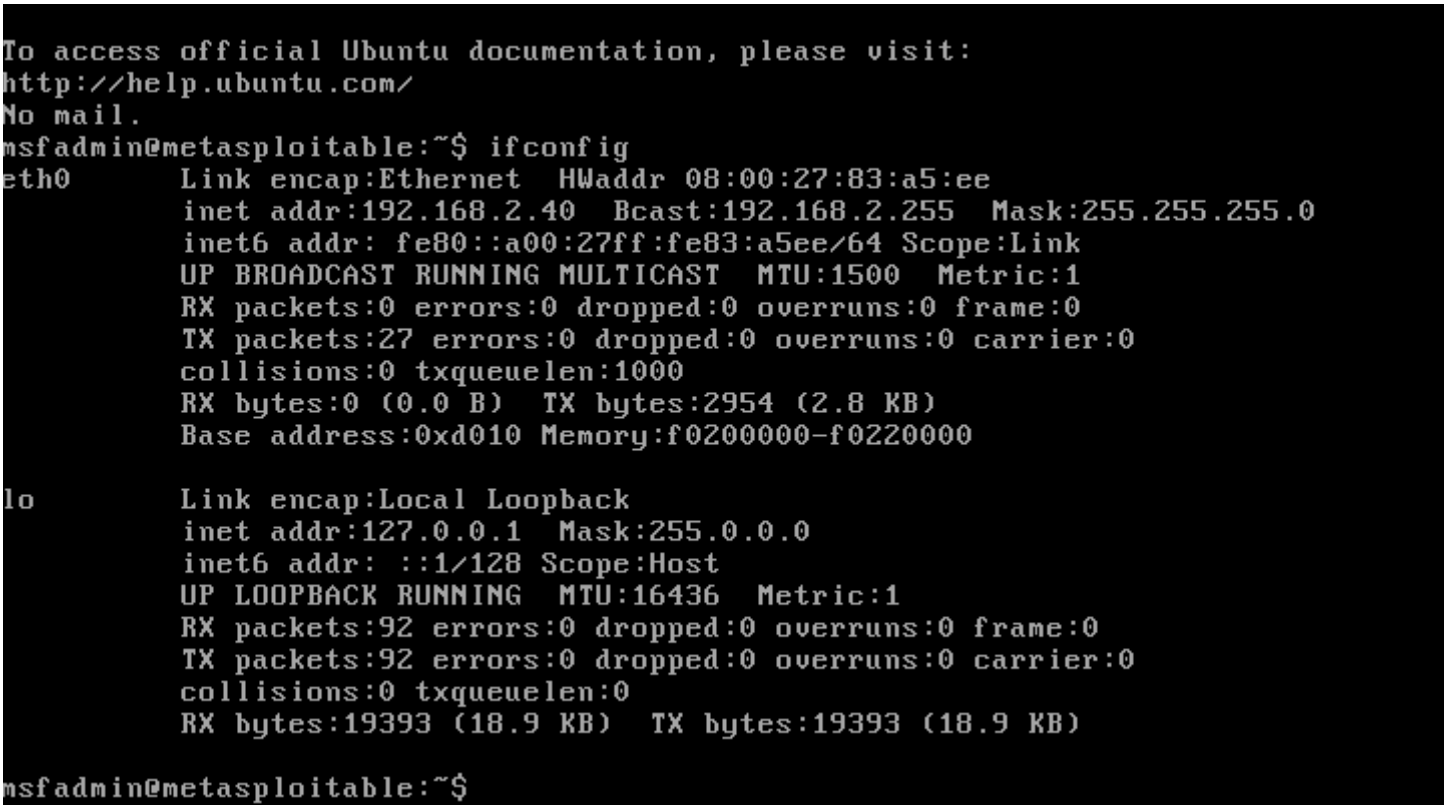
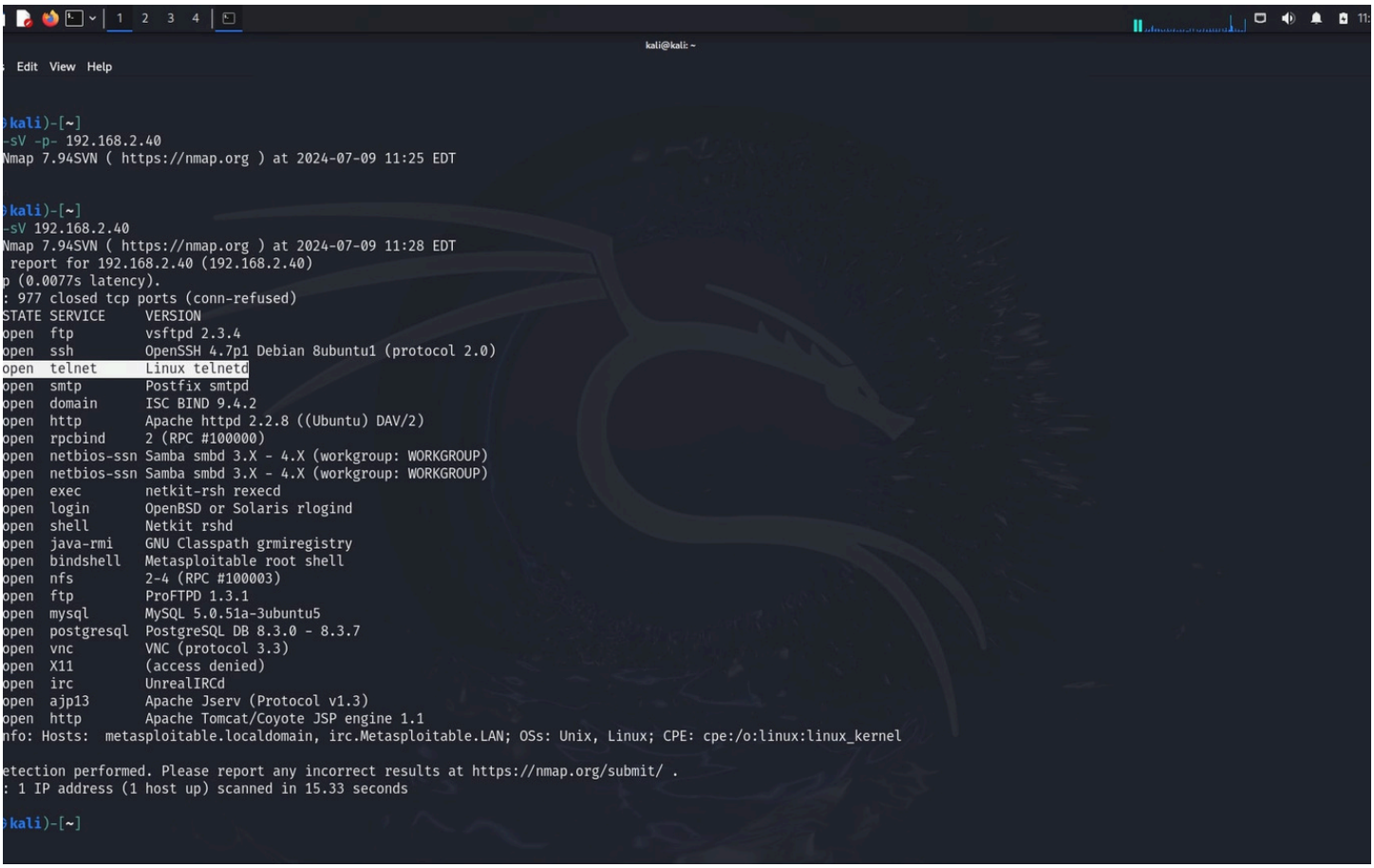
Report Hacking to Metasploitable

