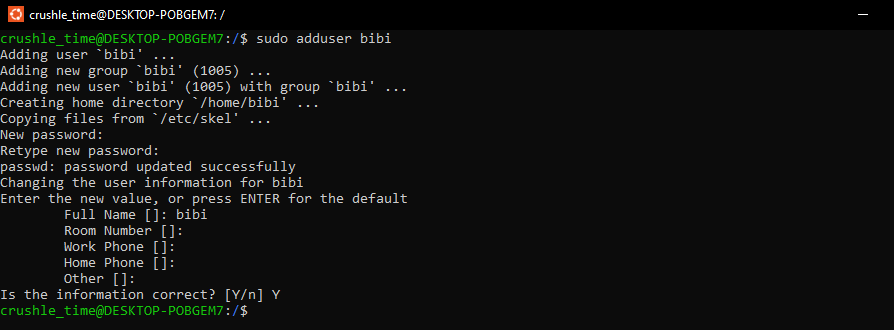
Linux commands

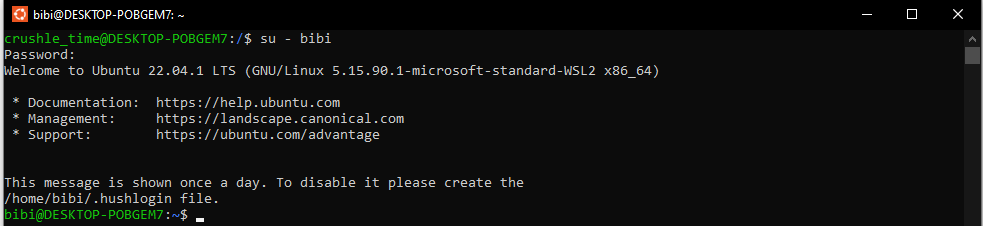
1.Elevate your user access to root:



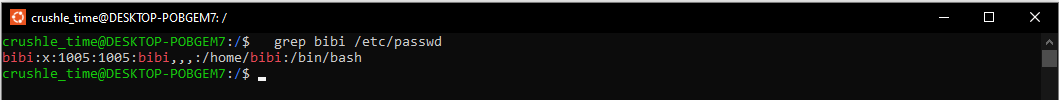
2. add a new user to your Linux OS and set a password for it:



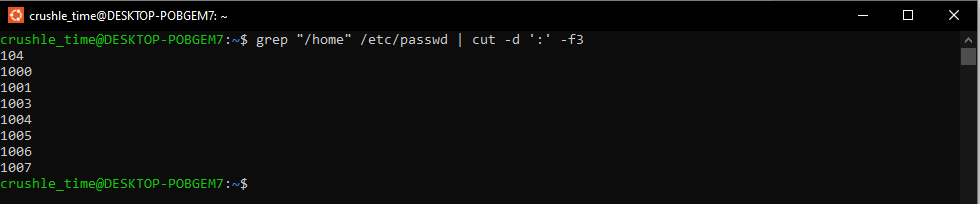
3. Test if you can log in using that user:



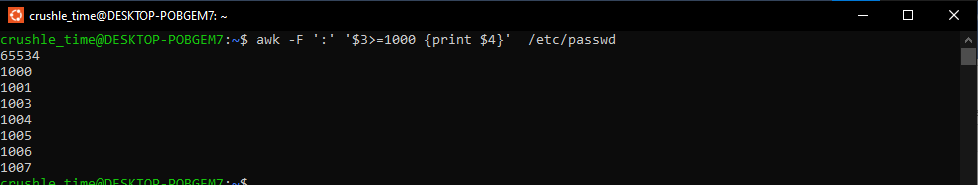
4. Using grep command check if the user is created



