



LAB 2

QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG, Ổ CỨNG VÀ HỆ THỐNG TẬP TIN

Họ tên và MSSV: Lê Tuấn Kiệt-B1909935

Nhóm học phần: 2

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.

- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết.

1. Cài đặt CentOS

Thực hiện cài đặt CentOS 6 (hoặc CentOS 7,8) vào máy tính cá nhân (hoặc máy ảo) của bạn (KHÔNG cần chụp hình minh họa).

2. Quản lý tài khoản

Tìm hiểu và thực hiện các yêu cầu sau:

2.1. Sử dụng lệnh **adduser** và **passwd** để tạo một tài khoản mới với tên đăng nhập có dạng **masosinhvien** (ví dụ: b1801234). (chụp hình minh họa).

Quan sát để thấy rằng khi một tài khoản mới được tạo, thư mục cá nhân trong **/home** và nhóm cá nhân trong **/etc/group** ứng với tài khoản đó cũng được tạo theo.

- Sử dụng tài khoản **root** để tạo người dùng mới như sau :

```
[b1909935@zen ~]$ su
Password:
[root@zen b1909935]# adduser B1909935_CTU
[root@zen b1909935]# passwd B1909935_CTU
Changing password for user B1909935_CTU.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

- Sử dụng lệnh **ls** hiển thị danh sách các file trong thư mục :

```
[root@zen b1909935]# ls /home
b1909935  B1909935_CTU
```

- Sử dụng lệnh **cat** để xem nội dung bên trong file :

```
[root@zen b1909935]# cat /etc/group
```

```
gnome-initial-setup:x:975:
sshd:x:74:
slocate:x:21:
rngd:x:974:
tcpdump:x:72:
b1909935:x:1000:
B1909935_CTU:x:1001:
```

- 2.2. Mở file **/etc/shadow** và cho biết mật khẩu bạn vừa tạo cho tài khoản mới sử dụng giải thuật mã hóa nào? Dựa vào đâu để biết điều đó? (chụp hình minh họa).

Sử dụng lệnh `cat` để xem nội dung bên trong file :

```
[root@zen b1909935]# cat /etc/shadow
```

```
b1909935:$6$0HwgNJZBoUELqEBK$VNteP7ChJQlgK4NV3mFw7iUA33YYdiTW7WvvSVwMZbGtB1..f9B  
k3xVMvK3hRrbc8w0b2GBCBS3jKTGAIDG5/::0:99999:7:::  
B1909935_CTU:$6$DY1MpfMf35ejTeYU$S8Yl9JuJEKTTVjEp7v2e810p.sjGyW0Jh30BT7soqZ8sw8i  
Lljc3R0p//RnHvlMSrfaic231DcGGM0Q157LlC.:18713:0:99999:7:::
```



==> CentOS sử dụng SHA512 để mã hoá mật khẩu, vì có ký hiệu `$6` trước dãy mật khẩu đã mã hoá

- 2.3. Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2020 (chụp hình minh họa).

Sử dụng (Yêu cầu người dùng `root`) :

- `usermod -e <date> <user>` : đặt ngày hết hạn cho tài khoản cụ thể
- `chage -l <user>` : Hiển thị thông tin hết hạn tài khoản cụ thể

```
[root@zen b1909935]# usermod -e 2020-12-31 B1909935_CTU  
[root@zen b1909935]# chage -l B1909935_CTU  
Last password change                : Mar 27, 2021  
Password expires                    : never  
Password inactive                    : never  
Account expires                     : Dec 31, 2020  
Minimum number of days between password change : 0  
Maximum number of days between password change : 99999  
Number of days of warning before password expires : 7
```

- 2.4. Tạo một nhóm người dùng với tên nhóm là mã lớp của bạn. Thêm tài khoản ở 2.1 vào nhóm vừa tạo (chụp hình minh họa).

Sử dụng (yêu cầu người dùng `root`) :

- `groupadd <group>` : thêm nhóm người dùng
- `usermod -a -G <group> <user>` : thêm người dùng vào nhóm
- `groups <user>` : Kiểm tra người dùng thuộc tất cả nhóm nào

