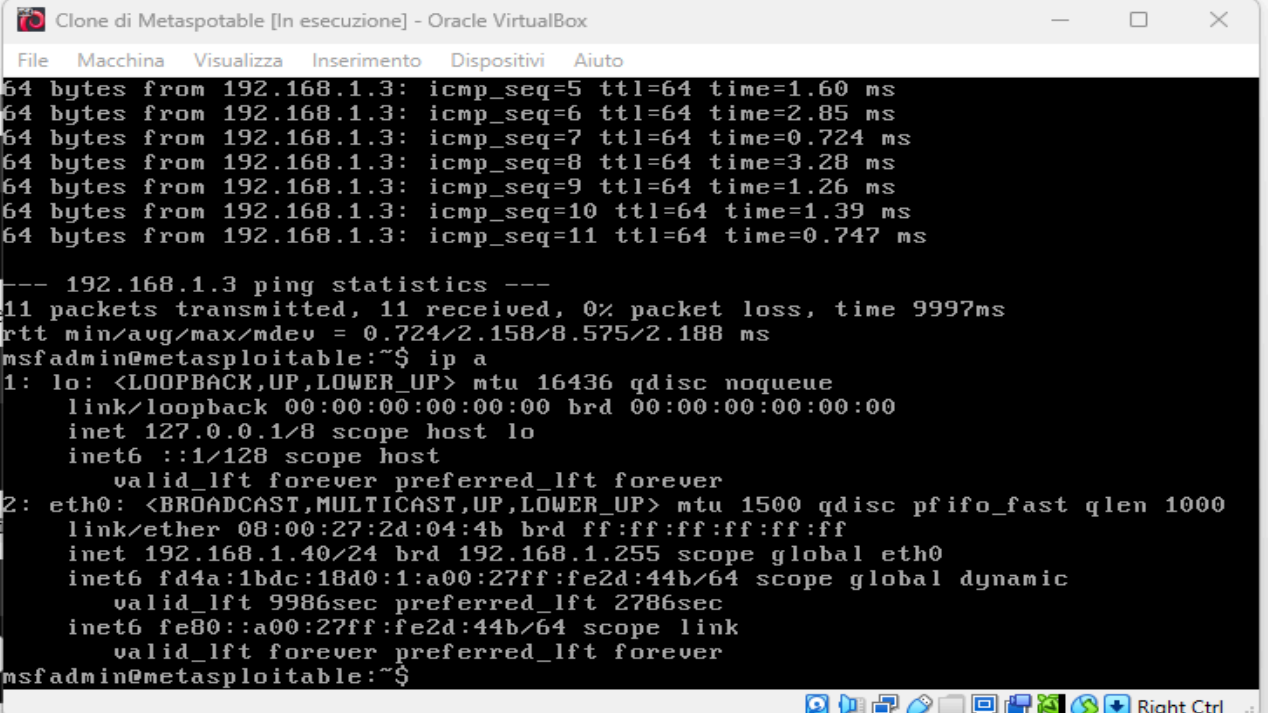


Esercizio 24-09

Ho modificato l'ip con `ifconfig eth0 .. netmask 255.255.255.0 up` mettendo l'ip dell'esercizio.

