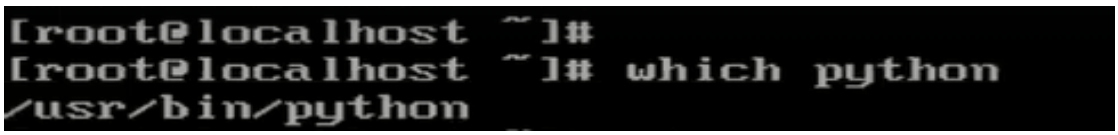
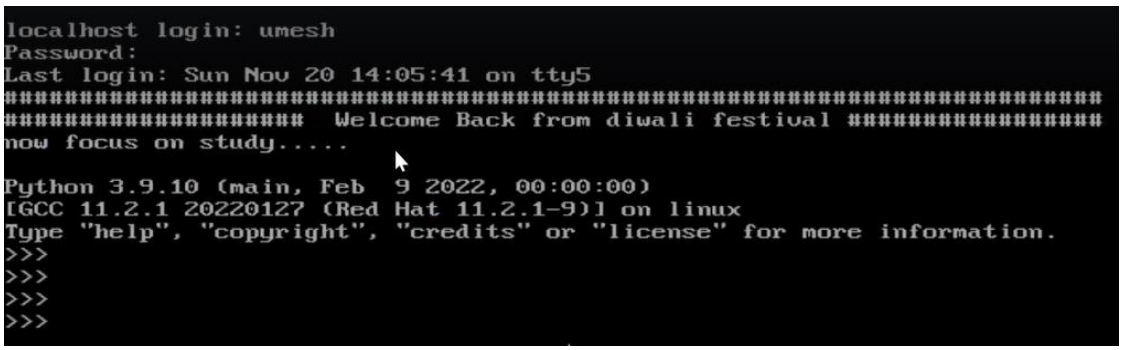
RHEL9

Session 8 – 20th Nov 2022 Summary

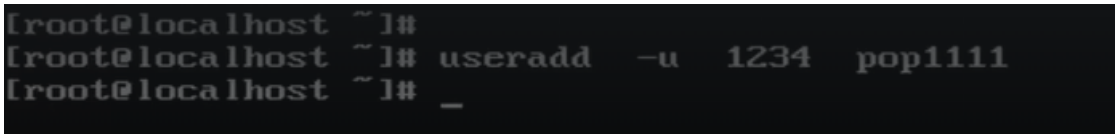
- There are three different users in linux
  - **Admin users** – unlimited power with UID 0
  - **General users**- limited power with UID > 1000 – 60000
  - **Service or System users** – that is used by processes with UID (1 - 999) or (> 60000 – 65335)
- The users can be created as per the application specific that is for testing, deploying applications, run program etc.
- The command to check the location of "python" command is "**which python**"



- The command used to open the "/etc/passwd" file is "**vim /etc/passwd**", the user "umesh" account is dedicated to run python program

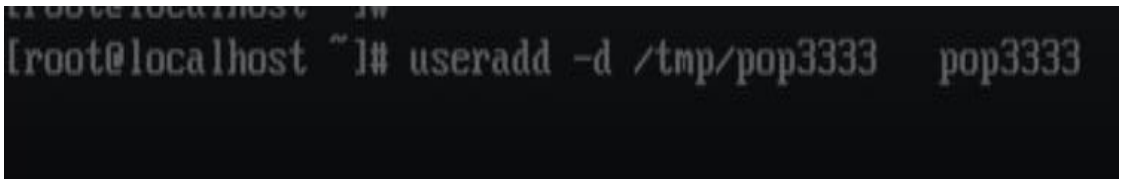


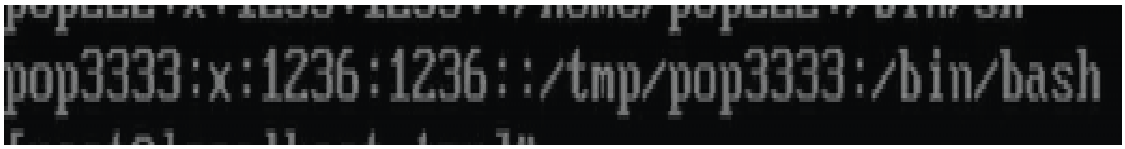
- The command used to create a user “pop1111” with a specific UID 1234 is “**useradd –u 1234 pop1111**”

