Unidad 5

Seguridad activa en el sistema

En esta unidad aprenderemos a:

- Instalar, probar y actualizar aplicaciones específicas para la detección y eliminación de software malicioso.
- Clasificar y detectar las principales incidencias y amenazas lógicas de un subsistema lógico.
- Aplicar técnicas de monitorización de accesos y actividad identificando situaciones anómalas.
- Valorar las ventajas que supone la utilización de sistemas biométricos.

Y estudiaremos:

- La seguridad en el arranque y en particiones.
- Las actualizaciones y parches de seguridad en el sistema y en las aplicaciones.
- La autenticación de usuarios.
- Listas de control de acceso.
- La monitorización del sistema.
- El software que vulnera la seguridad del sistema.

1. Introducción a la seguridad del sistema

El título del tema hace referencia a un concepto que vimos en la primera unidad, la seguridad activa, definido como el conjunto de medidas que previenen o intentan evitar los daños en el sistema informático.

Se trata de estudiar qué mecanismos de protección podemos utilizar en nuestro equipo informático para evitar accesos indeseados de intrusos (personas o programas informáticos).

Aprenderemos a mejorar la seguridad en el acceso al ordenador mediante el uso de contraseñas en la BIOS y en el gestor de arranque. También aprenderemos a impedir la carga de un sistema operativo desde dispositivos extraíbles, memoria externa USB, CD/DVD…, a configurar las contraseñas en las cuentas, a mejorar la seguridad ante los ataques definiendo políticas de contraseñas y mecanismos de autenticación, y por último, auditaremos todas las acciones anteriores.

2. Seguridad en el acceso al ordenador

Para evitar cualquier acceso indeseado a nuestro equipo debemos asegurar el arranque del mismo mediante el uso de contraseñas.

Si analizamos el proceso de encendido del ordenador, recordaremos la importancia que tiene la BIOS en el mismo; es la encargada de localizar y cargar el sistema operativo o gestor de arranque.

2.1. ¿Cómo evitamos que personas ajenas modifiquen la BIOS?

El uso de contraseñas para acceder a la BIOS evitará que personal no autorizado realice modificaciones indeseadas en la configuración de la misma, así como cambios en la secuencia de arranque, lo que permitiría la puesta en marcha del equipo desde medios extraíbles y el acceso a los datos almacenados en el mismo, vulnerando la confidencialidad de estos.

Claves y consejos

Debido a los numerosos fabricantes de BIOS que hay en el mercado, recomendamos consultar el manual de la placa base para ver las instrucciones específicas.

Importante

Para entrar en la BIOS debemos pulsar la tecla **Sup** o **F2** al iniciar el ordenador, aunque esto realmente depende de la BIOS del equipo. En el libro se ha hecho uso de la BIOS de VMWare.

Caso práctico 1

Definimos la clave de supervisor para proteger el acceso a la BIOS

Con esta práctica vamos a proteger el acceso a la BIOS contra personas no autorizadas y así dificultar el acceso al equipo a dicho personal.

Fig. 5.1. *Menú principal BIOS.*

1. Al entrar a la BIOS accedemos a la pantalla principal (Fig. 5.1). Nos desplazamos por el menú hasta la opción *Security* que se muestra en la parte superior de la imagen (Fig. 5.2).

(Continúa)

Caso práctico 1

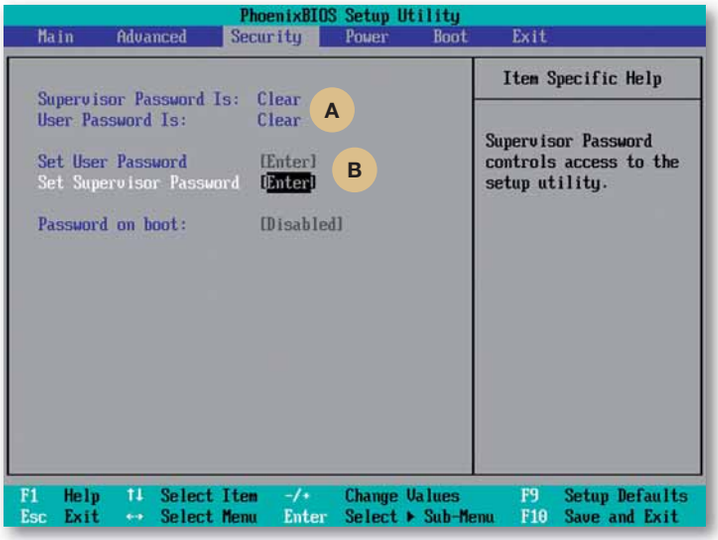


Fig. 5.2. *Menú Seguridad.*

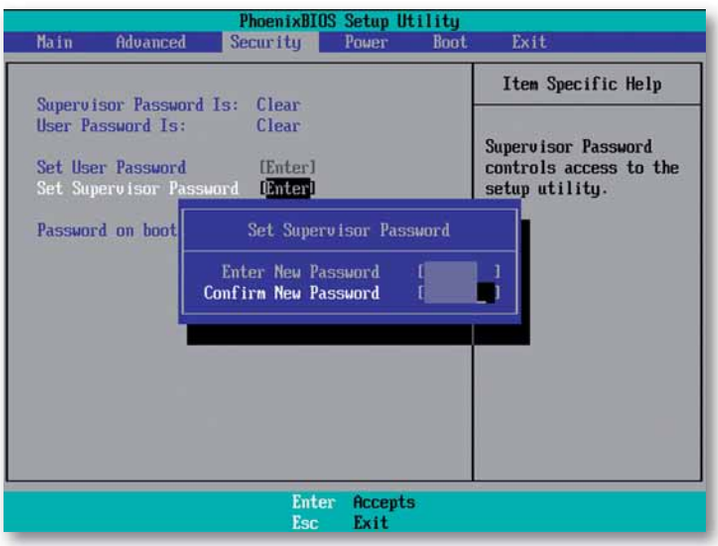


Fig. 5.3. *Introducción de contraseña.*

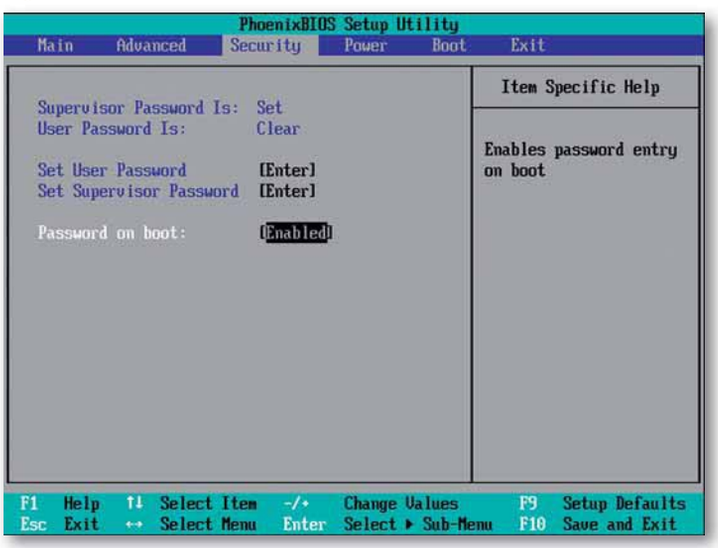


Fig. 5.4. *Contraseña Supervisor en arranque de la BIOS.*

(Continuación)

La Figura 5.2 muestra las opciones de seguridad que podemos configurar y el estado de las mismas.

A Como podemos ver en dicha figura, la contraseña de Supervisor está vacía *(Clear);* con esta opción permitimos la modificación de la BIOS a cualquier persona. Así, un intruso podría acceder a la BIOS y modificar la secuencia de arranque del equipo (Primero desde CD, segundo desde LAN, tercero desde HD).

El intruso podría reiniciar el ordenador con un CD provisto de software malintencionado que le permitiría descubrir a los usuarios y las contraseñas del equipo. Con la información conseguida, tendría acceso a los datos confidenciales de todos los usuarios del sistema.

B Con el fin de evitar los posibles intentos de modificación de la BIOS, definimos una nueva contraseña para el Supervisor.

2. Pulsamos **Enter** en la opción *Set Supervisor Password* (Definir clave del Supervisor).

3. Se abre un nuevo cuadro de diálogo (Fig. 5.3) en el que escribimos la contraseña para el Supervisor y posteriormente la verificamos escribiéndola nuevamente en el campo de confirmación.

   A continuación nos avisará de que los cambios se han realizado con éxito.

   Como vemos en la Figura 5.4 la contraseña de Supervisor figura como asignada *(Set).*

   A partir de este momento siempre que queramos acceder a la BIOS nos exigirá que escribamos la contraseña de Supervisor, en caso contrario denegará el acceso.

4. Otra medida de seguridad adicional que podemos configurar en la BIOS: evitar que personal no autorizado acceda al sistema introduciendo la clave de Supervisor en el momento de arrancar el equipo. Para ello activaremos la opción de *Password on boot* (contraseña en el arranque). Es decir, la contraseña que definimos en la BIOS será solicitada al usuario tanto en el acceso a la BIOS como en el acceso al sistema operativo o gestor de arranque.

   En resumen, con estas medidas hemos evitado que personas no autorizadas puedan modificar la configuración de la BIOS permitiendo, por ejemplo, el arranque del sistema mediante dispositivos extraíbles, y acceder así a los datos almacenados en el equipo vulnerando la confidencialidad de estos.

