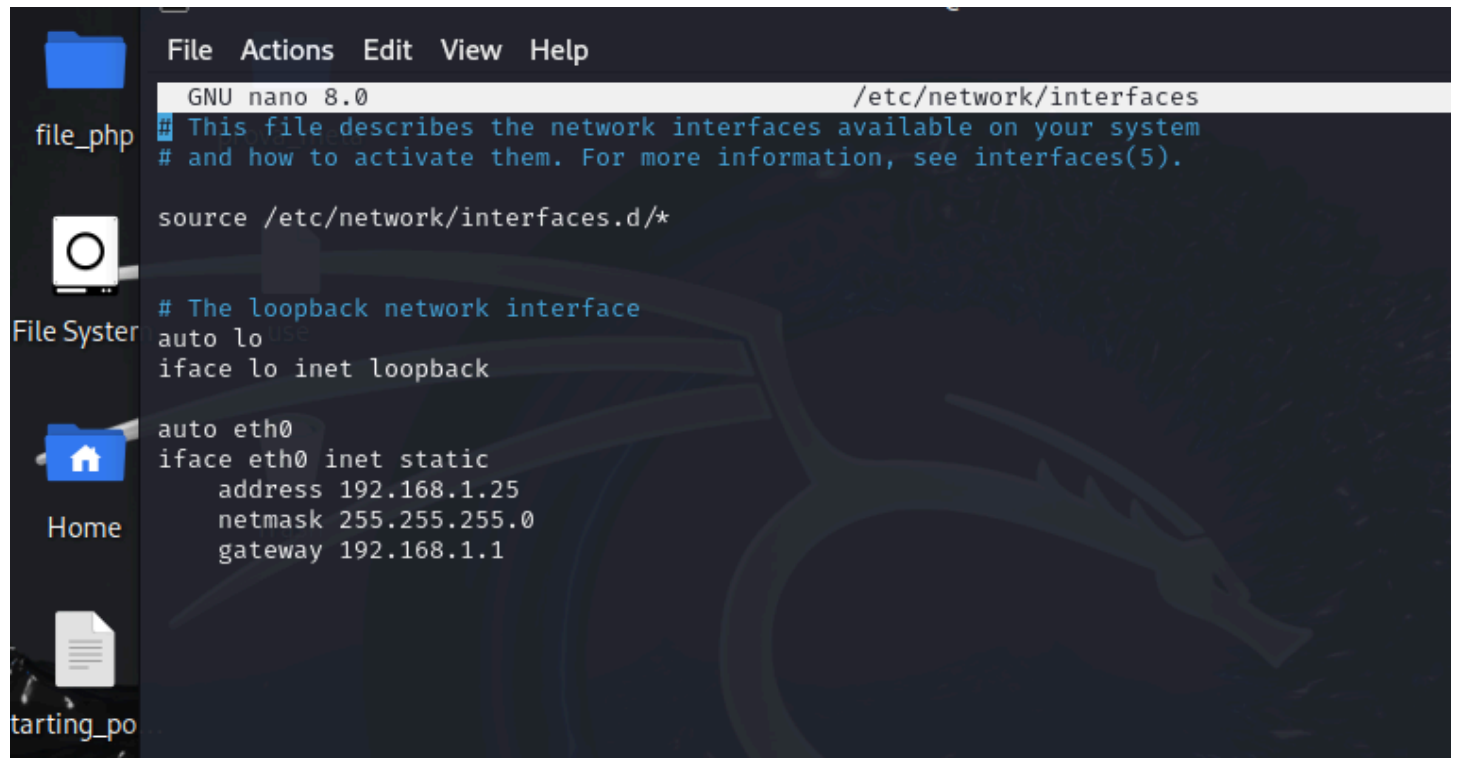


# S7-L2

Nel primo passaggio vediamo come cambiare l'IP su Kali tramite il comando "sudo nano /etc/network/interfaces"



