8次回滚主机的机会，博主只遇到1、2台机器回滚次数不够用。其实也可以换一台主机玩，不用死磕那台。
    - Exam环境可以无限revert，自己的独立环境不受其他学员影响
  - Proof.txt V.S. network-secret.txt
    - Proof.txt是奖励或证明文件
    - network-secret.txt是开启下一个网段的钥匙

2、模拟练习平台

```
Key Takeaway
```
OSCP
Lab环境价格太高了，下面推荐几个免费的跟Lab环境类似的练习平台。这样很久没做渗透测试的同学，也可以找找感觉先。直接去Lab环境下找感觉，这有点太奢侈了。。。

- 模拟练习平台（跟Lab环境类似）
  - vulnhub：https://www.vulnhub.com/
  - hackthebox：https://www.hackthebox.eu/
  - pentestit：https://lab.pentestit.ru/
- 专题练习平台（对某一种类型的漏洞或技术做专项训练）
  - Root Me：https://www.root-me.org/（官网提供的资料超级好，建议多看看）
- 不过自己在练习平台上练习的话，会有一个问题，就是时间上控制不好。容易在某个问题里陷进去，然后时间就过去了。

3、相关书籍

- 《Penetration Testing》:https://book.douban.com/subject/25883745/

4、考试必备

- https://www.google.com
- OSCP常用cheatsheet（几乎OSCP里面常用的命令在这里都可以找到）
  - https://github.com/frizb/OSCP-Survival-Guide
- Linux提权
  - Linux提权指南
    - https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
  - Linux提权辅助脚本
    - https://www.securitysift.com/download/linuxprivchecker.py
    - https://github.com/HappyTreeFriend/linux-exploit-suggester
  - LinuxExploits
    - https://github.com/HappyTreeFriend/kernel-exploits
- Windows提取
  - Windows提权指南
    - http://www.fuzzysecurity.com/tutorials/16.html
  - Windows提权辅助脚本
    - https://github.com/pentestmonkey/windows-privesc-check
  - WindowsExploits
    - https://github.com/abatchy17/WindowsExploits

三、个人历程

博主参加了10月份为期30天的培训，预约到了11月初的考试。
考完试很快就收到了邮件反馈。

1、培训前

7月-9月的时间，陆陆续续有在Root
Me、vulnhub上练习。特别在root-me上刷题的时候，多总结文章，考完OSCP，博主还想继续保持在rootme上刷题，真的很有帮助。

2、Lab进行中

- 一开始是打算把练习题和Lab环境报告写了的，因为可以在考试成绩上挣5分。
- 不过最后时间实在是不够了，如果你不是很有把握必过的话，30天Lab环境是不够做完练习题、10台Lab机器报告、50多台Lab环境提权的。而且还需要一些时间做总结
  - 最后博主Lab环境只剩2台admin机器的本地提权没做完，临Lab到期那天晚上本来博主准备再刷完的，可惜跟另外一个更紧急的事有时间冲突。
  - 做完了全部的练习题，但是没有写10台Lab机器的报告。临近考试前，写了1台机器的报告当练习。
- 当时在网上看别人的经验总结，说Public网段的humble、pain、sufferance三台机器很难。所以这三台机器是留到最后来做的，但出乎意料的是humble、sufferance、
- Stuck的时候，多google、多逛逛论坛、看看PDF、做做练习题。

- 有些机器暂时没有任何思路，有可能是需要结合其他机器上的信息。Lab环境有很多机器之间是有联系的，hostname为什么叫这个，网段名叫Public、Dev、IT、Admin
  - 特别是内网的机器上，很多需要依赖信息搜集，才能攻破的机器。
- 博主那段时间，经常都是2、3点才睡觉，经常都是思路来了，就想马上验证。但是觉得那样不好咯，因为不够清醒，可能会忽略掉一些信息。有思路了，记下来，睡个好

