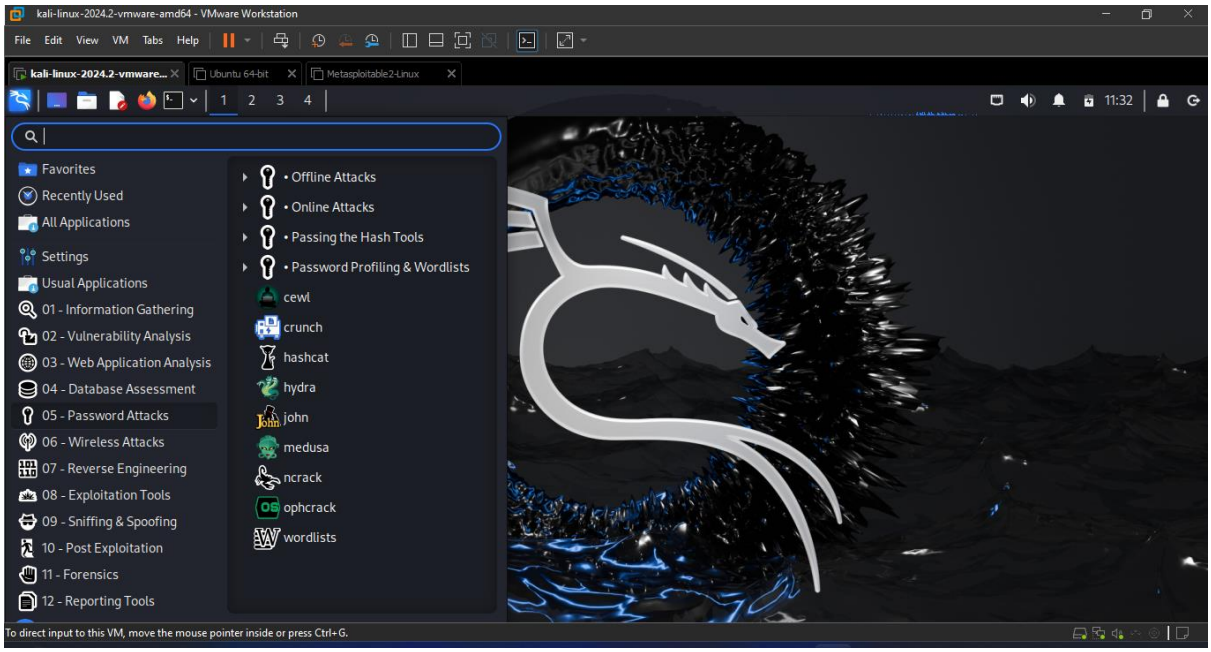
John The Ripper

- The John-the-ripper tool is an open-source application and post-exploitation Kali Linux operating system tool that allows users to view authentication credentials.
- This tool provides hashes from shadow file of Kali Linux operating system to users.
- Kali Linux store password data in a shadow file in the form of a hash. The forensics team can use John-the-ripper tool to get the password in plain text and pass it to the target computer to login.

Steps:

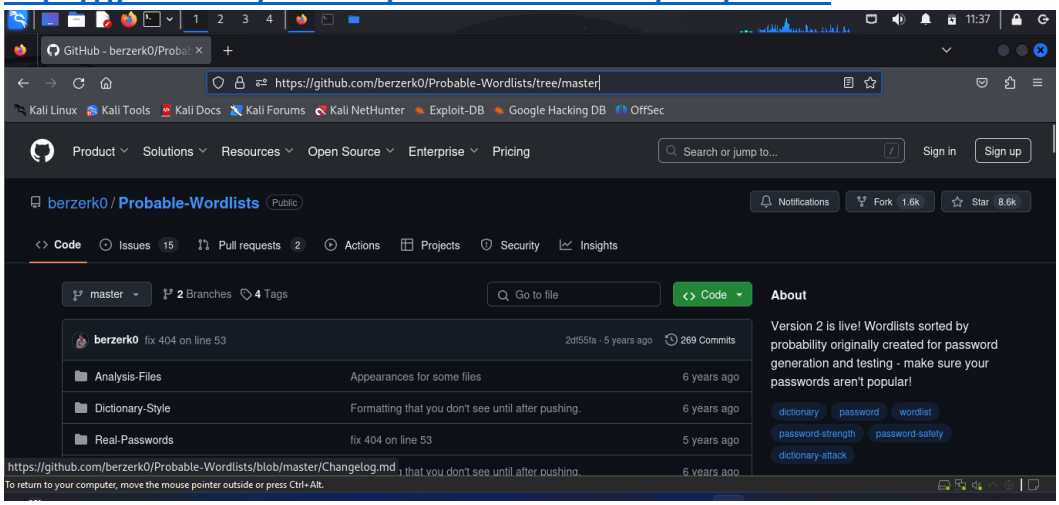
Step 1: Open Kali Linux operating system → Go to Applications → Password attacks → John.

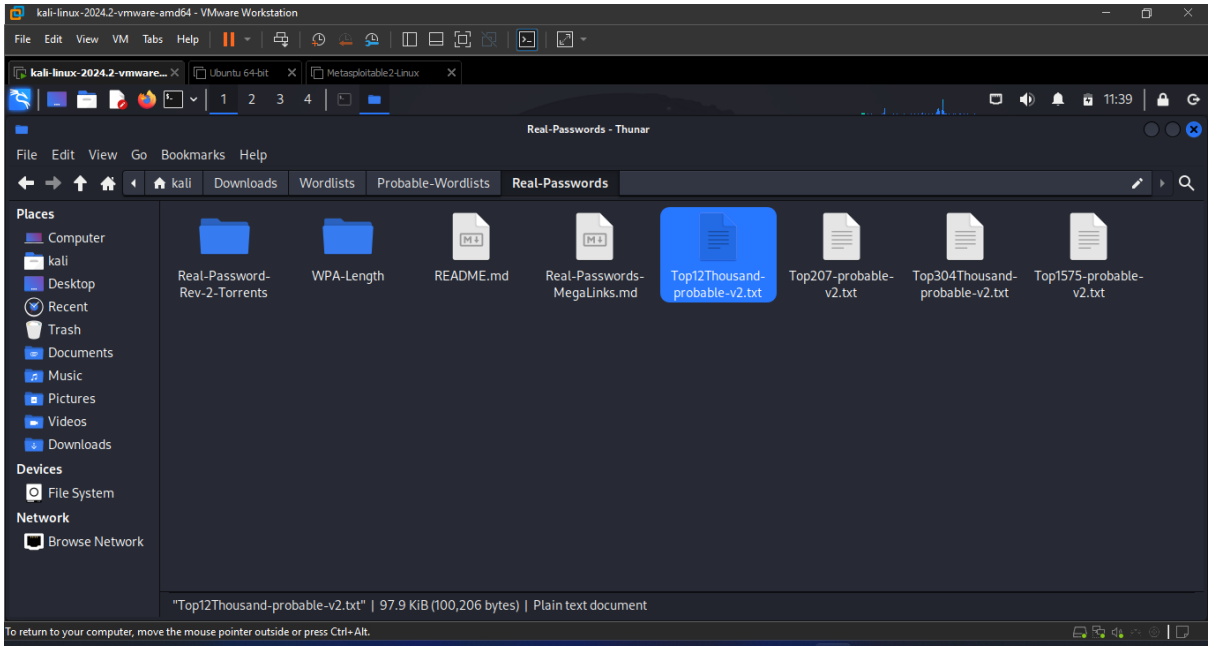


Step 2:

Download the Wordlists from the below Website.

https://github.com/berzerk0/Probable-Wordlists/tree/master



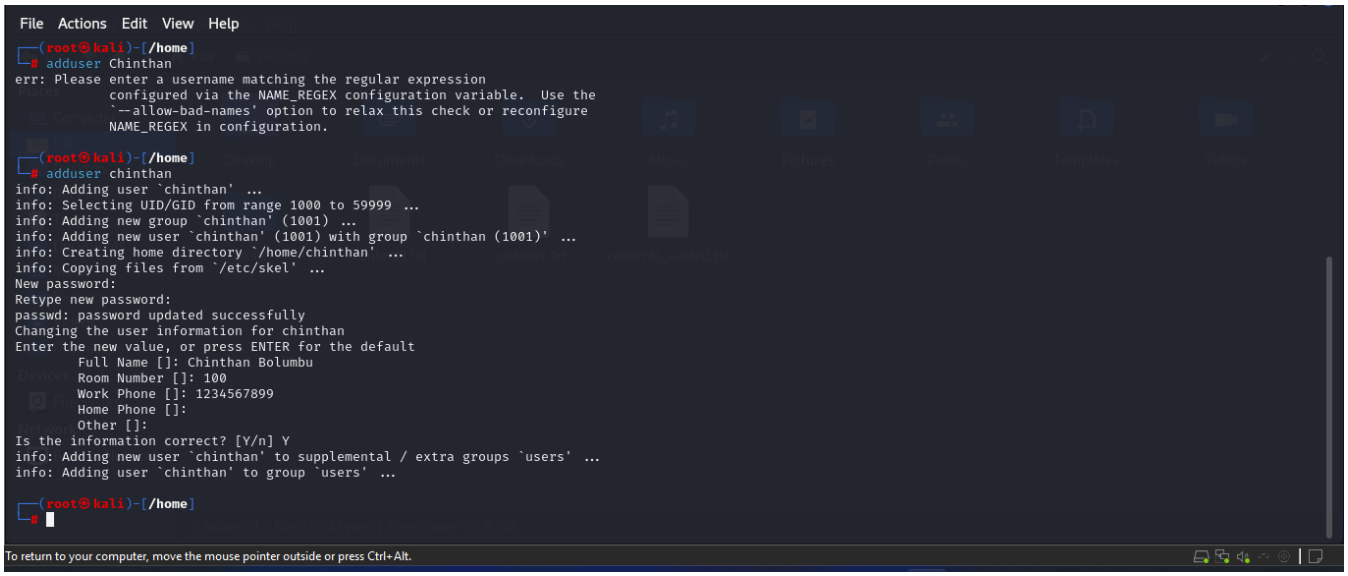


Step 3:

Go to root-kali by `sudo su` and then store file ‘wordlist.txt’ there.

Copy Wordlists to Home Directory and start with `adduser` command in terminal.

Add new users in kali Linux operating system, set a password and press ‘Y’ while creating new users.

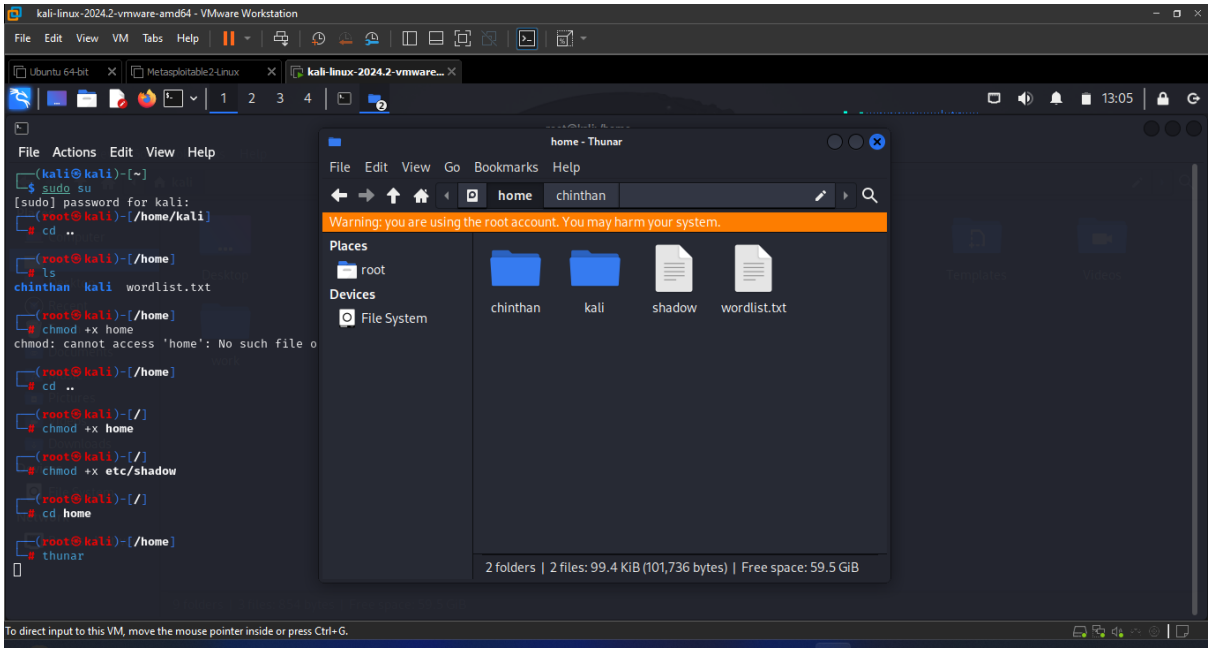


Step 4:

Command `Thunar` to access home Directory.

