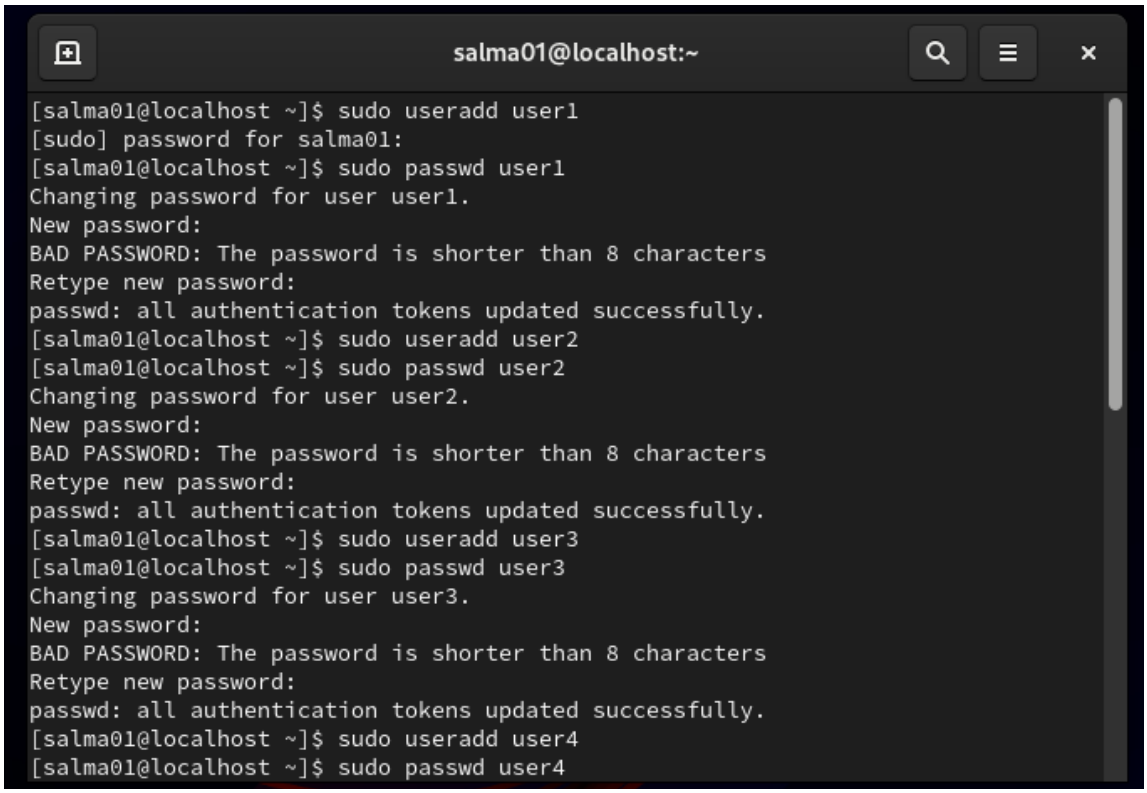
Lab

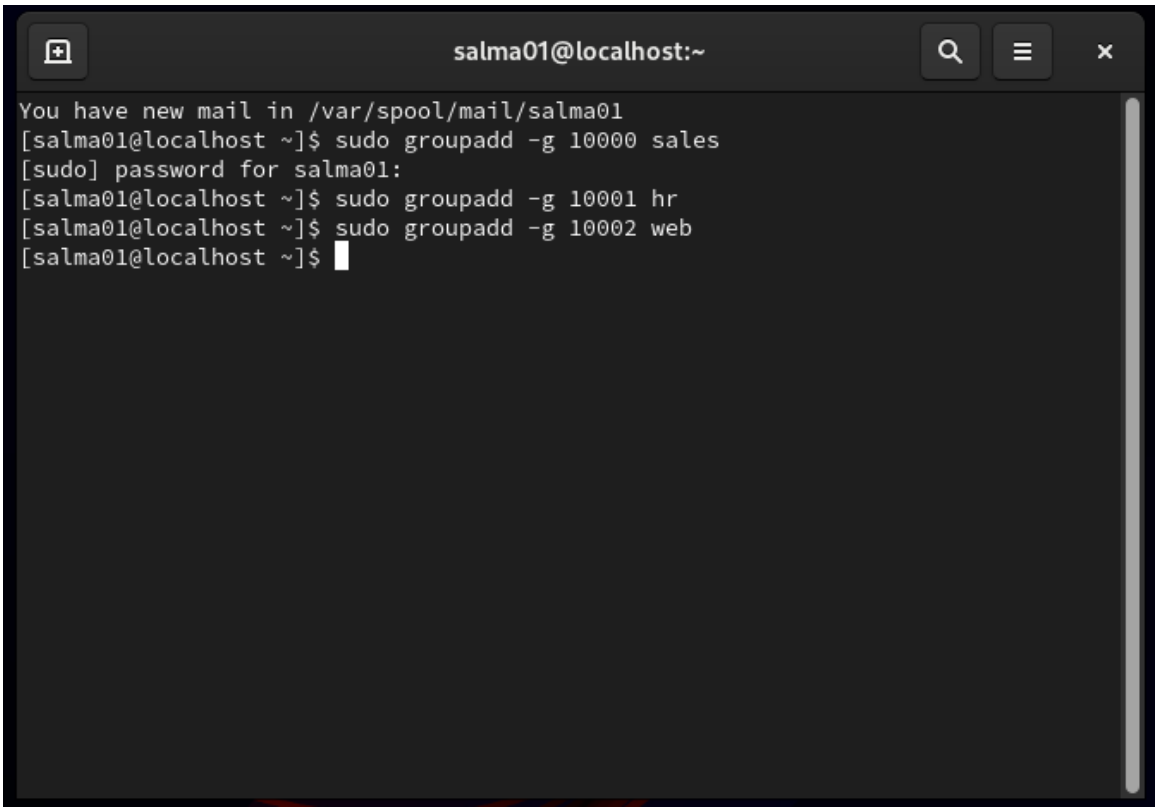
1. Using the useradd command, add accounts for the following users in your system: user1, user2, user3, user4, user5, user6 and user7. Remember to give each user a password.



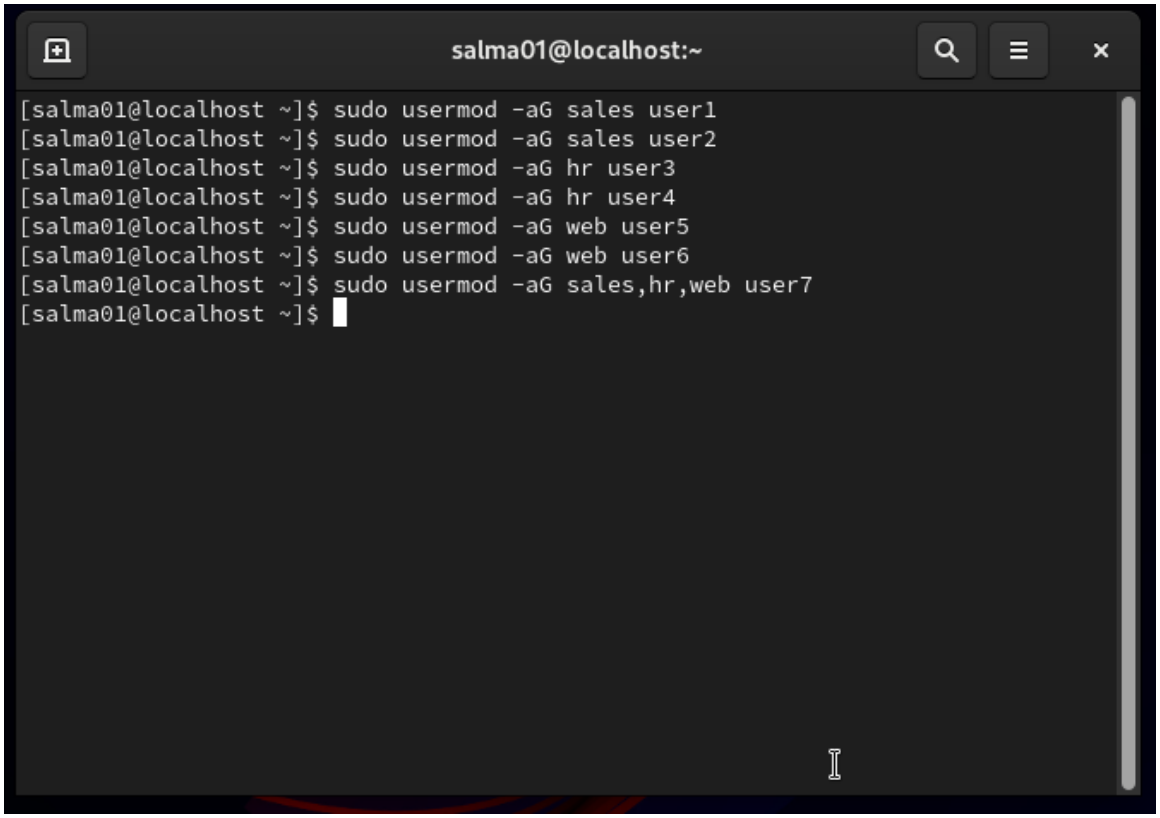
2. Using the groupadd command, add the following groups to your system.

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?
it allows you to have control over the numeric group identifier assigned to each group.