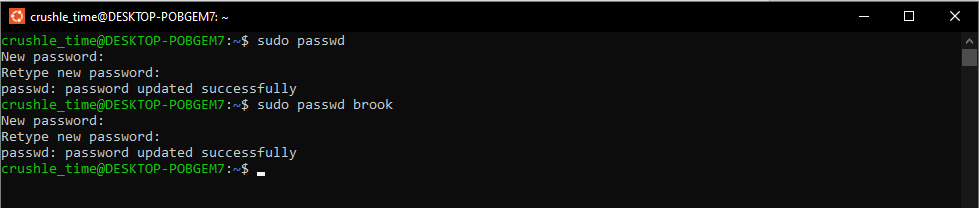
5. grep the UID of each user

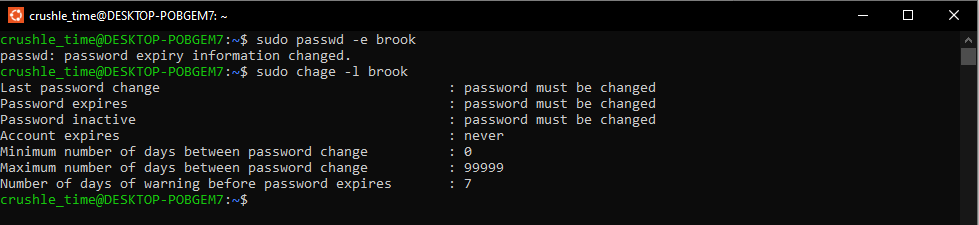


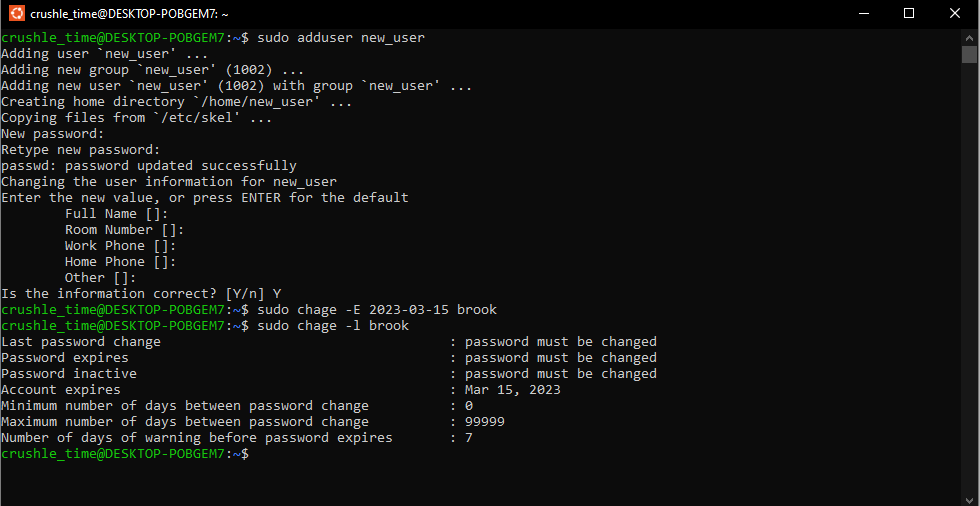
6. Find out the GID of the created user



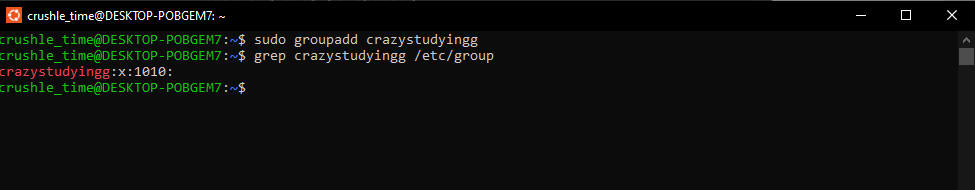
7. Change the password of the user and force it to change the pass on his next login

