

CYB613: Operating Systems Theory and Administration
Lab4: File Permission

Objective:

To learn how to manage and secure files in Linux OS

Complete Lab 9.1 thru 9.5 from the lab textbook. Rename this lab sheet to
[CYB613.lab4.firstName.lastName.docx](#)

Lab 9.1: Managing File Permissions

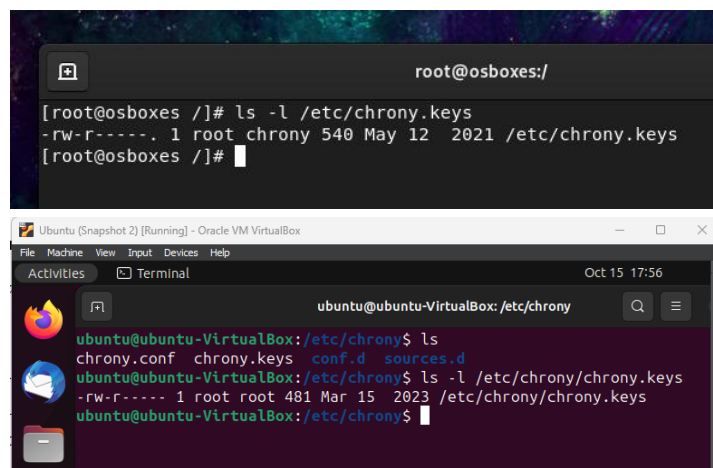
Aside of step 1 & Step 10, provide a screenshot evidence of the successful execution of the command run below each step in the lab.

STEP 1. Open a terminal window. *(no need to provide screenshot for this step)*

STEP 2. Execute the correct command to display the permissions on the `/etc/chrony.keys` file.

`ls -l /etc/chrony.keys`

or `ls -l /etc/chrony/chrony.keys`



The image contains two screenshots of terminal windows. The top screenshot shows a terminal window titled 'root@osboxes:/' with the command '[root@osboxes ~]# ls -l /etc/chrony.keys' and its output: '-rw-r-----. 1 root chrony 540 May 12 2021 /etc/chrony.keys'. The bottom screenshot shows a terminal window titled 'ubuntu@ubuntu-VirtualBox: /etc/chrony' with the command 'ubuntu@ubuntu-VirtualBox: /etc/chrony\$ ls' and its output: 'chrony.conf chrony.keys conf.d sources.d'. It also shows the command 'ubuntu@ubuntu-VirtualBox: /etc/chrony\$ ls -l /etc/chrony/chrony.keys' and its output: '-rw-r-----. 1 root root 481 Mar 15 2023 /etc/chrony/chrony.keys'.

STEP 3. Based on the output of the command from step 2, which user owns the `/etc/chrony.keys` file?

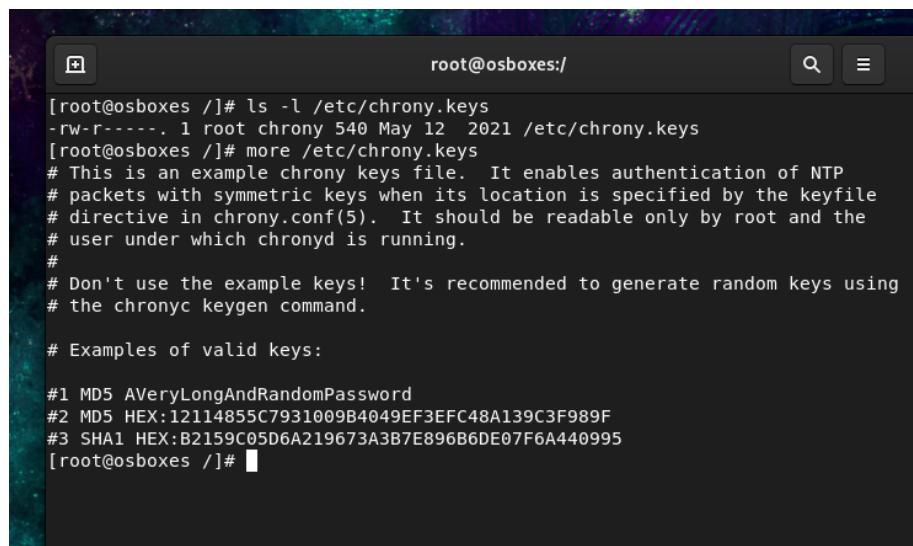
Owner

STEP 4. Based on the output of the command from step 2, which group owns the `/etc/chrony.keys` file?

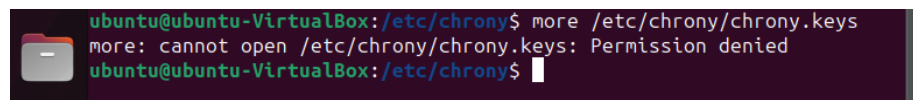
Group

STEP 5. Execute the `more/etc/chrony.keys` command and then explain why the command failed.

Because we don't have the necessary permissions to read the file.

A terminal window titled 'root@osboxes:/' showing the command 'ls -l /etc/chrony.keys' and its output: '-rw-r-----. 1 root chrony 540 May 12 2021 /etc/chrony.keys'. Then, the command 'more /etc/chrony.keys' is executed, displaying the contents of the file, which includes instructions on how to use the keys file and examples of valid keys.

```
root@osboxes:/  
[root@osboxes /]# ls -l /etc/chrony.keys  
-rw-r-----. 1 root chrony 540 May 12 2021 /etc/chrony.keys  
[root@osboxes /]# more /etc/chrony.keys  
# This is an example chrony keys file. It enables authentication of NTP  
# packets with symmetric keys when its location is specified by the keyfile  
# directive in chrony.conf(5). It should be readable only by root and the  
# user under which chronyd is running.  
#  
# Don't use the example keys! It's recommended to generate random keys using  
# the chronyc keygen command.  
  
# Examples of valid keys:  
  
#1 MD5 AVeryLongAndRandomPassword  
#2 MD5 HEX:12114855C7931009B4049EF3EFC48A139C3F989F  
#3 SHA1 HEX:B2159C05D6A219673A3B7E896B6DE07F6A440995  
[root@osboxes /]#
```

A terminal window titled 'ubuntu@ubuntu-VirtualBox:/etc/chrony\$' showing the command 'more /etc/chrony/chrony.keys' and its output: 'more: cannot open /etc/chrony/chrony.keys: Permission denied'.

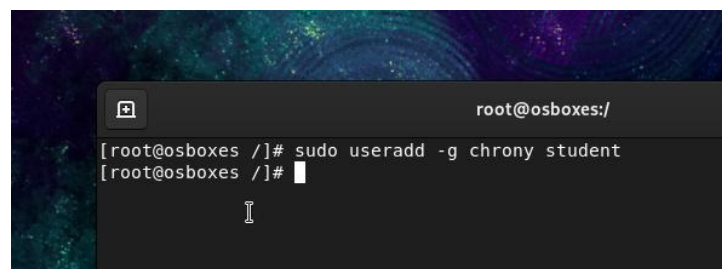
```
ubuntu@ubuntu-VirtualBox:/etc/chrony$ more /etc/chrony/chrony.keys  
more: cannot open /etc/chrony/chrony.keys: Permission denied  
ubuntu@ubuntu-VirtualBox:/etc/chrony$
```

STEP 6. Switch to the root account using the `su` command.

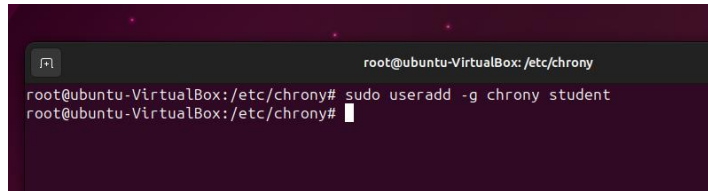
Switching to root user using su or sudo su

STEP 7. Execute the correct command to add the student user to the chrony group.

sudo useradd -g chrony student

A terminal window titled 'root@osboxes:/' showing the command 'sudo useradd -g chrony student' and its successful execution.

```
root@osboxes:/  
[root@osboxes /]# sudo useradd -g chrony student  
[root@osboxes /]#
```



```
root@ubuntu-VirtualBox: /etc/chrony
root@ubuntu-VirtualBox:/etc/chrony# sudo useradd -g chorny student
root@ubuntu-VirtualBox:/etc/chrony#
```

STEP 8. Log out of the system. (Note that this is necessary for the group ownership to take effect.)