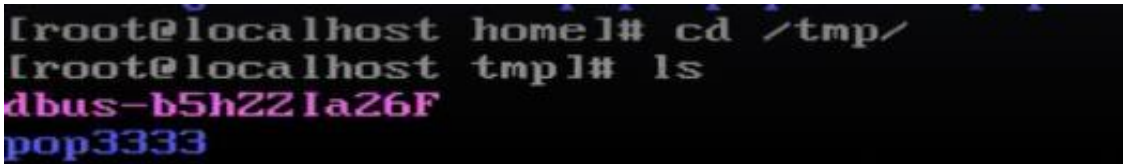


- The command used to create a user “pop222” with a specific shell “sh” is “**useradd –s /bin/sh pop222**”

- The command used to create a user “pop3333” with a specific home directory “/tmp/pop3333” is “**useradd –d /tmp/pop3333 pop3333**”

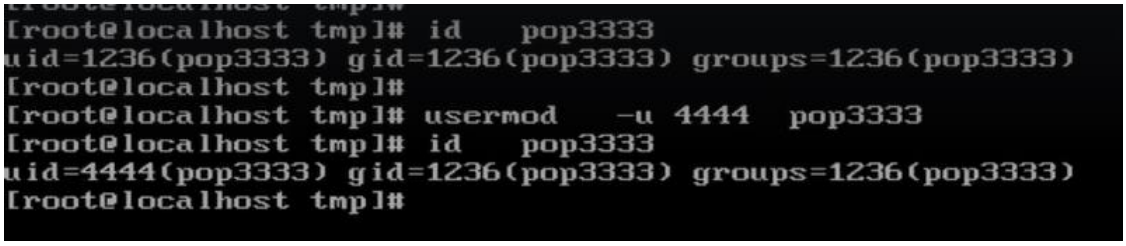


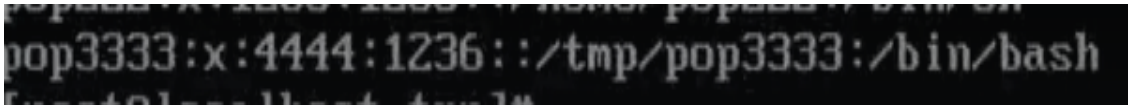




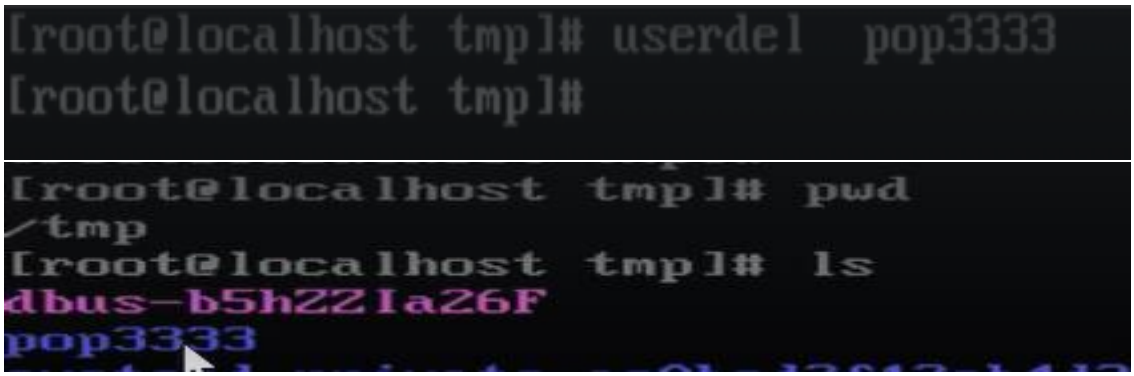
- The command used to modify the information of the pre-created users is “**usermod**” command

- The command used to change the UID of user “pop3333” to “4444” is “**usermod –u 4444 pop3333**”

