CENTRO UNIVERSITARIO DE
CIENCIAS EXACTAS E INGENIERÍAS

SISTEMAS OPERATIVOS 09
2023B

LUNES 14 DE MAYO DE 2023

MODULO 1 - CLASE 1 INTRODUCCIÓN 14-08-2023B

RAMIRO LUPERCIO CORONEL

CÓDIGO: 217536222
BENAVIDES CASTRO FERNANDO

Contenido:

PRESENTACIÓN:

Investigar cuales son las características y principales funciones del modo usuario y modo súper usuario en cada uno de los siguientes SO, como son Windows y Linux, así como las ventajas y desventajas de cada uno de ellos.

DESARROLLO:

WINDOWS

Modo Usuario (User Mode) en Windows:

Características y Funciones:

- Es un entorno restringido donde se ejecutan las aplicaciones.
- Las aplicaciones que se ejecutan en modo usuario no tienen acceso directo al hardware ni a las áreas críticas del sistema operativo.
- Windows utiliza la Virtual Memory Manager para asignar a cada proceso su propio espacio de memoria virtual privado.
- Es menos privilegiado que el modo kernel.

Ventajas:

- **Seguridad**: Las aplicaciones en modo usuario no pueden dañar directamente el sistema operativo ni otros procesos. Si una aplicación falla, no afectará al resto del sistema.
- **Estabilidad**: Al aislar cada proceso y no permitirle el acceso directo al hardware o al núcleo, se reduce el riesgo de que fallos en una aplicación causen problemas en otras o en el sistema en sí.
- **Flexibilidad**: Las aplicaciones pueden ser cerradas o reiniciadas sin afectar el funcionamiento global del sistema.

Desventajas:

- **Rendimiento**: El modo usuario puede ser más lento en comparación con el modo kernel para ciertas tareas, ya que las comunicaciones con el hardware deben ser mediadas por el sistema operativo.
- **Limitaciones**: Las aplicaciones en modo usuario no tienen la capacidad de realizar ciertas operaciones de bajo nivel que podrían requerir los drivers o software especializado.
-

Modo Kernel (Kernel Mode) en Windows:

Características y Funciones:

- Es el modo de operación con el nivel más alto de privilegio en el sistema.
- Los componentes que se ejecutan en modo kernel tienen acceso directo al hardware y al sistema operativo completo.
- Drivers de dispositivos, el núcleo del sistema operativo, y algunos servicios del sistema se ejecutan en modo kernel.
- Los fallos en este modo suelen provocar la conocida "pantalla azul de la muerte" (BSOD).

Ventajas:

- **Rendimiento**: Operar en modo kernel permite una comunicación más rápida y directa con el hardware, lo que es fundamental para tareas como

la gestión de dispositivos.
- **Capacidad**: Permite la ejecución de operaciones de bajo nivel que son esenciales para el funcionamiento del sistema operativo y el hardware.

Desventajas:
- **Seguridad**: Un error o vulnerabilidad en un componente del modo kernel puede comprometer la seguridad de todo el sistema.
- **Estabilidad**: Un fallo en el modo kernel, como un driver defectuoso, puede causar que todo el sistema se bloquee, resultando en una BSOD.
- **Complejidad**: Escribir software para el modo kernel requiere un conocimiento profundo y especializado del sistema operativo y el hardware.

El modo usuario y el modo kernel son esenciales para la arquitectura y el funcionamiento de Windows. Mientras que el modo usuario proporciona un entorno seguro y estable para ejecutar aplicaciones, el modo kernel ofrece la capacidad y rendimiento necesarios para gestionar el hardware y las operaciones críticas del sistema. Estas diferencias son importante especialmente al desarrollar software que quiera modificar el sistema a un nivel más profundo, como los drivers de dispositivos.

LINUX

Linux, con sus raíces en UNIX, ha sido diseñado con la seguridad y la multitarea en mente. El sistema de permisos y la diferenciación entre usuario y superusuario es un testimonio de este enfoque. Ahora, vamos a desglosar y analizar detalladamente la información presentada en el texto que has compartido:

Modo Usuario

Características y funciones:
- **Acceso Limitado**: Los usuarios normales no tienen permisos para modificar configuraciones del sistema, instalar software a nivel de sistema o acceder a archivos críticos.
- **Entorno Protegido**: Los errores o acciones malintencionadas realizadas por un usuario normal no afectan el funcionamiento global del sistema.

