👥 Linux User Management Summary

Effective user management is essential for Linux system administration. It ensures proper access control, system security, and collaboration between users and groups.

👩‍💻 Why User Management Matters

- Assign appropriate access rights
- Run commands with different privileges (e.g., using `sudo` or `su`)
- Group-based access control for shared resources
- Necessary for auditing and system maintenance

⚙️ Key Concepts

- **Users** can belong to one or more **groups**
- **Groups** define shared permissions for multiple users
- Some files (like `/etc/shadow`) are restricted to **root**

🔐 Running Commands as Another User

❌ Normal User Access

```
cat /etc/shadow
# Output: Permission denied
```

✅ Using `sudo` for Elevated Privileges

```
sudo cat /etc/shadow
# Access granted if user is in sudoers group
```

🦸 Using `su` to Switch Users

```
su - <username>    # Switches to the specified user (default is root)
```

> `sudo` is preferred over `su` for better logging and security.

🛠️ User Management Commands

Command	Description
`sudo`	Execute a command as another user (usually root)
`su`	Switch user account (requires password of target user)
`useradd`	Add a new user
`userdel`	Delete an existing user
`usermod`	Modify an existing user
`passwd`	Change a user's password
`addgroup`	Add a new group
`delgroup`	Delete a group

🧪 Example: Adding a New User

1. Add user Alex:

```
sudo useradd -m alex
```

1. Set password for Alex:

```
sudo passwd alex
```

1. Add Alex to a group (e.g., developers):

```
sudo usermod -aG developers alex
```

1. Verify group membership:

```
groups alex
```

📁 File Permissions Reminder

- `/etc/shadow` – Stores encrypted passwords. Readable only by **root**.
- Use `sudo` to read or modify system-protected files securely.

Tip: Always use `sudo` instead of logging in directly as root for better accountability and security.

✅ Managing users properly ensures secure, organized, and scalable Linux system administration.