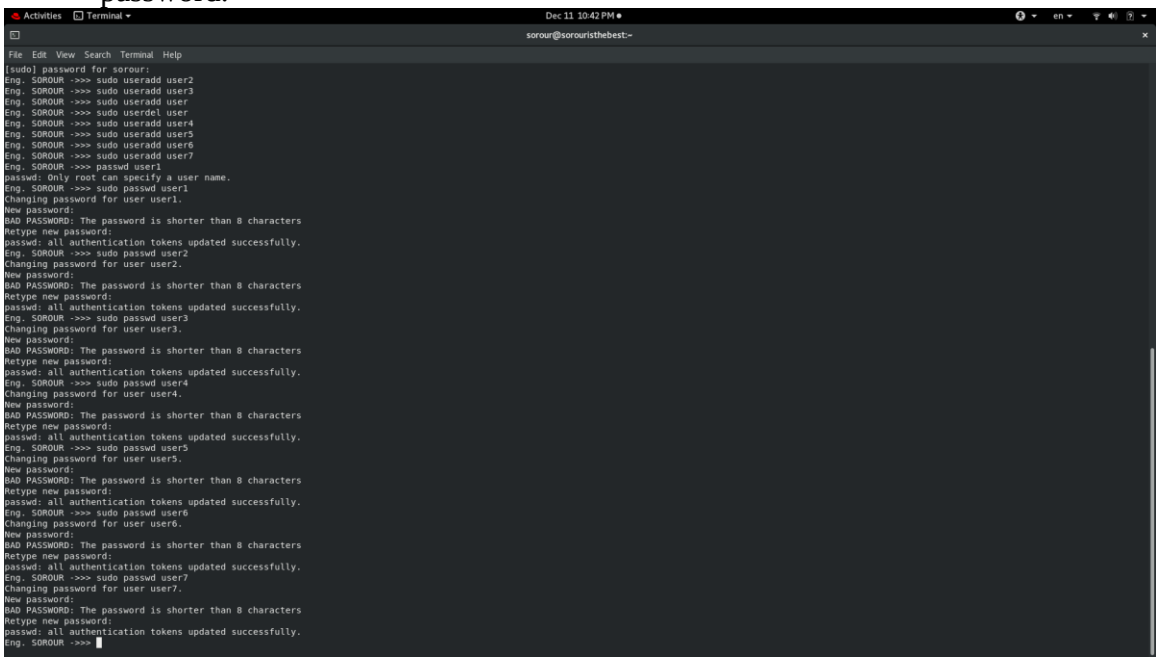
Lab 2

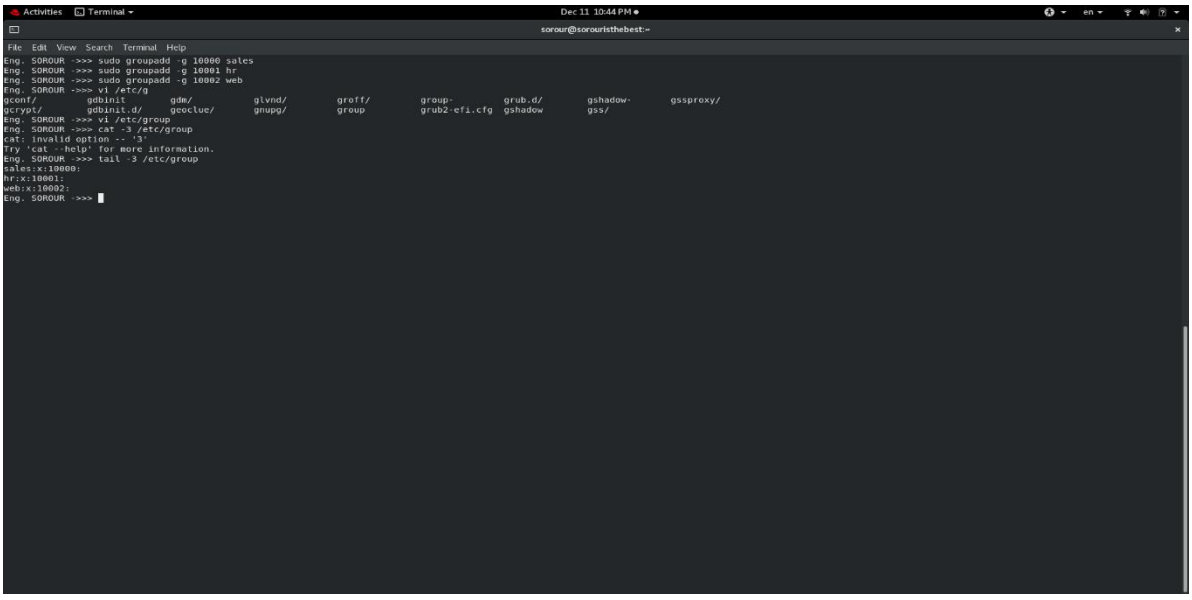
1. Using the useradd command, add accounts for the following users in your system: user1, user2, user3, user4, user5, user6 and user7. Remember to give each user a password.



