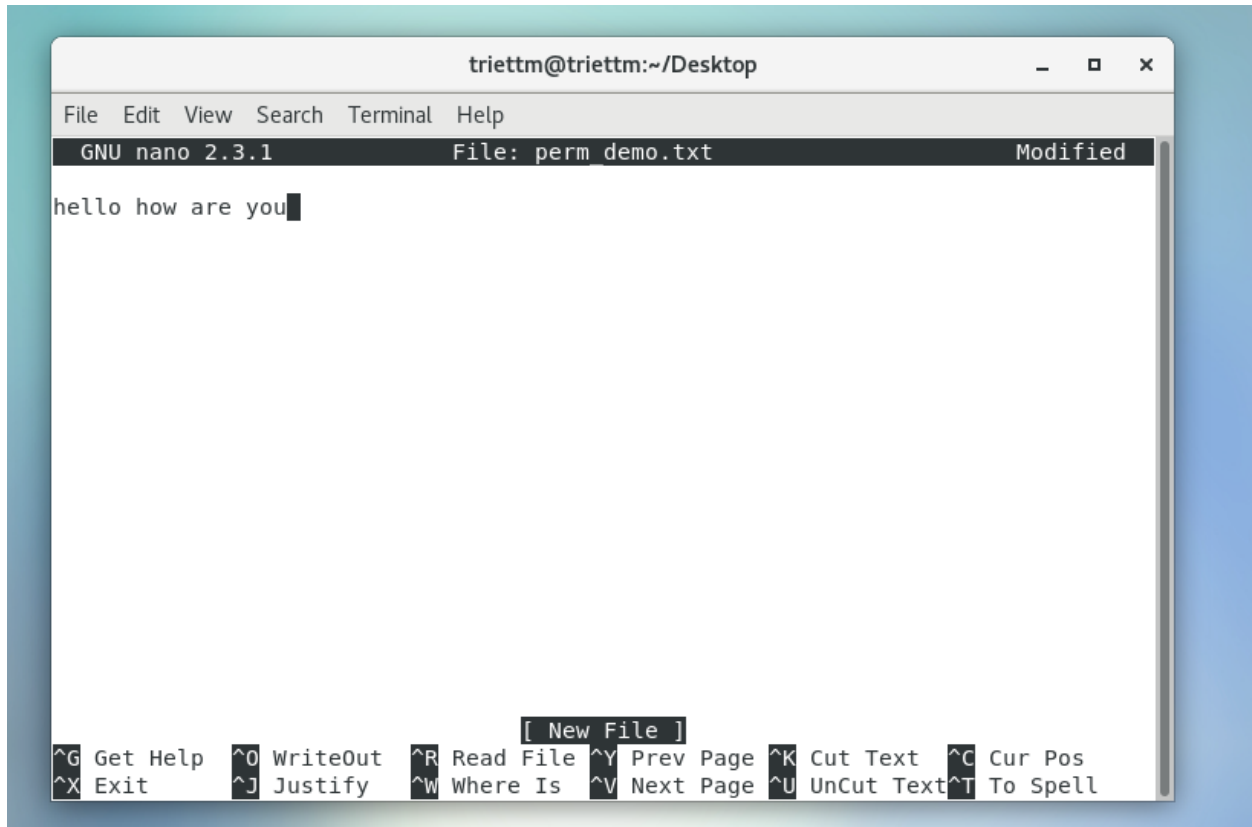


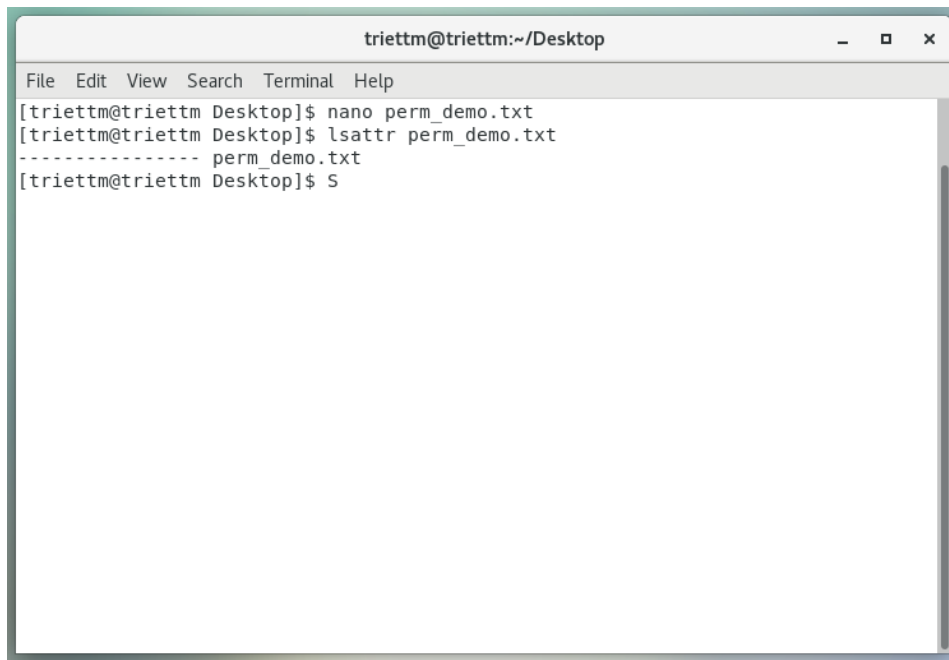
Hands-on lab – setting security-related extended file Attributes

