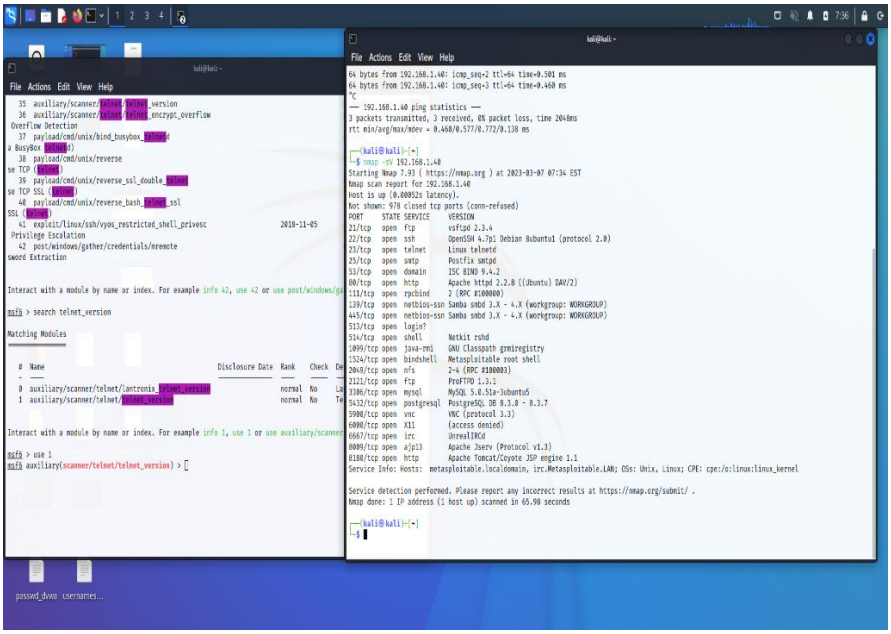
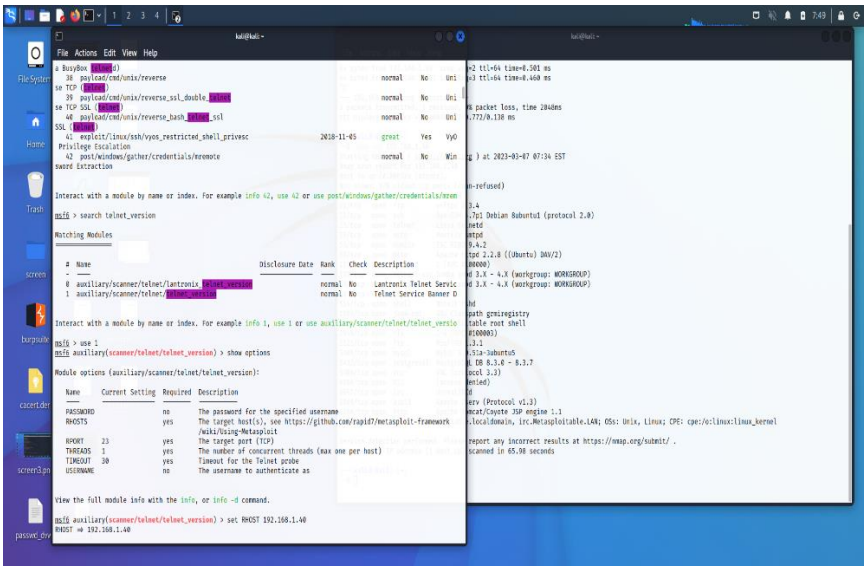
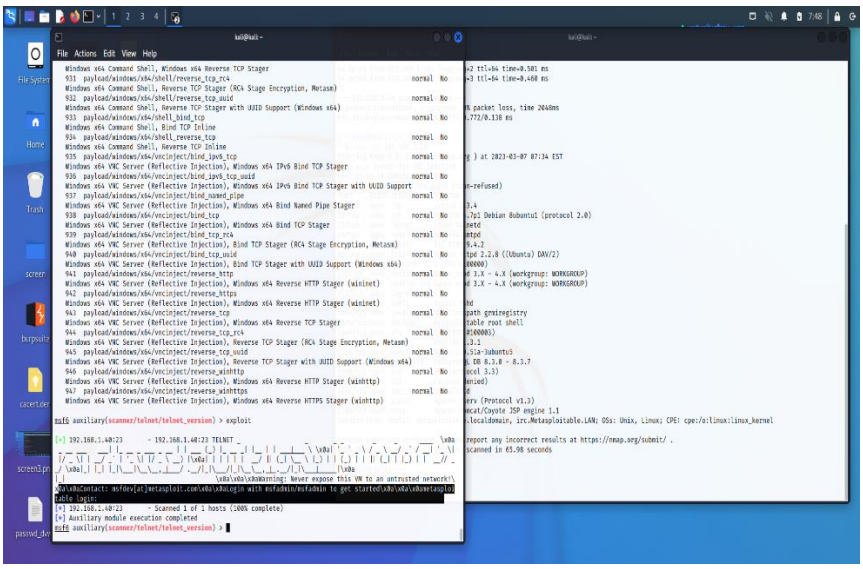


