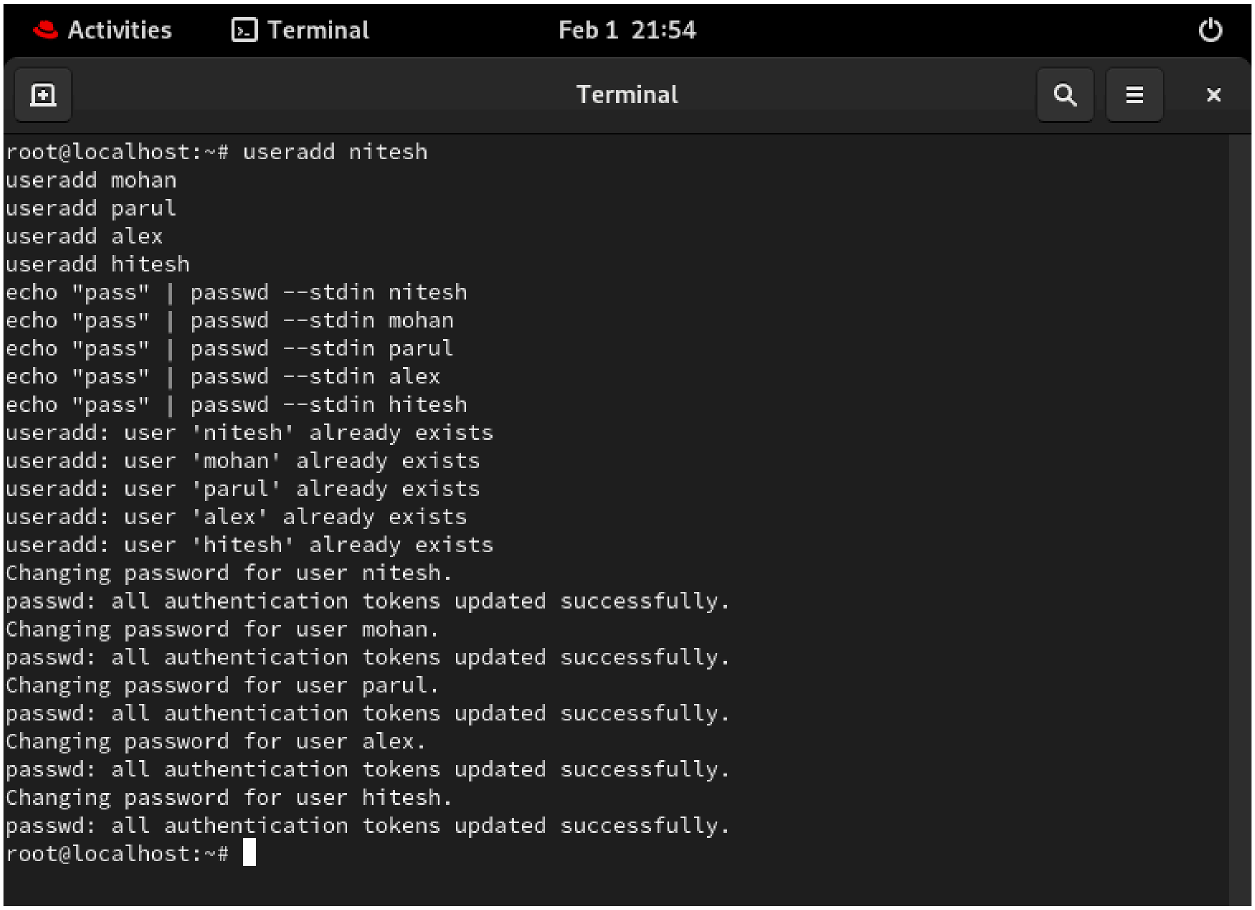
Question 1: Basic Understanding of Users in Linux Ÿ How many types of users exist in a Linux system? What is the UID range of it? Ÿ Write a Linux command to check which users have access to the shell for executing commands.

