UNIVERSIDAD TÉCNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

ESPECIALIDAD INGENIERÍA EN INFORMÀTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO

ESTUDIO Y ANALISIS DE SEGURIDADES DE RED BASADOS EN UN ENTORNO WINDOWS 2000 SERVER

TESIS DE GRADO PREVIO A LA OBTENCION DEL TITULO DE INGENIERO EN INFORMÀTICA Y SISTEMAS COMPUTACIONALES

CÉSAR VINICIO ARMAS MOREJÓN

DIRECTOR : ING. JESÚS GONZÁLEZ
ASESOR: ING. EDISON ERAZO

Latacunga - Ecuador
2003

RESÙMEN

La seguridad bajo Windows 2000 Server dentro de una red garantizan la confidencialidad de los datos, los cuales sólo las personas autorizadas deben poder ver la información, la integridad de los datos donde todos los usuarios autorizados deben estar seguros de que los datos que obtienen son precisos y de que no fueron modificados de forma inadecuada y la disponibilidad de los datos, en el cual los usuarios autorizados deben poder tener acceso a la información que necesiten, en cualquier momento.

La plataforma de estudio Windows 2000 Server proporciona unos servicios de administración flexibles basados en directivas que le permitirán proteger y administrar las redes, los servidores y los sistemas clientes, gracias a las novedades y las mejoras en los servicios (por ejemplo, el servicio de directorio Active Directory, la administración remota y los servicios de seguridad distribuidos de tipo empresarial), se simplifica y facilita la administración de la red.

CAPÍTULO I

ESTRATEGIAS DE DEFENSA

1.1.- Defensa en profundidad

Una estrategia de defensa en profundidad reduce el riesgo en su entorno, protege los recursos de amenazas externas e internas utilizado para describir la aplicación de contramedidas de seguridad con el fin de formar un entorno de seguridad sin un solo punto de error.

Con el despliegue de varias capas de seguridad, ayuda a garantizar que si se pone en peligro una capa, las otras ofrecerán la seguridad necesaria para proteger sus recursos (1). Por ejemplo, que el servidor de seguridad de una organización esté en peligro, no debe significar que un atacante pueda tener acceso sin trabas a los datos más confidenciales de la organización. En el caso ideal, cada capa debe proporcionar diferentes formas de contramedidas para evitar que se utilice el mismo método de explotación en varias capas.

En el siguiente gráfico (gráfico 1) se muestra una estrategia de defensa en profundidad eficaz.

Gráfico 1
Estrategia de defensa eficaz

http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch01secops.asp

(1)http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/default.asp 02 de mayo de 2003

Es importante recordar que sus recursos no son sólo datos, sino que cualquier elemento de su entorno es susceptible de ser atacado. Como parte de su estrategia de administración de riesgos debe examinar los recursos que protege y determinar si dispone de protección suficiente para todos.

La cantidad de medidas de seguridad que pueda aplicar dependerá de la evaluación de riesgos, el análisis de costos y beneficios de la aplicación de contramedidas (2). Sin embargo, el objetivo consiste en garantizar que un atacante necesitará unos conocimientos, tiempo y recursos significativos para superar todas las contramedidas y tener acceso a sus recursos.

Se debe tomar en cuenta siempre que la forma exacta en la que se aplique la defensa en profundidad dependerá de las características propias de su entorno. Se debe asegurar volver a evaluar la estrategia de defensa en profundidad cuando su entorno cambie.

1.2.- Defensa de datos

Para muchas empresas uno de los recursos más valiosos son los datos. Si estos datos cayeran en manos de la competencia o sufrieran daños, tendrían problemas importantes.

A nivel de cliente, los datos almacenados localmente son especialmente vulnerables. Si se roba un equipo portátil, es posible realizar copias de seguridad, restaurar y leer los datos en otro equipo, aunque el delincuente no pueda conectarse al sistema.

Los datos se pueden proteger de varias formas, incluido el cifrado de datos mediante EFS (Encrypting File Service).

(2)http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch01secops.asp 05 mayo 2003

Gracias al avance de todo lo relacionado con la Informática es cada vez más sencillo realizar más actividades por Internet como compras o suscripciones. Mucha gente tiene el temor de que sus datos puedan ser capturados por alguna otra persona y ser utilizados para sacar algún provecho de éstos.

Por ejemplo, al dar el número de alguna cuenta bancaria o tarjeta de crédito, si éste lo obtuviera otra persona podría emplearlo a su conveniencia y lograr alguna ventaja económica (3). Obviamente, muchas personas optarían por dedicarse a esto y nadie confiaría en las compras o actividades monetarias por Internet.

Es por esta razón que se utiliza la "encripción". Los datos viajan encriptados a través de la red para llegar a sus destinos sanos y salvos; casi todas las empresas cuentan con esta técnica.

La encriptación de la información se logra utilizando un código llamado ASCII, el cuál es el acrónimo de American Standard Code for Information Exchange. Es un esquema de codificación que asigna valores numéricos a las letras, números, signos de puntuación y algunos otros caracteres. Al normalizar los valores

utilizados para dichos caracteres, ASCII permite que los ordenadores o computadoras y programas informáticos intercambien información.

El código ASCII se basa en asignar a los dígitos caracteres que son difíciles de encontrar en el teclado. Para lograr dígitos de este código se tiene que presionar la tecla Alt y al mismo tiempo un número en el teclado numérico. Para lograr cada carácter se necesita una cifra distinta y por eso son tantos.

(3)http://microasist.com.mx/noticias/en/en0608.shtml *06 de mayo de 2003*

Sucede constantemente que nos sentimos observados, que cada movimiento que hacemos es vigilado por "alguien" y suele ser común que uno se sienta así cuando viaja por la red.

Hoy en día existen métodos para protegerte, para mantener a salvo la privacidad y asegurar secretos y documentos.

Internet no es un medio seguro, por este se revela muchísima información tanto de trabajo, como personal poniendo en riesgo la información que se envía y dejando un rastro fácil de seguir.

Una de las amenazas más comunes es la que se da por medio del correo y esta consiste en ataques a tu confidencialidad (4). Cada vez que viajamos por la Web hacemos uso de un servidor FTP y revelamos datos acerca de nuestros gustos, personalidad, economía, residencia etc.

En estos tiempos ya es un poco más sencillo hacer frente a todos estos ataques mediante protocolos de comunicaciones basados en procedimientos criptográficos.

Estos productos permiten asegurar el perímetro con la finalidad de que las transferencias de información confidencial a través de una WAN o LAN sean seguras impidiendo así el robo de la misma.

En la actualidad son más necesarios los productos de encripción que los Firewalls como herramientas de seguridad.

La encripción es un arma perfecta para combatir la violación de información, es u *(4)http://microasist.com.mx/noticias/en/aften0211.shtml* *08 de mayo de 2003* rer riesgos innecesarios

Ya no se tienen pretexto alguno para no estar protegidos, hay sistemas de seguridad muy efectivos que mantendrán la confidencialidad de nuestra información a toda costa.

En los últimos años con el acelerado crecimiento de la industria de computo e informática y dando paso al nuevo milenio, se a hecho necesaria ya el uso de una computadora además de esa nueva herramienta de trabajo como lo es el Internet.

La consecuencia del crecimiento del Internet es en la actualidad uno de nuestros mayores riesgos para la seguridad de las redes empresariales, gubernamentales y privadas (5). Esto debido a que las tecnologías más innovadoras que se utilizan en

el Internet requieren de una mayor protección contra intrusiones y daños en datos valiosos, la solución se basa en la posibilidad se establecer vínculos dinámicos entre la política de seguridad del cliente y la identidad del usuario.

La encripción es una herramienta valiosa y ofrece un nivel sin precedentes de protección de la seguridad ya que permite el acceso a través de una conexión adecuada para validar el paso lo que proporciona a las organizaciones un acceso transparente para los usuarios internos, externos autorizados y al mismo tiempo protege las redes internas del acceso no autorizado.

Tradicionalmente los métodos de encripción proporcionan protección de perímetro manteniendo un detallado control de estado de todas las conexiones entre los segmentos de red interconectados, Hoy en día más y más clientes desean implementar la encripción de información en su servicio de redes virtuales, como

(5)http://microasist.com.mx/noticias/en/fimen251102.shtml 21 de mayo de 2003

otos pueden acceder de forma segura a las redes de la empresa.

Cabe señalar que la encripción de información no esta siendo encaminada a los

(5)http://microasist.com.mx/noticias/en/fimen251102.shtml 21 de mayo de 2003

dades de cada usuario debido a que la encripción es una solución de administración centralizada que permite proteger los archivos guardados en cualquier PC y laptop de manera segura manteniendo los archivos confidenciales.

El encriptar los archivos guardados en el disco duro protege la información más valiosa, sin embargo es bastante complejo asegurar que todos los usuarios de

sistemas de computo utilicen este sistema como manera de protección de sus datos.

Dentro de Windows 2000 están integradas algunas opciones de seguridad. La intención es que cada usuario pueda entender y controlar como funcionan estas opciones, ya que funciona en tres niveles:

Local.- La protección local se realiza a través de un sistema de encriptación de archivos que funcionan en unidades NTFS (sistema de archivo de NT), este sistema esta diseñado para evitar que usuarios no autorizados se salten el sistema de arranque y por lo tanto también las funciones de seguridad.

Corporativo.- Es la protección de datos en una lan (red de área local) ya que Windows 2000 utiliza el protocolo kerberos versión 5, un estándar de seguridad en redes lan e intranets que verifica y hace un seguimiento de la actividad de cada usuario dentro de la red (6). Kerberos permite un control de acceso unificado a casi cualquier entorno en red eliminando la necesidad de obtener permisos y

(6)http://microasist.com.mx/noticias/en/gspen1801.shtml 22 de mayo de 2003

le la red.

Público.- Es la protección de conexiones internet. Windows 2000 utiliza también

(6)http://microasist.com.mx/noticias/en/gspen1801.shtml 22 de mayo de 2003

ad para mantener la seguridad que se maneja por Internet, de manera que verifique la procedencia de mensajes de correo o garantice las fuentes de donde proceden aplicaciones y controladores, por otra parte incluye redes privadas virtuales.

La encriptación de datos es la única solución para este problema. Existen varios productos en el mercado que permiten la encriptación de archivos a nivel de aplicaciones, utilizando claves derivadas de las contraseñas. Sin embargo, existen ciertas limitantes con la mayoría de estos enfoques:

1.2.2.1.- Encriptación y desencriptación manual en cada uso. Los servicios de encriptación no son transparentes para el usuario en la mayoría de los productos. El usuario tiene que desencriptar el archivo antes de cada uso y volver a encriptarlo al terminar (7). Si el usuario olvida encriptar un archivo, el archivo queda sin protección. Debido a que el usuario debe especificar que un archivo va a ser encriptado (y desencriptado) en cada uso, esto puede omitirse.

1.2.2.2.- Fugas de archivos temporales y de búsqueda. Varias aplicaciones crean archivos temporales mientras el usuario edita un documento (por ejemplo, Microsoft Word). Estos archivos temporales se dejan sin encriptar en el disco, aún cuando el documento original esté encriptado, haciendo que el robo de los datos es muy fácil. La encriptación a nivel de aplicaciones se ejecuta en el modo de usuario Windows. Esto significa que la clave de encriptación del usuario

(7)http://www.microsoft.com/latam/technet/info/edk/docs/Server/LowerTCO/whitepapers/encrypting_file_system.doc 23 de mayo de 2003

a todos los documentos encriptados utilizando una sola clave, con solo explotar en un archivo de búsqueda.

(7)http://www.microsoft.com/latam/technet/info/edk/docs/Server/LowerTCO/whitepapers/encrypting_file_system.doc 23 de mayo de 2003

1.2.2.3.- Seguridad débil. Las claves se derivan de contraseñas o frases de pase. Los ataques de diccionario fácilmente pueden abrir una brecha en este tipo de seguridad, si se utilizan contraseñas fáciles de recordar.

1.2.2.4.- Sin recuperación de datos. Muchos productos no proporcionan los servicios de recuperación de datos. Este es otro aspecto que desalienta a los usuarios, especialmente a quienes no desean tener que recordar otra contraseña. En los casos en que se brinda la recuperación de datos con base en una contraseña, se crea otro punto de acceso débil. El único dato que necesita un ladrón es la contraseña, para que el mecanismo de recuperación le permita acceder a los archivos encriptados.

El sistema de encriptación de archivos (EFS) resuelve todos los problemas mencionados anteriormente y más.

1.2.3.-- Tecnología de encriptación EFS

EFS se basa en la encriptación de clave pública, cada archivo se encripta utilizando una clave generada de manera aleatoria, que es independiente del par de clave privada/pública del usuario, evitando así varias formas de ataque con base en criptoánalisis.

El EFS reside o esta integrado firmemente con el NTFS. Cuando se crean archivos temporales, los atributos del archivo original se copian a los archivos temporales, siempre que los archivos estén en el volumen NTFS (8). Si encripta un archivo, el EFS también encripta sus copias temporales. El EFS reside en el kernel del sistema operativo y utiliza una agrupación de no búsqueda para almacenar las claves de encriptación de archivo lo cual asegura que nunca estén en el archivo de búsqueda.

La configuración predeterminada del EFS permite que los usuarios inicien la encriptación de archivos sin esfuerzo administrativo. El EFS genera automáticamente un par de clave pública para la encriptación de archivos para un usuario, en caso de que no exista.

La encriptación y desencriptación de archivos se soporta sobre una base de directorio completo o por archivos. La encriptación de directorios se refuerza de manera transparente. Todos los archivos (y subdirectorios) creados en un directorio marcado para encriptación se encriptan automáticamente. Cada archivo tiene una clave de encriptación única, lo que lo hace seguro para volver a nombrarlo. Si renombra un archivo desde un directorio encriptado a un directorio no encriptado en el mismo volumen, el archivo permanece encriptado. Los servicios de encriptación y desencriptación están disponibles en Windows Explorer. Las herramientas de la línea de comandos y las interfaces administrativas también se proporcionan para usuarios avanzados y agentes de recuperación, de manera que puedan aprovechar al máximo esta capacidad.

Un archivo no necesita desencriptarse antes de utilizarse. La encriptación y desencriptación se realiza de manera transparente cuando los bytes viajan hacia y desde el disco. El EFS detecta automáticamente un archivo encriptado y coloca una clave del usuario desde el almacén de claves del sistema los usuarios tienen la facilidad de almacenar claves en dispositivos seguros, tales como las tarjetas

La arquitectura del EFS está diseñada para poder compartir archivos entre

cualquier número de personas utilizando sus claves públicas. Los usuarios pueden desencriptar entonces de manera independiente los archivos mediante sus propias claves privadas. Los usuarios pueden ser agregados fácilmente (si cuentan con un par de clave pública configurado) o eliminados de un grupo con autorización para compartir.

El EFS cuenta con soporte de recuperación de datos. La infraestructura de seguridad Windows 2000 refuerza la configuración de claves de recuperación de datos. Puede utilizar la encriptación de archivos sólo si el sistema está configurado con una o más claves de recuperación. El EFS permite que los agentes de recuperación configuren las claves públicas que se utilizan para habilitar la recuperación de archivos. Utilizando la clave de recuperación, sólo está disponible la clave de encriptación del archivo generada de manera aleatoria y no una clave privada de usuario. Esto asegura que ninguna otra información privada sea revelada al agente de recuperación de manera accidental.

La recuperación de datos está pensada para la mayoría de los ambientes empresariales, en donde las organizaciones esperan poder recuperar los datos encriptados por un empleado después de que el empleado se retire, o cuando se pierdan las claves de encriptación. La política de recuperación se puede definir en el controlador de dominio de un dominio Windows. Esta política se refuerza en todas las computadoras en dicho dominio. Los administradores de dominio tienen el control de la política de recuperación y pueden delegar esto a cuentas de administradores de seguridad de datos, utilizando las funciones de delegación del

Servicio de directorio Windows. Esto proporciona un control mejor y más flexible de quién está autorizado para recuperar datos encriptados. El EFS también soporta diversos agentes de recuperación, al permitir múltiples configuraciones clave de recuperación que proporcionen a las organizaciones redundancia y flexibilidad al implementar sus procedimientos de recuperación.

El EFS también se puede utilizar en un ambiente local. El EFS genera automáticamente claves de recuperación y las guarda como claves de la máquina en donde no hay dominio de Windows. Los usuarios locales también pueden utilizar la herramienta de línea de comandos para recuperar los datos, utilizando la cuenta del administrador. Esto reduce la sobrecarga administrativa para un usuario local.

1.2.4.- Uso del sistema de encriptación de archivos

Las siguientes secciones brindan al usuario escenarios que demuestran cómo funciona el EFS.

El menú de contexto expone las siguientes funciones EFS para el usuario:

- **Encriptación:** Esta opción permite que el usuario encripte el archivo seleccionado actualmente. Si la selección actual es un directorio, permite al usuario encriptar todos los archivos (y subdirectorios) en el directorio y marcar el directorio como encriptado.
- **Desencriptación:** Esta opción es lo contrario de la encriptación. Permite que el usuario decodifique el archivo seleccionado actualmente. Si la selección

actual es un directorio, permite al usuario desencriptar todos los archivos que hay en el directorio y restablece el directorio como decriptado.

- **Configuración:** Los usuarios pueden generar, exportar, importar y manejar claves públicas utilizadas para la encriptación de archivos basados en EFS. La configuración se integra con el resto de las configuraciones de seguridad del usuario. Esta función está dirigida a los usuarios avanzados que desean administrar sus propias claves. Por lo regular, los usuarios no tienen que hacer ninguna configuración. El EFS genera automáticamente claves para el usuario que no cuenta con una clave configurada para uso de encriptación de archivos.

1.2.5.- Encriptación de archivos

Todo lo que debe hacer el usuario es seleccionar uno o más archivos y elegir encriptar del menú de contexto encriptación de archivos y el EFS encripta los archivos seleccionados.

Una vez que el archivo se encripta, éste se almacena ya encriptado en el disco. Todas las lecturas y escrituras al archivo se desencriptan y encriptan de manera transparente. Para saber si el archivo está encriptado, el usuario puede verificar las propiedades en el archivo para ver que el bit de atributo esté activado. Ya que la encriptación es transparente, el usuario puede utilizar el archivo como antes. Por ejemplo, puede seguir abriendo el documento en Word y editarlo como antes o abrir un archivo de texto utilizando Notepad y hacer lo mismo. Cualquier otro usuario que trate de abrir este archivo encriptado obtiene un error de acceso

denegado, debido a que el usuario no posee la clave para desencriptar el archivo.

Los usuarios (administradores en este caso) no deberán encriptar los archivos en el directorio del sistema, pues estos archivos se necesitan para que se inicie el sistema. Durante el proceso de inicio, no hay una clave de usuario disponible para desencriptar los archivos. Dicha operación puede dejar inservible al sistema. Windows Explorer evita esto al hacer fallar los intentos de encriptación en archivos con el atributo del sistema. Las versiones futuras de Windows brindarán capacidades de inicio seguras para soportar la encriptación de los archivos del sistema.

El EFS también da a los usuarios la capacidad de transferir archivos encriptados a través de los sistemas. Las funciones de exportar archivo encriptado e importar archivo encriptado son extensiones del comando copiar en un indicador de comandos Windows. Todo lo que el usuario debe hacer es especificar el archivo encriptado como la fuente y otro archivo en un directorio no encriptado como el destino con la opción de exportar. El archivo exportado continúa encriptado. El usuario puede copiar entonces este archivo exportado a diferentes sistemas de archivos incluyendo FAT, cintas de respaldo o enviarlo como adjunto de un correo electrónico como un archivo normal. Para poder utilizar el archivo en un sistema al que se copia, el usuario especifica el archivo exportado como la fuente y un nombre de archivo nuevo en un volumen NTFS como destino para importar el archivo, con lo que el nuevo archivo se crea como un archivo encriptado. **Nota:** Con sólo copiar el archivo se hace una copia en sólo texto, a menos que el

directorio en el que se copia el archivo esté marcado como encriptado, en cuyo caso la copia se reencripta. Esto se debe a que el comando de copia normal utiliza lecturas de archivo que se desencriptan de manera clara mediante el EFS. Esto se puede utilizar para crear copias de texto de un archivo encriptado para distribución.

1.2.6.- Encriptación de directorio

Los usuarios también pueden marcar directorios como encriptados utilizando el menú de contexto Windows Explorer. Marcar un directorio como encriptado asegura que se encripten todos los archivos futuros en dicho directorio de manera predeterminada y que todos los subdirectorios futuros del mismo se marquen como encriptados. La lista de archivos de directorio no está encintada y se pueden enumerar archivos como siempre, en caso de que tenga suficiente acceso al directorio.

Marcar los directorios para encriptación es similar a encriptar archivos. Un usuario selecciona el directorio y elige la opción de encriptación en Windows Explorer. En este caso, el usuario tiene las opciones de marcar sólo el directorio para encriptación o encriptar todos los archivos y subdirectorios bajo él. La encriptación de directorios brinda a los usuarios la capacidad de manejar sus archivos importantes copiándolos simplemente a directorios encriptados.

1.2.7.- Desencriptación de archivo o directorio

Los usuarios no necesitan desencriptar archivos o directorios para operaciones

normales debido a que el EFS brinda encriptación y desencriptación transparente durante las escrituras y lecturas de datos. No obstante, dichas operaciones pueden ser requeridas bajo circunstancias especiales en donde un usuario necesita compartir un archivo encriptado con otros usuarios.

Los usuarios pueden desencriptar archivos y marcar directorios no encriptados utilizando el menú de contexto Windows Explorer. La operación es similar a la encriptación. Realizar esta operación en uno o más archivos provoca que el EFS desencripte el archivo completo y lo marque como no encriptado. En el caso de la desencriptación de un directorio, el menú de contexto también brinda la opción de desencriptar todos los archivos y subdirectorios encriptados en dicho directorio.

1.2.8.- Operaciones de recuperación

La política de recuperación de EFS se implementa como parte de la política de seguridad general para el sistema, como parte de la política de seguridad de dominio, aplica a todas las computadoras basadas en Windows 2000 dicho dominio. La interfaz del usuario de la política de EFS se integra como parte de la política de dominio y las interfaces de política local. Esta interfaz permite que los agentes de recuperación generen, exporten, importen y respalden claves de recuperación a través de un control de administración de claves común. Integrar la política de recuperación con una política de seguridad del sistema brinda un modelo de refuerzo de seguridad coherente. El subsistema de seguridad Windows se encarga de reforzar, replicar y mandar a la memoria caché la política EFS. Por lo tanto, los usuarios pueden utilizar la encriptación de archivos en un sistema que

esté fuera de línea temporalmente, como una laptop, y también pueden registrar en su cuenta de dominio, utilizando credenciales con caché.

1.2.9.- Recuperación de encriptación

El EFS requiere que se establezca una política de recuperación de datos en un nivel de dominio (o localmente si la computadora no es miembro de un dominio) antes de que se pueda utilizar el EFS. Los administradores de dominio establecen la política de recuperación de dominio (o el personal delegado conocido como agentes de recuperación), quienes controlan las claves de recuperación para todas las computadoras en dicho dominio.

Si un usuario pierde una clave privada, un archivo protegido por dicha clave se puede recuperar exportando el archivo y enviándolo por correo electrónico a uno de los agentes de recuperación. El agente de recuperación importa el archivo en una computadora segura con las claves de recuperación privadas y utiliza la herramienta de la línea de comandos de recuperación para desencriptar el archivo. Entonces el agente de recuperación regresa el archivo de texto al usuario. En ambientes de pequeñas empresas o en ambientes de hogar, en donde no hay dominios, la recuperación se puede realizar en la computadora autónoma misma.

El EFS implementa la encriptación y desencriptación de datos, utilizando un esquema basado en clave pública. Los datos del archivo se encriptan utilizando un algoritmo simétrico rápido con la clave de encriptación de archivo (FEK). FEK es una clave generada aleatoriamente de una longitud determinada por el

algoritmo o por ley, si el algoritmo soporta claves de longitud variable.

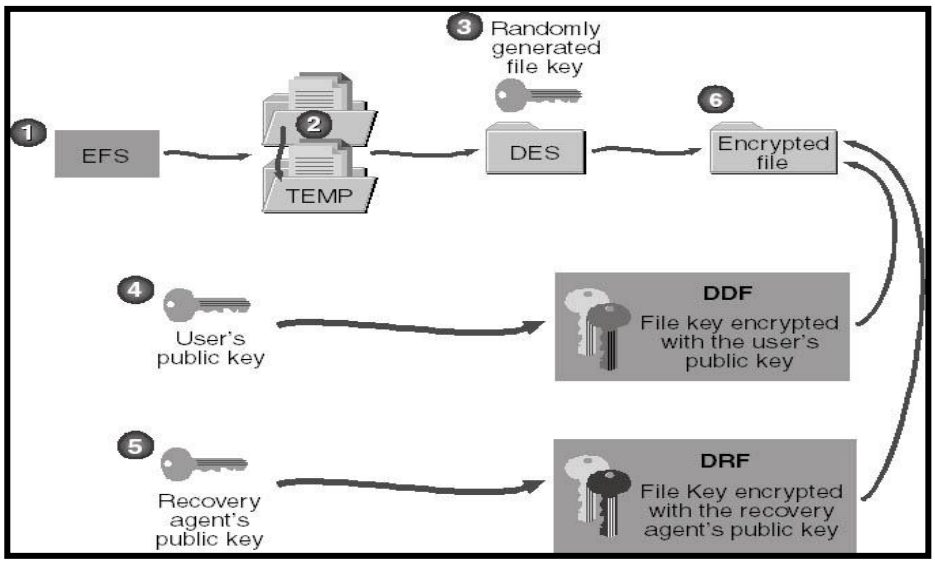
FEK se encripta utilizando una o más claves públicas de encriptación para generar una lista de las FEKs encriptadas. La parte pública de un par de claves de usuario se utiliza para encriptar las FEKs. La lista de las FEKs encriptadas se almacena junto con este archivo encriptado en un atributo EFS especial denominado campo de desencriptación de datos (DDF). La información de encriptación de archivos está muy ligada al archivo. La parte privada del par de claves del usuario se utiliza durante la desencriptación. La FEK se desencripta utilizando la parte privada del par de claves. La parte privada de un par de claves de usuario se almacena de manera segura en otro lado, en tarjetas inteligentes o en otros dispositivos de almacenamiento seguros.

Así mismo, la FEK se encripta utilizando una o más claves públicas de encriptación de clave. Una vez más, la parte pública de cada par de claves se utiliza para encriptar las FEKs. Esta lista de FEKs encriptadas también se almacena con el archivo en un atributo EFS especial denominado campo de recuperación de datos (DRF). Sólo las partes públicas de los pares de claves de recuperación se necesitan para la encriptación de FEK en el DRF. Estas claves públicas de recuperación se requieren en todo momento en un sistema EFS para operaciones normales de sistema de archivo. La recuperación es requerida sólo cuando los usuarios dejan las empresas o pierden las claves. Por esto, los agentes de recuperación pueden almacenar las partes privadas de las claves de manera segura en otro lado (en tarjetas inteligentes y en otros dispositivos de

almacenamiento seguro).

El gráfico siguiente (gráfico 2) muestra los procesos de encriptación, desencriptación y recuperación.

Gráfico 2
Proceso de encriptación, desencriptación y recuperación

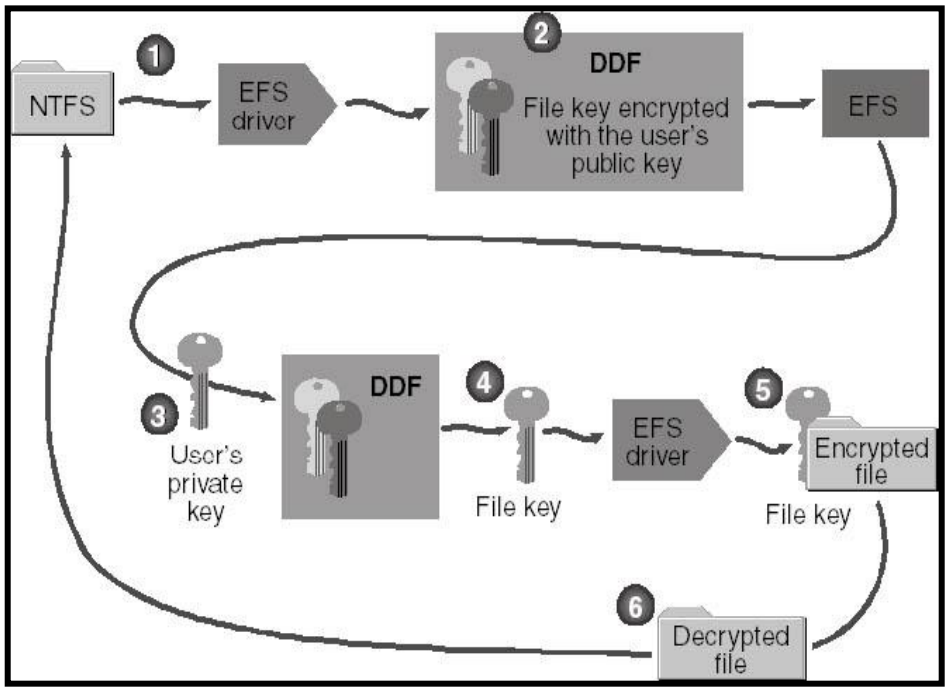


ms press - mcse training kit - microsoft windows 2000 server. published by microsoft press 2000 by microsoft corporation

El gráfico siguiente (gráfico 3) muestra el proceso de encriptación en donde el archivo de texto del usuario se encripta utilizando una FEK generada de manera aleatoria. Esta clave de encriptación de archivo se almacena junto con el archivo encriptado bajo una clave pública de usuario en el DDF y encriptado bajo la clave pública del agente de recuperación en el DRF. **Nota:** La figura muestra sólo un usuario y un agente de recuperación, esto puede ser, de hecho, una lista de

usuarios y una lista de agentes de recuperación con claves independientes. La primera versión de EFS soporta agentes de recuperación múltiples y usuarios únicos.

