```
View the full module info with the info, or info -d command.
   msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts ⇒ 192.168.1.40

~ auxiliary(scanner/telnet/telnet_version) > exploit
\times \t
      * 192.168.1.40:23
   [*] Auxiliary module execution completed
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 08:57:04 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/
    msfadmin@metasploitable:~$
```

Report di attività:

- L'indirizzo IP della macchina virtuale Kali è stato modificato da quello precedente a 192.168.1.25.
- L'indirizzo IP della macchina virtuale Metasploitable è stato cambiato da quello precedente a 192.168.1.40.
- Successivamente, è stato avviato il servizio msfconsole dalla macchina virtuale Kali per procedere con le attività pianificate.
- Inoltre, tramite il comando **search** all'interno di msfconsole, sono stati ricercati i servizi Telnet come parte delle attività di analisi e test.
- Utilizzando il comando use, è stato selezionato il modulo auxiliary/scanner/telnet/telnet_version per ulteriori analisi e test.
- È stato notato che la porta utilizzata per Telnet è la porta 23.
- Successivamente, è stato aggiunto l'host di destinazione tramite il comando **set rhosts** per specificare l'indirizzo IP del bersaglio, che è stato impostato su 192.168.1.40.
- Utilizzando il comando **exploit**, sono state ottenute le credenziali di accesso alla macchina Metasploitable, che sono risultate essere **msfadmin/msfadmin**.
- Successivamente, è stato utilizzato il comando **telnet 192.168.1.40** per accedere direttamente alla macchina virtuale Metasploitable tramite Telnet.

Utilizzando le credenziali di accesso ottenute precedentemente, è stato confermato l'accesso riuscito alla macchina virtuale Metasploitable.	