Intro to Linux

4.4.1 - Troubleshooting File Permissions

Issues With User Access and File Permissions

- User login issues pertain to difficulties users face when attempting to log into a system
    - Problems include username/password issues, authentication methods, or account lockouts due to multiple failed login attempts
- Users may encounter problems accessing files due to incorrect or inadequate group memberships
- Access permissions are often tied to user groups
    - Context-related issues involve users trying to access files in the wrong environment or context, such as attempting to access system files without the proper authorization
    - Permission issues occur when users lack the necessary file permissions to view, modify, or delete files

Issues With User Access and File Permissions cont’d

- An access control list (ACL) provides control over file access
  - ACL issues arise when they are not configured properly, leading to users being unable to access files they should have access to or vice versa
- Attribute issues refer to problems related to file attributes such as ownership, timestamps, or file type
- Policy/non-policy issues involve conflict between security polices and user actions

Password, Privilege Elevation, and Quota Issues

- Password issues encompass problems like forgotten passwords, weak password policies, or password expiration
  - Can lead to users being unable to log in or to security vulnerabilities
- Privilege elevation issues arise when users need to perform tasks that require higher levels of access than they currently have
  - Can involve seeking administrative privileges or elevated permissions to complete specific actions
- Quota issues involve users exceeding allocated storage quotas, resulting in limitations on file creation or access
  - Users may need to manage their storage space or request quota increases