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



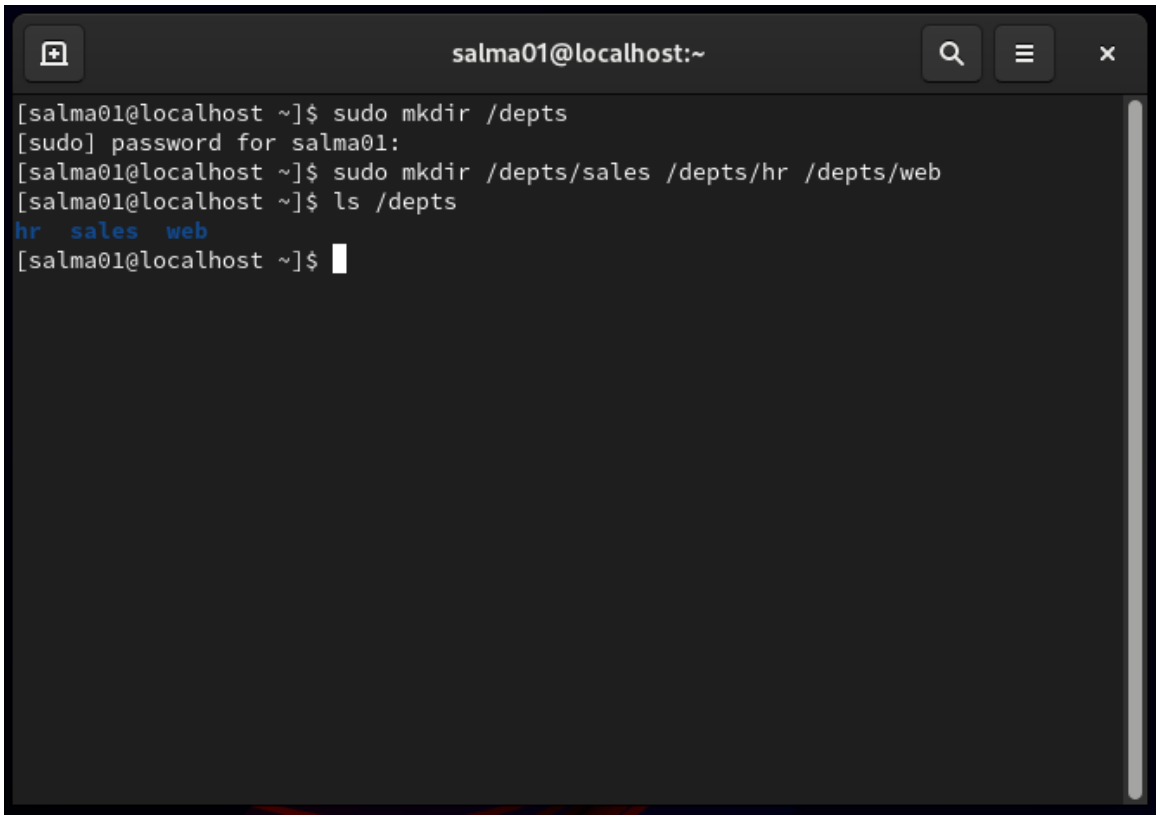
4. Login as each user and use id command to verify that they are in the appropriate groups. How else might you verify this information?

```
user5@localhost:~
[salma01@localhost ~]$ su - user1
Password:
[user1@localhost ~]$ id
uid=1004(user1) gid=1004(user1) groups=1004(user1),10000(sales) context=unconfin
ed_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user1@localhost ~]$ su - user2
Password:
[user2@localhost ~]$ id
uid=1005(user2) gid=1005(user2) groups=1005(user2),10000(sales) context=unconfin
ed_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user2@localhost ~]$ su - user3
Password:
[user3@localhost ~]$ id
uid=1006(user3) gid=1006(user3) groups=1006(user3),10001(hr) context=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user3@localhost ~]$ su - user4
Password:
[user4@localhost ~]$ id
uid=1007(user4) gid=1007(user4) groups=1007(user4),10001(hr) context=unconfined_
u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[user4@localhost ~]$ su - user5
Password:
[user5@localhost ~]$ id
uid=1008(user5) gid=1008(user5) groups=1008(user5),10002(web) context=unconfined
```

Another way: by using grep command

```
salma01@localhost:~
[user5@localhost ~]$ exit
logout
[user4@localhost ~]$ su - salma01
Password:
Hello Salma, Today is Wed Dec 13 12:57:16 PM EET 2023
[salma01@localhost ~]$ grep 'sales\|hr\|web' /etc/group
chrony:x:979:
sales:x:10000:user1,user2,user7
hr:x:10001:user3,user4,user7
web:x:10002:user5,user6,user7
[salma01@localhost ~]$
```

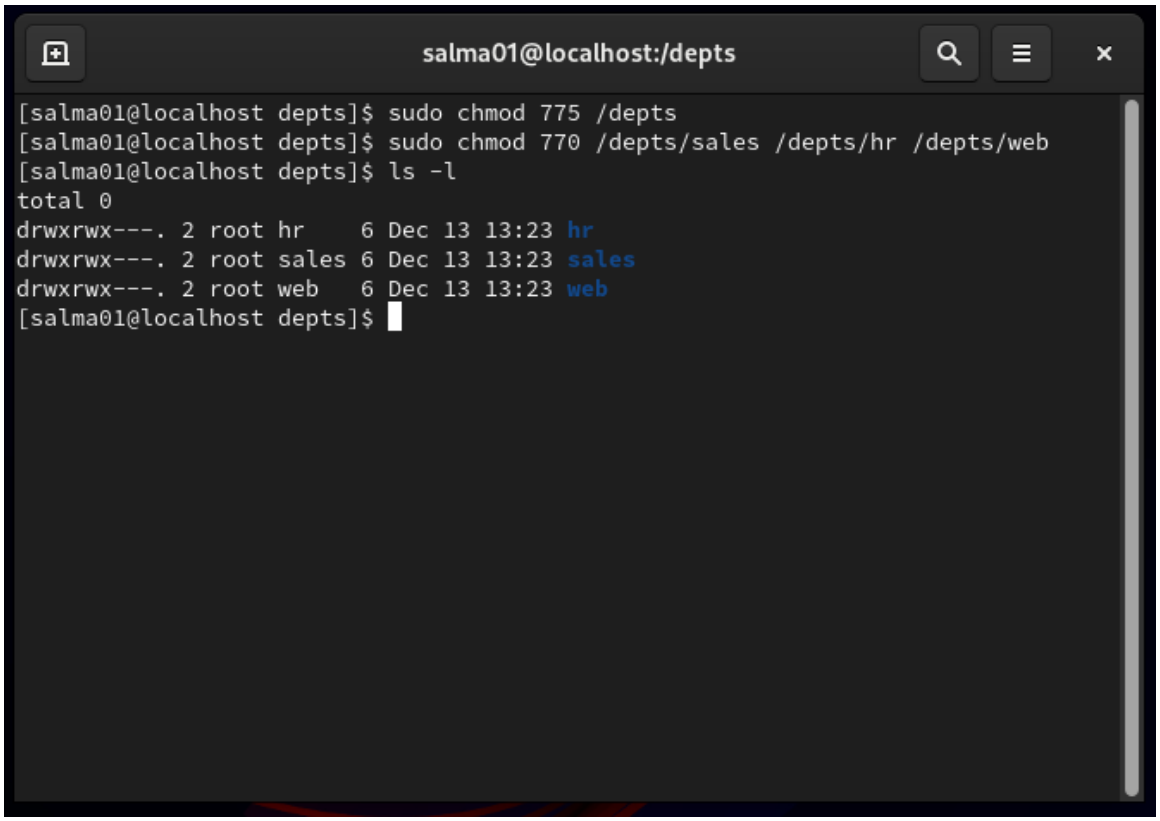
5. Create a directory called /depts with a sales, hr, and web directory within the /depts directory.



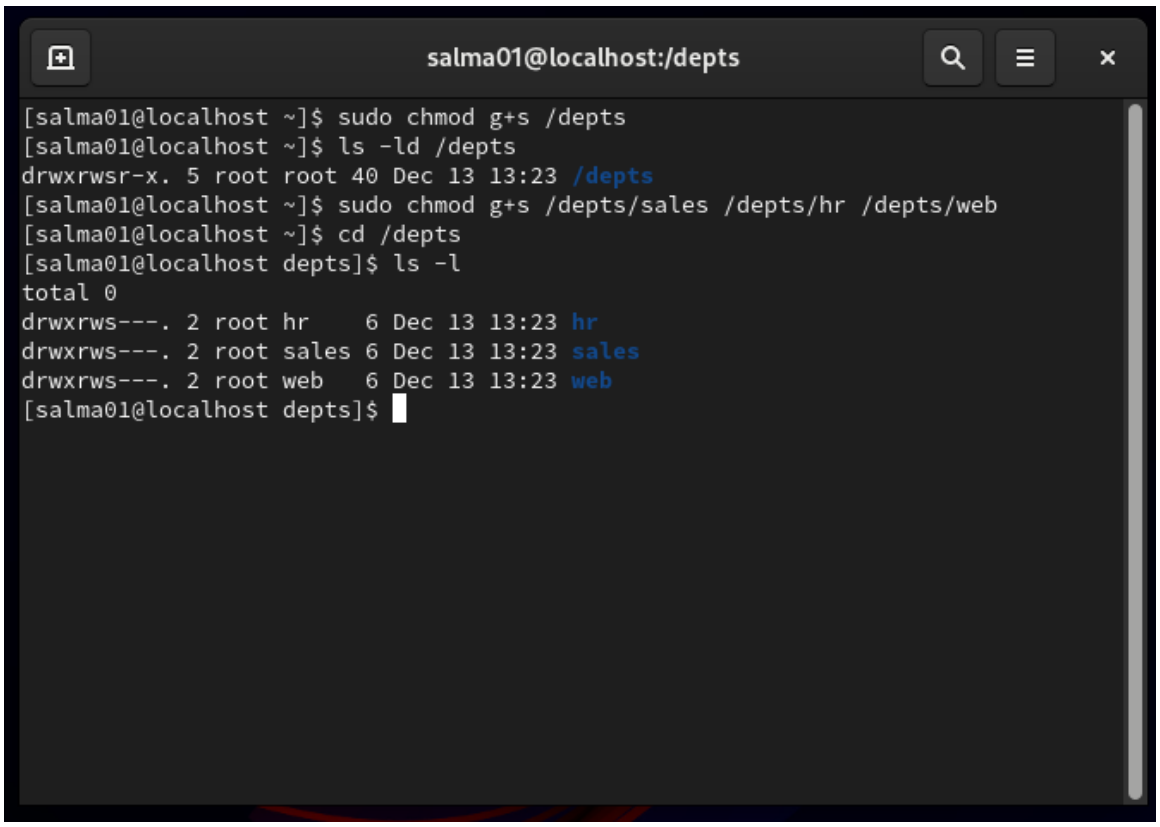
6. Using the chgrp command, set the group ownership of each directory to the group with the matching name.

```
salma01@localhost:/depts
[salma01@localhost depts]$ sudo chgrp hr /depts/hr
[salma01@localhost depts]$ ls -l
total 0
drwxr-xr-x. 2 root hr   6 Dec 13 13:23 hr
drwxr-xr-x. 2 root root 6 Dec 13 13:23 sales
drwxr-xr-x. 2 root root 6 Dec 13 13:23 web
[salma01@localhost depts]$ sudo chgrp sales /depts/sales
[sudo] password for salma01:
You have new mail in /var/spool/mail/salma01
[salma01@localhost depts]$ ls -l
total 0
drwxr-xr-x. 2 root hr    6 Dec 13 13:23 hr
drwxr-xr-x. 2 root sales 6 Dec 13 13:23 sales
drwxr-xr-x. 2 root root  6 Dec 13 13:23 web
[salma01@localhost depts]$ sudo chgrp web /depts/web
[salma01@localhost depts]$ ls -l
total 0
drwxr-xr-x. 2 root hr    6 Dec 13 13:23 hr
drwxr-xr-x. 2 root sales 6 Dec 13 13:23 sales
drwxr-xr-x. 2 root web   6 Dec 13 13:23 web
[salma01@localhost depts]$
```

