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

Name: Gaurav Uttam Ghandat

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).

SOLUTIONS

STEP 1 :

I Saved the "noida.txt" file on my Linux machine and Created a user account named "pjohnson" using the 'useradd' command. The command is shown below:

```
┌──(root㉿kali)-[/home/kali]
└─# sudo adduser pjhonson
info: Adding user `pjhonson' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `pjhonson' (1002) ...
info: Adding new user `pjhonson' (1002) with group `pjhonson (1002)' ...
info: Creating home directory `/home/pjhonson' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pjhonson
Enter the new value, or press ENTER for the default
        Full Name []: Mr.Penny Johnson
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `pjhonson' to supplemental / extra groups `users' ...
info: Adding user `pjhonson' to group `users' ...
```

STEP 2 :

Next I Create a project directory “Projects" using the 'mkdir' command. Use ls to verify the content of the Projects folder.

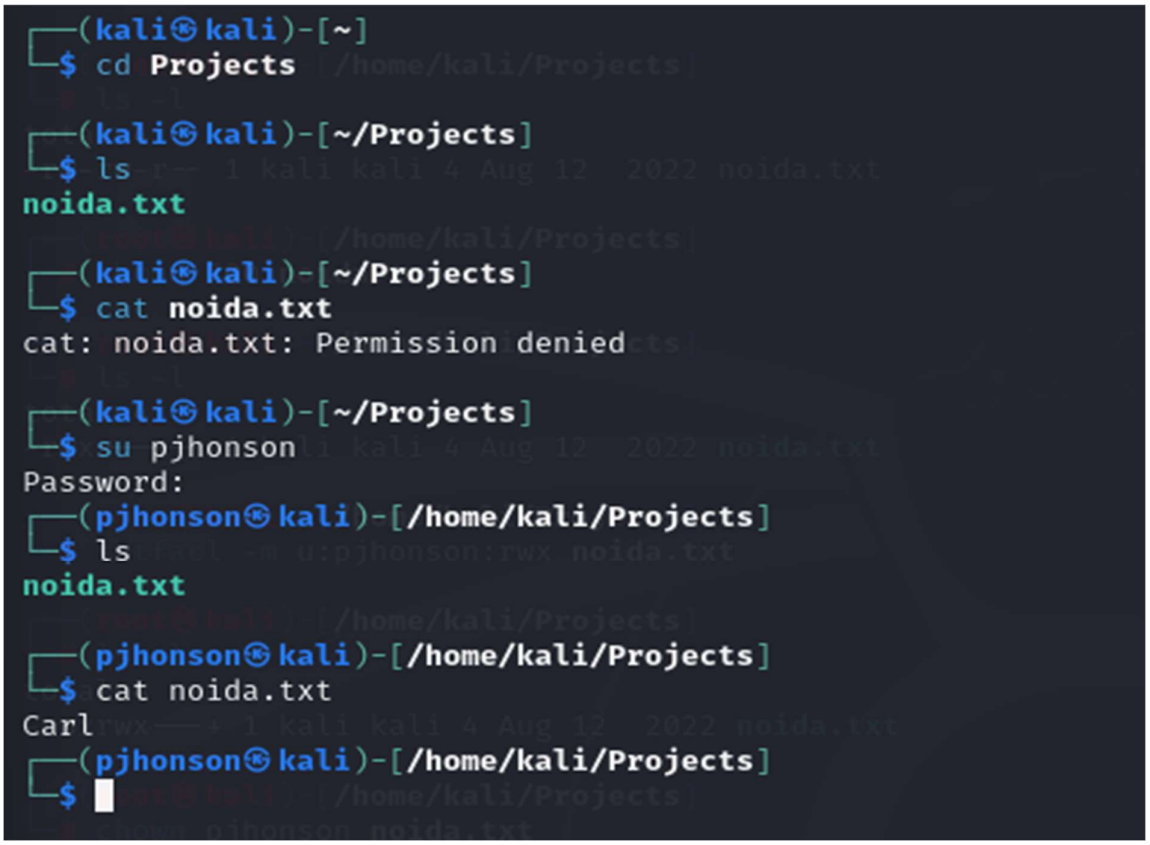
```
┌──(root㉿kali)-[/home/kali]
└─# cd Projects

┌──(root㉿kali)-[/home/kali/Projects]
└─# ls
noida.txt

┌──(root㉿kali)-[/home/kali/Projects]
└─#
```

STEP 3 :

Next assign the permission to the owner of the folder using the “chown”and “chmod” command. Conclude by ensuring permission is set to file And Implement the access control I have used the 'setfacl' command to give Mr. Johnson access to the file And I have also removed access for others using .

STEP 4 :

use the cat command to verify that all users can access file. Occasionally use the “su” command to change user and check all users can access the file And test that only Mr. Johnson has access. Switch users and login using the “su” command and try to access the file. Then also do this for pjhonson.



