Practical 10 – Linux File System – Security and File Ownership

Objectives

- Understanding /etc/passwd ; /etc/shadow
- lock and unlock password
- groupadd
- Configuring sudo command (/etc/sudoers)
- Sharing files and directory with group ownership (id ; usermod)

Exercise 1 - Understanding /etc/passwd

1. The **/etc/passwd** file stores the user account records. Each line of text contains one user account record. Fields in each record are delimited by colons.

S/N	Field name	Description
1.	User name	This field contains the user name used to log into the system.
2.	User password	This field contains the hash value of the user password. If the value is set to set to "x", the actual password is stored in a separate shadow password file.
3.	User identifier (UID)	This field contains a number used internally by the system to identify the user.
4.	Group identifier (GID)	This field contains a number which identify the primary group of the user. All files that are created by this user initially belong to this group.
5.	Gecos field	This field contains comments describing the account.
6.	Home directory	This field contains the home directory of the user.
7.	Shell program	This field contains the shell program to start when the user logs into the system.

```
student@localhost:~
File  Edit  View  Terminal  Help
[student@localhost ~]$ ls -l /etc/passwd
-rw-r--r--. 1 root root 1646 2010-05-13 18:54 /etc/passwd
[student@localhost ~]$ cat /etc/passwd | tail
apache:x:48:489:Apache:/var/www:/sbin/nologin
saslauth:x:495:488:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
mailnull:x:47:487::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:486::/var/spool/mqueue:/sbin/nologin
smolt:x:494:485:Smolt:/usr/share/smolt:/sbin/nologin
sshd:x:74:484:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
pulse:x:493:483:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:481::/var/lib/gdm:/sbin/nologin
student:x:500:500::/home/student:/bin/bash
guest:x:501:501::/home/guest:/bin/bash
[student@localhost ~]$
```


2. The shadowed password file is located in **etc/shadow**.

S/N	Field Name	Description
1.	User Name	User login name.
2.	Password	Salt and hashed password or a status exception value.
3.	Last change	Days since 1 January 1970 of last password change.
4.	Minimum	The minimum number of days required between password changes.
5.	Maximum	Days before change required.
6.	Warning	Days warning for expiration.
7.	Inactive	Days before account inactive.
8.	Expire	Days since 1 January 1970 when account expires.

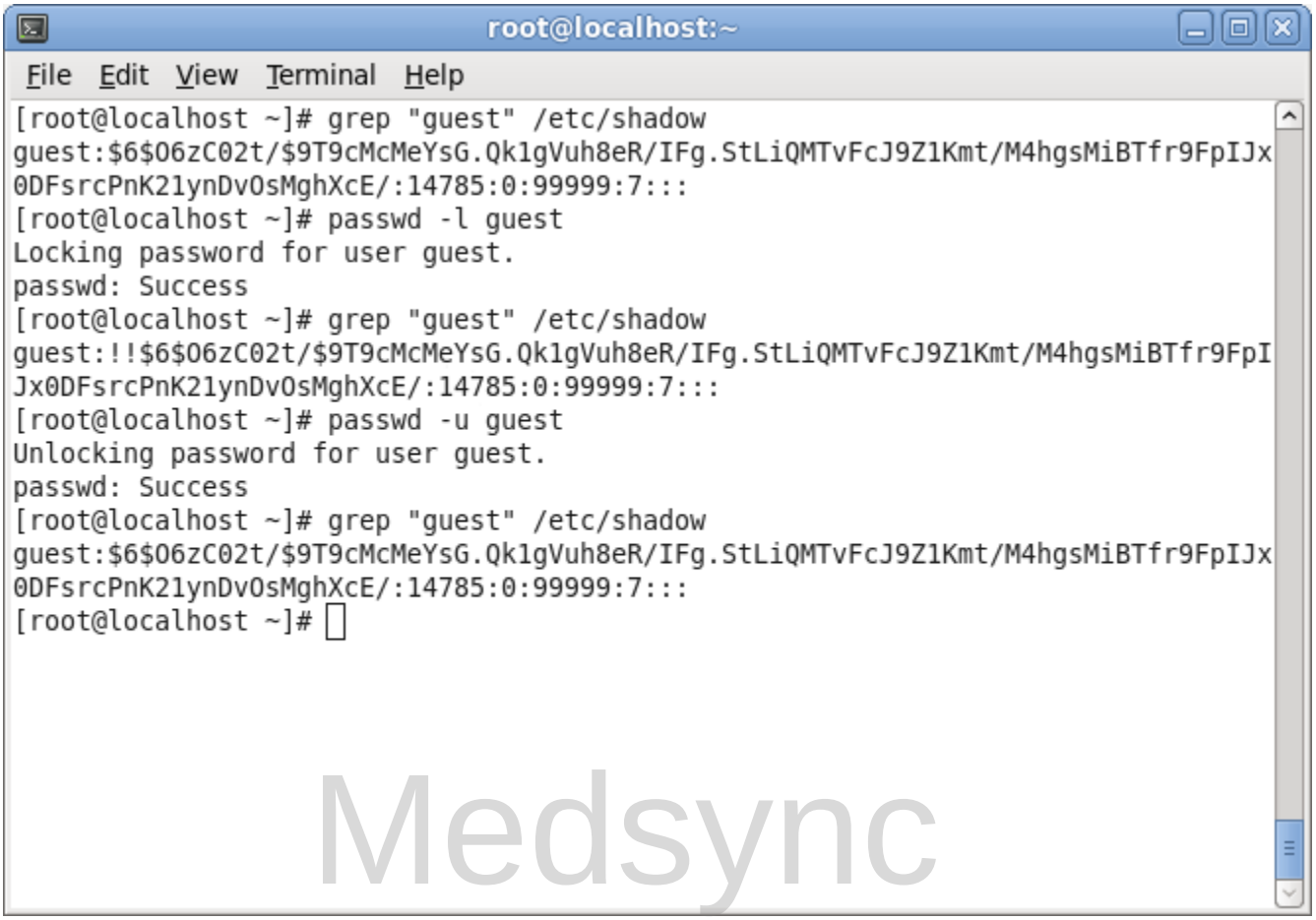
```
root@localhost:~
File  Edit  View  Terminal  Help
[student@localhost ~]$ ls -l /etc/shadow
----------. 1 root root 1156 2010-05-13 18:55 /etc/shadow
[student@localhost ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[student@localhost ~]$ su -
Password:
[root@localhost ~]# cat /etc/shadow | tail -n 1
guest:$6$xZmL95Qn$MhmVXjnHyIP65JACOKf0lOdyRyXqur8PR.9bjQm0r9RxVeAyaCVtol
3BqdK597XPMQ9COVzxn0cueXLF0iDce/:14742:0:99999:7:::
[root@localhost ~]# cat /etc/shadow | tail -n 1 | tr ":" "\n"
guest
$6$xZmL95Qn$MhmVXjnHyIP65JACOKf0lOdyRyXqur8PR.9bjQm0r9RxVeAyaCVtol3BqdK5
97XPMQ9COVzxn0cueXLF0iDce/
14742
0
99999
7



[root@localhost ~]#
```

3. Group information is stored in "/etc/group". Login as root and run the “cat /etc/group” command to display the group information.

