

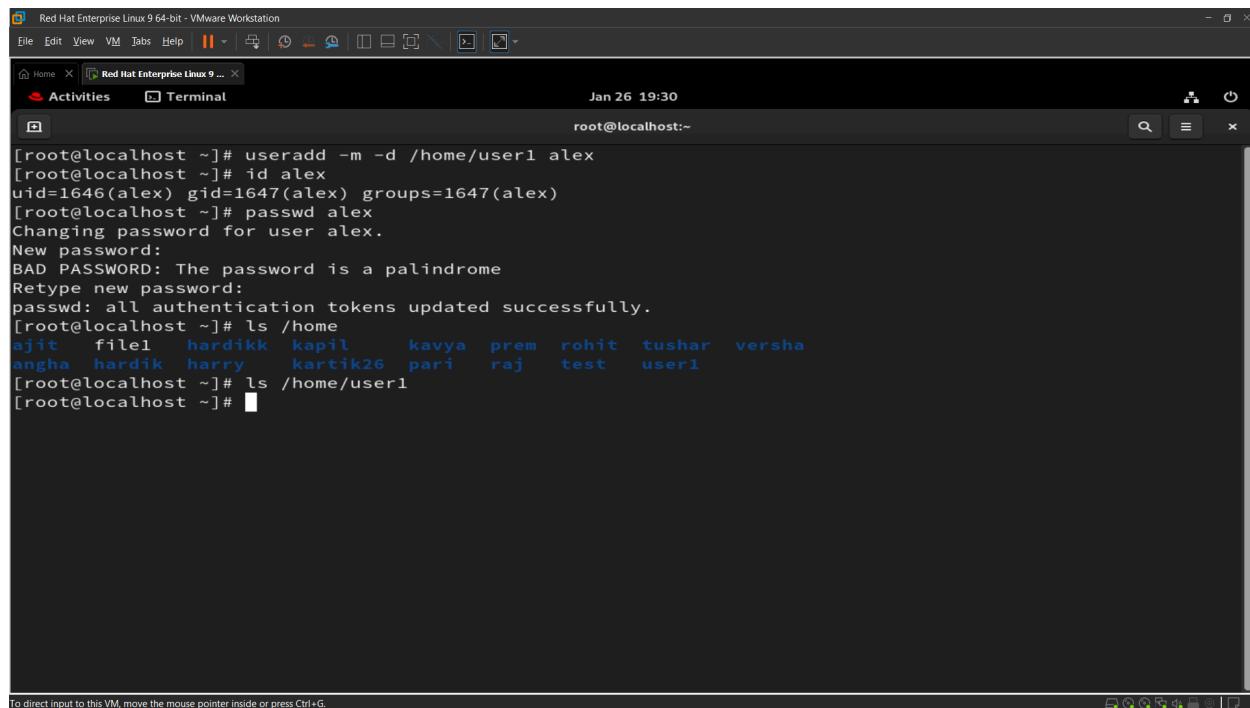
Name : Kartik Jain

TR : 2

Assignment No : 2

Q1 : Create some users:

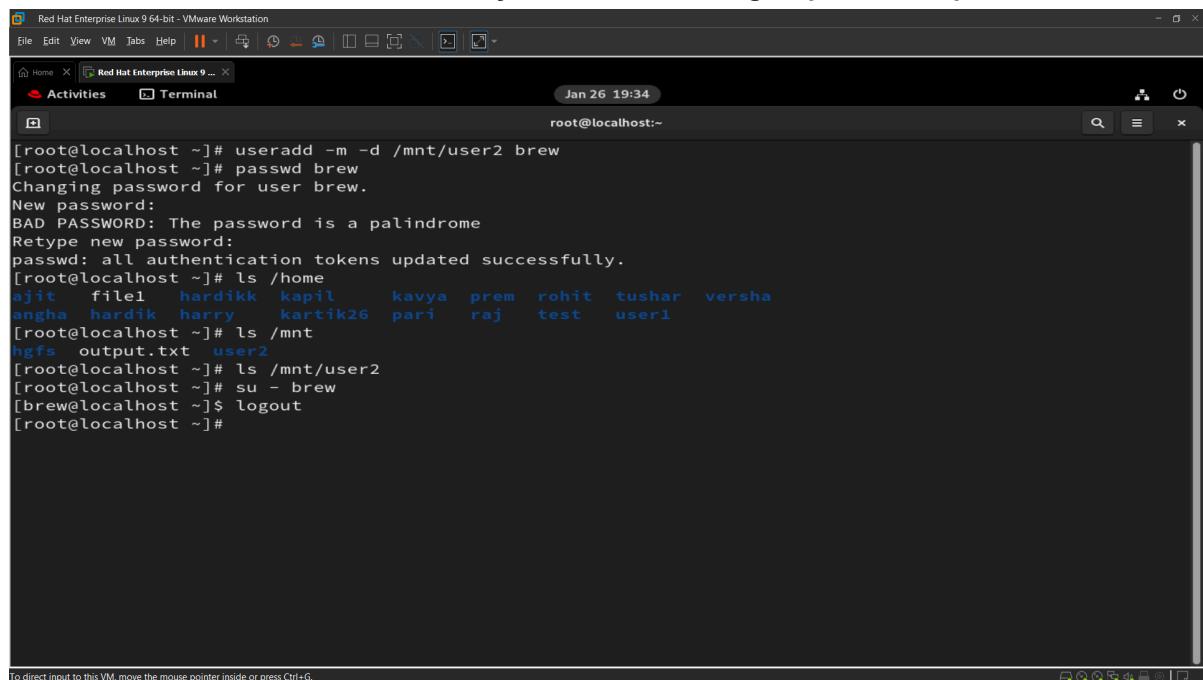
1. Named “alex” with its home directory at /home/user1 and give password “pass1”



The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal session is run as root, indicated by the "root@localhost:~" prompt. The user runs the command "useradd -m -d /home/user1 alex". The output shows the user was created with uid 1646 and gid 1647, and assigned to the group 1647. The user then changes their password, entering "pass1" twice. Finally, the user lists the contents of the "/home" directory, which includes "ajit", "file1", "hardikk", "kapil", "kavya", "prem", "rohit", "tushar", "versha", "angha", "hardik", "harry", "kartik26", "pari", "raj", "test", and "user1".

```
[root@localhost ~]# useradd -m -d /home/user1 alex
[root@localhost ~]# id alex
uid=1646(alex) gid=1647(alex) groups=1647(alex)
[root@localhost ~]# passwd alex
Changing password for user alex.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# ls /home
ajit  file1  hardikk  kapil    kavya  prem   rohit  tushar  versha
angha  hardik  harry   kartik26 pari   raj    test   user1
[root@localhost ~]# ls /home/user1
[root@localhost ~]#
```