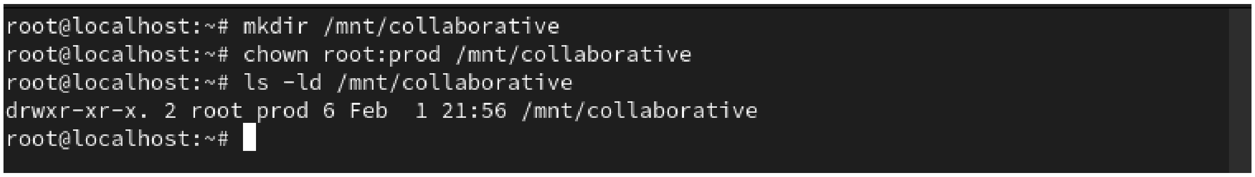
Types of Users

1. **Root User (Superuser)** → Has full control over the system (UID = 0).
2. **System Users** → Used for system services (UID = 1-999).
3. **Regular Users** → Normal users who log in (UID = 1000+) in a Linux system there are three main types of users:
4. **Root User, System Users, and Regular Users**. The **Root User (Superuser)** has complete control over the system and can modify any file, install or remove software, and manage other users. It has a unique **User ID (UID) of 0** and is the most powerful user in the system. **system users**, on the other hand, are created by Linux to run essential background services like web servers, database services, and system processes. These users usually have **UIDs ranging from 1 to 999** (or sometimes up to 1000, depending on the Linux distribution) and typically do not have login access, as their purpose is to keep the system running smoothly finally **regular users** are the ones created for human users to log in and use the system. They have **UIDs starting from 1000+** and are restricted from making major system changes unless granted special permissions using `sudo`. Each regular user has a home directory (e.g., `/home/alex`), where they store their personal files and settings. These three user types ensure that Linux maintains a **secure and well-organized** environment, preventing unauthorized changes while allowing normal users to perform their tasks efficiently…..

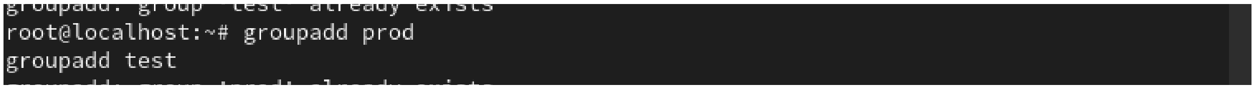
Question 2: An organization “Copex Pvt Ltd” has set up some users and groups for a project. Perform the following tasks step-by-step: User and Group Creation v Create the following users and set a common password “pass” for all users: Ÿ Nitesh, Mohan, Nitesh, Parul, Alex, Hitesh v Create the following groups for this project: Ÿ prod, test Collaborative Directory Setup v As the root administrator, create a collaborative directory named “collaborative” under “/mnt”. v Write a Linux command to change the owner & group-owner of the /mnt/collaborative directory to the “root & prod” group at a same time. Answer the following questions v Write a Linux command to check the “default permissions, owner, and group owner” of the directory. v Which users in this project fall under the "others" category for this directory?



```
root@localhost:~# useradd nitesh
useradd mohan
useradd parul
useradd alex
useradd hitesh
echo "pass" | passwd --stdin nitesh
echo "pass" | passwd --stdin mohan
echo "pass" | passwd --stdin parul
echo "pass" | passwd --stdin alex
echo "pass" | passwd --stdin hitesh
useradd: user 'nitesh' already exists
useradd: user 'mohan' already exists
useradd: user 'parul' already exists
useradd: user 'alex' already exists
useradd: user 'hitesh' already exists
Changing password for user nitesh.
passwd: all authentication tokens updated successfully.
Changing password for user mohan.
passwd: all authentication tokens updated successfully.
Changing password for user parul.
passwd: all authentication tokens updated successfully.
Changing password for user alex.
passwd: all authentication tokens updated successfully.
Changing password for user hitesh.
passwd: all authentication tokens updated successfully.
root@localhost:~#
```

