Lesson 7 Linux Permission

In operating system, permissions are required to access the file, enter the directory and change the file.

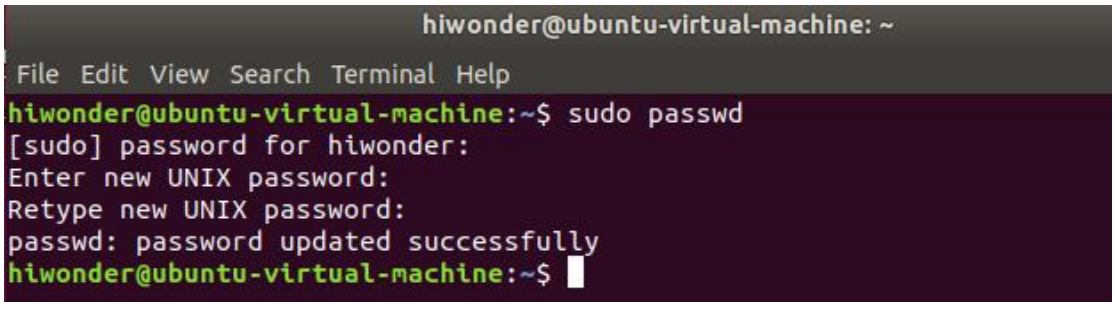
In Linux, different users, including supper user (root) and normal user, have different permission. Super user can do anything on Linux almost without limitation, while normal user can only operate within permissions.

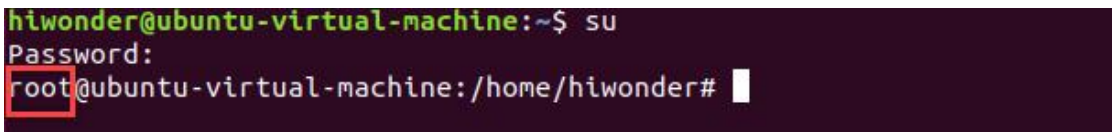
For example, in the same file, super user can edit it, while normal user can only read it without other operations.

1. Change User

It is simple to change user through command. But we need to set a fixed password first, as root password is generated randomly whenever Ubuntu reboots by default.

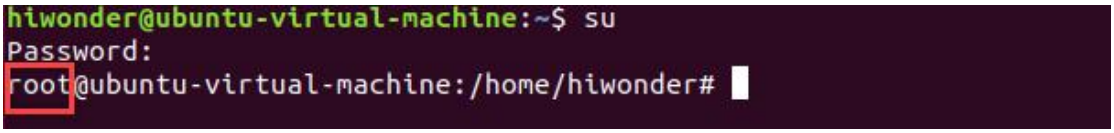
1) Open command line terminal and input "**sudo passwd**" command. Then input the password and press Enter to set root password. Pay attention you are required to input the password twice. (**Note: the password you input will be hidden and you can just press Enter after inputting**)





2) After setting root password, input "**su**", and then input the password

currently set and press **Enter**. When **$** at the end of the command changes to **#**, it means that the directory is switched to root directory.



2. File Permission

Files can be written, read and executed. And files can be divided into three types by visitor：

① Owner：user of files

② Group：group files belong to

③ Other

Owner, group and other indicate roles, such as programmer, while root user and normal user refer to specific person, such as you.

And each role has three permissions.

r：read

read permission grants the ability to read a file. When set for a directory, what is in the directory cannot be viewed.

w：write

The write permission grants the ability to write data to the file. When set for a directory, the files in the directory cannot be deleted.

x：execute

The execute permission grants the ability to execute a file, which is inapplicable to non-executable file. When set for directory, we cannot enter the

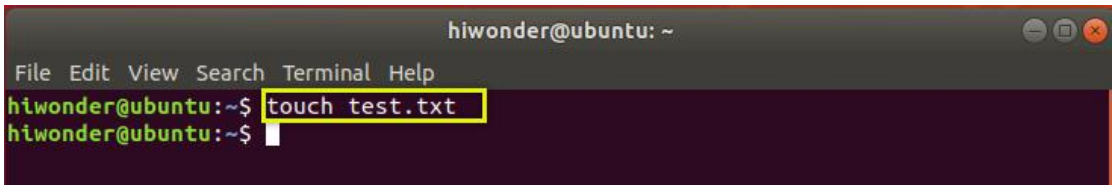
directory.

