

# Relazione S7/L2

```
(daveide@kali)-[~]
$ nmap -sV 192.168.1.40 -p 23
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:14 CET
Nmap scan report for 192.168.1.40
Host is up (0.00028s latency).
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: 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 23.14 seconds
```

Lo scopo di questo esercizio è quello di utilizzare metasploit per andare a scovare lo username e password del servizio telnet su metasploit.

Come prima cosa ho effettuato una scansione della porta 23 richiedendo il banner del servizio e una volta appurato che fosse aperto ho eseguito metasploit

```
Interact with a module by name or index. For example info 9, use 9 or use payload/cmd/unix/bind_busybox_telnetd
msf6 > search telnet_version

Matching Modules
=====
#  Name
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version
1  auxiliary/scanner/telnet/telnet_version

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) > show options

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

Name      Current Setting  Required  Description
-  -  -  -  -
PASSWORD  nil              no        The password for the specified username
RHOSTS    nil              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  nil              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) > show options

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

Name      Current Setting  Required  Description
-  -  -  -  -
PASSWORD  nil              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  nil              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
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Ho cercato il modulo ausiliario telnet\_version e una volta richiamato ho settato l'ip di kali. In questo modo sono andato a recuperare lo username e la password.

Davide Lecci