1. Create a user account with the following attribute

- username: islam
- Fullname/comment: Islam Askar
- Password: islam

```
[ghada@localhost ~]$ su -
Password:
[root@localhost ~]# useradd -c "Islam Bakr" -md /home/islam islam
[root@localhost ~]#
```

```
[root@localhost ~]# passwd islam
Changing password for user islam.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

2. Create a user account with the following attribute

- Username: baduser
- Full name/comment: Bad User
- Password: baduser

```
[root@localhost ~]# useradd -c "Bad User" -md /home/baduser baduser
[root@localhost ~]# passwd baduser
Changing password for user baduser.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

3. Create a supplementary (Secondary) group called pgroup with group ID of 30000

```
[root@localhost ~]# groupadd -g 3000 pgroup
```

4. Create a supplementary group called badgroup

```
[root@localhost ~]# groupadd badgroup
```

5. Add islam user to the pgroup group as a supplementary group

```
[root@localhost ~]# usermod -G pgroup islam
[root@localhost ~]# id islam
uid=1001(islam) gid=1001(islam) groups=1001(islam),3000(pgroup)
```

6. Modify the password of islam's account to password

```
[islam@localhost root]$ passwd
Changing password for user islam.
Current password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

7. Modify islam's account so the password expires after 30 days.

```
[root@localhost ~]# chage -M 30 islam
```

8. Lock bad user account so he can't log in

```
[root@localhost ~]# usermod -L baduser
```

9. Delete bad user account

```
[root@localhost ~]# userdel baduser
```

10. Delete the supplementary group called badgroup.

```
[root@localhost ~]# groupdel badgroup
```