

aperto msfconsole , cerco il modulo in questione cercando "telnet_version":

```
msf6 > search 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 > 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 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	The username to authenticate as

View the full module info with the `info`, or `info -d` command.

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

Una volta trovato il modulo, lo lancio con il comando “use” e compilo i parametri richiesti visti con il comando show options:

```
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 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	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
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://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	The username to authenticate as

View the full module info with the `info`, or `info -d` command.

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

Una volta rimessi i parametri con l'ip della macchina target (metasploitable), ed una volta settato il payload (di default), lancio l'attacco con il comando "exploit":

[illegible]

Per vedere se l'attacco è andato a buon, eseguo il comando telnet seguito dall'ip della macchina attaccata ed il servizio mi chiede password e utente, che ho recuperato nel passaggio prima (msfadmin e msfadmin).

```
metasploitable
File system

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  7 05:39:05 EST 2023 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:~$
```

```
msfadmin@metasploitable:~$ gcc -v
Using built-in specs.
Target: i486-linux-gnu
Configured with: ../src/configure -v --enable-languages=c,c++,fortran,objc,obj-c++,treelang --prefix=/usr --enable-shared --with-system-zlib --libexecdir=/usr/lib --without-included-gettext --enable-threads=posix --enable-nls --with-gxx-include-dir=/usr/include/c++/4.2 --program-suffix=-4.2 --enable-clocale-gnu --enable-libstdc++-debug --enable-objc-gc --enable-mpfr --enable-targets=all --enable-checking=release --build=i486-linux-gnu --host=i486-linux-gnu --target=i486-linux-gnu
Thread model: posix
gcc version 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ uname -mrs
Linux 2.6.24-16-server i686
```

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a5:d9:79
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea5:d979/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:309 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20562 (20.0 KB)  TX bytes:36539 (35.6 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:354 errors:0 dropped:0 overruns:0 frame:0
          TX packets:354 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:140801 (137.5 KB)  TX bytes:140801 (137.5 KB)

msfadmin@metasploitable:~$ route
Kernel IP routing table
Destination    Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0    *               255.255.255.0   U      0      0      0 eth0
default        192.168.1.1    0.0.0.0         UG     100    0      0 eth0
msfadmin@metasploitable:~$

```

Vediamo che dopo esser loggati con le credenziali “rubate”, abbiamo accesso al terminale vero e proprio della macchina attaccata e, con diversi comandi, recupero informazioni preziosi della macchina attaccata.