S7 LEZIONE 5

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 dell'esercizio sono:

-La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111

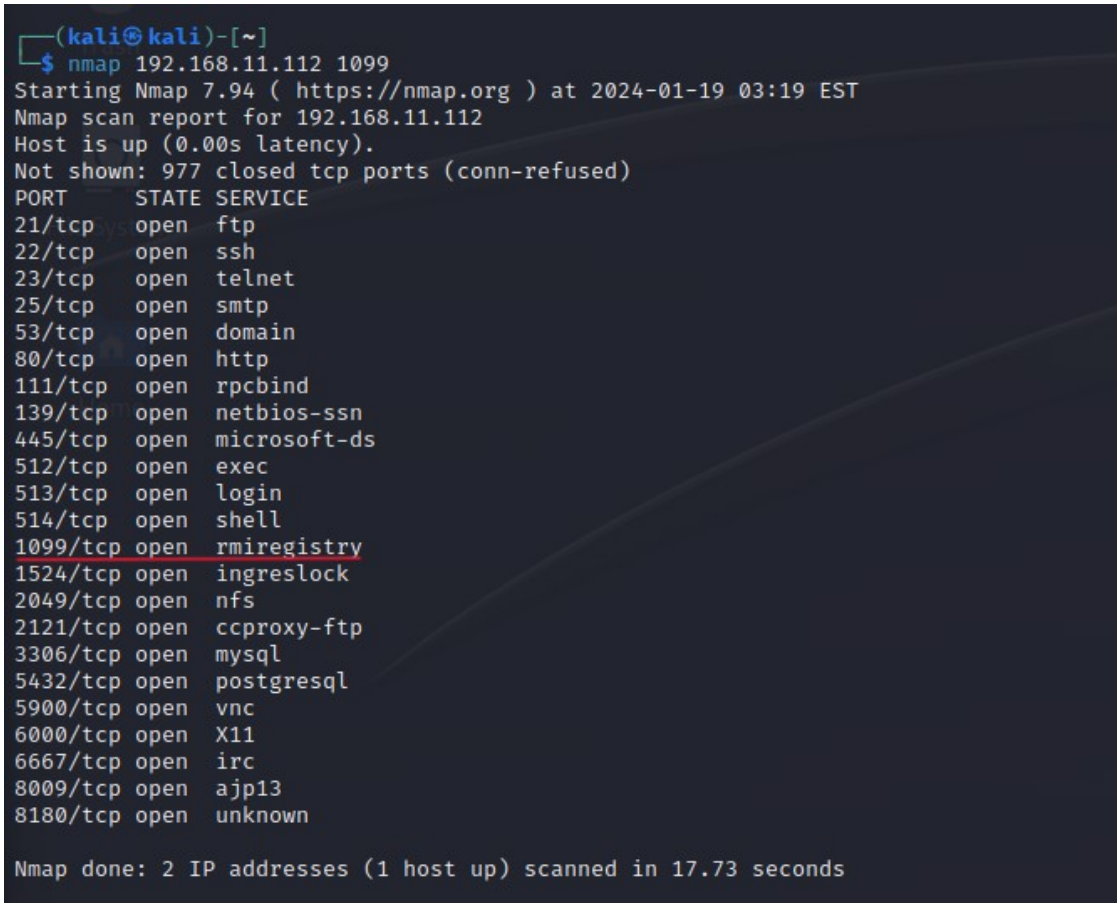
-La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112

-Scansione della macchina con nmap per evidenziare la vulnerabilità.