4. Follow the steps as show to create a new user "guest".

```
root@localhost:~
File  Edit  View  Terminal  Help
[root@localhost ~]# useradd guest
[root@localhost ~]# grep "guest" /etc/passwd
guest:x:506:507::/home/guest:/bin/bash
[root@localhost ~]# grep "guest" /etc/shadow
guest:!!:14785:0:99999:7:::
[root@localhost ~]# passwd guest
Changing password for user guest.
New password:
Retype new password:
BAD PASSWORD: it is based on a dictionary word
passwd: all authentication tokens updated successfully.
[root@localhost ~]# grep "guest" /etc/shadow
guest:$6$O6zC02t/$9T9cMcMeYsG.Qk1gVuh8eR/IFg.StLiQMTvFcJ9Z1Kmt/M4hgsMiBTfr9FpIJx
0DFsrcPnK21ynDvOsMghXcE/:14785:0:99999:7:::
[root@localhost ~]#
```

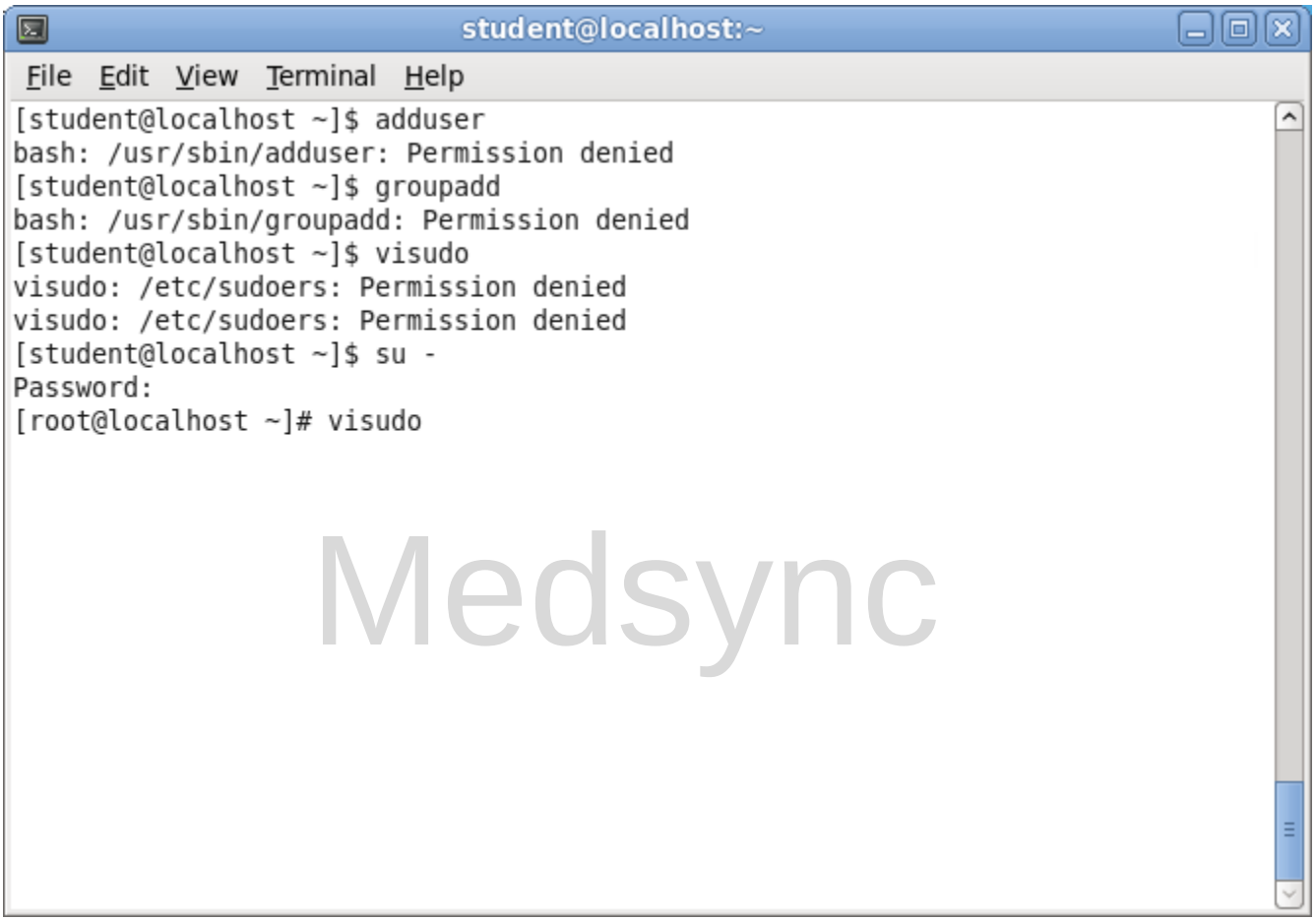

Note
The "!!" in the password field means user login is disabled.


root@localhost:~
File Edit View Terminal Help
[root@localhost ~]# grep "guest" /etc/shadow
guest:6O6zC02t/$9T9cMcMeYsG.Qk1gVuh8eR/IFg.StLiQMTvFcJ9Z1Kmt/M4hgsMiBTfr9FpIJx
0DFsrcPnK21ynDvOsMghXcE/:14785:0:99999:7:::
[root@localhost ~]# passwd -l guest
Locking password for user guest.
passwd: Success
[root@localhost ~]# grep "guest" /etc/shadow
guest:!!6O6zC02t/$9T9cMcMeYsG.Qk1gVuh8eR/IFg.StLiQMTvFcJ9Z1Kmt/M4hgsMiBTfr9FpI
Jx0DFsrcPnK21ynDvOsMghXcE/:14785:0:99999:7:::
[root@localhost ~]# passwd -u guest
Unlocking password for user guest.
passwd: Success
[root@localhost ~]# grep "guest" /etc/shadow
guest:6O6zC02t/$9T9cMcMeYsG.Qk1gVuh8eR/IFg.StLiQMTvFcJ9Z1Kmt/M4hgsMiBTfr9FpIJx
0DFsrcPnK21ynDvOsMghXcE/:14785:0:99999:7:::
[root@localhost ~]#
Medsync