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



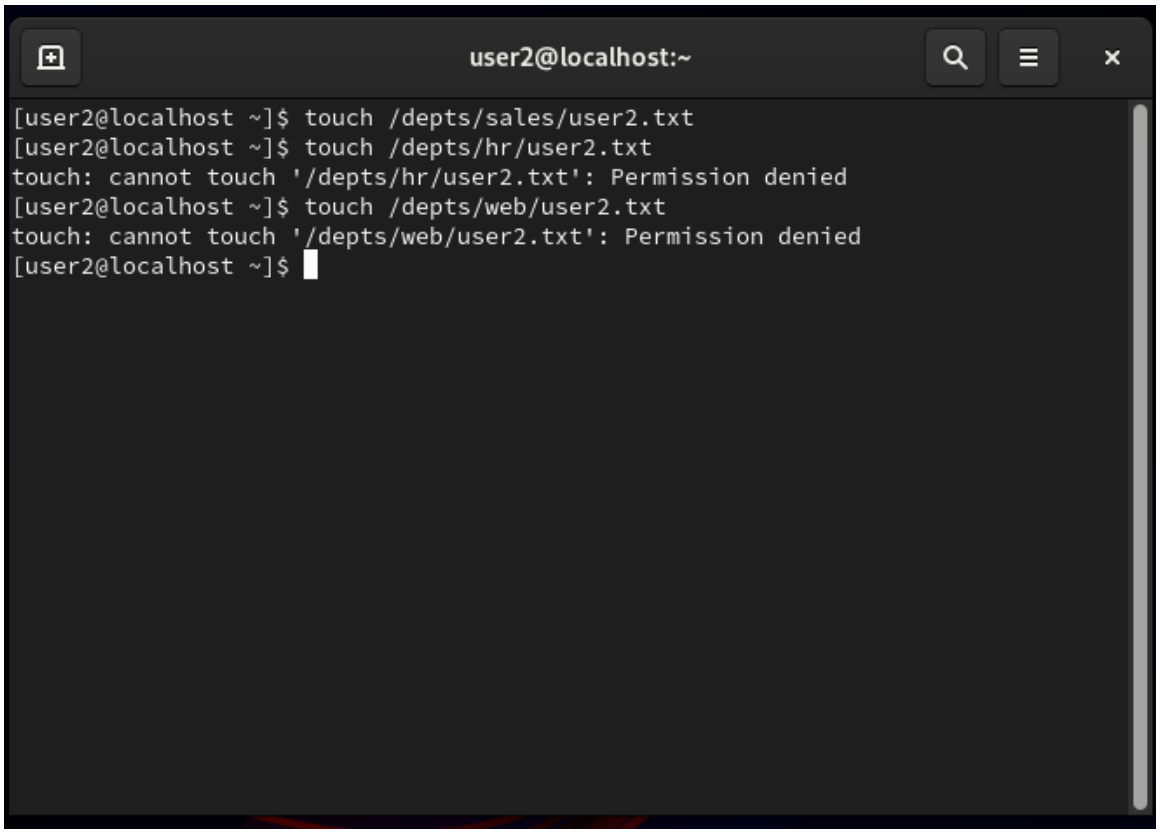
8. Set the set-gid bit on each departmental directory.



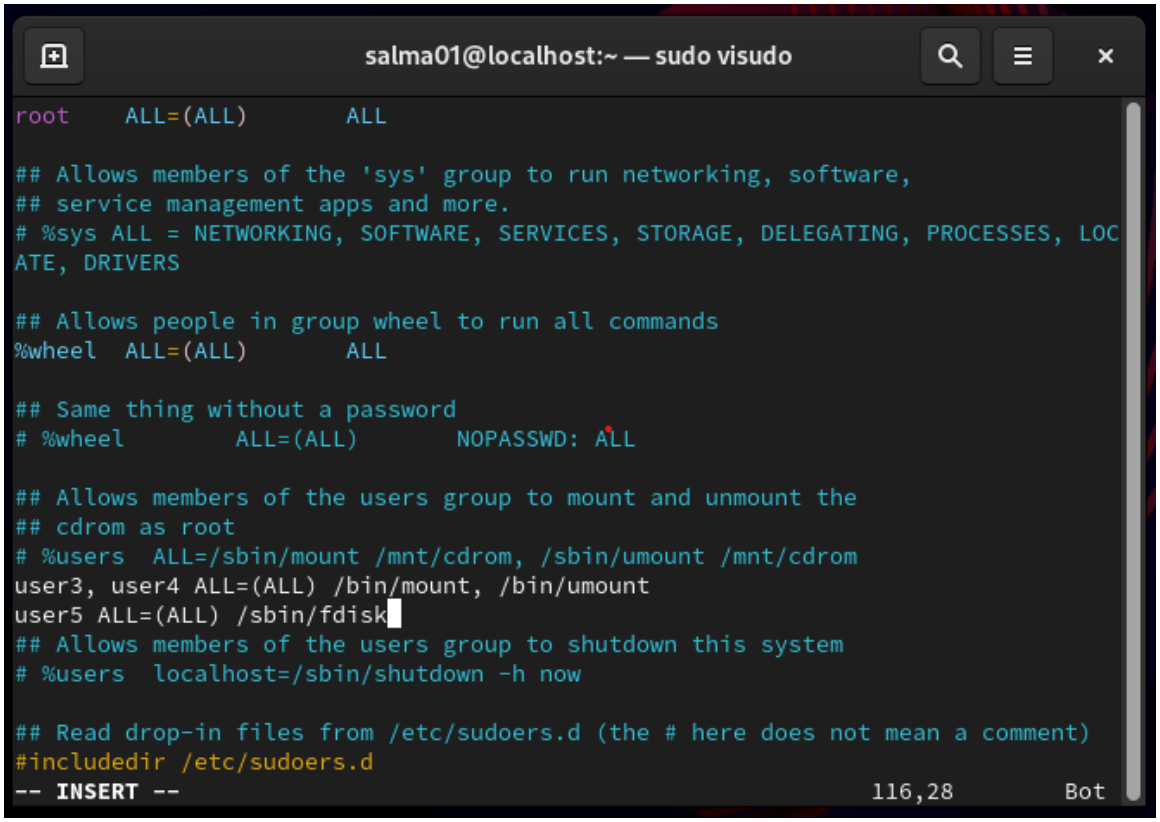
9. Use the su command to switch to the user2 account and attempt the following commands:
touch /depts/sales/user2.txt
touch /depts/hr/ user2.txt
touch /depts/web/ user2.txt

Which of these commands succeeded and which failed? What is the group ownership of the files that were created?

Only first command succeeded because user2 belongs only to sales group.

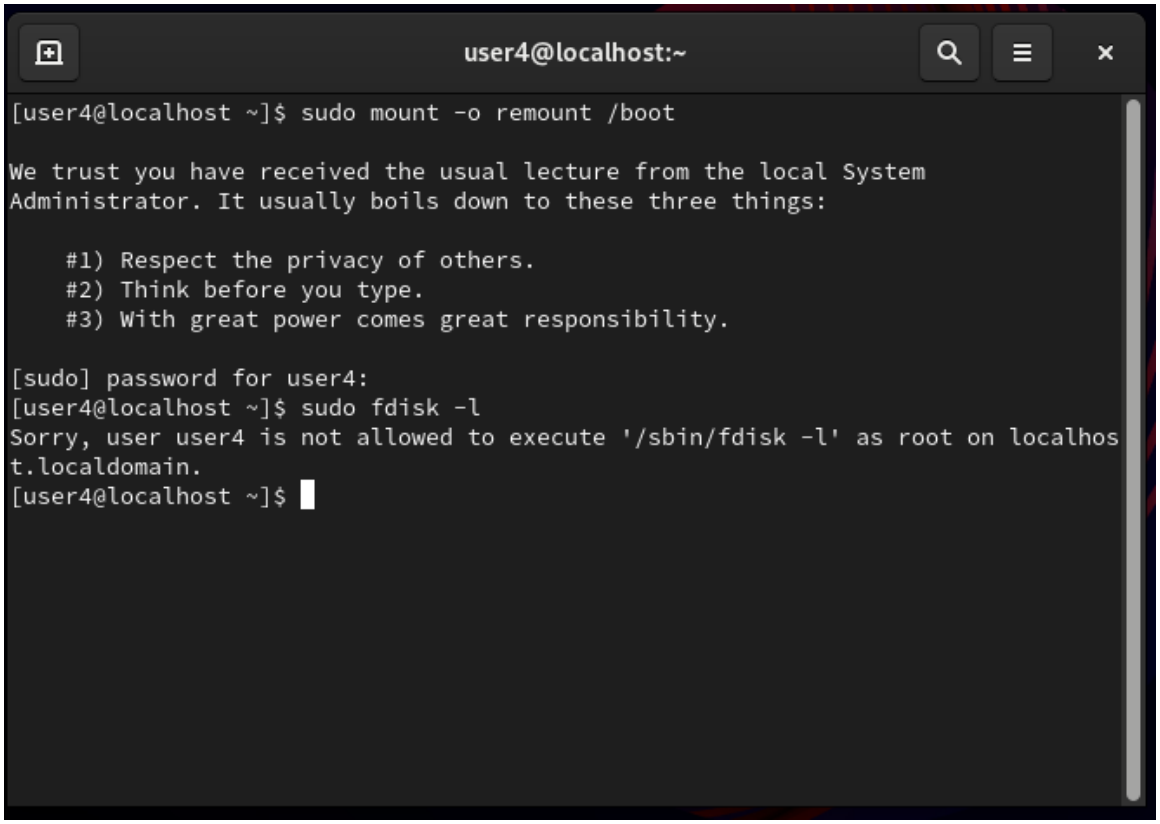


10. Configure sudoers file to allow user3 and user4 to use /bin/mount and /bin/umount commands, while allowing user5 only to use fdisk command.

