

Per l'esercizio di oggi, iniziamo con le configurazioni di rete delle macchine virtuali Metasploitable e Kali Linux, con indirizzi ip relativamente 192.168.1.40 e 192.168.1.25

```
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
gateway 192.168.1.1

[ Read 16 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^U Next Page ^U UnCut Text ^T To Spell
```

Editing Wired connection 1

Connection name: **Wired connection 1**

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method: **Manual**

Addresses

Address	Netmask	Gateway
192.168.1.25	24	192.168.1.1

DNS servers:

Search domains:

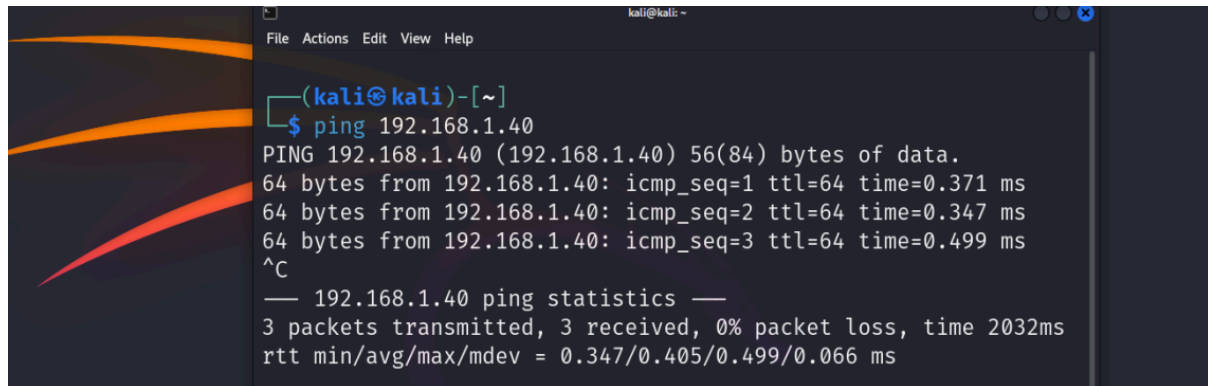
DHCP client ID:

☒ Require IPv4 addressing for this connection to complete

Routes...

Cancel Save

Una volta configurate, verifichiamo la connessione tra le due macchine:



```
(kali㉿kali)-[~]  
$ 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=0.371 ms  
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.347 ms  
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.499 ms  
^C  
— 192.168.1.40 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2032ms  
rtt min/avg/max/mdev = 0.347/0.405/0.499/0.066 ms
```

Data la traccia:

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary telnet_version` sulla macchina Metasploitable.

Viene richiesto di utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo *auxiliary telnet_version* sulla macchina Metasploitable.

Vulnerabilità Telnet sulla porta 23:




```
(kali㉿kali)-[~]  
$ nmap -sV -p 23 192.168.1.40  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 09:25 EDT  
Nmap scan report for 192.168.1.40 (192.168.1.40)  
Host is up (0.0052s latency).  
  
PORT      STATE SERVICE VERSION  
23/tcp    open  telnet  Linux telnetd  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Telnet è un protocollo di rete che consente agli utenti di accedere e gestire sistemi remoti tramite una connessione interattiva sulla

```
File Actions Edit View Help
```

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: You can pivot connections over sessions started  
with the  
ssh_login modules  
  
IIIIIII      dTb.dTb  
II           4' v 'B  
II          6. .P  
II         'T;. ;P'  
II        'T; ;P'  
IIIIIII     'YvP'
```



```
I love shells --egypt  
  
=[ metasploit v6.4.15-dev ]  
+ -- ==[ 2433 exploits - 1251 auxiliary - 428 post ]  
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > search telnet_version
```

Dopodiché cerchiamo il modulo in questione *auxiliary/scanner/telnet/telnet_version* attraverso **search telnet_version** e lo lanciamo utilizzando il comando **use 1**

```
# Name Disclo
sure Date Rank Check Description
- -
0 auxiliary/scanner/telnet/lantronix_telnet_version .
normal No Lantronix Telnet Service Banner Detec
tion
1 auxiliary/scanner/telnet/telnet_version .
normal No Telnet Service Banner Detection

Interact with a module by name or index. For example info 1, us
e 1 or use auxiliary/scanner/telnet/telnet_version

msf6 > use 1
```

Per usufruire correttamente di questo modulo, analizziamo le opzioni necessarie richieste attraverso il comando **show options**.

```
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
```

Quindi indichiamo il remote host (192.168.1.40), la porta remota 23, e il numero di threads. Metasploit imposta un valore predefinito per i threads, ma possiamo modificarlo in base alle nostre esigenze.

```
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) > set rport 23
rport => 23
msf6 auxiliary(scanner/telnet/telnet_version) > set threads 1
threads => 1
msf6 auxiliary(scanner/telnet/telnet_version) > set timeout 30
timeout => 30
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Dopodiché siamo pronti ad eseguire l'attacco con il comando **exploit**

[illegible]

Come si nota dalla figura, questo modulo ci mostra i dati di accesso al sistema con le credenziali *msfadmin/msfadmin*.

Eseguiamo una prova da Metasploitable per verificarne la veridicità.

```
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: msfadmin
Password:
Last login: Tue Jul 9 08:56:10 EDT 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:~$ ls
vulnerable
msfadmin@metasploitable:~$ ip a
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
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast glen 1000
    link/ether 08:00:27:17:e0:96 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe17:e096/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Effettivamente l'attacco è andato a buon fine, avendo avuto accesso non autorizzato al sistema.