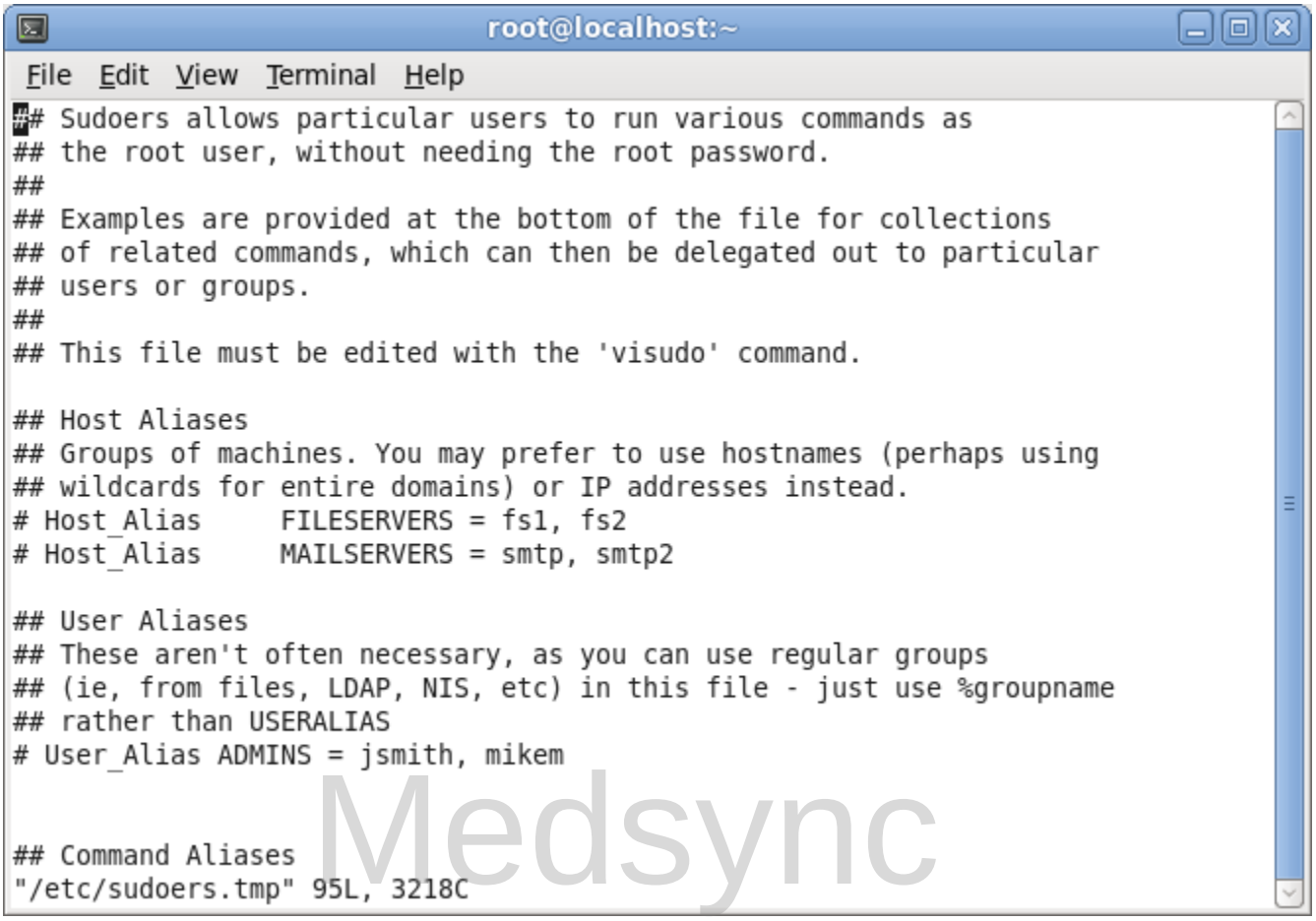
Exercise 2 - Configuring sudo command

1. Login as "student".

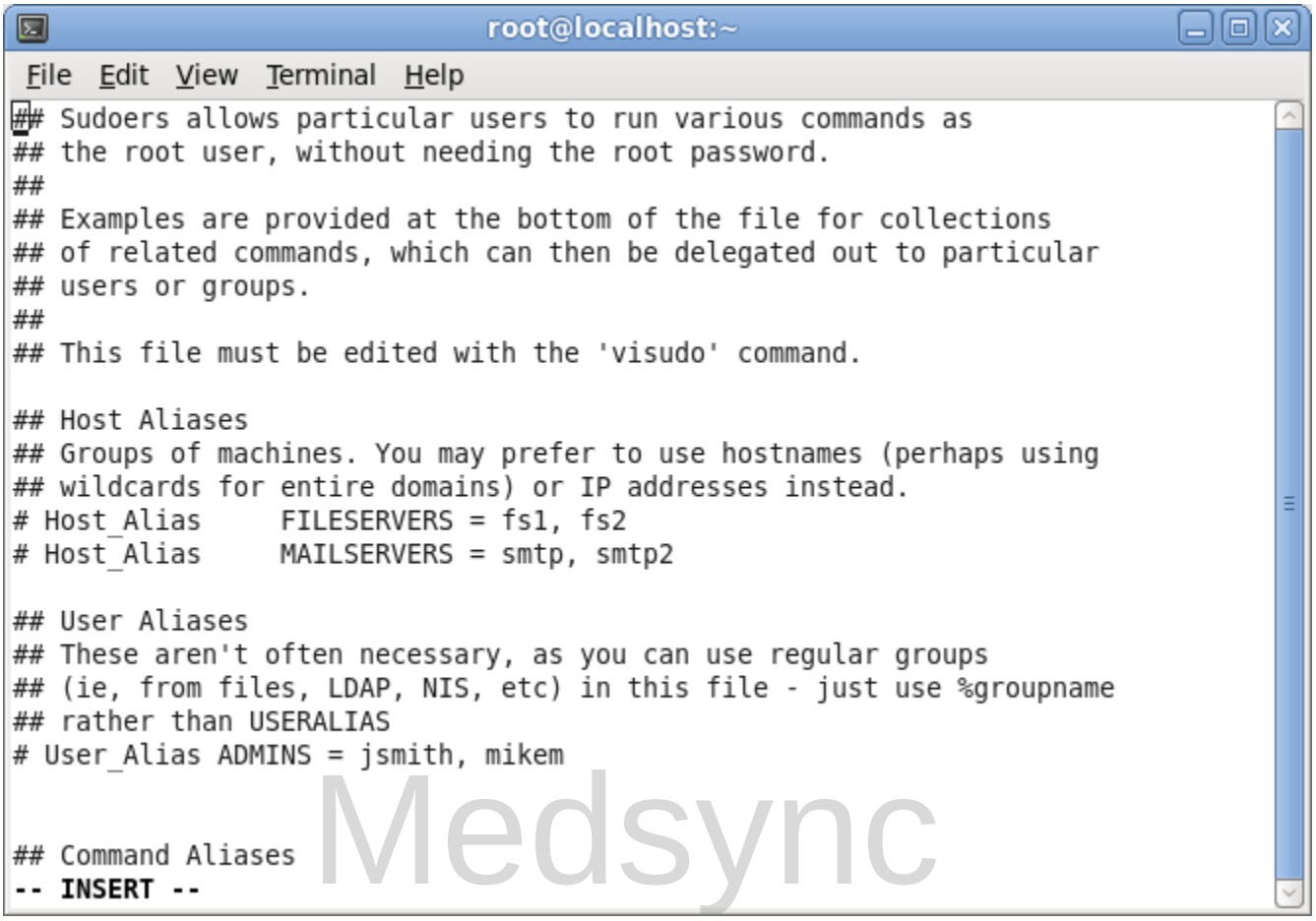
   The **sudo** command allows a permitted user to execute a command as the root or another user, as specified in the **/etc/sudoers** file.



Note
The **visudo** command edit the "sudoers" file. The default editor is the **vi** command. The path to the **visudo** command is "/usr/sbin/visudo".