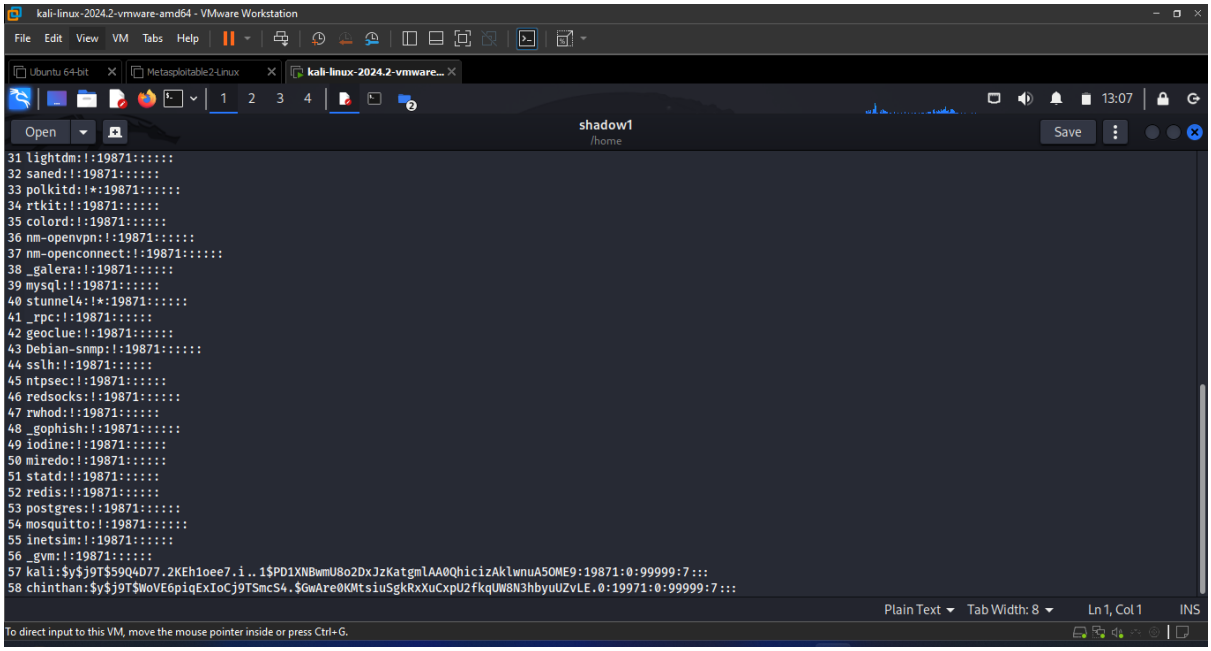
Copy the shadow file from file system and paste it to Home directory. OR

Command `cp /etc/shadow ./shadow1.txt` (Ignore Step 5)



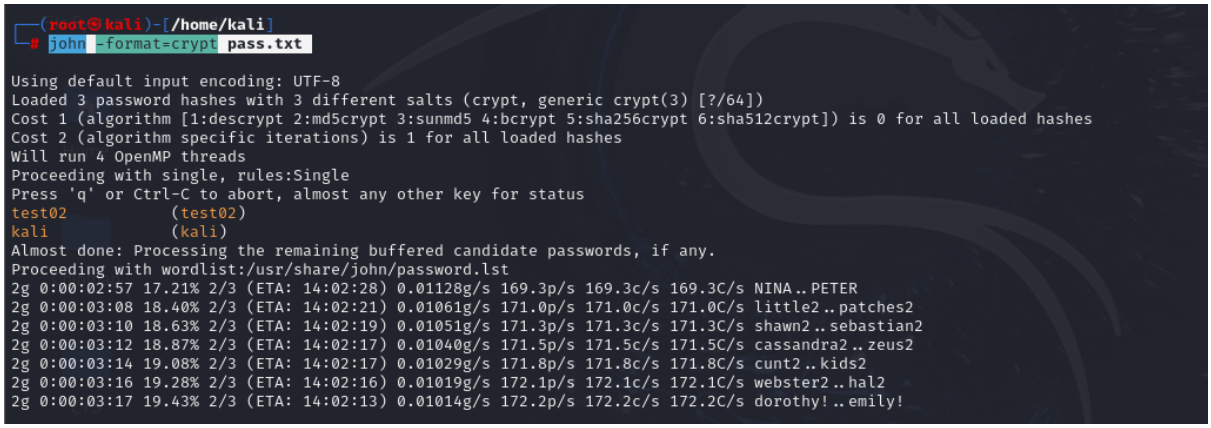
Step 5:

Rename Shadow file to Shadow1 and open the file and search for username and password. (if you Copy and paste in a directory)



Step 6:

Command `john -format=crypt pass.txt` to start cracking.



- If the password set is easy then tool (John the ripper) will fetch the password from wordlist quickly.
- If the password set is slightly difficult then tool (John the ripper) will fetch the password from wordlist by checking each and every combinations.
- The orange coloured listed above is the username and the password associated, where left side is the password and right side is the username.
- Since there were 3 users set, 2 users had simple password and one user had difficult password where difficult password is taking time.
- The processes that are scheduled after the Orange colorued text is that, it is trying to crack the password from predefined wordlist in every combinations taking more time.
- If the passwords are there in wordlists matching with users password then, passwords will be revealed.