1. Using your preferred text editor, create the perm_demo.txt file with a line of text.

A screenshot of a terminal window titled 'triетtm@triетtm:~/Desktop'. The window shows the GNU nano 2.3.1 text editor editing a file named 'perm_demo.txt'. The text 'hello how are you' is entered on the first line. The bottom of the screen displays a list of keyboard shortcuts for the nano editor, including '^G Get Help', '^O WriteOut', '^R Read File', '^Y Prev Page', '^K Cut Text', '^C Cur Pos', '^X Exit', '^J Justify', '^W Where Is', '^V Next Page', '^U UnCut Text', and '^T To Spell'. A '[New File]' prompt is also visible above the shortcuts.

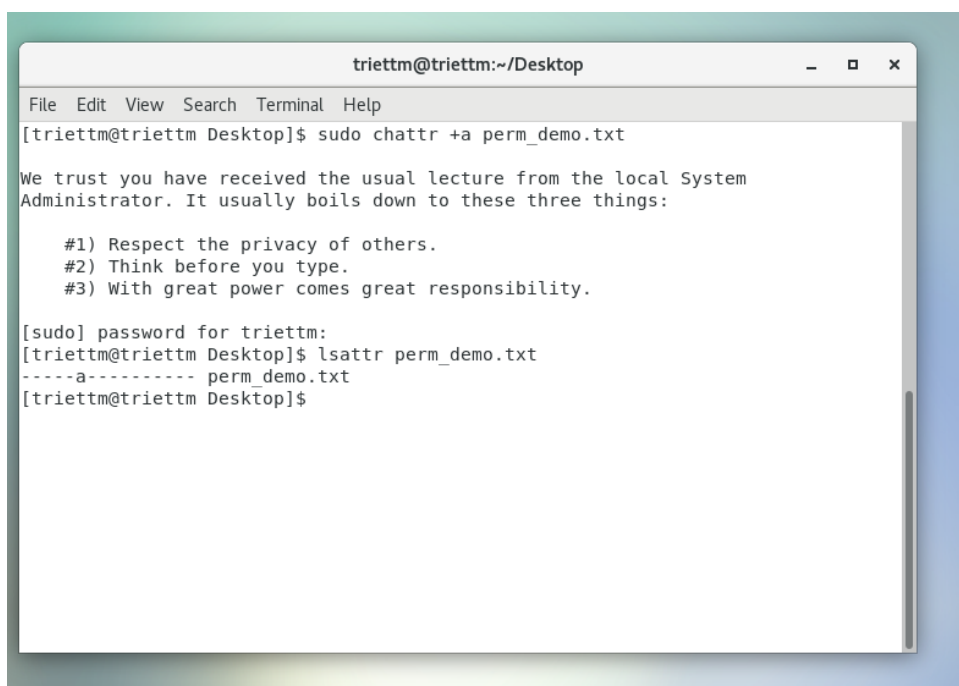
```
triетtm@triетtm:~/Desktop
File Edit View Search Terminal Help
GNU nano 2.3.1 File: perm_demo.txt Modified
hello how are you
[ New File ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

2. View the extended attributes of the file:



```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ nano perm_demo.txt
[triettm@triettm Desktop]$ lsattr perm_demo.txt
----- perm_demo.txt
[triettm@triettm Desktop]$ S
```

3. Add the a attribute:



```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ sudo chattr +a perm_demo.txt