Press "i" to edit the file.


root@localhost:~
File Edit View Terminal Help
Sudoers allows particular users to run various commands as
the root user, without needing the root password.
##
Examples are provided at the bottom of the file for collections
of related commands, which can then be delegated out to particular
users or groups.
##
This file must be edited with the 'visudo' command.
Host Aliases
Groups of machines. You may prefer to use hostnames (perhaps using
wildcards for entire domains) or IP addresses instead.
Host_Alias FILESERVERS = fs1, fs2
Host_Alias MAILSERVERS = smtp, smtp2
User Aliases
These aren't often necessary, as you can use regular groups
(ie, from files, LDAP, NIS, etc) in this file - just use %groupname
rather than USERALIAS
User_Alias ADMINS = jsmith, mikem
Command Aliases
-- INSERT --
Medsync

In the user alias section, add in the line as shown.

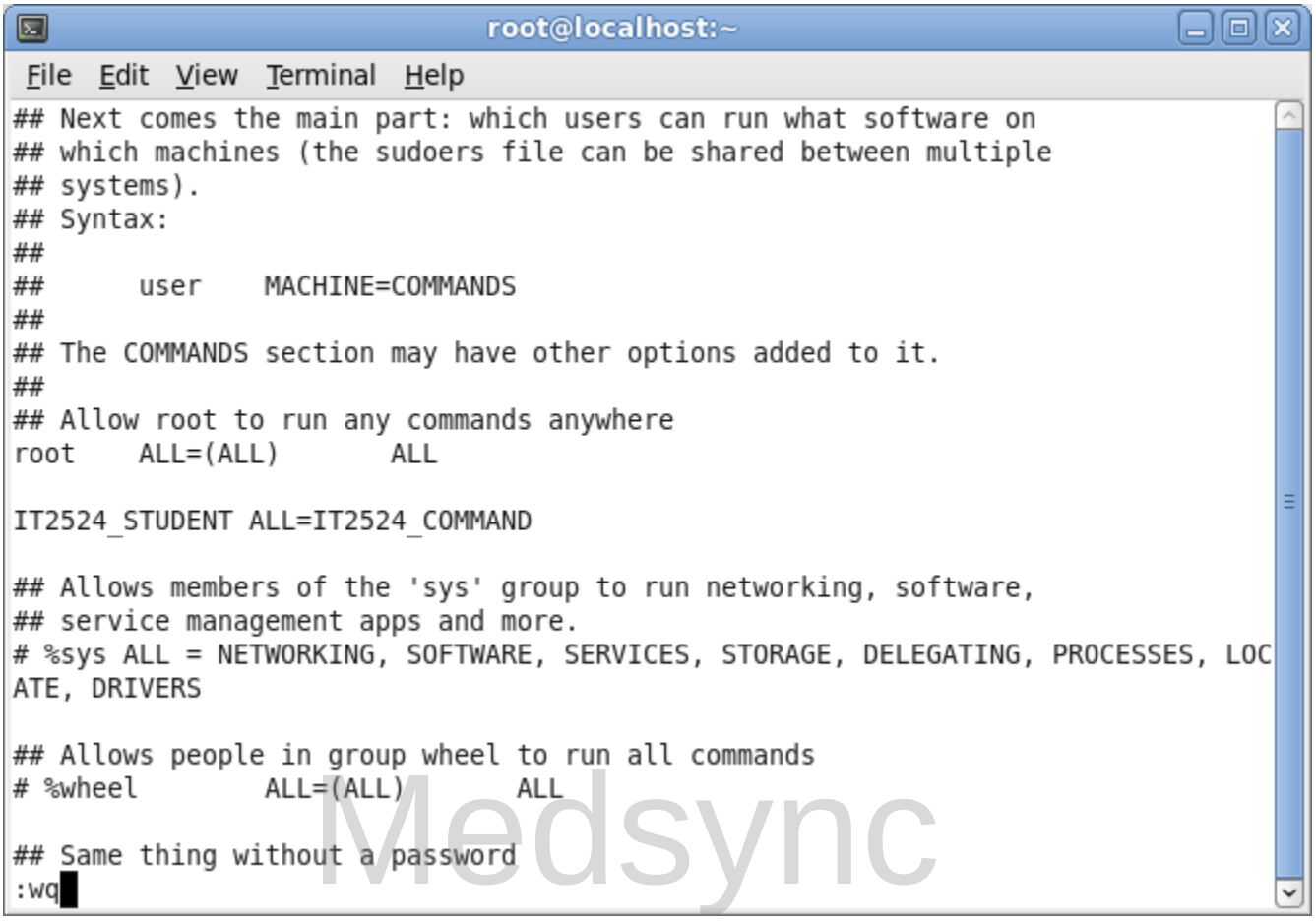
```
root@localhost:~
File  Edit  View  Terminal  Help
## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem
User_Alias  IT2524_STUDENT = student

## Command Aliases
## These are groups of related commands...


## Networking
Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient,
/usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig,
/sbin/mii-tool

## Installation and management of software
Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

## Updating the locate database
-- INSERT --
```

In the command alias section, add in the line as shown.

```
root@localhost:~
File  Edit  View  Terminal  Help
## Command Aliases
## These are groups of related commands...

Cmnd_Alias IT2524_COMMAND = /etc/sbin/visudo

## Networking
Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient,
/usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig,
/sbin/mii-tool

## Installation and management of software
Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig

## Updating the locate database
Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /
bin/mount, /bin/umount

-- INSERT --
```

In the user privilege section, add in the line as shown.
Check that the line allowing “people in group wheel” is commented out.

