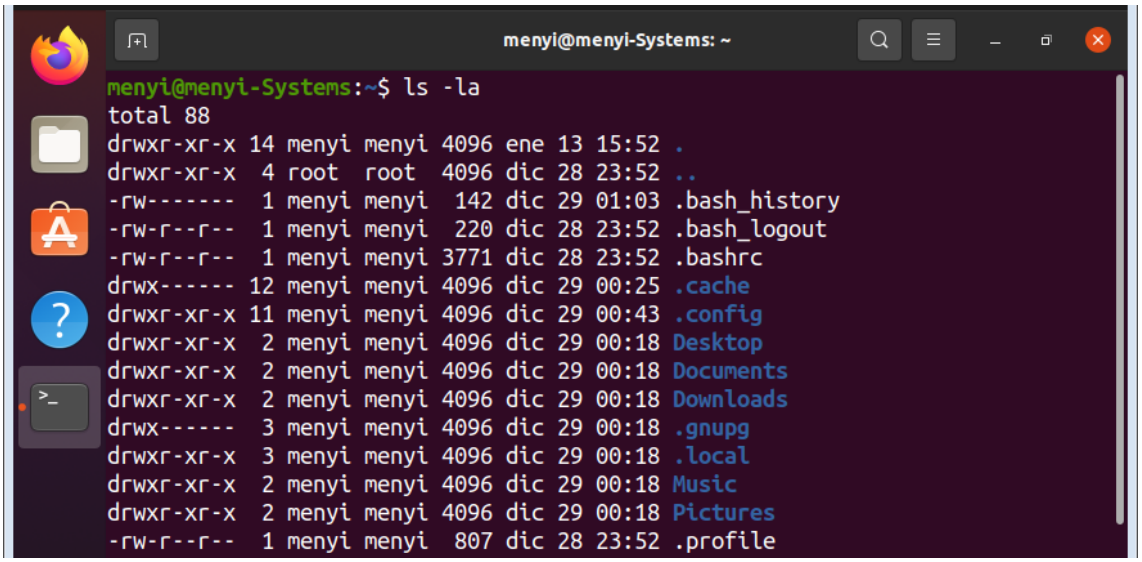
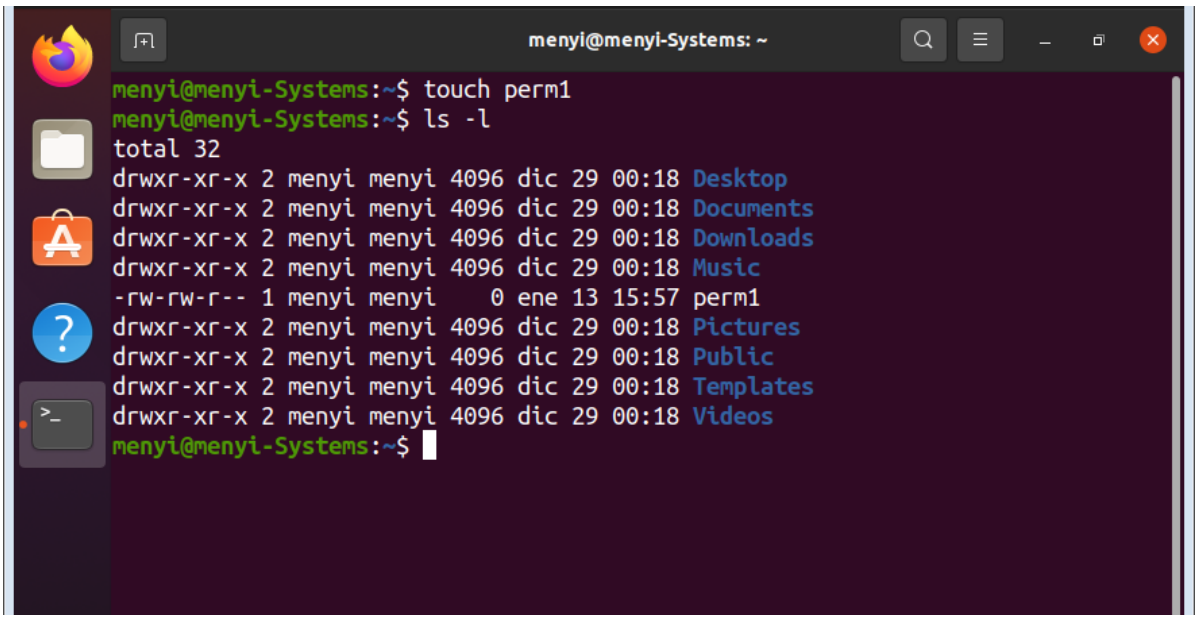
UNIT 03: Linux systems administration # Exercise 07

Part 3# EXERCISES ABOUT FILE AND DIRECTORY PERMISSION

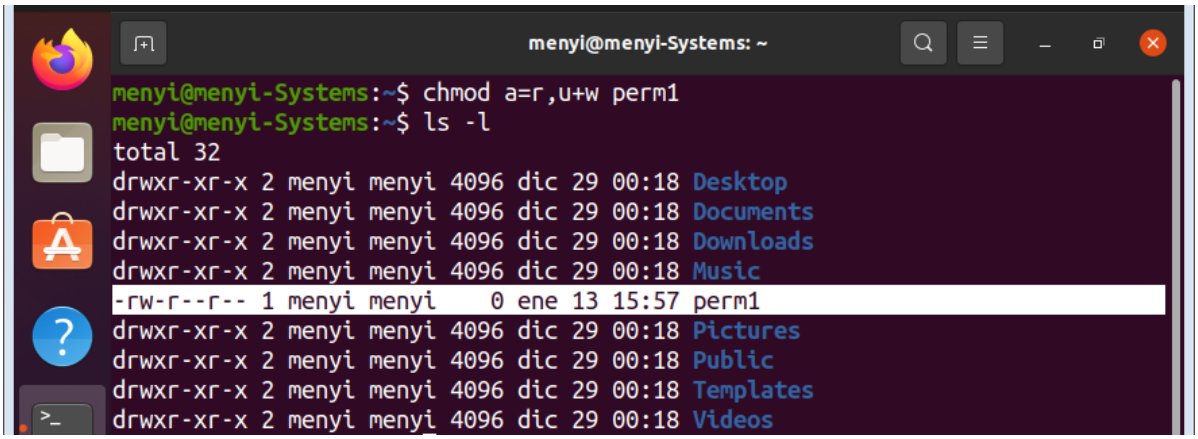
1. List the permissions in your current directory, including hidden files