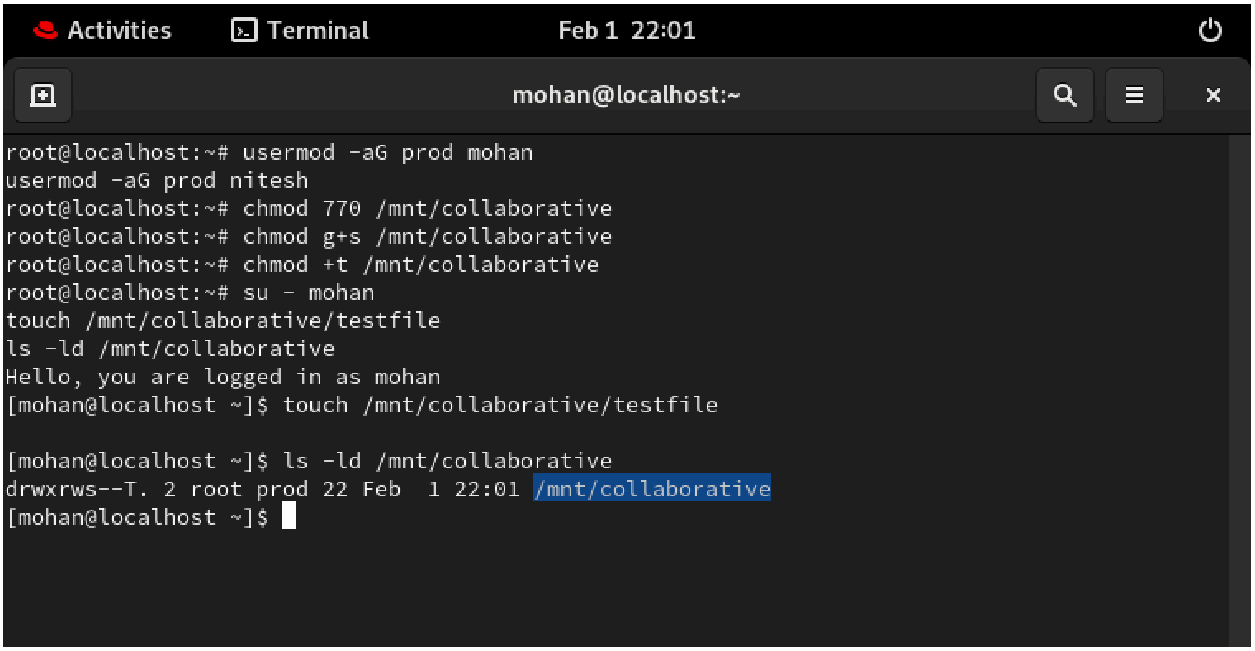


```
root@localhost:~# mkdir /mnt/collaborative
root@localhost:~# chown root:prod /mnt/collaborative
root@localhost:~# ls -ld /mnt/collaborative
drwxr-xr-x. 2 root prod 6 Feb  1 21:56 /mnt/collaborative
root@localhost:~#
```



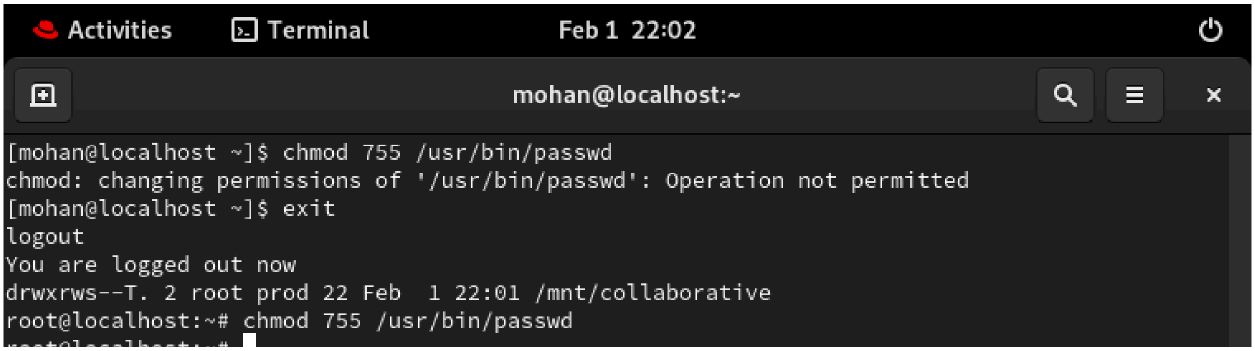
```
groupadd: group 'test' already exists
root@localhost:~# groupadd prod
groupadd test
groupadd: group 'prod' already exists
```