3、Exam环境考试

- 考试前，好怕报告被扣分，毕竟博主从来没写过英文报告。所以把Lab环境中找了一台机器写报告。其实OSCP的英文报告要求比起工作中的渗透测试报告要求简单多了。
  - 不过博主的英文报告的用词，肯定还是不够好的，这点博主是有自知之明的。所以OSCP真的只是博主的一个开始。
- 实战时间是23小时45分钟，目标是拿到5台机器的root/system权限
  - 机器总共是5台（2台25分、2台20分、1台10分）。
  - 最后博主只完成了4台的，加最后1台的有限的普通用户权限。
  - 考试这里还是时间的问题，其实考试的题目比Lab环境的要简单一些，思路都很明显。可能官方还是考虑到时间会不够的问题。
  - 考试时，如果你不确定这是5台中唯一会使用到metasploit的机器，最好不要对这个台机器使用MSF。因为官方只允许使用MSF在1台机器上。
  - 博主考试的时候，MSF的机会，用了1台机器，主要是因为时间快不够了。
- 时间安排
  - 博主因为是下午4点开始的考试，一开始时间还不紧迫。睡觉前搞定了一台10分和一台25分的机器，晚上还睡了个美容觉，结果第二天时间就有点紧张了。
  - 做完一台20分的题，还剩一台20分和一台25分的题。
    - 后面时间有点不够，剩下那台20分的就用的MSF。
    - 25分那题确定了只能手工搞，最后的时间就基本在手工测这台25分的机器。很遗憾不够时间做完。
  - 建议考前可以在vulhub上找一些机器预估一下自己的时间。
- 所以最后实战考试是做到了75分，不过我写报告的时候，也把最后那台的进展写上去了。

四、难易程度

- 总体来说，还是属于演练的难度，故意放上有漏洞的机器。除了有几台是故意搞了一些rabbit hole，还有一些有点脑洞（像是CTF那种题）。
- 难度不算太大，适合做训练。除了一些rabbit hole题、脑洞题，可能不太适合作为训练题。
- 难的机器基本都在Public网段，内网的机器很多都是靠信息搜集。
- OSCP的题目，是偏漏洞利用的，几乎不需要做太多编程、漏洞挖掘。
- 只能说一句，比起很多CTF比赛的题目，OSCP真的是太简单了。这可能也是跟定位有关，主要就是以培训、模拟渗透测试环境为目的。

五、其他建议

- 中国有很多类似OSCP的认证，形式、内容都差不多的结构，不过可能在国际上的认可度，还没像OSCP这样。所以看自己的需要吧。
- OSCP认证价格略贵，不太适合学生。学生党，多参加CTF、学校 / 公司的安全比赛，或者到我前面提到的"模拟练习平台"上做练习，性价比更高。当然如果你真的需要这
- OSCP资料全是英文的，单纯从学习、吸收效果上来看，对于英语不够好的同志来说是有点信息丢失的。光是从培训效果上来说，花了那么多钱，却丢失了信息，有点划不
- ■■■■■■■■■■■■■■■■■■■■■■■

上一篇：【酸爽系列CTF】（一）拿到Fla... 下一篇：高效Macbook工作环境配置

1. 14 条回复


hades 2017-11-15 13:36:28

@happytree 很贵很值得 O(∩_∩)O哈哈~

1 回复Ta


hades 2017-11-23 15:55:04

补充一些信息：

https://leonjza.github.io/blog/2014/11/22/trying-harder-oscp-and-me/

0 回复Ta


hades 2017-11-23 16:23:58

关于教材

300多页的教材涵盖了所有从基础知识到进阶的渗透测试技巧（当然不是深入）。所以对于没有渗透经验的朋友（但还是需要基本计算机和网络的知识，如果有编程基础

关于PWK Labs

相对于其他认证课程来说，OSCP与众不同也是最吸引人的是它设计详实的Online Lab（包括4个子网，57台主机/服务器，每一台主机/服务器都包含Offensive Security团队在真实工作环境中遇到的漏洞）。我的起点是VPN连接到Public Network中的一台主机，终点是渗透进入到Admin Network。
57台设备（除掉网关/防火墙）都是目标，都存在漏洞可以被攻破并获得最高权限。所以获取所有设备的最高权限（ROOT/SYSTEM）并读取证明文件（proof.txt或者ne
HARDER"是整个课程的标语。每攻破一个主机，都需要在后边自主的学习，查资料，有时还需要灵光一闪的运气。更难得的是，lab里边50多台主机服务器不是独立无关
forwarding）和Pivoting（实在不会翻译，类似于利用跳板进入不可路由网络）。

关于考试

OSCP的认证考试也是另类的存在，考生拥有24小时的时间（实际是23小时45分钟）去完成考试，具体如何分配时间由考生自己决定。题目是5台主机（随机抽取），目

我的经验

首先，虽然课程本身是没有门槛的，但是购买Lab机时还是不便宜的。对渗透了解的越少你所需要的时间就越多，所以我还是建议先对渗透测试有一定了解之后再选择这个
http://vulnhub.com/
https://www.pentesterlab.com/