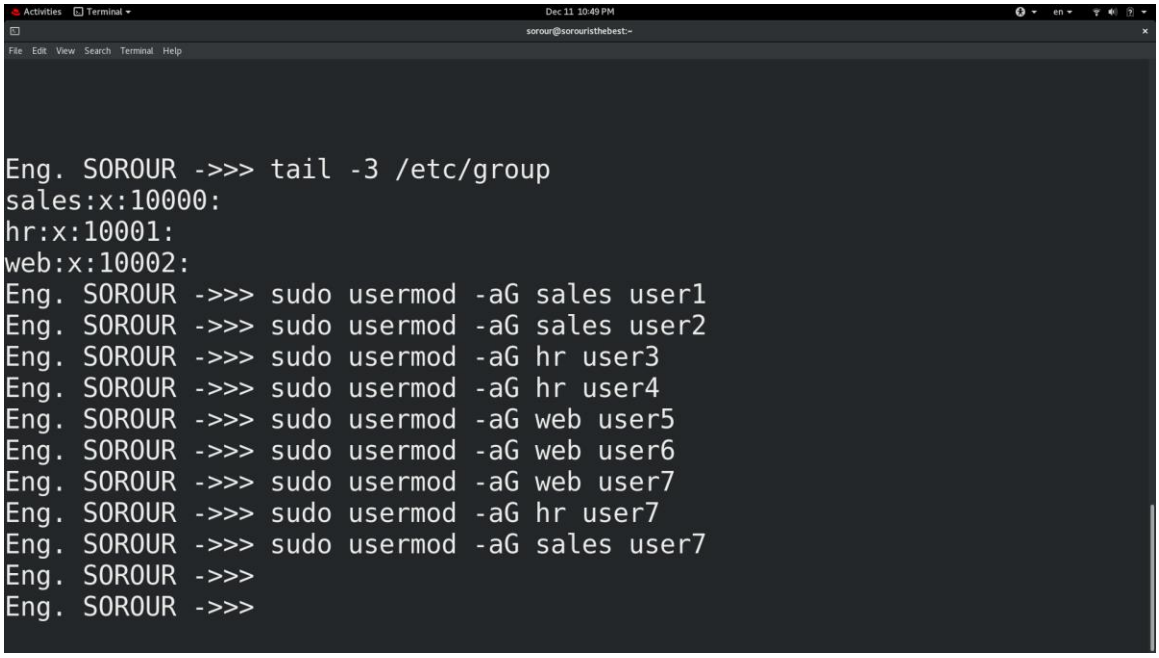
2. Using the groupadd command, add the following groups to your system.