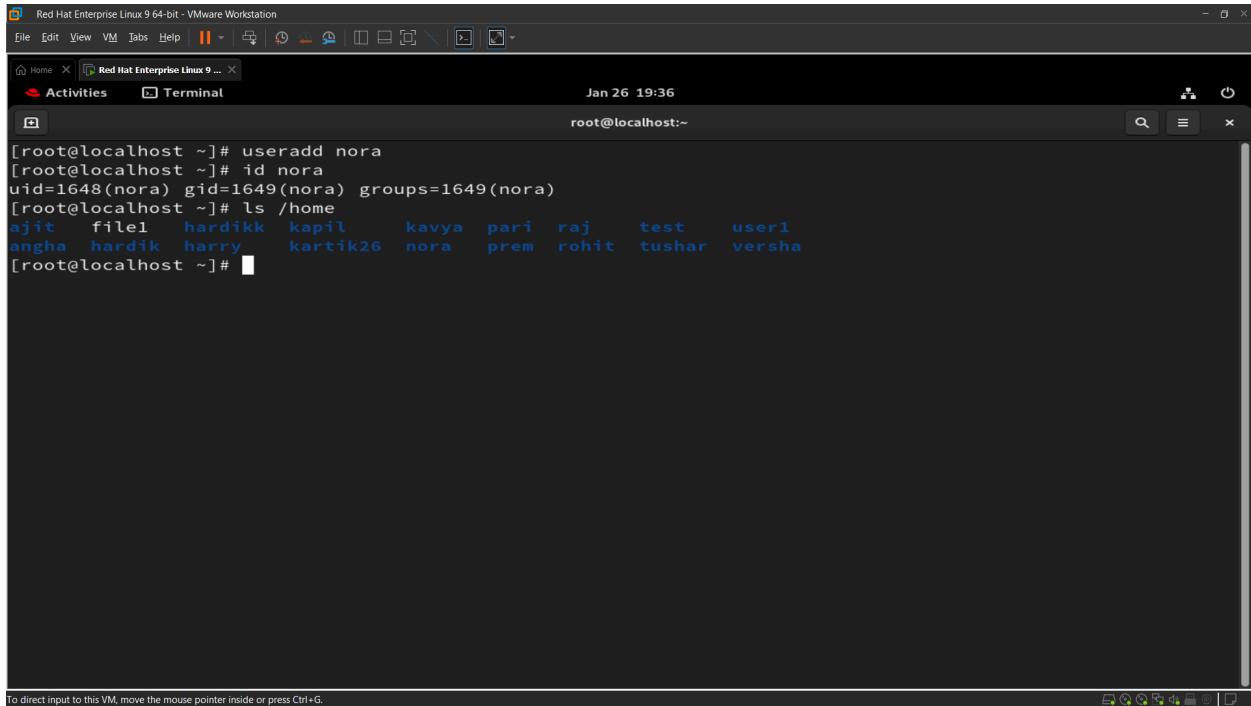
- 2 Named “brew” with its home directory at /mnt/user2 and give password “pass2”.



The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal session is run as root. The user creates a new user named "brew" with the command "useradd -m -d /mnt/user2 brew". They then change the password for "brew" using "passwd brew". After setting the password, they list the contents of the "/home" directory again, showing the same set of files as before. Finally, they list the contents of the "/mnt" directory, which contains "hgfs" and "output.txt". They switch to the "brew" user with "su - brew" and log out with "\$ logout".

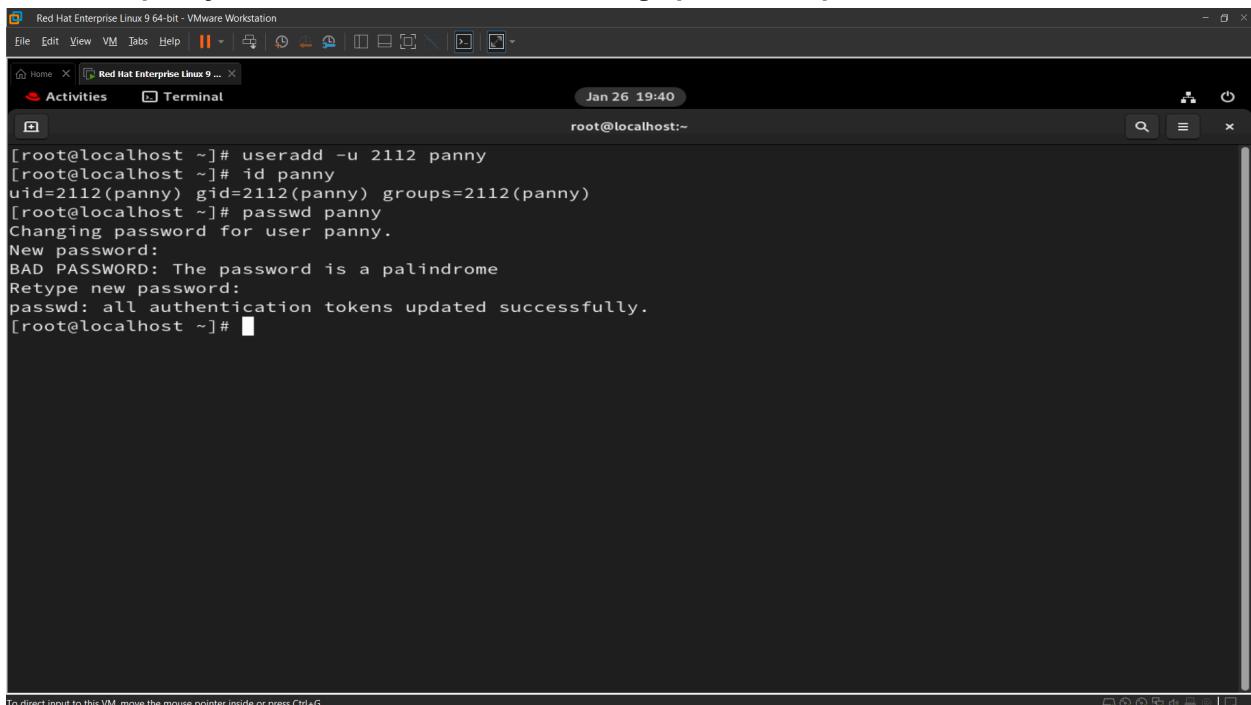
```
[root@localhost ~]# useradd -m -d /mnt/user2 brew
[root@localhost ~]# passwd brew
Changing password for user brew.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# ls /home
ajit  file1  hardikk  kapil    kavya  prem   rohit  tushar  versha
angha  hardik  harry   kartik26 pari   raj    test   user1
[root@localhost ~]# ls /mnt
hgfs  output.txt  user2
[root@localhost ~]# ls /mnt/user2
[root@localhost ~]# su - brew
[brew@localhost ~]$ logout
[root@localhost ~]#
```

