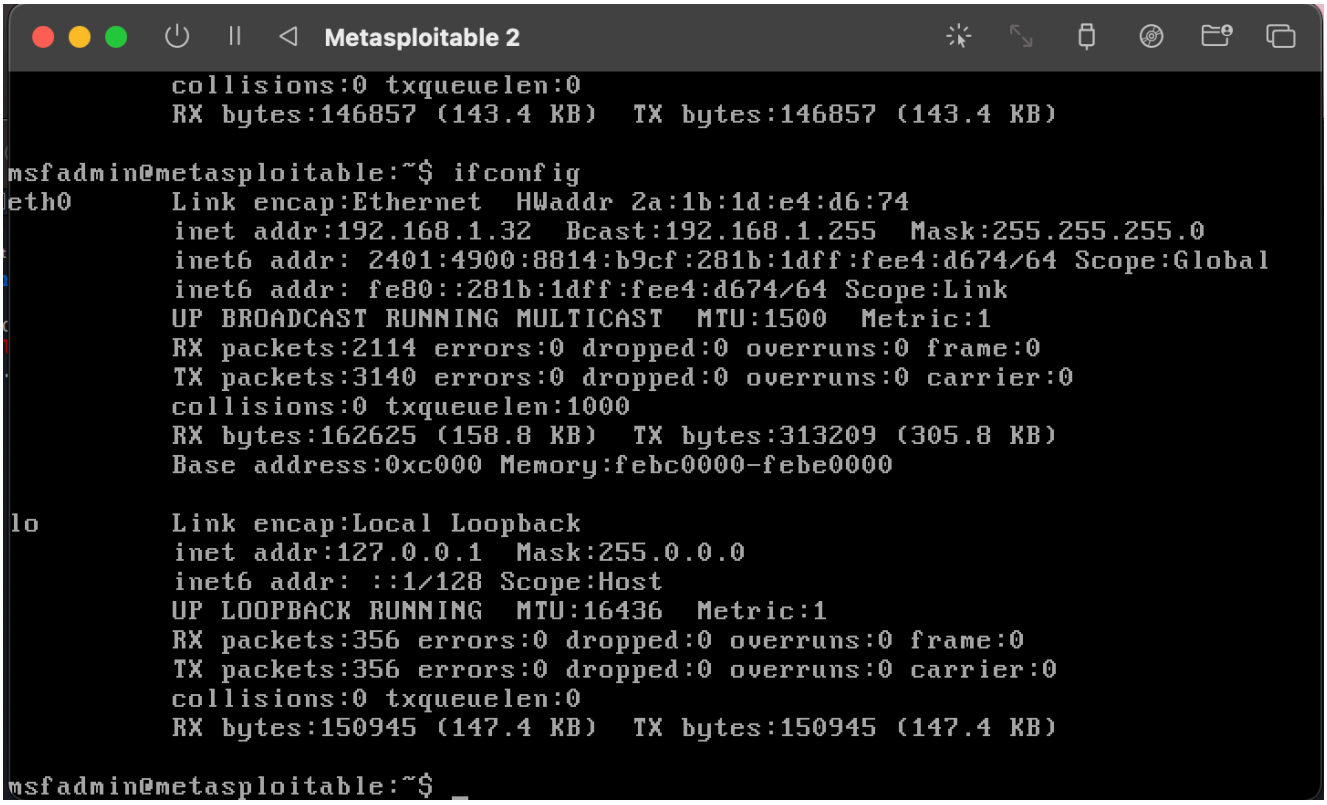
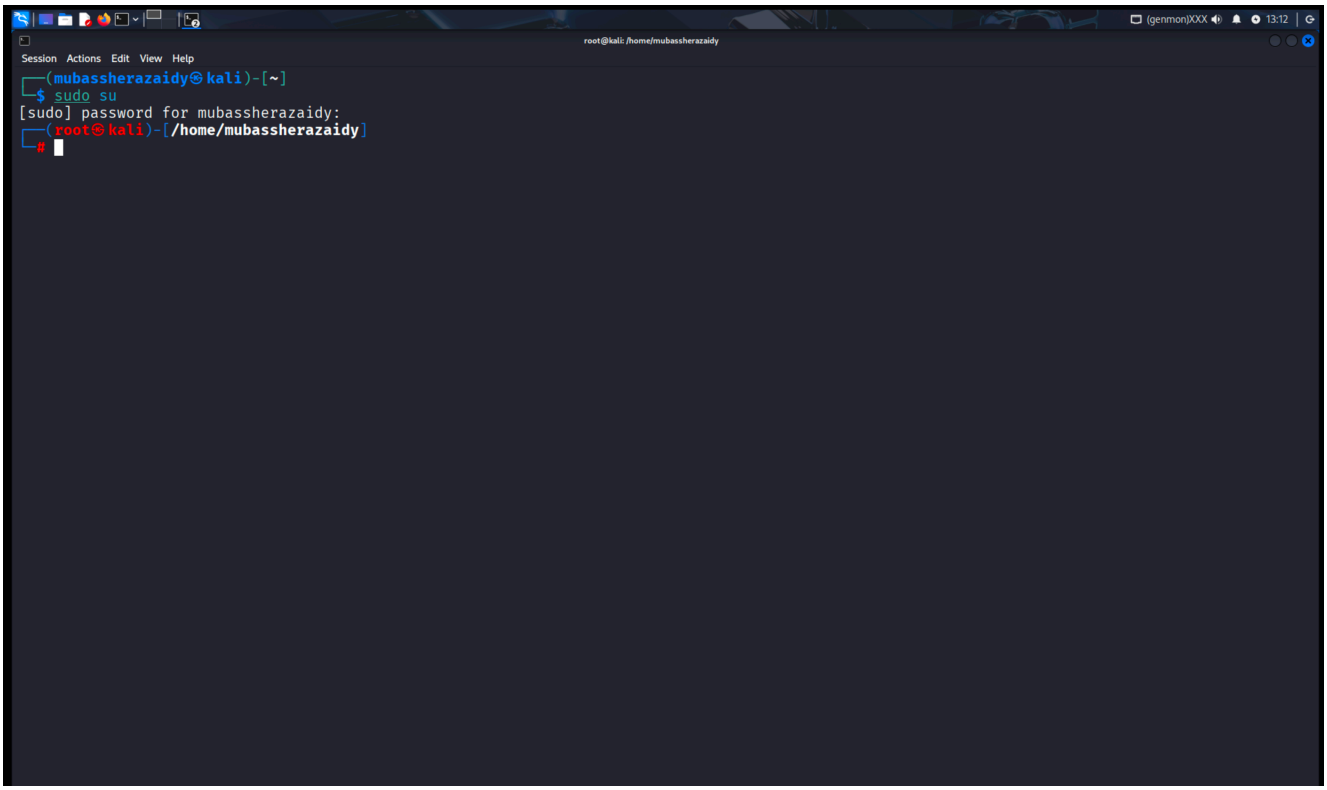
BRUTE-FORCE PASSWORD CRACKING USING HYDRA IN VM

