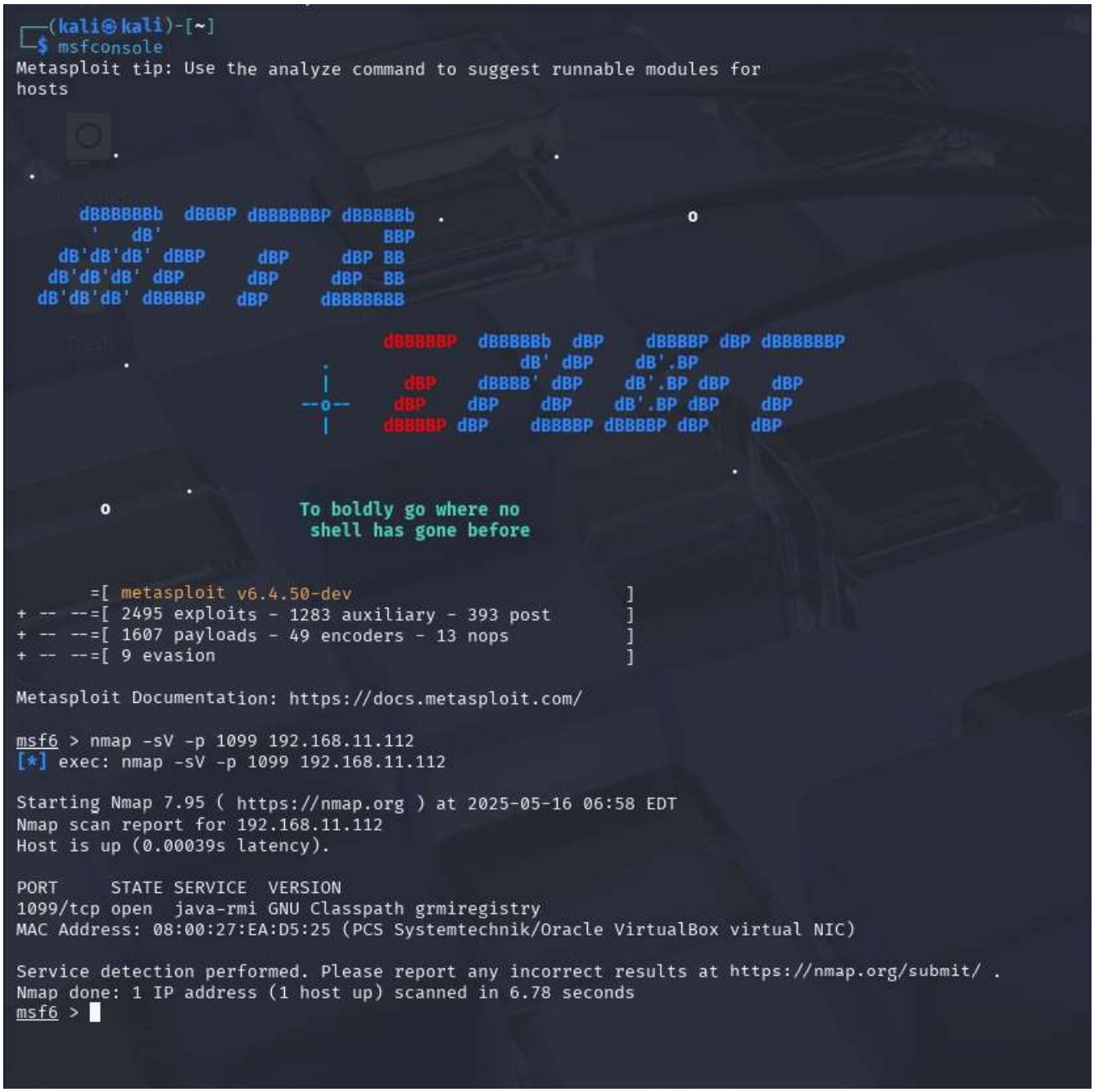
