UT 7: Seguridad Activa en el Sistema

Contenido

Seguridad en el acceso en el ordenador

Por muchas medidas de control de acceso que pongamos, un hacker se puede sentar delante del ordenador de nuestra empresa o bien robar un portátil a un directivo. Para ponerlo un poco más difícil se pueden poner algunos obstáculos como:

Se pueden poner impedimentos para que se pueda abrir la caja como:

1. Colocar un candado en las cajas. En los portátiles está el famoso **candado Kennsington.** Los candados son poco efectivos. La mayoría de las cajas de ordenadores profesionales llevan un detector que graba en la memoria de la BIOS la fecha y la hora en que se ha producido la apertura. Al día siguiente cuando se abre el ordenador aparecerá el mensaje.

Se debe asegurar el arranque usando contraseñas:

1. **La BIOS**: Es la encargada de localizar y cargar el sistema operativo o gestor de arranque.
2. **Proteger el Grub** con contraseñas. (Cuando tienes 2 S.O. en el mismo ordenador es la pantalla que sale al principio dándote a elegir el S.O. a arrancar).
3. **Cifrar particiones.**
4. **Cuotas de disco:** Es un mecanismo que permite impedir que ciertos usuarios hagan uso indebido de la capacidad del disco, para evitar la ralentización del equipo.

Autenticación de usuarios

A- Métodos de autenticación:

1- Algo que el usuario sabe
2- Algo que el usuario posee
3- Características propias del usuario: Huellas dactilares y reconocimiento biométricos.
4- Combinación de distintos métodos para tener mayor seguridad.

B- Políticas de contraseñas:

1. La autenticación se realiza poniendo nombre y contraseña.
2. La seguridad del sistema está muy relacionada con la elección de la contraseña. Las características que deben cumplir una buena contraseña son:
    1. No se deben poner palabras reconocidas en el diccionario.
    2. No se deben emplear solo letras mayúsculas, minúsculas y números.
    3. No se debe utilizar información personal.
    4. No se deben invertir las palabras.
    5. No se deben repetir los caracteres.
    6. No se debe escribir la contraseña en ningún sitio.

7. No se debe enviar por correo electrónico ni por teléfono.
8. Limitar el número de veces de entrada a una contraseña.
9. Cambiar la contraseña habitualmente.
10. No utilizar la misma contraseña para diferentes máquinas.

3. Las contraseñas deben ser:
    a. Cadenas de caracteres compuestas por mayúsculas, minúsculas, caracteres especiales.
    b. La longitud oscila entre 8 y 14 caracteres.
    c. En general se debe intentar cumplir todas las características vistas anteriormente.

C- **Sistemas biométricos**: Se utilizan para autenticar usuarios a través de rasgos físicos o conductas.

D- **Tarjetas**: en ocasiones las contraseñas no son suficientes y puede ser inseguro. En este caso se aplican la estrategia "**algo que tiene**" como son las tarjetas, Ejemplo los cajeros automáticos de los bancos aplican una seguridad doble: la tarjeta más un PIN.

Las tarjetas son de dos tipos: sencillas (magnéticas) o complejas (chip), estas últimas son más seguras pero más caras. Hay dos tipos:

- Las que son simplemente un dispositivo de almacenamiento: contienen nuestras claves para que las lea el dispositivo donde introducimos la tarjeta.
- Las que constituyen un dispositivo de procesamiento, contienen nuestras claves, pero nunca salen de la tarjeta. El chip se limita a cifrar con ellas algún desafío que lanza el dispositivo por donde introducimos la tarjeta.

E- **Elevación de privilegios**: Ya estamos autenticados en el sistema operativo y podemos trabajar con él, pero siempre limitados a los privilegios asociados al usuario con el que nos hemos presentado.

En las empresas, la mayoría de los empleados utilizan usuarios que no tienen permisos para realizar tareas de administración de la máquina (usuarios limitados, no administradores); así se reduce el daño que puedan causar, ya sea por error o porque se ha colado un virus.

Hay determinadas situaciones, para las que sí necesitamos ser administradores. Una solución es salir del usuario actual y entrar como administrador, pero es más sencillo solicitar, de manera puntual, **una elevación de privilegios. Consiste en pedirle al sistema ejecutar un determinado programa con permisos de administrador.** Se aplica solo a ese programa y solo a esa ejecución.: no afecta a las aplicaciones abiertas antes o después, ni siquiera cuando abramos ese mismo programa más adelante.

Practica elevación de privilegios en w7 y en Ubuntu

F- **Listas de control de acceso** (ACL): Mejoran la seguridad de los archivos de nuestro sistema y definen los privilegios que tiene el usuario de forma individual, permite limitar el acceso a los ficheros. Son tablas que le dicen al sistema operativo qué o quién tiene permiso para acceder y son exclusivas de las particiones del formato NTFS. Para acceder a las tablas se utiliza el comando **cacls**. Cualquier objeto y sobre un sistema NTFS tiene asociado unos parámetros de seguridad que se llaman descriptores de seguridad, éstos descriptores tienen la siguiente información:

   a. Quién es el propietario del objeto.
   b. A qué grupo de usuarios pertenece.
   c. Quién tiene acceso al objeto.
   d. Y qué permisos de acceso tiene.

   Los descriptores de seguridad no están guardados en ninguna carpeta, sino que están en forma de metadatos.

Cuotas

Hasta ahora hemos protegido nuestros sistemas evitando el acceso de personas no autorizadas; ahora vamos a proteger las personas que sí están autorizadas. Nuestros usuarios con intención o no, también pueden dañar el sistema. Por ejemplos se pueden descargar muchos archivos pesados, de manera que llenan el disco duro, y el sistema empieza a fallar, también se pueden lanzar ficheros muy pesados que ralenticen la CPU y no permiten trabajar a los demás usuarios.

Para evitarlos los sistemas se configuran para aplicar cuotas. Para el disco, se establece que cada usuario puede ocupar un número determinado de bytes (megabytes, gb). Cuando excede ese límite, podemos configurar de modo que el sistema no le permite extenderse más.

Hay que asignar las cuotas con cuidado.

- Si son **muy bajas**, tendremos a los usuarios quejándose todos los días porque no les dejamos trabajar. Hay que tener en cuenta que usuarios se crean y que se necesita para arrancar una aplicación.
- Si son **muy altas**, no tendrá el efecto disuasorio que se espera y al final se termina comparando más disco.

Actualizaciones y parches

El cd/DVd que se ha utilizado para instalar Windows, contiene una versión concreta liberada en una fecha concreta; desde entonces, los programadores de Microsoft han seguido trabajando. El resultado son las **actualizaciones: paquetes de software donde se introducen mejoras y, corrigen defectos.**

Como administradores responsables del sistema, debemos instalar esas actualizaciones, que podemos descargar automáticamente desde Internet.

Microsoft libera actualizaciones de forma rutinaria, y Service Pack, cada dos semanas.

Las actualizaciones se configuran desde **el panel de control**.

Podemos elegir:

- No buscar actualizaciones ni instalarla(no recomendado)
- Comprobar si hay actualizaciones, pero no descargarlas e instalarlas. Esto solo tiene sentido en equipos con poco disco o acceso limitado.
- Descargar actualizaciones, pero no instalarlas. En algunos sistemas podemos tener una configuración muy sensible a cambios en el sistema operativo.
- Descargar e instalar siempre. Es lo más habitual en puestos de usuarios.
- Este comportamiento no es único en Microsoft, todos los fabricantes de aplicsciones necesitan actualizar su software.

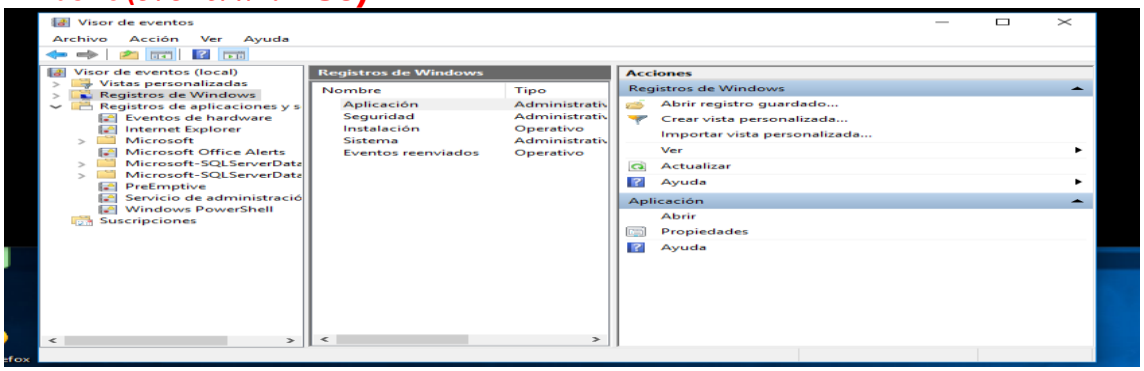
Los parches son parecidos a las actualizaciones, pero se utilizan solo para corregir defectos, y hay que descargarlos e instalarlos.