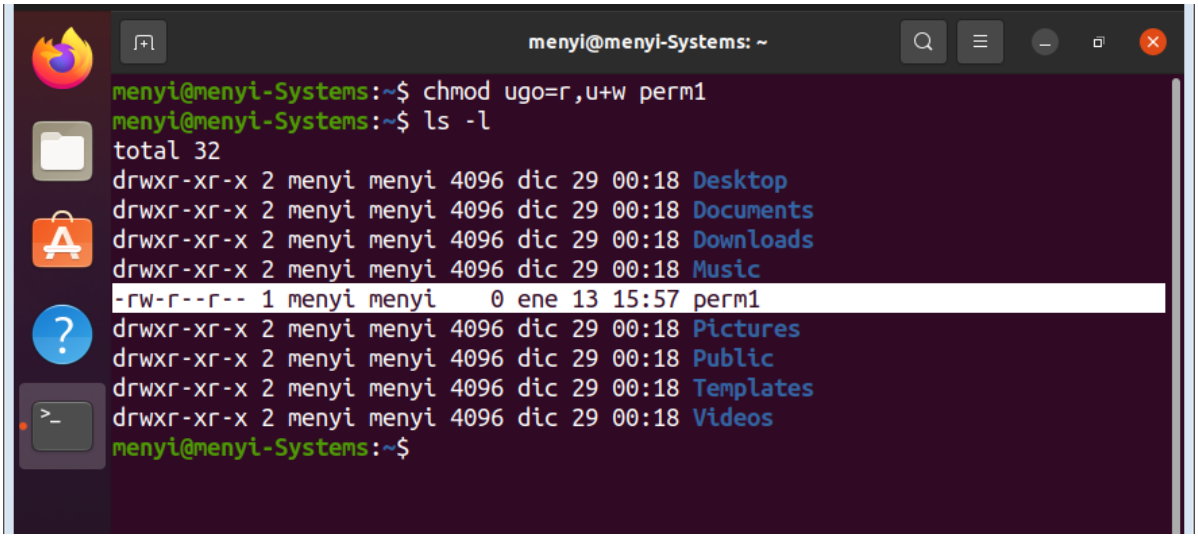


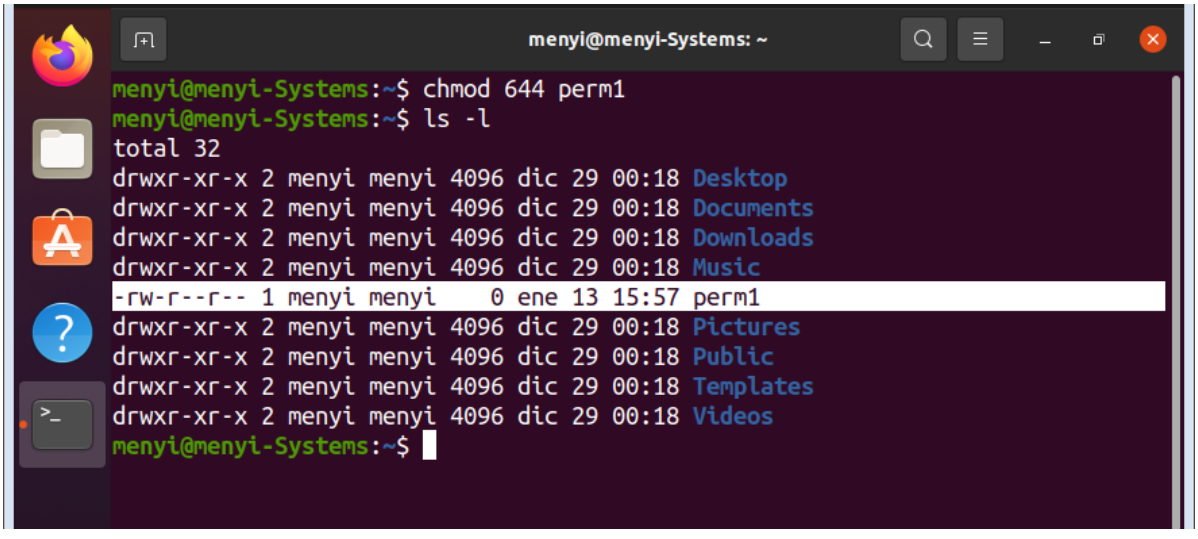
2. Create a file called perm1. Now, check the default permissions and user and group ownership



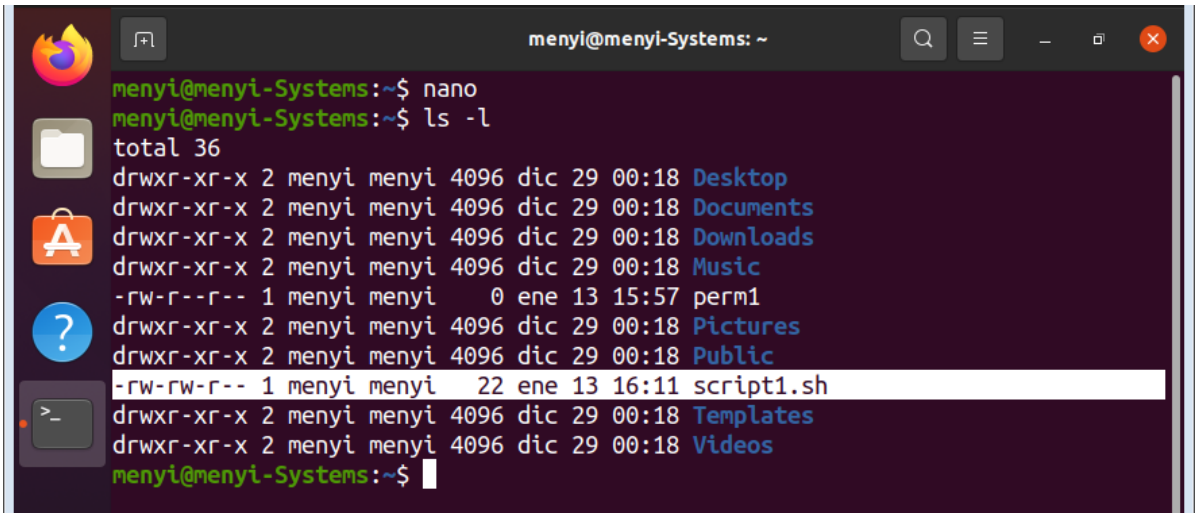
3. Change permissions of perm1 so that everyone can read and only the owner user can write. Specify the command in all possible ways.



