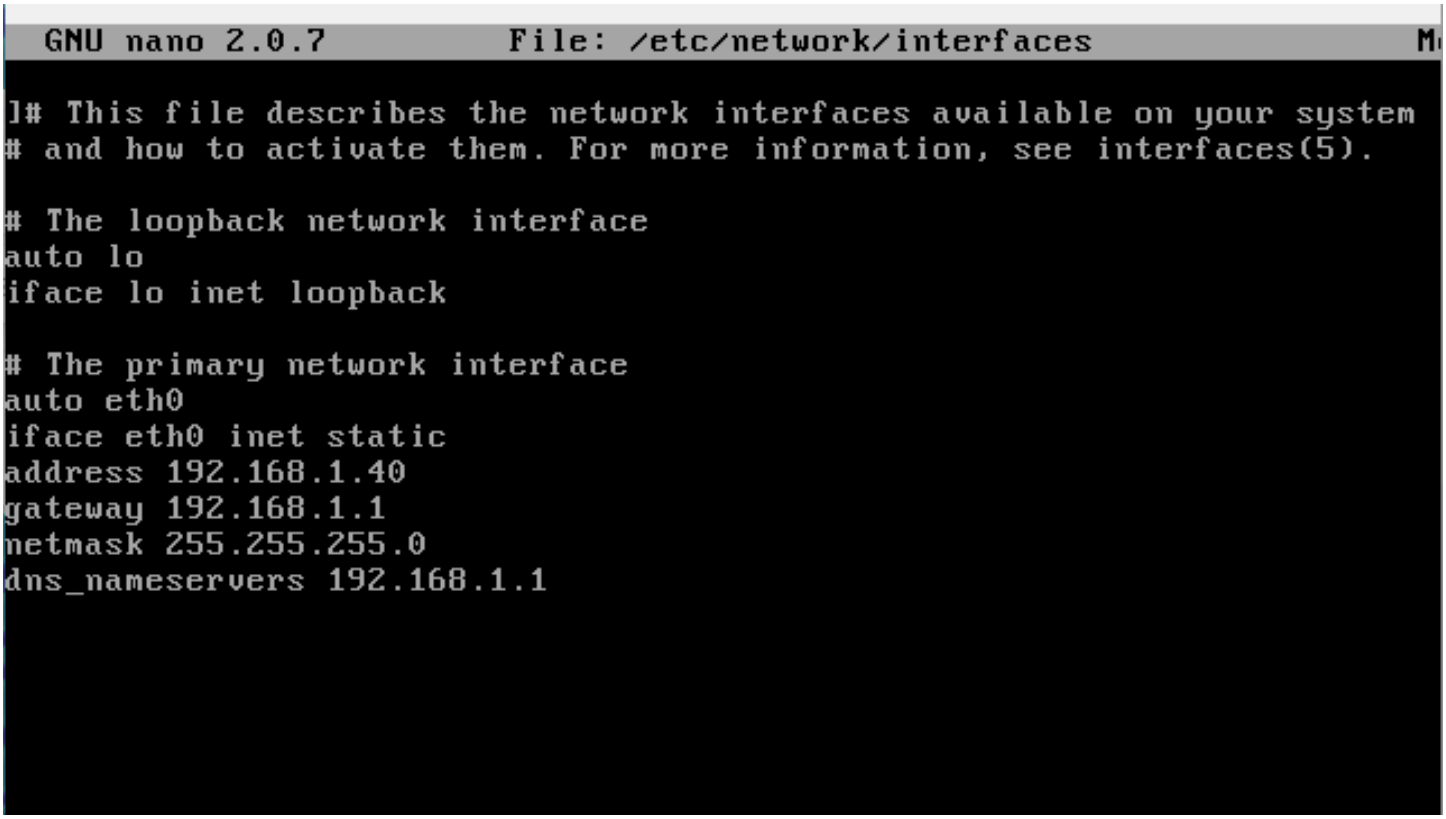
S7L2

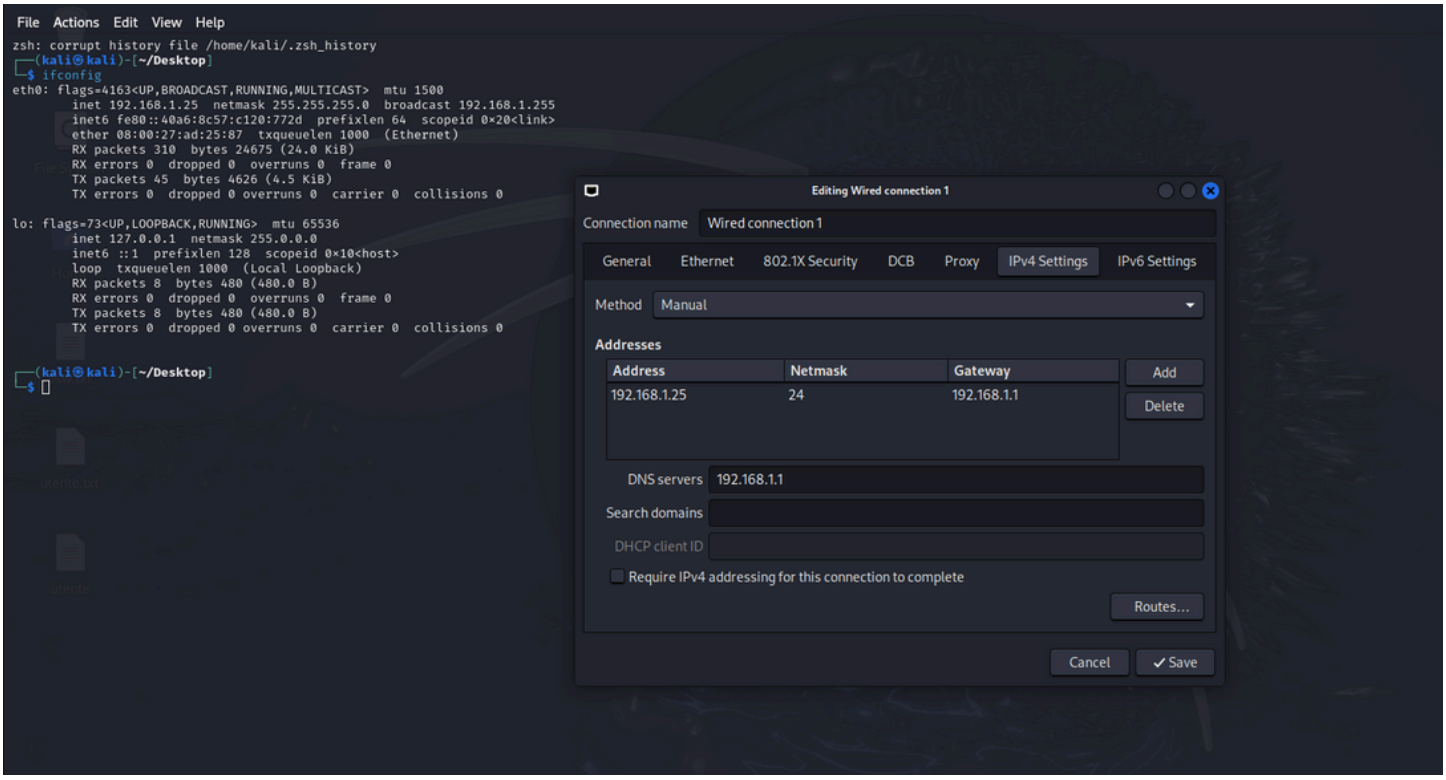
Data:12/11/24

INFORMAZIONI PRINCIPALI

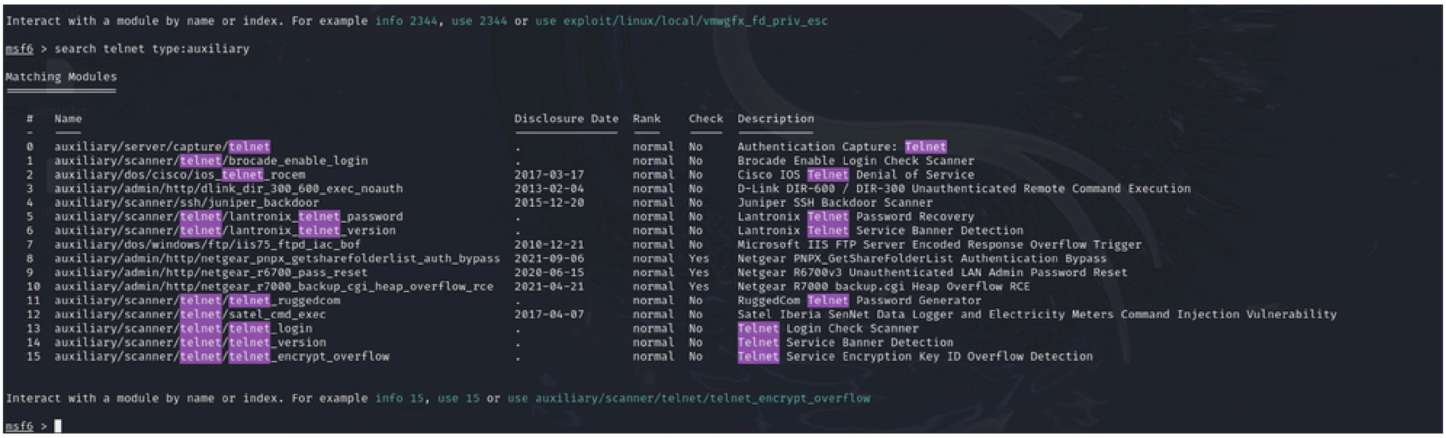
Imposta l'indirizzo IP della tua macchina Kali su 192.168.1.25 e quello di Metasploitable su 192.168.1.40. Avvia Metasploit e utilizza il modulo auxiliary/scanner/telnet/telnet_version per verificare la versione di Telnet sulla macchina Metasploitable. Esegui il modulo per identificare eventuali vulnerabilità e raccogli le informazioni sul servizio Telnet.

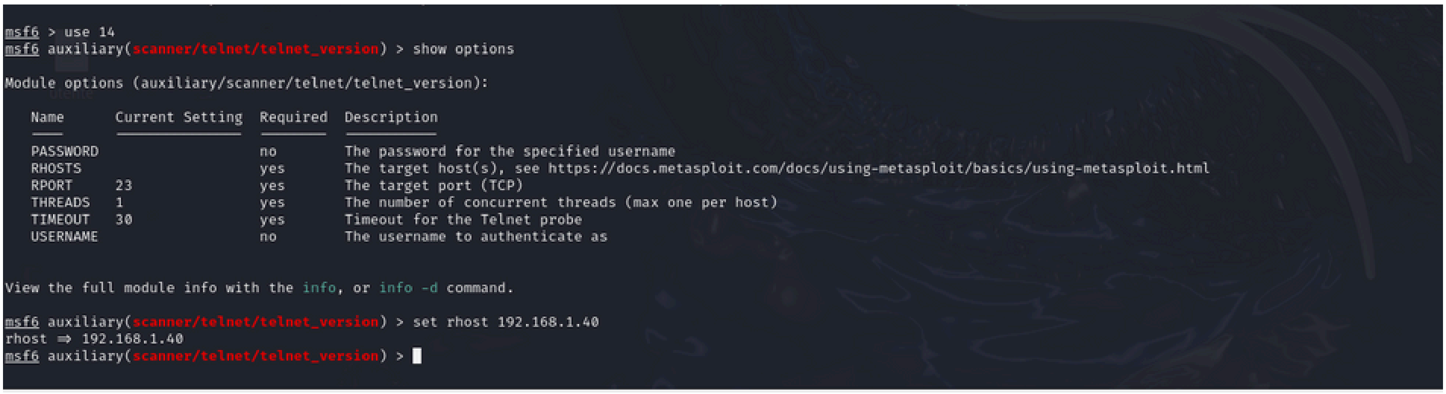
Ho iniziato impostando le macchina di metasploitable su 192.168.1.40 con i seguenti parametri.



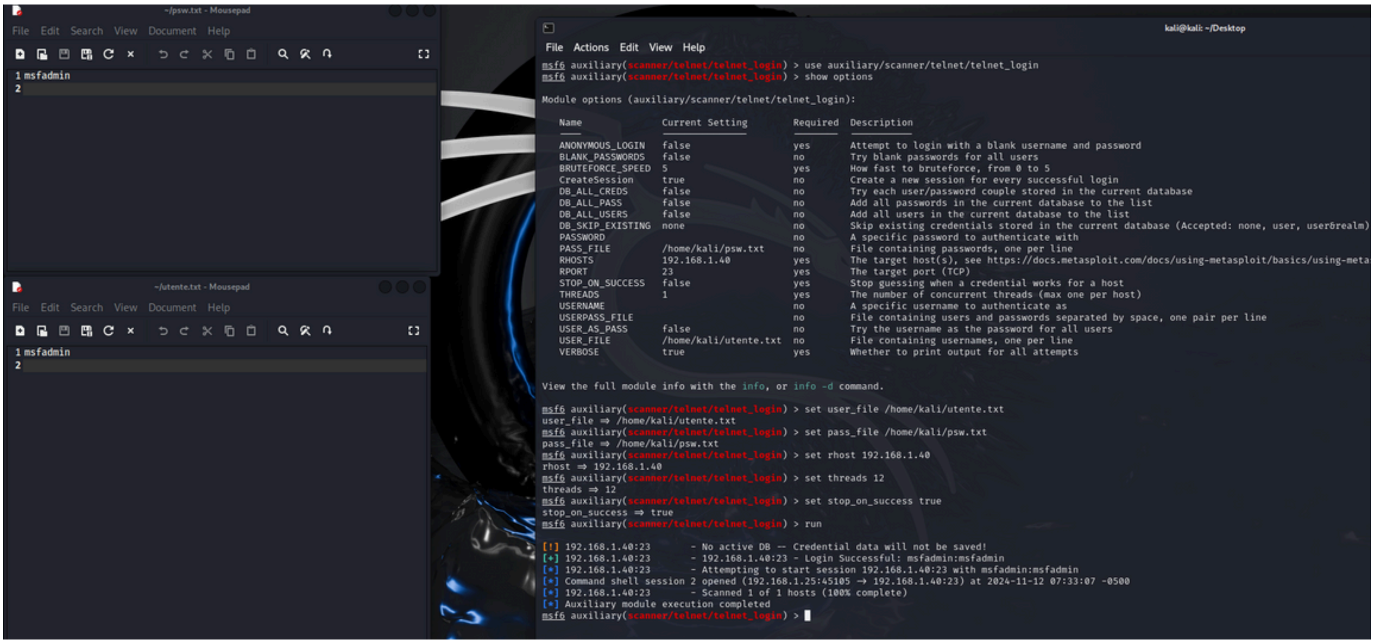


Dopodichè ho cercato dei moduli per telnet ed abbiamo utilizzato telnet_version per vedere le informazioni di telnet, lo impostiamo con set rhost e l'indirizzo ip della vittima ed eseguiamo con run.





Con il plugin telnet_login possiamo fare un attacco bruteforce a dizionario mirato (conosciamo la password e l'utente, altrimenti possiamo utilizzare dizionari più grandi come xato da 10 milioni o anche misti se conosciamo dei dettagli aggiuntivi sulla lunghezza dell'username, maiuscola all'inizio o 1 carattere speciale etc.) Una volta selezionato il file per l'utente e la password ed abbiamo impostato l'indirizzo ip della vittima con set rhost procediamo con run per eseguire l'exploit. Stop_on_success è per fermarsi una volta trovato un match. Con threads modifichiamo i tentativi di connessione contemporanei.



Conclusioni

ho configurato la macchina Metasploitable con un indirizzo IP statico e ho utilizzato Metasploit per eseguire un attacco brute-force su Telnet. Grazie al modulo telnet_version sono riuscito ad “indagare” sul servizio telnet. Mentre con telnet_login, sono riuscito a forzare l'accesso alla macchina target utilizzando un dizionario mirato, ottimizzando il processo con l'uso di threads e fermandomi al primo successo. Questa attività ha dimostrato l'efficacia di Metasploit per sfruttare vulnerabilità Telnet con un approccio mirato e automatizzato.