3. Named “nora” without its home directory.



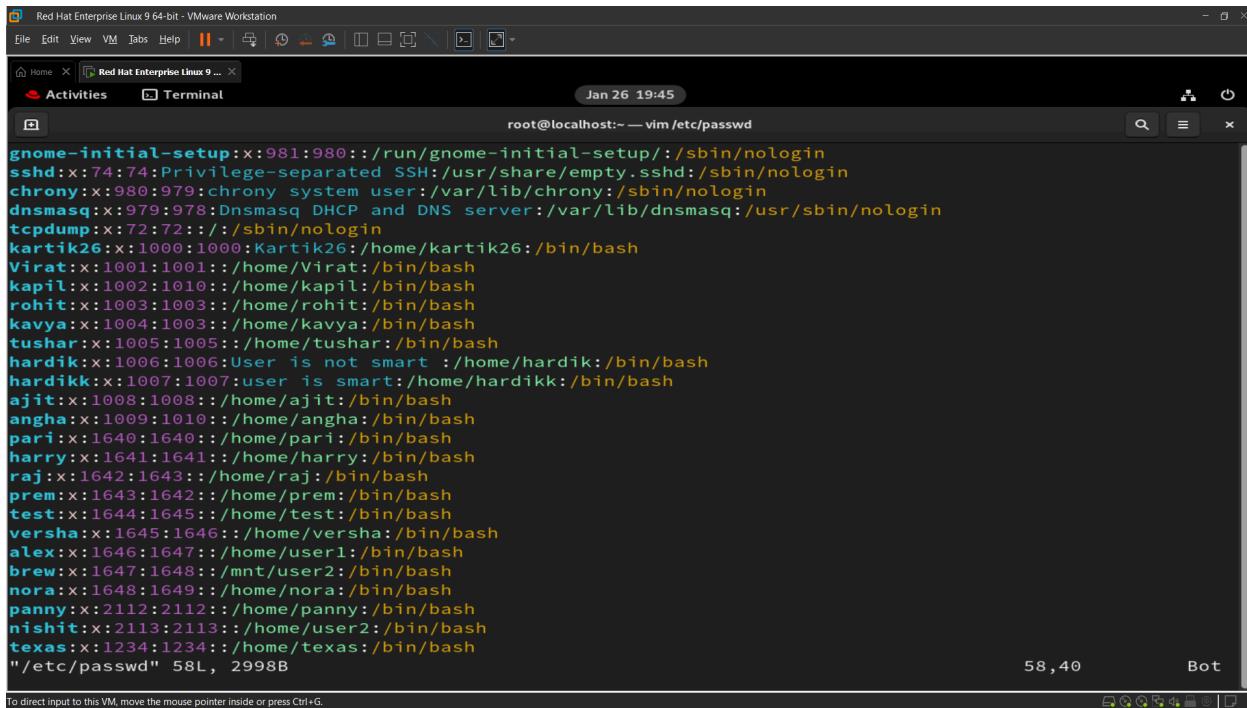
```
[root@localhost ~]# useradd nora
[root@localhost ~]# id nora
uid=1648(nora) gid=1649(nora) groups=1649(nora)
[root@localhost ~]# ls /home
ajit  file1  hardikk  kapil    kavya  pari   raj    test   user1
angha hardik  harry   kartik26  nora   prem   rohit tushar versha
[root@localhost ~]#
```

4. Named “panny” with custom UID 2112, and assign password “pass-4”



```
[root@localhost ~]# useradd -u 2112 panny
[root@localhost ~]# id panny
uid=2112(panny) gid=2112(panny) groups=2112(panny)
[root@localhost ~]# passwd panny
Changing password for user panny.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]#
```

5. Named 'texas' without using the useradd or adduser commands.



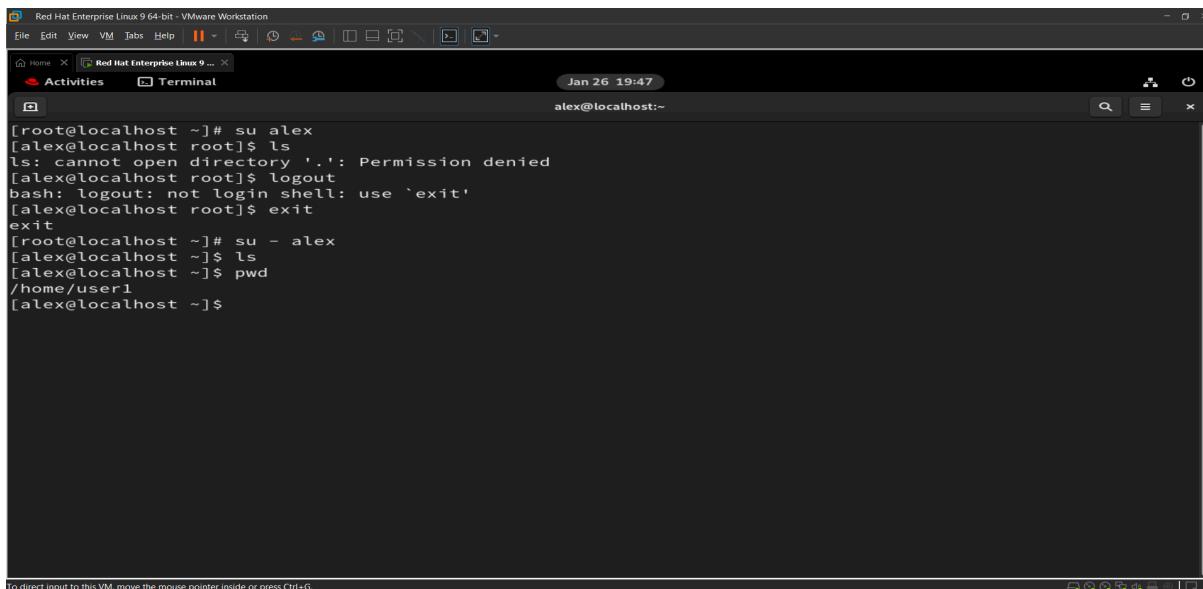
The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 ...". The command "root@localhost:~ — vim /etc/passwd" is run. The terminal displays the contents of the /etc/passwd file, which includes entries for various users like gnome-initial-setup, sshd, chrony, dnsmasq, tcpdump, kartik26, Virat, kapil, rohit, kavya, tushar, hardik, hardikk, ajit, angha, pari, harry, raj, prem, test, versha, alex, brew, nora, panny, nishit, and texas. The entry for "texas" is highlighted in purple. The bottom right corner of the terminal shows the number "58,40" and the word "Bot".

```
gnome-initial-setup:x:981:980::/run/gnome-initial-setup/:sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/usr/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
kartik26:x:1000:1000:Kartik26:/home/kartik26:/bin/bash
Virat:x:1001:1001:/home/Virat:/bin/bash
kapil:x:1002:1010:/home/kapil:/bin/bash
rohit:x:1003:1003:/home/rohit:/bin/bash
kavya:x:1004:1003:/home/kavya:/bin/bash
tushar:x:1005:1005:/home/tushar:/bin/bash
hardik:x:1006:1006:User is not smart:/home/hardik:/bin/bash
hardikk:x:1007:1007:user is smart:/home/hardikk:/bin/bash
ajit:x:1008:1008:/home/ajit:/bin/bash
angha:x:1009:1010:/home/angha:/bin/bash
pari:x:1640:1640:/home/pari:/bin/bash
harry:x:1641:1641:/home/harry:/bin/bash
raj:x:1642:1643:/home/raj:/bin/bash
prem:x:1643:1642:/home/prem:/bin/bash
test:x:1644:1645:/home/test:/bin/bash
versha:x:1645:1646:/home/versha:/bin/bash
alex:x:1646:1647:/home/user1:/bin/bash
brew:x:1647:1648:/mnt/user2:/bin/bash
nora:x:1648:1649:/home/nora:/bin/bash
panny:x:2112:2112:/home/panny:/bin/bash
nishit:x:2113:2113:/home/user2:/bin/bash
texas:x:1234:1234:/home/texas:/bin/bash
"/etc/passwd" 58L, 2998B
```

