ESERCIZIO: La nostra 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.

I requisiti dellʼesercizio sono:   
● 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:

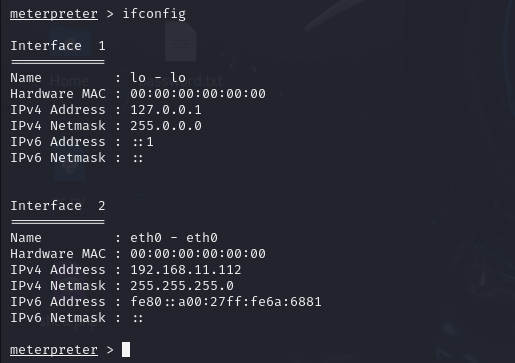
1) configurazione di rete.

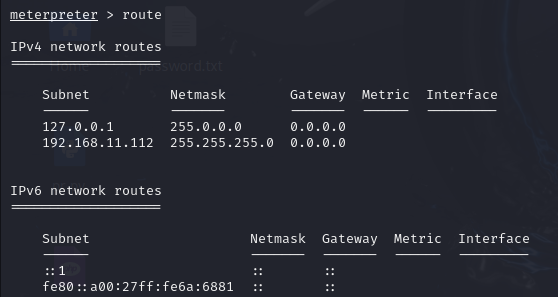
2) informazioni sulla tabella di routing della macchina vittima.

Sono entrato su meta col solito comando *msfconsole* e ho digitato *search java\_rmi*.

Ho avviato l’exploit dopo aver settato rhosts(192.168.11.112) e lhost(192.168.11.111).

una volta entrato su Meterpreter ho eseguito i due comandi richiesti per completare l’esercizio: *ifconfig* e *route*





IL servizio **Java-RMI**, attivo sulla porta 1099 TCP di Metasploit, è una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete. La vulnerabilità in questione è dovuta ad una configurazione errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

Un **exploit** è un pericoloso strumento, implementato in differenti modi, che consente di sfruttare le vulnerabilità hardware e software dei sistemi informatici per violarli e prenderne il controllo.

**Meterpreter** mette a disposizione degli script da utilizzare per recuperare determinati dati sul bersaglio. Gli script si utilizzano anteponendo al comando la keyword «run». Tra gli script più interessanti troviamo:

* **checkvm:** controlla se il target è una macchina virtuale oppure un sistema fisico.
* **getcountermeasure:** controlla le configurazioni di sicurezza sul target e può essere utilizzato anche per disabilitare misure di sicurezza come antivirus, firewall etc.
* **Get\_local\_subnet:** è utilizzato per recuperare la subnet mask della vittima.
* **killav:** può essere utilizzato per disabilitare la maggior parte degli antivirus che girano sulla macchina target.