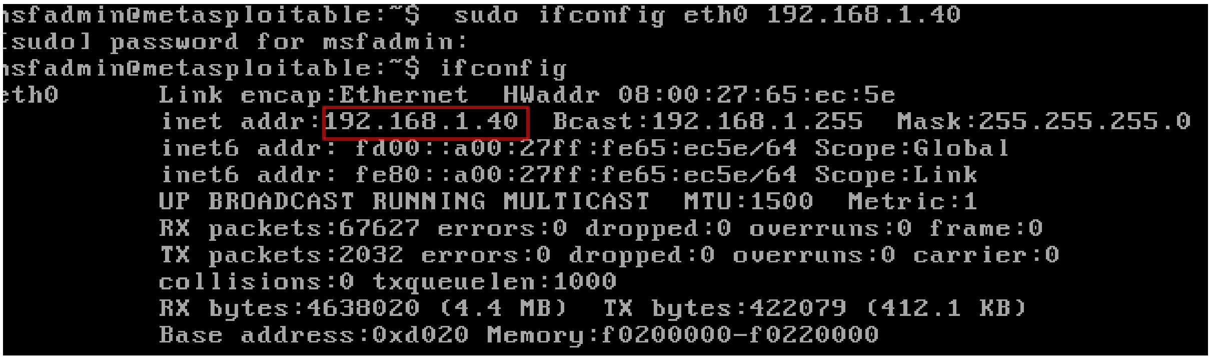
REPORT S7/L2

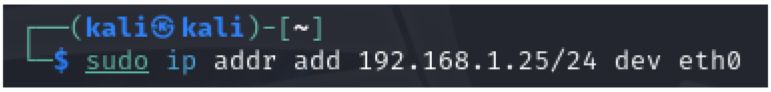
Obiettivo: Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

SVOLGIMENTO

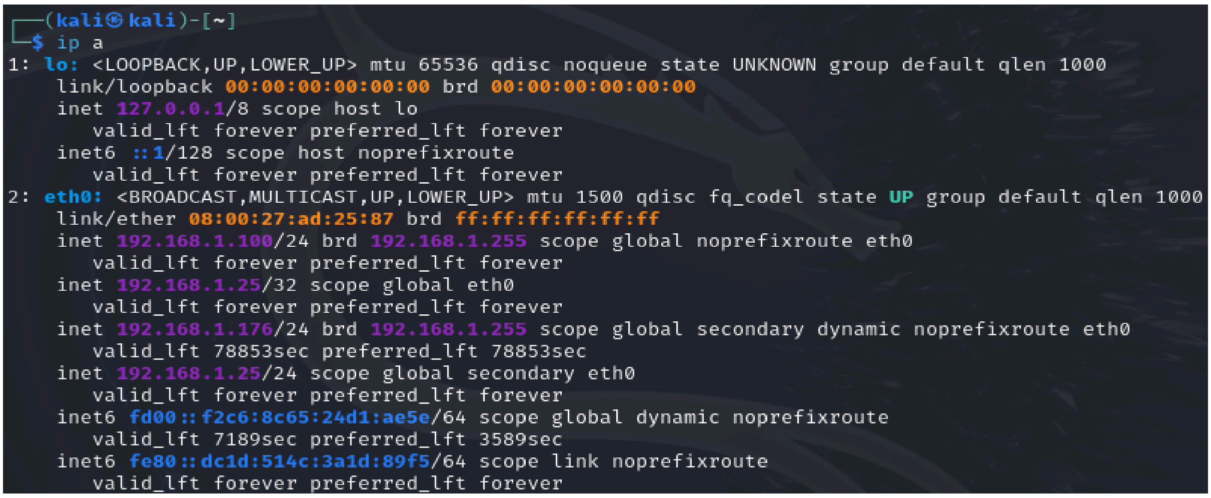
Imposto gli indirizzi IP delle VM Metasploitable e Kali-Linux come richiesto dalla traccia.
Kali-Linux: IP 192.168.1.25
Metasploitable: IP 192.168.1.40



```
sfadmin@metasploitable:~$  sudo ifconfig eth0 192.168.1.40
sudo] password for msfadmin:
sfadmin@metasploitable:~$ ifconfig
th0       Link encap:Ethernet  HWaddr 08:00:27:65:ec:5e
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fe65:ec5e/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe65:ec5e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:67627 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2032 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4638020 (4.4 MB)  TX bytes:422079 (412.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

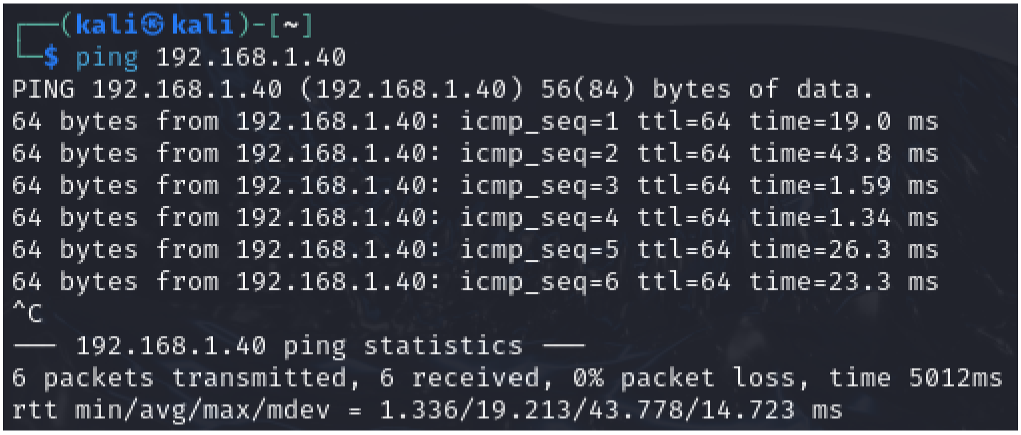


