**PROGETTO S7 L5**

**Traccia:**

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:

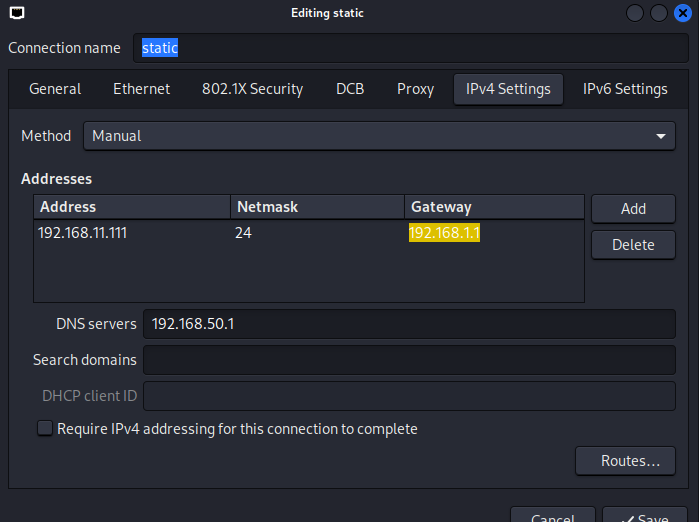
● La macchina attaccante (KALI) deve avere il seguente indirizzo IP 192.168.11.111

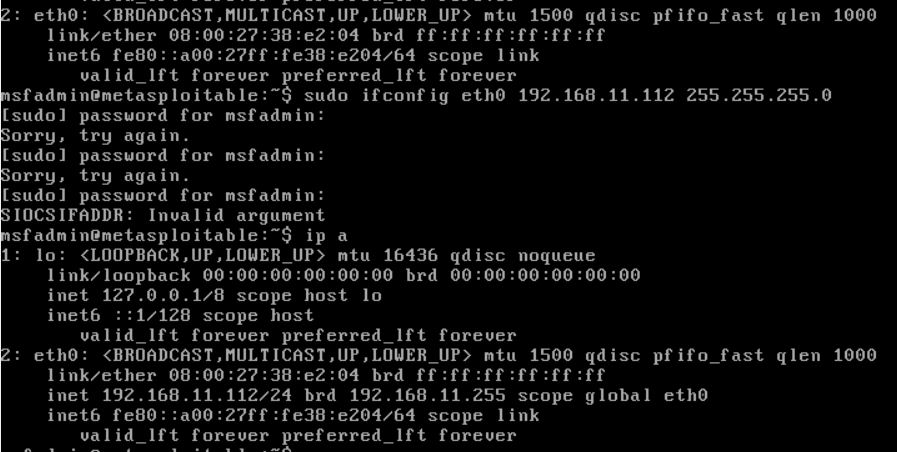
● La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP 192.168.11.112

● 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.

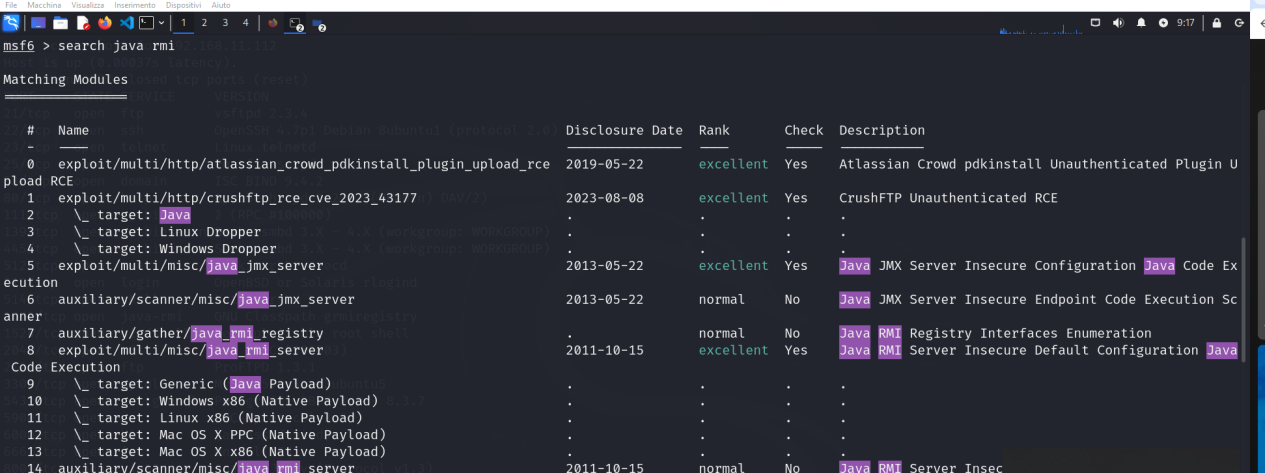
Per lo svolgimento dell’esercizio bisogna settare gli indirizzi IP delle due macchine (METASPLOITABLE e KALI) come indicato nella traccia:





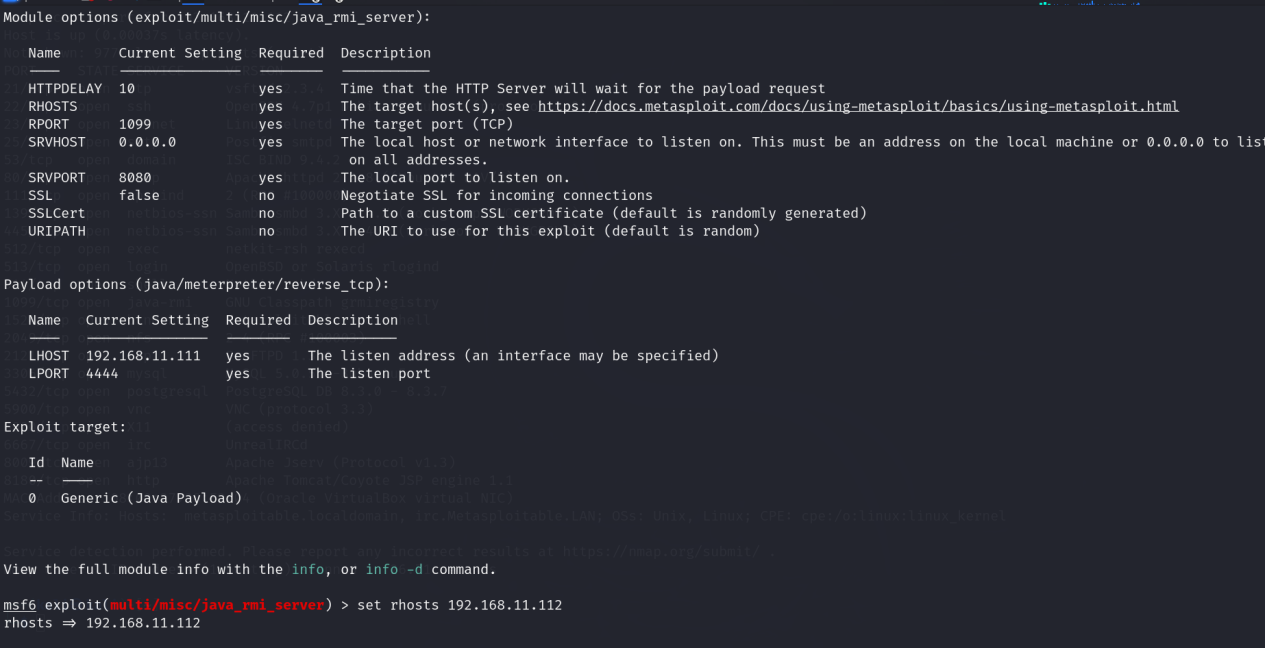
Una volta configurati i due indirizzi IP iniziamo a svolgere l’esercizio avviando il comando MSFCONSOLE.

