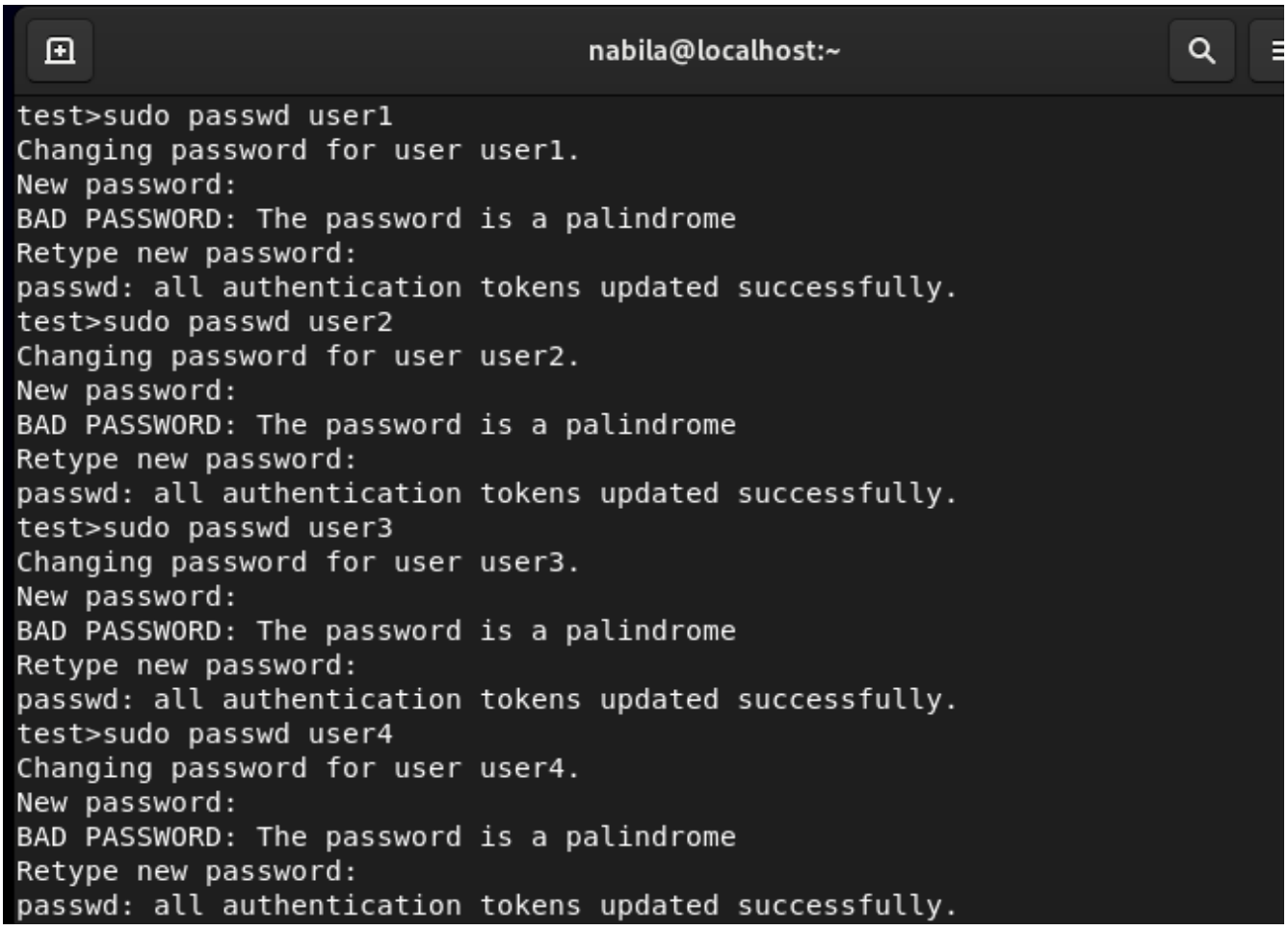
Lab 3
1. Using the useradd command, add accounts for the following users in your system:
user1, user2, user3, user4, user5, user6 and user7. Remember to give each user a
password.

