COMP3066 – Week 06 Assignment

- **This is an individual assignment.**
- **The completed work has to be uploaded to the drop box on D2L.**
  - **Email submissions will not be accepted.**
- **Reminder:**
- **The screenshot taking guidelines must be followed (these can be found in our course on D2L under the "Course Content"**
- **User account: Your lastname and then the first letter of the first name. For example: my name is Nikolai (first) Ivanov (last), so my user name is ivanovn**
- **Host name of your Linux VM: Your full last name, the dash character, and the two letters of the first name. For example: my name is Nikolai (first) Ivanov (last), so my host name is ivanov-ni**
- **Screenshots that do not show the properly configured user account and host name will not be accepted**

Objectives:

- Understand the Linux User Authentication
- Use ACLs for Advanced Access Control

Marks breakdown:

Total assignment marks: 10 marks

4 marks: Task 1: PAM Configuration to disable graphical root login
6 marks: Task 2: ACL
- Part 1: ACL of a directory – 2 marks
- Part 2: Default ACL of a directory – 2 marks
- Part 3: Delete ACL – 2 marks

Note: there are no partial marks: the configuration must be completed successfully to receive the marks

Lab Activity

Task 1: Change the PAM Configuration to Disable the Graphical Root Login Exercise

1. Log out of the KDE desktop environment.

NOTE: if you have the auto-login enabled, then open YaST→User and Group Administration and click the Expert Option button (found in the bottom-right corner of the User and Group Administration app), and then open the Login Settings, and uncheck the Auto Login option.

2. When the KDM login screen appears, log in with the following:

qUsername: **root**

Password: **yourpassword**

3. Log out again from the KDE desktop environment.

4. Log in as **geeko** with a password of **novell** (or your password if you did not use novell as password)

5. Open a terminal window and su to **root**.

6. Open the file **/etc/pam.d/xdm** in a text editor.

7. Add the following as the second line of the file:

auth required pam_securetty.so

8. Save and close the file.

8a.. OpenSuse 15 selects the displa manager which controls the login screen through update-alternatives. To list all display managers the alternatives system knows about, run as root:

```
sudo update-alternatives --list default-displaymanager
```

To change the display manager run the following command as root and **select the xdm display manager**:

```
sudo update-alternatives --config default-displaymanager
```

9. Reboot Linux and try to log in as **root** user at the KDM login screen again.

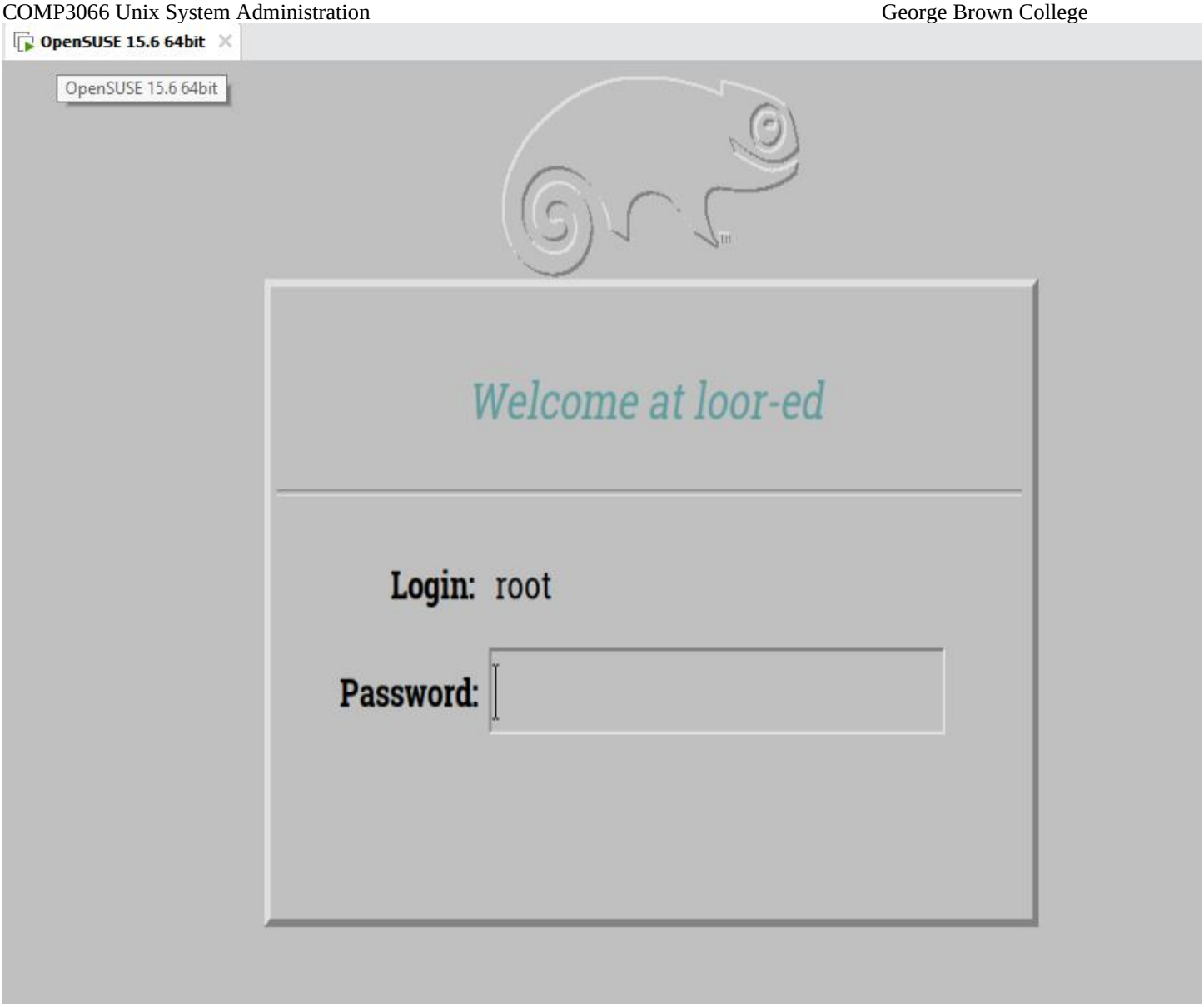
The root login must be denied.

