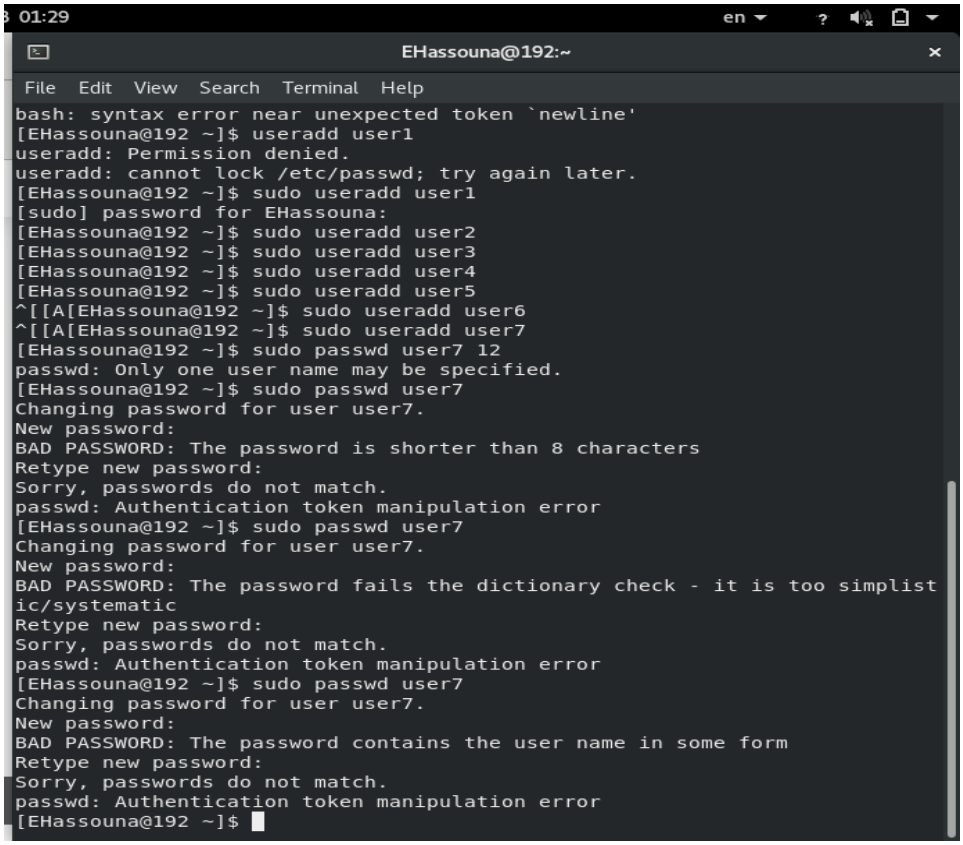
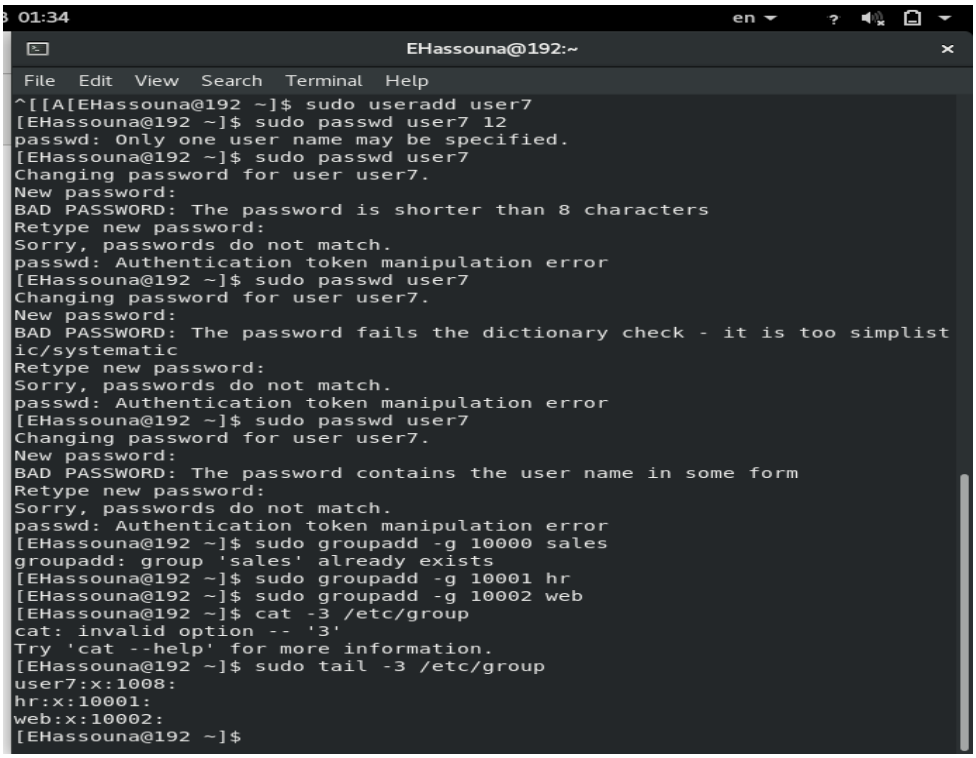
1. Using the useradd command, add accounts for the following users in your system: user1, user2, user3, user4, user5, user6 and user7. Remember to give each user a password.