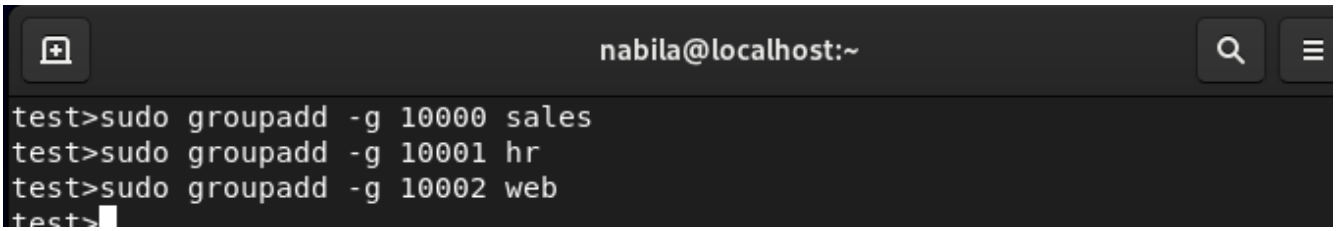
```
test>sudo useradd user1
[sudo] password for nabila:
test>sudo useradd user2
test>sudo useradd user3
test>sudo useradd user4
test>sudo useradd user5
test>sudo useradd user6
test>sudo useradd user7
```



```
test>sudo passwd user5
Changing password for user user5.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
test>sudo passwd user6
Changing password for user user6.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
test>sudo passwd user7
Changing password for user user7.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
test>
```

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

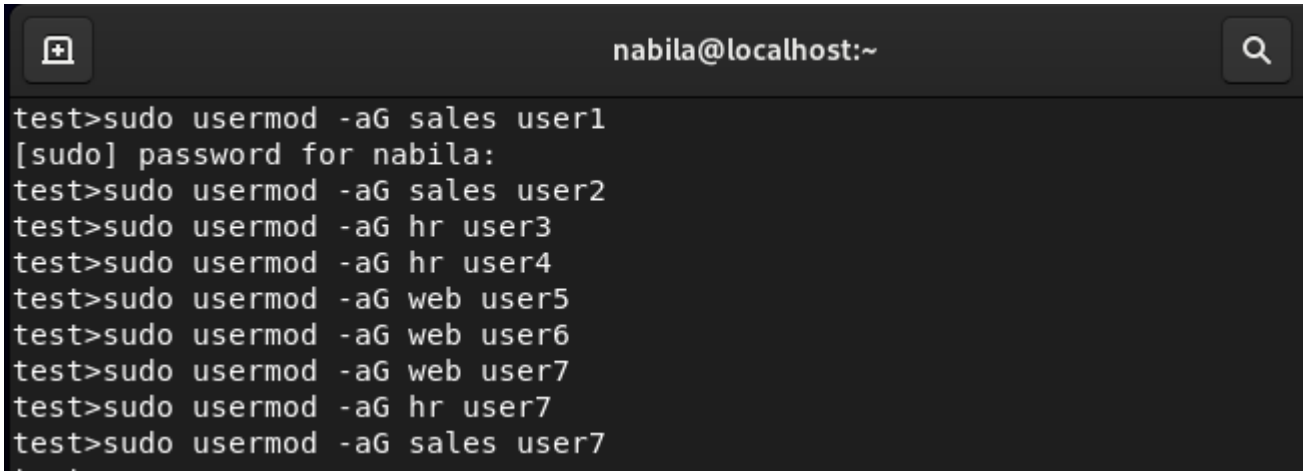
Group	GID
sales	10000
hr	10001
web	10002



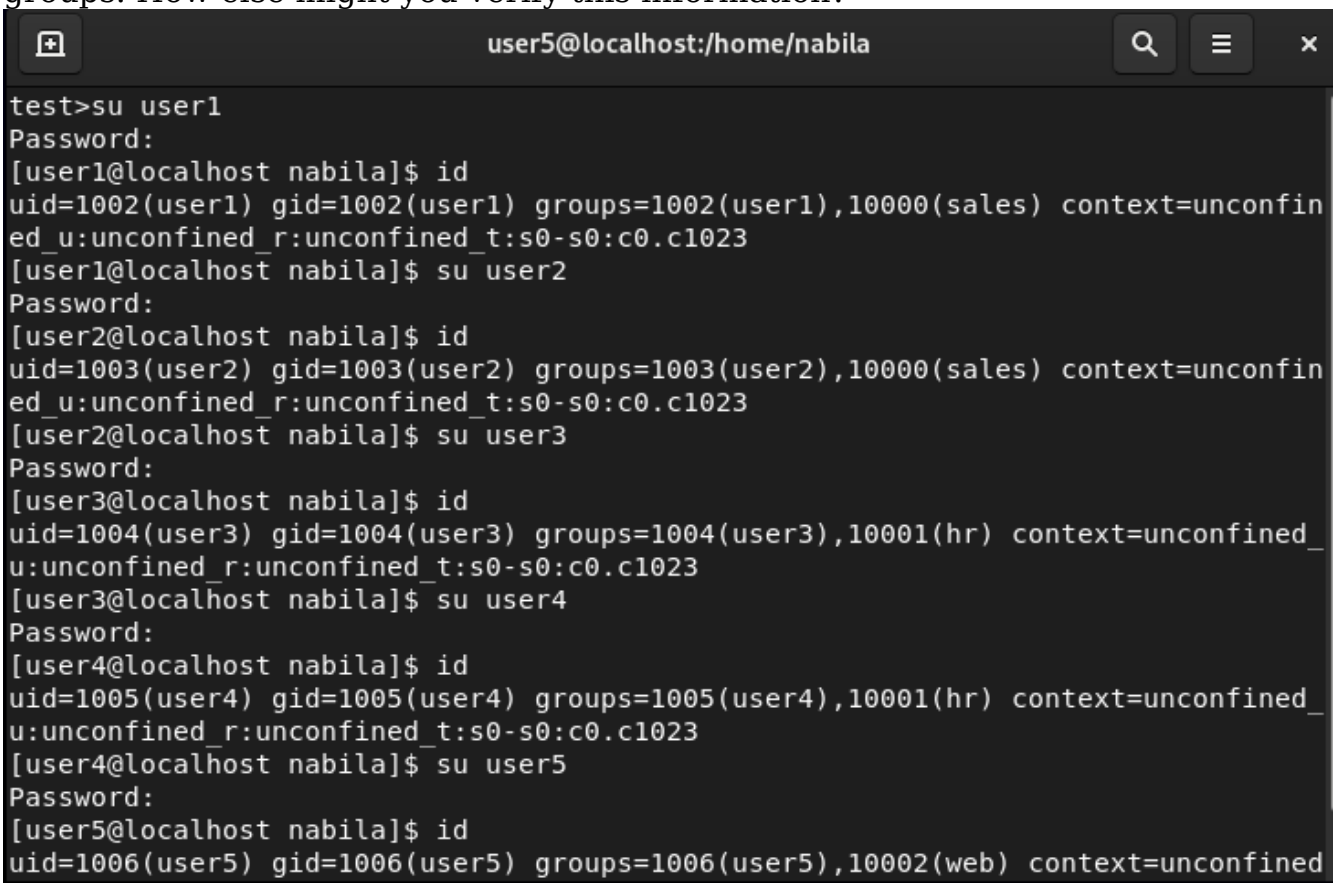
Why should you set GID in this manner instead of allowing the system to set the GID
by default?

Ans:If I didn’t give group id it will give it same ad user id who create group.

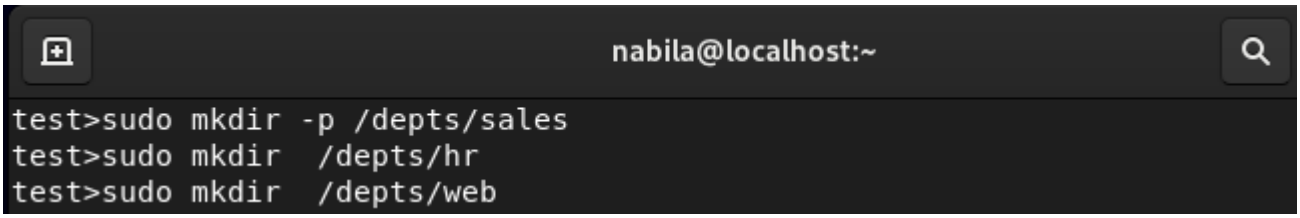
3. Using the usermod command to add user1 and user2 to the sales auxiliary group,
user3 and user4 to the hr auxiliary group. User5 and user6 to web auxiliary group.
And add user7 to all auxiliary groups