Question 3: Advanced Permission Management. Group Membership Assignment v As the root administrator, add users Mohan and Nitesh to the prod group as secondary group membersv Grant the prod group members permission to create and modify content in the /mnt/collaborative directory. v Restrict "others" from having no permissions in the /mnt/collaborative directory using the symbolic method. v Create some files and directories in /mnt/collaborative and ensure that any new content created in /mnt/collaborative automatically inherits the same group ownership as the parent directory. v Additionally, ensure that no one can delete the files created by others, except the file's creator. Verification Tasks v Log in as the user “Mohan” and: Ÿ Verify that user “Mohan” can create content in the “/mnt/collaborative” directory or not. Ÿ Now again what are the permissions for “Owner, Group & Other for ”/mnt/collaborative”, Describe the permission section of especially group & others.



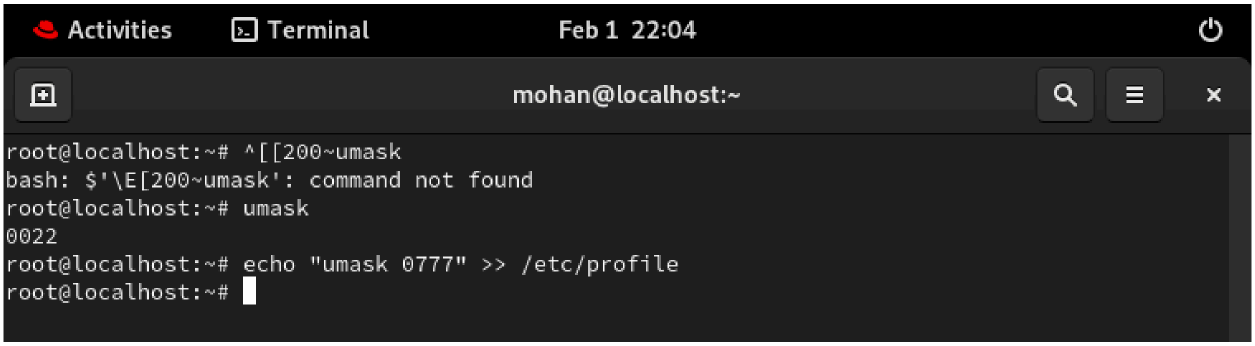
```
root@localhost:~# usermod -aG prod mohan
usermod -aG prod nitesh
root@localhost:~# chmod 770 /mnt/collaborative
root@localhost:~# chmod g+s /mnt/collaborative
root@localhost:~# chmod +t /mnt/collaborative
root@localhost:~# su - mohan
touch /mnt/collaborative/testfile
ls -ld /mnt/collaborative
Hello, you are logged in as mohan
[mohan@localhost ~]$ touch /mnt/collaborative/testfile

[mohan@localhost ~]$ ls -ld /mnt/collaborative
drwxrws--T. 2 root prod 22 Feb  1 22:01 /mnt/collaborative
[mohan@localhost ~]$
```

Question 4: Write a command to remove the SUID special permission from the file /usr/bin/passwd using the numerical method & explain the impact of this change.