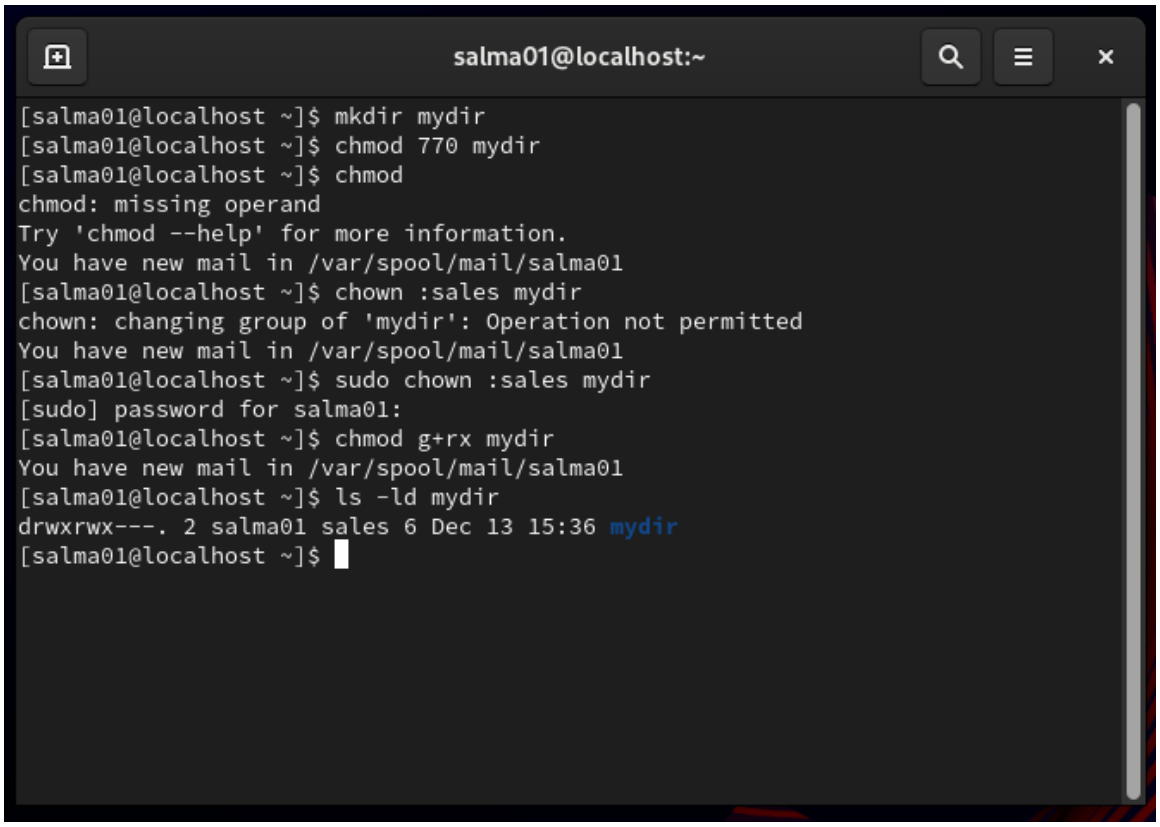


11. Login by user3 and try to unmount /boot.
    Su – user3
    sudo umount /boot

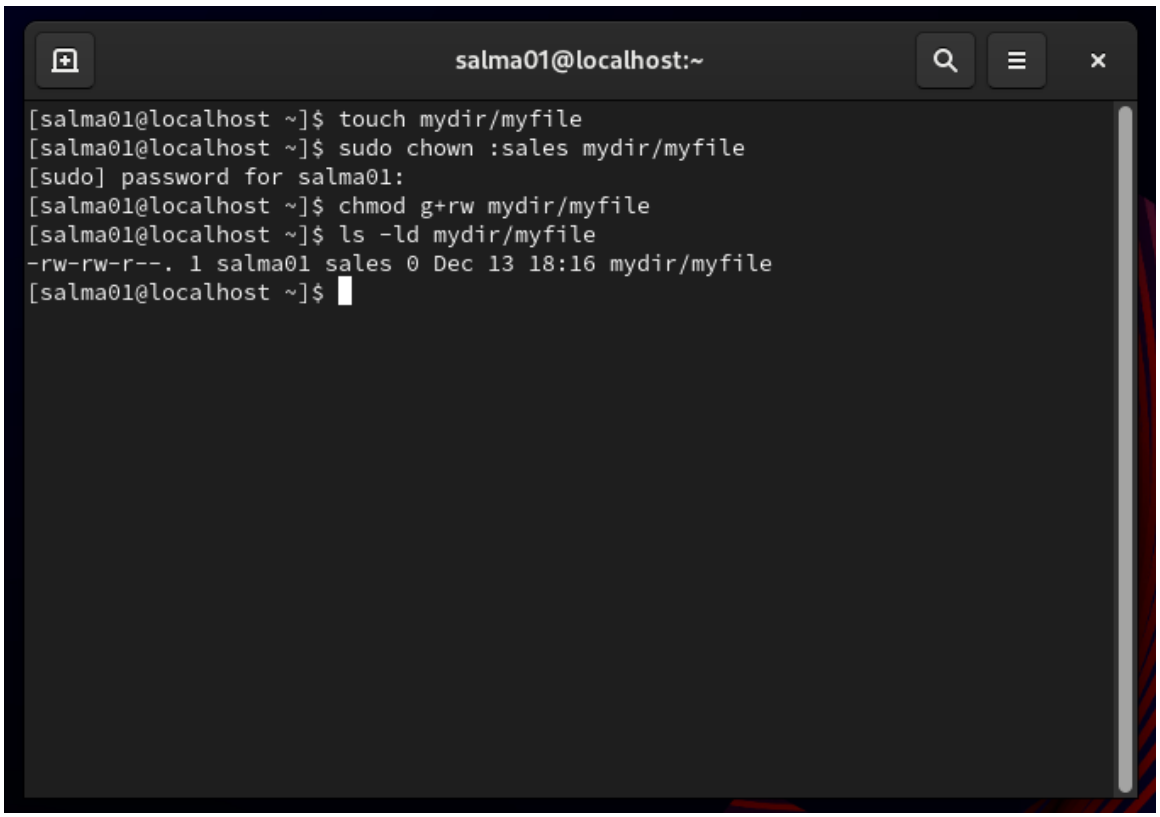
12. Login by user4 and remount /boot. Also try to view the partition table using fdisk. User4 does not has access to view the partition table using fdisk command.



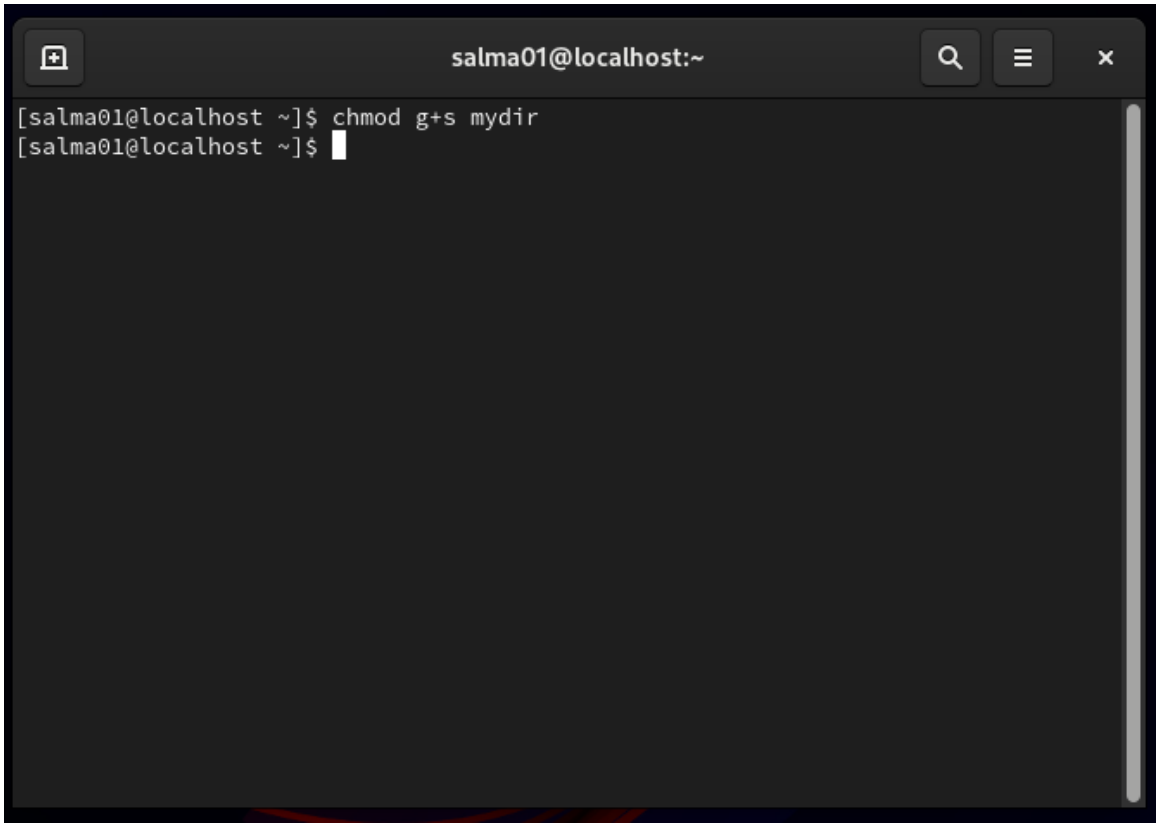
13. Create a directory with permissions rwxrwx---, grant a second group (sales) r-x permissions.



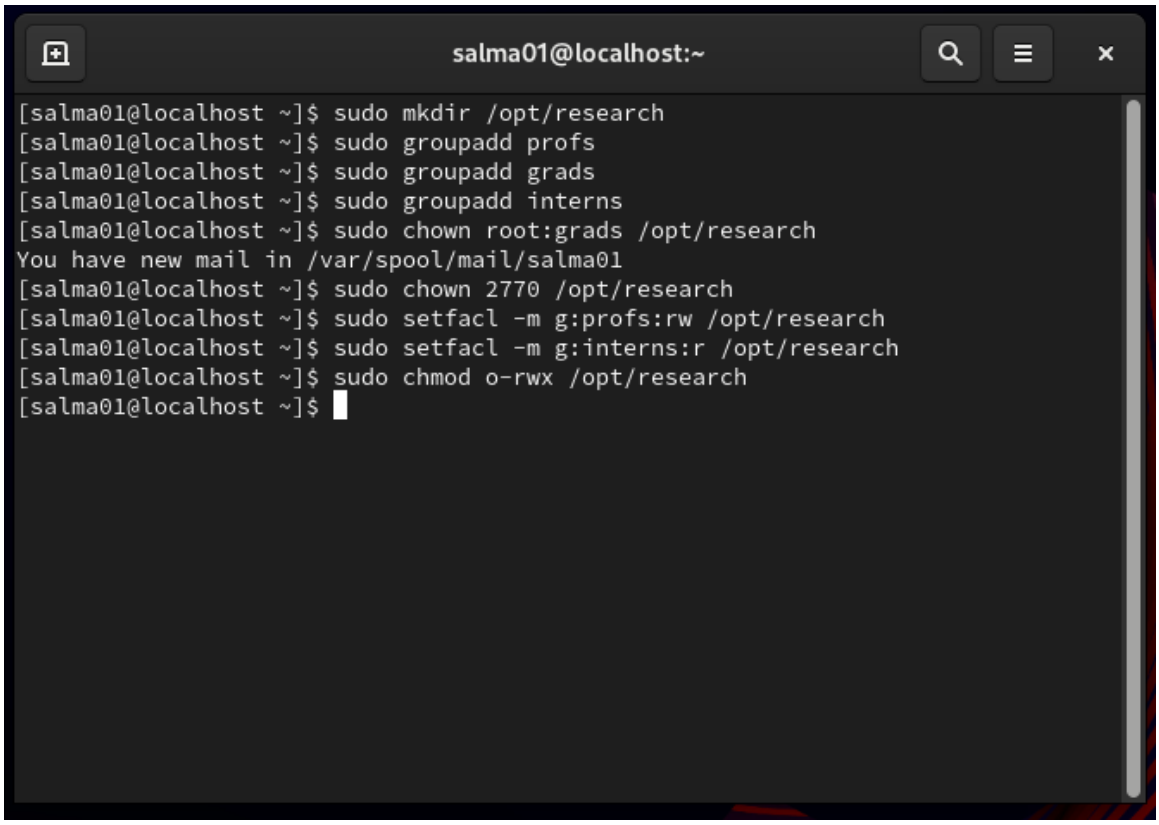
14. create a file on that directory and grant read and write to a second group (sales).