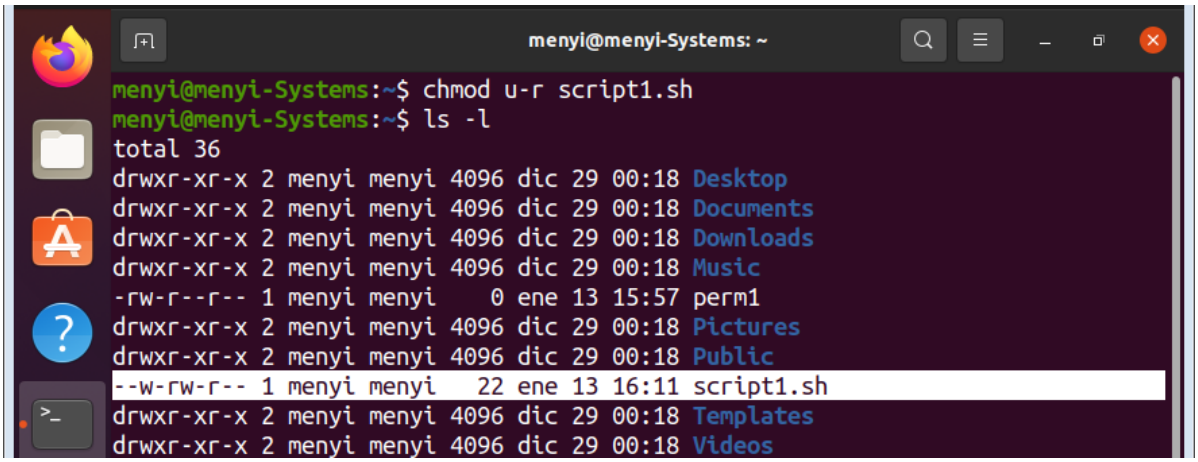


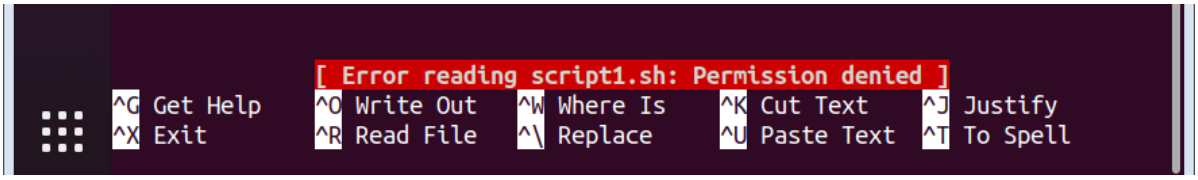


4. Create a file called script1.sh, including the content below. List the default permissions.

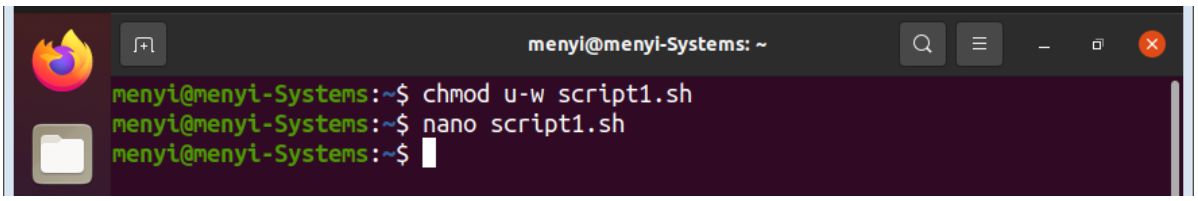


5. Remove the read permission from the owner and try to open the file



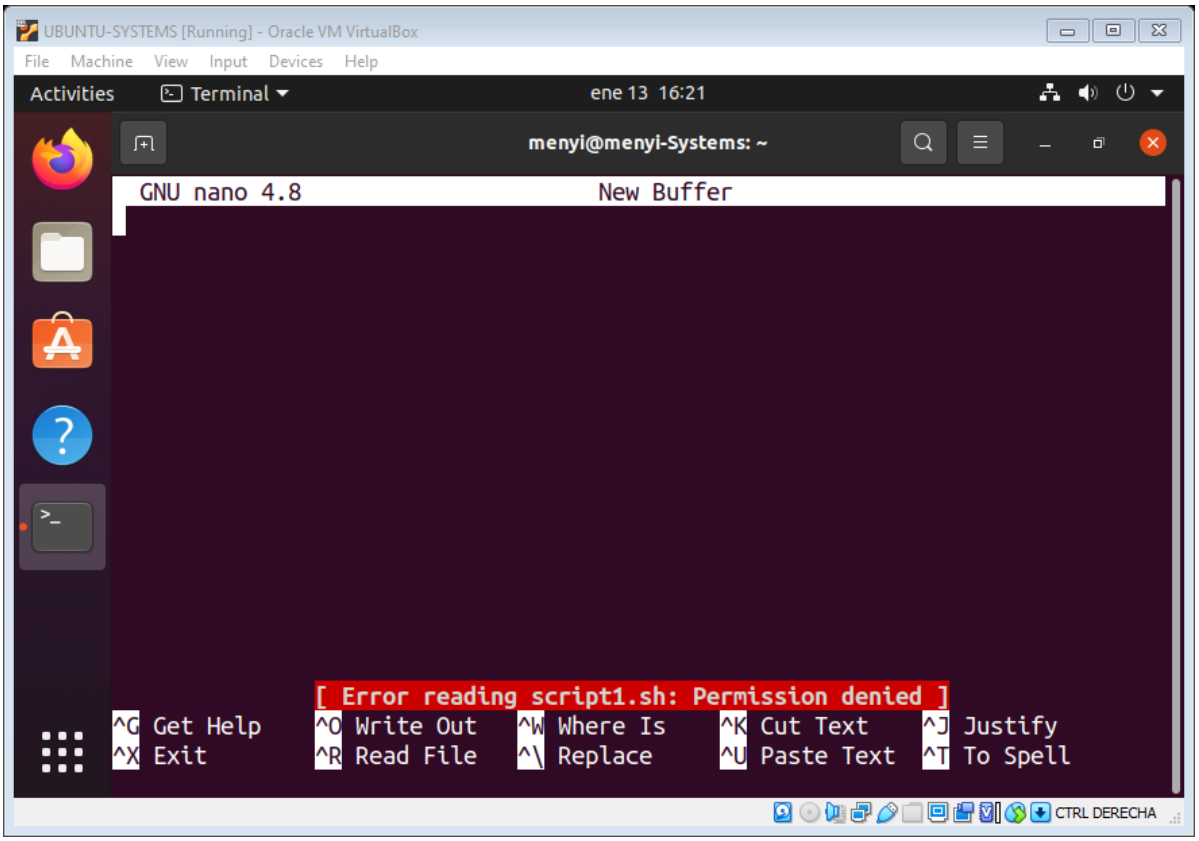


6. Remove the write permission from the owner on the file script1.sh.

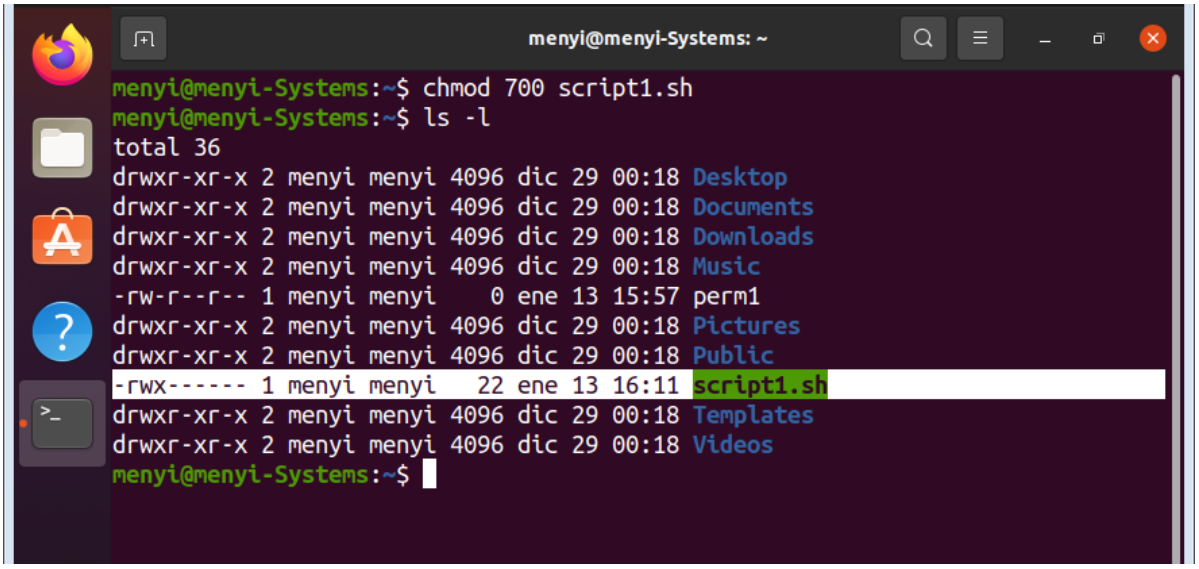


Add the line below. Is it possible? Why?

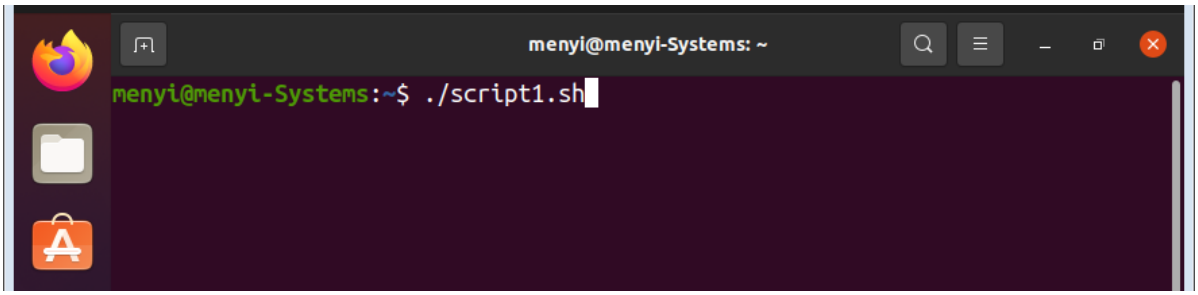
No, because the user doesn´t have permission to read or write.

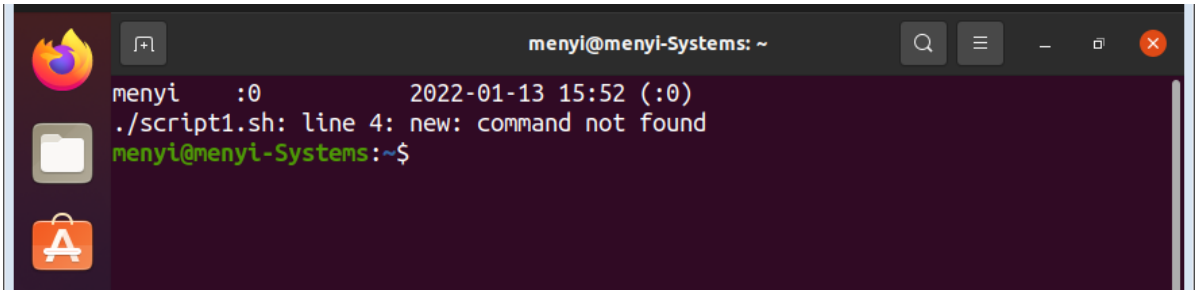


7. Change the permissions on the file script1.sh so that the owner can read, write and execute, but you deny all the permissions from the group and others.