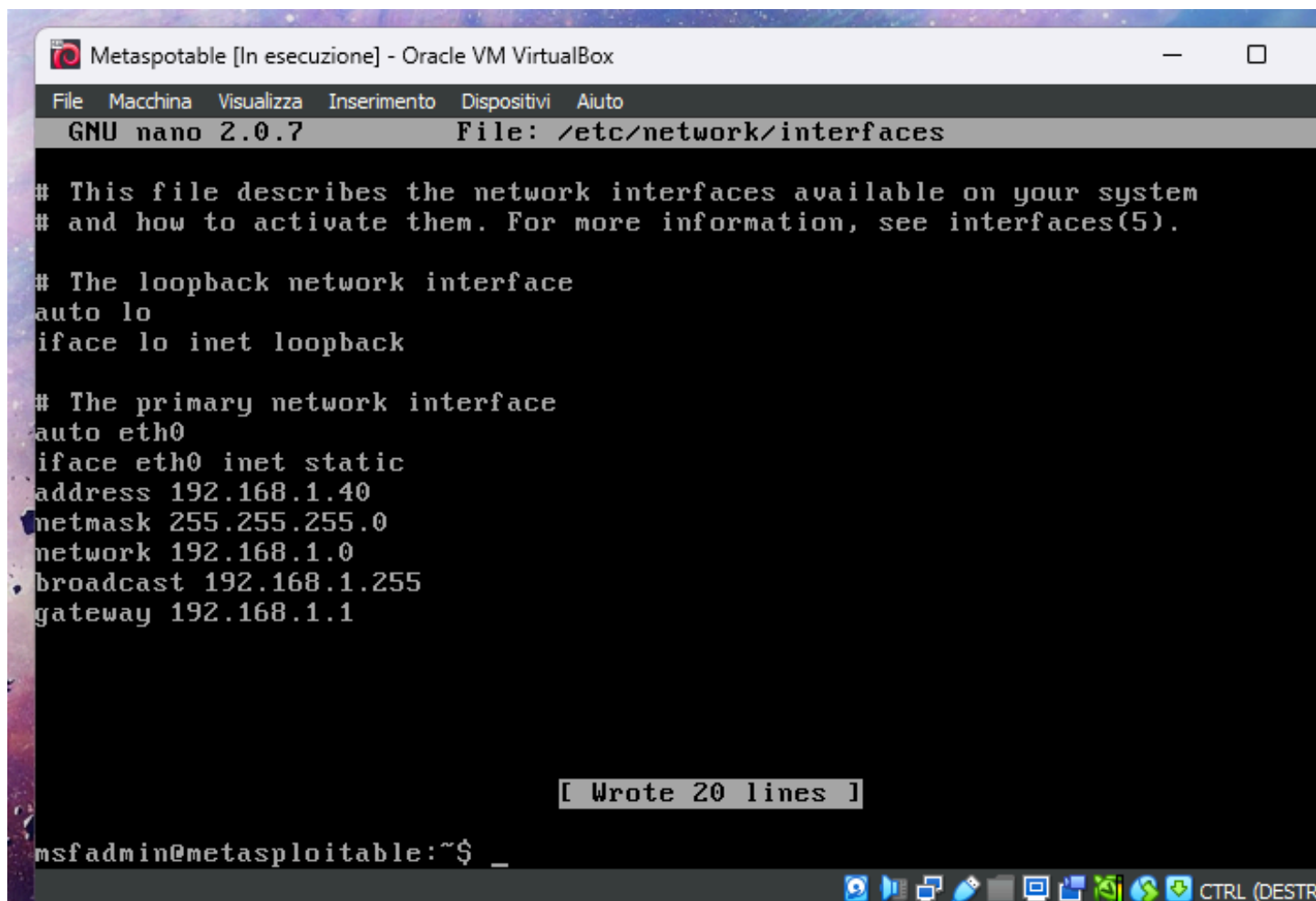
```
File Actions Edit View Help
GNU nano 8.0 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.1.25
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Nel secondo passaggio configuriamo l'ip di Metasploit con lo stesso comando, siccome è sempre una distribuzione Linux.



```
Metaspotable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7  File: /etc/network/interfaces

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

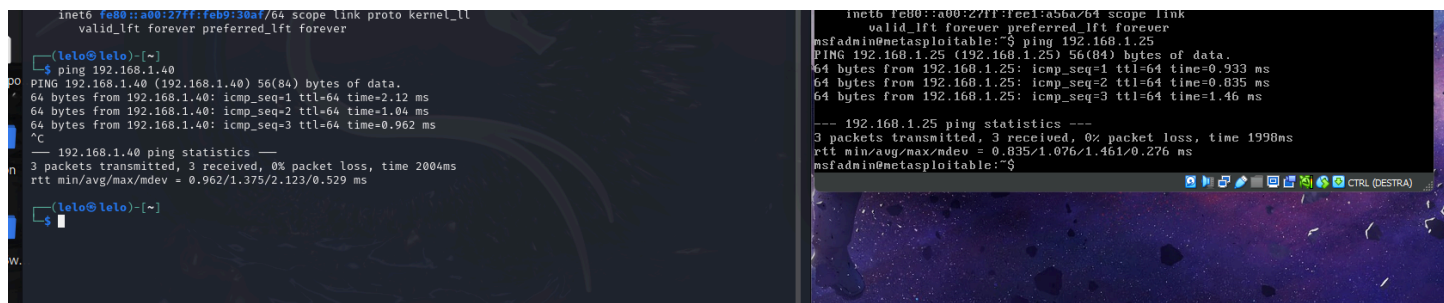
# The loopback network interface
auto lo
iface lo inet loopback

# 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

[ Wrote 20 lines ]

msfadmin@metasploitable:~$
```

Questa è la dimostrazione del ping tra le due macchine messe in rete interna.