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

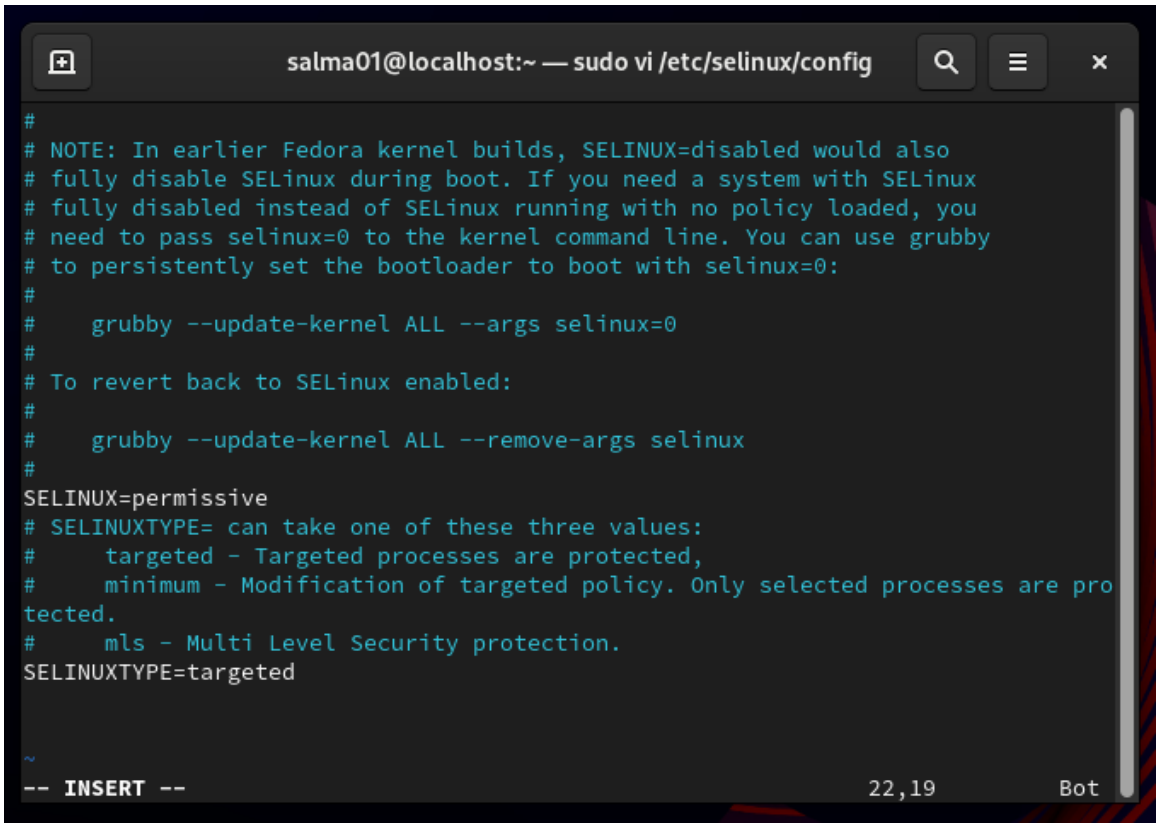


16. Grand your colleagues a collective directory called /opt/research, where they can store generated research results. Only members of group profs and grads should be able to create new files in the directory, and new file should have the following properties:
    - the directory should be owned by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

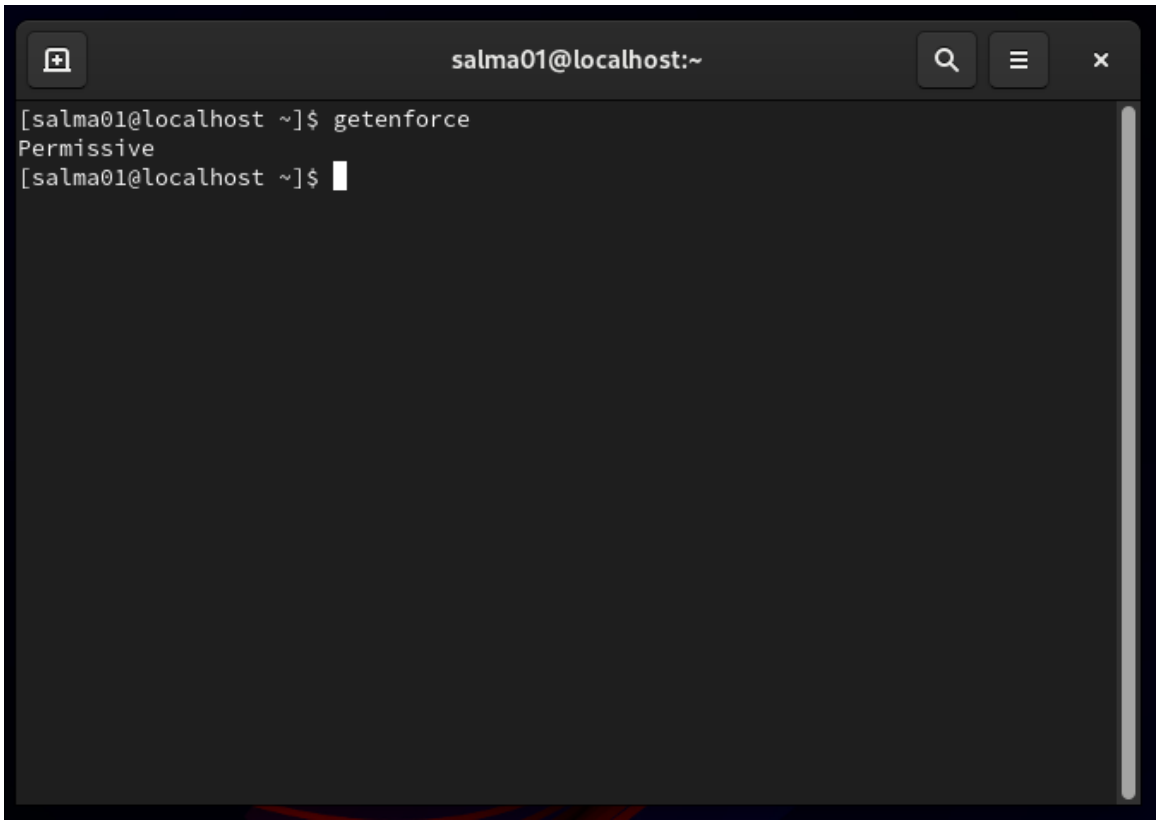


17. Change your default SELinux mode to permissive and reboot.

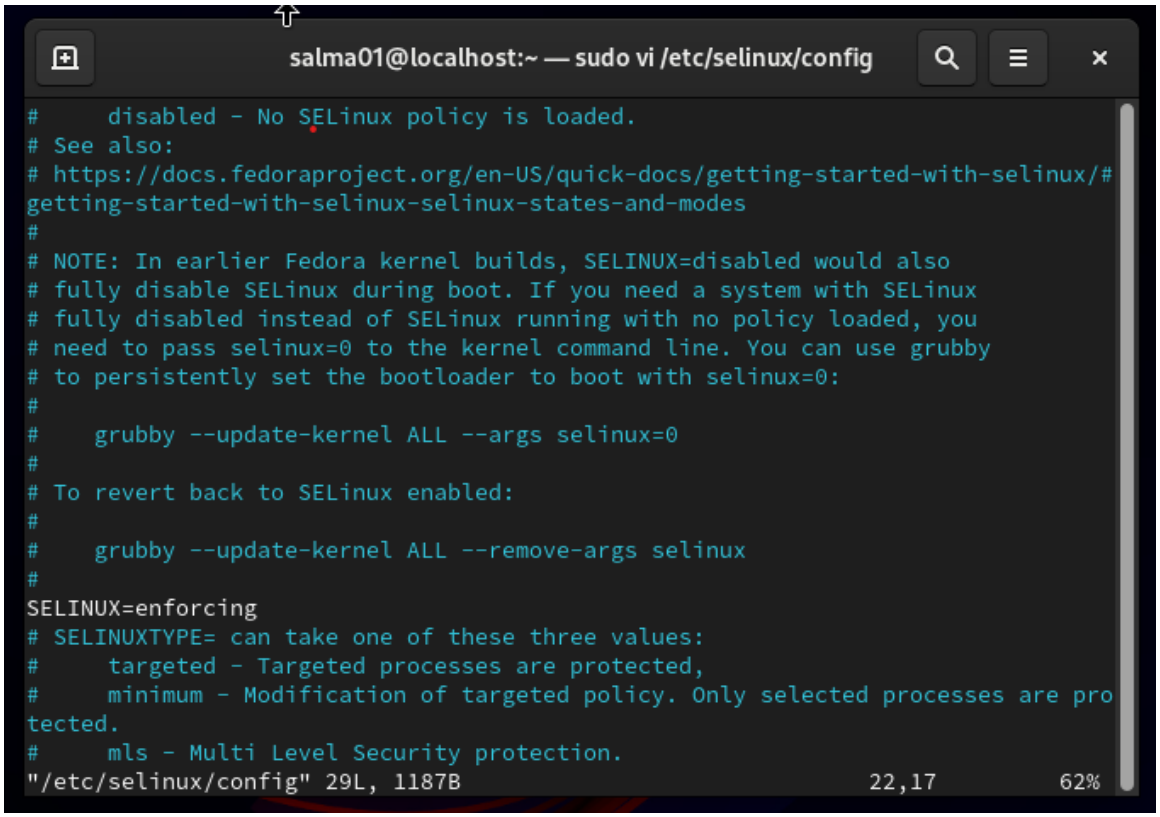
sudo nano /etc/selinux/config



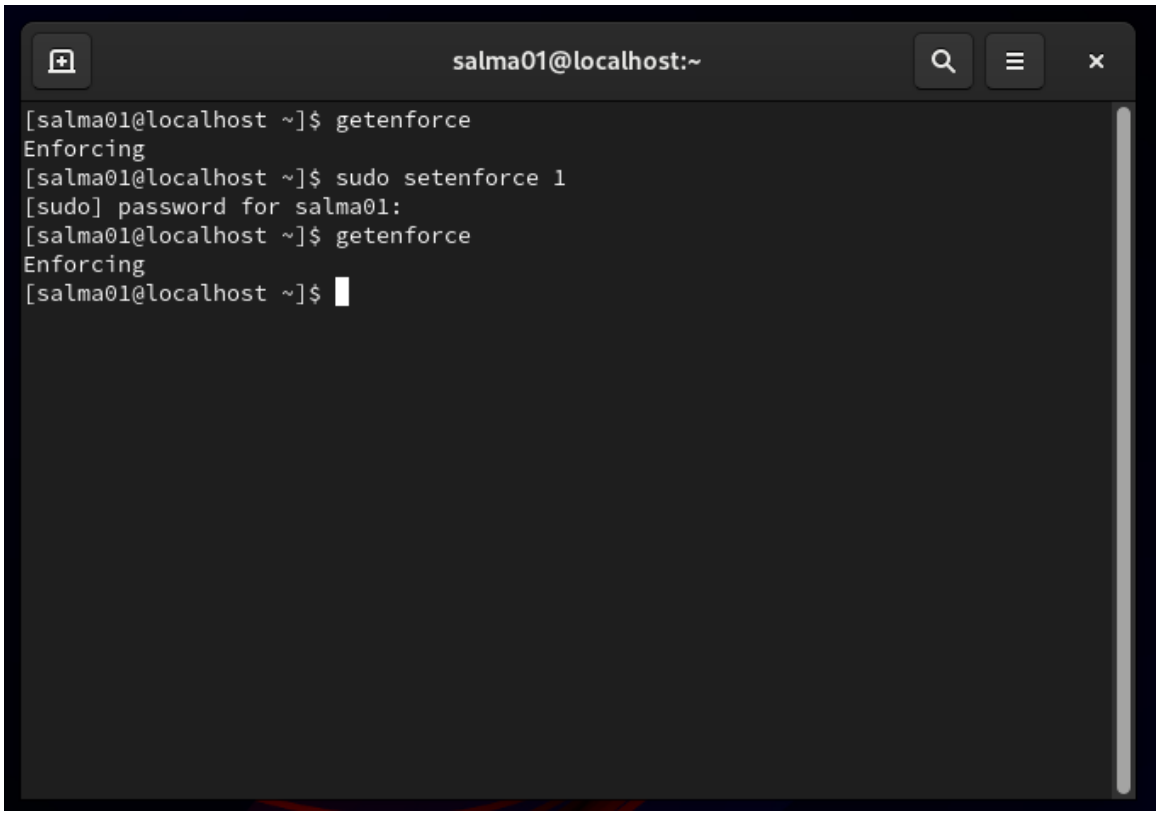
18. After reboot, verify the system is in permissive mode.