SUBMISSION: the screen shots of the window after completing steps 7, 8a, and 9. Replace the sample screenshots below with your screenshots.

```
loor-ed:/home/geeko # cat /etc/pam.d/xdm
#%PAM-1.0
auth required pam_securetty.so
auth     include        common-auth
account  include        common-account
password include        common-password
session  required       pam_loginuid.so
session  include        common-session
loor-ed:/home/geeko # update-alternatives --list default-displaymanager
/usr/lib/X11/displaymanagers/console
/usr/lib/X11/displaymanagers/sddm
/usr/lib/X11/displaymanagers/xdm
loor-ed:/home/geeko # update-alternatives --config default-displaymanager
There are 3 choices for the alternative default-displaymanager (providing /usr/lib/X11/displaymanagers/default
-displaymanager).

  Selection    Path                                  Priority   Status
------------------------------------------------------------
  0            /usr/lib/X11/displaymanagers/sddm      25        auto mode
  1            /usr/lib/X11/displaymanagers/console   5         manual mode
  2            /usr/lib/X11/displaymanagers/sddm      25        manual mode
* 3            /usr/lib/X11/displaymanagers/xdm       10        manual mode

Press <enter> to keep the current choice[*], or type selection number: 3
loor-ed:/home/geeko #
```



NOTE: the login attempt using the root account should be unsuccessful. You should only be able to login as the geeko or your regular user.

10. Log in as geeko again.

NOTE: If you cannot log in as geeko, restart the X server by pressing **Ctrl+Alt+Backspace** and try again. You might also need to reboot your server.

11. Open a terminal window and su to **root**.

12. Open the file **/etc/pam.d/xdm** in a text editor and remove or comment out the following line (the line you added):

auth required pam_securetty.so

13. Save and close the file.

14. Log out and try to log in as **root** at the KDM login screen again. You can now log in as root.

NOTE: If you cannot log in as root, restart the X server by pressing **Ctrl+Alt+Backspace** and try again. You might also need to reboot your server.

15. Log out of the KDE desktop environment and log back in as **geeko**.

Task 2: Use ACLs Exercise

Part I: Configure the ACL of a Directory

1. Open a terminal window and su to **root**.

2. Change to the directory /tmp by entering the following:

cd /tmp

3. Create a test directory by entering the following:

mkdir acl_test

4. Limit the file system permissions for the directory by entering the following:

chmod 700 acl_test

5. Open a second terminal window as the user **geeko**.

6. Try changing to the test directory by entering the following:

cd /tmp/acl_test/

The command fails because geeko (who is *not* the owner of the directory) has no permission to read the directory. In this exercise, you practice using ACLs by doing the following: Do the following:

7. Switch to the root terminal.

8. Display the minimum ACL of the directory by entering the following:

getfacl acl_test

9. Add an extended ACL by entering the following:

setfacl -m u:geeko:rwx acl_test/

10. Switch to the geeko terminal and try to access the directory again by entering the following:

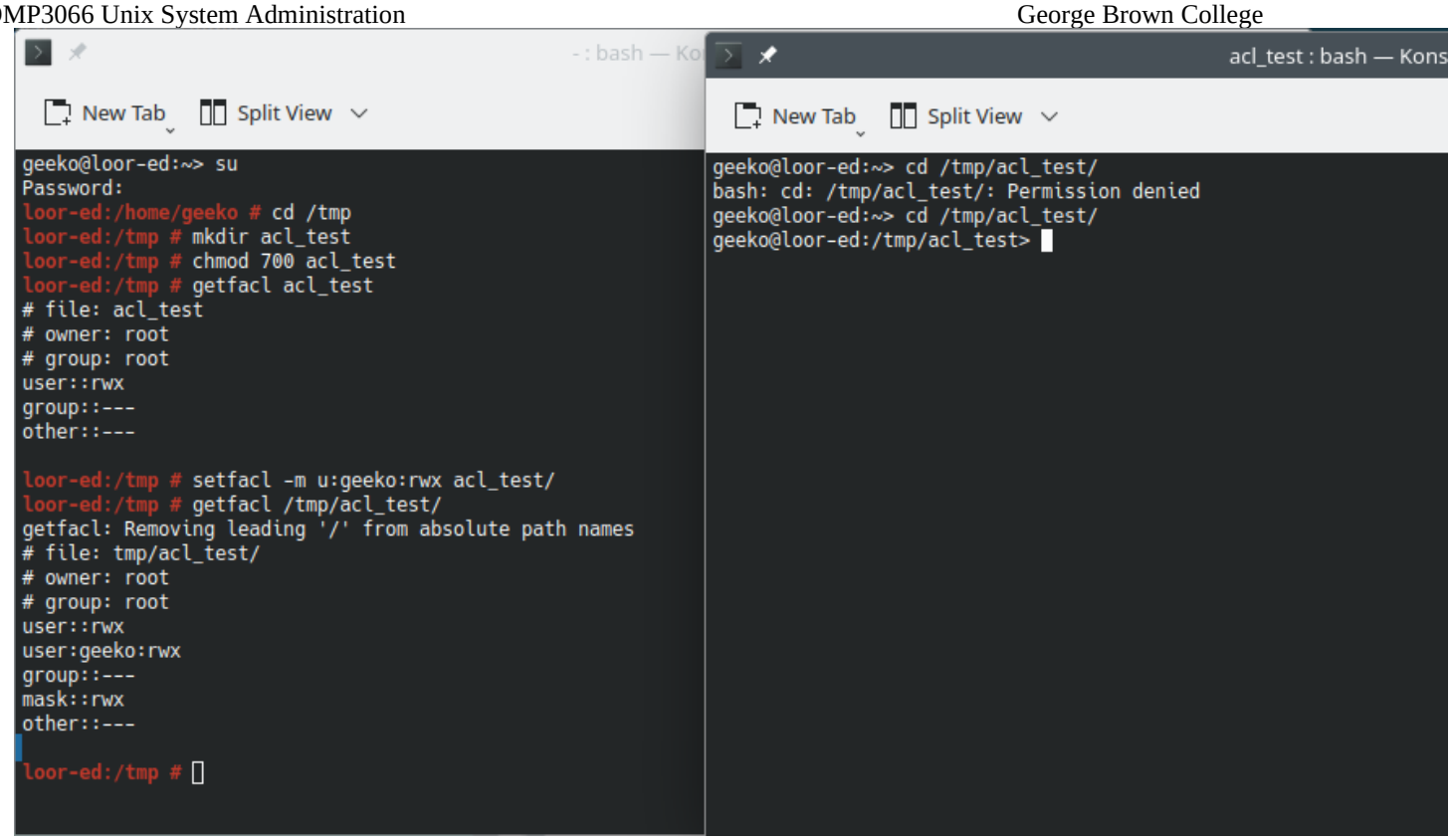
cd /tmp/acl_test

Because of the extended ACL, you can view the directory.

11. Switch to the root terminal and display the extended ACL of the directory by entering the following:

getfacl /tmp/acl_test/

SUBMISSION: the screen shots of the window after completing steps 6, 8, and 11. Replace the sample screenshot below with your own screenshot:



Part II: Configure a Default ACL for a Directory

1. From the root terminal window, change to the directory acl_test by entering the following:

cd /tmp/acl_test

2. Create a file by entering the following:

touch without_default_acl

3. Display the ACL of the new file by entering the following:

getfacl without_default_acl

As there is no default ACL for the parent directory, the new file does not have an extended ACL either.

4. Set a default ACL for the directory acl_test by entering the following:

setfacl -d -m u:geeko:rw /tmp/acl_test/

5. Create another test file by entering the following:

touch with_default_acl

6. Display the ACL of the new file by entering the following:

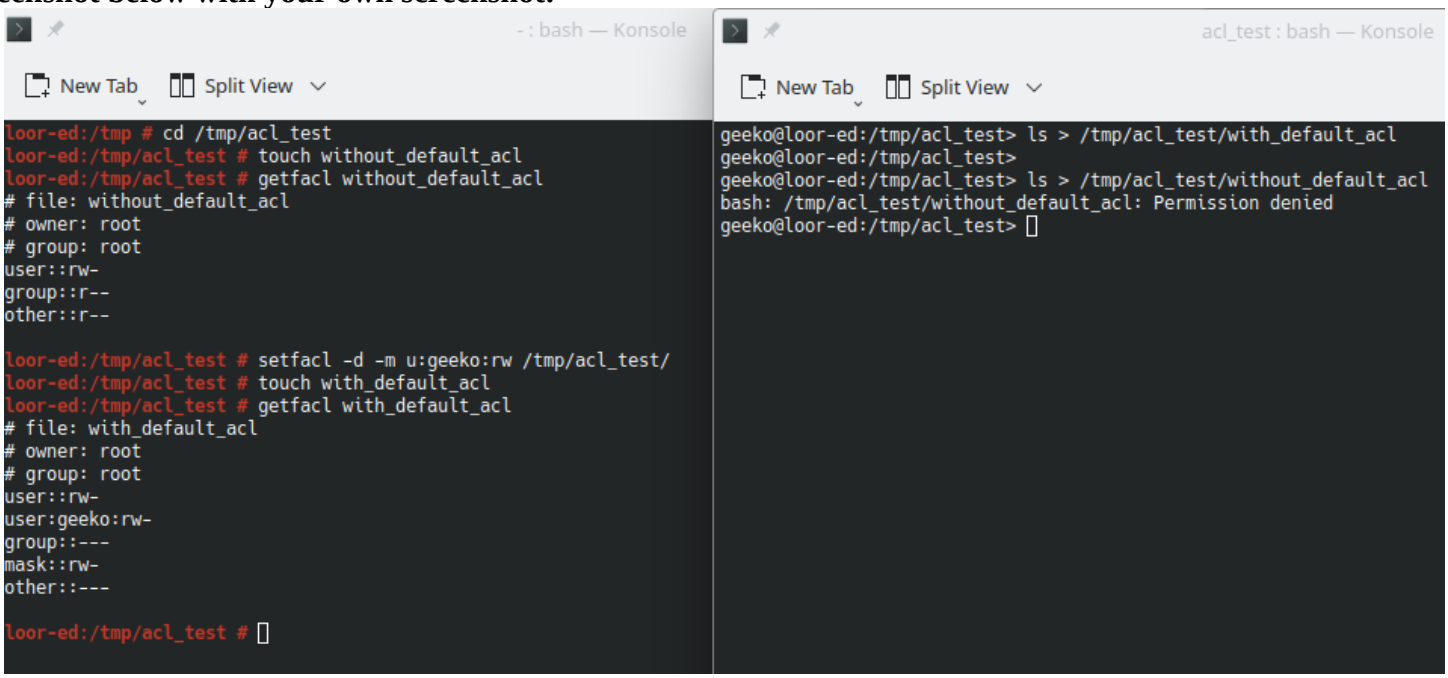
getfacl with_default_acl

As this file was created after the default ACL of the parent directory was set, the new file inherited the ACL.

Test the above by switching to the second console (where you are geeko user) window and trying to modify the content of both files. You should be able to modify the with_default_acl file but should be denied access

to the without_default_acl file. You can use the following two commands to run the test: 1) ls > /tmp/acl_test/with_default_acl and 2) ls > /tmp/acl_test/without_default_acl

SUBMISSION: the screen shot of the window after completing steps 3 and 6. Replace the sample screenshot below with your own screenshot:



Part III: Delete an ACL

1. From the root terminal window, remove the ACL by entering the following:

setfacl -x u:geeko with_default_acl

2. Display the ACL again by entering the following:

getfacl with_default_acl

As you can see, the ACL for the user geeko has been removed. If there were ACLs for other users, they would remain unaffected.

3. View the file attributes of with_default_acl by entering the following:

ls -l with_default_acl

There are still extended attributes (such as the mask "+") in the output.

4. Remove all ACLs by entering the following:

setfacl -b with_default_acl

5. Display the ACL again by entering the following commands:

getfacl with_default_acl

ls -l with_default_acl

Notice that the ACL has been removed. Your geeko user should not be able to modify any of the files you created in the /tmp/acl_test directory. Rerun the test commands from the Part II to confirm that.

6. Close all terminal windows.

SUBMISSION: the screen shots of the window after completing steps 2, and 5. Replace the sample screenshot below with your own screenshot: