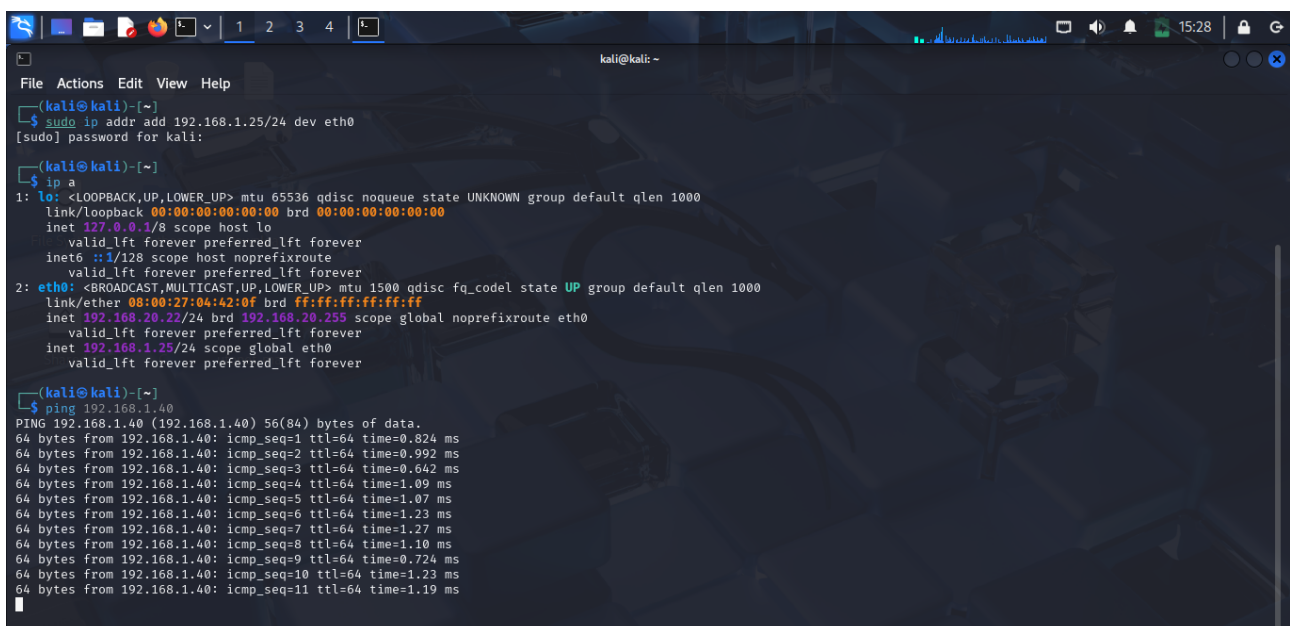


## Scansione e Accesso Telnet con Metasploit

**Esercizio richiesto:** sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo `auxiliary/telnet/telnet_version` sulla macchina Metasploitable.

Come richiesto dall'esercizio ho modificato in modo provvisorio gli indirizzi ip della kali in 192.168.1.25 e della MV Metasploitable in 192.168.1.40 verificando poi la comunicazione con il classico ping.



```
(kali@kali)-[~]
$ sudo ip addr add 192.168.1.25/24 dev eth0
[sudo] password for kali:

(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 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
   inet 192.168.20.22/24 brd 192.168.20.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet 192.168.1.25/24 scope global eth0
       valid_lft forever preferred_lft forever

(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=0.824 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.992 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.642 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=1.09 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=1.07 ms
64 bytes from 192.168.1.40: icmp_seq=6 ttl=64 time=1.23 ms
64 bytes from 192.168.1.40: icmp_seq=7 ttl=64 time=1.27 ms
64 bytes from 192.168.1.40: icmp_seq=8 ttl=64 time=1.10 ms
64 bytes from 192.168.1.40: icmp_seq=9 ttl=64 time=0.724 ms
64 bytes from 192.168.1.40: icmp_seq=10 ttl=64 time=1.23 ms
64 bytes from 192.168.1.40: icmp_seq=11 ttl=64 time=1.19 ms
```

Per il completamento dell'esercizio giornaliero ho avviato `msfconsole` e caricato il modulo richiesto:

**use auxiliary/scanner/telnet/telnet\_version**

Per poi impostare l'indirizzo ip della macchina target con il comando: **set RHOSTS 192.168.1.40**

Il modulo ha ricevuto come risposta un banner con le credenziali di accesso:

