```
File Actions Edit View Help
      =[ metasploit v6.3.43-dev
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search telnet_version
Matching Modules
  # Name
                                                   Disclosure Date Rank Check Description
                                                                  normal No
  0 auxiliary/scanner/telnet/lantronix_telnet_version
                                                                               Lantronix Telnet Service Banner D
  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):
           Current Setting Required Description
  Name
  PASSWORD
                                   The password for the specified username
  RHOSTS
                          ves
                                   The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
                                   /using-metasploit.html
                                   The target port (TCP)
  RPORT
                          yes
                                   The number of concurrent threads (max one per host)
   THREADS 1
                          ves
  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 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 _
\x0a\x0a\x0a\x0a\x0a\x0a\contact: msfdev[at]metasploit.com\x0a\x0a\x0aLo
gin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(s
```

```
—(kali⊕kali)-[~]
[sudo] password for kali:
—(<mark>root⊕kali</mark>)-[/home/kali]
 sudo nano /etc/network/interfaces
(root@kali)-[/home/kali]
___ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp seq=1 ttl=64 time=0.765 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.369 ms
—— 192.168.1.40 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.268/0.467/0.765/0.214 ms
          <del>(ali</del>)-[/home/kali]
 Meta2 [In esecuzione] - Oracle VM VirtualBox
                                                                                   File Macchina Visualizza Inserimento Dispositivi Aiuto
  Contact: msfdev[at]metasploit.com
  Login with msfadmin/msfadmin to get started
                                                              Acquisizione automatica della tastiera... 🤝 💢
   metasploitable login: msfadmin
                                                             Integrazione del mouse...
   Password:
   Last login: Tue Mar 5 08:43:49 EST 2024 on tty1
  Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr
   The programs included with the Ubuntu system are fre
   the exact distribution terms for each program are des
   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 visi
   http://help.ubuntu.com/
   No mail.
  msfadmin@metasploitable:~$ telnet 192.168.1.40
   Trying 192.168.1.40...
   Connected to 192.168.1.40.
   Escape character is '^l'.
                                                       O (DESTRA)
```

File Actions Edit View Help