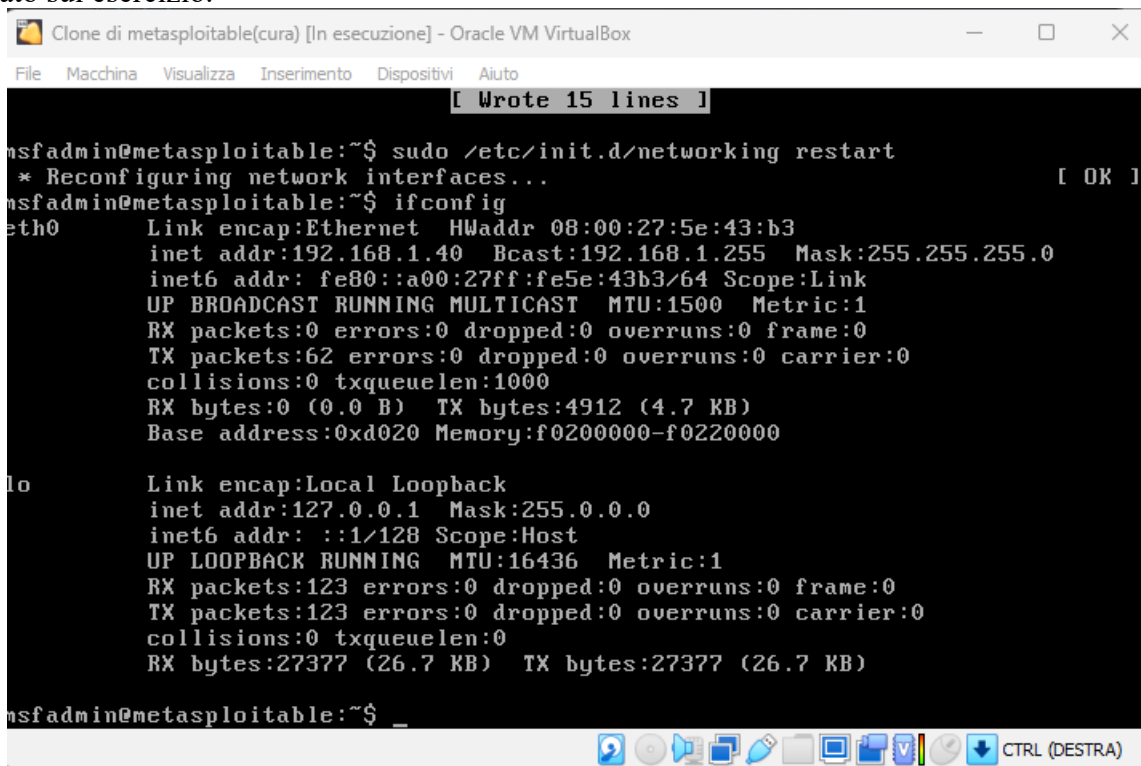


Obiettivo: sfruttare la vulnerabilità di Telnet presente su Metasploitable 2

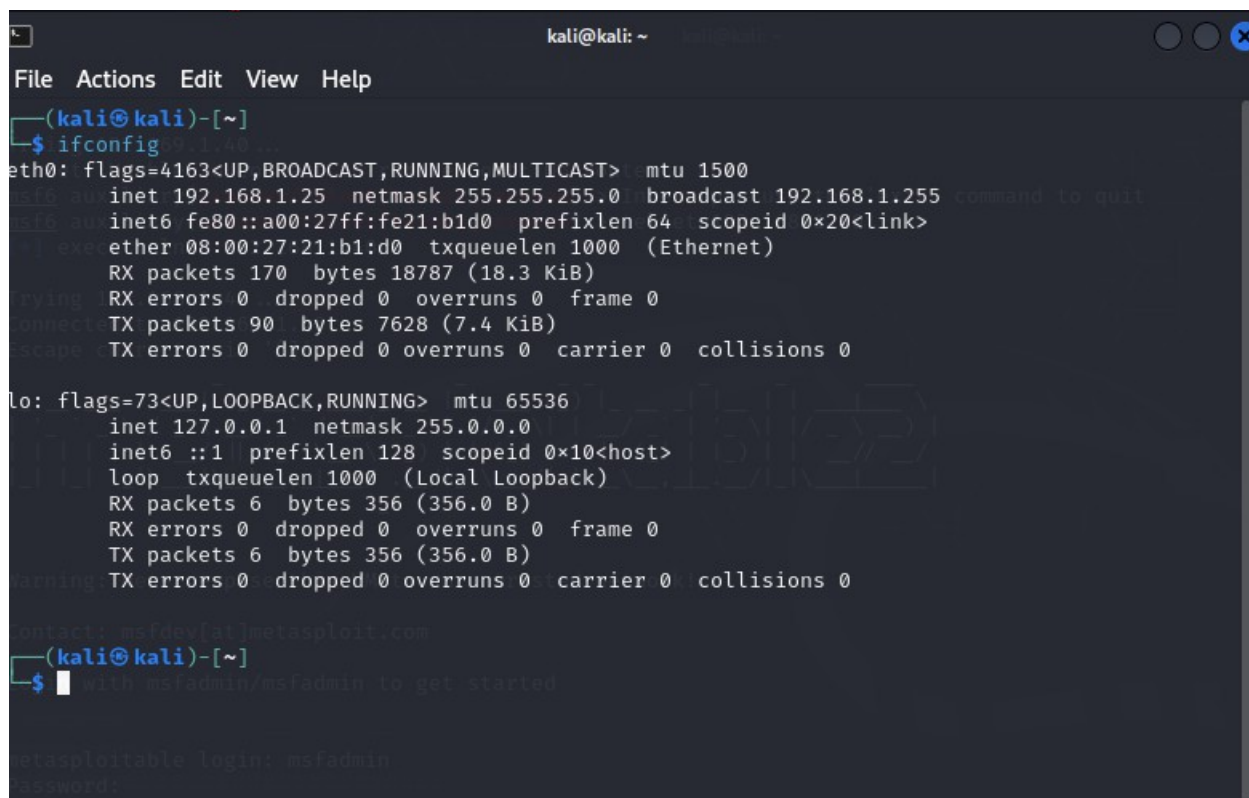
Come prima cosa andiamo a cambiare gli ip delle macchine virtuali Kali e Metasploitable come indicato sull'esercizio.



```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:5e:43:b3
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5e:43b3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4912 (4.7 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:123 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27377 (26.7 KB)  TX bytes:27377 (26.7 KB)

msfadmin@metasploitable:~$ _
```



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)~[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255 command to quit
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 170 bytes 18787 (18.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 90 bytes 7628 (7.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

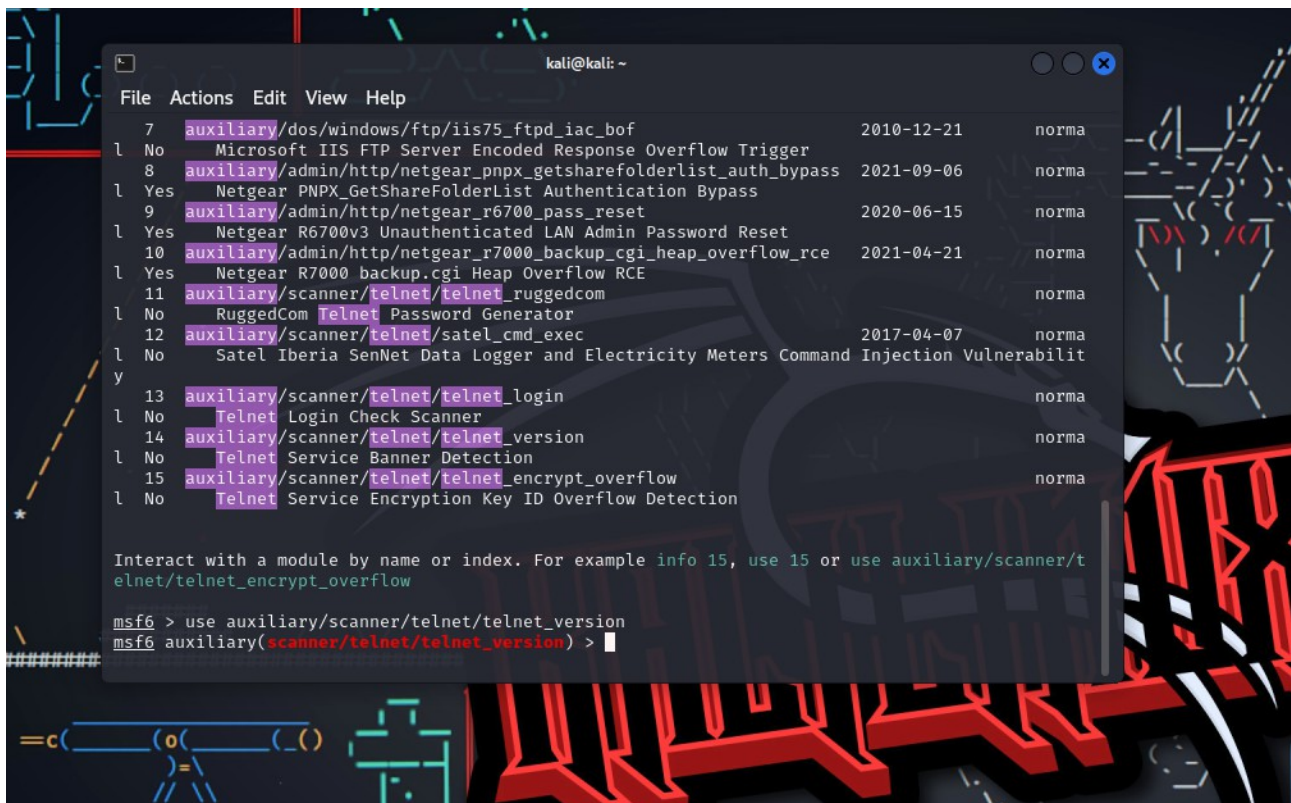
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6 bytes 356 (356.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 356 (356.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Warning: TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