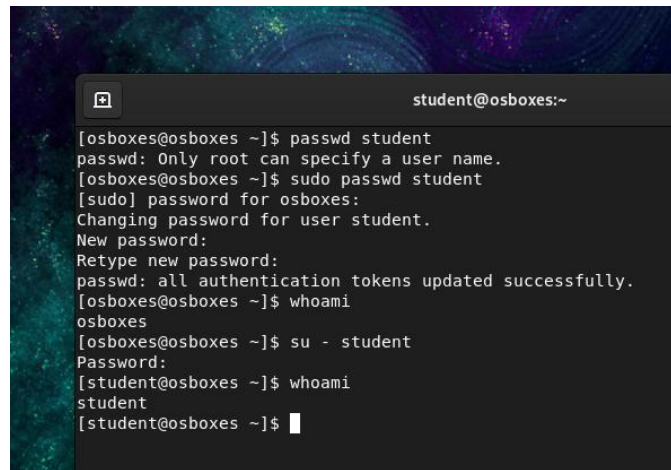
Logout or exit



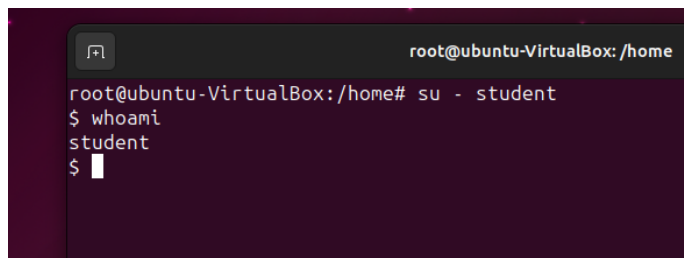
```
osboxes@osboxes:~
[root@osboxes /]# exit
exit
[osboxes@osboxes ~]$
```

STEP 9. Log in as the student user.

su – student



```
student@osboxes:~
[osboxes@osboxes ~]$ passwd student
passwd: Only root can specify a user name.
[osboxes@osboxes ~]$ sudo passwd student
[sudo] password for osboxes:
Changing password for user student.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[osboxes@osboxes ~]$ whoami
osboxes
[osboxes@osboxes ~]$ su - student
Password:
[student@osboxes ~]$ whoami
student
[student@osboxes ~]$
```

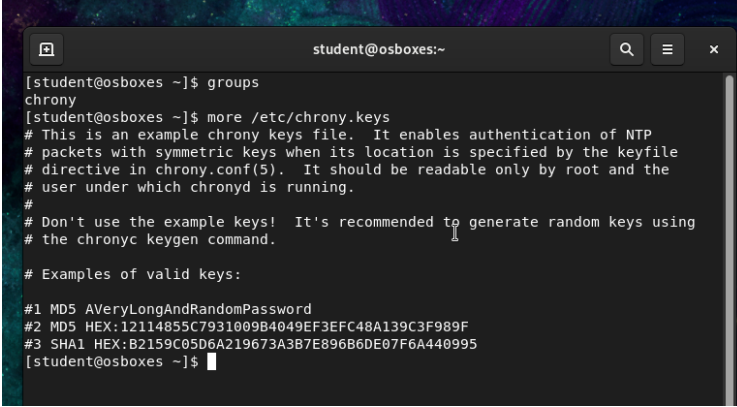


```
root@ubuntu-VirtualBox: /home
root@ubuntu-VirtualBox:/home# su - student
$ whoami
student
$
```

STEP 10. Open a terminal window. *(no need to provide screenshot for this step)*

STEP 11. Execute the correct command to display the current user's groups.

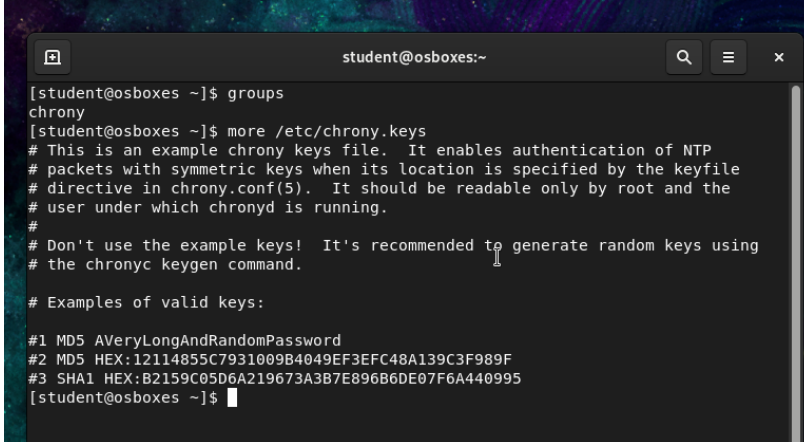
groups



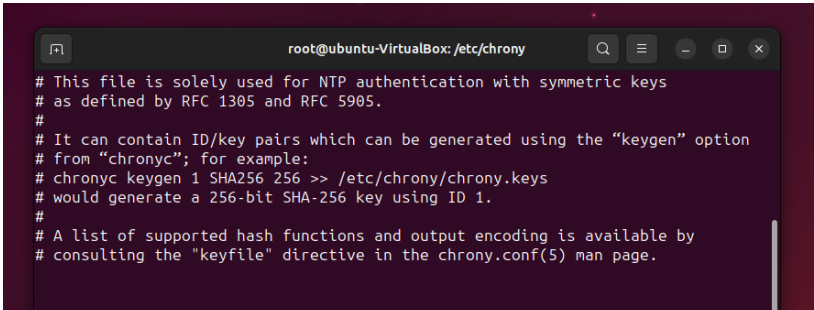
```
student@osboxes:~  
[student@osboxes ~]$ groups  
chrony  
[student@osboxes ~]$ more /etc/chrony.keys  
# This is an example chrony keys file. It enables authentication of NTP  
# packets with symmetric keys when its location is specified by the keyfile  
# directive in chrony.conf(5). It should be readable only by root and the  
# user under which chronyd is running.  
#  
# Don't use the example keys! It's recommended to generate random keys using  
# the chronyc keygen command.  
#  
# Examples of valid keys:  
#1 MD5 AVeryLongAndRandomPassword  
#2 MD5 HEX:12114855C7931009B4049EF3EFC48A139C3F989F  
#3 SHA1 HEX:B2159C05D6A219673A3B7E896B6DE07F6A440995  
[student@osboxes ~]$
```

STEP 12. Execute the *more/etc/chrony.keys* command to verify that this file's contents can now be displayed by the student user.

more/etc/chrony/chrony.keys



```
student@osboxes:~  
[student@osboxes ~]$ groups  
chrony  
[student@osboxes ~]$ more /etc/chrony.keys  
# This is an example chrony keys file. It enables authentication of NTP  
# packets with symmetric keys when its location is specified by the keyfile  
# directive in chrony.conf(5). It should be readable only by root and the  
# user under which chronyd is running.  
#  
# Don't use the example keys! It's recommended to generate random keys using  
# the chronyc keygen command.  
#  
# Examples of valid keys:  
#1 MD5 AVeryLongAndRandomPassword  
#2 MD5 HEX:12114855C7931009B4049EF3EFC48A139C3F989F  
#3 SHA1 HEX:B2159C05D6A219673A3B7E896B6DE07F6A440995  
[student@osboxes ~]$
```

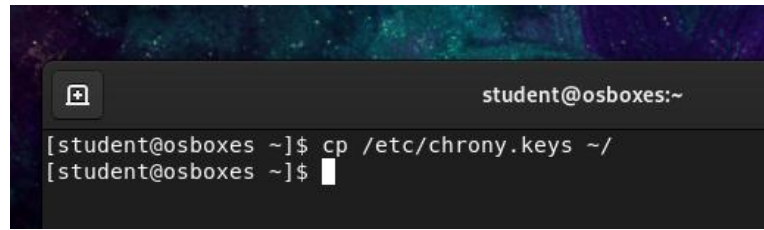


```
root@ubuntu-VirtualBox: /etc/chrony  
# This file is solely used for NTP authentication with symmetric keys  
# as defined by RFC 1305 and RFC 5905.  
#  
# It can contain ID/key pairs which can be generated using the "keygen" option  
# from "chronyc"; for example:  
# chronyc keygen 1 SHA256 256 >> /etc/chrony/chrony.keys  
# would generate a 256-bit SHA-256 key using ID 1.  
#  
# A list of supported hash functions and output encoding is available by  
# consulting the "keyfile" directive in the chrony.conf(5) man page.
```

