Unidad 6. Seguridad en Sistemas Operativos de Red

DESARROLLO Y GESTIÓN DE SEGURIDAD DE REDES

6.1 Sistemas Operativos basados en Windows - Introducción

El sistema operativo Windows siempre ha estado en el ojo de la mayoría de los administradores de sistemas debido al tema de Seguridad.

Debemos considerar que tradicionalmente Windows no da la necesaria robustez respecto al tema de capacidad de cómputo como lo ofrece Unix.

Otro aspecto a considerar que en mayor número las aplicaciones de negocio están corriendo en ambientes Windows, tales como Web servers, servidores de bases de datos, etc.

6.1 Sistemas Operativos basados en Windows

Windows 1 : Primera Versión de Microsoft Windows. Lanzado en 1985. Tomó un total de 55 programadores para desarrollarlo y no permitía ventanas en cascada.

Microsoft comenzó el desarrollo del "ADMINISTRADOR DE INTERFAZ", que posteriormente derivó en Microsoft Windows en Septiembre de 1981. La interfaz inicial tenía menús ubicados en la parte inferior de la ventana y la interfaz sufrió un cambio en 1982 cuando se diseñaron los ahora comunes menús desplegables.

6.1 Sistemas Operativos basados en Windows

Windows 2 : Segunda versión de Microsoft Windows, lanzada en 1987.

Windows 2 tenía más características que Windows 1, tales como íconos y ventanas traslapadas. Cuando se lanzó Windows/386, Windows 2 fue renombrado como Windows/286.

Nacen aplicaciones como Excel, Word for Windows, Corel Draw!, Ami, PageMaker).

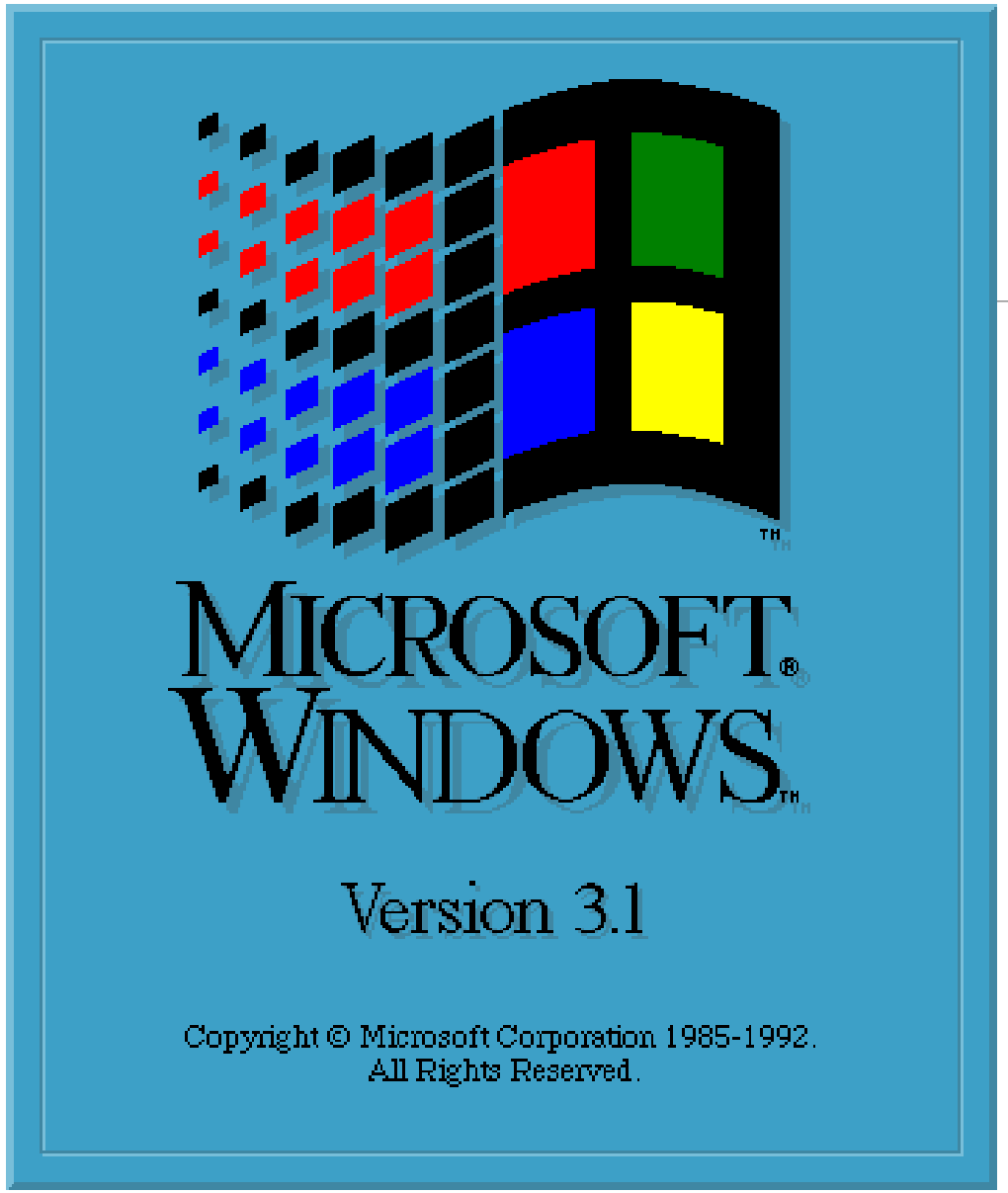
Las siguientes fueron las principales características de Windows 2.0:

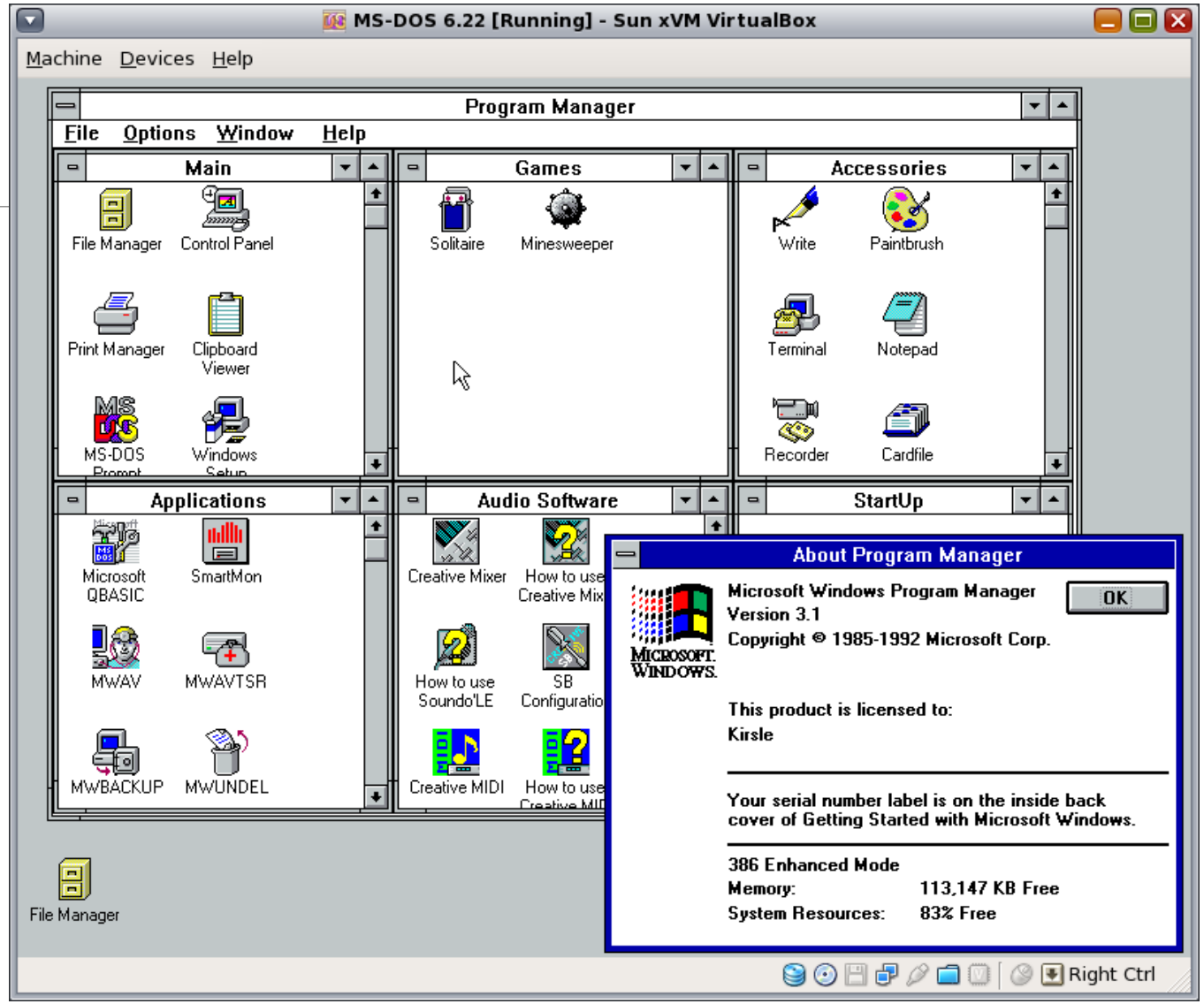
- Ventanas traslapadas
- Archivos PIF para aplicaciones DOS

6.1 Sistemas Operativos basados en Windows

Windows 3.0: Una completa reconstrucción de Windows con muchas facilidades tales como la habilidad de direccionar más allá de 640k. Fue lanzado en 1990, y vendió más de 10 millones de copias.

Windows 3.1: Una versión de Windows con muchas mejoras a Windows 3.0. incluye soporte para fuentes True Type y OLE. Esta versión fue testigo de la pérdida del modo real, lo cual significa que no corre en procesadores Intel 8086.


MICROSOFT®
WINDOWS™
Version 3.1
Copyright © Microsoft Corporation 1985-1992.
All Rights Reserved.


MS-DOS 6.22 [Running] - Sun xVM VirtualBox
Machine Devices Help
Program Manager
File Options Window Help
Main
File Manager
Control Panel
Print Manager
Clipboard Viewer
MS-DOS Prompt
Windows Setup
Games
Solitaire
Minesweeper
Accessories
Write
Paintbrush
Terminal
Notepad
Recorder
Cardfile
Applications
Microsoft QBASIC
SmartMon
MWAV
MWAVTSR
MWBACKUP
MWUNDEL
Audio Software
Creative Mixer
How to use Creative Mix
How to use Soundo'LE
SB Configuratio
Creative MIDI
How to use Creative MI
StartUp
About Program Manager
Microsoft Windows Program Manager
Version 3.1
Copyright © 1985-1992 Microsoft Corp.
OK
This product is licensed to:
Kirsle
Your serial number label is on the inside back cover of Getting Started with Microsoft Windows.
386 Enhanced Mode
Memory: 113,147 KB Free
System Resources: 83% Free
File Manager
Right Ctrl

6.1 Sistemas Operativos basados en Windows

Windows for Workgroups 3.1: Una versión de Windows 3.1 que trabaja en red.

Aunque Windows 3.1, por sí solo, puede trabajar en red, la instalación y configuración se mejoró con Windows for Workgroup.

Proveía capacidades para compartir punto a punto de archivos e impresoras.

Los archivos podía ser accedidos desde otras máquinas corriendo DOS o Windows.

6.1 Sistemas Operativos basados en Windows

Windows NT:(Windows New Technology, NT). El sistema operativo de 32 bits desarrollado originalmente para que sea OS/2 3.0 antes que Microsoft e IBM discontinuaran su trabajo con OS/2.

NT se diseñó para estaciones de trabajo avanzadas (Windows NT 3.1) y para servidores (Windows NT 3.1 Advanced Server).


Microsoft®
Copyright © 1985-1996
Microsoft Corporation
Microsoft®
Windows NT®
Workstation 4.0
with Microsoft Internet Explorer
This product is protected by US and international copyright laws as described in the About Box.

6.1 Sistemas Operativos basados en Windows

Windows CE: Un sistema operativo de la familia Windows y que fue el primero en no estar orientado a los equipos de escritorio. Los dispositivos en los que Windows CE presta servicios son Handheld PC y PalmSize PC.

- Windows CE también ha permitido la creación de un nuevo sistema denominado AutoPC, que consiste de un PC empotrado en un automóvil que va ubicado en donde actualmente va una radio. Permite controlar la radio, CD y revisar el correo electrónico.
- Windows CE también permite la creación de aplicaciones en tiempo real.

Windows y la Seguridad

La seguridad de Windows puede ser clasificada en tres diferentes áreas funcionales:

- Seguridad a nivel de red
- Seguridad del sistema operativo
- Seguridad en datos

Windows y la Seguridad

CAPI consiste en un juego de funciones que permiten a las aplicaciones y a los desarrolladores de sistemas de software acceder de forma independiente a los servicios de criptografía.

"NT dispone de un servicio básico de criptografía que nos permite codificar los datos facilitando así el almacenamiento seguro y una transmisión segura combinando claves públicas y privadas".

El método de encriptación es similar al PGP.

Windows y la Seguridad

Windows permite controlar, y monitorizar funciones de sistema.

Con el administrador de usuarios podrá controlar qué cuenta de usuario o grupo puede, por ejemplo, añadir estaciones de trabajo a un dominio, salvar o restaurar archivos y directorios, cambiar la hora del sistema, iniciar una sesión localmente, gestionar las registros de auditoria y seguridad y cerrar el sistema.

Windows y la Seguridad

Un dominio es una colección de máquinas, a las cuales el controlador de dominio administra como si se tratase de una única máquina, compartiendo una misma base de datos de seguridad.

Dicha base de datos mantiene información de todos los usuarios y grupos de ese dominio. Una cuenta de dominio, llamado de otra forma cuenta global, tiene el formato dominio\usuario. Si iniciamos una sesión en una máquina del dominio e intentamos conectarnos a una unidad de red, tendremos que introducir nuestros datos con ese formato.

Windows y la Seguridad

CONTRASEÑAS NO SEGURAS.

El personal de TI suele crear puertas traseras como medida de protección antibloqueo. Las contraseñas de estas puertas traseras suelen ser más sencillas, más fáciles de recordar y, por tanto, menos seguras.

Aunque esta situación se puede mitigar parcialmente aplicando y forzando las directivas de seguridad de Windows 2000, debe asegurarse de que los usuarios con acceso de alto nivel están sujetos a la directiva de grupo.

Windows y la Seguridad

En general, las instalaciones predeterminadas habilitan más servicios de los necesarios. Estos servicios adicionales proporcionan más entradas para posibles ataques y deben deshabilitarse. Sólo se deben ejecutar los servicios necesarios. Hay que auditar los servicios periódicamente para comprobar si aún son necesarios.

Windows y la Seguridad

Para mantener la seguridad del sistema, los servicios deben tener la menor cantidad posible de privilegios.

Debe asegurarse de que los administradores del sistema que configuran los privilegios de servicios y los programadores de aplicaciones que crean dependencias de servicios tienen esto en cuenta.

Windows y la Seguridad

Los usuarios suelen deshabilitar la protección antivirus para intentar obtener mayor velocidad de procesamiento.

Además, para conseguir mayor comodidad de uso, reducen o quitan la protección de seguridad de macros de las aplicaciones de producción, como Microsoft Word, Microsoft Excel, etc.

Es importante dejar claro a los usuarios la importancia de mantener los controles de seguridad.

Windows y la Seguridad (Conclusión)

Es importante señalar que las organizaciones necesitan entender la importancia de contar con sistemas operativos Windows y entender sus principales aspectos de seguridad de información.

6.2 Sistemas Operativos basados en UNIX

Unix podría tomarse como ejemplo de un sistema abierto.

- La fortaleza y estabilización de Unix lo equipa bien para servir como una base para estándares de sistemas abiertos en lo concerniente a lenguajes de alto nivel, herramientas para desarrollo de software y áreas de aplicaciones, tales como gráficos y comunicaciones.
- Las implementaciones de Unix corren en cientos de tipos diferentes de máquinas.
- Unix está más cerca de ser un sistema abierto que cualquier otro sistema operativo de equipos medianos.

Características de Unix

- Capacidad multiprogramación (jerarquía de procesos)
- Capacidad multiusuario.
- Transportabilidad.
- Gran selección de poderosas herramientas.
- Comunicaciones y correo electrónico.
- Biblioteca de software de aplicaciones.
- 95 % realizado en lenguaje de programación “C”.
- Estandarización fuerte.

Implementaciones de Unix

Solaris de Sun Microsystems. Uno de los sistemas operativos Unix más difundido en el entorno empresarial y conocido por su gran estabilidad. Parte del código fuente de Solaris se ha liberado con licencia de fuentes abiertas.

AIX de IBM. El UNIX "propietario" de IBM ha cumplido 20 años de vida en el 2006 y continúa en pleno desarrollo, con una perceptible herencia del mainframe en campos como la virtualización o la RAS de los servidores, heredada de sus "hermanos mayores".


Anwendungen
Orte
System
De
13:42
Persönlicher Ordner
Opera
Firefox Webbrowser
Thunderbird E-Mail
Software hinzufügen
opensolaris

Implementaciones de Unix

HP-UX de Hewlett-Packard. Este sistema operativo también nació ligado a las computadoras departamentales de este fabricante. También es un sistema operativo estable que continua en desarrollo

Seguridad en Unix

Unix es el sistema operativo de propósito general más seguro hoy en día.

CONTROL DE LOS PASSWORDS

- No utilizar el nombre de la cuenta (login), tal cual, al revés, en mayúsculas...
- No utilizar nuestro nombre, ni apellidos.
- No utilizar nombres de familiares.
- No emplear información personal que pueda ser obtenida fácilmente.
- No emplear una contraseña sólo con números o con la misma letra.

Seguridad en Unix

- No emplear palabras que se encuentren el los diccionarios.
- No utilizar palabras de menos de seis letras.
- Mezclar letras mayúsculas y minúsculas.
- Utilizar palabras que sean fáciles de recordar para que no haya que escribirlas.
- Emplear una contraseña que pueda ser tecleada rápidamente sin necesidad de mirar al teclado.
- No escribirlos en ningún sitio, ni siquiera ficheros.

Control de red

Configuración. Trata de la inicialización, mantenimiento, y apagado de los componentes individuales y subsistemas lógicos del sistema. Algunas de las funciones que se deben llevar a cabo en la gestión de la configuración son las siguientes:

- Elaboración de la información de la configuración.
- Establecer y modificar los valores de configuración.
- Definir y cambiar las relaciones
- Iniciar y finalizar operaciones de red.
- Distribución de software.
- Informar del estado de la configuración.

Control de las cuentas

Es posible que en algunos sitios, donde haya multitud de usuarios, existan viejas cuentas de personas que hayan abandonado la empresa.

Estas cuentas suelen suponer un agujero de seguridad importante, no sólo porque alguien pueda entrar en ellas, sino porque si se produce un acceso no autorizado es muy difícil de detectar. Para evitar esto hay que poner fecha de expiración en todas las cuentas.

La fecha puede almacenarse fácilmente en el fichero /etc/shadow

Control de las cuentas

Este archivo está pensado para no dejar en el /etc/passwd las contraseñas de los usuarios encriptadas. Puesto que UNIX requiere que sobre este archivo tengan derechos de lectura, las contraseñas se almacenan en el /etc/shadow.

El syslog

El syslog, es un mecanismo mediante el cual se manda cualquier mensaje de error a la consola del sistema.

Normalmente los mensajes se almacenan en */usr/adm/messages*, con la fecha, el tiempo que aparecieron, nombre del programa que envió el mensaje y el identificador del proceso.

Shells scripts con setuid

Los programas que tienen los bits de setuid o setguid activos no son seguros. Hay que tener especial cuidado cuando se escriben dichos programas.

Existen numerosos paquetes de software que intentan que estas shells sean seguras, pero no se ha conseguido resolver del todo. No se deben permitir nunca en UNIX. El problema de un script con este bit activo es que puede ser interrumpido, dejando al usuario que lo utiliza con los privilegios del propietario.

Shells scripts con setuid

Esto se puede hacer, por ejemplo, para el .profile. Para evitar esto hay que usar la orden trap.

También hay que tener cuidado cuando se llama a un programa ejecutable desde una shell, puesto que se ejecutará sobre su propia shell, que puede interrumpirse también.

Para prevenir esto, es preciso lanzar el programa con el comando exec.

Los distintos shells tratan de forma distinta el EUID.

Seguridad en Unix (Conclusión)

Es importante señalar que las organizaciones necesitan entender la importancia de contar con sistemas operativos UNIX.