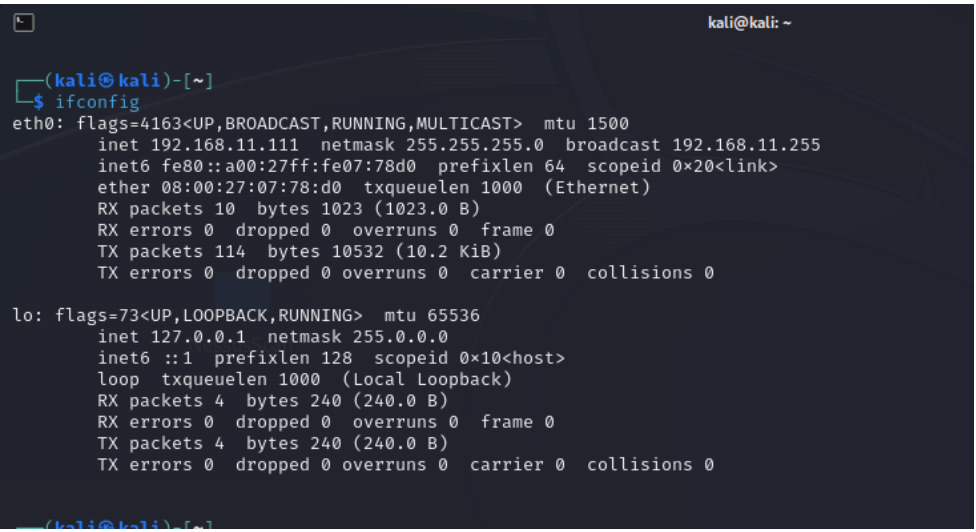
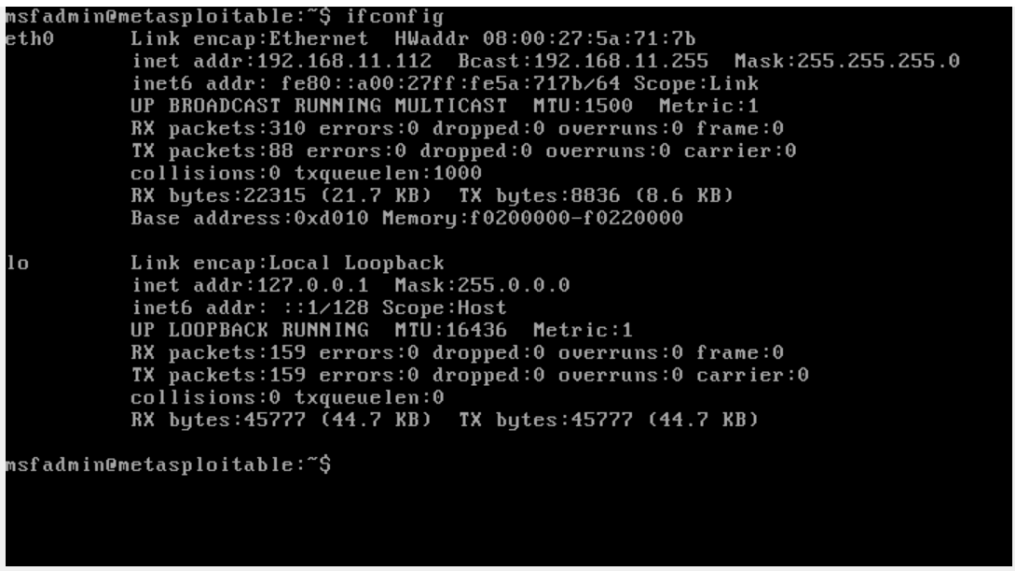
Esercizio pratica M4 EPICODE

