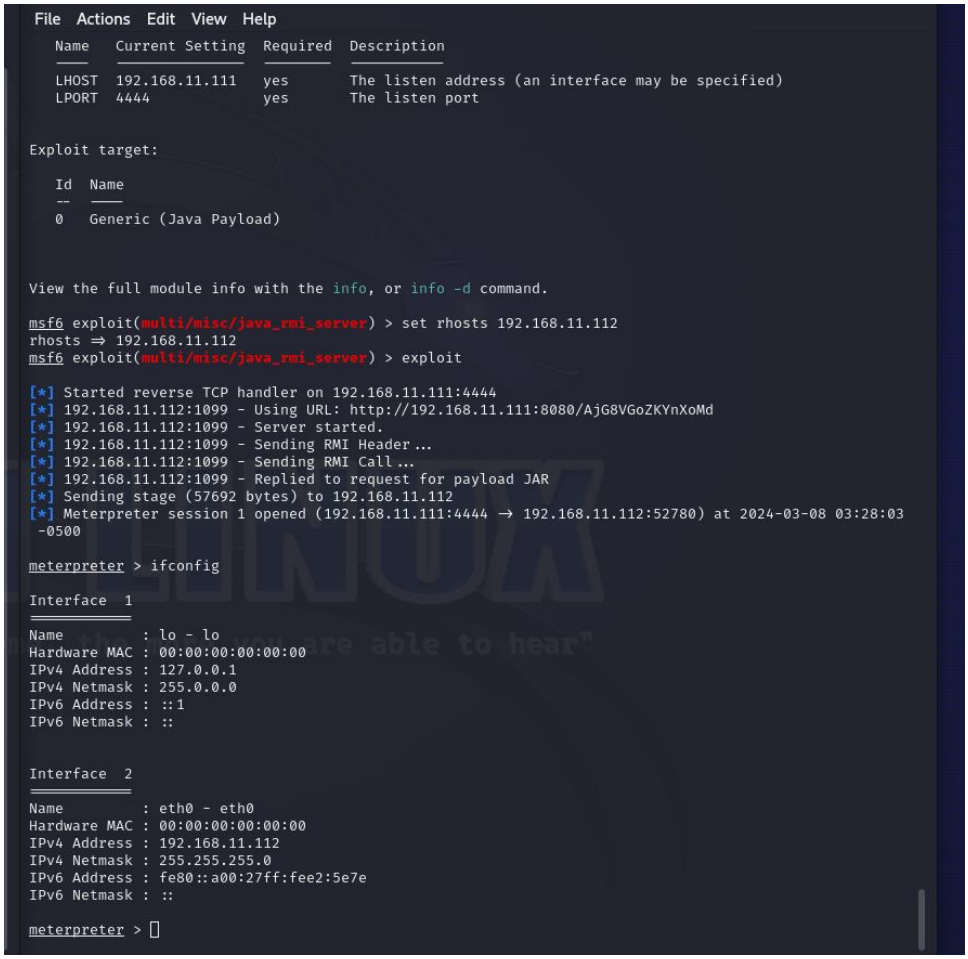
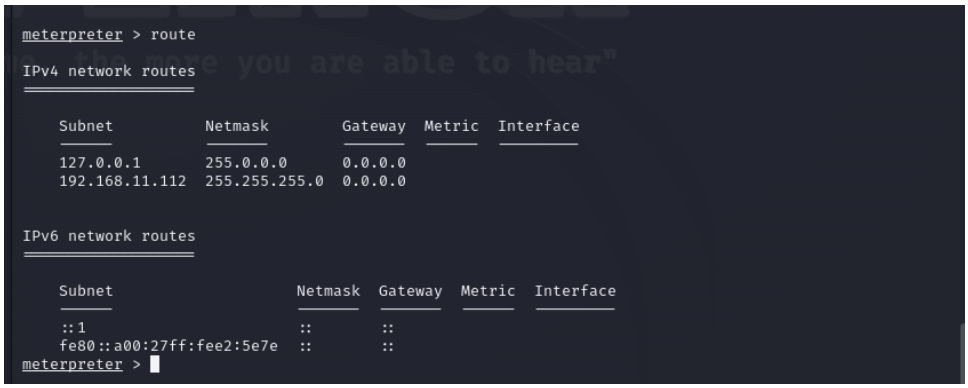
S7L5


File Actions Edit View Help
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-08 03:09 EST
Nmap scan report for 192.168.11.112
Host is up (0.0037s latency).
Not shown: 979 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
inet6 fe80::a00:27ff:fe9a:d414 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:9a:d4:14 txqueuelen 1000 (Ethernet)
RX packets 1267 bytes 93975 (91.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1315 bytes 216447 (211.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 13 bytes 1047 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 13 bytes 1047 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~]
$





Ho recentemente effettuato una serie di operazioni di configurazione e sfruttamento in un ambiente di rete simulato utilizzando due macchine virtuali, una Kali Linux e una Metasploitable. Inizialmente, ho modificato gli indirizzi IP di entrambe le macchine per adattarli alla mia rete locale.

Per fare ciò, ho utilizzato il comando **`sudo nano /etc/network/interfaces`** per accedere al file di configurazione delle interfacce di rete di Kali Linux. Ho cambiato l'indirizzo IP della macchina Kali in 192.168.11.111 e ho fatto lo stesso per la macchina Metasploitable, assegnandole l'indirizzo IP 192.168.11.112.

Successivamente, ho avviato una sessione di Metasploit Framework digitando **`msfconsole`** nel terminale. Una volta all'interno di Metasploit, ho eseguito una ricerca del modulo utilizzando il comando **`search rmiregistry`**. La ricerca ha individuato l'exploit **`exploit/multi/misc/java_rmi_server`**.

Dopo aver trovato il modulo desiderato, ho utilizzato il comando **`use`** per selezionarlo. Questo comando ha preparato Metasploit per l'utilizzo del modulo specificato.

Successivamente, ho visualizzato le opzioni disponibili per l'exploit utilizzando il comando **`show options`**. Qui ho notato che dovevo impostare l'indirizzo IP della macchina target utilizzando l'opzione **`set RHOSTS`**.

Una volta impostate correttamente tutte le opzioni necessarie, ho eseguito l'exploit per avviare una shell di Meterpreter sulla macchina target, fornendomi un accesso remoto completo al sistema compromesso.

Dalla shell di Meterpreter, ho eseguito i comandi **`ifconfig`** e **`route`** per recuperare la configurazione di rete e le informazioni sulla tabella di routing della macchina vittima. Queste informazioni sono cruciali per comprendere la topologia di rete e identificare eventuali altri obiettivi all'interno della rete.