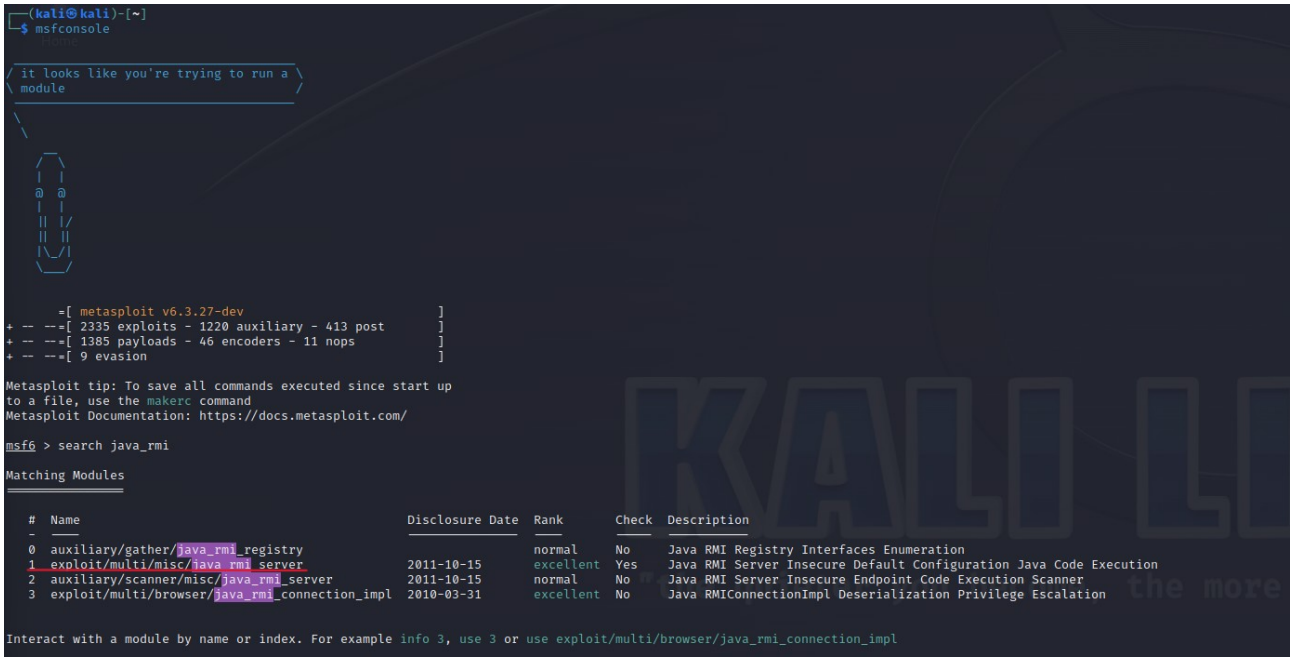
-Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
1) configurazione di rete ;
2) informazioni sulla tabella di routing della macchina vittima.

Per prima cosa ho impostato gli indirizzi IP delle due macchine come indicato dall'esercizio.

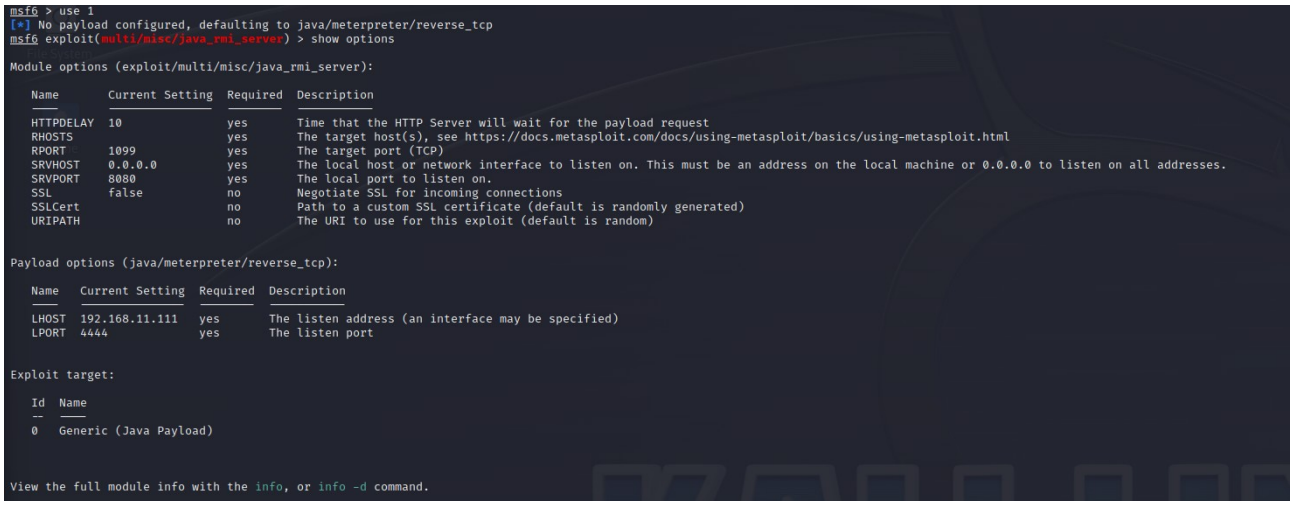
Con il comando **nmap** ho eseguito una scansione dei servizi e delle porte per trovare la vulnerabilità come si può vedere in figura.