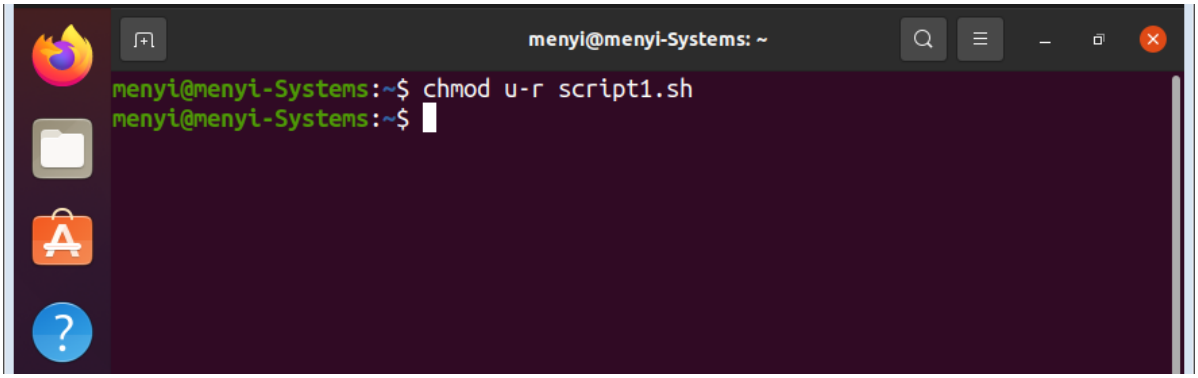


8. Add the line indicated in exercise 6, in case it was not possible.
Try to run the file like a command.

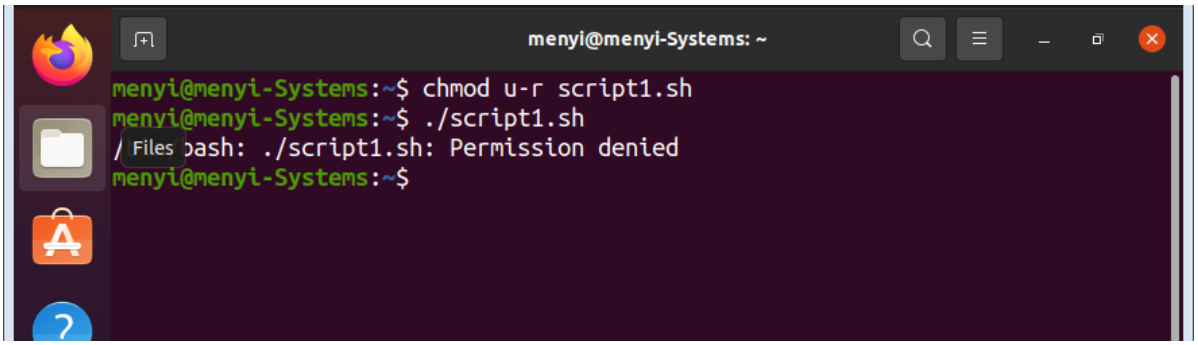




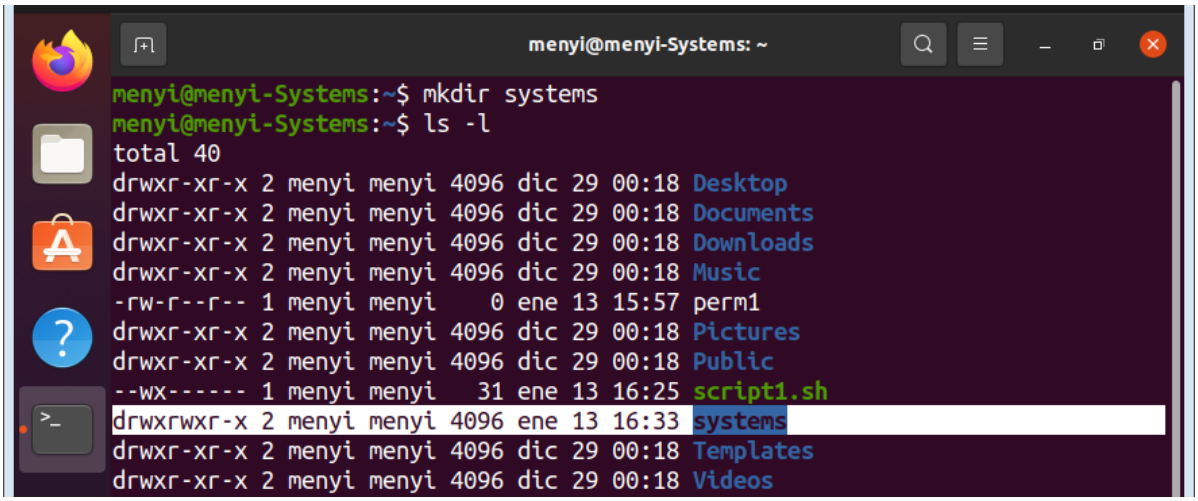
9. Remove the read permission from the owner on the file script1.sh

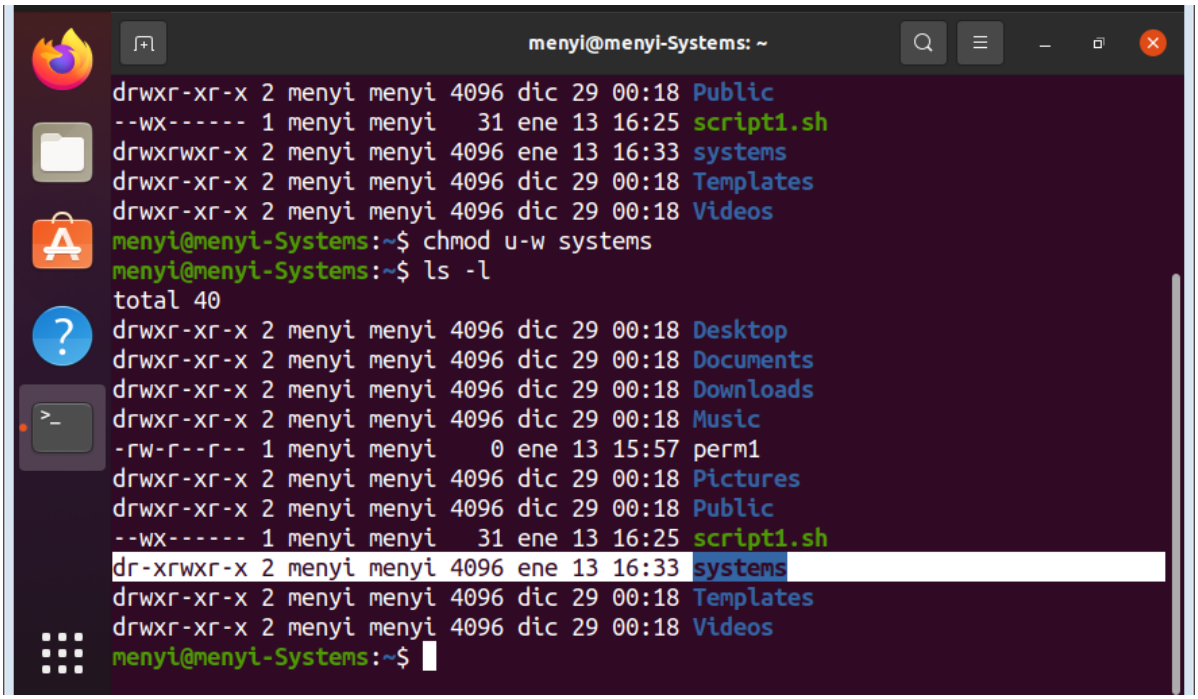


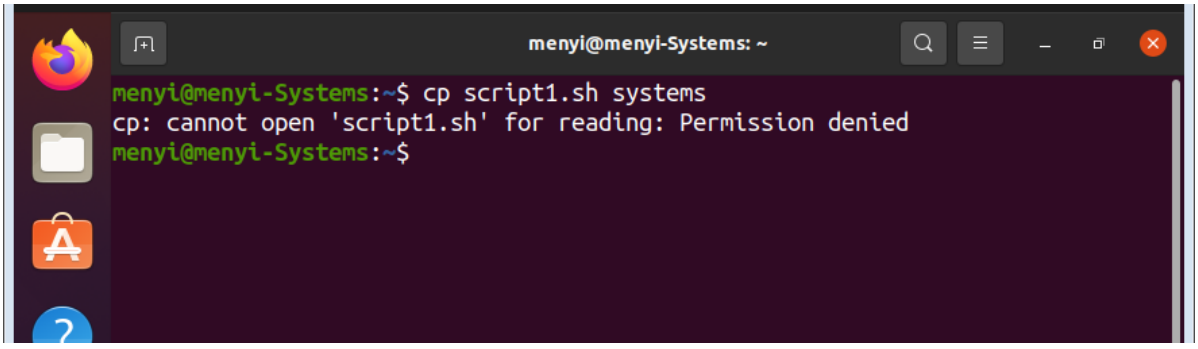
Try to run the file. Is it possible? No, permission denied



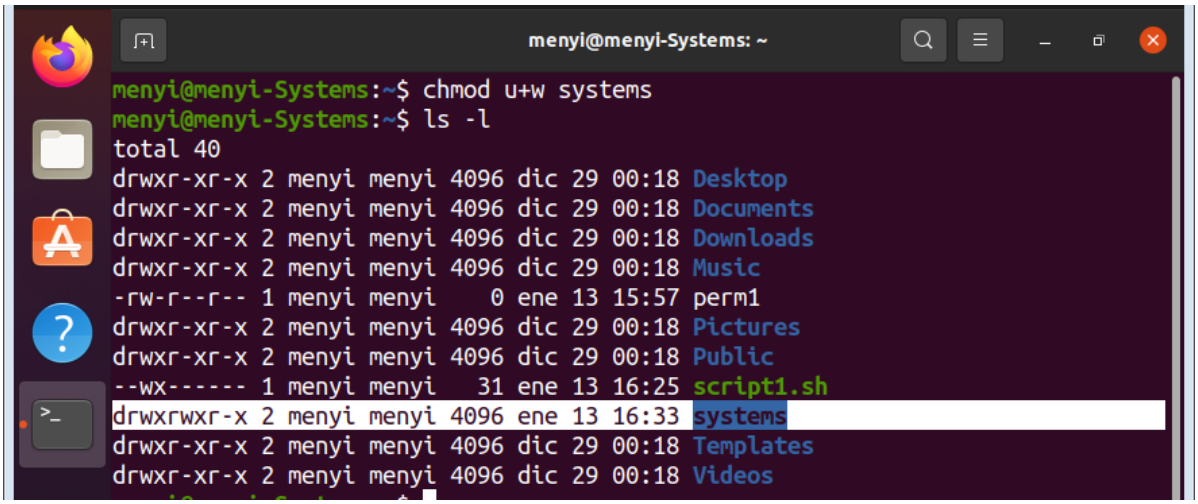
10. Create a directory called “systems”.
Remove the write permission from it and try to copy script1.sh inside.

