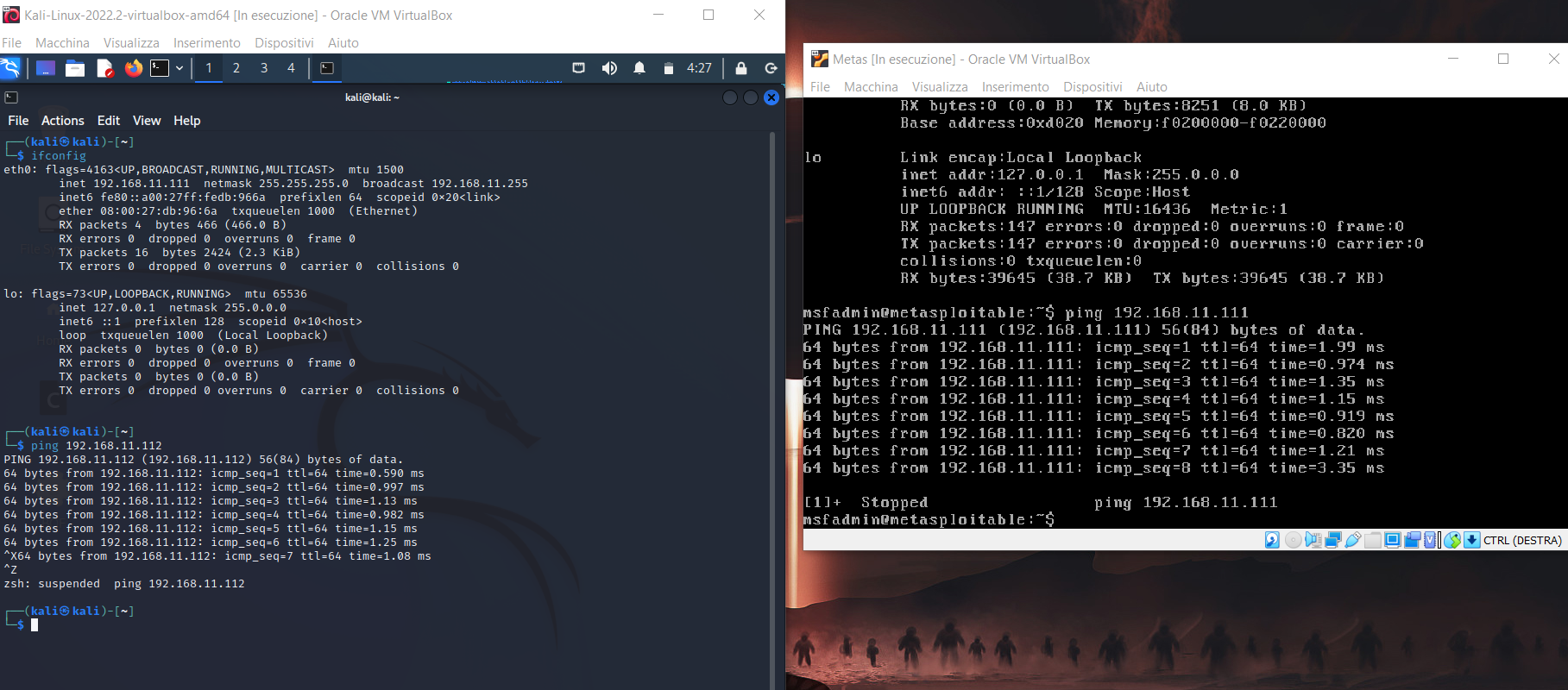
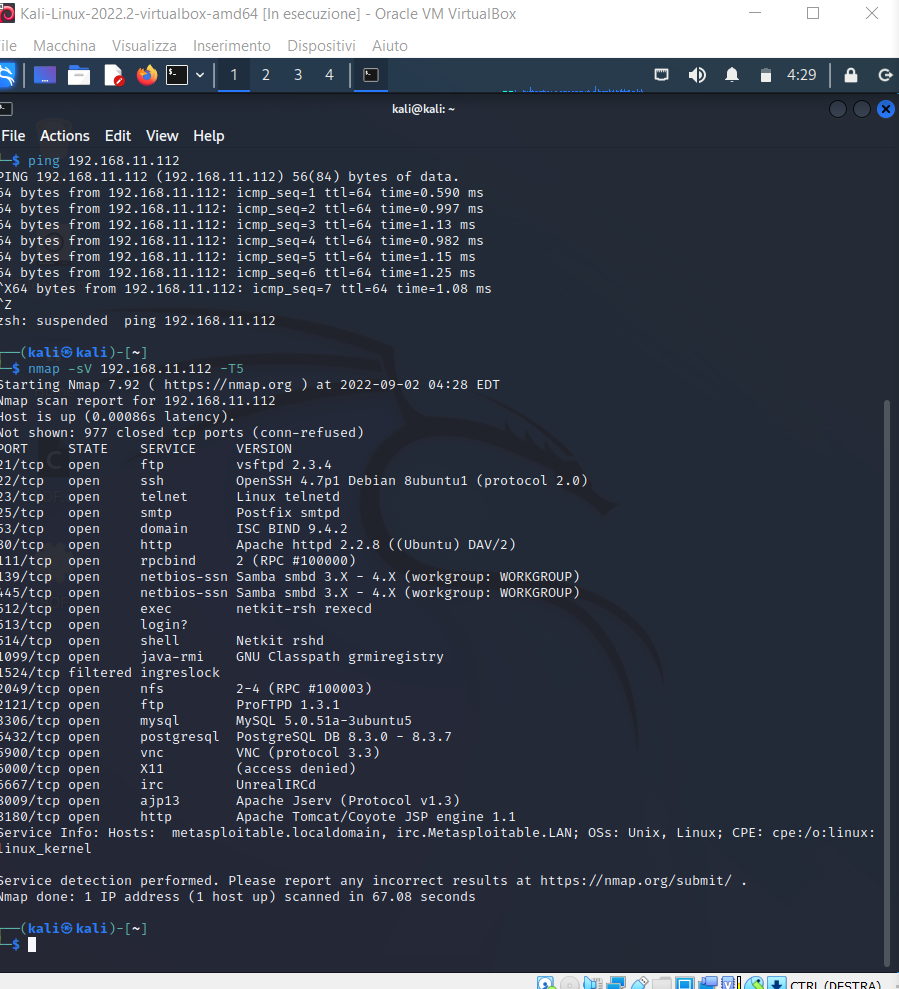
# Progetto settimanale

