Day3

Create a new group iot\_team and add your user to it.

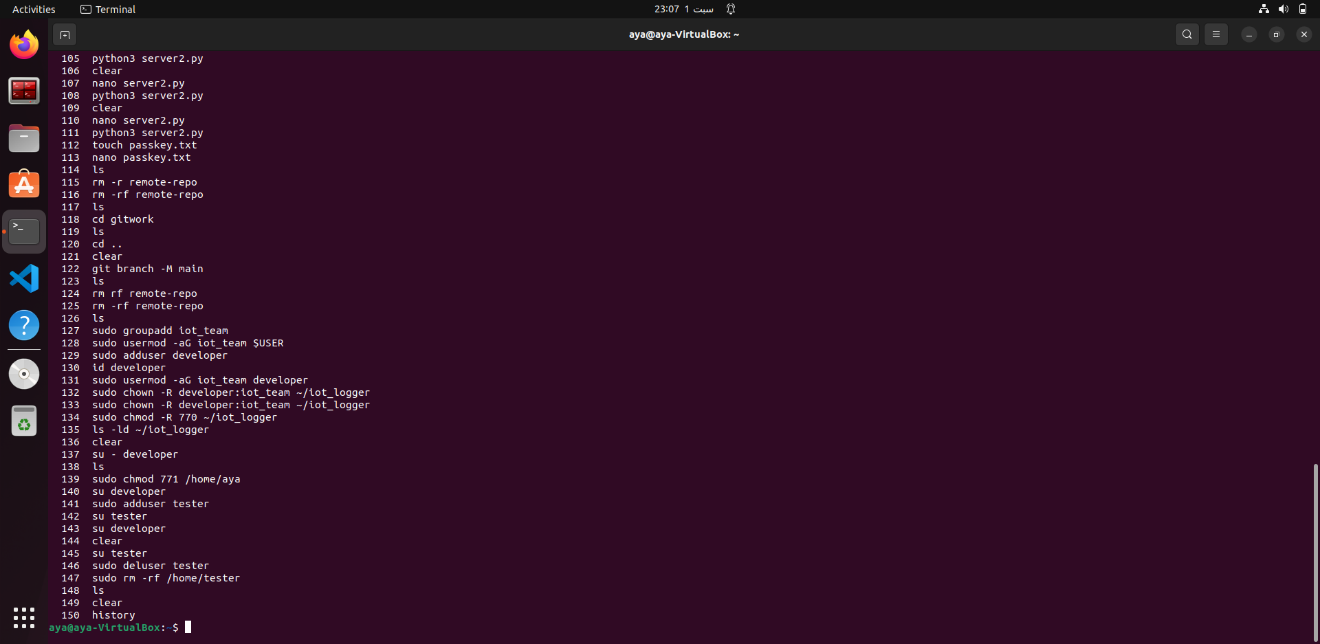
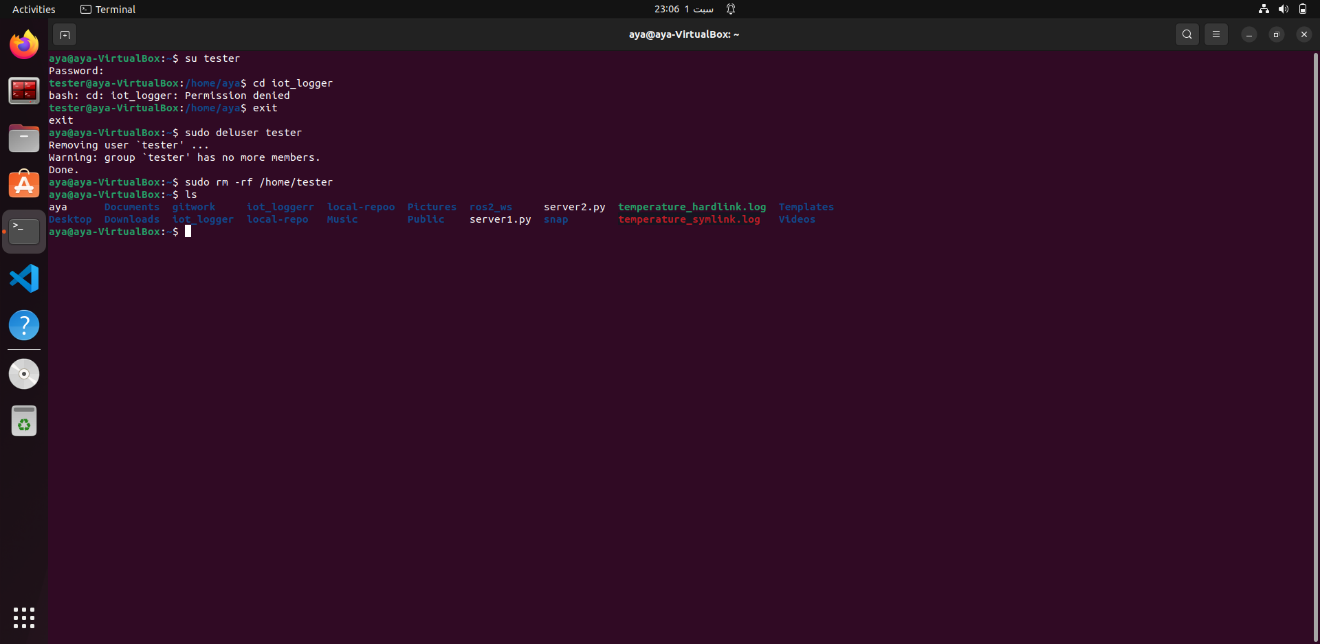