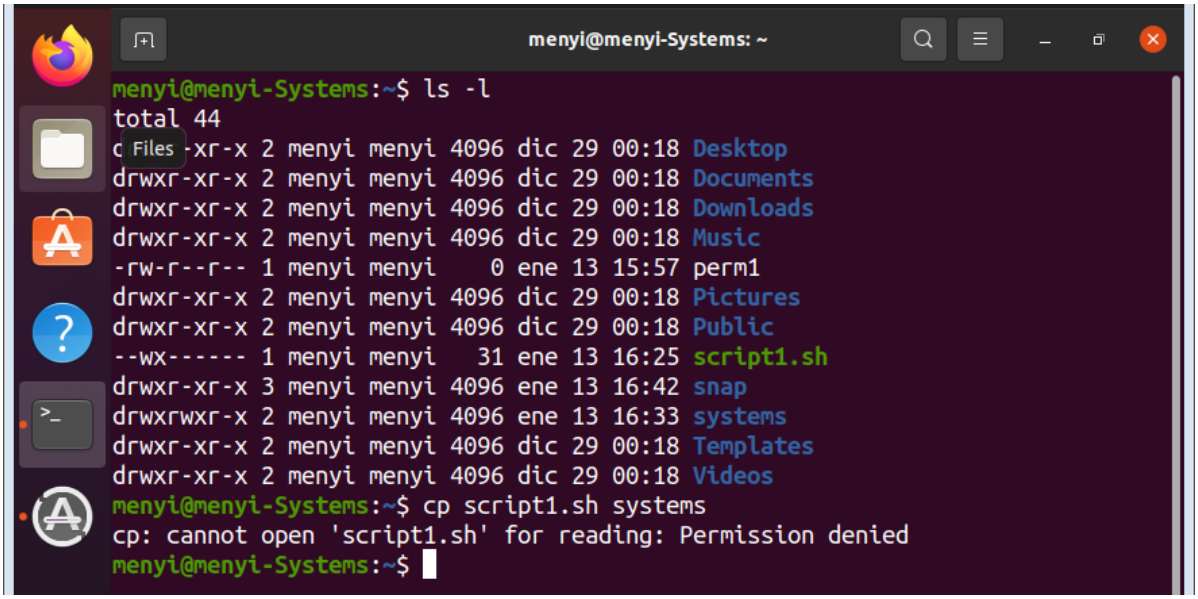


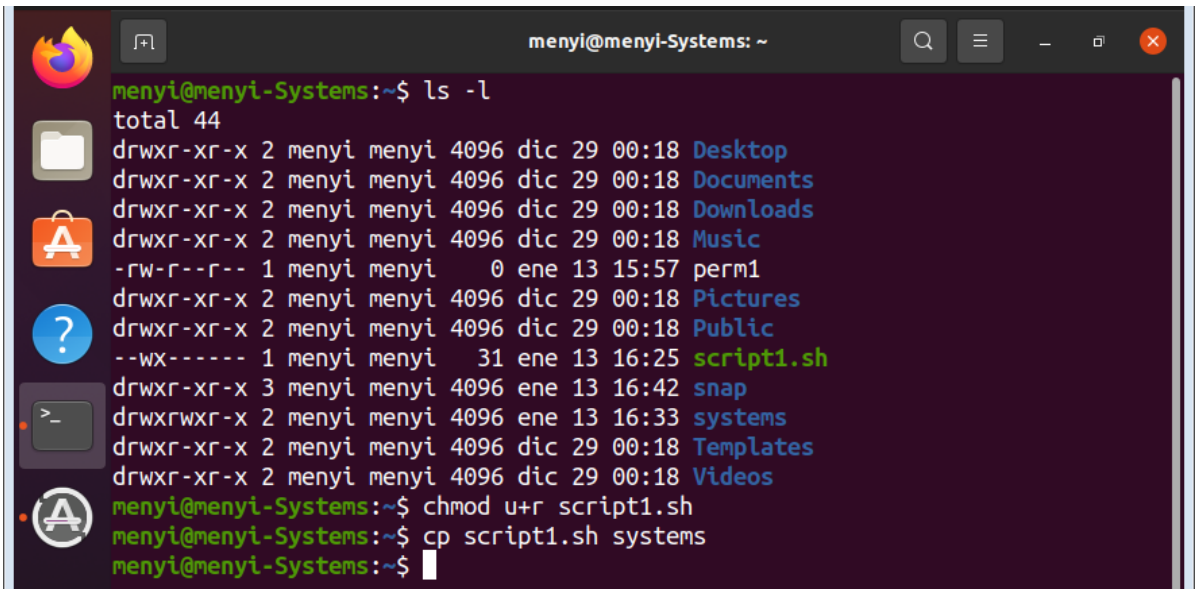


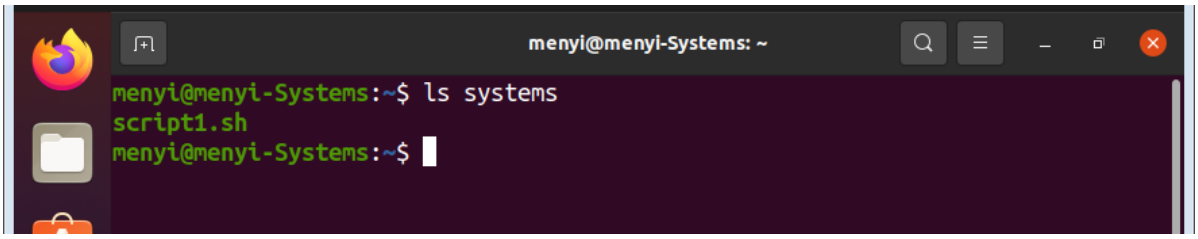


11. If you were not able to copy the file, add the write permission again and copy the file inside

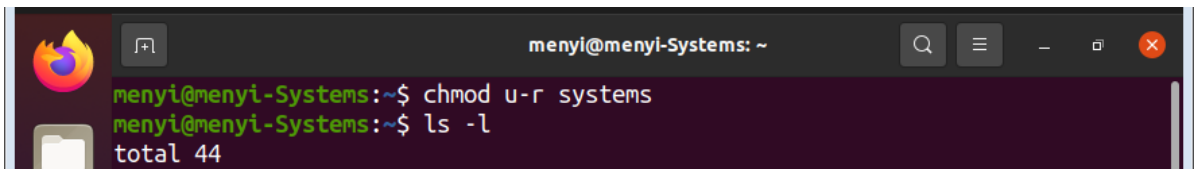


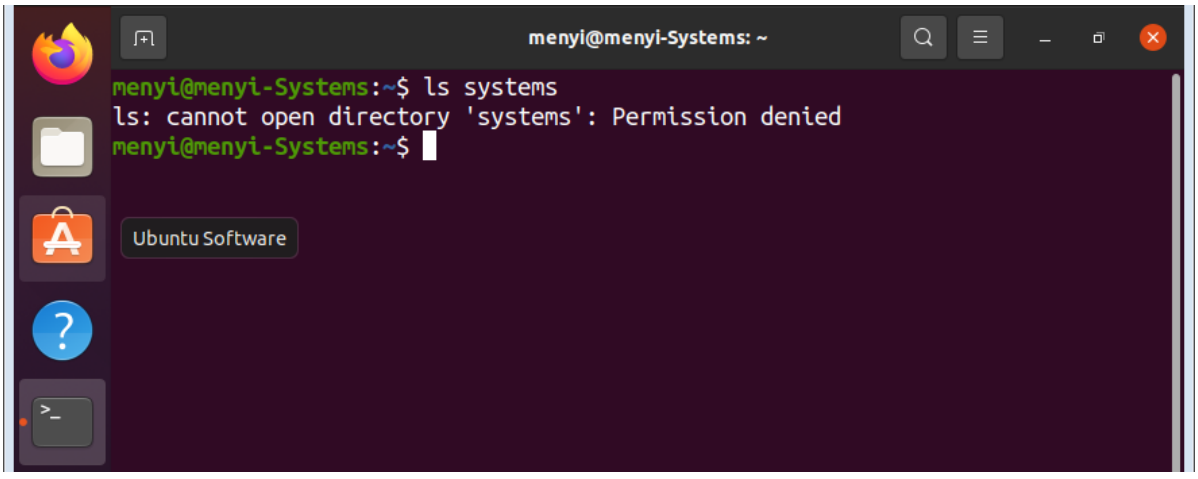




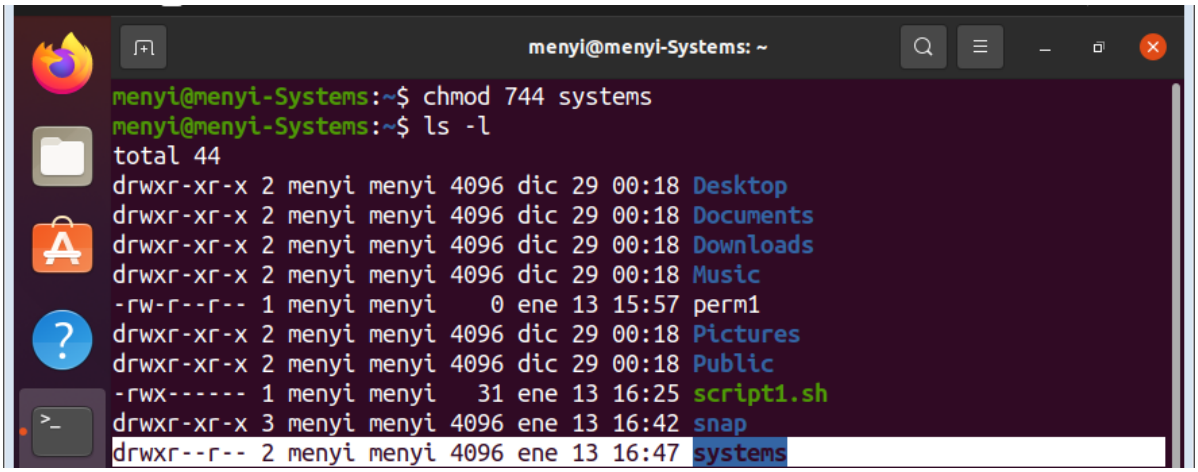


12. Remove the read permission from the user on the directory “systems” and try to list its contents.

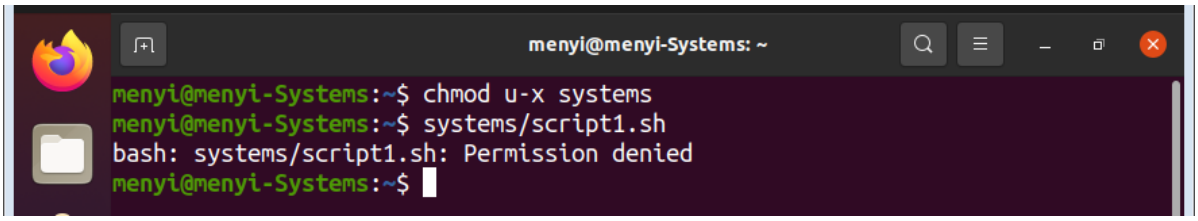




13. Change the permissions from “systems” so that the owner can read, write and execute but the group and others can only read.

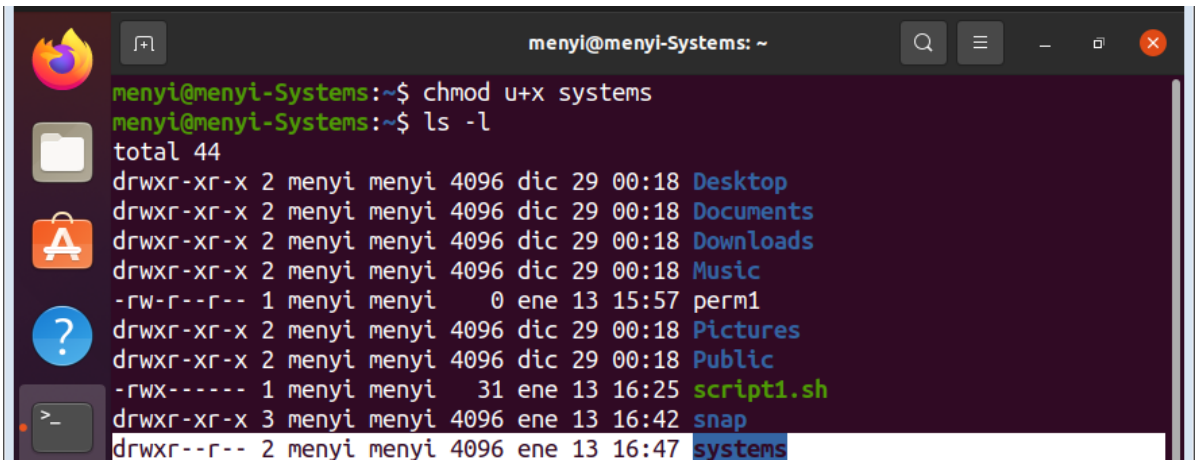


14. Remove the execute permission from “systems”

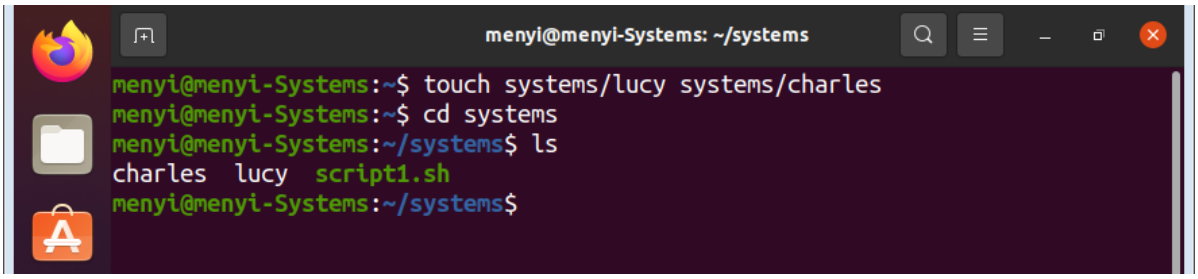


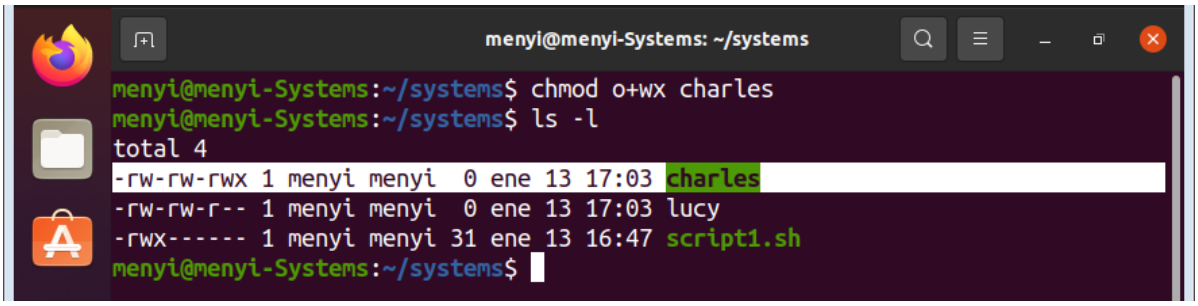
Can you execute systems/script1.sh? Is it possible to access the directory to execute the file?
It is not possible because user doesn’t have execute permission