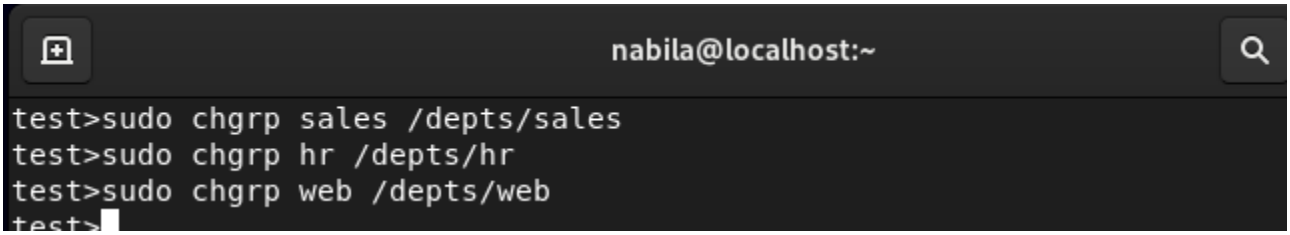
4. Login as each user and use id command to verify that they are in the appropriate
groups. How else might you verify this information?



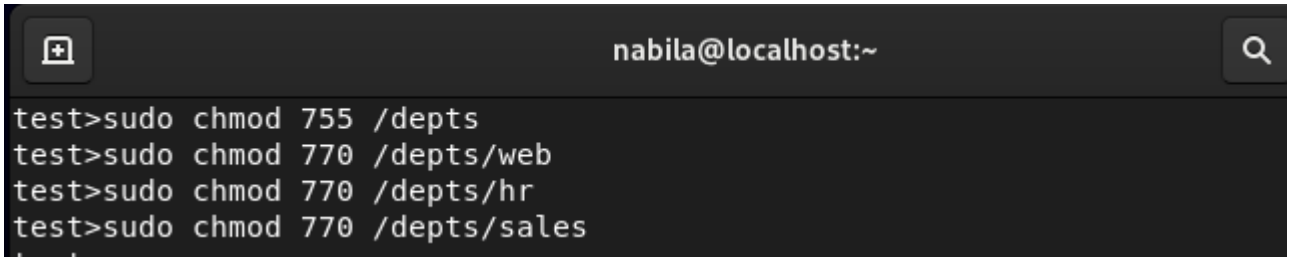
5. Create a directory called /depts with a sales, hr, and web directory within the /depts directory.



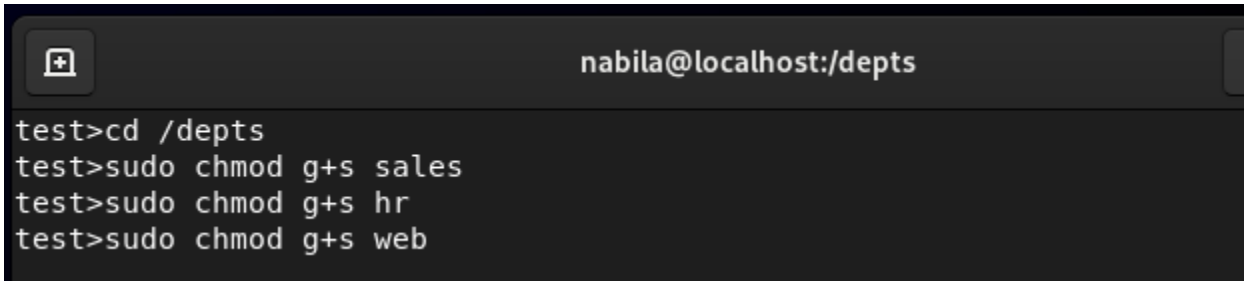
6. Using the chgrp command, set the group ownership of each directory to the group
with the matching name



