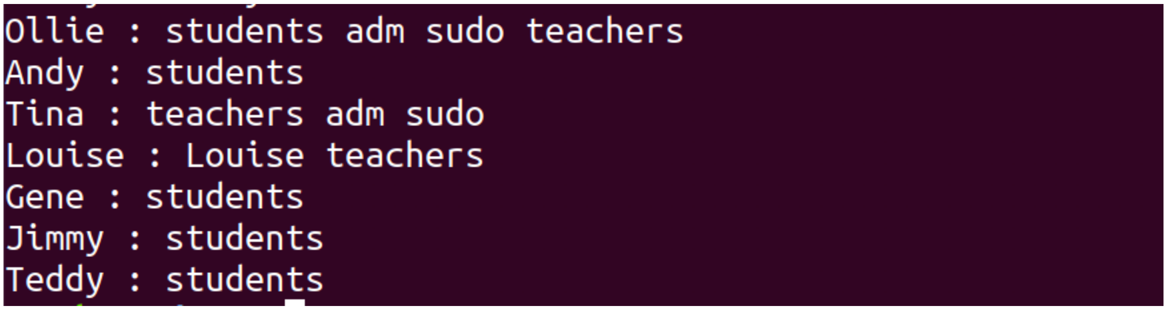
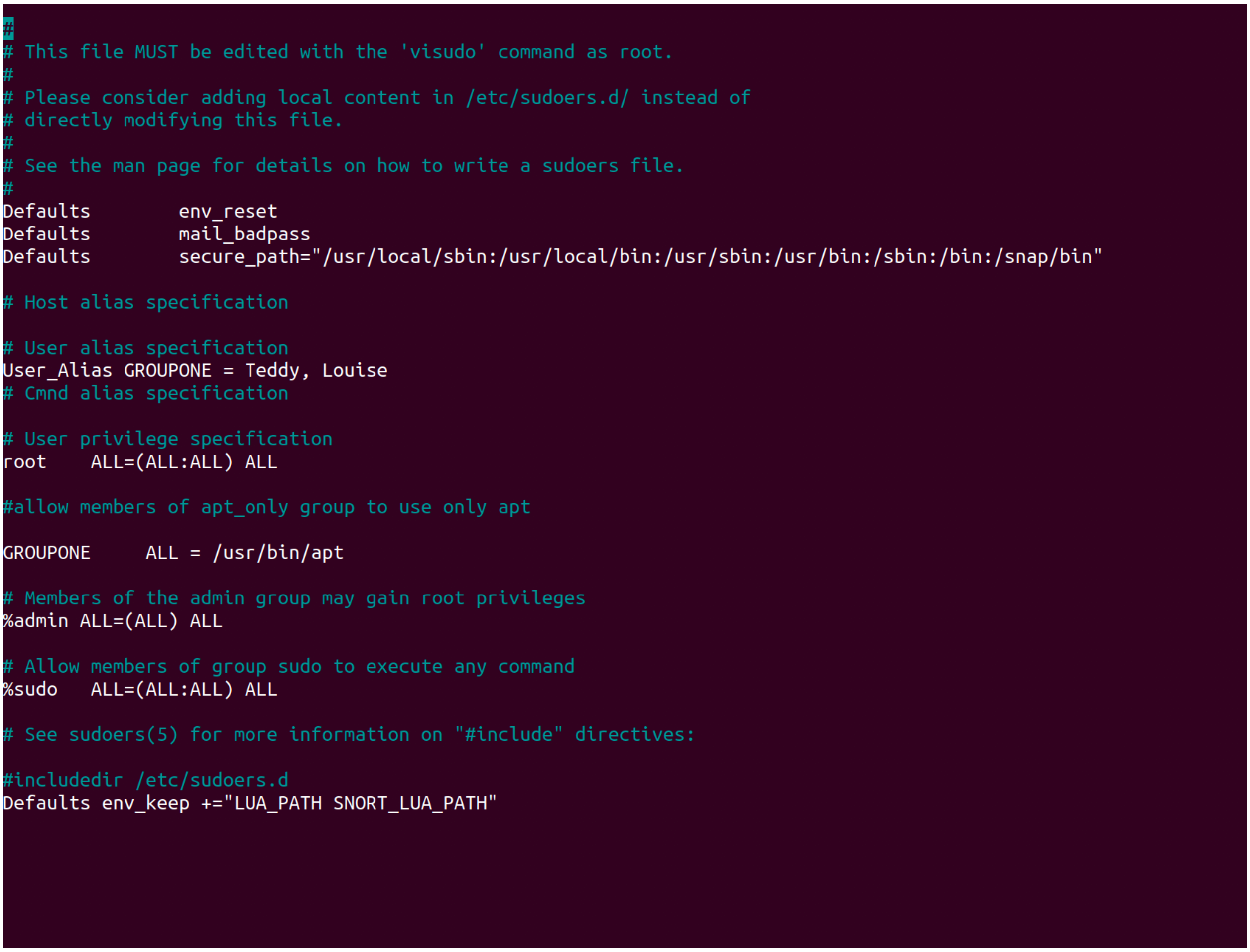
LINUX homework 8 assignment

Part 1: Users & Groups



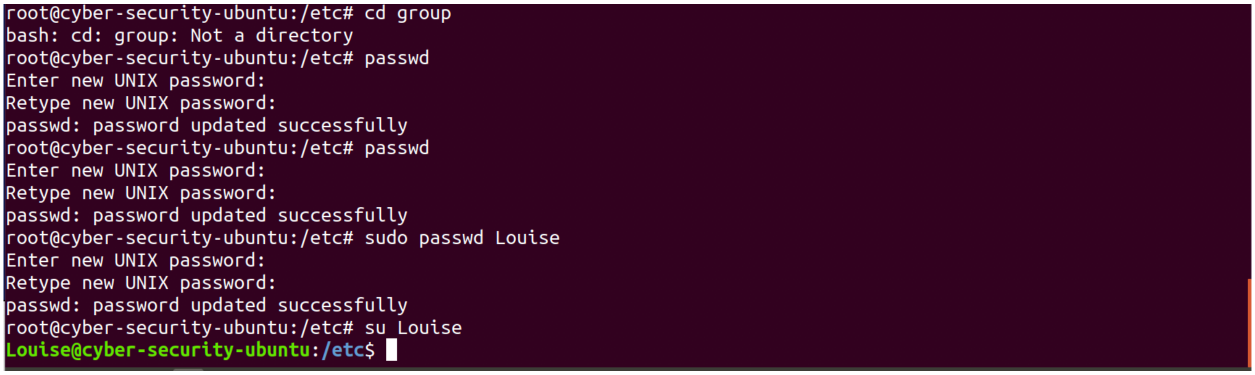
```
Ollie : students adm sudo teachers
Andy : students
Tina : teachers adm sudo
Louise : Louise teachers
Gene : students
Jimmy : students
Teddy : students
```

Part 2: Restricting Sudo Access

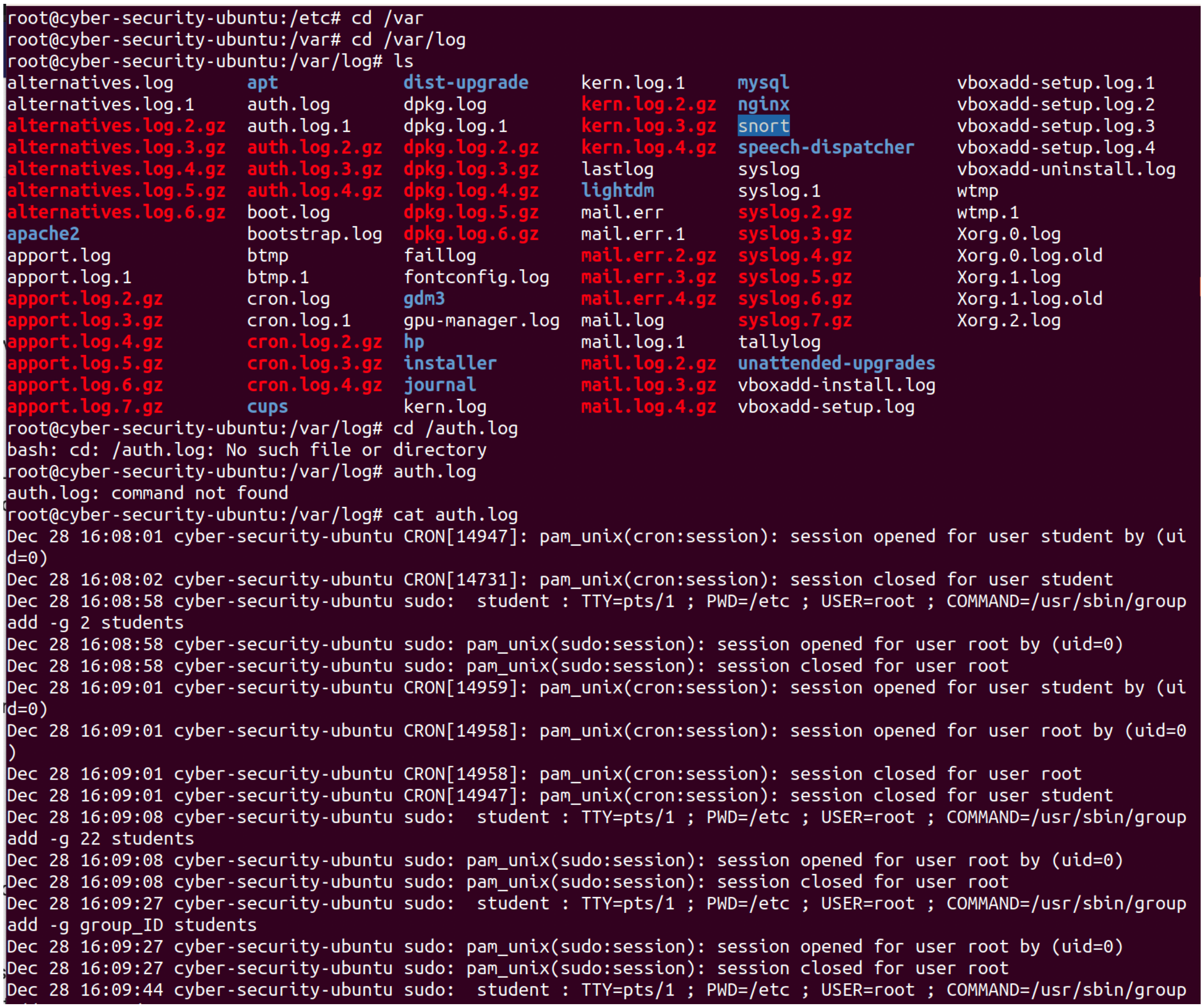


```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification
User_Alias GROUPONE = Teddy, Louise
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

#allow members of apt_only group to use only apt

GROUPONE     ALL = /usr/bin/apt

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
Defaults env_keep +="LUA_PATH SNORT_LUA_PATH"
```

Part 3: Logging Sudo Access Attempts



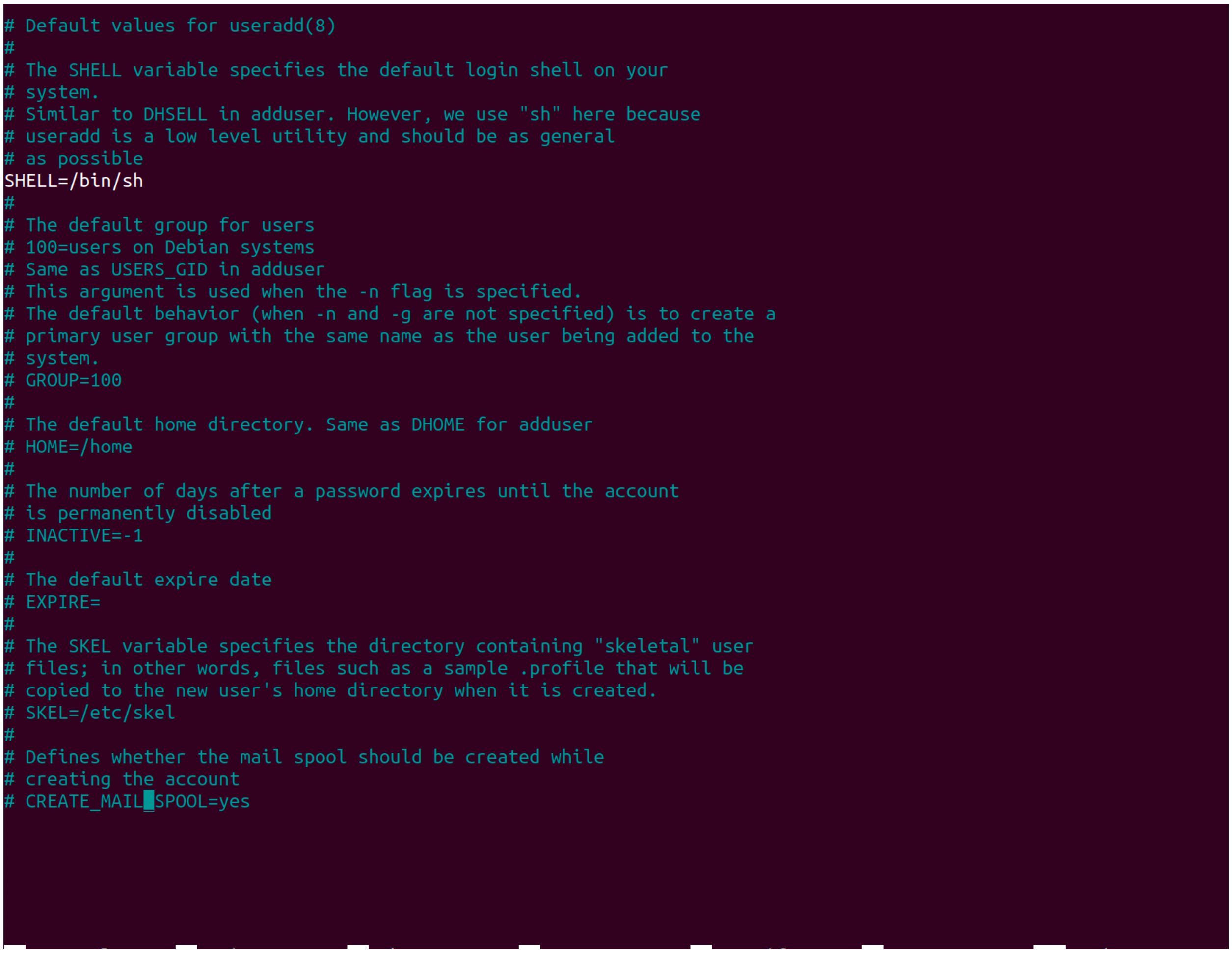
```
root@cyber-security-ubuntu:/etc# cd group
bash: cd: group: Not a directory
root@cyber-security-ubuntu:/etc# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@cyber-security-ubuntu:/etc# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@cyber-security-ubuntu:/etc# sudo passwd Louise
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@cyber-security-ubuntu:/etc# su Louise
Louise@cyber-security-ubuntu:/etc$
```



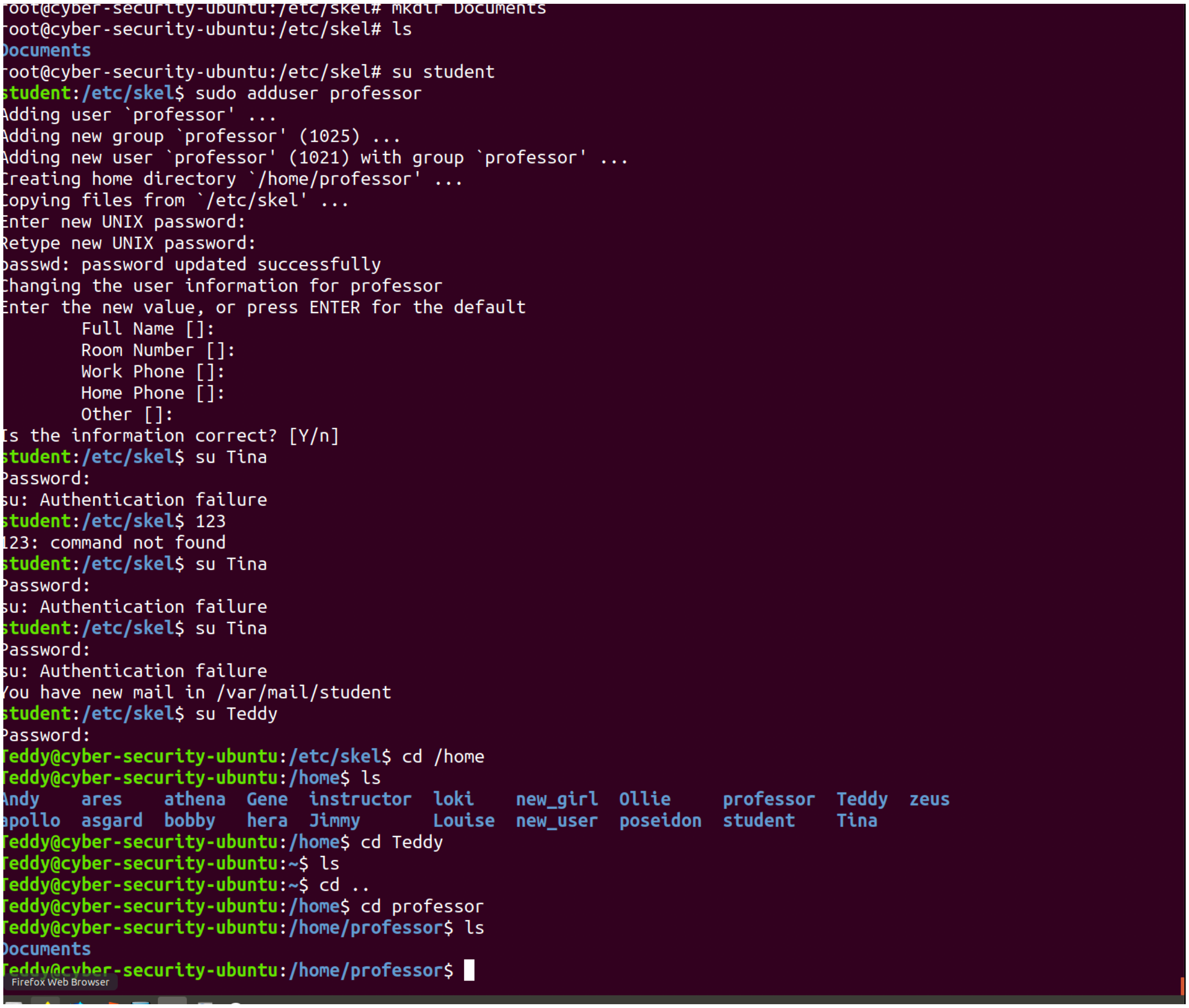
```
root@cyber-security-ubuntu:/etc# cd /var
root@cyber-security-ubuntu:/var# cd /var/log
root@cyber-security-ubuntu:/var/log# ls
alternatives.log       apt            dist-upgrade     kern.log.1     mysql                vboxadd-setup.log.1
alternatives.log.1     auth.log       dpkg.log         kern.log.2.gz  nginx                vboxadd-setup.log.2
alternatives.log.2.gz  auth.log.1     dpkg.log.1       kern.log.3.gz  snort                vboxadd-setup.log.3
alternatives.log.3.gz  auth.log.2.gz  dpkg.log.2.gz    kern.log.4.gz  speech-dispatcher    vboxadd-setup.log.4
alternatives.log.4.gz  auth.log.3.gz  dpkg.log.3.gz    lastlog        syslog               vboxadd-uninstall.log
alternatives.log.5.gz  auth.log.4.gz  dpkg.log.4.gz    lightdm        syslog.1             wtmp
alternatives.log.6.gz  boot.log       dpkg.log.5.gz    mail.err       syslog.2.gz          wtmp.1
apache2                bootstrap.log  dpkg.log.6.gz    mail.err.1     syslog.3.gz          Xorg.0.log
apport.log             btmp           faillog          mail.err.2.gz  syslog.4.gz          Xorg.0.log.old
apport.log.1           btmp.1         fontconfig.log   mail.err.3.gz  syslog.5.gz          Xorg.1.log
apport.log.2.gz        cron.log       gdm3             mail.err.4.gz  syslog.6.gz          Xorg.1.log.old
apport.log.3.gz        cron.log.1     gpu-manager.log  mail.log       syslog.7.gz          Xorg.2.log