Group	GID
sales	10000
hr	10001
web	10002

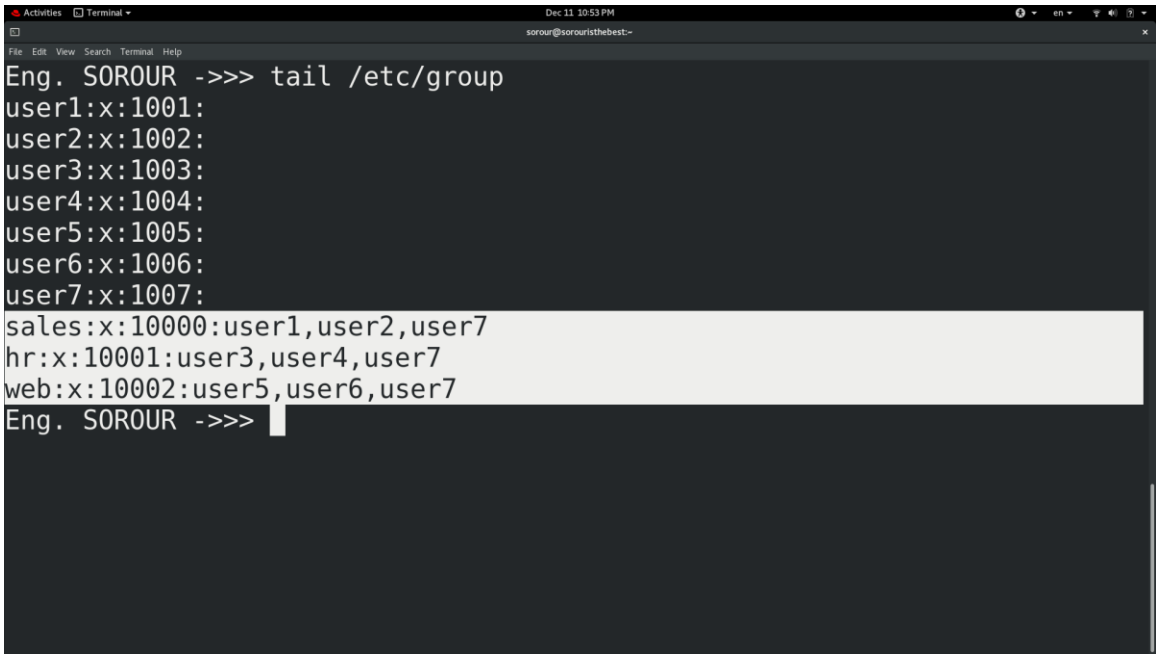
Why should you set GID in this manner instead of allowing the system to set the GID by default? → to make sure GID is known to me and is not confusing by UID



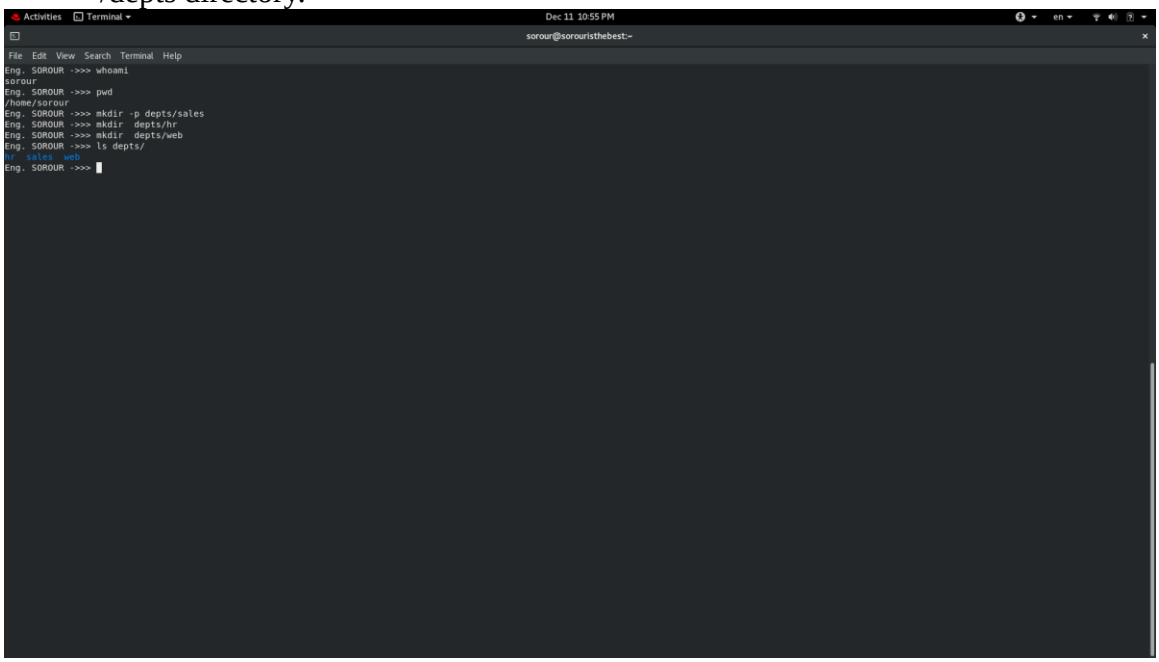
3. Using the usermod command to add user1 and user2 to the sales auxiliary group, user3 and user4 to the hr auxiliary group. User5 and user6 to web auxiliary group. And add user7 to all auxiliary groups