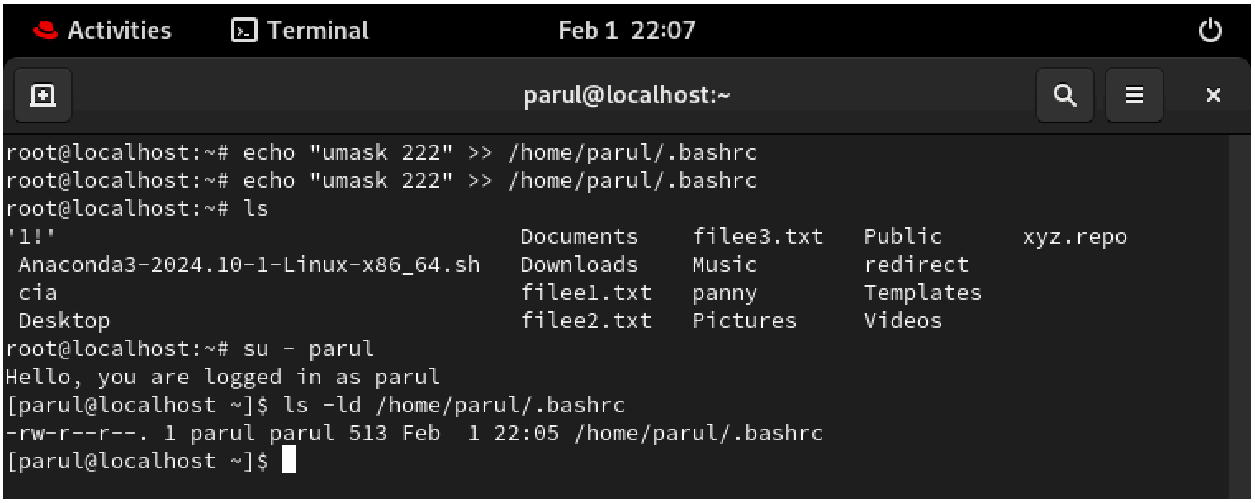
```
[mohan@localhost ~]$ chmod 755 /usr/bin/passwd
chmod: changing permissions of '/usr/bin/passwd': Operation not permitted
[mohan@localhost ~]$ exit
logout
You are logged out now
drwxrws--T. 2 root prod 22 Feb  1 22:01 /mnt/collaborative
root@localhost:~# chmod 755 /usr/bin/passwd
```

Question 5: Set the UMASK Value: v Write the Linux command to check the current “umask” value for the user's shell. v How would you change the “umask” setting so that all newly created users on the system have a default “umask” value of `0777`?



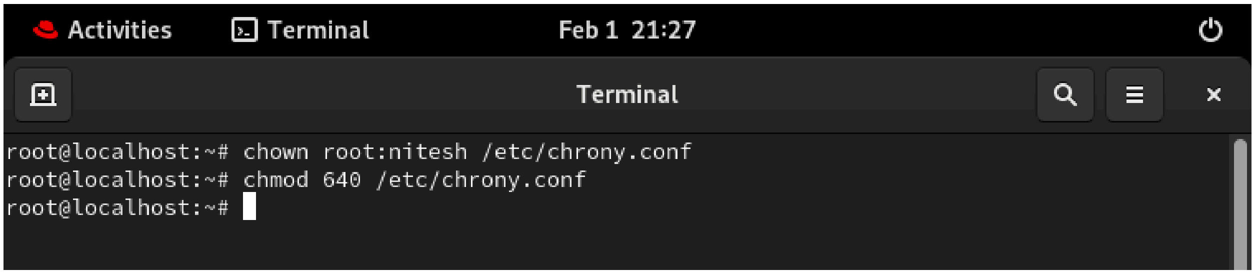
```
root@localhost:~# ^[[200~umask
bash: $'\E[200~umask': command not found
root@localhost:~# umask
0022
root@localhost:~# echo "umask 0777" >> /etc/profile
root@localhost:~# 
```

Question 6: Set the default permissions for the user Parul on newly created files and directories as follows: v Set the default permissions for all newly created files to r--r--r--. v Set the default permissions for all newly created directories to r-xr-xr-x..