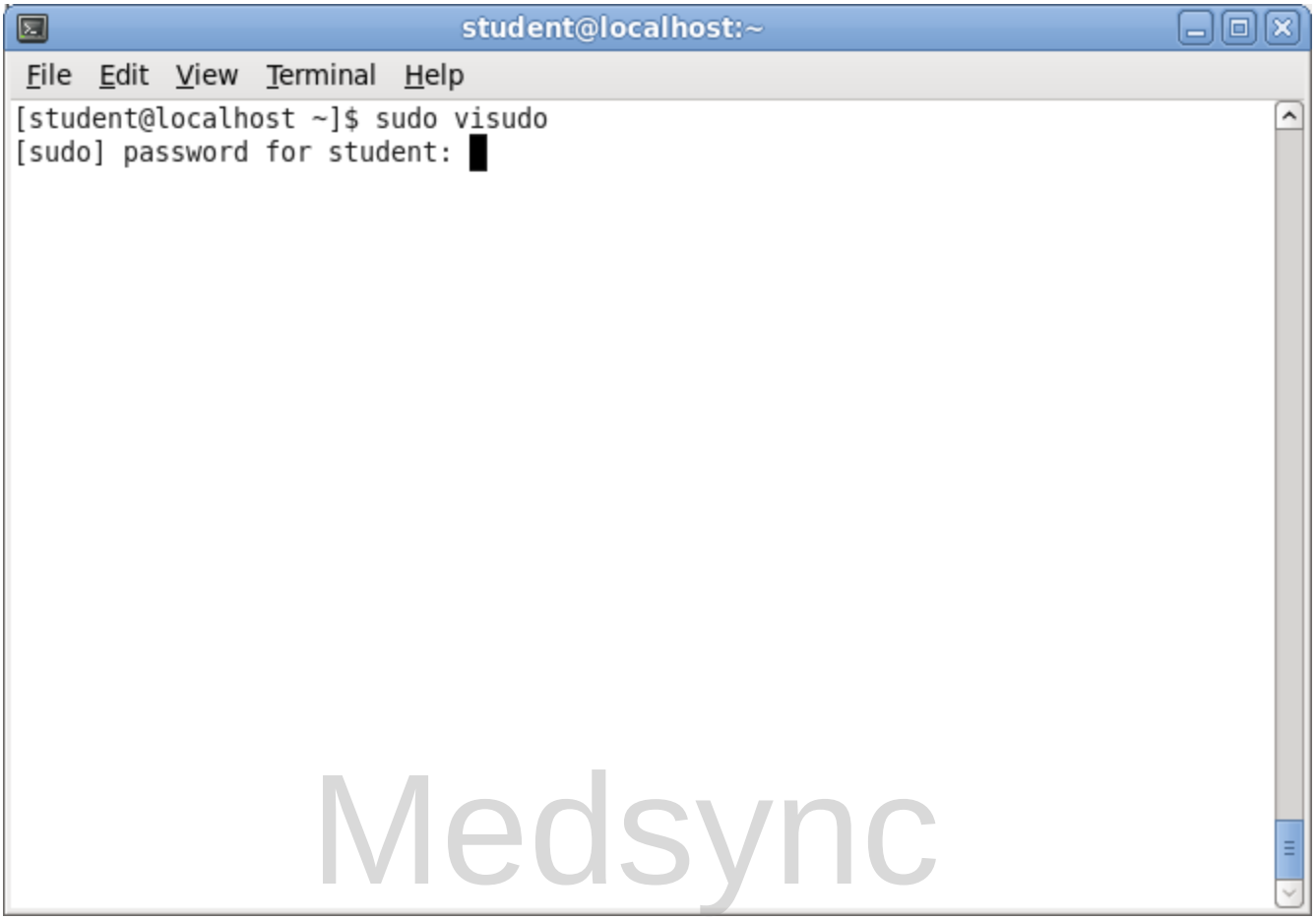
```
root@localhost:~
File  Edit  View  Terminal  Help
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

IT2524_STUDENT ALL=IT2524_COMMAND

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOC
ATE, DRIVERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
-- INSERT --
```



Logout from the root account and execute the "**sudo** visudo".

Are you able to execute the command? If not troubleshoot the configuration.

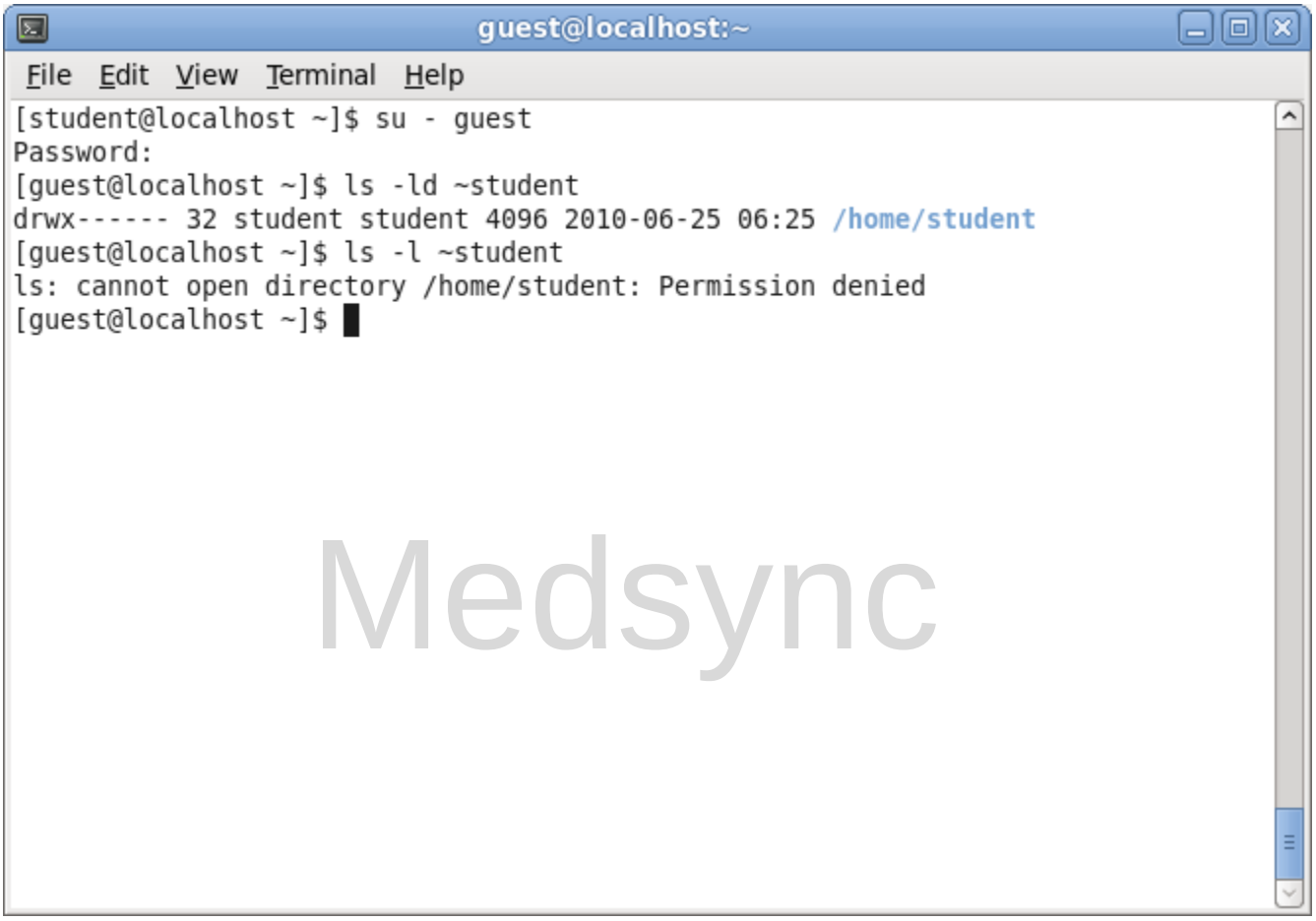
Ans: For the command alias section, the line should instead be:
Cmnd_Alias IT2524_COMMAND = /usr/sbin/visudo


student@localhost:~
File Edit View Terminal Help
[student@localhost ~]$ sudo visudo
[sudo] password for student:
Medsync

Exercise 3 - Sharing files and directory with group ownership

1. The configuration for this exercise is to enable user "student" to share the "~/project" subdirectory with users belonging to the "student" group.

2. Login as user "guest" and try to access the home directory "~student". Are you able to do so?



Login as "student" and follow the steps as shown to enable group access to "~student" and create the "~student/project" subdirectory. Add a file to the "~student/project" subdirectory.

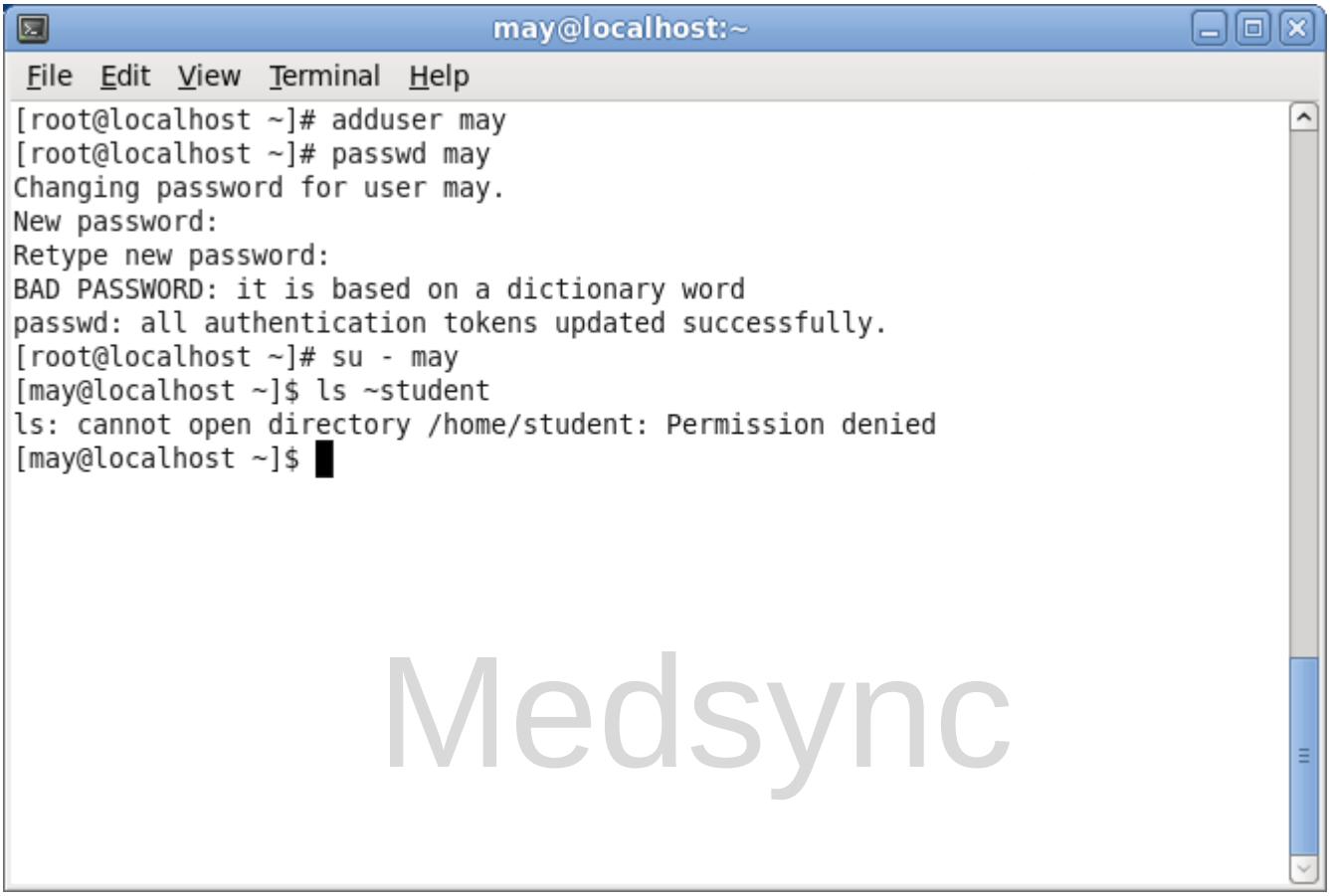
student@localhost:~

File Edit View Terminal Help

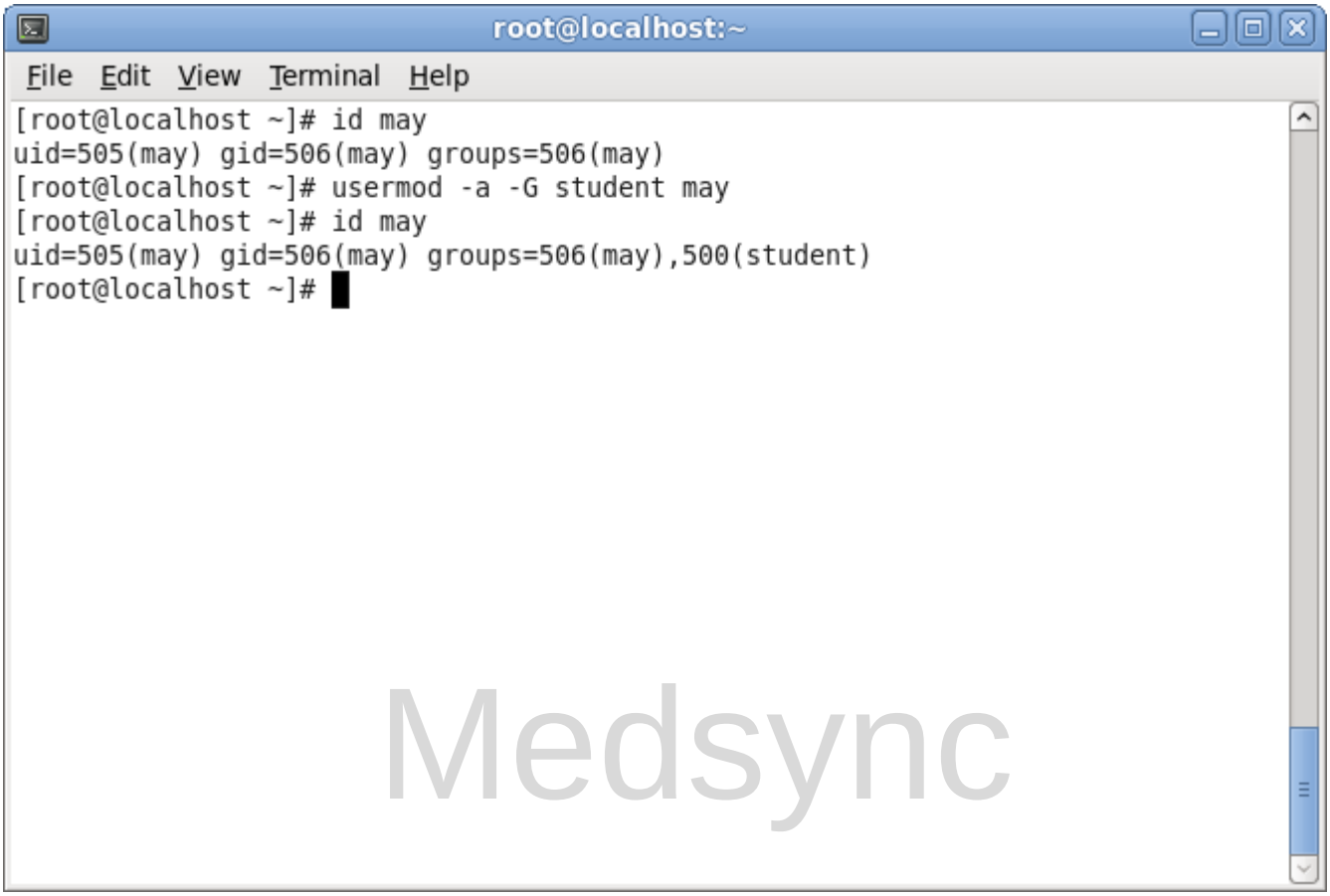
```
[student@localhost ~]$ chmod 750 ~
[student@localhost ~]$ ls -ld ~
drwxr-x--- 31 student student 4096 2010-06-24 23:30 /home/student
[student@localhost ~]$ mkdir project
[student@localhost ~]$ ls -ld ~/project
drwxrwxr-x 2 student student 4096 2010-06-24 23:56 /home/student/project
[student@localhost ~]$ echo "This is document 1." > document1.txt
[student@localhost ~]$ ls -l document1.txt
-rw-rw-r-- 1 student student 20 2010-06-24 23:57 document1.txt
[student@localhost ~]$
```

Edit : create the document1.txt inside project by first typing 'cd project'

Login as "root" and follow the steps as shown to create a new user "may" and verify if user "may" access the home directory "~student".