Lab 2:

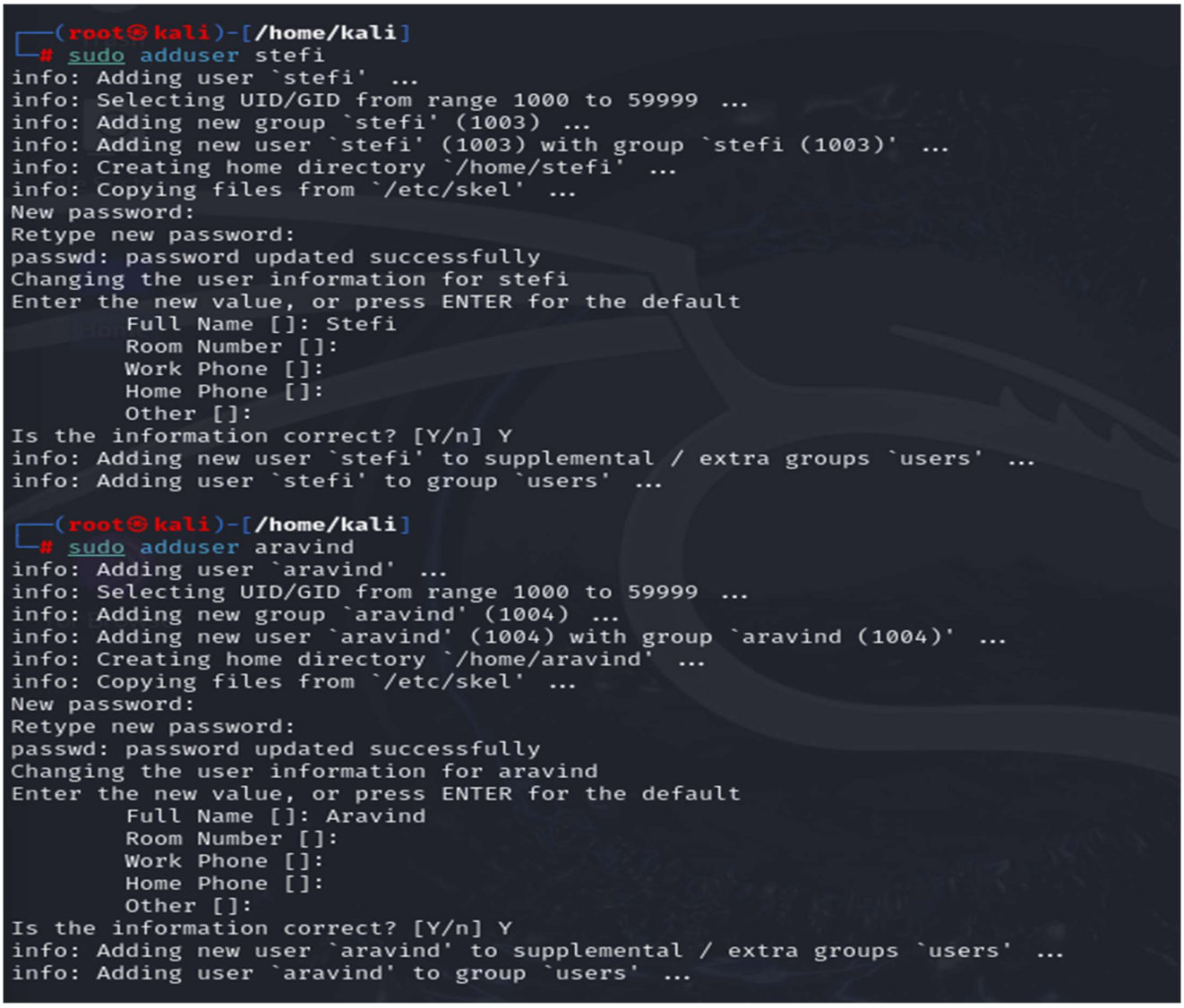
You are a part of the IT Security team at the census department, the government of India. Three representatives were chosen from three states namely Goa, Delhi, and Gujarat who need to have access to specific files. Those files are attached herewith. Following is the activity to be performed. Create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

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.

SOLUTIONS

STEP 1:

I Saved the "goverment" file on my Linux machine and Created user accounts with the given names using the 'useradd' command. The command is shown below:



```
┌──(root㉿kali)-[/home/kali]
└─# sudo adduser jignesh
info: Adding user `jignesh' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `jignesh' (1005) ...
info: Adding new user `jignesh' (1005) with group `jignesh (1005)' ...
info: Creating home directory `/home/jignesh' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jignesh
Enter the new value, or press ENTER for the default
        Full Name []: Jignesh
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `jignesh' to supplemental / extra groups `users' ...
info: Adding user `jignesh' to group `users' ...
```

STEP 2 :

create a group called “citizen” using the ‘groupadd‘ command. add the three users to this group using the “usermod”.