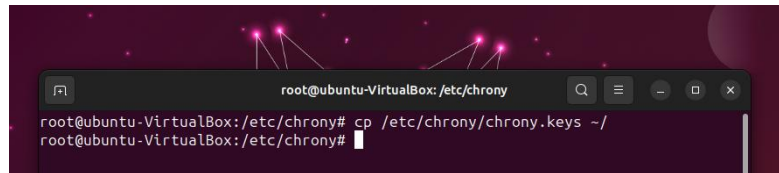
STEP 13. Copy the */etc/chrony.keys* file to the current directory (the home directory for the student user).

cp /etc/chrony/chrony.keys ~/

`cp /etc/chrony.keys ~/`



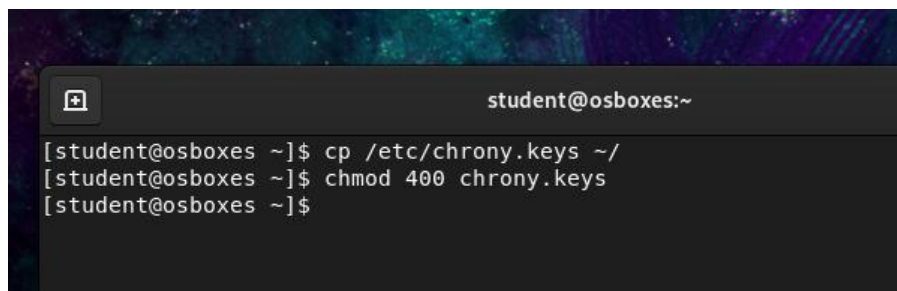
```
student@osboxes:~  
[student@osboxes ~]$ cp /etc/chrony.keys ~/
```



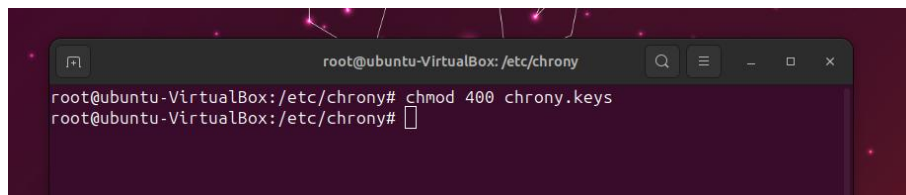
```
root@ubuntu-VirtualBox:/etc/chrony  
root@ubuntu-VirtualBox:/etc/chrony# cp /etc/chrony/chrony.keys ~/
```

STEP 14. Using octal notation, change the permissions of the *chrony.keys* file that is in the current directory to *-r-----*.

`chmod 400 chrony.keys`



```
student@osboxes:~  
[student@osboxes ~]$ cp /etc/chrony.keys ~/
```



```
root@ubuntu-VirtualBox:/etc/chrony  
root@ubuntu-VirtualBox:/etc/chrony# chmod 400 chrony.keys
```

STEP 15. Using symbolic notation, change the permissions of the *chrony.keys* file that is in the current directory to allow group members the read permission.

`chmod g+r chrony.keys`



```
student@osboxes:~  
[student@osboxes ~]$ chmod g+r chrony.keys
```

```
root@ubuntu-VirtualBox: /etc/chrony
root@ubuntu-VirtualBox:/etc/chrony# chmod g+r chrony.keys
root@ubuntu-VirtualBox:/etc/chrony#
```

STEP 16. Using octal notation, try to change the permissions of the *chrony.keys* file that is in the */etc* directory to *-r-----*. Explain why this command fails.

`sudo chmod 400 /etc/chrony.keys`

//This command fails due to lack of permissions or due to SELinux or AppArmor Policies

```
student@osboxes:~
[student@osboxes ~]$ sudo chmod 400 /etc/chrony.keys
[sudo] password for student:
student is not in the sudoers file. This incident will be reported.
[student@osboxes ~]$
```

```
student@osboxes:~
[student@osboxes ~]$ sudo chmod 400 /etc/chrony.keys
[sudo] password for student:
student is not in the sudoers file. This incident will be reported.
[student@osboxes ~]$ ls -l /etc/chrony.keys
-rw-r-----. 1 root chrony 540 May 12 2021 /etc/chrony.keys
[student@osboxes ~]$
```

```
root@ubuntu-VirtualBox: /etc/chrony
root@ubuntu-VirtualBox:/etc/chrony# sudo chmod 400 /etc/chrony/chrony.keys
root@ubuntu-VirtualBox:/etc/chrony#
```

STEP 17. Change the mask value for the current shell so any new directory would have the following permissions: *drwxr-x---*

`umask 027`

```
student@osboxes:/etc
[student@osboxes etc]$ umask 027
[student@osboxes etc]$
```

```
root@ubuntu-VirtualBox: /etc/chrony
root@ubuntu-VirtualBox: /etc/chrony# umask 027
root@ubuntu-VirtualBox: /etc/chrony#
```

STEP 18. Based on the mask value from step 17, what permissions would all new files that are created in this shell have?

drwxr-x---

The permissions `drwxr-x---` can be classified as follows:

- The leading `d` indicates that it's a directory.
- Owner (User): Read, Write, and Execute (rwx)
- Group: Read and Execute (r-x)
- Others: No Permissions (---)

Lab 9.2 Managing Special Permissions

List the commands you will use without the need to provide a screenshot

Scenario 1: You are concerned about SUID permissions on this system. Start by running the command to find all files that have SUID permissions set. Then change the *newgrp* command so it is not a SUID file.

find / -type f -perm /4000

sudo chmod u-s /usr/bin/newgrp

```
student@osboxes:/
[student@osboxes /]$ find / -type f -perm /4000
find: '/boot/efi/EFI/centos': Permission denied
find: '/boot/grub2': Permission denied
find: '/boot/loader/entries': Permission denied
find: '/home/osboxes': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1/task/1/fd': Permission denied
find: '/proc/1/task/1/ns': Permission denied
find: '/proc/1/fd': Permission denied
find: '/proc/1/map_files': Permission denied
find: '/proc/1/ns': Permission denied
find: '/proc/2/task/2/fd': Permission denied
find: '/proc/2/task/2/ns': Permission denied
find: '/proc/2/fd': Permission denied
find: '/proc/2/map_files': Permission denied
find: '/proc/2/ns': Permission denied
find: '/proc/3/task/3/fd': Permission denied
find: '/proc/3/task/3/ns': Permission denied
find: '/proc/3/fd': Permission denied
find: '/proc/3/map_files': Permission denied
find: '/proc/3/ns': Permission denied

root@osboxes:/home/osboxes
/usr/bin/fusermount3
/usr/bin/mount
/usr/bin/umount
/usr/bin/su
/usr/bin/vmware-user-suid-wrapper
/usr/bin/pkexec
/usr/bin/crontab
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/Xorg.wrap
/usr/libexec/dbus-1/dbus-daemon-launch-helper
/usr/libexec/cockpit-session
/usr/libexec/sss/krb5_child
/usr/libexec/sss/ldap_child
/usr/libexec/sss/selinux_child
[root@osboxes osboxes]#
```



```
root@osboxes:/home/osboxes
[root@osboxes osboxes]# sudo chmod u-s /usr/bin/newgrp
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /home/ubuntu/Desktop
root@ubuntu-VirtualBox: /home/ubuntu/Desktop# find / -type f -perm /4000
find: '/run/user/1000/gvfs': Permission denied
find: '/run/user/1000/doc': Permission denied
/usr/libexec/polkit-agent-helper-1
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/fusermount3
/usr/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/su
/usr/bin/mount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/sbin/pppd
find: '/proc/2165/task/2165/fdinfo/6': No such file or directory
find: '/proc/2165/fdinfo/5': No such file or directory
/snap/snapd/20290/usr/lib/snapd/snap-confine
/snap/snapd/20092/usr/lib/snapd/snap-confine
/snap/core22/864/usr/bin/chfn
/snap/core22/864/usr/bin/chsh
/snap/core22/864/usr/bin/gpasswd
/snap/core22/864/usr/bin/mount
/snap/core22/864/usr/bin/newgrp
/snap/core22/864/usr/bin/passwd
/snap/core22/864/usr/bin/su
/snap/core22/864/usr/bin/sudo
/snap/core22/864/usr/bin/umount
/snap/core22/864/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core22/864/usr/lib/openssh/ssh-keysign
/snap/core22/687/usr/bin/chfn
/snap/core22/687/usr/bin/chsh
/snap/core22/687/usr/bin/gpasswd
/snap/core22/687/usr/bin/mount
/snap/core22/687/usr/bin/newgrp
/snap/core22/687/usr/bin/passwd
/snap/core22/687/usr/bin/su
/snap/core22/687/usr/bin/sudo
/snap/core22/687/usr/bin/umount
/snap/core22/687/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core22/687/usr/lib/openssh/ssh-keysign
root@ubuntu-VirtualBox: /home/ubuntu/Desktop
```

```
root@ubuntu-VirtualBox: /
root@ubuntu-VirtualBox: /# sudo chmod u-s /usr/bin/newgrp
root@ubuntu-VirtualBox: /#
```

