

```
heskarieth@kali: ~
$ msfconsole

[*] msfconsole v0.3.15-dev
[*] 2315 exploits - 1208 auxiliary - 412 post
[*] 975 payloads - 46 encoders - 11 nops
[*] 9 evasion

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

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) >
```

```
heskarieth@kali: ~
$ msfconsole

[*] msfconsole v0.3.15-dev
[*] 2315 exploits - 1208 auxiliary - 412 post
[*] 975 payloads - 46 encoders - 11 nops
[*] 9 evasion

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_version
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) > exploit

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

A screenshot of a Kali Linux terminal window titled "heskarioth@kali -". The terminal shows the execution of several commands to install and configure Metasploit. First, `telnet 192.168.1.40` is run, connecting to a remote host. Then, the Metasploit framework is installed using `apt-get install metasploit`. After installation, the user runs `msfdev[at]metasploit.com` and logs in with `msfadmin/msfadmin`. The terminal displays the Metasploit logo, a warning about network security, contact information, login status, system details (Ubuntu 20.04 LTS), and a list of included programs. Finally, the user enters the command `msfadmin@metasploitable:~\$` at the prompt.

```
heskarioth@kali ~$ telnet 192.168.1.40
Connected to 192.168.1.40.
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 Jun 9 12:52:46 EDT 2022 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:~\$