

```

davide@kali: ~
File Actions Edit View Help
└─(davide@kali)-[~]
$ mfsconsole
mfsconsole: command not found

└─(davide@kali)-[~]
$ msfconsole

Metasploit tip: Start commands with a space to avoid saving them to history

      dBBBBBb  dBBP dBBBBBP dBBBBb
      ' dB'      BBP
      dB'dB'dB' dBBP  dBP  dBP BB
      dB'dB'dB' dBP   dBP  dBP BB
      dB'dB'dB' dBBBBP dBP  dBBBBBB

      dBBBBBP dBBBBBb dBP dBBBBBP dBP dBBBBBBP
      ' dB' dBP dB' .BP
      dBP dBBBB' dBP dB' .BP dBP dBP
      dBP dBP dBP dB' .BP dBP dBP
      dBBBBBP dBP dBBBBBP dBBBBBP dBP dBP

      .
      |
      -o-
      |

To boldly go where no
shell has gone before

=[ metasploit v6.3.51-dev ]
+ --=[ 2384 exploits - 1235 auxiliary - 418 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

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

msf6 >

```

Scegliamo il secondo con il comando `use 1`.

```
msf6 > search telnet_version

Matching Modules



| #                                         | Name                                              | Disclosure Date | Rank   | Check |
|-------------------------------------------|---------------------------------------------------|-----------------|--------|-------|
| 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 1
msf6 auxiliary(scanner/telnet/telnet_version) > show options
```

```
msf6 > use 1
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.

[illegible][illegible]

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:00:22:5b
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe00:225b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:269 errors:0 dropped:0 overruns:0 frame:0
          TX packets:370 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18808 (18.3 KB)  TX bytes:32636 (31.8 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:271 errors:0 dropped:0 overruns:0 frame:0
          TX packets:271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:86653 (84.6 KB)  TX bytes:86653 (84.6 KB)

msfadmin@metasploitable:~$
```