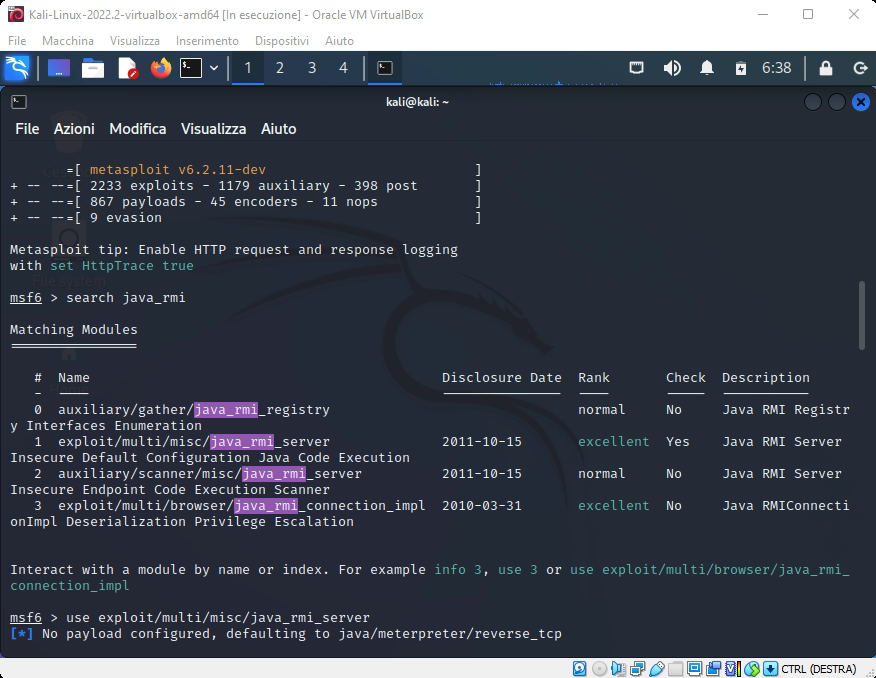
REPORT VULNERABILTY EXPLOIT CON METASPLOIT

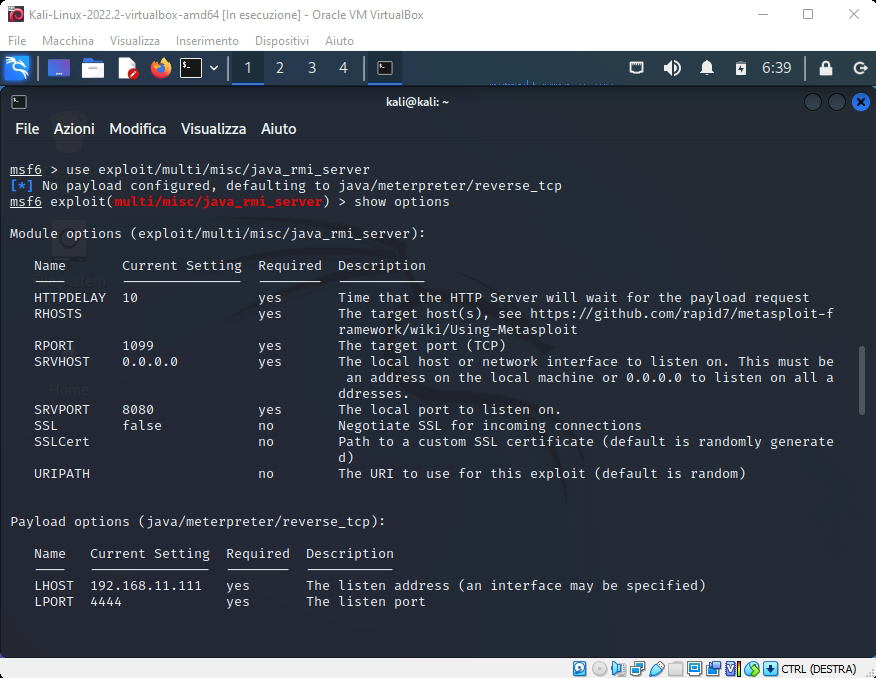
In questo report verranno spiegati i passaggi atti all’esecuzione di un exploit dalla macchina attaccante verso la macchina target per generare una connessione e di conseguenza ottenere informazioni e di conseguenza il controllo di essa ovvero Metasploitable.

Come primo passaggio è stata usata una scansione con nmap per l’enumerazione delle porte e dei servizi aperti e successivamente è stato effettuato un passaggio di vulnerability scanning con nessus per identificare le vulnerabilità più critiche.