```
[root@zen b1909935]# groupadd CT179_2  
[root@zen b1909935]# usermod -a -G CT179_2 B1909935_CTU  
[root@zen b1909935]# groups B1909935_CTU  
B1909935_CTU : B1909935_CTU CT179_2
```

2.5. Thực hiện khoá tài khoản ở 2.1, sau đó đăng nhập thử và quan sát (chụp hình minh hoạ).

Sử dụng (yêu cầu người dùng `root`) :

- `usermod -L <user>` : khoá tài khoản người dùng

```
[root@zen Desktop]# usermod -L B1909935_CTU
```

⚠ Sau khi **khóa tài khoản**, chuỗi mật khẩu mã hoá sẽ thêm **!** vào trước.

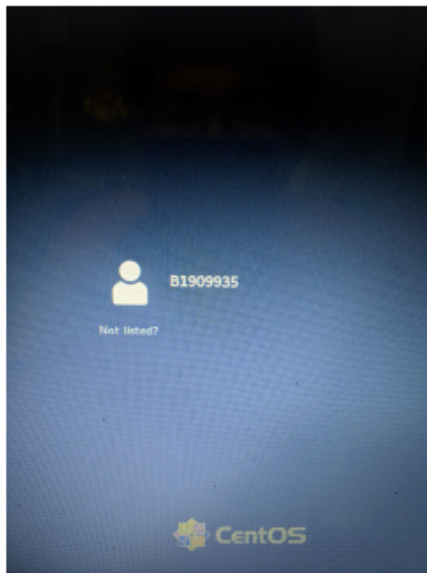
```
B1909935_CTU: !$6$DY1MpFmf35ejTeYU$S8Yl9JujEKTTVjEp7v2e810p.sjGyW0Jh30BT7soqZ8sw8iLljc3R0p//RnHv\MSrfaic231DcGGM0Q157LlC.:18713:0:99999:7:::18627:
```

- Sử dụng lệnh `su` để chuyển tài khoản :

```
[b1909935@zen ~]$ su B1909935_CTU
Password:
su: Authentication failure
```



⚠ Ở **CentOS 8** khi ta **khóa tài khoản**, màn hình đăng nhập sẽ không có tài khoản đã khóa



2.6. Mở khóa tài khoản ở 2.1 (chụp hình minh hoạ).

Sử dụng (yêu cầu tài khoản `root`) :

- `usermod -U <user>` : Mở khóa tài khoản

```
[root@zen Desktop]# usermod -U B1909935_CTU
```

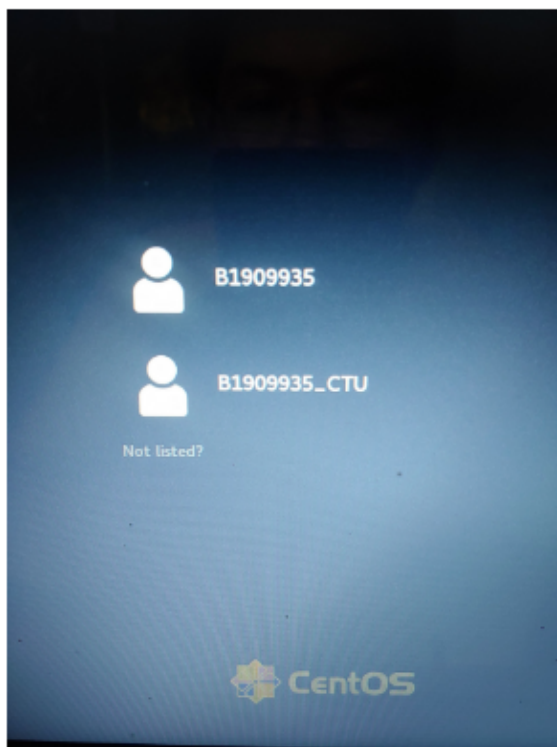


⚠ Sau khi **mở khóa**, chuỗi mật khẩu sẽ xoá đi **!** trước nó ==> trở lại như xưa

- Sử dụng lệnh `su` để chuyển đổi tài khoản (từ tài khoản thường) :

```
[b1909935@zen Desktop]$ su B1909935_CTU
Password:
[B1909935_CTU@zen Desktop]$
```

⚠ Màn hình đăng nhập đã hiển thị tài khoản



3. Quyền root (Root privilege)

Tìm hiểu và thực hiện các yêu cầu sau:

3.1. Quyền root là gì?

Quyền `root` là quyền thực thi cao dưới người quản trị cao nhất.

3.2. Nếu các ưu điểm của việc dùng `sudo` so với dùng `su` (chuyển sang tài khoản root).

Có sự khác biệt lớn giữa các lệnh `su` và `sudo` :

- `su` chuyển bạn sang tài khoản người dùng `root` .
- `sudo` chạy lệnh với đặc quyền `root` .

Về cơ bản, `sudo` là một `binary setuid` là thực hiện lệnh `root` thay mặt người dùng uỷ quyền khác.

- 3.3.** Mô tả các bước (chụp hình minh họa) để cấp quyền sudo cho tài khoản ở 2.1. Sau đó cho một ví dụ để kiểm chứng xem tài khoản này đã thực sự được cấp quyền hay chưa (chụp hình minh họa).

Để cho riêng người dùng quyền truy cập `root`, bạn cần thêm người dùng vào nhóm quyền truy cập `root`.

- **B1:** Gõ lệnh `visudo` dưới tài khoản `root`

```
[root@zen b1909935]# visudo
```

- **B2:** Kéo xuống tìm và chỉnh sửa như sau :

```
## Allow root to run any commands anywhere
root    ALL=(ALL)        ALL
B1909935 CTU    ALL=(ALL)    ALL
## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES,
ATE, DRIVERS

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

💡 Tuy nhiên tôi khuyên bạn nên cấp quyền `root` cho `group`, vì ta có thể dễ dàng quản lí nó, CentOS 8 đã tạo cho ta sẵn nhóm `wheel`

- **B3:** Thêm tài khoản vào nhóm `wheel` :

```
[root@zen b1909935]# usermod -a -G wheel B1909935_CTU
[root@zen b1909935]# groups B1909935_CTU
B1909935 CTU : B1909935 CTU wheel CT179 2
```

=> Vậy là đã xong các bước cấp quyền `root` cho tài khoản, thử như sau :

```
[B1909935_CTU@zen b1909935]$ sudo nano /etc/shadow
```

```

B1909935_CTU@zen:/home/b1909935
File Edit View Search Terminal Help
GNU nano 2.9.8 /etc/shadow

root:$6$A7Z16Geqmc9AS6dg$F1YPzjY9J60tH65RfKQDkZkv9YXIsFwLhgUum2.oG9DrE2aEzWefKF$
bin:!:18397:0:99999:7:::
daemon:!:18397:0:99999:7:::
adm:!:18397:0:99999:7:::
lp:!:18397:0:99999:7:::
sync:!:18397:0:99999:7:::
shutdown:!:18397:0:99999:7:::
halt:!:18397:0:99999:7:::
mail:!:18397:0:99999:7:::
operator:!:18397:0:99999:7:::
games:!:18397:0:99999:7:::
ftp:!:18397:0:99999:7:::
nobody:!:18397:0:99999:7:::
dbus:!!:18700:0:99999:7:::
systemd-coredump:!!:18700:0:99999:7:::
systemd-resolve:!!:18700:0:99999:7:::
tss:!!:18700:0:99999:7:::
polkitd:!!:18700:0:99999:7:::
geoclue:!!:18700:0:99999:7:::

[ Read 49 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
    
```