Q2 : 2. Log in as user alex using the su and su - commands, and explain their differences

su alex: Switches user but retains the current environment.

su - alex: Switches user and starts a new shell session with **alex's** environment.



The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 ...". The user is root. They run "su alex" and get prompted for a password. After entering the password, they run "ls" and get an error message: "ls: cannot open directory '.': Permission denied". Then they run "logout" and "exit". Finally, they run "su - alex" and get a new prompt: "alex@localhost:~". They run "ls" and "pwd" to show they are now in the "/home/user1" directory.

```
[root@localhost ~]# su alex
[alex@localhost root]$ ls
ls: cannot open directory '.': Permission denied
[alex@localhost root]$ logout
bash: logout: not login shell: use `exit'
[alex@localhost root]$ exit
exit
[root@localhost ~]# su - alex
[alex@localhost ~]$ ls
[alex@localhost ~]$ pwd
/home/user1
[alex@localhost ~]$
```

Q3 : Set a password policy for all above users with the following requirements:

- o The maximum password age should be 30 days, and the minimum password age should be 10 days.
- o Set the password expiry date for all users to December 31, 2025.

```
[root@localhost ~]# chage -M 30 -m 10 alex brew nora panny texas
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

[root@localhost ~]# chage -E 2025-12-31 alex brew nora panny texas
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
```

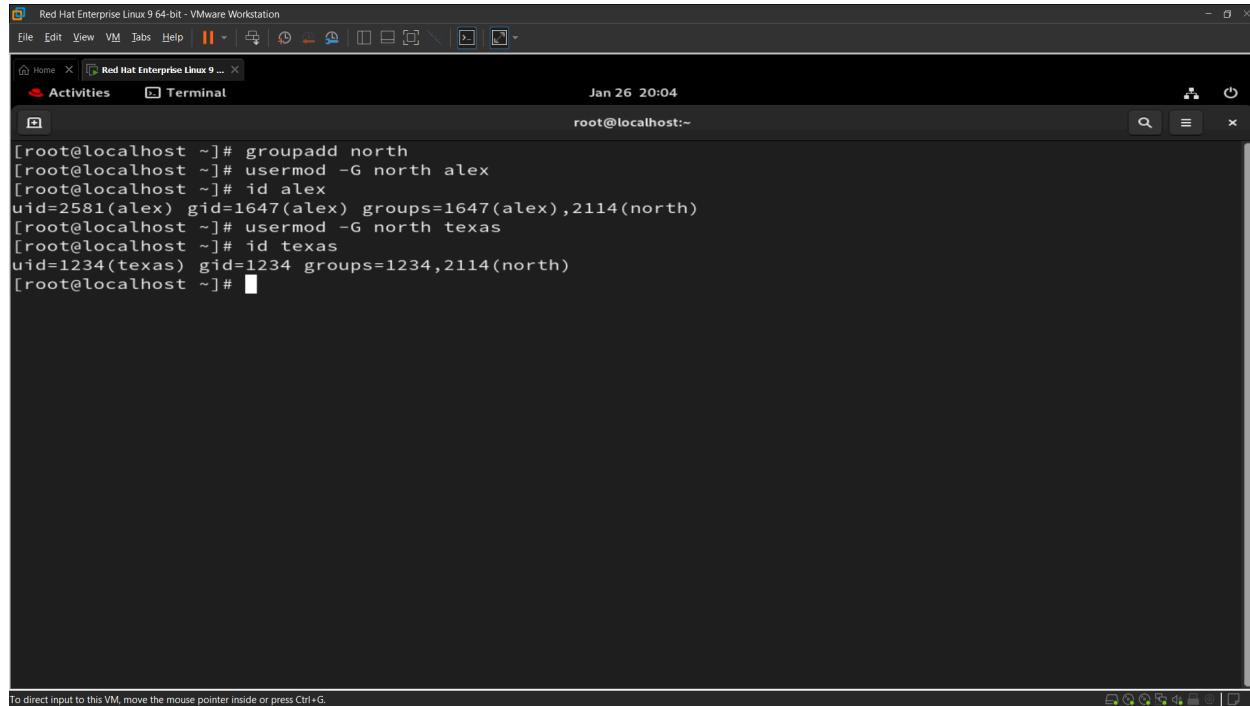
Q4 : . Modify the user "alex":

- Add a comment: "I am alex"
- Change the UID to 2581
- Change the shell to "nologin"

```
[root@localhost ~]# usermod -c " I am alex " alex
[root@localhost ~]# usermod -u 2581 alex
[root@localhost ~]# usermod -s /sbin/nologin alex
[root@localhost ~]# id alex
uid=2581(alex) gid=1647(alex) groups=1647(alex)
[root@localhost ~]# su - alex
This account is currently not available.
[root@localhost ~]#
```

Q5 : Create group with following configuration:

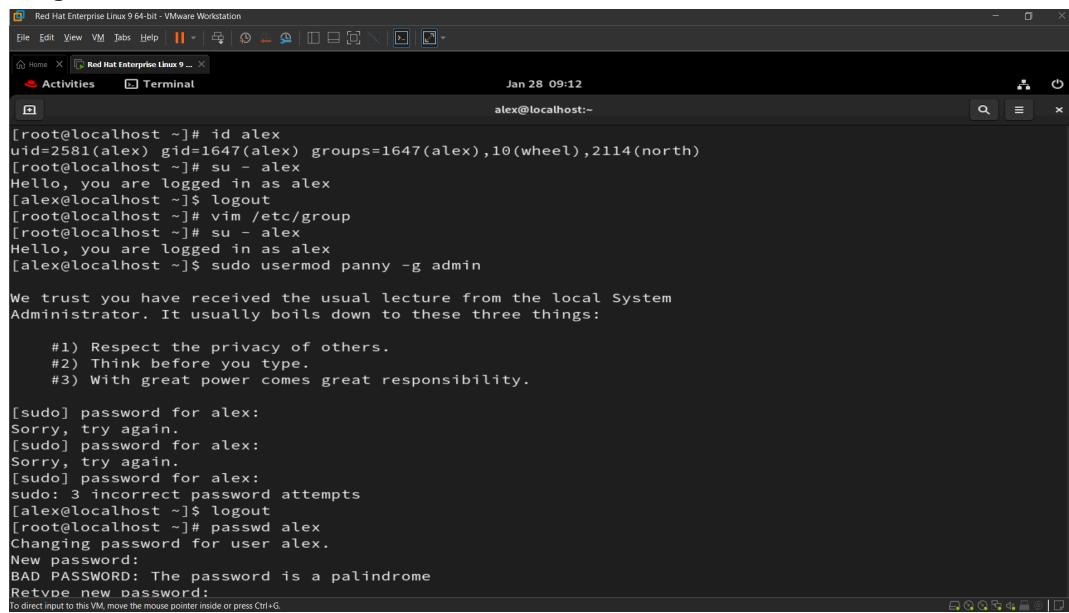
- o Named “north” with secondary group member “alex” & “texas”.
- o Named “south” with GID “2222”.



```
[root@localhost ~]# groupadd north
[root@localhost ~]# usermod -G north alex
[root@localhost ~]# id alex
uid=2581(alex) gid=1647(alex) groups=1647(alex),2114(north)
[root@localhost ~]# usermod -G north texas
[root@localhost ~]# id texas
uid=1234(texas) gid=1234 groups=1234,2114(north)
[root@localhost ~]#
```

Q6 : Grant user Alex administrative privileges through the wheel group so that Alex can add Panny to the admin group without requiring root access.

Image for Q6 :



```
[root@localhost ~]# id alex
uid=2581(alex) gid=1647(alex) groups=1647(alex),10(wheel),2114(north)
[root@localhost ~]# su - alex
Hello, you are logged in as alex
[alex@localhost ~]$ logout
[root@localhost ~]# vim /etc/group
[root@localhost ~]# su - alex
Hello, you are logged in as alex
[alex@localhost ~]$ sudo usermod panny -g admin

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for alex:
Sorry, try again.
[sudo] password for alex:
Sorry, try again.
[sudo] password for alex:
sudo: 3 incorrect password attempts
[alex@localhost ~]$ logout
[root@localhost ~]# passwd alex
Changing password for user alex.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
```

Image for Q6 :

```
[sudo] password for alex:  
Sorry, try again.  
[sudo] password for alex:  
Sorry, try again.  
[sudo] password for alex:  
sudo: 3 incorrect password attempts  
[alex@localhost ~]$ logout  
[root@localhost ~]# passwd alex  
Changing password for user alex.  
New password:  
BAD PASSWORD: The password is a palindrome  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@localhost ~]# su - alex  
Hello, you are logged in as alex  
[alex@localhost ~]# sudo usermod panny -g admin  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for alex:  
[alex@localhost ~]$ id panny  
uid=2112(panny) gid=2223(admin) groups=2223(admin)  
[alex@localhost ~]$
```

Q7 : 7. Change the group name from “south” to “dakshin”.

```
[root@localhost ~]# groupmod -n dakshin south  
[root@localhost ~]# getent group dakshin  
dakshin:x:2222:  
[root@localhost ~]#
```

Q8 : Create a system user named “ping” and check its UID

The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal session is run by root at localhost (~). The user runs the command "useradd -r ping" to create a new system user named "ping". Then, they run "id ping" to check its details, showing it has a uid of 978 and is part of the group "ping". Finally, they run "ls /home" to list all users, and "grep ping /etc/passwd" to find the entry for the new user.

```
[root@localhost ~]# useradd -r ping
[root@localhost ~]# id ping
uid=978(ping) gid=977(ping) groups=977(ping)
[root@localhost ~]# ls /home
ajit  file1  hardikk  kapil    kavya  panny  prem   rohit  tushar  user2
angha  hardik  harry   kartik26  nora   pari   raj    test   user1   versha
[root@localhost ~]# grep ping /etc/passwd
ping:x:978:977::/home/ping:/bin/bash
[root@localhost ~]#
```

Q9 : Create a group named goa with GID 11000. Set this group as the supplementary group for “brew”

The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal session is run by root at localhost (~). The user runs "groupadd -g 11000 goa" to create a new group named "goa" with a GID of 11000. Then, they run "usermod -aG goa brew" to add the "goa" group to the supplementary groups of the user "brew". Finally, they run "id brew" to verify that "brew" now has a uid of 1647, a gid of 1648, and is part of the groups "brew" and "goa".

```
[root@localhost ~]# groupadd -g 11000 goa
[root@localhost ~]# usermod -aG goa brew
[root@localhost ~]# id brew
uid=1647(brew) gid=1648(brew) groups=1648(brew),11000(goa)
[root@localhost ~]#
```

Q10 : Create a group named “prod”. Then, create two users, user2 and user1, and set both the user’s primary group to prod.

```
Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help Jan 26 20:34
Activities Terminal root@localhost:~>

-a, --append      append the user to the supplemental GROUPS
-h, --help        mentioned by the -G option without removing
-l, --login NEW_LOGIN    the user from other groups
-L, --lock         display this help message and exit
-m, --move-home   new value of the login name
-o, --non-unique  lock the user account
-p, --password PASSWORD  move contents of the home directory to the
-R, --root CHROOT_DIR    new location (use only with -d)
-P, --prefix PREFIX_DIR  allow using duplicate (non-unique) UID
-s, --shell SHELL       use encrypted password for the new password
-u, --uid UID         directory to chroot into
-U, --unlock          prefix directory where are located the /etc/* files
-v, --add-subuids FIRST-LAST  new login shell for the user account
-V, --del-subuids FIRST-LAST  new UID for the user account
-w, --add-subgids FIRST-LAST  unlock the user account
-W, --del-subgids FIRST-LAST  add range of subordinate uids
-Z, --selinux-user SEUSER   remove range of subordinate uids
                           new SELinux user mapping for the user account

[root@localhost ~]# usermod -g prod User1
[root@localhost ~]# usermod -g prod User2
[root@localhost ~]# id User1
uid=2583(User1) gid=11001(prod) groups=11001(prod)
[root@localhost ~]# id User2
uid=2584(User2) gid=11001(prod) groups=11001(prod)
[root@localhost ~]#
```

