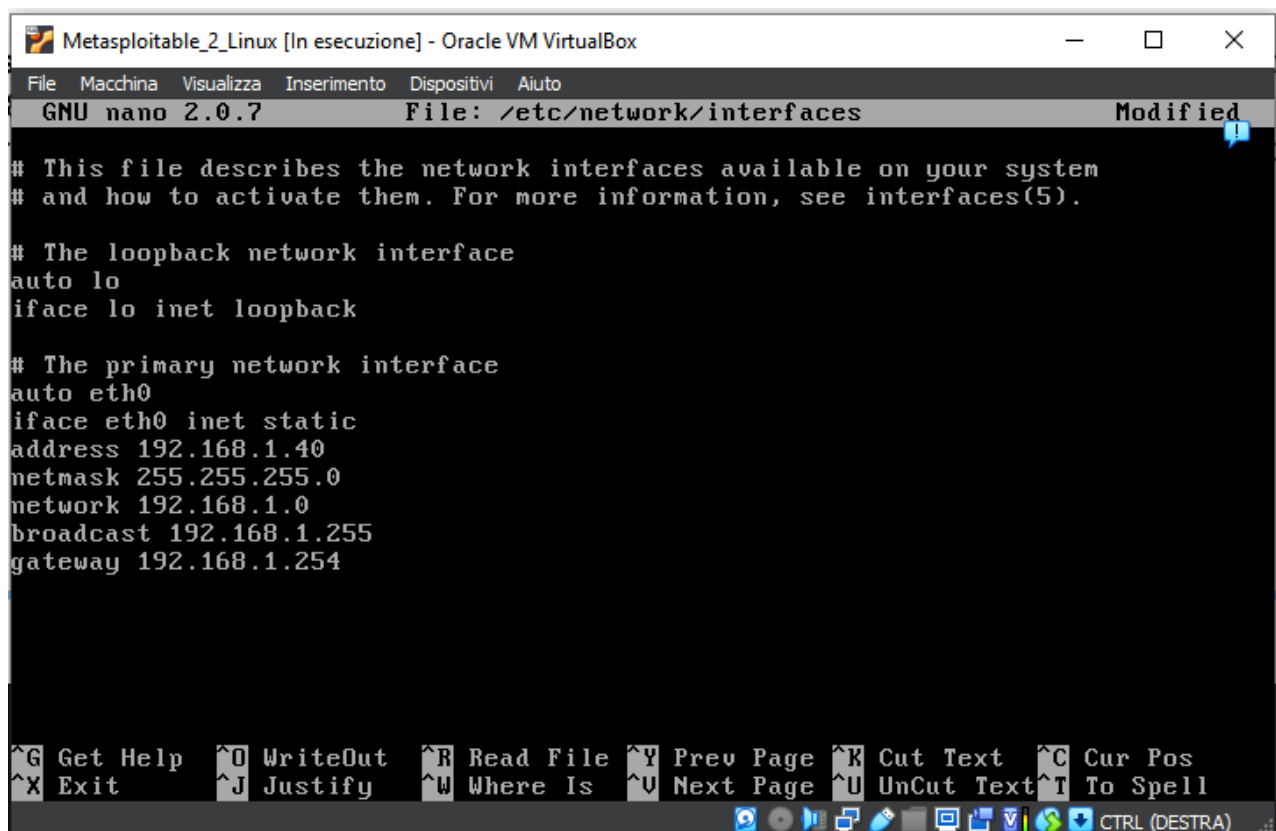


Esercizio S7 L2

Un exploit è un termine che si riferisce a un tipo di software o tecnica che sfrutta vulnerabilità o debolezze in un sistema informatico al fine di ottenere un accesso non autorizzato o eseguire azioni dannose.

Il protocollo Telnet è un protocollo di rete utilizzato per consentire a un utente di accedere e interagire con un sistema remoto tramite una connessione a una rete, come Internet.