Configurazione indirizzo IP della macchina **Metasploitable.**



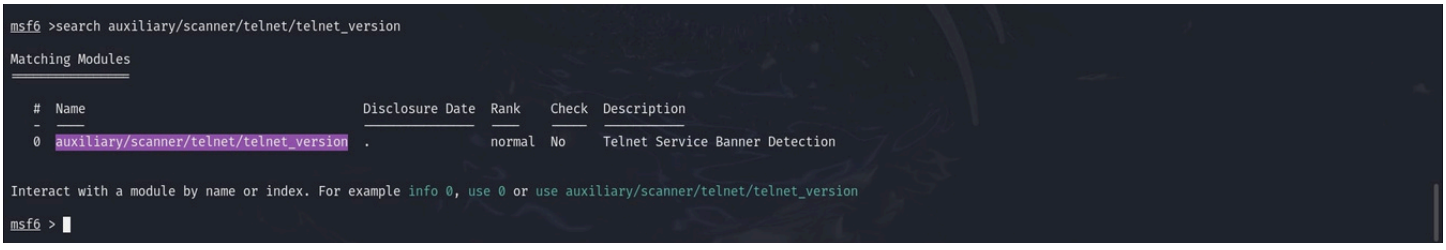
Configurazione indirizzo IP della macchina **Kali Linux.**

Scansione con **nmap** verso la macchina **Metasploitable** per identificare le **porte aperte** e in particolar modo la porta di nostro interesse che è la **porta n° 23.**

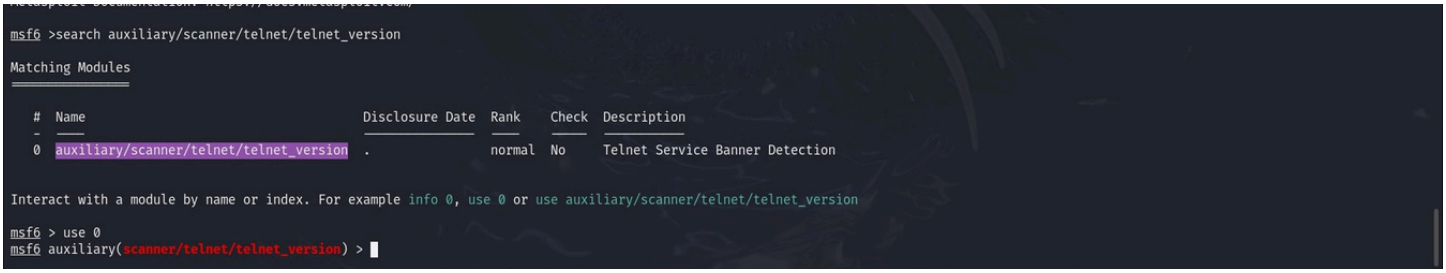


Avvio di **msfconsole** tramite il comando “**msfconsole**”.

