**Have ROOT password control:**

Open a terminal window. To do so, press Ctrl+Alt+T,[[1]](https://www.wikihow.com/Change-the-Root-Password-in-Linux#_note-1)which will open a new terminal window with a command prompt in most Linux desktop environments.

Type sudo su at the command prompt, and press ↵ Enter.[[2]](https://www.wikihow.com/Change-the-Root-Password-in-Linux#_note-2)A Password: line will open below the command prompt. (password = cybersecurity)

Type the current root password, then press ↵ Enter. When the password is accepted, you’ll be brought back to the command prompt as the root user.

* If you type the password incorrectly, run su and try again.
* Passwords are case-sensitive.

**Important commands:**

**Whoami** = determins the current user

**Su** = switches to the user you want to switch too. Su root or su sally

**Sudo** = invokes the root user for one command only

**Sudo** -l = lists the sudo privileges for a user

**Visudo** = edits the sudoers file

**ID Commands:**

Linux associates a specific number with each user, known as the user ID (UID).

* **Groups**: get group info for the user. Example mike
* **Usermod**: lock Mike’s account to prevent him from logging in or you can remove Mike from the general group.
* **Deluser**: delete the user example: deluser –remove-home
* **Delgroup**: delete the general group
* **Adduser**: Create the new user. Example Josephsud
* **Addgroup**: create a new group. Example developer group
* **Usermod**: add the user joseph to the developer group
* **Sudo** -i = takes you to root so you can write in root

**What is hashing?**

Hashing is a one-way process. The hashed result cannot be reversed to expose the original data. The checksum is a string of output that is a set size. Technically, that means that hashing is not encryption because encryption is intended to be reversed (decrypted).

Hash is stored in the shadow file: /etc/shadow

When a user logs in, the hash of the submitted password is compared to the hash stored in the ect/shadow.

**ls**: a word list of potential passwords that create hashes for each password. Password cracking tools cannot revearse a password hash.

**A hash is a cryptographic function that takes data as input and translates it to a string of different, seemingly random data.**

**Password: Apple34Pie Hash: 597de3854al4600**

So basically a HASH is a more secure password that the computer changes so people cant actually see your password but the computer knows your password.

<http://www.openwall.com/john/clear>

A picture containing text, screenshot, screen

Description automatically generated

So to run John:

Run sudo nano (name of file)

Run sudo john (name of file)

--show = this will show you the passwords that you have cracked

rm -r (recursive) will delete all folders inside a folder

<https://gtfobins.github.io>

**Open a terminal window.** To do so, press Ctrl+Alt+T,[[1]](https://www.wikihow.com/Change-the-Root-Password-in-Linux#_note-1)which will open a new terminal window with a command prompt in most Linux desktop environments.

**Type sudo su at the command prompt, and press ↵ Enter.**[[2]](https://www.wikihow.com/Change-the-Root-Password-in-Linux#_note-2)A Password: line will open below the command prompt. (password = cybersecurity)

**Type the current root password, then press ↵ Enter.** When the password is accepted, you’ll be brought back to the command prompt as the root user.

* If you type the password incorrectly, run su and try again.
* Passwords are case-sensitive.

**--show command**

sudo john --show /etc/shadow

sudo john (the password crack file) –show and the absolute path

or

sudo john --show shadow\_copy