```
┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 192.168.1.25/24 dev eth0
```

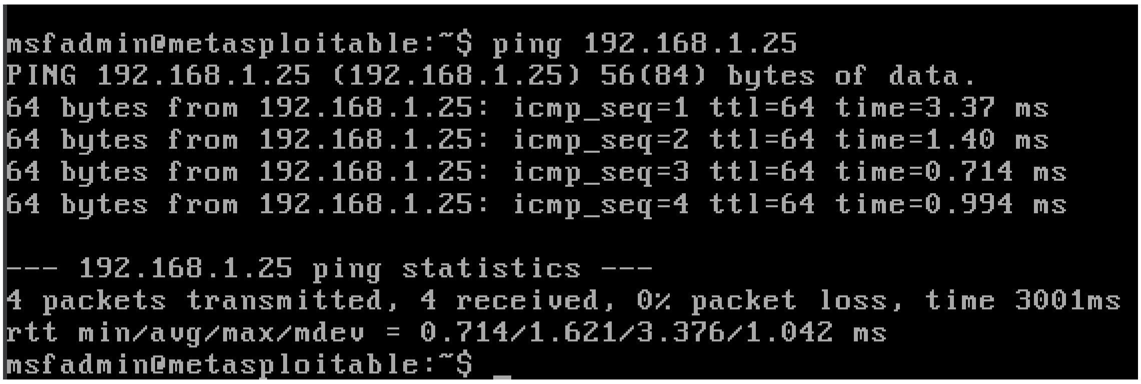


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet 192.168.1.25/32 scope global eth0
       valid_lft forever preferred_lft forever
    inet 192.168.1.176/24 brd 192.168.1.255 scope global secondary dynamic noprefixroute eth0
       valid_lft 78853sec preferred_lft 78853sec
    inet 192.168.1.25/24 scope global secondary eth0
       valid_lft forever preferred_lft forever
    inet6 fd00::f2c6:8c65:24d1:ae5e/64 scope global dynamic noprefixroute
       valid_lft 7189sec preferred_lft 3589sec
    inet6 fe80::dc1d:514c:3a1d:89f5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Verifico la connessione tra le macchine facendo un ping.

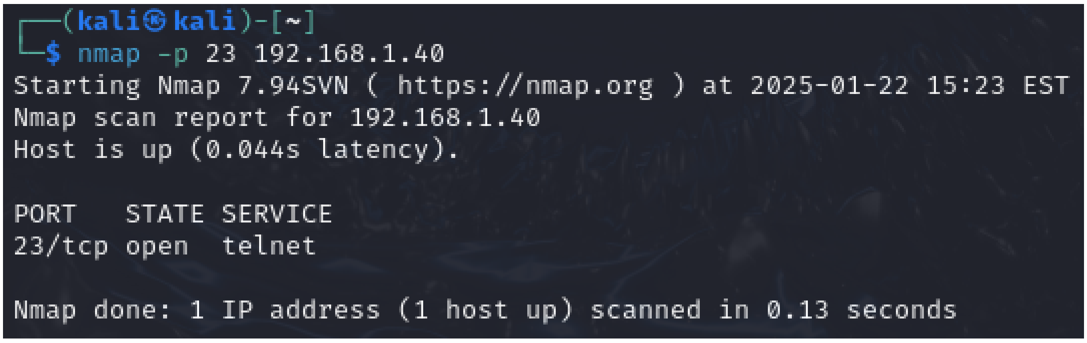


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=19.0 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=43.8 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=1.59 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.34 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=26.3 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=23.3 ms
^C
--- 192.168.1.40 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5012ms
rtt min/avg/max/mdev = 1.336/19.213/43.778/14.723 ms
```



