

## Solution in red color

# Instructions

## Case Scenario

- As the Linux Administrator for fast-growing company, you have been tasked with creating, modifying, and removing user accounts from the Linux server. The company has just hired 9 new employees to fill 3 newly designed departments. The departments that have been created are Engineering, Sales and IS. The server must be setup with the appropriate files, folders, users, groups and permissions to ensure a successful launch of the newly designed departments.

## Objectives

- Create a directory at the root (/) of the file system for each department. This name should reflect the department name that will use the directory.

```
root@localhost:/# mkdir Engineering Sales IS
root@localhost:/# ls
```

- Create a group for each department. This name should reflect the department name that the group will be assigned.

```
root@localhost:/# groupadd Engineering
root@localhost:/# groupadd Sales
root@localhost:/# groupadd IS
root@localhost:/# cat /etc/group
```

- Create an administrative user for each of the departments.
  - The user will have a Bash login shell.
  - The user will belong to the respective group for each department. This will need to be the user's primary group.
- Create two additional users for each department.
  - The users will have a Bash login shell.
  - The users will belong to their respective group for each department. This will need to be the user's primary group.

```
root@localhost:/# useradd -m -g Engineering Engineering-admin
root@localhost:/# useradd -m -g Engineering Engineering-user-1
root@localhost:/# useradd -m -g Engineering Engineering-user-2
root@localhost:/# useradd -m -g Sales Sales-admin
root@localhost:/# useradd -m -g Sales Sales-user-1
root@localhost:/# useradd -m -g Sales Sales-user-2
root@localhost:/# useradd -m -g IS IS-admin
root@localhost:/# useradd -m -g IS IS-user-1
root@localhost:/# useradd -m -g IS IS-user-2
```

## Solution in red color

- For security reasons, the following modifications will need to be made to each of the departments' respective directories:
  - Ensure that the owner of each of the directories is the department administrator and the group ownership is the group for each department.

```
root@localhost:/# chown Engineering-admin:Engineering /Engineering
```

```
root@localhost:/# chown Sales-admin:Sales /Sales
```

```
root@localhost:/# chown IS-admin:IS /IS
```

- The department administrator will have full access to their respective department directories.

```
root@localhost:/# ls -l
```

**the department admin already have full access**

- Ensure that only the owner of a file in the department's directory can delete the file. The user will also have ownership of their respective department folders.
- Normal users in each department will have full access (Read, Write and Execute) to their respective department folders.
- The department folders will ONLY be accessible by users/administrators in each of the respective departments. Ensure that no one else will have permissions to the folders.

```
root@localhost:/# chmod 1770 /Engineering
```

```
root@localhost:/# chmod 1770 /Sales
```

```
root@localhost:/# chmod 1770 /IS
```

- Create a document in each of the department directories.
  - The ownerships on this file will be the same as the directory it is located in.
  - The document should contain only one line of text that states, "This file contains confidential information for the department."
  - This file can be read by any user in the department, but can only be modified by the department administrator. No one else has permissions to this file.

```
root@localhost:/# echo "This file contains confidential information for the  
department." > /Engineering/document.txt
```

```
root@localhost:/# echo "This file contains confidential information for the  
department." > /Sales/document.txt
```

```
root@localhost:/# echo "This file contains confidential information for the  
department." > /IS/document.txt
```

```
root@localhost:/# chown Engineering-admin:Engineering  
/Engineering/document.txt
```

```
root@localhost:/# chown Sales-admin:Sales /Sales/document.txt
```

## Solution in red color

```
root@localhost:/# chown IS-admin:IS /IS/document.txt
```

```
root@localhost:/# chmod 740 /Engineering/document.txt
```

```
root@localhost:/# chmod 740 /Sales/document.txt
```

```
root@localhost:/# chmod 740 /Sales/document.txt
```

## Curriculum Resources

- Module 8 – Managing Files and Directories
- Module 15 – System and User Security
- Module 16 – Creating Users and Groups
- Module 17 – Ownership and Permissions
- Module 18 – Special Directories and Files

## Deliverables

- Use the appropriate command to verify each user and group has been created.

```
root@localhost:/# cat /etc/group
```

- Use the appropriate command to verify each user's group assignment.

```
root@localhost:/# ls -l
```

- Use the appropriate command to verify the directory creation and the permission settings.

```
root@localhost:/# ls -l
```

- Use the appropriate command to verify the files are created in their respective directories.

```
root@localhost:/# ls -l /Engineering
```

```
root@localhost:/# ls -l /Sales
```

```
root@localhost:/# ls -l /IS
```