OSOC

1.

**Grep**is an acronym that stands for **G**lobal **R**egular **E**xpression **P**rint.

Grep is a Linux / Unix command line tool used to search for a string of characters in a specified file. The text search pattern is called a regular expression. When it finds a match, it prints the line with the result.

SYNTAX: grep[options] pattern [files]

Options:

**-c** : This prints only a count of the lines that match a pattern

**-h :** Display the matched lines, but do not display the filenames.

**-i :** Ignores, case for matching

**-l :** Displays list of a filenames only.

**-n :** Display the matched lines and their line numbers.

**-v :** This prints out all the lines that do not matches the pattern

**-e exp :** Specifies expression with this option. Can use multiple times.

**-f file :** Takes patterns from file, one per line.

**-E :** Treats pattern as an extended regular expression (ERE)

**-w :** Match whole word

**-o :** Print only the matched parts of a matching line,

with each such part on a separate output line.

2

“-rw-rw-r-x"it is a string contain 10 characters.

**-** means it’s a regular file

**2 to 4** characters represent file permissions for user/owner.

**5 to 7** characters represent file permissions for groups.

**8 to 10** characters represent file permissions for others.

r stands for read.

w stands for write.

x stands for execute.

There are grouped into three sets that represent different levels of ownership:

1 **Owner or user permissions**

After the directory (d) slot, the first set of three characters indicate permission settings for the owner (also known as the user).

In the example **-rw-r--r--**, the owner permissions are **rw-,** indicating that the owner can read and write to the file but can't execute it as a program.

In the example drwxr-xr-x, the owner permissions are rwx, indicating that the owner can view, modify, and enter the directory.

**2 Group permissions**

The second rwx set indicates the group permissions. In the fourth column of the example above, group1 is the group name.

In the example -rw-r--r--, group members can only read the file.

In the example drwxr-xr-x, group members can view as well as enter the directory.

**3 Other permissions**

The final rwx set is for "other" (sometimes referred to as "world"). This is anyone outside the group. In both examples above, these are set to the same permissions as the group.

To change file and directory permissions, use the command**chmod** (change mode). The owner of a file can change the permissions for user (u), group (g), or others (o) by adding (+) or subtracting (-) the read, write, and execute permissions.

There are two basic ways of using**chmod** to change file permissions: The symbolic method and the absolute form.

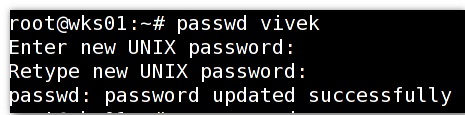
**5.**

1. A normal user may only change the password for his/her own account.
2. The **superuser (root user)** may change the password for**any account or specific account**.
3. The passwd command also changes the account or associated password validity period.

First, login as the root user. Use sudo -s or su - command to login as root. To change password of specific user account, use the following syntax:

|  |
| --- |
| **passwd** userNameHere |

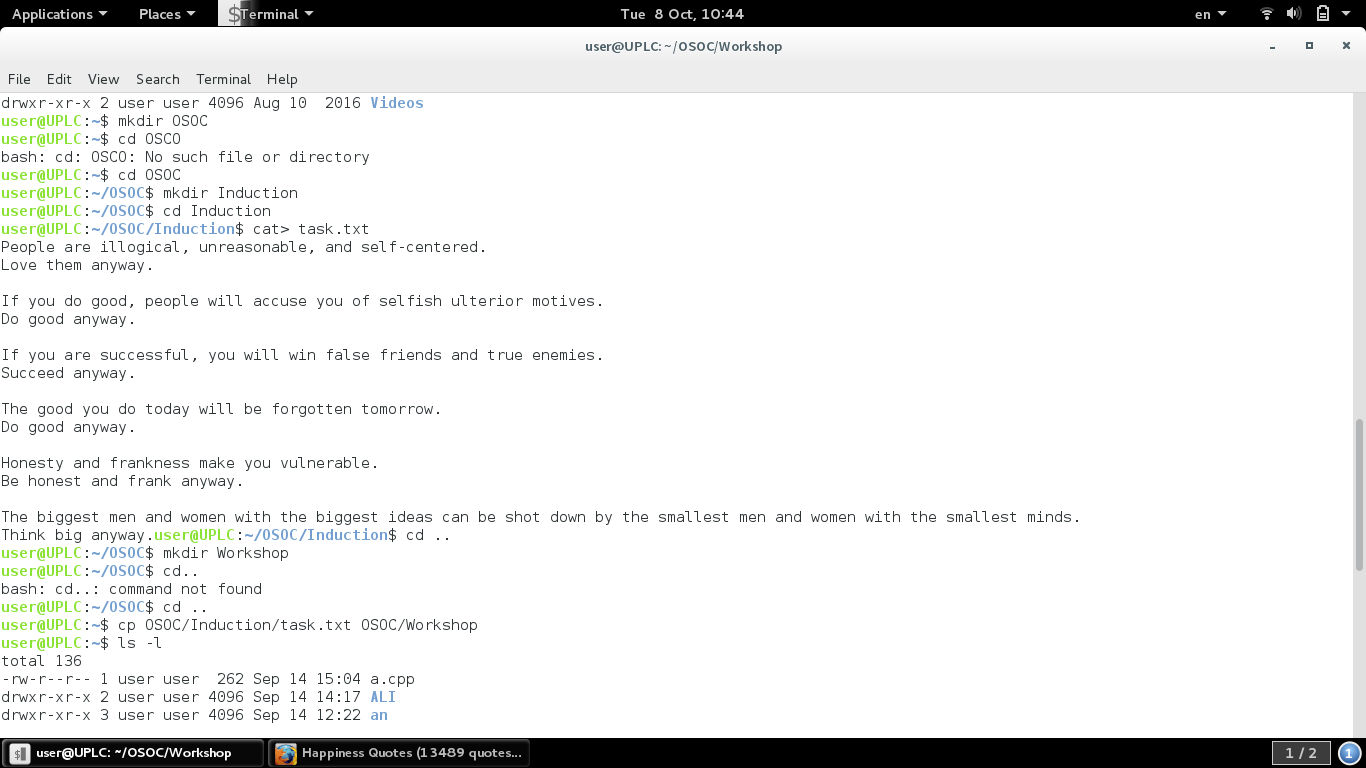
To change the password for user called vivek, enter:  
# passwd vivek

****

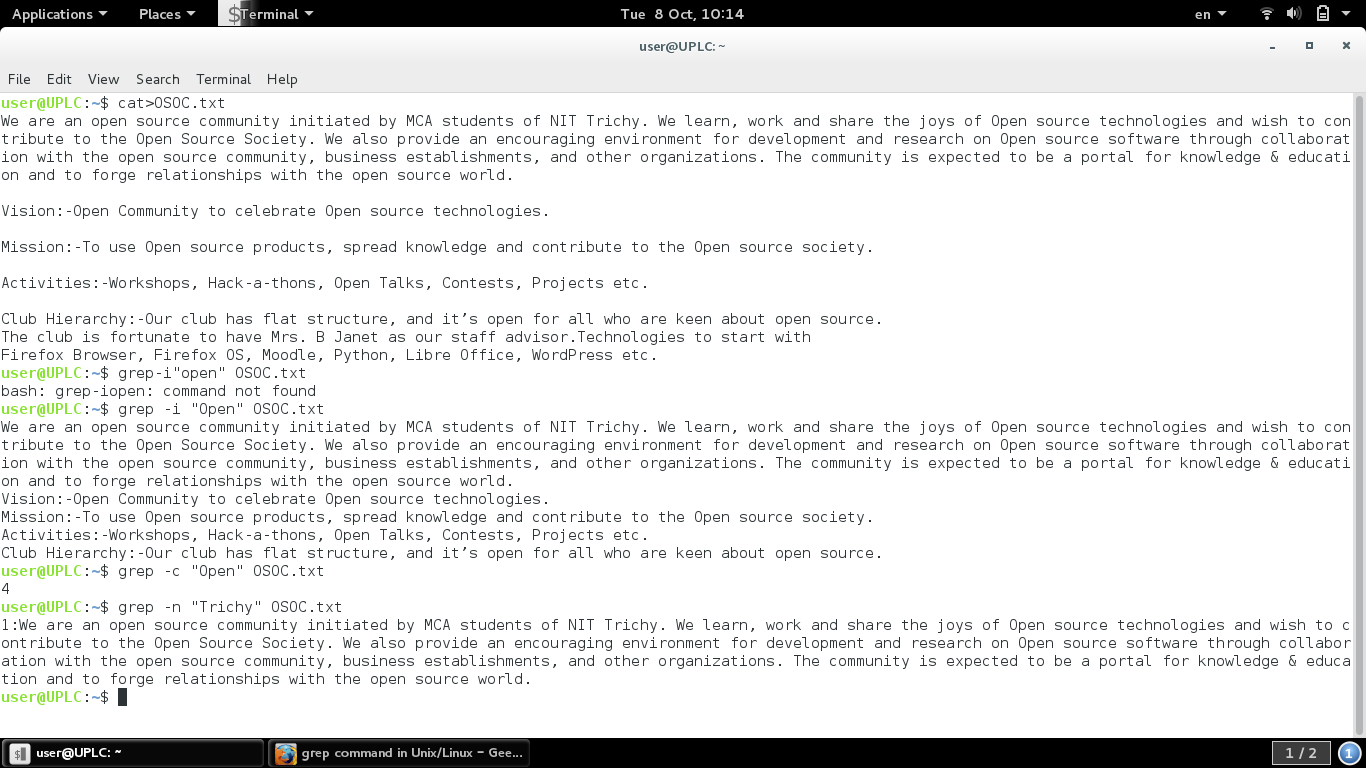
To see password status of any user account, enter:  
# passwd -S userNameHere  
# passwd -S vivek