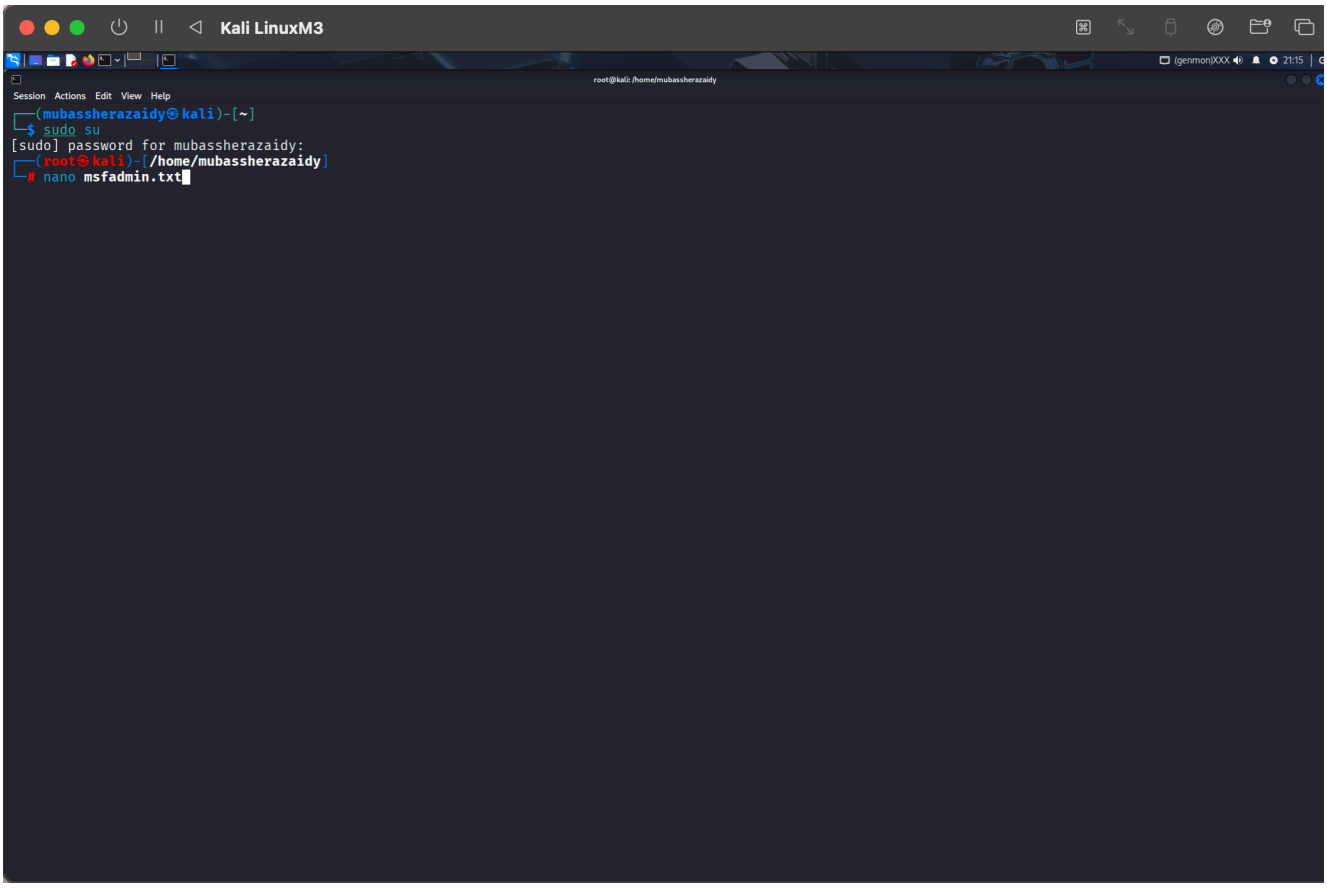
STEP 1: On your Metasploitable machine, type `ifconfig` in the terminal to find its IP address. Inet addr is your IP address