Dopo aver avviato il comando bisogna cercare l’exploit adatto:

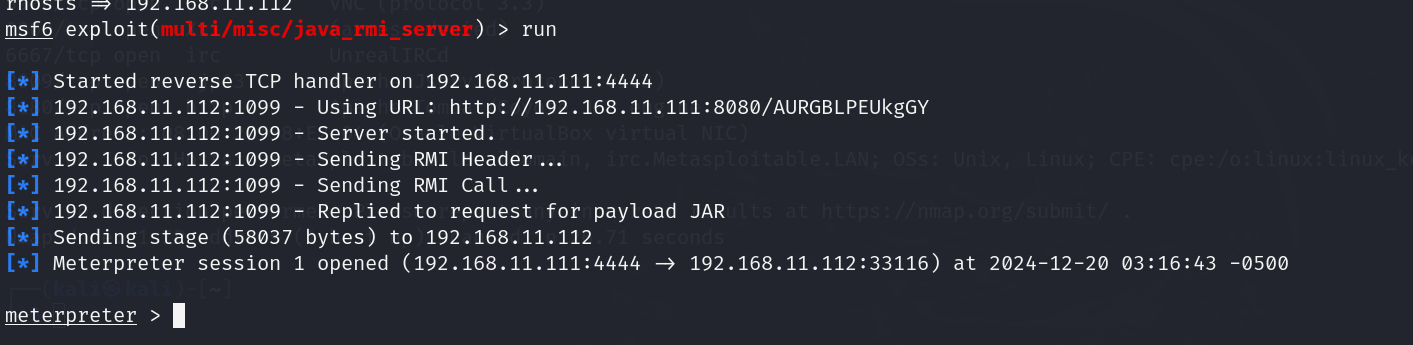


In questo caso è stato scelto il n° 8.

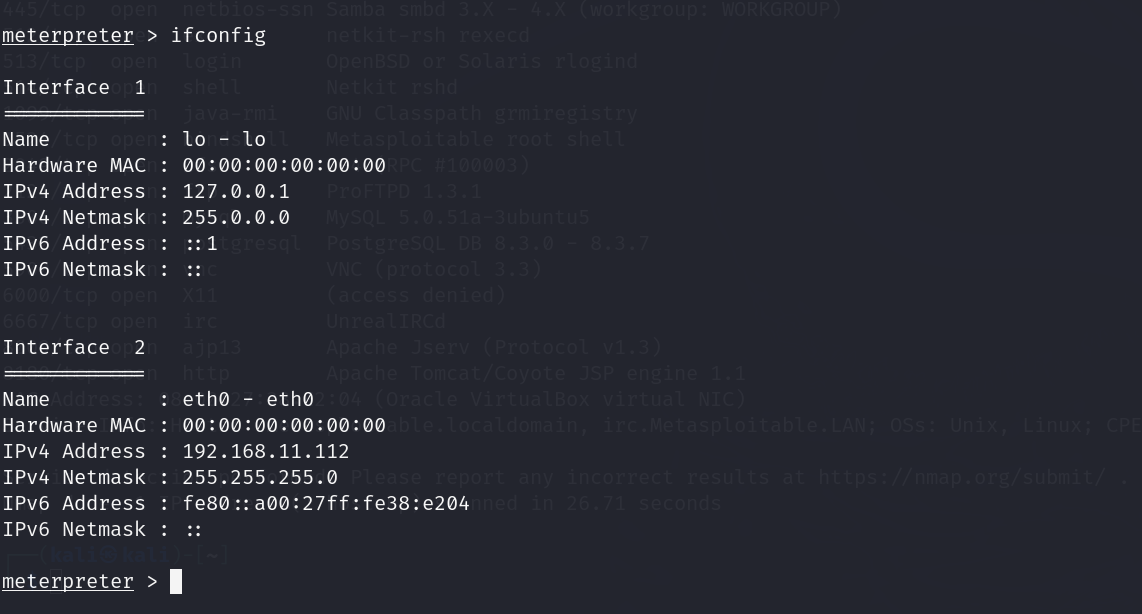
Per ottenere la sessione Meterpreter bisogna configurare RHSOSTS con l’IP della macchina vittima (192.168.11.112):



Fatto ciò avviare il comando RUN o EXPLOIT:



Ottenuta la sessione remota Meterpreter come richiesto bisogna vedere la configurazione della macchina vittima con il comando IFCONFIG:



Ed infine sempre come richiesto dalla traccia bisogna vedere, sempre della macchina vitima, la tabella di routing:

