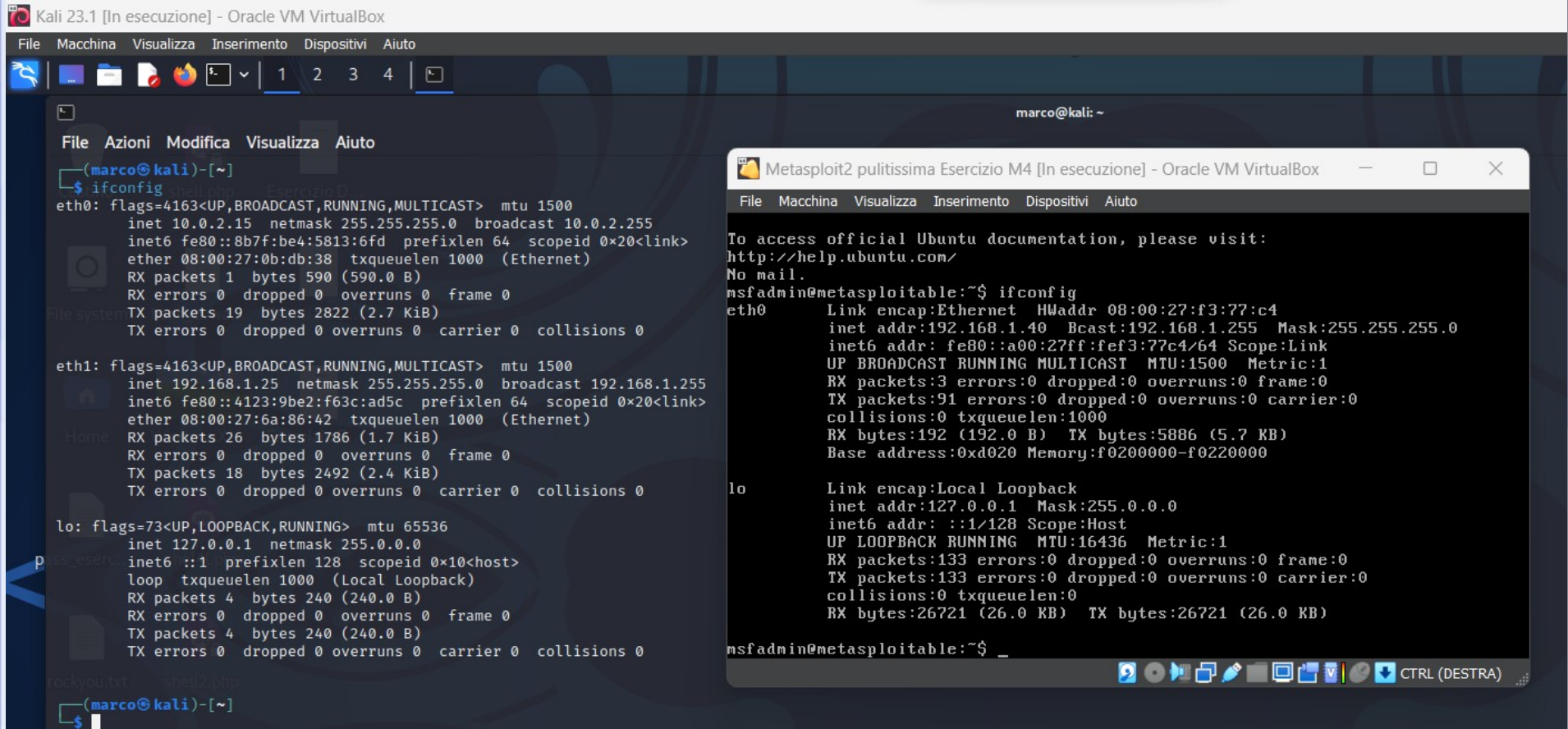


# ESERCIZIO M4 D7

- Exploit TELNET (Metasploitable2)

# Cambio indirizzi IP



The image shows two overlapping Oracle VM VirtualBox windows. The background window is titled 'Kali 23.1 [In esecuzione] - Oracle VM VirtualBox' and shows a terminal session where the user 'marco' has run the 'ifconfig' command. The output shows three network interfaces: eth0 (10.0.2.15), eth1 (192.168.1.25), and lo (127.0.0.1). The foreground window is titled 'Metasploit2 pulitissima Esercizio M4 [In esecuzione] - Oracle VM VirtualBox' and shows a terminal session where the user 'msfadmin' has run the 'ifconfig' command. The output shows the same three interfaces, but with different IP addresses: eth0 (192.168.1.40), eth1 (192.0.0.1), and lo (127.0.0.1). The user 'msfadmin' has also run the 'ip netns exec' command to change the IP address of the 'lo' interface to 127.0.0.1.

```
(marco@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::8b7f:be4:5813:6fd prefixlen 64 scopeid 0<20<link>  
    ether 08:00:27:0b:db:38 txqueuelen 1000 (Ethernet)  
    RX packets 1 bytes 590 (590.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 19 bytes 2822 (2.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::4123:9be2:f63c:ad5c prefixlen 64 scopeid 0<20<link>  
    ether 08:00:27:6a:86:42 txqueuelen 1000 (Ethernet)  
    RX packets 26 bytes 1786 (1.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 18 bytes 2492 (2.4 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 0<10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(marco@kali)-[~]  
$
```

```
Metasploit2 pulitissima Esercizio M4 [In esecuzione]  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:f3:77:c4  
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fef3:77c4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:192 (192.0 B)  TX bytes:5886 (5.7 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:133 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:133 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:26721 (26.0 KB)  TX bytes:26721 (26.0 KB)  
  
msfadmin@metasploitable:~$
```