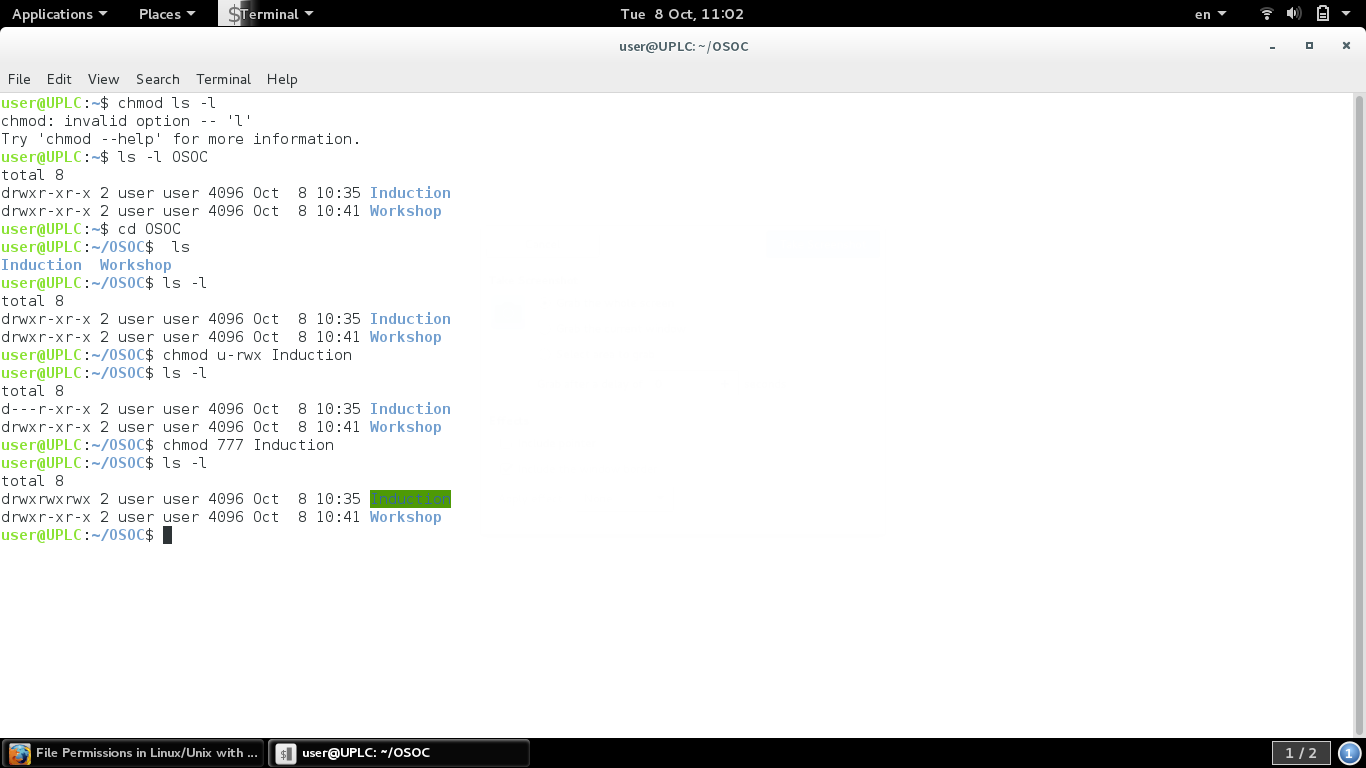
3

****

****

**1**

****

**2**