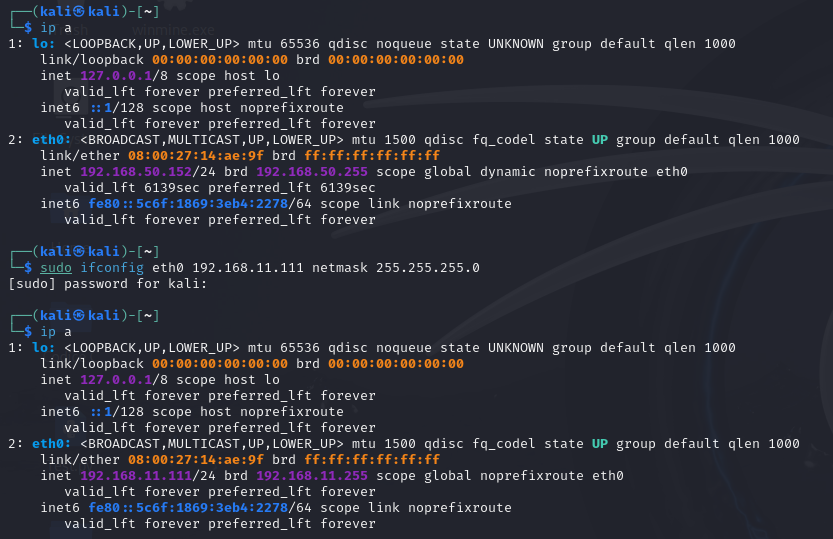
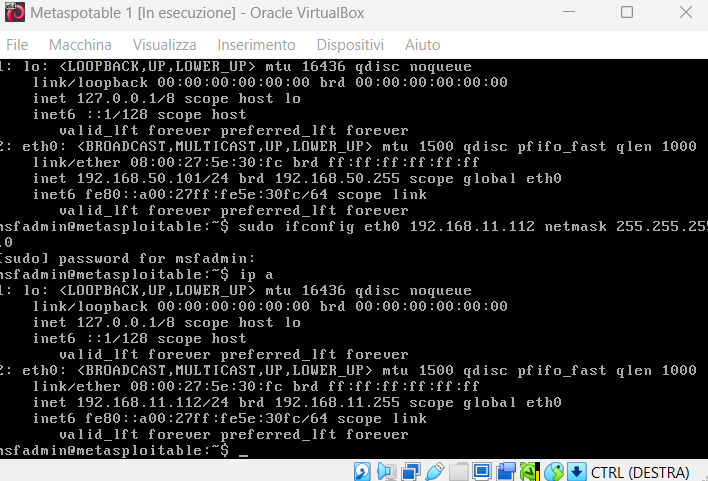
**Progetto Metasploitable:**

Sono partita cambiando gli indirizzi ip della mia macchina attaccante Kali in 192.168.11.111 e della macchina vittima Metasploitable in 192.168.11.112.  
  


Successivamente avvio msfconsole e ricerco il servizio **java\_rmi**

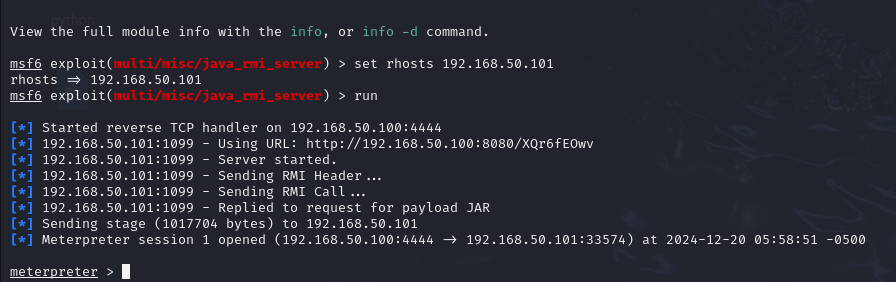
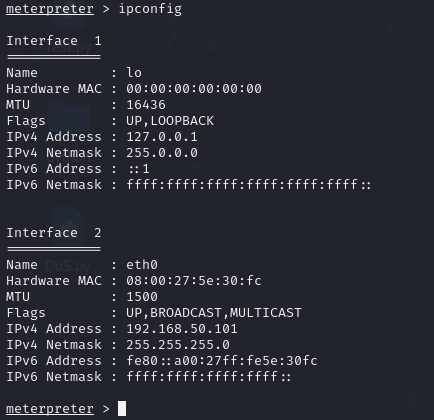


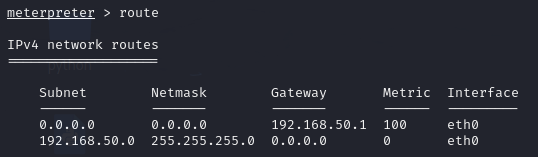
scelgo il payload **4** con **use 4** e con il comando **options** verifico le opzioni da settare.



Imposto solamente il parametro **rhosts** con l’ip della macchina vittima e mando l’exploit.

L’exploit è andato a buon fine, la sessione di **meterpreter** è avviata e sono all’interno della macchina vittima.

  
Come richiesto dalla traccia vado a verificare la configurazione della macchina vittima con il comando **ifconfig**, ed informazioni sulla tabella di routing con il comando **route**.  




Termino la sessione con il comando **exit** per uscire dalla macchina, il comando **bg** per lasciare la sessione di meterpreter in background ed **exit -y** per uscire da msfconsole.