Claves y consejos

Si se te olvida la contraseña de la BIOS, tendrás que abrir el PC y quitar durante un rato la pila de la placa base. Después volvemos a instalarla y ya tenemos reseteada la BIOS con la configuración del fabricante.

Actividades

1. Un técnico de seguridad informática inexperto tiene protegido el acceso a la BIOS mediante la contraseña de Supervisor. Cuando otros usuarios pretenden entrar en la BIOS de los ordenadores les solicita la clave del Supervisor. Este no quiere comunicar esta contraseña a los usuarios de los equipos e idea una solución para solventar el problema: definir la contraseña de usuario en la BIOS. Indica los pasos que debe realizar.
2. Desactiva la opción de la BIOS, en caso de tenerla activada, que sirve para encender el equipo de forma remota a través de la red.

Vocabulario

El gestor de arranque **GRUB** *(Grand Unifier Bootloader)* permite seleccionar entre los distintos sistemas operativos que tengamos instalados en el equipo. Este gestor es el que habitualmente instalan por defecto las nuevas distribuciones de sistemas GNU/Linux.

2.2. ¿Cómo proteger el GRUB con contraseña?

Para evitar que personas no autorizadas tengan acceso a la edición de las opciones de arranque de los distintos sistemas operativos que controla el GRUB, estableceremos una contraseña.

Caso práctico 2

Definición de contraseñas en el GRUB en modo texto

Durante este proceso, vamos a modificar el fichero que almacena la configuración del gestor de arranque (GRUB), por lo que es recomendable realizar una copia de seguridad del mismo, para poder restaurarla en caso de que se produjese algún error en el arranque como consecuencia de las modificaciones realizadas.

1. Para ello, abrimos un nuevo terminal y tecleamos las instrucciones que aparecen en la Figura 5.5. Estas instrucciones realizan una copia de seguridad del fichero `menu.lst` y la edición del mismo.

Fig. 5.5. *Instrucción para editar* `menu.lst`.

2. Buscamos la línea `#password topsecret`.
3. Borramos la almohadilla, es decir le quitamos el comentario y cambiamos la contraseña topsecret por la que nosotros queramos; en nuestro ejemplo hemos elegido «patata» (Fig. 5.6). Se guardan los cambios en el fichero `menu.lst` y se reinicia la máquina para probar la modificación realizada.

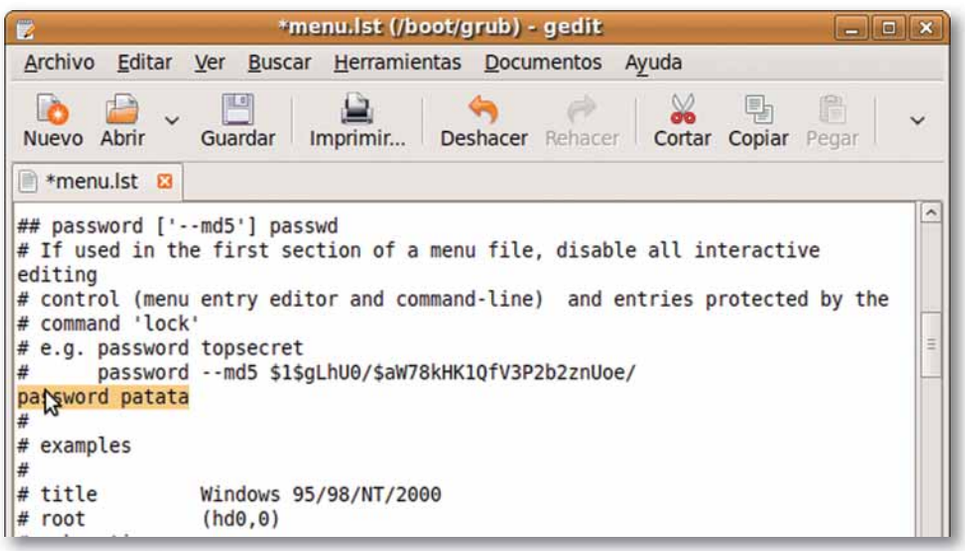


Fig. 5.6. *Modificación del parámetro password en el archivo* `menu.lst`.

Para finalizar reiniciamos el equipo y comprobamos, simulando ser un usuario que no conoce la contraseña, que no podremos modificar las opciones de arranque que nos muestra el gestor de arranque.

Caso práctico 3

Definición de contraseñas cifradas en el GRUB en modo texto

1. Debemos abrir un nuevo terminal y escribir `grub`.
2. A continuación, como podemos ver en la Figura 5.7, escribimos el subcomando `md5crypt` que nos permitirá encriptar la contraseña que queramos poner.
3. Escribimos la clave a codificar y el programa nos muestra el password codificado.
4. Por último, para salir del grub debemos escribir `quit` (salir).

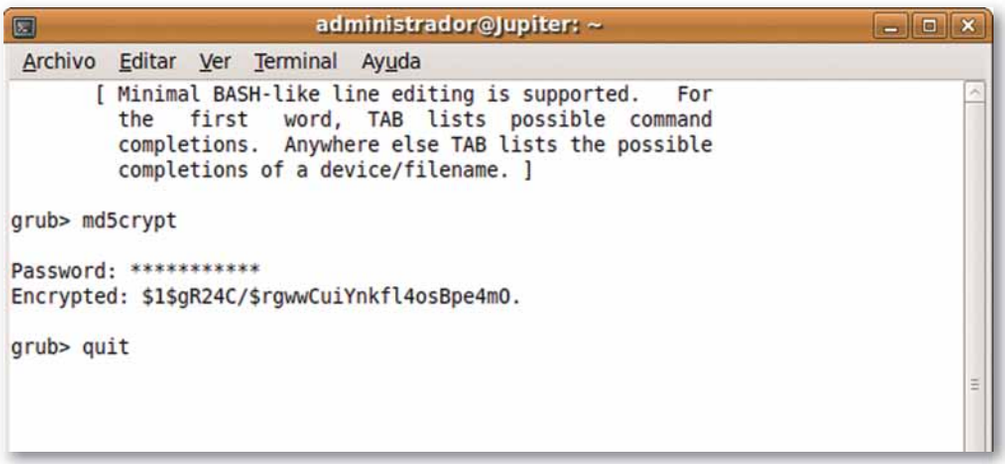


Fig. 5.7. *Encriptación de la contraseña.*

5. Una vez encriptada la contraseña, deberemos copiarla en el fichero `menu.lst`, como podemos ver en la Figura 5.8. Fíjate que la línea no es similar a la de la práctica anterior, ya que se ha añadido la opción `--md5`, que indica que la contraseña está encriptada.

Fig. 5.8. *Contraseña de acceso a GRUB cifrada.*

Claves y consejos

Las contraseñas para acceder a los sistemas operativos gestionados por el gestor de arranque deben cifrarse. Si nos descubren la clave que permite acceder a la edición del GRUB verían la contraseña y por tanto accederían al sistema. Si por el contrario la clave se encuentra cifrada verían una cadena de caracteres sin sentido.

¿Sabías que...?

Podemos abrir un nuevo terminal de diversas maneras: pulsando **ALT** + **F2,** que nos abrirá una ventana en la que debemos escribir `gnome-terminal` (Fig. 5.9) o bien haciendo clic sobre *Aplicaciones, Accesorios y Terminal.*

Fig. 5.9. *Arranque Terminal.*

Caso práctico 4

Establecer contraseñas al arranque de los sistemas operativos controlados por el GRUB

Con esta práctica evitaremos el acceso a los sistemas operativos gestionados por el GRUB a personal no autorizado.

1. Editamos el fichero de configuración del GRUB, `menu.lst` y al final del mismo buscamos las líneas donde se define el título del sistema operativo (title) y a continuación escribiremos `password --md5` y la contraseña.

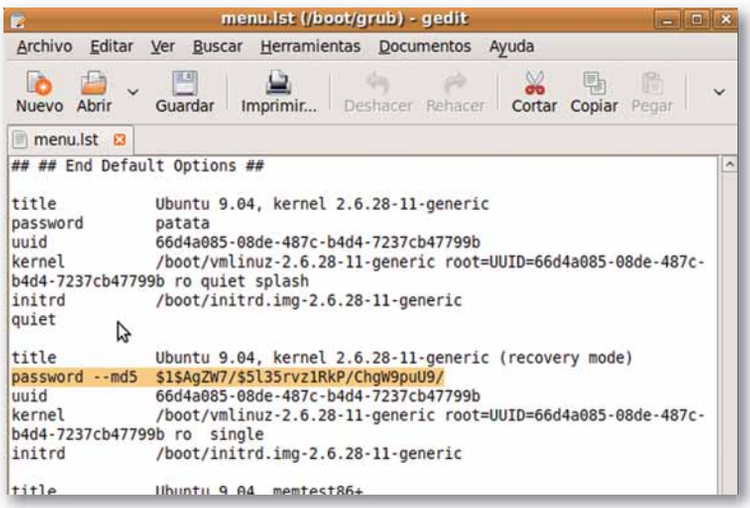


Fig. 5.10. *Contraseña de acceso al sistema Ubuntu cifrada.*

Caso práctico 5

Establecer contraseña del gestor de arranque mediante la aplicación startupmanager en LINUX, distribución Ubuntu 9.04, para evitar el acceso a los sistemas operativos gestionados por el GRUB a personal no autorizado utilizando una aplicación visual

Fig. 5.11. *Gestor Synaptic.*

1. En primer lugar debemos instalar la aplicación en Ubuntu mediante el gestor de paquetes Synaptic, como podemos ver en las Figuras 5.11 y 5.12.

