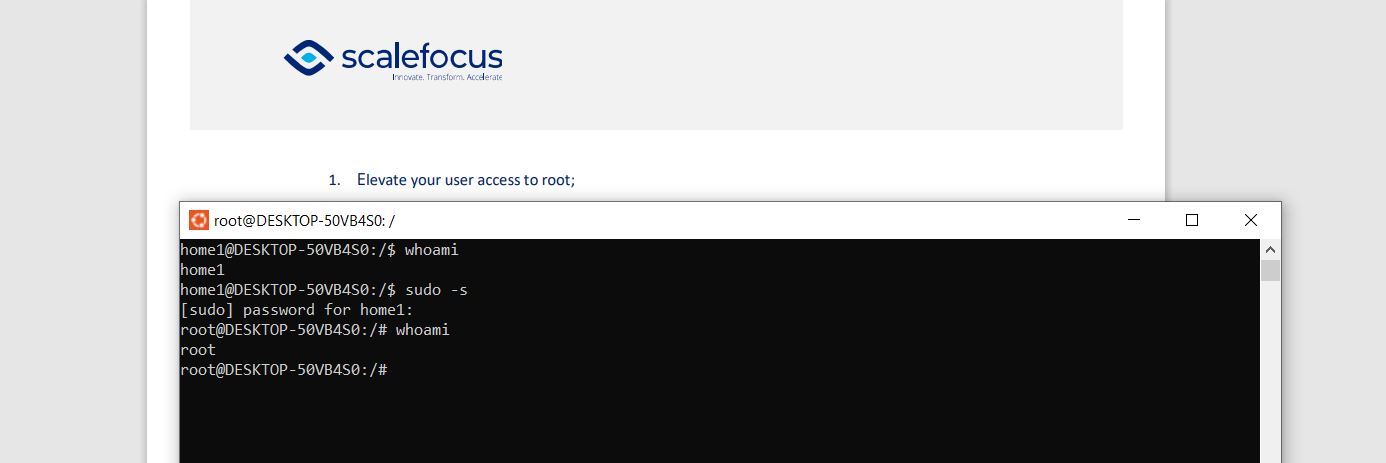
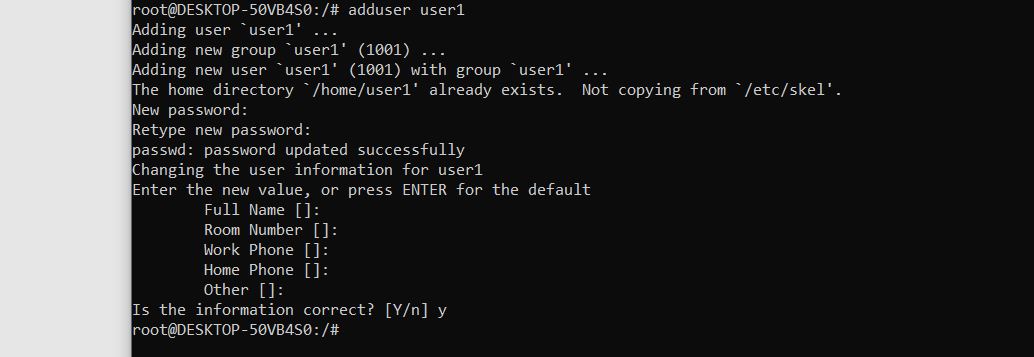
1. Elevate your user access to root.



On Ubuntu Linux root is a particular user account. By default, the root user has access to all commands, files, services on an Ubuntu Linux operating system. It is also known as the root account, root user and the superuser. The superuser or root user has root privileges. It is the most privileged account on Ubuntu with complete access to everything. The MS-Windows equivalent of root is the Administrators group or Administrator user.