Scenario 2: Three users need to share files on the system, but no other user can have access to these files. Create user accounts for sophia, olivia, and emma, using default values for account parameters. Create a common group named shared, which will be used to allow these three users to share files with each other. Finally, create a directory named `/home/shared` for only these three users to access and to also automatically give group ownership of all new files to the shared group.

paste a screen shot, below, for the file showing after you make the changes.

```
root@osboxes:/home/osboxes
[root@osboxes osboxes]# sudo useradd sophia
[root@osboxes osboxes]# sudo useradd olivia
[root@osboxes osboxes]# sudo useradd emma
[root@osboxes osboxes]# sudo groupadd shared

root@osboxes:/home/osboxes
[root@osboxes osboxes]# sudo usermod -aG shared sophia
[root@osboxes osboxes]# sudo usermod -aG shared olivia
[root@osboxes osboxes]# sudo usermod -aG shared emma
[root@osboxes osboxes]# sudo mkdir /home/shared
[root@osboxes osboxes]#
```



```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# sudo usermod -aG shared sophia
[root@osboxes osboxes]# sudo usermod -aG shared olivia
[root@osboxes osboxes]# sudo usermod -aG shared emma
[root@osboxes osboxes]# sudo mkdir /home/shared
[root@osboxes osboxes]# sudo chown :shared /home/shared
[root@osboxes osboxes]# sudo chmod 770 /home/shared
[root@osboxes osboxes]#
```

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# sudo usermod -aG shared sophia
[root@osboxes osboxes]# sudo usermod -aG shared olivia
[root@osboxes osboxes]# sudo usermod -aG shared emma
[root@osboxes osboxes]# sudo mkdir /home/shared
[root@osboxes osboxes]# sudo chown :shared /home/shared
[root@osboxes osboxes]# sudo chmod 770 /home/shared
[root@osboxes osboxes]# grep shared /etc/group
shared:x:1005:sophia,olivia,emma
[root@osboxes osboxes]#
```

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# sudo usermod -aG shared sophia
[root@osboxes osboxes]# sudo usermod -aG shared olivia
[root@osboxes osboxes]# sudo usermod -aG shared emma
[root@osboxes osboxes]# sudo mkdir /home/shared
[root@osboxes osboxes]# sudo chown :shared /home/shared
[root@osboxes osboxes]# sudo chmod 770 /home/shared
[root@osboxes osboxes]# grep shared /etc/group
shared:x:1005:sophia,olivia,emma
[root@osboxes osboxes]# ls -ld /home/shared
drwxrwx---. 2 root shared 6 Oct 16 18:20 /home/shared
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# sudo useradd sophia
root@ubuntu-VirtualBox:/# sudo useradd olivia
root@ubuntu-VirtualBox:/# sudo useradd emma
root@ubuntu-VirtualBox:/# sudo groupadd shared
root@ubuntu-VirtualBox:/# sudo usermod -aG shared sophia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared olivia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared emma
root@ubuntu-VirtualBox:/# sudo mkdir /home/shared
root@ubuntu-VirtualBox:/#
```

```

root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# sudo useradd sophia
root@ubuntu-VirtualBox:/# sudo useradd olivia
root@ubuntu-VirtualBox:/# sudo useradd emma
root@ubuntu-VirtualBox:/# sudo groupadd shared
root@ubuntu-VirtualBox:/# sudo usermod -aG shared sophia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared olivia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared emma
root@ubuntu-VirtualBox:/# sudo mkdir /home/shared
root@ubuntu-VirtualBox:/# sudo chown :shared /home/shared
root@ubuntu-VirtualBox:/# sudo chmod 770 /home/shared
root@ubuntu-VirtualBox:/#
  
```

```

root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# sudo useradd sophia
root@ubuntu-VirtualBox:/# sudo useradd olivia
root@ubuntu-VirtualBox:/# sudo useradd emma
root@ubuntu-VirtualBox:/# sudo groupadd shared
root@ubuntu-VirtualBox:/# sudo usermod -aG shared sophia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared olivia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared emma
root@ubuntu-VirtualBox:/# sudo mkdir /home/shared
root@ubuntu-VirtualBox:/# sudo chown :shared /home/shared
root@ubuntu-VirtualBox:/# sudo chmod 770 /home/shared
root@ubuntu-VirtualBox:/# grep shared /etc/group
shared:x:1007:sophia,olivia,emma
root@ubuntu-VirtualBox:/#
  
```

```

root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# sudo useradd sophia
root@ubuntu-VirtualBox:/# sudo useradd olivia
root@ubuntu-VirtualBox:/# sudo useradd emma
root@ubuntu-VirtualBox:/# sudo groupadd shared
root@ubuntu-VirtualBox:/# sudo usermod -aG shared sophia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared olivia
root@ubuntu-VirtualBox:/# sudo usermod -aG shared emma
root@ubuntu-VirtualBox:/# sudo mkdir /home/shared
root@ubuntu-VirtualBox:/# sudo chown :shared /home/shared
root@ubuntu-VirtualBox:/# sudo chmod 770 /home/shared
root@ubuntu-VirtualBox:/# grep shared /etc/group
shared:x:1007:sophia,olivia,emma
root@ubuntu-VirtualBox:/# ls -ld /home/shared
drwxrwx--- 2 root shared 4096 Oct 16 15:03 /home/shared
root@ubuntu-VirtualBox:/# stat /home/shared
  File: /home/shared
  Size: 4096          Blocks: 8          IO Block: 4096   directory
Device: 8,2         Inode: 1442594      Links: 2
Access: (0770/drwxrwx---)  Uid: (  0/   root)   Gid: (1007/  shared)
  
```

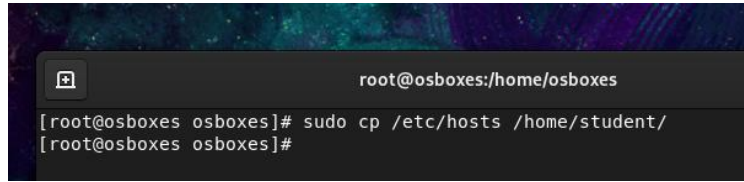
Lab 9.3 Enabling Access Control Lists

Aside of step 1, provide a screenshot evidence of the successful execution of the command run below each step in the lab.

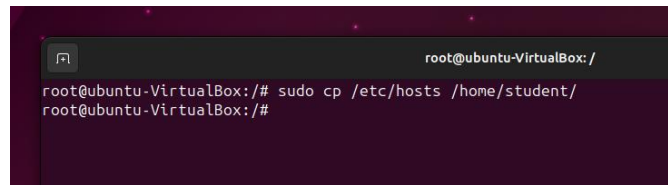
STEP 1. Open a terminal window. *(no need to provide screenshot for this step)*

STEP 2. Copy the `/etc/hosts` file to the student user's home directory.

`sudo cp /etc/hosts /home/student/`



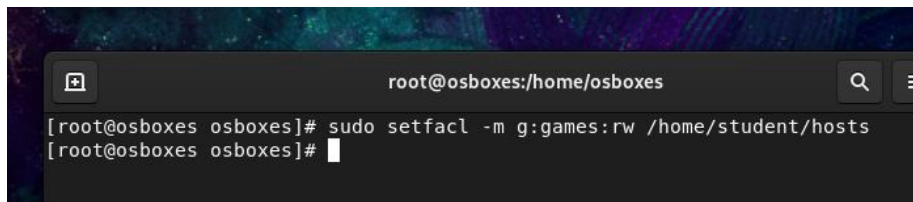
```
root@osboxes:/home/osboxes
[root@osboxes osboxes]# sudo cp /etc/hosts /home/student/
[root@osboxes osboxes]#
```



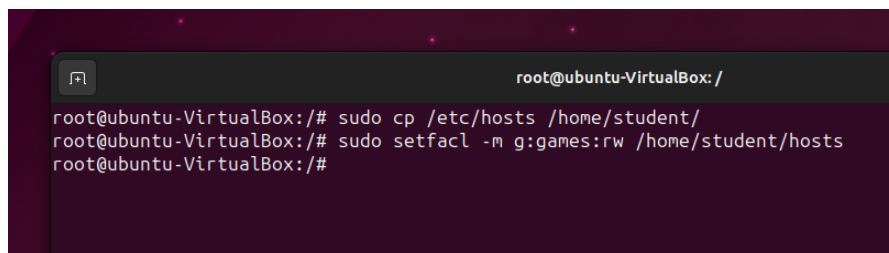
```
root@ubuntu-VirtualBox: /
root@ubuntu-VirtualBox:/# sudo cp /etc/hosts /home/student/
root@ubuntu-VirtualBox:/#
```

STEP 3. Set an access control list (ACL) for the games group that allows read and write permissions for that group on the `hosts` file.