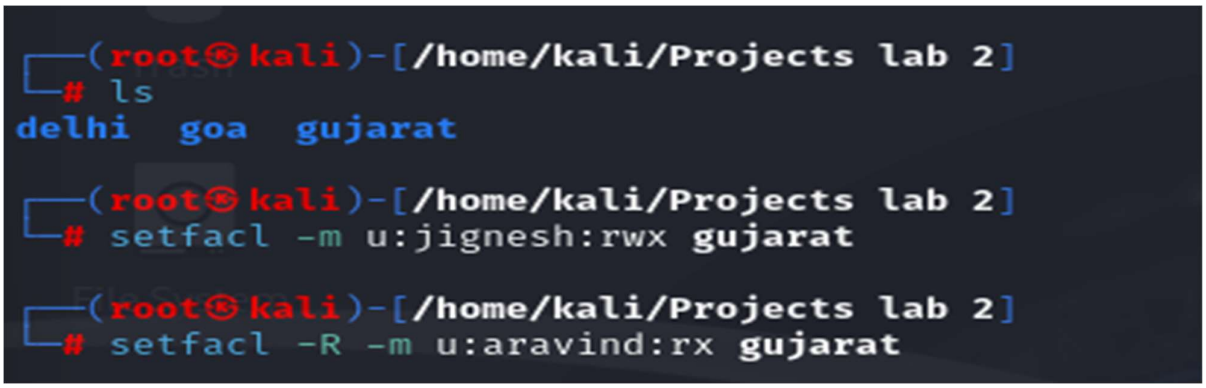
```
┌──(root㉿kali)-[/home/kali]
└─# sudo groupadd citizen

┌──(root㉿kali)-[/home/kali]
└─# cat /etc/group | grep citizen
citizen:x:1006:

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo usermod -a -G citizen stefi

┌──(root㉿kali)-[/home/kali]
└─# sudo usermod -a -G citizen aravind

┌──(root㉿kali)-[/home/kali]
└─# sudo usermod -a -G citizen jignesh

┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# cat /etc/group | grep citizen
citizen:x:1006:stefi,aravind,jignesh

┌──(root㉿kali)-[/home/kali]
└─#
```

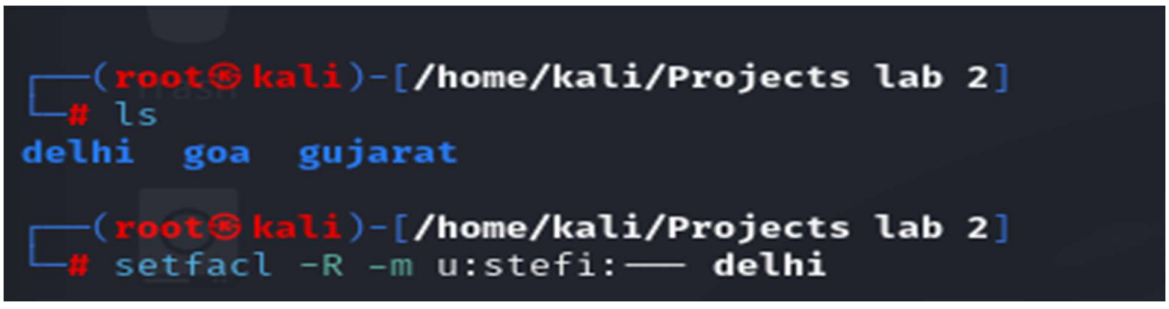
STEP 3 :

Unzip the folder government.zip And Change the permissions for Gujarat so that jignesh has full permissions and aravind has only read and execute permissions. Give Jignesh full permission with the code below



STEP 4 :

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. Reset stefi permissions using the setfacl command and root permissions. Switch user using ”su” command and check if stefi can access