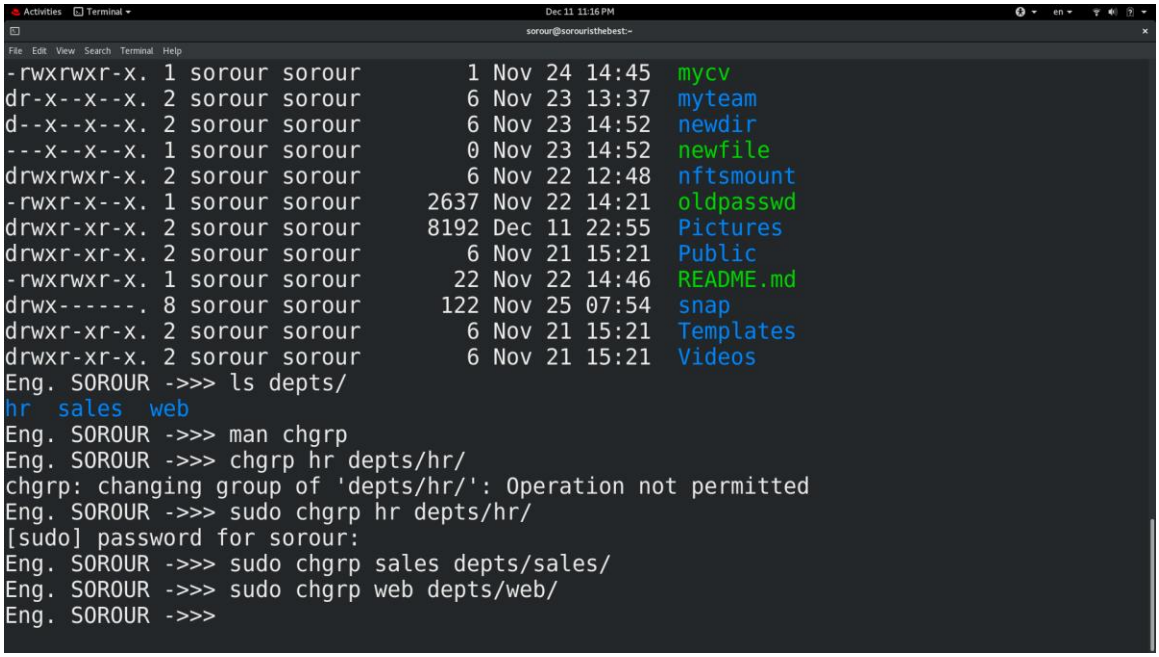
4. Login as each user and use id command to verify that they are in the appropriate groups. How else might you verify this information? → tail /*etc*/group



