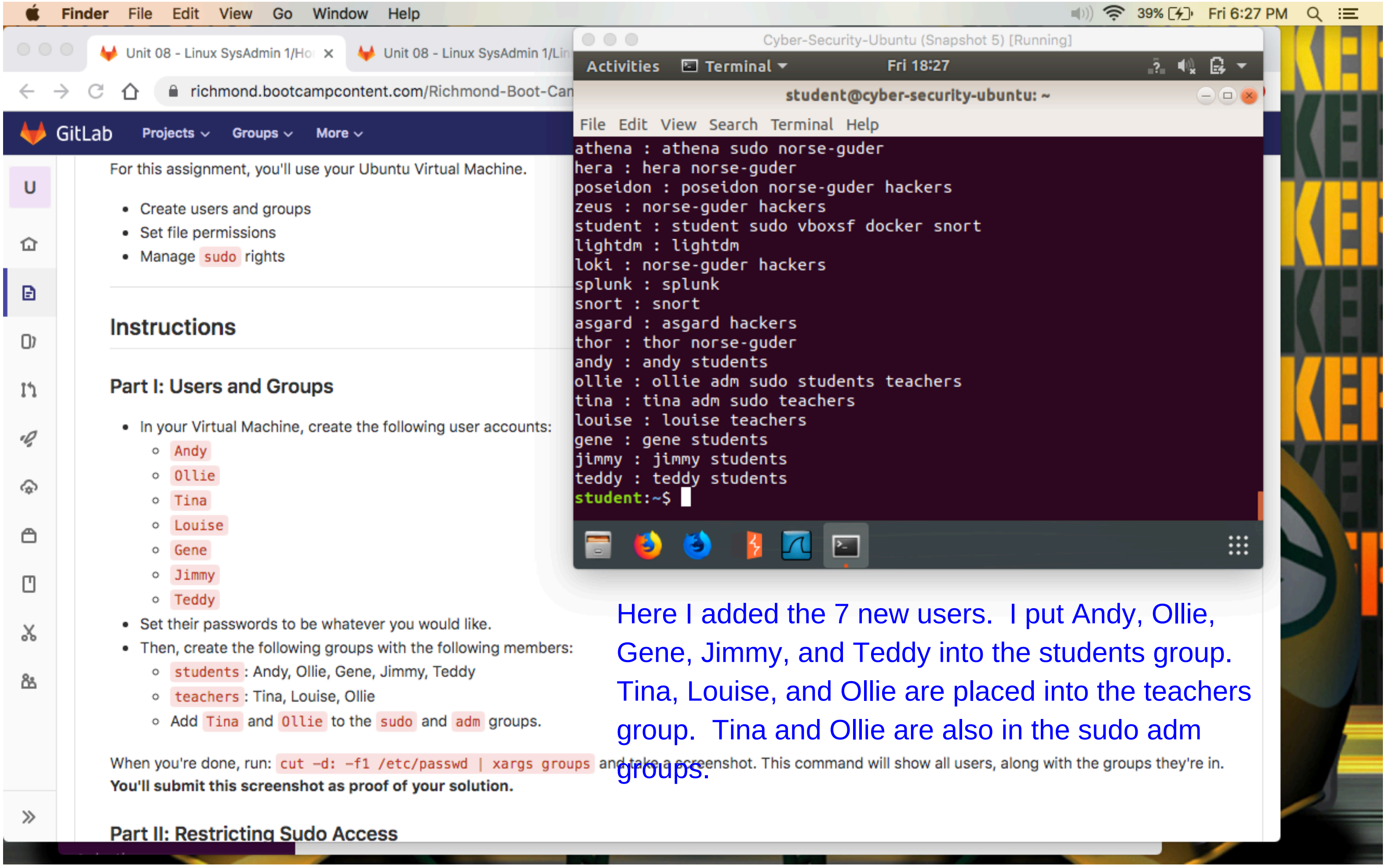

Finder File Edit View Go Window Help
39% Fri 6:27 PM
Unit 08 - Linux SysAdmin 1/Ho
Unit 08 - Linux SysAdmin 1/Lin
richmond.bootcampcontent.com/Richmond-Boot-Can
GitLab Projects Groups More
Cyber-Security-Ubuntu (Snapshot 5) [Running]
Activities Terminal Fri 18:27
student@cyber-security-ubuntu: ~
File Edit View Search Terminal Help

For this assignment, you'll use your Ubuntu Virtual Machine.