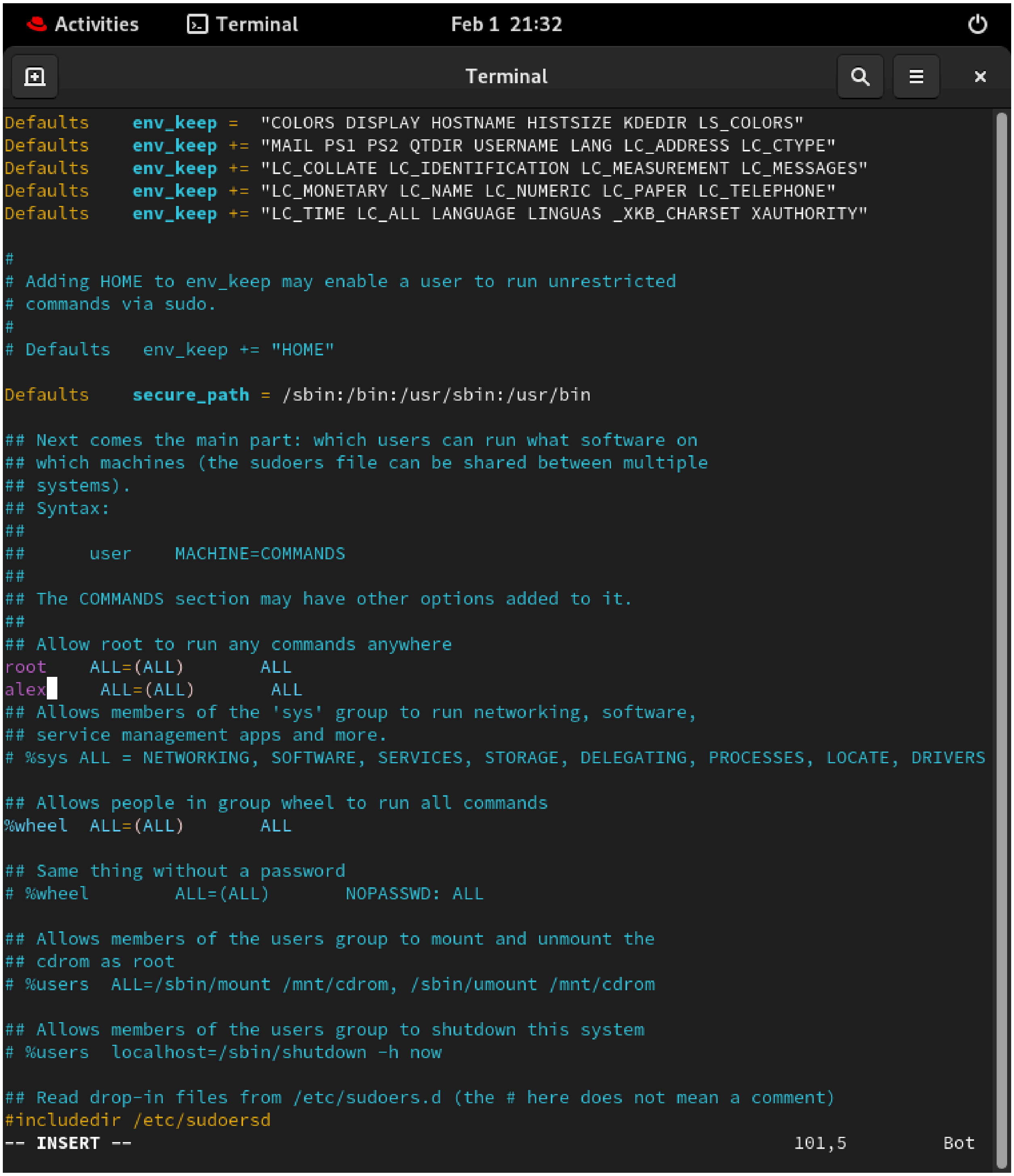
```
root@localhost:~# echo "umask 222" >> /home/parul/.bashrc
root@localhost:~# echo "umask 222" >> /home/parul/.bashrc
root@localhost:~# ls
'1!'                                 Documents    filee3.txt   Public      xyz.repo
 Anaconda3-2024.10-1-Linux-x86_64.sh  Downloads    Music        redirect
 cia                                  filee1.txt   panny        Templates
 Desktop                              filee2.txt   Pictures     Videos
root@localhost:~# su - parul
Hello, you are logged in as parul
[parul@localhost ~]$ ls -ld /home/parul/.bashrc
-rw-r--r--. 1 parul parul 513 Feb  1 22:05 /home/parul/.bashrc
[parul@localhost ~]$ 
```

Question 7: As a system administrator, configure the system to ensure that only the user Nitesh and the root user can modify the /etc/chrony.conf file, while all other users should have read-only access to it. Write the commands.