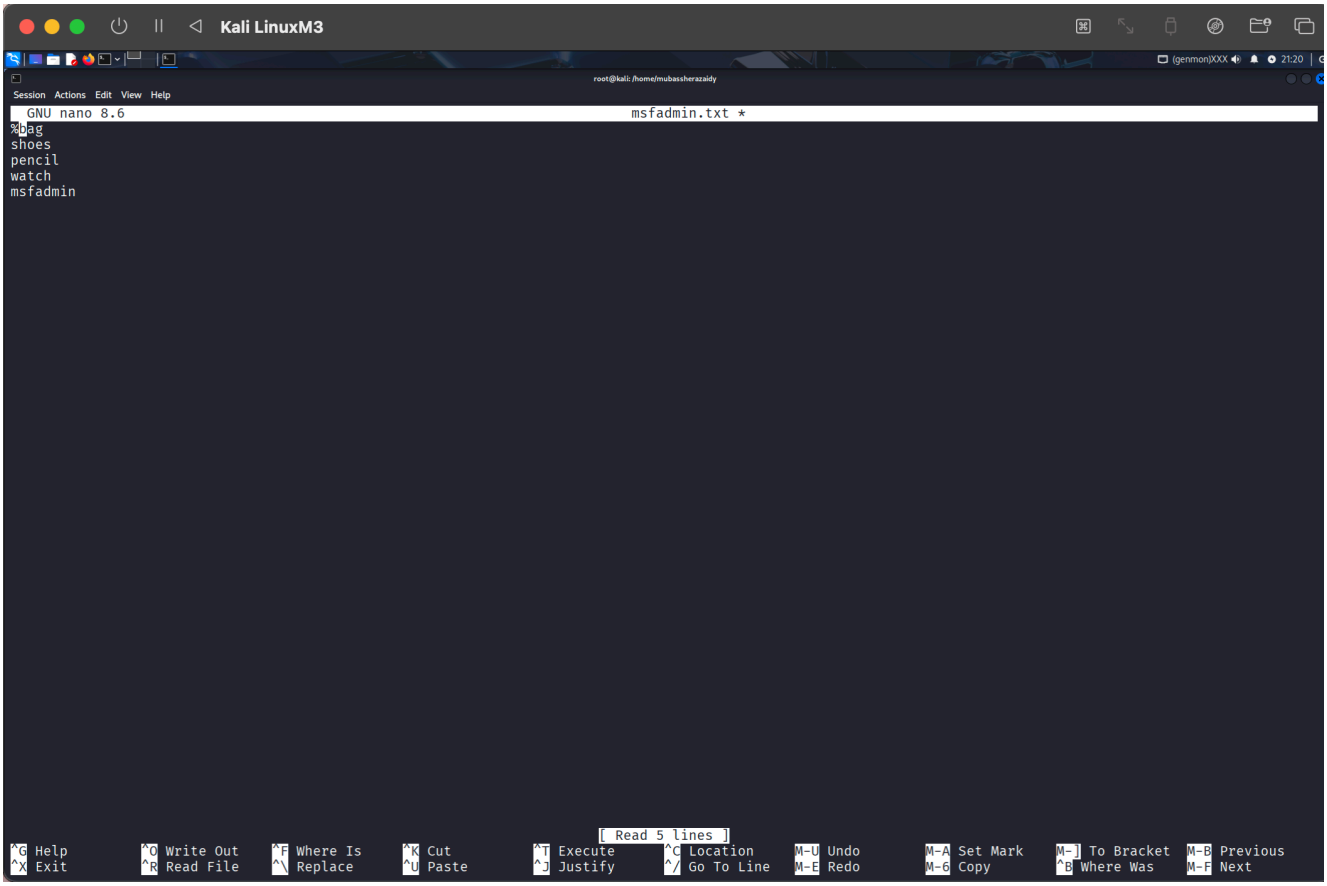
STEP 2 : Open the Kali Linux terminal and switch to the root user.



