

Esercizio

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

Configurazione IP Metasploitable2 e Kali Linux.

Modifico l'indirizzo IP di Metasploitable2. Metto la scheda di rete su rete interna e assegno l'indirizzo IP statico 192.168.1.40.

```
sudo su
```

```
nano /etc/network/interfaces
```

sostituisco iface eth0 con:

```
auto eth0
```

```
iface eth0 inet static
```

```
    address 192.168.1.40
```

```
    netmask 255.255.255.0
```

```
    gateway 192.168.1.1
```

Riavvio l'interfaccia di rete:

```
ifdown eth0 && ifup eth0
```

Verifico ora indirizzo IP:

```
root@metasploitable:/home/msfadmin# 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:ab:f8:47 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:feab:f847/64 scope link
        valid_lft forever preferred_lft forever
root@metasploitable:/home/msfadmin# _
```

Configuro la rete statica anche sulla Kali:

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::6a63:b2a1:c85a:91b1 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:04:42:0f txqueuelen 1000 (Ethernet)
    RX packets 10 bytes 1540 (1.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 72 bytes 25182 (24.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Faccio una prova di connettività

```
(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=1.08 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.542 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.542 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.519 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.519 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=0.451 ms
```

Sfrutto la vulnerabilità relativa a Telnet

Avvio msfconsole

```
$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

Metasploit

+ -- ==[ metasploit v6.4.50-dev ]
+ -- ==[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

Digito search telnet_version

```
msf6 > search 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`

Digito use 1

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Digito **OPTIONS**

```
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		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

Digito set RHOSTS 192.168.1.40

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

Digito exploit

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET _\x0a _\x0a_\x0a_\x0aWarning: Never
expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get starte
d\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Digito il comando **telnet 192.168.1.40**

```
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 '^['.
```

[illegible]

Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

Entro con le credenziali

```
metasploitable login: msfadmin
Password:
Last login: Tue May 13 08:17:03 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.
```

```
msfadmin@metasploitable:~$
```