



LAB 2

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

Họ tên và MSSV: Huỳnh Quốc Dinh B2110009

Nhóm học phần: Nhóm 03

- 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 9 Stream vào máy tính cá nhân (hoặc máy ảo) của bạn **nếu cần** (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 **tên.họ** (ví dụ: **bao.quoc**). (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.

```
b2110009:x:1000:1000:Huynh Quoc Dinh:/home/b2110009:/bin/bash
dinh.huynh:x:1001:1001::/home/dinh.huynh:/bin/bash
```

```
Retype new password:
passwd: all authentication tokens updated successfully.
```

```
b2110009:x:1000:
dinh.huynh:x:1001:
```

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

Trả lời:

- Mật khẩu vừa tạo sử dụng giải thuật băm SHA-512 dựa vào các kí tự là: `6`

```
dinh.huynh:$6$VNSRm.uBjotKUQg3$TcXTq3Sfw/7Im0CmKb.qGAXL8WQIzCU00bosQCyQKs2mNcQWc
oTnnCe3JSTEpE.EITyGumjvW0JjJaq5EWymD1:19772:0:99999:7:::
```

2.3. Thiết lập ngày hết hạn cho tài khoản ở 2.1 là ngày 31/12/2024 (chụp hình minh họa).

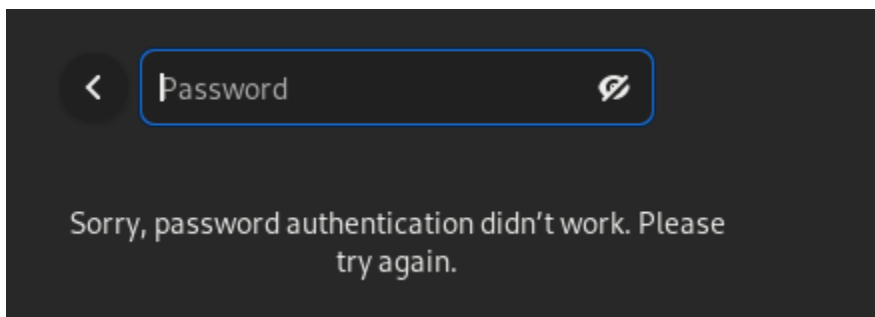
```
[b2110009@localhost ~]$ sudo chage -l dinh.huynh
Last password change           : Feb 19, 2024
Password expires                : never
Password inactive              : never
Account expires                : Dec 31, 2024
Minimum number of days between password change : 0
Maximum number of days between 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).

```
[b2110009@localhost ~]$ sudo usermod -a -G CT17903 dinh.huynh
[b2110009@localhost ~]$ groups dinh.huynh
dinh.huynh : dinh.huynh CT17903
```

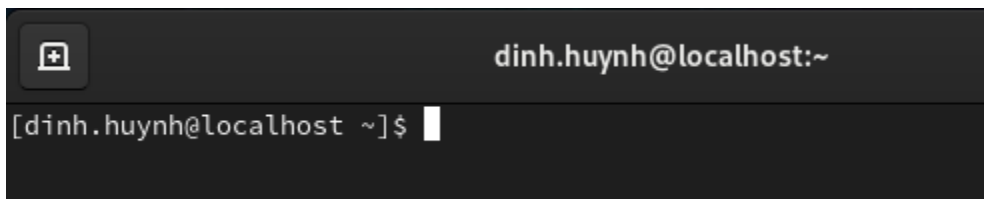
- 2.5. Thực hiện khóa tài khoản ở 2.1, sau đó đăng nhập thử và quan sát (chụp hình minh họa).