Vulnerabilidades de los sistemas

Para evitar las vulnerabilidades se deben mantener actualizados los sistemas operativos utilizando las herramientas propias de cada uno, utilizando **Windows update**, o bien buscando actualizaciones desde las páginas oficiales de los propios sistemas.

Monitorización del sistema

Windows (*eventvwr*.msc)



elementos:

1. Número de eventos de aplicación.

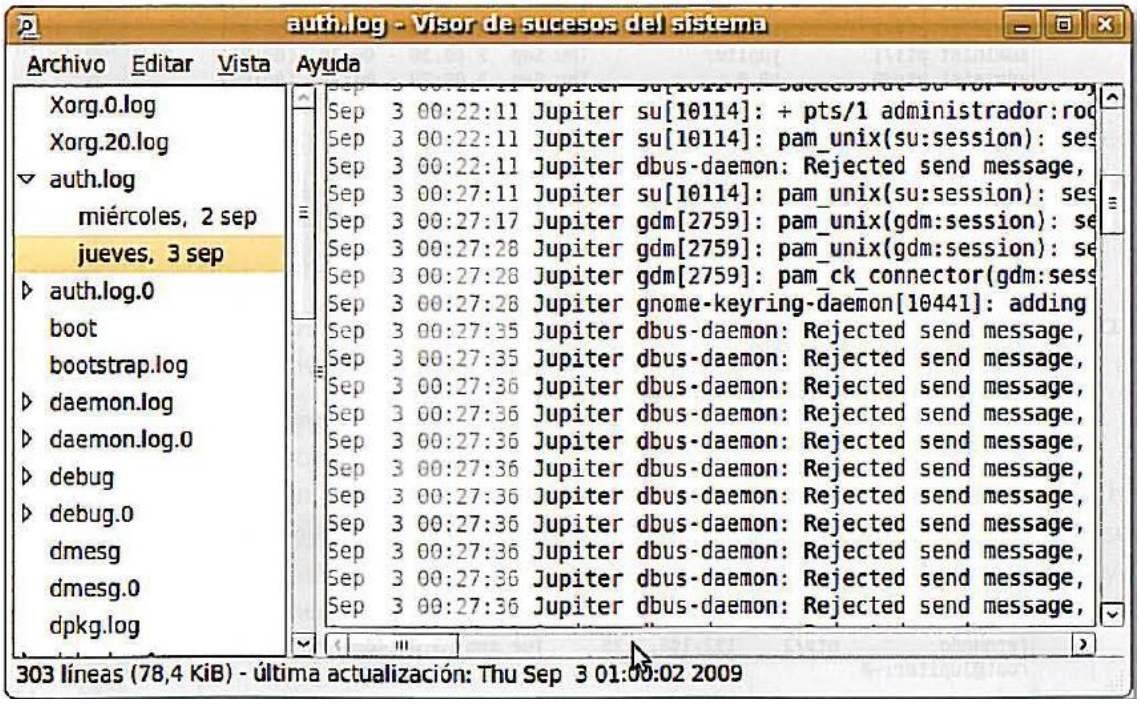
2. Número de eventos de seguridad.

3. Número de eventos de instalación.

4. Número de eventos del sistema.

Guardar una copia del listado de eventos. 1.3. Identificar tres tipos de eventos (Información, Error, Advertencia). Analizar los detalles de cada uno ellos: Origen, Fecha, Equipo….

Linux (*Siste*ma> *Administración> Visor de archivos de* sucesos.)



Comandos:

Last: Con este comando podemos ver los últimos usuarios que se han logueado en el sistema y que terminales usaron, así como también los últimos reinicios del sistema. Sirve para auditar las entradas al sistema.

Lastb: Nos muestra una información que puede ser tan útil como la anterior, los intentos fallidos de login en el sistema, su uso es similar al anterior, la diferencia reside en que se "fija" en el archivo /var/log/btmp.