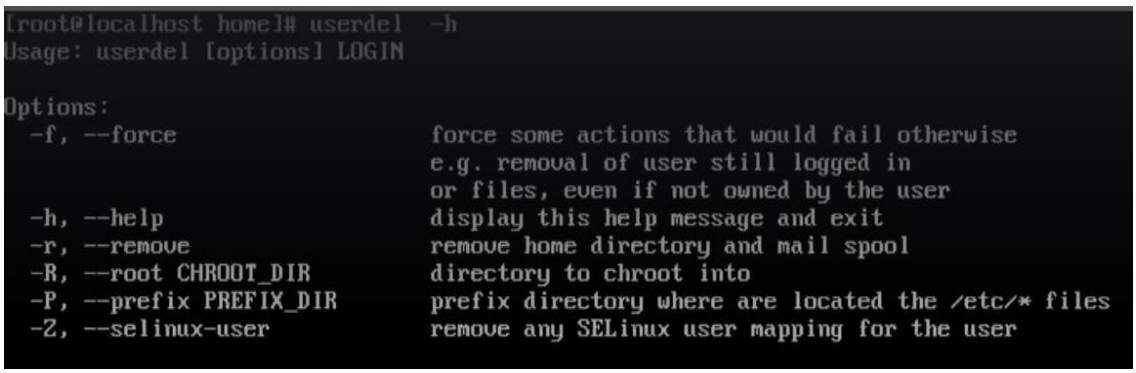




- The command used to delete the user “pop3333” is “**userdel pop3333**”, the user home directory is not deleted, while deleting user if you want to delete the home directory we can use “-r” option in the “userdel” command. Ex:- “**userdel –r user_name**”

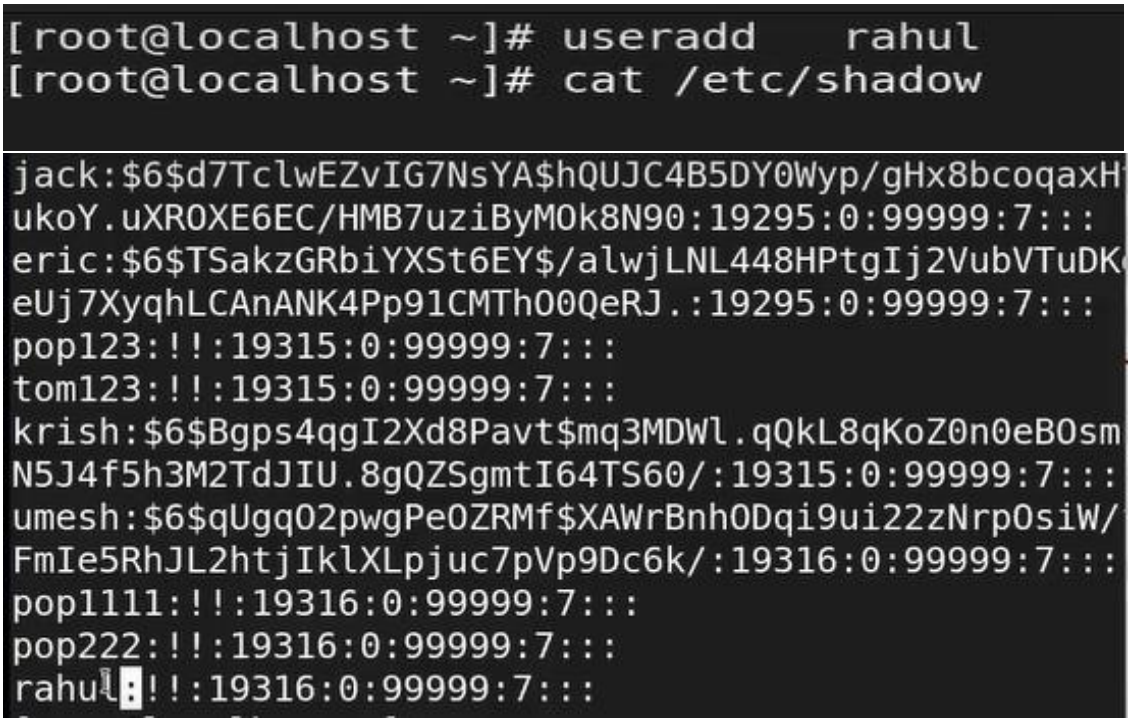


- To see more options of “userdel” command is “userdel –h”