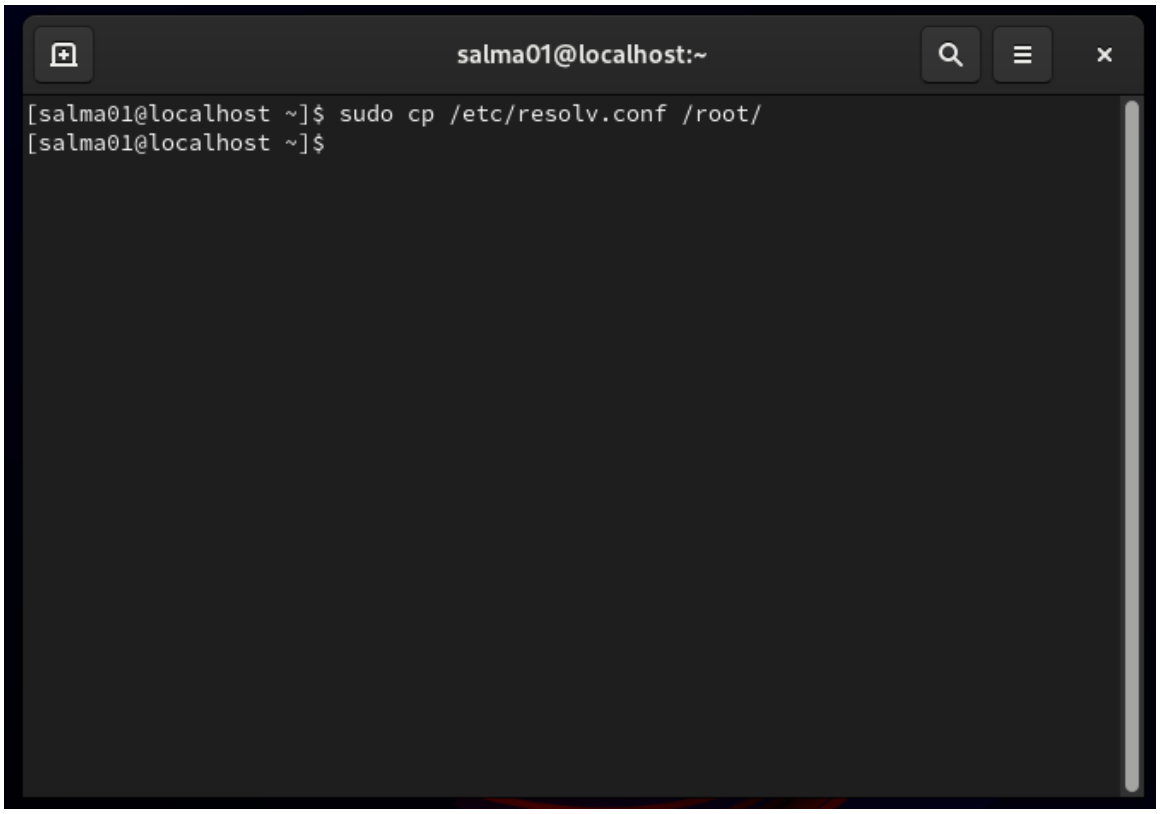
19. Change the default SELinux mode to enforcing.



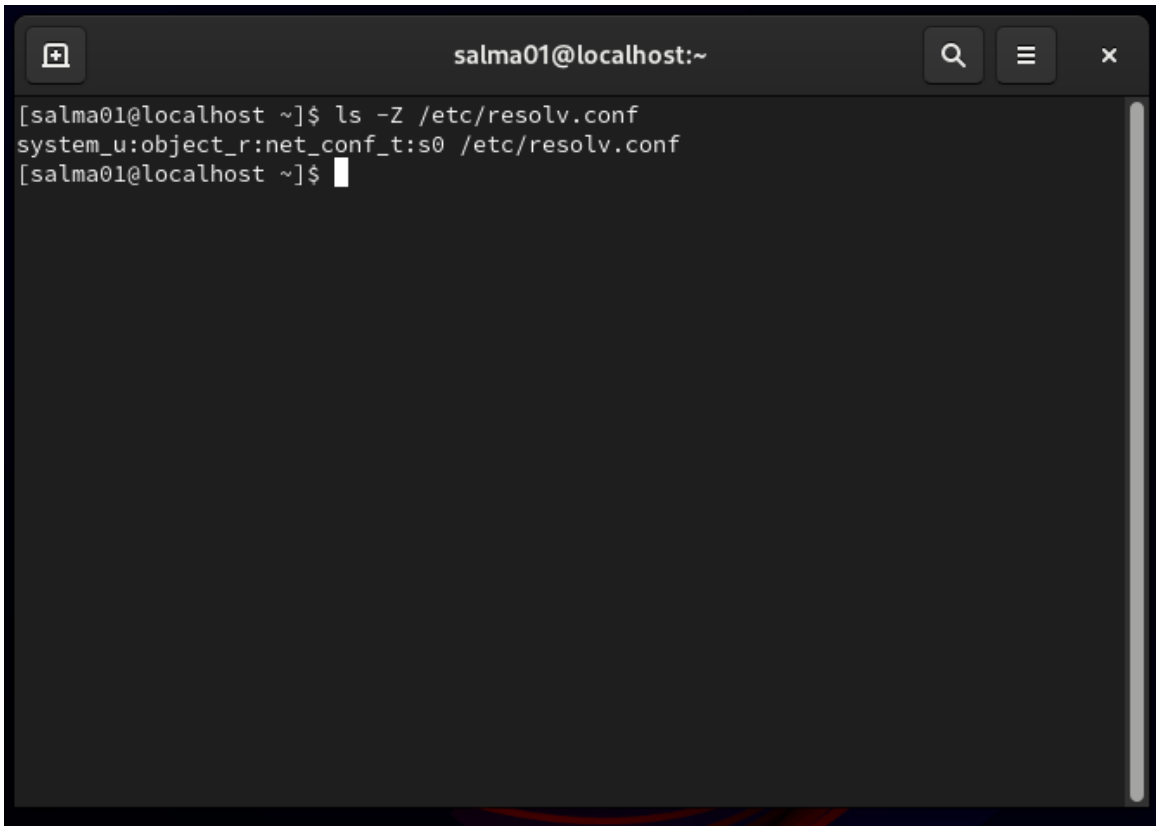
20. Change the current SELinux mode to enforcing.



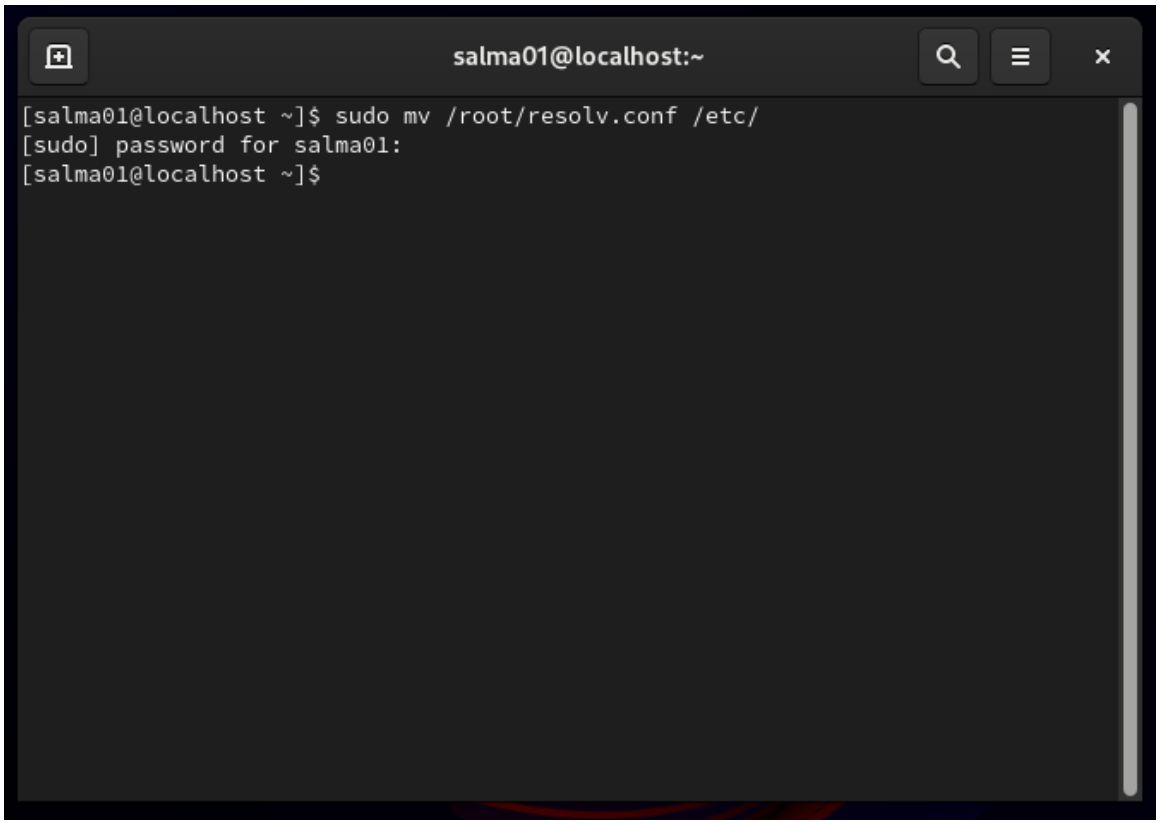
21. Copy /etc/resolv.conf file to root's home directory.



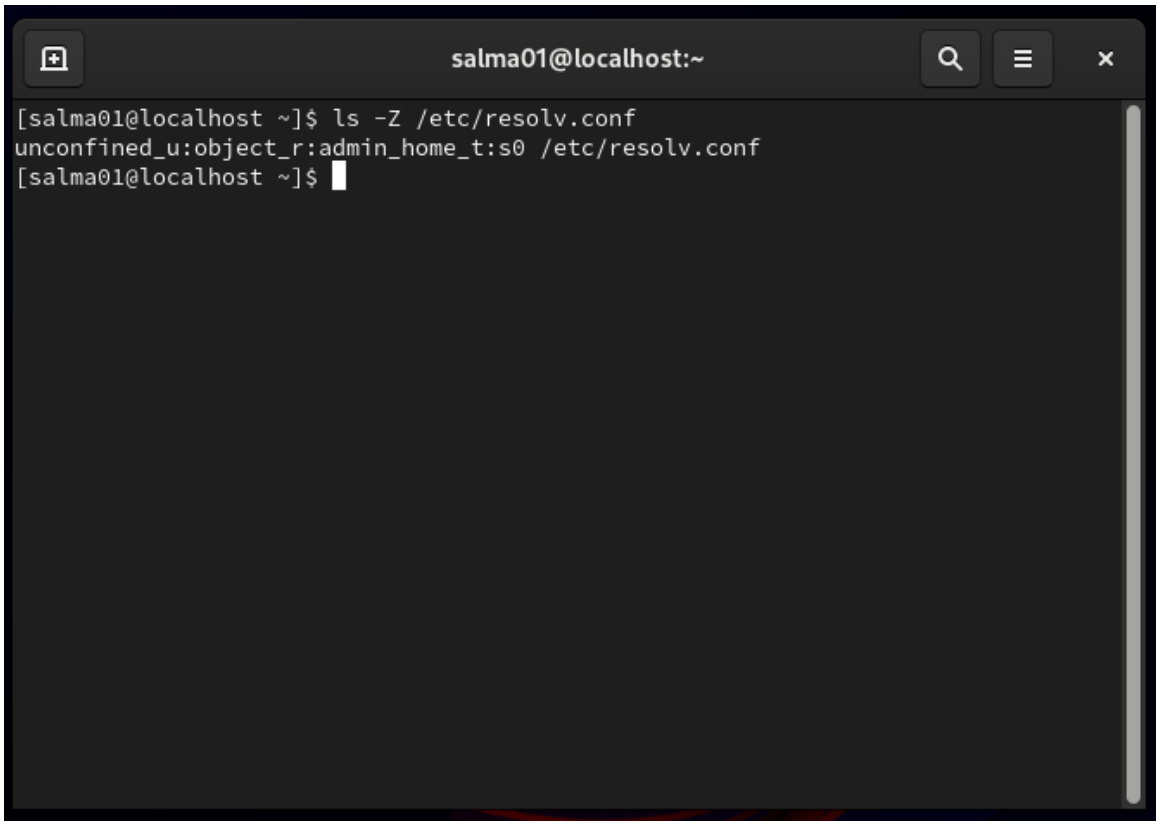
22. Observe the SELinux context of the intial /etc/resolv.conf.