下面就是我的120天学习经历

由于不知道水深水浅，一开始买了60天的Lab时间。拿到教材和视频之后，大概用了一周多的时间把教材和视频过完，并完成课后练习题（这个时间取决于你的基础有多

终于可以摩拳擦掌进入在线Lab了。我的起点是Public
Network里的一台电脑，利用课程里学到的知识对目标网络进行信息收集和枚举（enumeration）。Nmap是用的最多的工具之一。目标主机/服务器有着不同的难度，用
panel里解开不同的子网（IT, DEV and
Admin）。有些主机里还包含攻克其他主机的线索，所以对每台被攻破的主机都需要仔细检查一番，搜集尽可能多的线索。

很快的60天的Lab时间就用完了，我只拿下了30几台主机并解锁了2个子网（IT和DEV）。我显然还没有准备好考试，于是又续了30天的Lab。这30天里剩下的都是一些硬

我约的考试是从周五晚上7点开始，时长23小时45分钟。一共五台目标机器跟Lab里的一样包含已知漏洞。总分100分，70分过。

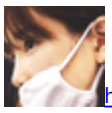
晚上8点27分，拿下第一台主机。 10点，第二台主机。 凌晨1点27分，第三台主机也被攻破。
然后一直到凌晨5点多，再没有建树。困得不行的我，决定小睡三小时，闹铃上到早上8点半起。截止到这时候，我只有50分。
8点半起来继续研究，终于10点52分，拿下第四台主机（我认为是最难的一台）。
这时已经拿到75分，可以过了。中午简单的吃了些午饭，回来继续最后一个主机。

又过了几个小时的网上搜索，修改和测试，终于在下午2点35分的时候攻破最后一台主机。这时我拿到了100分。在反复检查和做好所有截屏工作之后，我决定先去好好的
一觉睡到晚上9点多，起来写报告。因为只有五台主机，又有了之前Lab报告的经验，截屏和记录工作做的还不错，报告花了我大概2两个多小时就结束了。之后就是打包
:)

过了一天，收到了下边的邮件，写下了开头的那句话。

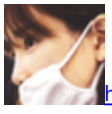
最后，感谢IRC里的admin们和所有聊过天，帮助过我的朋友

0 回复Ta

 hades 2017-11-24 14:18:39

https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf

0 回复Ta

 hades 2017-11-30 09:49:32

Given I have been working in information security for the past few years, I became well aware of the different certifications available as a means of professional development. The certification that stood out as gaining the most respect from the security community seemed to be the "(OSCP) Offensive Security Certified Professional" certificate, I witnessed this time and time again in conversations online. The reason often given is that it is a tough 24 hour practical exam vs a multiple choice questionnaire like many other security certificates. The OSCP is also listed regularly as a desirable requirement for many different kinds of infosec engineering jobs.

I recently received confirmation that I have successfully achieved this certification. To anyone interested in pursuing the OSCP, I would completely encourage it. There is no way you can come away from this experience without adding a few new tricks or tools to your security skills arsenal and aside from all of that, it's also very fun. This certificate will demonstrate to clients or to any potential employer that you have a good wide

understanding of penetration testing with a practical skill-set to back up the knowledge. I wanted to get this as I've had clients in the past not follow up on using my services due to me not having any official security certificates (especially CREST craving UK based customers). Hopefully this opens up some doors to new customers.

Before undertaking this course I already had a lot of experience performing vulnerability assessments and penetrations tests, I also had a few CVEs under my belt and have been quite active in the wider information security community by creating tools, taking part in bug bounties and being a fan of responsible disclosure in general. I found the challenge presented by this exam to be quite humbling and very much a worthwhile engagement.

I would describe the hacking with kali course materials and videos as very entry-level friendly which is perfect for someone with a keen interest looking to learn the basics of penetration testing. The most valuable part of the course for those already familiar with the basics is the interactive lab environment, this is an amazing experience and it's hard not to get excited thinking about it. There were moments of frustration and teeth-grinding but it was a very enjoyable way to sharpen skills and try out new techniques or tools.

I signed up for the course initially a full year ago while working full time on contracts and found it extremely difficult to find the time to work on the labs as I had multiple ongoing projects and was doing bug bounties quite actively too. I burnt out fairly quick and didn't concentrate on it at all. I did one or two of the "known to be hard" machines in the labs fairly easily which convinced me I was ready and sat the exam having compromised less than 10 of the lab hosts. This was of course silly and I only managed 2 roots and one local access shell which wasn't near enough points to pass and very much dulled my arrogance at the time. I didn't submit an exam report and decided to focus on my contracts and dedicate my time to the labs properly at a later date.

