



**Points Covered in this Assignment-2**

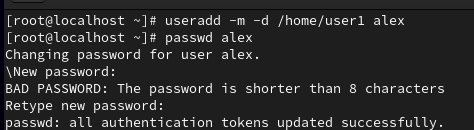
1. **User Administration** o Authentication, Authorization, and Auditing
2. **Commands to Learn** o useradd, passwd, userdel, usermod o groupadd, groupdel, groupmod o su and su -with examples
3. **User and Group Information** o User and group information files o Password information files
4. **Password Policies** o chage command and its options
5. **User Monitoring and Auditing** o Commands: w, last, lastb
6. **Sudo Power** o wheel group
7. **Default Configuration Files** o /etc/default/useradd o /etc/login.defs o /etc/security/limits.conf

1. **Create some users:** 
   * + Named **“alex”** with its home directory at **/home/user1** and give password **“pass1”.**

Command to create user:

**useradd -m -d /home/user1 alex**

**passwd alex**

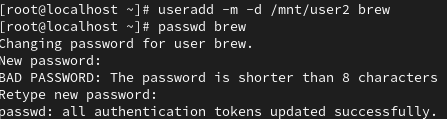
****

* + - Named **“brew”** with its home directory at **/mnt/user2** and give password **“pass2”.**

Command to create brew user with given home directory:

**useradd -m -d /mnt/user2 brew**

**passwd brew**



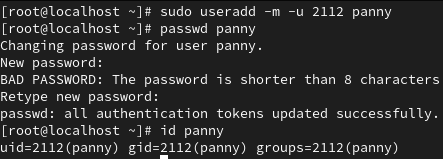
* + - Named **“nora”** without its home directory

Command to create user nora is **useradd nora**



* + - Named **“panny”** with custom UID **2112,** and assign password **“pass-4”**

Command to create user “panny” with custom UID we use -u with the specified UID to a user Command: **sudo useradd -m -u 2112 panny**



* + - Named **'texas'** without using the **useradd** or **adduser** commands.

Adding user to passwd:

**echo "texas:x:1002:1002::/home/texas:/bin/bash" | sudo tee -a /etc/passwd**

Adding user to shadow:

**echo "texas:$(openssl passwd -6 pass123):0:0:99999:7:::" | sudo tee -a /etc/shadow**

Creating home directory

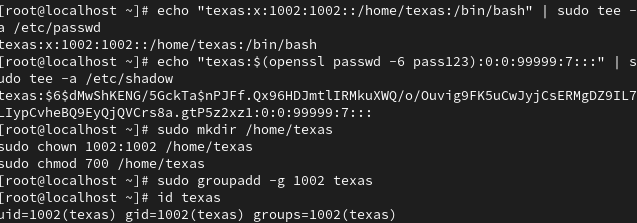
**sudo mkdir /home/texas**

**sudo chown 1002:1002 /home/texas**

**sudo chmod 700 /home/Texas**

Add Group:

**sudo groupadd -g 1002 texas**



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

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

Soln>

su = When you use su without a dash (-), it switches to the target user without loading the target user's environment.

i.e Switches to the user "alex" but keeps the current user's environment variables and working directory.

Command: su alex



su - = When you use su -, it simulates a full login shell for the target user.

Switches to the user "alex" **and** loads their full login environment, as if "alex" had logged in directly.

This command starts a new login shell for "alex," updating environment variables (e.g., PATH, HOME) and changing the working directory to "alex's" home directory.

Command: su – alex



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

Soln>

Password policy- A **password policy** is a set of rules designed to enhance the security of user accounts by enforcing good password practices.

Command for minimun password age 10 days and maximum password age 30 days:

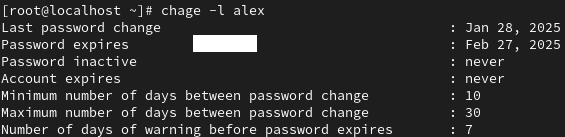
**chage -m 10 -M 30 <username> (alex)**

here,

-m -> min pass age

-M -> max pass age





1. **Modify the user "alex":** 
   * Add a comment: "I am alex"

Command: **usermod -c "I am alex" alex**

* + Change the UID to 2581

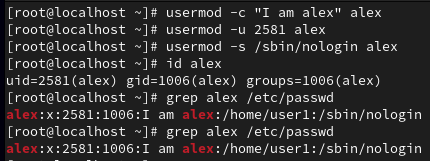
Use the -u option to change the UID to 2581

Command: **usermod -u 2581 alex**

* + Change the shell to "nologin"

use -s option

Command: **usermod -s /sbin/nologin alex**



1. Create group with following configuration:

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

Soln>

Create north group: groupadd north

Add alex and Texas to north a secondary members:

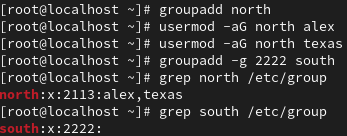
usermod -aG north alex

usermod -aG north texas

here -aG adds members to a group without removing them from previous group.