- Create users and groups
- Set file permissions
- Manage `sudo` rights

Instructions

Part I: Users and Groups

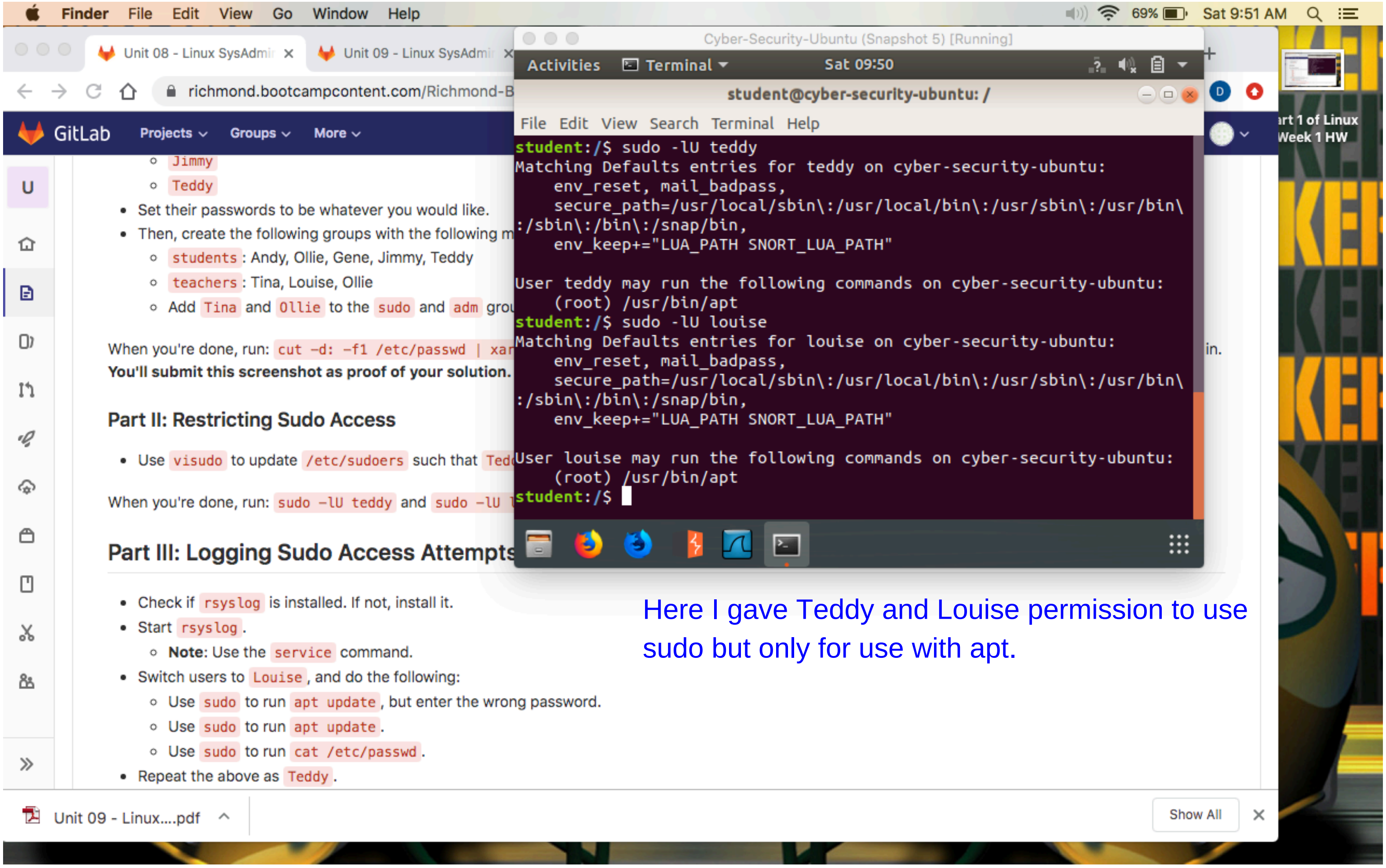
- In your Virtual Machine, create the following user accounts:
  - `Andy`
  - `Ollie`
  - `Tina`
  - `Louise`
  - `Gene`
  - `Jimmy`
  - `Teddy`
- Set their passwords to be whatever you would like.
- Then, create the following groups with the following members:
  - `students`: Andy, Ollie, Gene, Jimmy, Teddy
  - `teachers`: Tina, Louise, Ollie
  - 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 II: Restricting Sudo Access

```
athena : athena sudo norse-guder
hera : hera norse-guder
poseidon : poseidon norse-guder hackers
zeus : norse-guder hackers
student : student sudo vboxsf docker snort
lightdm : lightdm
loki : norse-guder hackers
splunk : splunk
snort : snort
asgard : asgard hackers
thor : thor norse-guder
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:~$
```

Here I added the 7 new users. I put Andy, Ollie, Gene, Jimmy, and Teddy into the students group. Tina, Louise, and Ollie are placed into the teachers group. Tina and Ollie are also in the sudo adm groups.