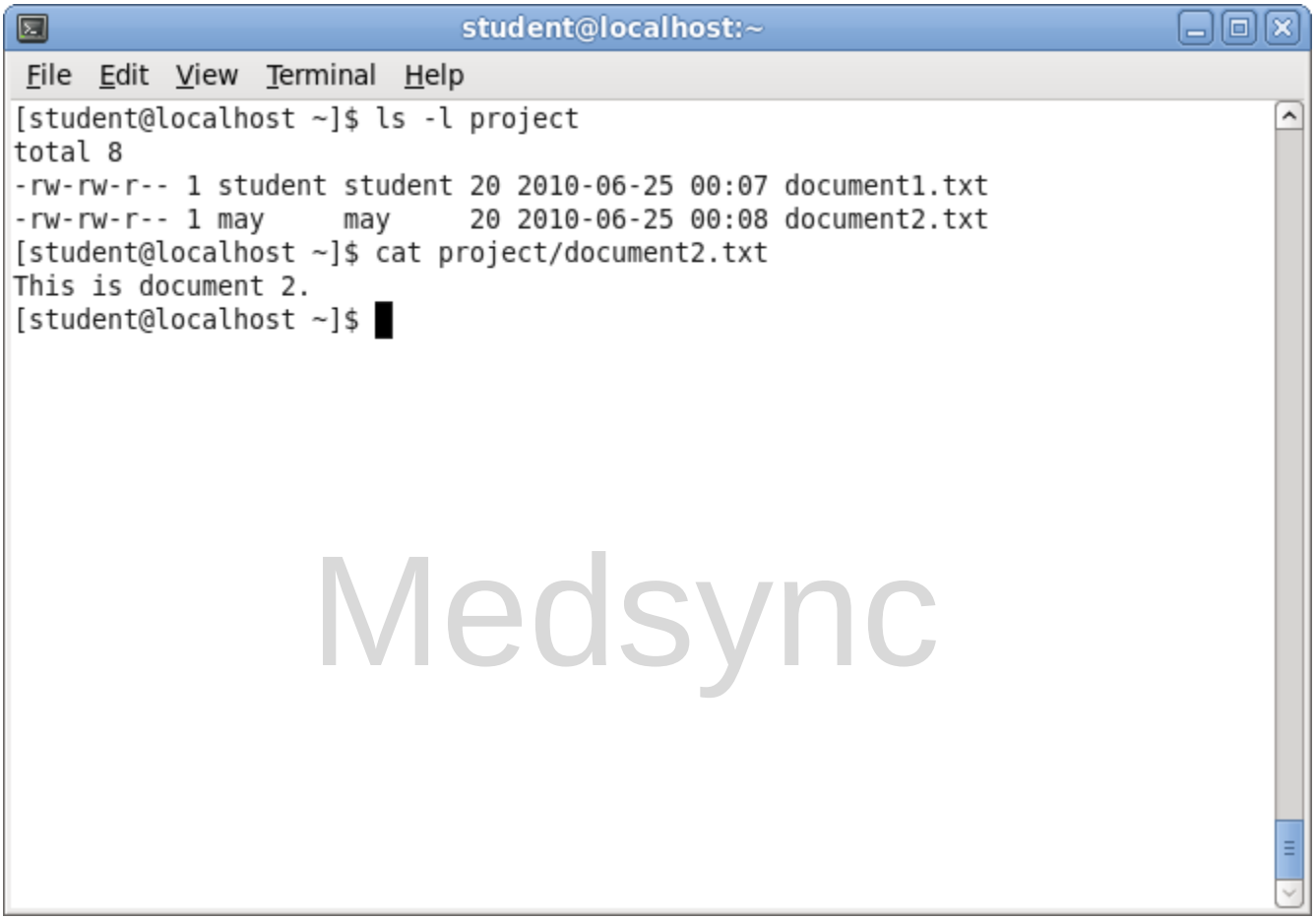
Login as "root" and follow the steps as shown to add user "may" to the "student" group.



Login as "may" to and follow the steps as shown access the "~student/project" subdirectory.

```
may@localhost:~
File  Edit  View  Terminal  Help
[may@localhost ~]$ ls -ld ~student
drwxr-x--- 32 student student 4096 2010-06-25 00:05 /home/student
[may@localhost ~]$ ls -l ~student/project
total 0
[may@localhost ~]$ ls -l ~student/project
total 4
-rw-rw-r-- 1 student student 20 2010-06-25 00:07 document1.txt
[may@localhost ~]$ cat ~student/project/document1.txt
This is document 1.
[may@localhost ~]$ echo "This is document 2." > ~student/project/document2.txt
[may@localhost ~]$ cat ~student/project/document2.txt
This is document 2.
[may@localhost ~]$ ls -l ~student/project
total 8
-rw-rw-r-- 1 student student 20 2010-06-25 00:07 document1.txt
-rw-rw-r-- 1 may     may     20 2010-06-25 00:08 document2.txt
[may@localhost ~]$
```