5. Create a directory called /depts with a sales, hr, and web directory within the /depts directory.



6. Using the chgrp command, set the group ownership of each directory to the group with the matching name

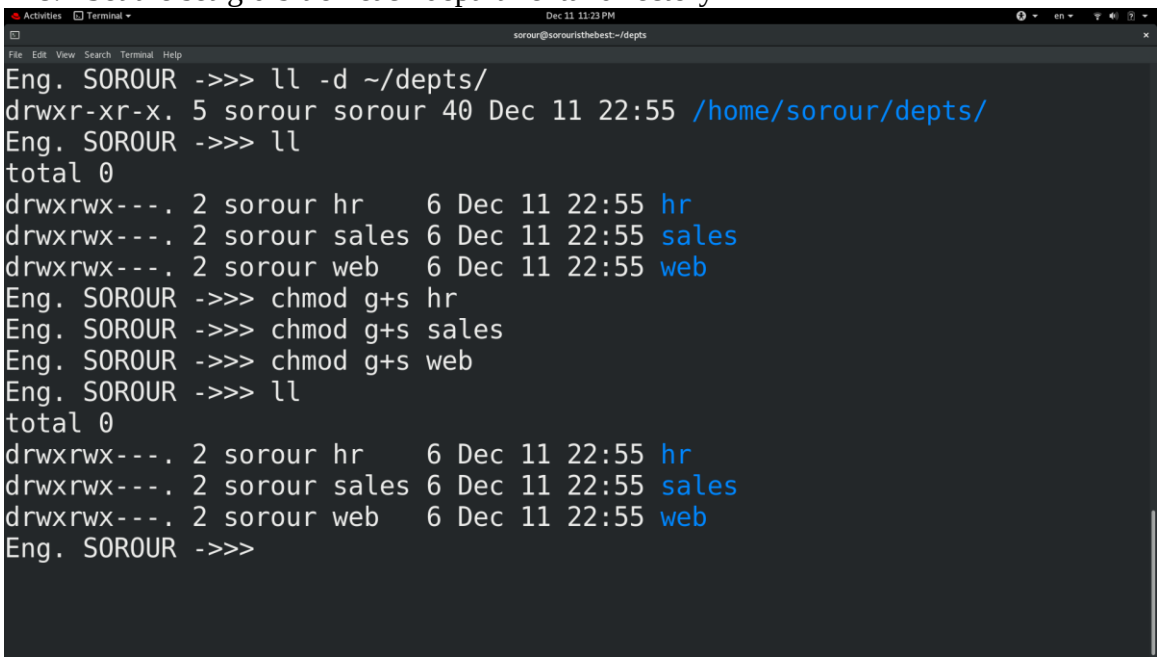


7. Set the permissions on the /depts directory to 755, and each subdirectory to 770

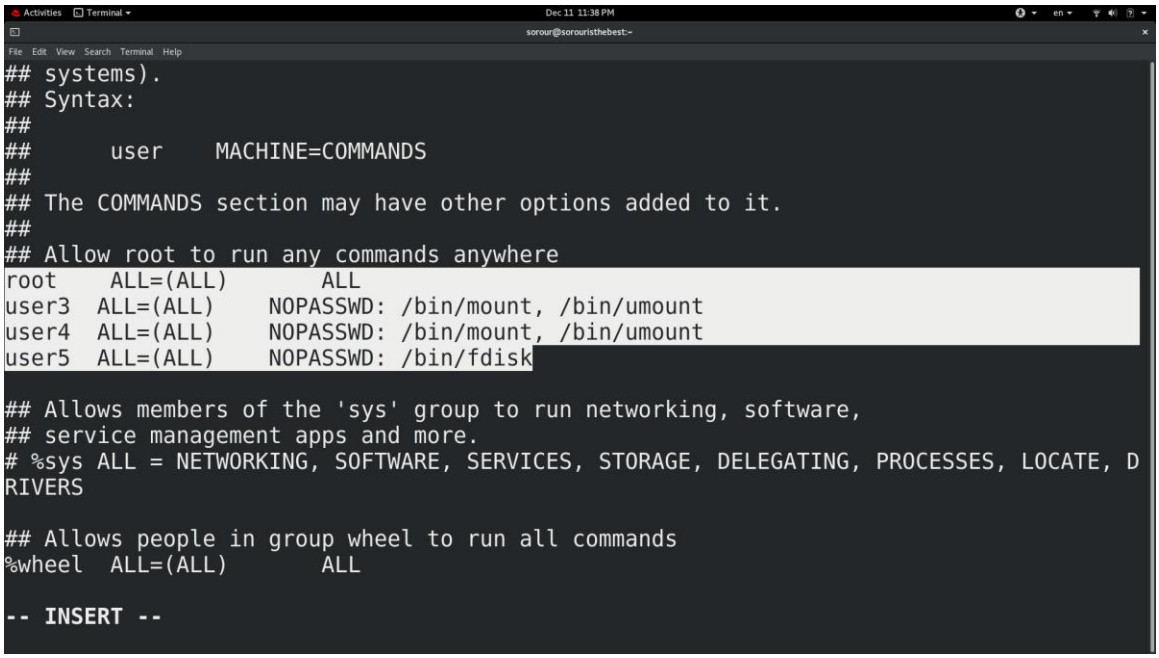
Eng. SOROUR ->>> chmod 755 depts
Eng. SOROUR ->>> chmod 770 depts/hr