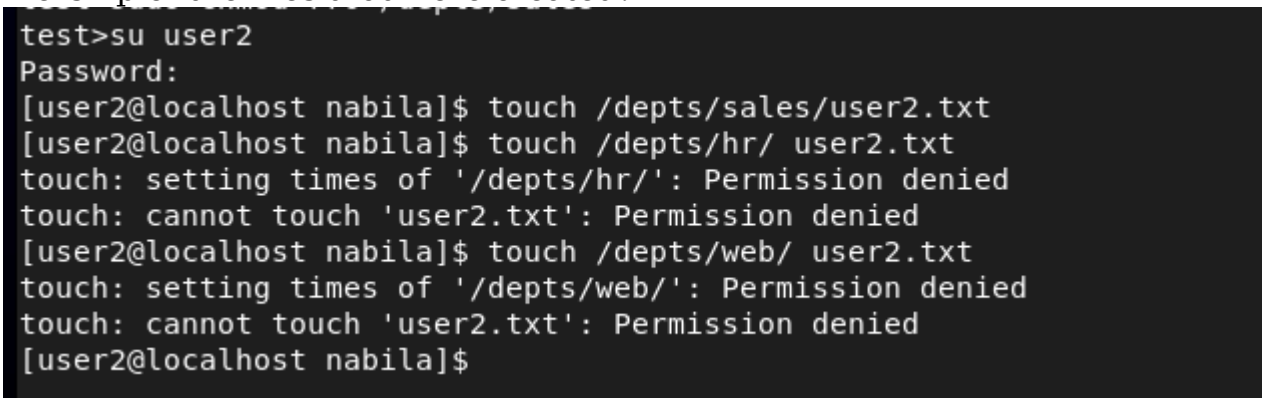
7. Set the permissions on the /depts directory to 755, and each subdirectory to 770



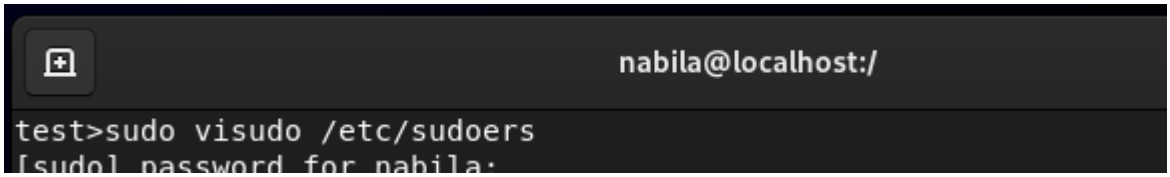
8. Set the set-gid bit on each departmental directory