`sudo setfacl -m g:games:rw /home/student/hosts`



```
root@osboxes:/home/osboxes
[root@osboxes osboxes]# sudo setfacl -m g:games:rw /home/student/hosts
[root@osboxes osboxes]#
```



```
root@ubuntu-VirtualBox: /
root@ubuntu-VirtualBox:/# sudo cp /etc/hosts /home/student/
root@ubuntu-VirtualBox:/# sudo setfacl -m g:games:rw /home/student/hosts
root@ubuntu-VirtualBox:/#
```

STEP 4. Display the ACLs for the `hosts` file.

`getfacl /home/student/hosts`

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# sudo setfacl -m g:games:rw /home/student/hosts
[root@osboxes osboxes]# getfacl /home/student/hosts
getfacl: Removing leading '/' from absolute path names
# file: home/student/hosts
# owner: root
# group: root
user::rw-
group::r--
group:games:rw-
mask::rw-
other::r--

[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# sudo cp /etc/hosts /home/student/
root@ubuntu-VirtualBox:/# sudo setfacl -m g:games:rw /home/student/hosts
root@ubuntu-VirtualBox:/# getfacl /home/student/hosts
getfacl: Removing leading '/' from absolute path names
# file: home/student/hosts
# owner: root
# group: root
user::rw-
group::r--
group:games:rw-
mask::rw-
other::r--

root@ubuntu-VirtualBox:/#
```

STEP 5. Change the ACL mask value to read-only for the *hosts* file.

```
sudo setfacl -m m::r /home/student/hosts
```

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# sudo setfacl -m m::r /home/student/hosts
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox:/# sudo setfacl -m m::r /home/student/hosts
root@ubuntu-VirtualBox:/#
```

STEP 6. Display the ACLs for the *hosts* file to verify the ACL mask.

```
getfacl /home/student/hosts
```

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# getfacl /home/student/hosts
getfacl: Removing leading '/' from absolute path names
# file: home/student/hosts
# owner: root
# group: root
user::rw-
group::r--
group:games:rw-          #effective:r--
mask::r--
other::r--

[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox:/# sudo setfacl -m m::r /home/student/hosts
root@ubuntu-VirtualBox:/# getfacl /home/student/hosts
getfacl: Removing leading '/' from absolute path names
# file: home/student/hosts
# owner: root
# group: root
user::rw-
group::r--
group:games:rw-          #effective:r--
mask::r--
other::r--

root@ubuntu-VirtualBox:/#
```

STEP 7. Create a directory called *test_acl*.

`mkdir /home/student/test_acl`

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# mkdir /home/student/test_acl
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# mkdir /home/student/test_acl
```

STEP 8. Create a default ACL for the *test_acl* directory so the adm user has read and write permissions for all new files and directories created in the *test_acl* directory.

`sudo setfacl -d u:adm:rw /home/student/test_acl`

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# sudo setfacl -d u:adm:rw /home/student/test_acl/
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try 'setfacl --help' for more information.
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# sudo setfacl -d u:adm:rw /home/student/test_acl/
Usage: setfacl [-bkndRLP] { -m|-M|-x|-X ... } file ...
Try 'setfacl --help' for more information.
root@ubuntu-VirtualBox:/# DS
```

STEP 9. Use the *touch* command to create a new file named *test_file* in the *test_acl* directory.

`touch /home/student/test_acl/test_file`

```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# touch /home/student/test_acl/test_file
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# touch /home/student/test_acl/test_file
root@ubuntu-VirtualBox:/#
```

STEP 10. Verify the default ACLs by viewing the ACLs for the *test_file* file.

`getfacl /home/student/test_acl/test_file`


```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# getfacl /home/student/test_acl/test_file
getfacl: Removing leading '/' from absolute path names
# file: home/student/test_acl/test_file
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /

root@ubuntu-VirtualBox:/# touch /home/student/test_acl/test_file
root@ubuntu-VirtualBox:/# getfacl /home/student/test_acl/test_file
getfacl: Removing leading '/' from absolute path names
# file: home/student/test_acl/test_file
# owner: root
# group: root
user::rw-
group::r--
other::r--

root@ubuntu-VirtualBox:/#
```

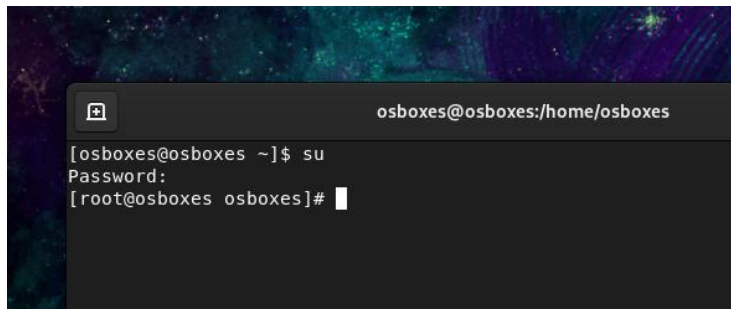
Lab 9.4 Managing File Ownership and Attributes

Aside of step 1, provide a screenshot evidence of the successful execution of the command run below each step in the lab.

STEP 1. Open a terminal window. *(no need to provide screenshot for this step)*

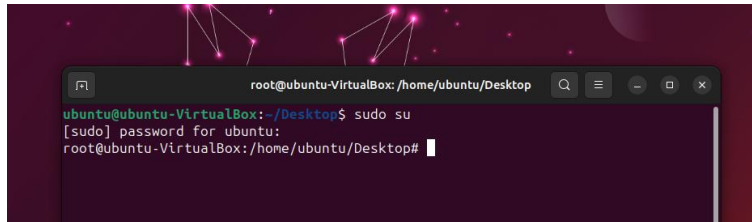
STEP 2. Use the `su` command to switch to the root account.

su



```
osboxes@osboxes:/home/osboxes

[osboxes@osboxes ~]$ su
Password:
[root@osboxes osboxes]#
```

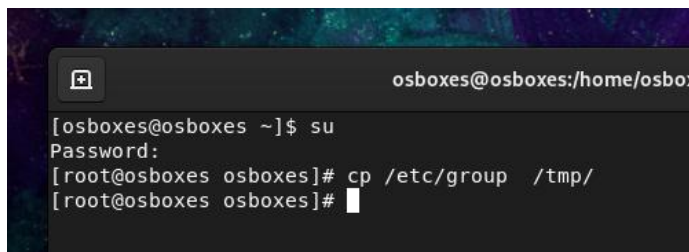


```
root@ubuntu-VirtualBox: /home/ubuntu/Desktop

ubuntu@ubuntu-VirtualBox:~/Desktop$ sudo su
[sudo] password for ubuntu:
root@ubuntu-VirtualBox: /home/ubuntu/Desktop#
```

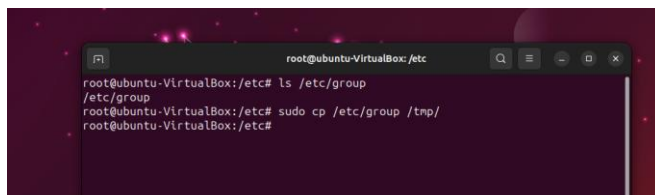
STEP 3. Copy the `/etc/group` file to the `/tmp` directory.

`cp /etc/group /tmp/`