```
[b2110009@localhost ~]$ sudo usermod -L dinh.huynh
```



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

```
[b2110009@localhost ~]$ sudo usermod -U dinh.huynh
```



3. Quyền root (Root privilege) và sudo

Tìm hiểu và thực hiện các yêu cầu sau:

- 3.1. Quyền root là gì?

Trả lời:

- Quyền root là quyền hạn mà tài khoản root có trên hệ thống. Tài khoản root là đặc quyền lớn nhất trên hệ thống và có quyền lực tuyệt đối với nó (tức là truy cập đầy đủ vào tất cả các file và lệnh)

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

Trả lời:

- Sudo có khả năng xác định các ràng buộc về việc người dùng có thể sử dụng sudo hay không và có thể sử dụng các lệnh nào với nó. Các tập tin có thể chỉnh sửa.
- Ngoài ra sudo còn là nhật kí được lưu giữ cho mọi lệnh, giúp dễ dàng theo dõi những lỗi đã thực hiện và sửa lỗi.
- Sudo không cần chia sẻ mật khẩu vì nó có thể nâng cao các đặc quyền của người dùng cá nhân và cho phép họ có quyền truy cập vào những thứ họ cần.
- Các ưu điểm của sudo:
 - Sudo thường bao gồm 1 lệnh khác trong khi su thì không
 - Sudo có các ràng buộc có thể xác định trong khi su thì không
 - Sudo giữ 1 bản ghi của tất cả các lệnh trong khi su thì không
 - Bạn cần chia sẻ mật khẩu với su nhưng không phải với sudo
 - Sudo nâng cao các đặc quyền của người dùng trong khi su thì không

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).

Trả lời:

- Để cấp quyền cho 1 tài khoản nào đó, ta thực hiện thao tác trên tập tin sudoers. Hình minh họa cho cấu trúc lệnh:

```
[b2110009@localhost ~]$ sudo vi /etc/sudoers
```

- Bước 1: Phân quyền trên nhóm người dùng:

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

- Bước 2: Thêm người dùng vào nhóm wheel:

```
[b2110009@localhost ~]$ sudo usermod -a -G QTHT dinh.huynh
```

- Người dùng đã được thêm vào nhóm QTHT

```
[b2110009@localhost ~]$ groups dinh.huynh
dinh.huynh : dinh.huynh CT17903 QTHT
```

- Người dùng đã vào được file passwd

```
b2110009:x:1000:1000:Huynh Quoc Dinh:/home/b2110009:/bin/bash
dinh.huynh:x:1001:1001::/home/dinh.huynh:/bin/bash
38,1 Bot
```

- Người dùng đã vào được file shadow

```
dinh.huynh:$6$VNSRm.uBjotKUQg3$TcXTq3Sfw/7ImOCmKb.qGAXL8WQIzCU00bosQCyQKs2mNcQWq
oTnnCe3JSTEpE.EITyGumjvW0JjJaQ5EWymD1:19772:0:99999:7:20088:
"/etc/shadow" [readonly] 38L, 1277B
38,135 Bot
```

- Người dùng đã vào được file sudoers:

```
## Allows people in group wheel to run all commands
%wheel ALL=(ALL) ALL
%QTHT ALL=(ALL) ALL
## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
:wq
## Allows members of the users group to mount and unmount the
## cdrom as root
# %users ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d#
```

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

Trả lời:

Cú pháp xóa người dùng ra khỏi nhóm có quyền quản trị

```
[b2110009@localhost ~]$ sudo gpasswd -d dinh.huynh QTHT
```

Kết quả::

```
Removing user dinh.huynh from group QTHT
```

- Sau khi đã xóa tài khoản người dùng quản trị ra khỏi nhóm, tài khoản không còn được phép truy cập vào các file bảo mật

```
[dinh.huynh@localhost b2110009]$ sudo vi /etc/shadow
```

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

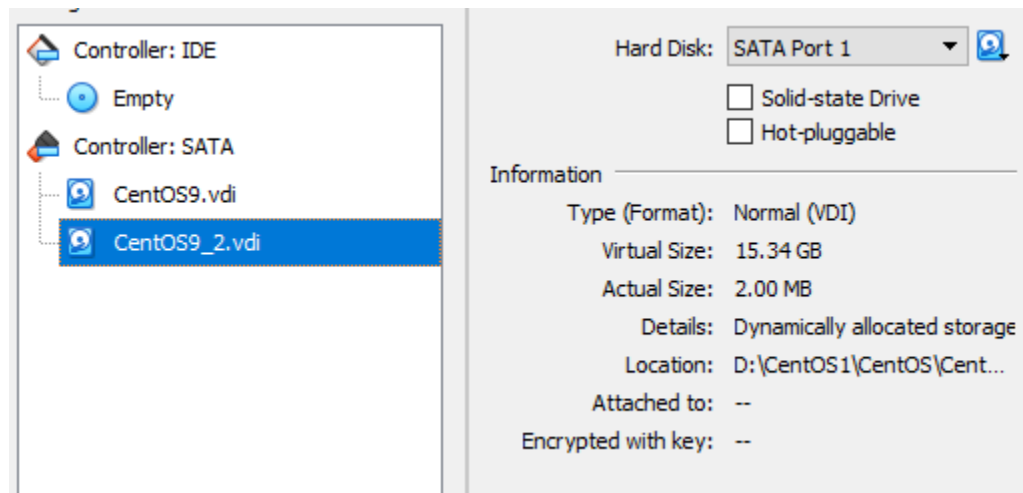
- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
[sudo] password for dinh.huynh:
Sorry, try again.
```

