User and Group Permissions Setup

**3 - User and Group Permissions Setup:**

Task: Create a set of user accounts and groups with specific permissions. Develop a scenario where different users need different access to certain directories. Document the user-group permissions and provide examples of commands used to achieve this

# Scenario:

In this scenario, we have three directories - ,

**finance\_data**

, and

**marketing\_data**

. Different users from the finance and marketing departments need access to specific directories, and there's a public directory for general access.

**public\_data**

# Step 1: Create Users and Groups

## Finance Department:

**Create a Group for the Finance Department:**

sudo groupadd finance\_group

## Explanation:

The

**groupadd**

command is used to create a new group.

We create the department.

**finance\_group**

to associate users from the finance

## Create Users for the Finance Department:

sudo useradd -m -G finance\_group finance\_user1 sudo useradd -m -G finance\_group finance\_user2

**Explanation:**

The

**useradd**

command is used to add a new user.

The



**m**

The case,



**G**

option creates the user's home directory.

option adds the user to the specified supplementary group (in this

).

**finance\_group**

## Marketing Department:

**Create a Group for the Marketing Department:**

sudo groupadd marketing\_group

## Explanation:

The

**groupadd**

command is used to create a new group.

We create the department.

**marketing\_group**

to associate users from the marketing

## Create Users for the Marketing Department:

bashCopy code

sudo useradd -m -G marketing\_group marketing\_user1 sudo useradd -m -G marketing\_group marketing\_user2

**Explanation:**

The

**useradd**

command is used to add a new user.

The



**m**

The case,



**G**

option creates the user's home directory.

option adds the user to the specified supplementary group (in this

).

**marketing\_group**

# Step 2: Create Directories

sudo mkdir /finance\_data

sudo mkdir /marketing\_data sudo mkdir /public\_data

## Explanation:

The

**mkdir**

command is used to create directories.

**public\_data**

We create three directories - , represent different data storage areas.

**finance\_data**

**marketing\_data**

## Expected Output:

, and

- to

No explicit output is generated for successful directory creation.

By following these steps, we have established the necessary users, groups, and directories for our scenario. These elements will be further configured for specific access permissions in the subsequent steps.

# Step 3: Set Permissions

## Finance Data Directory:

sudo chown :finance\_group /finance\_data sudo chmod 770 /finance\_data

**Explanation:**

The directory.

**chown**

command changes the owner and/or group ownership of a file or

sets the group ownership of to .

**:finance\_group**

**/finance\_data**

**finance\_group**

The

command changes the permissions of a file or directory.

grants read (4), write (2), and execute (1) permissions to the owner and group. No permissions are granted to others.

**chmod**

**770**

## Marketing Data Directory:

bashCopy code

sudo chown :marketing\_group /marketing\_data sudo chmod 660 /marketing\_data

**Explanation:**

The

**chown**

**marketing\_group**

The

**chmod**

command changes the group ownership of to

.

**/marketing\_data**

command changes the permissions of .

**/marketing\_data**

grants read (4) and write (2) permissions to the owner and group. No permissions are granted to others.

**660**

## Public Data Directory:

bashCopy code

sudo chown :public\_group /public\_data sudo chmod 555 /public\_data

**Explanation:**

The

**chown**

**public\_group**

The

**chmod**

command changes the group ownership of to

.

**/public\_data**

command changes the permissions of .

**/public\_data**

grants read (4) and execute (1) permissions to the owner, group, and others. No write permissions are granted.

**555**

## Verification:

ls -l /

**Expected Output:**

drwxrwx--- drwxr-xr--

dr-xr-xr-x

2 root finance\_group

4096 Jan 6 12:00 finance\_

2 root marketing\_group 4096 Jan 6 12:00 marketin

2 root public\_group

4096 Jan 6 12:00 public\_d

## Explanation:

The

**ls -l**

command displays detailed information about the root directory.

The output shows the permissions, owner, group, and other details for each directory.

By setting these permissions, we have defined access levels for users belonging to different groups, ensuring secure and controlled access to the respective directories.

# Step 4: Verify Permissions

ls -l /

## Expected Output:

drwxrwx---

drwxr-xr-- dr-xr-xr-x

2 root finance\_group

4096 Jan 6 12:00 finance\_

2 root marketing\_group 4096 Jan 6 12:00 marketin

2 root public\_group

4096 Jan 6 12:00 public\_d

**Explanation:**

The

**ls -l**

command is used to list detailed information about the root directory

and its contents.

The output provides information on each directory, including permissions, owner, group, size, modification time, and name.

## Verification Process:

* 1. **Finance Data Directory:**

: The directory belongs to the

**drwxrwx---**

**finance\_group**

is owned by the root user and

. The owner and group have read, write, and

**/finance\_data**

execute permissions. Others have no permissions.

## Marketing Data Directory:

: The directory belongs to the

**drwxr-xr--**

**marketing\_group**

is owned by the root user and

. The owner has read, write, and execute

**/marketing\_data**

permissions, while the group has read-only permissions. Others have no permissions.

## Public Data Directory:

: The directory is owned by the root user and belongs

**dr-xr-xr-x**

**/public\_data**

to the . The owner, group, and others have read and execute

**public\_group**

permissions. No write permissions are granted.

## Explanation:

The output confirms that the permissions have been successfully set according to the defined scenario.

Each directory has specific access levels based on its group ownership and the permissions granted.

By verifying these permissions, you ensure that the configured access levels match the intended security requirements for each directory in the scenario. This step is crucial for confirming the effectiveness of the permission settings.