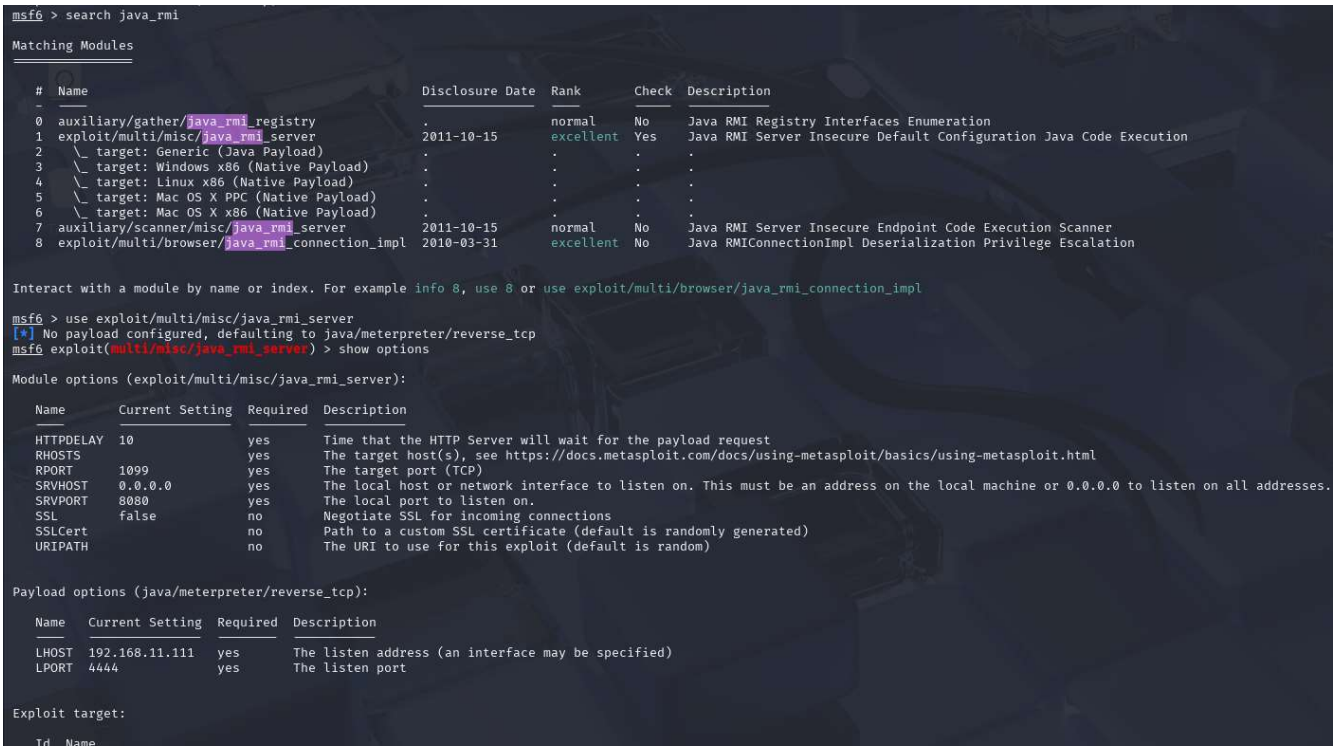
Creazione sessione Meterpreter