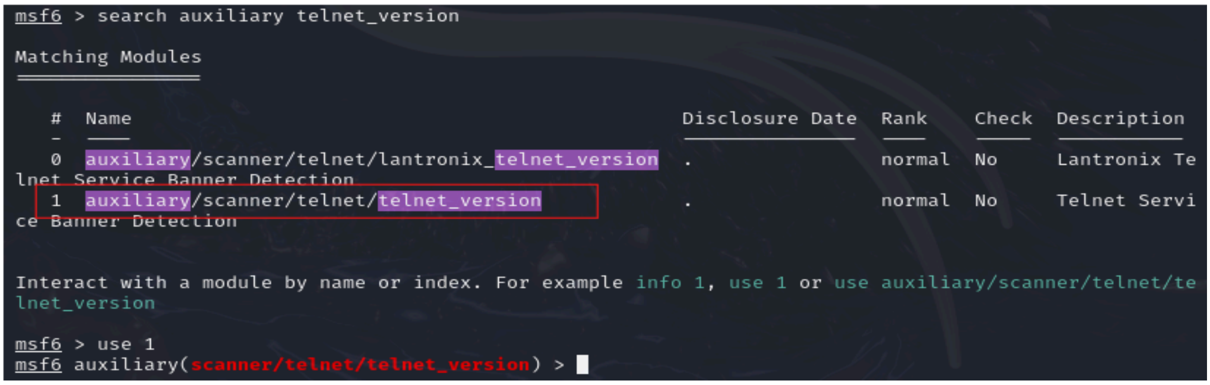
```
msfadmin@metasploitable:~$ ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=3.37 ms
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=1.40 ms
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.714 ms
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.994 ms

--- 192.168.1.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.714/1.621/3.376/1.042 ms
msfadmin@metasploitable:~$ _
```

Eseguo una scansione con il comando *nmap* per verificare che la porta 23, riservata al servizio telnet, sia aperta e libera.



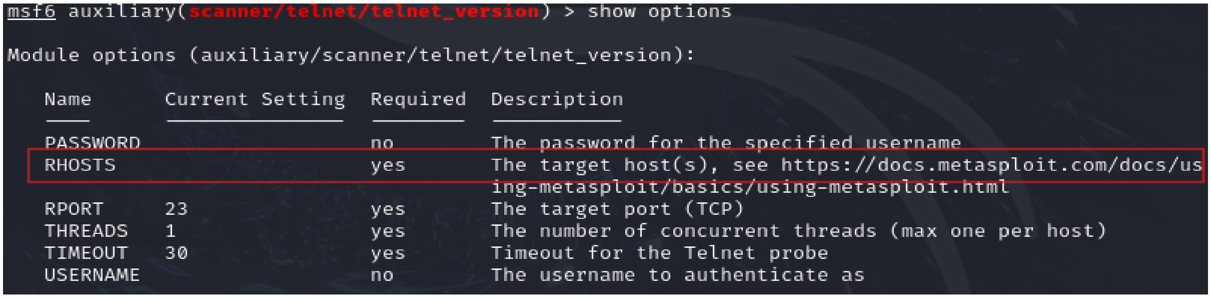
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 23 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 15:23 EST
Nmap scan report for 192.168.1.40
Host is up (0.044s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Avvio Metasploit ed effetto una scansione per cercare il modulo “auxiliary telnet_version” richiesto dalla traccia e utilizzo il modulo 1.