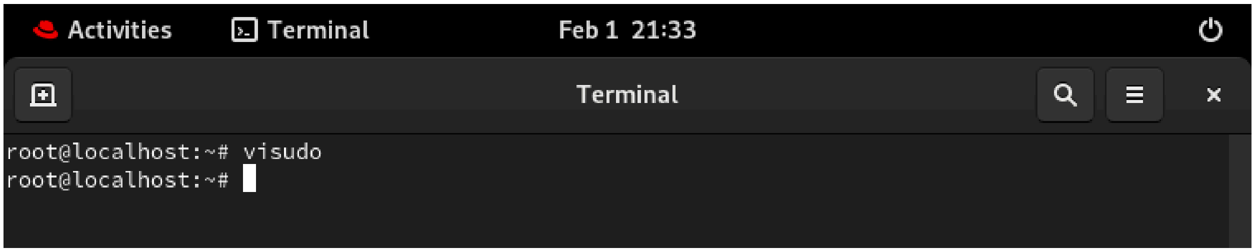
```
root@localhost:~# chown root:nitesh /etc/chrony.conf
root@localhost:~# chmod 640 /etc/chrony.conf
root@localhost:~# 
```

Question 8: User Alex needs to be granted administrative privileges equivalent to the root user to manage the system, while ensuring that all other users retain their restricted access based on their roles. Describe how you would implement this configuration. Write the commands.

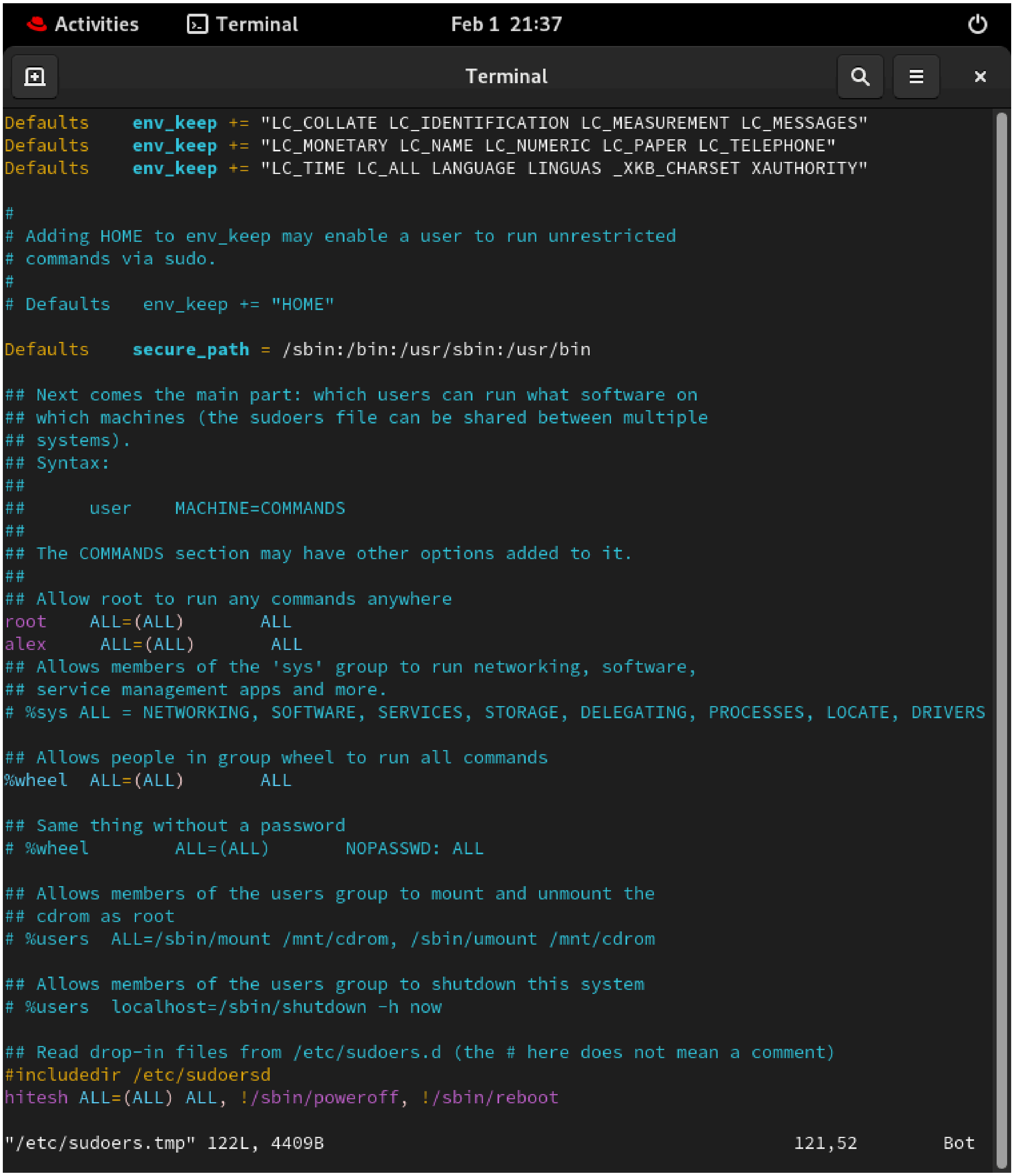


```
Defaults    env_keep =  "COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS"
Defaults    env_keep += "MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE"
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
alex     ALL=(ALL)       ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoersd
-- INSERT --                                                101,5         Bot
```