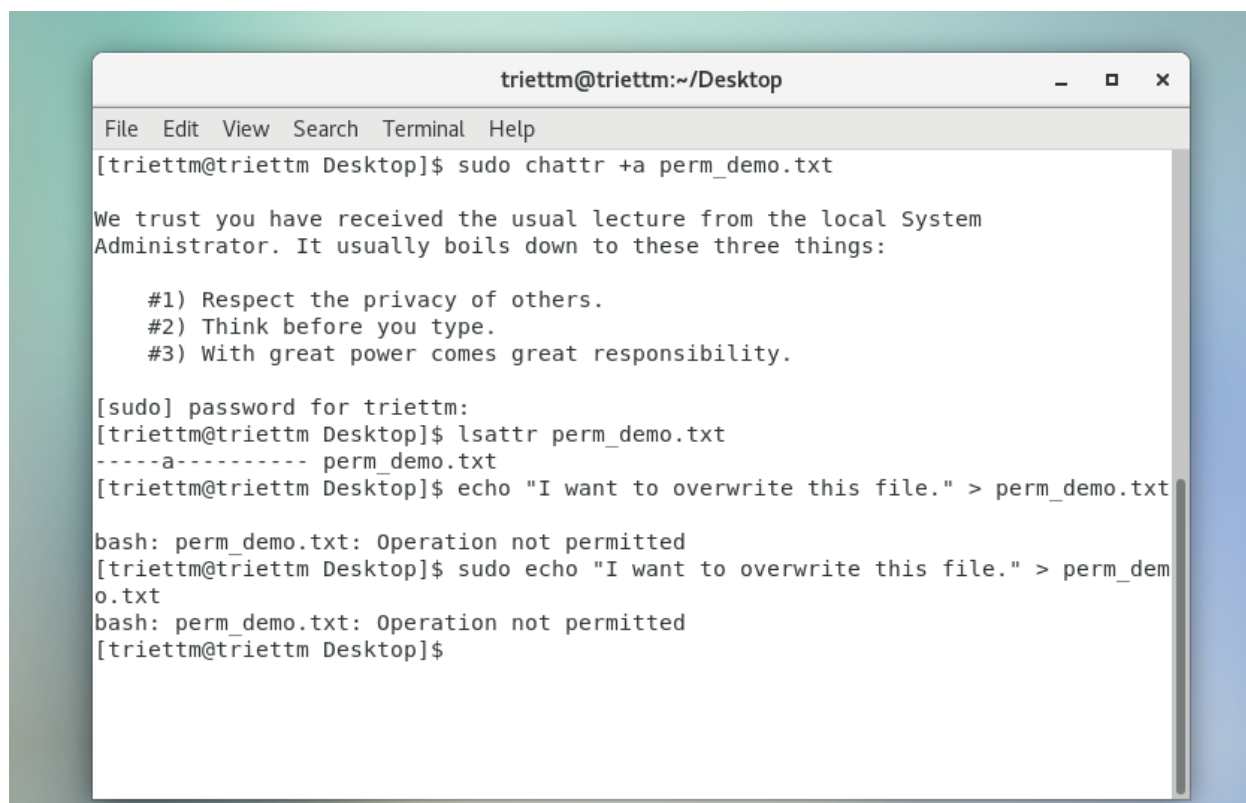
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

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

[sudo] password for triettm:
[triettm@triettm Desktop]$ lsattr perm_demo.txt
-----a----- perm_demo.txt
[triettm@triettm Desktop]$
```

Quyền “a” chỉ cho phép ta ghi nối chứ không được ghi đè hay xóa nội dung file.

4. Try to overwrite and delete the file:



```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ sudo chattr +a perm_demo.txt