=> Vậy là chúng ta không cần tài khoản `root` vẫn có thể vào file `/etc/shadow`

3.4. Thu hồi quyền root của một tài khoản ở 2.1 (chụp hình minh họa).

Sử dụng `gpasswd -d <user> <group>` : Xóa người dùng ra khỏi nhóm

```

[root@zen b1909935]# gpasswd -d B1909935_CTU wheel
Removing user B1909935_CTU from group wheel
[root@zen b1909935]# groups B1909935_CTU
B1909935_CTU : B1909935_CTU CT179_2
    
```

=> Vậy là đã thu hồi quyền `root` cho tài khoản, thử như sau :

```


[root@zen b1909935]# su B1909935_CTU
[B1909935_CTU@zen b1909935]$ sudo nano /etc/shadow
B1909935_CTU is not in the sudoers file. This incident will be reported.
    
```

=> Vậy là tài khoản `B1909935_CTU` không thể truy cập vào file `/etc/shadow`

4. Đĩa và phân vùng ổ cứng

Tìm hiểu và thực hiện các yêu cầu sau:

- 4.1. Thêm một ổ cứng vào máy ảo CentOS. Nếu đã cài CentOS trực tiếp vào máy tính cá nhân thì có thể sử dụng 1 USB để thay thế.

Cắm  USB vào máy và gõ lệnh `sudo fdisk -l` để xem thiết bị :

```
[b1909935@zen ~]$ sudo fdisk -l
```

```
Disk /dev/sde: 14.3 GiB, 1537600000 bytes, 30031250 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 0A4ED522-CA10-49A6-A00B-38F3EEBD1ABB
```

==> Vậy  USB của ta là `/dev/sde` và có dung lượng 14.3GB

- 4.2. Sử dụng lệnh **fdisk** và **mkfs** để tạo và format một phân vùng trên ổ cứng vừa mới thêm ở 4.1 (chụp hình minh họa)

B1: Gõ lệnh `fdisk <đường dẫn ổ cứng>`


```
[root@zen b1909935]# fdisk /dev/sde

Welcome to fdisk (util-linux 2.32.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

The old ext4 signature will be removed by a write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x1f93d9ab.

Command (m for help):
```

 Gõ `m` để đọc hướng dẫn

==> Nếu ổ cứng có dữ liệu hãy gõ `d` để xóa ổ cứng


B2 : Gõ `n` để tạo phân vùng mới

```
Command (m for help): n
Partition number (1-128, default 1):
First sector (34-30031216, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-30031216, default 30031216):

Created a new partition 1 of type 'Linux filesystem' and of size 14.3 GiB.
```

B3: Gõ `w` để ghi phân vùng

```
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

=> Đã tạo xong phân vùng cần thiết 

💡 Kiểm tra bằng cách gõ `fdisk -l <đường dẫn ổ cứng>`

```
[root@zen b1909935]# fdisk -l /dev/sde
Disk /dev/sde: 14.3 GiB, 15376000000 bytes, 30031250 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 0A4ED522-CA10-49A6-A00B-38F3EEBD1ABB

Device      Start      End  Sectors  Size Type
/dev/sde1   2048 30031216 30029169 14.3G Linux filesystem
```

Sử dụng lệnh `mkfs.<chuẩn file system> <đường dẫn ổ cứng>` để **format** ổ cứng theo chuẩn file system mình muốn :

```
[root@zen b1909935]# mkfs.ext4 /dev/sde
mke2fs 1.45.6 (20-Mar-2020)
Found a gpt partition table in /dev/sde
Proceed anyway? (y,N) y
Creating filesystem with 3753906 4k blocks and 940240 inodes
Filesystem UUID: 7220b374-fbe0-4dbd-ac13-elec3fcaaafe
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208

Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

4.3. Tạo thư mục mới có tên **/data** bằng tài khoản root. Mount phân vùng ổ cứng ở 4.2 tới thư mục **/data** (chụp hình minh họa)

Sử dụng (yêu cầu tài khoản `root`)

- `mkdir` : tạo thư mục
- `mount <đường dẫn ổ cứng> <đường dẫn thư mục>` : Gắn ổ cứng vào đường dẫn cụ thể

```
[root@zen b1909935]# mkdir /data
[root@zen b1909935]# ls /
bin  data  etc  lib  lost+found  mnt  proc  run  srv  tmp  var
boot dev  home lib64 media  opt  root  sbin sys  usr
[root@zen b1909935]# mount /dev/sde /data
```


4.4. Thực hiện lệnh **df -h** để xem kết quả. (chụp hình minh họa)

```
[root@zen b1909935]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        5.7G   0    5.7G   0% /dev
tmpfs           5.8G  11M   5.7G   2% /dev/shm
tmpfs           5.8G   18M   5.7G   1% /run
tmpfs           5.8G   0    5.8G   0% /sys/fs/cgroup
/dev/sda2       59G   6.3G   50G   12% /
/dev/sda1       200M   6.9M  193M   4% /boot/efi
tmpfs           1.2G   1.2M   1.2G   1% /run/user/42
tmpfs           1.2G   6.0M   1.2G   1% /run/user/1000
/dev/sde        15G   41M   14G   1% /data
```

💡 Ổ cứng `/dev/sde` có `15G`, khả dụng `14G` và đã sử dụng `41M(1%)` đã được mount vào trong `/data`

5. Phân quyền trên hệ thống tập tin

5.1. Tạo nhóm người dùng **quantri**, thêm người dùng ở 2.1 vào nhóm **quantri**

Làm theo câu 2.4 trên :

```
[root@zen b1909935]# groupadd quantri
[root@zen b1909935]# usermod -a -G quantri B1909935_CTU
[root@zen b1909935]# groups B1909935_CTU
B1909935_CTU : B1909935_CTU CT179_2 quantri
```

5.2. Chuyển *nhóm chủ sở hữu* của thư mục **/data** sang **quantri**. Phân quyền cho thư mục **/data** là chủ sở hữu có toàn quyền read, write và execute, nhóm chủ sở hữu có quyền read và execute, những người khác không có quyền gì (chụp hình minh họa).

- Sử dụng lệnh `chgrp <group> <đường dẫn>` : thay đổi nhóm sử dụng cho thư mục cụ thể

```
[root@zen b1909935]# chgrp quantri /data
[root@zen b1909935]# ls -l /
total 72
lrwxrwxrwx. 1 root root      7 Nov  3 22:22 bin -> usr/bin
dr-xr-xr-x. 5 root root    4096 Mar 14 22:03 boot
drwxr-xr-x. 3 root quantri 4096 Mar 27 18:27 data
drwxr-xr-x. 21 root root    3540 Mar 27 18:27 dev
```

💡 Như bạn đã thấy quyền sở hữu nhóm đổi qua `quantri`

- Sử dụng lệnh `chmod <option> <đường dẫn thư mục>` : thay đổi quyền cho thư mục

```
[root@zen b1909935]# chmod 750 /data
[root@zen b1909935]# ls -l /
total 72
lrwxrwxrwx. 1 root root      7 Nov  3 22:22 bin -> usr/bin
dr-xr-xr-x. 5 root root    4096 Mar 14 22:03 boot
drwxr-x---. 3 root quantri 4096 Mar 27 18:27 data
drwxr-xr-x. 21 root root    3540 Mar 27 18:27 dev
```

💡 Như bạn đã thấy :

- `drwxr` là toàn quyền cho `user`
- `x` là quyền thực thi cho `group`
- `---` là không có quyền gì cho `other`

5.3. Dùng tài khoản root tạo tập tin `/data/file1.txt`. Sau đó dùng tài khoản ở 2.1 tạo tập tin `/data/file2.txt`. Quan sát và cho biết kết quả trong 2 trường hợp (chụp hình minh họa).