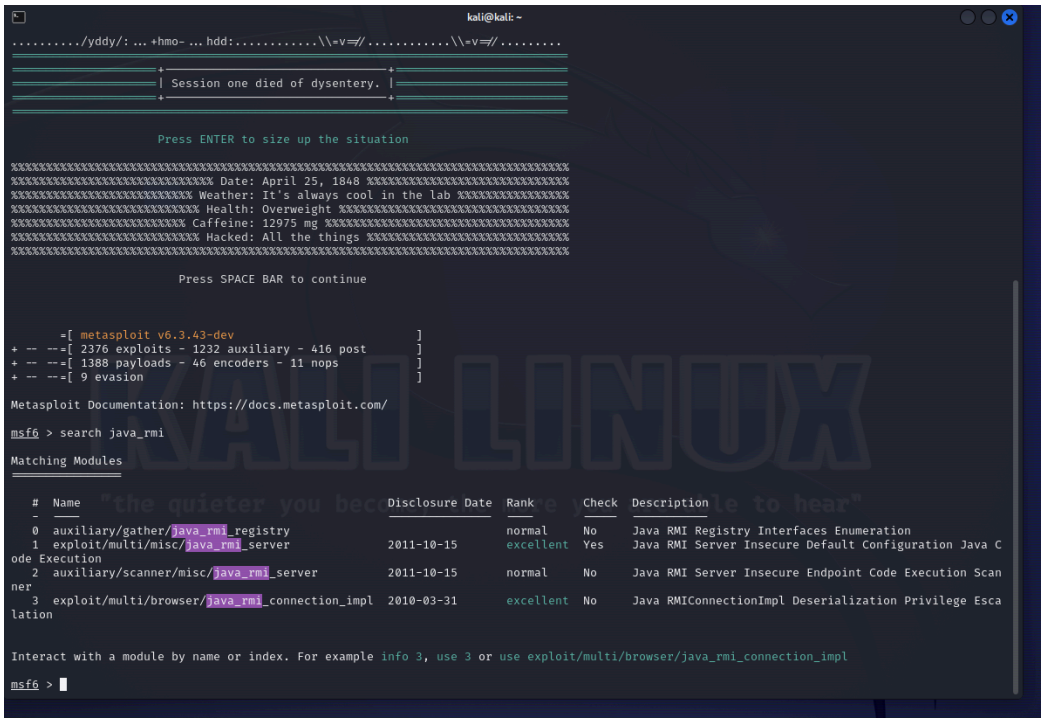
Daniele Atzori

Per prima cosa setto l'IP delle macchine kali e metasploitable, rispettivamente 192.168.11.111 e 192.168.11.112. Provo a fare il ping e ha successo.

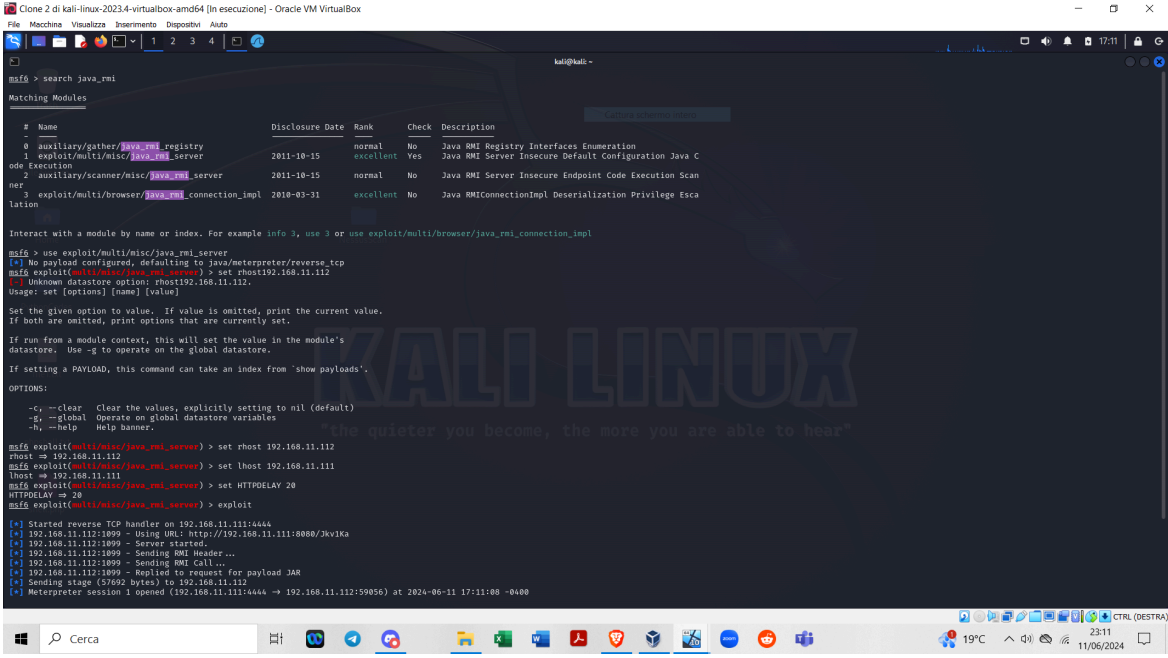




Una volta confermato che le macchine comunichino tra di loro avvio MSFConsole e cerco il tipo di exploit desiderato, partendo dalla vulnerabilità attesa, in questo caso un servizio sulla porta 1099 Java RMI.



Utilizziamo il comando “use” prima dell’exploit scelto e premiamo invio. Dopo aver confermato, settiamo la macchina attaccata (nel nostro caso metasploitable) con il comando “rhost” seguita dal suo IP (192.168.11.112) e poi la macchina attaccante (in questo caso il kali che stiamo usando) con il suo IP (192.168.11.111). Come consigliato settiamo anche l’HTTPDELAY a 20. Il parametro HTTPDELAY rappresenta il tempo che il server deve aspettare prima di processare la richiesta del payload. Se questo valore è troppo basso, potrebbe causare la chiusura della connessione prima che il payload completi la sua esecuzione.



Una volta aperta una finestra meterpreter all'interno di metasploitable andiamo prima a visualizzare le configurazioni di rete con "ifconfig" e poi quelle del routing con il comando "route".