Per prova ho fatto il Ping all'ip vecchio della Kali

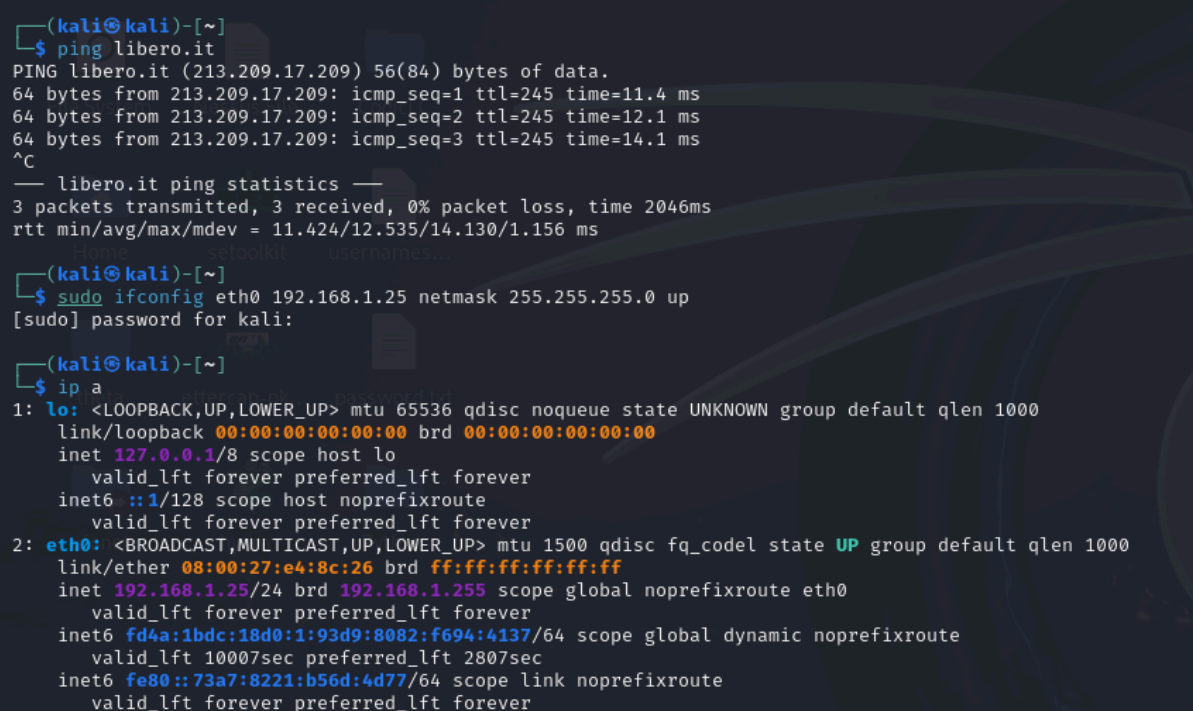
E poi ip a, per vedere l'IP



```
64 bytes from 192.168.1.3: icmp_seq=5 ttl=64 time=1.60 ms
64 bytes from 192.168.1.3: icmp_seq=6 ttl=64 time=2.85 ms
64 bytes from 192.168.1.3: icmp_seq=7 ttl=64 time=0.724 ms
64 bytes from 192.168.1.3: icmp_seq=8 ttl=64 time=3.28 ms
64 bytes from 192.168.1.3: icmp_seq=9 ttl=64 time=1.26 ms
64 bytes from 192.168.1.3: icmp_seq=10 ttl=64 time=1.39 ms
64 bytes from 192.168.1.3: icmp_seq=11 ttl=64 time=0.747 ms

--- 192.168.1.3 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 9997ms
rtt min/avg/max/mdev = 0.724/2.158/8.575/2.188 ms
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 08:00:27:2d:04:4b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
        inet6 fd4a:1bdc:18d0:1:a00:27ff:fe2d:44b/64 scope global dynamic
            valid_lft 9986sec preferred_lft 2786sec
    inet6 fe80::a00:27ff:fe2d:44b/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Stessa cosa fatta con la Kali



```
(kali@kali)-[~]
$ ping libero.it
PING libero.it (213.209.17.209) 56(84) bytes of data:
64 bytes from 213.209.17.209: icmp_seq=1 ttl=245 time=11.4 ms
64 bytes from 213.209.17.209: icmp_seq=2 ttl=245 time=12.1 ms
64 bytes from 213.209.17.209: icmp_seq=3 ttl=245 time=14.1 ms
^C
--- libero.it ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2046ms
rtt min/avg/max/mdev = 11.424/12.535/14.130/1.156 ms

(kali@kali)-[~]
$ sudo ifconfig eth0 192.168.1.25 netmask 255.255.255.0 up
[sudo] password for kali:

(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:e4:8c:26 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fd4a:1bdc:18d0:1:93d9:8082:f694:4137/64 scope global dynamic noprefixroute
        valid_lft 10007sec preferred_lft 2807sec
    inet6 fe80::73a7:8221:b56d:4d77/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Dopo aver impostato l'ip, ho aperto msfconsole.

Search telnet_version.

Options. per vedere quali parametri impostare

Set rhost. con L'ip della Meta bersaglio

run. per avviare il comando

```
kali@kali: ~  
File Actions Edit View Help  
1 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detection  
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_version  
msf6 > use 1  
msf6 auxiliary(scanner/telnet/telnet_version) > options  
Module options (auxiliary/scanner/telnet/telnet_version):  


| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                |
| RHOSTS   |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                  |
| THREADS  | 1               | yes      | The number of concurrent threads (max one per host)                                                    |
| TIMEOUT  | 30              | yes      | Timeout for the Telnet probe                                                                           |
| USERNAME |                 | no       | The username to authenticate as                                                                        |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40  
rhost => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > options  
Module options (auxiliary/scanner/telnet/telnet_version):  


| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                |
| RHOSTS   | 192.168.1.40    | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                  |
| THREADS  | 1               | yes      | The number of concurrent threads (max one per host)                                                    |
| TIMEOUT  | 30              | yes      | Timeout for the Telnet probe                                                                           |
| USERNAME |                 | no       | The username to authenticate as                                                                        |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/telnet/telnet_version) > run  
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

Telnet 192.168.1.40 per vedere la scritta Metasploitable2 correttamente e non in binario.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40  
[*] exec: telnet 192.168.1.40  
  
Trying 192.168.1.40 ...  
Connected to 192.168.1.40.  
Escape character is '^]'.  
  
Warning: Never expose this VM to an untrusted network!  
Contact: msfdev[at]metasploit.com  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: █
```