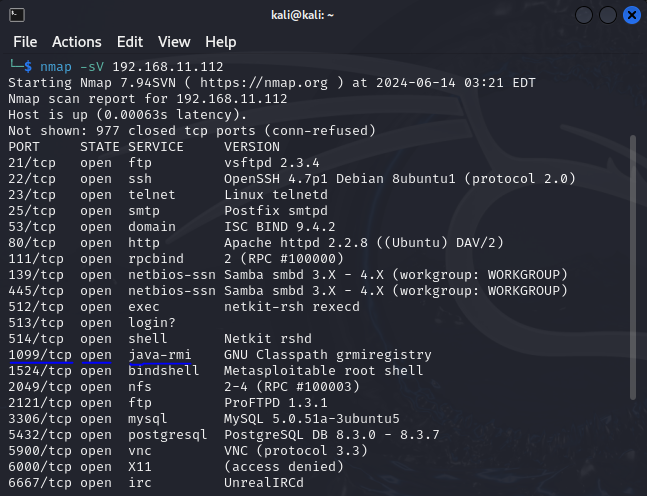
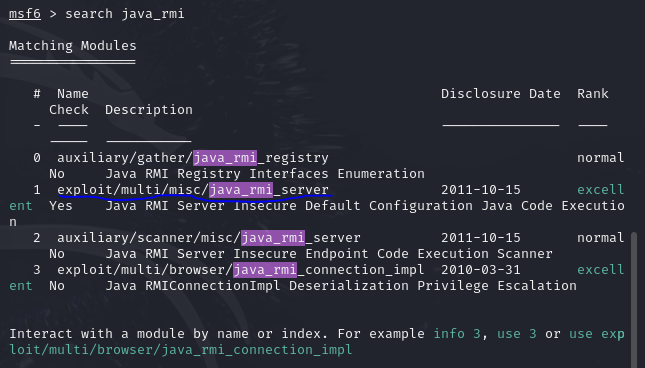
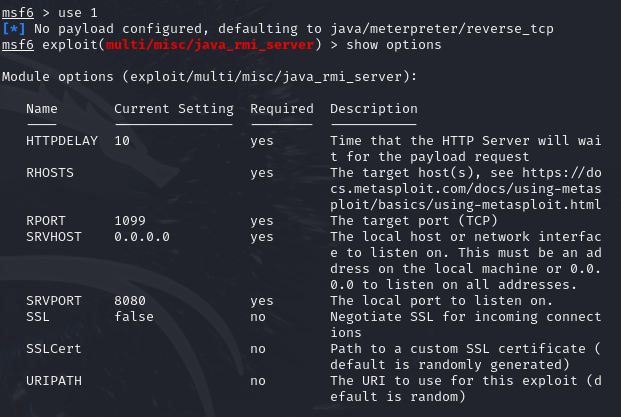
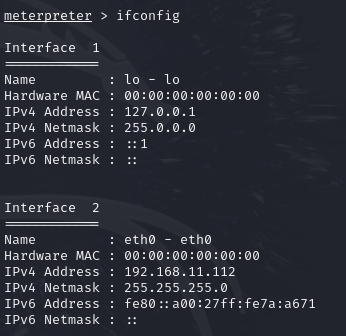
Il nostro obiettivo è lanciare un’exploit da kali per sfruttare una vulnerabilità della porta 1099 ed attaccare la macchina Metasploitable. Le due macchine sono sulla stessa rete.per prima cosa ho usato il comando “nmap –sV 192.168.11.112” cercare i servizi attivi e se presentano delle vulnerabilità. Come vediamo la porta 1099 è aperta e presenta una vulnerabilità su java-rmi avendo questa informazione basta cercare “java\_rmi” pervedere i possibili exploit sfruttabili e nel nostro caso useremo il primo che ci fornisce digitando “use 1”

dopo aver inserito alla voce “RHOST” l’ip della macchina targhet ed alla voce “LHOST” la macchina attaccante, si può lanciare l’exploit





adesso abbiamo a disposizione una shell in cui digitare comandi, ed alla voce “Intrface 2” abbiamo l’interfaccia della macchina vittima. Nel mio caso ho chiesto con “ifconfig” alla stessa macchina vittima, il suo indirizzo ip.