Assignment 9

Access Control List - Use Case

Use Case 1 : Create a use case where , you set permission on facl/facl_file1.txt and facl/facl_file2.txt , create a grp facl_grp , create 2 user underneath user1_facl and user2_facl , this group should be given permission in a way that any user belongs to this group can edit the mentioned 2 files.

Point 1: Make directory facl and file facl_file1.txt and facl_file2.txt. Check permission for it.

```
bhushan@ubuntu:/home$ sudo mkdir facl
bhushan@ubuntu:/home$ cd facl
bhushan@ubuntu:/home/facl$ sudo touch facl_file{1..2}.txt
bhushan@ubuntu:/home/facl$ ls -la
total 8
drwxr-xr-x 2 root root 4096 Feb 10 02:14 .
drwxr-xr-x 6 root root 4096 Feb 10 02:13 ..
-rw-r--r-- 1 root root    0 Feb 10 02:14 facl_file1.txt
-rw-r--r-- 1 root root    0 Feb 10 02:14 facl_file2.txt
bhushan@ubuntu:/home/facl$ cd ..
bhushan@ubuntu:/home$
```

Point 2: If we want to check details of files or directory we use getfacl. Getfacl gives us complete listing of all regular permissions and access control lists permissions on a file or directory.

```
bhushan@ubuntu:/home$ getfacl facl
# file: facl
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

bhushan@ubuntu:/home$ cd facl
bhushan@ubuntu:/home/facl$ getfacl facl_file1.txt
# file: facl_file1.txt
# owner: root
# group: root
user::rw-
group::r--
other::r--

bhushan@ubuntu:/home/facl$ getfacl facl_file2.txt
# file: facl_file2.txt
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

Point 3: Now, create facl_grp and if we check currently there are no users inside this group.

```
bhushan@ubuntu:/home/facl$ sudo groupadd facl_grp
bhushan@ubuntu:/home/facl$ sudo /etc/group
sudo: /etc/group: command not found
bhushan@ubuntu:/home/facl$ sudo cat /etc/group
```

```
facl_grp:x:1005:
bhushan@ubuntu:/home/facl$ sudo cat /etc/group | grep facl_grp
facl_grp:x:1005:
bhushan@ubuntu:/home/facl$
```

Point 4: Create 2 users having the names user1_facl and user2_facl.

```
bhushan@ubuntu:/home$ sudo adduser user1_facl
Adding user `user1_facl' ...
Adding new group `user1_facl' (1006) ...
Adding new user `user1_facl' (1003) with group `user1_facl' ...
Creating home directory `/home/user1_facl' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user1_facl
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
bhushan@ubuntu:/home$ sudo adduser user2_facl
Adding user `user2_facl' ...
Adding new group `user2_facl' (1007) ...
Adding new user `user2_facl' (1004) with group `user2_facl' ...
Creating home directory `/home/user2_facl' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user2_facl
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
bhushan@ubuntu:/home$
```

```
bhushan@ubuntu:/home$ ls -la
total 252
drwxr-xr-x  8 root       root         4096 Feb 10 02:33 .
drwxr-xr-x 22 root       root         4096 Feb  9 11:24 ..
drwxr-xr-x  2 angular    devops       4096 Feb  6 02:46 angular
-rw-r--r--  1 root       root       219610 Feb  6 03:21 ass5.txt
drwxr-xr-x 20 bhushan    bhushan      4096 Feb  9 22:38 bhushan
drwxr-xr-x  2 devops     devops       4096 Feb  6 03:10 devops
drwxr-xr-x  2 root       root         4096 Feb 10 02:14 facl
drwxr-xr-x  2 user1_facl user1_facl   4096 Feb 10 02:33 user1_facl
drwxr-xr-x  2 user2_facl user2_facl   4096 Feb 10 02:33 user2_facl
bhushan@ubuntu:/home$
```

Point 5: First we change the primary group of both users.

