Linux Assignment - 3

Points to be Covered in Linux Assignment-3

How Permission & Access Control works

- Understanding read, write, and execute options for files and directories

Numerical & Symbolic Methods of permission

- Usage of chmod, chown, and chgrp commands with examples

ACL Permissions & Special Permissions

- SUID, SGID, Sticky-Bit

Password Policies

- chage command and its options

File attributes and masking

- chattr attributes

Linux Assignment - 3

Questions

Question 1: Basic Understanding of Users in Linux

- How many types of users exist in a Linux system? What is the UID range of it?
- Write a Linux command to check which users have access to the shell for executing commands.

Question 2: An organization "**Copex Pvt Ltd**" has set up some users and groups for a project. Perform the following tasks step-by-step:

User and Group Creation

- Create the following users and set a common password **"pass"** for all users:
  - *Nitesh, Mohan, Nitesh, Parul, Alex, Hitesh*
- Create the following groups for this project:
  - *prod, test*

Collaborative Directory Setup

- As the root administrator, create a collaborative directory named **"collaborative"** under "**/mnt".**
- Write a Linux command to change the owner & group-owner of the **/mnt/collaborative** directory to the "**root** & **prod"** group at a same time.

Answer the following questions

- Write a Linux command to check the "**default permissions, owner, and group owner"** of the directory.
- Which users in this project fall under the "others" category for this directory?

Question 3: Advanced Permission Management.

Group Membership Assignment

- As the root administrator, add users **Mohan** and **Nitesh** to the **prod** group as secondary group members.

Linux Assignment - 3

Questions

Write the Linux commands to Apply the appropriate permissions as the root administrator and concepts to achieve this.

- Grant the **prod** group members permission to **create and modify** content in the **/mnt/collaborative** directory.
- Restrict **"others"** from having **no** permissions in the **/mnt/collaborative** directory using the symbolic method.
- Create some files and directories in **/mnt/collaborative** and ensure that any new content created in /mnt/collaborative automatically inherits the same group ownership as the parent directory.
- Additionally, ensure that no one can delete the files created by others, except the file's creator.

Verification Tasks

- Log in as the user “**Mohan**” and:
  - Verify that user “Mohan” can create content in the “**/mnt/collaborative”** directory or not.
  - Now again what are the permissions for “Owner, Group & Other for ”**/mnt/collaborative**”, Describe the permission section of especially group & others.

Question 4: Write a command to remove the SUID special permission from the file /usr/bin/passwd using the numerical method & explain the impact of this change.

Question 5: Set the UMASK Value:

- Write the Linux command to check the current **“umask”** value for the user's shell.
- How would you change the “umask” setting so that all newly created users on the system have a default “umask” value of `0777`?

Question 6: Set the default permissions for the user Parul on newly created files and directories as follows:

- Set the default permissions for all newly created files to r--r--r--.
- Set the default permissions for all newly created directories to r-xr-xr-x..

Linux Assignment - 3

Questions

Question 7: As a system administrator, configure the system to ensure that only the user Nitesh and the root user can modify the **/etc/chrony.conf** file, while all other users should have read-only access to it. Write the commands.

Question 8: User Alex needs to be granted **administrative privileges** equivalent to the root user to manage the system, while ensuring that all other users retain their restricted access based on their roles. Describe how you would implement this configuration. Write the commands.

Question 9: User Hitesh, a senior team member, requires **full access to the system** for daily operations. However, to prevent accidental shutdowns or reboots, configure the system so that Hitesh can execute all commands except **poweroff** and **reboot**. Write the commands.

Question 10: To safeguard all-important and critical system directories, ensure they cannot be deleted or removed by the root user. Write the commands you would use to implement this protection.

*Hint: (/ is a top-level file system directory)