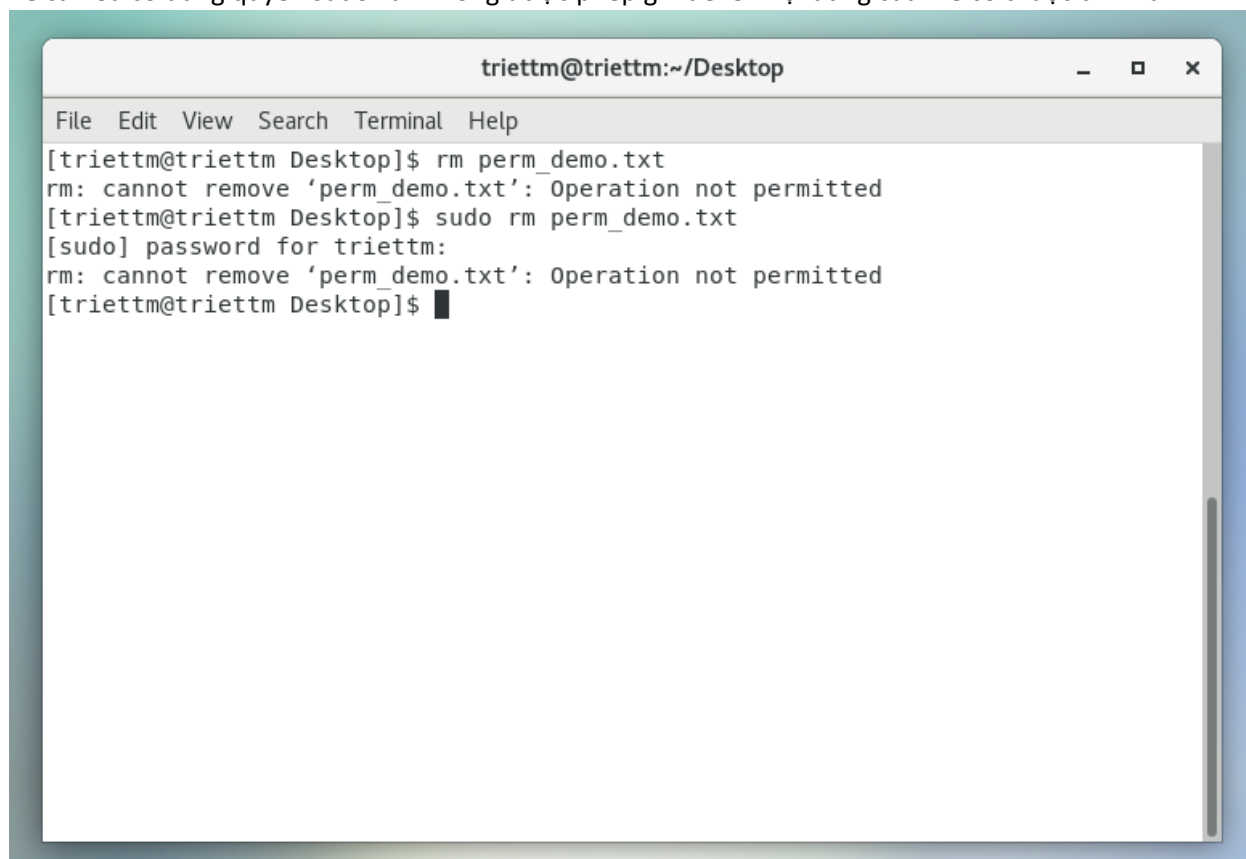
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

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

[sudo] password for triettm:
[triettm@triettm Desktop]$ lsattr perm_demo.txt
-----a----- perm_demo.txt
[triettm@triettm Desktop]$ echo "I want to overwrite this file." > perm_demo.txt

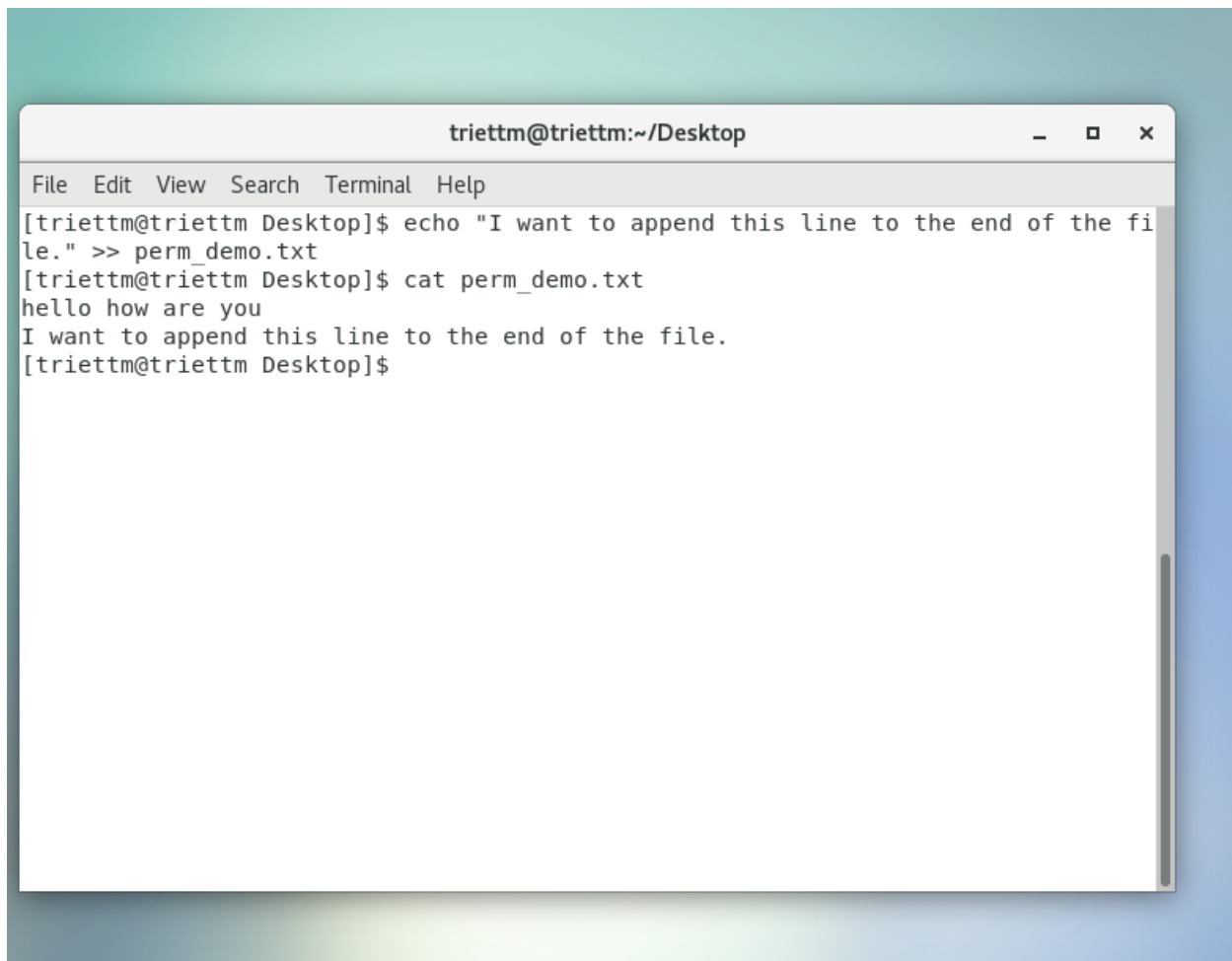
bash: perm_demo.txt: Operation not permitted
[triettm@triettm Desktop]$ sudo echo "I want to overwrite this file." > perm_demo.txt
bash: perm_demo.txt: Operation not permitted
[triettm@triettm Desktop]$
```

Kể cả nếu có dùng quyền sudo vẫn không được phép ghi đè lên nội dung của file có thuộc tính +a



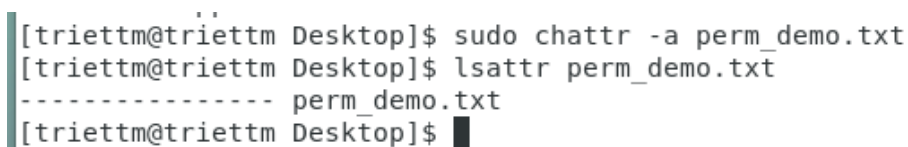
```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ rm perm_demo.txt
rm: cannot remove 'perm_demo.txt': Operation not permitted
[triettm@triettm Desktop]$ sudo rm perm_demo.txt
[sudo] password for triettm:
rm: cannot remove 'perm_demo.txt': Operation not permitted
[triettm@triettm Desktop]$
```

Tương tự như vậy kể cả dùng quyền sudo vẫn không thể xóa file có thuộc tính +a

A screenshot of a terminal window titled "triettm@triettm:~/Desktop". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal shows the following commands and output:

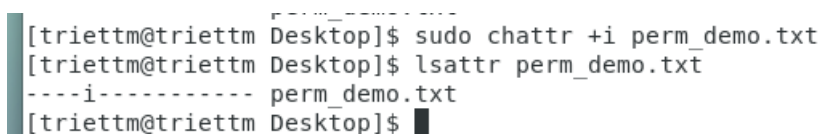
```
[triettm@triettm Desktop]$ echo "I want to append this line to the end of the file." >> perm_demo.txt
[triettm@triettm Desktop]$ cat perm_demo.txt
hello how are you
I want to append this line to the end of the file.
[triettm@triettm Desktop]$
```

Tuy nhiên quyền +a lại cho phép ta ghi nối nội dung của file.

A terminal snippet showing the following commands and output:

```
[triettm@triettm Desktop]$ sudo chattr -a perm_demo.txt
[triettm@triettm Desktop]$ lsattr perm_demo.txt
----- perm_demo.txt
[triettm@triettm Desktop]$
```

Xóa bỏ quyền a

A terminal snippet showing the following commands and output:

```
[triettm@triettm Desktop]$ sudo chattr +i perm_demo.txt
[triettm@triettm Desktop]$ lsattr perm_demo.txt
----i----- perm_demo.txt
[triettm@triettm Desktop]$
```

Thêm quyền I cho file

```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ sudo echo "I want to overwrite this file." > perm_demo.txt
bash: perm_demo.txt: Permission denied
[triettm@triettm Desktop]$ sudo rm perm_demo.txt
rm: cannot remove 'perm_demo.txt': Operation not permitted
[triettm@triettm Desktop]$
```

Quyền i không cho phép bất cứ ai hay bất cứ thứ gì thay đổi nội dung của nó hết.

```
[triettm@triettm Desktop]$ mv perm_demo.txt some_file.txt
mv: cannot move 'perm_demo.txt' to 'some_file.txt': Operation not permitted
[triettm@triettm Desktop]$ sudo mv perm_demo.txt some_file.txt
mv: cannot move 'perm_demo.txt' to 'some_file.txt': Operation not permitted
[triettm@triettm Desktop]$
```

Đổi tên cũng không cho

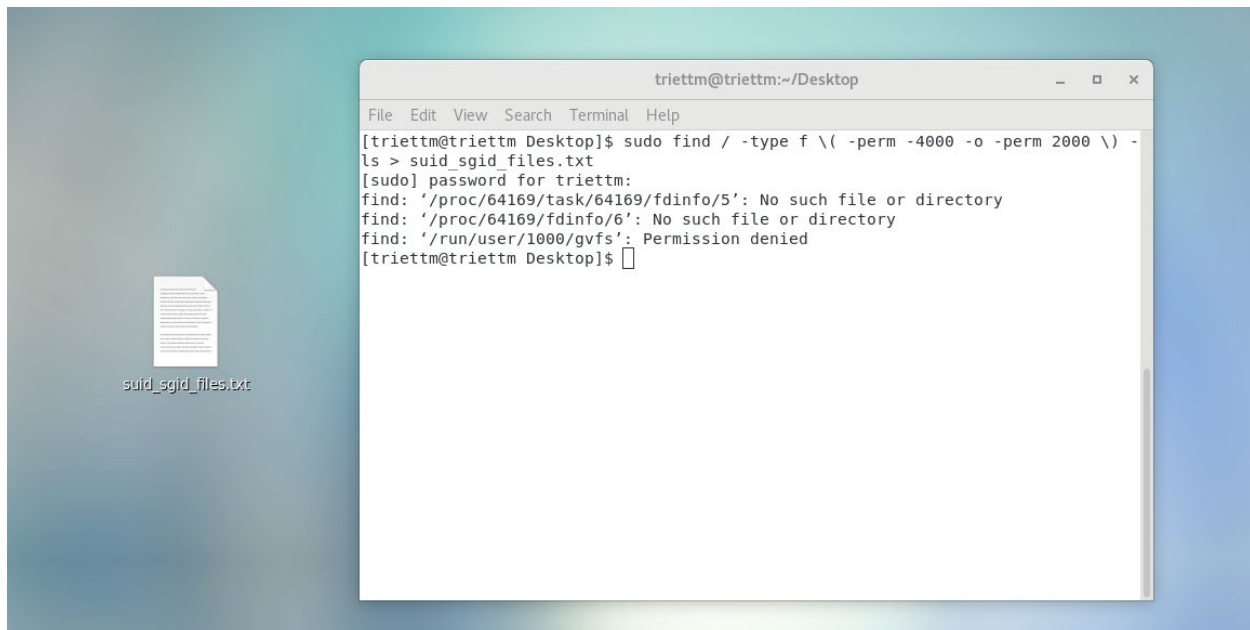
```
[triettm@triettm Desktop]$ ln ~/perm_demo.txt ~/some_file.txt
ln: failed to access '/home/triettm/perm_demo.txt': No such file or directory
[triettm@triettm Desktop]$ sudo ln ~/perm_demo.txt ~/some_file.txt
ln: failed to access '/home/triettm/perm_demo.txt': No such file or directory
[triettm@triettm Desktop]$
```

Link cũng không cho

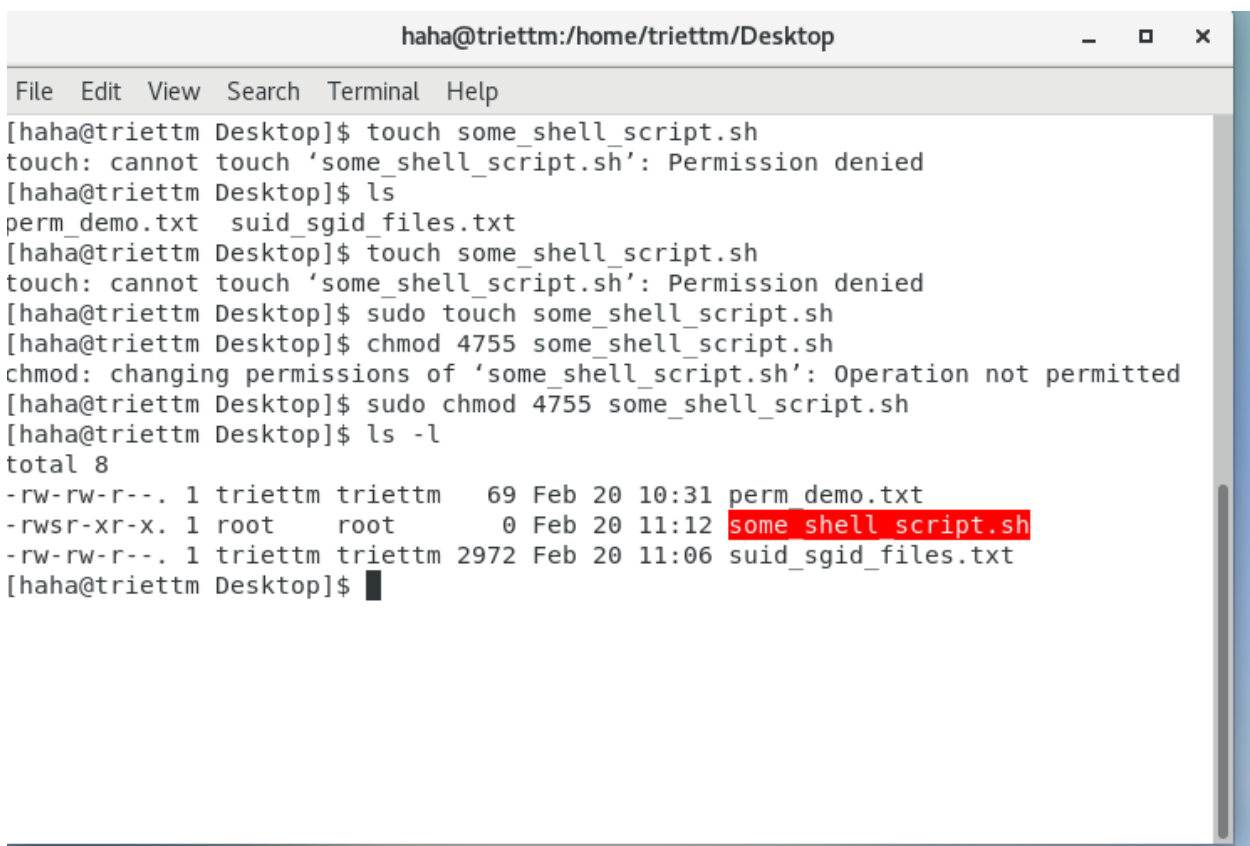
```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ ln -s ~/perm_demo.txt ~/some_file.txt
[triettm@triettm Desktop]$ ls -la
total 8
drwxr-xr-x. 2 triettm triettm 27 Feb 20 09:55 .
drwx----- 15 triettm triettm 4096 Feb 20 10:37 ..
-rw-rw-r--. 1 triettm triettm 69 Feb 20 10:31 perm_demo.txt
[triettm@triettm Desktop]$
```

Tạo symbolic link thì cho

Hands-on lab – searching for SUID and SGID files



Tìm tất cả các file có quyền SUID là 4000 và quyền GUID là 2000 rồi ghi kết quả vào file suid_guid_files.txt.



Tạo một shell script với quyền SUID.

```
triettm@triettm:~/Desktop
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ sudo find / -type f \( -perm -4000 -o -perm 2000 \) -ls > suid_sgid_files_2.txt
find: '/proc/65035/task/65035/fdinfo/5': No such file or directory
find: '/proc/65035/fdinfo/6': No such file or directory
find: '/run/user/1000/gvfs': Permission denied
[triettm@triettm Desktop]$ diff suid_sgid_files_2.txt suid_sgid_files.txt
33d32
< 68222713      0 -rwsr-xr-x   1 root      root          0 Feb 20 11:12 /home/triettm/Desktop/some_shell_script.sh
[triettm@triettm Desktop]$
```

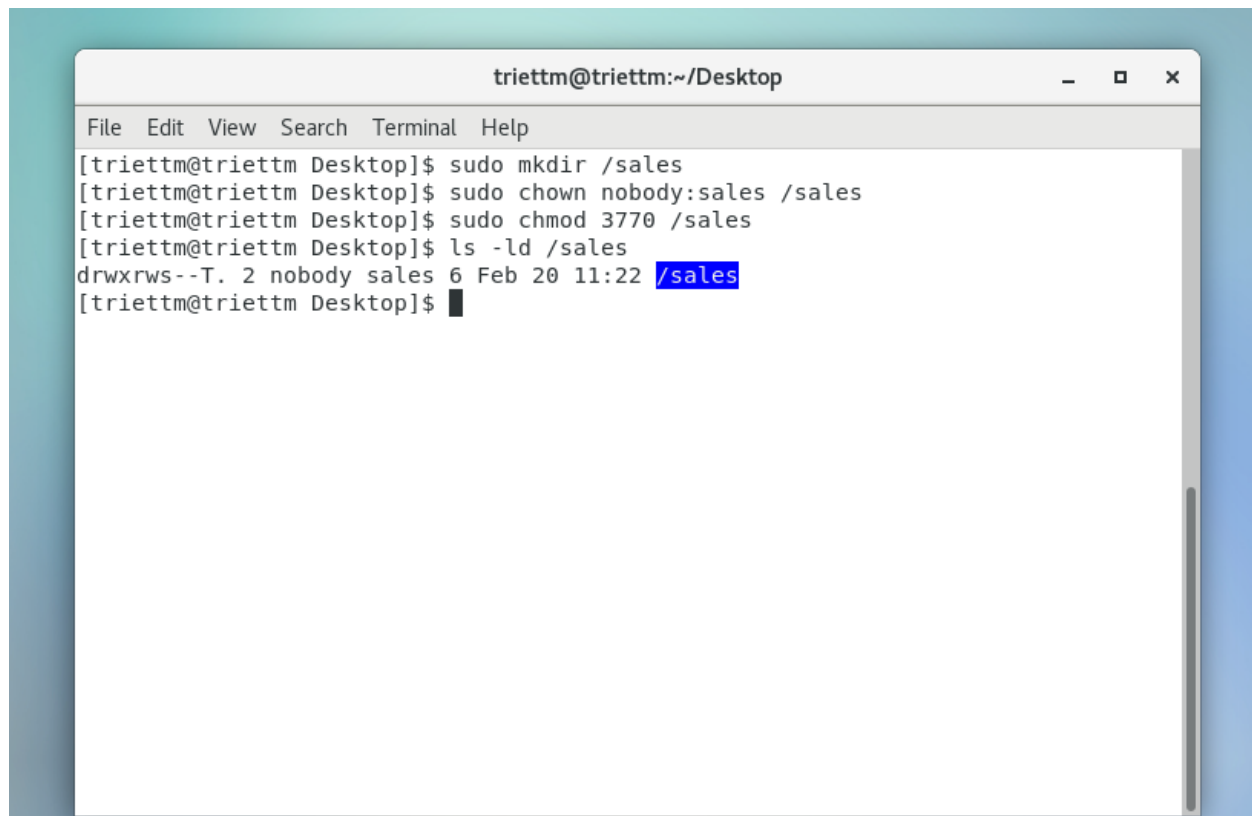
Hai file có content khác nhau do ta đã thêm một file có quyền SUID vào file system.

Hands-on lab – creating a shared group directory

```
triettm@triettm Desktop
[triettm@triettm Desktop]$ sudo groupadd sales
[triettm@triettm Desktop]$
```

Tạo group sales.

```
[triettm@triettm Desktop]$ sudo groupadd sales
[triettm@triettm Desktop]$ sudo useradd -G sales mimi
[triettm@triettm Desktop]$ sudo useradd -G sales mrgray
[triettm@triettm Desktop]$ sudo useradd -G sales mommy
[triettm@triettm Desktop]$
```



A terminal window titled "triettm@triettm:~/Desktop" with standard window controls (minimize, maximize, close). The menu bar includes "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal content shows a series of commands to create and configure the "/sales" directory:

```
[triettm@triettm Desktop]$ sudo mkdir /sales
[triettm@triettm Desktop]$ sudo chown nobody:sales /sales
[triettm@triettm Desktop]$ sudo chmod 3770 /sales
[triettm@triettm Desktop]$ ls -ld /sales
drwxrws--T. 2 nobody sales 6 Feb 20 11:22 /sales
[triettm@triettm Desktop]$
```

The output of the final command shows the directory permissions as "drwxrws--T. 2 nobody sales 6 Feb 20 11:22 /sales", with the path "/sales" highlighted in blue.


```
mimi@triettm:/sales
File Edit View Search Terminal Help
[triettm@triettm Desktop]$ su - mimi
Password:
Last failed login: Mon Feb 20 11:22:50 +07 2023 on pts/0
There was 1 failed login attempt since the last successful login.
[mimi@triettm ~]$ cd /sales
[mimi@triettm sales]$ echo "This file belongs to Mimi." > mimi_file.txt
[mimi@triettm sales]$ ls -l
total 4
-rw-rw-r--. 1 mimi sales 27 Feb 20 11:23 mimi_file.txt
[mimi@triettm sales]$
```

```
mimi@triettm:/sales
File Edit View Search Terminal Help
[mimi@triettm sales]$ chmod 600 mimi_file.txt
[mimi@triettm sales]$ setfacl -m u:mrgray:r mimi_file.txt
[mimi@triettm sales]$ getfacl mimi_file.txt
# file: mimi_file.txt
# owner: mimi
# group: sales
user::rw-
user:mrgray:r--
group:---
mask::r--
other:---
[mimi@triettm sales]$
```