

## Relazione 17-12

L'obiettivo dell'esercizio è stato quello di analizzare la vulnerabilità del servizio Telnet in esecuzione sulla macchina Metasploitable utilizzando il modulo `auxiliary/scanner/telnet/telnet_version` di Metasploit.

Per prima cosa ho modificato gli indirizzi IP della Kali e della metasploit come richiesto dalla traccia.

```
(kali@kali)-[~]
$ sudo ifconfig eth0 192.168.1.25 netmask 255.255.255.0 up

[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::b042:64ab:8995:eedb/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Metasploitable [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0 up
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:60:1e:3e
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe60:1e3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:832 (832.0 B)  TX bytes:15310 (14.9 KB)
          Base address:0xd010 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:713 errors:0 dropped:0 overruns:0 frame:0
          TX packets:713 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:300865 (293.8 KB)  TX bytes:300865 (293.8 KB)

msfadmin@metasploitable:~$
```

msfconsole

[illegible]

Scrivendo `search telnet_version` ci trova l'auxiliary che ci interessa, utilizzo il modulo `auxiliary/scanner/telnet/telnet_version` di Metasploit per analizzare il servizio Telnet attivo sulla macchina Metasploitable. Dopo aver caricato il modulo, è stato configurato il parametro `RHOSTS` con l'indirizzo IP del target (`192.168.1.40`) per definire l'host remoto da analizzare. Successivamente, l'attacco è stato avviato tramite il comando `run`, consentendo al modulo di raccogliere informazioni sul servizio Telnet.

L'esecuzione del modulo ha confermato la presenza del servizio Telnet in ascolto sulla porta standard 23/TCP. 192.168.1.40:23 TELNET

Con il comando **Telnet 192.168.1.40** tento di stabilire una connessione con l'IP della metasploit e verifico che va a buon fine.

```
File Actions Edit View Help
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 Detect
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

msf6 > use 1
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-
RPORT 23 yes The target port (TCP)
THREADS 10 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.

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

[*] 192.168.1.40:23 [*] 192.168.1.40:23 TELNET
[+] [Lantronix Telnet Service Banner Detected] [Lantronix Telnet Service Banner Detected]
[*] 192.168.1.40:23 [*] 192.168.1.40:23 [*] Scanned 3 of 1 hosts (100% complete)
msf6 auxiliary(module execution completed)
msf6 auxiliary(scanner/telnet/telnet_version) >
```