Assignment-2

Q1. Create some users:

- Named “alex” with its home directory at /home/user1 and give password “pass1”.
- Named “brew” with its home directory at /mnt/user2 and give password “pass2”.
- Named “nora” without its home directory
- Named “panny” with custom UID 2112, and assign password “pass-4”
- Named 'texas' without using the useradd or adduser commands.

*(Hint: Make changes in the 7 user configuration files)

Ans.

1. -m: Creates the home directory for the user.

2. -d /home/user1: Specifies the path for the home directory.

3. useradd: Adds the new user.

4. chpasswd: Sets the password for the user.

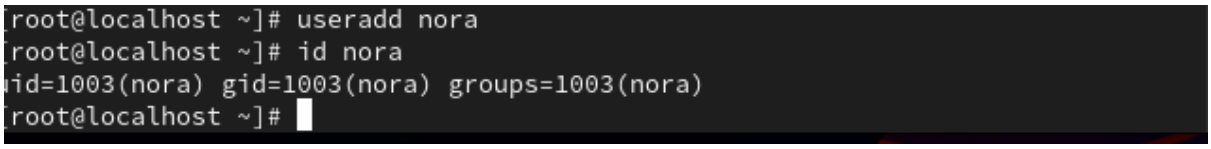
ALEX:

```
[root@localhost ~]# useradd -m -d /home/user1 alex
Creating mailbox file: File exists
[root@localhost ~]# echo "alex:pass1" | chpasswd
[root@localhost ~]# grep alex /etc/passwd
alex:x:1001:1001::/home/user1:/bin/bash
[root@localhost ~]# chmod 700 /home/user1
[root@localhost ~]#
```

BREW:

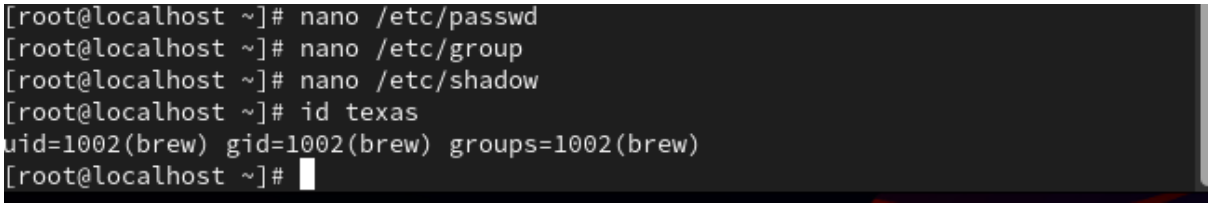
```
[root@localhost ~]# useradd -m -d /mnt/user2 brew
[root@localhost ~]# echo "brew:pass2"  | chpasswd
[root@localhost ~]# su - brew
[brew@localhost ~]$ cd
[brew@localhost ~]$ logout
[root@localhost ~]# grep brew /etc/passwd
brew:x:1002:1002::/mnt/user2:/bin/bash
[root@localhost ~]# chmod 700 /mnt/user2
[root@localhost ~]#
```

NORA:



Panny:

TEXAS:



1. Setting nano /etc/passwd :

texas:x:1002:1002::/home/texas:/bin/bash

2. Setting nano /etc/shadow:

texas:6hashed_password:19430:0:99999:7:::

3. Hashed passwd with :

opnessl passwd -6 , enter passwd as pass123 it will give u desired password.

4. Setting nano /etc/group:

texas:x:1002:

5. mkdir /home/Texas

6. chmod 700 /home/Texas

7. id texas

8. ls -ld /home/texas

Q2. Log in as user alex using the su and su - commands, and explain their differences.

Ans.

```
[root@localhost ~]# su alex
[alex@localhost root]$ logout
bash: logout: not login shell: use `exit'
[alex@localhost root]$ exit
exit
[root@localhost ~]# su - alex
[alex@localhost ~]$
```

su(Substitute user)	su – (Substitute user with login shell)
Switches to another user without changing the environment.	Switches to another user and resets the environment.
Retains the current user's environment variables.	Loads the target user's login environment (e.g., paths, variables).
You need to provide the password of the user you're switching to.	Requires the password of the target user.