Q11 : Change the password policy for the USER3 and USER4 accounts to expire on 2026-01-15.

```
Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help Jan 26 20:37
Activities Terminal root@localhost:~

[root@localhost ~]# useradd USER3
[root@localhost ~]# useradd USER4
[root@localhost ~]# id USER3
uid=2585(USER3) gid=2585(USER3) groups=2585(USER3)
[root@localhost ~]# id USER4
uid=2586(USER4) gid=2586(USER4) groups=2586(USER4)
[root@localhost ~]# chage -E 2026-01-15 USER3 USER4
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

[root@localhost ~]#
```

Q12 : Configure administrative rights for all members of the Goa group to execute any command as any user.

```
Red Hat Enterprise Linux 9 64-bit - VMware Workstation
File Edit View VM Tabs Help || Back Forward Stop Refresh Home Red Hat Enterprise Linux 9 ...
Activities Terminal Jan 26 20:40
root@localhost:~ — visudo

##      user      MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)        ALL

## 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
%goa    ALL=(ALL)        ALL

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

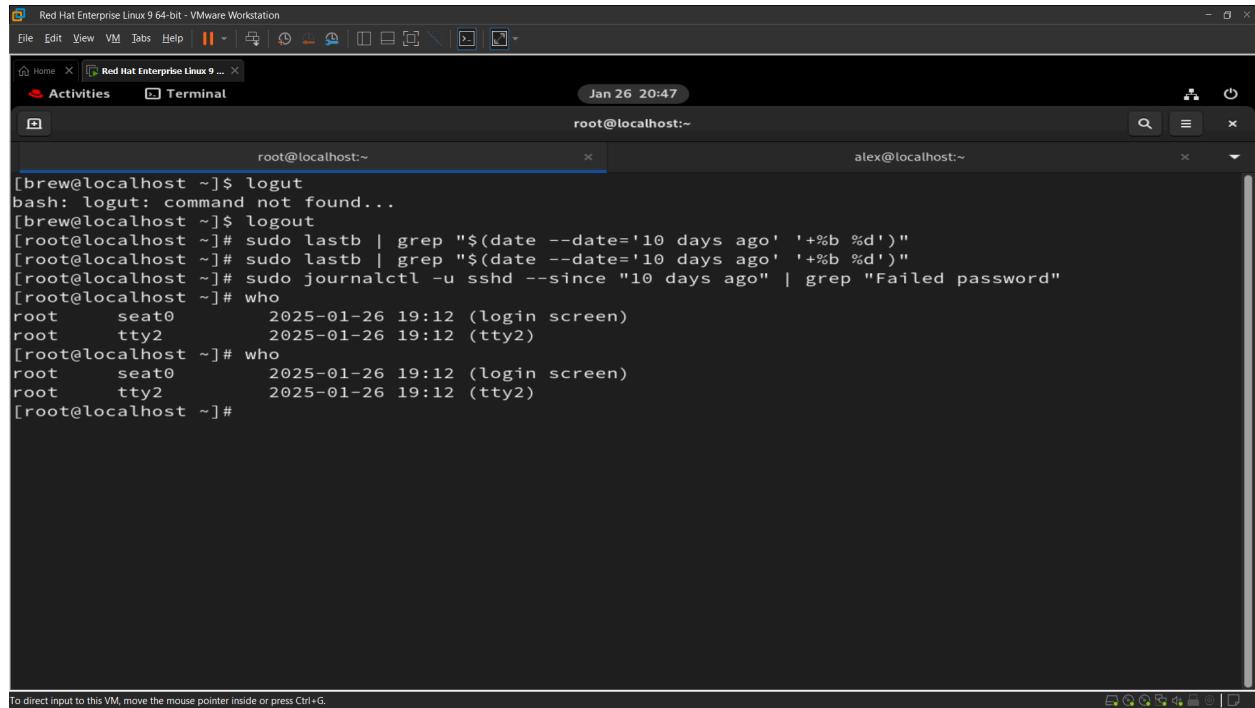
## Allows members of the users group to mount and umount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
:wq
```

Q13 : . How would you check all failed login attempts on the system from the last 10 days? Write the command and display the output.

Q14 : How would you determine how many users are currently logged into the system? Write the command to achieve this.



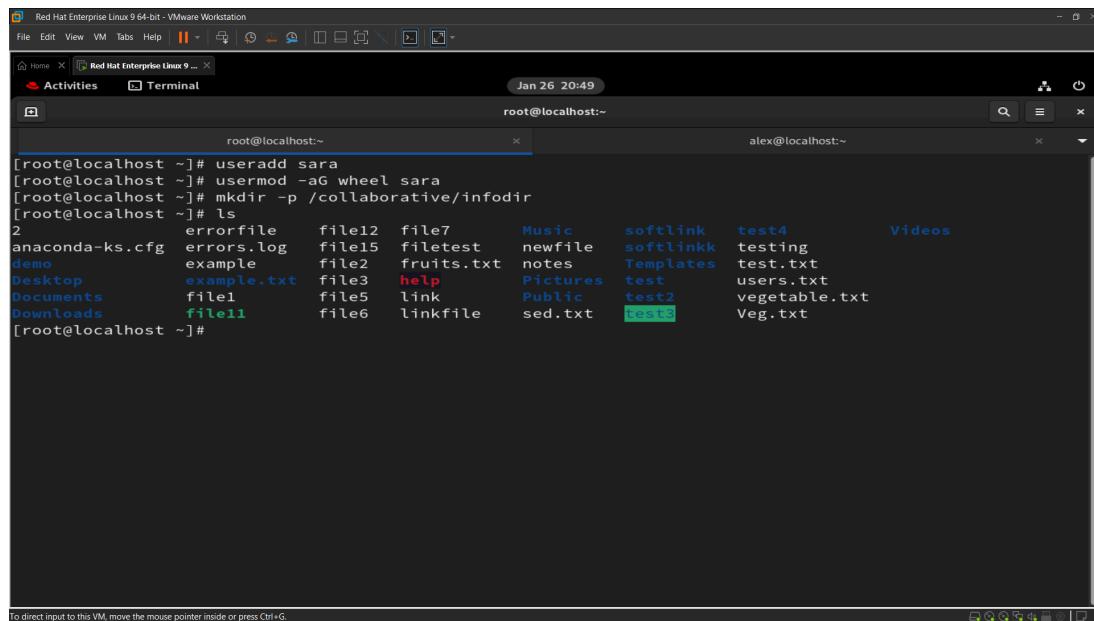
The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal has two tabs: "root@localhost:~" and "alex@localhost:~". The "root" tab displays a series of commands and their outputs:

```
[brew@localhost ~]$ logout  
bash: logout: command not found...  
[brew@localhost ~]$ logout  
[root@localhost ~]# sudo lastb | grep "$(date --date='10 days ago' '+%b %d')"  
[root@localhost ~]# sudo lastb | grep "$(date --date='10 days ago' '+%b %d')"  
[root@localhost ~]# sudo journalctl -u sshd --since "10 days ago" | grep "Failed password"  
[root@localhost ~]# who  
root    seat0        2025-01-26 19:12 (login screen)  
root    tty2        2025-01-26 19:12 (tty2)  
[root@localhost ~]# who  
root    seat0        2025-01-26 19:12 (login screen)  
root    tty2        2025-01-26 19:12 (tty2)  
[root@localhost ~]#
```

The "alex" tab is visible but contains no output. The status bar at the bottom of the terminal window indicates "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

Q15 : Add the user "sara" to the "wheel" group and create a collaborative directory /collaborative/infodir

IMAGE FOR Q15.

