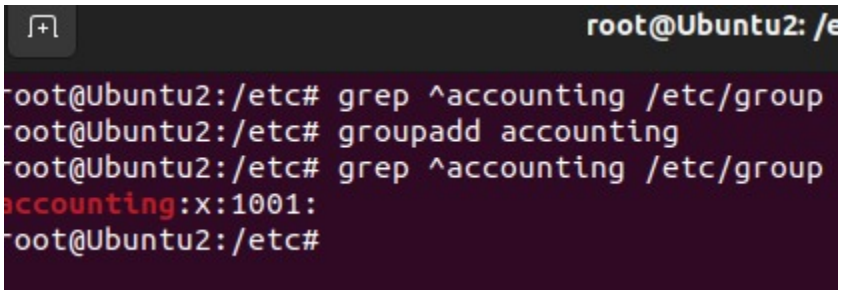
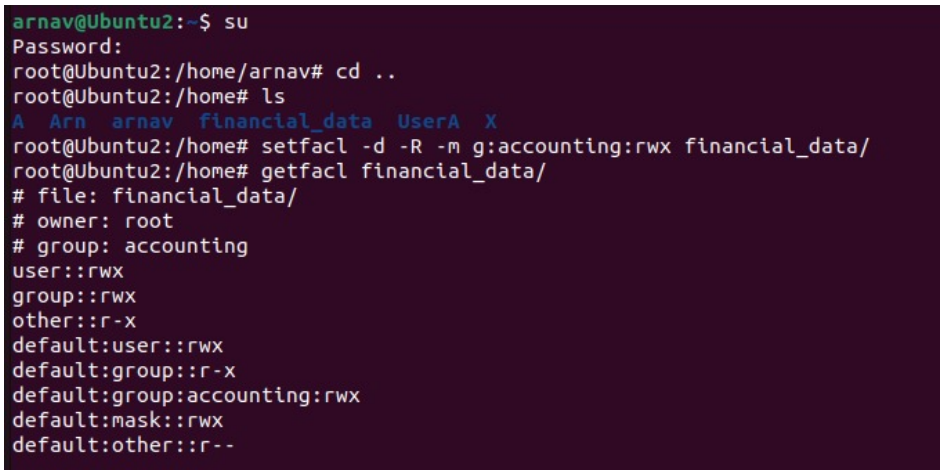
FCS Question 2

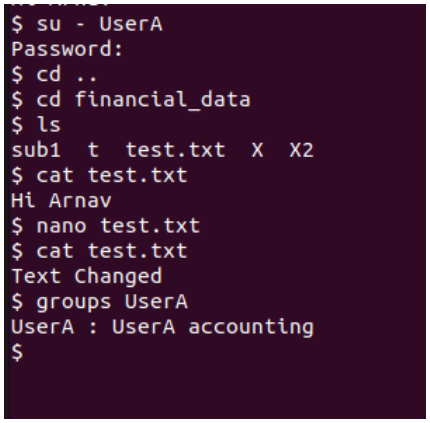
Our first step is to create a new group called accounting.



1)a)Now we create a directory called financial_data in the home directory. We change the ownership of this directory to accounting group. Now we use the setfacl to change the acl for the financial_data. The -d flag is to specify the default ACL, -R to apply the changes recursively and -m to modify the ACL. The below command gives Read-Write-Execute permissions to accounting group for financial data and its contents.



2)a) Now we show that UserA(accounting group) has read-write access to financial_data using test.txt whose text is changed by this user. We also demonstrate that UserA really belongs to group accounting.