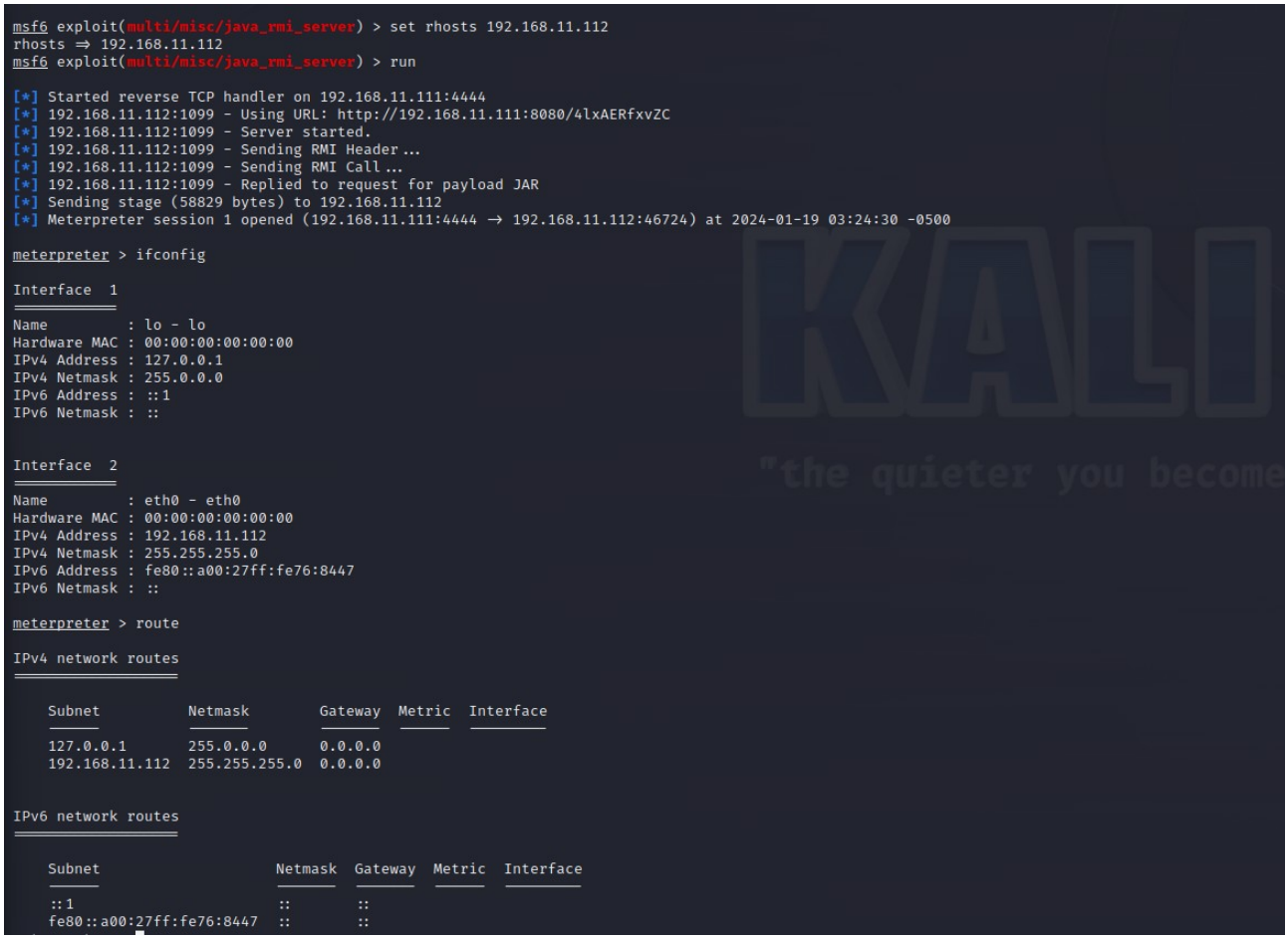
Una volta trovata la vulnerabilità ho aperto una sessione di **Metasploit** ed ho cercato l'expolit **java_rmi** con il comando search.



Con il comando **use 1** ho scelto di utilizzare il secondo exploit dell'elenco, dopodiché ho controllato i parametri dell'exploit con il comando **show options.**



Una volta settato l'indirizzo IP della macchina bersaglio con il comando **set rhosts** ho lanciato il comando **run** per eseguire l'exploit.



L'attacco è andato a buon fine, infatti si è aperta una sessione di **Meterpreter** nella quale ho eseguito prima il comando **ifconfig** per controllare la configurazione di rete della macchina bersaglio e dopo il comando **route** per ottenere informazioni sulla tabella di routing della macchina vittima.

Metasploit è un framework open-source usato per il penetration testing e lo sviluppo di exploit.
Un exploit è un codice malevolo che sfrutta delle vulnerabilità già presenti su un software, la fase di exploiting si può dividere in 3 fasi:

- si crea una connessione verso il target
- si inietta un payload
- si crea la shell

Esistono 2 tipi di shell:

- **shell reverse:** quando il payload crea la connessione dal target verso l'attaccante
- **shell bind:** quando il payload crea la connessione dall'attaccante verso il target