Fast forward over a year later to the start of this month (September) and I had 2 weeks free that I couldn't get contract work for. So I purchased a lab extension with the full intention of dedicating my time completely to obtaining this certificate. In the two weeks I got around 20 or so lab machines and set the date for my first real exam attempt. This went well but I didn't quite make it over the line. I rooted 3 machines and fell short of privilege escalating on a 4th windows host. I was so close and possibly could have passed if I did the lab report and exercises, however this time around I wasn't upset by the failure and became more determined than ever to keep trying. I booked another 2 weeks in the labs, focused on machines with manual windows privilege escalation and booked my next exam sitting, successfully nailing it.

As I had learned a lot of penetration testing skills doing bug bounties, I found that it was very easy to identify and gain remote access to the lab machines, I usually gained remote shell access within the first 20 or 30 minutes for the large majority of the attempted targets. I very quickly found out that my weakest area was local privilege escalation. During my contract engagements, it is a regular occurrence that my clients request I don't elevate any further with a remote code execution issue on a live production environment. This activity is also greatly discouraged in bug bounties so I can very much see why I didn't have much skill in this area. The OSCP lab environment taught me a large amount of techniques and different ways of accomplishing this. I feel I have massively skilled up with regard to privilege escalation on Linux or Windows hosts.

I'm very happy to join the ranks of the (OSCP) Offensive Security Certified Professionals and would like to thank anyone who helped me on this journey by providing me with links to quality material produced by the finest of hackers. Keeping the hacker knowledge sharing mantra in mind, below is a categorized list of very useful resources I have used during my journey to achieving certification. I hope these help you to overcome many obstacles by trying harder!

Mixed

https://www.nop.cat/nmapscans/
https://github.com/1N3/PrivEsc
https://github.com/xapax/oscp/blob/master/linux-template.md
https://github.com/xapax/oscp/blob/master/windows-template.md
https://github.com/slyth11907/Cheatsheets
https://github.com/erik1o6/oscp/
https://backdoorshell.gitbooks.io/oscp-useful-links/content/
https://highon.coffee/blog/lord-of-the-root-walkthrough/

MsfVenom

https://www.offensive-security.com/metasploit-unleashed/msfvenom/
https://netsec.ws/?p=331

Shell Escape Techniques

https://netsec.ws/?p=337
https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells
https://airnesstheman.blogspot.ca/2011/05/breaking-out-of-jail-restricted-shell.html
https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells

Pivoting

http://www.fuzzysecurity.com/tutorials/13.html
http://exploit.co.il/networking/ssh-tunneling/
https://www.sans.org/reading-room/whitepapers/testing/tunneling-pivoting-web-application-penetration-testing-36117
https://highon.coffee/blog/ssh-meterpreter-pivoting-techniques/
https://www.offensive-security.com/metasploit-unleashed/portfwd/

Linux Privilege Escalation

https://0x90909090.blogspot.ie/2015/07/no-one-expect-command-execution.html
https://resources.infosecinstitute.com/privilege-escalation-linux-live-examples/\#gref
https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
https://github.com/mzet-/linux-exploit-suggester
https://github.com/SecWiki/linux-kernel-exploits
https://highon.coffee/blog/linux-commands-cheat-sheet/
https://www.defensecode.com/public/DefenseCode_Unix_WildCards_Gone_Wild.txt
https://github.com/lucyoa/kernel-exploits
https://www.rebootuser.com/?p=1758
https://www.securitysift.com/download/linuxprivchecker.py
https://www.youtube.com/watch?v=1A7yJxh-fyc
https://www.youtube.com/watch?v=2NMB-pfCHT8
https://www.youtube.com/watch?v=dk2wsyFiosg
https://www.youtube.com/watch?v=MN3FH6Pyc_g
https://www.slideshare.net/nullthreat/fund-linux-priv-esc-wprotectionshttps://www.exploit-db.com/exploits/39166/https://www.exploit-db.com/exploits/1

Windows Privilege Escalation

https://blog.cobaltstrike.com/2014/03/20/user-account-control-what-penetration-testers-should-know/
https://github.com/foxglovesec/RottenPotato
https://github.com/GDSSecurity/Windows-Exploit-Suggester/blob/master/windows-exploit-suggester.py
https://github.com/pentestmonkey/windows-privesc-check
https://github.com/PowerShellMafia/PowerSploit
https://github.com/rmusser01/Infosec_Reference/blob/master/Draft/ATT%26CK-Stuff/Windows/Windows_Privilege_Escalation.md
https://github.com/SecWiki/windows-kernel-exploits
https://hackmag.com/security/elevating-privileges-to-administrative-and-further/
https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
https://toshellandback.com/2015/11/24/ms-priv-esc/
https://www.gracefulsecurity.com/privesc-unquoted-service-path/
https://www.commonexploits.com/unquoted-service-paths/
https://www.exploit-db.com/dll-hijacking-vulnerable-applications/
https://www.youtube.com/watch?v=kMG8IsCohHA&feature=youtu.be
https://www.youtube.com/watch?v=PC_iMqiuIRQ
https://www.youtube.com/watch?v=vqfC4gU0SnY
https://www.exumbraops.com/penetration-testing-102-windows-privilege-escalation-cheatsheet/X
https://www.fuzzysecurity.com/tutorials/16.html
http://www.labofapenetrationtester.com/2015/09/bypassing-uac-with-powershell.html