```
bhushan@ubuntu:/home$ sudo chown :facl_grp user1_facl
bhushan@ubuntu:/home$ sudo chown :facl_grp user2_facl
bhushan@ubuntu:/home$ getfacl user1_facl
# file: user1_facl
# owner: user1_facl
# group: facl_grp
user::rwx
group::r-x
other::r-x

bhushan@ubuntu:/home$ getfacl user2_facl
# file: user2_facl
# owner: user2_facl
# group: facl_grp
user::rwx
group::r-x
other::r-x

bhushan@ubuntu:/home$ ls -la
total 252
drwxr-xr-x  8 root       root       4096 Feb 10 02:33 .
drwxr-xr-x 22 root       root       4096 Feb  9 11:24 ..
drwxr-xr-x  2 angular    devops     4096 Feb  6 02:46 angular
-rw-r--r--  1 root       root     219610 Feb  6 03:21 ass5.txt
drwxr-xr-x 20 bhushan    bhushan    4096 Feb  9 22:38 bhushan
drwxr-xr-x  2 devops     devops     4096 Feb  6 03:10 devops
drwxr-xr-x  2 root       root       4096 Feb 10 02:14 facl
drwxr-xr-x  2 user1_facl facl_grp   4096 Feb 10 02:33 user1_facl
drwxr-xr-x  2 user2_facl facl_grp   4096 Feb 10 02:33 user2_facl
bhushan@ubuntu:/home$
```

Point 6: Add user1_facl and user2_facl user's in the facl_grp group.

```
bhushan@ubuntu:/home$ sudo adduser user1_facl facl_grp
Adding user `user1_facl' to group `facl_grp' ...
Adding user user1_facl to group facl_grp
Done.
bhushan@ubuntu:/home$ sudo adduser user2_facl facl_grp
Adding user `user2_facl' to group `facl_grp' ...
Adding user user2_facl to group facl_grp
Done.
bhushan@ubuntu:/home$
```

```
bhushan@ubuntu:/home$ sudo cat /etc/group | grep user1_facl
facl_grp:x:1005:user1_facl,user2_facl
user1_facl:x:1006:
bhushan@ubuntu:/home$ sudo cat /etc/group | grep user2_facl
facl_grp:x:1005:user1_facl,user2_facl
user2_facl:x:1007:
bhushan@ubuntu:/home$
```

Point 7: If we are trying to modify the facl_file1.txt and facl_file2.txt from user1_facl as this user is present in the facl_grp then user1_facl is unable to modify the file.

```
~
~
~
~
"facl/facl_fil1.txt"
"facl/facl_fil1.txt" E212: Can't open file for writing
Press ENTER or type command to continue
```

Point 8: So to solve the above problem we have an Access Control List. So to provide the permission to specific directory or file we use setfacl command. Now we provide access to the group so that whatever user present in that group can access or modify the file.

```
bhushan@ubuntu:/home$ getfacl facl
# file: facl
# owner: root
# group: root
user::rwx
group::r-x
other::r-x

bhushan@ubuntu:/home$ sudo setfacl -m g:facl_grp:rwx facl
[sudo] password for bhushan:
bhushan@ubuntu:/home$ getfacl facl
# file: facl
# owner: root
# group: root
user::rwx
group::r-x
group:facl_grp:rwx
mask::rwx
other::r-x
```

```
user1_facl@ubuntu:/home$ vi /home/facl/facl_file1.txt
user1_facl@ubuntu:/home$ cat /home/facl/facl_file1.txt
Trying to modify the facl_file1.txt using user1_facl as this user is in the facl_grp!

user1_facl@ubuntu:/home$
```

```
bhushan@ubuntu:~$ su user2_facl
Password:
user2_facl@ubuntu:/home/bhushan$ cd ~
user2_facl@ubuntu:~$ vi /home/facl/facl_file1.txt
user2_facl@ubuntu:~$ vi /home/facl/facl_file1.txt
user2_facl@ubuntu:~$ cat /home/facl/facl_file1.txt
Trying to modify the facl_file1.txt using user1_facl as this user is in the facl_grp!


Trying to modify the facl_file1.txt using user2_facl as this user is in the facl_grp!
user2_facl@ubuntu:~$
```

Point 9 : For more clarification we add angular user to facl_grp and modify the facl_file1.txt file. Angular user are able to modify the file.