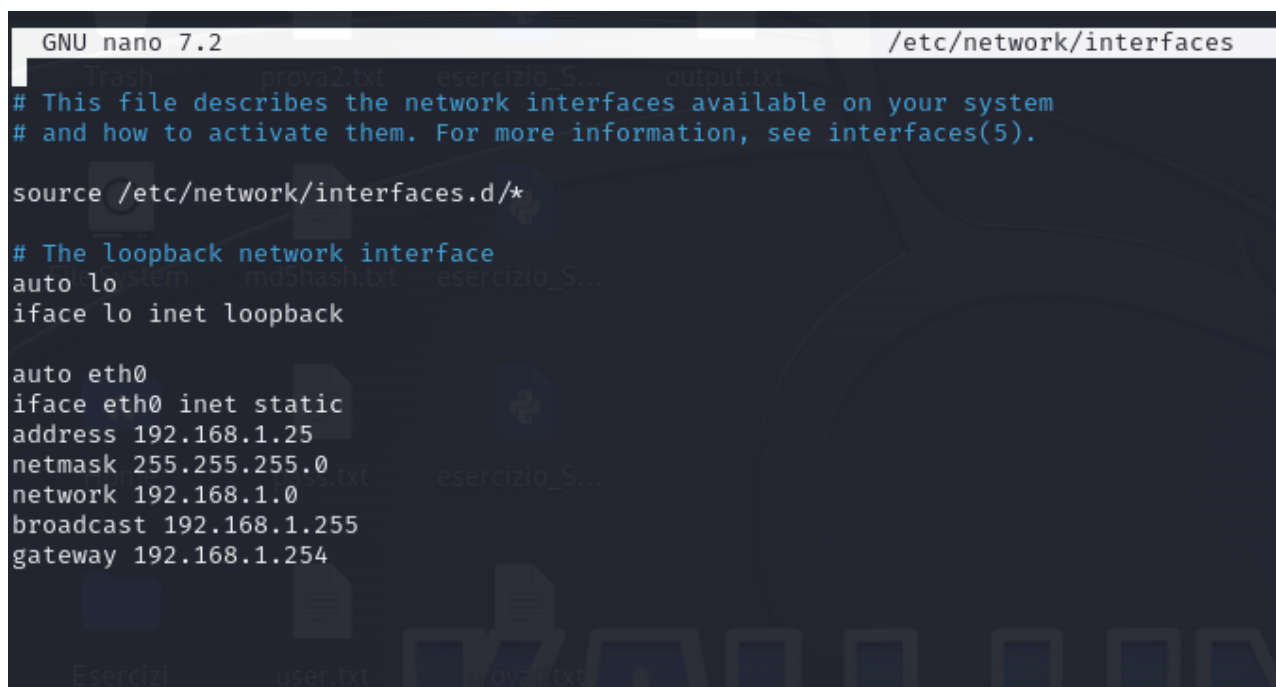
```
Metasploitable_2_Linux [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces      Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, 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 192.168.1.254

^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
CTRL (DESTRA)
```

Configuro Ip di metasploitable 2



```
GNU nano 7.2      /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
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.254
```

Configuro Ip di Kali

```

(kali@kali)-[~]
$ nmap -A -T4 192.168.1.40
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 06:18 EST
Stats: 0:02:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.51% done; ETC: 06:21 (0:00:00 remaining)
Stats: 0:03:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.87% done; ETC: 06:21 (0:00:00 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 06:22 (0:00:00 remaining)
Nmap scan report for 192.168.1.40
Host is up (0.00021s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 192.168.1.25
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateS/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

```

scansiono con nmap per verificare che la porta di telnet sia aperta

```

msf6 > use auxiliary/scanner/telnet/telnet_version
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.html">https://docs.metasploit.com/docs/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) > show options

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



| Name     | Current Setting | Required | Description                                                                                                                                         |
|----------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                                                             |
| RHOSTS   | 192.168.1.40    | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit.html">https://docs.metasploit.com/docs/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) >

```

Utilizzo metasploit per sfruttare la vulnerabilità di telnet configurando l'ip target con quello di metasploitable

```

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) >

```

L'exploit ci mostra le credenziali di telnet

```
(kali@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 Nov  7 06:16:57 EST 2023 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:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:58:10:a1
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:a3d:c3e9:a00:27ff:fe58:10a1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe58:10a1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2910 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2249 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:285304 (278.6 KB)  TX bytes:207616 (202.7 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:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
```

Testiamo che le credenziali siano corrette e utilizziamo il comando ifconfig per verificare che siamo realmente collegati a metasploitable