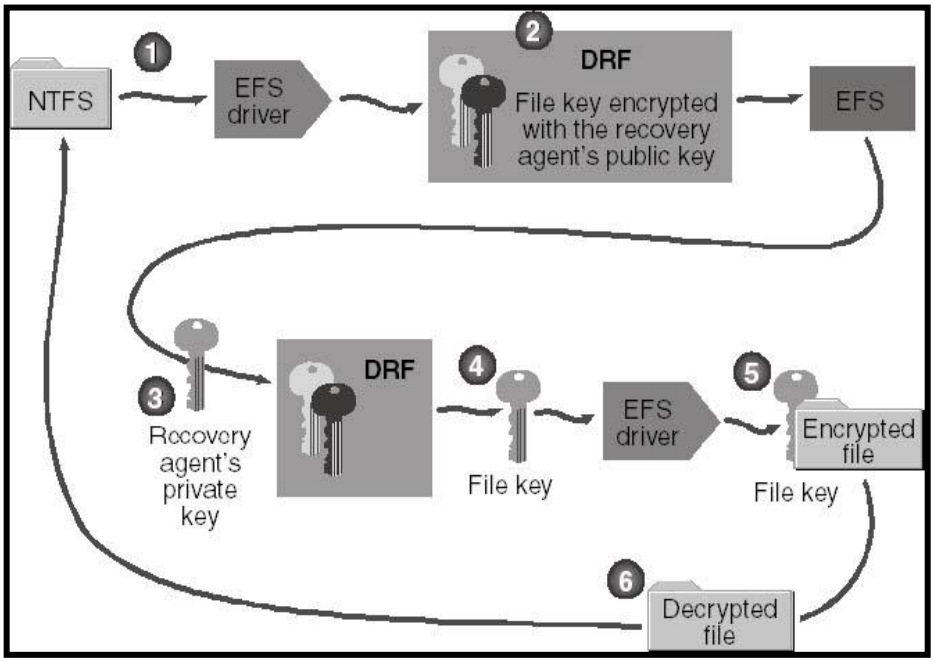
Gráfico 3
Proceso de encriptación.



ms press - mcse training kit - microsoft windows 2000 server. published by microsoft press 2000 by microsoft corporation

El siguiente grafico (gráfico 4) muestra el proceso de desencriptación. Una clave privada de usuario se utiliza para desencriptar la FEK, utilizando el elemento FEK encriptado correspondiente en el DDF. La FEK se utiliza para desencriptar lecturas de datos de archivos por bloque. El acceso aleatorio a un archivo grande desencripta sólo la lectura de bloques específicos del disco para dicho archivo. El archivo completo no tiene que ser decriptado.

Gráfico 4
Proceso de desencriptación.



ms press - mcse training kit - microsoft windows 2000 server. published by microsoft press 2000 by microsoft corporation

El proceso de recuperación. Es similar a la desencriptación, excepto que utiliza una clave privada de agente de recuperación para desencriptar la FEK en el DRF.

Este esquema simple brinda una tecnología de encriptación sólida y la capacidad de permitir a los usuarios múltiples compartir un archivo encriptado, además de proporcionar a diferentes agentes de recuperación la capacidad de recuperar el archivo, si así lo requieren. El esquema es un algoritmo completamente ágil y cualquier algoritmo criptográfico se puede utilizar en las diferentes fases de encriptación. Esto será muy importante a medida que se inventen nuevos y mejores algoritmos.

1.3.- Defensa de aplicaciones

El refuerzo de las aplicaciones es una parte esencial de cualquier modelo de seguridad. Muchas aplicaciones utilizan el subsistema de seguridad de Windows 2000 para proporcionar seguridad. No obstante, es responsabilidad del programador incorporar la seguridad en la aplicación para proporcionar una protección adicional a las áreas de la arquitectura a las que la aplicación puede tener acceso. Una aplicación existe en el contexto del sistema, de modo que siempre se debe tener en cuenta la seguridad de todo el entorno al considerar la seguridad de una aplicación.

Se debe probar en profundidad el cumplimiento de la seguridad de cada aplicación de la organización en un entorno de prueba antes de permitir que se ejecute en una configuración de producción.

1.4.- Defensa de hosts

Debe evaluar cada host del entorno y crear directivas que limiten cada servidor sólo a las tareas que tenga que realizar. De este modo, se crea otra barrera de seguridad que un atacante deberá superar antes de poder provocar algún daño.

Un modo de hacerlo consiste en crear directivas individuales en función de la clasificación y el tipo de datos que contiene cada servidor. Por ejemplo, las directivas de una organización pueden estipular que todos los servidores Web son de uso público y por lo tanto sólo pueden contener información pública. Sus

servidores de bases de datos están designados como confidenciales de la empresa, lo que significa que la información debe protegerse a cualquier precio.

En la siguiente tabla (tabla 1) se muestra una clasificación y definición de cada uno de los servidores más usados en el mercado.

Tabla 1
Clasificación de servidores

Valor	Definición
De uso público	La distribución de este material no está limitada. Incluye información de marketing, materiales de venta e información seleccionada para uso público. Los datos incluidos en servidores de Internet públicos deben ser de uso público.
Sólo para uso interno	La revelación de esta información es segura para la distribución interna, pero puede provocar daños considerables a la organización si se hace pública. Debe colocarse por lo menos un servidor de seguridad entre esta información e Internet.
Confidencial de la empresa	La revelación de esta información puede provocar daños graves a la organización en conjunto. Esta información es del tipo más confidencial y sólo se expone si es absolutamente necesario. Deben colocarse por lo menos dos servidores de seguridad entre esta información e Internet.

http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch01secops.asp

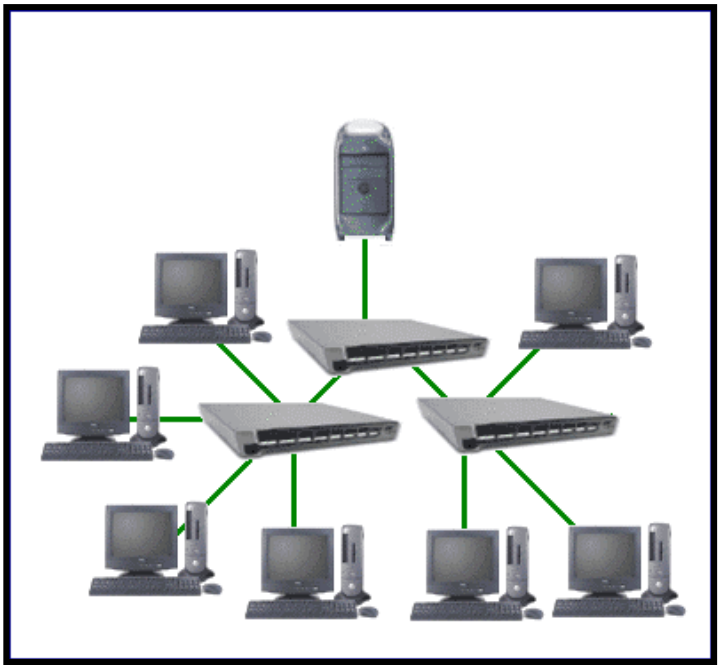
1.5.- Defensa de redes

Si dispone de una serie de redes en la organización, debe evaluarlas individualmente para asegurarse de que se ha establecido una seguridad apropiada. Si un enrutador sufre un ataque eficaz, puede denegar el servicio a partes enteras de la red.

Debe examinar el tráfico admisible en sus redes y bloquear el que no sea necesario. Así mismo, debe supervisar la existencia de detectores de paquetes en la red, que sólo deben usarse bajo controles estrictos.

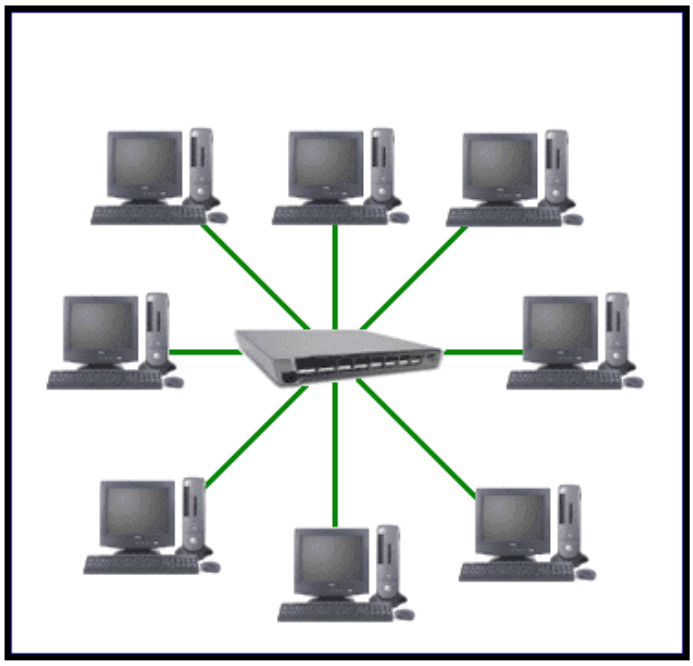
En los gráficos (gráfico 5 y gráfico 6) siguientes se muestra una configuración y conexiones diferentes en cada uno.

Gráfico 5
Conexión a través de un router



http://www.htmlweb.net/redes/topologia/topologia_2.html

Gráfico 6
Conexión a través de un concentrador / hub



http://www.htmlweb.net/redes/topologia/topologia_2.html

Cuando se tenga una red con un concentrador ya sea este HUB/MAU, el mismo no es tan seguro ya que al recibir la información esta se dispersa por todas las estaciones de trabajo preguntando cual es el dueño de la información que ha sido enviada y esta buscando destinatario, la mejor opción es aplicar un router o switch ya que este se dirige específicamente al host destinatario, el router busca su destinatario mediante el IP, y el swith mediante el código de la tarjeta de red.

1.6.- Defensa de perímetros

La protección del perímetro de su red es el aspecto más importante para detener los ataques externos. Si su perímetro permanece seguro, la red interna estará

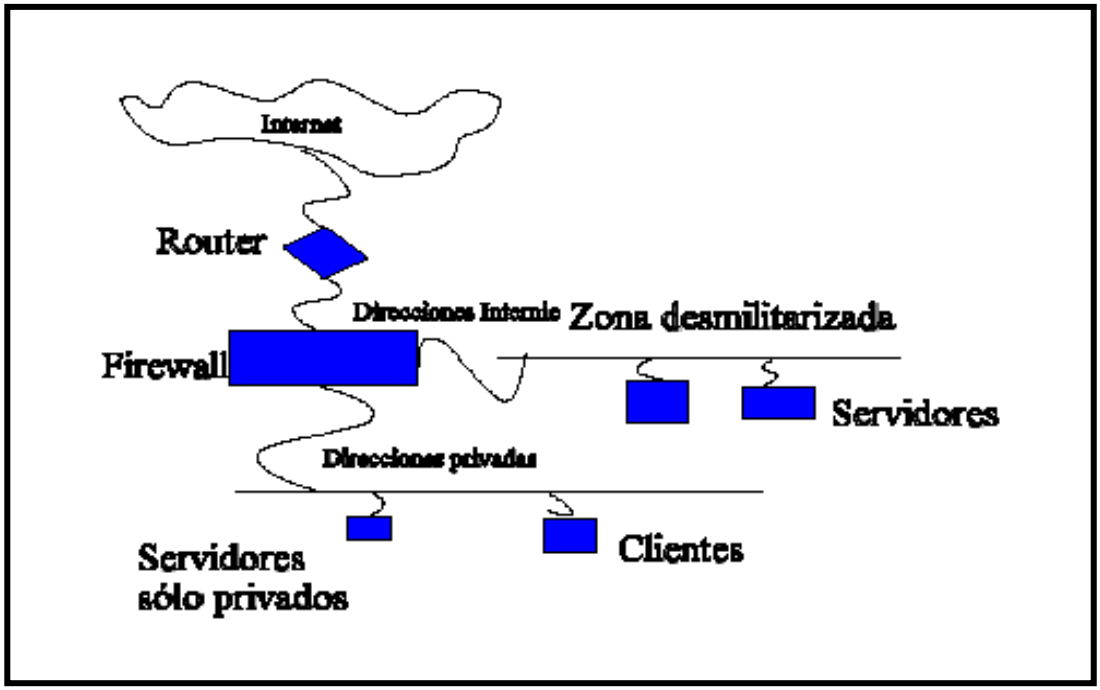
protegida de ataques externos. La organización debe disponer de algún tipo de dispositivo de seguridad para proteger cada punto de acceso a la red. Es necesario evaluar cada dispositivo, decidir qué tipos de tráfico se permiten y desarrollar un modelo de seguridad para bloquear el resto del tráfico.

Los servidores de seguridad son una parte importante de la defensa del perímetro. En algunos casos se necesitará uno o más servidores de seguridad para asegurarse de minimizar los ataques externos, junto con la auditoría y la detección de intrusiones para estar seguro de detectar los ataques en caso de que se produzcan.

También debe recordar que para las redes que permiten el acceso remoto, el perímetro puede incluir los equipos portátiles del personal e incluso los equipos domésticos. Deberá asegurarse de que estos equipos cumplen con los requisitos de seguridad antes de que se conecten a la red.

En el gráfico siguiente (gráfico 7) se muestra una configuración de un firewall.

Gráfico 7
Conexión de un firewall



http://arcos.inf.uc3m.es/~juange/ro/9899/98seguro.pdf

1.7.- Directivas y procedimientos

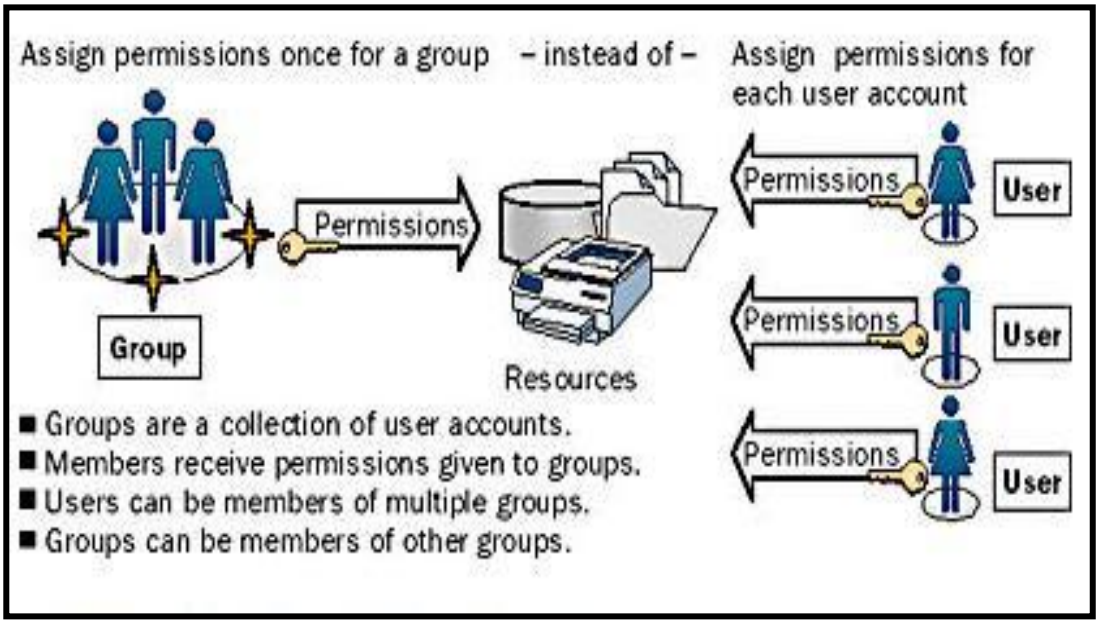
Casi todas las medidas descritas anteriormente están destinadas a evitar el acceso no autorizado a los sistemas. No obstante, está claro que habrá personas de su entorno que necesiten acceso de alto nivel a los sistemas. Toda estrategia de seguridad será imperfecta a menos que pueda garantizar que estas personas no van a hacer un uso indebido de los derechos que se les han concedido.

Respecto a los empleados existentes, resulta esencial que sean conscientes de las directivas de seguridad y de lo que está permitido y prohibido (y preferiblemente también por qué). Esto es importante por dos razones. En primer lugar, si los empleados no son conscientes de lo que está prohibido pueden llevar a cabo acciones que inconscientemente pongan en peligro la seguridad del entorno. En segundo lugar, si un empleado ataca de manera intencional su entorno de TI y no se ha prohibido explícitamente en las directivas de la empresa, puede resultar muy difícil entablar demanda contra esta persona.

Ningún empleado debe tener más acceso administrativo del que sea estrictamente necesario para realizar su trabajo.

En el gráfico siguiente (gráfico 8), se muestra un ejemplo de directivas y procedimientos.

Gráfico 8
Directivas y procedimientos



ms press - mcse training kit - microsoft windows 2000 network infrastructure. published by microsoft press 2003 by microsoft corporation

CAPÍTULO II

MÉTODOS DE ATAQUE COMUNES Y MEDIDAS PREVENTIVAS

Como parte de la estrategia de defensa en profundidad, debe comprender los métodos empleados por los atacantes y defenderse contra los ataques más comunes. En este capítulo se estudia una serie de tipos de ataques y se sugieren medidas para proteger su entorno contra los mismos.

2.1.- Obtención de información

Los atacantes siempre intentan conseguir información sobre su entorno. A veces la información resulta útil por sí misma y en otras ocasiones es un medio para conseguir otras informaciones y otros recursos.

La clave para evitar la obtención de información es restringir el acceso no autorizado a los recursos desde el exterior. Los métodos para conseguirlo incluyen:

- Asegurarse de que sólo dispositivos específicos e identificados de la red permiten la conectividad mediante acceso remoto. Una utilidad de búsqueda de módems debe comprobar todos los prefijos de empresas para

buscar dispositivos no autorizados (9). Los dispositivos de acceso remoto también se pueden detectar activando la detección de exploración en el sistema telefónico cuando esté disponible.

- Deshabilitar NetBIOS sobre TCP/IP, incluidos los puertos 135, 137 (Compartir impresoras y archivos para redes Microsoft" a través de NetBEUI), 139(compartir archivos y carpetas 9x y mell) y 445 (puerto 445 no haya sido tan explotado, es porque el atacante requiere también tener

(9)http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch02secops.asp 03 junio 2003

Internet a través del servidor de seguridad externo. Esto hace más difícil para las personas externas la utilización de redes estándar para conectarse a servidores.

- Habilitar sólo los puertos 80 y 443 (https) tanto en los adaptadores de red orientados a Internet y el servidor de seguridad para el tráfico destinado a un conjunto de servidores Web. De este modo se elimina la mayor parte de las técnicas de reconocimiento basadas en puertos.
- Revisar la información del sitio web público para asegurarse de que las direcciones de correo electrónico utilizadas en el sitio no son cuentas de administrador.
- La información general de la empresa publicada en el sitio es apropiada y no se puede utilizar para descubrir o deducir características del sistema de seguridad. Este tipo de información incluye sucesos actuales y recientes (10). Por ejemplo, si en el sitio web se anuncia que su empresa acaba de adquirir otra firma, los atacantes pueden elegir a la nueva adquisición

como objetivo pensando que su red se ha conectado precipitadamente a la nueva red corporativa y que por lo tanto, es menos segura.

- Administrar el tipo de contenido que contiene el código fuente del sitio web para evitar que un atacante revise este código para obtener información valiosa. Algunos de los elementos que el equipo de seguridad debe buscar en el código fuente son los comentarios incorrectos, las contraseñas incrustadas y las etiquetas ocultas.
- Revisar la información proporcionada al público en general para su dirección IP y los registros de nombre de dominio.
- *(10)http://webs.ono.com/usr009/Coburn44/Contrase.htm 3 de junio 2003* a

puerto 53 para comunicarse) para obtener la red de referencia o conseguir que realice una transferencia de zona completa. Para evitar que se interrogue al DNS, se pueden asignar derechos al servidor DNS de Windows 2000 mediante la opción notificar y habilitando las transferencias de zona sólo para los servidores autorizados. Otro enfoque consiste en implementar un DNS de sólo lectura con directivas y procedimientos para actualizarlo.

2.2.-Secuestro de sesión

Las herramientas de secuestro de sesión permiten a un atacante interrumpir, finalizar o apoderarse de una sesión en curso. Estos tipos de ataques suelen centrarse en las aplicaciones basadas en sesiones. Muchas herramientas de secuestro de sesión pueden visualizar varias sesiones de forma simultánea.

El peor destino que puede sufrir un administrador es que su servidor sea reventado. De hecho, aunque estos ataques pueden parecer dramáticos y suelen generar grandes titulares, no son nada si se los compara con un ataque real (11). Los intrusos reales no suelen anunciar su presencia ni hacen alarde de lo que consiguen, sino que instalan dispositivos de monitorización ocultos que furtivamente recogen la información de la red.

Dichas herramientas reciben el nombre de analizadores de protocolos, aunque también se las conoce como sniffers. El sniffing de paquetes es la práctica de capturar datos de red que no están destinados a la máquina, sino que generalmente

(11)http://ccia.ei.uvigo.es/docencia/SSI/SniffersPDF.pdf 4 de junio de 2003) su

correo. Por desgracia no existe una forma de detectar un sniffer de paquetes, puesto que es una actividad pasiva, sin embargo mediante la utilización de switches de red y backbones de fibra óptica (que son muy difíciles de pinchar) se puede minimizar la amenaza.

Los sniffers representan un alto nivel de riesgo, ya que:

- Pueden capturar contraseñas.
- Pueden capturar información confidencial o patentada.
- Pueden utilizarse para hacer mella en la seguridad de los entornos de red u obtener acceso por la fuerza.

De hecho, los ataques de sniffers han provocado acuerdos más serios que cualquier otro tipo de ataque. Para enfatizar este punto, rápidamente se comentará

que en el pasado por 1994, un ataque masivo de sniffers obligó a un centro de investigación naval a publicar la siguiente nota:

"En febrero de 1994, una persona no identificada instaló un sniffer de red en varios hosts y en varios elementos de backbones que recopiló más de 100.000 nombres de usuarios y contraseñas válidas a través de Internet y milnet (la primera y la más grande, se destinó para aplicaciones militares). Se considera que todos los equipos del sistema que permitan la existencia de registros de FTP, Telnet o remotos corren peligro".

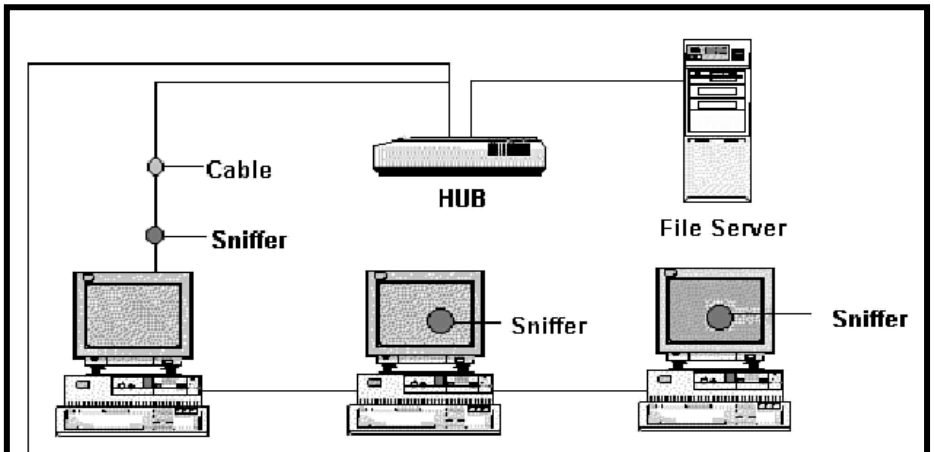
Un sniffer de paquetes es un programa de "pinchado" (wiretap), que se instala en una red y pueden ver todos los paquetes que circulan por ella.

Un Sniffer más que una herramienta de ataque en manos de un administrador de red puede ser una valiosa arma para la auditoría de seguridad en la red. Puesto que el acceso a la red externa debe estar limitado a un único punto (12). Un Sniffer puede ser la herramienta ideal para verificar como se está comportando la red.

A continuación se muestra un gráfico (gráfico 9) en donde se muestra como se instala un sniffer, en una red.

Gráfico 9

Sniffer



http://ccia.ei.uvigo.es/docencia/SSI/SniffersPDF.pdf

La mayoría de los sniffers tiene sus componentes entre los cuales son:

a).- El hardware

La mayoría de los productos trabajan con las tarjetas de red standard, aunque algunos requieren un hardware especial.

b).- Driver de captura

(12)http://www.idg.es/comunicaciones/articulo.asp?id=115341 *5 de junio de 2003*

Ésta es la parte más importante. Captura el tráfico de la red desde el cable, lo filtra según se desee y luego almacena los datos en el buffer.

c).- Buffer

Una vez que los paquetes son capturados desde la red, se almacenan en un buffer.Hay dos modos de captura distintos: captura hasta que el buffer se llene o usar el buffer donde los datos más recientes reemplazan a los más antiguos capturando los datos a velocidades de 100-mbps y generando un buffer que puede tener varios gigabytes de información.

d).- Análisis de Tiempo - Real

El programa pionero fue el “Network General Sniffer”; esta opción hace un análisis al por menor a nivel de bits de los frames mientras van por la red. Esto es capaz de encontrar una medida de la calidad de la red y de posibles fallos mientras a la vez captura la información (13). Por ejemplo: Network intrusion detection systems hace esto e incluso incorpora detección de posibles hackers.

e).- Decodificar

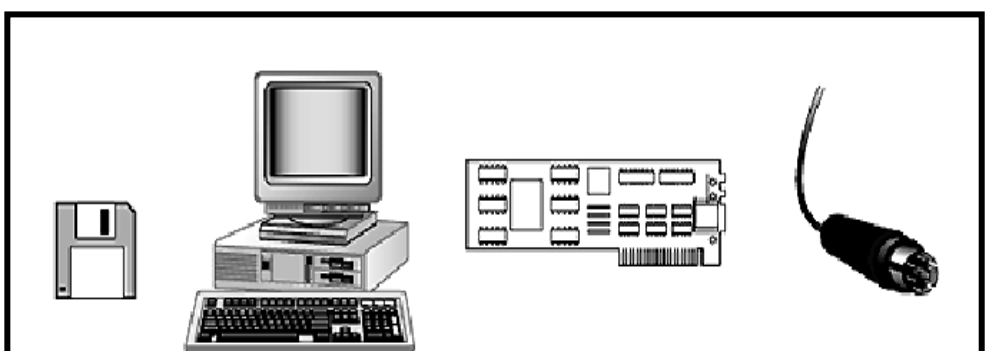
Esta opción muestra el contenido del tráfico de la red con un texto descriptivo para que el analista sepa qué está pasando.

(13)hackers beware. eric cole. publisher: new riders publishing. first edition august 13, 2001 *5 junio 2003*

Algunos programas contienen opciones que permiten editar los propios paquetes de red y transmitirlos luego a la red.

En el siguiente grafico (gráfico 10) se muestra los componentes que usa un usuario que ataca mediante un sniffer.

Gráfico 10
Elementos de uso de un sniffer

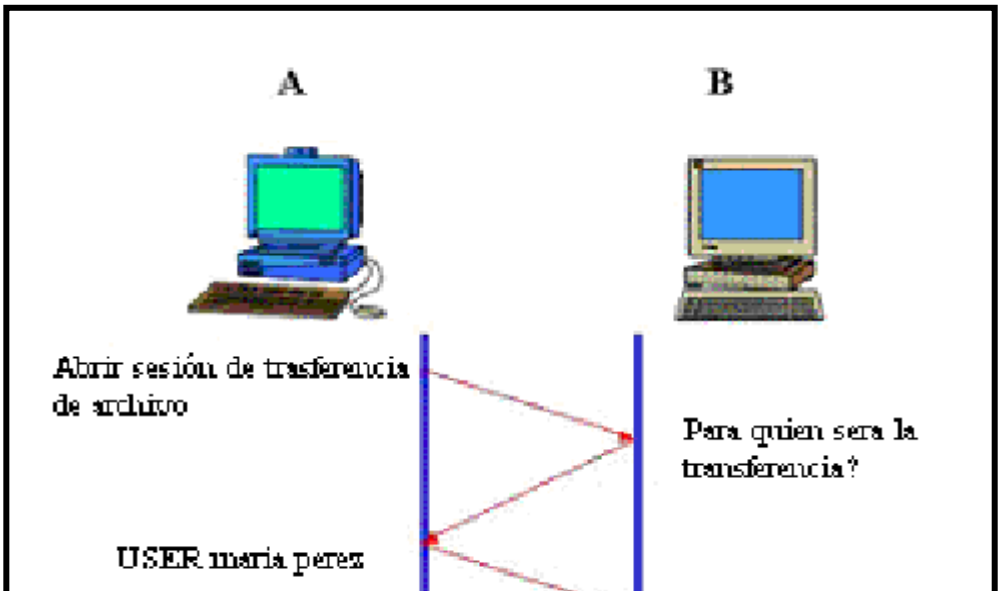


http://ccia.ei.uvigo.es/docencia/SSI/SniffersPDF.pdf

En el siguiente gráfico (gráfico 11) se muestra el proceso de conversación entre dos máquinas remotas, donde la identificación del usuario pasa abiertamente por la red de una máquina a otra. Este ejemplo es de transferencia de archivos vía FTP (14): (La máquina A inicia la conexión con la máquina B, que solicita la identificación del usuario. Al autenticarse en la maquina remota B el sniffer captura la clave.)

(14)http://glub.ehu.es/seguridad/ataques.html *06 de junio de 2003*

Captura de clave de un sniffer



http://ccia.ei.uvigo.es/docencia/SSI/SniffersPDF.pdf

Para saber cómo funciona un sniffer, necesita saber que cada ordenador de un LAN puede "ver" todos los paquetes de datos que son transmitidos dentro de la red (15). Así cada ordenador de la red puede ejecutar un programa sniffer para ver todos los paquetes y guardar una copia. Básicamente, los pasos seguidos por los atacantes son:

(1) El atacante penetra en su red, rompiendo una determinada máquina.

(2) Instala un programa sniffer.