Question 9: User Hitesh, a senior team member, requires full access to the system for daily operations. However, to prevent accidental shutdowns or reboots, configure the system so that Hitesh can execute all commands xcept po

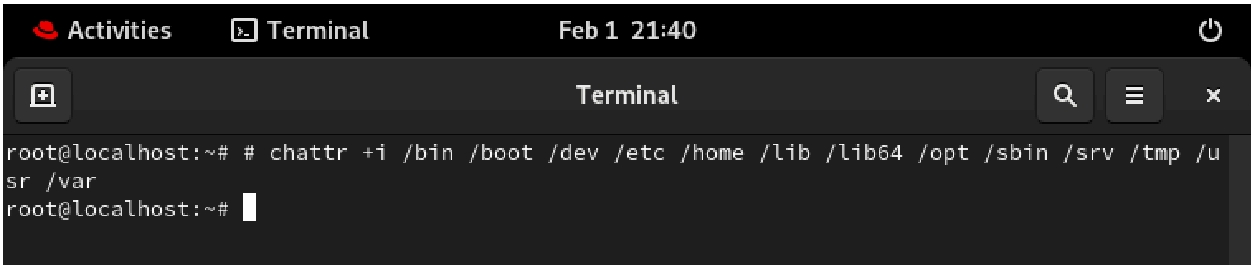


```
root@localhost:~# visudo
root@localhost:~# 
```



```
Defaults    env_keep += "LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES"
Defaults    env_keep += "LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE"
Defaults    env_keep += "LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

#
# Adding HOME to env_keep may enable a user to run unrestricted
# commands via sudo.
#
# Defaults   env_keep += "HOME"

Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
alex     ALL=(ALL)       ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoersd
hitesh ALL=(ALL) ALL, !/sbin/poweroff, !/sbin/reboot

"/etc/sudoers.tmp" 122L, 4409B                                            121,52        Bot
```

Question 10: To safeguard all-important and critical system directories, ensure they cannot be deleted or removed by the root user. Write the commands you would use to implement this protection. *Hint: (/ is a top-level file system directory



```
root@localhost:~# # chattr +i /bin /boot /dev /etc /home /lib /lib64 /opt /sbin /srv /tmp /u
sr /var
root@localhost:~# 
```