15. Assign the execute permission to the directory again

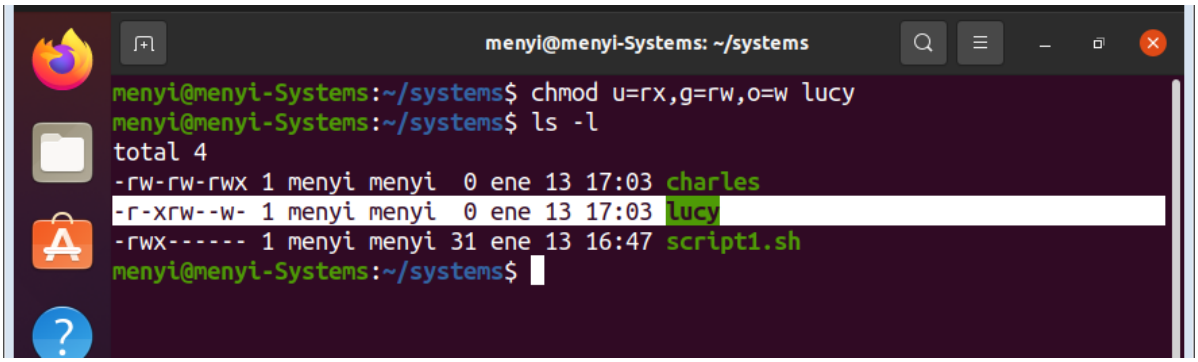


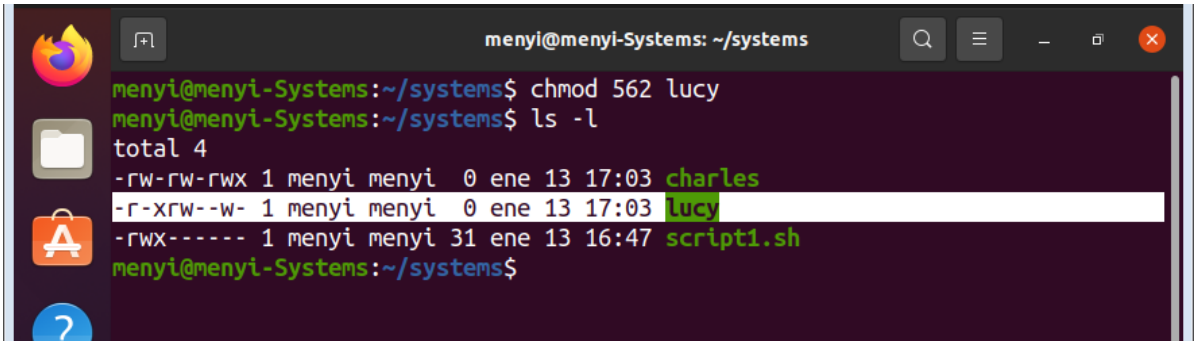
16. Create two files called “lucy” and “charles” into “systems”.
Change permissions of “charles”, so that others can write and execute.



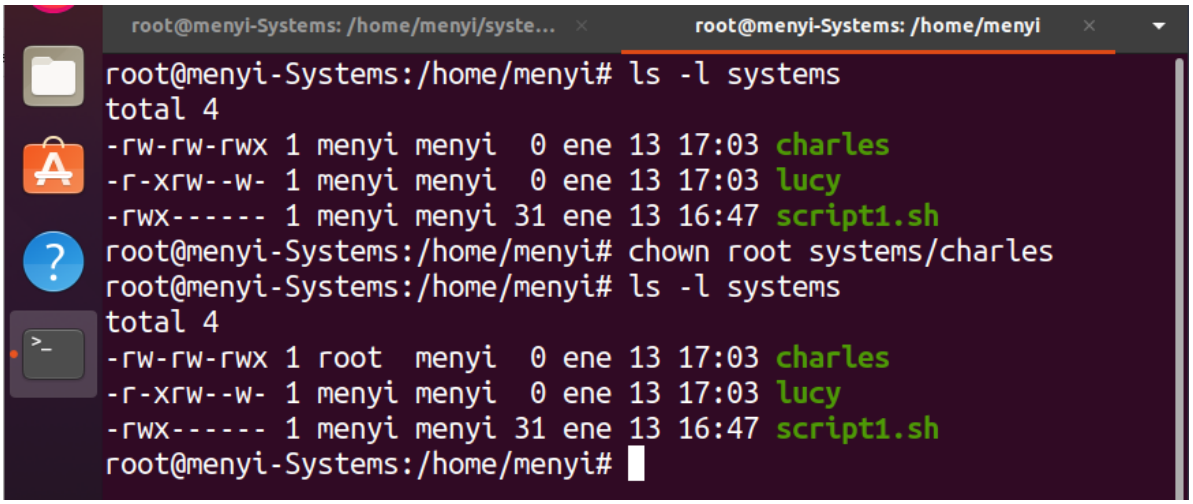


17. Change permissions of “lucy” so that the owner can read and execute, the group can read and write, and others can only write. Specify the command in all possible ways.

