LESSON NOTES

Intro to Linux

Troubleshooting

4.4.1 Troubleshooting File Permissions

Lesson Overview:

Students will:

- Understand what causes file permission issues and how to resolve them

Guiding Question: What causes issues with file permissions?

Suggested Grade Levels: 9 - 12

Technology Needed: None

CompTIA Linux+ XK0-005 Objective:

4.4 - Given a scenario, analyze and troubleshoot user access and file permissions

- User login issues
- User file access issues
  - Group
  - Context
  - Permission
  - ACL
  - Attribute
  - Policy/Non-Policy
- Password issues
- Privilege elevation
- Quota issues

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER
Copyright © 2024 Cyber Innovation Center
All Rights Reserved. Not for Distribution.

Troubleshooting File Permissions

User access and file permission issues encompass a range of challenges related to controlling and managing user interactions with computer systems and files. The following are some associated topics.

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 can have issues accessing files. Users may encounter problems accessing files due to incorrect or inadequate group memberships. Access permissions are often tied to user groups, so being in the wrong group can restrict access. 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. This can result from incorrect permission settings or inadequate privileges. An access control list (ACL) provides control over file access. ACL issues arise when they are not configured properly. This can lead 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. Incorrect attributes may hinder user access. Policy/non-policy issues involve conflict between security polices and user actions. Users may face restrictions due to security policies, or the lack of clear policies can result in unauthorized access.

Password issues encompass problems like forgotten passwords, weak password policies, or password expiration. These 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. This 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.

User access and file permission issues encompass various challenges that can hinder users' ability to log in, access files, manage passwords, elevate privileges, or work within storage quotas. These issues often stem from misconfigurations, incorrect permissions, or policy conflicts and require proper management and troubleshooting to ensure smooth system operation and user productivity.

Copyright © 2024 Cyber Innovation Center
All Rights Reserved. Not for Distribution.