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

Group GID sales 10000 hr 10001 web 10002



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

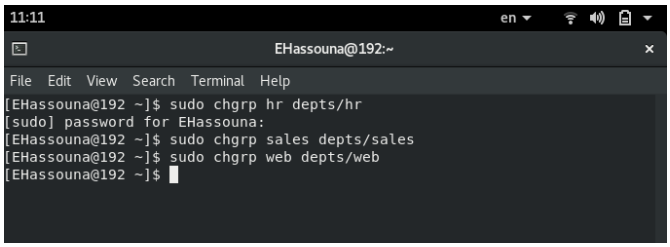
```
[EHassouna@192 ~]$ sudo groupadd -g 10000 sales
groupadd: group 'sales' already exists
[EHassouna@192 ~]$ sudo groupadd -g 10001 hr
[EHassouna@192 ~]$ sudo groupadd -g 10002 web
[EHassouna@192 ~]$ cat -3 /etc/group
cat: invalid option -- '3'
Try 'cat --help' for more information.
[EHassouna@192 ~]$ sudo tail -3 /etc/group
user7:x:1008:
hr:x:10001:
web:x:10002:
[EHassouna@192 ~]$
```

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?

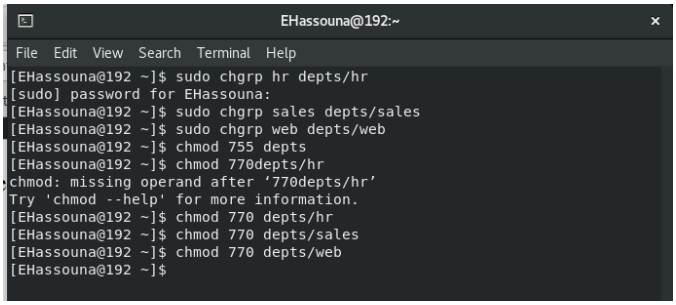
5. Create a directory called /depts with a sales, hr, and web directory within the /depts directory.

```
[EHassouna@192 ~]$ whoami
EHassouna
[EHassouna@192 ~]$ pwd
/home/EHassouna
[EHassouna@192 ~]$ mkdir -p depts/sales
[EHassouna@192 ~]$ mkdir -p depts/hr
[EHassouna@192 ~]$ mkdir -p depts/web
[EHassouna@192 ~]$ ls depts/
hr  sales  web
[EHassouna@192 ~]$
```

