

ESERCIZIO S7/L2

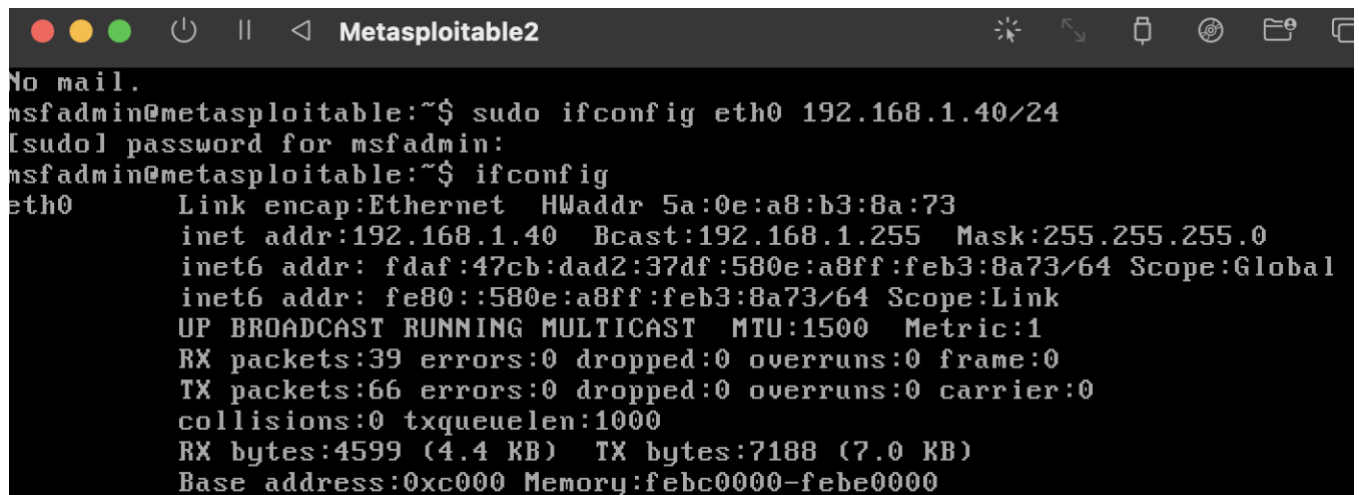
TRACCIA:

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

Per eseguire questo esercizio per prima cosa andiamo ad avviare le VM e cambiamo l'indirizzo IP di entrambe come richiesto dall'esercizio:

```
valid_lft forever preferred_lft forever
inet 192.168.1.25/24 scope global secondary eth0
    valid_lft forever preferred_lft forever
inet6 fdaf:47cb:dad2:37df:2077:e7ff:fe90:a3c5/64 scope global dynamic mngtmpaddr proto kernel_r
    valid_lft 2591885sec preferred_lft 604685sec
inet6 fe80::2077:e7ff:fe90:a3c5/64 scope link proto kernel_ll
    valid_lft forever preferred_lft forever
```



```
No mail.
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.40/24
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 5a:0e:a8:b3:8a:73
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fdaf:47cb:dad2:37df:580e:a8ff:feb3:8a73/64 Scope:Global
          inet6 addr: fe80::580e:a8ff:feb3:8a73/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4599 (4.4 KB)  TX bytes:7188 (7.0 KB)
          Base address:0xc000 Memory:feb00000-febe0000
```

