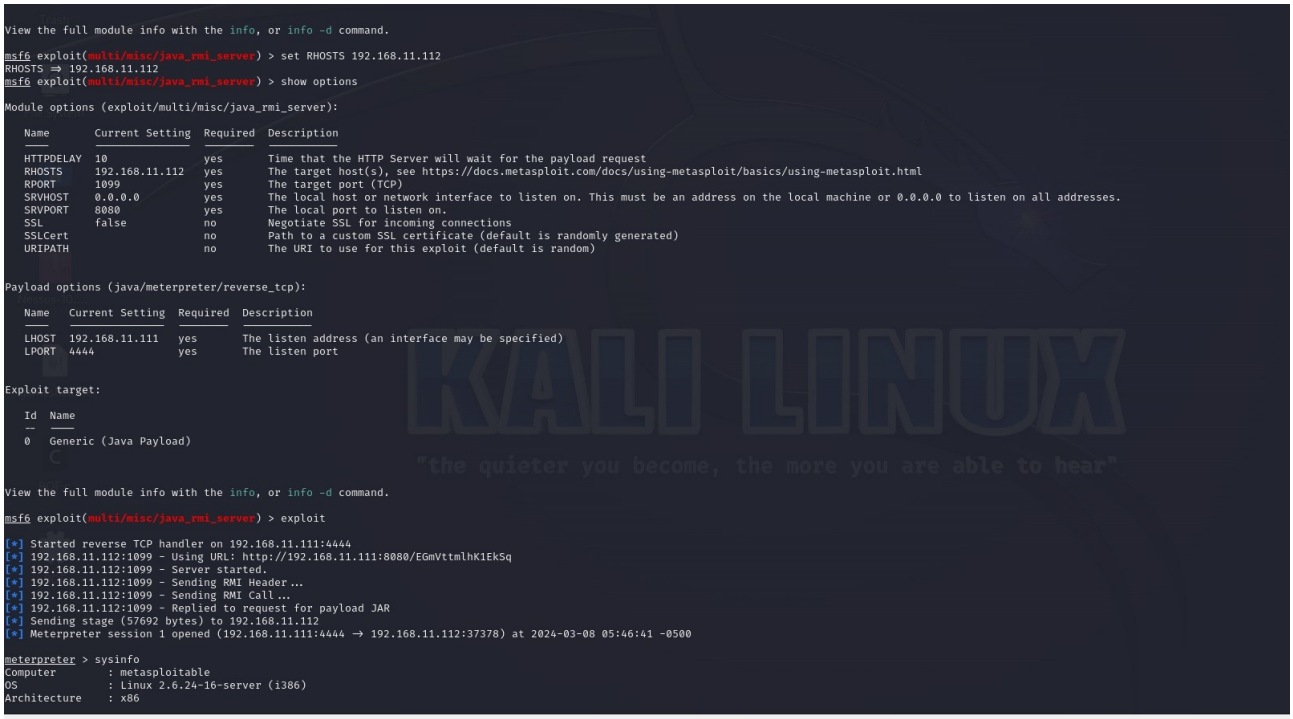
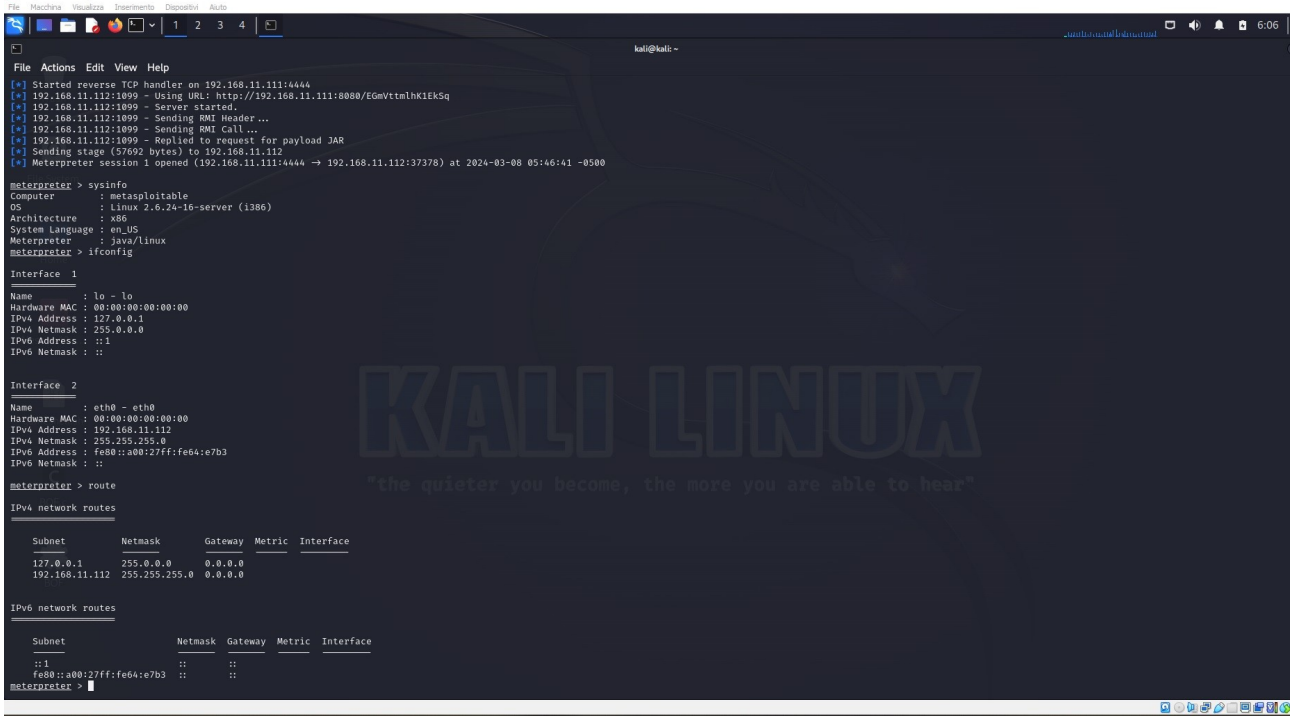
PROGETTO SETTIMANA 7

Sfruttare il servizio vulnerabile sulla porta 1099 – Java RMI della macchina metasploitable. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota. I requisiti dell'esercizio sono:
● La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
● La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
● Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota: 1) configurazione di rete ; 2) informazioni sulla tabella di routing della macchina vittima.



Avviando il framework metasploit dal terminale kali, ricerco la vulnerabilita' che sfrutta java rmi(remote method invocation), con il comando 'use' la seleziono e con 'show options' verifico i parametri necessari al funzionamento, in questo caso devo soltanto inserire l'indirizzo ip target che aggiungo col comando 'set RHOSTS'.
Finiti i preparativi avvio l'attacco col comando 'exploit' e va a buon fine come da immagine sopra.



L'attacco in questione apre una sessione meterpreter dalla quale con 'sysinfo' si possono vedere le specifiche del sistema operativo target; invece con 'ifconfig' e 'route' si vedono rispettivamente l'interfaccia di rete e la tabella di routing del sistema tartget come da immagine sopra.
Meterpreter e' un payload di metasploit che permette di controllare lo schermo del dispositivo bersaglio.