Finder File Edit View Go Window Help
69% Sat 9:51 AM
Unit 08 - Linux SysAdmi
Unit 09 - Linux SysAdmi
richmond.bootcampcontent.com/Richmond-B
GitLab Projects Groups More
Cyber-Security-Ubuntu (Snapshot 5) [Running]
Activities Terminal Sat 09:50
student@cyber-security-ubuntu: /
File Edit View Search Terminal Help
art 1 of Linux Week 1 HW
Unit 09 - Linux....pdf
Show All

- Jimmy
- Teddy
- Set their passwords to be whatever you would like.
- Then, create the following groups with the following m
  - `students`: Andy, Ollie, Gene, Jimmy, Teddy
  - `teachers`: Tina, Louise, Ollie
  - Add `Tina` and `Ollie` to the `sudo` and `adm` grou

When you're done, run: `cut -d: -f1 /etc/passwd | xar` in.
You'll submit this screenshot as proof of your solution.

Part II: Restricting Sudo Access

- Use `visudo` to update `/etc/sudoers` such that `Ted`

When you're done, run: `sudo -lU teddy` and `sudo -lU`

Part III: Logging Sudo Access Attempts

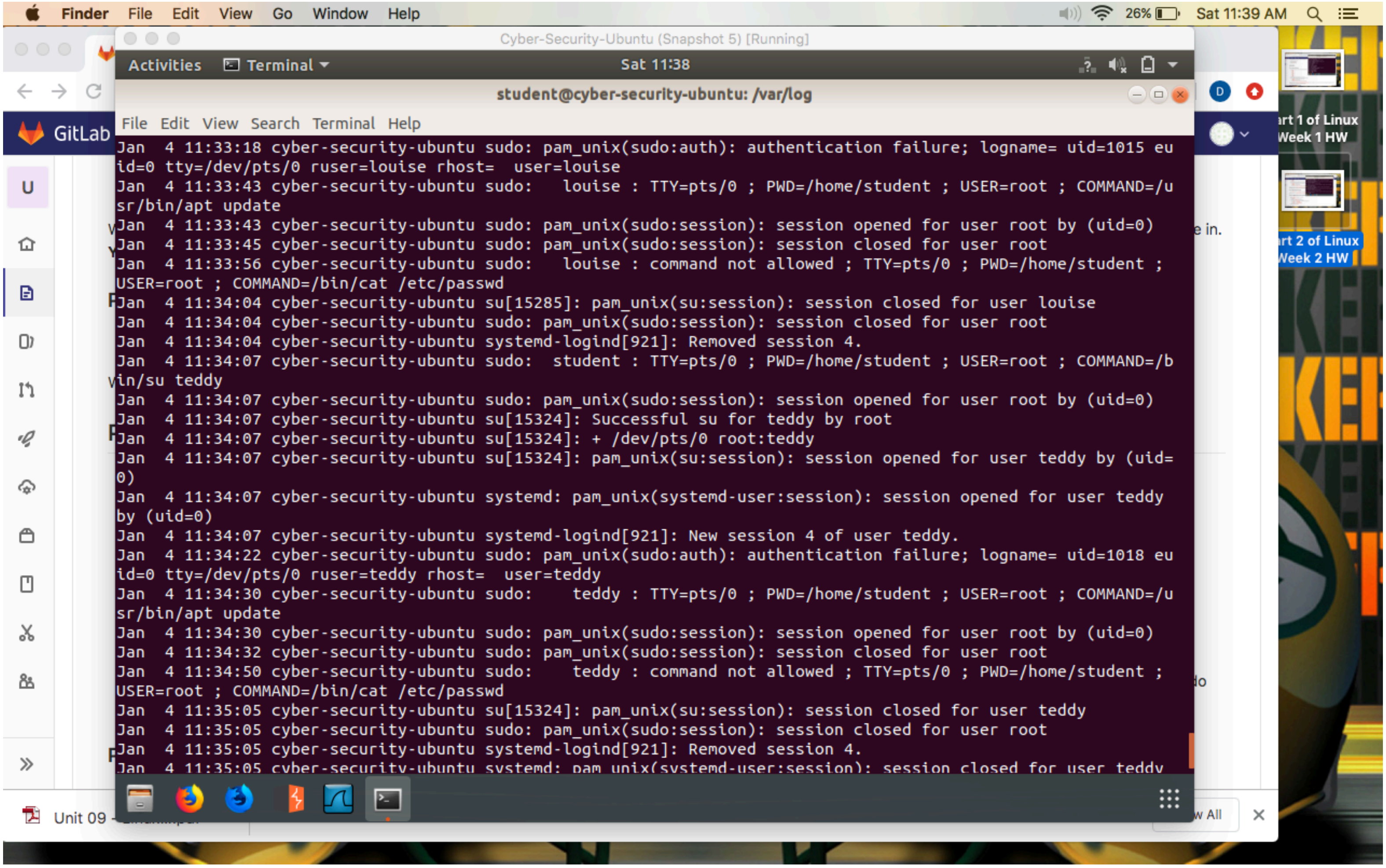
- Check if `rsyslog` is installed. If not, install it.
- Start `rsyslog`.
  - **Note:** Use the `service` command.
- Switch users to `Louise`, and do the following:
  - Use `sudo` to run `apt update`, but enter the wrong password.
  - Use `sudo` to run `apt update`.
  - Use `sudo` to run `cat /etc/passwd`.
- Repeat the above as `Teddy`.

```
student:/$ 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) /usr/bin/apt
student:/$ 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) /usr/bin/apt
student:/$ 
```

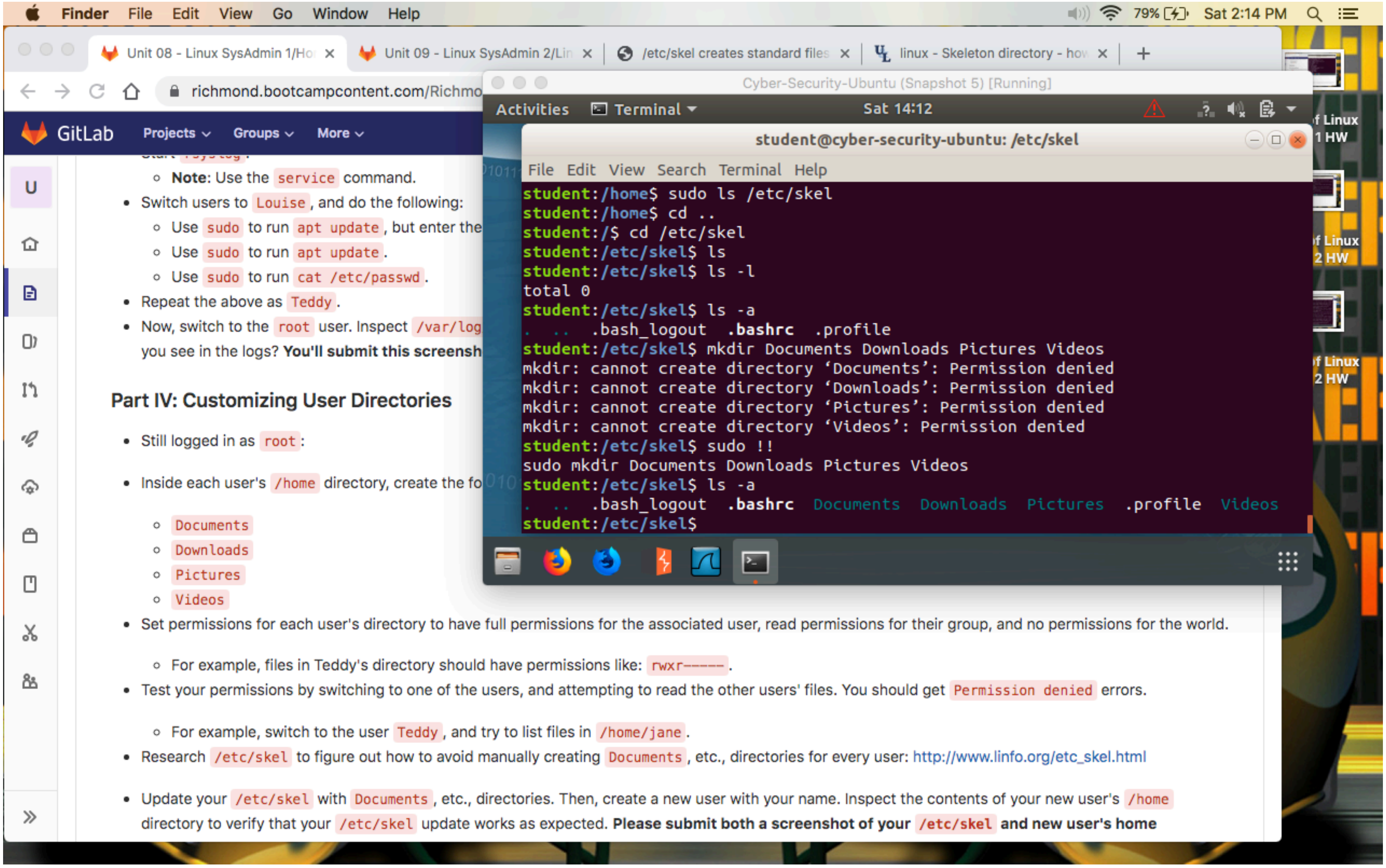
Here I gave Teddy and Louise permission to use sudo but only for use with apt.