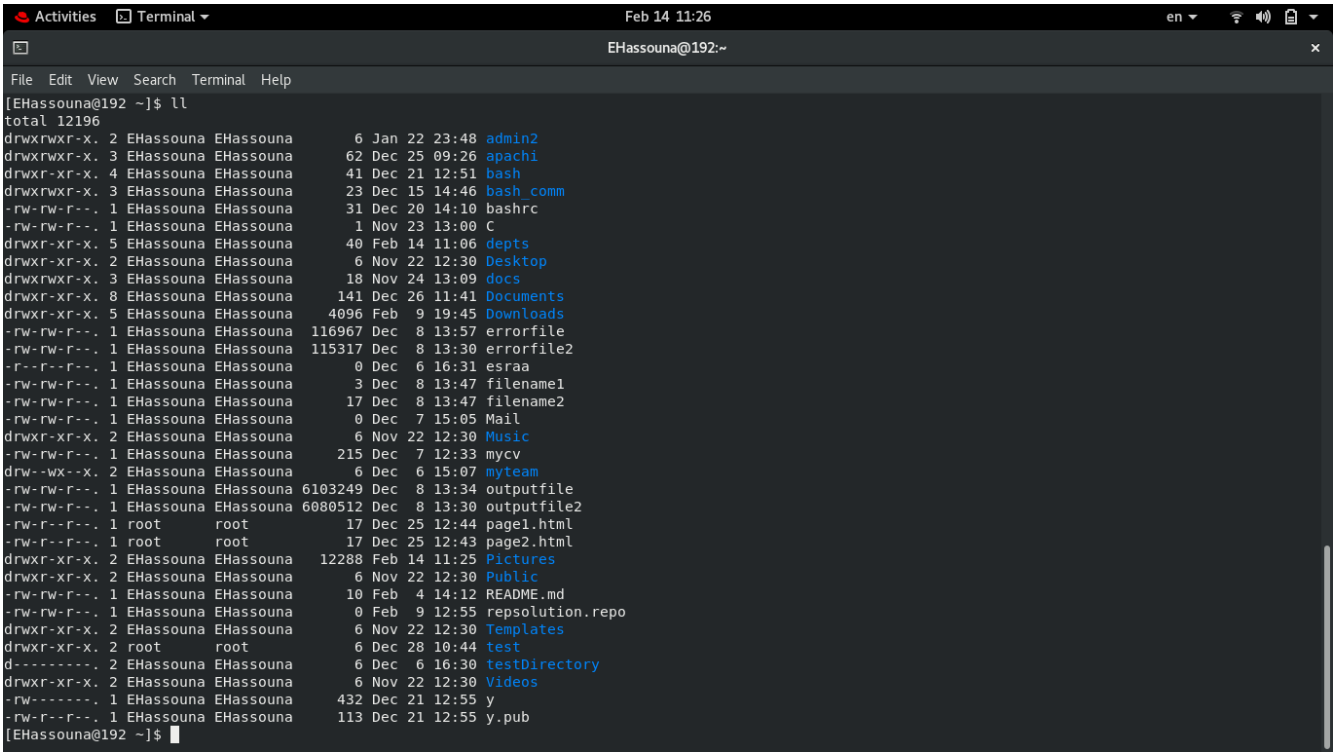
6. Using the chgrp command, set the group ownership of each directory to the group with the matching name