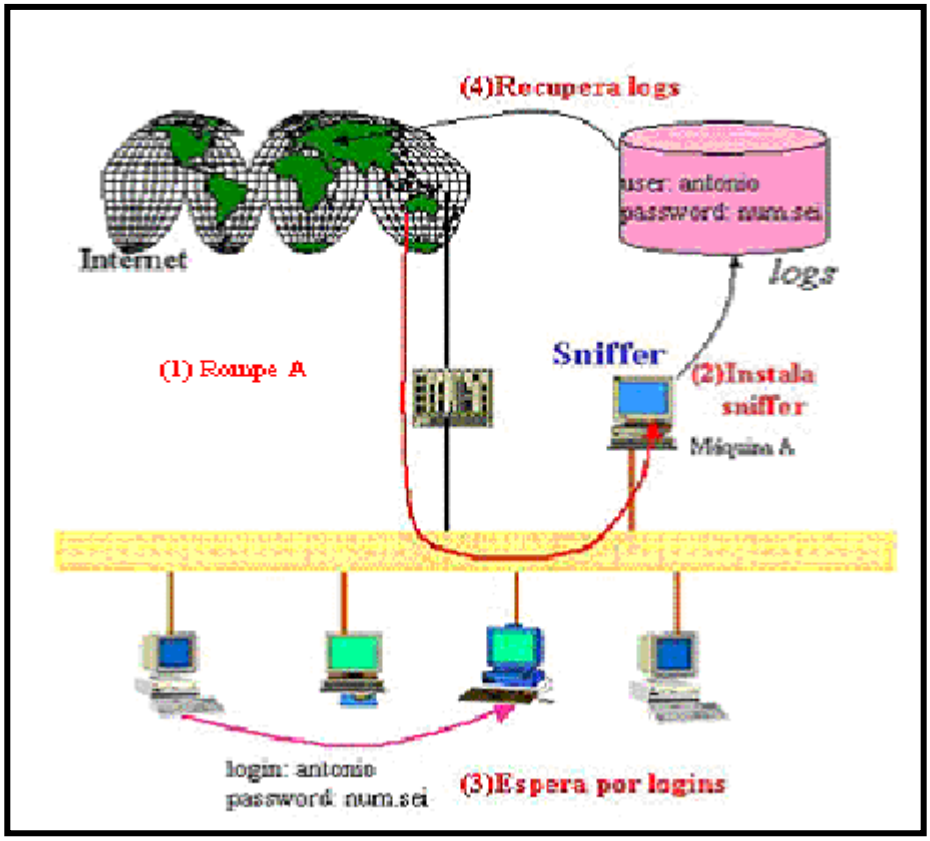
(3) Este programa monitoriza la red en busca de acceso a servicios de red, las

(15)http://gsyc.escet.urjc.es/docencia/asignaturas/itigtransmision_datos/transpas/node9.html *06 de junio de 2003*

(4) El archivo de logs es recuperado por el atacante.

A continuación se muestra en el gráfico 12 el funcionamiento de lo que esta detallado anteriormente.

Grafico 12
Funcionamiento de un Sniffer



http://ccia.ei.uvigo.es/docencia/SSI/SniffersPDF.pdf

Existen diversas razones que llevan a las personas a robar las claves, desde simplemente molestar a alguien (enviar un mail haciéndose pasar por ti) hasta practicar actividades ilegales (invadir otros ordenadores, robar otras informaciones, etc.)(16). Un atractivo para los hackers es la capacidad de utilizar la identidad de terceros en estas actividades.

(16)http://www.idg.es/comunicaciones/articulo.asp?id=115342 *06 junio de 2003*

s e instalar sniffers es poder capturar rápidamente el máximo número de cuentas

posibles, así cuantas más cuentas posea el atacante más fácil tiene el mantenerse escondido y puede hacerse pasar por otros usuarios “inocentes”.

A continuación se menciona algunos programas los más destacados.

a).- Linsniffer es sencillo y directo su propósito principal es capturar nombres de usuarios y contraseñas.

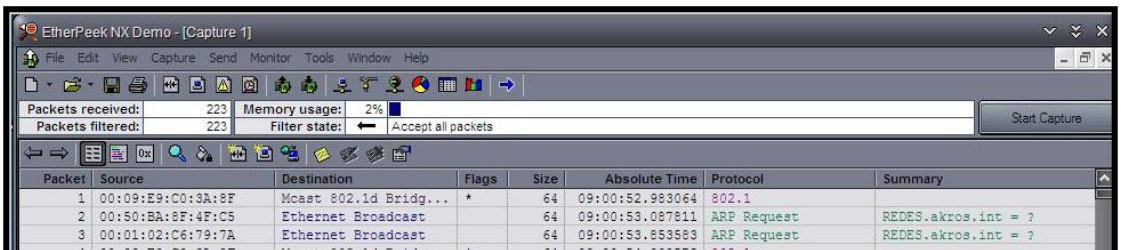
b).-Hunt permite especificar las conexiones determinadas en las que se esté interesado, en lugar de tener que vigilar y registrar todo.

c).- ANM Angel Network Monitor es un monitor de sistemas, monitorizará los tiempos de espera de las conexiones, los mensajes de conexión rechazada, etc.

d).- Iptraf Es una utilidad que utiliza una consola para ver las estadísticas de la red, recopila recuentos de bytes, paquetes de las conexiones TCP indicadores de actividad, estadísticas de la interfaz, interrupciones del tráfico de TCP/UDP y recuentos de bytes paquetes de las estaciones de LAN.

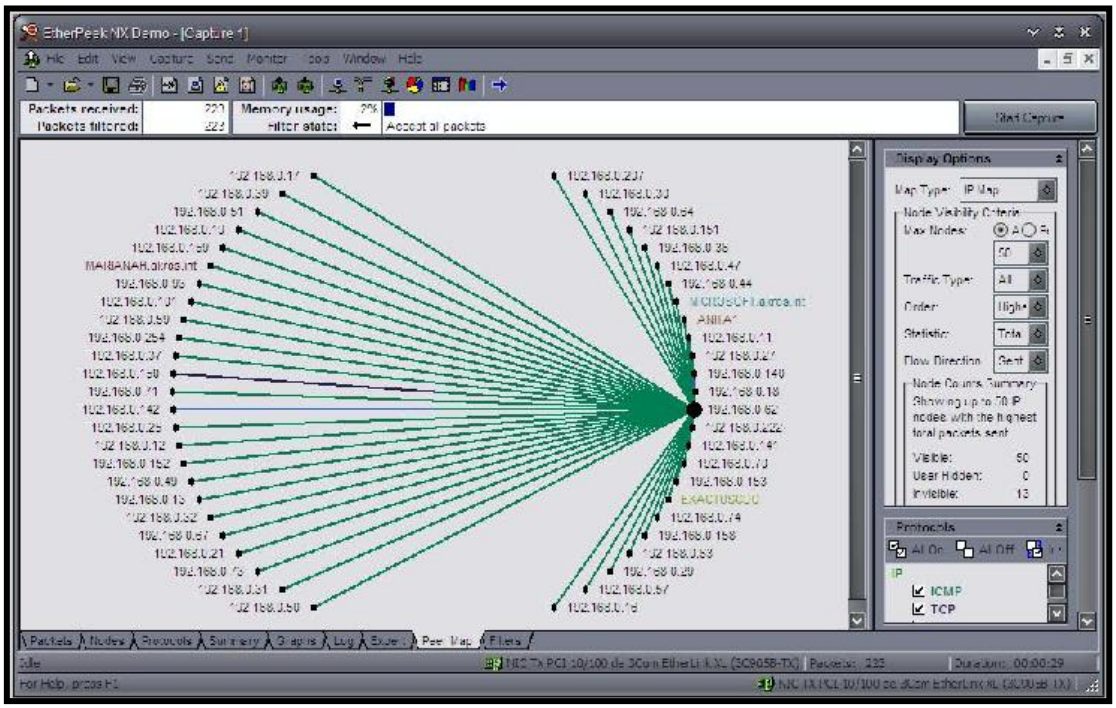
En los gráficos 13 y 14 se muestra la pantalla de un sniffer en funcionamiento.

Gráfico 13
Programa sniffer



hack proofing your network: internet tradecraft. ryan russell, stace cunningham, syngress2002.

Gráfico 14



hack proofing your identity in the information age teri bidwell, michael cross. syngress 2002

2.3.- Evitar que el DNS sea inalcanzable

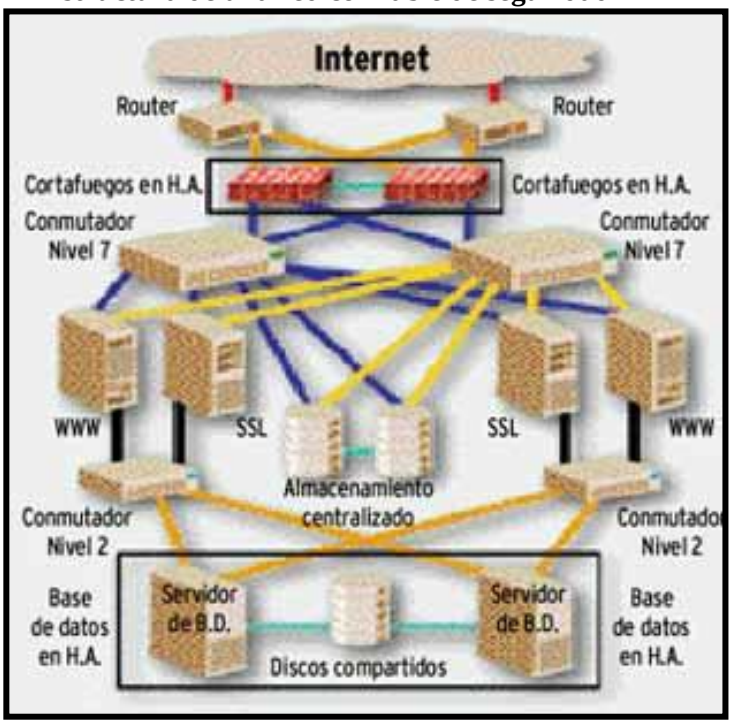
Los servidores DNS son una parte vital de cualquier red basada en Windows 2000. Todos los clientes de red consultan a los servidores DNS para ubicar servidores con los que necesitan comunicarse. Al atacar el DNS, un atacante puede utilizar el DNS inalcanzable. Por ejemplo, un atacante puede utilizar una variedad de técnicas de penetración para sobrescribir el archivo de caché del servidor DNS con información maliciosa. Como resultado, cuando un usuario consulta al DNS de producción, es reenviado a un servidor DNS fantasma que el atacante controla y puede utilizar para dañar el sistema. Se pueden utilizar los siguientes enfoques para evitar ataques al DNS:

- Utilice distintos servidores DNS para resolver solicitudes para la red interna y asegurarse de que estos servidores DNS no responden a solicitudes de equipos externos. Esto se denomina DNS dividido.
- Utilice un DNS de sólo lectura que no permita actualizaciones.
- Haga segura la base de datos de DNS mediante la seguridad de Active Directory y permitiendo únicamente las actualizaciones de DNS seguras.

En el gráfico siguiente (gráfico 15) se muestra una estructura de una red confiable de seguridad (lo más recomendado pero costoso) donde presenta los nuevos elementos necesarios para ofrecer transacciones en la red sin descanso. La idea principal que guía este diseño es una base de datos, mail, Internet y mas, es la necesaria para cualquier comercio, y el plus de seguridad que requiere esta actividad, junto con los imprescindibles servidores, complican estructura y los

métodos necesarios para eliminar los puntos únicos de fallo, a la vez que se mantiene la flexibilidad.

Gráfico 15
Estructura de una red confiable de seguridad



http://www.idg.es/comunicaciones/articulo.asp?id=115342

2.4.- Atacar el archivo de administrador de cuentas de seguridad

Atacando el archivo de administrador de cuentas de seguridad (SAM), un atacante puede obtener acceso a nombres de usuario y contraseñas. Una vez un atacante ha conseguido esta información, puede usarla para obtener acceso aparentemente legítimo a recursos de su red. Administrar el archivo SAM es por lo tanto un paso importante en la prevención de ataques. Los métodos para conseguirlo incluyen:

- Utilizar claves de sistema (Syskey) para habilitar cifrado adicional en el archivo SAM.
- Aplicar una directiva, utilizar otras formas de autenticación así como certificados y dispositivos biométricos.
- Establecer y aplicar una directiva de contraseñas complejas.

Las contraseñas hoy en día cualquier usuario normal disponen de muchas, sobre todo si utiliza servicios en Internet como cuentas de correo, foros o comunidades de acceso restringido a miembros. La tendencia natural es a unificar muchas de ellas al objeto de facilitar su manejo y recordarlas con facilidad. También se tiende a elegir contraseñas cortas, obviamente más cómodas hay que tener claro que establecer buenas contraseñas no es elegir una palabra más o menos larga y más o menos complicada o incoherente. Es más bien una cuestión de educación, de hábito. Por otro lado, si la contraseña es tan complicada que obliga al usuario a tenerla apuntada en un papel debajo del teclado (práctica más común de lo que se cree y buscar ahí de por sí es un método hacker) no cumple el objetivo de protección al que está destinada, una contraseña puede ser el punto más vulnerable de un sistema y el que tiene más probabilidades de ser atacado.

Se deberá usar recursos que faciliten que se familiarice con la contraseña para recordarla. Está claro que cualquiera puede recordar una secuencia de letras y signos al azar, pero esto puede resultar incomodo y el mismo produce a la larga el efecto "dejadez" con lo que no adelantamos. Hay que lograr un equilibrio razonable entre la seguridad y la comodidad.

En principio no se recomienda usar claves con una relación personal con el usuario, así como usar fechas significativas, números de teléfono, nombre de los hijos, novias etc.

Utilizar palabras con algún sentido (que no relación) para el usuario, pero combínenlas introduciendo entre ellas números y signos, pues la inclusión de signos no alfanuméricos y números, mayúsculas y minúsculas es otra de las normas de las contraseñas seguras. De esa forma, se obliga a un posible atacante a buscar en un rango mucho mayor de caracteres.

En ocasiones el usuario puede estar condicionado por los requisitos del sitio donde se vaya a establecer la contraseña, pues en algunos estas se restringen a letras y números.

Una contraseña larga de sólo minúsculas puede ser más segura que otra combinada de signos, letras y números, si esta es de menos caracteres. Si tiene ambas características, longitud y complejidad, mejor se puede incluir código ASCII utilizado en aquellos servicios que lo admitan, es una muy buena opción incluir algún carácter ASCII en el password.

Dicho código se compone de 255 símbolos que no figuran en el teclado.

2.5.- Ataques por denegación de servicio

Un atacante no necesita obtener acceso a un sistema para provocar problemas importantes. Los ataques por denegación de servicio implican una interrupción de

los recursos de un sistema suficiente para evitar que funcione normalmente. Algunos ejemplos incluyen el uso de todas las conexiones de red de un servidor o conseguir que un servidor de correo deba ocuparse de mucho más correo del que está diseñado para tratar. Los ataques por denegación de servicio pueden deberse a un ataque directo, o bien pueden estar provocados por virus.

Los ataques por denegación de servicio es el más común en los ataques en Internet. Cada semana se documentan nuevos ataques por denegación de servicio que se agregan a las bases de datos de seguimiento de errores. Deberá asegurarse de que siempre está al corriente sobre estos ataques y sobre cómo protegerse de los mismos.

Un ataque "denegación de servicio" esta caracterizado por un intento, por parte de los agresores, de evitar que los legítimos usuarios puedan utilizar un determinado servicio así como:

- Intento de "inundar" una red, impidiendo el trafico legítimo de esa red.
- Intento de romper la conexión entre dos máquinas, impidiendo el acceso a un servicio determinado.
- Intento de impedir el acceso de un usuario individual a un servicio.
- Intento de romper los servicios a un sistema especifico.

No todas las paradas de un servicio, que provengan de una actividad maliciosa, son necesariamente ataques "denegación de servicio". Otros tipos de ataque pueden incluir una denegación de servicio como una componente más. Ilegitimar

el uso de recursos puede también ser un ataque denegación de servicio. El impacto del ataque "denegación de servicio" esencialmente puede deshabilitar el equipo o la red. Dependiendo de la naturaleza de la empresa puede llegar a deshabilitar la organización entera. Algunos de esto ataques pueden ser llevados a cabo con un número limitado de recursos, afectando a redes mucho más sofisticadas (17). Estos tipos de ataques se llaman a veces "ataques asimétricos", así por ejemplo, un atacante con un viejo PC y un módem lento puede llegar a debilitar equipos más grandes y redes mucho mas sofisticadas.

Lo ataques "denegación de servicio" vienen dados en una variedad de formas y se dirigen hacia una gran variedad de servicios. Hay tres tipos básicos de ataque:

- Consumo de recursos, limitados o no renovables.
- Destrucción o alteración de información sobre configuración.
- Destrucción física o alteración de componentes de una red.

a).- Consumo de recursos limitados.

Tanto ordenadores y redes necesitan ciertas cosas para funcionar: ancho de banda para la red, memoria, espacio de disco, tiempo de CPU, estructuras de datos, acceso a otros equipos y redes, y unos ciertos recursos de entorno como son; potencia o aire frío.

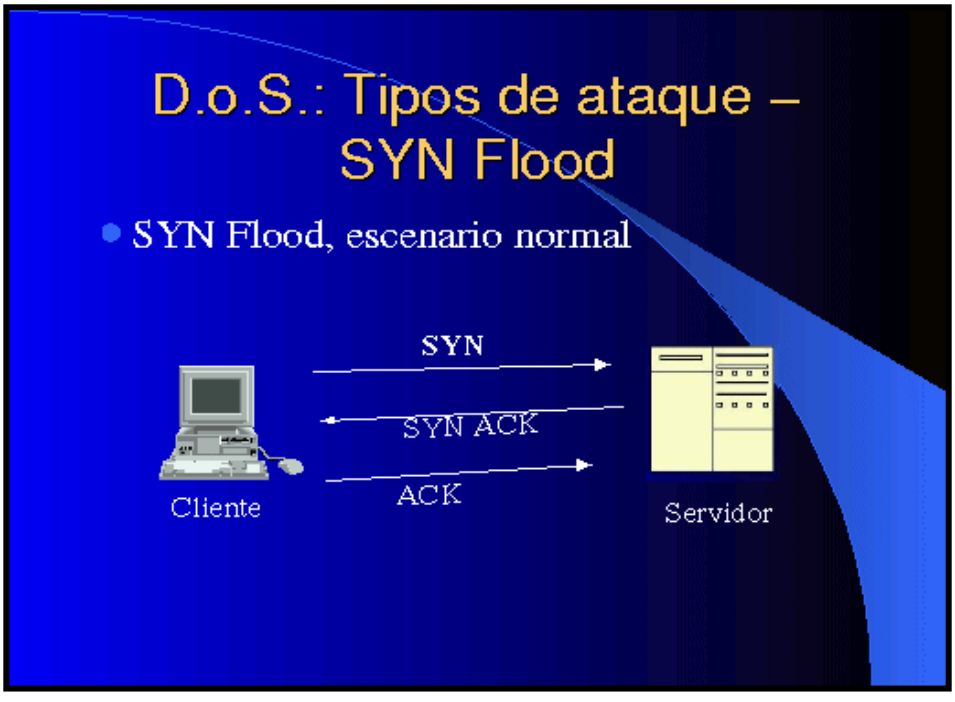
Los ataques por denegación de servicio se llevan a cabo frecuentemente contra la capacidad de conectividad entre redes. La intención es evitar que los equipos o las subredes se puedan comunicar con el resto de la red. Un ejemplo de este tipo de

ataque es el "SYN flood" en este tipo de ataque, se comienza por el proceso de establecimiento de conexión de la máquina víctima, la culminación del ataque llega cuando la máquina víctima ha reservado uno de los limitados números de estructuras de datos requeridos para completar la conexión. El resultado es que la legítima conexión se deniega mientras que la máquina víctima espera a que se complete la conexión, cosa que no llega a suceder. Hay que notar que este tipo de ataque no se pretende consumir ancho de banda sino los recursos de memoria y procesador que se consumen con las estructuras de datos usadas para establecer una comunicación. Esto implica que un atacante puede llevar a cabo su ataque desde un módem contra una red mucho más rápida.

Para evitar estos ataque se puede instalar filtros en routeadores, aumentar back Log, disminuir time out.

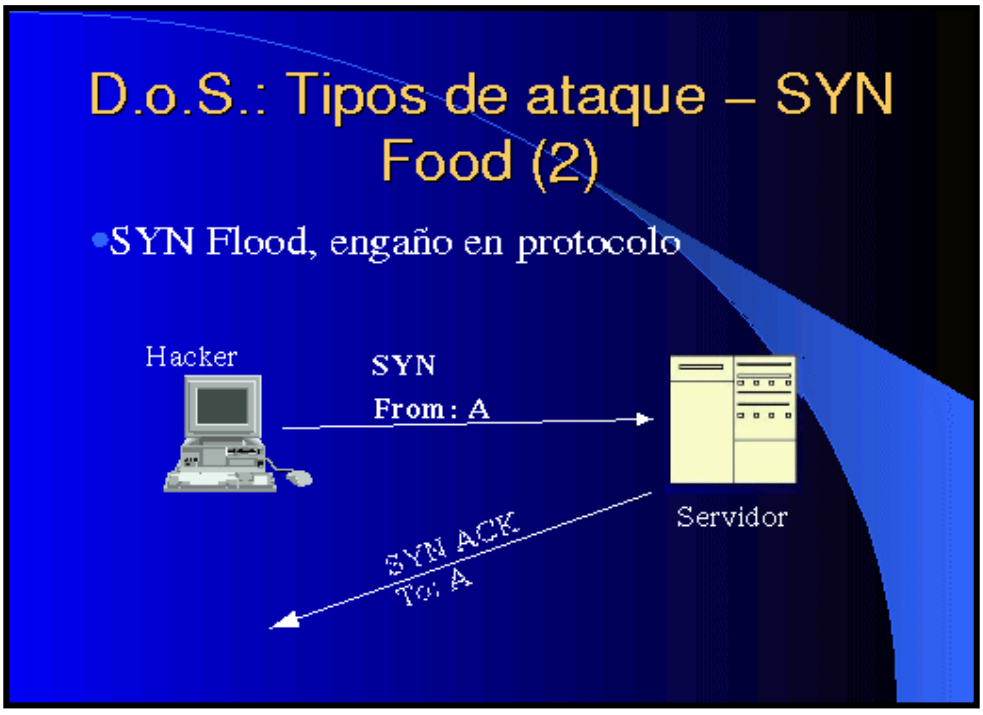
En los gráficos siguientes (gráfico 16 y 17) se indica como funciona este software denominado Syn Flood

Gráfico 16
Funcionamiento de un syn flood



http://www.dcc.uchile.cl/~hsalgado/dos/siframes.htm

Gráfico 17
Funcionamiento de un syn flood



http://www.dcc.uchile.cl/~hsalgado/dos/siframes.htm

Un intruso puede usar tus propios recursos contra ti de inesperadas maneras usando paquetes UDP perdidos para conectar el servicio de "echo" en la máquina que usa el servicio de otra máquina. El resultado es que los dos servicios consumen todo el ancho de banda disponible en la red.

UDP (Protocolo de Data gramas de Usuario) es un protocolo de transporte sin conexión previa de Internet, ofrece un mecanismo para enviar data gramas sin tener que establecer y liberar conexiones. Es un servicio no fiable ya que no agrega al mensaje IP funciones de confiabilidad, control de flujo y recuperación de errores. Por esto el UDP es mucho más ligero que TCP y como su encabezado es mucho mas pequeña genera menos carga en la red

UDP es un protocolo sencillo que implementa un nivel de transporte orientado a data gramas, NO orientado a conexión, NO fiable.

Los data gramas, son empleados para enviar rápidamente sencillos bloques de datos a una o más máquinas el servicio de data gramas ofrece una conexión no estable entre una máquina y otra. Los paquetes de datos son simplemente enviados o difundidos de una máquina a otra, sin considerar el orden en que estos llegan al destino, o si han llegado todos. El uso de data gramas no incrementa tanto el trafico de la red como el uso de sesiones,

En el siguiente gráfico (gráfico 18) se muestra un ataque de los paquetes UDP.

Gráfico 18
Ataques de paquetes udp

http://pin.uax.edu.mx/monica/tcpudp.html

Un intruso también puede ser capaz de consumir todo el ancho de banda disponible en la red generando una gran cantidad de paquetes dirigidos a la red pero en principio pueden ser de cualquier otro tipo. El intruso no tiene porque actuar desde una de las máquinas de la subred, puede ser capaz de coordinar varias máquinas de diferentes redes para obtener el mismo resultado (18).

Junto con el consumo de ancho de banda, los intrusos pueden ser capaces de consumir otros recursos que el sistema necesita para operar correctamente. Por ejemplo, hay sistemas en los que existen un número limitado de estructuras de datos para proporcionar información sobre procesos (identificadores de procesos, tablas de entradas de procesos, etc.). Muchos sistemas operativos modernos, aunque no todos, tienen cuotas para proteger contra estos ataques de todas formas,

si la tabla de procesos no está llena, la CPU puede estar ocupada con un gran número de procesos y el correspondiente tiempo para conmutar entre procesos. Un intruso también puede intentar consumir espacio de disco de otras maneras, por ejemplo;

- Generar excesivo número de mensajes de correo.

En general, cualquier cosa que permita datos en disco, puede ser utilizada para llevar a cabo un ataque denegación de servicio. Por otro lado en algunos lugares, aparece el mensaje "lockout" después de un cierto número de intentos fallidos de acceso a una determinada cuenta, normalmente 3 o 5. Un intruso puede usar este hecho para evitar el acceso a la cuenta a su legítimo usuario. En algunos casos las cuentas con privilegios suelen ser blancos de estos ataques. Lo mejor es estar seguro de tener un método alternativo para acceder al sistema en caso de emergencia. Un intruso puede hacer que un sistema se venga abajo o que se vuelva inestable enviando datos inesperados a través de la red. Si el sistema se

e.

Hay otras cosas que pueden ser vulnerables para un ataque denegación de servicio y que es conveniente monitorizar:

- Impresoras.
- Cintas de backup.
- Conexiones a redes.
- Cualquier recurso importante para las operaciones de la empresa.

b).- Destrucción o alteración de los datos de configuración

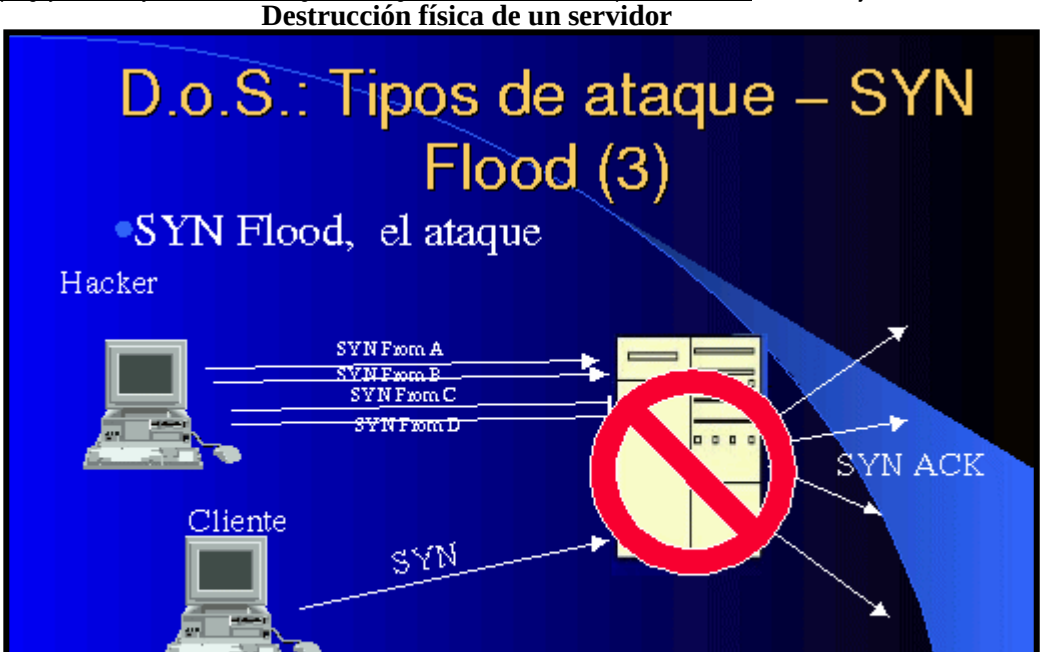
Un equipo mal configurado puede no operar correctamente o dejar de hacerlo. Un intruso puede alterar o destruir la información de la configuración evitando así el uso correcto del equipo o de la red (19). Por ejemplo, si un intruso puede cambiar la información sobre las rutas, la red puede venirse abajo. Si es capaz de modificar el registro de una máquina NT, ciertas funciones pueden dejar de funcionar.

c).- Destrucción física o alteración de componentes de red

Lo primero que se debe hacer para evitar este tipo de ataques es salvaguardar la seguridad física de lo equipos contra accesos, sin autorización, a ordenadores, routers, redes, segmentos de red, generadores de potencia, estaciones refrigeradas, y cualquier otro componente crítico.

En el gráfico siguiente (gráfico 19) se muestra un ataque en el cual saturan al servidor y este colapsa.

Gráfico 19
Destrucción física de un servidor



(19)http://gsyc.escet.urjc.es/docencia/asignaturas/itig/transmision_datos/transpas/node9.html 10 de junio de 2003

http://www.dcc.uchile.cl/~hsalgado/dos/siframes.htm

Los ataques por denegación de servicio pueden suponer una importante pérdida de tiempo y dinero para la mayoría de las organizaciones. Recomendamos considerar las siguientes opciones dependiendo de las necesidades personales:

- Implementar routers pues esto disminuirá la exposición a ciertos ataques. Adicionalmente, esto puede prevenir que usuarios de tu red lancen ciertos ataques.
- Si es posible, instalar parches para protegerse contra ataques. Esto puede reducir substancialmente la exposición a estos ataques, aunque no elimina el riesgo por completo.
- Desactivar cualquier servicio de red que no sea necesario. Esto puede limitar la capacidad del intruso de utilizar estos servicios para realizar su ataque.

- Activar mecanismos de cuota en el sistema operativo si es posible. Por ejemplo si el sistema operativo soporta cuotas de disco, activarlas para todas las cuentas, especialmente para cuentas que operan con servicios de red. Además si el sistema operativo soporta particionado de discos, es conveniente considerar particionar sistemas de ficheros para separar funciones críticas de otras actividades.
- Observar el rendimiento y estabilidad de las líneas básicas de la actividad cotidiana. Observar niveles inusuales de actividad de disco, uso de CPU o tráfico de red.
- Examinar rutinariamente la seguridad física. Considerar servidores, routers, terminales, puntos de acceso a la red y otros componentes del sistema.
- Activar en la red configuraciones redundantes y tolerantes a fallos.
- Establecer y mantener calendarios y políticas de backup, sobre todo para información importante sobre configuración.
- Establecer y mantener políticas de claves apropiadas, especialmente para acceso a cuentas con privilegios como es la de root. Muchas organizaciones pueden sufrir perdidas financieras como resultado de estos ataques y pueden decidir presentar cargos contra el intruso.
- Mantenga los sistemas actualizados con las revisiones de seguridad más recientes (service packs).

- Desarrolle un plan de defensa con su proveedor de servicios de Internet (ISP) que permita responder con rapidez a un ataque cuyo objetivo sea el ancho de banda entre su ISP y la red de perímetro.

2.6.- Ataques por la puerta trasera

Para evitar que los atacantes descarguen información del sistema, debe protegerse contra la posibilidad de que un atacante utilice un caballo de troya (un programa dentro de otro programa) para instalar una puerta trasera en el sistema. Normalmente, esta es una cuestión que atañe más bien al cliente que a un servidor totalmente seguro. Sin embargo, un atacante puede utilizar este tipo de mecanismo para atacar a un usuario en una estación de trabajo del administrador y luego utilizar ese sistema para lanzar ataques en una red de perímetro de producción.