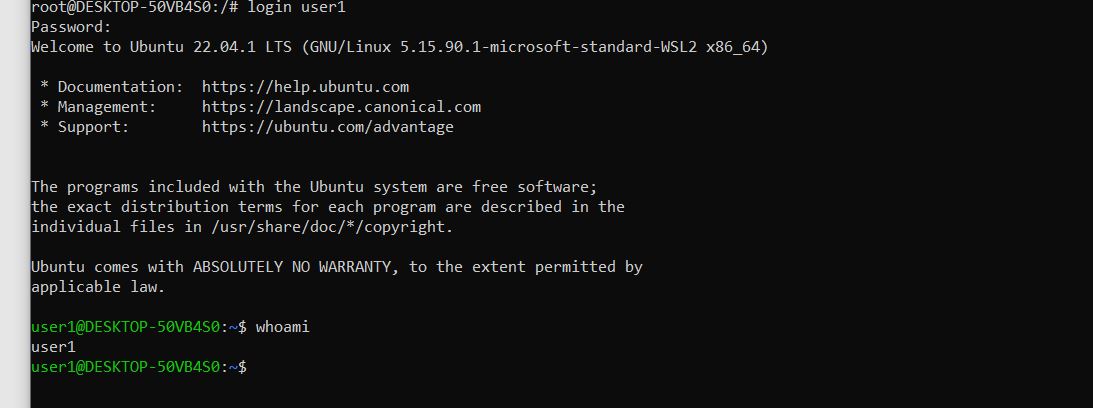
We can use “sudo -s” to login as root user.

1. add a new user to your Linux OS and set a password for it.

****

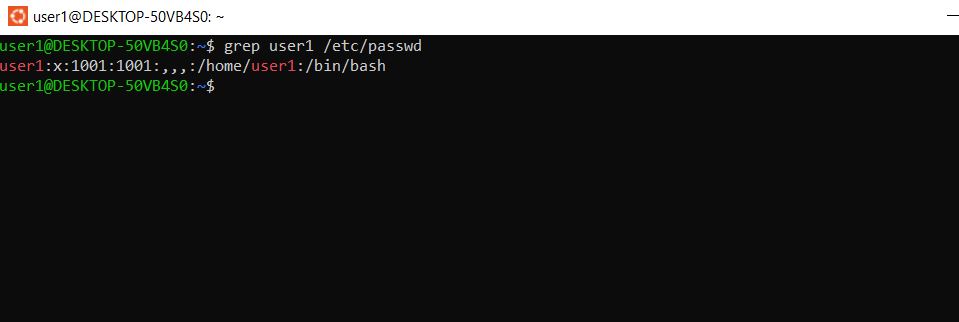
To add user ,we need to use “adduser NAME” command and enter password for the new user.

1. Test if you can log in using that user



To login with another user ,we will use “login USERNAME” command , than type the correct password and we are logged with user1.

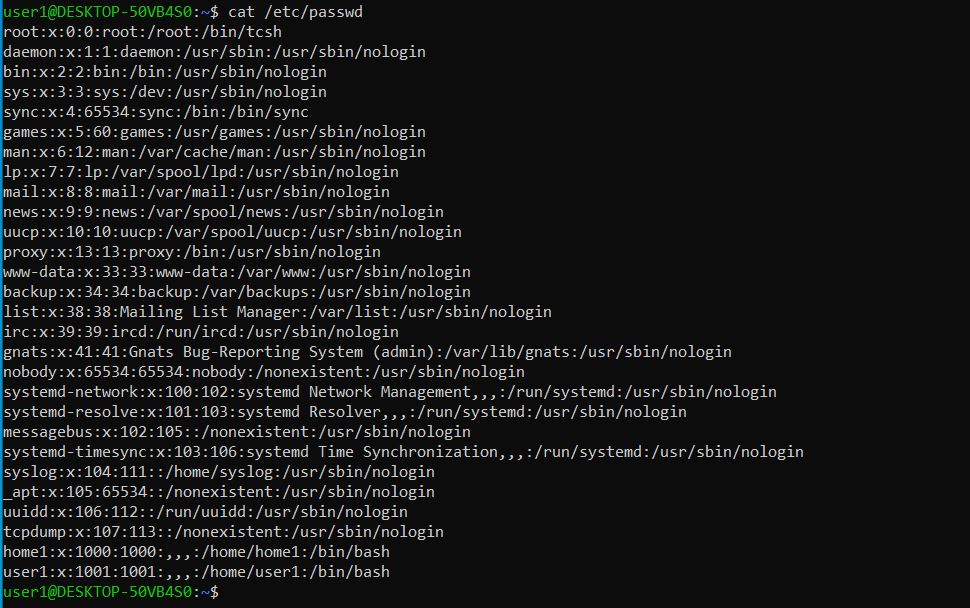
1. Using grep command check if the user is created.