- The “**useradd**” command is used to create users, behind the scene it updates the files such as “/etc/passwd”, “/etc/shadow”, “/etc/group” etc

- The "**/etc/shadow**" file has the database of all users, every line is the information of a particular user, it has **nine fields** separated by colon(:) called as **field separator**



- The seven fields are separated by colon (:)
    - First field - **User name or Login name**
    - Second field- **Password** – not readable by general users, this field is updated by passwd command. The symbol "!" , means password is locked
    - Third field- the date when the **password was last changed**
    - Fourth field- **Minimum password age**- "0" – multiple times password can be changes by the user
    - Fifth field **– Maximum password age** – password expiry
    - Sixth field – **Warning** – "7" – means before 7 days of password expiry there will be a warning
    - Seventh field- **Password Inactive-** this field is empty – this means after password expires the password never becomes inactive. Suppose if you specify "2" here, it means after 2 days of password expiry, it becomes inactive.
    - Eight field – **Account Expiry** - this field is empty – this means that account is never expired.
    - Ninth field – **Reserved** for future use.
- The command used to give the password for a user "rahul" is "**passwd rahul"**

```
[root@localhost ~]# passwd  rahul
Changing password for user rahul.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfu
```

- The password is updated in the "/etc/shadow" file, the command used to print the file "**cat /etc/shadow**", here the password stored in hash format that is "sha512" algorithm.

```
[root@localhost ~]# cat /etc/shadow
```

```
eric:$6$TSakzGRbiYXSt6EY$/alwjLNL448HPtgIj2VubVTuDK
eUj7XyqhLCAnANK4Pp91CMThO0QeRJ.:19295:0:99999:7:::
pop123:!!:19315:0:99999:7:::
tom123:!!:19315:0:99999:7:::
krish:$6$Bgps4qgI2Xd8Pavt$mq3MDWl.qQkL8qKoZ0n0eBOsm
N5J4f5h3M2TdJIU.8gQZSgmtI64TS60/:19315:0:99999:7:::
umesh:$6$qUgqO2pwgPeOZRMf$XAWrBnhODqi9ui22zNrpOsiW/
FmIe5RhJL2htjIklXLpjuc7pVp9Dc6k/:19316:0:99999:7:::
pop1111:!!:19316:0:99999:7:::
pop222:!!:19316:0:99999:7:::
rahul:$6$Strr38BmnVhJY7kY$IURguYlLaYLSRv9lFebv5frqC
sXnMrcEmn5N4Ub.s5hW7xAAT2Lr4h51:19316:0:99999:7:::
```

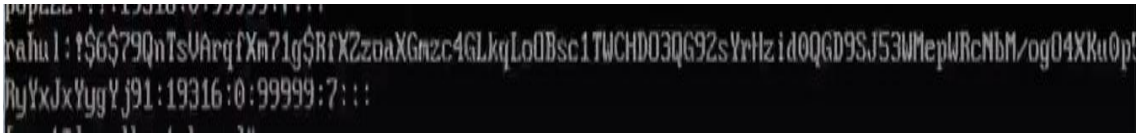
- The command to **remove** the password for the user "rahul" is "**passwd –d rahul**"

```
[root@localhost home]# passwd  -d rahul
Removing password for user rahul.
passwd: Success
```

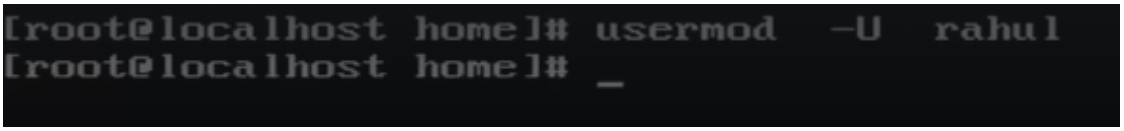
```
rahul::19316:0:99999:7:::
```

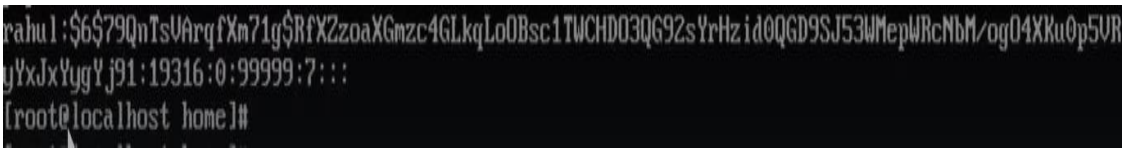
- The command to **lock** the password of a user "rahul" is "**usermod –L rahul**"

```
[root@localhost home]#
[root@localhost home]# usermod  -L  rahul
[root@localhost home]#
```