Fig. 5.12. *Instalación startupmanager.*

(Continúa)

Caso práctico 5

(Continuación)

2. Una vez instalado, ejecutamos el programa accediendo a *Sistema* > *Administración* > *Administrador de Arranque* (Fig. 5.13).

3. Hacemos clic sobre la pestaña de seguridad, activamos la opción de *Proteger con contraseña el cargador de arranque* y escribimos la clave elegida como podemos ver en la Figura 5.14. Para finalizar reiniciamos la máquina y comprobamos cómo afecta el cambio a la configuración del arranque.

Fig. 5.13. *Administrador de Arranque.*

Fig. 5.14. *Configurando contraseña en startupmanager.*

Actividades

3. Haz el Caso práctico 5 ejecutando el programa directamente en el terminal.

Recuerda que deberás tener privilegios de administrador para poder realizarlo.

4. Comprueba si el programa startupmanager escribe las contraseñas en el archivo `menu.lst` del GRUB cifradas o en texto claro.

2.3. Cifrado de particiones

En este apartado vamos a estudiar cómo proteger la confidencialidad de los datos almacenados en los distintos volúmenes del equipo mediante el cifrado de particiones.

Cualquier software de encriptación de disco protege la información contra el acceso de personas no autorizadas.

Caso práctico 6

Cifrar una partición en Windows

Con esta práctica conseguiremos proteger una partición de Windows, la información no será accesible para aquellas personas que no conozcan la clave.

Para realizar esta actividad vamos a utilizar un programa de código abierto, gratuito, DiskCryptor **(http://www.diskcryptor.de/en/downloads/).**

Para instalar esta aplicación sólo necesitamos 10 MB de espacio en disco duro y Microsoft Windows.

1. Nos descargamos DiskCryptor 0.7, lo descomprimimos y hacemos doble clic sobre el archivo dcrypt que se encuentra en la carpeta i386 (Fig. 5.15); a continuación respondemos afirmativamente a la pregunta sobre la instalación del controlador DiskCryptor.

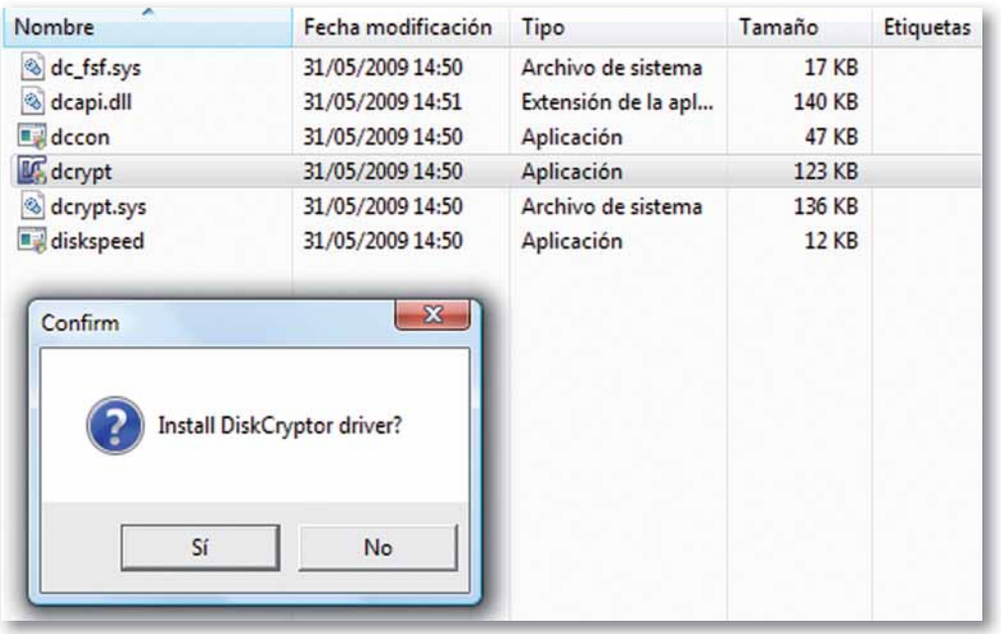


Fig. 5.15. *Instalación del controlador DiskCryptor.*

2. Una vez instalado ejecutamos la aplicación dcrypt.

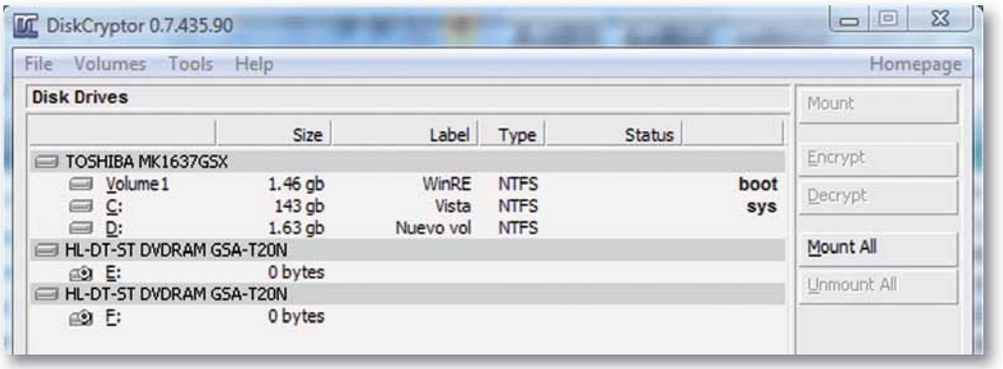


Fig. 5.16. *Programa DiskCryptor.*

(Continúa)

Caso práctico 6

(Continuación)

Como hemos visto en la Figura 5.16 la aplicación visualiza las unidades de disco que puedes encriptar. En nuestro caso, lo que queremos encriptar es la D:, unidad dedicada a datos.

3. La seleccionamos y hacemos clic sobre el botón Encrypt (cifrar). Posteriormente deberemos seleccionar entre los distintos algoritmos de encriptación (AES, Twofish, Serpent, AES-Twofish, Serpent-AES, AES-Twofish-Serpent…) y hacer clic en el botón *Next* (siguiente).

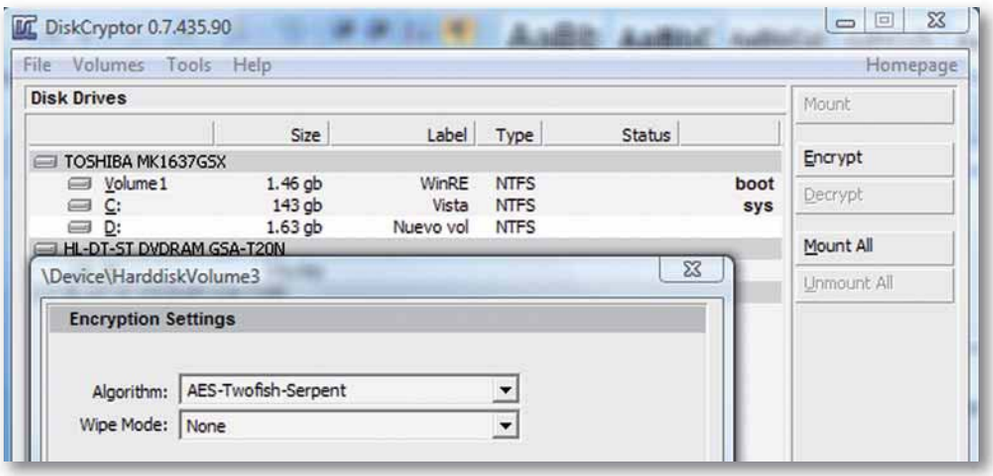


Fig. 5.17. *Selección del algoritmo de encriptación.*

4. En la siguiente pantalla, deberemos escribir la contraseña de encriptación. Además, en este paso la aplicación nos informa de la vulnerabilidad de nuestra contraseña según un gráfico. La contraseña que hemos escrito es $1Nab74c$b!@12 y es considerada de dificultad Media. Pulsamos *OK* y después de unos minutos tendremos cifrada la unidad y fuera del alcance de personas que no conozcan la clave de cifrado.