```
osboxes@osboxes:/home/osboxes

[osboxes@osboxes ~]$ su
Password:
[root@osboxes osboxes]# cp /etc/group /tmp/
[root@osboxes osboxes]#
```

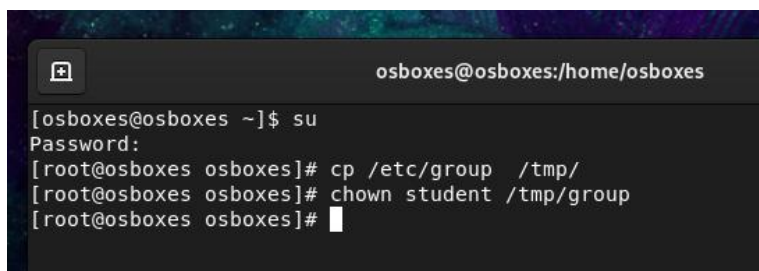


```
root@ubuntu-VirtualBox: /etc

root@ubuntu-VirtualBox:/etc# ls /etc/group
/etc/group
root@ubuntu-VirtualBox:/etc# sudo cp /etc/group /tmp/
root@ubuntu-VirtualBox:/etc#
```

STEP 4. Change the user ownership of the `/tmp/group` file to the student user.

`chown student /tmp/group`



```
osboxes@osboxes:/home/osboxes

[osboxes@osboxes ~]$ su
Password:
[root@osboxes osboxes]# cp /etc/group /tmp/
[root@osboxes osboxes]# chown student /tmp/group
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /etc
root@ubuntu-VirtualBox:/etc# ls /etc/group
/etc/group
root@ubuntu-VirtualBox:/etc# sudo cp /etc/group /tmp/
root@ubuntu-VirtualBox:/etc# chown student /tmp/group
root@ubuntu-VirtualBox:/etc#
```

STEP 5. Change the group ownership of the `/tmp/group` file to the bin group.

`chgrp bin /tmp/group`

```
osboxes@osboxes:/home/osboxes
[root@osboxes osboxes]# chgrp bin /tmp/group
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /etc
root@ubuntu-VirtualBox:/etc# ls /etc/group
/etc/group
root@ubuntu-VirtualBox:/etc# sudo cp /etc/group /tmp/
root@ubuntu-VirtualBox:/etc# chown student /tmp/group
root@ubuntu-VirtualBox:/etc# chgrp bin /tmp/group
root@ubuntu-VirtualBox:/etc#
```

STEP 6. Make the `/tmp/group` file immutable.

`chattr +i /tmp/group`

```
osboxes@osboxes:/home/osboxes
[root@osboxes osboxes]# chgrp bin /tmp/group
[root@osboxes osboxes]# chattr +i /tmp/group
[root@osboxes osboxes]#
```

```
root@ubuntu-VirtualBox: /etc
root@ubuntu-VirtualBox:/etc# ls /etc/group
/etc/group
root@ubuntu-VirtualBox:/etc# sudo cp /etc/group /tmp/
root@ubuntu-VirtualBox:/etc# chown student /tmp/group
root@ubuntu-VirtualBox:/etc# chgrp bin /tmp/group
root@ubuntu-VirtualBox:/etc# chattr +i /tmp/group
root@ubuntu-VirtualBox:/etc#
```

STEP 7. Run the correct command to display the file attributes of the `/tmp/group` file.

`lsattr /tmp/group`

```
osboxes@osboxes:/home/
[osboxes@osboxes ~]$ lsattr /tmp/group
-----i----- /tmp/group
[osboxes@osboxes ~]$
```

```
root@ubuntu-VirtualBox: /etc
root@ubuntu-VirtualBox:/etc# ls /etc/group
/etc/group
root@ubuntu-VirtualBox:/etc# sudo cp /etc/group /tmp/
root@ubuntu-VirtualBox:/etc# chown student /tmp/group
root@ubuntu-VirtualBox:/etc# chgrp bin /tmp/group
root@ubuntu-VirtualBox:/etc# chmod +i /tmp/group
root@ubuntu-VirtualBox:/etc# lsattr /tmp/group
-----i-----e----- /tmp/group
root@ubuntu-VirtualBox:/etc#
```

STEP 8. Attempt to remove the `/tmp/group` file. Explain why this fails.

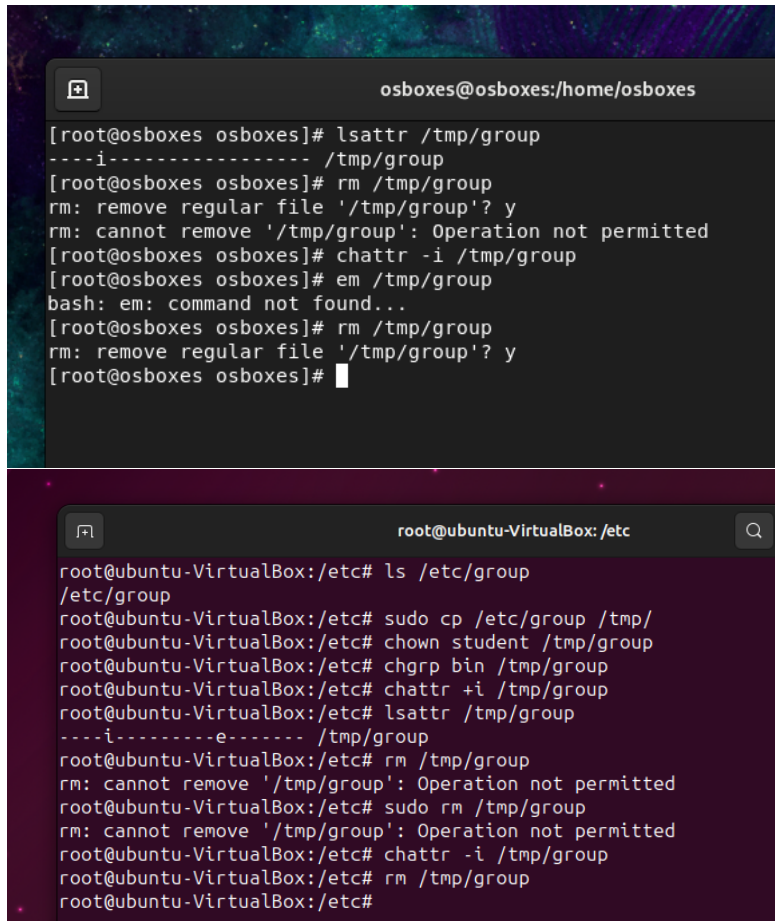
`rm /tmp/group`

```
osboxes@osboxes:/home/osboxes
[osboxes@osboxes ~]$ lsattr /tmp/group
-----i----- /tmp/group
[osboxes@osboxes ~]$ rm /tmp/group
rm: remove regular file '/tmp/group'? y
rm: cannot remove '/tmp/group': Operation not permitted
[osboxes@osboxes ~]$
```