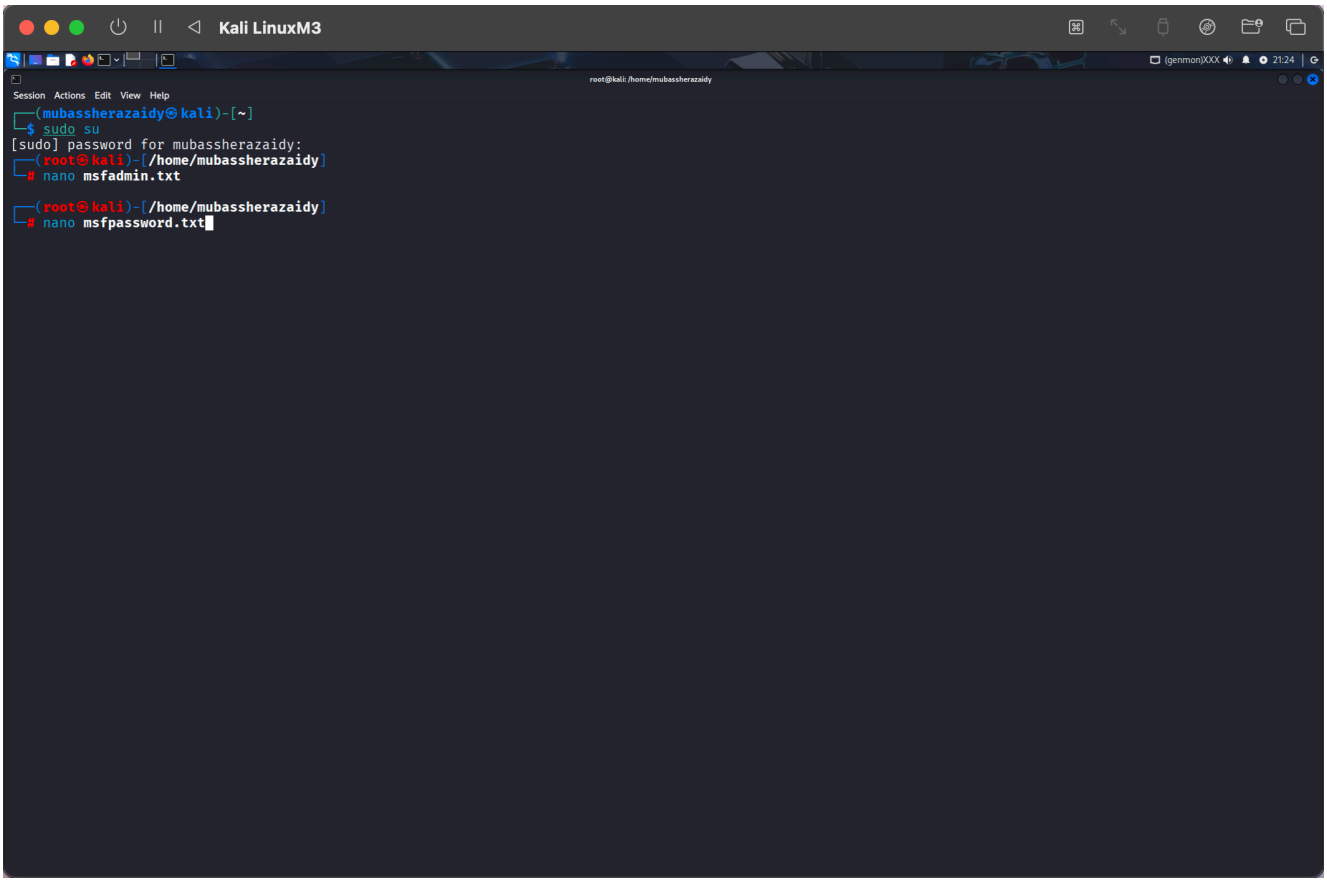
STEP 3 : Create a text file for login name using the nano command



