* Users and Groups :

1st User	2nd User
Rizon	Tasa

Rizon can't access tasa user.

Rizon ⇒ UID
↓
Username

* Linux system uses the UID the user ID, to identifying a user.

* Groups :

The system also use groups to manage the permission and this groups are simply just a set of users with similar permissions.

Web developers	Devops	DBMS
↓	↓	↓
3	2	1 → people

You can create certain groups for this users and grant these groups some permissions which would also applicable to the specific users of that groups so that where groups come handy to catergorize different people into different categories.

So different groups has different GID, unlike UID

So different groups has different GID, where GID

↳ Group ID

* Root User / Superuser :

  * The most powerful user in the system.
  * It can access any file in the system
  * It can also start and terminate any process in the entire system.

```
rizon@rizon:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

You cannot access everything e.g. ↑ for that we have sudo.

* Sudo :

  * Superuser do

```
rizon@rizon:~$ sudo cat /etc/shadow
[sudo] password for rizon:
root:!:19128:0:99999:7:::
daemon:*:19101:0:99999:7:::
bin:*:19101:0:99999:7:::
sys:*:19101:0:99999:7:::
sync:*:19101:0:99999:7:::
games:*:19101:0:99999:7:::
man:*:19101:0:99999:7:::
lp:*:19101:0:99999:7:::
mail:*:19101:0:99999:7:::
```

Now you can access it.

But it's not good pratice to always use Sudo command, as you might end up deleting some file and ultimate system crash.

* Sudo su : It make root user of my system inside the home directory

```
rizon@rizon:~$ sudo su
[sudo] password for rizon:
root@rizon:/home/rizon#
```

→ To go out from this type 'exit'.

* /etc/sudoers : controls who can run what commands as what users on what machine and can also control special things such as whether you need a password for particular commands.

* sudo cat /etc/passwd : You can see lot of users here.

```
rizon@rizon:~$ sudo cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin
/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin
/nologin
```

root : x : 0 : 0 : root : /root : /bin/bash

① ② ③ ④ ⑤ ⑥ ⑦

① → username

② → password (stored in file called shadow)

③ → UserID

④ → groupID

⑤ → comment about the user/ user info

⑥ → Home directory

⑦ → User Shell

* /etc/shadow :

```
rizon@rizon:~$ sudo cat /etc/shadow
root:!:19128:0:99999:7:::
daemon:*:19101:0:99999:7:::
bin:*:19101:0:99999:7:::
sys:*:19101:0:99999:7:::
sync:*:19101:0:99999:7:::
games:*:19101:0:99999:7:::
man:*:19101:0:99999:7:::
lp:*:19101:0:99999:7:::
mail:*:19101:0:99999:7:::
news:*:19101:0:99999:7:::
uucp:*:19101:0:99999:7:::
proxy:*:19101:0:99999:7:::
www-data:*:19101:0:99999:7:::
```

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

① → username

② → encrypted password

③ → Date of last pass change

↳ Days since 1st Jan 1970 (that how it maintain date)

④ → minimum password age. (no of days to change the password here it's '0').

⑤ → maximum password age (the no of days you need to change the password)

⑥ → Warning period for the password

⑦ → password expiry period

⑧ → Account Exp date

⑨ → Reserved field

* PAM : Pluggable Authentication Module

* etc/group :

```
rizon@rizon:~$ sudo cat /etc/group
```

```
root:x:0:
```

① ② ③ ④

(1) → Group Name

(2) → Group Password

(3) → Group ID (GID)

(4) → List of users.

* Useradd and Userdel :

```
rizon@rizon:~$ sudo userdel tasa
```

* change Password:

```
rizon@rizon:~$ sudo passwd rizon
```

↑ username

* Sudo - hostname :

```
rizon@rizon:~$ sudo hostname rizonkumar
```