```
inet6 fe80::a00:27ff:feb9:30af/64 scope link proto kernel ll
valid_lft forever preferred_lft forever

(lolo@lolo)-[~]
$ 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=2.12 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.962 ms
^C
--- 192.168.1.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.962/1.375/2.123/0.529 ms

(lolo@lolo)-[~]

inet6 fe80::a00:27ff:feb9:30af/64 scope link
valid_lft forever preferred_lft forever
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=0.933 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.835 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=1.46 ms
^C
--- 192.168.1.25 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1990ms
rtt min/avg/max/mdev = 0.835/1.076/1.461/0.276 ms
msfadmin@metasploitable:~$
```

Successivamente avviamo msfconsole per avere attiva l'interfaccia della console del framework Metasploit.

```
(lelo@lelo)-[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

Travis

< HONK >

e

+ -- ==[ metasploit v6.3.55-dev ]
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

Tramite un "nmap -f 192.168.1.40", possiamo vedere che la porta 23 telnet è aperta e quindi possiamo collegarci.

```

(lelo@lelo)-[~]
$ sudo nmap -f 192.168.1.40
[sudo] password for lelo:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 15:07 CEST
Nmap scan report for 192.168.1.40
Host is up (0.011s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8180/tcp  open  unknown
MAC Address: 08:00:27:E1:A5:6A (Oracle VirtualBox virtual NIC)

```

Ho eseguito il comando “search telnet\_version” in Metasploit e il risultato mostra due moduli ausiliari (auxiliary) relativi alla rilevazione delle versioni del servizio Telnet

```

msf6 > search telnet_version

Matching Modules
=====
#  Name
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version
ice Banner Detection
1  auxiliary/scanner/telnet/telnet_version
Detection

Disclosure Date  Rank  Check  Description
-----
                normal No      Lantronix Telnet Serv
                normal No      Telnet Service Banner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_vers
ion
msf6 >

```

Il comando “show options” mostra le opzioni globali configurate nel framework Metasploit. Queste opzioni sono impostazioni generali che si applicano a tutte le sessioni di Metasploit.

Mentre il comando "use 1" seleziona il modulo telnet\_version per l'uso. Il numero "1" si riferisce all'indice del modulo elencato precedentemente con il comando search telnet\_version.

```
msf6 > show options

Global Options:

Option           Current Setting  Description
-----
ConsoleLogging   false           Log all console input and output
LogLevel         0              Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter     The meterpreter prompt string
MinimumRank      0              The minimum rank of exploits that will run without explicit confirmation

Prompt           msf6           The prompt string
PromptChar       >             The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging   false          Log all input and output for sessions
SessionTlvLogging false          Log all incoming and outgoing TLV packets
TimestampOutput  false          Prefix all console output with a timestamp

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

"msf6 auxiliary(scanner/telnet/telnet\_version) > set rhost 192.168.1.40". Questo comando imposta l'opzione RHOSTS per specificare l'host remoto da scansionare. In questo caso, l'host remoto ha l'IP 192.168.1.40.

Mostro nuovamente le opzioni configurate per il modulo, confermando che l'opzione RHOSTS è stata impostata correttamente a 192.168.1.40.

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-----
PASSWORD  no              no        The password for the specified username
RHOSTS    yes             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              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) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

Name      Current Setting  Required  Description
-----
PASSWORD  no              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              no        The username to authenticate as

View the full module info with the info, or info -d command.

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

Qui ho eseguito il comando “run” che avvia l'esecuzione del modulo telnet\_version, che cerca di rilevare la versione del servizio Telnet in esecuzione sull'host target (192.168.1.40) sulla porta 23. Possiamo anche vedere che lo scan è riuscito, e mostra il banner con i dati per fare il login e password.

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

Qui possiamo vedere la connessione diretta con il comando “telnet 192.168.1.40”

```
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 '^]'.  
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Dopo aver ottenuto i dati per fare l'accesso, sono acceduto e dimostrato grazie al comando “Ip a” di essere all'interno.