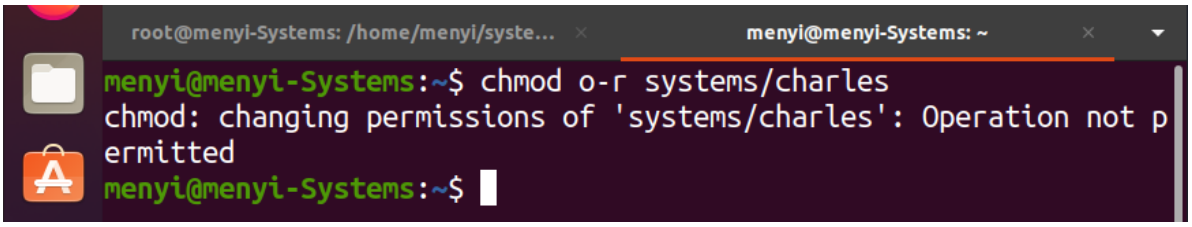




18. Log in as root. Change the ownership of “charles” to “root”.

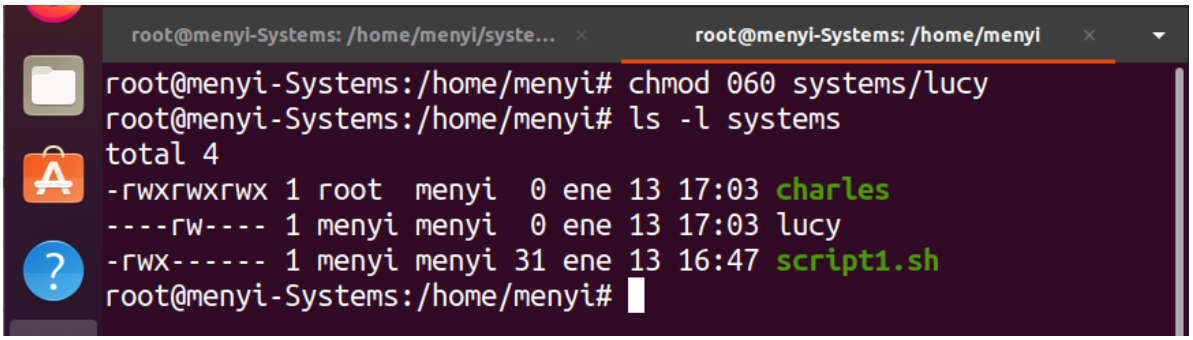


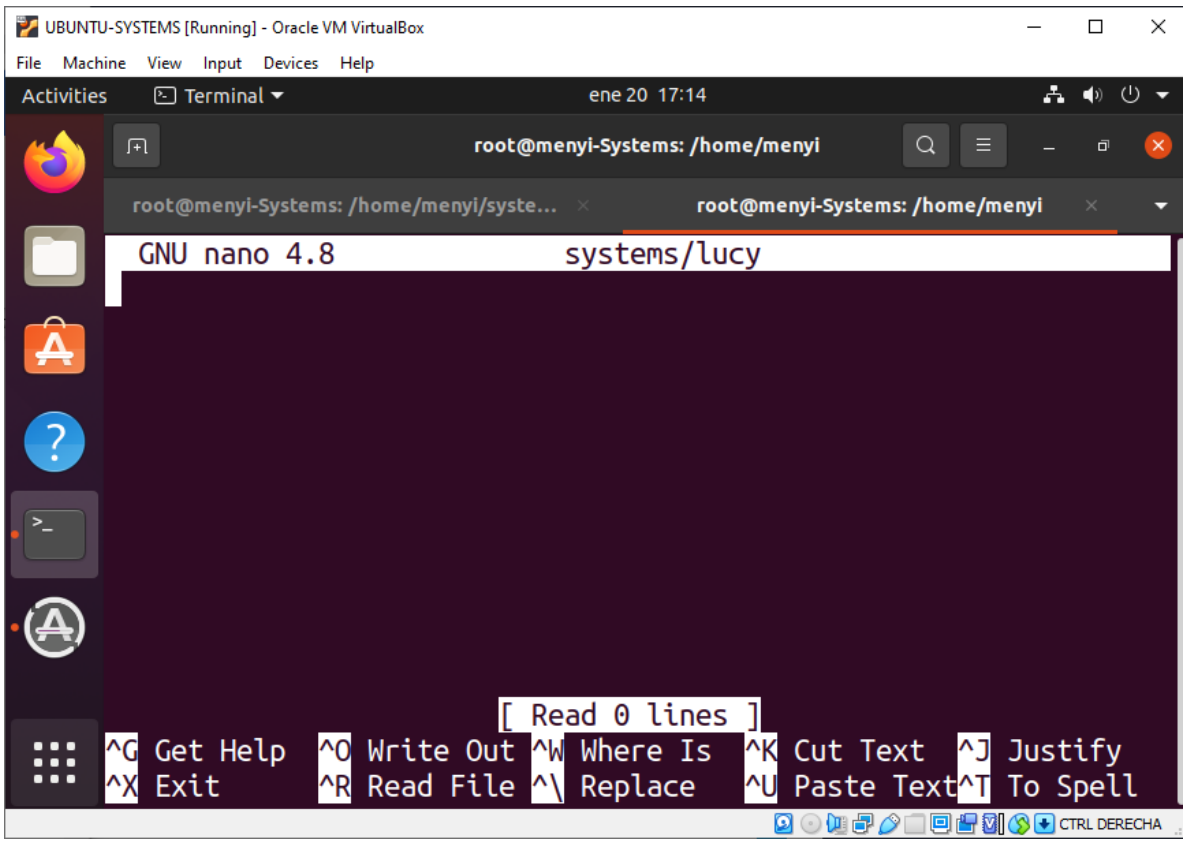
Exit the root session. Now, try to change the permission so that others cannot read and execute. Is it possible? Why? Operation not permitted because we don´t have permission to do so.



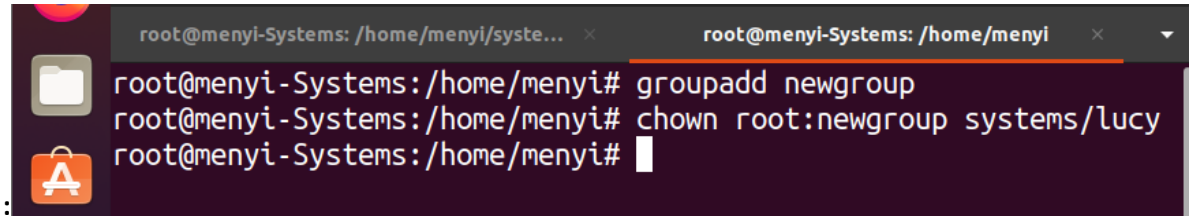
19. Change the permissions of “charles” so that everybody can do everything

20. Change the permissions of "lucy" so that the group can read and write, but the owner and others cannot do anything**. Can you open the file? Yes, because user belongs to the group**



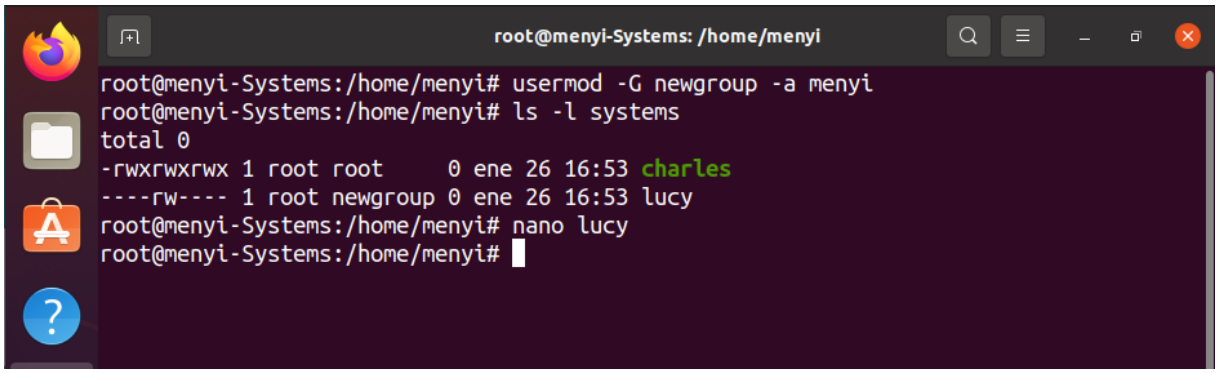


21. Create a group called "newgroup". Set the group as the owner of the file "lucy" and "root" as the owner user.

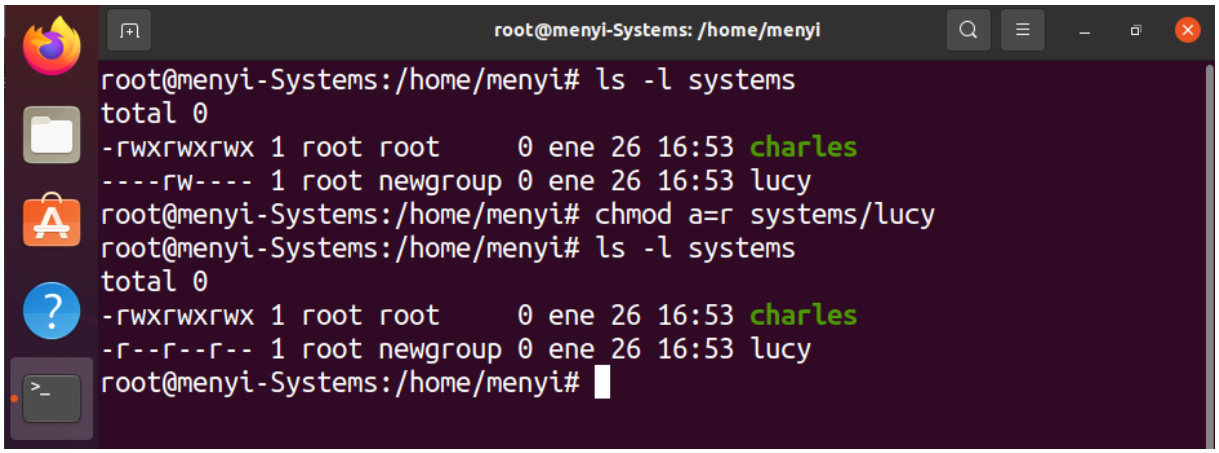


:

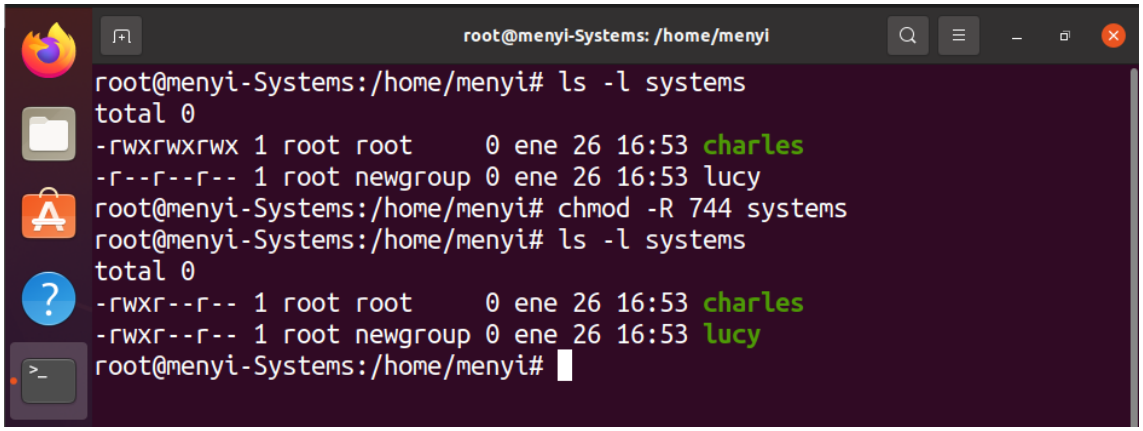
22. Add your user to the secondary group “newgroup”. Try to open the file “lucy” now. **Is it possible? Yes**



23. Change permissions of “lucy” so that everybody can read.



24. Do exercise 13 again, but this time granting permissions to the folder “systems” including files and subfolders



25. Change the group owner of “systems” to “root” including files and subfolders