3. Set a password policy for all above users with the following requirements: o The maximum password age should be 30 days, and the minimum password age should be 10 days. o Set the password expiry date for all users to December 31, 2025.

Ans.

- **Maximum** :chage -M 30 username
- **Minimum:** chage m 10 username
- **Password Expiry Date**: chage -E 2025-12-31 username
- chage -M 30 -m 10 -E 2025-12-31 username
- chage -l username

```
[root@localhost ~]# chage -M 30 -m 10 -E 2025-12-31 alex
[root@localhost ~]# chage -l alex
Last password change                                    : Jan 26, 2025
Password expires                                        : Feb 25, 2025
Password inactive                                       : never
Account expires                                         : Dec 31, 2025
Minimum number of days between password change          : 10
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
[root@localhost ~]# chage -M 30 -m 10 -E 2025-12-31 texas
[root@localhost ~]# chage -l texas
Last password change                                    : Mar 14, 2023
Password expires                                        : Apr 13, 2023
Password inactive                                       : never
Account expires                                         : Dec 31, 2025
Minimum number of days between password change          : 10
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
```

```
[root@localhost ~]# chage -M 30 -m 10 -E 2025-12-31 brew
[root@localhost ~]# chage -l brew
Last password change                                    : Jan 26, 2025
Password expires                                        : Feb 25, 2025
Password inactive                                       : never
Account expires                                         : Dec 31, 2025
Minimum number of days between password change          : 10
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
[root@localhost ~]# chage -M 30 -m 10 -E 2025-12-31 panny
[root@localhost ~]# chage -l panny
Last password change                                    : Jan 26, 2025
Password expires                                        : Feb 25, 2025
Password inactive                                       : never
Account expires                                         : Dec 31, 2025
Minimum number of days between password change          : 10
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
[root@localhost ~]#
```

```
[root@localhost ~]# chage -M 30 -m 10 -E 2025-12-31 nora
[root@localhost ~]# chage -l nora
Last password change                                    : Jan 26, 2025
Password expires                                        : Feb 25, 2025
Password inactive                                       : never
Account expires                                         : Dec 31, 2025
Minimum number of days between password change          : 10
Maximum number of days between password change          : 30
Number of days of warning before password expires       : 7
[root@localhost ~]#
```

4. Modify the user "alex":

- Add a comment: "I am alex"
- Change the UID to 2581
- Change the shell to "nologin"

Ans.

usermod -c “comment” username

usermod -u <no> username

usermod -s /sbin/nologin username

grep username /etc/passwd

```
[root@localhost ~]#  usermod -c "I am alex" alex
[root@localhost ~]#  usermod -u 2581 alex
[root@localhost ~]# usermod -s /sbin/nologin alex
[root@localhost ~]# grep alex /etc/passwd
alex:x:2581:1001:I am alex:/home/user1:/sbin/nologin
[root@localhost ~]#
```

5. Create group with following configuration:

- Named “north” with secondary group member “alex” & “texas”.
- Named “south” with GID “2222”.

Ans.

A)

```
[root@localhost ~]# groupadd north
[root@localhost ~]# usermod -aG north alex
[root@localhost ~]# usermod -aG north texas
```

```
[root@localhost ~]# groups alex
alex : alex north
[root@localhost ~]# groups texas
texas : brew north
```

B)

```
[root@localhost ~]# groupadd -g 2222 south
```

```
[root@localhost ~]# getent group south
south:x:2222:
[root@localhost ~]#
```

6.Grant user Alex administrative privileges through the wheel group so that Alex can add Panny to the admin group without requiring root access.

Ans.