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.



- 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)

Trả lời:

- Tạo phân vùng với lệnh `fdisk`:

```
[b2110009@localhost ~]$ sudo fdisk /dev/sdb
```

+Lần lượt tạo 2 phân vùng trong 4 phân vùng chính:

```
Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-32171359, default 2048): 2048
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-32171359, default 32171359):
 21000000
Created a new partition 1 of type 'Linux' and of size 10 GiB.
```

```
Command (m for help): n
Partition type
  p   primary (1 primary, 0 extended, 3 free)
  e   extended (container for logical partitions)
Select (default p): p
Partition number (2-4, default 2): 2
First sector (21000001-32171359, default 21000192): 21000001
Last sector, +/-sectors or +/-size{K,M,G,T,P} (21000001-32171359, default 32171359):
32171359
Created a new partition 2 of type 'Linux' and of size 5.3 GiB.
```

- Tạo thành công 2 phân vùng cho đĩa

| Device | Boot | Start | End | Sectors | Size | Id | Type |
|-----------|------|-----------|-----------|----------|------|----|-------|
| /dev/sdb1 | | 2048 | 210000000 | 20997953 | 10G | 83 | Linux |
| /dev/sdb2 | | 210000001 | 32171359 | 11171359 | 5.3G | 83 | Linux |

- Định dạng cho phân vùng:theo tập tin:

```
[b2110009@localhost ~]$ sudo mkfs.ext4 /dev/sdb1
```

Kết quả:

```
[sudo] password for b2110009:
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 2624744 4k blocks and 657072 inodes
Filesystem UUID: 48ed2a8f-da39-48a8-9cc8-3cb4afea38f4
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

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 quyền sudo. Mount phân vùng ổ cứng ở 4.2 tới thư mục /data (chụp hình minh họa)

Trả lời:

- Tạo thư mục /data:

```
[b2110009@localhost ~]$ sudo mkdir /data
```

```
[b2110009@localhost ~]$ ls -l /
total 24
dr-xr-xr-x.  2 root root    6 Aug 10  2021 afs
lrwxrwxrwx.  1 root root    7 Aug 10  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root 4096 Jan 28 12:22 boot
drwxr-xr-x.  2 root root    6 Feb 20 11:09 data
```

- Mount phân vùng ổ cứng ở 4.2 tới thư mục /data

- Mount tạm thời:

```
[b2110009@localhost ~]$ sudo mount /dev/sdb1 /data
```

Kết quả:

```
[b2110009@localhost ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0    4.0M   0% /dev
tmpfs           1.8G   0    1.8G   0% /dev/shm
tmpfs           733M   9.2M 723M   2% /run
/dev/mapper/cs-root 14G   5.3G 8.2G  40% /
/dev/sda1       960M  303M 658M  32% /boot
tmpfs           366M   96K 366M   1% /run/user/1000
/dev/sdb1       9.8G   24K 9.3G   1% /data
```

- mount cố định:

- + In ID của Partition

```
[b2110009@localhost ~]$ sudo blkid /dev/sdb1
```

- + Thực hiện paste ID vào /etc/fstab

```
GNU nano 5.6.1 /etc/fstab
#
# /etc/fstab
# Created by anaconda on Sun Jan 28 05:02:17 2024
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/cs-root / xfs defaults 0 0
UUID=181f8b0e-f3a1-44e8-bba3-a8d8c1a148e9 /boot xfs defaults 0 0
/dev/mapper/cs-swap none swap defaults 0 0
UUID=48ed2a8f-da39-48a8-9cc8-3cb4afea38f4 /data ext4 defaults 0 0
```

- + Kiểm tra mount thông tin trong file fstab nếu không lỗi thông tin sẽ cập nhật đúng

```
[b2110009@localhost ~]$ sudo mount -a
```

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

```
[b2110009@localhost ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M   0    4.0M   0% /dev
tmpfs           1.8G   0    1.8G   0% /dev/shm
tmpfs           733M   9.2M 723M   2% /run
/dev/mapper/cs-root 14G   5.3G 8.2G  40% /
/dev/sda1       960M  303M 658M  32% /boot
tmpfs           366M   96K 366M   1% /run/user/1000
/dev/sdb1       9.8G   24K 9.3G   1% /data
```

5. Phân quyền trên hệ thống tập tin

5.1. Tạo nhóm người dùng `nhanvien`, thêm người dùng ở 2.1 vào nhóm `nhanvien`

Trả lời:

```
[b2110009@localhost ~]$ sudo groupadd nhanvien
```

```
[b2110009@localhost ~]$ sudo usermod -a -G nhanvien dinh.huynh
```

Kết quả:

```
[b2110009@localhost ~]$ groups dinh.huynh
dinh.huynh : dinh.huynh CT17903 nhanvien
```

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

Trả lời:

```
[b2110009@localhost ~]$ sudo chgrp nhanvien /data
```

- Thư mục data được tạo bởi tài khoản root, nhóm chủ sở hữu cũng là tài khoản root sau lệnh **chgrp tên_nhóm tên_thư_mục_cần_chuyển**
- Quyền trên thư mục data đã được thay đổi

```
[b2110009@localhost ~]$ ls -l /
total 28
dr-xr-xr-x.  2 root root      6 Aug 10  2021 afs
lrwxrwxrwx.  1 root root      7 Aug 10  2021 bin -> usr/bin
dr-xr-xr-x.  5 root root  4096 Jan 28 12:22 boot
drwxr-xr-x.  3 root nhanvien 4096 Feb 20 11:03 data
```

- chủ sở hữu có quyền read, write và execute, nhóm chủ sở hữu có quyền read và execute, những người khác không có bất kỳ quyền gì cả (chụp hình minh họa)
- Lệnh dùng thay đổi quyền chủ sở hữu

```
[b2110009@localhost ~]$ sudo chmod 750 /data
```

Kết quả:

```
# file: data
# owner: root
# group: nhanvien
user::rwx
group::r-x
other::---
```

- 5.3.** Dùng quyền sudo 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).

Trả lời:

- Tạo tập tin /data/file1.txt với quyền sudo

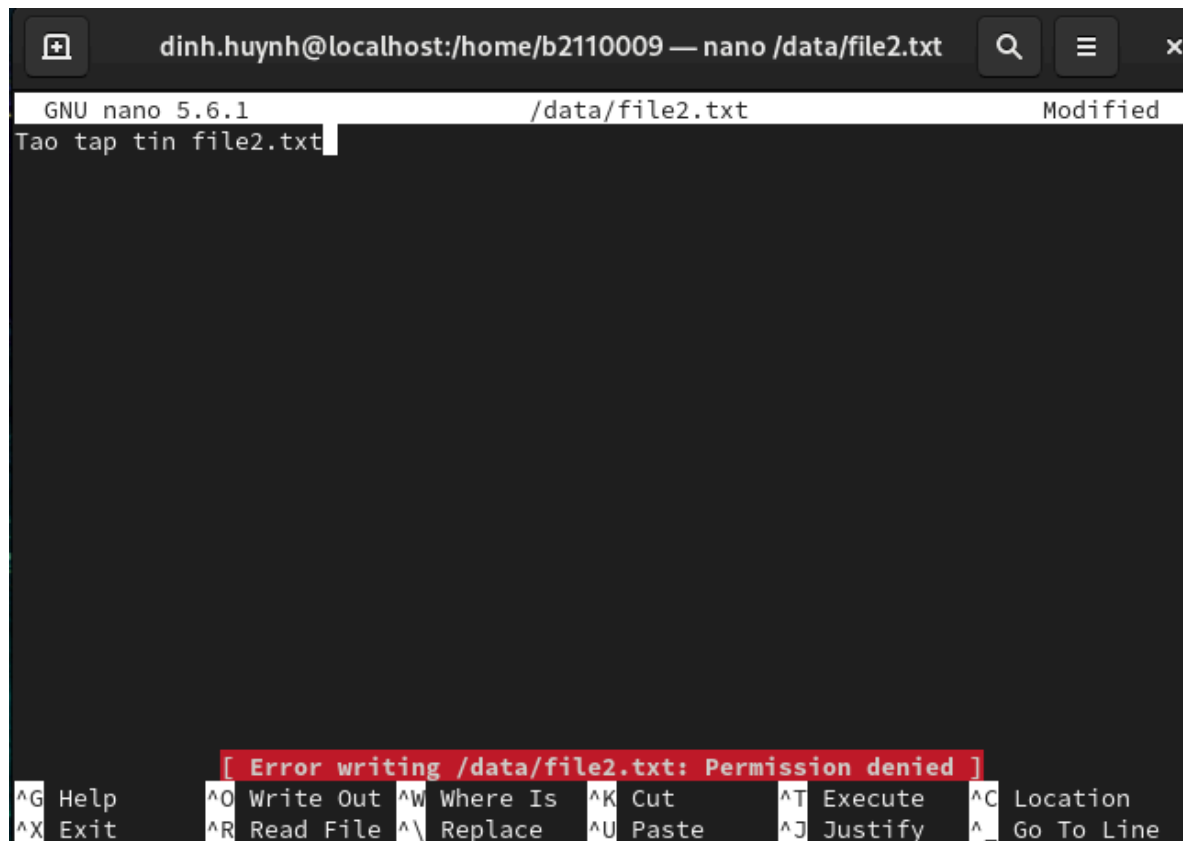
```
[b2110009@localhost ~]$ sudo nano /data/file1.txt
```



```
[b2110009@localhost ~]$ sudo cat /data/file1.txt
```

Tap tin file1.txt

- Tạo tập tin với quyền của người dùng 2.1



```
dinh.huynh@localhost:/home/b2110009 — nano /data/file2.txt
GNU nano 5.6.1 /data/file2.txt Modified
Tao tap tin file2.txt

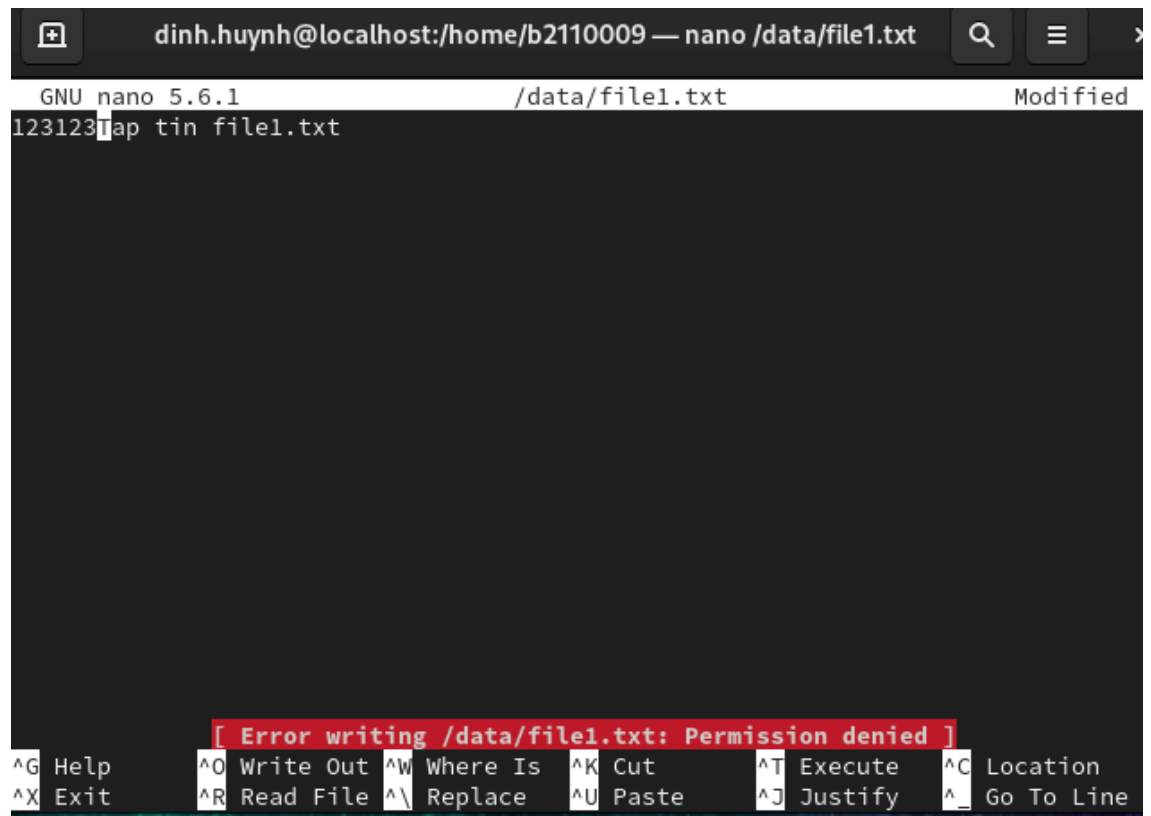
[ Error writing /data/file2.txt: Permission denied ]
^G Help  ^O Write Out  ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit  ^R Read File  ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