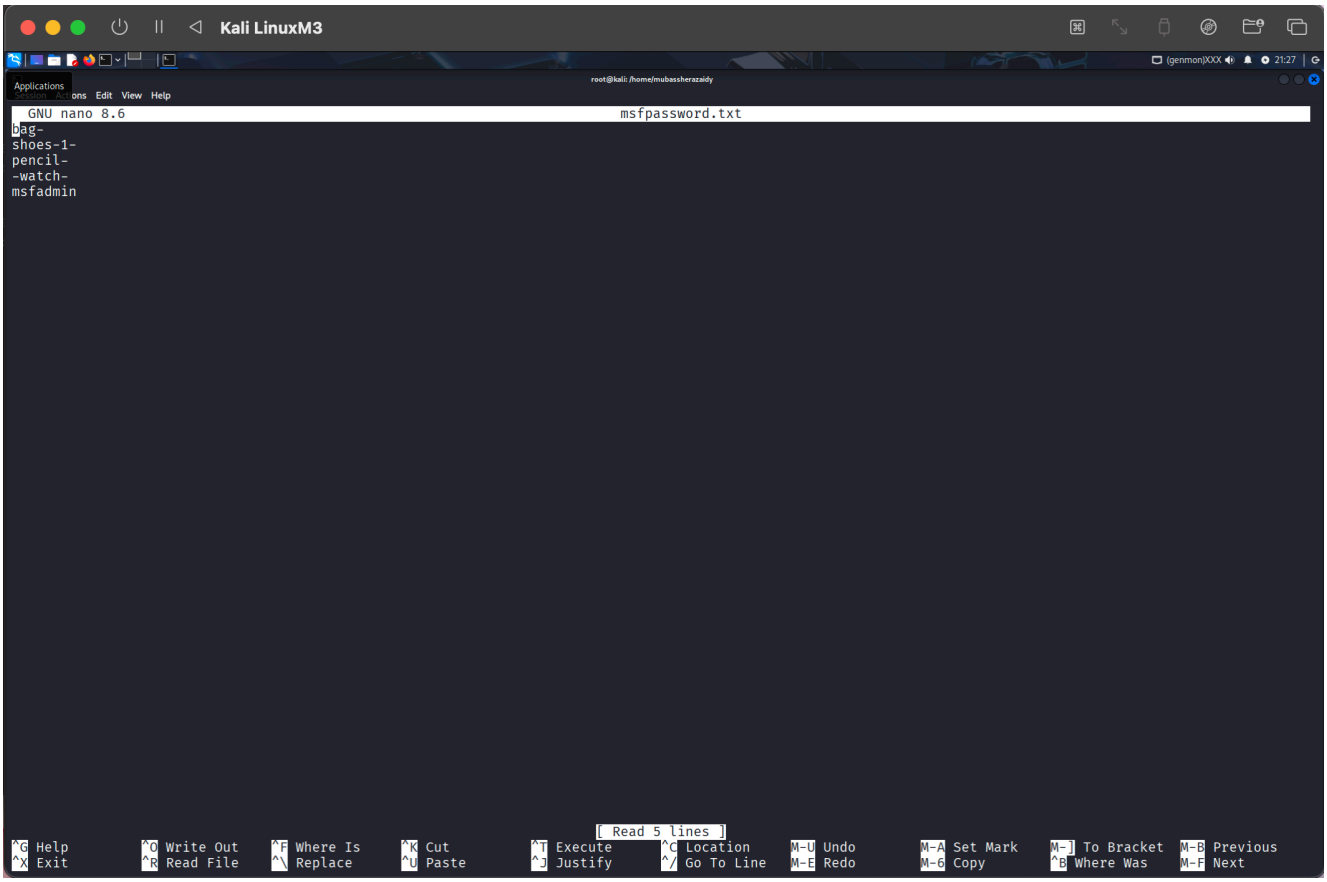
STEP 4: In the text file, type few random words and at the end the login name of metasploitable - msfadmin and save it.



