The encrypted passwords and other information such as password expiry information (the password aging information) are stored in /etc/shadow file. All fields are separated by a colon (:) symbol. It contains one entry per line for each user listed in /etc/passwd file. Generally, shadow file entry looks as follows:

Text

Description automatically generated with medium confidence

The order is as follows:

1. **Username** : It is your login name.
2. **Password** : It is your encrypted password hash. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to $id$salt$hashed, The $id is the algorithm used On GNU/Linux as follows:
   1. **$1$** is MD5
   2. **$2a$** is Blowfish
   3. **$2y$** is Blowfish
   4. **$5$** is SHA-256
   5. **$6$** is SHA-512
3. **Last password change (lastchanged)** : Days since Jan 1, 1970 that password was last changed
4. **Minimum** : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5. **Maximum** : The maximum number of days the password is valid (after that user is forced to change his/her password)
6. **Warn** : The number of days before password is to expire that user is warned that his/her password must be changed
7. **Inactive** : The number of days after password expires that account is disabled
8. **Expire** : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used.

A password hash is nothing but a string that verifies the integrity of your password during login against the stored hash so that your actual password never has to be held in /etc/shadow file. It is a security feature.

How to view the contents of the /etc/shadow file

The normal user cannot access the /etc/shadow file directly. For example, try out the following [cat command](https://www.cyberciti.biz/faq/linux-unix-appleosx-bsd-cat-command-examples/?utm_source=Linux_Unix_Command&utm_medium=faq&utm_campaign=nixcmd):  
$ cat /etc/shadow  
Sample outputs:

cat: /etc/shadow: Permission denied

You can only access the /etc/shadow file via few commands such as the passwd command. Login as root user and execute cat command on /etc/shadow file:  
$ su -  
Provide root user password when prompted:

Password:

Try to display the file:  
# cat /etc/shadow  
Sample outputs:

root: $1$s83Ugoff$EDT83WAAFpCQHWDp07E9Ux:0:99999:7:::

daemon:\*:13031:0:99999:7:::

bin:\*:13031:0:99999:7:::

Here is how my encrypted password hash looks on Linux:

vivek:$6$LONG\_STRING\_HASH\_HERE1:18770:0:99999:7:::

We can use the chage command to get account aging information in easy to understand format:  
chage -l vivek  
And now I see:

Last password change : May 23, 2021

Password expires : never

Password inactive : never

Account expires : never

Minimum number of days between password change : 0

Maximum number of days between password change : 99999

Number of days of warning before password expires : 7

Each each entry in the /etc/shadow (or outputs from the chage command) is divided into following fields:

* vivek – Login name
* $6$LONG\_STRING\_HASH\_HERE1 – Encrypted password hash
* never – Days since Jan 1, 1970 that password was last changed
* 99999 – Days before password may be changed
* never – Days after which password must be changed
* 7 – Days before password is to expire that user is warned
* never – Days after password expires that account is disabled
* 0 – Days since Jan 1, 1970 that account is disabled

Of course you can use the sudo command as follows:  
$ sudo cat /etc/shadow  
Or [grep command](https://www.cyberciti.biz/faq/howto-use-grep-command-in-linux-unix/?utm_source=Linux_Unix_Command&utm_medium=faq&utm_campaign=nixcmd) along with the sudo:  
$ sudo cat /etc/shadow | grep vivek  
Please note that FreeBSD uses /etc/master.shadow file.

Say hello to getent command

To get entries from Name Service Switch libraries use the getent command. The syntax is:  
getent database key  
getent [option] database key  
Where database can be:

1. passwd – Read user account info.
2. shadow – Read user password info.
3. group – Read group info.
4. key – Can be a user name/group name.

Examples

getent passwd  
getent passwd vivek  
getent group  
getent group vivek  
sudo getent shadow  
sudo getent shadow vivek

Conclusion

Now you know where are the passwords of the users located in Linux. I suggest that you read the following man pages using the [man command](https://bash.cyberciti.biz/guide/Man_command?utm_source=Linux_Unix_Command&utm_medium=faq&utm_campaign=nixcmd):  
$ man getent  
$ man 5 shadow  
$ man 5 passwd