```
root@ubuntu-VirtualBox: /etc
root@ubuntu-VirtualBox:/etc# ls /etc/group
/etc/group
root@ubuntu-VirtualBox:/etc# sudo cp /etc/group /tmp/
root@ubuntu-VirtualBox:/etc# chown student /tmp/group
root@ubuntu-VirtualBox:/etc# chgrp bin /tmp/group
root@ubuntu-VirtualBox:/etc# chmod +i /tmp/group
root@ubuntu-VirtualBox:/etc# lsattr /tmp/group
-----i-----e----- /tmp/group
root@ubuntu-VirtualBox:/etc# rm /tmp/group
rm: cannot remove '/tmp/group': Operation not permitted
root@ubuntu-VirtualBox:/etc# sudo rm /tmp/group
rm: cannot remove '/tmp/group': Operation not permitted
root@ubuntu-VirtualBox:/etc#
```

STEP 9. Remove the immutable attribute from the `/tmp/group` file.

`chattr -i /tmp/group`

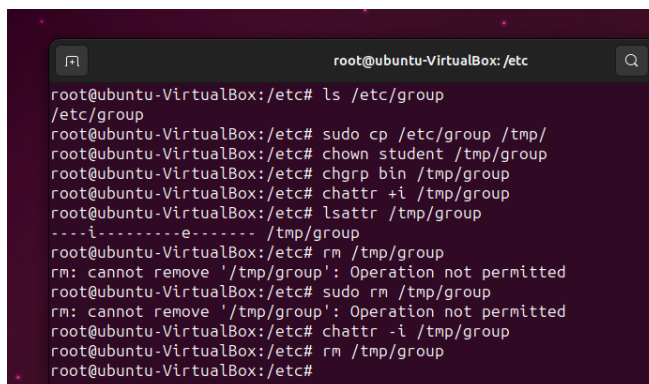


The first terminal window shows the user `osboxes` at `osboxes:/home/osboxes`. The user runs `lsattr /tmp/group`, which shows the file has the immutable attribute (`-----i-----`). Then, the user runs `rm /tmp/group`, which fails with the message "rm: cannot remove '/tmp/group': Operation not permitted". The user then runs `chattr -i /tmp/group` successfully. Finally, the user runs `rm /tmp/group` again, which succeeds.

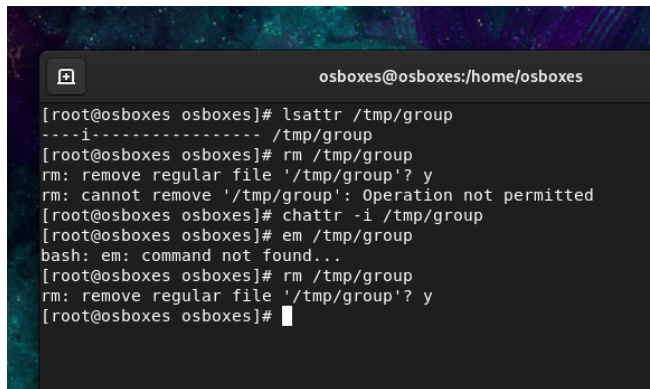
The second terminal window shows the user `root` at `ubuntu-VirtualBox:/etc`. The user runs `ls /etc/group`, which shows the file has the immutable attribute (`-----i-----e-----`). The user then runs `sudo cp /etc/group /tmp/`, `chown student /tmp/group`, and `chgrp bin /tmp/group`. The user then runs `chattr +i /tmp/group` to set the immutable attribute. The user then runs `lsattr /tmp/group`, which shows the file has the immutable attribute (`-----i-----e-----`). The user then runs `rm /tmp/group`, which fails with the message "rm: cannot remove '/tmp/group': Operation not permitted". The user then runs `sudo rm /tmp/group`, which also fails with the message "rm: cannot remove '/tmp/group': Operation not permitted". The user then runs `chattr -i /tmp/group` successfully. Finally, the user runs `rm /tmp/group` again, which succeeds.

STEP 10. Remove the `/tmp/group` file.

`rm /tmp/group`



The terminal window shows the user `root` at `ubuntu-VirtualBox:/etc`. The user runs `ls /etc/group`, which shows the file has the immutable attribute (`-----i-----e-----`). The user then runs `sudo cp /etc/group /tmp/`, `chown student /tmp/group`, and `chgrp bin /tmp/group`. The user then runs `chattr +i /tmp/group` to set the immutable attribute. The user then runs `lsattr /tmp/group`, which shows the file has the immutable attribute (`-----i-----e-----`). The user then runs `rm /tmp/group`, which fails with the message "rm: cannot remove '/tmp/group': Operation not permitted". The user then runs `sudo rm /tmp/group`, which also fails with the message "rm: cannot remove '/tmp/group': Operation not permitted". The user then runs `chattr -i /tmp/group` successfully. Finally, the user runs `rm /tmp/group` again, which succeeds.



```
osboxes@osboxes:/home/osboxes
[root@osboxes osboxes]# lsattr /tmp/group
----i----- /tmp/group
[root@osboxes osboxes]# rm /tmp/group
rm: remove regular file '/tmp/group'? y
rm: cannot remove '/tmp/group': Operation not permitted
[root@osboxes osboxes]# chattr -i /tmp/group
[root@osboxes osboxes]# em /tmp/group
bash: em: command not found...
[root@osboxes osboxes]# rm /tmp/group
rm: remove regular file '/tmp/group'? y
[root@osboxes osboxes]#
```

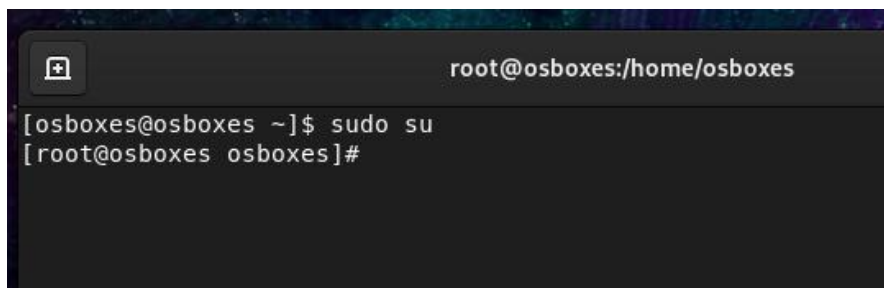
Lab 9.5 Monitoring Security Issues with SELinux

Aside of step 1, provide a screenshot evidence of the successful execution of the command run below each step in the lab.

STEP 1. Open a terminal window. *(no need to provide screenshot for this step)*

STEP 2. Use the `su` command to switch to the root account.

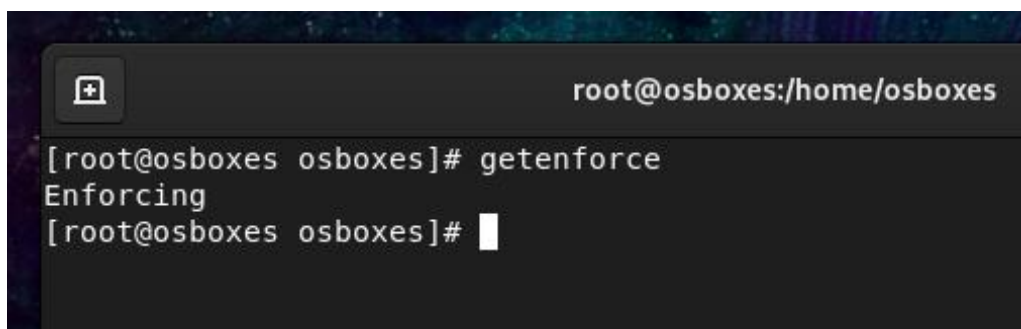
`su`



```
root@osboxes:/home/osboxes
[osboxes@osboxes ~]$ sudo su
[root@osboxes osboxes]#
```

STEP 3. Execute the correct command to determine what mode (enforcing or permissive) SELinux is currently in. <<check the remarks in the book for this step>>

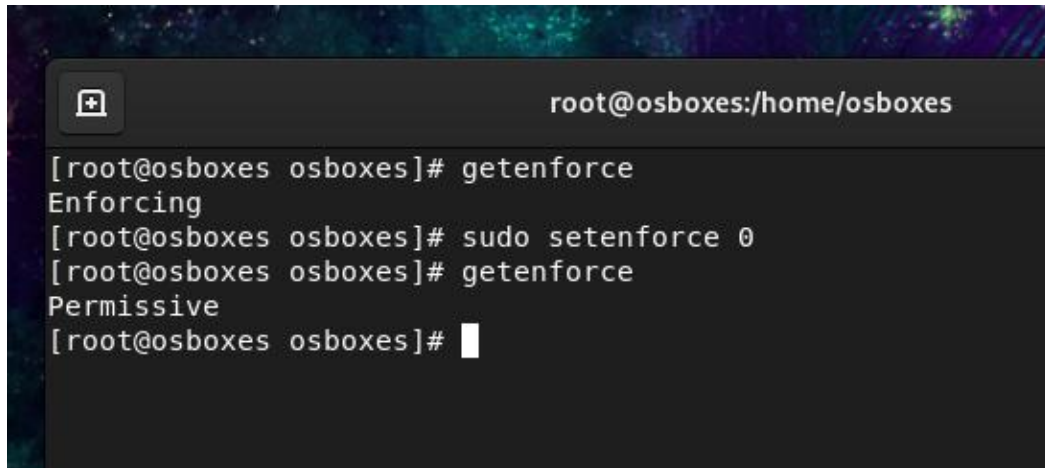
`getenforce`



```
root@osboxes:/home/osboxes
[root@osboxes osboxes]# getenforce
Enforcing
[root@osboxes osboxes]#
```


STEP 4. Change the current mode to permissive.