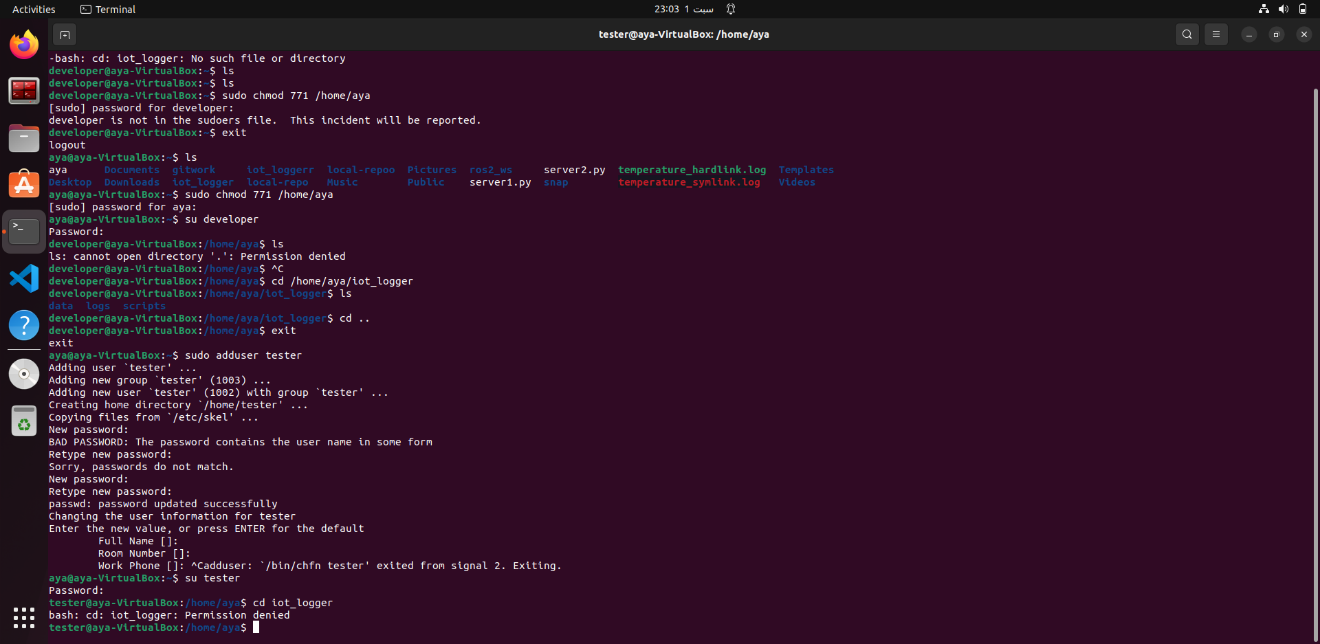
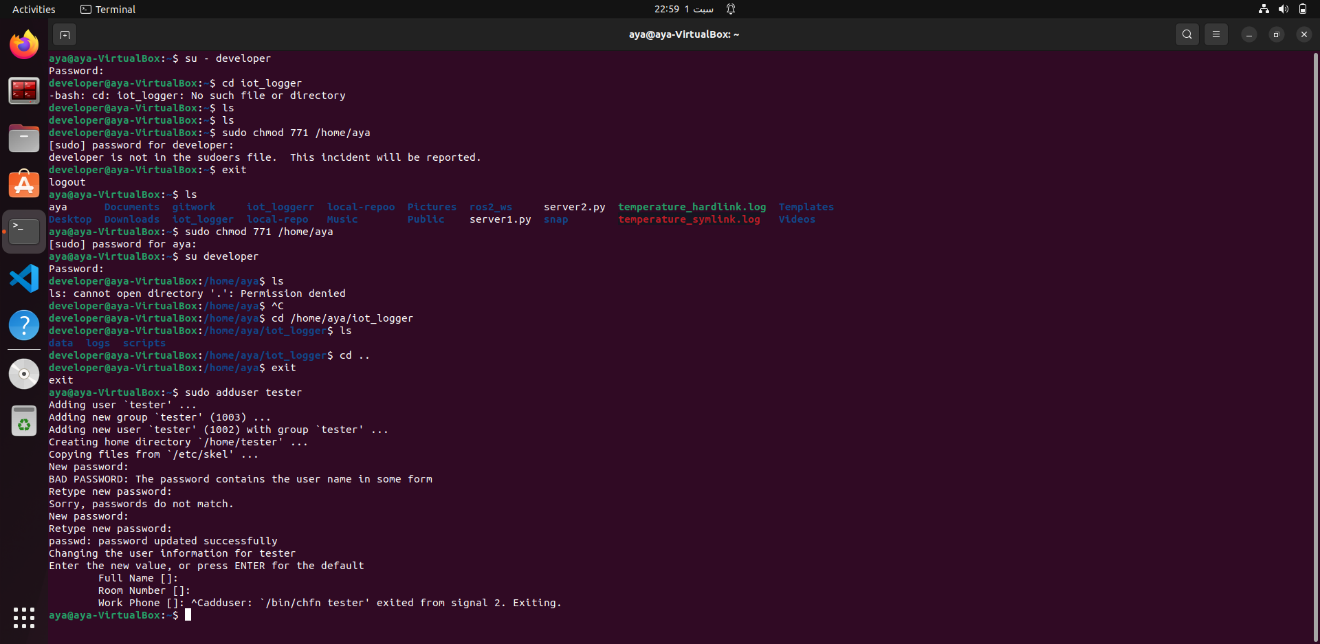
 Create a new developer user, add it to the group.