```
bhushan@ubuntu:/home$ sudo adduser angular facl_grp
Adding user `angular' to group `facl_grp' ...
Adding user angular to group facl_grp
Done.
```

```
bhushan@ubuntu:/home$ su angular
Password:
angular@ubuntu:/home$ vi /home/facl/facl_file1.txt
angular@ubuntu:/home$ cat /home/facl/facl_file1.txt
Trying to modify the facl_file1.txt using user1_facl as this user is in the facl_grp!


Trying to modify the facl_file1.txt using user2_facl as this user is in the facl_grp!


For More Clarification we add angular existing user to facl_grp and then trying to modify the facl_file1.txt!

angular@ubuntu:/home$
```

Point 10: If we want to delete the existing access control lists on directories then we use setfacl command with -b argument.

```
bhushan@ubuntu:/home$ setfacl -b facl
setfacl: facl: Operation not permitted
bhushan@ubuntu:/home$ sudo setfacl -b facl
bhushan@ubuntu:/home$ ls -la
total 252
drwxr-xr-x  8 root       root       4096 Feb 10 02:33 .
drwxr-xr-x 22 root       root       4096 Feb  9 11:24 ..
drwxr-xr-x  2 angular    devops     4096 Feb 10 03:46 angular
-rw-r--r--  1 root       root     219610 Feb  6 03:21 ass5.txt
drwxr-xr-x 20 bhushan    bhushan    4096 Feb  9 22:38 bhushan
drwxr-xr-x  2 devops     devops     4096 Feb  6 03:10 devops
drwxr-xr-x  2 root       root       4096 Feb 10 03:46 facl
drwxr-xr-x  2 user1_facl facl_grp   4096 Feb 10 03:31 user1_facl
drwxr-xr-x  2 user2_facl facl_grp   4096 Feb 10 03:40 user2_facl
bhushan@ubuntu:/home$ getfacl facl
# file: facl
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
```

Use Case 2: Consider there are 2 groups india and aus. In the india group there are 3 users are rohit, virat and prithvi. Similarly, In aus group there are 2 users are there ricky and mark.

```
bhushan@ubuntu:/home$ sudo cat /etc/group | grep india
india:x:1008:prithvi,virat,rohit
bhushan@ubuntu:/home$ sudo cat /etc/group | grep aus
aus:x:1009:ricky,mark
bhushan@ubuntu:/home$
```

Point 1: In home there is one file i.e file1.txt. Check the details permission of it.

```
bhushan@ubuntu:/home$ ls
angular   bhushan  file1.txt  mark     ricky  virat
ass5.txt  devops   iccevents  prithvi  rohit
bhushan@ubuntu:/home$ getfacl file1.txt
# file: file1.txt
# owner: prithvi
# group: india
user::rw-
group::r--
other::r--
```

Point 2: If we login with a prithvi user and try to modify the file1.txt then the prithvi user is not able to modify it. Prithvi users only read the file as groups have only read permission.

```
"/home/file1.txt"
"/home/file1.txt" E212: Can't open file for writing
Press ENTER or type command to continue
```

If we login with a virat user and try to modify the file1.txt then the virat user is not able to modify it. Virat user only reads the file as group has only read permission.

```
"/home/file1.txt"
"/home/file1.txt" E212: Can't open file for writing
Press ENTER or type command to continue
```

Point 3: There is no ACL set on the file1.txt user owner is root and group owner is india. User owner has read and write permission and the group owner has read permission. It means that member of the inida group can only be read the contents of file1.txt. Now let's check who are the members of the linux group. Prithvi, virat and rohit is the member of the india group and one of the member prithvi is the owner of the file1.txt.

```
bhushan@ubuntu:/home$ sudo cat /etc/group | grep india
[sudo] password for bhushan:
india:x:1008:prithvi,virat,rohit
bhushan@ubuntu:/home$
```

Point 4: Login with virat user since virat is the member of the india group he can only read the file. But if we try to modify the file it will pop up the error.