Por ejemplo, Back Orifice 2000 es un programa de puerta trasera que permite a los atacantes controlar remotamente un equipo a través de la red, capturar pulsaciones de teclas y utilizar la información para convertirse en usuario de una estación de trabajo de la red, las nuevas versiones de Back Orifice crean distintas mutaciones que los antivirus no detectan. También se ejecuta en modalidad sigilosa y no aparece en la lista de tareas porque el tamaño de su huella es inferior a 100 kilobytes (KB). Back Orifice es tan sólo uno de muchos programas de puerta trasera. Puede evitar que este tipo de ataques tengan resultado con las siguientes medidas:

- Ejecutar una búsqueda de virus completa y mantener la herramienta antivirus actualizada con las firmas más recientes.
- Prestar atención a todo el contenido enviado a través del correo electrónico y restringir la ejecución de datos adjuntos desconocidos.
- Ejecutar herramientas como el explorador de Internet Security Systems (ISS), para comprobar en toda la red la presencia de herramientas de ataque como Back Orifice, asegurándose de que la base de datos del explorador esté actualizada.
- Aceptar únicamente controles Microsoft ActiveX® firmados.
- Educar a los usuarios acerca de los peligros de instalar programas desconocidos, abrir datos adjuntos dudosos o descargar contenido de Internet sin firma o desconocido.

En el siguiente gráfico (gráfico 20) se muestra el entorno del programa Back orifice.

Gráfico 20
Programa back orifice

www.cultdeadcow.com

2.7.- Código malicioso

Todo código ejecutable representa un posible riesgo para su organización. El código malicioso puede adoptar la forma de código perjudicial que se propaga dentro de las organizaciones y entre ellas (por ejemplo, a través del correo electrónico) o bien puede ser código deliberadamente ejecutado desde el interior de una organización con finalidades maliciosas.

El código malicioso se puede clasificar básicamente en cuatro tipos principales:

- Virus.
- Gusanos.
- Caballos de Troya.
- Otros tipos de código malicioso.

En la tabla siguiente (tabla 2) se muestra las definiciones y funciones de estos códigos maliciosos.

Tabla 2
Tipos de código malicioso

Tipo de código malicioso	Descripción

Virus	Infecta a otro programa, sector de inicio, sector de partición o archivo insertándose o adjuntándose a ese medio. Luego se replica a otros equipos a partir de ese punto. Es posible que los virus sólo se repliquen, pero muchos también dañarán los sistemas que infecten.
Gusano	Se copia a sí mismo de una unidad de disco a otra o a través de la red mediante el correo electrónico u otro mecanismo de transporte. Puede dañar y poner en peligro la seguridad del equipo.
Caballo de Troya	No se replica por sí mismo, pero su funcionalidad maliciosa está escondida en otros programas que parecen tener alguna utilidad, por lo que suele pasarse a otros equipos (a menudo puede presentarse en forma de programa de broma). Una vez presente en un sistema, dañará o pondrá en peligro la seguridad del equipo, lo que puede ser el primer paso para permitir el acceso no autorizado.
Otros tipos de código malicioso	Código ejecutable que daña el entorno, ya sea de forma intencionada o no,

http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch02secops.asp

Las utilidades antivirus evitarán la ejecución de muchos tipos de código malicioso, pero no de todos. Si evita el acceso a CD-ROM, discos y otros dispositivos de entrada y salida, se protegerá aún más contra muchos tipos de este código, aunque no podrá evitar el código escrito en sistemas internos. El código también se puede enviar por correo electrónico a una persona de su organización. Aunque el tipo de datos adjuntos no esté permitido, esto se puede burlar fácilmente cambiando la extensión del archivo para introducirlo en la organización y volviéndola a cambiar para ejecutarlo.

CAPÍTULO III

ADMINISTRAR LA SEGURIDAD CON LA DIRECTIVA DE GRUPO DE WINDOWS 2000

En un entorno basado en Windows 2000, esto se lleva a cabo principalmente por medio de la directiva de grupo.

Antes de comenzar con la explicación se debe saber que un grupo es un conjunto de usuarios, equipos, contactos y otros grupos. Los grupos se pueden utilizar como conjuntos de distribución de correo electrónico o de seguridad. Los grupos de distribución sólo se utilizan para correo electrónico. Los grupos de seguridad se utilizan como listas de distribución de correo electrónico y para permitir el acceso a los recursos. En el caso de clústeres de servidores, conjunto de recursos administrados como un único objeto. Normalmente, un grupo contiene todos los recursos necesarios para ejecutar una aplicación o un servicio específico

(20). Un grupo pertenece en cualquier momento a un único nodo. La migración y la recuperación tras error siempre actúan sobre los grupos. También se conocerá que una directiva es un mecanismo por el que los valores del escritorio se configuran automáticamente, de la forma establecida por el administrador.

3.1.- Importancia de utilizar la directiva de grupo

El objetivo de las directivas de seguridad es definir los procedimientos de configuración y administración de la seguridad del entorno. La directiva de grupo de Windows 2000 puede ayudarle a implementar las recomendaciones técnicas de la directiva de seguridad para todas las estaciones de trabajo puede utilizar la Directiva de grupo para implementar una configuración de seguridad específica para determinadas funciones del servidor.

(20)http://www.microsoft.com/windows2000/es/server/help/default.asp?url=/windows2000/es/server/help/sag_ADgroups_7migration.htm 16 junio 2003

Si utiliza la directiva de grupo para implementar la configuración de seguridad, puede garantizar que todos los cambios realizados en una directiva se apliquen a todos los servidores que la utilizan y que los servidores nuevos obtengan automáticamente la nueva configuración.

La directiva de grupo se puede abrir de varias maneras en función de la acción que se desea realizar con el complemento.

La configuración de directiva de grupo define los distintos componentes del entorno de escritorio del usuario que tiene que administrar un administrador del sistema; por ejemplo, los programas que se encuentran disponibles para los

usuarios, los programas que aparecen en el escritorio del usuario y las opciones del menú inicio (21). Para crear una configuración específica de escritorio para un grupo de usuarios en particular, se utiliza el complemento directiva de grupo. La configuración de directiva de grupo que se especifique está contenida en un objeto de directiva de grupo que a su vez está asociado a objetos seleccionados de Active Directory, sitios, dominios o departamentos.

Directiva de grupo es la herramienta primaria del administrador para modificar y controlar cómo los programas, los recursos de red y el sistema operativo se comportarán con los usuarios y equipos en una organización.

3.2.- Cómo aplicar la Directiva de grupo

(21)http://www.microsoft.com/spanish/msdnlarquitectura/das_docIChapter1_Introduction.doc 17 junio 2003

Los usuarios y los equipos son los únicos tipos de objetos de Active Directory que reciben directivas. Específicamente a los grupos de seguridad no se les aplica directivas. En lugar de ello, por motivos de rendimiento, los grupos de seguridad se usan para filtrar la directiva por medio de una entrada de control de acceso (ACE) aplicar directiva de grupo, la cual se puede configurar para permitir o denegar, o dejar sin configurar.

3.2.1.- Orden de aplicación

Las directivas se aplican en este orden:

1. El objeto de directiva de grupo local único.
2. Objetos de directiva de grupo del sitio, en orden especificado administrativamente.
3. Objetos de directiva de grupo del dominio, en orden especificado administrativamente.
4. Objetos de directiva de grupo del departamento, de departamento mayor a menor (de departamento principal a secundario), y en orden especificado administrativamente en el nivel de cada departamento.

De forma predeterminada, las directivas aplicadas posteriormente sobrescriben las directivas aplicadas con anterioridad cuando las directivas son incoherentes (22). Sin embargo, si no hay incoherencias de configuración, tanto las directivas anteriores como las posteriores contribuyen a la directiva efectiva.

3.2.2.- La directiva se puede filtrar por medio de la pertenencia a un grupo de seguridad

(22)http://www.microsoft.com/spanish/msdnlarquitectura/das_doc\Chapter1_Introduction.doc 17 junio 2003

Una ACE para un grupo de seguridad en un objeto de directiva de grupo puede establecerse como no configurada (no hay preferencia), permitida o denegada donde denegada tiene prioridad sobre permitida.

Las directivas que normalmente se heredarían de sitios, dominios o departamentos superiores se pueden bloquear en el nivel del sitio, dominio o departamento.

Las directivas que de otro modo serían sobrescritas por directivas de departamentos secundarios pueden configurarse como no anular en el nivel de objeto de Directiva de grupo.

Los grupos en Microsoft Windows 2000 son objetos del servicio de directorio Active Directory o del equipo local que pueden contener usuarios, contactos, equipos a otros grupos. Sin embargo en general, un grupo es normalmente una colección de cuentas de usuario (23). El objetivo de los grupos es simplificar la administración permitiendo al administrador de la red asignar derechos y permisos por grupo en lugar de a usuarios individuales.

Cuando se crea un grupo, se le asigna un ámbito de grupo que define cómo se asignaran los permisos. Las tres posibilidades de ámbitos de grupo son: global, local de dominio y universal.

Dominio Local: Se utilizan para garantizar permisos dentro de un único dominio, los miembros de los grupos de dominio local puede incluir solamente cuentas

(23)http://www.microsoft.com/windows2000/es/advanced/help/default.asp?url=/windows2000/es/advanced/help/sag_SEconceptsUnAudLoc.htm 19 junio 2003

Global: Se utilizan para otorgar permisos a objetos en cualquier dominio en el árbol de dominio o en el bosque. Los miembros de los grupos globales pueden incluir solamente cuentas y grupos del dominio en el que están definidos.

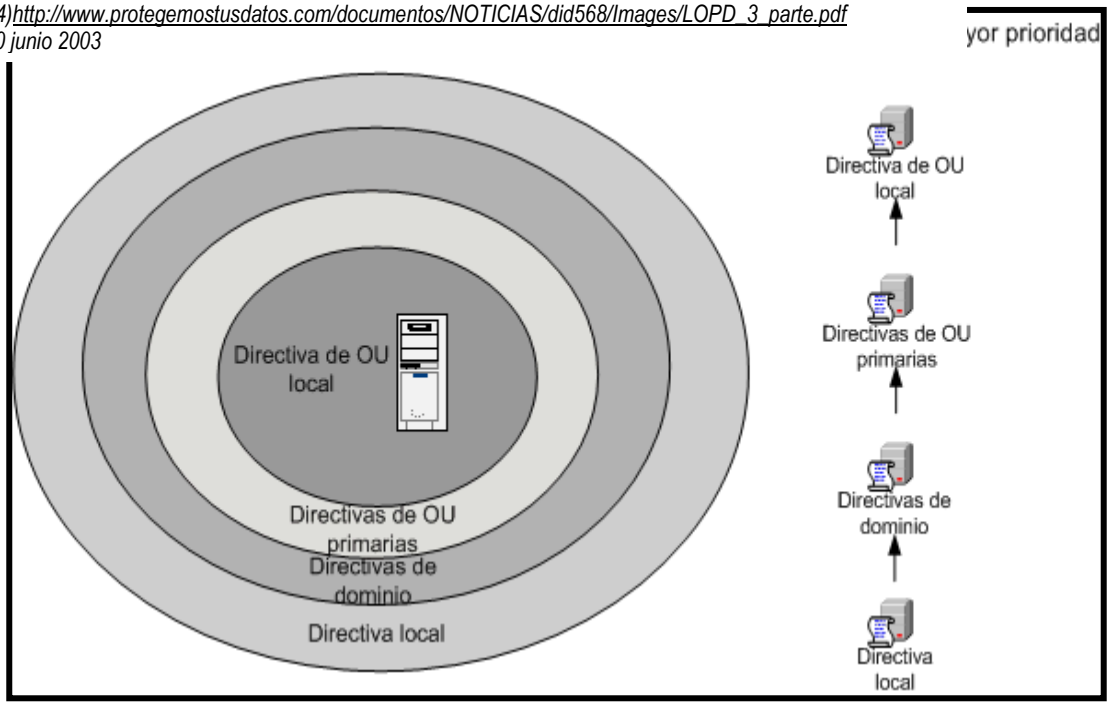
Universal: Se utilizan para otorgar permisos a gran escala en el árbol de dominio o en el bosque. Los miembros de los grupos globales son las cuentas y grupos de cualquier dominio en el árbol de dominio o en el bosque.

Para utilizar la directiva de grupo de forma segura y eficaz, es especialmente importante comprender cómo aplicarla. Un objeto de usuario o de equipo puede estar sujeto a varios GPO (Objetos de directiva de grupo) (24). Éstos se aplican de forma secuencial y la configuración se acumula, excepto cuando se produce un conflicto, en cuyo caso la configuración de las directivas posteriores prevalecerá sobre la configuración de directivas anteriores de forma predeterminada.

En el siguiente gráfico (gráfico 21), se muestra la jerarquía de aplicación de GPO

Gráfico 21
Jerarquía de aplicación de GPO

(24)http://www.protegemostusdatos.com/documentos/NOTICIAS/did568/Images/LOPD_3_parte.pdf
20 junio 2003



http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch03secops.asp

3.2.3.- Grupos locales predefinidos

Los servidores tienen grupos locales predefinidos que otorgan derechos para realizar tareas en una única maquina.

- **Administradores:** Sus miembros pueden realizar todas las tareas administrativas en el equipo. La cuenta predefinida Administrador que se crea cuando se instala el sistema operativo es un miembro del grupo.
- **Duplicadores:** No se deben añadir cuentas de usuario de usuarios a este grupo. Si es necesario se puede usar una cuenta de usuario "ficticia" a este grupo para permitir iniciar sesión en los servicios replicador de un controlador de un dominio para administrar la replica de archivos y directorios (25).
- **Invitados:** Sus miembros sólo pueden realizar tareas para las cuales el administrador haya concedido permisos. Los miembros solo pueden utilizar aquellos recursos para los que un administrador haya concedido permisos especificamente.
- **Operadores de copia:** Sus miembros pueden iniciar sesión en el equipo, hacer copia de seguridad, recuperar la información del equipo y apagar el equipo. Los miembros no pueden cambiar la configuración de seguridad. No hay miembros predeterminados en el grupo.
- **Usuarios:** Los miembros de este grupo pueden iniciar sesión en el equipo, acceder a la red, almacenar documentos y apagar el equipo. Los miembros

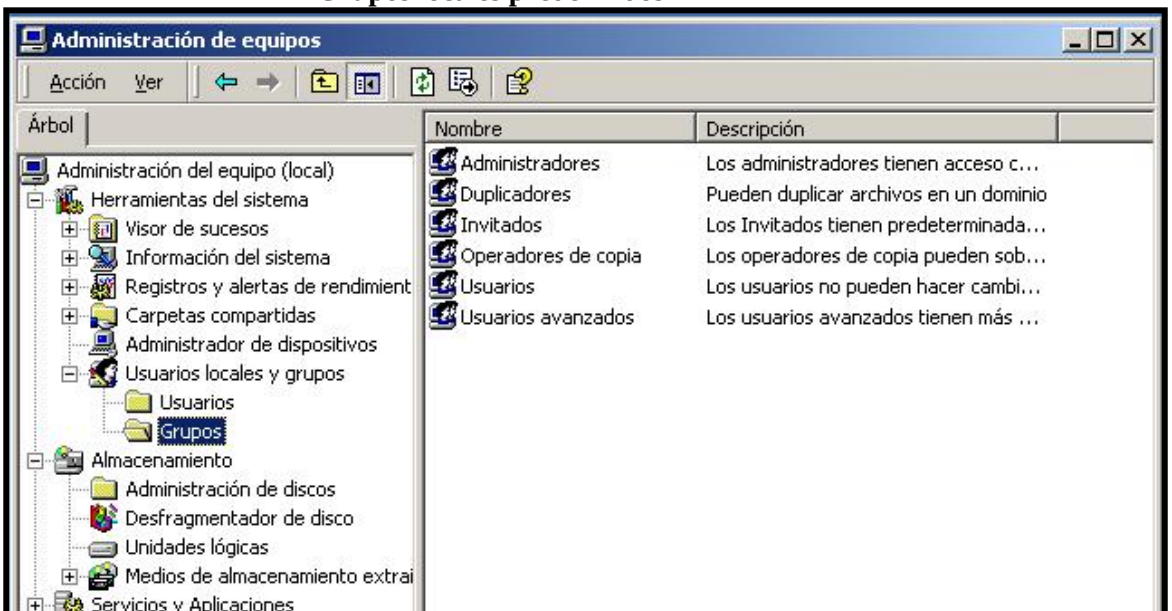
(25) http://fmc.axarnet.es/win2000srv/tema-10/tema_10_m.htm 24 junio 2003

no pueden instalar programas o hacer cambios en el sistema. Cuando un servidor miembro o una máquina Windows 2000 Profesional se une a un dominio, el grupo usuarios del dominio se añade a este grupo.

- **Usuarios avanzados:** Sus miembros pueden crear y modificar cuentas de usuario e instalar programas en el equipo local pero no pueden ver los archivos de otros usuarios.

En el gráfico siguiente (gráfico 22) se muestra los grupos locales predefinidos.

Gráfico 22
Grupos locales predefinidos



3.3.- Estructura de la directiva de grupo

Las opciones de configuración de la directiva de grupo se almacenan en dos ubicaciones:

- GPO - situados en Active Directory
- Archivos de plantillas de seguridad - situados en el sistema de archivos local

Los cambios realizados en el GPO se guardan directamente en Active Directory, mientras que los cambios realizados en los archivos de plantillas de seguridad se deben volver a importar al GPO dentro de Active Directory para poder aplicarlos.

3.4.- Formato de las plantillas de seguridad

Las plantillas de seguridad son archivos de texto. Para modificar los archivos de plantillas, se pueden utilizar las plantillas de seguridad del complemento de MMC o un editor de texto como el block de notas.

Windows 2000 incluye varias plantillas de seguridad incrementales. Estas plantillas se almacenan de forma predeterminada.

Estas plantillas predefinidas pueden personalizarse mediante el complemento plantillas de seguridad de Microsoft Management Console (MMC) y pueden importarse en la extensión configuración de seguridad del complemento directiva de grupo.

Estas plantillas de seguridad están construidas asumiendo que se aplicarán a equipos con Windows 2000 que utilizan la configuración de seguridad predeterminada para Windows 2000 (26). En otras palabras, estas plantillas modifican incrementalmente la configuración de seguridad predeterminada si están presentes en el equipo, no instalan la configuración de seguridad predeterminada para después hacer las modificaciones.

No puede aplicar seguridad a sistemas Windows 2000 instalados en sistemas de archivos FAT.

Plantillas de seguridad es una herramienta para crear y asignar plantillas de seguridad a uno o más equipos. Una plantilla de seguridad es una representación de un archivo físico de una configuración de seguridad y puede ser aplicada a un equipo local o importada a un objeto de directiva de grupos en Active Directory.

(26)http://usuarios.lycos.es/victordc/Redes1/protegiendo_la_red.htm 25 junio 2003

Cuando se importa una plantilla de seguridad a un objeto de directiva de grupos, directiva de grupos procesa la plantilla y realiza los cambios correspondientes a los miembros de ese objeto de directiva de grupos, que pueden ser usuarios o equipos.

Las plantillas de seguridad predefinidas son:

- Estación de trabajo predeterminada (basicwk.inf)
- Servidor predeterminado (basicsv.inf)
- Controlador de dominio predeterminado (basicdc.inf)
- Servidor o estación de trabajo compatible (compatws.inf)
- Servidor o estación de trabajo segura (securews.inf)
- Servidor de estación de trabajo de alta seguridad (hisecws.inf)
- Controlador de dominio dedicado (dedicadc.inf)
- Controlador de dominio seguro (securedc.inf)
- Controlador de dominio de alta seguridad (hisecdc.inf)

Las plantillas fueron diseñadas para cumplir cinco requisitos comunes de seguridad entre las cuales se mencionará algunas:

- Básica (basic*.inf)

  Las plantillas de configuración básica se suministran como medio para invertir la aplicación de una configuración de seguridad diferente. Las configuraciones básicas aplican los valores de seguridad predeterminados de Windows 2000 a todas las áreas de seguridad salvo las relativas a

derechos de usuario. Éstas no se modifican en la plantilla básica ya que los programas de instalación de aplicaciones suelen modificar los derechos de usuario para permitir que se pueda utilizar la aplicación. Los archivos de configuración básica no tienen por objeto deshacer dichas modificaciones.

- Compatible (compat*.inf)

  La configuración de seguridad predeterminada de Windows 2000 proporciona a los miembros del grupo local usuarios una configuración de seguridad estricta, mientras que los miembros del grupo local usuarios avanzados tienen una configuración de seguridad compatible con las asignaciones de usuarios de Windows NT 4.0. Esta configuración predeterminada permite la ejecución de aplicaciones certificadas para Windows 2000 en el entorno estándar de Windows para el grupo usuarios, pero permite la ejecución correcta de aplicaciones no certificadas para Windows 2000 con la configuración menos segura del grupo usuarios avanzados. No obstante, puede resultar poco seguro en algunos entornos que usuarios de Windows 2000 sean miembros del grupo usuarios avanzados para poder ejecutar aplicaciones no certificadas para Windows 2000. Algunas organizaciones pueden preferir asignar usuarios de forma predeterminada sólo como miembros del grupo usuarios y después reducir los privilegios de seguridad de este grupo hasta el nivel donde se ejecuten correctamente las aplicaciones no certificadas para Windows 2000. La plantilla compatible está diseñada para este tipo de organizaciones. Al

reducir los niveles de seguridad en determinados archivos, carpetas y claves del registro a los que las aplicaciones tienen acceso con frecuencia, la plantilla compatible permite que se ejecuten correctamente la mayoría de las aplicaciones en un contexto usuario. Además, puesto que se entiende que el administrador que aplica la plantilla compatible no desea que los usuarios sean usuarios avanzados, se quitan todos los miembros del grupo usuarios avanzados.

- Segura (secure*.inf)

  Las plantillas seguras implementan la configuración de seguridad recomendada para todas las áreas de seguridad con excepción de los archivos, carpetas y claves del registro. Éstos no se modifican gracias a la configuración segura predeterminada de los permisos del registro y el sistema de archivos.

- De alta seguridad (hisec*.inf)

  Las plantillas de alta seguridad definen la configuración de seguridad para las comunicaciones de red de Windows 2000. Las áreas de seguridad se definen para requerir la máxima protección del tráfico y los protocolos de red utilizados entre equipos que ejecutan Windows 2000. Como resultado, dichos equipos configurados con una plantilla de alta seguridad sólo se pueden comunicar con otros equipos Windows 2000. No podrán comunicarse con equipos que ejecuten Windows 95 o 98, ni Windows NT.

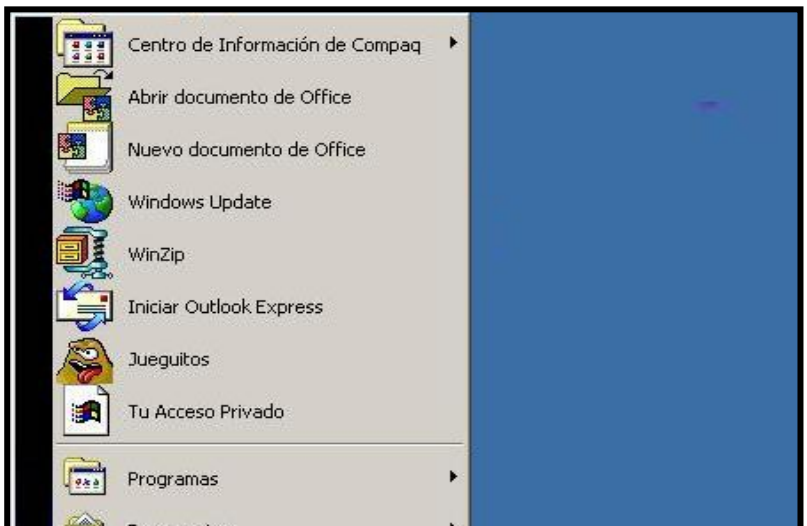
- Controlador de dominio dedicado (dedicadc.inf)

  La seguridad de usuario local de los controladores de dominio que ejecutan Windows 2000 no es de forma predeterminada.

  Esto hace posible que un administrador ejecute las aplicaciones existentes basadas en servidor sobre los controladores de dominio (no recomendado) en modo inverso compatible. Si no ejecuta aplicaciones basadas en servidor sobre controladores de dominio (recomendado), los permisos del registro y el sistema de archivos predeterminados del grupo de usuarios local pueden definirse del mismo modo que el definido de forma predeterminada para las estaciones de trabajo Windows 2000 y servidores independientes. Al implementar una plantilla de seguridad dedicada se aplica esta configuración de seguridad ideal para usuarios locales en controladores de dominio de Windows 2000.

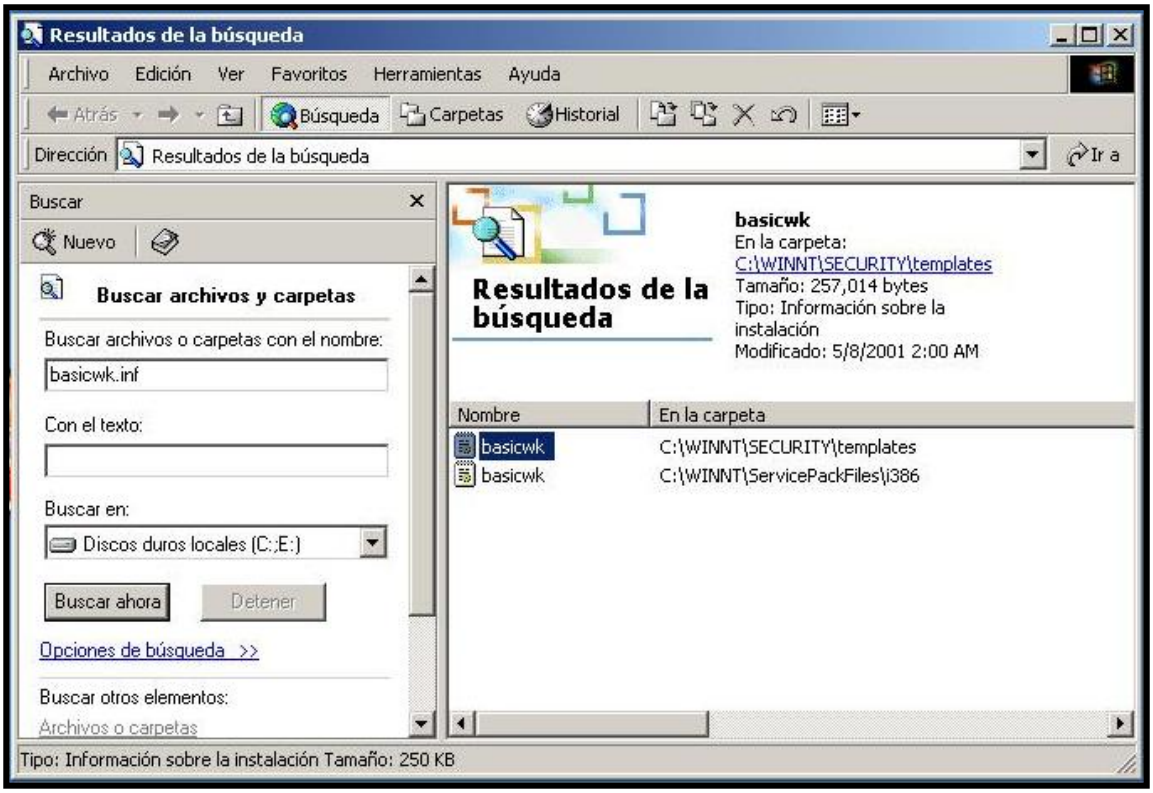
En los siguientes gráficos (gráfico 23, gráfico 24, gráfico 25) se muestra como se puede encontrar y ver una plantilla en este caso el nombre de la plantilla se llama basicwk.inf

Gráfico 23
Ejecutar la búsqueda



Sistema operativo w2kServer

Archivo encontrado



Sistema operativo Windows 2000 Server

Gráfico 25
Archivo abierto

3.5.- Comprobar l

DNS es una abreviatura para Sistema de nombres de dominio (*Domain Name System*), un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres sencillos. Cuando un usuario escriba un nombre DNS en una aplicación los servicios DNS podrán traducir el nombre a otra información asociada con el mismo como una dirección IP.

Por ejemplo, la mayoría de los usuarios prefieren un nombre fácil de utilizar como ejemplo.microsoft.com para localizar un equipo (como un servidor Web o de correo electrónico) en la red. Un nombre sencillo resulta más fácil de aprender y recordar. Sin embargo, los equipos se comunican a través de una red mediante

direcciones numéricas. Para facilitar el uso de los recursos de red, los servicios de nombres como DNS proporcionan una forma de asignar estos nombres sencillos de los equipos o servicios a sus direcciones numéricas. Si utilizó alguna vez un explorador web, también utilizó DNS.

El gráfico siguiente (gráfico 26) muestra un uso básico de DNS consistente en la búsqueda de la dirección IP de un equipo basada en su nombre.

Gráfico 26
Uso básico de dns

http://www.microsoft.com/windows2000/es/server/help/default.asp?url=/windows2000/es/server/help/sag_ADgroups_7migration.htm

En este ejemplo, un equipo cliente consulta a un servidor preguntando la dirección IP de un equipo configurado para utilizar host-a.ejemplo.microsoft.com como nombre de dominio. Como el servidor puede utilizar la base de datos local para responder la consulta, contesta con una respuesta que contiene la información solicitada, un registro de recursos de direcciones host (A) que contiene la información de dirección IP para host-a.ejemplo.microsoft.com.

El sistema de nombres de dominio (DNS) se definió originalmente en los documentos de Petición de comentarios (RFC, *Request for Comments*). Estos documentos especifican elementos comunes a todas las implementaciones de software relacionadas con DNS, entre los que se incluyen:

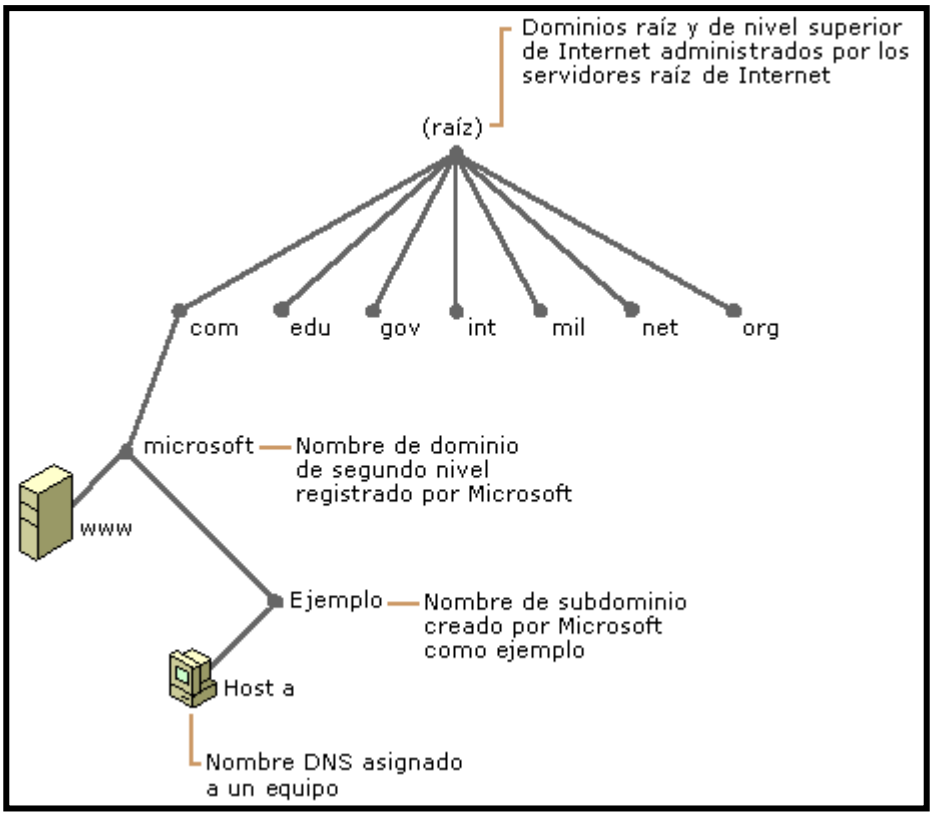
- Un espacio de nombres de dominio DNS, que especifica una jerarquía estructurada de dominios utilizados para organizar nombres.
- Los registros de recursos que asignan nombres de dominio DNS a un tipo específico de información de recurso para utilizar cuando se registra o se resuelve el nombre en el espacio de nombres.
- Los servidores DNS, que almacenan y responden a las consultas de nombres para los registros de recursos.
- Los clientes DNS, también llamados solucionadores, que consultan a los servidores para buscar y resolver nombres de un tipo de registro de recursos especificado en la consulta.

El espacio de nombres de dominio DNS se basa en el concepto de un árbol de dominios con nombre. Cada nivel del árbol puede representar una rama o una hoja del árbol. Una rama es un nivel donde se utiliza más de un nombre para identificar una colección de recursos con nombre. Una hoja representa un nombre único que se utiliza una vez en ese nivel para indicar un recurso específico.

En el gráfico siguiente (gráfico 27) muestra cómo Microsoft es la autoridad asignada por los servidores raíz de Internet para su propia parte del árbol del espacio de nombres de dominio DNS en Internet. Los clientes y los servidores DNS usan las consultas como el método fundamental para resolver los nombres en el árbol como información específica de los tipos de recurso. Los servidores DNS proporcionan esta información a los clientes DNS en las respuestas a las

consultas, quienes a continuación extraen la información y la pasan al programa solicitante para resolver el nombre consultado.

Gráfico 27
Estructura de un dominio



http://www.microsoft.com/windows2000/es/server/help/default.asp?url=/windows2000/es/server/help/sag_ADgroups_7migration.htm

Cualquier espacio de nombres de dominio DNS que se utiliza en el árbol es técnicamente un dominio. Sin embargo, la mayor parte de las explicaciones de DNS identifica los nombres de una de cinco formas, según el nivel y la forma en que se utiliza normalmente un nombre. Por ejemplo, el nombre de dominio DNS registrado para Microsoft (microsoft.com.) se conoce como un dominio de segundo nivel. Esto se debe a que el nombre tiene dos partes (llamadas etiquetas)

que indican que se encuentra dos niveles por debajo de la raíz o la parte superior del árbol. La mayor parte de los nombres de dominio DNS tienen dos etiquetas o más, cada una de las cuales indica un nuevo nivel en el árbol. En los nombres se utilizan puntos para separar las etiquetas.

3.6.- Diseño e implementación de directivas

Para utilizar la directiva de grupo de forma eficiente, deberá determinar cuidadosamente su aplicación. Con el fin de simplificar el proceso de aplicación y comprobación de la configuración de seguridad de la directiva de grupo, se recomienda aplicarla en dos niveles:

- Nivel de dominios. Para cumplir los requisitos de seguridad comunes como las directivas de cuentas y de auditoría que deben respetarse para todos los servidores.
- Nivel de unidad organizativa. Para cumplir los requisitos de seguridad específicos de servidores que no son comunes a todos los servidores de la red. Las opciones de configuración de la directiva de grupo que afectan a la seguridad se encuentran divididas en varias secciones.

La tabla siguiente (tabla 3), muestra las secciones de la directiva de grupo y su finalidad.

Tabla 3
Secciones de la Directiva de grupo y su finalidad.

Sección Directivas	Descripción

Directiva de cuentas\Directiva de contraseñas	Duración, longitud y complejidad de la contraseña configuradas
Directiva de cuentas\Directiva de bloqueo de cuentas	Duración, umbral y contador de restablecimiento de bloqueo configurados
Directivas locales\Directiva de auditoría	Activar/Desactivar el registro de sucesos específicos
Directivas locales\Derechos de usuario	Definir derechos tales como el inicio de sesión local, el acceso desde la red, etc.
Directivas locales\Opciones de seguridad	Modificar valores del registro específicos relacionados con la seguridad
Registro de sucesos	Supervisión de aciertos y errores activada
Grupos restringidos	Los administradores pueden controlar los miembros de grupos específicos
Servicios del sistema	Controla el modo de inicio de cada servicio
Registro	Configurar los permisos de claves de registro
Sistema de archivos	Configurar los permisos de carpetas, subcarpetas y archivos

http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch03secops.asp

Todos los equipos tienen una directiva local predefinida. Antes de modificar cualquier directiva predeterminada es importante documentar la configuración que contiene, de forma que se pueda volver fácilmente al estado anterior si se produce un problema.

El diseño de una directiva de grupo implica la toma de decisiones sobre su arquitectura lógica y física, así como sobre la tecnología e infraestructura que se emplearán para implementar su funcionalidad. Para tomar estas decisiones, debe tener un conocimiento claro de los procesos empresariales (sus requisitos funcionales), así como los niveles de escalabilidad, disponibilidad, seguridad y mantenimiento necesarios (sus requisitos no funcionales, funcionales u operativos).

El objetivo consiste en diseñar una directiva que:

- Solucione el problema empresarial para el que se diseña.
- Tenga en consideración la seguridad desde el principio, teniendo en cuenta los mecanismos adecuados de autenticación, la lógica de autorización y la comunicación segura.
- Proporcione un alto rendimiento y esté optimizada para operaciones frecuentes entre patrones de implementación.
- Esté disponible y sea resistente, capaz de implementarse en centros de datos de alta disponibilidad y redundantes.
- Permita la escalabilidad para cumplir las expectativas de la demanda y admita un gran número de actividades y usuarios con el mínimo uso de recursos.
- Se pueda administrar, permitiendo a los operadores implementar, supervisar y resolver los problemas de la aplicación en función del escenario.
- Se pueda mantener. Cada parte de funcionalidad debería tener una ubicación y diseño predecibles teniendo en cuenta distintos tamaños de aplicaciones,

equipos con conjuntos de habilidades variadas y requisitos técnicos y cambios empresariales.

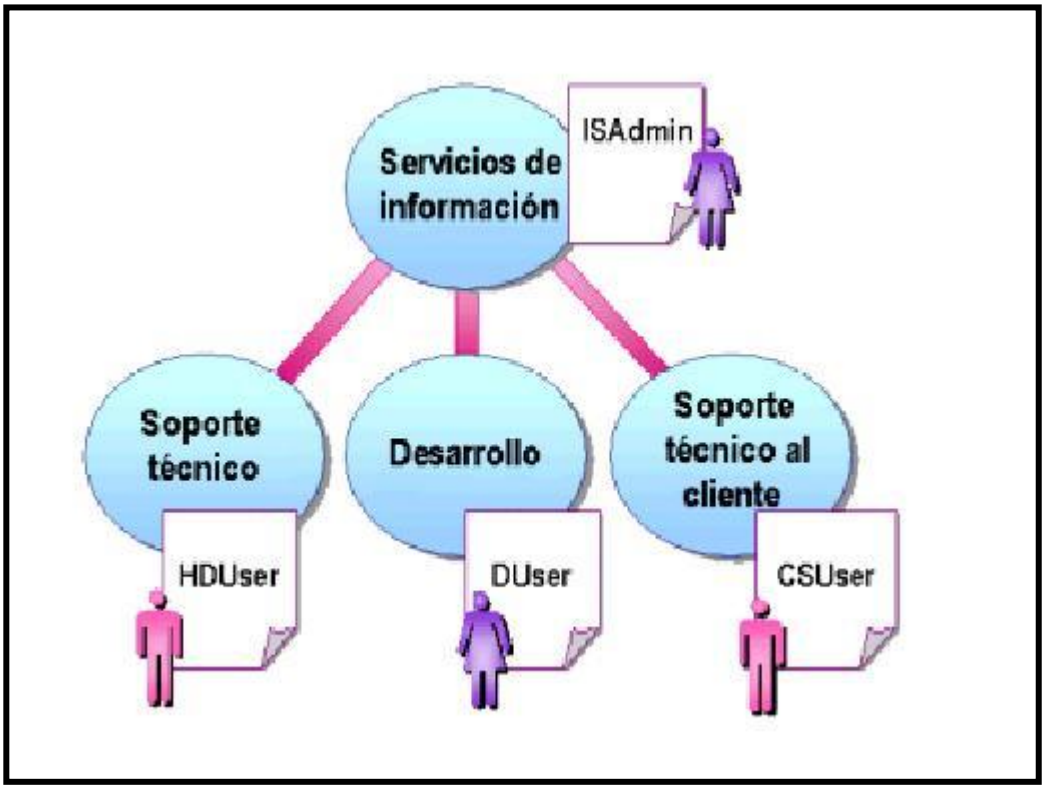
- Funcione en los distintos escenarios de aplicaciones y patrones de implementación.

A medida que crece Internet y las tecnologías relacionadas, las organizaciones buscan integrar sus sistemas entre límites de departamentos y de organización, ha evolucionado un enfoque de generación de soluciones basado en servicios. Desde el punto de vista del consumidor los servicios son conceptualmente similares a los componentes tradicionales, salvo que los servicios encapsulan sus propios datos y no forman parte de la aplicación sino que son utilizados por ésta. Aplicaciones y servicios que necesitan integrarse se pueden generar en distintas plataformas, por distintos equipos, en diferentes programas, se pueden mantener y actualizar de forma independiente. Por tanto, es esencial que implemente la comunicación entre ellos con el mínimo acoplamiento.

En el gráfico siguiente (gráfico 28) se muestra un ejemplo de diseño de una directiva de grupo.

Gráfico 28

Directiva de grupo



http://asignaturas.deusto.es/edr/Practica/Ejercicios/EjerDirecGrupoAsinSol.pdf

3.7.- Funciones del servidor

Se han definido varias funciones del servidor para aumentar la seguridad, en la tabla siguiente (tabla 4) se describe las funciones de Windows 2000 Server.

Tabla 4
Funciones de Windows 2000 Server

Función del servidor	Descripción
Controlador de dominio de Windows 2000	Controlador de dominio de Active Directory
Servidor de aplicaciones de Windows 2000	Servidor miembro bloqueado en el que se pueden instalar servicios como Exchange 2000. Para que el servicio funcione

	correctamente, será necesario disminuir la seguridad.
Servidor de archivos e impresión de Windows 2000	Servidor de archivos e impresión bloqueado
Servidor de infraestructuras de Windows 2000	Servidor DNS, WINS (Windows Internet Name Service) y DHCP bloqueado

http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch03secops.asp

Los requisitos de seguridad de cada una de estas funciones son distintos.

Los servidores realizan funciones específicas bien definidas. Si los servidores no coinciden con estas funciones o tiene servidores multiuso, deberá utilizar las opciones de configuración aquí definidas como pauta para crear sus propias plantillas de seguridad. No obstante, deberá tener en cuenta que cuanto mayor sea el número de funciones realizadas por los servidores, más vulnerables serán a los ataques.

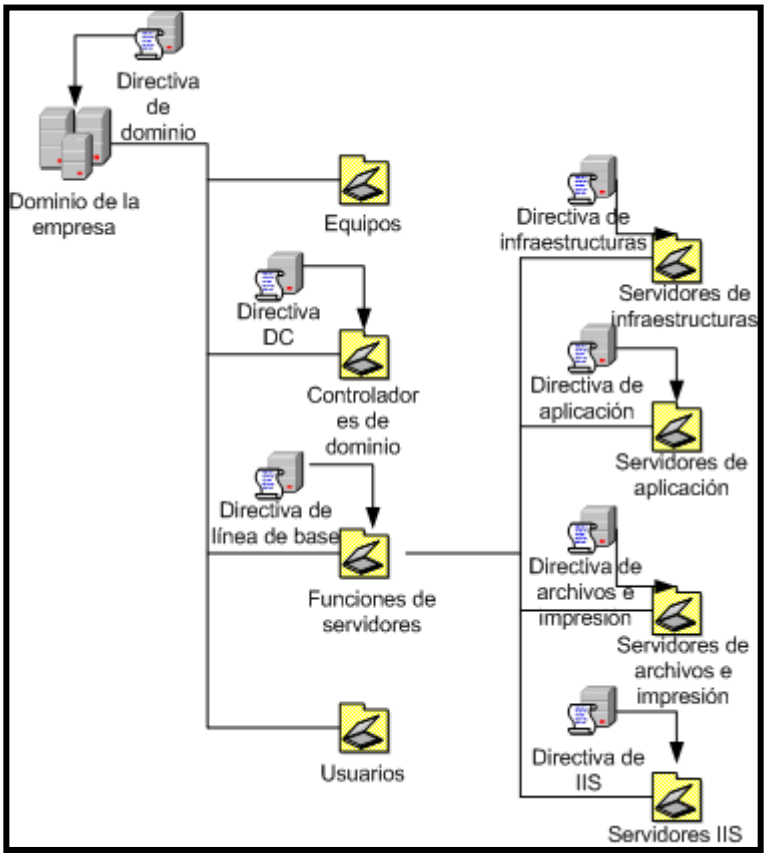
3.8.- Estructura de Active Directory para admitir las funciones del servidor

Active Directory es el servicio de directorio para Windows 2000 Server, almacena información acerca de objetos de la red, facilita la búsqueda y utilización de esa información por parte de usuarios y/o administradores. El servicio de directorio Active Directory utiliza un almacén de datos estructurado como base de una organización lógica jerárquica de la información del directorio.

La seguridad está integrada en Active Directory mediante la autenticación del inicio de sesión y el control de accesos a los objetos del directorio. Con un único inicio de sesión en la red los administradores pueden administrar datos del directorio y de la organización en cualquier punto de la red, y los usuarios autorizados de la red pueden tener acceso a recursos en cualquier lugar de la red. La administración basada en directivas facilita la tarea del administrador incluso en las redes más complejas.

A continuación en el siguiente gráfico (gráfico 29) se muestra la estructura de unidad organizativa.

Gráfico 29
Estructura de unidad organizativa para el uso con GPO definidos



http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch03secops.asp

La seguridad está totalmente integrada en Active Directory. El control de acceso se puede definir no sólo para cada objeto del directorio, sino también para cada una de las propiedades del objeto.

Active Directory proporciona el almacenamiento y el ámbito de aplicación para las directivas de seguridad. Una directiva de seguridad puede incluir información de cuentas, como las restricciones de contraseña para todo el dominio o los derechos sobre determinados recursos del dominio. Las directivas de seguridad se aplican mediante la configuración de la directiva de grupo.

Active Directory puede ampliarse ya que los administradores tienen la posibilidad de agregar nuevas clases de objetos al esquema y nuevos atributos a las clases de objetos ya existentes.

Active Directory incluye uno o varios dominios, cada uno con uno o varios controladores de dominio, lo que permite escalar el directorio para satisfacer cualquier requisito de la red. En un árbol de dominios se pueden combinar múltiples dominios y múltiples árboles de dominios se pueden combinar en un bosque.

El servicio de directorio de Active Directory tiene las siguientes características:

- Un almacén de datos también conocido como directorio, que almacena información acerca de los objetos de Active Directory. Estos objetos

incluyen normalmente recursos compartidos como servidores, archivos, impresoras, las cuentas de usuario y de equipo de red.

- Un conjunto de reglas, el esquema, que define las clases de objetos y los atributos contenidos en el directorio, las restricciones y los límites en las instancias de estos objetos así como el formato de sus nombres.
- Un catálogo global que contiene información acerca de cada uno de los objetos del directorio. Esto permite a los usuarios y administradores encontrar información del directorio con independencia de cuál sea el dominio del directorio que realmente contiene los datos.
- Un sistema de índices y consultas, para que los usuarios o las aplicaciones de red puedan publicar, encontrar los objetos y sus propiedades.
- Un servicio de replicación que distribuye los datos del directorio por toda la red. Todos los controladores de dominio de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio de sus dominios. Cualquier cambio en los datos del directorio se replica en todos los controladores de dominio del dominio.
- Integración con el subsistema de seguridad para asegurar el proceso de inicio de sesión en la red así como control de acceso tanto de las consultas de datos del directorio como de las modificaciones de los datos.
- Para sacarle el mayor provecho a Active Directory, el equipo que tiene acceso a Active Directory a través de la red debe ejecutar el software de cliente correcto. En equipos que no ejecutan el software de cliente de

Active Directory, el directorio aparecerá igual que un directorio de Windows NT.

3.9.- Mantener la seguridad de la configuración de la Directiva de grupo

Si aplica la configuración de seguridad por medio de la directiva de grupo, es importante garantizar que la configuración sea lo más segura posible. Para ello, se suele comprobar que los permisos de los GPO, de las unidades organizativas y los dominios en los que se aplica se hayan configurado correctamente. Las plantillas proporcionadas con esta guía no modifican los permisos predeterminados de Active Directory, por lo que necesitará modificarlos de forma manual.

Puede suceder que la configuración de la directiva de grupo definida en contenedores de nivel superior sea reemplazada por la configuración de contenedores de nivel inferior. Para evitar que se reemplace la configuración de un contenedor de nivel superior, utilice la opción “no reemplazar del GPO”.

Nota: no establezca “no reemplazar” en la directiva de línea de base para los servidores miembros. Si lo hace, las directivas de funciones del servidor no podrán activar los servicios y las opciones de configuración adecuados.

Además de separar las funciones del servidor en el nivel de unidad organizativa, también deberá crear las funciones de administrador correspondientes por separado y asignarles derechos administrativos sobre las unidades organizativas que les correspondan. De este modo, si un intruso consigue hacerse con los

derechos administrativos del servidor IIS, no podrá tener acceso a los servidores de infraestructuras y así sucesivamente.

Sólo los administradores del nivel de dominios y superiores deben tener derechos para modificar los miembros de una unidad organizativa. Si un administrador del nivel de unidad organizativa puede eliminar un servidor de la misma, podrá modificar la configuración de seguridad de los servidores.

Una vez aplicada la directiva a los servidores, todavía deberán llevarse a cabo varias tareas. Deberá comprobar los servidores regularmente para asegurarse de que:

- Se ha aplicado la directiva correcta al servidor.
- Ningún administrador ha cambiado una opción de configuración de la directiva y ha disminuido el nivel de seguridad de los servidores.
- Se han aplicado todos los cambios o las actualizaciones a todos los servidores.

Al comprobar que la configuración del GPO se ha aplicado a los servidores de forma correcta sabrá que los servidores se han asegurado adecuadamente. Puede utilizar varios métodos para examinar la directiva de grupo de un servidor y comprobar si se ha configurado correctamente.

3.10.- Auditar la Directiva de grupo

Auditar es un proceso que realiza un seguimiento de las actividades de los usuarios registrando sucesos de tipos seleccionados en el registro de seguridad de un servidor o una estación de trabajo.

Se pueden auditar los cambios de la directiva de grupo. La auditoría de los cambios de la directiva puede servir para realizar un seguimiento de las personas que están modificando o intentando modificar la configuración de directiva.

La auditoría de ciertos equipos, usuarios y sucesos del sistema operativo es una parte necesaria de la administración de una red. Hay que escoger lo que se desea auditar y después, revisando los registros de sucesos, controlar los patrones de uso, los problemas de seguridad y las tendencias de tráfico en la red. No obstante, hay que tener cuidado con el impulso de auditarlo todo. Cuantos más sucesos se auditen, más grandes serán los registros. Revisar enormes registros de sucesos es una tarea desagradable y al final nadie los vuelve a mirar. Por lo tanto, resulta crítico decidir una directiva de seguridad que proteja la red sin crear una gran carga administrativa. Tampoco conviene olvidar que cada suceso auditado provoca un pequeño aumento de la sobrecarga del sistema.

De forma predeterminada, todas las categorías de auditoría están desactivadas cuando se instala Windows 2000. Las categorías de sucesos que se pueden auditar son.

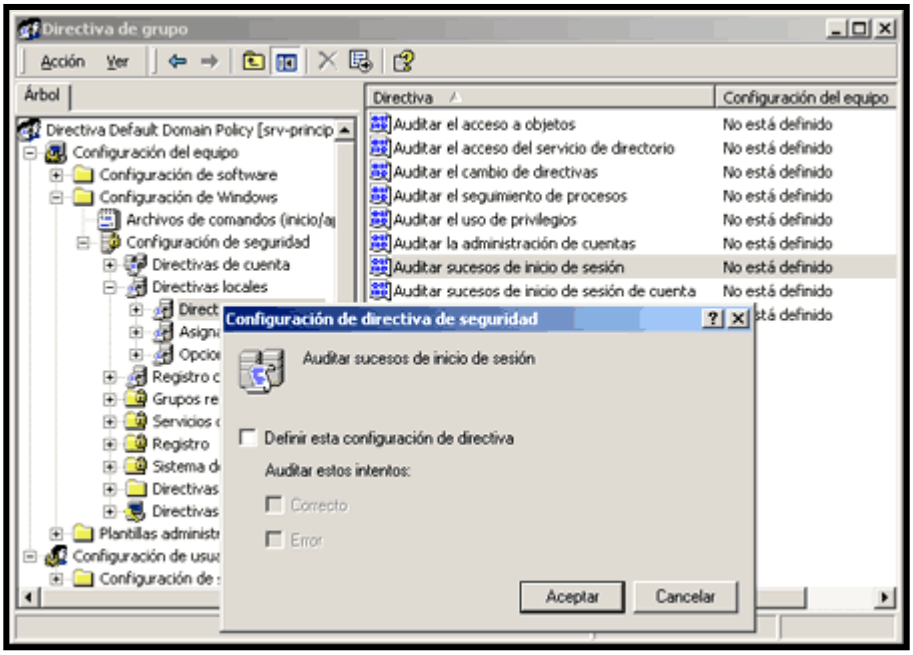
- **Acceso a objetos:** Se activa cuando se accede a un objeto.

- **Acceso a servicio de directorio:** Se activa cuando se accede a un objeto Active Directory.
- **Administración de cuentas:** Se activa cuando una cuenta de usuario o un grupo se crea o modifica.
- **Cambio de directiva:** Se activa cuando se modifica una directiva que afecta a la seguridad, a los derechos de usuario o a la auditoría.
- **Seguimiento de proceso:** Se activa cuando una aplicación ejecuta una acción que se está registrando.
- **Sucesos de inicio de sesión:** Se activa cuando un usuario inicia o cierra una sesión.
- **Sucesos de inicio de sesión de cuenta:** Se activa cuando un controlador de dominio recibe una petición de inicio de sesión.
- **Sucesos del sistema:** Se activa cuando un equipo se reinicia o se apaga u ocurre otro suceso que afecta a la seguridad.
- **Uso de privilegios:** Se activa cuando se utiliza un derecho de usuario para realizar una acción.

Cada suceso auditado dice algo, pero no siempre es algo que sea necesario saber. Por ejemplo, la auditoría de inicios y cierres de sesión con éxito puede revelar el uso de una contraseña robada, pero también puede simplemente producir interminables páginas que muestran que los usuarios debidamente autorizados están iniciando y cerrando sesiones como era de esperar. Sin embargo, la auditoría de los fallos al iniciar sesión recompensará definitivamente si alguien intenta un ataque con contraseñas aleatorias.

En el gráfico siguiente (gráfico 30), se muestra la pantalla para la auditoría de directivas de seguridad.

Gráfico 30
Auditar Directivas de seguridad



http://www.lavioleta.net/capitulo14.htm

Establecer una buena estrategia de auditoría de este tipo de eventos es vital debido a la importancia que puede tener sobre el rendimiento del servidor y en la carga administrativa, no obstante lo anterior en un sistema basado en directorio Activo podemos minimizar esta carga administrativa mediante el empleo de políticas de grupo.

CAPÍTULO IV

ASEGURAR SERVIDORES BASÁNDOSE EN SU FUNCIÓN

Se puede definir para todos los servidores miembros y controladores de dominio de la organización, y otras modificaciones que puede aplicar a funciones específicas del servidor.

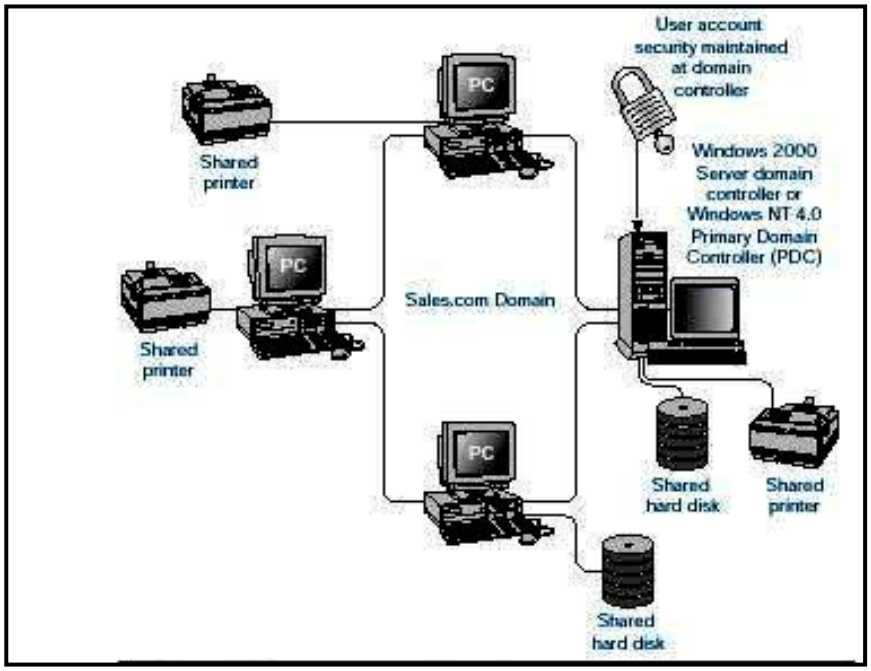
Este enfoque va a permitir que los administradores bloqueen los servidores por medio de directivas de líneas de base centralizadas, aplicadas de forma coherente a todos los servidores de la organización. Las directivas de línea de base sólo permiten una funcionalidad mínima, pero sí permiten que los servidores se comuniquen con otros equipos en el mismo dominio y su autenticación a través de los controladores de dominio. A partir de este estado más seguro, se pueden aplicar otras directivas incrementales más, que permiten que cada servidor realice únicamente las tareas específicas definidas por su función (27).

4.1.- Directiva para todo el dominio. Aborda los requisitos de seguridad comunes, como las directivas de cuentas que se deben aplicar para todos los servidores y estaciones de trabajo.

Gráfico 31

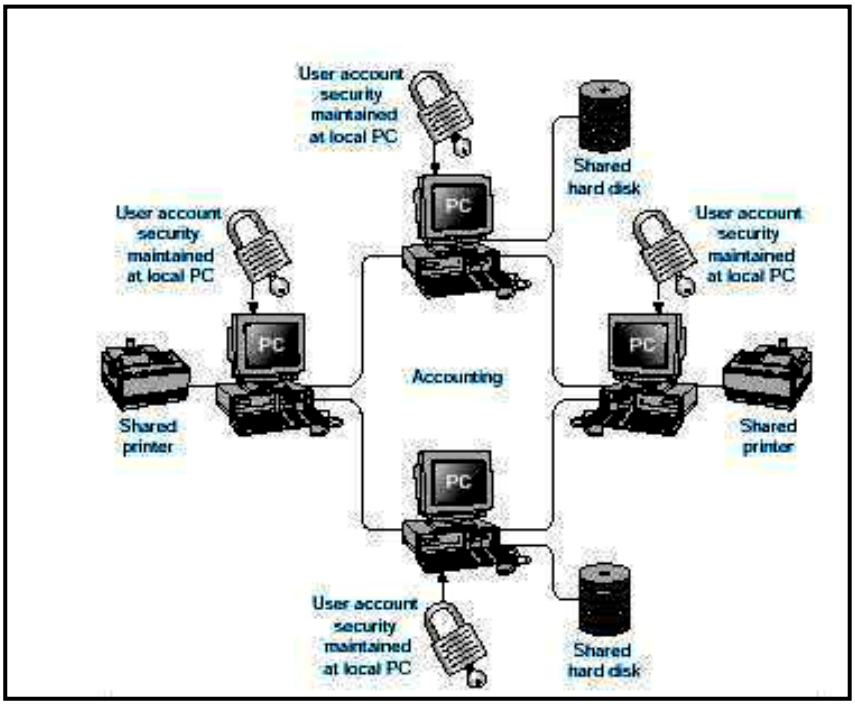
(27)http://www.compuayuda.net/guia31-1.htm 4 julio 2003

Directiva de seguridad para un dominio



www.bankhacker.com/seguridad/

Gráfico 32
Directiva de seguridad para cada estación de trabajo



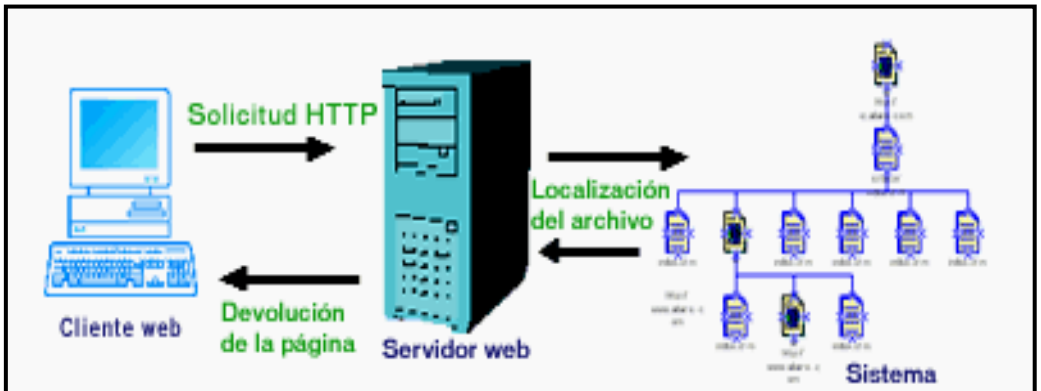
4.2.- Directivas para el controlador de dominio (ejecutan Active Directory y proporcionan autenticación y directivas**)**. Directivas que se aplican a la OU de los controladores de dominio. En particular, la configuración afecta a las directivas de auditoría, las opciones de seguridad y la configuración de servicios.

4.3.- Directivas de línea de base para los servidores miembros (proporcionan servicios, como servicios de archivo, impresión y aplicaciones**)**. La configuración común para todos los servidores miembros, como las directivas de auditoría, la configuración de servicios, las directivas que restringen el acceso al registro, el sistema de archivos y otros parámetros de seguridad específicos.

4.4.-Directivas para la función del servidor. Se definen cuatro funciones distintas de servidor: servidores de aplicaciones, servidores de archivos y de impresión, servidores de infraestructura y servidores IIS. Para cada función, se describen necesidades y configuraciones de seguridad específicas (28).

En el gráfico 33, se muestra el funcionamiento de petición de servicios a un servidor, por parte de un cliente.

Gráfico 33
Petición de servicios a un servidor



http://www.macromedia.com/es/software/coldfusion/resources/get_started/articles/introduction.html

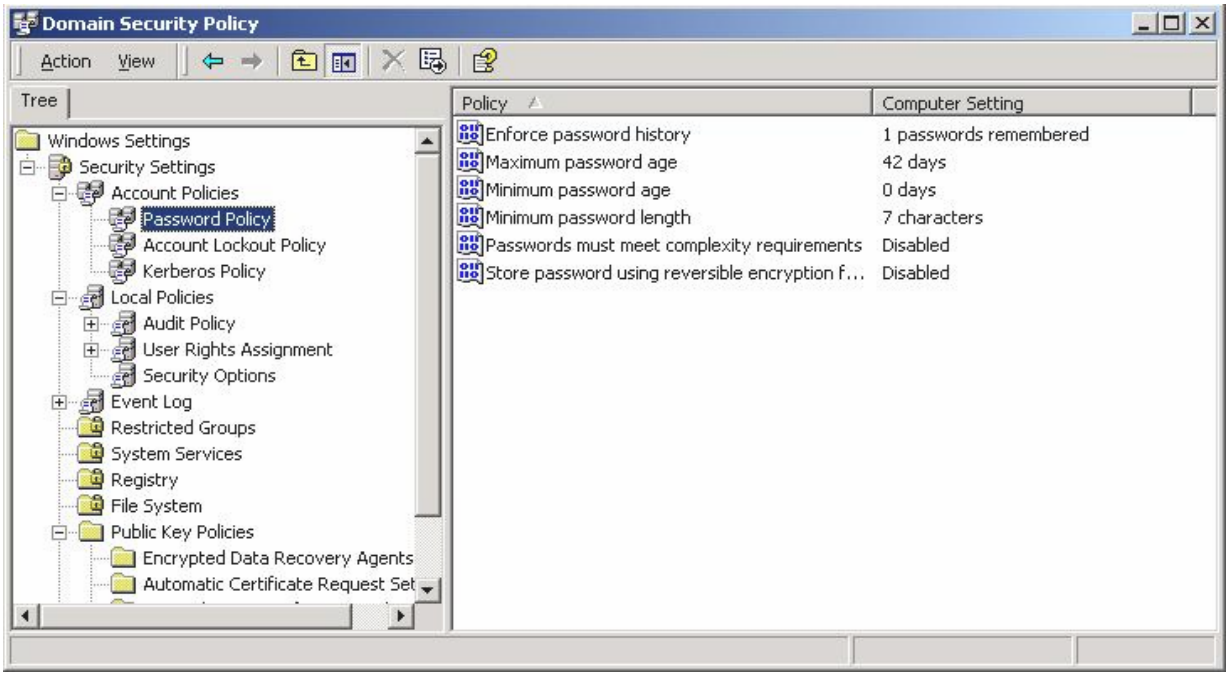
4.5.- Directivas de dominio

(28) www.todalaley.com/ Habilidades-directivas-curso-curso65.php *8 julio 2003*

En este no se aplica una configuración específica en el nivel de dominio ya que muchos de estos parámetros, como la longitud de la contraseña, varían dependiendo de las directivas de seguridad globales de la organización. No obstante, es muy importante que defina esta configuración de manera apropiada (29).

En el gráfico siguiente (gráfico 34), se muestra las directivas que se pueden aplicar.

Gráfico 34
Políticas de un dominio



Windows 2000 Server

(29)http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch04secops.asp
14 julio 2003

De forma predeterminada se aplica una directiva de contraseñas estándar a todos los servidores del dominio. Para garantizar su seguridad las contraseñas deben utilizarse con mucho cuidado. Las siguientes recomendaciones protegerán sus contraseñas:

- Nunca anote por escrito la contraseña.
- Nunca diga a nadie sus contraseñas.
- Nunca utilice la contraseña de inicio de sesión en la red para otro propósito.
- Utilice contraseñas diferentes para su inicio de sesión en la red y para la cuenta de Administrador en el equipo.
- Cambie la contraseña de red cada 60 o 90 días.
- Cambie la contraseña de inmediato si piensa que puede estar en peligro.

También debe tener cuidado a la hora de guardar la contraseña en el equipo. Algunos cuadros de diálogo como los de conexiones de accesos remotos o telefónicos, presentan una opción para guardar o recordar la contraseña. No seleccione esa opción.

Entre las medidas necesarias para asegurar correctamente el equipo se incluye el uso de contraseñas seguras para el inicio de sesión en la red y la cuenta Administrador en el equipo (30).

Las contraseñas pueden ser el vínculo más vulnerable en el esquema de seguridad de un equipo. Las contraseñas seguras son importantes porque las herramientas para averiguar contraseñas son cada vez mejores y los equipos utilizados son más eficaces. Las contraseñas de red que antes se tardaban semanas en descifrar ahora se pueden descifrar en cuestión de horas.

(30)http://www.microsoft.com/windows2000/es/professional/help/default.asp?url=/windows2000/es/professional/help/security_overview.htm 17 julio 2003

suposiciones inteligentes, ataques de diccionario y herramientas automatizadas que intentan todas las combinaciones de caracteres posibles. Contando con tiempo suficiente el método automatizado puede averiguar cualquier contraseña. Sin embargo, aún así se puede tardar meses en averiguar una contraseña segura.

Las contraseñas de Windows 2000 pueden incluir hasta 127 caracteres. No obstante, si utiliza Windows 2000 en una red que también contiene equipos con Windows 95 o Windows 98, considere el uso de contraseñas que no tengan más de 14 caracteres. Windows 95 y Windows 98 admiten contraseñas de hasta 14

caracteres. Si la contraseña es más larga, es posible que no se puedan iniciar sesiones en la red desde estos equipos (31).

Para cambiar la contraseña presione CTRL+ALT+SUPR y, después, haga clic en cambiar contraseña.

4.7.- Requisitos de complejidad

Cuando está activada la opción Las contraseñas deben cumplir los requisitos de complejidad de la directiva de grupo, es necesario que las contraseñas tengan una longitud de al menos 6 caracteres (aunque se recomienda establecerla en 8 caracteres). También se necesita que las contraseñas contengan caracteres de al menos tres de estas clases:

- Letras del alfabeto en mayúsculas A, B, C… Z
- Letras del alfabeto en minúsculas a, b, c… z
- Números arábigos 0, 1, 2… 9

(31)http://www.microsoft.com/windows2000/es/professional/help/default.asp?url=/windows2000/es/professional/help/security_overview.htm 18 julio 2003

La directiva de contraseñas no sólo debe aplicarse en los servidores que ejecutan Windows 2000, sino en todos los dispositivos que utilicen una contraseña para la autenticación. Los dispositivos de red, como los enrutadores y los conmutadores, son muy sensibles a los ataques si utilizan contraseñas simples. Los atacantes pueden intentar controlar estos dispositivos de red para superar los servidores de seguridad (32).

4.8.- Directiva de bloqueo de cuentas

Una directiva eficaz de bloqueo de cuentas puede evitar que un atacante adivine las contraseñas de sus cuentas. En la siguiente tabla (tabla 5) se muestra la configuración de una directiva de bloqueo de cuentas predeterminada y los requisitos mínimos recomendados para su entorno.

Tabla 5
Configuración predeterminada y recomendada

Directiva	Configuración predeterminada	Configuración mínima recomendada
Duración del bloqueo de cuenta	No definido	30 minutos
Umbral de bloqueo de cuenta	0	5 intentos incorrectos de inicio de sesión
Restablecer el bloqueo de cuenta después de	No definido	30 minutos

http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch05secops.asp

Con los mínimos recomendados que se indican aquí, una cuenta que tenga cinco intentos incorrectos de inicio de sesión en un plazo de 30 minutos se bloquea d *(32)www.todalaley.com/ Habilidades-directivas-curso-curso65.php* *18 julio 2003* ración en 0 intentos incorrectos y se puede volver a intentar iniciar una sesión). La cuenta sólo se puede activar antes de que hayan transcurrido los 30 minutos si un administrador restablece el bloqueo. Para aumentar el nivel de seguridad de su

organización, debe considerar la posibilidad de aumentar la duración del bloqueo de cuenta y disminuir el umbral de bloqueo.

4.9.- Directiva de auditoría: Determina cómo se lleva a cabo la auditoría en los servidores, a veces, los ataques más sutiles son los más peligrosos, ya que pasan desapercibidos y es difícil determinar los cambios realizados por lo cuál es imprescindible habilitar la auditoría, como mínimo de los procesos de inicio de sesión, tanto los correctos como los erróneos. De nada servirá tener habilitada la auditoría si no se chequea periódicamente. Sobre todo, revisar si alguien ha intentado autenticarse con la cuenta señuelo de administrador que se ha creado. Tenga en cuenta que lo primero que intentará hacer un hacker, al menos uno experimentado, será deshabilitar la auditoría. Este evento es registrado por la auditoría del sistema (33). Será de vital importancia estar al tanto de este suceso. Si un sistema de administración controla regularmente los registros para detectar suceso específicos, extrae, reenvía los detalles a una base de datos de administración, se capturarán los datos necesarios y por lo tanto podrá establecer que los archivos de registro se sobrescriban y podrá consultar más claramente los sucesos que interesan.

Para auditar los archivos y carpetas, debe iniciar una sesión como miembro del

{ *(33)http://www.iespana.es/dalamachia/pagina_nueva_8.htm* *18 julio 2003* ón administrar el registro de auditoría y seguridad en Directiva de grupo.

Es posible definir la auditoría de archivos y carpetas sólo en las unidades con formato para utilizar NTFS.

4.10.-Restricciones adicionales para conexiones anónimas

De forma predeterminada, Windows 2000 permite que los usuarios anónimos realicen ciertas actividades, como enumerar los nombres de las cuentas de dominio y los recursos compartidos de la red. Esto permite que un atacante vea estas cuentas y comparta nombres en un servidor remoto sin tener que autenticarse con una cuenta de usuario.

4.11.- Consideraciones de seguridad para los ataques a la red

Algunos ataques de denegación de servicio pueden ser una amenaza para TCP/IP en los servidores basados en Windows 2000. Esta configuración del registro ayuda a aumentar la resistencia TCP/IP de Windows 2000 a los ataques de denegación de servicio a la red de tipo estándar.

En el mundo conectado del Internet, algunos individuos maliciosos pueden significar una preocupación mayor en la seguridad de la red para los administradores de sistemas expuestos a las redes públicas. Los recientes ataques como negación de servicio en muchos de los sitios más populares del web hacen esto más claro que nunca. Muchos de estos ataques generan grandes volúmenes de tráfico de TCP/IP. Comúnmente el sitio en la mira podría parecer no disponible en el extenso Internet debido a la saturación de su segmento de red. Internamente, sin embargo, los servidores de web difícilmente parecían ser afectados por el ataque.

La pila de TCP/IP de Microsoft, parte de los sistemas operativos de la familia de Windows ha sido probada, demuestra ser confiable contra todos los ataques y en

su estado habitual por defecto maneja los tipos más comunes. Además de estas capacidades integradas, existen algunos pasos de sentido común que pueden tomarse en cuenta para disminuir la vulnerabilidad de un sitio web a estos y otros ataques a redes:

- Monitorear los límites de las redes en caso de ataques. Muchas otras compañías ofrecen herramientas que pueden detectar estos tipos de ataques.
- Asegúrese que los enrutadores no están convirtiendo la difusión de capa 3 a difusión de capa 2.
- Restrinja los enrutadores para permitir sólo el uso de los puertos que sean necesarios para que funcione el sitio.
- Deshabilite los servicios opcionales o innecesarios.
- Habilite la filtración de TCP/IP y restrinja el acceso sólo a los puertos que son necesarios para que funcione el sitio.
- Deshaga el enlace de NetBIOS en TCP/IP en donde no se necesita.
- Configure direcciones estáticas de IP y parámetros para adaptadores públicos.
- Configure los parámetros del registro para una máxima protección

4.12.- Seguridad de la cuenta de administrador local

Cada servidor miembro tiene una base de datos de cuentas locales y una cuenta de administrador local que proporciona control total sobre el servidor. Por lo tanto, esta cuenta es muy importante. Debe cambiar el nombre de la misma y asegurarse de que tenga una contraseña compleja. También debe asegurarse de que las contraseñas del administrador local no se repliquen en los servidores miembros. Si fuera así un atacante que obtuviera acceso a un servidor miembro podría obtener acceso a todos los demás con la misma contraseña.

No debe hacer que las cuentas de administrador locales formen parte del grupo de administradores de dominio, es importante asegurarse de que sólo se utilicen las cuentas locales para administrar los servidores miembros.

Con esta cuenta hay un pequeño problema y es que cualquier persona no deseada (Hacker, etc.) siempre deseara entrar en un ordenador haciendo uso de esta cuenta que permite el acceso total al mismo. Para evitar que esto sea fácil se cambiará el nombre de la cuenta de administrador, esto es muy importante ya que así le evitamos que el intruso tenga la ventaja de conocer cual es el nombre de la cuenta de administrador (por defecto es "administrador").

La administración de la seguridad consiste en proteger datos de los clientes de los ataques (intencionados o no). Es esencial que sus clientes tengan una visión clara de la naturaleza y el significado de la administración de la seguridad, que incluye en qué consiste la directiva de seguridad y qué niveles de seguridad deben cumplirse. Las medidas de seguridad incluyen a las personas, el proceso y la tecnología. El proceso está relacionado con la comunicación, el escalado,

los procesos y los procedimientos relativos a la administración de la seguridad. El personal debe recibir entrenamiento, tener la posibilidad de comprender y aplicar todas las medidas de seguridad y la tecnología cambiante que las acompaña.

Todas las partes deben estar equilibradas para garantizar un nivel de seguridad que cumpla los requisitos de los clientes.

La Administración de la seguridad está destinada a garantizar la protección de la información. Concretamente, el valor de la información debe quedar protegido. Este valor se determina en los siguientes términos:

- Confidencialidad. Proteger la información confidencial frente a divulgación no autorizada o interceptación inteligible.
- Integridad. Salvaguardar la precisión y la integridad de la información y el software
- Disponibilidad. Garantizar que la información y las soluciones del ASP están disponibles cuando es necesario.

La protección del valor de la información implica un costo económico, la ausencia de protección también. Para determinar el nivel de protección, las medidas de seguridad deben ser explícitas. Por lo tanto, una administración eficaz de la seguridad depende de análisis de riesgos precisos, de modo que se comprenda el efecto de los riesgos y de los costos que implica evitarlos. Los riesgos son inevitables, pero sólo deberían admitirse aquéllos que se puedan

controlar. La administración de la seguridad se ocupa de las actividades necesarias para mantener los riesgos dentro de proporciones que se puedan controlar.

CAPÍTULO V

SERVICE PACKS

Los service packs mantienen el producto actualizado, corrigen los problemas conocidos y también pueden ampliar la funcionalidad del equipo. Incluyen herramientas, controladores y actualizaciones, así como mejoras desarrolladas después de la comercialización del producto. Todo esto se agrupa en un solo paquete que puede descargarse fácilmente.

Los service packs son específicos para cada producto y por lo tanto, existen distintos service packs para los diferentes productos. No obstante, generalmente se usa el mismo para distintas versiones del mismo producto. Por ejemplo, se utiliza el mismo service packs para actualizar Windows 2000 Server y Windows 2000 Professional.

También son acumulativos; cada service packs nuevo contiene todas las reparaciones incluidas en los anteriores, además de las nuevas reparaciones y modificaciones del sistema recomendadas desde el último. No necesita instalar el service packs anterior antes de instalar el más reciente (34).

La Ingeniería de corrección rápida (QFE) es un grupo interno de Microsoft que crea revisiones (hotfix) es decir, revisiones de código para los productos. Estas

revisiones se envían a clientes específicos que experimentan problemas críticos para los que no existe una solución factible.

Las revisiones no se someten a pruebas regresivas exhaustivas y son específicas para cada problema; sólo deben aplicarse si se experimenta el problema exacto que abordan y si está utilizando la versión del software actualizada con el service packs más reciente.

Periódicamente, se incorporan grupos de revisiones a los service packs, se someten a comprobaciones más rigurosas y se ponen a disposición de todos los clientes.

Cuando la gente piensa en la seguridad de sus sistemas, casi siempre lo hace más en las revisiones de seguridad que en los service packs. En realidad, uno de los errores que con más frecuencia se cometen al realizar el mantenimiento de seguridad es sobrevalorar las revisiones e infravalorar los service packs. Quizá le sorprenda saber que hay diferencias significativas entre ambos y que, para el trabajo de fondo, debe utilizar los service packs antes que las revisiones (35).

De igual manera que las plantas y los animales se pueden clasificar en familias, géneros y especies, se puede clasificar informalmente el software de Microsoft para indicar su ámbito y propósito. En orden de importancia, estos son los términos que generalmente utilizamos:

- Una familia de productos es un conjunto de productos con un propósito relacionado. Por ejemplo, la familia de productos Windows® incluye

todos los sistemas operativos Windows, como Windows 3.11, Windows 95 y Windows 2000.

- Un producto es un miembro de una familia de productos. Por ejemplo, Windows NT es un producto de la familia Windows.
- Una versión es una instancia de un producto. Por ejemplo, Windows NT 3.5, Windows NT 4.0 y Windows 2000 son versiones diferentes del

(35)http://www.microsoft.com/technet/security/contact.asp *11 julio del 2003*

Los service packs son estratégicos. Es decir, los service packs se administran y diseñan cuidadosamente con el objetivo de que ofrezcan un conjunto de correcciones, global y bien comprobado, que sea conveniente para su uso en cualquier sistema del cliente. Lo que hay que recordar como clave de los service packs es que son lanzamientos planeados. En un service packs todo está planeado: cuántos habrá, con cuánta frecuencia se publicarán y cómo se ofrecerán a los clientes. La razón de la necesidad de tanto plan es que en nuestra opinión todo cliente debe aplicar cada service packs lo antes posible en cuanto se publique.

Los service packs tienen un ámbito cuidadosamente seleccionado y se ofrecen en intervalos cuidadosamente pensados. Si produjeran service packs de escasa importancia con intervalos rápidos, los administradores podrían pensar que no merece la pena el esfuerzo y el tiempo de aplicarlos a cientos o miles de máquinas. Por otra parte, si produjera service packs muy grandes con muy escasa frecuencia, los administradores podrían mostrarse recelosos de instalar

un cambio de código tan grande. Por eso tratamos de alcanzar un "punto de equilibrio" en el que los service packs tienen el tamaño justo y se ofrecen en el intervalo adecuado para que los administradores lo instalen rápidamente (36).

Los service packs son generales ya que estos tratan una amplia variedad de errores. Un service packs no trata sólo los errores de seguridad, sino también los que afectan a la escalabilidad, rendimiento, el funcionamiento correcto de las características del producto y otras áreas, además los service packs resuelven errores de pequeña y de gran importancia.

(36)http://www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch05secops.asp 14 julio 2003

Los service packs son acumulativos, cada uno incluye todos los que salieron anteriormente para ese producto: por ejemplo, Windows NT 4.0 service packs 6a incluye todos los cambios que se hicieron entre los service packs 1 y 5.

La consecuencia de todo lo anterior es que los service packs son la mejor manera de mantener su sistema en las mejores condiciones.

Los service packs están mejor probados ya que como son versiones planeadas, los service packs están impulsados por razones de calidad. Es decir, no se lanza un service packs hasta que cumple los mismos niveles de calidad que el propio producto. Los service packs se prueban constantemente a medida que se crean, sometiéndose después a varias semanas de pruebas finales rigurosas, en las que se comprueban junto con cientos o miles de productos de otros proveedores. Si las pruebas revelan errores que impiden alcanzar nuestro estándar de calidad se retrasa el lanzamiento del service packs.

Probablemente ya será evidente que la mejor manera de asegurar su sistema consiste en mantenerse actualizado con respecto a los service packs y en utilizar las revisiones para el propósito con el que se han creado: proteger su sistema hasta que esté disponible el siguiente service packs. ¿Pero qué significa esto exactamente?

En primer lugar, significa que debe planear la adopción de los service packs. Ejecutar un service packs anticuado para apilar encima una revisión tras otra no es una manera efectiva de mantener su sistema al día y funcionando (aunque es mucho mejor que ejecutar un service packs anticuado y no instalar las revisiones). Considere la posibilidad de configurar un laboratorio de pruebas para evaluar pronto los service packs, desarrollando planes y directivas para distribuirlo con prontitud. Quizás incluso quiera inscribirse siempre que pueda a programas beta de los service packs, como una manera de poder echar pronto un vistazo a lo que va a llegar (37).

En segundo lugar, sea selectivo por lo que se refiere a las revisiones que instala. Una de las razones es que los clientes puedan entender perfectamente los riesgos que plantean una vulnerabilidad, el efecto que podría producir y las máquinas que se ven primordialmente afectadas. Si una vulnerabilidad no afecta a su entorno, no tiene que aplicarla. Además, considere también la categorización de las revisiones de acuerdo con el riesgo que plantea la vulnerabilidad. Si una vulnerabilidad amenaza sus sistemas con un riesgo grave, aplique la revisión inmediatamente. Pero en el caso de las

vulnerabilidades menores, considere un proceso de actualización programado con regularidad que le permita instalar varias revisiones de una vez. De esa manera la vida será más fácil para usted y para sus usuarios.

Siguiendo estas directrices simples obtendrá tiempos de actividad mejores, usuarios más felices, más tiempo libre y lo mejor de todo, seguridad. Simplemente se trata de utilizar cada herramienta como más le beneficie.

5.2.- Revisiones de seguridad

Las revisiones de seguridad están diseñadas para eliminar las vulnerabilidades de la seguridad. Los atacantes que desean entrar en un sistema pueden aprovechar estas vulnerabilidades. Las revisiones de seguridad son análogas a las revisiones (hotfix), pero se consideran obligatorias si las circunstancias lo justifican y deben

(37)Microsft Technet manual windows 2000 server *14 julio del 2003*

Muchas de las actualizaciones que se generan son para resolver problemas del cliente (con frecuencia, relacionados con el explorador). Estos problemas pueden ser o no relevantes para una instalación de servidor concreta. Es necesario obtener la revisión del cliente para actualizar la base de clientes actual y la revisión de administración para actualizar el área de creación de clientes del servidor.

Una revisión es una actualización que se produce entre dos service packs. En inglés el término habitual para revisión es patch, aunque en ocasiones se utiliza hotfix. Casi todas las revisiones se crean para corregir vulnerabilidades de la

seguridad, aunque también tienen como objetivo la corrección de problemas críticos de estabilidad o rendimiento.

Los service packs y las revisiones de seguridad están estrechamente relacionados ambos son vehículos que utiliza Microsoft para corregir errores de sus productos pero las semejanzas terminan ahí. Las revisiones y los service packs tienen ámbitos totalmente distintos.

Las revisiones son tácticas y se desarrollan conforme va siendo necesario para combatir amenazas inmediatas y específicas a la seguridad del cliente además proporcionan soluciones intermedias a los problemas de seguridad que surgen entretanto. Por su propia naturaleza, las revisiones no están planeadas... y siempre se tiene la esperanza de que no necesitemos crear una. Pero el desarrollo de software es una ciencia poco precisa, por lo que sabemos que siempre habrá errores, algunos de los cuales afectan a la seguridad. En consecuencia, siempre

(38)www.gnomos/revisiones/acceso.asp *15 julio del 2003* nte en un problema y tienen ciertamente su sitio, pero aunque instalara todas las revisiones que ha lanzado Microsoft no eliminaría con ello tantos errores como con la instalación del service packs más reciente.

El tiempo de respuesta es la cuestión primordial cuando se crea una revisión de seguridad, puesto que ésta se hace como respuesta a un peligro claro y presente para los clientes. En consecuencia, la rigurosidad de las pruebas pesa menos que la necesidad de entregar la revisión lo antes posible. El alcance de las pruebas varía dependiendo de varios factores:

¿Se ha hecho público el problema? En tal caso aumenta significativamente el factor tiempo del problema y se reduce el tiempo disponible para probar la revisión. Esta es una de las razones por las cuales los profesionales de la seguridad responsables colaboran con el proveedor siempre que encuentran una vulnerabilidad de la seguridad: así se obtiene una revisión mejor.

¿Qué funciones se ven afectadas por la revisión? Una revisión de una vulnerabilidad que afecta a una función básica del sistema operativo requiere una comprobación más profunda que la que afecta a una parte aislada del sistema.

¿A qué productos de otros proveedores afectará la revisión? Una revisión que cambia la manera en que los productos de otros proveedores funcionan con los nuestros requerirá una comprobación mucho mayor.

Siempre se comprueba las revisiones tanto como se debe dentro de los límites de tiempo en que se ha de operar. Pero en última instancia, las revisiones tienen más probabilidades que los service packs de incluir errores de regresión.

5.3.- Sistemas de actualización de la seguridad

En muchos entornos, puede ser conveniente tener equipos especializados en los que se puedan llevar a cabo muchos de los pasos del proceso de administración de revisiones. Estos sistemas proporcionan ubicaciones especializadas para las herramientas de seguridad, las revisiones, los service packs y la documentación (39). Puede usar estos sistemas para realizar el análisis, la recuperación y la

instalación de las revisiones. Debe asegurarse de que los sistemas de actualización de la seguridad estén en uno o varios equipos dedicados que puedan asegurarse y controlarse estrechamente, ya que son los que se utilizarán para instalar y mantener las revisiones de seguridad para todos los sistemas de su entorno. Los sistemas de actualización de la seguridad generalmente no necesitan ser servidores muy potentes, ya que la carga que soportan suele ser bastante ligera. No obstante, la alta disponibilidad es muy importante, ya que estos equipos serán la base para mantener el entorno actualizado con las revisiones más recientes.

Para poder aplicar correctamente un sistema de actualización de la seguridad, el equipo necesita tener acceso directo o indirecto a Internet para descargar la información más reciente de las revisiones de fuentes confiables, así como acceso a todos los equipos a los que debe mantener actualizados.

(39)http://www.microsoft.com/spain/seguridad/xp/mbsa/default.asp *16 julio del 2003*

Si la compañía es pequeña, es posible que sea suficiente con una persona encargada de mantener las revisiones actualizadas, realizar pruebas con las mismas, instalarlas y leer los distintos archivos de registro. Sin embargo, en los entornos más grandes suele haber varias personas encargadas de los diferentes aspectos de la seguridad (40). Es muy importante que exista una comunicación eficaz entre todas las personas involucradas en la administración de las revisiones.

Esto permite garantizar que se toman decisiones sin duplicar esfuerzos y que no se omite ningún paso del proceso.

5.5.- Procesos de administración de revisiones

Es el proceso de coordinar y administrar las revisiones por las que se planean, prueban e implementan todas las revisiones de un entorno de tecnologías de la información. La administración de revisiones trabajan para asegurar la entrada y salida de las aplicaciones.

Esto ayuda a las empresas a planear cómo van a mejorar su operación, administración de revisiones específicamente, ayuda a los clientes a evaluar el nivel de madurez de sus procesos de operaciones y administración actuales.

Los pasos de los procesos de administración de revisiones se los detalla a continuación:

5.5.1.- Análisis. Observe el entorno actual y determine las posibles amenazas se determina qué revisiones debe instalar para reducir amenazas.

5.5.2.- Plan. Determine qué revisiones debe instalar para reducir las posibles amenazas y vulnerabilidades detectadas. Identifique quién llevará a cabo las pruebas y la instalación

(40)www.microsoft.com/latam/windows2000/server/ evaluacion/noticias/boletines/sp2.asp
17 julio del 2003

5.5.3.- Realización de pruebas. Revise las revisiones disponibles y clasifíquelas en categorías para su entorno, compruebe todas las revisiones identificadas para asegurarse de que funcionan en su entorno sin efectos secundarios negativos.

Comprenda qué hace realmente la revisión y cómo afecta al entorno. Asegúrese de que tiene el efecto previsto.

5.5.4.- Instalación. Instale las revisiones adecuadas para asegurar el entorno.

5.5.5.- Control. Compruebe todos los sistemas después de instalar las revisiones para asegurarse de que no producen efectos no deseados.

Esta implementación trata el problema de determinar qué está sucediendo en una infraestructura distribuida al aplicar mejores prácticas desde la función de monitoreo de servicios y de administración de los servicios de control.

5.5.6.- Revisión. Como parte del proceso, debe revisar periódicamente las nuevas revisiones que han ido apareciendo, el entorno y las revisiones que necesita la compañía. Si durante este proceso determina que se necesitan nuevas revisiones, vuelva a empezar desde el primer paso.

Nota: es muy conveniente que realice copias de seguridad de todos los sistemas de producción antes de instalar una revisión.

Esto trata el problema de asegurar que las revisiones y las actualizaciones se implementen de una manera controlada, oportuna y rentable al aplicar las mejores prácticas de administración de cambios, de configuraciones y de versiones con el reto de cumplir con cambios frecuentes, pero relativamente pequeños.

5.6.- Administración de revisiones del lado del cliente

Aquí se analizará acerca del proceso de administración de revisiones del lado del servidor, pero debe recordar que muchas veces los virus y otras amenazas para la seguridad de la organización obtienen acceso por el lado del cliente.

La mayoría de los elementos anteriores también se aplican a la administración del lado del cliente, pero existen algunas diferencias. En la mayoría de los casos, las diferencias no están tanto en lo que hace la revisión sino en cómo se determina en la organización, qué revisiones se necesitan, cómo se realizan las pruebas y cómo se instalan.

Hay varias herramientas que ayudan específicamente con la administración de revisiones del lado del cliente.

Una forma sencilla de comprobar y aplicar correcciones es utilizando windows update. Al entrar en el sitio web de windows update, se explora el equipo y se muestra una lista de todas las revisiones, tanto de seguridad como de otro tipo, que no están instaladas y se pueden descargar.

Para ejecutar windows update, debe ser un administrador del equipo local. Esto puede hacer que la herramienta no sea práctica en muchos entornos.

El sitio web de Windows Update Corporate Edition proporciona un catálogo completo de las actualizaciones que se pueden distribuir a través de una red corporativa (41). En la misma ubicación se encuentra el contenido de windows update.

Windows Update Corporate Edition nos permite buscar las actualizaciones más recientes del software y los controladores por palabras clave, sistema operativo, tipo de actualización, tipo de componente, idioma, fecha de publicación y fabricante, con el fin de encontrar las más relevantes para su organización así como:

* Descargar las actualizaciones necesarias de una en una o seleccionar varias para descargarlas como un paquete listo para distribuirlo en toda la red.

* Utilizar el historial de descargas para revisar las actualizaciones descargadas previamente y dónde están ubicadas.

* Usar el archivo Lea esto primero suministrado con cada descarga para obtener información detallada acerca de cada actualización antes de descargarla. Los archivos Lea esto primero se proporcionan con todos los paquetes de descarga y contienen vínculos a sitios Web relevantes que contienen más información.

El principal interés de la administración de la versión es facilitar la introducción de versiones de software y hardware en entornos administrados de TI. Principalmente, incluye el entorno de producción y los entornos administrados previos a la producción. La administración de la versión es el punto de coordinación entre el desarrollo de la versión y equipo del proyecto, y los grupos de operaciones responsables de la ejecución de la versión para la producción.

(41)www.intel.com/espanol/business/upgrade/ *18 julio 2003*

Ante la complejidad de los entornos distribuidos de TI de hoy en día, la función de supervisión de la administración de la versión resulta esencial para el correcto desarrollo de las versiones que suele implicar a muchos proveedores de servicios, centros de operaciones y grupos de usuarios (42). El diseño y administración adecuados de los recursos es esencial para el empaquetamiento y distribución correctos de una versión al cliente. La administración debería garantizar que todos los aspectos de una versión, tanto técnicos como de otra naturaleza, se consideraran de modo conjunto.

La administración del cambio funciona en estrecha relación con los procesos de administración del cambio y la configuración, para garantizar que la base de datos de administración de configuración que comparten se mantiene al día.

Las actividades básicas de la administración de la versión son:

- Implementar software y hardware nuevos en el entorno operativo mediante procesos de control de configuración y administración del cambio. Las versiones se deberían someter al control del cambio y pueden componerse de una combinación de hardware, software, firmware y elementos de configuración de documentos.
- Elaborar y administrar el plan de implantación de la versión.
- Comunicar y administrar las expectativas entre los equipos de operaciones y con el cliente durante el diseño e implantación de nuevas versiones.

- Diseñar e implementar procedimientos eficaces para la distribución e instalación de cambios a gran escala en los sistemas de TI.
- Crear y administrar el plan de reversión de la versión.

] *(42)www.abcdatos.com/programas/utilidades/ actualizacionsoftwareysistemas/* *18 julio del 2003*

personal necesario para identificar, asignar, diagnosticar, hacer un seguimiento y resolver problemas, cuestiones y solicitudes dentro de los requisitos aprobados contenidos en el contrato de nivel de servicio.

El objetivo de la fase de asistencia técnica es resolver puntualmente los incidentes, problemas y consultas.

La fase de asistencia técnica incluye dos tipos de planteamientos para el problema y su resolución. Los dos planteamientos poseen elementos proactivos y reactivos. El planteamiento reactivo depende de la capacidad de una organización para reaccionar y resolver problemas rápidamente (43). El planteamiento proactivo más deseable, es evitar cualquier posible interrupción del servicio mediante la identificación y solución de los problemas antes de que se vea afectado cualquier nivel de servicio. Esto se consigue a través de una buena supervisión de la solución de servicio contra umbrales predefinidos y al dar tiempo al personal de operaciones para que reaccione ante posibles problemas antes de que éstos se manifiesten en forma de interrupción del servicio.

La provisión de ayuda técnica es la función de administración de servicio fundamental en la fase de asistencia técnica. Coordina todas las comunicaciones de clientes y actividades acerca de los asuntos, problemas y consultas relacionadas con los sistemas de producción. Es el único punto de contacto diario entre proveedores de servicio y clientes o usuarios. La ayuda técnica es principalmente reactiva, siendo su objetivo preeminente el de restablecer los niveles de servicio tan rápido como sea posible. Las solicitudes llegan aquí en busca de ayuda técnica para la resolución de asuntos y problemas procedentes

(43)http://www.microsoft.com/spain/servidores/management/MSM/msm.asp 18 julio 2003

configuraciones de equipos de escritorio y demás facilidades.

Muchos modelos avanzados de ayuda técnica están incorporando en su función el concepto de supervisión del sistema. Han establecido unos métodos proactivos con los que tratar ciertas clases de incidentes antes de que afecten de modo adverso al cliente. El riesgo de combinar actividades reactivas y proactivas en el nivel de ayuda técnica es que las actividades reactivas abruman la capacidad de actuar de forma proactiva del personal. Dedicar operaciones y otros grupos de asistencia a las actividades proactivas contribuye a garantizar que se realiza este trabajo lo que, en última instancia, reduce el trabajo en modo "activo" de la ayuda técnica.

El objetivo de la función típica de la ayuda técnica se limita a la identificación, diagnóstico y resolución final de los incidentes. Éstos se definen, simplemente, como cualquier aspecto relativo a la asistencia técnica que los miembros del

grupo con dicha función puedan finalmente diagnosticar y resolver. En un modelo de asistencia con múltiples niveles, se hace referencia a esta función como soporte de primer nivel (44). Los distintos procedimientos de asignación de los problemas en función de su gravedad o dificultad permiten ir escalando la asignación de la resolución de los incidentes al personal con la especialización adecuada. Una vez que se ha escalado un incidente fuera del ámbito de la ayuda técnica, se clasifica como problema y la función de administración de servicios de administración de problemas se hace cargo de él para resolverlo. La ayuda técnica conserva la propiedad del problema y toda la comunicación con el cliente. La administración del problema se describe en la sección siguiente.

Las actividades clave de la ayuda técnica incluyen:

- Operaciones del centro de llamadas.
- Presentación de incidentes electrónicos.
- Clasificación de incidentes, registro, asignación, diagnóstico y escala.
- Estado del incidente y comunicación.
- Resolución del incidente.
- Generación de informes y estadísticas de apoyo sobre los incidentes.

La administración de problemas está estrechamente emparejada con la administración de incidentes que se lleva a cabo desde el nivel de ayuda técnica. La administración de problemas es responsable de definir con claridad el modelo de asistencia utilizado, los procedimientos de escala, la resolución de

problemas, el análisis de la causa que se halla en el trasfondo de los incidentes y problemas, la resolución de problemas y la generación de informes.

La administración de problemas se fundamenta, generalmente y en gran medida, en el uso de modelos de asistencia técnica con niveles. En muchas implementaciones, el número de niveles variará en función del sistema o la aplicación de la que se ofrece asistencia técnica.

Un área fundamental en la administración de problemas en la que merece la pena hacer hincapié es el análisis de las causas originales y la respuesta proactiva a las tendencias de incidentes y problemas antes de que afecten a los clientes. Los mejores modelos de asistencia técnica que se utilizan actualmente subrayan la necesidad de evitar los problemas antes de que éstos ocurran. Con clientes que exigen un porcentaje de disponibilidad muy elevado (del 99,99 y hasta el 99,999 por ciento) en las aplicaciones, la única manera de satisfacer su demanda es planear, crear, distribuir y administrar teniendo muy clara esta exigencia de alta disponibilidad desde el principio. Esto significa diseñar y crear de modo que los grupos de operaciones puedan identificar y reaccionar ante los cambiantes patrones de uso antes de que se manifiesten en forma de incidentes y problemas que requieran asistencia técnica. Las funciones de administración de servicios de disponibilidad, capacidad y contingencia desempeñan un papel esencial en esta actitud de evitar los problemas e incidentes referentes a la asistencia técnica.

5.7.- Microsoft Baseline Security Analyzer

Es una herramienta que permite a los usuarios y administradores de sistemas Windows garantizar y verificar revisiones de seguridad que faltan, contraseñas débiles, servicios innecesarios, configuración de seguridad de Internet Explorer y Outlook Express y configuración de protección de las macros de Office. También proporciona información acerca del problema de seguridad detectado, cómo repararlo y vínculos con información adicional acerca del problema (45).

Gracias a MBSA (Microsoft® Baseline Security Analyzer) los usuarios desde casa o el trabajo y/o los administradores pueden analizar máquinas compatibles con Windows® en busca de posibles problemas en la configuración de seguridad. El MBSA escanéa el ordenador y comprueba el sistema operativo así como el resto de los componentes que hay instalados, y de este modo identifica problemas en la configuración de la seguridad y averigua si se cumplen las últimas exigencias en hotfixes y parches de seguridad.

(45)http://www.microsoft.com/spain/seguridad/xp/mbsa/default.asp *21 julio 2003*

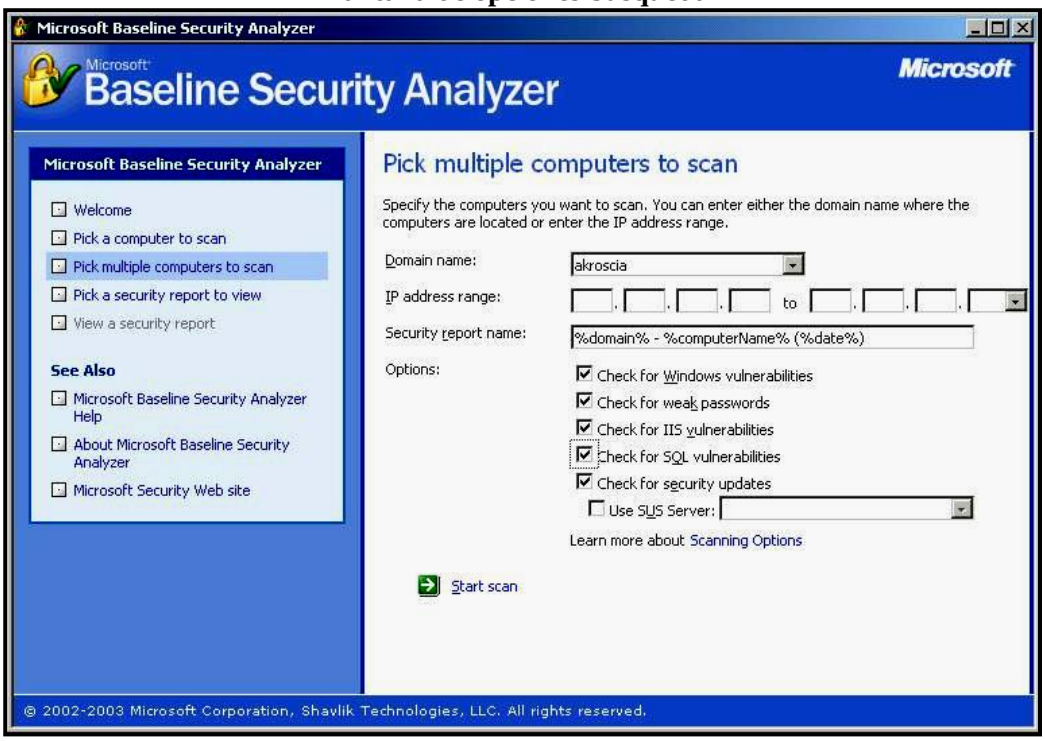
en equipos que estén ejecutando los sistemas operativos Microsoft Windows 2000/2003, Windows XP, (Pro y home edition). En ningún caso puede instalarse y ejecutarse correctamente desde equipos Windows NT4, ya que no está diseñada para ello.
Aunque sí es posible realizar un reconocimiento de equipos que estén ejecutando el sistema operativo.

A continuación se muestra las fases principales del programa antes mencionado.

Si se toma la red completa, se tiene que ingresar el nombre del dominio y luego mandar a ejecutarlo.

Gráfico 35

Pantalla de opciones búsqueda

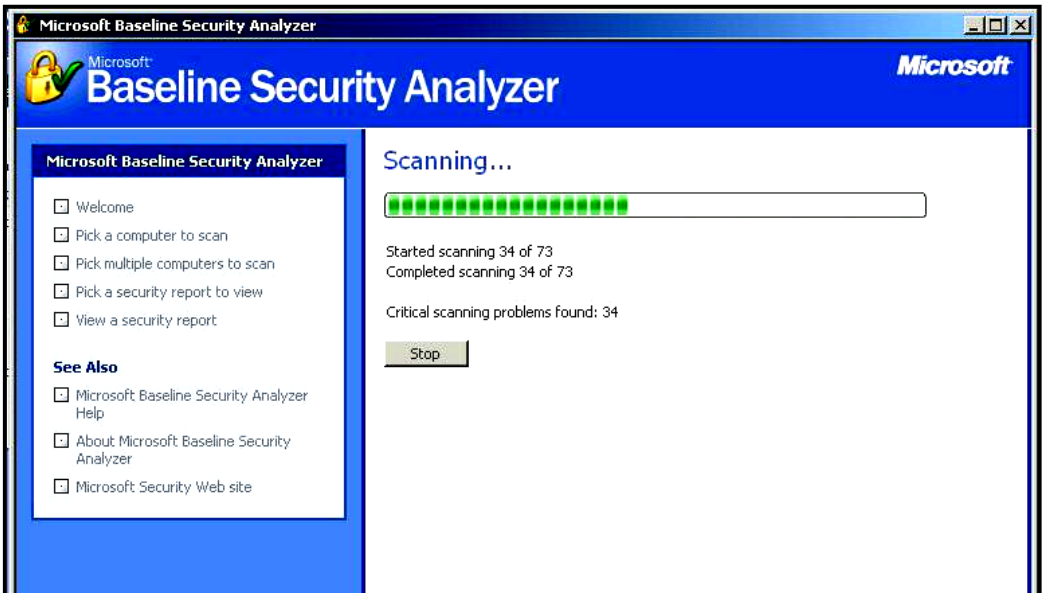


http://www.microsoft.com/spain/seguridad/xp/mbsa/default.asp

A continuación se presenta el proceso de búsqueda.

Gráfico 36

Proceso de búsqueda de pc´s

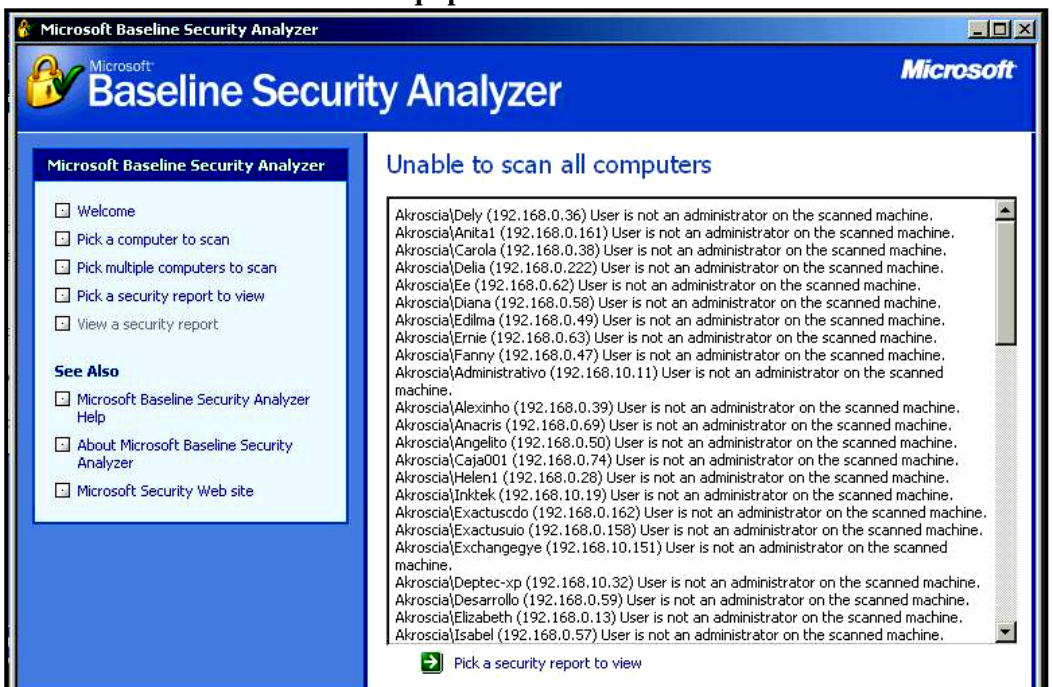


http://www.microsoft.com/spain/seguridad/xp/mbsa/default.asp

Al terminar la búsqueda se muestra un informe de las pc`s encontradas en el dominio, y así se obtendrá un informe donde se mostrará las IP, nombres de máquina y que sistema operativo usan.

Gráfico 37

Equipos encontrados

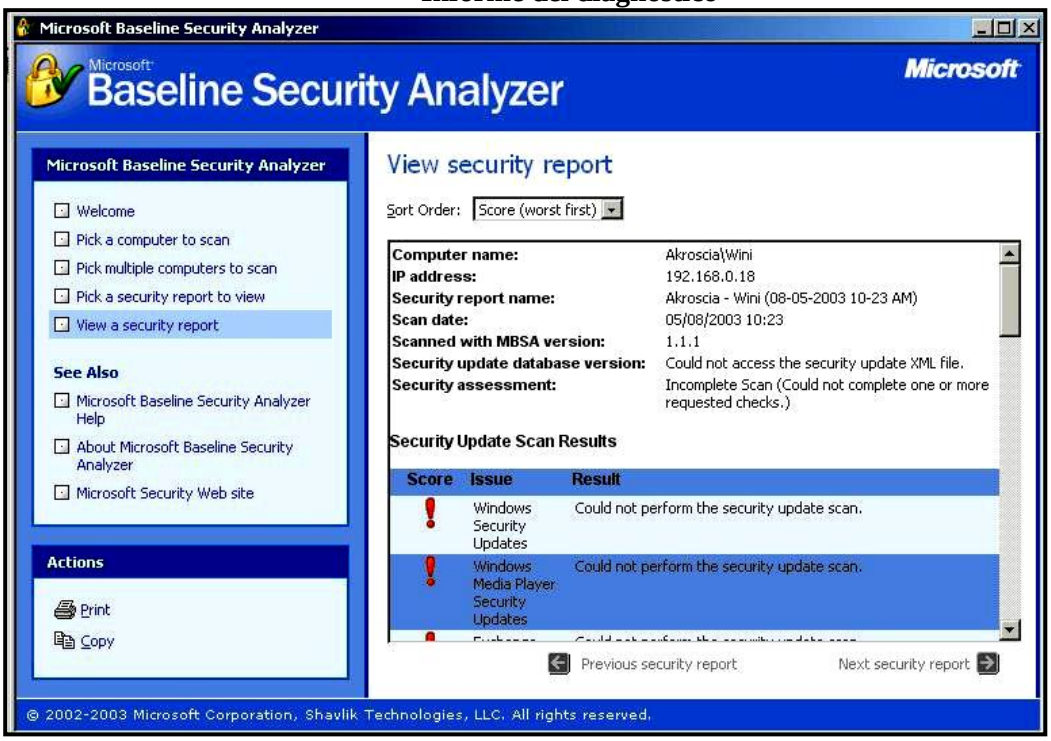


http://www.microsoft.com/spain/seguridad/xp/mbsa/default.asp

Luego con la IP o nombre de máquina se podrá examinar la pc que desee, y el cual presentará un informe completo de las fallas de la misma.

Gráfico 38

Informe del diagnóstico



CAPÍTUL http://www.microsoft.com/spain/seguridad/xp/mbsa/default.asp

AUDITORÍA Y DETECCIÓN DE INTRUSIONES

Un registro de auditoría registra una entrada cada vez que los usuarios realizan determinadas acciones especificadas. Por ejemplo, si se modifica un archivo o una

directiva, se generará una entrada de auditoría. La entrada de auditoría muestra la acción llevada a cabo, la cuenta de usuario asociada y la fecha y la hora de la acción. Se pueden realizar auditorías de los intentos de acciones correctos y fallidos.

En un equipo, el estado del sistema operativo y de las aplicaciones es dinámico. Por ejemplo, quizás sea necesario cambiar temporalmente los niveles de seguridad para permitir la resolución inmediata de un problema de administración o de red. Con frecuencia, este cambio puede ser irreversible. Esto significa que un equipo puede dejar de cumplir los requisitos de seguridad empresarial.

La ejecución de análisis frecuentes permite a los administradores realizar seguimientos y asegurar un nivel adecuado de seguridad en cada equipo como parte de un programa empresarial de administración de riesgos. Los análisis contienen datos muy específicos de todos los aspectos del sistema relacionados con la seguridad (46). De esta manera, el administrador puede optimizar los niveles de seguridad y lo que es más importante, detectar cualquier brecha de seguridad que pueda ocurrir en el sistema con el tiempo.

La auditoría de seguridad es extremadamente importante para cualquier sistema empresarial ya que los registros de auditoría pueden ser los únicos indicadores de que se ha producido una brecha en la seguridad. Si se descubre la brecha por otros medios y los servicios de auditoría están configurados correctamente, se generará un registro de auditoría con información importante acerca de la misma.

(46)www.artscouncil.ie/auditoría/default.asp *23 julio 2003*

Con una configuración correcta de los servicios de auditoría, se asegurará de que se registran algunas acciones así como:

- Actividades de inicio y cierre de sesión, entre ellas, las conexiones remotas y de red.
- Acceso a los archivos y a objetos, como el acceso a archivos y directorios, y el envío de trabajos de impresión.
- Creación y eliminación de archivos y objetos.
- Acceso a privilegios de usuario, excepto a aquéllos relacionados con actividades de inicio y cierre de sesión.
- Actividades de administración de usuarios y grupos, entre ellas, la creación, eliminación, cambio de nombre y otros cambios en cuentas y contraseñas de usuario.
- Cambios en la directiva de seguridad.
- Funciones de administrador del sistema, como los reinicios y cierres del sistema y sus funciones de seguridad.
- Seguimiento de los procesos que se ejecutan en el sistema, incluidos los duplicados y el cierre de programas.
- Hay que tener en cuenta que se deben realizar auditorías de las acciones mencionadas anteriormente, tanto si son correctas como si son fallidas. Con frecuencia, los registros de errores proporcionan más información que los registros de acciones realizadas correctamente, ya que en los primeros se indican los errores generados. Por ejemplo, si un usuario inicia sesión correctamente en el sistema, esta acción se considera normal. Sin

embargo, si el usuario intenta infructuosamente iniciar sesión en el sistema varias veces, esto puede indicar que alguien está intentando entrar con el identificador de usuario de otra persona.

En cualquier entorno seguro, deberá supervisar de forma activa que no se produzcan intrusiones ni ataques. No sería sensato instalar sistemas seguros y asumir que no se va a producir ningún ataque.

Existen varias razones que denotan la importancia de la auditoría y la supervisión de intrusiones entre las cuales se pueden mencionar las siguientes:

- Cualquier entorno informático funcional puede estar sujeto a ataques. Por muy alta que sea la seguridad, siempre existe el riesgo de que se produzca un ataque.
- Los ataques verdaderos suelen producirse a menudo tras varios ataques infructuosos. Si no supervisa que no se produzcan ataques, no los detectará antes de que sean efectivos.
- Si se produce un ataque efectivo, cuanto antes lo detecte, más fácil le resultará contener los daños.
- Para recuperarse de un ataque, necesitará conocer los daños que se han producido.
- La auditoría y la detección de intrusiones le ayudan a determinar el origen del ataque.

- La combinación de la auditoría y la detección de intrusiones permite establecer una correlación entre la información para identificar las pautas de los ataques.
- La revisión habitual de los registros de seguridad ayuda a identificar problemas de configuración de la seguridad desconocidos, como permisos incorrectos u opciones de configuración de bloqueo de cuentas poco estrictas (47).
- Una vez detectado un ataque, la auditoría puede ayudar a determinar los recursos de red que se ven comprometidos.

En las redes conectadas a Internet se hace cada vez más necesario el uso de un sistema de detección de intrusiones. Aunque no sustituye a una revisión diligente de los registros de servidores y servidores de seguridad, la capacidad de un sistema de detección de intrusiones para identificar posibles intrusiones en sus primeras fases permite disponer de más tiempo para responder a un incidente. Coloque el sistema de detección de intrusiones en la zona desmilitarizada clásica DMZ.

Los sistemas de detección de intrusiones son semejantes a las utilidades antivirus, ya que avisan a los administradores únicamente cuando detectan algún elemento que reconocen. Los sistemas de detección de intrusiones contienen una base de datos de firmas de ataques, pero no todos los sistemas de detección tienen la misma capacidad para reconocer distintos tipos de ataques o de mantenerse actualizados (las bases de datos de firmas y los sistemas de

actualización de los distintos proveedores de sistemas de detección de intrusiones son secretos comerciales). La mayor parte de los sistemas de detección de intrusiones funciona en el nivel de red, desde donde se alerta a los administradores después de que la red haya sufrido un ataque. Recientemente, ha surgido una nueva categoría de sistemas de detección de intrusiones los sistemas de detección de intrusiones basados en host. Estas herramientas se ejecutan en los propios servidores y avisan a los administradores cuando un equipo es atacado. Este tipo de mecanismo de alerta es especialmente importante para los equipos que contienen datos operativos valiosos, tales como servidores finales de base de datos.

La combinación de sistemas de detección de intrusiones basados en la red y en host, y el examen periódico de los registros por parte de expertos en seguridad son los métodos más efectivos para proteger la red, recopilar pruebas y controlar incidentes de seguridad.

Una zona desmilitarizada clásica (DMZ) tiene dos servidores de seguridad (48). El servidor de seguridad externo está configurado para permitir únicamente el tráfico necesario para las conexiones entre Internet y la DMZ. El servidor de seguridad interno está configurado para proteger la red interna de la DMZ, una DMZ es una red en la que no se confía, por lo que necesita protección para la red interna.

Piense en la única zona desmilitarizada política del mundo un pequeño territorio entre Corea del Norte y Corea del Sur. Una DMZ está definida por sus

límites de protección en este caso, dos fronteras físicas, cada una de ellas supervisada y asegurada por una entidad de protección distinta. Una DMZ en la red viene a ser algo similar: un segmento de red independiente conectado (normalmente) a dos redes a través de servidores de seguridad distintos.

¿Por qué se debe implementar una DMZ? Los ataques a las redes están en auge, ya sea por simple diversión o con propósitos de espionaje corporativo y destrucción. Una arquitectura de seguridad eficaz presenta barreras ante los ataques a la vez que proporciona la posibilidad de escalar. Las ventajas de una arquitectura de DMZ real son las siguientes:

- Directivas de seguridad individualizadas. Cada servidor de seguridad

(48)www.vnunet.es/Actualidad/Noticias/Seguridad/ Sistemas_de_protección/20030416038 25 julio 2003

- Defensa en profundidad. Existen diversos equipos que proporcionan a los administradores de seguridad más tiempo para responder durante una infracción de la seguridad. Ésa es la principal razón para implementar una arquitectura de DMZ reales en vez de subredes filtradas.
- Rendimiento mejorado. Las tareas de inspección del tráfico se dividen entre dos dispositivos, cada uno de los cuales está configurado para su zona de protección específica.
- Escalabilidad. Puede escalar los servidores de seguridad como sea necesario: a menudo, el servidor de seguridad externo debe controlar una carga muy superior a la del servidor de seguridad interno.

Para conseguir una alta disponibilidad, deberá distribuir al menos una pareja de equilibradores de carga totalmente integrados con una pareja de servidores de seguridad (49). Los servidores de seguridad se integran completamente con los conmutadores básicos de la DMZ.

6.1.- Auditoría

Como parte de la estrategia general de seguridad, deberá determinar el nivel de auditoría que sea apropiado para el entorno. La auditoría debe identificar los ataques, tanto si son efectivos como infructuosos, que representan una amenaza para la red o ataques contra recursos que considera valiosos como parte de la evaluación de riesgos.

Al decidir el nivel de auditoría, deberá tener en cuenta que cuanto más alto sea el

(49)http://www.crammusergroup.org.uk/. 28 julio 2003 esos críticos (50).

Los sucesos de auditoría pueden dividirse en dos categorías: sucesos de acierto y sucesos de error. Los sucesos de acierto indican que un usuario ha conseguido obtener acceso a un recurso, mientras que los sucesos de error indican que se produjo un intento fallido. Los sucesos de error resultan muy útiles a la hora de realizar un seguimiento de intentos de ataque en el entorno, pero los sucesos de acierto son mucho más difíciles de interpretar. Aunque la inmensa mayoría de los sucesos de auditoría de acierto son simplemente indicaciones de actividad normal, si un atacante consigue obtener acceso al sistema, también se generará un suceso

de acierto. A menudo, la pauta de sucesos es tan importante como los sucesos en sí. Por ejemplo, varios errores seguidos por un acierto pueden indicar un intento de ataque que acabó teniendo éxito.

Siempre que sea posible, deberá combinar sucesos de auditoría con otra información acerca de los usuarios. Por ejemplo, si los usuarios se van de vacaciones, puede desactivar las cuentas durante ese período y auditar si se activan de nuevo.

La auditoría se activa mediante la directiva de grupo en el nivel de sitio, dominio, unidad organizativa o equipo local.

Normalmente, deberá implementar la auditoría en un nivel alto de la jerarquía de Active Directory, puesto que le ayudará a mantener la coherencia de la configuración de auditoría. Todos los sucesos generados por la auditoría aparecen en el visor de sucesos. Debe determinar cómo almacena el registro de sucesos que se generan. Cada una de las opciones de configuración puede definirse directamente en el visor de sucesos o en la directiva de grupo. Es posible que

(50)www.microsoft.com/latam/technet/articulos/windows2ksrvr/staysecure/chapters/ch06secops.asp
29 julio 2003

configuración en otro nivel. Por ejemplo, puede suceder que el registro de seguridad se llene con los servidores IIS y el sistema se colapse. Para evitarlo, modifique la directiva de grupo en la unidad organizativa de servidores IIS para aumentar el tamaño del registro de seguridad o modifique la directiva de forma que el sistema no se colapse cuando se llene el registro de seguridad.