1.sudo usermod -aG wheel alex

2.sudo visudo -> alex ALL=(ALL) NOPASSWD: /usr/sbin/usermod

3.sudo groupadd admin

4.sudo usermod -aG admin panny

5.sudo usermod -s /bin/bash alex(for move out to nologin shell)

6.groups alex -> alex : alex wheel north

7.groups panny -> panny : panny admin

```
[root@localhost ~]# suo usermod -aG wheel alex
bash: suo: command not found...
^C
[root@localhost ~]# sudo usermod -aG wheel alex
[root@localhost ~]# sudo visudo
[root@localhost ~]# sudo usermod -aG admin panny
usermod: group 'admin' does not exist
[root@localhost ~]# group alex
bash: group: command not found...
[root@localhost ~]# groups alex
alex : alex wheel north
[root@localhost ~]# su - alex
This account is currently not available.
[root@localhost ~]# sudo whoami
root
[root@localhost ~]# sudo groupadd admin
[root@localhost ~]# sudo usermod -aG admin panny
[root@localhost ~]# sudo usermod -s /bin/bash alex
[root@localhost ~]# sudo groupadd admin
groupadd: group 'admin' already exists
[root@localhost ~]# groups alex
alex : alex wheel north
[root@localhost ~]# groups panny
panny : panny admin
```

7. Change the group name from “south” to “dakshin”.

Ans.

```
[root@localhost ~]# groupmod -n dakshin south
[root@localhost ~]# getent group dakshin
dakshin:x:2222:
[root@localhost ~]#
```

8. Create a system user named “ping” and check its UID.

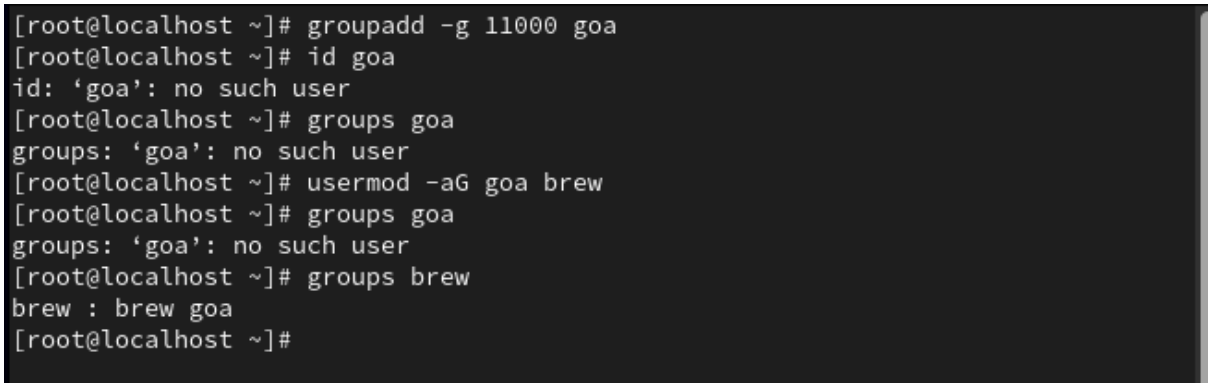
Ans.

```
[root@localhost ~]# useradd -r ping
[root@localhost ~]# id ping
uid=978(ping) gid=977(ping) groups=977(ping)
[root@localhost ~]#
```

9. Create a group named goa with GID 11000. Set this group as the supplementary group for “brew”

Ans.

1. groupadd -g 11000 goa
2. usermod -aG goa brew
3. groups brew



10.Create a group named "prod". Then, create two users, user2 and user1, and set both the user's primary group to prod.

Ans.