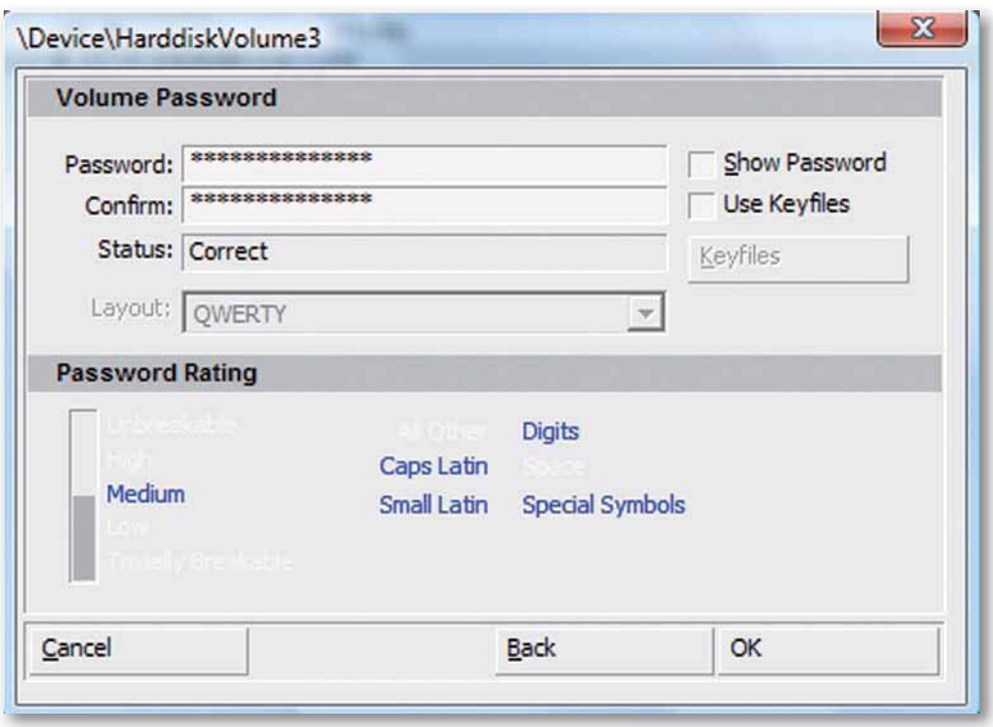


Fig. 5.18. *Configuración de la contraseña.*

Caso práctico 7

Cifrar una partición en Linux

Vamos a aprender a encriptar una unidad USB en Linux con el programa TrueCrypt, aplicación gratuita que nos podemos descargar de la página **http://www.truecrypt.org.**

Con ello conseguimos que aquellas personas que no conozcan la clave no puedan acceder a la información almacenada en la unidad USB.

1. Para instalar TrueCrypt, debemos descargarnos la versión para la distribución de GNU/Linux del programa (en nuestro caso Ubuntu) de dicha página, descomprimirlo y ejecutar el programa de instalación.
2. Tras instalarlo, ejecutamos la aplicación y veremos una ventana similar a la Figura 5.19.

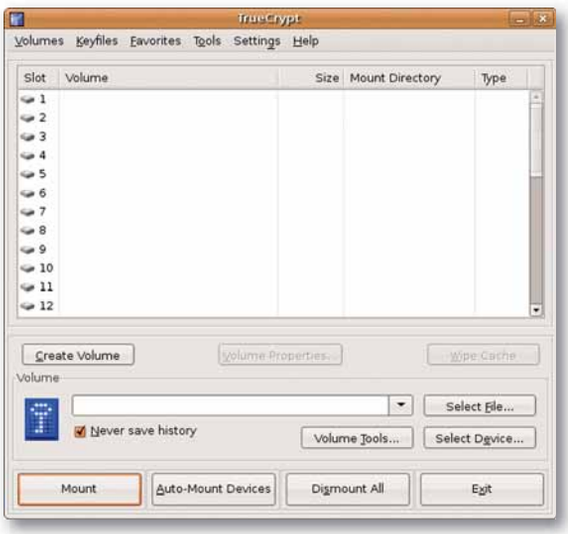


Fig. 5.19. *Ventana principal TrueCrypt.*

En la Figura 5.19 vemos una lista de todas las unidades de TrueCrypt. Como acabamos de instalarlo, no tiene ninguna de ellas asignada.

3. Para cifrar la unidad de USB, debemos hacer clic en el botón *Create Volume* (crear unidad). A continuación, se abrirá una ventana, en la que se muestran dos opciones:
   - *Create an encrypted file container* (crear una carpeta cifrada).
   - *Create a volumen within a partition/drive* (crear una unidad para una partición o dispositivo).

   La primera de ellas es la que el programa recomienda para el personal inexperto. En este caso no es necesario formatear la unidad, solo crea una carpeta donde su contenido será cifrado.
4. La segunda opción será la que seleccionaremos para alcanzar nuestro objetivo. La aplicación nos advierte que al realizar esta elección se formateará la unidad y cifrará la partición. A continuación, deberemos ver una nueva pantalla similar a la Figura 5.20.

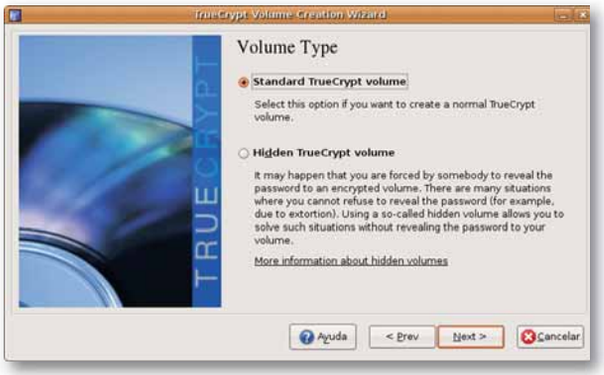


Fig. 5.20. *Selección de tipo de unidad.*

(Continúa)

Caso práctico 7

(Continuación)

5. Seleccionamos la primera opción *Standard TrueCrypt volumen* (crear una unidad TrueCryprt normal) y hacemos clic sobre el botón *Next.*

6. En la siguiente pantalla (Fig. 5.21), debemos seleccionar la unidad a formatear. Hacemos clic en el botón *Select Device* (seleccionar dispositivo).

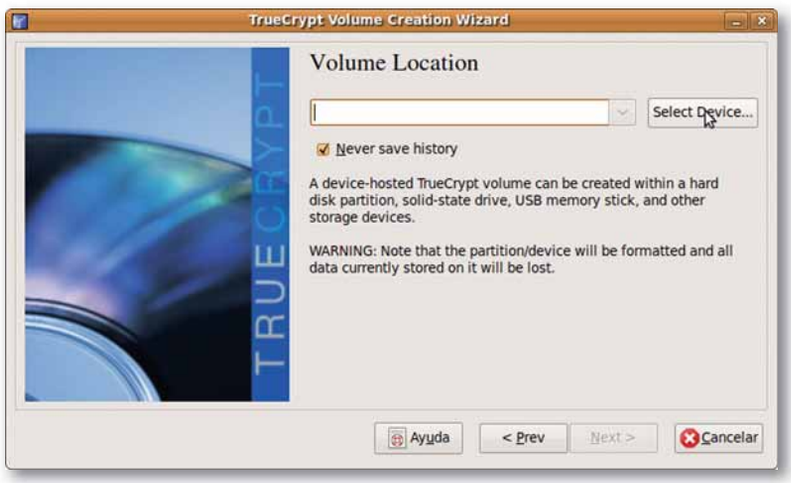


Fig. 5.21. *Selección de dispositivo.*

7. Aparece una pantalla (Fig. 5.22) con todos los dispositivos de almacenamiento que tenemos conectados al ordenador. Seleccionamos el dispositivo USB reconocido en nuestro caso como /dev/sdb1 de 483 MB. Dependiendo de la distribución de Linux y de los distintos dispositivos conectados en el equipo puede ser reconocida con otro nombre.

8. Posteriormente, como podemos ver en la imagen (Fig. 5.23), debemos seleccionar el algoritmo de encriptación. Las opciones son numerosas, AES, Blowfish, Serpent, Twofish, AES-Twofish-Serpent… En nuestro ejemplo hemos seleccionado el algoritmo AES-Twofish-Serpent y RIPEMD-160 para generar la clave. A continuación hacemos clic sobre el botón *Next.*

Fig. 5.22. *Selección de partición.*

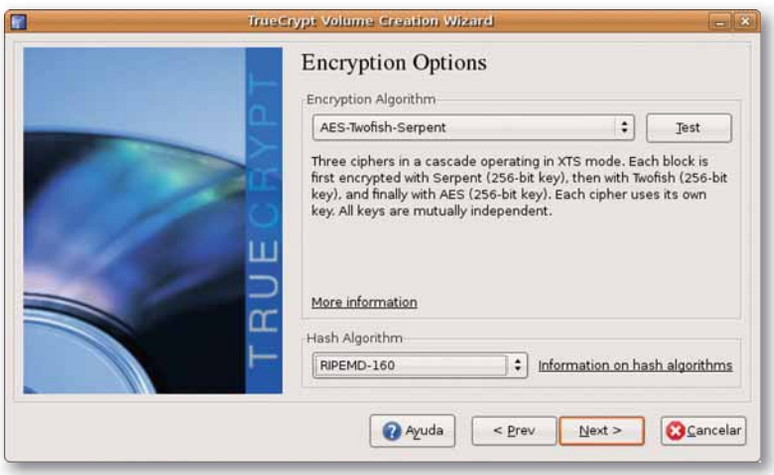


Fig. 5.23. *Elección del algoritmo de cifrado.*

9. Aparece una nueva pantalla (Fig. 5.24) en la que introduciremos la contraseña. En este punto, la aplicación nos advierte de la importancia de elegir una buena contraseña; que no sean palabras que podamos encontrar en diccionarios o combinaciones de varias. La clave no debe tener información personal como nombre o fecha de nacimiento. Una buena contraseña debe ser una combinación de letras mayúsculas, minúsculas, números y caracteres especiales, $,+,-@,… Recomienda que el tamaño de la misma sea de más de 20 caracteres.

Cuanto mayor sea el número, menos vulnerable será la contraseña.

TrueCrypt admite contraseñas de hasta 64 caracteres.

