Computer Science 530 - Lab Assignment #3 -- Fall 2021

Due: Friday October 1, 2021, 4:30 p.m.

Overview

This lab features the linux permissions system, a filesystem authorization mechanism. It governs access to files, and to anything else represented in the filesystem as if it were a file: directories, devices, symbolic links, kernel variables, etc.

Students will exercise and record results of the filesystem permissions system to grasp that the authorization decision is a function of *two* variables, not one. For a user who wants to access a file, permission depends on *which file*. For a file that a user might access, permission depends on *which user*. Knowing only one of those variables tells nothing about permission to do anything. Sometimes the view is taken, from grammar, of subject and object. Here the user is a subject and a file an object.

Infrastructure for Lab

You will be using a fedora Linux appliance for this lab. The virtual appliance was created for last years lab and may be loaded into Virtual Box. It can also be loaded into VMWare if you prefer.

Location of files

The ova file for this appliance is available in the CSci530 google drive in the folder for Lab 3. You can find the folder: here

Please note that you may need to login to google drive with your USC account in order to access these files.

There is also a file authorizationlab.doc in the same folder. You should download this file and you will use this file to enter the results of your lab experiment. It will be this file, once edited,that you upload to D2L to submit your lab assignment.

Some notes on this instance of fedora Linux

We have already loaded most of the programs you will need for this lab into the virtual appliance. When you start the virtual machine you will be asked to login. For this lab you will be logging in to the root account and the Passwords for the account is "c$l@bLinuX". The third character is the letter "l" as in lab.

Create user accounts and groups; create files, set group ownership and permissions strings

Log in to virtual machine as user root. There are 3 users, 3 groups, and 3 files to set up.

Create the user accounts: useradd bill useradd mary useradd joe	Observe the result: tail /etc/passwd tail /etc/shadow

Assign a password to each account. When prompted in each case, supply "password" as the password. Ignore the on-screen complaints (you are root and can override them). passwd bill passwd mary passwd joe Are these passwords all the same?	Observe the result: tail /etc/shadow Are these passwords all the same?

Create the groups groupadd executives groupadd humanresources groupadd employees	Observe the result: tail /etc/group

Put users into groups: usermod -G executives bill usermod -G humanresources mary usermod -G employees joe	Observe the result: tail /etc/group

Create files: mkdir /tmp/lab3 cd /tmp/lab3 echo stuff > workschedule echo stuff > salaries echo stuff > strategies	Observe the result: ls -l

Set files' group ownerships: chgrp employees workschedule chgrp humanresources salaries chgrp executives strategies	Observe the result: ls -l

Set files' permissions settings: chmod 644 workschedule chmod 660 salaries chmod 640 strategies	Observe the result: ls -l

2. test authorization to read for each user against each file

Baseline

Now that you're set up, determine for each of the three users, against each of the three files, who can read what. (cat-ting a file is a test of its readability.) Identify each of the nine outcomes (file is readable, yes or no) by observing the files' permissions and group affiliations, and the users' group memberships. Write your predictions in the pre-established grid in the supplied answer file authorizationlab.doc, as a "yes" or "no" in each cell. Then test all 9 cases empirically. Do so by logging in successively as each user, and testing each of the 3 files as that user to see whether you were right. Or, you could use the "su" command, without an actual login, to run any other command as any user. For example:

```
su bill -c "cat salaries"
```

causes a read attempt on salaries *by bill*.

For best understanding don't make the empirical attempt untill you have predictively written down your expected results; then check your predctions with the empirical test. Note that this test is confined to reading. In the grammar metaphor, a subject and object need to have an accompanying verb. That's what the r, w, and x are for. Given a subject and object, whether the one can read the other, and whether the one can write the other, are two distinct considerations. Here we only go so far as to explore readability.

modified (by access control lists)

You will make one change to the access control list attached to "strategies" and two changes to the one attached to "salaries." The change to "strategies" will affect a *user*, joe. One of the changes to "salaries" will affect a *user*, joe, while the other will affect a *group*, executives. Check these two files' initial access control lists:

```
getfacl  salaries strategies
```

Then make the changes:

```
setfacl --modify u:joe:rw- salaries strategies
setfacl --modify g:executives:rw- salaries
```

and note the files' changed access control lists:

```
getfacl  salaries strategies
```

Note also, the long listing option (-l) of ls now shows a small plus sign to the right of the permission string:

ls -l

It denotes the existence of an access control list for those files that have one (in this case, salaries and strategies but not workschedule).

Repeat the above 9-square test of who can read what and produce a new written 9-square grid of the results. Write your predictions into the second grid before actually testing them to see whether you were right. For any square that exhibits a change, make sure you understand how the above commands are responsibile for it.

3. clean up

When you have finished, please erase your tracks:

rm workschedule salaries strategies

userdel -r bill
userdel -r mary
userdel -r joe

groupdel executives
groupdel humanresources
groupdel employees

The assignment:

Prepare your answers in the supplied Microsoft Word doc file named authorizationlab.doc found in the Google drive for this lab, linked above.

1. Above you wrote predictions in the grids for both the baseline "before" case and the modified "after" case following creation of an ACL. Then you tested them. Maybe all your predictions were right, maybe not. Change the predictions, as needed, to reflect the actual empirical outcomes you saw. "Yes" or "no" should appear in each cell. In each, under "yes" or "no," write the very brief reason for that outcome. Do this for both of the grids appearing in the authorizationlab.doc answer file.

2. When you assigned identical passwords to bill, mary, and joe, different content appeared for each user in the /etc/shadow file where passwords are stored. Why?

Submission

Please upload the completed template and answersheet to the Lab 3 folder in D2L.