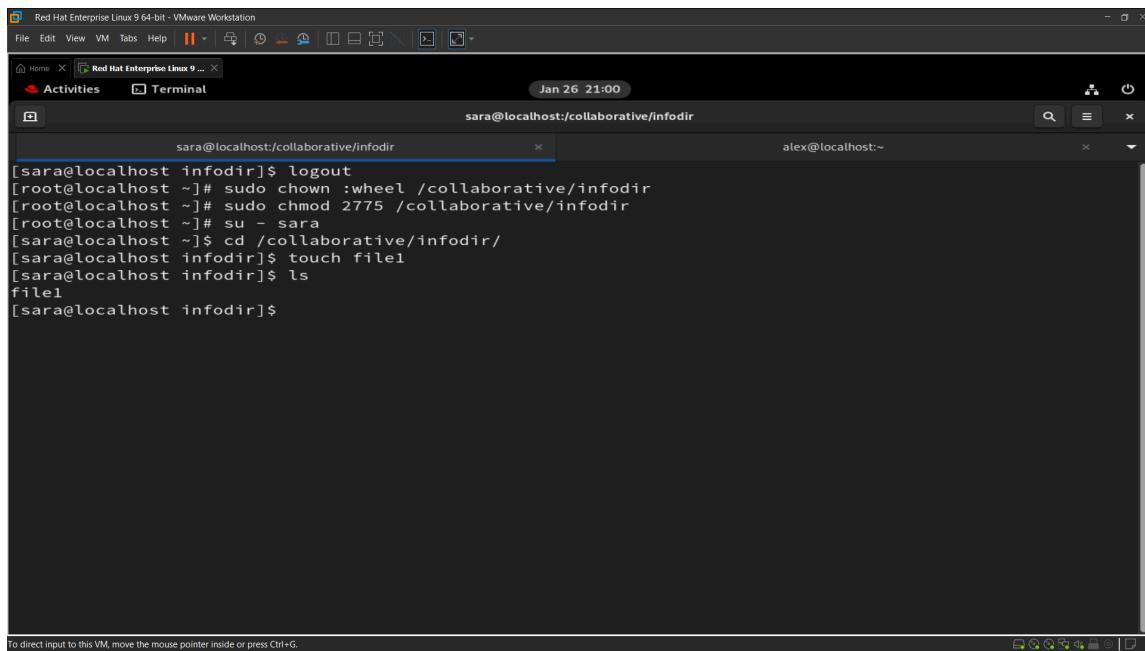


The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal has two tabs: "root@localhost:~" and "alex@localhost:~". The "root" tab displays the following commands and their outputs:

```
[root@localhost ~]# useradd sara  
[root@localhost ~]# usermod -aG wheel sara  
[root@localhost ~]# mkdir -p /collaborative/infodir  
[root@localhost ~]# ls  
2           errorfile   file12  file7      Music      softlink    test4          Videos  
anaconda-ks.cfg  errors.log   file15  filetest  newfile  softlinkk  testing  
demo          example     file2   fruits.txt  notes    Templates  test.txt  
Desktop        example.txt  file3   help       Pictures  test      users.txt  
Documents       file1     file5   link      Public    test2    vegetable.txt  
Downloads      file11    file6  linkfile  sed.txt  test3    Veg.txt  
[root@localhost ~]#
```

The "alex" tab is visible but contains no output. The status bar at the bottom of the terminal window indicates "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

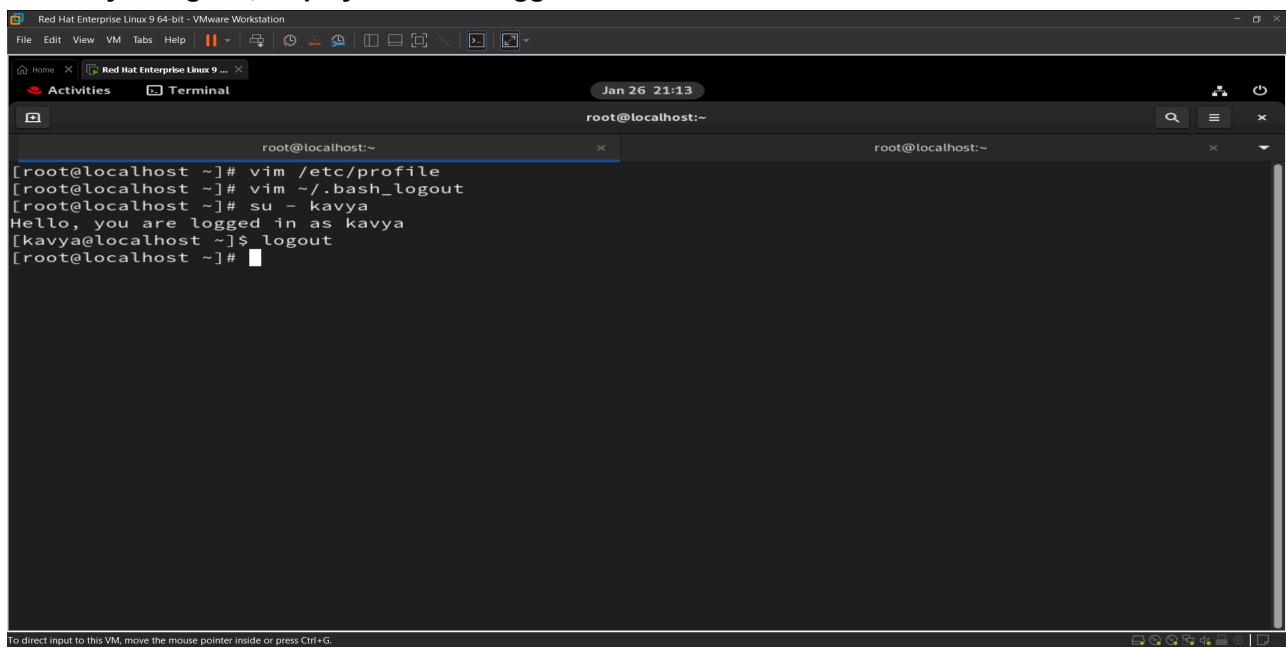
IMAGE FOR Q15



```
sara@localhost infodir]$ logout
[root@localhost ~]# sudo chown :wheel /collaborative/infodir
[root@localhost ~]# sudo chmod 2775 /collaborative/infodir
[root@localhost ~]# su - sara
[sara@localhost ~]$ cd /collaborative/infodir/
[sara@localhost infodir]$ touch file1
[sara@localhost infodir]$ ls
file1
[sara@localhost infodir]$
```

