Assignment -3

By - Pratibha Singh [TR2]

Roll No. - 22ETCCS121

1.Basic Understanding of Users in Linux

- How many types of users exist in a Linux system? What is the UID range of it?
- Write a Linux command to check which users have access to the shell for executing commands.

Ans. In a **Red Hat Enterprise Linux (RHEL) system**, there are three main types of users:

1. Root User (Superuser)
   - The most powerful user with UID 0.
   - Has unrestricted access to all system files and configurations.
   - Can perform administrative tasks like installing software, modifying system settings, and managing other users.
2. System Users (Service Accounts)
   - These users are created for running system services like databases, web servers, and daemons.
   - Their UIDs typically range from 1 to 999 in RHEL.
   - Examples: nobody, apache, mysql.
3. Local Users (Normal Users)
   - Created for human users to perform daily tasks.
   - Their UIDs start from 1000 onwards (on RHEL) by default.
   - Can access system resources but have limited privileges.

2. An organization “Copex Pvt Ltd” has set up some users and groups for a project. Perform the following tasks step-by-step:
User and Group Creation

- Create the following users and set a common password “pass” for all users: Nitesh, Mohan, Nitesh, Parul, Alex, Hitesh
- Create the following groups for this project: prod, test

Collaborative Directory Setup

- As the root administrator,create a collaborative directory named “collaborative” under “/mnt”.
- Write a Linux command to change the owner & group-owner of the /mnt/collaborative directory to the “root & prod” group at a same time.

Answer the following questions

- Write a Linux command to check the “default permissions, owner, and group owner” of the directory.
- Which users in this project fall under the "others" category for this directory?

Ans.

```
pratibhasingh@rhel:~
pratibhasingh@rhel [~] $ sudo useradd -m -p $(openssl passwd -6 'pass') nitesh
[sudo] password for pratibhasingh:
pratibhasingh@rhel [~] $ sudo useradd -m -p $(openssl passwd -6 'pass') mohan
pratibhasingh@rhel [~] $ sudo useradd -m -p $(openssl passwd -6 'pass') parul
pratibhasingh@rhel [~] $ sudo useradd -m -p $(openssl passwd -6 'pass') alex
pratibhasingh@rhel [~] $ sudo useradd -m -p $(openssl passwd -6 'pass') hitesh
pratibhasingh@rhel [~] $ sudo groupadd prod
pratibhasingh@rhel [~] $ sudo groupadd test
pratibhasingh@rhel [~] $ tail -5 /etc/passwd
nitesh:x:1001:1001::/home/nitesh:/bin/bash
mohan:x:1002:1002::/home/mohan:/bin/bash
parul:x:1003:1003::/home/parul:/bin/bash
alex:x:1004:1004::/home/alex:/bin/bash
hitesh:x:1005:1005::/home/hitesh:/bin/bash
pratibhasingh@rhel [~] $ tail -2 /etc/group
prod:x:1006:
test:x:1007:
pratibhasingh@rhel [~] $
```

```
pratibhasingh@rhel:~
pratibhasingh@rhel [~] $ sudo mkdir /mnt/collaborative
[sudo] password for pratibhasingh:
pratibhasingh@rhel [~] $ sudo chown root:prod /mnt/collaborative
pratibhasingh@rhel [~] $ ls -d /mnt/collaborative/
/mnt/collaborative/
pratibhasingh@rhel [~] $ ls -ld /mnt/collaborative/
drwxr-xr-x. 2 root prod 6 Jan 31 14:12 /mnt/collaborative/
pratibhasingh@rhel [~] $
```

Users in this project fall under the "others" category for this directory are Nitesh, Mohan, Parul, Alex, Hitesh.If a user is not added to the "prod" group, they belong to "others."

3. Advanced Permission Management. Group Membership Assignment

- As the root administrator, add users Mohan and Nitesh to the prod group as secondary group members.

Write the Linux commands to Apply the appropriate permissions as the root administrator and concepts to achieve this.

- Grant the prod group members permission to create and modify content in the /mnt/collaborative directory.
- Restrict "others" from having no permissions in the /mnt/collaborative directory using the symbolic method.
- Create some files and directories in /mnt/collaborative and ensure that any new content created in /mnt/collaborative automatically inherits the same group ownership as the parent directory.
- Additionally, ensure that no one can delete the files created by others, except the file's creator.

  Verification Tasks

  Log in as the user “Mohan” and: Verify that user “Mohan” can create content in the “/mnt/collaborative” directory or not. Now again what are the permissions for “Owner, Group & Other for ”/mnt/collaborative”, Describe the permission section of especially group & others.