(Continúa)

Caso práctico 7

(Continuación)

10. Si activamos la opción *Display password* (visualizar clave), podemos ver los caracteres de la contraseña. Escribimos la clave y hacemos clic en el botón *Next.*

Fig. 5.24. *Definición de contraseña.*

11. A continuación, debemos elegir el tipo de sistema de ficheros que utilizaremos en nuestro USB. Debemos tener en cuenta dónde vamos a utilizar el dispositivo; si solo lo fuésemos a utilizar en Linux, lo formatearíamos en EXT3, pero si además quisiésemos utilizarlo en Windows, deberíamos formatearlo en FAT.

Como nosotros lo vamos a utilizar indistintamente en Linux y en Windows, lo formateamos con el sistema de archivos FAT.

Antes de formatear la aplicación nos recomiendan que hagamos movimientos con el ratón. Estos calcularán los valores aleatorios que se utilizarán para crear la clave de cifrado. Si estás seguro de que no tienes ningún dato importante que pudieses perder en el USB puedes seguir con el proceso dando formato al dispositivo.

El proceso ha finalizado, la unidad ya está preparada para que todos los datos que introduzcamos en ella sean cifrados automáticamente, es decir que trabaje de forma transparente para el usuario.

12. Antes de utilizar la unidad USB debemos montarla con la aplicación TrueCrypt, para ello debemos volver a la pantalla inicial de dicha aplicación (Fig 5.19) y hacer clic sobre *Select Device* (seleccionar dispositivo). Se abrirá una ventana similar a la de la Figura 5.22, donde elegiremos la unidad que hemos cifrado. A continuación la aplicación solicitará la contraseña. Una vez que introducimos la contraseña, la unidad se monta como `truecrypt1` (Fig. 5.25).

Fig. 5.25. *Unidad montada.*

2.4. Cuotas de disco

La mayoría de los sistemas operativos poseen mecanismos para impedir que ciertos usuarios hagan un uso indebido de la capacidad del disco, y así evitar la ralentización del equipo por saturación del sistema de ficheros y el perjuicio al resto de los usuarios al limitarles el espacio en el disco.

Las cuotas de disco se pueden configurar en función de varios criterios, según usuarios, grupos o por volúmenes.

Veamos esto último con ejemplos:

- Supongamos una familia de tres miembros, Macarena, Fernando y Gustavo. Podríamos establecer una cuota de disco para Gustavo de 2GB, para Macarena de 2GB y para Fernando que suele manejar planos que ocupan mucho espacio, le permitimos una cuota de 20 GB. Es decir, cada usuario puede tener una cuota distinta en función de sus necesidades; no tienen por qué tener todos la misma.
- Supongamos la empresa de construcción SiCom, en la que los usuarios se encuentran clasificados por grupos, Contabilidad, Arquitectos y Dirección. Repartiremos el sistema de ficheros entre los diversos grupos en función de las necesidades de los mismos. El grupo de Contabilidad suele trabajar con archivos Excel y Word, de pequeño tamaño, al igual que el grupo de dirección.

  Sin embargo, el grupo de Arquitectos necesitan mucho espacio, ya que suelen trabajar con herramientas CAD. En función de las necesidades anteriores y el número de usuarios adscritos a esos grupos se definen las cuotas, 20 GB para el grupo de contabilidad, 8 GB para el grupo de dirección y 1 TB para el grupo de arquitectos.
- Supongamos que en un PC hay dos particiones, una de las particiones podría tener cuotas de usuario muy restrictivas y en la otra partición tener otras cuotas menos limitadas o incluso ni siquiera tenerlas.

Vocabulario

Herramientas CAD. Son aplicaciones de Diseño Asistido por Ordenador.

Importante

Las cuotas de disco en Windows solo se pueden utilizar sobre volúmenes con sistemas de ficheros NTFS.

Claves y consejos

Cuidado con ser excesivamente restrictivo con la cuota.

Podríamos impedir incluso el inicio de sesión de un usuario, por no tener suficiente espacio para crear su carpeta en *Documents and Settings*.

Activación y uso de cuotas de disco en Windows

Para activar las cuotas de disco en una partición en Windows debemos seguir los siguientes pasos:

Debemos hacer clic en el botón derecho sobre la partición donde queremos establecer las cuotas y elegir la opción *Propiedades*.

Habilitamos la administración de la cuota seleccionando la casilla (Fig. 5.26).

Si solo queremos hacer un seguimiento del uso del sistema de ficheros por parte de los usuarios y grupos no seleccionaremos la siguiente opción que muestra la Figura 5.27, *Denegar espacio de disco a usuarios que excedan el límite de cuota*.

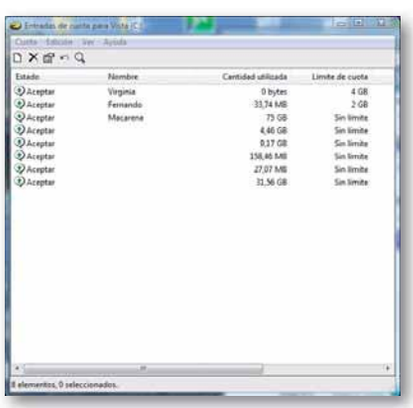


Fig. 5.26. *Cuotas.*

Claves y consejos

Para ejecutar el visor de sucesos podemos escribir *eventvwr.msc* en la consola o en el menú ejecutar de *Inicio*, o ir a *Panel de Control > Herramientas Administrativas > Visor de Sucesos*.

Actividades

5. Piensa de qué forma un administrador de un servidor de correo electrónico podría asignar 100 MB de espacio en disco a usuarios de pago y 5MB al resto de usuarios registrados.
6. Crea un usuario y asígnale una cuota de tan solo 1 MB. ¿Puedes arrancar una nueva sesión con este usuario? Justifica la respuesta.

Si por el contrario queremos limitar el espacio del sistema de ficheros a los usuarios, debemos definir la capacidad de disco de la que van a disponer cada uno de ellos, así como del nivel de advertencia y activar la opción de *Denegar espacio de disco a usuarios que excedan el límite de cuota*.

Fig. 5.27. *Limitación de espacios.*

Si se marcan las dos opciones que aparecen al final de la Figura 5.27, el sistema operativo registraría los eventos, haber superado el nivel de advertencia o haber superado el límite de cuota, en el visor de sucesos.

El usuario puede ver mediante el visor de sucesos dicha información (Figs. 5.28 y 5.29).

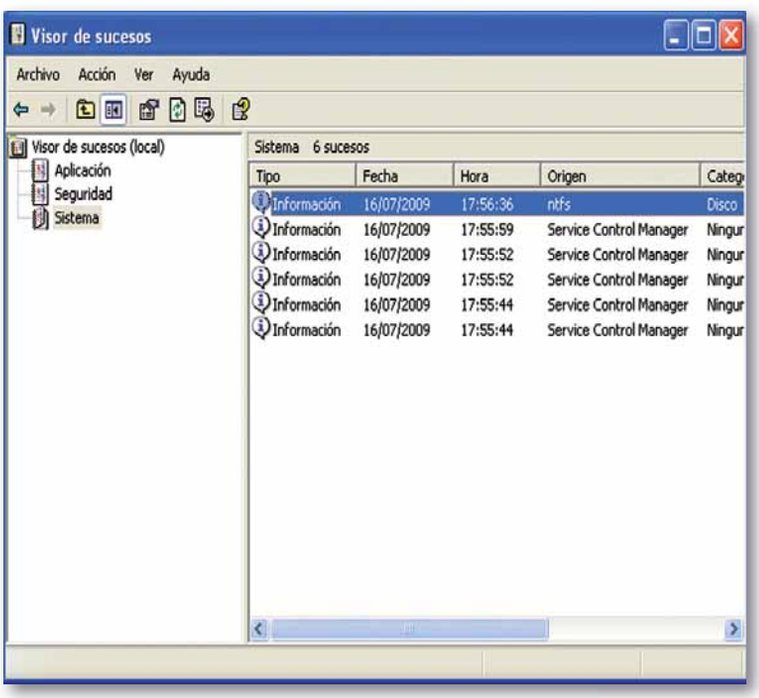


Fig. 5.28. *Visor de sucesos.*

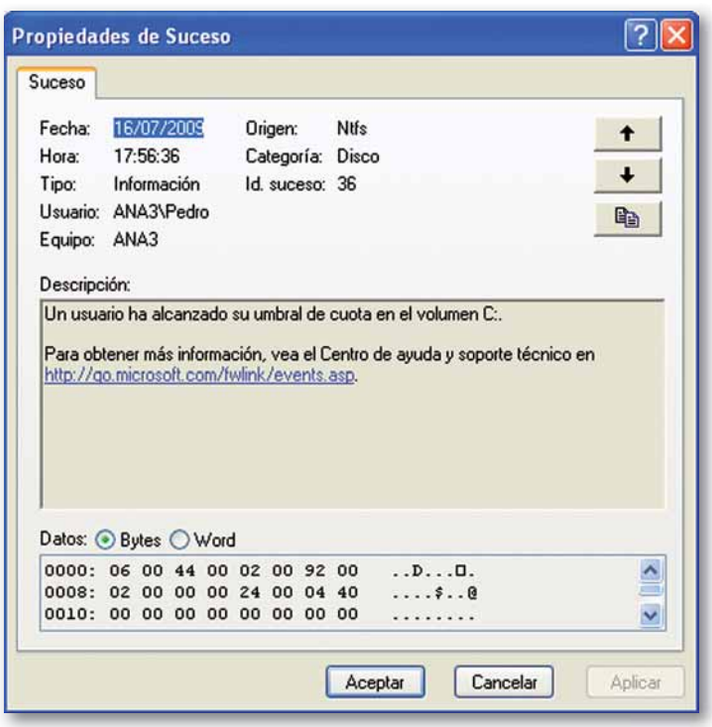


Fig. 5.29. *Propiedades de suceso.*

Cuotas de usuario en UBUNTU

Para gestionar las cuotas de discos en Linux vamos a utilizar la herramienta de configuración del sistema conocida como Webmin. Esta herramienta no viene instalada por defecto con el sistema operativo, así que tendremos que instalarla utilizando el gestor de paquetes Synaptic o utilizando el comando `apt-get`.