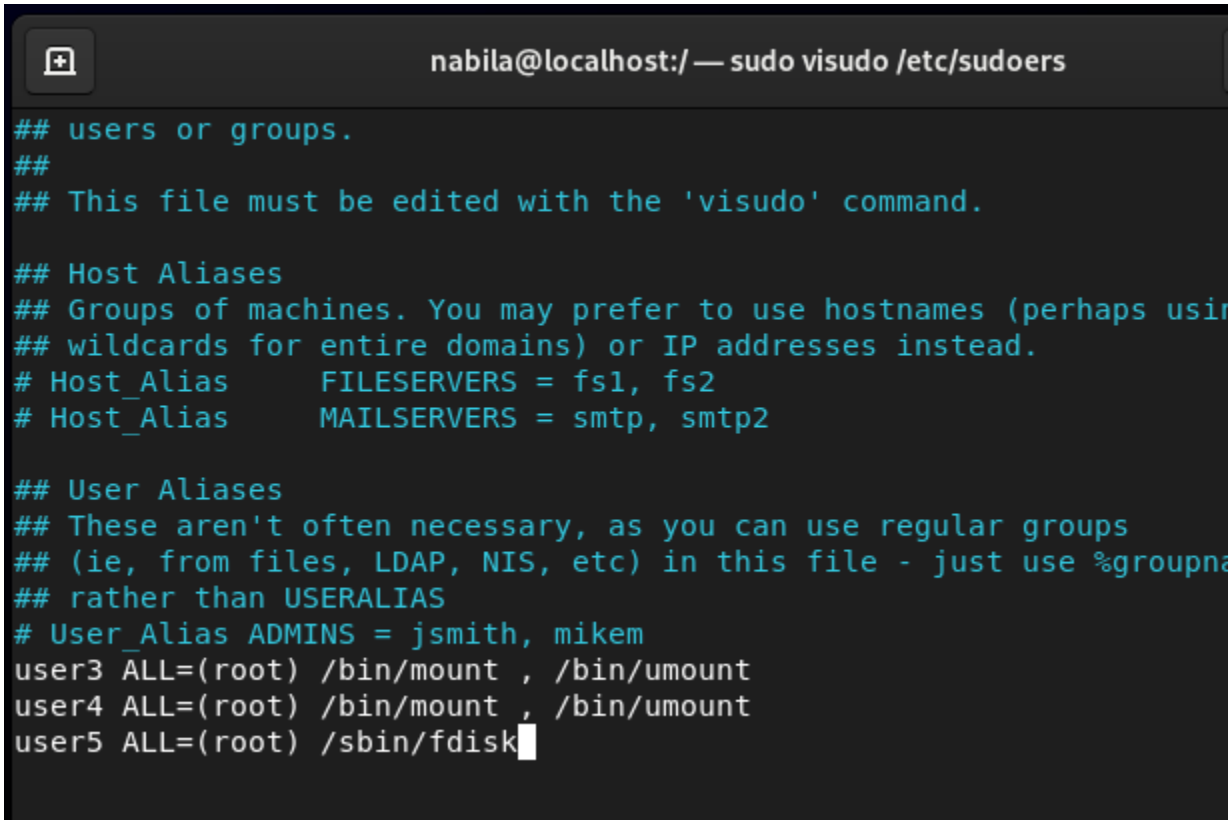


9. Use the su command to switch to the user2 account and attempt the following commands:
touch /depts/sales/user2.txt
touch /depts/hr/ user2.txt
touch /depts/web/ user2.txt
Which of these commands succeeded and which failed? What is the group ownership of the files that were created?



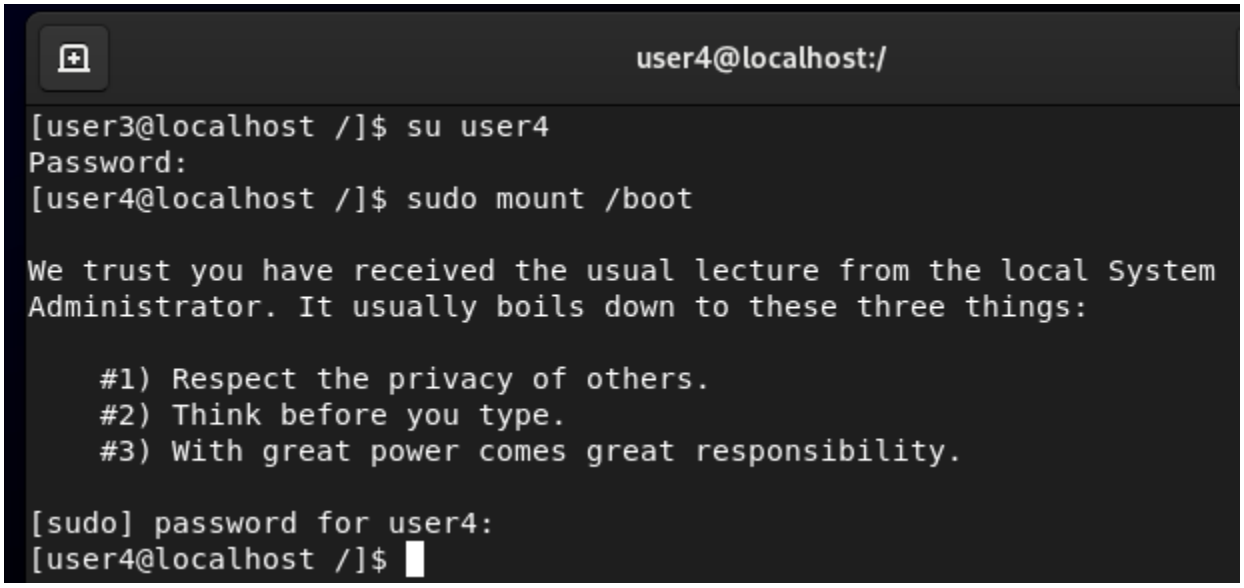
10. Configure sudoers file to allow user3 and user4 to use /bin/mount and /bin/umount commands, while allowing user5 only to use fdisk command.
user3 ALL=(root) /bin/mount , /bin/unmount

