

# Esercizio S7L2

**Traccia:**

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary/telnet/version` sulla macchina Metasploitable.

**Requisito:** Configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40.

Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

- 1) Per Exploit s'intende un codice malevolo che va a sfruttare le vulnerabilità del codice o del software.  
Per Malware s'intende un codice malevolo che crea problemi al dispositivo o al software.

La differenza tra i due è che l'exploit non ha bisogno dell'interazione dell'uomo dato che la vulnerabilità è già presente nel codice o nel software invece il malware ha bisogno dell'interazione dell'uomo per poter iniziare ad infettare.

- 2) Il protocollo attaccato è il Telnet è quel protocollo che ci permette di connetterci e di comunicare con un altro dispositivo da remoto.

```
File Actions Edit View Help
[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=0.810 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.510 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.382 ms
^C
-- 192.168.1.40 ping statistics --
3 packets transmitted, 3 received, 0% packet loss, time 2028ms
rtt min/avg/max/mdev = 0.510/1.713/3.821/1.495 ms

[kali@kali:]-
$ nmap -v 192.168.1.40
Starting Nmap 7.94 (https://nmap.org) at 2023-11-07 04:49 EST
Nmap scan report for 192.168.1.40 (192.168.1.40)
Host is up (0.0021s latency).
Not shown: 997 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 Bubuntu1 (protocol 2.0)
23/tcp    open  telnet          Linux telnet
24/tcp    open  smtp            Postfix smtpd
53/tcp    open  domain          DNS BIND 9.4.2
80/tcp    open  http            Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind         TPC (RPC #10000)
139/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login           OpenBSD or Solaris rlogind
514/tcp   open  tcpwrap
1099/tcp  open  java-rmi        GNU Classpath gmirregistry
1524/tcp  open  bindshell       Metasploitable root shell
2049/tcp  open  nfs             2-4 (RPC #10000)
2121/tcp  open  ftp             ProFTPD 1.3.1
3306/tcp  open  mysql           MySQL 5.0.51a-3ubuntu0
5432/tcp  open  postgresql      PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc             VNC (protocol 3.3)
6000/tcp  open  x11             (access denied)
6667/tcp  open  irc             UnrealIRCd (Admin email admin@metasploitable.LAN)
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)
8180/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1
Service Info: host = metasploitable.localdomain; OS=Unix; Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.97 seconds
```

- 3) si va a vedere se le due macchine comunicano, si fa una scansione con nmap per vedere la versione del protocollo che effettueremo l'attacco

Si cerca il servizio da fare l'exploit, controlliamo le opzioni necessarie per vedere se abbiamo inserito tutti i parametri necessari.

In questo caso l'unico parametro richiesto che mancava era l'`RHOSTS`.

Si avvia Metasploit

```
[kali@kali:~]$ msfconsole
```

```
##### dR0P #####  
db'                                db'  
db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db'  
db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db'
```

```
--|--  
|--o-- | db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db'  
      |--o-- db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db' db'
```

To boldly go where no  
she'll has gone before

```
+ --[ metasploit v6.3.7-dev ]  
+ --[ 2335 exploits - 1228 auxiliary - 413 post ]  
+ --[ 1385 payloads - 46 encoders - 11 nops ]  
+ --[ 9 evasion ]
```

Metasploit tip: Use the analyze command to suggest runnable modules for hosts  
Metasploit Documentation: https://docs.metasploit.com/  
  
msfa > use auxiliary/scanner/telnet/telnet\_version  
msfa 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
PROSITS		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

View the full module info with the info, or info -d command.

quindi si va a settare per l'RHOSTS l'indirizzo IP della vittima cioè Windows XP.

si rifà il controllo dei parametri necessari

Poi è possibile effettuare l'exploit

si fa un controllo se l'exploit è andato a buon fine inserendo l'username e la password trovati con l'exploit

come si può vedere mi ha permesso di accedere alla schermata della vittima in questo caso Metasploitable

```
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) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  192.168.1.40    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              no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET -
-//\x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aLogin with msfadmin/msfadmin to get started\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) >

kali@kali: ~
File Actions Edit View Help
Password: Connection closed by foreign host.

(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 Nov 7 06:31:09 EST 2023 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:~$
```

Da qui si può vedere l'username e la password per accedere a Telnet