-> **Lỗi** do người dùng chỉ có quyền đọc và thực thi trên thư mục data và **không có quyền ghi**

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

Trả lời:

- Người dùng không thể thay đổi nội dung vì người dùng chỉ có quyền đọc và thực thi



The screenshot shows the nano 5.6.1 text editor interface. The title bar indicates the user is 'dinh.huynh@localhost' and the file being edited is '/data/file1.txt'. The editor content shows the text '123123' followed by a cursor and the text 'Tập tin file1.txt'. A red error message is displayed at the bottom: '[Error writing /data/file1.txt: Permission denied]'. The bottom status bar shows various keyboard shortcuts: ^G Help, ^O Write Out, ^W Where Is, ^K Cut, ^T Execute, ^C Location, ^X Exit, ^R Read File, ^\ Replace, ^U Paste, ^J Justify, and ^_ Go To Line.

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

Trả lời:

- Dùng tài khoản có quyền thay đổi nội dung, cấp quyền cho người dùng khác có quyền ghi

```
[b2110009@localhost ~]$ sudo chmod o+w /data/file1.txt
```

```
[b2110009@localhost ~]$ sudo ls -l /data
```

```
-rw-r--rw-. 1 root root  18 Feb 20 13:37 file1.txt
drwx----- 2 root root 16384 Feb 20 11:03 lost+found
```

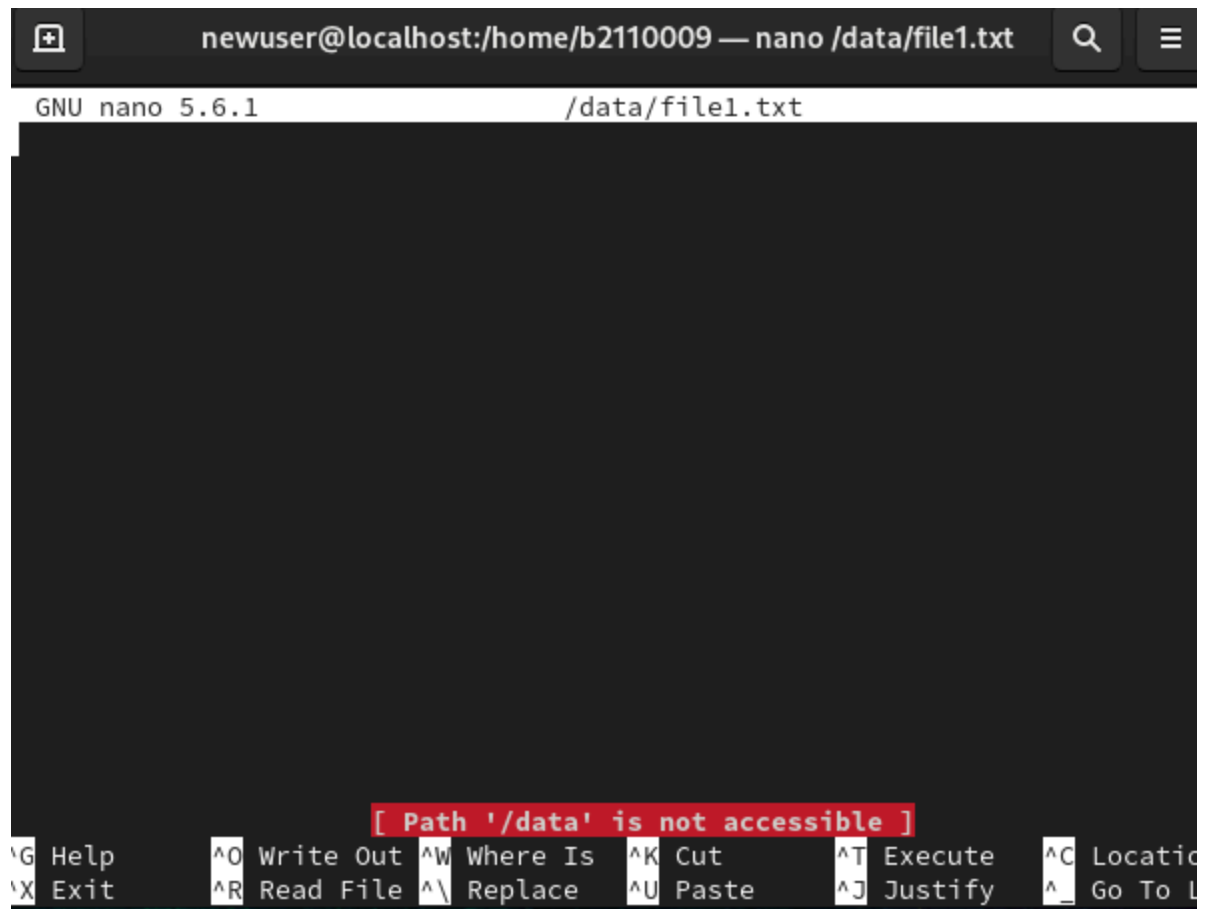
Kết quả: Chỉnh sửa thành công

```
[dinh.huynh@localhost b2110009]$ cat /data/file1.txt
Sua Tap tin file1.txt
```

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

Trả lời:

- Không thể truy cập



- 5.7. Dùng quyền sudo** tạo thư mục /report và tạo nhóm người dùng quantri. Phân quyền trên thư mục /report sao cho nhóm quantri có quyền read, write và execute, nhóm nhanvien có quyền read và execute, người dùng ở 2.1 có quyền execute, những người khác không có bất kỳ quyền gì cả (chụp hình minh họa).

Trả lời:

- Tạo thư mục /report

```
[b2110009@localhost ~]$ sudo mkdir /report
```

```
dr-xr-xr-x. 263 root root      0 Feb 20 12:56 proc
drwxr-xr-x.   2 root root      6 Feb 20 14:10 report
```

- Tạo nhóm quantri

```
[b2110009@localhost ~]$ sudo groupadd quantri
```

- Cấp quyền cho nhóm quantri

```
[b2110009@localhost ~]$ sudo setfacl -m g:quantri:rwX /report
/etc/sudoers:111:1: syntax error
```

```
group::r-x
group:quantri:rwx
```

- **Cấp quyền cho nhóm nhanvien:**

```
[b2110009@localhost ~]$ sudo setfacl -m g:nhanvien:rx /report
```

```
group::r-x
group:nhanvien:r-x
```

- **Người dùng ở 2.1 có quyền execute**

```
[b2110009@localhost ~]$ sudo setfacl -m u:dinh.huynh:x /report
/etc/sudoers:111:1: syntax error
```

```
user:dinh.huynh:--x
```

- **Người dùng khác không có quyền**

```
[b2110009@localhost ~]$ sudo setfacl -m o:---:x /report
```

```
mask::rwx
other:---
```

--- Hết ---