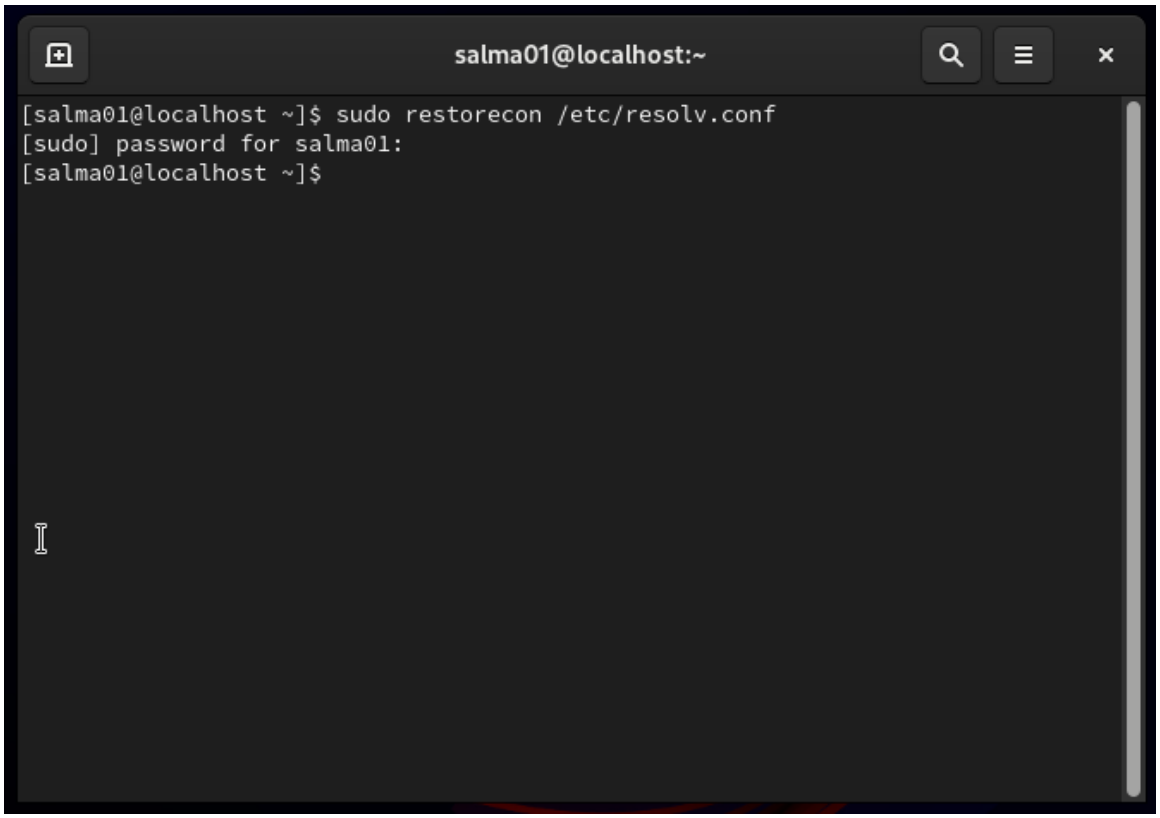
23. Move resolv.conf from root's home directory to /etc/resolv.conf.



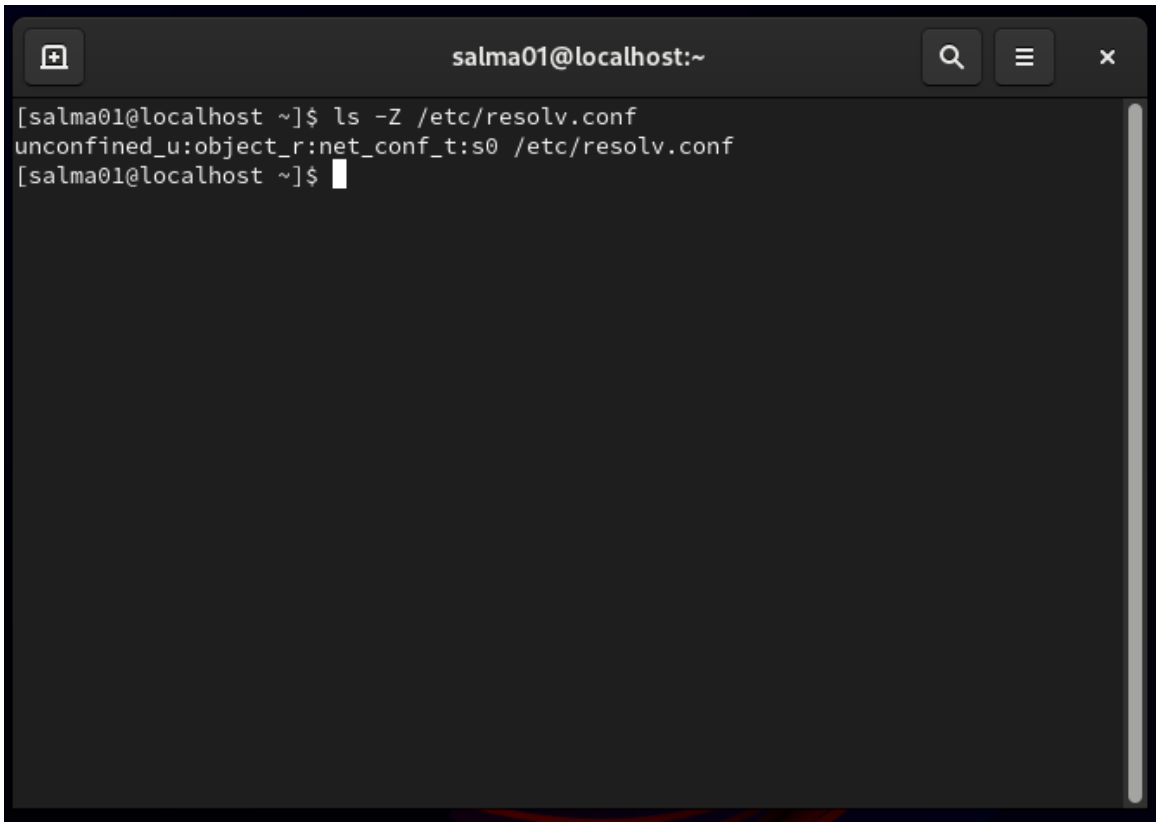
24. Observe the SELinux of the newly copied /etc/resolv.conf.



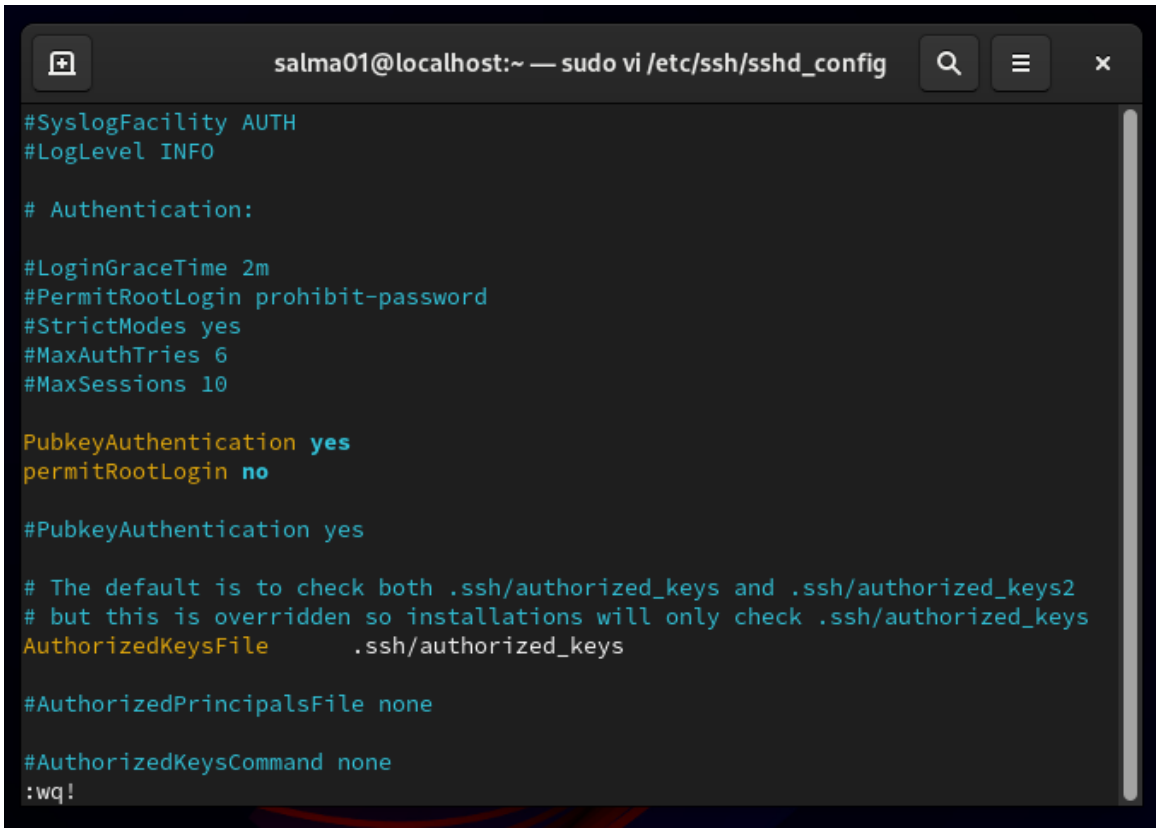
25. Restore the SELinux context of the newly positioned /etc/resolv.conf.