👤 Sử dụng lệnh `nano` hoặc `gedit` để tạo file và ghi :

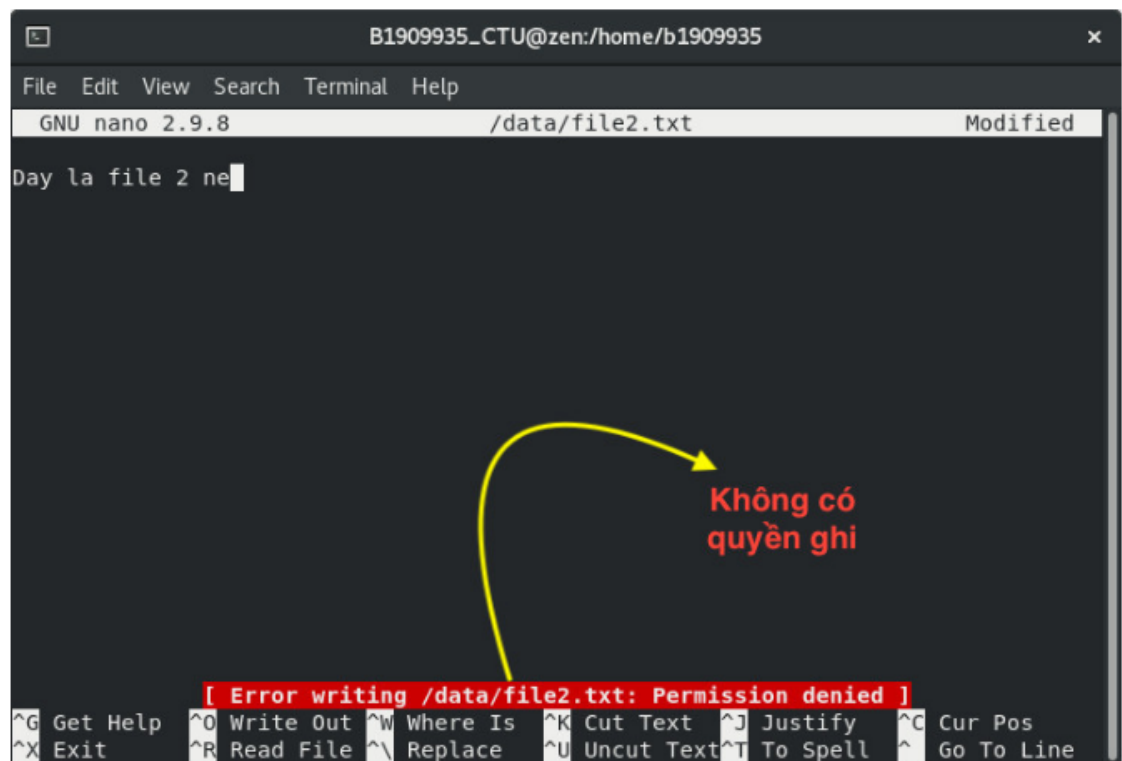
- Người dùng `root` :

```
[root@zen b1909935]# nano /data/file1.txt
[root@zen b1909935]# cat /data/file1.txt
Day la file 1 ne
```

- Người dùng `B1909935_CTU` :

```
[B1909935_CTU@zen b1909935]$ nano /data/file2.txt
```

⚠ Ngay lập tức sẽ lỗi vì `B1909935_CTU` nằm trong group `quantri` chỉ có quyền `x` (thực thi), không có quyền `w` (ghi)



- 5.4. Dùng tài khoản 2.1 *mở và thay đổi nội dung* tập tin /data/file1.txt, cho biết kết quả (chụp hình minh họa).

Sử dụng lệnh `nano` ở tài khoản `B1909935_CTU` :

```
[B1909935_CTU@zen b1909935]$ nano /data/file1.txt
```

⚠ Sẽ phát sinh ra lỗi không có quyền ghi

==> Vì chủ sở hữu của `file1.txt` là `root`, và người dùng khác chỉ có quyền `r` (đọc)
 ==> `B1909935_CTU` không thể ghi

```
[B1909935_CTU@zen b1909935]$ ls -l /data/
total 20
-rw-r--r--. 1 root root 17 Mar 27 18:49 file1.txt
drwx-----. 2 root root 16384 Mar 27 18:27 lost+found
```

- 5.5. Cấp quyền cho tài khoản 2.1 có thể thay đổi nội dung tập tin /data/file1.txt (chụp hình minh họa).

Sử dụng lệnh `chmod <option> <đường dẫn thư mục>` để cấp quyền cho thư mục

```
[root@zen b1909935]# chmod o+w /data/file1.txt
[root@zen b1909935]# su B1909935_CTU
[B1909935_CTU@zen b1909935]$ nano /data/file1.txt
[B1909935_CTU@zen b1909935]$ cat /data/file1.txt
Day la file 1 ne
Thay doi duoc noi dung ne
```

- 5.6.** Tạo thêm một tài khoản mới, dùng tài khoản này mở tập tin `/data/file1.txt`, cho biết kết quả (chụp hình minh hoạ).

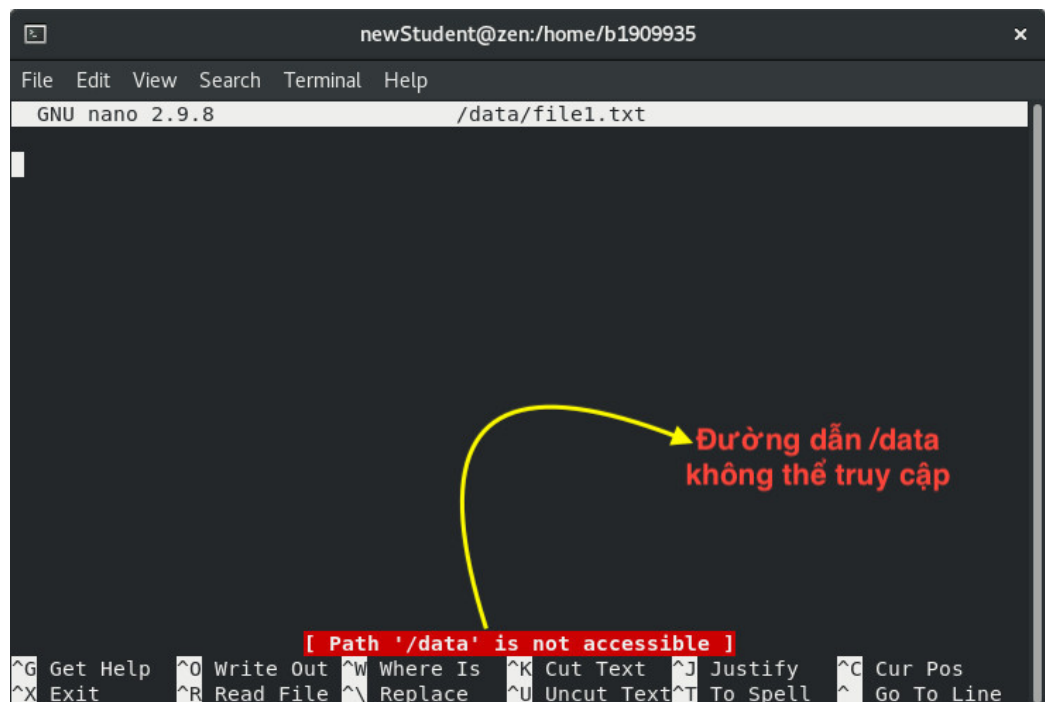
Làm theo câu 2.1 để tạo người dùng mới

```
[root@zen b1909935]# adduser newStudent
[root@zen b1909935]# passwd newStudent
Changing password for user newStudent.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@zen b1909935]# su newStudent
[newStudent@zen b1909935]$
```

Sử dụng lệnh sau để mở thư mục `/data/file1.txt`

```
$ nano /data/file1.txt
# Thực thi lệnh ở người dùng newStudent vừa tạo
```

⚠ Sẽ đưa ra lỗi không thể truy cập vào `/data`



🤖 Vì trong câu 5.2, chúng ta thiết lập `/data`, người khác không có quyền gì cả và nhóm sở hữu là `quantri`, tài khoản `newStudent` không thuộc nhóm đó.

--- Hết ---