Types of Users in Linux

❖ Root User (Superuser / Privileged User):

The root user is a special system account with complete, unrestricted access to the entire operating system. It is created automatically during OS setup.

- Username: root
- User ID (UID): 0
- Has full control over the entire system

Root can:

- Install or remove software
- Modify system files
- Create or delete users
- Access any file

Important:

Due to its unlimited power, the root account is not used for daily activities like browsing the web or editing personal documents. Mistakes or malware running as root can irreparably damage the system. Regular users perform administrative tasks using privilege escalation tools like sudo instead of logging in directly as root.

❖ Normal User:

- Standard accounts for people or admins to do daily tasks.
- Purpose: Work safely without affecting critical system files.

Permissions:

- Can read most system files.
- Can write or run files in their own home folder (`/home/username`) or places they have access to.
- Admin tasks: Only possible if given `sudo` rights (configured in `/etc/sudoers`).

Technical Info:

- Usually has a high UID (starting from 1000).

❖ System / Service Users

- Special accounts used to run background services (like daemons).
- Purpose: Keep services secure by giving only the permissions they need.
- Creation: Automatically created by the system or software during installation.

Key Features:

- Cannot log in (no password, uses /sbin/nologin).
- Have low-numbered UIDs (usually 1–999).
- Can access only the files needed for the service.

Examples:

- mysql → runs the database server.
- nginx or www-data → runs the web server.
- syslog → handles system logs.