

Esercitazione S7-L2

Per prima cosa ho impostato gli indirizzi IP consigliati dal testo della traccia: **192.168.1.25** per la kali e **192.168.1.40** per la metasploitable. Fatto ciò, ho effettuato il **ping** per verificare la connessione tra le due macchine.

```
(kali@kali)-[~]
└─$ in a
    net <LOOPBACK>,UP_LOWER_UP<->mtu 65536 qdisc noqueue state UNKNOWN queue default qlen 1000
    link loopback 80:00:00:00:00:00 brd 00:00:00:00:00:00
    valid_lft forever preferred_lft forever
    valid_lft forever preferred_lft forever
    inet 192.168.1.0/24 scope host lo
        valid_lft forever preferred_lft forever
    eth0 <BROADCAST,MULTICAST,UP,>LOWER_UP<->mtu 1500 qdisc fq_codel state UP queue default qlen 1000
    link ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.224/24 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::1122:557c:a5b5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(64) bytes of data.
 64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.389 ms
 64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.307 ms
 64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.261 ms
 64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.478 ms
 64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.293 ms
^C
- - - 192.168.1.40 ping statistics - - -
 5 packets transmitted, 5 received, 0% packet loss, time 4076ms
 rtt min/avg/max/mdev = 0.261/0.344/0.470/0.075 ms
```

Avvio Metasploit

```

kali@kali:~$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

d8888888b  d888P d8888888P d88888b
      db'
db'db'db'db' d88P      d8P      d8P 88
db'db'db'db' d8P      d8P      d8P 88
db'db'db' d8888P      d8P      d88888888

      d88888P  d88888b d8P  d888888P d8P d888888P
      |
      | d8P      d888P d8P      db' 8P d8P      d8P
  --o--| d8P      d8P      d8P      db' 8P d8P      d8P
      | d888P d88P  d888P d8888P d8P      d8P

To boldly go where no
shell has gone before

-=[ metasploit v6.4.38-dev ]=
+ --=[ 2467 exploits - 1273 auxiliary - 431 post ]=
+ --=[ 1478 payloads - 49 encoders - 13 nops ]=
+ --=[ 9 evasion ]=

Metasploit Documentation: https://docs.metasploit.com/

```

Esecuzione nmap

```
msf6 > nmap -sV -O 192.168.1.40
[*] exec: nmap -sV -O 192.168.1.40

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 18:42 CET
Nmap scan report for 192.168.1.40
Host is up (0.00041s latency).
Not shown: 977 Closed tcp ports (reset)
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
513/tcp   open  login?
516/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
3386/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5327/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
MAC Address: 08:00:27:CE:95:91 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.03 seconds
msf6 >
```

Ricerca modulo auxiliary **telnet_version**

```
msf6 > search --auxiliary telnet_version

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/telnet/lantronix_telnet_version	.	normal	No	Lantronix Telnet Service Banner Detection
1	auxiliary/scanner/telnet/telnet_version	.	normal	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 > 
```

Selezione e controllo opzioni del modulo scelto

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > options

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



| Name     | Current Setting | Required | Description                                                                                                                                                                                         |
|----------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PASSWORD |                 | no       | The password for the specified username                                                                                                                                                             |
| RHOSTS   |                 | 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) > 
```

Settaggio parametri

```
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
```

Avvio **exploit** e visualizzazione in chiaro di **username** e **password**.

[illegible]