**🐧 Access Control Lists(ACL) and Special(Intro) Problems**

**Access Control Lists (ACLs)**

1. Use ACL to give user neeta full access to the directory /data/mumbai which is owned by user rohit and group mi\_group.
2. Use ACL to allow user mukesh to read files and enter the directory /data/mumbai, but prevent any changes.
3. Display all ACL entries set on the directory /data/mumbai.
4. Remove the ACL entry for user mukesh on /data/mumbai without affecting any other user or group.
5. Use ACL to give full access to the group mi\_owner on the directory /data/mumbai.
6. Remove all ACL entries from /data/mumbai so that only the normal owner, group, and others permissions remain.

**Special Permissions**

1. Set the SUID permission on the file /usr/bin/passwd so it always runs with the privileges of its owner.
2. Remove the SUID permission from /usr/bin/passwd.
3. Set the SGID permission on the directory /project\_data so that all new files created inside it automatically belong to the same group as the directory.
4. Verify that new files created in /project\_data inherit the group of the directory.
5. Remove the SGID permission from /project\_data.
6. Set the Sticky Bit on the directory /shared/data so that users can create files, but only the owner of each file can delete or rename it.
7. Verify that users cannot delete or rename files owned by other users inside /shared/data.
8. Remove the Sticky Bit from /shared/data.