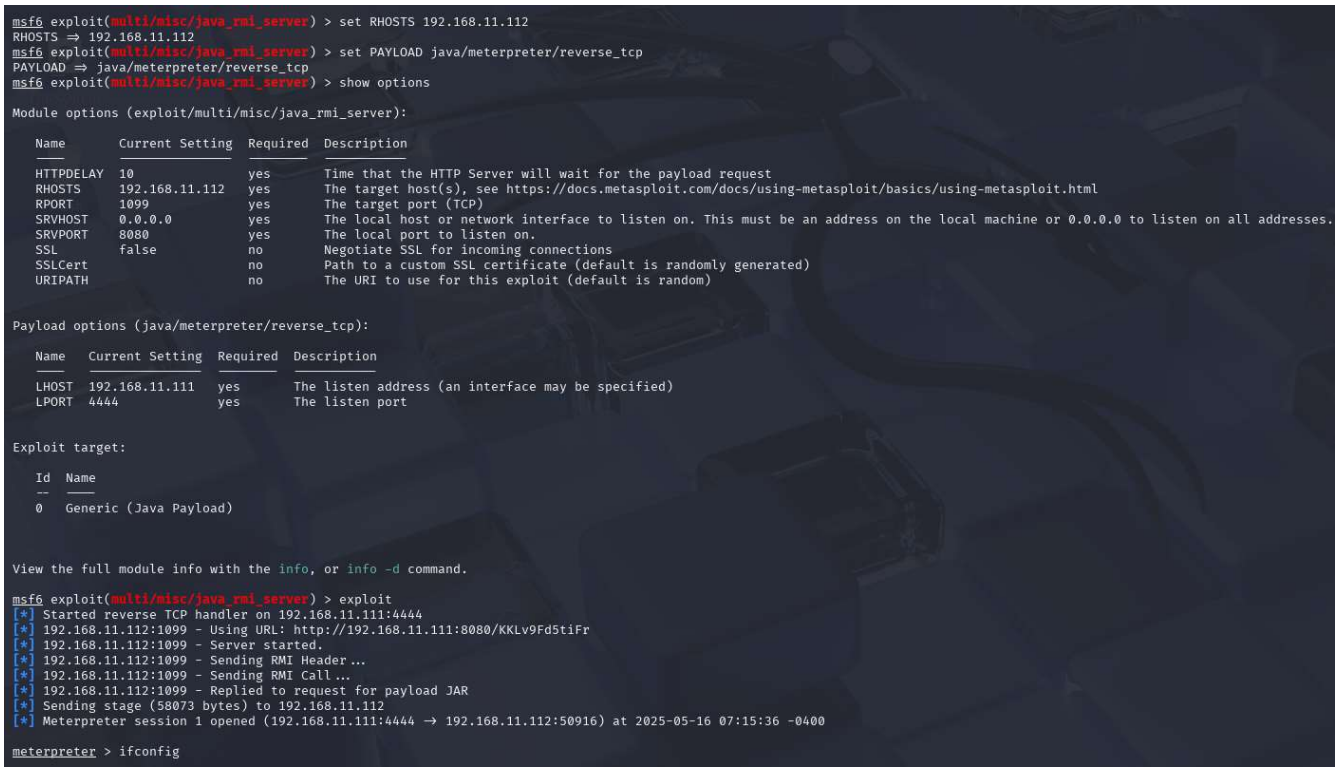
Dopo aver settato gli indirizzi e le configurazioni di Kali e Metaspotable secondo la consegna, provvediamo a entrare in msfconsole nel terminale di Kali e facciamo una scansione mirata con nmap per verificare che la porta del servizio Java-rmi sia aperta e quindi vulnerabile.



Per mandare avanti il nostro exploit con successo, cerchiamo tra I moduli di msfconsole quello più indicato, che nel nostro caso è Java-rmi con il comando search java-rmi. Una volta trovato il modulo per l'exploit che ci serve usiamo il comando use seguito dal percorso dell'exploit, e usiamo show option per vedere quali parametri inserire o modificare.



Da questo risultato, notiamo che manca l'indirizzo IP della macchina target e lo impostiamo con il comando set, e impostiamo anche il payload con quello suggerito di default. Controlliamo che tutti I parametri siano impostati correttamente, e possiamo lanciare l'exploit.



Siamo riusciti ad entrare nella nostra macchina vittima e creare la nostra shell avanzata con la sessione Meterpreter. Adesso estrapoliamo con il comando ifconfig le configurazione di rete e con il comando route le informazioni sulla tabella di routing della macchina vittima.

Oppure possiamo migrare in una shell e inserire il comando ip route per avere una shell diretta del sistema remoto.