En este caso, vamos a realizarlo utilizando la orden `apt-get`. Debemos seguir los pasos que se detallan a continuación.

Para que el comando `apt-get` funcione e instale correctamente esta herramienta, debemos añadir el repositorio http://download.webmin.com/download/repository sarge contrib al final del fichero `sources.list` mediante la orden `gedit`, como vemos en la Figura 5.30.

Importante

En caso de no tener instalado el paquete quota (permite definir las cuotas de disco en Linux) usaremos la orden `apt-get install quota`.

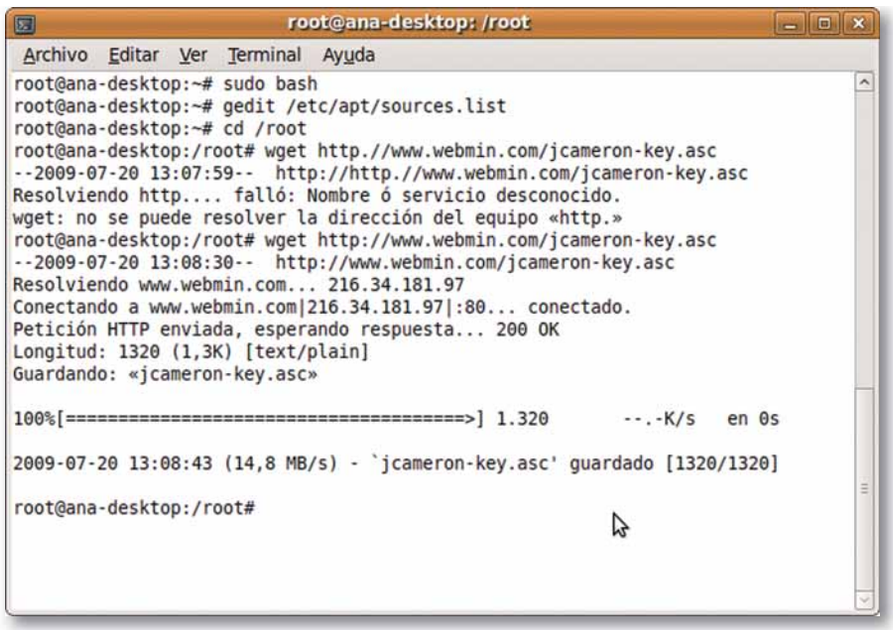


Fig. 5.30. *Comandos.*

A continuación, debemos ejecutar los siguientes tres comandos que aparecen en la Figura 5.30 para añadir la clave pública, pareja de la privada, con la que se ha firmado el repositorio.

Por último, actualizamos e instalamos la herramienta webmin, mediante la ejecución de los siguientes comandos (Figs. 5.31 y 5.32).

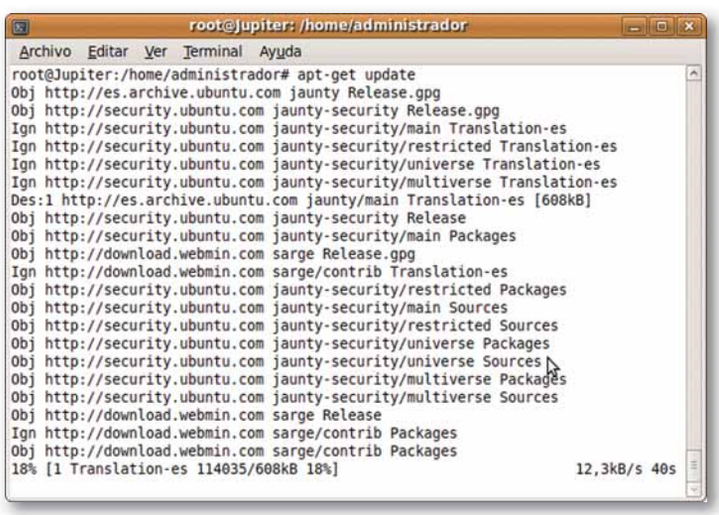


Fig. 5.31. *Orden* `apt-get update`.

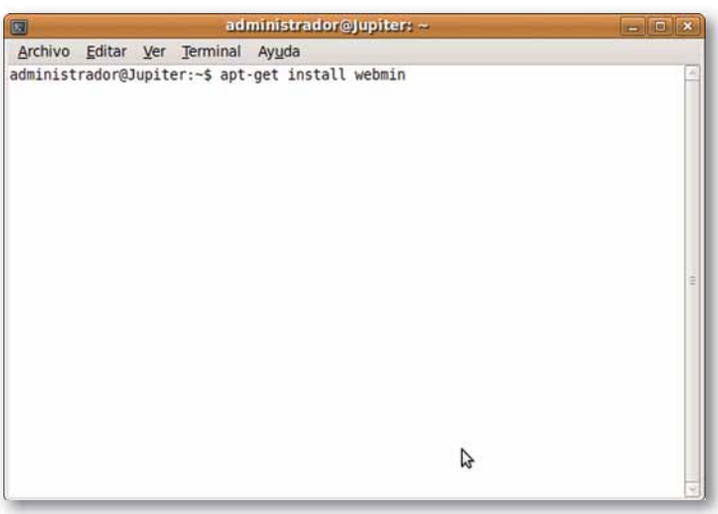


Fig. 5.32. *Instalación webmin.*

Para ejecutar la aplicación tendremos que abrir un navegador web, en nuestro caso Firefox, e ir a la siguiente dirección https://localhost:10000. Es muy probable que al acceder a dicha dirección el sistema nos devuelva un error como el que se muestra en la Figura 5.33.

Fig. 5.33. *Error del certificado.*

Para solucionar dicho error debemos crear una excepción.

A continuación aparecerá una página como la que se muestra en la Figura 5.34.

Fig. 5.34. *Formulario de conexión a la aplicación Webmin.*

Claves y consejos

Si no tienes una partición independiente para */home,* puedes crear una nueva partición y realizar el caso práctico sobre esa partición.

Introducimos como usuario al administrador root y la contraseña del mismo. A continuación veremos una nueva ventana como la que se muestra en la Figura 5.35.

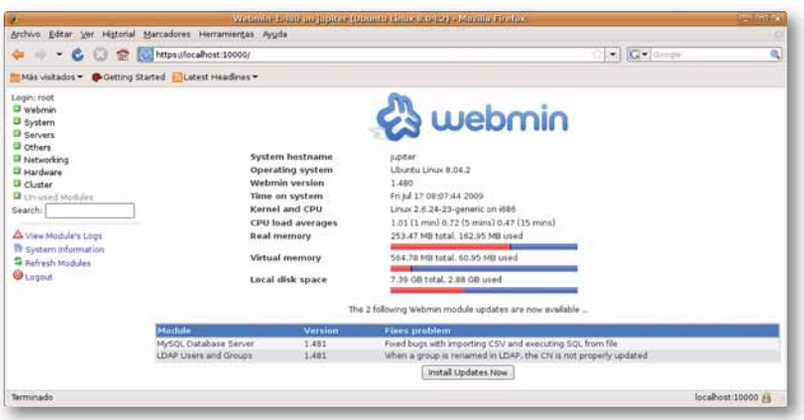


Fig. 5.35. *Pantalla inicial webmin.*

Como podemos ver, este programa es una aplicación web que se puede utilizar para configurar multitud de opciones del sistema.

Como vemos en la Figura 5.35, la página de entrada tiene un marco a la izquierda con un menú. Escogemos la opción *System* (sistema) y dentro de esta la opción *Disk and Network Filesystems* (Disco y Sistemas de archivos en red). Una vez realizada la selección, el marco de la derecha se actualiza visualizando todos los sistemas de archivos de nuestro equipo (Fig. 5.36).