1)b)The next step is to ensure all other groups and users have only read access to financial_data using the setfacl command.

```
arnav@Ubuntu2:~$ su
Password:
root@Ubuntu2:/home/arnav# cd ..
root@Ubuntu2:/home# setfacl -d -R -m o::rx financial_data
root@Ubuntu2:/home# getfacl financial_data/
# file: financial_data/
# owner: root
# group: accounting
user::rwx
group::rwx
other::r-x
default:user::rwx
default:group::r-x
default:group:accounting:rwx
default:mask::rwx
default:other::r-x
```

We demonstrate the read access for a User called X who doesnt belong to the accounting group. He can neither create a new file nor cd into any of the subdirectories but he can view contents of the text files which shows his read access to contents of financial_data.

```
root@Ubuntu2: /home
$ su - X
Password:
$ groups X
X : X
$ cd ..
$ cd financial_data
$ ls
sub1  t  test.txt
$ touch t.txt
touch: cannot touch 't.txt': Permission denied
$ cat test.txt
Text changed
$ cat t
ad
$ cd sub1
-sh: 8: cd: can't cd to sub1
$
```

1)c) & 2)c)Now we demonstrate how any directory inside the financial data folder inherits these ACL settings of the parent directory. We ensured this by specifying the -R flag which applies these ACL settings recursively. We demonstrate by the below screenshot. The ACL for the sub1 subdirectory is the same as the ACL for the parent financial_data directory.

```
$ getfacl sub1
# file: sub1
# owner: UserA
# group: UserA
user::rwx
group::r-x
group:accounting:rw-
mask::rwx
other::r--
default:user::rwx
default:group::r-x
default:group:accounting:rwx
default:mask::rwx
default:other::r-x
```

3)

We try to give a UserB from tempAccess group access to a subdirectory called tempDir in the financial_data directory. These are the steps-

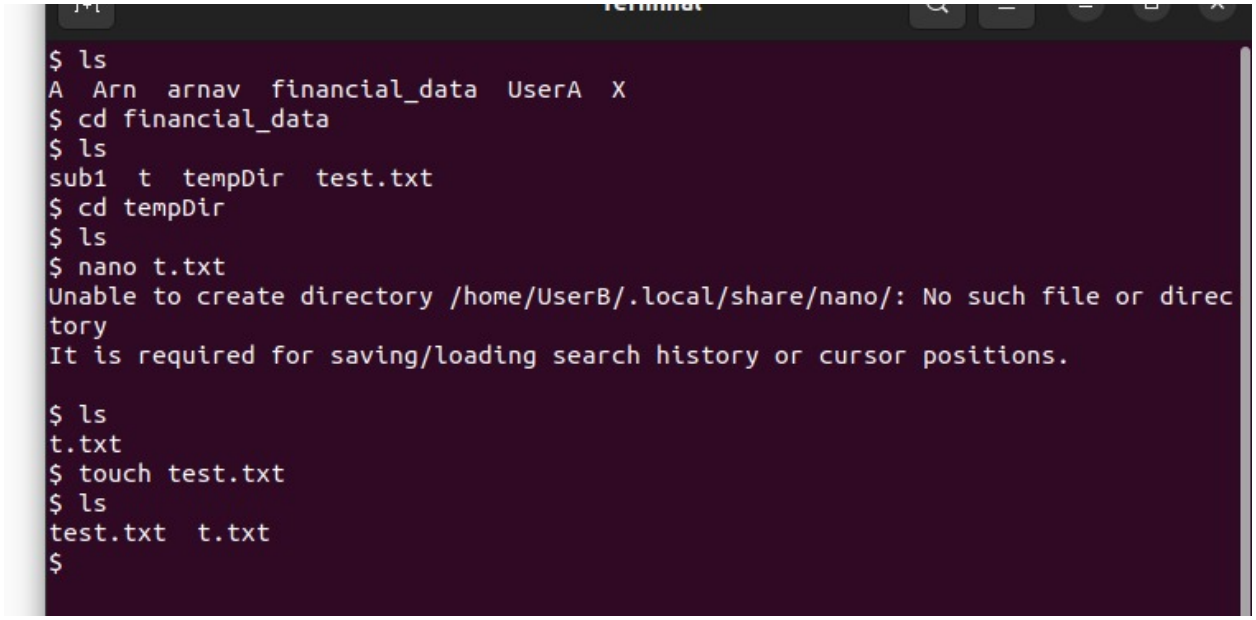
1)Use setfacl to set up the read-write-execute access to directory tempDir for group tempAccess. getfacl confirms that the changes were applied.

```
root@Ubuntu2:/home# sudo useradd UserB
root@Ubuntu2:/home# sudo passwd UserB
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
root@Ubuntu2:/home# sudo groupadd tempAccess
root@Ubuntu2:/home# usermod -aG tempAccess UserB
root@Ubuntu2:/home#
```

```
root@Ubuntu2:/home/financial_data# mkdir tempDir
root@Ubuntu2:/home/financial_data# setfacl -m g:tempAccess:rwx tempDir
root@Ubuntu2:/home/financial_data# ls
sub1  t  tempDir  test.txt
root@Ubuntu2:/home/financial_data# getfacl tempDir
# file: tempDir
# owner: root
# group: root
user::rwx
group::r-x
group:accounting:rwx
group:tempAccess:rwx
mask::rwx
other::r-x
default:user::rwx
default:group::r-x
default:group:accounting:rwx
default:mask::rwx
default:other::r-x

root@Ubuntu2:/home/financial_data#
```

