

# S7-L2 EXPLOIT TELNET



# TRACCIA

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version con Kali linux sulla macchina metasploitable2

# RICERCA NMAP + MSFCONSOLE

```
mattia@vbox: ~/Desktop
File Actions Edit View Help
(mattia@vbox)-[~/Desktop]
$ nmap -sV 192.168.0.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 14:12 CET
Nmap scan report for 192.168.0.134 (192.168.0.134)
Host is up (0.028s latency).
Not shown: 977 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 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smptd
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?
513/tcp   open  login
514/tcp   open  tcpwrapped
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
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

mattia@vbox: ~/Desktop
File Actions Edit View Help
l Hats*Hava*Team Neu*
*Cyb3rDoctor*Techlock Inc*kinakomochi*Dubb3Dopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CL
OVERS*ev4d3rx10-team*ir4n6*
*PEQUI_ctf*HKLBD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Rai
se The Black*CTErr0r*
*Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gaut
i*
*San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*Or
deringChaos*Pickle_Ricks*
*Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris
Wheel*Ficus*ONO*jameless*
*Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhou
nd Gang*society*HackJWU*
*asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*Starc
hThingIDK*Tieto_alaviiva_turva*
*InspiV*RPCA Cyber Club*kurageOverfl0w*lammm*pelicans_for_freedom*switchteam*tim*depart
edcomputerchairs*cool_runnings*
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUCKys_Angels*
OrangeJuice*DemDirtyUserz*
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits
33kr*root_rulzz*InfosecIITG*
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hama
d*Immortals*arasan*MouseTrap*
*damn_sadboi*tadaaa>null2root*HowestCSP*fezfezf*LordVader*Fl0g_Hunt3rs*bluenet*P@Ge2mE*
-[ metasploit v6.4.18-dev
+ ---[ 2437 exploits - 1255 auxiliary - 429 post
+ ---[ 1471 payloads - 47 encoders - 11 nops
+ ---[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary/scanner/telnet/telnet_version
```

# SET RHOSTS

Una volta effettuata ricerca su nmap e avviato msfconsole, procediamo a configurare il nostro target hosts manualmente con il comando “set RHOSTS ip di metasploit”.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.0.134
RHOSTS => 192.168.0.134
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        192.168.0.134    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.
```

# EXPLOIT

Una volta settato l'ip target, si procede all'exploit. Quest'ultimo ha avuto successo come si può vedere dallo screen in basso.

La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Questo significa che un potenziale attaccante potrebbe intercettare la comunicazione e rubare informazioni sensibili come username, password e i comandi scambiati tra client e server.



**THANKS**  
**MATTIA DI DONATO**