Eng. SOROUR ->>> chmod 770 depts/sales
Eng. SOROUR ->>> chmod 770 depts/web

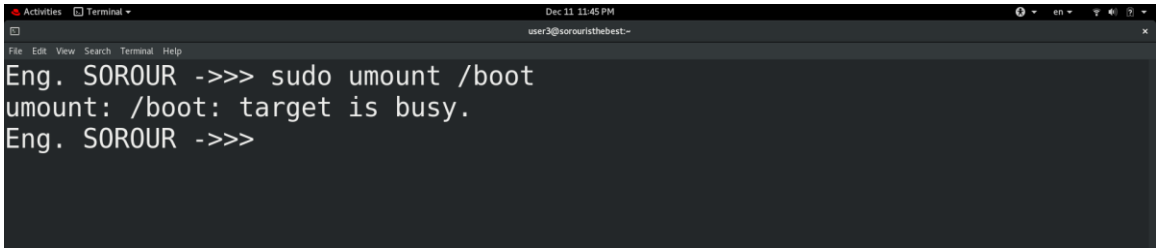
8. Set the set-gid bit on each departmental directory



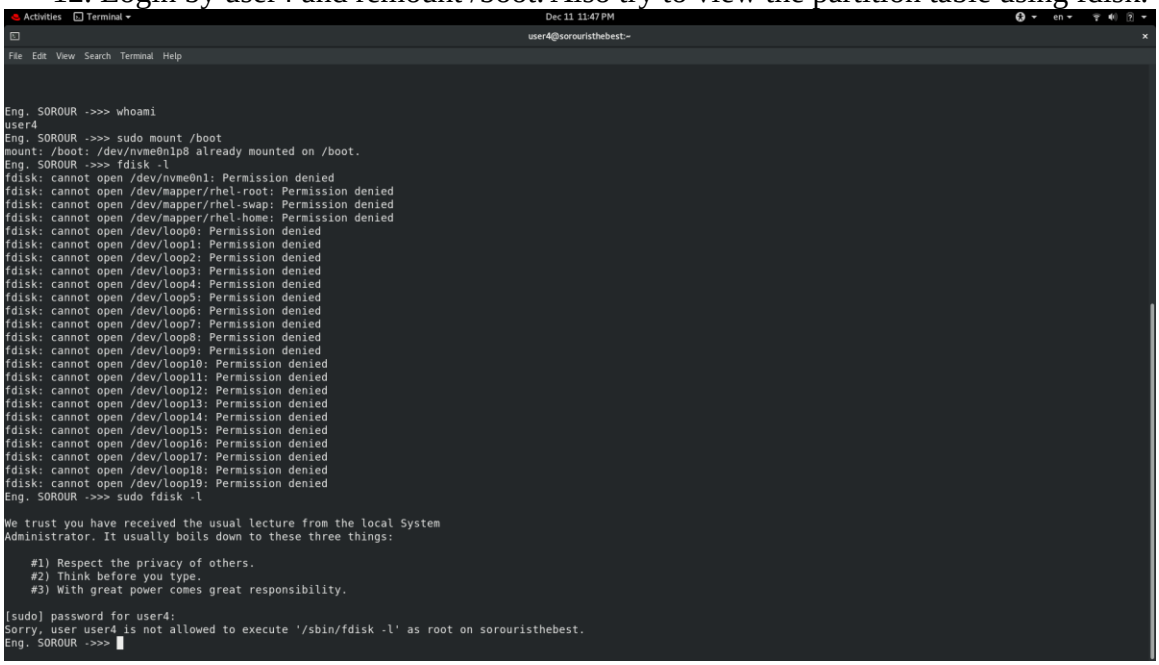
9. Use the su command to switch to the user2 account and attempt the following commands:
   touch /depts/sales/user2.txt
   touch /depts/hr/ user2.txt
   touch /depts/web/ user2.txt
   Eng. SOROUR ->>> touch /home/sorour/depts/sales/user2.txt
   Eng. SOROUR ->>> touch /home/sorour/depts/hr/user2.txt
   touch: cannot touch '/home/sorour/depts/hr/user2.txt': Permission denied
   Eng. SOROUR ->>> touch /home/sorour/depts/web/user2.txt
   touch: cannot touch '/home/sorour/depts/web/user2.txt': Permission denied
   Which of these commands succeeded and which failed? What is the group ownership of the files that were created? → only touch /home/sorour/depts/sales/user2.txt because user2 have the same group as sales dir.
   → Group ownership of the files that were created is sales because we set SGID which makes child inhernebt parents group
10. Configure sudoers file to allow user3 and user4 to use /bin/mount and /bin/umount commands, while allowing user5 only to use fdisk command.