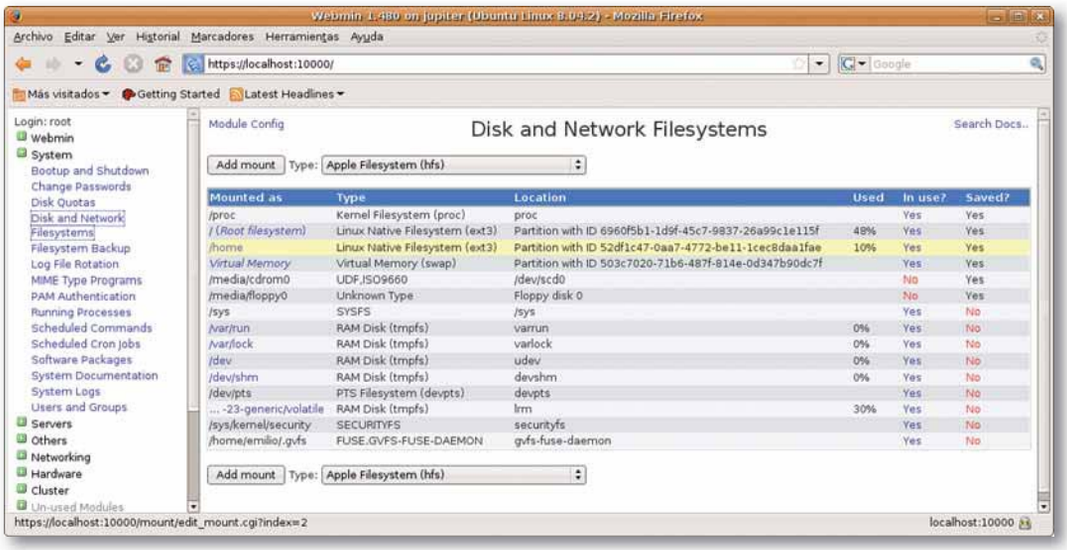


Fig. 5.36. *Disk and Network Filesystems.*

De todos ellos nos vamos a centrar en el directorio */home,* que está montado en una partición independiente y es la idónea para activar las cuotas de usuario, por ser en ella donde se guardarán todos los archivos de los mismos. En el marco de la derecha de la página, seleccionamos con el ratón la opción */home,* que nos llevará a una nueva pantalla (Fig. 5.37).

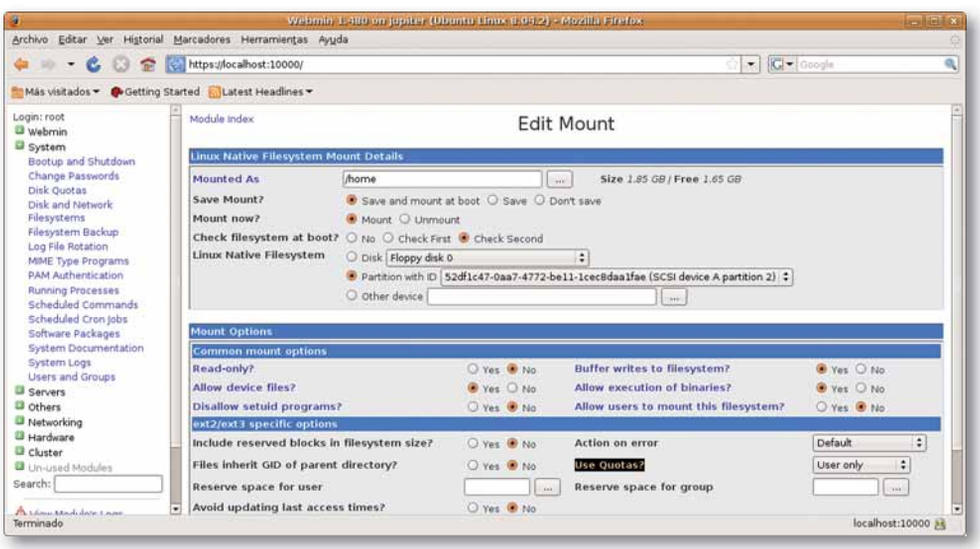


Fig. 5.37. *Edit Mount.*

En esta nueva página, tendremos que poner la opción *Use Quotas?* (¿usar cuotas?) con el valor *User only* (sólo usuario), pues vamos a aplicar las cuotas de disco por usuario y no por grupos.

El siguiente paso consistirá en establecer las cuotas que queramos a cada uno de los usuarios del sistema. Para ello elegiremos en el marco de la derecha la opción *System* (Sistema) y en ella la opción *disk quotas* (cuotas de disco), como podemos ver en la Figura 5.38.

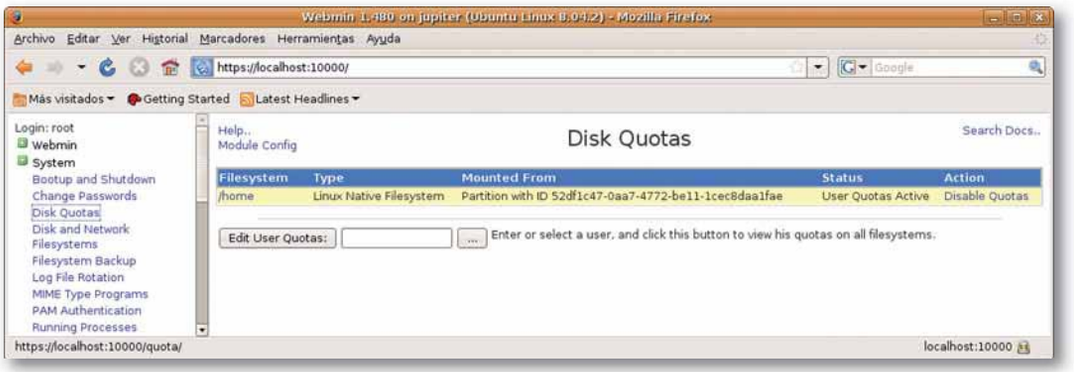


Fig. 5.38. *Cuotas de disco.*

En esta nueva pantalla aparecen los sistemas de ficheros para los que se hayan establecido cuotas de disco, que como se ve, solo se ha realizado en la partición */home*. Si marcamos con el ratón la opción */home,* iremos a una nueva pantalla que contiene una línea por cada usuario del sistema (Fig. 5.39).

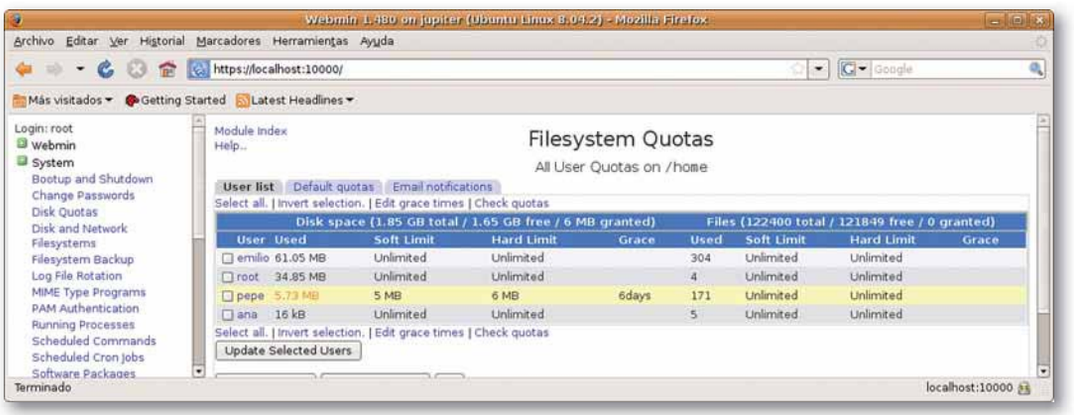


Fig. 5.39. *Cuotas de los usuarios.*

Por último, sólo nos queda seleccionar los usuarios a los que queremos asignarles cuotas de disco y establecer las mismas. Para ello se seleccionará el usuario elegido, apareciendo una nueva pantalla como la que se muestra en la Figura 5.40.

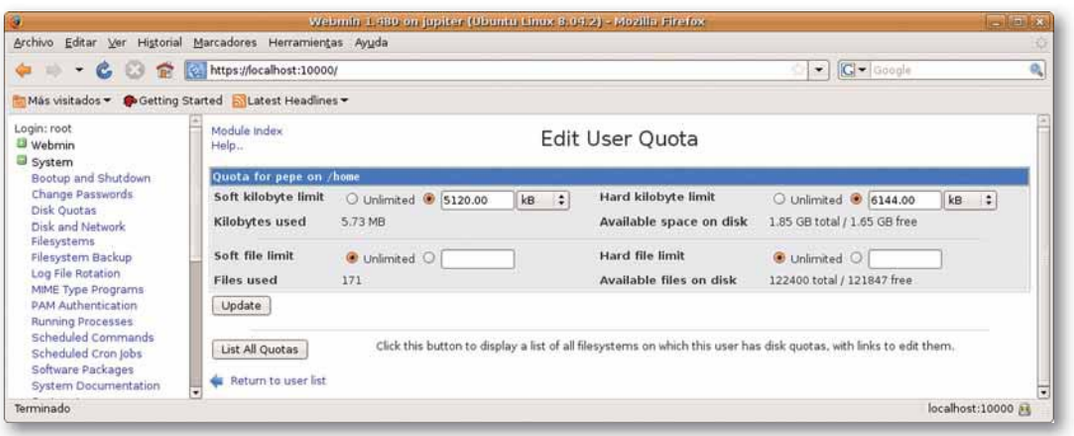


Fig. 5.40. *Asignación de cuota a usuario.*

Una vez definidas las cuotas, hacemos clic sobre el botón *Update* (actualizar). Si quisiésemos poner cuotas a otro usuario, repetiríamos el proceso anterior.

3. Autenticación de los usuarios

Según la Real Academia Española, *autenticar* se define como «dar seguridad de que alguien o algo es lo que representa o parece».

Los métodos de autenticación, en nuestro caso, son los mecanismos que una máquina tiene para comprobar que el usuario que intenta acceder es quien dice ser.