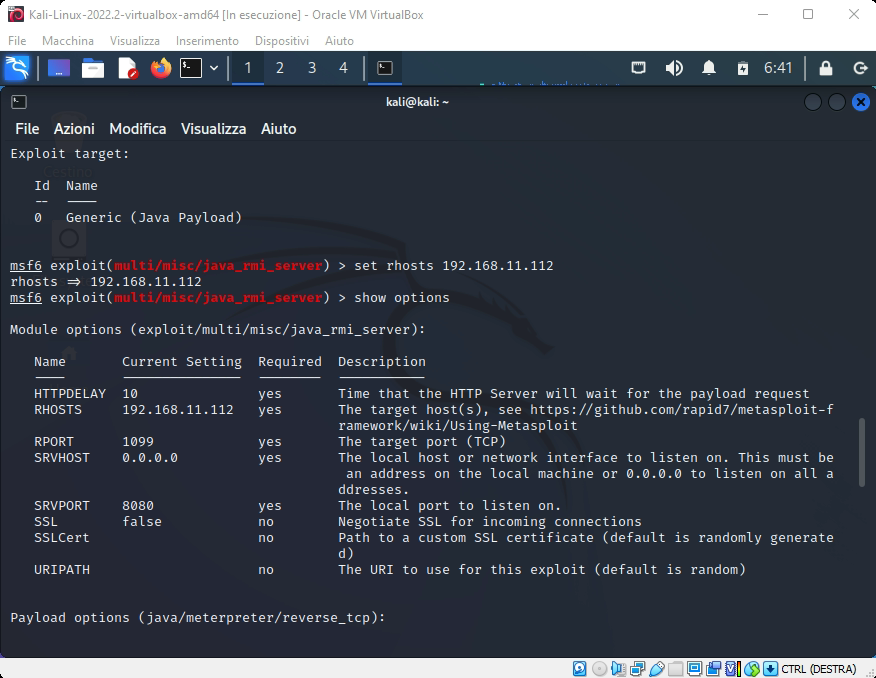
Una volta completato questo passaggio si procede a mettere in pratica le vulnerabilità trovate.



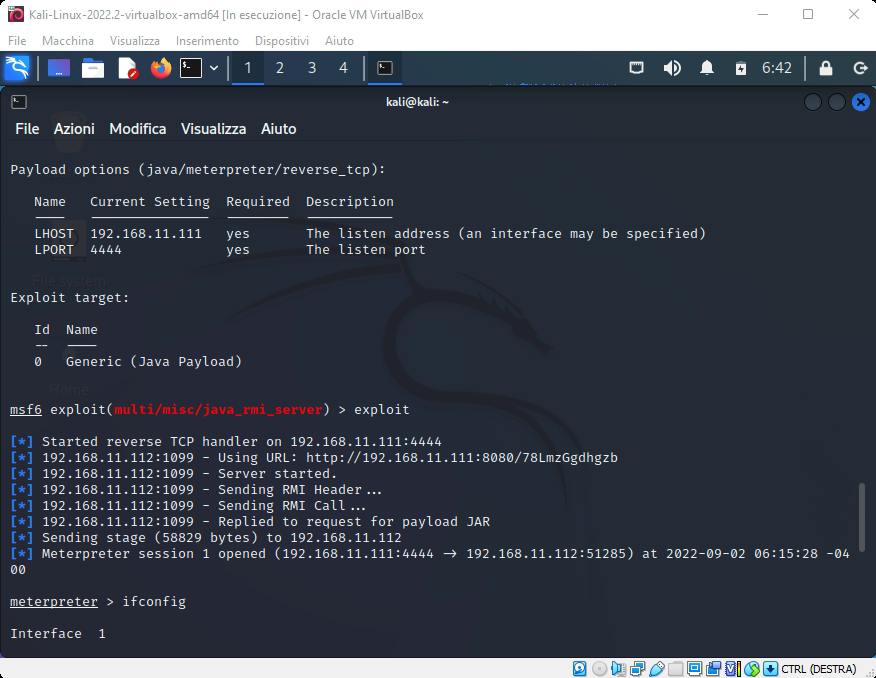
Nel seguente screenshot sono elencate le vulnerabilità che sono state trovate dal programma con a fianco i dettagli e il tipo di classificazione di vulnerabilità indicato (excellent come critico in termini di sfruttabilità dell’exploit)