Ventajas:
- **Seguridad**: Al limitar el acceso, se minimiza el riesgo de daño accidental o malicioso.
- **Contención**: Los problemas causados por un usuario típicamente no afectan a otros usuarios ni al sistema en su conjunto.

Desventajas:
- **Restricciones**: No pueden realizar tareas administrativas o configurar aspectos esenciales del sistema.

Modo Superusuario (root)

Características y funciones:
- **Acceso Total**: Root tiene permisos para realizar cualquier acción en el sistema, desde la instalación de software hasta la modificación de cualquier archivo.
- **Herramientas de Administración**: Con herramientas como "su" y "sudo", se puede cambiar temporalmente al modo superusuario para realizar tareas

específicas.

Ventajas:

- **Control Completo**: Puedes personalizar, modificar y controlar cualquier aspecto del sistema operativo.
- **Eficiencia en Tareas Administrativas**: Con herramientas como "sudo", puedes ejecutar comandos específicos con privilegios de superusuario sin necesidad de cambiar al usuario root.

Desventajas:

- **Riesgo Elevado**: Un error en este modo, o un ataque malicioso ejecutado con permisos de root, puede resultar en daño irreparable al sistema.
- **Exposición al Malware**: Es más fácil para el software malicioso causar daños si se ejecuta con permisos de superusuario.

SU vs SUDO:

- **SU**: "su" permite cambiar al usuario root o a cualquier otro usuario. Es una forma de obtener acceso de superusuario permanentemente hasta que se decida salir. Requiere la contraseña del usuario al que se desea cambiar.
- **SUDO**: "sudo" permite ejecutar comandos específicos con privilegios de superusuario sin cambiar al usuario root. Es una medida de seguridad añadida en algunas distribuciones de Linux. En lugar de requerir la contraseña de root, "sudo" típicamente requiere la contraseña del usuario actual, y proporciona acceso de superusuario temporalmente.

El diseño y estructura de permisos en Linux ofrece una combinación única de flexibilidad y seguridad. Al separar los roles de usuario y superusuario, Linux garantiza que los usuarios comunes no puedan realizar acciones que puedan comprometer la integridad del sistema. Sin embargo, para aquellos que necesitan control total, las herramientas y capacidades de superusuario están disponibles, aunque con las advertencias y riesgos asociados. La clave es utilizar estas herramientas con cuidado y conocimiento, y siempre ser consciente del poder y responsabilidad que conlleva operar como superusuario.

CONCLUSIONES

En sistemas operativos modernos como Windows y Linux, la diferencia entre el usuario estándar y el superusuario/administrador es esencial para mantener un equilibrio entre seguridad y control del sistema. El usuario estándar, al operar con restricciones, previene modificaciones accidentales o maliciosas que puedan comprometer el sistema, ofreciendo una experiencia protegida para la mayoría de las tareas diarias. Por otro lado, el superusuario o administrador, con capacidades casi ilimitadas, tiene el poder de modificar, personalizar y administrar profundamente el sistema, pero también porta el riesgo de que un error o acción imprudente pueda resultar en consecuencias graves para el sistema. Esta dualidad es esencial: ofrece a los usuarios cotidianos una operación segura, mientras permite a los expertos y administradores adaptar y optimizar el sistema según necesidades específicas.

REFERENCIAS

Administración de usuarios en Linux. (s. f.). https://www.linuxtotal.com.mx/index.php?cont=info_admon_008

Aviviano. (2023, 15 junio). *Modo de usuario y modo kernel - Windows Drivers*. Microsoft Learn. https://learn.microsoft.com/es-es/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

Equipo editorial de IONOS. (2021). Linux vs. Windows: soluciones de alojamiento web. *IONOS Digital Guide*. https://www.ionos.mx/digitalguide/servidores/know-how/linux-vs-windows-el-gran-cuadro-comparativo/

Escobar, N. (2021, 11 marzo). Qué es el superusuario en Linux y cuál es su importancia. *Hipertextual*. https://hipertextual.com/2015/10/superusuario-en-linux

KeepCoding, R. (2023, 11 enero). ¿Qué es sudo en Linux? | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-sudo-en-linux/

Tipos de usuarios, roles y privilegios—Portal for ArcGIS | Documentación de ArcGIS Enterprise. (s. f.). https://enterprise.arcgis.com/es/portal/latest/administer/windows/roles.htm