Assignment – User Management
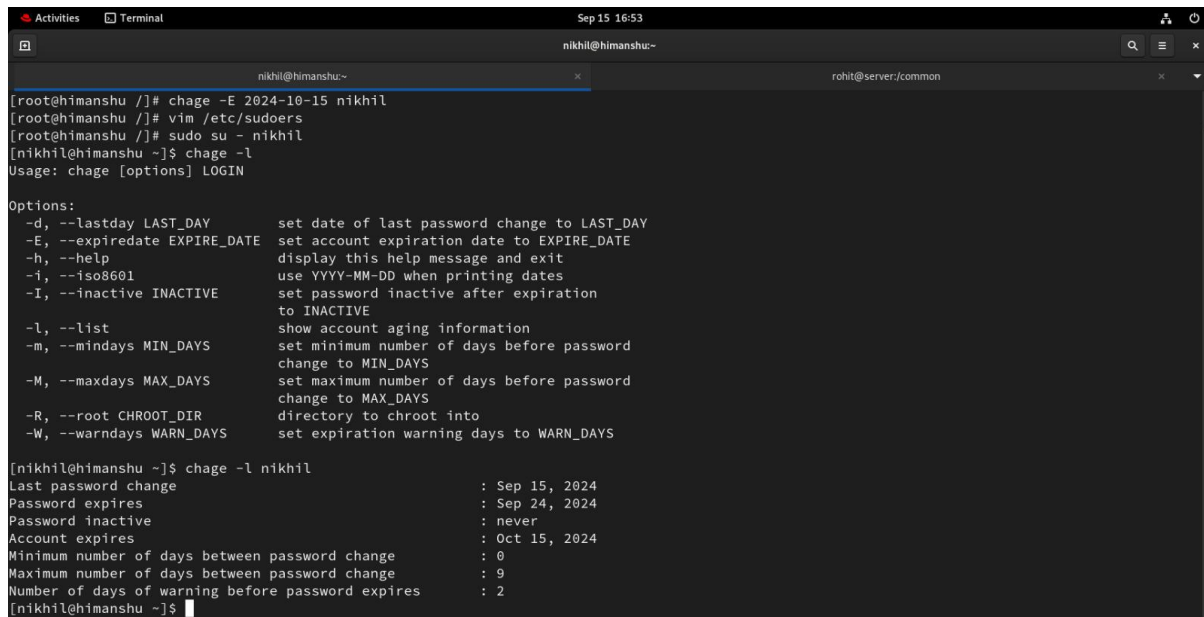
1) Create user "nikhil" with home directory set as "/home/nikhil"

 a) nikhil user should have "/bin/sh" shell for his environment

 b) His password should expire in 9 days and 2 days before password expiry, he should get warning. User account must expire in 1 month from creation date
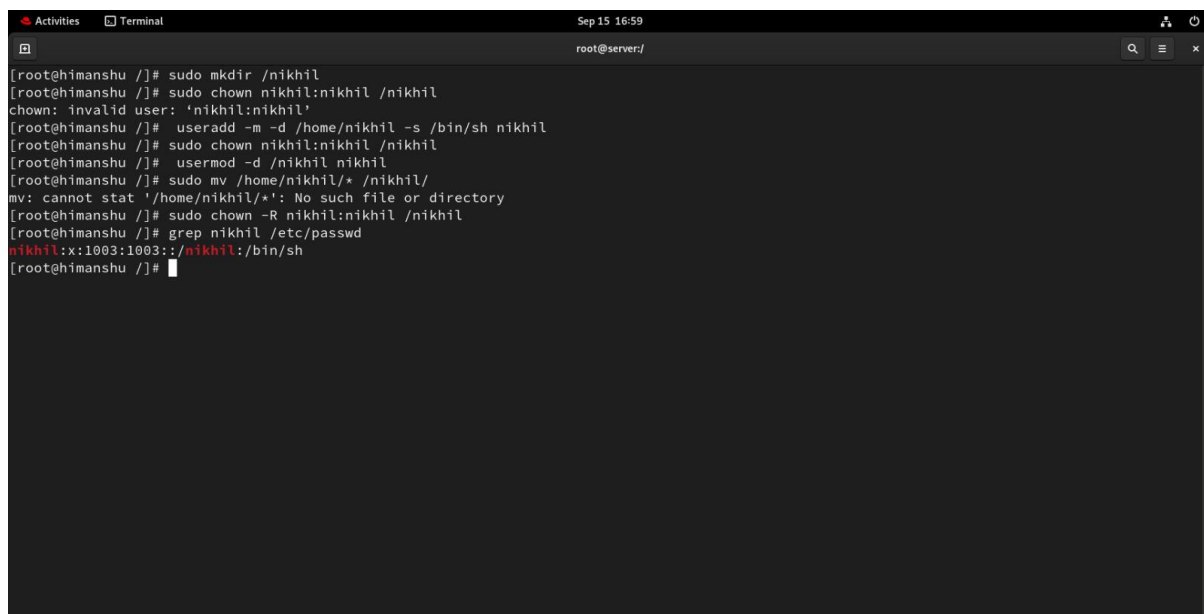
c) Give him root privileges to start/stop cron daemon.


```
[root@himanshu /]# chage -E 2024-10-15 nikhil
[root@himanshu /]# vim /etc/sudoers
[root@himanshu /]# sudo su - nikhil
[nikhil@himanshu ~]$ chage -l
Usage: chage [options] LOGIN

Options:
  -d, --lastday LAST_DAY        set date of last password change to LAST_DAY
  -E, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -h, --help                    display this help message and exit
  -i, --iso8601                 use YYYY-MM-DD when printing dates
  -I, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -l, --list                    show account aging information
  -m, --mindays MIN_DAYS        set minimum number of days before password
                                change to MIN_DAYS
  -M, --maxdays MAX_DAYS        set maximum number of days before password
                                change to MAX_DAYS
  -R, --root CHROOT_DIR         directory to chroot into
  -W, --warndays WARN_DAYS      set expiration warning days to WARN_DAYS

[nikhil@himanshu ~]$ chage -l nikhil
Last password change                                    : Sep 15, 2024
Password expires                                        : Sep 24, 2024
Password inactive                                       : never
Account expires                                         : Oct 15, 2024
Minimum number of days between password change          : 0
Maximum number of days between password change          : 9
Number of days of warning before password expires       : 2
[nikhil@himanshu ~]$
```

2) Inside folder "/" , create new home directory as "nikhil" (/nikhil) and setup this folder as a home directory for user "nikhil"


```
[root@himanshu /]# sudo mkdir /nikhil
[root@himanshu /]# sudo chown nikhil:nikhil /nikhil
chown: invalid user: 'nikhil:nikhil'
[root@himanshu /]#  useradd -m -d /home/nikhil -s /bin/sh nikhil
[root@himanshu /]# sudo chown nikhil:nikhil /nikhil
[root@himanshu /]#  usermod -d /nikhil nikhil
[root@himanshu /]# sudo mv /home/nikhil/* /nikhil/
mv: cannot stat '/home/nikhil/*': No such file or directory
[root@himanshu /]# sudo chown -R nikhil:nikhil /nikhil
[root@himanshu /]# grep nikhil /etc/passwd
nikhil:x:1003:1003::/nikhil:/bin/sh
[root@himanshu /]#
```

```
# Defaults    env_keep += "HOME"

Defaults       secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
nikhil ALL=(root) NOPASSWD: /bin/systemctl start cron, /bin/systemctl stop cron

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
:wq
```