6.2.- Sucesos para auditar

Windows 2000 incluye varias categorías de auditoría para los sucesos de seguridad. Al diseñar la estrategia de auditoría de la empresa, deberá decidir si va a incluir las categorías de sucesos de auditoría de seguridad, como los que se menciona a continuación:

6.2.1.- Sucesos de inicio de sesión

Si audita sucesos de inicio de sesión, cada vez que un usuario inicie o cierre la sesión en un equipo, se generará un suceso en el registro de seguridad del equipo en que se produce el intento de inicio de sesión. Además, cuando un usuario se conecta a un servidor remoto, se genera un suceso de inicio de sesión en el registro de seguridad del servidor remoto. Los sucesos de inicio de sesión se generan cuando se crean o destruyen respectivamente la sesión y el testigo de inicio de sesión (51).

Los sucesos de inicio de sesión pueden resultar útiles para realizar un seguimiento de los intentos de inicio de sesión interactivo en servidores o para investigar los ataques iniciados desde un equipo determinado. Las auditorías de aciertos generan una entrada de auditoría cuando un intento de inicio de sesión es efectivo. Las auditorías de errores generan una entrada de auditoría cuando un intento de inicio

(51)www.microsoft.com/windows2000/es/advanced/ help/sag_SEprocsAuditing.htm 30 julio 2003

Los sucesos de inicio de sesión incluyen tanto sucesos de inicio de sesión de equipos como de usuarios. Comprobará que existen entradas de registro de

sucesos de seguridad independientes para la cuenta del equipo y la cuenta del usuario cuando se intenta realizar una conexión a la red desde un equipo basado en Windows NT o Windows 2000. Los equipos basados en Windows 9x no tienen cuentas de equipo en el directorio y no generan entradas de registro de sucesos de inicio de sesión de equipos para sucesos de inicio de sesión de red.

Como parte de las directivas de línea de base para servidores miembros y controladores de dominio, la auditoría de aciertos y errores de sucesos de inicio de sección se encuentra activada.

En la tabla (6) se describe los sucesos de inicio de sesión que aparecen en el registro de suceso.

Tabla 6
Sucesos de inicio de sesión que aparecen en el registro de sucesos

Suceso	Descripción
528	Un usuario inició la sesión correctamente en un equipo.
529	El intento de inicio de sesión se realizó con un nombre de usuario desconocido o con un nombre de usuario conocido y una contraseña incorrecta.
530	La cuenta de usuario intentó iniciar la sesión fuera del período de tiempo permitido.
531	Se produjo un intento de inicio de sesión con una cuenta desactivada
532	Se produjo un intento de inicio de sesión con una cuenta caducada
533	El usuario no tiene permiso para iniciar la sesión en este equipo.
534	El usuario intentó iniciar la sesión con un tipo de inicio de sesión no permitido (de red, interactivo, por lotes, de servicios o interactivo remoto).

535	La contraseña de la cuenta especificada ha caducado.
536	El servicio Inicio de sesión en la red no está activo.
537	Error del intento de inicio de sesión por otras razones
538	Un usuario cerró la sesión.
539	La cuenta se bloqueó cuando se intentó iniciar la sesión. Este suceso puede indicar un ataque de contraseñas infructuoso, lo que hace que se bloquee la cuenta.
540	Inicio de sesión en la red correcto. Este suceso indica que un usuario remoto se ha conectado correctamente de la red a un recurso local del servidor y que se ha generado un testigo para el usuario de red.
682	Un usuario se ha conectado de nuevo a una sesión de Servicios de Terminal Server desconectada. Este suceso indica la conexión a una sesión anterior de Servicios de Terminal Server.
683	Un usuario ha desconectado la sesión de Servicios de Terminal Server sin cerrarla primero. Este suceso se genera cuando un usuario está conectado a una sesión de Servicios de Terminal Server en la red. Aparece en Terminal Server.

www.eu.microsoft.com/spain/technet/seguridad/ 2000server/chapters/ch06secops.asp

Los siguientes sucesos de seguridad pueden diagnosticarse por medio de entradas de sucesos de inicio de sesión:

6.2.2.- Intentos de inicio de sesión local infructuosos. Cualquiera de los siguientes Id. de suceso indica intentos de inicio de sesión infructuosos: 529, 530, 531, 532, 533, 534 y 537. Verá los sucesos 529 y 534 si un atacante intenta adivinar una combinación de nombre de usuario y contraseña para una cuenta local y no lo consigue. No obstante, estos sucesos también pueden producirse cuando un usuario se olvida de la contraseña o empieza a explorar la red por medio de mis sitios de red. En un entorno de grandes dimensiones, puede resultar

difícil interpretar correctamente estos sucesos (52). Como norma general, deberá investigar estas pautas si se producen de forma repetida o coinciden con otros factores poco habituales. Por ejemplo, varios sucesos 529 seguidos por un suceso 528 durante la noche podrían indicar un ataque de contraseñas efectivo (aunque podría ser simplemente un administrador demasiado cansado).

6.2.3.- Uso incorrecto de cuentas. Los sucesos 530, 531, 532 y 533 pueden representar el uso incorrecto de una cuenta de usuario. Los sucesos indican que se introdujo correctamente la combinación de cuenta y contraseña, pero que otras restricciones no permiten el inicio de sesión correcto. Siempre que sea posible, deberá investigar estos sucesos para determinar si se ha utilizado incorrectamente una cuenta o si se deben modificar las restricciones actuales. Por ejemplo, es posible que necesite ampliar las horas de inicio de sesión de determinadas cuentas.

6.2.4.- Bloqueo y administración de cuentas. El suceso 539 indica que se bloqueó una cuenta. Puede ser indicativo de un ataque de contraseñas infructuoso. Deberá buscar sucesos 529 anteriores de la misma cuenta de usuario para averiguar la pauta de intentos de inicio de sesión.

Ataques de los Servicios de Terminal Server, las sesiones de los Servicios de Terminal Server pueden dejarse conectadas de forma que los procesos puedan continuar ejecutándose tras el cierre de la sesión. El Id. de suceso 683 indica cuándo un usuario no cierra la sesión de Servicios de Terminal Server y el Id. de

suceso 682 indica cuándo alguien se conecta a una sesión previamente desconectada.

La auditoría de la administración de cuentas sirve para determinar cuándo se crean, modifican o eliminan los usuarios o grupos. Esta auditoría puede utilizarse para determinar cuándo se creó un principal de seguridad y quién realizó la tarea.

Como parte de las directivas de línea de base para servidores miembros y controladores de dominio, la auditoría de aciertos y errores de la administración de cuentas se encuentra activada. Por lo tanto, en la tabla 7 se muestra el suceso de administración de cuentas de suceso registrados en el registro de seguridad.

Tabla 7
Sucesos de administración de cuentas que aparecen en el registro de sucesos

Suceso	Descripción
624	Cuenta de usuario creada
625	Cambio de tipo de cuenta de usuario
626	Cuenta de usuario habilitada
627	Intento de cambio de contraseña
628	Contraseña de cuenta de usuario establecida
629	Cuenta de usuario deshabilitada
630	Cuenta de usuario eliminada
631	Grupo global habilitado de seguridad creado
632	Miembro de grupo global habilitado de seguridad agregado
633	Miembro de grupo global habilitado de seguridad eliminado
634	Grupo global habilitado de seguridad eliminado

635	Grupo local deshabilitado de seguridad creado
636	Miembro de grupo local habilitado de seguridad agregado
637	Miembro de grupo local habilitado de seguridad eliminado
638	Grupo local habilitado de seguridad eliminado
639	Grupo local habilitado de seguridad modificado
641	Grupo global habilitado de seguridad modificado
642	Cuenta de usuario modificada
643	Directiva de dominio cambiada
644	Cuenta de usuario bloqueada

www.eu.microsoft.com/spain/technet/seguridad/ 2000server/chapters/ch06secops.asp

6.3.- Uso de privilegios

Los usuarios que trabajan en un entorno de TI ejercitan derechos de usuario definidos. Si audita los aciertos y errores del uso de privilegios, se generará un suceso cada vez que un usuario intente ejercer un derecho de usuario.

Incluso si se audita el uso de privilegios, no se auditarán todos los derechos de usuario.

La auditoría de aciertos del uso de privilegios creará un alto número de entradas en el registro de seguridad (53). Por esta razón, las directivas de línea de base para servidores miembros y controladores de dominio sólo auditan sucesos de error del uso de privilegios.

Cuando la auditoría del uso de privilegios está activada, se generan los siguientes sucesos como se muestra en la tabla 8

Tabla 8
Sucesos de uso de privilegios que aparecen en el registro de sucesos.

576	Se agregaron privilegios específicos al testigo de acceso de un usuario (este evento se genera cuando el usuario inicia la sesión).
577	Un usuario intentó realizar una operación de servicios del sistema privilegiada.
578	Se utilizaron privilegios en un identificador ya abierto de un objeto protegido.

(53)www.eu.microsoft.com/spain/technet/seguridad/ 2000server 7 agosto 2003

www.eu.microsoft.com/spain/technet/seguridad/ 2000server/chapters/ch06secops.asp

6.4.- Programar revisiones regulares de los registros de sucesos

Tal y como se mencionó anteriormente, el registro de seguridad y potencialmente los otros registros de sucesos deberían escribirse en materiales extraíbles o consolidarse en una ubicación central para su revisión. La revisión de los registros es el paso de la auditoría que se suele omitir más a menudo.

Deberá asegurarse de que una persona o un equipo adopten la revisión de los registros de sucesos como tarea habitual en su descripción de trabajo. La revisión

de los registros de sucesos puede programarse como un suceso diario o semanal, en función de la cantidad de datos que se recojan en el registro de seguridad. Esto suele depender del nivel de auditoría aplicado en la red. Si se incluyen más sucesos en la auditoría, aumentará el volumen de entradas del registro. Si programa revisiones regulares del registro de sucesos, ayudará a conseguir lo siguiente:

6.4.1.- Detección más rápida de problemas de seguridad. Si se lleva a cabo la revisión diaria de los registros de sucesos, la antigüedad de un suceso de seguridad nunca superará las 24 horas. Esto acelera la detección y reparación de vulnerabilidades de seguridad.

6.4.2.- Definición de la responsabilidad. Si resulta necesaria la revisión regular de los registros de sucesos, la persona responsable de la tarea de revisar los archivos de registro puede ser responsable de la identificación de posibles ataques en última instancia.

6.5.- Supervisar y analizar los puertos abiertos

Los ataques se inician a menudo con la detección de puertos para identificar servicios conocidos que se ejecutan en el equipo de destino. Deberá asegurarse de supervisar cuidadosamente los puertos que están abiertos en los servidores, lo que normalmente implica realizar una detección de los puertos para determinar aquellos a los que se puede tener acceso.

Las detecciones de puertos deberán realizarse tanto de forma local, en el equipo de destino, como desde un equipo remoto. Si se puede obtener acceso al equipo desde una red pública, la detección de puertos deberá llevarse a cabo desde un equipo externo para garantizar que el software del servidor de seguridad permita solamente el acceso a los puertos deseados.

Si se descubren puertos abiertos no reconocidos, deberá investigarlos para determinar si el servicio correspondiente resulta necesario en el equipo. De lo contrario, deberá desactivar o eliminar el servicio asociado para evitar que el equipo escuche en ese puerto. Se han desactivado varios servicios de las directivas de línea de base para servidores miembros y controladores de dominio incluidas en esta guía.

Puesto que muchos servidores están protegidos por servidores de seguridad o enrutadores de filtrado de paquetes. La detección remota de puertos indica los puertos que se encuentran disponibles para usuarios externos cuando intentan conectarse al equipo.

La detección de puertos también puede utilizarse para probar el sistema de detección de intrusiones y así garantizar que registra la detección de puertos mientras se está llevando a cabo.

El análisis de todos los puertos es un método utilizado por atacantes para determinar los puertos abiertos de un equipo o una red de destino. El motor de detección de intrusiones detecta varios intentos de conexión a los puertos y envía

una alerta cuando el número de intentos de conexión supera el umbral configurado por un administrador.

6.6.- Supervisar las intrusiones y los sucesos de seguridad

La supervisión de intrusiones y sucesos de seguridad incluye tanto tareas activas como pasivas. Muchas intrusiones se detectan una vez que se ha producido el ataque por medio de la inspección de los archivos de registro (54). La detección de ataques se suele denominar detección de intrusiones pasiva. La inspección de los archivos de registro es la única forma en que se puede revisar y reconstruir el ataque en función de la información del registro.

Otros intentos de intrusión pueden detectarse mientras se produce el ataque. Este método, denominado detección de intrusiones activa, busca pautas o comandos de

(54)www.eu.microsoft.com/spain/technet/seguridad/ 2000server 7 agosto 2003

Otro ataque común consiste en el rastreo de paquetes en la conexión. Las redes creadas con concentradores simples facilitan mucho este rastreo, a pesar de la reciente introducción de herramientas de protección contra rastreo que a menudo pueden no ser confiables (55). (Las herramientas anti herramientas de rastreo confirman este punto). El uso de conmutadores en lugar de concentradores elimina este punto débil. En una red de medios compartidos (es decir, una red creada con concentradores) todos los dispositivos ven todo el tráfico.

6.7.- Soluciones de terceros para la detección de intrusiones

Existen soluciones de terceros tanto para sistemas de detección de intrusiones de red como de extremos. Estas soluciones de terceros son compatibles con otros protocolos además de HTTP y también realizan un análisis para detectar ataques conocidos de equipos de red.

Entre los tipos de ataques habituales que deberían identificar los sistemas de detección de intrusiones, figuran:

6.7.1.- Ataques de reconocimiento. Se producen cuando un atacante mantiene vigilada una red para encontrar vulnerabilidades. Entre los posibles ataques se incluyen los rastreos ping, las transferencias de zonas de DNS, el reconocimiento de correo electrónico, los análisis de puertos y la descarga de contenido de sitios web para buscar archivos de comandos y páginas de muestra vulnerables.

(55)es.sun.com/services/training/catalogue/ courses/WT-1254.html *8 agosto 2003*

características o problemas ocultos para obtener acceso al sistema. A menudo los puntos de ataque se identifican por medio de un ataque de explotación previo.

6.7.3.- Ataques de denegación de servicio. Se producen cuando un atacante intenta bloquear un servicio que se ejecuta en un equipo sobrecargando recursos, como los vínculos de red, la CPU o el subsistema de disco (56). El atacante no está intentando obtener información, sino desactivar el equipo.

Un buen sistema de detección de intrusiones debe poder identificar los tres tipos de ataques. Se utilizan dos métodos distintos para identificar ataques:

6.7.4.- Detección de anomalías. Está basado en tomar como referencia una línea de base de un equipo en la red. Las desviaciones de la línea de base pueden identificar un intento de intrusión. Por ejemplo, el aumento de intentos de inicio de sesión durante horas no punta puede identificar un equipo en peligro. La ventaja de la detección de anomalías radica en que puede identificar ataques sin tener que conocer exactamente el funcionamiento de los mismos.

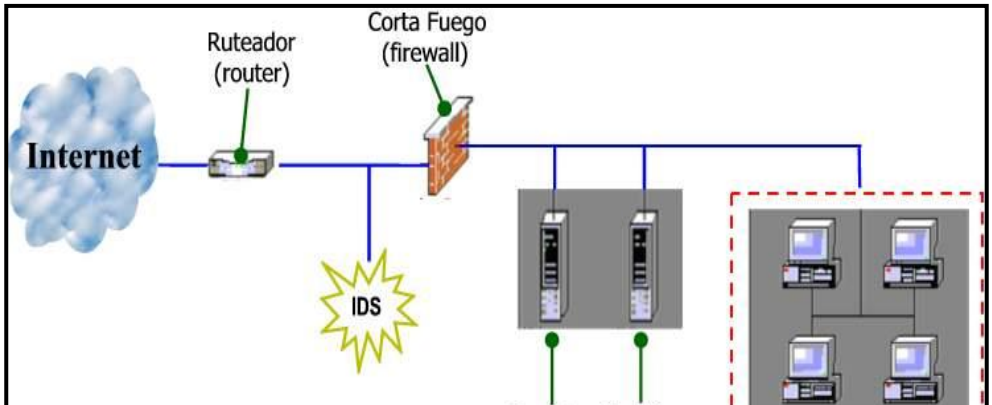
6.7.5.- Reconocimiento de firmas. Identifica ataques en función de las pautas conocidas de los mismos. Por ejemplo, muchos ataques de servidores web utilizan pautas comunes de fácil identificación. El sistema de detección de intrusiones puede identificar estos ataques por medio de la comparación del tráfico de aplicaciones entrante con cadenas de firmas de una base de datos. La desventaja de este método del sistema de detección de intrusiones es que se debe actualizar a menudo la base de datos de firmas para poder identificar nuevas firmas de ataques.

(56)www.dggomez.arrakis.es/secinf/ids/IDS_v1.0.pdf *11 agosto 2003*

de intrusiones.

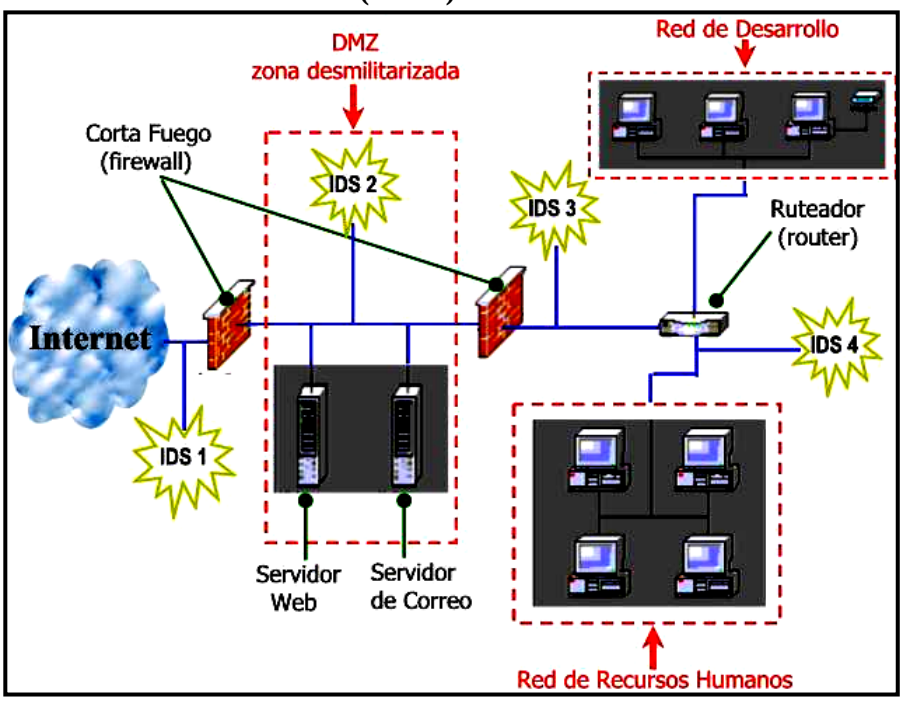
En los gráficos siguientes (gráfico 39 y gráfico 40) se muestra una red con uno y varios IDS.

Gráfico 39
IDS



http://www.tlc-sa.com.ar/images/Red_con_IDS.jpg

Gráfico 40
IDS(varios)



6.8.- Evaluación

http://www.tlc-sa.com.ar/images/Red_sin_IDS1.jpg

Además de llevar a cabo la detección de intrusiones activa y pasiva, también deberá realizar evaluaciones periódicas de vulnerabilidad. Las evaluaciones de vulnerabilidad simulan un ataque en la red y detectan las vulnerabilidades que encontraría un atacante.

Si lleva a cabo evaluaciones periódicas, podrá descubrir las vulnerabilidades antes que los atacantes y asegurar la parte menos sólida de la red para protegerla de la vulnerabilidad.

Al estudiar herramientas de evaluación de vulnerabilidad, incluya los siguientes requisitos en el proceso de toma de decisiones:

6.8.1.- Mecanismo de actualización de bases de datos. La herramienta debería incluir un método automático de actualización de las firmas para vulnerabilidades de forma que no se quede obsoleta en poco tiempo.

6.8.2.- Minimizar positivos falsos. La herramienta debería excluir los positivos falsos de forma que la organización no pierda el tiempo investigando sucesos no relacionados con la seguridad.

Capacidad de almacenar los resultados en una base de datos. La herramienta deberá permitir el archivado de los resultados de la detección para poder llevar a cabo un análisis de tendencias y detectar cambios en la seguridad con el tiempo.

6.8.3.- Proporcionar soluciones a las vulnerabilidades encontradas. Si se encuentra una vulnerabilidad, la herramienta debería incluir documentación acerca de cómo solucionarla o secuencias de comandos que realicen las tareas necesarias para protegerse de la vulnerabilidad.

Como alternativa, puede resultar más apropiado utilizar un servicio de asesoramiento de terceros para que lleve a cabo la evaluación de vulnerabilidad.

La ventaja de utilizar un servicio de terceros radica en que no disponen de conocimientos previos acerca de la red y trabajarán con el mismo punto de partida que un atacante externo (57). Con frecuencia, estas evaluaciones externas proporcionan la información más útil gracias a la neutralidad del equipo de evaluación.

Clasificar las amenazas a la vulnerabilidad (valorar cada una de las amenazas identificadas). Los activos que intervienen reciben una clasificación de seguridad basada en la confidencialidad, integridad, disponibilidad, y relacionada con las amenazas identificadas. El sistema de clasificación debe adaptarse siempre a las necesidades de la organización del cliente así como:

- Confidencialidad:

  Esencial.- Los intereses empresariales del ASP quedarán gravemente dañados si se producen accesos no autorizados (por ejemplo, a información estratégica).

  Importante.- Datos a los que sólo pueden tener acceso las personas directamente implicadas (información de cuentas, fichas médicas).

  Necesaria.- Datos que sólo deben ser vistos por un grupo determinado.

  Innecesaria.- Información puede ser publicada.

- Integridad

(57)www.intelap.com.ar/vulnerabilidad.htm *12 agosto 2003*

Esencial.- El proceso empresarial del ASP y de los clientes exige información sin errores (como las soluciones ATM y otras soluciones de banca).

Importante.- Se puede admitir un número muy pequeño de errores detectables.

Necesaria.- Los procesos empresariales del ASP y de los clientes toleran algunos errores.

Innecesaria.- No se necesita ninguna medida adicional de protección de la integridad.

- Disponibilidad

Esencial.- Sólo para operaciones con una misión crítica (como contingencias).

Importante.- Prácticamente ningún tiempo de inactividad durante las horas laborables (alta disponibilidad).

Necesaria.- Se pueden aceptar tiempos de inactividad ocasionalmente.

Innecesaria.- No se necesitan garantías (acceso gratuito a Internet).

Cuando los niveles de riesgo para la seguridad estén evaluados, a partir de ahí se puede medir el riesgo general. Esta operación puede realizarse como medida

si se han recopilado datos cuantitativos o cualitativos mediante una evaluación subjetiva de nivel bajo, medio o alto.

CAPITULO VII

Conclusiones

1.- Bajo este sistema operativo se logró auditar el entorno para mejorar al máximo la detección de ataques y trata la supervisión de intrusiones, como el uso de sistemas de detección de intrusiones.

2.- Windows 2000 Server ofrece una plataforma aún más confiable y escalable para las necesidades empresariales esenciales del usuario. Además proporciona una administración de memoria mejorada, una arquitectura de sistema más robusta y una gran variedad de utilidades de diagnóstico y de solución de problemas. A medida que agregue usuarios y funcionalidad al sistema, tendrá la seguridad de obtener un servicio confiable.

3.- Windows 2000 Server proporciona unos servicios de administración flexibles basados en directivas que le permitirán proteger y administrar las redes, los servidores y los sistemas clientes. Gracias a las novedades y las mejoras en los servicios (por ejemplo, el servicio de directorio Active

Directory, la administración remota y los servicios de seguridad distribuidos de tipo empresarial), se simplifica y facilita la administración de la red.

4.- Las aplicaciones existentes se ejecutarán mejor en Windows 2000 Server, ya que se podrán aprovechar un sistema operativo de servidor más confiable, rápido y fácil de administrar. Esta versión incluye Servicios de componentes, cuya compatibilidad integrada supera la del resto de los sistemas operativos de servidor; esta herramienta permite escribir y distribuir aplicaciones basadas en componentes eficaces y escalables.

5.- Windows 2000 Server facilita todavía más la configuración del hardware y el software y reduce significativamente el número de veces que debe reiniciarse el sistema.

6.- Mediante el sistema Plug and Play, una combinación de compatibilidad de hardware y software, el servidor puede reconocer y adaptarse automáticamente a los cambios en la configuración del hardware, sin que sea necesaria la intervención del usuario o el reinicio del sistema.

7.- La familia Windows 2000 Server abarca desde distribuciones de grupos de trabajo pequeños a distribuciones de centros de datos empresariales. La familia Windows 2000 Server incluye productos que admiten un máximo de 32 procesadores y sistema de E/S avanzado. También integra el equilibrio de la

carga de la red y nuevas optimizaciones de multiprocesador para las aplicaciones empresariales.

8.- Para reducir los costos totales de propiedad, Windows 2000 Server proporciona servicios de administración completos y eficaces que permiten administrar servidores, redes y sistemas clientes. Windows 2000 Server introduce Active Directory, un servicio de directorios basado en los estándares Internet que integra de manera única la administración de sistemas flexible basada en directivas y los servicios de autenticación y autorización eficaces con características como la consolidación de directorios, e infraestructura y aplicaciones habilitadas para directorio.

Recomendaciones

1.- Para la instalación de Windows 2000 Server se debe establecer una organización o un grupo de seguridad, escribir una directiva de seguridad completa para la organización, llevar a cabo un análisis de riesgos, desarrollar un plan de implementación, realizar un mantenimiento continuado.

2.- Ocuparse de todos los aspectos relacionados con la administración de los empleados, desde determinar los conocimientos y habilidades necesarios para realizar determinadas tareas hasta establecer el número de personas requeridas en una determinada función o su contratación y dirección. En esta función se debe realizar la comprobación de los conocimientos cuando se contrata a los empleados y al revisar de forma continuada el rendimiento. Se deberá asegurar de que se

realizan las comprobaciones de conocimiento necesarias antes de permitir la entrada del empleado en las instalaciones de la compañía o el acceso a los sistemas informáticos de la organización. En segundo lugar, es posible que los empleados descontentos intenten dañar los datos o los recursos de la organización.

3.- Prestar atención a la administración de los movimientos de los empleados. Cuando cambian de un puesto a otro, es posible que sea necesario modificar sus accesos de seguridad para que se adapten a sus nuevas áreas de responsabilidad. Se debe retirar el acceso a aquellos empleados que abandonen la organización después de su último día. Por estos motivos, el grupo de seguridad debe trabajar conjuntamente con los administradores de la organización, a todos los niveles, con el fin de coordinar sus actividades ya que puede implicar algún riesgo adicional los cambios de puesto dentro del propio grupo de tecnologías de la información. Si un individuo que deja una compañía tiene acceso a varios sistemas, puede ser preciso volver a establecer numerosas contraseñas y deshabilitar toda la información de inicio de sesión personal.

4.-Los problemas de seguridad más frecuentes incluye una lista de problemas de seguridad comunes que pueden darse en una organización. Estos errores aumentarán significativamente por esto se debe definir directivas de seguridad, apropiadas donde deberá asegurarse de minimizar la posibilidad de que ocurran estos problemas.

5.- Proteger los archivos clave de sistema y de datos contra el acceso no autorizado es una parte esencial de la protección contra cualquier código de ataque hostil.

6.- Minimizar los riesgos de seguridad con una buena administración de revisiones., tomando en serio la administración de revisiones, la cual puede reducir notablemente los costos asociados con los problemas de seguridad.

7.- La administración de la seguridad garantiza que la seguridad del sistema no se verá comprometida con independencia del modelo elegido ya que la administración del sistema examina las ventajas e inconvenientes de cada modelo. Cada tipo de modelo de administración del sistema tiene requisitos singulares de red en donde la administración del sistema está relacionada con el modelo de administración utilizado en una organización. Algunas organizaciones prefieren un modelo en el que todas las funciones informáticas se ejecuten en un solo sitio con un equipo de profesionales ubicados en él. Otras prefieren un modelo con sucursales distribuidas donde la tecnología y el personal de asistencia técnica estén esparcidos geográficamente.

8.- Asignar tareas de procesamiento por lotes en diferentes momentos del día (o de la noche), de forma que se aprovechen al máximo los recursos del sistema, pero sin comprometer el funcionamiento del sistema o del negocio. Es importante que todos los trabajos relacionados con la seguridad se programen y ejecuten correctamente, y que se comuniquen con rapidez los resultados de estos trabajos y cualquier problema que pueda existir al equipo encargado de la seguridad.

Algunos ejemplos de trabajos de seguridad por lotes pueden ser una secuencia de comandos que valide si los usuarios activos de un sistema son empleados que aún se encuentran en la base de datos de personal o una secuencia de comandos que compare los registros de auditoría del sistema operativo y de la base de datos para comprobar si coinciden elementos como las horas de inicio y cierre de sesión.

9.- Según el entorno y la programación, puede ser necesario programar y ejecutar las tareas de seguridad en momentos específicos de un día, semana o mes, de forma que se pueda garantizar que únicamente están activos en el sistema los usuarios autorizados. A menudo, en estas tareas se suele avisar a los usuarios antes de que finalice el plazo de su autorización y luego se les expulsa del sistema si aún están activos. Estos trabajos pueden ser esenciales para garantizar la integridad de los datos en algunos entornos en los que, por ejemplo, es imprescindible que cuadren las cifras financieras al finalizar la jornada laboral. La ejecución de estos trabajos debe coordinarse cuidadosamente dentro del entorno tecnológico, así como con los administradores de la empresa, y se debe supervisar su correcta ejecución antes de iniciar la siguiente fase de las operaciones del sistema.

10.- La seguridad es un componente esencial en la administración de la configuración. Esta función incluye el seguimiento del hardware propiedad de la organización, así como de las versiones utilizadas del software interno. Los administradores deben estar al tanto de las versiones de sistemas operativos, sistemas de administración de bases de datos y aplicaciones usadas en los equipos

de la red y detentar un control absoluto sobre ellas. Si la administración de la configuración no se realiza correctamente, podría facilitar la entrada de código malintencionado en los sistemas operativos o en una aplicación.

11.- Debe existir una continuidad del servicio cuya función se ocupa del cambio automático a un servidor alternativo cuando un servidor está inactivo temporalmente y la transferencia posterior al servidor principal cuando vuelve a estar operativo. El componente de seguridad principal en este proceso es el mantenimiento de toda la información de seguridad (como los derechos de acceso y las configuraciones del registro de auditoría) y de los procesos de seguridad (como la creación del registro de auditoría) en el sistema alternativo, en las mismas condiciones en que se mantiene en el original. Además, se deben proteger los registros de auditoría de seguridad para evitar que se eliminen si un servidor se apaga repentinamente.