Ans.

```
Mohan@rhel:/mnt/collaborative
pratibhasingh@rhel [~] $ sudo usermod -aG prod Mohan
[sudo] password for pratibhasingh:
pratibhasingh@rhel [~] $ sudo usermod -aG prod Nitesh
pratibhasingh@rhel [~] $ sudo chmod 770 /mnt/collaborative
pratibhasingh@rhel [~] $ sudo chmod o-rwx /mnt/collaborative
pratibhasingh@rhel [~] $ ls -ld /mnt/collaborative/
drwxrwx---. 2 root prod 6 Jan 31 14:12 /mnt/collaborative/
pratibhasingh@rhel [~] $ sudo chmod g+s /mnt/collaborative
pratibhasingh@rhel [~] $ sudo chmod +t /mnt/collaborative
pratibhasingh@rhel [~] $ ls -ld /mnt/collaborative/
drwxrws--T. 2 root prod 6 Jan 31 14:12 /mnt/collaborative/
pratibhasingh@rhel [~] $ sudo touch /mnt/collaborative/sample_file.txt
[sudo] password for pratibhasingh:
pratibhasingh@rhel [~] $ sudo mkdir /mnt/collaborative/sample_folder
pratibhasingh@rhel [~] $ ls -ld /mnt/collaborative/sample_file.txt
ls: cannot access '/mnt/collaborative/sample_file.txt': Permission denied
pratibhasingh@rhel [~] $ sudo ls -ld /mnt/collaborative/sample_file.txt
-rw-r--r--. 1 root prod 0 Jan 31 14:41 /mnt/collaborative/sample_file.txt
pratibhasingh@rhel [~] $ sudo ls -ld /mnt/collaborative/sample_folder
drwxr-sr-x. 2 root prod 6 Jan 31 14:42 /mnt/collaborative/sample_folder
pratibhasingh@rhel [~] $ sudo su - Mohan
Hello, you are logged in as Mohan
[Mohan@rhel ~]$ cd /mnt/collaborative/
[Mohan@rhel collaborative]$ touch mohan_sample.txt
[Mohan@rhel collaborative]$ mkdir mohan_sample
[Mohan@rhel collaborative]$ ls -ld /mnt/collaborative
drwxrws--T. 4 root prod 94 Jan 31 14:45 /mnt/collaborative
[Mohan@rhel collaborative]$
```

4. Write a command to remove the SUID special permission from the file /usr/bin/passwd using the numerical method & explain the impact of this change.

Ans.

```
pratibhasingh@rhel:~
pratibhasingh@rhel [~] $ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 32648 Aug 10  2021 /usr/bin/passwd
pratibhasingh@rhel [~] $ sudo chmod 755 /usr/bin/passwd
[sudo] password for pratibhasingh:
pratibhasingh@rhel [~] $ ls -l /usr/bin/passwd
-rwxr-xr-x. 1 root root 32648 Aug 10  2021 /usr/bin/passwd
pratibhasingh@rhel [~] $
```

Impact of Removing SUID from /usr/bin/passwd

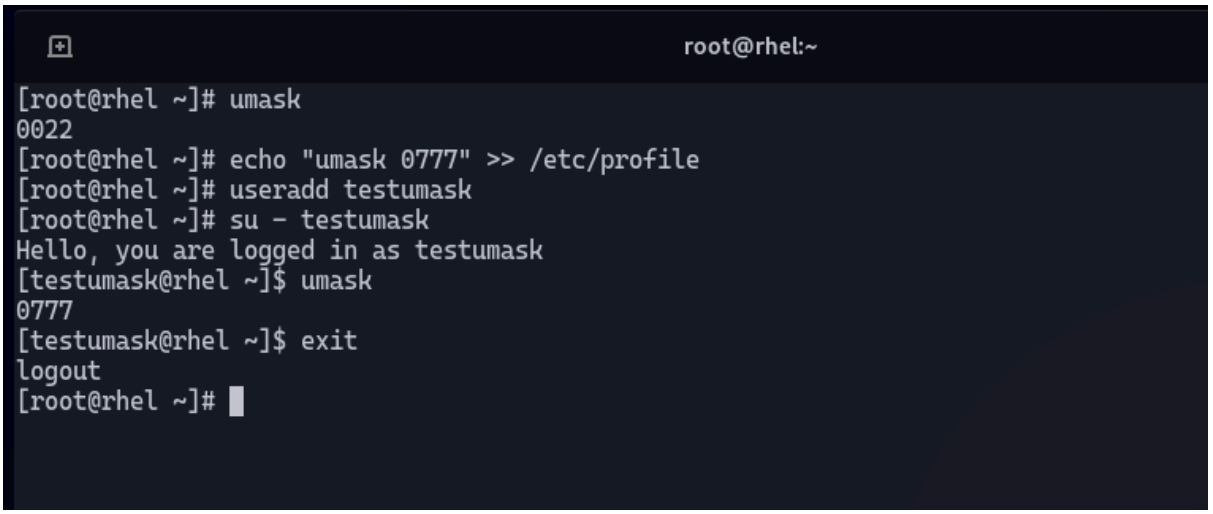
1. Users Cannot Change Their Own Passwords Anymore
    - The /usr/bin/passwd command relies on SUID to allow regular users to change their own passwords.