1.[root@localhost ~]# groupadd -r prod

2.[root@localhost ~]# useradd -g prod user1

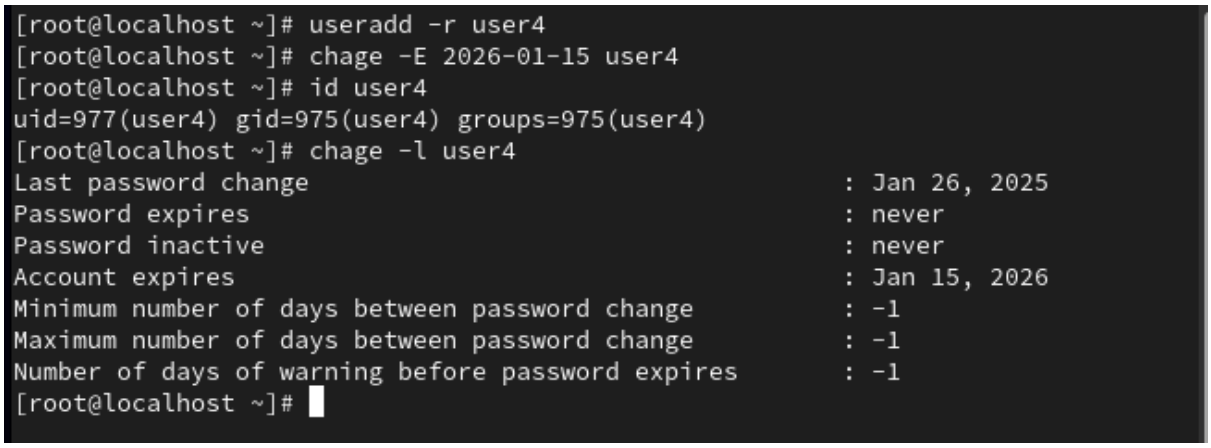
3.[root@localhost ~]# useradd -g prod user2

4.[root@localhost ~]# id user1-> uid=2584(user1) gid=976(prod) groups=976(prod)

5.[root@localhost ~]# id user2-> uid=2583(user2) gid=976(prod) groups=976(prod)

11. Change the password policy for the USER3 and USER4 accounts to expire on 2026-01-15.

Ans.



```
[root@localhost ~]# useradd -r user3
[root@localhost ~]# chage -E 2026-01-15 user3
[root@localhost ~]# chage -l user3
Last password change                                    : Jan 26, 2025
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : Jan 15, 2026
Minimum number of days between password change          : -1
Maximum number of days between password change          : -1
Number of days of warning before password expires       : -1
[root@localhost ~]#
```

12. Configure administrative rights for all members of the Goa group to execute any command as any user.

Ans.

1. sudo visudo -> %goa ALL=(ALL) ALL
2. su - brew
3. sudo whoami

```
[root@localhost ~]# su - brew
[brew@localhost ~]$ sudo whoami

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 brew:
root
[brew@localhost ~]$
```

13. How would you check all failed login attempts on the system from the last 10 days? Write the command and display the output.

Ans.

journalctl -u sshd --since "10 days ago" | grep "Failed password"

14. How would you determine how many users are currently logged into the system? Write the command to achieve this.

Ans.

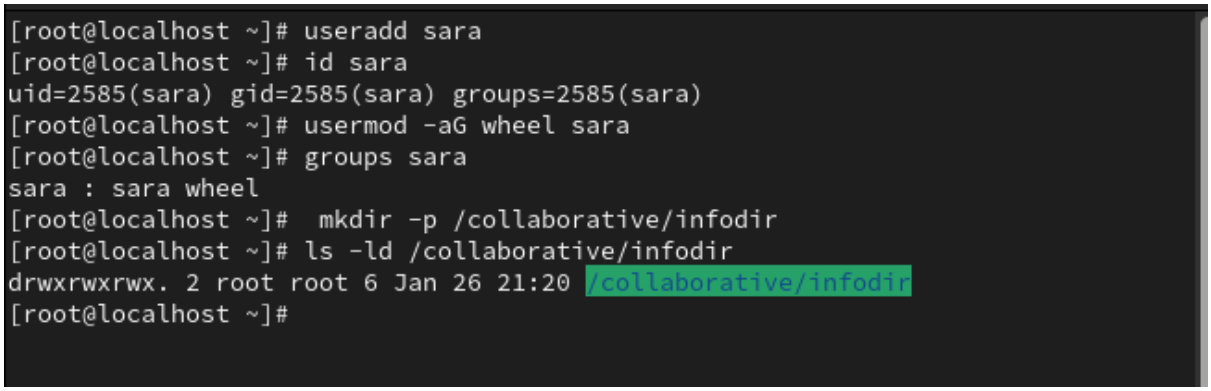
1. who | wc -l -> The who command shows a list of users currently logged in. You can count the number of users

2. w -h | wc -l -> The w command also provides information about currently

logged-in users, along with details about their activity.