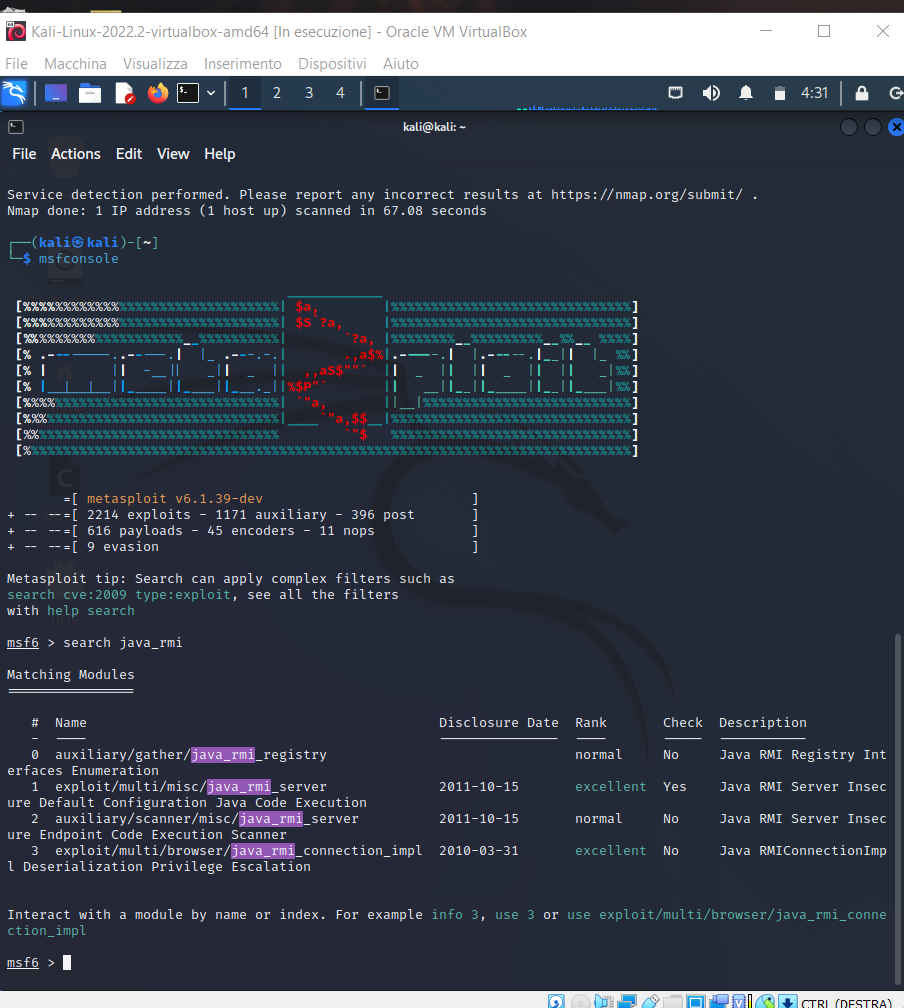
L’esercizio di oggi ci chiedeva di sfruttare una vulnerabilità del servizio java-rmi attivo sulla porta 1099.