# msfconsole

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4

marco@kali: ~
File Azioni Modifica Visualizza Aiuto
-
0 exploit/linux/misc/asus_infosvr_auth_bypass_exec 2015-01-04 excellent No ASUS infosvr Auth Bypass Command Execution
1 exploit/linux/http/asuswrt_lan_rce 2018-01-22 excellent No AsusWRT LAN Unauthenticated Remote Code Execution
2 auxiliary/server/capture/telnet normal No Authentication Capture: telnet
3 auxiliary/scanner/telnet/brocade_enable_login normal No Brocade Enable Login Check Scanner
4 exploit/windows/proxy/ccproxy/telnet_ping 2004-11-11 average Yes CCProxy telnet Proxy Ping Overflow
5 auxiliary/dos/cisco/ios/telnet_rocem 2017-03-17 normal No Cisco IOS telnet Denial of Service
6 auxiliary/admin/http/dlink_dir_300_600_exec_noauth 2013-02-04 normal No D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
7 exploit/linux/http/dlink_diagnostic_exec_noauth 2013-03-05 excellent No D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
8 exploit/linux/http/dlink_dir300_exec_telnet 2013-04-22 excellent No D-Link Devices Unauthenticated Remote Command Execution
9 exploit/unix/webapp/dogfood_spell_exec 2009-03-03 excellent Yes Dogfood CRM spell.php Remote Command Execution
10 exploit/freebsd/telnet/telnet_encrypt_keyid 2011-12-23 great No FreeBSD telnet Service Encryption Key ID Buffer Overflow
11 exploit/windows/telnet/gamsoft_telnet_username 2000-07-17 average Yes GAMSoft TelSrv 1.5 Username Buffer Overflow
12 exploit/windows/telnet/goodtech_telnet 2005-03-15 average No GoodTech telnet Server Buffer Overflow
13 exploit/linux/misc/hp_jetdirect_path_traversal 2017-04-05 normal No HP Jetdirect Path Traversal Arbitrary Code Execution
14 exploit/linux/http/huawei_hg532n_cmdinject 2017-04-15 excellent Yes Huawei HG532n Command Injection
15 exploit/linux/misc/igel_command_injection 2021-02-25 excellent Yes Igel OS Secure VNC/Terminal Command Injection RCE
16 auxiliary/scanner/ssh/juniper_backdoor 2015-12-20 normal No Juniper SSH Backdoor Scanner
17 auxiliary/scanner/telnet/lantronix_telnet_password normal No Lantronix telnet Password Recovery
18 auxiliary/scanner/telnet/lantronix_telnet_version normal No Lantronix telnet Service Banner Detection
19 exploit/linux/telnet/telnet_encrypt_keyid 2011-12-23 great No Linux BSD-derived telnet Service Encryption Key ID Buffer Overflow
20 auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21 normal No Microsoft IIS FTP Server Encoded Response Overflow Trigger
21 exploit/linux/telnet/netgear_telnetenable 2009-10-30 excellent Yes NETGEAR telnetEnable
22 auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass 2021-09-06 normal Yes Netgear PNPX_GetShareFolderList Authentication Bypass
23 auxiliary/admin/http/netgear_r6700_pass_reset 2020-06-15 normal Yes Netgear R6700v3 Unauthenticated LAN Admin Password Reset
24 auxiliary/admin/http/netgear_r7000_backup.cgi_heap_overflow_rce 2021-04-21 normal Yes Netgear R7000 backup.cgi Heap Overflow RCE
25 exploit/unix/misc/polycom_hdx_auth_bypass 2013-01-18 normal Yes Polycom Command Shell Authorization Bypass
26 exploit/unix/misc/polycom_hdx_traceroute_exec 2017-11-12 excellent Yes Polycom Shell HDX Series Traceroute Command Execution
27 exploit/freebsd/ftp/proftpd_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b telnet IAC Buffer Overflow (FreeBSD)
28 exploit/linux/ftp/proftpd_telnet_iac 2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.3b telnet IAC Buffer Overflow (Linux)
29 auxiliary/scanner/telnet/telnet_ruggedcom normal No RuggedCom telnet Password Generator
30 auxiliary/scanner/telnet/satel_cmd_exec 2017-04-07 normal No Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
31 exploit/solaris/telnet/ttprompt 2002-01-18 excellent No Solaris in.telnetd TTYPROMPT Buffer Overflow
32 exploit/solaris/telnet/fuser 2007-02-12 excellent No Sun Solaris telnet Remote Authentication Bypass Vulnerability
33 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection 2015-12-20 excellent No TP-Link SC2020n Authenticated telnet Injection
34 auxiliary/scanner/telnet/telnet_login normal No telnet Login Check Scanner
35 auxiliary/scanner/telnet/telnet_version normal No telnet Service Banner Detection
36 auxiliary/scanner/telnet/telnet_encrypt_overflow normal No telnet Service Encryption Key ID Overflow Detection
37 payload/cmd/unix/bind_busybox_telnetd normal No Unix Command Shell, Bind TCP (via BusyBox telnetd)
38 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
39 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
40 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
41 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great Yes VyOS restricted-shell Escape and Privilege Escalation
42 post/windows/gather/credentials/mremote normal No Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote
msf6 > use 35
```



# Set delle opzioni dell'Exploit

```
msf6 > use 35 telnet.php
msf6 auxiliary(scanner/telnet/telnet_version) > show 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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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 rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