0 回复Ta


simeon 2017-12-06 22:28:05

收藏一下。不错

0 回复Ta


north 2017-12-20 16:59:50

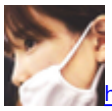
感谢分享

0 回复Ta

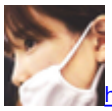

hades 2018-03-14 13:13:03

- Shellterlabs : Writing exploits - https://shellterlabs.com/en/training/get-started/writing-exploits/
- Shellter Hacking Express challenges - https://shellterlabs.com/en/contests/challenges/?event=10
- Windows BOF PCMan FTP - http://netsec.ws/?p=180
- Hack the box - http://hackthebox.eu
- Nishang : PowerShell scripts - https://github.com/samratashok/nishang
- Windows Privilege Escalation Fundamentals - http://www.fuzzysecurity.com/tutorials/16.html
- Basic Linux Privilege Escalation - https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- Pentest Tips and Tricks - https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/
- Nmap cheat sheet - https://highon.coffee/blog/nmap-cheat-sheet/
- SANS Institute : Port Knocking basics - https://www.sans.org/reading-room/whitepapers/sysadmin/port-knocking-basics-1634
- Teck_K2 OSCP review - https://teckk2.github.io/category/OSCP.html
- m4lv0id OSCP review - https://medium.com/@m4lv0id/and-i-did-oscp-589babbfea19
- The definitive hacking playlist - https://soundcloud.com/intrd/sets/hacking

0 回复Ta


hades 2018-03-14 13:13:40

0 回复Ta


hades 2018-03-14 13:14:28

- SPARTA - Network Infrastructure Penetration Testing: This is a python application which simplifies the scanning on the 1st enumeration phase. This tool was developed by a guy while taking the PWK course and it is a awesome time-saver that gives you a overview of the target.
- terminator - Like tmux, this tool allows you arranging terminals in grids. You can create more terminals by right clicking on one and choosing to split. This is very useful here, Its normal your screen will w/ 7+ running terminals. it vertically or horizontally.
- gliffy - Online diagramming tool alternative to MS Visio. This was very useful to illustrate some details of the network in the report.
- sshuttle - After understanding how dynamic tunneling and port forwarding works with SSH, try this tool. This is where transparent proxy meets VPN meets SSH. It will help you a lot on pivoting.
- enum.py - Scripted local linux wnumeration & privilege escalation checks. The real gem of this script is the recommended privilege escalation exploits given at the conclusion of the script. This is a great starting point for escalation.
- enum.sh - Alternative to above, useful when the machine has no Python installed.
- windows-privesc-check2 - This is standalone executable that runs on Windows systems. It tries to find misconfigurations that could allow local unprivileged users to escalate privileges to other users or to access local apps.
- shutter - The best linux feature-rich screenshot tool!

- nozzlr - Nozzlr is a multithread bruteforcer, trully modular and script-friendly. The other bruteforce tools are amazing, but the hardcoded parameters make it painful to script over complex tasks. Nozzlr comes to solve this problem. All your task parameters/engine is managed directly in the task template(a python script). This tool was developed by me, feel free to help me w/ this project!

0 回复Ta

60528****@qq.com 2018-07-13 01:07:14

请问连接pentestit：https://lab.pentestit.ru/ open * * n使用不了，不管是kali还是windows，一直在不断连接，这个您有遇到过么？

0 回复Ta

madneal 2019-03-02 17:24:43

感谢分享 有一个问题就是 oscp 的 lab 环境在国内可以直连么，因为像 hack the box 国内直连延迟太高了，很多操作都没法做

0 回复Ta


madneal 2019-03-02 17:26:46

@hades 想和你请教一下 有一个问题就是 oscp 的 lab 环境在国内可以直连么，因为像 hack the box 国内直连延迟太高了，很多操作都没法做

0 回复Ta


qd****@163.com 2019-11-01 12:48:42

国内有没有培训OSCP的机构？

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板