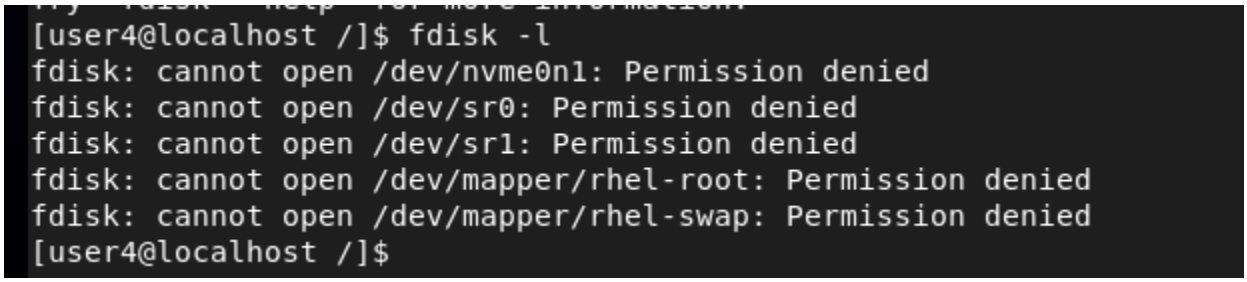




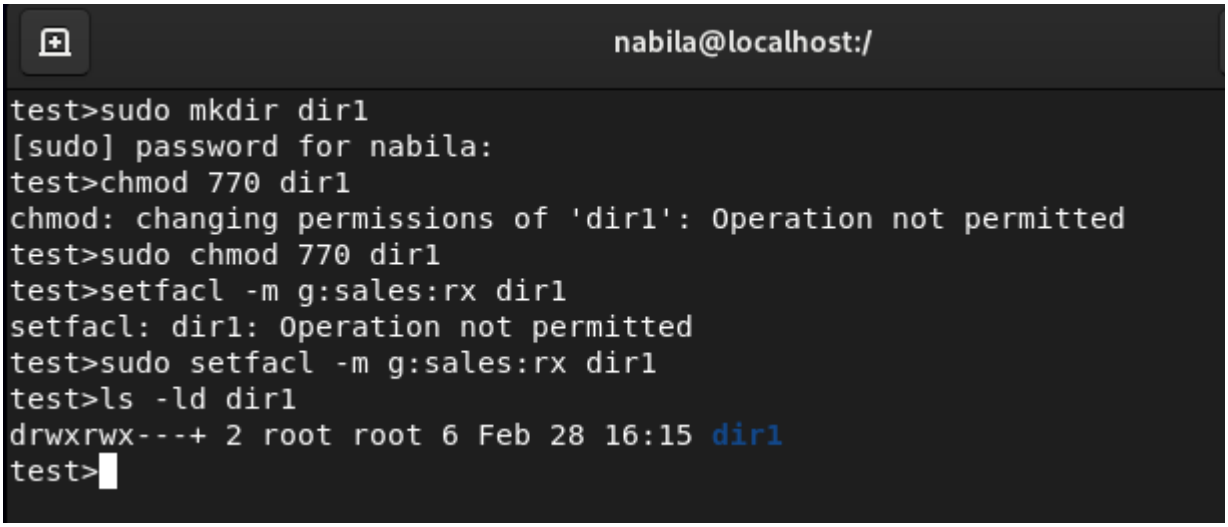
11. Login by user3 and try to unmount /boot.

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

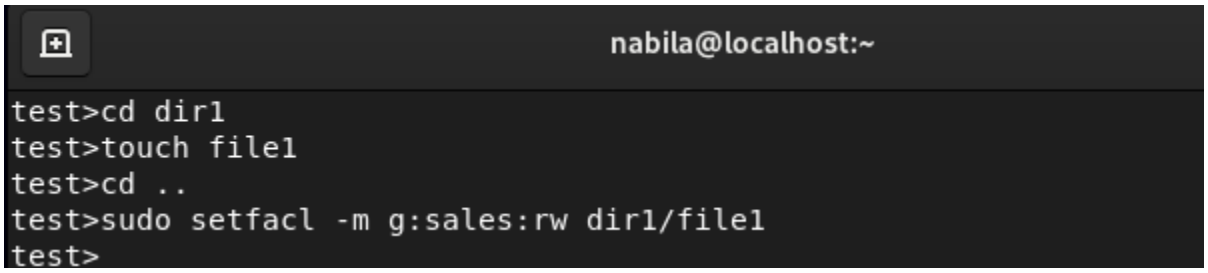




13. Create a directory with permissions rwxrwx---, grant a second group (sales) r-x
permissions



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.