

```

auto eth0
iface eth0 inet static
address 192.168.1.25
netmask 255.255.255.0
gateway 192.168.1.1
#iface eth0 inet dhcp

```

```

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.2.255
gateway 192.168.1.1

```

```

(kali㉿kali)-[~]
$ msfconsole

IIIIII Systemd
II      4' v 'B
II      6. .P
II      'T; .;P'
II      'T; ;P'
IIIIII      'YvP'

I love shells --egypt

      =[ metasploit v6.3.4-dev ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

```

```

msf6 > search auxiliary telnet_version

Matching Modules
=====
#  Name
-  -
0  auxiliary/scanner/telnet/lantronix_telnet_version
1  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.me">https://docs.me</a>
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max o
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40  
rhost => 192.168.1.40
```

```
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  
metasploitable login:  
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

```
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: █

metasploitable login: msfadmin

Password:

Last login: Mon Sep 18 05:27:56 EDT 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:~\$ █