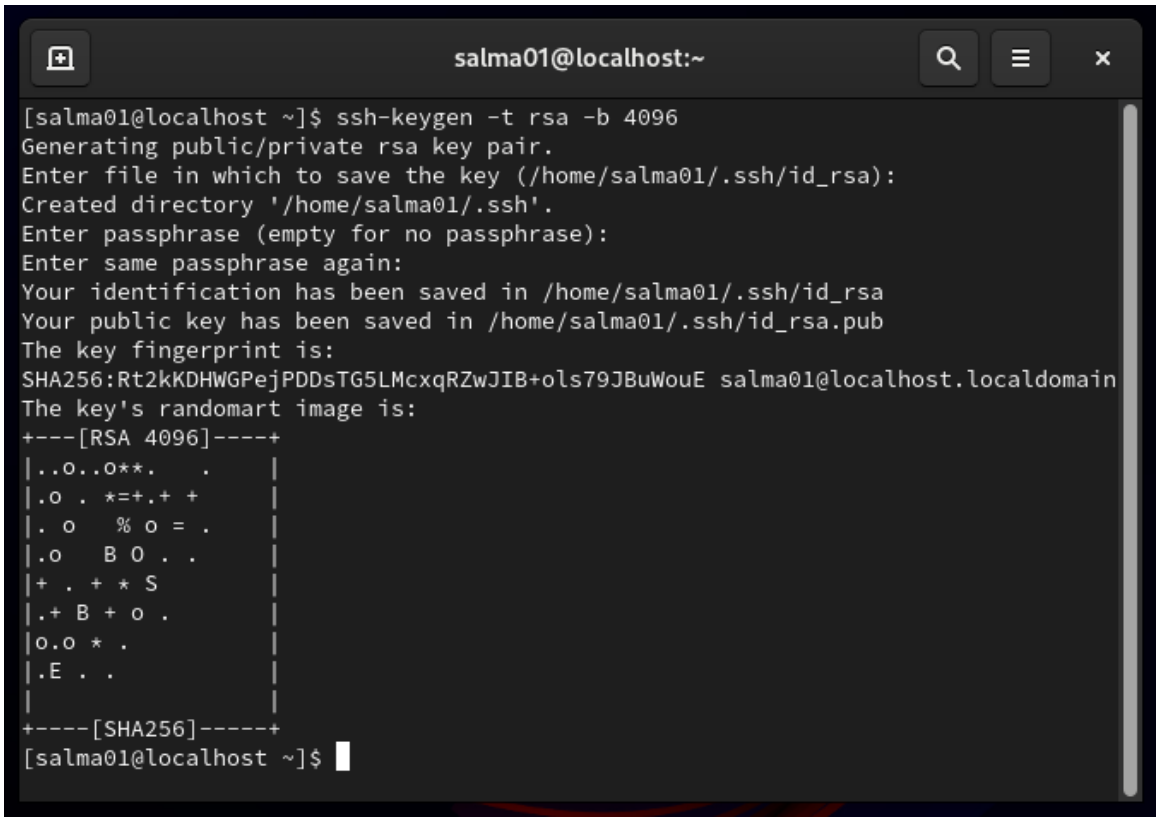
26. Observe the SELinux context of the restored /etc/resolv.conf



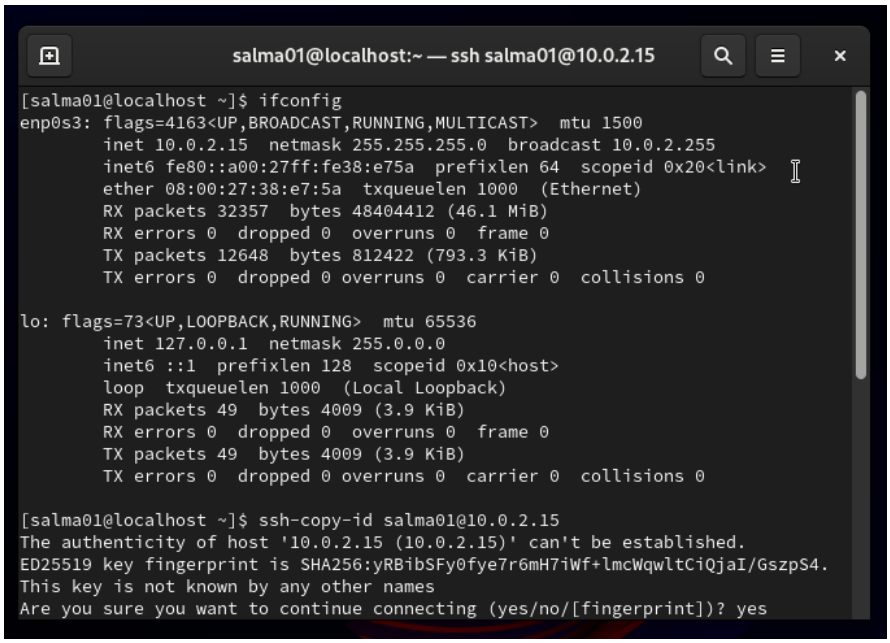
27. Configure OpenSSH to allow pulic key-based login credentials

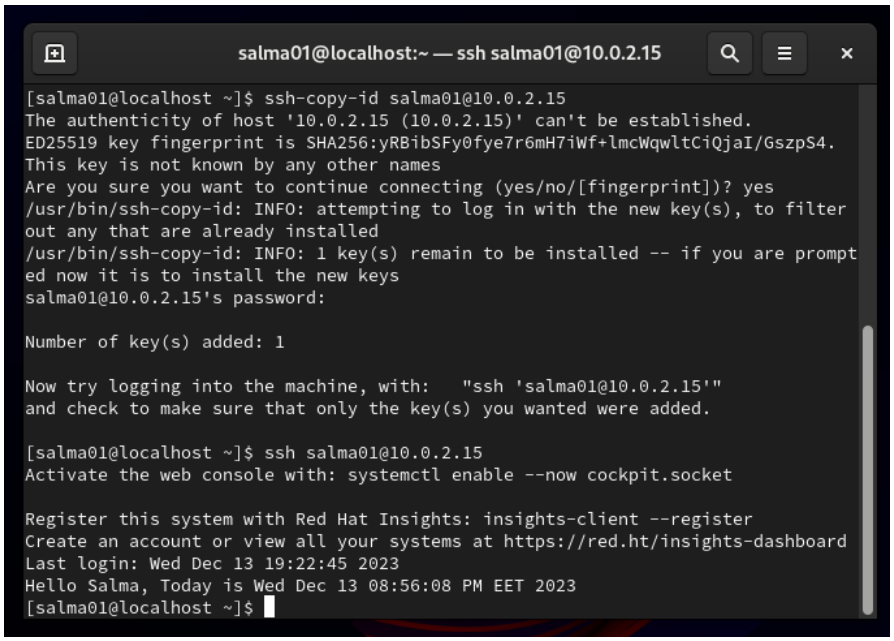


28. Create an SSH key-pair.

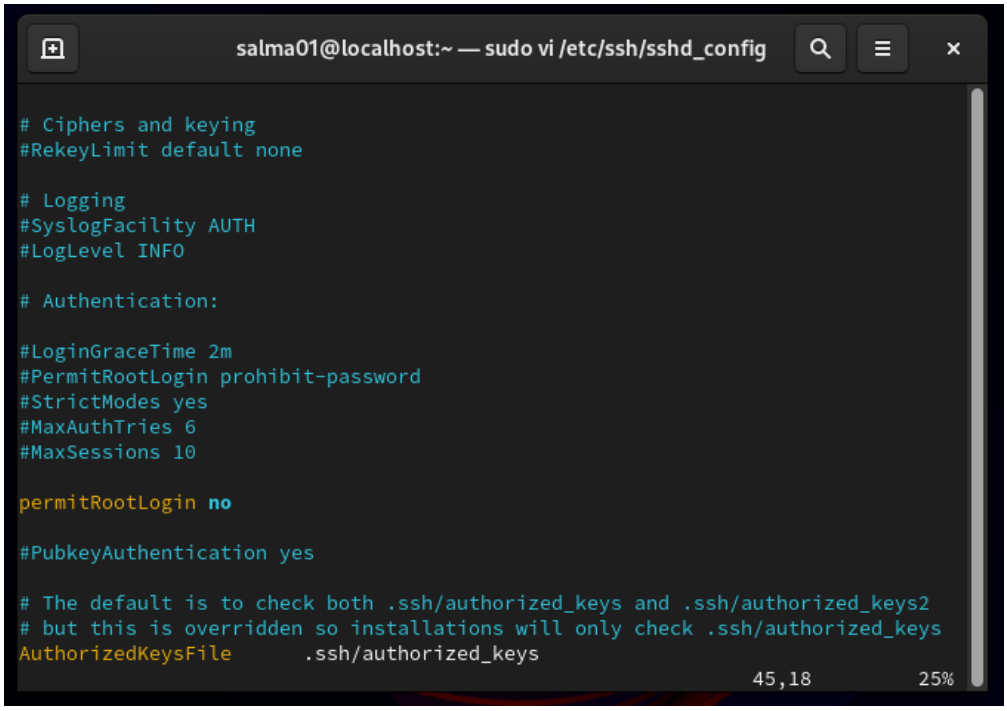


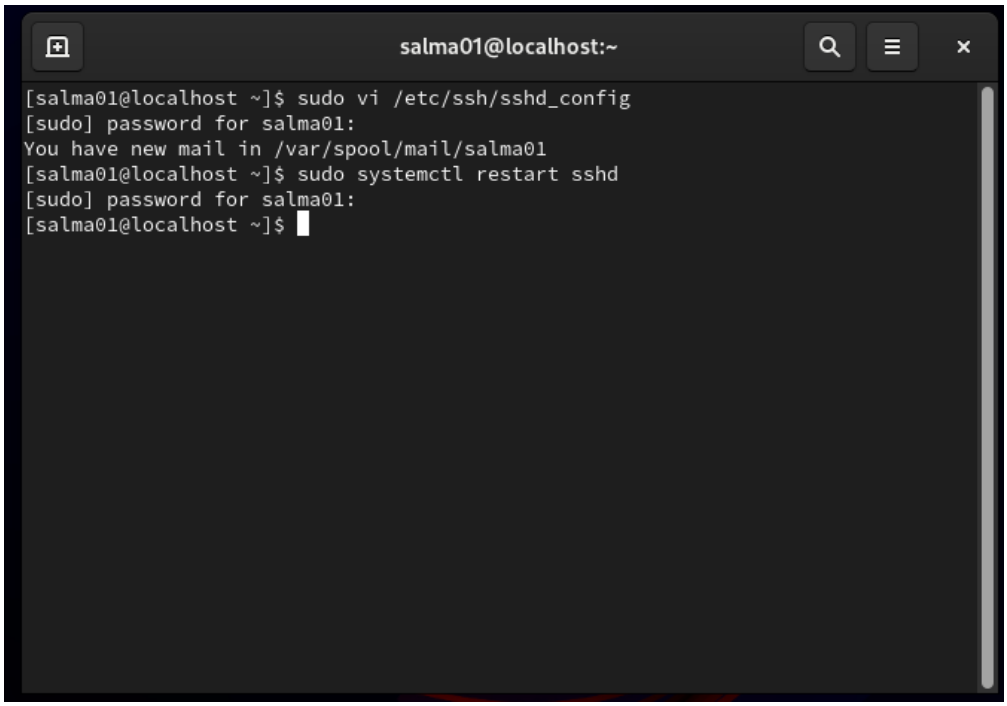
29. Configure to login without the need of a password.





30. Configure SSH to prevent root logins.





31. Configure logrotate default setting to compress log files when they are rotated.