

User Management and File Permissions in Linux

Project Description

[cite_start]This project involved the administration of users, groups, and file permissions within a Linux environment to ensure proper access control for research project files.

Tasks Performed

- **Creation and Configuration:** Added the user researcher9 and set their primary group to research_team using useradd and usermod.
- **Ownership Management:** Transferred ownership of the file /home/researcher2/projects/project_r.txt to the new user using the chown command.
- **Group Escalation:** Added the user to the sales_team secondary group using the -a -G flags to preserve existing group memberships.
- **Decommissioning:** Performed complete user removal and cleaned up associated groups after the user's activities were terminated.

Technical Challenges and Resolutions

During execution, I encountered and resolved the following technical hurdles:

1. **Primary Group Dependencies:** When attempting to delete the research_team group, the system returned an integrity violation error because the group was still set as the primary group for users analyst and researcher2.
2. **Resolution:** I reconfigured the primary group of the active users utilizing sudo usermod -g, successfully releasing the group for secure deletion.
3. **Privilege Management:** All administrative tasks were executed with sudo to ensure the required authority over system files and accounts.