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

innanzitutto cambiamo gli ip:

```
collisions:0 txqueuelen:0
           RX bytes:293397 (286.5 KB)
                                            TX bytes:293397 (286.5 KB)
msfadmin@metasploitable:/etc/network$
msfadmin@metasploitable:/etc/network$ ifconfig
           Link encap:Ethernet HWaddr 08:00:27:e5:9f:28
inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fee5:9f28/64 Scope:Link
eth0
           UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
           RX packets:261 errors:0 dropped:0 overruns:0 frame:0
           TX packets:295 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:25590 (24.9 KB) TX bytes:34769 (33.9 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:721 errors:0 dropped:0 overruns:0 frame:0
           TX packets:721 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:318671 (311.2 KB) TX bytes:318671 (311.2 KB)
eth1: 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::3dd5:ce22:b282:58a0 prefixlen 64 scopeid 0×20<link>
        ether 08:00:27:8f:0d:ed txqueuelen 1000 (Ethernet)
RX packets 6 bytes 1100 (1.0 KiB)
        RX errors 0 dropped 0 overruns 0
        TX packets 43 bytes 6792 (6.6 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 0×10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 4 bytes 240 (240.0 B)
        RX errors 0 dropped 0 overruns 0
                                            frame 0
        TX packets 4 bytes 240 (240.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

controlliamo che le due macchine comunichino tra loro

```
(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=0.786 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.358 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.457 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.416 ms
^C
— 192.168.1.40 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.358/0.504/0.786/0.166 ms
```

```
(kali@ kali)-[~]
$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for hosts
```

attiviamo l'estensione telnet e dopo aver settato l'IP target lanciamo il programma con il comando "exploit"

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(
                                                     m) > set RHOSTS 192.168.1.40
RHOSTS ⇒ 192.168.1.40
                                             _version) > exploit
msf6 auxiliary(s
[+] 192.168.1.40:23
                                - 192.168.1.40:23 TELNET _
                                \x0a _ ____
al '_ _ \ / _ \
| | | | | __/ ||
                            \x0a|
                      |
|\x0a| |
                                                 ī `(<u>    </u>`
                  \x0a|_| |_
           |\x0a
\x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0a
Contact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get star
ted\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23
                          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(:
```

## ed infine usiamo il comando telnet per entrare nella macchina

```
msf6 auxiliary(
                                            ) > 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 msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Tue Mar 5 03:25:15 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:~$
```

controlliamo di aver effettivamente eseguito I accesso lanciando il comando ifconfig e controlliamo di essere nella macchina target

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0
          Link encap:Ethernet HWaddr 08:00:27:e5:9f:28
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee5:9f28/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:433 errors:0 dropped:0 overruns:0 frame:0
          TX packets:429 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:37955 (37.0 KB) TX bytes:46641 (45.5 KB)
          Base address:0×d020 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:792 errors:0 dropped:0 overruns:0 frame:0
          TX packets:792 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:352047 (343.7 KB) TX bytes:352047 (343.7 KB)
msfadmin@metasploitable:~$
```