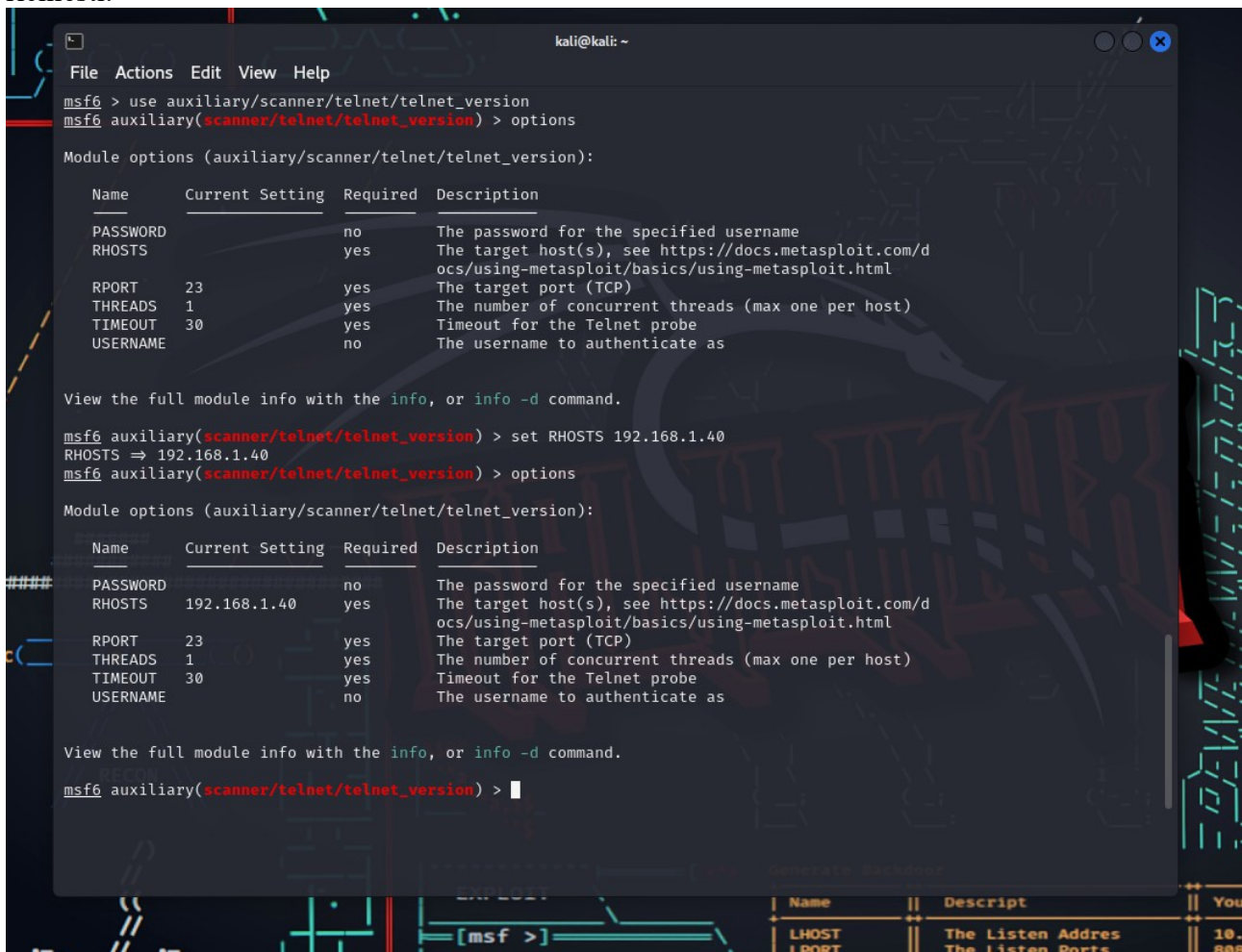
Contact: msfdev[at]metasploit.com
(kali@kali)~[~]
$ _ with msfadmin/msfadmin to get started

metasploitable login: msfadmin
password:
```

Una volta modificati gli indirizzi ip apriamo la console di Metasploit e andiamo a ricercare e selezionare il modulo relativo a telnet.



Individuato e caricato il modulo ausiliario per Telnet andiamo a controllare ed impostare i valori richiesti.



Una volta configurato con l'ip della macchina vittima(Metasploitable 2) lo lanciamo e otteniamo i dati relativi a telnet.

File Actions Edit View Help

```
Trying 192.169.1.40 ...
telnet: Unable to connect to remote host: No route to host
msf6 auxiliary(scanner/telnet/telnet_version) > Interrupt: use the 'exit' command to quit
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 '^'.
```

metasploit

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin

Password:

Last login: Tue Mar 5 03:25:34 EST 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:~\$

msfadmin@metasploitable:~\$

Generate Backdoor

EXPLOIT

Name	Description
LHOST	The Listen Address