Una volta settati gli IP proviamo a pingare per vedere se le macchine comunicano, facciamo la prova da entrambe le macchine:

```
Metasploitable2
collisions:0 txqueuelen:1000
RX bytes:4599 (4.4 KB) TX bytes:7188 (7.0 KB)
Base address:0xc000 Memory:febc0000-febe0000

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:97 errors:0 dropped:0 overruns:0 frame:0
TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21529 (21.0 KB) TX bytes:21529 (21.0 KB)

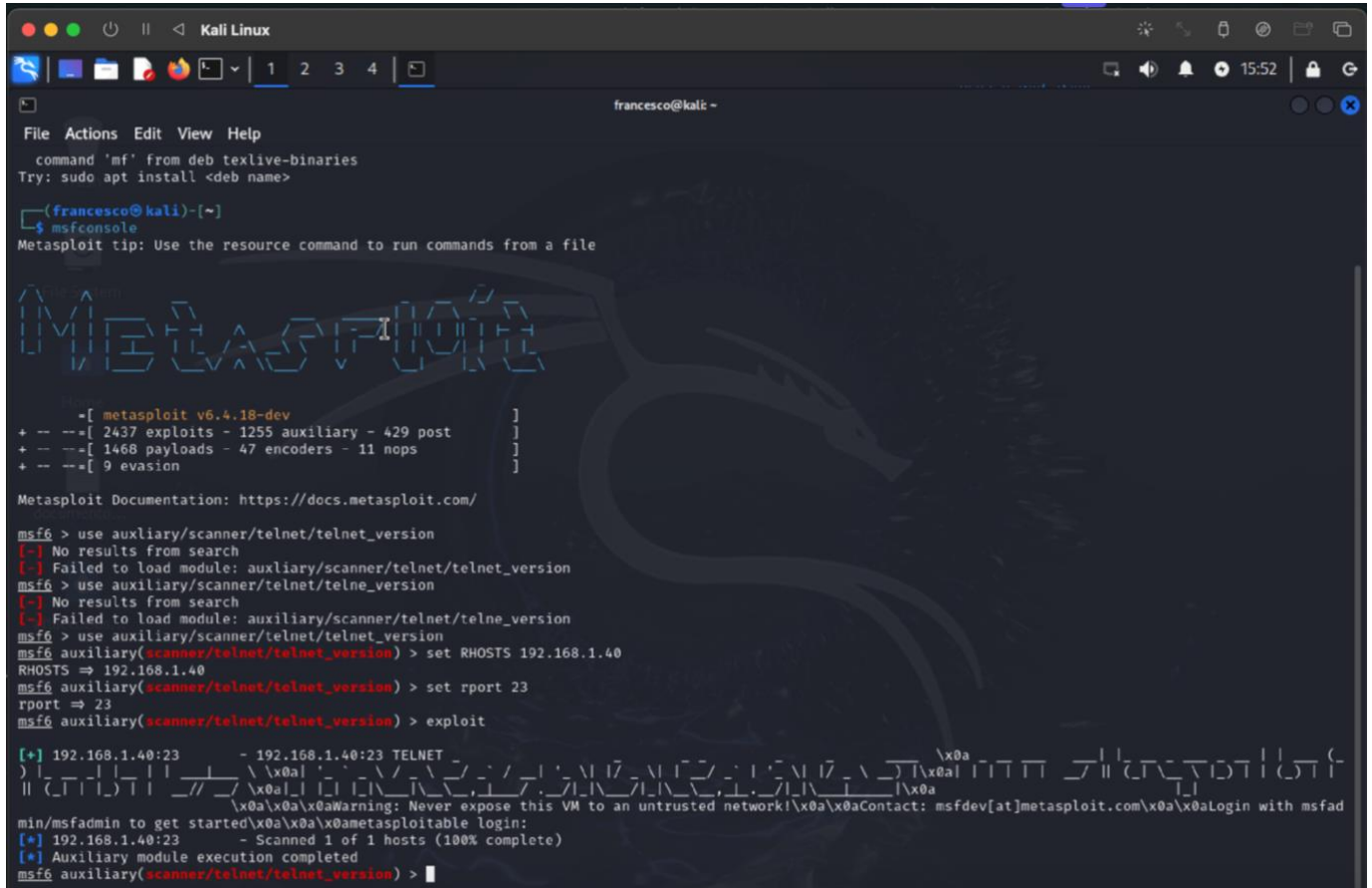
msfadmin@metasploitable:~$ ping -c 5 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=12.7 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=1.00 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.680 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.799 ms
64 bytes from 192.168.1.25: icmp_seq=5 ttl=64 time=0.840 ms

--- 192.168.1.25 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.680/3.215/12.752/4.769 ms
msfadmin@metasploitable:~$ _
```

```
Kali Linux
File Actions Edit View Help
zsh: corrupt history file /home/francesco/.zsh_history
(francesco@kali)-[~]
$ ping -c 5 192.168.1.40
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=1.13 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.787 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.987 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.782 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=1.02 ms

— 192.168.1.40 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4031ms
rtt min/avg/max/mdev = 0.782/0.942/1.133/0.137 ms
```

