The system provides rights and permissions to the superuser which is present in each operating system. For Linux, the superuser is "Root". It has the highest privileges as compared with other users. The root can do so many things that normal users can not do like installation, assigning permissions and managing other user's accounts. If you have logged in from any ordinary user and trying to do some activity that is not permitted to you, the system will give the message 'permission denied'. The solution to avoid such problems is to use the word 'sudo' before an actual command. Like, sudo yum install httpd.

If you want to add a new user whose name is sana, put a command " useradd sana". Every user has its own and unique password, to assign a password, put a command "passwd sana". Don't forget to put the name of the user to whom you want to assign a password after a passwd command otherwise system will take it as the user is changing the password of the root user.

As soon as root adds a new user, the system assigns UID (User identifier) number to the user, creates a directory inside the home directory whose name is as same as newly added user name (/home/sana), and assigns default shell i.e. /bin/bash. Shell is an interface between the user and the Linux system. It takes input from the user and executes the program depending on the input.

Linux stores all the user details in /etc/passwd file. To view the content of that file, put a command "cat /etc/passwd". The cat command is used to display the content of a particular file mention in command. The content of /etc/passwd file for user sana looks like:

sana:x:1001:1001::/home/sana:/bin/bash

Each and every field of syntax is separated by colons(:). here is the description of each field:
The **first field** indicates the user name.

Mostly, the **second field** is set to x and it indicates that shadow passwords are in use. You can see * or ! signs also. the asterisk sign (*) is to indicate that the user has no password configured and exclamation mark (!) indicates the user account is locked.

The **third field** indicates UID which is a unique identification number of each user. You can change this ID by using the command "usermod -u <new UID> <username>".

The **next field** shows GID which is a group identifier and this is the primary group identifier.

The **fifth field** is empty here but it is reserved for comment about the user.

The **next field** shows the path of the default home directory.

And the **last field** shows the default shell of the user.

In Linux, encrypted password data gets stored in /etc/shadow file. As like passwd file, shadow file also has different fields.
The **first field** shows the username.

The **second field** is the encrypted password of the user. If the password is not set then this field shows two exclamation marks (!!).

The **next field** shows the days of the last changed password from January 1, 1970.

The **fourth field** shows a minimum number of days left to change the password, if it showing 0 (Zero) it means the user can change the password anytime.

The **fifth field** indicates the maximum number of days the password is valid after that user has to change the password forcefully.

The **next field** is the warning field, it shows after how many days the user will get the warning to change password.

The **seventh field** indicates how many days are remaining to inactive the user's account.

The **last field** shows the expiry date of login, after that login may no longer be used.
For user sana content will look like

sana:$2gfhvhfdfjh8$7f8kdvb@y*t&#4:13064:0:99999:7:::

/etc/shadow file can be only accessible from root user only, a normal user can not access this file.

To remove or delete a user put a command "userdel <username>"