Linux	Octal	Explanation
r--	4	Read permission only
-w-	2	Write permission only
--x	1	Execute permission only
r-x	5	Read and execute permission
rw-	6	Read and write permission
-wx	3	Write and execute permission
rwx	7	Wire, read and execute permission

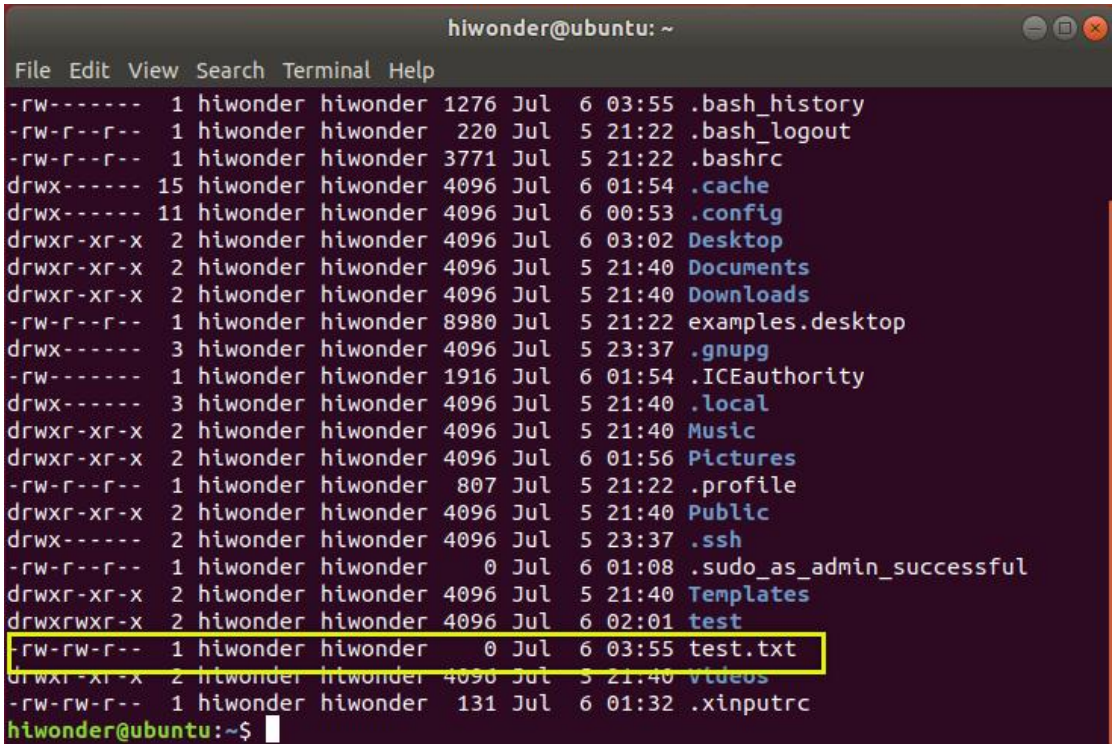
3. Change Permission

chmod command is used to change permission, which is divided into two ways. One is change the permission through number code, the other is change the permission through character code.

1) Open the terminal interface, and input "**touch test.txt**" command to create txt file.

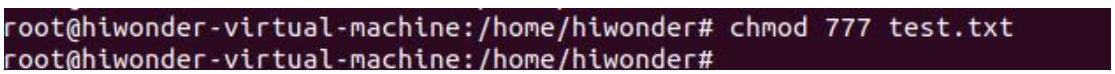


2) Then enter "**ls -al**" command to list the files under this path and display their specific properties.