****

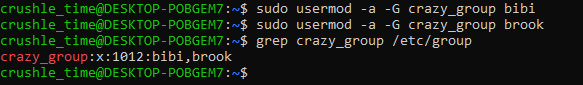
****

8. Add a new user and set an expiration date for it, with a five-day warning period****

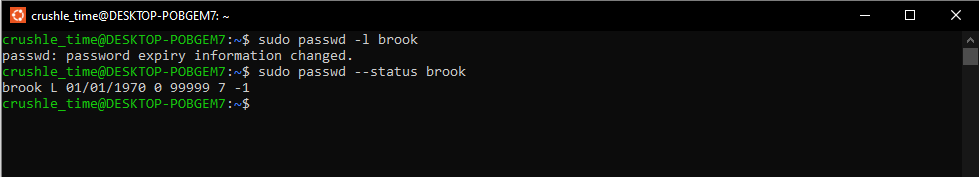
9. Create a new group

****

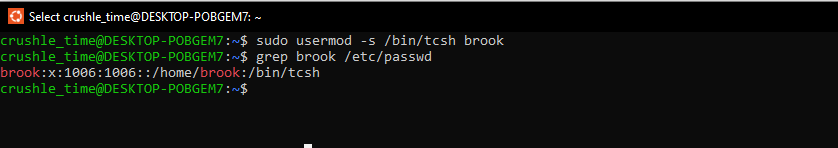
10. Assign the two new users to that group

****

11. Lock one of the user accounts

****

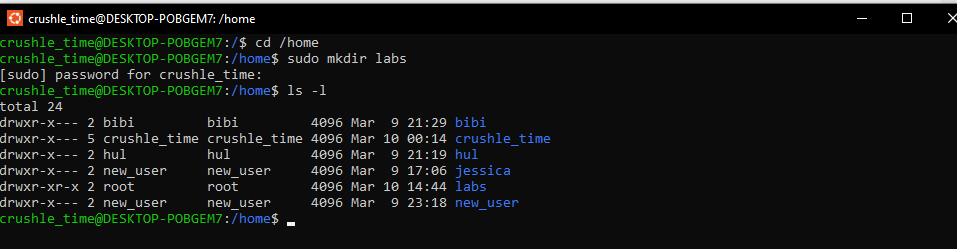
12. Change the shell of one user to tcsh



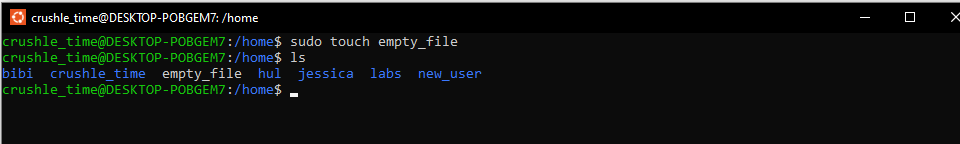
13. Make sure your home directory has “execute” access enabled for group and other.

****

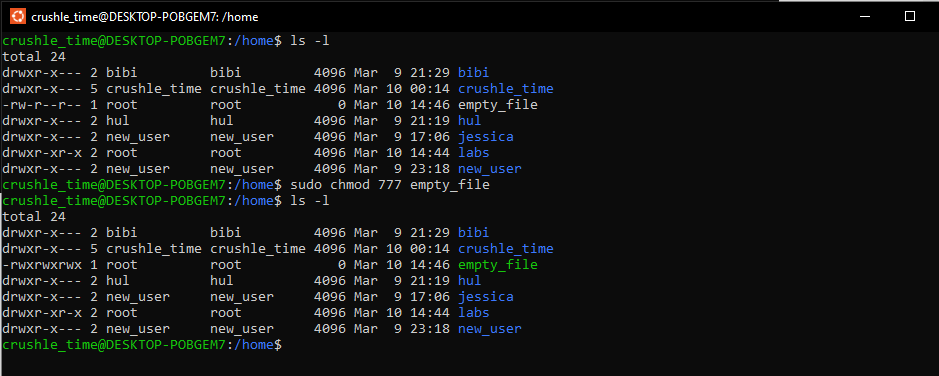
14. Change to your home directory, and create a directory called labs

****

15. Create an empty file in labs directory

****

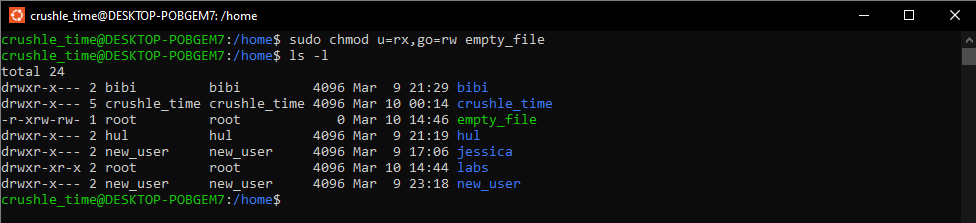
16. Change permissions of file to rwx-rwx-rwx

****

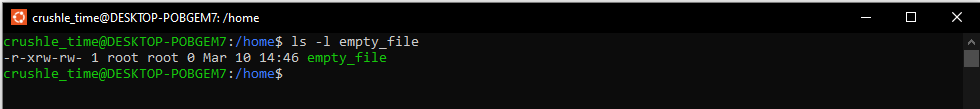
17. List the file. What color is the file?

**THE FILE IS GREEN**

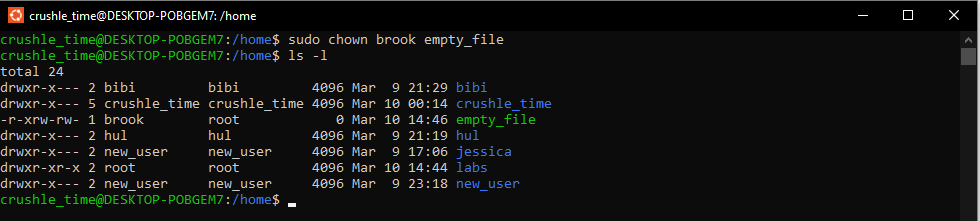
18. Change the permissions back to rx-rw-rw



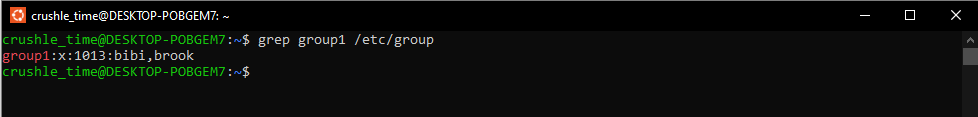
19. Check what owners does the file have.



20. Change the user ownership of the file to another user



21. Create a group called group1 and assign two users to the group

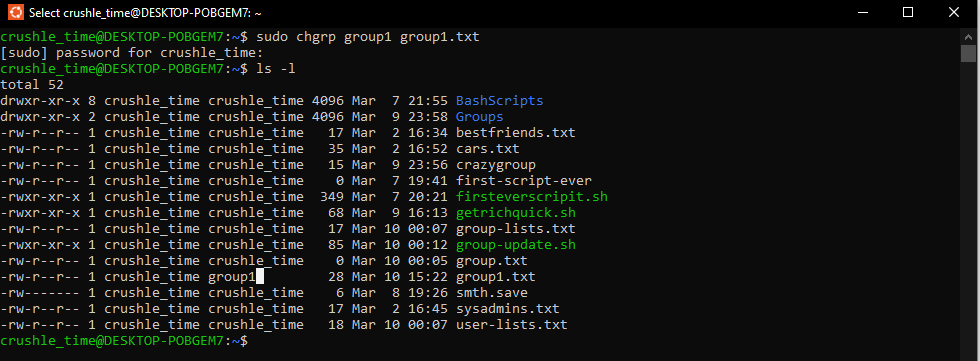
****

22. Create a file called group1.txt and redirect below input into the file: “This is our group test file”.

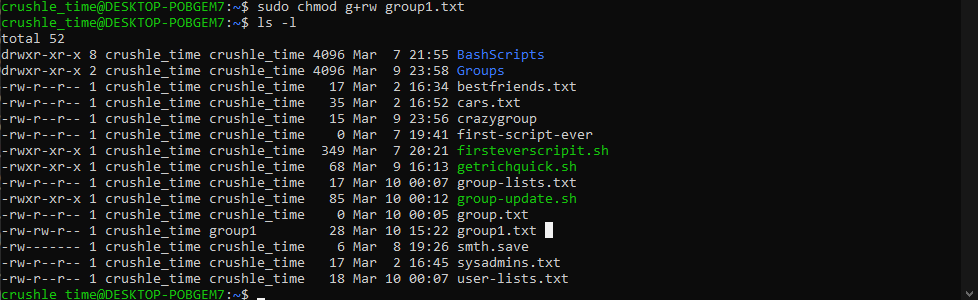
****

****

23. Change the group of the file to one of your users

****

24. Give members of the group group1 read/write access to this file?

****