

## S7\_L2

**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

### 1. Apriamo la console di Metasploite con il comando di msfconsole

```
msf6 > search telnet

Matching Modules
=====
```

#	Name	Disclosure Date
0	exploit/linux/misc/asus_infosvr_auth_bypass_exec	2015-01-04
1	exploit/linux/http/asuswrt_lan_rce	2018-01-22
2	auxiliary/server/capture/telnet	.
3	auxiliary/scanner/telnet/brocade_enable_login	.
4	exploit/windows/proxy/ccproxy_telnet_ping	2004-11-11
5	\ target: Automatic	.
6	\ target: Windows 2000 Pro All - English	.
7	\ target: Windows 2000 Pro All - Italian	.
8	\ target: Windows 2000 Pro All - French	.
9	\ target: Windows XP SP0/1 - English	.
10	\ target: Windows XP SP2 - English	.

### 2. Visualizziamo il servizio che ci serve

```
73 auxiliary/scanner/telnet/telnet_version . normal No Telnet Service Banner Detection
```

### 3. Visualizziamo le opzioni disponibili

```
msf6 > use 73
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

Name	Current Setting	Required	Description
PASSWORD	__PASSWORD__	no	The password for the specified u
RHOSTS		yes	The target host(s), see https://
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

#### 4. Possiamo già visualizzare nella prima riga lo user e la password

[illegible]

**5. Inserendo il comando telnet con l'indirizzo ip del target riusciamo a visualizzare il banner di Metasploitable e di conseguenza inserire le credenziali per accedere**

```

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: Thu May 23 11:04:26 EDT 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:~$

```