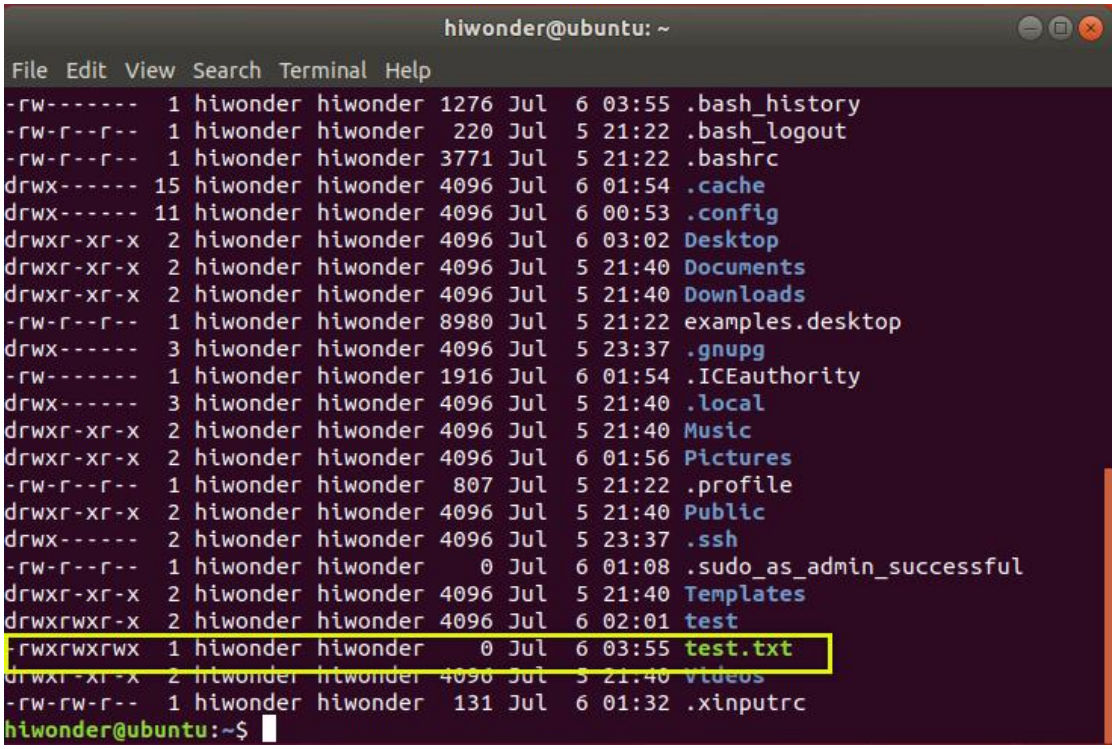


As the picture shown above, the owners of the files are granted with read and write permission, while group and other users only have read permission.

For example, we can grant execute permission to group and other users. Input "**chmod 777 test.txt**" command.

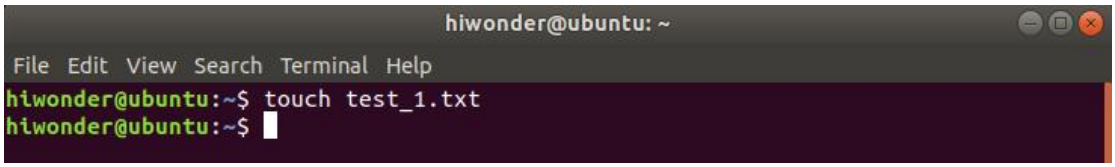


3) Next, input "**ls -al**" again to check whether the permission is changed.

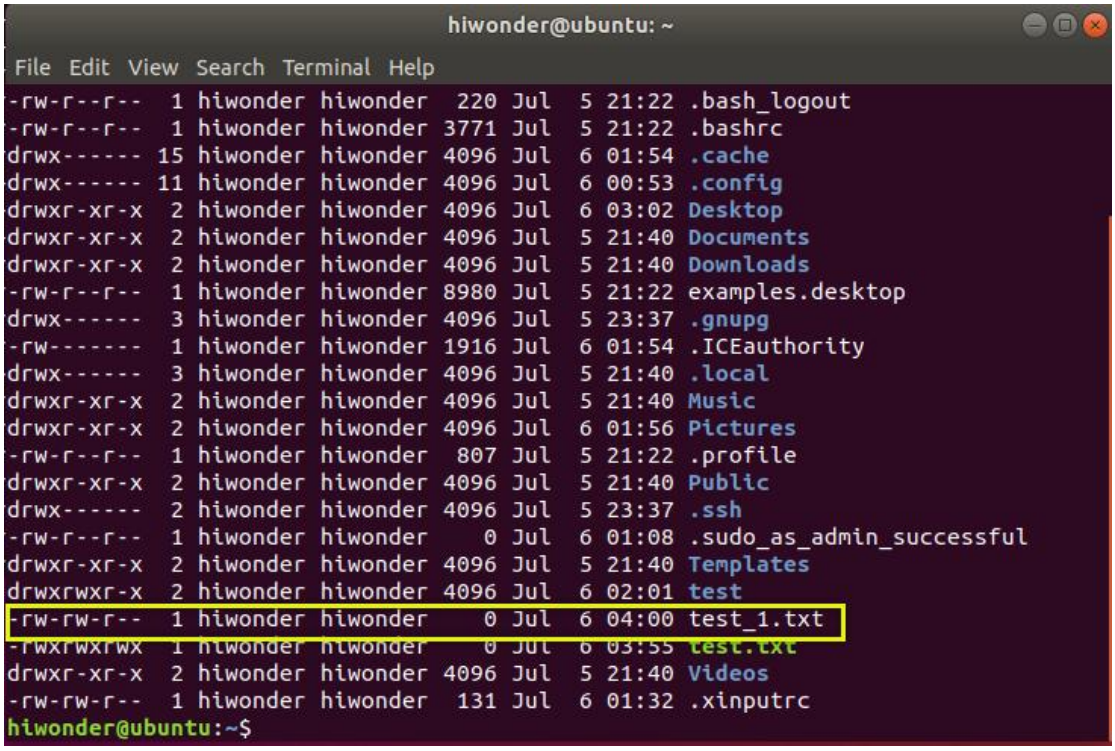


All permissions of these three roles can be changed through number code for one time. For changing permission through character code, please check the operations below.

Compared with number code, it is more flexible to change permission through character code. We can set individual permission for one role, for example enter command “**touch test_1.txt**” to create a txt file named **test_1**



4) Next, input “**ls -al**” command to view the file permission.

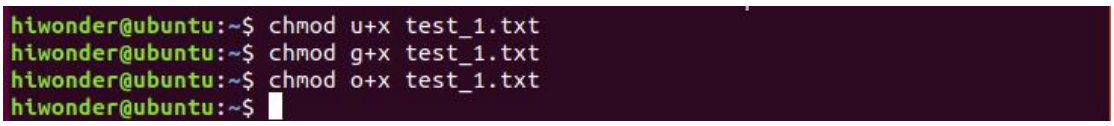


5) Take granting execute permission to owner, group and other users separately for example.

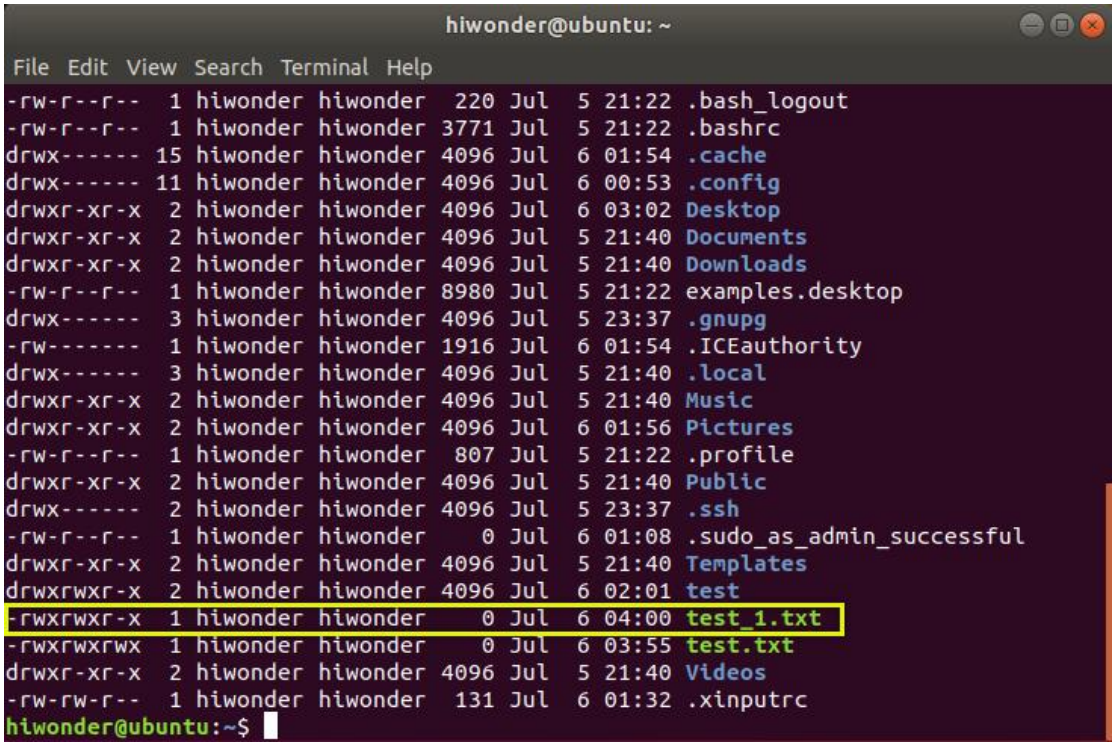
The commands are as follow.

```
chmod u+x test_1.txt

chmod g+x test_1.txt

chmod o+x test_1.txt
```

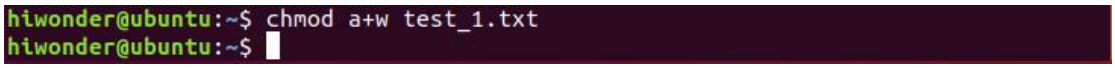
6) As the same, we can modify x(execute) as r (read) or w(write) to set read or write permission.



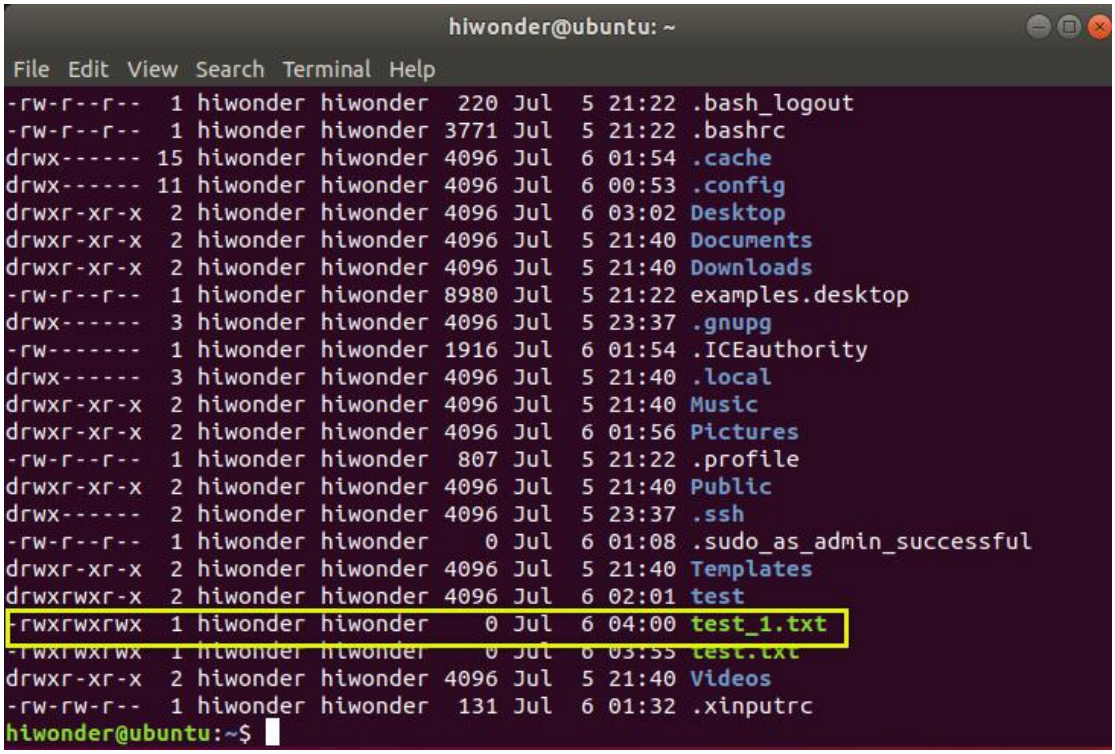
7) After setting, input "**ls -al**" command to check the properties.



8) If you don't want to set separately, for example, we can input "**chmod a+w test_1.txt**" command to set write permission for three roles. And "**a**" represents three roles.



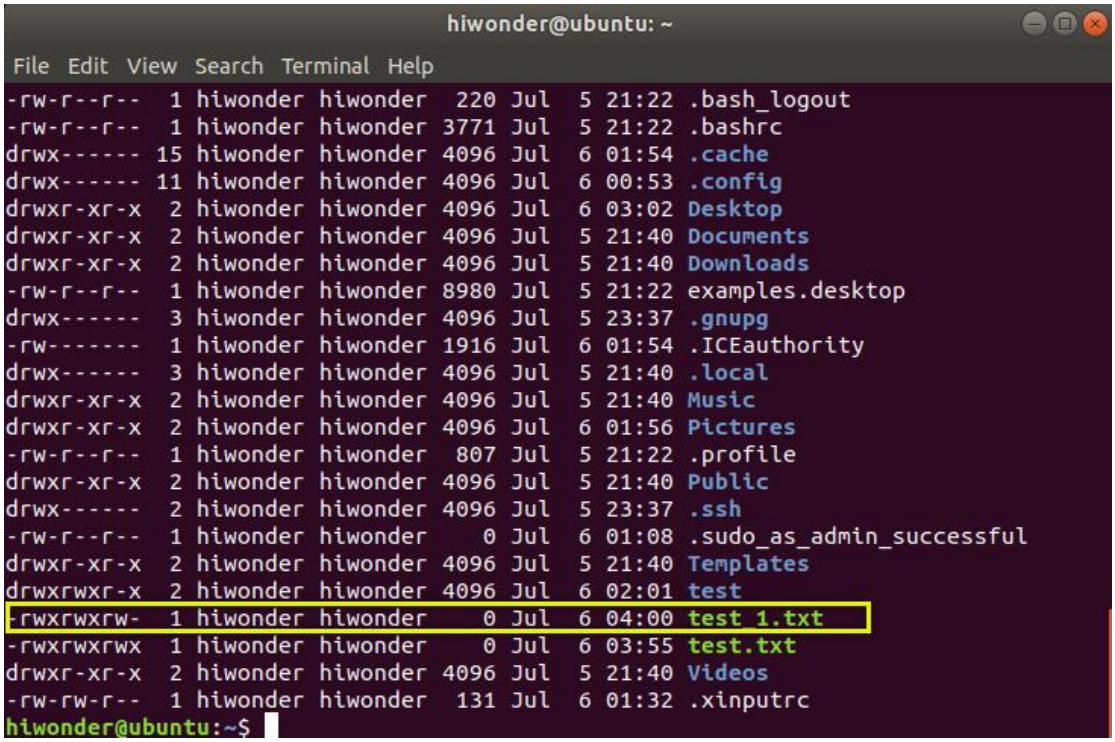
9) Next, input "**ls -al**" command to check the properties.



If want to remove the permission from visitor, we can change "**+**" as "**-**". For example, remove the execute permission of other users.

10) Input "**chmod o-x test_1.txt**" command.

11) Then enter "ls -al" command to view the properties.


hiwonder@ubuntu: ~
File Edit View Search Terminal Help
-rw-r--r-- 1 hiwonder hiwonder 220 Jul 5 21:22 .bash_logout
-rw-r--r-- 1 hiwonder hiwonder 3771 Jul 5 21:22 .bashrc
drwx------ 15 hiwonder hiwonder 4096 Jul 6 01:54 .cache
drwx------ 11 hiwonder hiwonder 4096 Jul 6 00:53 .config
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 6 03:02 Desktop
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 5 21:40 Documents
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 5 21:40 Downloads
-rw-r--r-- 1 hiwonder hiwonder 8980 Jul 5 21:22 examples.desktop
drwx------ 3 hiwonder hiwonder 4096 Jul 5 23:37 .gnupg
-rw------- 1 hiwonder hiwonder 1916 Jul 6 01:54 .ICEauthority
drwx------ 3 hiwonder hiwonder 4096 Jul 5 21:40 .local
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 5 21:40 Music
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 6 01:56 Pictures
-rw-r--r-- 1 hiwonder hiwonder 807 Jul 5 21:22 .profile
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 5 21:40 Public
drwx------ 2 hiwonder hiwonder 4096 Jul 5 23:37 .ssh
-rw-r--r-- 1 hiwonder hiwonder 0 Jul 6 01:08 .sudo_as_admin_successful
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 5 21:40 Templates
drwxrwxr-x 2 hiwonder hiwonder 4096 Jul 6 02:01 test
-rwxrwxrw- 1 hiwonder hiwonder 0 Jul 6 04:00 test 1.txt
-rwxrwxrwx 1 hiwonder hiwonder 0 Jul 6 03:55 test.txt
drwxr-xr-x 2 hiwonder hiwonder 4096 Jul 5 21:40 Videos
-rw-rw-r-- 1 hiwonder hiwonder 131 Jul 6 01:32 .xinputrc
hiwonder@ubuntu:~$