**Actividad en clase 12 con Ubuntu**

**¿Qué es un usuario root en Linux?**

En Linux, el usuario "root" es el usuario administrativo de más alto nivel en el sistema. También se le conoce como el "superusuario" o el "administrador del sistema". El usuario root tiene todos los privilegios y permisos en el sistema, lo que le permite realizar cualquier acción, acceder y modificar cualquier archivo o configuración, y ejecutar comandos de administración que están restringidos para otros usuarios regulares.

Características clave del usuario root:

1. Privilegios completos: El usuario root tiene privilegios de lectura, escritura y ejecución en todos los archivos y directorios del sistema, incluyendo aquellos que son críticos para el funcionamiento del sistema operativo.
2. Acceso a funciones de administración: El usuario root puede realizar tareas de administración del sistema, como instalar y desinstalar software, configurar servicios del sistema, administrar usuarios y permisos, modificar la configuración de red, realizar copias de seguridad, etc.
3. Mayor riesgo y responsabilidad: Dado que el usuario root tiene un control absoluto sobre el sistema, también conlleva un mayor riesgo. Un mal uso o un comando incorrecto por parte del usuario root puede causar daños irreversibles en el sistema.
4. Precaución recomendada: Es importante tener precaución al utilizar la cuenta de root y reservar su uso solo para tareas que requieran privilegios administrativos. Es recomendable utilizar una cuenta de usuario regular para las tareas diarias, y solo cambiar al usuario root cuando sea necesario.

Por razones de seguridad, muchos comandos y acciones en Linux requieren privilegios de root y pueden necesitar ser ejecutados con el comando sudo (SuperUser DO) por parte de un usuario regular. Esto proporciona una capa adicional de protección, ya que requiere que los usuarios autoricen explícitamente el acceso de administrador antes de ejecutar comandos sensibles.

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

Este enfoque es parte de la filosofía de seguridad de Ubuntu y está diseñado para promover prácticas seguras de administración del sistema. Al no tener una contraseña establecida para la cuenta de root, se evita el uso indiscriminado de esa cuenta, lo que ayuda a prevenir accesos no autorizados y reduce el riesgo de errores graves o daños en el sistema causados por usuarios sin experiencia.

Cuando se necesita realizar tareas administrativas, como instalar software o configurar el sistema, se puede utilizar el comando sudo. Al ejecutar un comando con sudo, se pedirá la contraseña de cuenta de usuario regular para verificar su identidad antes de otorgar privilegios temporales de administración.

**¿Cuáles son los procesos típicos de Linux?**

En un sistema Linux, hay varios procesos que son comunes y esenciales para el funcionamiento del sistema operativo. Estos son algunos de los procesos típicos que se pueden encontrar:

1. Init (init/systemd): Es el primer proceso que se ejecuta cuando se inicia el sistema. Es responsable de iniciar y gestionar otros procesos y servicios del sistema.
2. Kernel (kthreadd): Es el núcleo del sistema operativo Linux. Controla todos los recursos del hardware y brinda servicios a los procesos en ejecución.
3. Systemd (systemd): Es un sistema de inicio y administración de servicios que reemplaza al antiguo init en muchas distribuciones modernas de Linux. Es responsable de iniciar y supervisar los servicios del sistema.
4. CROND (cron): Es un demonio responsable de ejecutar tareas programadas automáticamente según una programación específica. Se utiliza para automatizar tareas recurrentes como copias de seguridad, actualizaciones y otros procesos periódicos.
5. Network Manager (NetworkManager): Es un proceso encargado de gestionar y configurar la conectividad de red en el sistema, incluyendo la administración de interfaces de red, conexiones inalámbricas, VPN, etc.
6. SSHD (sshd): Es el demonio responsable de proporcionar servicios de Secure Shell (SSH) para permitir conexiones remotas seguras al sistema.
7. Xorg (X server): Es el servidor de visualización del sistema X Window System, que maneja la interfaz gráfica de usuario y permite la ejecución de aplicaciones gráficas en entornos de escritorio.
8. Apache/Nginx (httpd/nginx): Son servidores web populares utilizados para alojar y servir sitios web y aplicaciones web.
9. MySQL/PostgreSQL (mysqld/postgres): Son servidores de bases de datos utilizados para almacenar y administrar datos en aplicaciones web y otros sistemas.
10. SSH Agent (ssh-agent): Es un proceso que administra las claves de autenticación para conexiones SSH y permite un inicio de sesión seguro sin ingresar la contraseña cada vez.

\*demonio: es un tipo de proceso que se ejecuta en segundo plano, generalmente sin interacción directa con los usuarios.

**¿Cómo identificarlos?**

Existen varias formas de identificar los procesos típicos en un sistema Linux.

1. Comando ps: El comando ps muestra información sobre los procesos en ejecución en el sistema. Para ver todos los procesos en ejecución, puedes ejecutar el siguiente comando en la terminal:

ps aux

Esto mostrará una lista detallada de todos los procesos en ejecución, incluidos los procesos típicos. Puedes buscar por nombres de procesos específicos o filtrar los resultados para encontrar los procesos que te interesan.

1. Herramientas de monitoreo del sistema: Hay varias herramientas de monitoreo del sistema que proporcionan información detallada sobre los procesos en ejecución y los recursos del sistema. Algunas herramientas populares incluyen top, htop, glances y htop. Estas herramientas suelen presentar los procesos en forma de lista o tabla, mostrando detalles como el nombre del proceso, el ID del proceso (PID), el uso de CPU y memoria, etc.
2. Explorar directorios de inicio de demonios: Los demonios a menudo se inician automáticamente al arrancar el sistema y tienen scripts o archivos de configuración asociados en directorios específicos. Puedes explorar los siguientes directorios para identificar procesos típicos:
   1. /etc/init.d/: Este directorio contiene scripts de inicio del sistema.
   2. /etc/systemd/system/: Aquí encontrarás archivos de unidades del sistema systemd.
   3. /etc/rc.d/: En algunas distribuciones, se utilizan los scripts de este directorio para la inicialización del sistema.
3. Documentación del sistema operativo y paquetes de software: Si tienes una distribución Linux específica, puedes consultar la documentación oficial o los recursos en línea para obtener información sobre los procesos típicos asociados con esa distribución en particular. Además, los paquetes de software también pueden proporcionar información sobre los demonios y procesos que incluyen.

**Investigar y establecer una contraseña para el usuario root.**

En Linux, puedes establecer una contraseña para el usuario root utilizando el siguiente procedimiento:

1. Abre una terminal en tu sistema Linux.
2. Ejecuta el siguiente comando para cambiar al usuario root:

sudo su

Se te pedirá ingresar tu contraseña de usuario actual para autenticarte como superusuario.

1. Una vez que hayas cambiado al usuario root, puedes establecer una nueva contraseña utilizando el siguiente comando:

passwd

Se te pedirá ingresar y confirmar la nueva contraseña para el usuario root. Asegúrate de elegir una contraseña segura y fácil de recordar.

4.Después de ingresar la nueva contraseña y confirmarla, se te notificará si la contraseña se cambió correctamente.

Una vez que hayas establecido una contraseña para el usuario root, podrás usarla para autenticarte como root en tu sistema Linux. Sin embargo, es importante recordar que el uso del usuario root debe ser cuidadoso y reservado para tareas de administración específicas. Se recomienda utilizar una cuenta de usuario regular para las tareas diarias y solo cambiar al usuario root cuando sea necesario.

Texto

Descripción generada automáticamente

**La vaquita y la fortuna jasjajs**

Texto

Descripción generada automáticamente