La prima cosa che ho fatto, dopo aver cambiato gli indirizzi Ip è stata di controllare quali servizi fossero attivi tramite nmap.

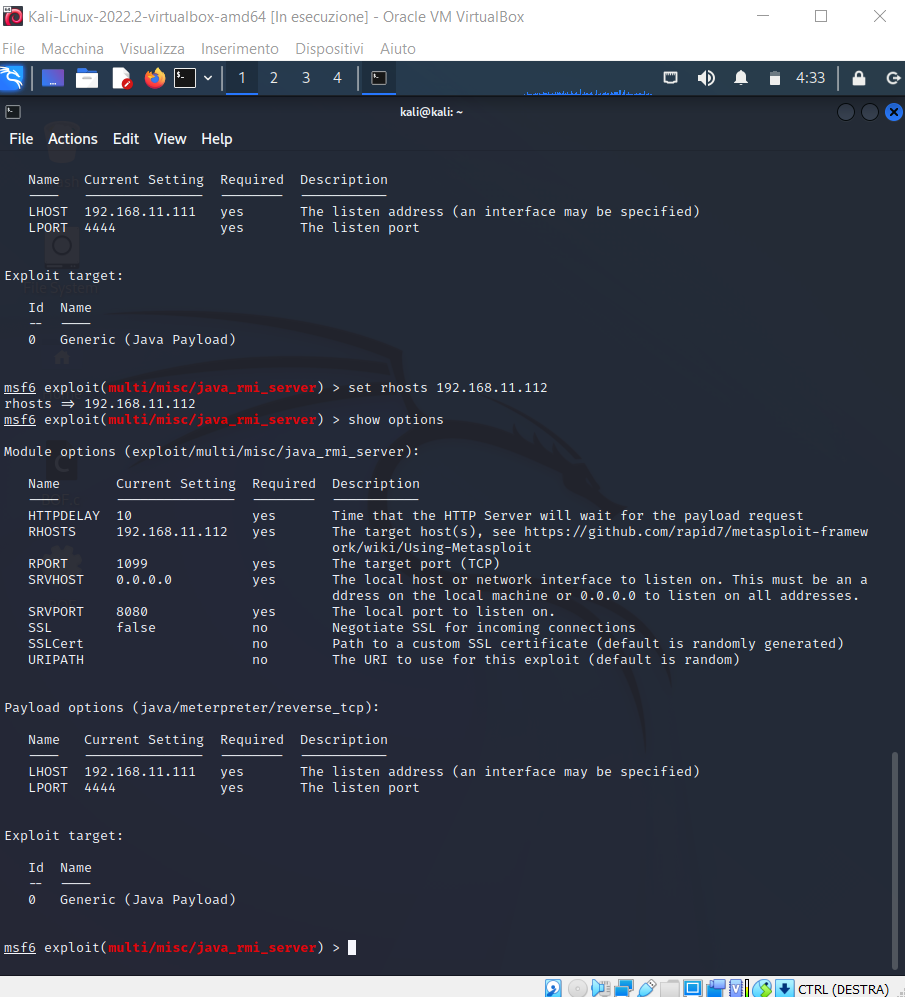


Per questo esercizio ho sfruttato la vulnerabilità del servizio java-rmi, per creare una connessione con la macchina target e ottenerne l’accesso.

