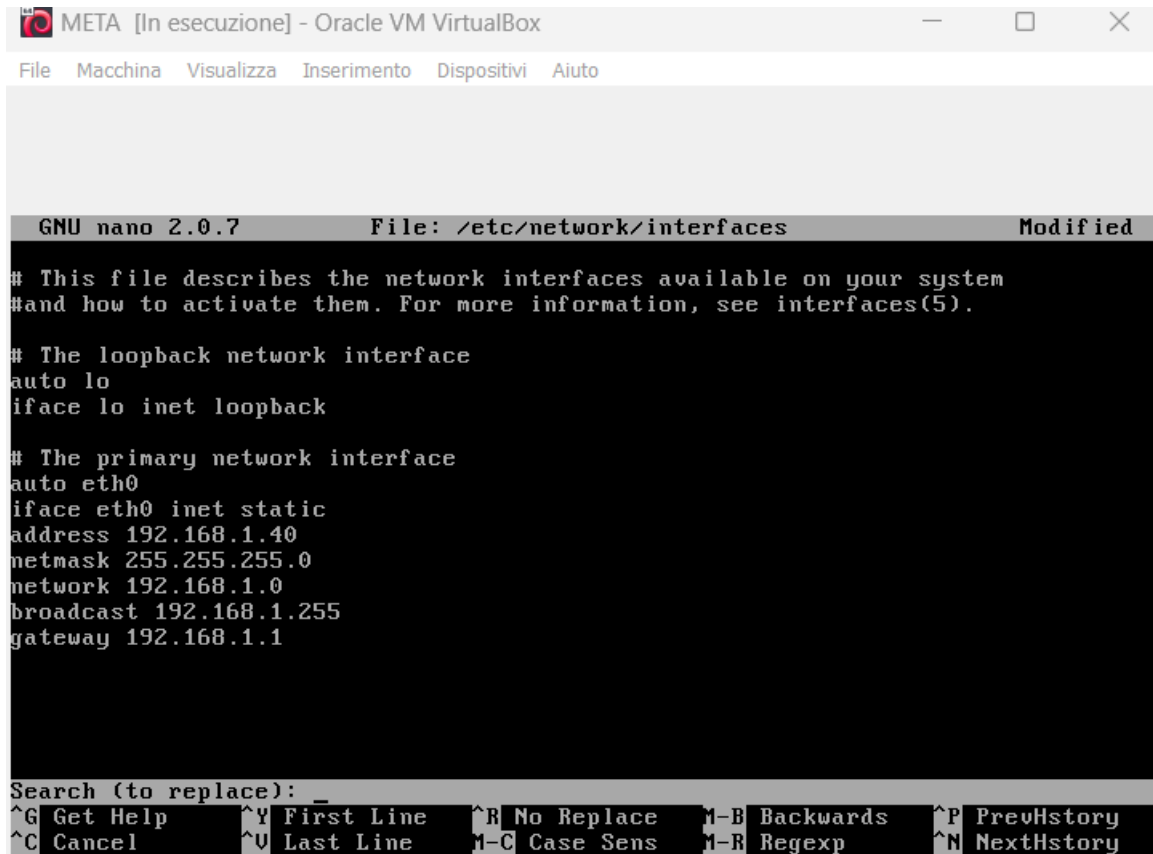


**“TRACCIA”**

**“RISOLUZIONE”**

**“CONFIGURAZIONE DI META”**



The screenshot shows a terminal window titled "META [In esecuzione] - Oracle VM VirtualBox". The window contains a nano 2.0.7 editor editing the file /etc/network/interfaces. The file content is as follows:

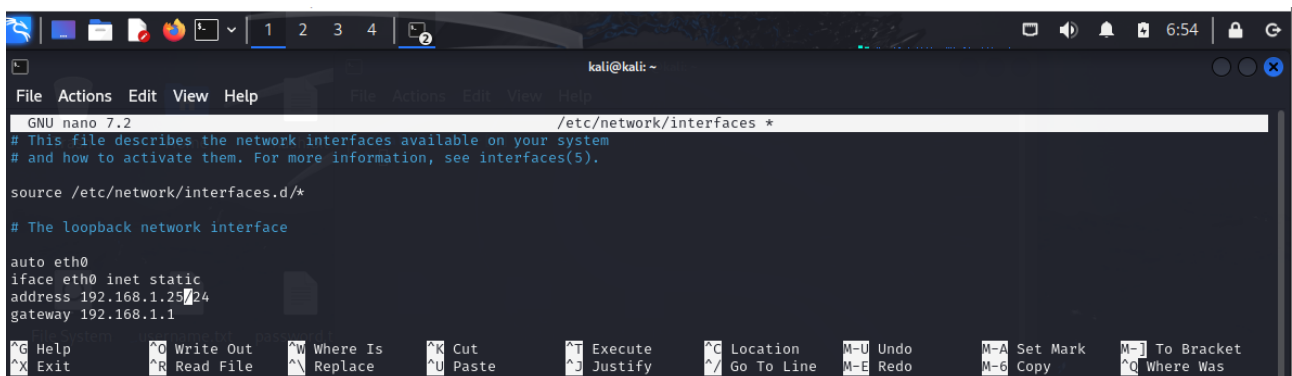
```
# This file describes the network interfaces available on your system
#and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

The bottom of the window shows the nano editor's status bar with search and navigation options.

**“CONFIGURAZIONE DI RETE KALI”**



The screenshot shows a terminal window titled "kali@kali: ~". The window contains a nano 7.2 editor editing the file /etc/network/interfaces. The file content is as follows:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto eth0
iface eth0 inet static
address 192.168.1.254
gateway 192.168.1.1
```

The bottom of the window shows the nano editor's status bar with search and navigation options.

## “PING TRA LE DUE MACCHINE PER CONSTATARE IL FUNZIONAMENTO”

```
ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=2.34 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.83 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=2.20 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.510 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.539 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.793 ms
64 bytes from 192.168.1.40: icmp_seq=7 ttl=64 time=0.509 ms
64 bytes from 192.168.1.40: icmp_seq=8 ttl=64 time=1.48 ms
64 bytes from 192.168.1.40: icmp_seq=9 ttl=64 time=0.453 ms
64 bytes from 192.168.1.40: icmp_seq=10 ttl=64 time=0.390 ms
64 bytes from 192.168.1.40: icmp_seq=11 ttl=64 time=0.567 ms
64 bytes from 192.168.1.40: icmp_seq=12 ttl=64 time=3.66 ms
64 bytes from 192.168.1.40: icmp_seq=13 ttl=64 time=0.475 ms
64 bytes from 192.168.1.40: icmp_seq=14 ttl=64 time=0.515 ms
64 bytes from 192.168.1.40: icmp_seq=15 ttl=64 time=2.27 ms
64 bytes from 192.168.1.40: icmp_seq=16 ttl=64 time=0.469 ms
```

```
No mail.
msfadmin@metasploitable:~$ ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.746 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=2.66 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.976 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.594 ms
64 bytes from 192.168.1.25: icmp_seq=5 ttl=64 time=0.064 ms
64 bytes from 192.168.1.25: icmp_seq=6 ttl=64 time=0.907 ms
64 bytes from 192.168.1.25: icmp_seq=7 ttl=64 time=0.540 ms
```

Come possiamo constatare le due macchine si connettono perfettamente sulla rete e sono pronte ad interagire