Lastlog: Muestra información de los logins recientes de todos los usuarios. No es un fichero ascii. Debemos utilizar el comando lastlog para ver el contenido de este log. Conexiones a la red.

Software que vulnera la seguridad del sistema

Antivirus

Los virus informáticos son de muchos tipos, en cualquier caso estamos hablando **de malware** (software maligno):

- virus: Son programas que se propagan entre equipos y normalmente el código se suele adjuntar a otro archivo.
- Gusanos: Se propagan por la red.
- Troyanos: Son aplicaciones que en la mayoría de los casos acceden de forma remota.
  Para evitar estos ataques se desarrollan los antivirus, cuyo objetivo es mantener actualizados sus ficheros de firmas.

Monitorización

Hemos visto que cualquiera de las medidas aplicadas es imperfecta. Nuestra labor es instalarlas, formar a los usuarios y, todos los días vigilar que todo esté normal. Esta vigilancia consiste en:

- **Revisar los log.** Del sistema y las aplicaciones. Cualquier suceso anómalo quedará anotado en alguna parte. Para cada aplicación hay que saber donde lo hace.
- **Si el sistema lo permite, activar la copia sincronizada del log** en otra máquina, es decir cada aviso se escribe a la vez en nuestra máquina y en la otra. De esta forma podremos analizar un desastre, evitando que el hacker borre sus huellas.
- **Revisar la ocupación del sistema,** principalmente el disco y la CPU
  Suscribirse a las newletters de los fabricantes de nuestro hardware y software, para tener a mano la información oficial: actualizaciones, parches….
- **Participar en foros de usuarios** de las mismas aplicaciones, para estar al día de los problemas que aparecen.

La monitorización de los log consiste primero en diferenciar que es un problema y que no lo es. El texto del log ayuda porque suele tener un indicador de gravedad (critica, alto, medio , bajo o simple aviso) .

Para conocer la ocupación de recursos de una máquina podemos entrar en ella y lanzar herramientas locales(gadget de rendimiento) o el comando **top** en Linux

Conviene instalar una **herramienta de inventario y monitorización. El inventario es la lista de equipos y conexiones y la configuración de ambos; la monitorización es la supervisión del estado de los elementos del inventario.. Estas herramientas facilitan el trabajo de administración porque:**

- Rastrean la red
- Pueden identificar distintos equipos
- Obtienen la configuración para todos los equipos y la registran en una base de datos para generar informes.
- Incorporan alertas sobre ocupación de disco.

Aplicaciones web

Están ampliamente extendidas en Internet (Google Apps, ZoHo, Twitter, WordPress YouTube, etc.), y también dentro de las empresas, las intranets. Pero debemos tener cuidado con:

- **La máquina que aloja el servidor web y sus aplicaciones accesorias (base de datos y otras).** Si un hacker toma esta máquina, tiene acceso a toda la información y todas las conexiones de los usuarios. Hay que aplicar las medidas de protección que hemos estudiado en este tema.
- **Si la máquina del servidor web** no es nuestra, sino **alquilada** (hosting web), no tenemos control sobre las medidas de protección. Debemos confiar en la profesionalidad del proveedor y repasar el contrato, en especial el apartado de los niveles de servicio (SLA [Service Level Agreement]). Por ejemplo, podemos exigir al

proveedor que si el servidor web está caído más de dos horas al año, nos haga un descuento del 25 % en la siguiente cuota.

- **La transmisión entre el cliente web (navegador) y el servidor web.** Muchas aplicaciones todavía utilizan el protocolo HTTP, donde todo viaja en texto en claro. En algún tramo de red puede estar escuchando un hacker y conocer qué hacemos, incluso modificarlo para su provecho. Debemos optar por HTTPS.
- **La máquina de un usuario conectado puede haber sido hackeada y su navegador también.** Por ejemplo, se ha instalado un keylogger que envía todas las contraseñas fuera de nuestro control. En este punto es importante el antivirus.

Buscar información sobre las aplicaciones en internet **: cloud computing y cloud storage**

LaaS➔Infrastructure as a service . Primera solución al cloud computing (parecida a las máquinas virtuales
SaaS➔Software as a Service. Aplicaciones completas donde el mismo proveedor se encarga del desarrollo de la aplicación del mantenimiento y tb pone las máquinas y la conectividad.