```
andy : andy students
ollie : ollie adm sudo students teachers
tina : tina adm sudo teachers
louise : louise teachers
gene : gene students
jimmy : jimmy students
teddy : teddy students
student:~$
```

```
student:/etc$ sudo -lU teddy
Matching Defaults entries for teddy on
   cyber-security-ubuntu:
   env_reset, mail_badpass,
   secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:
/usr/bin\:/sbin\:/bin\:/snap/bin,
   env keep+="LUA PATH SNORT LUA PATH"
User teddy may run the following commands on
       cyber-security-ubuntu:
   (root) /sbin/apt
student:/etc$ sudo -lU louise
Matching Defaults entries for louise on
   cyber-security-ubuntu:
   env_reset, mail_badpass,
   secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:
/usr/bin\:/sbin\:/bin\:/snap/bin,
   env keep+="LUA PATH SNORT LUA PATH"
User louise may run the following commands on
       cyber-security-ubuntu:
   (root) /sbin/apt
student:/etc$
```

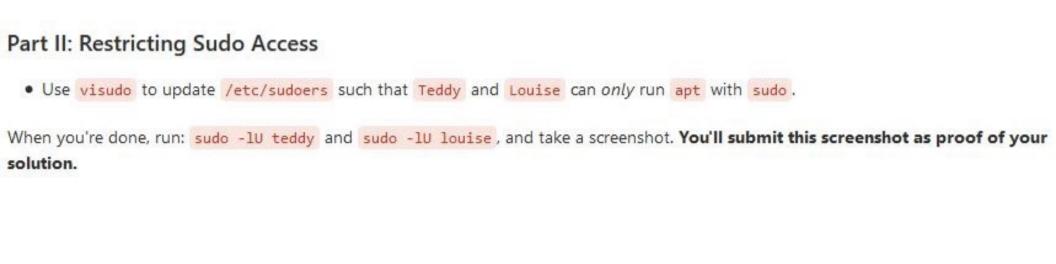
```
Dec 18 19:29:36 cyber-security-ubuntu sudo: louise : comma
nd not allowed; TTY=pts/0; PWD=/etc; USER=root; COMMAND=
/usr/bin/apt update
Dec 18 19:30:07 cyber-security-ubuntu sudo: louise : comma
nd not allowed; TTY=pts/0; PWD=/etc; USER=root; COMMAND=
/bin/cat /etc/passwd
Dec 18 19:30:59 cyber-security-ubuntu sudo: pam_unix(sudo:au
th): authentication failure; logname= uid=1019 euid=0 tty=/d
ev/pts/0 ruser=teddy rhost= user=teddy
Dec 18 19:31:07 cyber-security-ubuntu sudo: teddy : comma
nd not allowed; TTY=pts/0; PWD=/etc; USER=root; COMMAND=
/usr/bin/apt update
Dec 18 19:31:20 cyber-security-ubuntu sudo: teddy : comma
nd not allowed; TTY=pts/0; PWD=/etc; USER=root; COMMAND=
/bin/cat /etc/passwd
student:/etc$
```

```
student:/etc/skel$ ls
Documents Downloads Pictures Videos
student:/etc/skel$ useradd -m michael
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
student:/etc/skel$ sudo useradd -m michael
student:/etc/skel$ ls /etc/
Display all 243 possibilities? (y or n)
student:/etc/skel$ cd ~
student:~$ cd ../
student:/home$ ls
andy Downloads jimmy ollie
                                          sudoers
apollo felix loki poseidon teddy
ares gene louise shadow.bak tina
asgard hera michael shadow.cracked zeus
athena instructor new user student
student:/home$ cd michael/
student:/home/michael$ ls
Documents Downloads Pictures Videos
student:/home/michaei$ cd /etc/skel/
student:/etc/skel$ ls
Documents Downloads Pictures Videos
student:/etc/skel$
```

Part I: Users and Groups

- In your Virtual Machine, create the following user accounts:
 - O Andy
 - O Ollie
 - O Tina
 - O Louise
 - O Gene
 - O Jimmy
 - O Teddy
- Set their passwords to be whatever you would like.
- Then, create the following groups with the following members:
 - o students: Andy, Ollie, Gene, Jimmy, Teddy
 - o teachers : Tina, Louise, Ollie
 - O Add Tina and Ollie to the sudo and adm groups.

When you're done, run: cut -d: -f1 /etc/passwd | xargs groups and take a screenshot. This command will show all users, along with the groups they're in. You'll submit this screenshot as proof of your solution.



Part III: Logging Sudo Access Attempts

- · Check if rsyslog is installed. If not, install it.
- · Start rsyslog.
 - O Note: Use the service command.
- Switch users to Louise, and do the following:
 - O Use sudo to run apt update, but enter the wrong password.
 - O Use sudo to run apt update.
 - O Use sudo to run cat /etc/passwd.
- · Repeat the above as Teddy.
- Now, switch to the root user. Inspect /var/log/auth.log. Look for messages about sudo. Which of the commands you ran as Teddy
 and Louise do you see in the logs? You'll submit this screenshot as proof of your solution.

Part IV: Customizing User Directories

- · Still logged in as root:
- Inside each user's /home directory, create the following folders:
 - O Documents
 - O Downloads
 - O Pictures
 - O Videos
- Set permissions for each user's directory to have full permissions for the associated user, read permissions for their group, and no permissions for the world.
 - For example, files in Teddy's directory should have permissions like: rwxr----.
- Test your permissions by switching to one of the users, and attempting to read the other users' files. You should get Permission denied errors.
 - o For example, switch to the user Teddy , and try to list files in /home/jane .
- Research /etc/skel to figure out how to avoid manually creating Documents, etc., directories for every user: http://www.linfo.org/etc_skel.html
- Update your /etc/skel with Documents, etc., directories. Then, create a new user with your name. Inspect the contents of your new user's
 /home directory to verify that your /etc/skel update works as expected. Please submit both a screenshot of your /etc/skel and new user's home directory as proof of your solution.