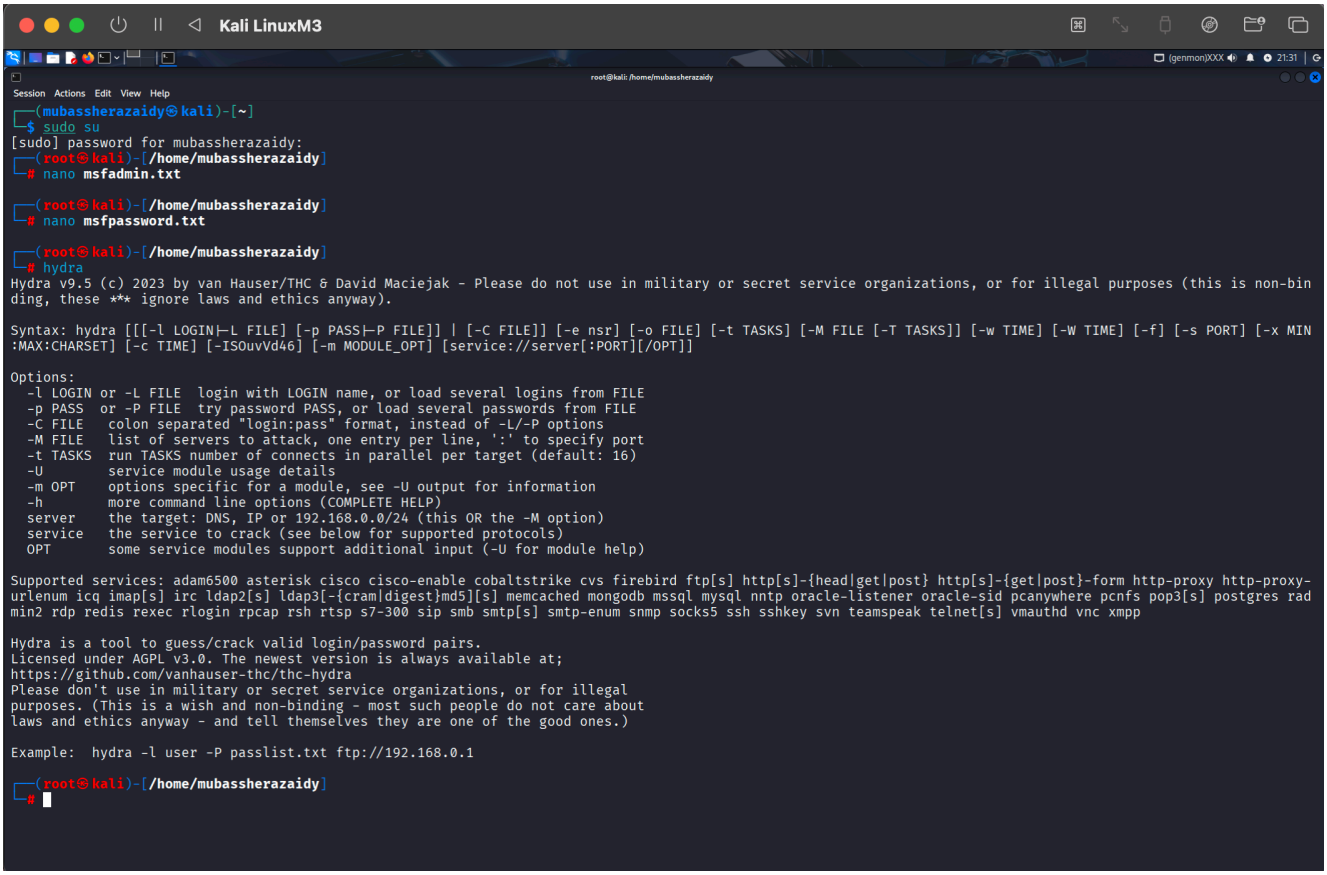
STEP 5 : Now create a txt file for password using nano command