Finder File Edit View Go Window Help
26%
Sat 11:39 AM
Cyber-Security-Ubuntu (Snapshot 5) [Running]
Activities
Terminal
Sat 11:38
student@cyber-security-ubuntu: /var/log
File Edit View Search Terminal Help
GitLab
art 1 of Linux Week 1 HW
art 2 of Linux Week 2 HW
Unit 09

```
Jan  4 11:33:18 cyber-security-ubuntu sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1015 eu
id=0 tty=/dev/pts/0 ruser=louise rhost=  user=louise
Jan  4 11:33:43 cyber-security-ubuntu sudo:   louise : TTY=pts/0 ; PWD=/home/student ; USER=root ; COMMAND=/u
sr/bin/apt update
Jan  4 11:33:43 cyber-security-ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jan  4 11:33:45 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Jan  4 11:33:56 cyber-security-ubuntu sudo:   louise : command not allowed ; TTY=pts/0 ; PWD=/home/student ;
USER=root ; COMMAND=/bin/cat /etc/passwd
Jan  4 11:34:04 cyber-security-ubuntu su[15285]: pam_unix(su:session): session closed for user louise
Jan  4 11:34:04 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Jan  4 11:34:04 cyber-security-ubuntu systemd-logind[921]: Removed session 4.
Jan  4 11:34:07 cyber-security-ubuntu sudo:  student : TTY=pts/0 ; PWD=/home/student ; USER=root ; COMMAND=/b
in/su teddy
Jan  4 11:34:07 cyber-security-ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jan  4 11:34:07 cyber-security-ubuntu su[15324]: Successful su for teddy by root
Jan  4 11:34:07 cyber-security-ubuntu su[15324]: + /dev/pts/0 root:teddy
Jan  4 11:34:07 cyber-security-ubuntu su[15324]: pam_unix(su:session): session opened for user teddy by (uid=
0)
Jan  4 11:34:07 cyber-security-ubuntu systemd: pam_unix(systemd-user:session): session opened for user teddy
by (uid=0)
Jan  4 11:34:07 cyber-security-ubuntu systemd-logind[921]: New session 4 of user teddy.
Jan  4 11:34:22 cyber-security-ubuntu sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1018 eu
id=0 tty=/dev/pts/0 ruser=teddy rhost=  user=teddy
Jan  4 11:34:30 cyber-security-ubuntu sudo:    teddy : TTY=pts/0 ; PWD=/home/student ; USER=root ; COMMAND=/u
sr/bin/apt update
Jan  4 11:34:30 cyber-security-ubuntu sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Jan  4 11:34:32 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Jan  4 11:34:50 cyber-security-ubuntu sudo:    teddy : command not allowed ; TTY=pts/0 ; PWD=/home/student ;
USER=root ; COMMAND=/bin/cat /etc/passwd
Jan  4 11:35:05 cyber-security-ubuntu su[15324]: pam_unix(su:session): session closed for user teddy
Jan  4 11:35:05 cyber-security-ubuntu sudo: pam_unix(sudo:session): session closed for user root
Jan  4 11:35:05 cyber-security-ubuntu systemd-logind[921]: Removed session 4.
Jan  4 11:35:05 cyber-security-ubuntu systemd: pam_unix(systemd-user:session): session closed for user teddy
```

The logs here show that both Louise and Teddy get a "command not allowed" message when trying to run "sudo cat /etc/passwd". However it also shows that Teddy, and not shown Louise too, can run "sudo apt update" and it will run, as long as they know their password.



