# MÓDULO 2 MF0964_3: DESARROLLO DE ELEMENTOS DE SOFTWARE PARA GESTIÓN DE SISTEMAS

## UNIDAD 2 UF1287: DESARROLLO DE COMPONENTES SOFTWARE PARA EL MANEJO DE DISPOSITIVOS (DRIVERS)

1 El núcleo del sistema operativo

core networks

# 1 El núcleo del sistema operativo

## 1.1 Introducción

core networks

# Núcleo del sistema operativo

El núcleo o kernel de un sistema operativo, es una colección de módulos de software que se ejecutan en forma privilegiada, lo que significa que tienen acceso pleno a los recursos del sistema.

El núcleo normalmente representa sólo una pequeña parte de lo que por lo general se piensa que es todo el sistema operativo, pero es tal vez el código que más se utiliza.

# 1 El núcleo del sistema operativo

## 1.2 Arquitectura general del núcleo

core networks

# Núcleo del sistema operativo

El núcleo reside en general en la memoria principal, mientras que otras partes del sistema operativo son cargadas en la memoria principal sólo cuando se necesitan.

Los núcleos se diseñan para ejecutar el procesamiento “mínimo” posible en cada interrupción y dejar que el resto de procesamiento lo realice el proceso apropiado del sistema, que puede operar mientras el núcleo se habilita para atender otras interrupciones.

El núcleo de un sistema operativo normalmente contiene el código necesario para realizar las siguientes funciones:

# Funciones del núcleo del sistema operativo (I)

El núcleo de un sistema operativo normalmente contiene el código necesario para realizar las siguientes funciones:

- Manejo de interrupciones.
- Creación y destrucción de procesos.
- Cambio de estado de los procesos.
- Despacho.
- Suspensión y reanudación de procesos.
- Sincronización de procesos.

# Funciones del núcleo del sistema operativo (II)

- Comunicación entre procesos.
- Manipulación de los bloques de control de procesos.
- Apoyo para las actividades de entrada/salida.
- Apoyo para asignación y liberación de memoria.
- Apoyo para el sistema de archivos.
- Apoyo para el mecanismo de llamada y retorno de un procedimiento.
- Apoyo para ciertas funciones de contabilidad del sistema.

# 1 El núcleo del sistema operativo

## 1.3 Subsistemas del núcleo

core networks

# Administradores del núcleo

- Administrador de memoria principal
- Administrador del procesador
- Administrador de dispositivos
- Administrador de archivos

# 1 El núcleo del sistema operativo

## 1.4 Aspectos de seguridad sobre el desarrollo de elementos del núcleo

core networks

# Medidas de seguridad

El sistema operativo es el entorno físico en el que se ejecuta la aplicación. Cualquier vulnerabilidad en el sistema operativo puede comprometer la seguridad de la aplicación. La protección del sistema operativo garantiza la estabilidad del entorno, el control del acceso a los recursos y el control del acceso externo al entorno.

Siempre es interesante revisar las políticas de seguridad y las recomendaciones del sistema operativo, considerando la posibilidad de implementar los siguientes métodos recomendados de seguridad:

# Medidas de seguridad

El sistema operativo es el entorno físico en el que se ejecuta la aplicación. Cualquier vulnerabilidad en el sistema operativo puede comprometer la seguridad de la aplicación. La protección del sistema operativo garantiza la estabilidad del entorno, el control del acceso a los recursos y el control del acceso externo al entorno.

Siempre es interesante revisar las políticas de seguridad y las recomendaciones del sistema operativo, considerando la posibilidad de implementar los siguientes métodos recomendados de seguridad:

# Cuentas de usuario

- Limite el número de cuentas de usuario en los sistemas servidores.
- Las cuentas de usuario innecesarias y heredadas aumentan la complejidad del sistema y pueden presentar vulnerabilidades en el sistema.
- Un menor número de cuentas de usuario reduce la cantidad de tiempo que los administradores dedican a la administración de las cuentas.
- Asegúrese de que sólo unos cuantos usuarios de confianza tengan acceso administrativo a los sistemas servidores.
- Un menor número de administradores facilita el mantenimiento de la responsabilidad. Los administradores deben ser competentes.
- Asigne los permisos de acceso mínimos necesarios para la cuenta que ejecuta la aplicación.
- Si los atacantes obtienen acceso a la aplicación, tendrán los permisos del usuario que ejecuta la aplicación.

# Políticas de las cuentas

- Desarrolle y administre políticas de contraseña que promuevan la seguridad del sistema operativo.
- Ejemplos de dichas políticas son la regla de contraseña segura y la planificación de cambio de contraseña.
- Compruebe la fortaleza de las contraseñas de los usuarios descifrando las contraseñas.
- Los usuarios que no cumplan con la regla de contraseña segura recibirán una notificación para actualizar sus contraseñas según la política de contraseñas de la organización.

# Sistema de archivos

- Otorgue a los usuarios permisos de sólo lectura para los directorios necesarios.
- Si los atacantes obtiene acceso a una aplicación, tendrán los permisos de usuario.
- Deniegue el acceso de forma predeterminada.
- El acceso a los recursos se deniega a todos los usuarios excepto a los que se concede acceso explícitamente.
- Puede denegar los permisos de lectura y escritura para todas las estructuras de directorios a todos los usuarios. Sólo los usuarios a los que se otorgan estos permisos explícitamente tienen acceso a los directorios y archivos. Esta política también protege los recursos que un administrador ha pasado por alto.

# Servicios de red

- Proporcione el número mínimo de servicios necesarios en el sistema servidor.
- Utilice sólo los servicios que necesita para ejecutar la aplicación. Cada servicio es un punto de entrada potencial para un ataque malintencionado. Reducir el número de servicios en ejecución también permite gestionar mejor el sistema. Por ejemplo, es posible que no necesite los servicios ftp, rlogin o ssh.
- Reduzca el nivel de permisos de acceso para los usuarios de los servicios de red.

# Servicios de red (II)

- Suprima o marque como comentario los puertos que no tenga previsto utilizar para eliminar los posibles puntos de entrada al sistema.
- Asegúrese de que los servicios son actuales comprobando con frecuencia si hay actualizaciones de seguridad.
- Evite, si es posible, utilizar servicios que tengan una interfaz gráfica de usuario (GUI). Estos servicios introducen muchas vulnerabilidades de seguridad conocidas.

# Integridad del sistema

- Cree sistemas de producción a partir de un proceso conocido y repetible para garantizar la integridad del sistema.
- Compruebe los sistemas periódicamente con instantáneas del sistema original.
- Utilice software de auditoría de terceros disponible para comprobar la integridad del sistema.
- Realice regularmente copias de seguridad de los recursos del sistema.

# 1 El núcleo del sistema operativo

## 1.5 Resumen

core networks

# Resumen

- Funcionalidades del núcleo del sistema operativo.
- Subsistemas del núcleo del sistema operativo.
- Aspectos de seguridad en sistemas operativos.