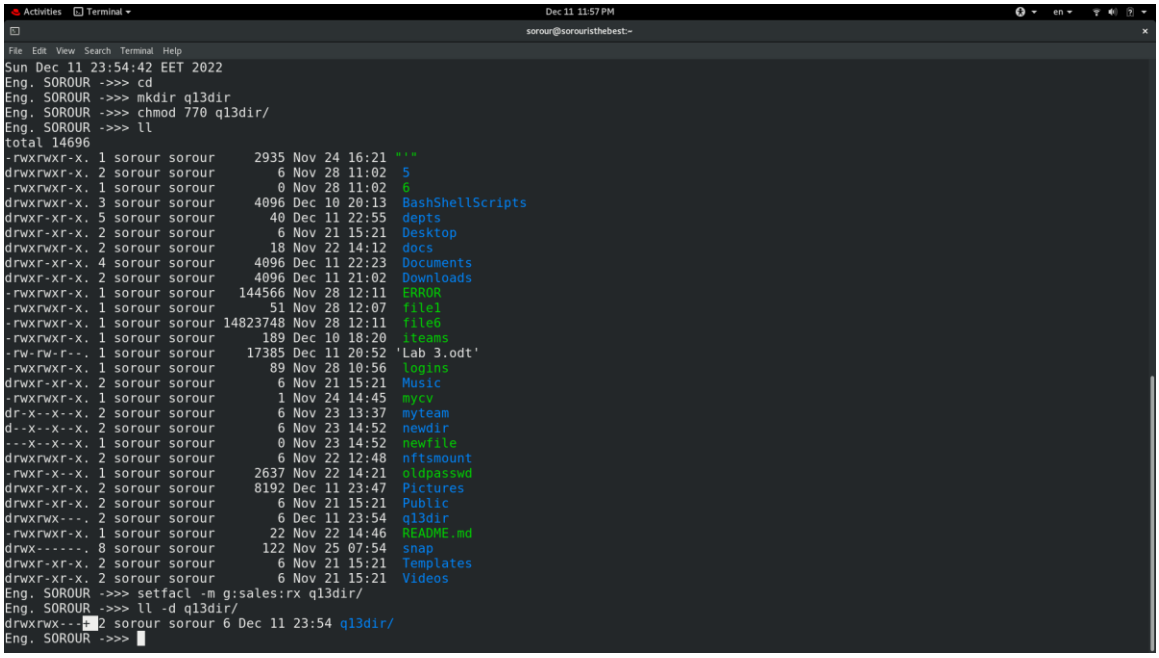
11. Login by user3 and try to unmount /boot. → done but target is busy



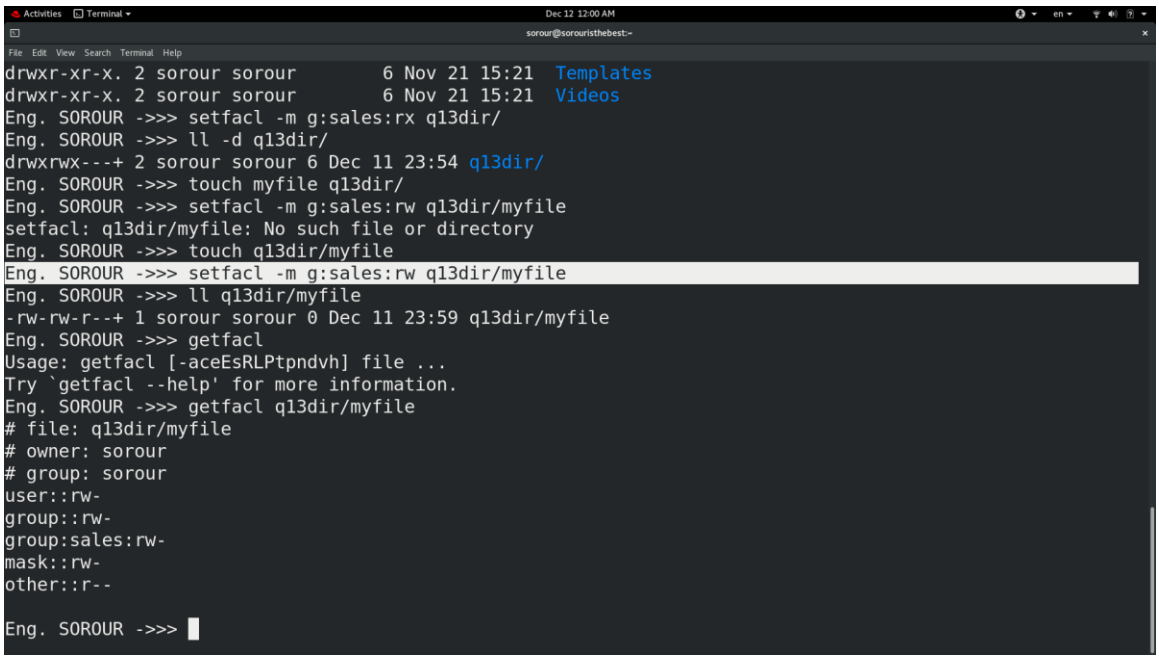
12. Login by user4 and remount /boot. Also try to view the partition table using fdisk.