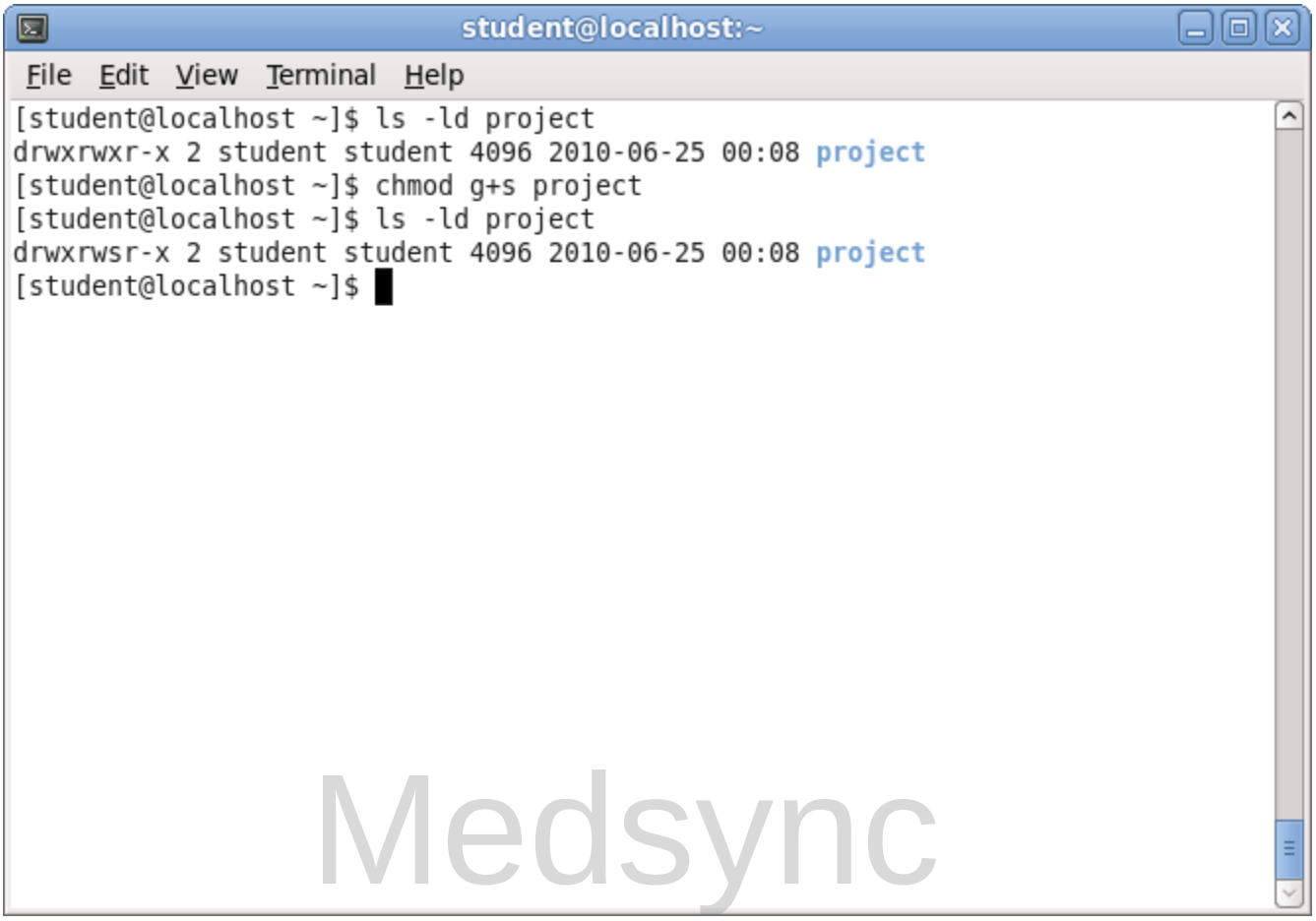
Login as "student" and follow the steps as shown to verify if user "student" have read permission to the file "~student/project/document2.txt". Without verifying using commands, does user "student" have write permission to the same file?



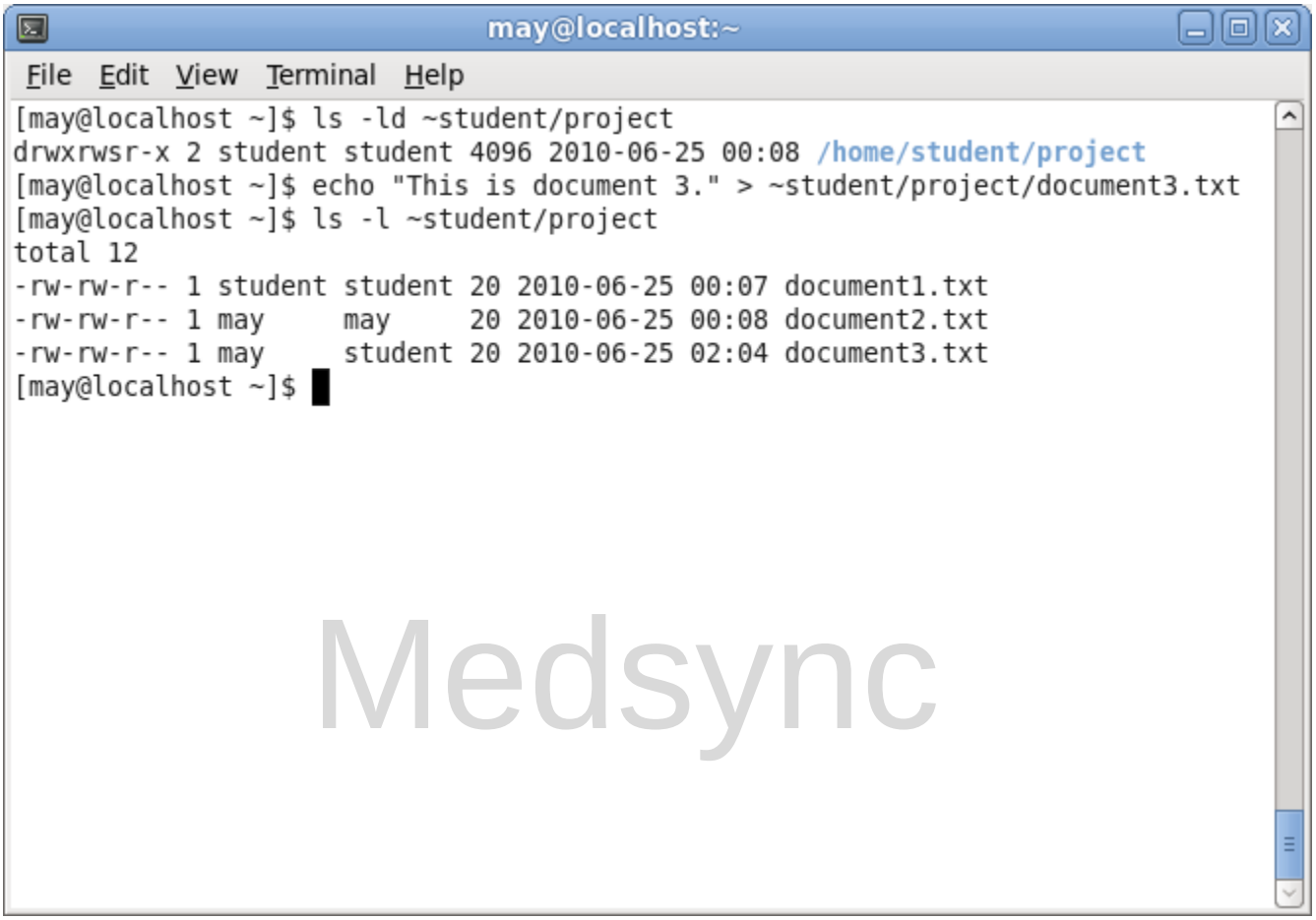
3. Compare the group ownership of the files in the "~student/project" directory. You will notice that the group ownership of the files created by user "may" is not "student".

4. Login as "student" and follow the steps as shown to set the SGID ("set Group ID") of the "~student/project".

> **Note**
> If the SGID bit on a directory entry is set, files in that directory will have the group ownership as the directory, instead of the group of the user that created the file.


student@localhost:~
File Edit View Terminal Help
[student@localhost ~]$ ls -ld project
drwxrwxr-x 2 student student 4096 2010-06-25 00:08 project
[student@localhost ~]$ chmod g+s project
[student@localhost ~]$ ls -ld project
drwxrwsr-x 2 student student 4096 2010-06-25 00:08 project
[student@localhost ~]$
Medsync

Login as "may" and follow the steps as shown to create a new file "~student/project/document3.txt". Are the group ownership of "document2.txt" and "document3.txt" the same?



Login as "student" and follow the steps to verify the permissions of all the files in "~student/project".