```
sudo setenforce 0
```

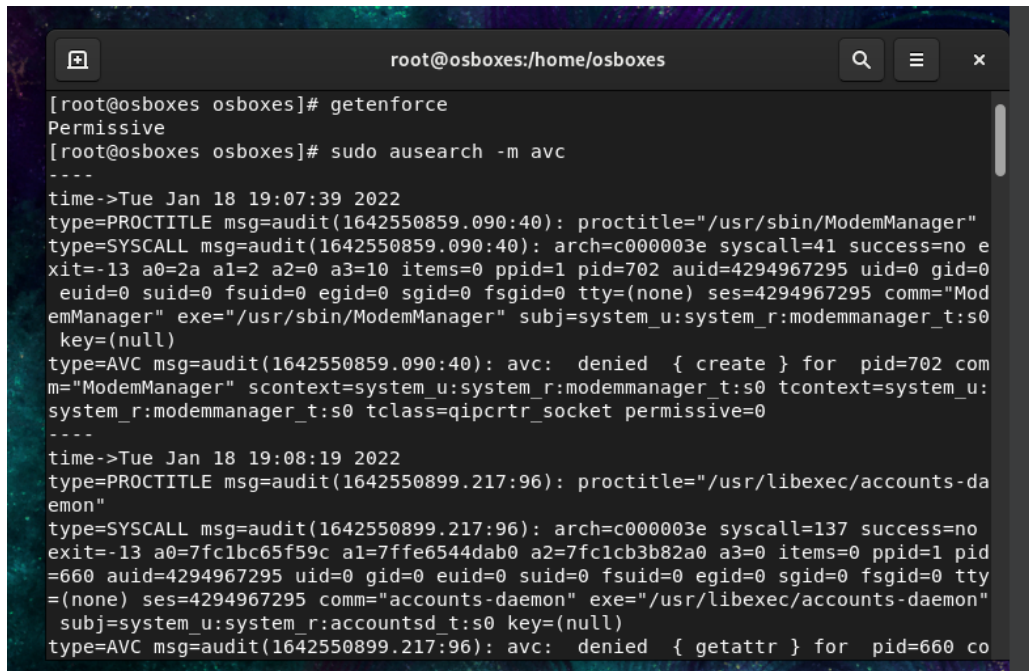


```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# getenforce
Enforcing
[root@osboxes osboxes]# sudo setenforce 0
[root@osboxes osboxes]# getenforce
Permissive
[root@osboxes osboxes]#
```

STEP 5. Display any log entries related to SELinux.

```
sudo ausearch -m avc
```

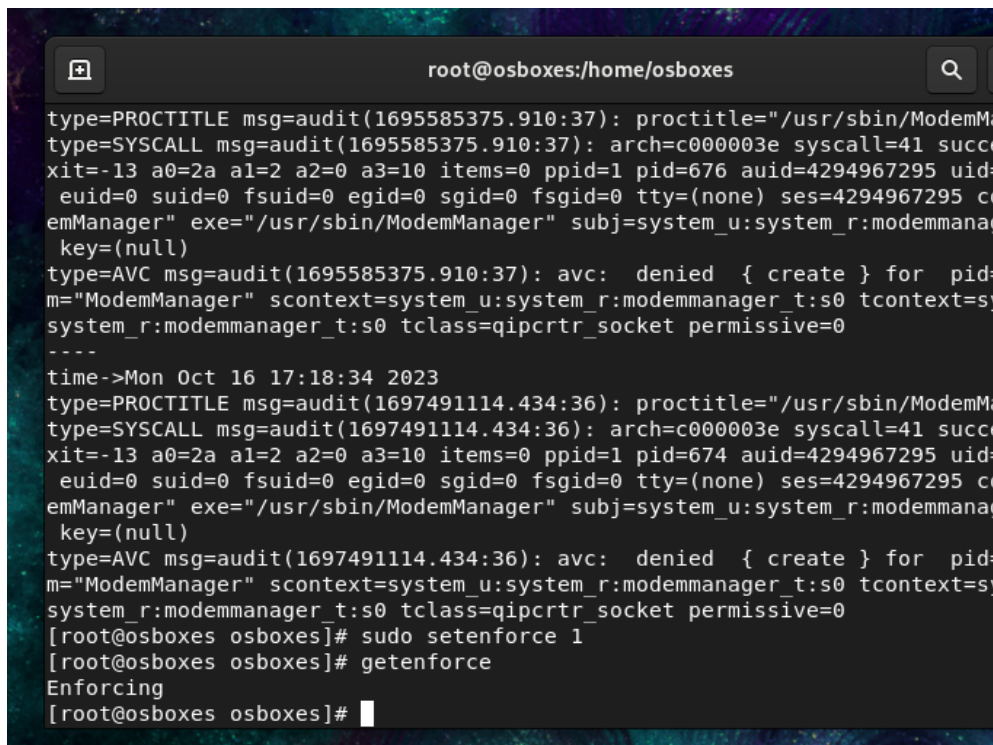


```
root@osboxes:/home/osboxes

[root@osboxes osboxes]# getenforce
Permissive
[root@osboxes osboxes]# sudo ausearch -m avc
----
time->Tue Jan 18 19:07:39 2022
type=PROCTITLE msg=audit(1642550859.090:40): proctitle="/usr/sbin/ModemManager"
type=SYSCALL msg=audit(1642550859.090:40): arch=c000003e syscall=41 success=no e
xit=-13 a0=2a a1=2 a2=0 a3=10 items=0 ppid=1 pid=702 auid=4294967295 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="Mod
emManager" exe="/usr/sbin/ModemManager" subj=system_u:system_r:modemmanager_t:s0
key=(null)
type=AVC msg=audit(1642550859.090:40): avc: denied { create } for pid=702 com
m="ModemManager" scontext=system_u:system_r:modemmanager_t:s0 tcontext=system_u:
system_r:modemmanager_t:s0 tclass=qipcrt_socket permissive=0
----
time->Tue Jan 18 19:08:19 2022
type=PROCTITLE msg=audit(1642550899.217:96): proctitle="/usr/libexec/accounts-da
emon"
type=SYSCALL msg=audit(1642550899.217:96): arch=c000003e syscall=137 success=no
exit=-13 a0=7fclbc65f59c a1=7ffe6544dab0 a2=7fclcb3b82a0 a3=0 items=0 ppid=1 pid
=660 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty
=(none) ses=4294967295 comm="accounts-daemon" exe="/usr/libexec/accounts-daemon"
subj=system_u:system_r:accounts-daemon_t:s0 key=(null)
type=AVC msg=audit(1642550899.217:96): avc: denied { getattr } for pid=660 co
```

STEP 6. Change the current mode to enforcing. <<check the remarks in the book for this step>>

`sudo setenforce 1`

A terminal window titled 'root@osboxes:/home/osboxes' with a search icon in the top right. The terminal displays several lines of audit logs. The first log entry is a PROCTITLE message for '/usr/sbin/ModemManager'. The second is a SYSCALL message for 'syscalls=41'. The third is an AVC (Access Vector Cache) message showing a 'denied { create }' for 'pid=676' and 'modemmanager'. The terminal then shows the command 'sudo setenforce 1' being executed, followed by the output 'Enforcing'. The prompt returns to '[root@osboxes osboxes]#'.

```
root@osboxes:/home/osboxes
type=PROCTITLE msg=audit(1695585375.910:37): proctitle="/usr/sbin/ModemManager"
type=SYSCALL msg=audit(1695585375.910:37): arch=c000003e syscall=41 success=1
exit=-13 a0=2a a1=2 a2=0 a3=10 items=0 ppid=1 pid=676 auid=4294967295 uid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm=
ModemManager exe="/usr/sbin/ModemManager" subj=system_u:system_r:modemmanager_t:s0
key=(null)
type=AVC msg=audit(1695585375.910:37): avc: denied { create } for pid=676
process="ModemManager" scontext=system_u:system_r:modemmanager_t:s0 tcontext=system_u:system_r:modemmanager_t:s0 tclass=qipcrt_socket permissive=0
----
time->Mon Oct 16 17:18:34 2023
type=PROCTITLE msg=audit(1697491114.434:36): proctitle="/usr/sbin/ModemManager"
type=SYSCALL msg=audit(1697491114.434:36): arch=c000003e syscall=41 success=1
exit=-13 a0=2a a1=2 a2=0 a3=10 items=0 ppid=1 pid=674 auid=4294967295 uid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm=
ModemManager exe="/usr/sbin/ModemManager" subj=system_u:system_r:modemmanager_t:s0
key=(null)
type=AVC msg=audit(1697491114.434:36): avc: denied { create } for pid=674
process="ModemManager" scontext=system_u:system_r:modemmanager_t:s0 tcontext=system_u:system_r:modemmanager_t:s0 tclass=qipcrt_socket permissive=0
[root@osboxes osboxes]# sudo setenforce 1
[root@osboxes osboxes]# getenforce
Enforcing
[root@osboxes osboxes]#
```