**Consigna Clase 12 con Ubuntu**

**¿Que es un usuario root en Linux?**

El usuario root en Linux es una cuenta predeterminada que tiene privilegios de acceso a todos los ficheros y comandos del sistema. El usuario root es el superusuario que más tiene privilegios en Linux.

El usuario root puede hacer lo que quiera en el sistema operativo, así que hay que utilizarlo con mucho cuidado porque podríamos llegar a dejar nuestro sistema inutilizable por un comando mal ejecutado

**¿Por qué ubuntu no me deja establecer la contraseña durante la instalación?**

Por defecto, root no tiene contraseña y la cuenta de root está bloqueada hasta que le dé una contraseña. Cuando se instala Ubuntu, se pide crear un usuario con una contraseña. Si se le da a este usuario una contraseña tal como se solicitó, esta es la contraseña que se necesita para la cuenta root.

La cuenta root está deshabilitada de forma predeterminada, lo que significa que root no tiene contraseña. Ubuntu está usando sudo – sudo permite a los “usuarios normales” ejecutar comandos con privilegios de superusuario y “ejecutar” sudo están usando su propia contraseña.

**¿Cuáles son los procesos típicos de Linux (demonios)?**

Un [demonio](http://es.wikipedia.org/wiki/Demonio_(inform%C3%A1tica)) o servicio es un programa que se ejecuta en segundo plano, fuera del control interactivo de los usuarios del sistema ya que carecen de interfaz con estos. El término [demonio](http://es.wikipedia.org/wiki/Demonio_(inform%C3%A1tica)) se usa fundamentalmente en sistemas UNIX y basados en UNIX, como GNU/Linux o Mac OS X. En Windows y otros sistemas operativos se denominan servicios porque fundamentalmente son programas que ofrecen servicios al resto del sistema.

El sistema generalmente inicia los demonios durante el arranque, siendo las funciones más comunes de estos las de ofrecer servicios a otros programas, ya sea respondiendo a las peticiones que llegan a través de la red o atendiendo a procesos que se ejecutan en el mismo sistema, así como responder ante cierta actividad del hardware. Por ejemplo, *acpid* maneja el apagado del sistema cuando el usuario pulsa el botón de encendido del equipo. Algunos demonios sirven para configurar hardware como es el caso de *udevd* en algunos sistemas GNU/Linux ejecutar tareas planificadas como hace *cron* o realizar otras funciones similares.

**¿Cómo identificarlos?**

Tradicionalmente en sistemas UNIX y derivados los nombres de los demonios terminan con la letra *d*. Por ejemplo *syslogd* es el demonio que implementa el registro de eventos del sistema, mientras que *sshd* es el que sirve a las conexiones SSH entrantes.

**Cómo establecer una contraseña para el usuario root**

**Por qué el usuario root está deshabilitado**

Debido al gran poder y peligro que tiene el usuario root, en Ubuntu y otras distribuciones basadas en Ubuntu viene deshabilitado por defecto.

En realidad no es necesario tener permisos root para las tareas diarias como navegar por internet, programar, editar vídeos, fotografías o audios. Si quisiéramos instalar cualquier programa o hacer algo que requiere más permisos de los que tiene nuestro usuario podríamos utilizar el comando *sudo*.

## **Cómo ejecutar un comando como root**

En Linux es necesario ejecutar ciertos comandos como root porque si no, nos dará error de permisos con nuestro usuario. ¿Y cómo se ejecuta un comando en Linux como root? Simplemente utilizando *sudo.* Por ejemplo, para actualizar nuestro sistema operativo tenemos que ejecutar el comando apt update. Sin embargo, sin s*udo* nos dirá que no tenemos permisos suficientes para ello, Sin embargo, si introducimos *sudo* nos pedirá nuestra contraseña y ya podremos ejecutar el comando.

sudo es un programa muy potente que permite a cada usuario que lo utilice ejecutar comandos con permisos de administrador.

## **Cómo pasar a ser usuario root**

Aunque acabamos de mencionar que utilizando sudo podemos ejecutar cualquier comando con permisos de administrador, a veces necesitamos ejecutar múltiples comandos y es un poco tedioso tener que estar poniendo sudo delante de cada uno de ellos y luego introducir de nuevo la contraseña de nuestro usuario. Para hacer el proceso más cómodo, podemos hacer login directamente como root con el comando *sudo -i.*

Es importante fijarse en que cuando estamos utilizando la consola como usuario root, el último carácter antes de introducir nuestro comando es una almohadilla #.

Por otra parte, para volver a utilizar nuestro usuario basta con introducir el comando exit.

## **Cómo habilitar el usuario root**

Ahora que ya sabemos que el usuario root está deshabilitado por defecto, para habilitarlo simplemente tenemos que asignarle una contraseña con el siguiente comando, pero cuidado, no te recomiendo hacer este paso porque como se te olvide la contraseña de root podrías perder el acceso:

sudo passwd root

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

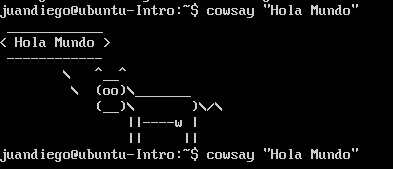
Introducimos la contraseña deseada dos veces y ya habremos terminado.

## **Cómo deshabilitar el usuario root**

Para bloquear de nuevo el usuario root en Linux simplemente hay que introducir el siguiente comando:

sudo passwd -dl root

**cowsay “ Hola mundo “**



**fortune**