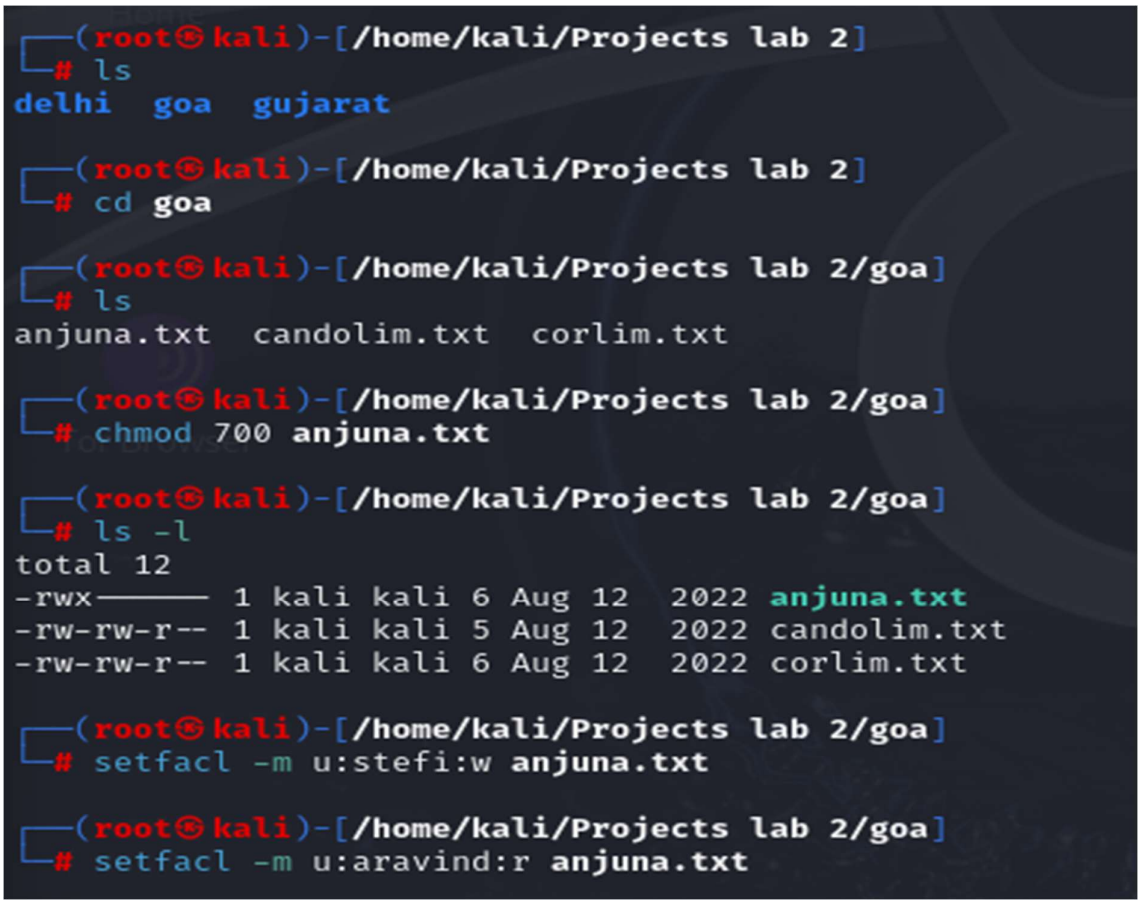


```
┌──(stefi㉿kali)-[/home/kali/Projects lab 2]
└─$ ls
delhi  goa  gujarat

┌──(stefi㉿kali)-[/home/kali/Projects lab 2]
└─$ cd delhi
bash: cd: delhi: Permission denied

┌──(stefi㉿kali)-[/home/kali/Projects lab 2]
└─$
```

STEP 5 :

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, First remove the read/write command from the group using the group option of setfacl and then add permissions for stefi and Aravind and then confirm by switching users.

```
┌──(root㉿kali)-[/home/kali/Projects lab 2]
└─# ls
delhi  goa  gujarat

┌──(root㉿kali)-[/home/kali/Projects lab 2]
└─# setfacl -m g:citizen:rwx goa
```



STEP 6 :

And for goa\candolim.txt so that only jignesh can write and stefi to read. First remove the read/write command from the group using the group option of setfacl and then add specific permissions.

```
┌──(root㉿kali)-[/home/kali/Projects lab 2/goa]
└─# ls
anjuna.txt  candolim.txt  corlim.txt

┌──(root㉿kali)-[/home/kali/Projects lab 2/goa]
└─# chmod 700 candolim.txt

┌──(root㉿kali)-[/home/kali/Projects lab 2/goa]
└─# setfacl -m u:jignesh:w candolim.txt

┌──(root㉿kali)-[/home/kali/Projects lab 2/goa]
└─# setfacl -m u:stefi:r candolim.txt
```

```
┌──(root㉿kali)-[/home/kali/Projects lab 2/goa]
└─# ls -l
total 12
-rwxrw----+ 1 kali kali 6 Aug 12  2022 anjuna.txt
-rwxrw----+ 1 kali kali 5 Aug 12  2022 candolim.txt
-rw-rw-r--  1 kali kali 6 Aug 12  2022 corlim.txt
```

STEP 6 :

Switch user and check work.

```
┌──(jignesh㉿kali)-[/home/kali]
└─$ cat candolim.txt
cat: candolim.txt: Permission denied

┌──(jignesh㉿kali)-[/home/kali]
└─$
```

```
┌──(stefi㉿kali)-[/home/kali/Projects lab 2/goa]
└─$ cat candolim.txt
Tulip
┌──(stefi㉿kali)-[/home/kali/Projects lab 2/goa]
└─$
```