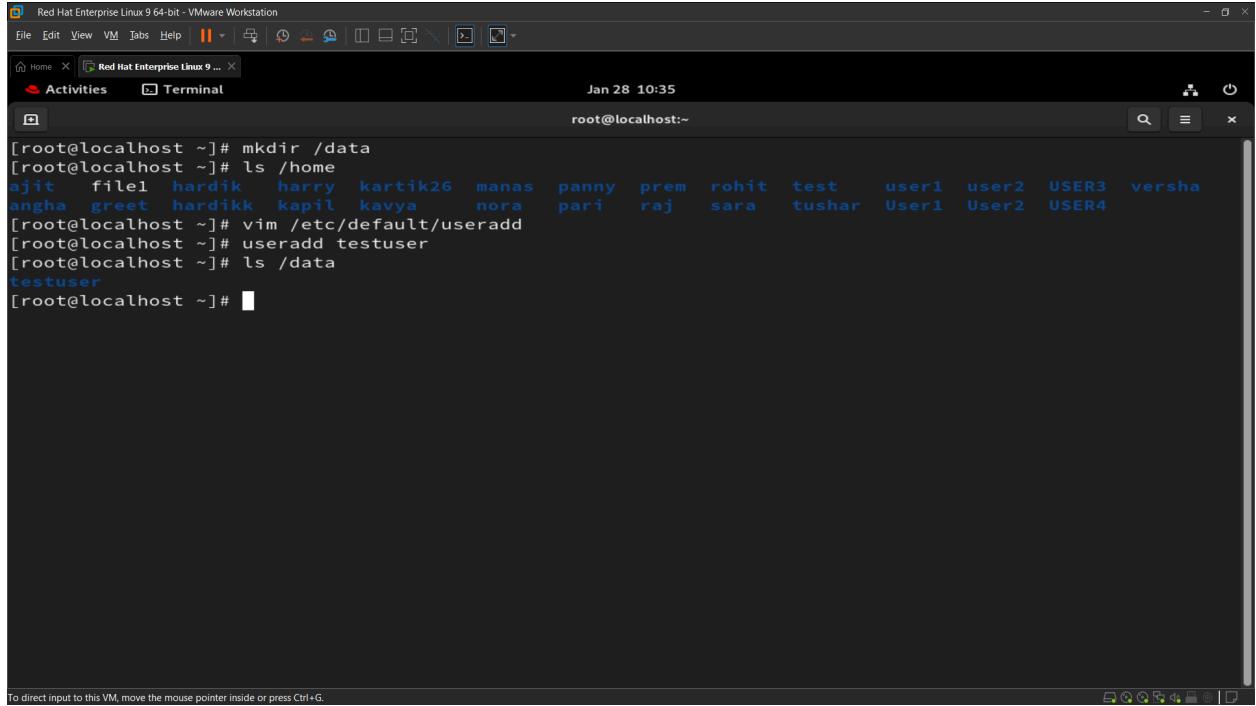
Q16 : 16. Configure login/logout messages:

- o When you log in with a new user, display a message: "Hello, you are logged in as **USER**" (where **USER** is replaced with the logged-in username).
- o When you log out, display: "You are logged out now"



```
root@localhost:~# vim /etc/profile
root@localhost:~# vim ~/.bash_logout
[root@localhost ~]# su - kavya
Hello, you are logged in as kavya
[kavya@localhost ~]$ logout
[root@localhost ~]#
```

Q18 : Create a directory /data and configure the system so that all newly created users get /data as their home directory by default



```
[root@localhost ~]# mkdir /data
[root@localhost ~]# ls /home
ajit  file1  hardik  harry  kartik26  manas  panny  prem  rohit  test  user1  user2  USER3  versha
angha  greet  hardikk  kapil  kavya  nora  pari  raj  sara  tushar  User1  User2  USER4
[root@localhost ~]# vim /etc/default/useradd
[root@localhost ~]# useradd testuser
[root@localhost ~]# ls /data
testuser
[root@localhost ~]#
```

Q19 : Name a file where we can set a file size limit upto 200 MB for a single file.

```
# vim /etc/security/limits.conf
# * soft fsiz 204800 * hard fsiz 204800
```

Q20 : Check the last three users who logged into your system.



```
[root@localhost ~]# ls
2          errorfile  file12  file7      help      Pictures  test      users.txt
anaconda-ks.cfg  errors.log  file15  file99~    link      Public   test2  vegetable.txt
demo          example   file2   file99~    linkfile  sed.txt  test3  Veg.txt
Desktop        example.txt  file3   filee     Music    softlink  test4  Videos
Documents       file1    file5   filetest  newfile  softlinkk testing
Downloads       file11   file6   fruits.txt notes   Templates test.txt
[root@localhost ~]# last -n 3
root        tty2          Tue Jan 28 09:52  still logged in
root        seat0         login screen  Tue Jan 28 09:52  still logged in
kartik26    tty2          Tue Jan 28 09:51 - 09:52  (00:00)

wtmp begins Mon Jan 20 09:49:44 2025
[root@localhost ~]#
```

Q21 : As a system administrator, how would you configure the system to ensure that:

- o Automatically create an instructions.txt file in the home directory of every new user upon account creation.
- o Ensure that the mail directory for every newly created user is set to /home/spool/mail/ by default?"

The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal session is run as root, indicated by the "root@localhost:~" prompt. The user runs several commands to demonstrate the creation of a new user and the generation of a welcome message file:

```
[root@localhost ~]# sudo echo "Welcome to your new account! Please read the instructions carefully." > /etc/skel/instructions.txt
[root@localhost ~]# useradd testuser1
[root@localhost ~]# ls /home/testuser1
instructions.txt
[root@localhost ~]# cat /home/testuser1/instructions.txt
Welcome to your new account! Please read the instructions carefully.
[root@localhost ~]#
```

The terminal window has a dark background with light-colored text. It includes standard Linux navigation icons at the top and bottom. A status bar at the bottom indicates "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

Q22 : Delete some users o Named 'alex' and 'brew' with its all data contents including mail data.

The screenshot shows a terminal window titled "Red Hat Enterprise Linux 9 64-bit - VMware Workstation". The terminal session is run as root, indicated by the "root@localhost:~" prompt. The user runs commands to delete the users "alex" and "brew" and then checks if they still exist using the "id" command:

```
[root@localhost ~]# userdel -r alex
[root@localhost ~]# userdel -r brew
[root@localhost ~]# id alex
id: 'alex': no such user
[root@localhost ~]# id brew
id: 'brew': no such user
[root@localhost ~]#
```

The terminal window has a dark background with light-colored text. It includes standard Linux navigation icons at the top and bottom. A status bar at the bottom indicates "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."