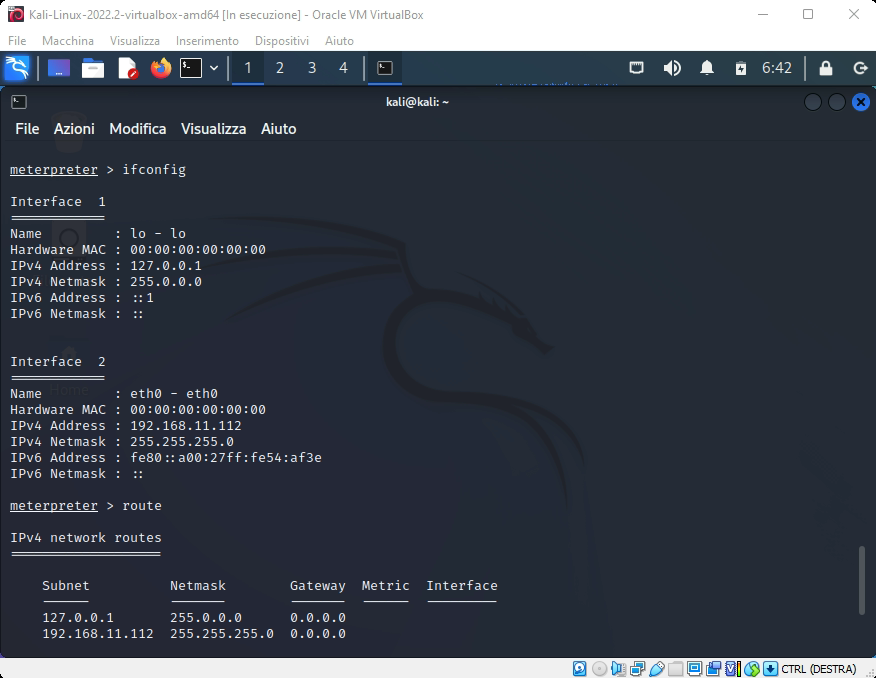


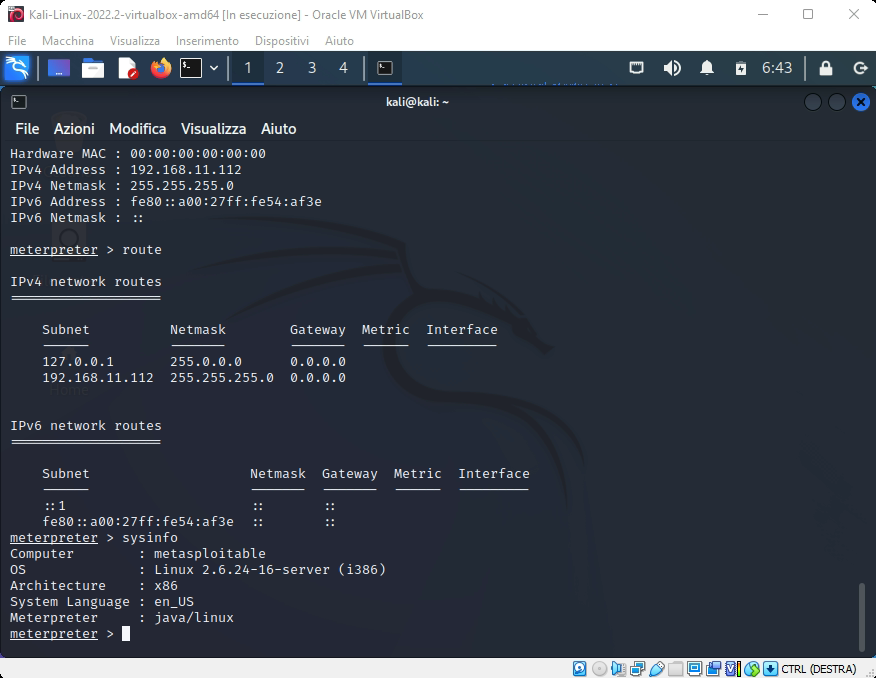
Dopodichè si procede ad usare l’exploit selezionato qui in figura, con il comando show options per verificare se diversi servizi possono essere utilizzati o configurati manualmente (determinati da yes, no)



Si procede quindi a impostare l’indirizzo ip della macchina target tramite il comando set rhosts e di conseguenza l’avvio dell’exploit tramite il payload meterpreter come mostrato nella figura successiva.



Arrivati a questo punto si è dentro la macchina target ovvero la macchina vittima tramite connessione reverse\_tcp, ovvero creando una connessione dalla macchina target alla macchina attaccante per evitare il firewall ed essere rilevati con meno facilità.

Quindi si procede a raccogliere informazioni sulla configurazione di rete della macchina tramite il comando ifconfig e le informazioni sulla tabella di routing della macchina.

In aggiunta a ciò è stata fatta anche un’elencazione delle informazioni di sistema della macchina vittima, per avere più informazioni circa un possibile attacco più efficiente.