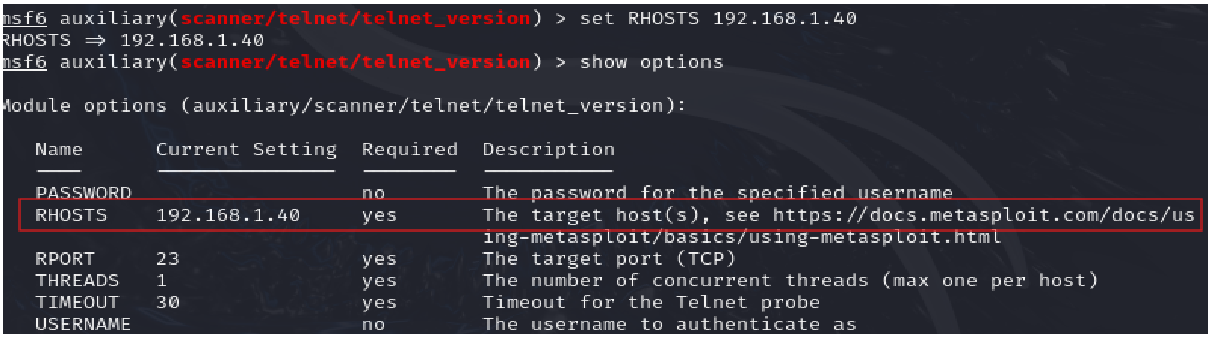
```
msf6 > search auxiliary telnet_version

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

   #  Name                                               Disclosure Date  Rank    Check  Description
   -  ----                                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version  .                normal  No     Lantronix Te
lnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version            .                normal  No     Telnet Servi
ce Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/te
lnet_version

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Utilizzando il comando show options visualizzo le informazioni per poter eseguire l’attacco.



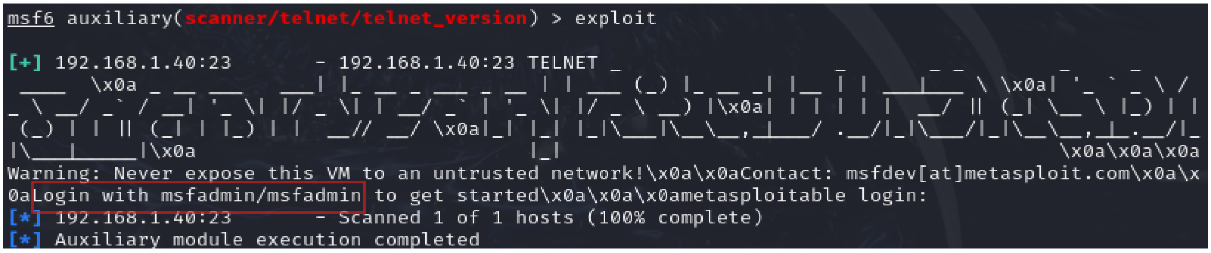
```
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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/us
                                        ing-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
```

Inserisco il remote host, in questo caso, la VM Metasploitable.



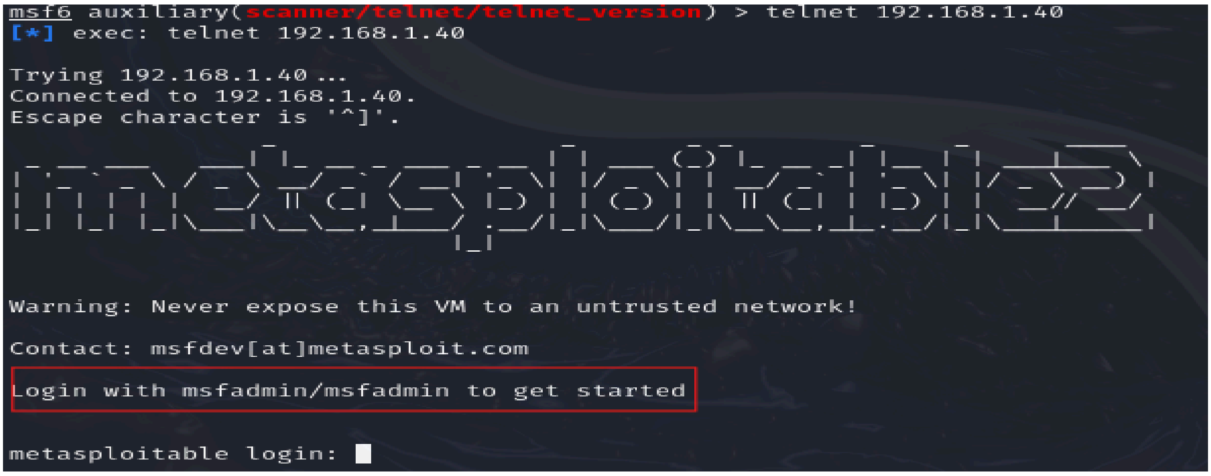
```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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/us
                                        ing-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
```

Successivamente lancio l’attacco con il comando *exploit* ottenendo come risultato i dati di login del servizio.



```
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\x0a
Warning: 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
```

Infine per verificare la correttezza delle informazioni ottenute eseguo il comando *telnet 192.168.1.40.*



```
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: █
```