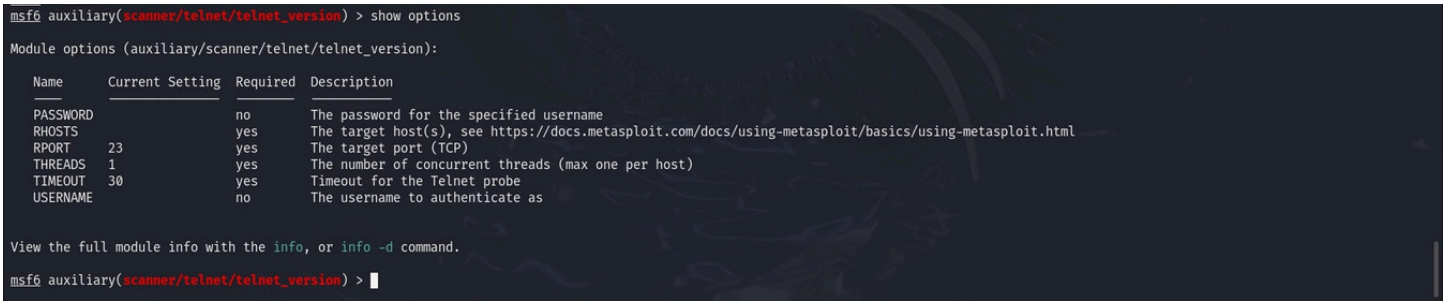
Ricerca dell’exploit telnet tramite il comando “**search auxiliary/scanner/telnet/telnet_version**”.



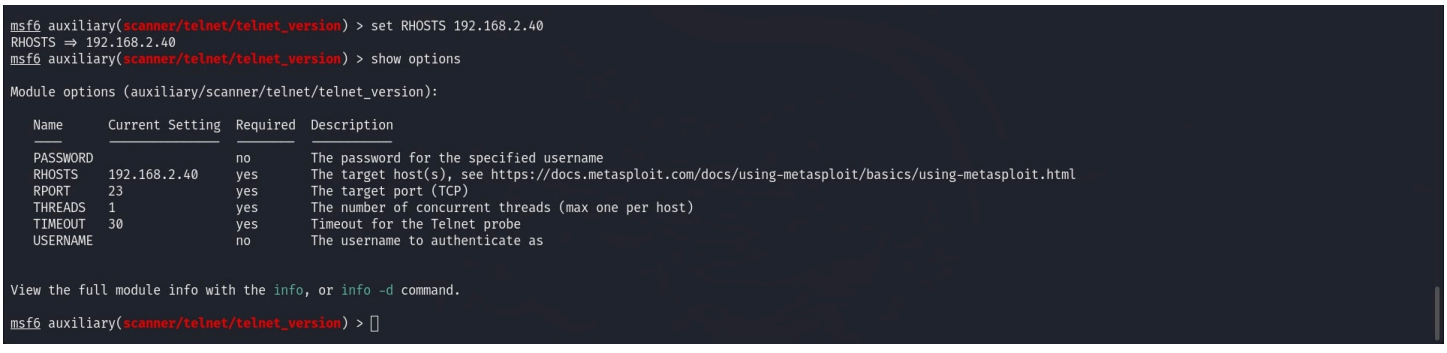
Scelta del payload “**search auxiliary/scanner/telnet/telnet_version**” tramite il codice di appartenenza “**0**”.



Esecuzione del comando “**show options**” per controllare che le configurazioni fossero giuste.



Esecuzione del comando “**set rhosts + indirizzo IP della macchina target**” per impostare e memorizzare **l’indirizzo IP del target** e successiva verifica dell’effettiva memorizzazione dell’IP tramite il comando “**show options**”.



Esecuzione del comando “**run**” che equivale al comando “**exploit**”, dove entrambi eseguono l’attacco verso il target prescelto. Inoltre, come è possibile vedere tramite lo screen, il risultato mostra anche i dati di login che serviranno successivamente per entrare all’interno della macchina metasploitable.

Effettiva avvenuta dell’attacco e ingresso all’interno della macchina metasploitable tramite i dati di login recuperati precedentemente, quali: **username**(msfadmin), **password**(msfadmin).