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

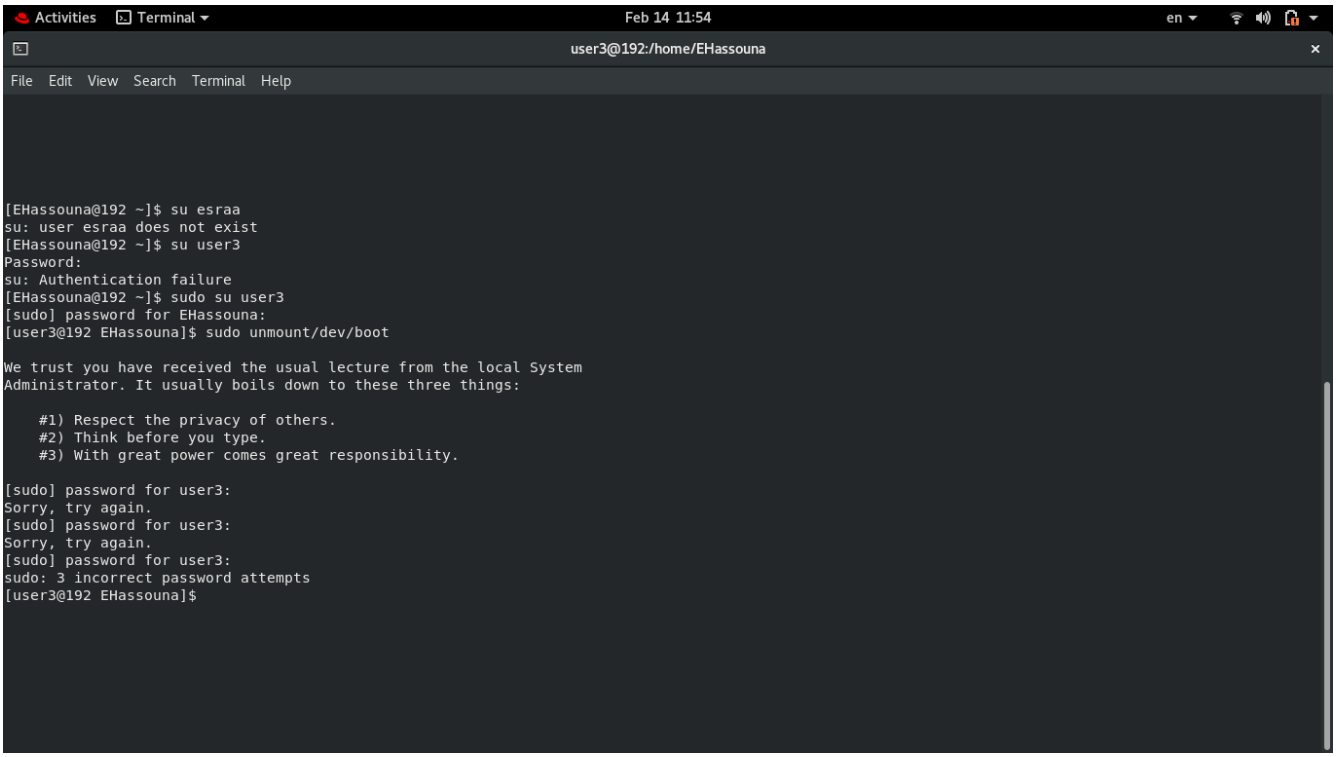


8. Set the set-gid bit on each departmental directory

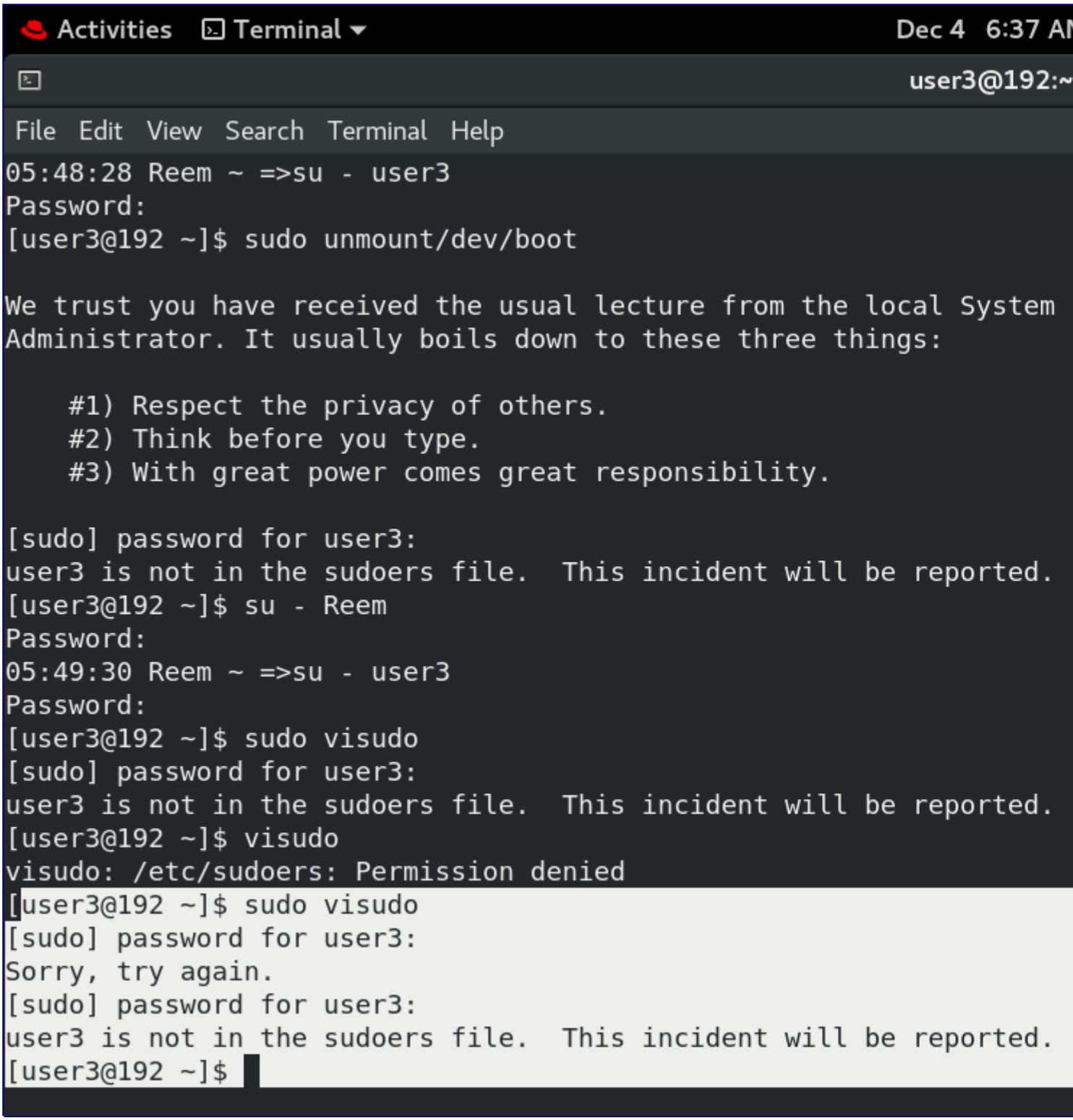


9. Use the su command to switch to the user2 account and attempt the following commands:

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.


Activities
Terminal
Dec 4 6:37 AM
user3@192:~
File Edit View Search Terminal Help
05:48:28 Reem ~ =>su - user3
Password:
[user3@192 ~]$ sudo unmount/dev/boot
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
[sudo] password for user3:
user3 is not in the sudoers file. This incident will be reported.
[user3@192 ~]$ su - Reem
Password:
05:49:30 Reem ~ =>su - user3
Password:
[user3@192 ~]$ sudo visudo
[sudo] password for user3:
user3 is not in the sudoers file. This incident will be reported.
[user3@192 ~]$ visudo
visudo: /etc/sudoers: Permission denied
[user3@192 ~]$ sudo visudo
[sudo] password for user3:
Sorry, try again.
[sudo] password for user3:
user3 is not in the sudoers file. This incident will be reported.
[user3@192 ~]$

11. Ans:- sudo visudo user3 ALL=(ALL) !ALL, /bin/mount, /bin/umount user4 ALL=(ALL) !ALL, /bin/mount, /bin/umount user5 ALL=(ALL) !ALL, /sbin/fdisk
12. Login by user3 and try to unmount /boot. Ans:- sudo umount /dev/boot
13. Login by user4 and remount /boot. Also try to view the partition table using fdisk. Ans:- fdisk /dev/boot
14. Create a directory with permissions rwxrwx---, grant a second group (sales) r-x permissions mkdir dir1 chmod 770 dir1 setfacl -m g:sales:rx ~/dir1
15. create a file on that directory and grant read and write to a second group (sales)
16. set the the owning group as the owning group of any newly created file in that directory.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: • the directory should be owned by root • new files should be group owned by group grads • group profs should automatically have read/write access to new files • group interns should automatically have read only access to new files • other users should not be able to access the directory and its contents at all.

• Bonus Your boss thinks it’s a great idea to have one central logging server. Satisfy his requirements 💍 Hint: Set up rsyslogd on the "logging server" machine to accept logging messages from other machines. On the your "workstation", set up rsyslogd to send messages to the "logging server Test the new setup by using the logger command on the "workstation" to generate a log message Does the message appear in the "logging server's" /var/log/messages file? Why does this message also appear in the "workstation's" /var/log/messages file? How could you have the message only appear in the "logging server's" files?