Una volta consolidata la connessione tra le macchine, possiamo procedere e sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary telnet_version` sulla macchina Metasploitable.



```
francesco@kali ~$ msfconsole
Metasploit tip: Use the resource command to run commands from a file

+-- metasploit v6.4.18-dev
+-- --[ 2437 exploits - 1255 auxiliary - 429 post
+-- --[ 1468 payloads - 47 encoders - 11 nops
+-- --[ 9 evasion

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

msf6 > use auxiliary/scanner/telnet/telnet_version
[-] No results from search
[-] Failed to load module: auxiliary/scanner/telnet/telnet_version
msf6 > use auxiliary/scanner/telnet/telne_version
[-] No results from search
[-] Failed to load module: auxiliary/scanner/telnet/telne_version
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > set rport 23
rport => 23
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
min/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) >
```

Con il comando ***msfconsole*** iniziamo ad interagire con Meta, successivamente settiamo l'host inserendo l'IP di Metasploitable con il seguente comando: ***set rhost 192.168.1.40***, e impostiamo manualmente la porta 23 con il comando: ***set rport 23***.

Una volta completati i passaggi precedenti, eseguiamo exploit ed attendiamo:

```
Kali Linux
francesco@kali: ~
File Actions Edit View Help
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scamer/telnet/telnet_version) > telnet 192.168.1.40 23
[*] exec: telnet 192.168.1.40 23

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

metasploitable

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

metasploitable login: msfadmin^H^H^H^H^H[[D
Password:
Login incorrect
metasploitable login: msfadmin
Password:
Last login: Tue Jan 21 09:27:04 EST 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.
msfadmin@metasploitable:~$
```

Dopo aver eseguito il comando exploit, ecco che ci appare la schermata principale di Metasploitable, dove sono specificati user e password, inserendoli entriamo nel sistema.

BONUS 1:

Il **servizio** distcc è un programma che permette di distribuire i processi di compilazione su più macchine in rete, in modo da velocizzare il processo di compilazione di codice sorgente su sistemi complessi. Distcc utilizza una architettura Client-Server, in cui il server (che esegue la compilazione vera e propria) è in grado di ricevere e processare le richieste di compilazione inviate dai client (di solito, altre macchine che inviano il codice da compilare).

Il **servizio** distcc è un programma che permette di distribuire i processi di compilazione su più macchine in rete, in modo da velocizzare il processo di compilazione di codice sorgente su sistemi complessi. distcc utilizza una architettura Client-Server, in cui il server (che esegue la compilazione vera e propria) è in grado di ricevere e

processare le richieste di compilazione inviate dai client (di solito, altre macchine che inviano il codice da compilare).

Distcc offre un utile strumento per la distribuzione delle compilazioni, ma se non protetto adeguatamente, può diventare un vettore di attacco. La sua vulnerabilità principale risiede nell'esposizione della porta di comunicazione senza un controllo sufficiente sull'autenticazione e sulla cifratura, rendendolo facilmente attaccabile in ambienti non sicuri. Per proteggere adeguatamente il servizio, è consigliabile:

- Limitare l'accesso alla porta 3632 tramite firewall.
- Utilizzare reti sicure e private per la comunicazione tra i nodi.
- Abilitare l'autenticazione robusta e la cifratura del traffico (se possibile).