Finder File Edit View Go Window Help
79% Sat 2:14 PM
Unit 08 - Linux SysAdmin 1/Ho
Unit 09 - Linux SysAdmin 2/Lin
/etc/skel creates standard files
linux - Skeleton directory - how
richmond.bootcampcontent.com/Richmo
GitLab Projects Groups More
Cyber-Security-Ubuntu (Snapshot 5) [Running]
Activities Terminal Sat 14:12
student@cyber-security-ubuntu: /etc/skel
File Edit View Search Terminal Help

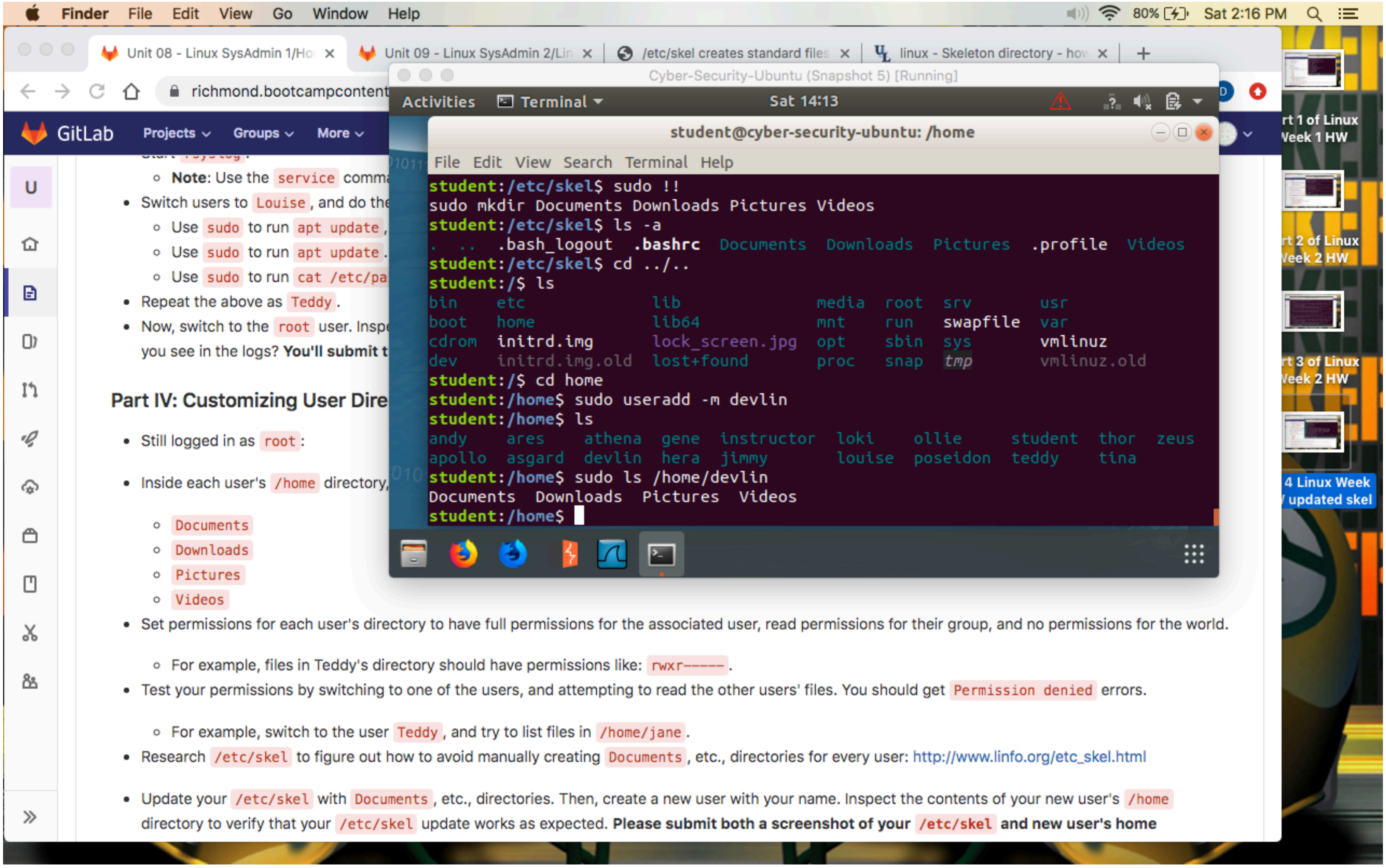
- Note: Use the `service` command.
- Switch users to `Louise`, and do the following:
  - Use `sudo` to run `apt update`, but enter the
  - Use `sudo` to run `apt update`.
  - Use `sudo` to run `cat /etc/passwd`.
- Repeat the above as `Teddy`.
- Now, switch to the `root` user. Inspect `/var/log`
  you see in the logs? **You'll submit this screensh**