Create the "south" group with GID 2222:

groupadd -g 2222 south



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

Soln>

Ensure the "wheel" Group Has Sudo Privileges

**sudo visudo**

uncomment **%wheel ALL=(ALL) ALL**

Save and exit (:wq)

Add Alex to the "wheel" Group

**usermod -aG wheel alex**

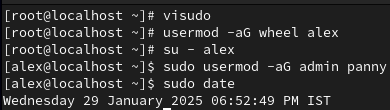
Add Panny to the "admin" group

**sudo usermod -aG admin panny**

Now check sudo previliges to alex

**su – alex**

**sudo date**

****

1. Change the group name from “**south”** to “**dakshin**”.

SOln>

**groupmod -n dakshin south**

Checking changes: grep dakshin /etc/group



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

Soln> Command: **useradd -r ping**

-r is used to create a system user

Check the UID of the User "ping": id ping

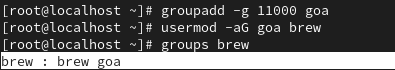


1. Create a group named **goa** with GID 11000. Set this group as the supplementary group for “**brew**”

Soln> Command: **groupadd -g 11000 goa**

Add brew to goa as supplementary group: **usermod -aG goa brew**

Verify group of brew: groups brew



1. Create a group named **“prod”**. Then, create two users, user2 and user1, and set both the user’s

primary group to **prod**.

SOln> creating group prod: **groupadd prod**

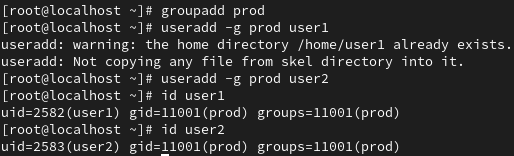
Create the Users "user1" and "user2" with "prod" as their Primary Group

**useradd -g prod user1**

**useradd -g prod user2**

verify group of users: **id user1**

**id user2**

****

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

**Soln>** USER3 and USER4 doesn’t exists so we have to create them first:

**useradd USER3**

**useradd USER4**

Use the chage Command to Set Password Expiry

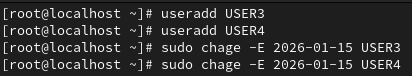
**sudo chage -E 2026-01-15 USER3**

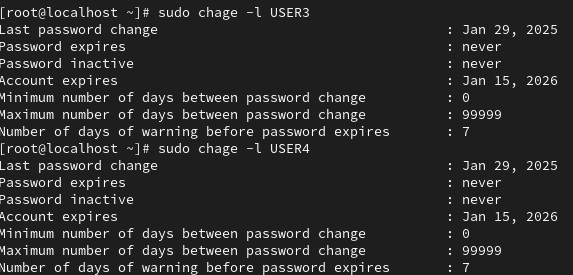
**sudo chage -E 2026-01-15 USER4**

verify password expiry date:

**sudo chage -l USER3**

**sudo chage -l USER4**

****

****

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

Soln>

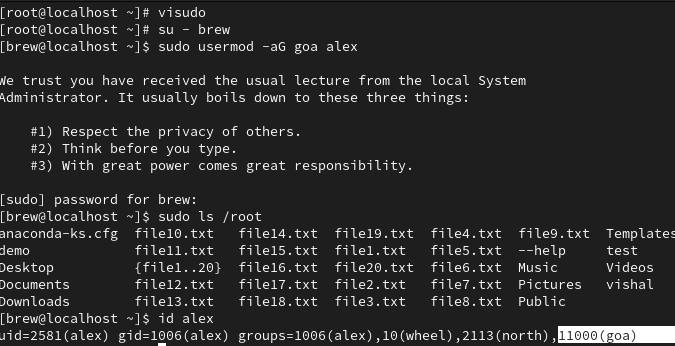
sudo visudo

%goa ALL=(ALL) ALL

Save and edit

Verify: sudo usermod -aG goa <username>

Test: sudo ls /root



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

Soln>

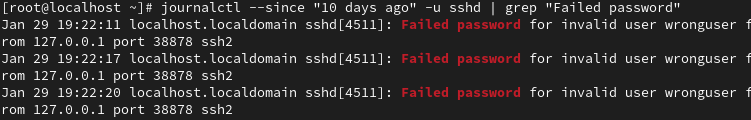
**journalctl --since "10 days ago" -u sshd | grep "Failed password"**

journalctl – fetches system logs

--since “10 days ago” – Filters logs from the last **10 days**.

-u sshd - filter logs for the SSH device

grep "Failed password" - Extracts lines containing **failed login attempts**.



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

Soln>

Command: who | wc -l

Who – Displays logged in users

wc -l – Counts the no. of lines, giving the total no. of logged-in users.