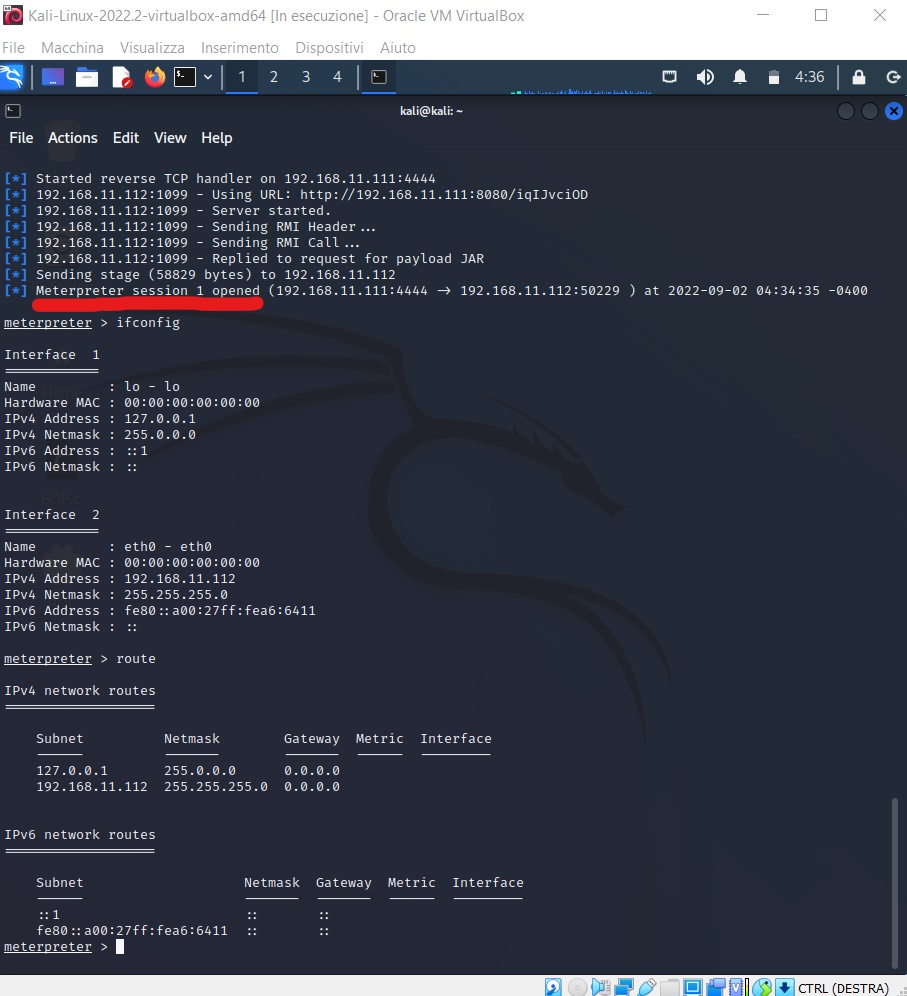


Ho quindi avviato msfconsole e cercato degli exploit utili per questo tipo di vulnerabilità.

Una volta scelta quella che mi serviva, ho controllato quali parametri servissero e configurati in modo che fosse tutto corretto.



Controllato che fossero settate tutte le impostazioni richieste (ip macchina target per esempio), non avendo bisogno del payload in quanto andava bene quello di default, non restava che far partire l’exploit.



Creata la shell come possiamo vedere, non restava che dimostrare tramite dei comandi, di aver preso controllo della macchina target.

Si può vedere come con il comando ifconfig e route, sono riuscito a recuperare informazioni sulla reta della macchina e sulla tabella di route.