Cyber Security and Ethical Hacking Program

Secure User Access Management in Linux

1. Secure User Access Management in Linux

- Essential Linux commands
- File handling
- User access control (groups, ownership)

Introduction

Linux is a powerful operating system that is pervasively used today, even though it might not be apparent to you. Data from TOP500 shows that Linux powers 100% of the world's top 500 supercomputers, which is an astonishing statistic.

Linux is so ubiquitous that it is present in cell phones, cars, refrigerators, and Roku devices. It runs most of the internet and several supercomputers. In fact, stock exchanges across the world in several countries run on Linux.

The reason Linux is so popular is that it is one of the most reliable, secure, and robust operating systems available. Here, we list and explain some important basic Linux commands so you can learn how to use Linux with ease.

Problem Statement Document

Identity and Access Management (IAM) is a centralized and consistent way to manage user identities (that is, people, services, and servers), automate access controls, and meet compliance requirements across traditional and containerized environments.

User management includes everything from creating a user to deleting a user on your system. User management can be done in three ways on a Linux system. Graphical tools are easy and suitable for new users, as they make sure you'll not run into any trouble.

Requirement:

1. Students are free to use any Linux distro (Kali is preferred)
2. Basic understanding of user access management in Linux

Goal:

1. To demonstrate the understanding of IAM in Linux
2. To implement IAM in day-to-day scenarios

Lab 1:

The CTO of the company, Mr. Penny Johnson, has recently discussed a new project with a potential client. He has sent you the file and asked you to —

noida.txt

save it on your Linux machine. Once saved, you are instructed to create a user account "pjohnson" and the project directory and place the file in the folder. Applying the concepts of FACL (Access Control List), you have to give access to Mr. Johnson. **No one else should be able to access the file except Mr. Johnson**. Make sure to **remove any other user access to that file**. As a part of the assignment, kindly log in as another user and try accessing the file.

Kindly compile and explain the process in a report (support with visual evidence).

Note: You are expected to demonstrate that Mr. Penny has access and that any other user cannot access the file.

Lab2:

You are a part of the IT Security team at the census department, the government of India. Three representatives were chosen from three states namely Goa, Delhi, and Gujarat who need to have access to specific files. Those files are attached herewith. Following is the activity to be performed.

Create users "stefi, aravind, and jignesh". Keep the password as "india". Create a new group called "citizen".

Download the following and extract it to the desktop:

government.zip

Change the permissions for **Gujarat** so that **jignesh** has full permissions and **aravind** has only read and execute permissions. Log in as **aravind**. Is he able to edit *Gujarat\ahmedabad.txt*?

Edit the permissions for **Delhi** recursively in such a way that **stefi** has no access. Log in as **stefi** and check if he is unable to access the content of **Delhi**.

Grant full rights to the **citizen** of **Goa**. Edit the rights for *goa\anjuna.txt* so that only **stefi** can write and **aravind** to read, and for *goa\candolim.txt* so that only **jignesh** can write and **stefi** to read.

Considerations:

You have root privileges.