## “UTILIZZO DEL TELNET ATTRAVERSO IL TOOL METASPLOIT”

### - AVVIO DEL TOOL

Cmd = <msfconsole>

```
msf@kali:~/msf$ msfconsole
Metasploit tip: After running db_map, be sure to check out the result
of hosts and services

*Neutrin0 Cannon*PrettyBeefy*PostalTime*binbash*deadst0nauts*EvilBunny*Wrote
*LITMail.ruw() { ;;}; echo vulnerable*
*Team sorcerer*ADMC*HsionQuadesocialdistancing*LeukeTeamKaas*OWASP Moncton
*Algora*evill*Vampire Bunnie*ADP55*
*QuePas*ZombiesAndFriends*MetSecBG*coincoin*Shroom2*Slow Coders*Scavenger Sec
urity*Drub*MoTeam*Feminal Cult*
*edopler*RFQ*Magnum*ats*evill*scuzski*AlphaPwners*FILANA*Raffaella*HackSu
rvivett*outout*HackSouth*Corax*yeeb01z*
*SKUA*Cyber CORBA*Flaghunters*CDAI Generated*SEC*p3nm3d*IFS*CTF_Circle*I
moteLab*basdf*Hobbit*Switchers*8n00ds*
*IPwns - Intergalactic Team of PWNers*PCSquared*fr334aks*runQND*194*Kapit
al Kzrkens*ReddyPlayer1337*from 44*
*HACKS*H0w*InfoSec*CTF Community*DCZia*NicWay*9*BlueSky*ME*Tipi*Hack*Porg P
wn Platoon*Hackerty*hackstreetboys*
*Ideagines*87*eggcellent*Husceid7*localhorst*Original Cyan Lonkers*Sad_Pand
a*Fals*Flag*OurHeart*leeds*Orange*GBMASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz
*VulSec*enorbit*Delta Squad Zero*Hukehe*
*x00-x00*BlackCat*ARE5x*cpw*vaporsec*purplehax*RedTeamMTU*UsalamaTeam*vitali
pk*RISC*forkbomb44*hoonowbrowncow
*ethermot*cheesehagurt*leedmg*side*FRJND5*badfirmware*Cut3D*4g8n*dc615*nora
*Polaris One*team*hall hydra*Takoyaki*
*Sudo Society*incognito-Flash*TheScientists*Tea Party*Reapers of Pwname*OldBo
ys*Whill37*118137*HearShaw*DC54b*
*IMosuke*Infosec_zitron*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber*T
HMC*The_Pirhacks*btwinseArch*MadDaws*
*HilceThe Pigthy Mangle*line*CSF_RandSec*x4n8n*x8rc3r3rs*emhacc*Ph4n70n_R34p3r
*Hunz1q*Preeminence*UMGC*8*te8Brigade*
*TeamFastMark*Townson-Cyberkat*meow*xrzhev*PA Hackers*Kuolena*Nakateam*Logi
c8m*H0WA*InfoSec*teamstyle*Panice
*BBNG8R3*
*Les Cadets Rouges*bufx
*Les Tontons Flag*ewrta
*484 : Flag Not Founde
* UNION SELECT 'password'
*OC2K7*Sparkle Pony*
```

## - RICERCA DEL TELNET

Cmd = < search telnet >



## - USO DELLA PATCH N°35 <AUXILIARY/SCANNER/TELNET/TELNET\_VERSION> E CONTROLLO DELLE OPZIONI DI CONFIGURAZIONE

Cmd = < use 35> “utilizzo della patch”

Cmd = < show options> “visualizzazione delle opzioni di configurazione”

```
msf6 > use 35
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 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.
```

## - IMPOSTAZIONE DEL TARGET (RHOSTS)

Cmd = <set RHOSTS “IP BERSAGLIO”>

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
```

## - ESTRAPOLAZIONE DEI DATI DI ACCESSO AL SISTEMA (FASE DI EXPLOIT)

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 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
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Da questo possiamo evincere i dati di accesso al sistema che saranno

User : msfadmin

Password : msfadmin

## - CONNESSIONE AL DISPOSITIVO CON LE CREDENZIALI SOPRA CITATE CON TOOL TELNET

Cmd = < telnet “ip bersaglio”>

```
(root@kali) ~/home/kali  
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: