Exsercise 11: Managing Files - Part 2

I. Prepare the environment
II. Manage file permission and ownership

1. Login to the CentOS server with user student
2. In your home directory, create directories: mydir/subdir1/subdir2
3. Display the permission and ownership information of those directories
4. Change the permission of subdir1 to rwxrwxr—using symbolic mode
5. Change the permission of subdir2 to 777 using octal mode
6. Change the user owner of subdir1 to user root and group owner to group root
7. Could you list the files inside the subdir1? Why?
8. Could you list the files inside the subdir2? Why?
9. You need to ensure that all the new file created on your session will have the permission as rw-rw-r--. Please do the appropriate configuration and create a new file to review the result
10. Create a new file, named it backup.sh. Imagine that the file you created is a backup script. It need super user privilege to run but you have to assign sufficient privileges for user student can run the script. Change the permission of that file to satisfy that requirement.
11. You need to ensure that every file created inside the mydir have the same group owner. How you can do that.
12. Assume that mydir is a share directory and everyone have write permission on it. You must change the permission of that directory to ensure that every file created inside mydir just could be deleted by the user owner only. How you can do that?

Exsercise Instructions

I. Prepare the environment
II. Manage file permission and ownership

1. Login to the CentOS server with the provided username and pasword: **student/lpic1@123**

2. In your home directory, create directories: mydir/subdir1/subdir2
   $ mkdir -p /mydir/subdir1/subdir2

3. Display the permission and ownership information of those directories
   $ ls -ld mydir
   $ ls -l mydir
   $ ls -l mydir/subdir1

4. Change the permission of subdir1 to rwxrwxr—using symbolic mode
   $ chmod ug=rwx,o=r mydir/subdir1

5. Change the permission of subdir2 to 777 using octal mode
   $ chmod 777 mydir/subdir1/subdir2

6. Change the user owner of subdir1 to user root and group owner to group root
   $ chown root mydir/subdir1
   $ chgrp root mydir/subdir1
   Or
   $ chown root:root mydir/subdir1

7. Could you list the files inside the subdir1? Why?
   $ ls mydir/subdir1
   You could list the files existed in subdir1 because you have read permission on it.

8. Could you list the files inside the subdir2? Why?
   You could not list the files inside the subdir2 althought you have sufficient permission on subdir2. The reason is you do not have the execute permission on the subdir1 (subdir2's parent directory)

9. You need to ensure that all the new file created on your session will have the permission as rw-rw-r--. Please do the appropriate configuration and create a new file to review the result
   $ umask 002

10. Create a new file, named it backup.sh. Imagine that the file you created is a backup script. It need super user privilege to run but you have to assign sufficient privileges for user student can run the script. Change the permission of that file to satisfy that requirement.
    $ cd mydir

$ touch backup.sh
$ sudo chown root backup.sh
$ sudo chmod 4755 backup.sh

11. You need to ensure that every file created inside the mydir have the same group owner. How you can do that.
    $ chmod g+s mydir

12. Assume that mydir is a share directory and everyone have write permission on it. You must change the permission of that directory to ensure that every file created inside mydir just could be deleted by the user owner only. How you can do that?
    $ chmod o+s mydir