



# Compito S7-L2

# Exploit Telnet con Metasploit

Apriamo un terminale di Kali e inseriamo il comando `msfconsole`. Poi, in un altro terminale, effettuiamo la scansione delle porte con `nmap -Pn -sV ip`. Ora torniamo su `msfconsole` e eseguiamo `search auxiliary telnet_version`.

```
msf6 > search auxiliary telnet_version

Matching Modules
=====
#  Name                                     Disclosure Date  Ran
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version  nor
mal No   Lantronix Telnet Service Banner Detection
1  auxiliary/scanner/telnet/telnet_version           nor
mal 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
```

7

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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         netkit-rsh rexecd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
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
```

# Exploit Telnet con Metasploit

Andiamo a vedere le opzioni e, per tutte le informazioni necessarie, le compiliamo.

```
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 user name
RHOSTS	localhost, interface: eth0, 192.168.1.104	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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.

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.168
RHOSTS => 192.168.1.168
```

# Exploit Telnet con Metasploit

Ora andiamo a far partire l'exploit. Possiamo notare di aver ricevuto la scansione con successo e di conseguenza ottenuto le credenziali. Ora possiamo accedere a Telnet normalmente con le credenziali ottenute.

[illegible]

# Exploit Telnet con Metasploit

Come puoi vedere, ho inserito con successo le credenziali ottenute e sono entrato nel servizio normalmente.

```
[root@kali:~]# telnet 192.168.1.168 23
Trying 192.168.1.168 ...
Connected to 192.168.1.168.
Escape character is '^I'.

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 Jan 23 05:33:12 EST 2024 from 192.168.1.167 on pts/1
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:
```