 Change ownership of iot\_logger to the developer + group.

 Set permissions: group can read/write logs, others blocked.

 Test access as new user, then remove test user.

A screenshot of a computer

AI-generated content may be incorrect.

* **How do Linux file permissions (r, w, x) work for files vs directories? Give an example using ls -l.**

File permissions r, w, and x work differently for files and directories. For files, r read the content, w allows editing or deleting, and x makes the file executable. For directories, r list the names of files inside, w allows creating, renaming, or deleting files, and x enter the directory (cd) and access its contents.So, rwx on a file controls how the user use the file itself, while rwx on a directory controls how to access and manage the files within it.

* **Explain octal notation for permissions and what the umask command does. Give one calculation example.**

Linux permissions use numbers: 4 = read, 2 = write, 1 = execute. Add them up for owner, group, others. Example: rwxr-xr-- = 754.

umask decides what permissions to take away when you create a new file or folder. Example: default folder is 777, if umask is 022 → result is 755.

* **What is the difference between the root user and a normal user? Why is root considered dangerous?**

The root user in Linux is the boss of the system. It can do anything: delete files, install programs, change settings, or manage other users. A normal user can only work with their own files and has limited power.

Root is dangerous because one mistake (like deleting the wrong file) can break the whole system. That’s why the user normally use a normal user, and only switch to root when he really need to.