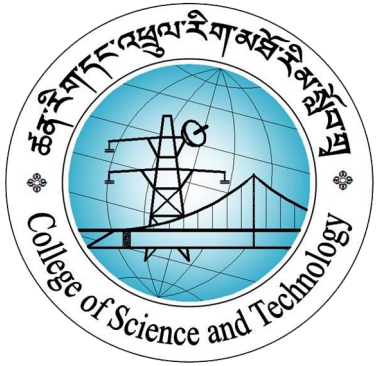

Royal University of Bhutan

LESSON – 10

USER AND GROUP MANAGEMENT

Learning Outcomes

- Identify types of users on Linux system
- Configure sudoer for the normal user
- Switch between user in the terminal windows
- Explain the /etc/passwd and /etc/shadow files
- Create users and groups
- Manage users in Linux system

USER TYPES

1. Privileged:
   - root (a default privileged user)
   - Has full access to everything on a Linux System

2. Non Privileged:
   - All other users
   - Use **id** command to get information about user
   - Example:

```
#id username
```

Working as a root

commands:

- **su**

- Switch user to root user

- **sudo:**

- Make the administrative user account member of the group sudo by using

- usermod –aG sudo user

- Type **visudo** and make sure the line % admin ALL = (ALL) ALL is included.

Example:

- $ su
- #

- work on user shell. No root shell has been provided

- If no user is specified, it is switch to root user by default

- $ su - root

- work on root shell.

- #sudo

- Privileged user escalation

System User and

Normal User Account:

- **/etc/passwd**

- Users account information

Example:

#cat /etc/passwd

jiwan:x:1001:1001:Jiwan,,,,ICTO:/home/jiwan:/bin/bash

- This file stores the user's login(**jiwan**), encrypted password entry(*****), UID(**1001**), default GID (**1001**), name(**Jiwan**), home directory(**/home/jiwan**), and login shell(**/bin/bash**).
- Field delimiter is colon (**:**)
- UID 0 is always assigned to super user, root
- UID 1-200 is a range of "system users" assigned statially to system processes
- UID 201-999 is a range of "system users" used by system processes that do not own files on the file system.
- UID 1000+ is the range available for assignment to regular users.

System User and

Normal User Account:

- **/etc/shadow**

Encrypted password and aging information.

This is encrypted password file, accessible by ONLY root

Example:

#cat /etc/shadow

jiwan:yj9T$Md0m3WIZ5yjrPGsxRSuZv/$Kkmno2eQu2DrKoUSoqypFeN0mrl6PpuaufRApTSggVB:19986:0:99999:7:::

The shadow file has nine colon-separated fields:

1. Username (**jiwan**)
2. Encrypted password of the user (discussed on next slide)
3. The day on which password was last changed started from 09/20/2024 (**19986**)
4. The minimum no. of days that have to elapse since the last password change before the user can change it again
5. The max no. of days that can pass without a password change before the password expires
6. Warning period (**7**)
7. Inactive period
8. The days on which the password expired. An empty means it does not expire
9. Usually empty, reserved for future use

System User and

Normal User Account:

- **`/etc/shadow`**

Format of an Encrypted Password

Example:

```
#cat /etc/shadow
```

jiwan:yj9T$Md0m3WlZ5yjrPGsxRSuZv/$Kkmno2eQu2DrKoUSoqypFeN0mrl6PpuaufRApTSggVB:19986:0:99999:7:::

- This file stores three pieces of information; the *hashing algorithm* used, the *salt* (**j9T$Md0m3WlZ5yjrPGsxRSuZv/**), and the *encrypted hash* (**Kkmno2eQu2DrKoUSoqypFeN0mrl6PpuaufRApTSggVB**). Each piece of information is delimited by $.
- The hashing algorithm is yescrypt hash (default in Ubuntu 22.04 and above).
- The salt – used to encrypt password. It is choosen as random
- salt + unencrypted password = encrypted hash

(Ubuntu security)

Managing Group Accounts:

- **/etc/group**

  it contains name, password, identify and group members

Example:

```
#cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,cst
```

Command-Line User:

- User: useradd, userdel, usermod
- Group: groupadd, groupdel, groupmod

Example:

```
#adduser username
#tail  -1 /etc/passwd
#sudo adduser username groupname
#sudo deluser username
#sudo passwd -l username -> LOCK User
# sudo passwd username or passwd ->
Change Password
```

Adding user to Group:

- Using usermod command
- Editing /etc/group

Example:

```
#sudo adduser username groupname
```

```
#id userA
uid=1003(userA) gid=1003(userA)
groups=1003(userA),1005(IT)
```

```
#vim /etc/group
IT:x:1005:userA
```

ACTIVITY I:

- Creating users with password and deleting user.

1. In the terminal, switch to the **root** user
2. Create **userA** and password of this user.
3. Switch to virtual console tty2 and login with **userA** credential
4. Switch back to graphical environment and create another user (**userB**) without password
5. Switch to virtual console tty3 and login with **userB**. Are you successful in signing in?
6. Again switch back to graphical and create empty password with **passwd -D userB** command. Again, switch back to tty3 and log in to the system. This time, you will be successful.
7. Delete users one by one using **userdel** command. Make sure to use **–r** option to remove all related files with user.

ACTIVITY II:

- Locking and Unlocking user
- Enable password expiry for users.

1. In the terminal, switch to the **root** user
2. Create **userA** and with empty password of this user. Examine the shadow file.
3. create another user (**userB**) with password
4. Switch to new virtual console and login with **userB**. Are you successful in signing in?
5. Lock the user with usermod command and examine the shadow file. What difference did you observe?
6. Lock the user with passwd command and examine the shadow file.
7. Change the password expiry for userB with change command to 21-09-2024. Examine the shadow file.

SUMMARY

- The Linux system has built-in users, system users and service
- users.
- The usage of commands such as useradd, userdel, usermod, groupadd, and so on.
- The configuration of sudoer to have an administrative access