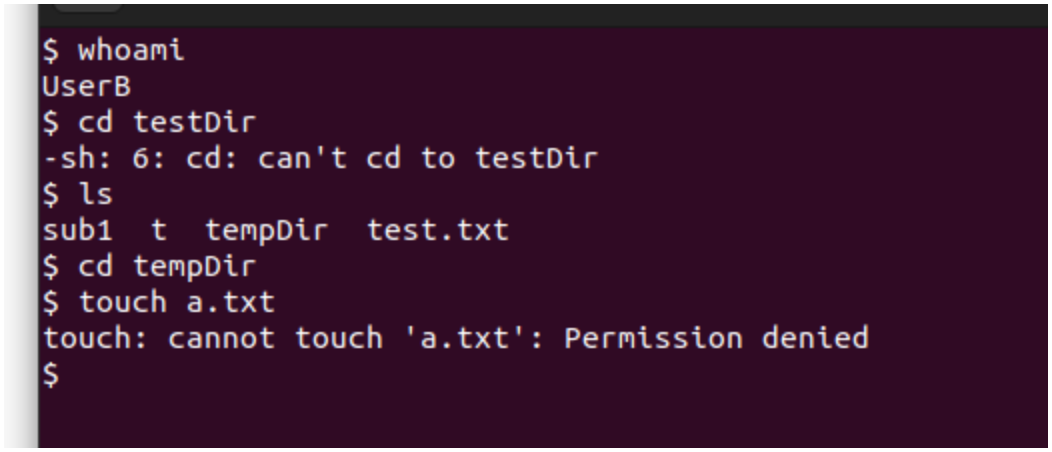
2)Now demonstrate newly acquired read write access to tempDir directory for userB by creating a new text file test.txt in this subdirectory.



3)Now revoke access for this group using the -x flag in setfacl.We confirm that the changes were applied using the getfacl command.

```
arnav@Ubuntu2:~$ su
Password:
root@Ubuntu2:/home/arnav# cd ..
root@Ubuntu2:/home# cd financial_data
root@Ubuntu2:/home/financial_data# setfacl -x g:tempAccess tempDir
root@Ubuntu2:/home/financial_data# getfacl tempDir/
# file: tempDir/
# owner: root
# group: root
user::rwx
group::r-x
group:accounting:rwx
mask::rwx
other::r-x
default:user::rwx
default:group::r-x
default:group:accounting:rwx
default:mask::rwx
default:other::r-x
```

4)We demonstrate that the access has been revoked, UserB should only have read-execute access on this tempDir like other non-accounting users. We notice that the UserB can no longer create a new text file using touch command but it has read access to the files like other users.


$ whoami
UserB
$ cd testDir
-sh: 6: cd: can't cd to testDir
$ ls
sub1 t tempDir test.txt
$ cd tempDir
$ touch a.txt
touch: cannot touch 'a.txt': Permission denied
$