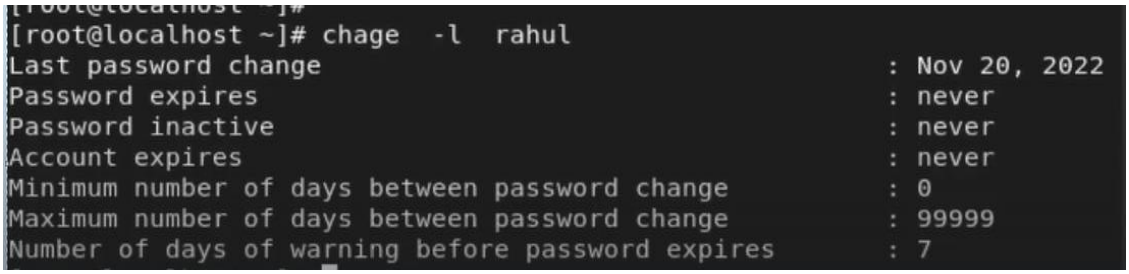


- The command to **unlock** the password of a user "rahul" is "**usermod –U rahul**"





- The **chage** command gives information of a user in "/etc/shadow" in simple human readable format



- The command to see the manual of the file "/etc/shadow" is "man 5 shadow"

- To restrict the user "rahul" to not change the password for next 5 days – this can be directly specified in the **fourth field** in the "/**etc/shadow**" file

- Now if user "rahul" login and tries to change the password, it is restricted to change the password

```
localhost login: rahul
Password:
Last login: Sun Nov 20 14:48:09 on tty4
################################################################################
#####################  Welcome Back from diwali festival ######################
now focus on study.....

[rahul@localhost ~]$ passwd
Changing password for user rahul.
Current password:
You must wait longer to change your password.
Current Password: _
```

- The command to change the number of days of **warning** to 50 before password expires of a user "rahul" is "**chage –W 50 rahul**"

```
[root@localhost ~]# chage -W  50  rahul
[root@localhost ~]# _
```

```
[root@localhost ~]# chage -l  rahul
Last password change                                    : Nov 20, 2022
Password expires                                        : Jan 19, 2023
Password inactive                                       : Jan 21, 2023
Account expires                                         : Nov 19, 2022
Minimum number of days between password change          : 2
Maximum number of days between password change          : 60
Number of days of warning before password expires       : 50
[root@localhost ~]#
```

- The default login information is stored in a file **"/etc/login.defs"**

```
[root@localhost ~]#
[root@localhost ~]# vim  /etc/login.defs
```

```
# Default initial "umask" value used by login(1) on non-PAM enabled systems.
# Default "umask" value for pam_umask(8) on PAM enabled systems.
# UMASK is also used by useradd(8) and newusers(8) to set the mode for new
# home directories if HOME_MODE is not set.
# 022 is the default value, but 027, or even 077, could be considered
# for increased privacy. There is no One True Answer here: each sysadmin
# must make up their mind.
UMASK           022

# HOME_MODE is used by useradd(8) and newusers(8) to set the mode for new
# home directories.
# If HOME_MODE is not set, the value of UMASK is used to create the mode.
HOME_MODE       0700

# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes
#       PASS_MIN_LEN    Minimum acceptable password length.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   9999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

# Currently PASS_MIN_LEN is not supported

# Currently SU_WHEEL_ONLY is not supported

# Currently CRACKLIB_DICTPATH is not supported

#
# Min/max values for automatic uid selection in useradd(8)
#
UID_MIN                  1000
UID_MAX                 60000
```