    - Removing SUID means /usr/bin/passwd will run with the user's privileges instead of root's.
2. Password Updates Will Require Root Privileges
    - If a user tries to change their password using passwd, they will get a permission denied error.
3. Only the Root User Can Modify Passwords
    - Without SUID, only the root user can execute passwd and change passwords for any user

5. Set the UMASK Value:

- Write the Linux command to check the current "umask" value for the user's shell.
- How would you change the "umask" setting so that all newly created users on the system have a default "umask" value of `0777`?

Ans.



6. Set the default permissions for the user Parul on newly created files and directories as follows:

- Set the default permissions for all newly created files to r--r--r--.
- Set the default permissions for all newly created directories to r-xr-xr-x..

Ans.

```
Parul@rhel:~
[root@rhel pratibhasingh]# echo "umask 0222" >> /home/Parul/.bashrc
[root@rhel pratibhasingh]# su - Parul
Hello, you are logged in as Parul
[Parul@rhel ~]$ touch testfile
[Parul@rhel ~]$ mkdir testdir
[Parul@rhel ~]$ ls -l
total 4
-rw-r--r--. 1 Parul Parul 27 Jan 28 15:47 instruction.txt
dr-xr-xr-x. 2 Parul Parul  6 Jan 31 15:21 testdir
-r--r--r--. 1 Parul Parul  0 Jan 31 15:21 testfile
[Parul@rhel ~]$
```

7. As a system administrator, configure the system to ensure that only the user Nitesh and the root user can modify the /etc/chrony.conf file, while all other users should have read-only access to it. Write the commands.

Ans.

```
root@rhel:~
[root@rhel ~]# ls -l /etc/chrony.conf
-rw-r--r--. 1 root root 1369 Dec  5  2023 /etc/chrony.conf
[root@rhel ~]# setfacl -m u:Nitesh:rwx /etc/chrony.conf
[root@rhel ~]# getfacl /etc/chrony.conf
getfacl: Removing leading '/' from absolute path names
# file: etc/chrony.conf
# owner: root
# group: root
user::rw-
user:Nitesh:rwx
group::r--
mask::rwx
other::r--

[root@rhel ~]#
```

8. User Alex needs to be granted administrative privileges equivalent to the root user to manage the system, while ensuring that all other users retain their restricted access based on their roles. Describe how you would implement this configuration. Write the commands.

Ans.

```
pratibhasingh@rhel:~
pratibhasingh@rhel [~] $ sudo su - alex
[alex@rhel ~]$ sudo whoami
[sudo] password for alex:
alex is not in the sudoers file.  This incident will be reported.
[alex@rhel ~]$ exit
logout
pratibhasingh@rhel [~] $ sudo visudo
pratibhasingh@rhel [~] $ cat /etc/sudoers | grep -n alex
cat: /etc/sudoers: Permission denied
pratibhasingh@rhel [~] $ sudo cat /etc/sudoers | grep -n alex
101:alex    ALL=(ALL)       ALL
pratibhasingh@rhel [~] $ sudo su - alex
[alex@rhel ~]$ sudo whoami
[sudo] password for alex:
root
[alex@rhel ~]$ exit
logout
pratibhasingh@rhel [~] $
```

9. User Hitesh, a senior team member, requires full access to the system for daily operations. However, to prevent accidental shutdowns or reboots, configure the system so that Hitesh can execute all commands except power off and reboot. Write the commands.

Ans.

```
pratibhasingh@rhel:~
pratibhasingh@rhel [~] $ sudo cat /etc/sudoers | grep -n hitesh
101:hitesh  ALL=(ALL)       ALL, !/sbin/poweroff, !/sbin/reboot, !/sbin/shutdown
pratibhasingh@rhel [~] $ sudo su - hitesh
[hitesh@rhel ~]$ sudo whoami
root
[hitesh@rhel ~]$ sudo reboot
Sorry, user hitesh is not allowed to execute '/sbin/reboot' as root on rhel.
[hitesh@rhel ~]$ sudo poweroff
Sorry, user hitesh is not allowed to execute '/sbin/poweroff' as root on rhel.
[hitesh@rhel ~]$ sudo shutdown
Sorry, user hitesh is not allowed to execute '/sbin/shutdown' as root on rhel.
[hitesh@rhel ~]$ exit
logout
pratibhasingh@rhel [~] $
```

10. To safeguard all-important and critical system directories, ensure they cannot be deleted or removed by the root user. Write the commands you would use to implement this protection. *Hint: (/ is a top-level file system directory)

Ans.

```
root@rhel:~
[root@rhel ~]# lsattr -d /
---------------------- /
[root@rhel ~]# chattr +i /
[root@rhel ~]# lsattr -d /
----i----------------- /
[root@rhel ~]# chattr -i /
[root@rhel ~]# lsattr -d /
---------------------- /
[root@rhel ~]#
```