

S7L2

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.

Requisito:

Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Obiettivo

Utilizzare **Metasploit** per analizzare il servizio **Telnet** esposto su **Metasploitable2**, rilevandone la versione tramite il modulo auxiliary/scanner/telnet/telnet_version.

Configurazione IP

Kali Linux

```
sudo ip addr add 192.168.1.25/24 dev eth0
```

```
sudo ip link set eth0 up
```

Metasploitable2

```
sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0 up
```

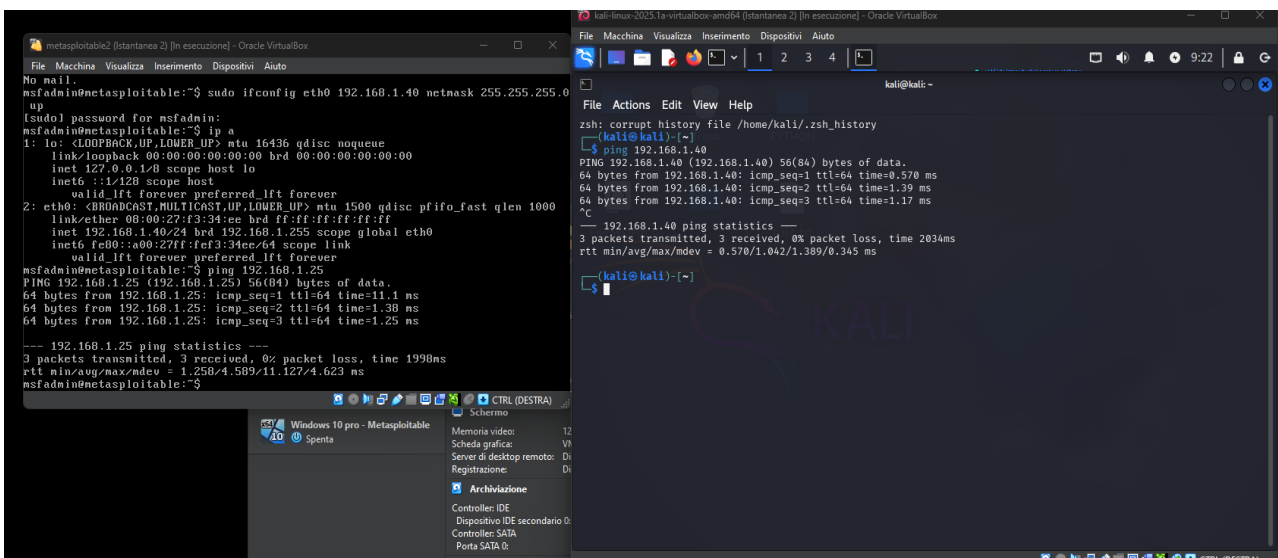
Verifica con ping

- Da Kali:

```
ping 192.168.1.40
```

- Da Metasploitable:

```
ping 192.168.1.25
```



```
set RHOSTS 192.168.1.40
```

```
kali@kali: ~  
File Actions Edit View Help  
n swapper task - not syncing  
Home Trash PYTHON  
-- ==[ metasploit v6.4.56-dev ]  
-- ==[ 2505 exploits - 1291 auxiliary - 431 post ]  
-- ==[ 1610 payloads - 49 encoders - 13 nops ]  
-- ==[ 9 evasion ]  
metasploit Documentation: https://docs.metasploit.com/  
sf6 > use auxiliary/scanner/telnet/telnet_version  
sf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40  
RHOSTS => 192.168.1.40  
sf6 auxiliary(scanner/telnet/telnet_version) > 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 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.  
sf6 auxiliary(scanner/telnet/telnet_version) > 
```

Mi accerto con il comando **options** che la configurazione di targhet sia corretta

Avvio la scansione:

Run

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
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       | The password for the specified username                                                                        |
| RHOSTS   | 192.168.1.40    | yes      | The target host(s), see https://docs.m<br>etasploit.com/docs/using-metasploit/basi<br>cs/using-metasploit.html |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                          |
| THREADS  | 1               | yes      | The number of concurrent threads (max o<br>ne 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) > 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: msfadmin/msfadmin
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Risultato della scansione

L'output ottenuto conferma:

- Il servizio **Telnet** è **attivo** sulla porta 23 di Metasploitable2.
- È stato rilevato il **banner del servizio**, che include:
 - Una grafica ASCII che conferma l'ambiente Metasploitable
 - Il messaggio: Login with msfadmin/msfadmin to get started

Conclusione

- La scansione è andata a buon fine: **Telnet è attivo e vulnerabile**, pronto per ulteriori fasi di test o attacco.
- Abbiamo identificato:
 - L'indirizzo IP del target (192.168.1.40)
 - Il servizio attivo (Telnet)
 - Le credenziali di default suggerite (msfadmin/msfadmin)

Prossimi step possibili

Accesso diretto via Telnet:

```
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 '^['.

```
. _ . _ | _ | / - \ - \ _ | _ | ( ) ^ _ | _ | | _ | _ | _ | _ |  
| | _ | _ | _ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  
_ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ |  
|_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_| |_|  
      |_|
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmind/msfdadmin to get started

metasploitable login: msfdadmin
Password:
Last login: Tue May 13 09:18:09 EDT 2025 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.

msfdadmin@metasploitable:~\$ █

```
use auxiliary/scanner/telnet/telnet_login
set RHOSTS 192.168.1.40
set USERNAME msfadmin
set PASSWORD msfadmin
run
```

Sfruttamento post-accesso (privilege escalation, pivot, ecc.)