**UNIT-3**

1 Mark Questions

1.Define a user in a Linux environment?

2.Define a group in a Linux environment?

3.UID stands for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4.GID stands for\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5.Which command can be used to login as a different user?

6.\_\_\_\_ is a special administrate group in a RedHat Linux?

7.What is the use of sudo command in RedHat Linux?

7 Mark Questions

1.What is shadow password? What is its advantages explain?

2.Explain the procedure to create a active user in a Linux system?

3.Explain the procedure to create a group in the system and adding a user in that group?

4.What is a significance of group directories in Linux environment explain?

5.Demonstrate the procedure to create a group directory and set its GID group So that group of directory

work on particular directory?

6.Explain the procedure to restrict the access to su command only to few users?

7.What is the use of sudo command in RedHat Linux?

**Answers:-**

**One mark**

1. Entities who or which has access to the system are known as Users
2. Group is a organization or similar type of users together for common purpose
3. UID:- user ID
4. GID:- Group ID
5. Command used to login as different user is “su
6. Wheel-special administrate group in a red hat linux.
7. “Sudo” is a systems command that provides an efficient way to give specific users permission to use specific system commands at the root (most powerful) level of the system. Sudo also logs all commands and arguments.Or Login/switch to Super User

**Seven mark**

1)In environments with multiple users, it is very important to use shadow passwords provided by

the shadow-utils package to enhance the security of system authentication files. For this

reason, the installation program enables shadow passwords by default.

The following is a list of the advantages shadow passwords have over the traditional way of

storing passwords on UNIX-based systems:

Shadow passwords improve system security by moving encrypted password hashes from

the world-readable /etc/passwd file to /etc/shad o w, which is readable only by the ro

ot user.

Shadow passwords store information about password aging.

Shado w passwo rds allow the /etc/l ogin.de fs file to enforce security policies.

Most utilities provided by the shadow-utils package work properly whether or not shadow

passwords are enabled. However, since password aging information is stored exclusively

in the /etc/shad o w file, some utilities and commands do not work without first enabling

shadow passwords:

2)To add the new active user we use the command:-

Useradd [option] “user\_name” It uses “useradd” with option that can be given

And we can give user defined username

3)To create the group we use groupadd [options] group\_name

We use Groupadd command to add group with user-defined group\_name

To add user a specified user group we use usermod -a -g dir\_name user\_name

Here -a is a append and we have to specify directory name username

4) Group Directory will be specific to that specified group the group users and the group owner can only access the directory. Here any file that created in the directory can only be accessed by the owner of the file and the group user and owner.

5)

* As root user create directory:- mkdir /opt/mydir
* Add group to the system:- groupadd mygroup
* Change ownership to root to the new user:-chown root:mygroup /opt/mydir
* Change permission or give permissions:- chmod 2775 /opt/mydir
* To set the group ID we use “set gid” so that file created inside the group can be accessed only by group members

6) To restrict the use of su command we can add a trusted users in the the group called “wheel”.Usermod -a -g wheel username And modify pluggable authentication module (PAM) config file.Here uncomment the line inside of that file “#character auth required

pam\_wheel

7)”Sudo” is a systems command that provides an efficient way to give specific users permission to use specific system commands at the root (most powerful) level of the system. Sudo also logs all commands and arguments.

Or Login/switch to Super User