15.Add the user "sara" to the "wheel" group and create a collaborative directory /collaborative/infodir.

Ans.



16. Configure login/logout messages:

- When you log in with a new user, display a message: "Hello, you are logged in as USER" (where USER is replaced with the logged-in username).

- When you log out, display: "You are logged out now".

Ans.

1. nano /home/USER/.bash_profile
2. echo "Hello, you are logged in as $(whoami)"
3. sudo nano /etc/bash.bash_logout
4. echo "You are logged out now"

17. Configure system parameters for newly created users:

- Warning period for password expiry: 5 days
- Minimum user UID: 2000
- Maximum user UID: 70000

Ans.

1. nano /etc/login.defs ->
   PASS_WARN_AGE 5
2. nano /etc/login.defs ->

   UID_MIN 2000

   UID_MAX 70000

18. Create a directory /data and configure the system so that all newly created users get /data as their home directory by default.

Ans.

```
[root@localhost ~]# mkdir /data
[root@localhost ~]# chmod 755 /data
[root@localhost ~]# nano /etc/default/useradd
[root@localhost ~]# nano /etc/adduser.conf
[root@localhost ~]# useradd testuser
[root@localhost ~]# ls -ld /data/testuser
drwx------. 3 testuser testuser 78 Jan 27 09:41 /data/testuser
[root@localhost ~]#  cat /etc/passwd | grep testuser
testuser:x:2586:2586::/data/testuser:/bin/bash
[root@localhost ~]#
```

1.mkdir /data

2. chmod 755 /data

3. nano /etc/default/useradd -> Add if not:

HOME=/data

4.nano /etc/adduser.conf ->
DIR_MODE=755, DHOMEDIR=/data

5.useradd testuser

6.ls -ld /data/testuser

7.cat /etc/passwd | grep testuser

19. Name a file where we can set a file size limit upto 200 MB for a single file.

Ans.

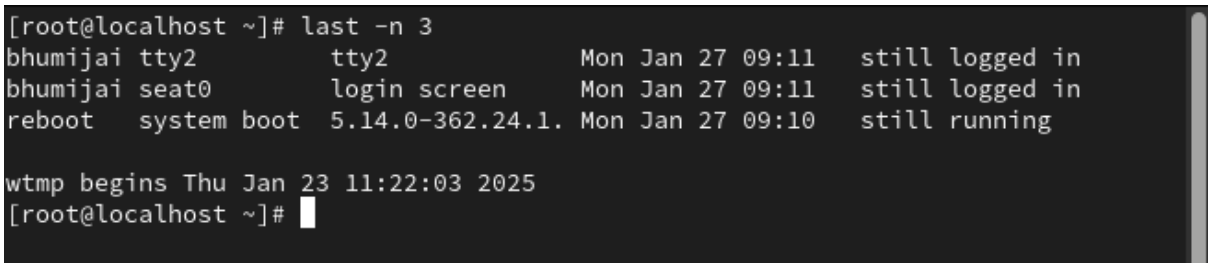
1. nano /etc/security/limits.conf -> add :

    * hard fsize 204800

2. verify by switching off and logging in

20. Check the last three users who logged into your system.

Ans.



21.As a system administrator, how would you configure the system to ensure that:

- Automatically create an instructions.txt file in the home directory of every new user upon account creation.
- Ensure that the mail directory for every newly created user is set to /home/spool/mail/ by default?"

Ans.

1. cd /etc/skel
2. echo "Welcome to the system. Please follow the instructions carefully." > instructions.txt
3. ls -l /etc/skel/instructions.txt

1. vi /etc/default/useradd ->

MAIL_DIR=/home/spool/mail

2. mkdir -p /home/spool/mail
3. hmod 755 /home/spool/mail
4. chown root:mail /home/spool/mail
5. grep "MAIL_DIR" /etc/default/useradd
6. useradd testuser
7. ls -l /home/testuser/instructions.txt
8. ls -l /home/spool/mail/testuser

22. Delete some users

Named ‘alex’ and ‘brew’ with its all data contents including mail data

Ans.