apport.log.4.gz        cron.log.2.gz  hp               mail.log.1     tallylog
apport.log.5.gz        cron.log.3.gz  installer        mail.log.2.gz  unattended-upgrades
apport.log.6.gz        cron.log.4.gz  journal          mail.log.3.gz  vboxadd-install.log
apport.log.7.gz        cups           kern.log         mail.log.4.gz  vboxadd-setup.log
root@cyber-security-ubuntu:/var/log# cd /auth.log
bash: cd: /auth.log: No such file or directory
root@cyber-security-ubuntu:/var/log# auth.log
auth.log: command not found
root@cyber-security-ubuntu:/var/log# cat auth.log
Dec 28 16:08:01 cyber-security-ubuntu CRON[14947]: pam_unix(cron:session): session opened for user student by (ui
d=0)
Dec 28 16:08:02 cyber-security-ubuntu CRON[14731]: pam_unix(cron:session): session closed for user student
Dec 28 16:08:58 cyber-security-ubuntu sudo:  student : TTY=pts/1 ; PWD=/etc ; USER=root ; COMMAND=/usr/sbin/group
add -g 2 students
Dec 28 16:08:58 cyber-security-ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 28 16:08:58 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Dec 28 16:09:01 cyber-security-ubuntu CRON[14959]: pam_unix(cron:session): session opened for user student by (ui
d=0)
Dec 28 16:09:01 cyber-security-ubuntu CRON[14958]: pam_unix(cron:session): session opened for user root by (uid=0
)
Dec 28 16:09:01 cyber-security-ubuntu CRON[14958]: pam_unix(cron:session): session closed for user root
Dec 28 16:09:01 cyber-security-ubuntu CRON[14947]: pam_unix(cron:session): session closed for user student
Dec 28 16:09:08 cyber-security-ubuntu sudo:  student : TTY=pts/1 ; PWD=/etc ; USER=root ; COMMAND=/usr/sbin/group
add -g 22 students
Dec 28 16:09:08 cyber-security-ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 28 16:09:08 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Dec 28 16:09:27 cyber-security-ubuntu sudo:  student : TTY=pts/1 ; PWD=/etc ; USER=root ; COMMAND=/usr/sbin/group
add -g group_ID students
Dec 28 16:09:27 cyber-security-ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Dec 28 16:09:27 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Dec 28 16:09:44 cyber-security-ubuntu sudo:  student : TTY=pts/1 ; PWD=/etc ; USER=root ; COMMAND=/usr/sbin/group
```

- In this part of the assignment I discovered two different ways to change user password (for Louise) while in root and student
- Switching to student user or root user and using the command sudo passwd Louise will change the password if a specific user needs access

Part 4: Customizing Users Directories



```
# Default values for useradd(8)
#
# The SHELL variable specifies the default login shell on your
# system.
# Similar to DHSELL in adduser. However, we use "sh" here because
# useradd is a low level utility and should be as general
# as possible
SHELL=/bin/sh
#
# The default group for users
# 100=users on Debian systems
# Same as USERS_GID in adduser
# This argument is used when the -n flag is specified.
# The default behavior (when -n and -g are not specified) is to create a
# primary user group with the same name as the user being added to the
# system.
# GROUP=100
#
# The default home directory. Same as DHOME for adduser
# HOME=/home
#
# The number of days after a password expires until the account
# is permanently disabled
# INACTIVE=-1
#
# The default expire date
# EXPIRE=
#
# The SKEL variable specifies the directory containing "skeletal" user
# files; in other words, files such as a sample .profile that will be
# copied to the new user's home directory when it is created.
# SKEL=/etc/skel
#
# Defines whether the mail spool should be created while
# creating the account
# CREATE_MAIL_SPOOL=yes
```



```
root@cyber-security-ubuntu:/etc/skel# mkdir Documents
root@cyber-security-ubuntu:/etc/skel# ls
Documents
root@cyber-security-ubuntu:/etc/skel# su student
student:/etc/skel$ sudo adduser professor
Adding user `professor' ...
Adding new group `professor' (1025) ...
Adding new user `professor' (1021) with group `professor' ...
Creating home directory `/home/professor' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for professor
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]
student:/etc/skel$ su Tina
Password:
su: Authentication failure
student:/etc/skel$ 123
123: command not found
student:/etc/skel$ su Tina
Password:
su: Authentication failure
student:/etc/skel$ su Tina
Password:
su: Authentication failure
You have new mail in /var/mail/student
student:/etc/skel$ su Teddy
Password:
Teddy@cyber-security-ubuntu:/etc/skel$ cd /home
Teddy@cyber-security-ubuntu:/home$ ls
Andy    ares    athena  Gene  instructor  loki    new_girl  Ollie     professor  Teddy  zeus
apollo  asgard  bobby   hera  Jimmy       Louise  new_user  poseidon  student    Tina
Teddy@cyber-security-ubuntu:/home$ cd Teddy
Teddy@cyber-security-ubuntu:~$ ls
Teddy@cyber-security-ubuntu:~$ cd ..
Teddy@cyber-security-ubuntu:/home$ cd professor
Teddy@cyber-security-ubuntu:/home/professor$ ls
Documents
Teddy@cyber-security-ubuntu:/home/professor$
```

- The takeaway from using skel, was understanding that by switching to root user and adding folders such as “Documents” to /skel folder, will add this folder to every users’ /home directory; however, only to preceding new users (i.e professor) which was created after the folder was added to /skel
- Teddy’s home directory was empty because this user was created prior to adding Documents to skel