13. Create a directory with permissions rwxrwx---, grant a second group (sales) r-x permissions

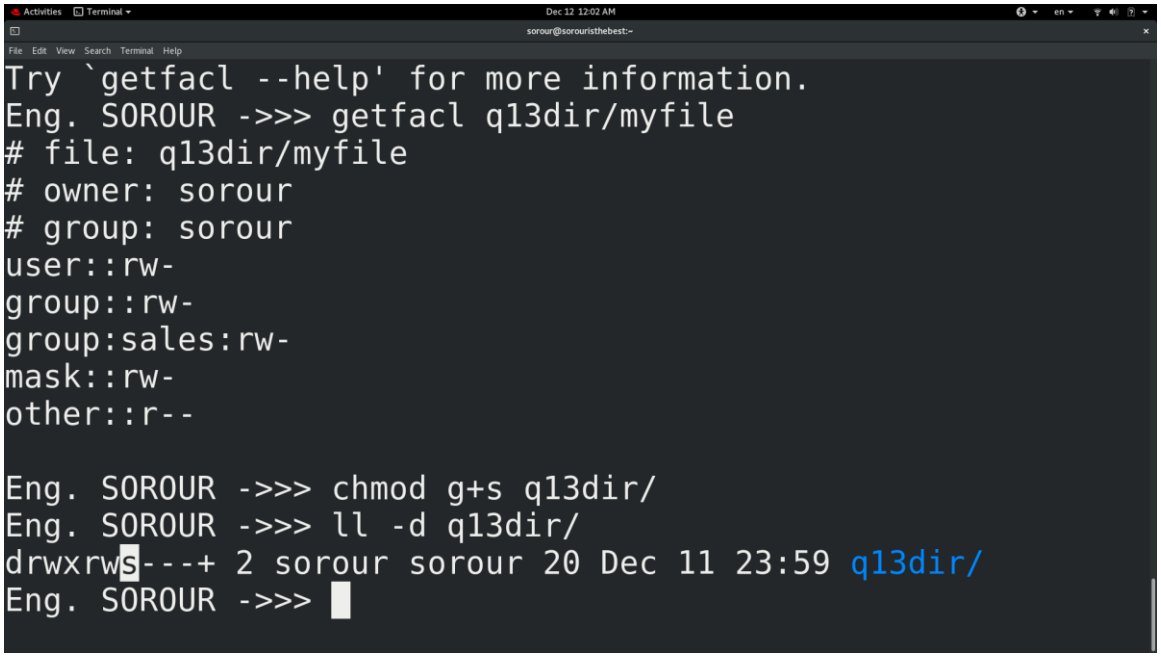


14. create a file on that directory and grant read and write to a second group (sales)



15. set the the owning group as the owning group of any newly created file in that directory.

Eng. SOROUR ->>> chmod g+s q13dir/



16. Grand your colleagues a collective directory called /opt/research, where they can store generated research results. Only members of group profs and grads should be able to create new files in the directory, and new file should have the following properties:

    setfacl -m g:profs:wx ~/opt/research/
    setfacl -m g:grads:wx ~/opt/research/

    - the directory should be owned by root
      sudo chown root:grads ~/opt/research/
    - new files should be group owned by group grads
      sudo chmod g+s ~/opt/research/
    - group profs should automatically have read/write access to new files
      done by default
    - group interns should automatically have read only access to new files
      sudo setfacl -m d:g:interns:r ~/opt/research/
    - other users should not be able to access the directory and its contents at all.
      sudo setfacl -m o:--- ~/opt/research/