STEP 6 :In the password txt file, type few random password and the end the password of metasploitable - msfadmin



STEP 7 : Now type hydra in the terminal



STEP 8 : Now run the following command - `hydra -L msfadmin.txt -P msfpassword.txt ftp://192.168.1.31 -f -t 4`

Interpretation:

`hydra` :The tool used for parallelized login cracking.

`-L` : Specifies a file containing of list of potential login names.

`msfadmin.txt` : file containing the potential login names

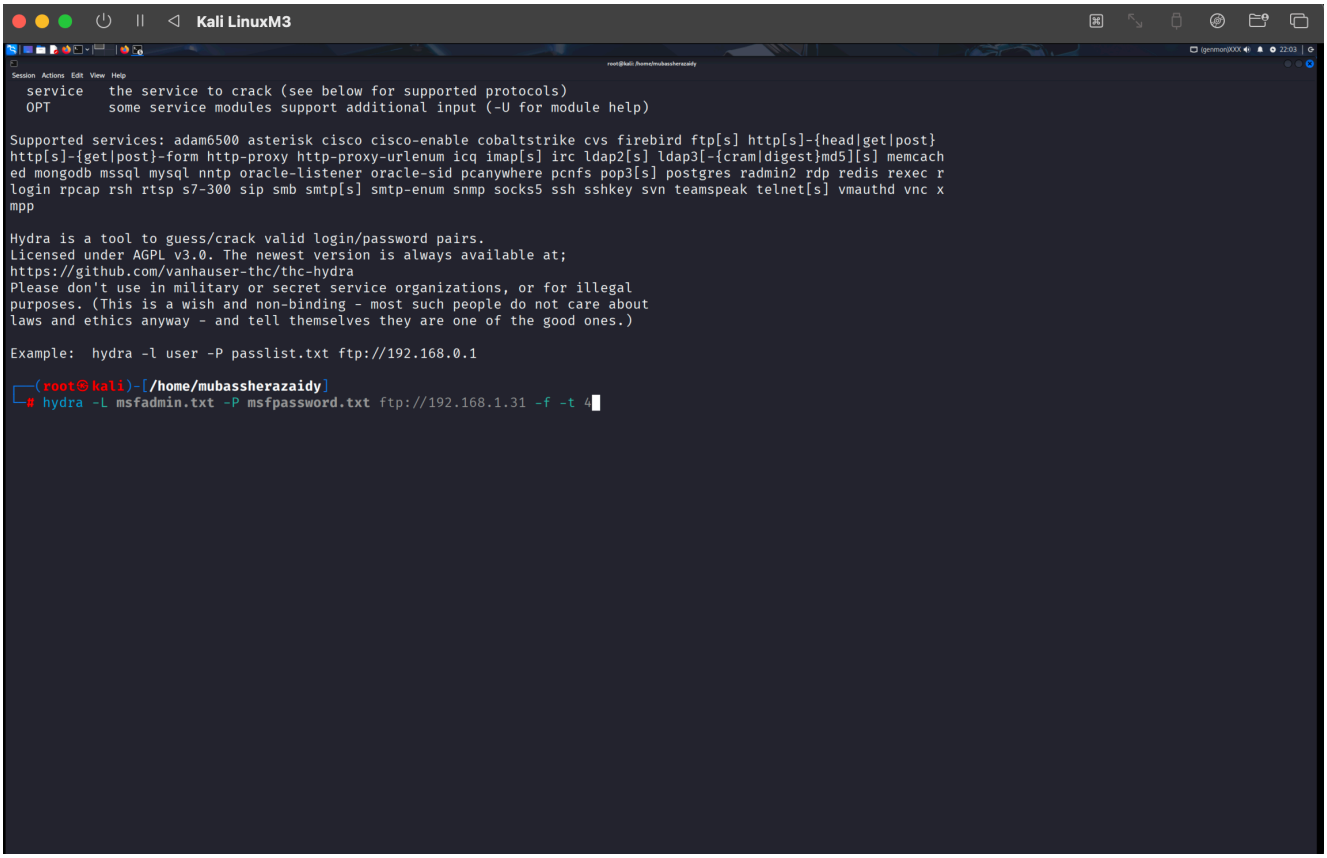
`-P` : Specifies a file containing of list of potential password names.

`msfpassword.txt` : file containing the potential password names

`ftp://192.168.1.31` : Target FTP service hosted at the given IP address.

`-f` : Tells Hydra to stop after the first successful login is found.

`-t 4` : Sets the number of parallel threads to 4, speeding up the attack.



STEP 9 :The username and password should appear highlighted in green text.