1. Add the user "**sara**" to the "wheel" group and create a collaborative directory

/collaborative/infodir.

Soln>

First add user sara: **useradd sara**

Add "sara" to the wheel group: **sudo usermod -aG wheel sara**

Change user to sara: **su - sara**

Create a collaborative directory:

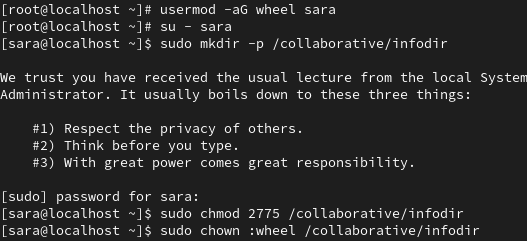
**sudo mkdir -p /collaborative/infodir**

**sudo chmod 2775 /collaborative/infodir**

**sudo chown :wheel /collaborative/infodir**

chmod 2775 → Enables group collaboration.

chown :wheel → Sets wheel as the group owner.

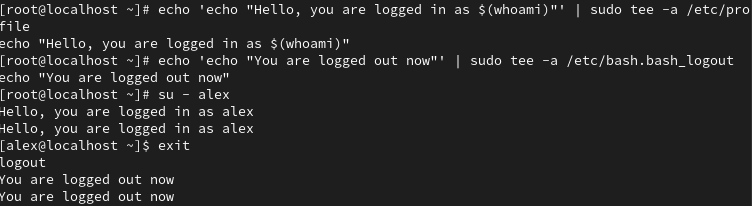


1. **Configure login/logout messages**:
   * + When you log in with a new user, display a message: "Hello, you are logged in as USER" (where USER is replaced with the logged-in username).

Soln> **echo 'echo "Hello, you are logged in as $(whoami)"' | sudo tee -a /etc/profile**

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

Soln> **echo 'echo "You are logged out now"' | sudo tee -a /etc/bash.bash\_logout**



1. **Configure system parameters for newly created users**:
   * + Warning period for password expiry: 5 days
     + Minimum user UID: 2000 o Maximum user UID: 70000

Soln>

Edit the /etc/login.defs file:

**sudo nano /etc/login.defs**

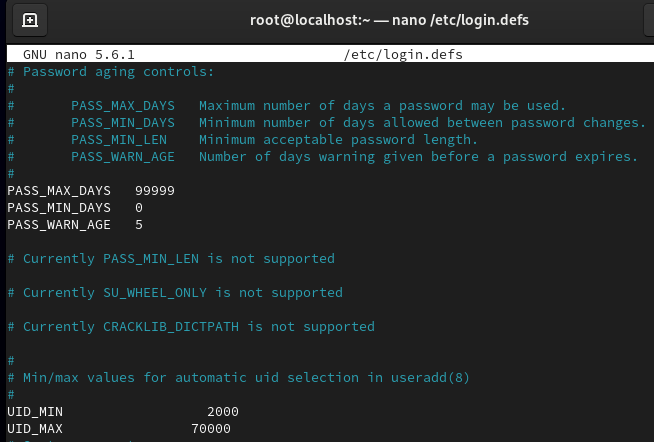
Set password expiry warning:

**PASS\_WARN\_AGE 5**

Set minimum and maximum UID:

**UID\_MIN 2000**

**UID\_MAX 70000**

****

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

Soln>

Set default home directory to /data for new users

Edit /etc/default/useradd: **nano /etc/default/useradd**

Change: **HOME=/data**

Create the /data directory:

**mkdir -p /data**

**chmod 755 /data**



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

Soln>

Edit /etc/security/limits.conf: **nano /etc/security/limits.conf**

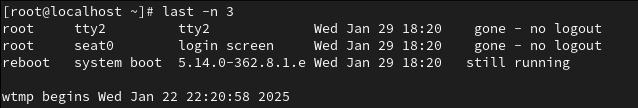
Add: **\* hard fsize 204800**

****

1. **Check the last three users** who logged into your system.

Soln>

Command: **last -n 3**

****

1. 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?"

Soln>

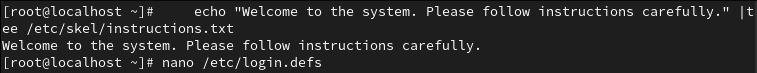
Automatically create instructions.txt in new users' home directories:

**echo "Welcome to the system. Please follow instructions carefully." |tee /etc/skel/instructions.txt**

Set default mail directory to /home/spool/mail/ Edit /etc/login.defs:

**sudo nano /etc/login.defs**

Change: **MAIL\_DIR /home/spool/mail/**



1. **Delete some users** o Named **‘alex’ and ‘brew’** with its all data contents including mail data.

Soln>

Command:

**sudo userdel -r alex**

**sudo userdel -r brew**