User id, password. * Usernames and password stored in /etc/passwd and /etc/shadow file respectively

* When you supplies password, it encrypts and compare with password stored in /etc/shadow, which is also in encrypted format. If both are equal, you are in.

* You can obtain your user id and other information using id command.

$ id

Outputs- uid=1002(vivek) gid=1002(vivek) groups=1002(vivek), 0(wheel)

Numbers are used to represent users and groups in Linux kernel. ① simplified user and group mgt ② security mgt easy ③ your uid applied to all files you create.

* Zero UID is special and used by the root user.
* GID is used by Linux to refer group names.
* Single user can be member of multiple groups.
* The wheel group used as power user group.
* Zero GID value enjoys the unrestricted/unlimited access to Linux system
* Effective user ID (EUID) - It is used to determine what level of access the current process has.

$ whoami
$ id -un

* Real user ID: It is used to identify who you actually are.
  * It can not be changed till your session terminates.
  * only root (or person having zero UID) can change the RUID.

$ id -ru

* The Saved User ID (SUID): * When new process/executable file such as passwd, started the effective user id that is in force at the time is copied to the saved id.

* Because of this feature, you are able to update your own password stored in /etc/shadow file.

* off course, executable file must have set-user-id bit on in order to set uid (system call).

* Before process ending itself it switches back to SUID.

Managing Group Access: * Linux groups are a mechanism to manage a collection of computer system users.

* Groups can be assigned to logically tie users together for a common security, privilege and access purpose.

Set file, directory and device permissions:

* These can be set to allow or deny access to members of their own group or all others.
* Modification of the file, directory and device access is achieved with the chmod command.
* The permissions can be assigned in octal notation or in the more easily recognized character format where the command form is: chmod [ugoa] [+-=] [rwxXst] file/directory name

u - User access
g - Group access
o - Other system users access
a - Equivilent to "ugo"
w - permission to delete or modify

+ All access
- Remove access
= Access explicitly assigned
r - permission to read a file

x permission to execute a file

User id, password. * Usernames and password stored in /etc/passwd and /etc/shadow file respectively

* When you supplies password, it encrypts and compare with password stored in /etc/shadow, which is also in encrypted format. If both are equal, you are in.

* You can obtain your user id and other information using id command.

$ id

Outputs. uid=1002(vivek) gid=1002(vivek) groups=1002(vivek), 0(wheel)

Numbers are used to represent users and groups in Linux Kernel. ① Simplified user and group mgt ② security mgt easy ③ your uid applied to all files you create.

* Zero UID is special and used by the root user.
* GID is used by Linux to refer group names.
* Single user can be member of multiple groups.
* The wheel group used as power user group.
* Zero GID value enjoys the unrestricted/unlimited access to Linux system
* Effective user ID (EUID) - It is used to determine what level of access the current process has.

$ whoami
$ id -un.

* Real user ID: It is used to identify who you actually are.
  * It can not be changed till your session terminates.
  * only root (or person having zero UID) can change the RUID.

$ id -ru