Part IV: Customizing User Directories

- Still logged in as `root`:
- Inside each user's `/home` directory, create the fo
  - `Documents`
  - `Downloads`
  - `Pictures`
  - `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.
  - 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**

```
student:/home$ sudo ls /etc/skel
student:/home$ cd ..
student:/$ cd /etc/skel
student:/etc/skel$ ls
student:/etc/skel$ ls -l
total 0
student:/etc/skel$ ls -a
.  ..  .bash_logout  .bashrc  .profile
student:/etc/skel$ mkdir Documents Downloads Pictures Videos
mkdir: cannot create directory ‘Documents’: Permission denied
mkdir: cannot create directory ‘Downloads’: Permission denied
mkdir: cannot create directory ‘Pictures’: Permission denied
mkdir: cannot create directory ‘Videos’: Permission denied
student:/etc/skel$ sudo !!
sudo mkdir Documents Downloads Pictures Videos
student:/etc/skel$ ls -a
.  ..  .bash_logout  .bashrc  Documents  Downloads  Pictures  .profile  Videos
student:/etc/skel$
```

Here I have updated the /etc/skel folder to include the following directories: Documents, Downloads, Pictures, and Videos.


Finder File Edit View Go Window Help
80% Sat 2:16 PM
Unit 08 - Linux SysAdmin 1/Ho
Unit 09 - Linux SysAdmin 2/Lin
/etc/skel creates standard files
linux - Skeleton directory - how
richmond.bootcampcontent
GitLab
Projects
Groups
More
Cyber-Security-Ubuntu (Snapshot 5) [Running]
Activities
Terminal
Sat 14:13
student@cyber-security-ubuntu: /home
File Edit View Search Terminal Help
rt 1 of Linux Week 1 HW
rt 2 of Linux Week 2 HW
rt 3 of Linux Week 2 HW
4 Linux Week updated skel

- Note: Use the `service` comma
- Switch users to `Louise`, and do the
  - Use `sudo` to run `apt update`,
  - Use `sudo` to run `apt update`.
  - Use `sudo` to run `cat /etc/pa`
- Repeat the above as `Teddy`.
- Now, switch to the `root` user. Inspe you see in the logs? **You'll submit t**

Part IV: Customizing User Dire

- Still logged in as `root`:
- Inside each user's `/home` directory,
  - `Documents`
  - `Downloads`
  - `Pictures`
  - `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.
  - 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**

```
student:/etc/skel$ sudo !!
sudo mkdir Documents Downloads Pictures Videos
student:/etc/skel$ ls -a
.  ..  .bash_logout  .bashrc  Documents  Downloads  Pictures  .profile  Videos
student:/etc/skel$ cd ../..
student:/$ ls
bin    etc           lib              media  root  srv       usr
boot   home          lib64            mnt    run   swapfile  var
cdrom  initrd.img    lock_screen.jpg  opt    sbin  sys       vmlinuz
dev    initrd.img.old  lost+found     proc   snap  tmp       vmlinuz.old
student:/$ cd home
student:/home$ sudo useradd -m devlin
student:/home$ ls
andy    ares    athena  gene  instructor  loki    ollie     student  thor  zeus
apollo  asgard  devlin  hera  jimmy       louise  poseidon  teddy    tina
student:/home$ sudo ls /home/devlin
Documents  Downloads  Pictures  Videos
student:/home$
```

Here I have created a new user, myself, with the folders that were added to /etc/skel. Using the command "sudo useradd -m devlin" the new user has Documents, Downloads, Pictures, and Videos upon user creation.