1.) DOPO aver messo le macchine in comunicazione e provato un ping da kali a meta per vedere se arrivano i pacchetti, lanciamo un NMAP -SV verso meta per vedere le porte aperte, il relativo servizio e la versione. Per vedere ulteriori info sulla porta scelte che vogliamo attaccare, lanciamo il comando NMAP -p 23 -A IP_ADDRESS. Apriamo nel frattempo MSFCONSOLE da una shell (abbiamo scelto di aprirlo in kali perchè da meta non vi è il comando). Dalla Console di meta aperta cerchiamo l'exploit TELNET_VERSION con SEARCH.

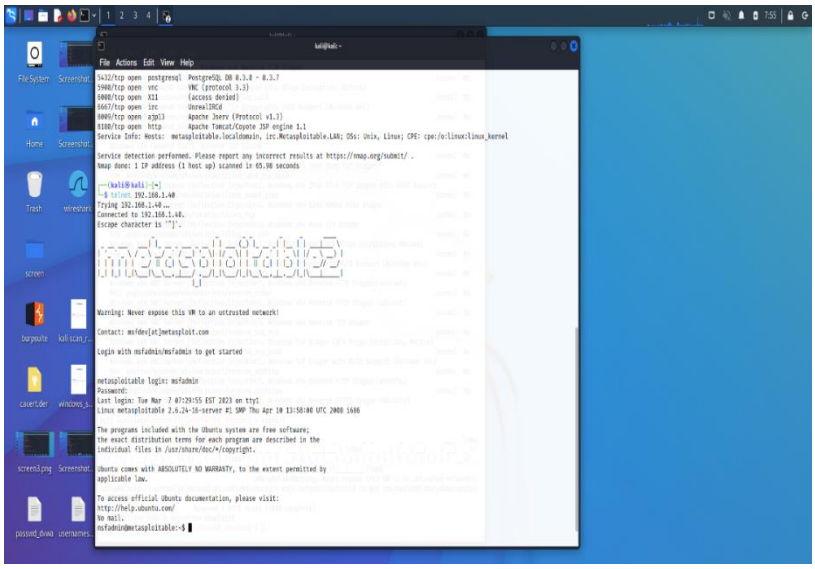


2.) Scegliamo con USE l'exploit 1, con SHOW OPTIONS andiamo a vedere i settaggi obbligatori, sono già tutti impostati eccetto RHOST,per cui settiamo solo RHOST ovvero l'indirizzo di meta con il comando SET RHOSTS IP_ADDRESS. Notiamo che per questo payload non sono previsti payload.



3.) Possiamo lanciare direttamente l'attacco con EXPLOIT (oppure RUN)

4.) L'attacco è andato a buon fine, la scansione ci restituisce la login per accedere a meta tramite la porta 23.



5.) Facciamo la prova, ci colleghiamo da kali a meta tramite la porta 23 con il comando TELNET IP_ADDRESS, e proviamo ad accedere con i dati di login recuperati.

I dati sono corretti e siamo entrati.