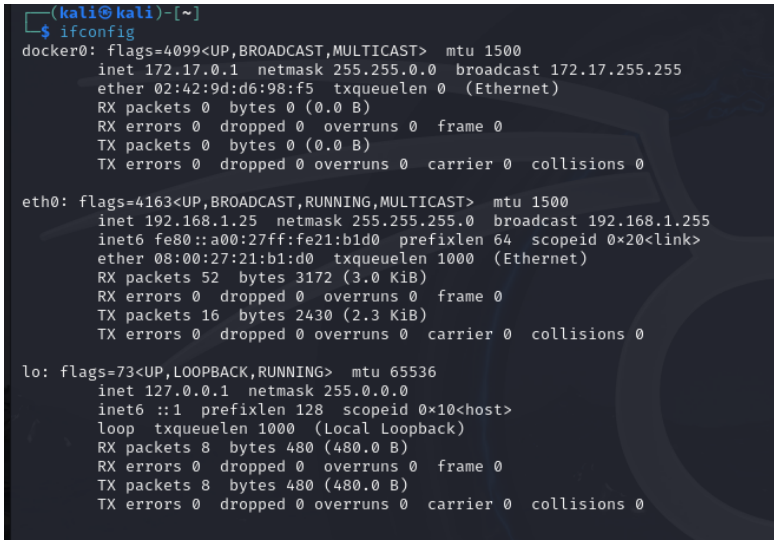
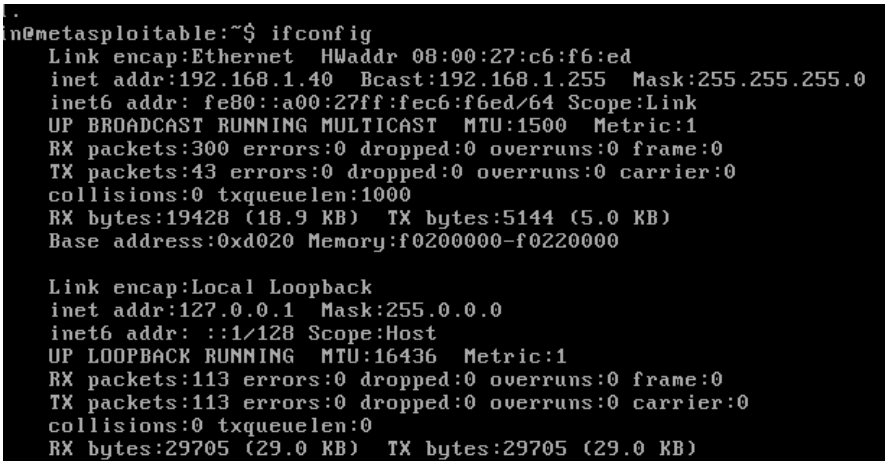
**ESERCIZIO W16D1 PRATICA 1**

**Attività:** Scansione della versione del servizio Telnet su Metasploitable utilizzando Kali Linux e Metasploit Framework.

**Passaggi eseguiti:**

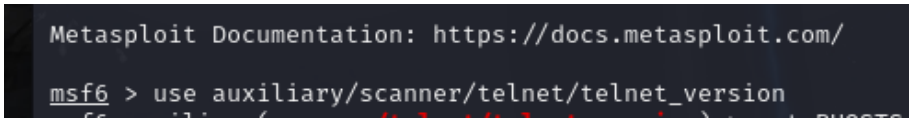
1. Configurazione degli indirizzi IP: L'indirizzo IP della macchina Kali è stato impostato su 192.168.1.25 e l'indirizzo IP della macchina Metasploitable è stato impostato su 192.168.1.40.



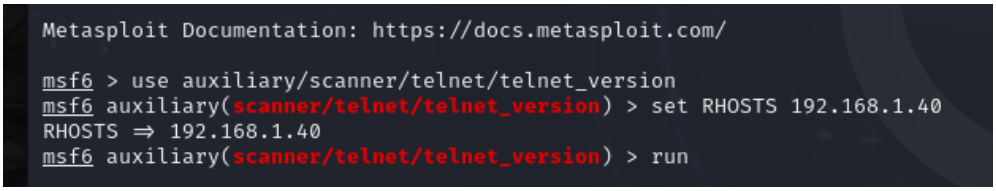

2. Avvio di Metasploit Framework: Metasploit Framework è stato avviato nel terminale della macchina Kali Linux utilizzando il comando **msfconsole**.

3. Caricamento del modulo: Il modulo auxiliary telnet_version è stato caricato utilizzando il comando **use auxiliary/scanner/telnet/telnet_version**.



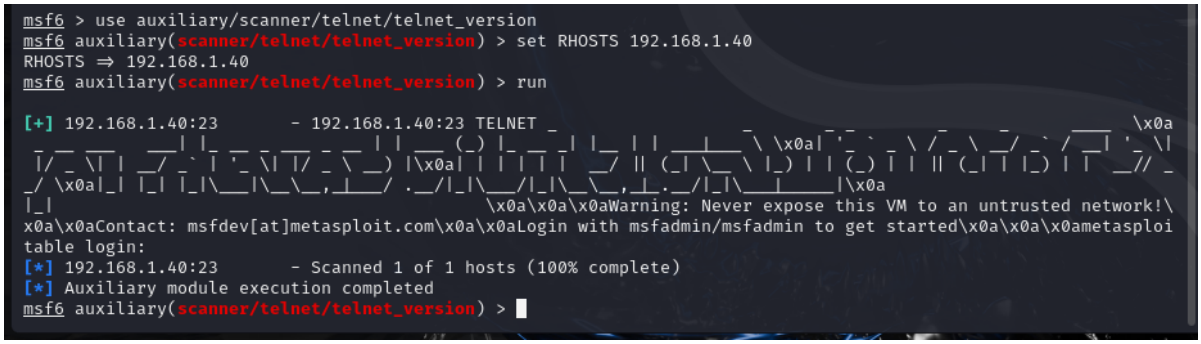

4. Impostazione delle opzioni del modulo: L'indirizzo IP di destinazione per la scansione Telnet è stato impostato su 192.168.1.40 utilizzando il comando **set RHOSTS 192.168.1.40**.

5. Esecuzione del modulo: La scansione della versione del servizio Telnet su Metasploitable è stata avviata utilizzando il comando **run**.




**Risultati ottenuti:**

- La scansione ha rivelato che il servizio Telnet è in esecuzione sulla porta 23 della macchina Metasploitable.
- Il banner del servizio Telnet mostra un messaggio di avviso e fornisce le credenziali predefinite ("msfadmin/msfadmin") per accedere alla macchina Metasploitable.




**Conclusioni:** L'esercizio è stato completato con successo, ottenendo informazioni sulla versione del servizio Telnet e le credenziali di accesso per la macchina Metasploitable. Questo dimostra l'efficacia di Metasploit Framework nell'identificare vulnerabilità e nel fornire informazioni utili per scopi di test di penetrazione e sicurezza informatica.