"grep user1 /etc/passwd"(Using grep command we can check if the user is created)

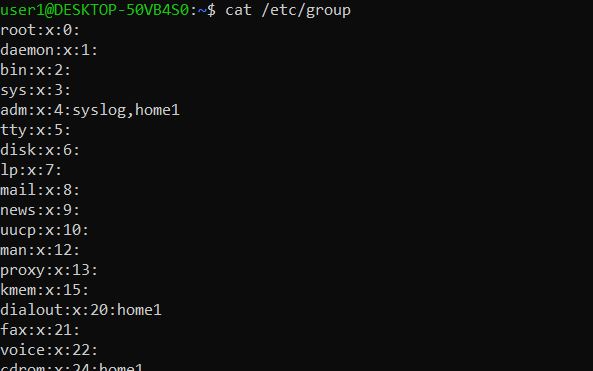
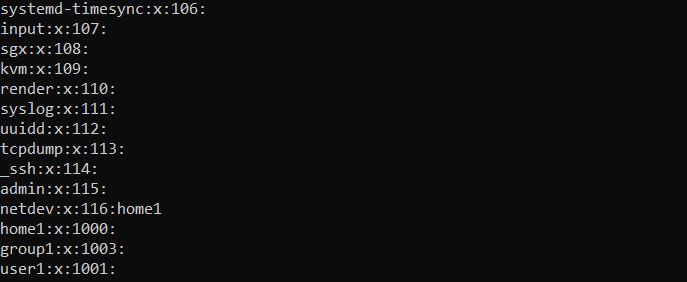
5. grep the UID of each user.

The User ID or UID in Linux is a unique entity through which a user is identified on a system. Every user on a Linux system has a dedicated UID. You can use ‘’cat /etc/passwd’’ command to find the UID of all users.



6. Find out the GID of the created user

Groups in Linux are defined by GIDs (group IDs). Just like with UIDs, the first 100 GIDs are usually reserved for system use. The GID of 0 corresponds to the root group and the GID of 100 usually represents the users group. GIDs are stored in the /etc/groups file:



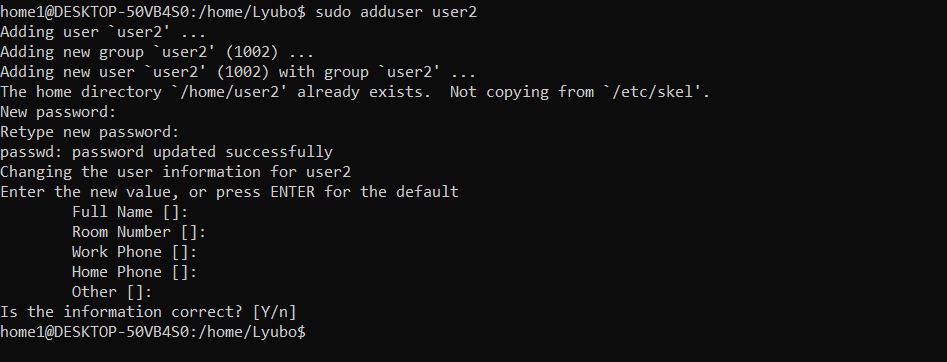
7. Change the password of the user and force it to change the pass on his next login.

We can change the password with the “passwd” command, the terminal is going to ask you to enter current password, than to enter new password and retype it again.



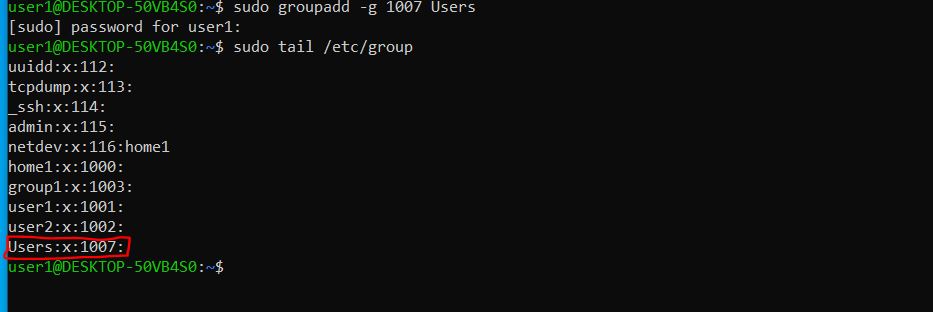
8. Add a new user and set an expiration date for it, with a five-day warning period.

We are using the “adduser” command to create a user, but we need to add expiration date with “-e YYYY-MM-DD username ”.



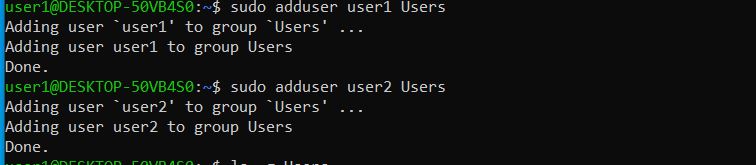
9. Create a new group

We will use “addgroup -g Group\_ID Group\_Name” command to create a group and group ID number. The -g parameter indicates that a group number will follow. This is the group number that will be assigned to this new group. The group number must be unique. “Group\_Name” is the name of the group you would like to add. Group names should be entered in lowercase and may contain underscores. It is recommended that you do not use the same group name more than once.



10. Assign the two new users to that group.

We can assign the users to the group with “sudo adduser USERNAME GROUPNAME ”command.



11. Lock one of the user accounts.

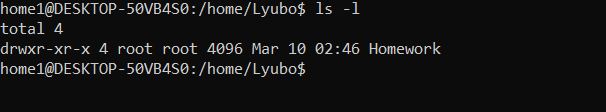
12. Change the shell of one user to tcsh.

First we need to see which script we are with “echo $0”command.

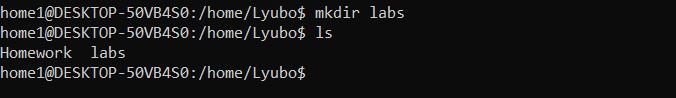
Than we need to login into the wanted user and than we use “chsh -s ”command.

13. Make sure your home directory has “execute” access enabled for group and other.

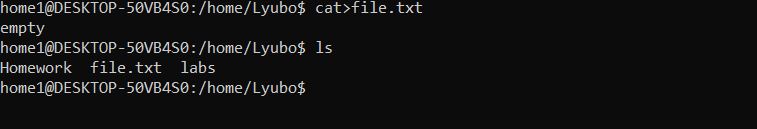
The ls -l command displays directory contents in long format. The long format contains both permissions and ownership. You can see that the user account that created the resources also owns those resources. The group association is also that user's primary group.



14. Change to your home directory, and create a directory called labs.



15. Create an empty file in labs directory.



16. Change permissions of file to rwx-rwx-rwx.

17. List the file. What color is the file?

To change directory permissions in Linux, use the following:

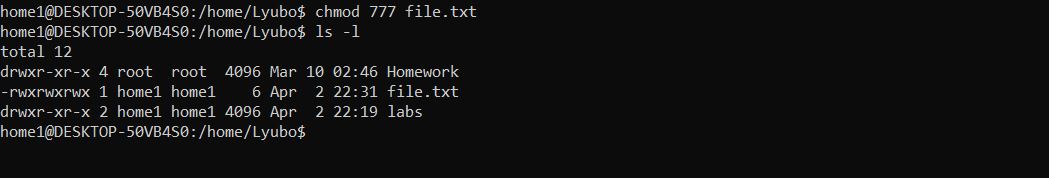
chmod +rwx filename to add permissions

chmod -rwx directoryname to remove permissions.

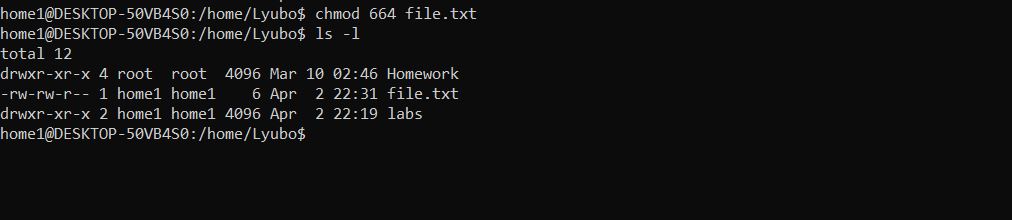
chmod +x filename to allow executable permissions.

chmod -wx filename to take out write and executable permissions.

Note that “r” is for read, “w” is for write, and “x” is for execute.



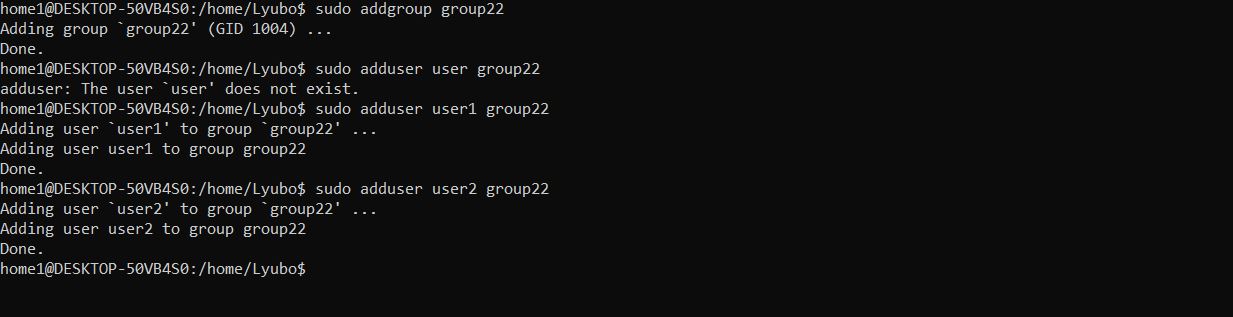
18. Change the permissions back to rx-rw-rw19. Check what owners does the file have.



20. Change the user ownership of the file to another user.

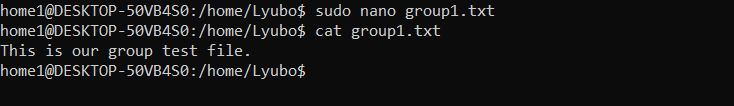


21. Create a group called group1 and assign two users to the group.

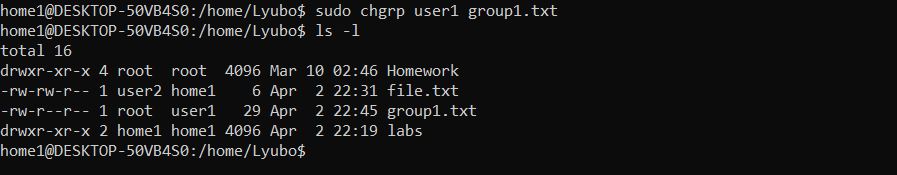


22. Create a file called group1.txt and redirect below input into the file:

“This is our group test file”.



23. Change the group of the file to one of your users.



24. Give members of the group group1 read/write access to this file?

