Exercise 35.3   Using Access Control Lists

1. Create a file using your usual user name and run **getfacl** on it to see its properties.

2. Create a new user account with default properties (or reuse one from previous exercises.

3. Login as that user and try to add a line to the file you created in the first step. This should fail.

4. User **setfacl** to make the file readable by the new user and try again.

5. User **setfacl** to make the file not readable by the new user and try again.

6. Clean up as necessary

Solution 35.3

It is probably easiest to open two terminal windows, one to work in as your normal user account, and the other as the secondary one.

1. In window 1:

```
$ echo This is a file > /tmp/afile
$ getfacl /tmp/afile

getfacl: Removing leading '/' from absolute path names
# file: tmp/afile
# owner: coop
# group: coop
user::rw-
group::rw-
other::r--
```

2. In window 1:

```
$ sudo useradd fool
$ sudo passwd fool
...
```

3. In window 2:

```
$ sudo su - fool
$ echo another line > /tmp/afile

-bash: /tmp/afile: Permission denied
```

4. In window 1:

```
$ setfacl -m u:fool:rx /tmp/afile
$ getfacl /tmp/afile

getfacl: Removing leading '/' from absolute path names
# file: tmp/afile
# owner: coop
# group: coop
user::rw-
user:fool:r-x
group::rw-
mask::rwx
other::r--
```

In window 2:

```
$ echo another line > /tmp/afile
```

5. In window 1:

```
$ setfacl -m u:fool:rx /tmp/afile
```

In window 2:

```
$ echo another line > /tmp/afile
-bash: /tmp/afile: Permission denied
```

6. Cleaning up:

```
$ rm /tmp/afile
$ sudo userdel -r fool
```