```
virat@ubuntu:~$ cat /home/file1.txt
Try
virat@ubuntu:~$
```

```
"/home/file1.txt"
"/home/file1.txt" E212: Can't open file for writing
Press ENTER or type command to continue
```

Point 5: User virat misbehaved and as admin we don't want to allow any access to file1.txt but at the same time we dont want to remove user virat from india group. So this is done with the help of setfacl command to restrict virat while any members not affecting the group india.

```
bhushan@ubuntu:/home$ sudo setfacl -m u:virat:--- file1.txt
[sudo] password for bhushan:
bhushan@ubuntu:/home$ getfacl file1.txt
# file: file1.txt
# owner: prithvi
# group: india
user::rw-
user:virat:---
group::r--
mask::r--
other::r--
```

So virat users have no permission. Login with virat user and try to access the file1.txt virat user unable to access it.

```
virat@ubuntu:~$ cat /home/file1.txt
cat: /home/file1.txt: Permission denied
```

Whereas we login with rohit. Rohit is the member of the india group. So if Rohit tries to read the content of the file1.txt then he can read the content because the group has read permission.

```
bhushan@ubuntu:/home$ su rohit
Password:
rohit@ubuntu:/home$ cd ~
rohit@ubuntu:~$ cat /home/file1.txt
Try
rohit@ubuntu:~$
```

Point 6: Now, if we want to remove the ACL from the file then we setfacl command with -b argument.

```
bhushan@ubuntu:/home$ sudo setfacl -b file1.txt
bhushan@ubuntu:/home$ getfacl file1.txt
# file: file1.txt
# owner: prithvi
# group: india
user::rw-
group::r--
other::r--
```

We removed ACL and revoke virat permission so now virat user able to read the content of the file.

```
virat@ubuntu:~$ cat /home/file1.txt
Try
```

Use CAse 3: We also grant certain specific permission to group also. So we grant specific permission to group aus. We have aus group in which 2 users are there, Ricky and mark.

```
bhushan@ubuntu:/home$ sudo cat /etc/group | grep aus
aus:x:1009:ricky,mark
```

Point 1: As of now they are part of other as far as file1.txt is concerned. So login with ricky user and try to read the content of file1.txt. Ricky user are only able to read the content of the file1.txt but not able to modify it. As other have only read permission.

```
bhushan@ubuntu:~$ su ricky
Password:
ricky@ubuntu:/home/bhushan$ cd ~
ricky@ubuntu:~$ cat /home/file1.txt
Try
ricky@ubuntu:~$ vi /home/file1.txt
```

```
"/home/file1.txt"
"/home/file1.txt" E212: Can't open file for writing
Press ENTER or type command to continue
```

Similarly with mark user. So login with mark user and try to read the content of file1.txt. Mark user are only able to read the content of the file1.txt but not able to modify it. As other have only read permission.

```
bhushan@ubuntu:/home$ su mark
Password:
mark@ubuntu:/home$ cd ~
mark@ubuntu:~$ cat /home/file1.txt
Try
```

```
"/home/file1.txt"
"/home/file1.txt" E212: Can't open file for writing
Press ENTER or type command to continue
```

Point 2: Now we set the permission to group aus with the help of setfacl.

```
bhushan@ubuntu:/home$ sudo setfacl -m g:aus:rw file1.txt
bhushan@ubuntu:/home$ getfacl file1.txt
# file: file1.txt
# owner: prithvi
# group: india
user::rw-
group::r--
group:aus:rw-
mask::rw-
other::r--
```

Point 3: Now login with user ricky and try to read the content of file1.txt. Ricky user are now able to read the content of the file1.txt as well as able to modify it as the group have rw permission.

```
ricky@ubuntu:~$ vi /home/file1.txt
ricky@ubuntu:~$ cat /home/file1.txt
Try to modify the file1.txt after seting the permission. So Ricky user are able
to modify it !
ricky@ubuntu:~$
```

Point 4: If we want to remove the ACL then we use setfacl command with -b argument.

```
bhushan@ubuntu:/home$ sudo setfacl -b file1.txt
bhushan@ubuntu:/home$ getfacl file1.txt
# file: file1.txt
# owner: prithvi
# group: india
user::rw-
group::r--
other::r--
```