Operating Systems

Lab – 12

Objectives:

- User Management
- File Permissions
    - Special Permissions

Linux Environment

Perform all the tasks on your machine and write in your notebook the particular one's.

1. Create a **lab12/** directory on your desktop and perform the following tasks in it.

User Management

Task01: Create a new username **kakamanna**.

a) View the contents of **/etc/passwd**, **/etc/shadow**, and **/etc/group** which of these files you cannot **see** as kakamanna.
b) As root, assign a **password** to kakamanna and try **logging** in again as kakamanna.
c) Login in as **kakamanna**, and see the contents of his home directory.
d) Login as **root**, and delete user **kakamanna**. See the contents of files **/etc/passwd**, **/etc/shadow**, and **/etc/group**. Note your observations. Also, see if the home directory of the user is **deleted** or not?

Task 02: Login as root, create **three groups** with the name of **faculty**, **staff** and **students** and perform the following tasks.

a) Create three users and make them members of the **faculty** group.
b) Create three users and make them members of the **staff** group.
c) Create three users and make them members of the **students** group.
d) Give **Sudo privileges** to the users of the **faculty** group by adding them to the **Sudo** group.

*What happens if you forget to use that **append flag** while assigning a group to the user?*

File Permissions

Task 01:

As a **regular** user, create a directory **lab12/permissions**.

a) Create a file **owned** by yourself in this directory.
b) Copy a file owned by **root** from **/etc/passwd** to your **permissions** dir.

Who **owns** this file now and **why**?

c) As **root**, create a file in the user's **lab12/permissions** directory.
d) As a **regular** user, look at the **newly** created file.

Who **owns** this file created by root. Try to access it as a **regular** user.

Task 02: Change the ownership of all files in **lab12/permissions** to **kakamanna**. Ensure that **kakamanna** has all rights to these files and that **others** can only **read** them.

Task 03: Create a file as a regular user, and give **only a read** to others. Can another regular user read this file? Test **writing** to this file with vim. Can **root** read this file? Can **root** write to this file with **vim**?

Task 04: To copy **f1.txt** from **lab12/d1/d2/d3/f1.txt** to **lab12/d4/d5/d6/** directory, what should be the **minimum** permissions on these directories and **why**? Think of the **executable** permission on directories.

Special File Permissions

Task 01: What is a **Sticky** bit, and what is it **used for**? Find all the files in your system that have **SUID** bit on. Save **ONLY** the filenames in **attackDB.txt** using **I/O Redirection**.

Task 02: Create a new directory named "**lab**" in your **Lab12/** directory.

a) Create a new **"sample"** file in the **"lab"** directory using the **touch** command.
b) Use the **chmod** command to set the following permissions on the **"sample"** file:

4754 (-rwsr-xr--) , **2774 (-rwxr-sr--)** , **1755 (-rwxr-xr-t)**

c) Use the **ls -l** command to **observe** the changes in the file permissions.
d) Try to execute the **"sample"** file and observe the result.
e) Try to **modify** the content of the **"sample"** file and observe the result.
f) Explain the **purpose** and usage of **SUID, SGID,** and **Sticky** Bit in **real-world** scenarios.

Note your **observation** on a paper and show it while **evaluating** the lab.

<---------->

"Linux is a **long trip** but this **journey** is going to **end**."