

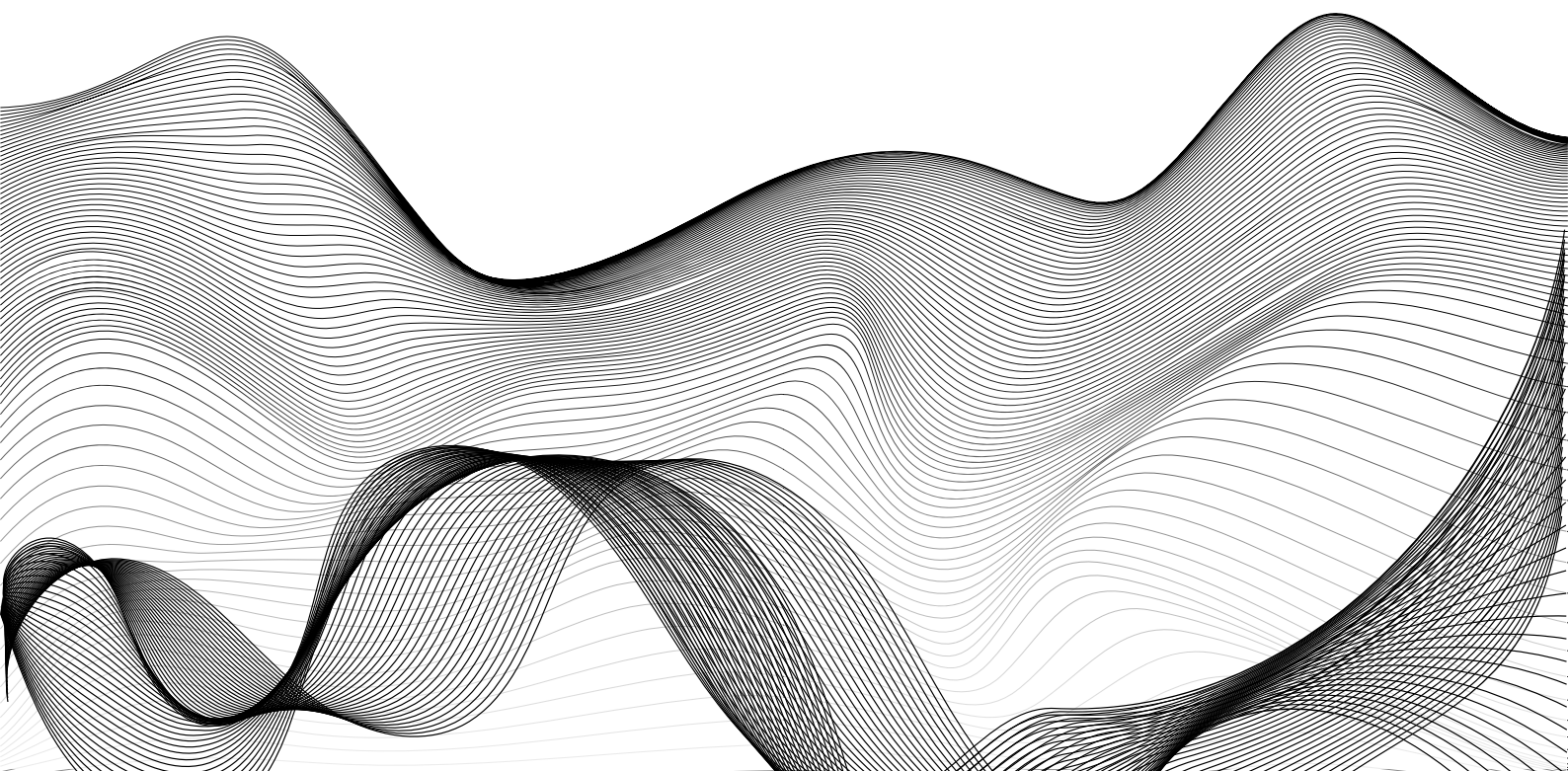
ELEONORA
VIOLA

DATASHIELDS



E X P L O I T
T E L N E T C O N
M E T A S P L O I T

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**

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Enable verbose logging with set VERBOSE true

/ it looks like you're trying to run a \
\ module                               /

[
  @ @
  || ||
  \ /
]

+ -- ==[ metasploit v6.4.15-dev ]
+ -- ==[ 2433 exploits - 1251 auxiliary - 428 post ]
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

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

```
msf6 > search telnet_version

Matching Modules

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

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

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

Utilizzo **show options** per vedere le info

```
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.
```


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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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

[illegible]

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

```
(kali㉿kali)-[~]  
$ telnet meta  
Trying 192.168.1.40 ...  
Connected to meta.  
Escape character is '^]'.  
  
metasploitable  
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 Jul 9 11:30:16 EDT 2024 on pts/1  
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.
```