Estos métodos se pueden clasificar en tres grupos, en función de los medios que se vayan a utilizar para identificarse:

- **Algo que el usuario sabe** y que el resto de las personas desconocen: es lo más utilizado. Lo usamos para acceder a nuestra cuenta de correo electrónico, para conectarnos a Tuenti… (utilizamos un nombre de usuario y una contraseña que solo conocemos nosotros).
- **Algo que el usuario posee,** por ejemplo, una tarjeta de identidad.
- **Alguna característica propia del usuario,** rasgos físicos o comportamientos. Ejemplos: la huella dactilar, característica utilizada en el DNI para identificarnos; la retina, la manera de teclear… A este tipo de medidas se le conoce como mecanismos biométricos.

Hay sistemas de autenticación que combinan distintos métodos para alcanzar un mayor grado de seguridad; pensemos cuando vamos a sacar dinero de un cajero automático, que primero debemos insertar nuestra tarjeta de crédito (algo que poseo) y luego solicita el número de identificación, PIN (algo que conozco).

Actividades

7. Define una política de contraseñas para la red del aula. Dicha política deberá incluir los siguientes apartados:
   - Objetivo del documento.
   - Ámbito de la aplicación (a qué usuarios influye).
   - Formato de las contraseñas.
   - Longitud de las contraseñas.
   - Tiempo de vida de la contraseña.
   - Forzar el historial de contraseñas.
   - Indica tras cuántos intentos se bloqueará la cuenta.

3.1. Políticas de contraseñas

En la mayoría de los equipos informáticos, la autenticación de los usuarios se realiza introduciendo un nombre y una contraseña. Cada usuario tiene asignado un identificador y una clave, que permitirán comprobar la identidad del mismo en el momento de la autenticación.

Como es lógico pensar, la seguridad del sistema va a estar fuertemente relacionada con la buena elección de la contraseña y la confidencialidad de la misma. Por este motivo, las empresas suelen tener definidas políticas de contraseñas donde se establece la longitud mínima de la misma, su formato, el tiempo que será válida, etc.

A continuación, vamos a estudiar las características que debe cumplir una buena contraseña:

- No deben estar formadas por palabras que encontremos en diccionarios, ni en español ni en ningún otro idioma, ya que cualquier programa de fuerza bruta lo descubriría con facilidad.
- No deben usarse sólo letras mayúsculas o minúsculas, porque se reducirían las combinaciones en un alto grado; ejemplos rechazables: ANA, avestruz, abcdef.
- No deben estar formadas exclusivamente por números, por el mismo motivo que en el caso anterior. Ejemplos: 273456, 373009.
- No debemos utilizar información personal: nombre de nuestros familiares, fecha de nacimiento, número de teléfono… ya que cualquier persona cercana a nosotros podría descubrirla. Ejemplos: cp28007, 06/06/1965. Este fallo es muy habitual en las preguntas que te realizan determinadas páginas (correos electrónicos) cuando no recuerdas la contraseña.
- No debemos invertir palabras reconocibles, como atatap, zurtseva. Cualquier programa creado para este fin lo descubriría en un corto espacio de tiempo.
- No debemos repetir los mismos caracteres en la misma contraseña.

- No debemos escribir la contraseña en ningún sitio, ni en papel ni en documentos electrónicos que no hayan sido encriptados.
- No debemos enviarla en ningún correo electrónico que nos la solicite.
- No debemos comunicarla a nadie por teléfono.
- Debemos limitar el número de intentos fallidos. Si excede el número máximo de intentos permitidos, el usuario debe quedar bloqueado, por lo que tendrá que ponerse en contacto con el técnico de seguridad. Es lo que ocurre en los cajeros automáticos, si te equivocas tres veces al introducir la clave, el cajero se queda con la tarjeta. Con ello evitamos que se puedan seguir haciendo intentos indefinidamente y al final se descubra el número secreto.
- Debemos cambiar las contraseñas de acceso, dadas por defecto por los fabricantes de routers y otros periféricos, que nos permiten el acceso a la red.
- No debemos utilizar la misma contraseña en las distintas máquinas o sistemas, ya que si nos la descubren, haríamos vulnerables el resto de equipos a los que tenemos acceso.
- Las contraseñas deben caducar y exigir que se cambien cada cierto tiempo, al menos una vez al año.
- No debemos permitir que las aplicaciones recuerden las contraseñas.

Por lo tanto, las contraseñas deben ser cadenas de caracteres que incluyan tanto letras mayúsculas, minúsculas, números y caracteres especiales sin ningún tipo de lógica aparente. La longitud de la misma debe ser superior a ocho caracteres, aunque lo más recomendable es que supere los quince.

Algunos consejos para poder recordar la contraseña, ya que como hemos comentado anteriormente no podremos escribirla en ningún sitio, sería elegir palabras sin sentido pero que sean pronunciables, o bien elegir la primera letra de una frase que recordemos por ser parte de una canción que nos gusta, o de algún recuerdo, por ejemplo: «Nací el 6 de junio del 65 en Madrid cerca de las 6 de la madrugada», Ne6dJd6eMcdl6dlm; para complicarla, se puede poner algún símbolo especial en una posición que podamos recordar.

Si cumplimos con todas las recomendaciones expuestas anteriormente, haremos que cualquier intruso que intente descubrir la clave de acceso mediante programas de fuerza bruta, como John the Ripper o similares, tenga que perder mucho tiempo y desista del proceso.

Recordad, una contraseña mal elegida o mal protegida puede suponer un importante agujero en la seguridad del sistema.

Para aquellos de vosotros que no tengáis mucha imaginación para crear claves, hay multitud de programas que os permiten generar contraseñas con las características que vosotros queráis. Ejemplos de esos programas son Max Password y Password Generator.

Actividades

8. Descargaos la aplicación John the Ripper **(www.openwall.com)** y comprobad los tiempos que tarda en descubrir contraseñas:

- Formadas por una palabra que podéis encontrar en el diccionario, por ejemplo patata.
- Formadas solo por números 373009.
- Formadas por palabras invertidas, por ejemplo patata al revés, atatap.
- Formadas por palabras en otros idiomas, computer.
- Formada por un conjunto de caracteres sin sentido: $1Ah%4Unb89{3.

3.2. Sistemas biométricos

Los sistemas biométricos, se utilizan para autenticar a los usuarios a través de sus rasgos físicos o conductas.

Estos sistemas se están popularizando en la actualidad; podemos encontrar portátiles que nos obligan a autenticarnos para acceder a su sistema operativo a través de la detección de la huella digital.

Otro caso similar nos lo encontramos en Disney World, la identificación de los usuarios que poseen entrada válida para varios días, se realiza mediante sistemas biométricos; de esta manera, se evita que un grupo de amigos saquen entradas para varios días aprovechando el descuento y que posteriormente accedan al parque en distintos días repartidos en pequeños grupos.

¿Cómo funciona un sistema biométrico?

El funcionamiento del sistema biométrico se compone de dos módulos, el de inscripción y el de identificación (Fig. 5.41).

El primero de ellos, mediante sensores, lee y extrae la característica que identifica al usuario, almacenando el patrón en una base de datos.

El módulo de identificación lee y extrae la característica que reconoce al usuario. Ese patrón es comparado con los que se tienen almacenados en la base de datos y se devuelve la decisión sobre la identidad del usuario.

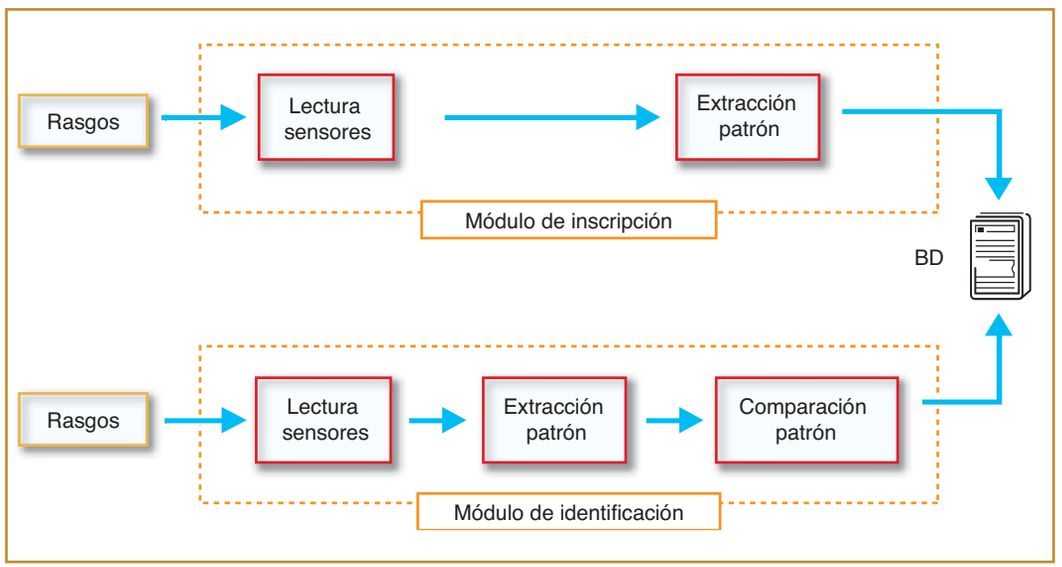


Fig. 5.41. *Funcionamiento de un sistema biométrico.*

Fig. 5.42. *Sistemas biométricos.*

Los tipos de sistemas biométricos más populares son:

- Verificaciones anatómicas:
  - Mano: huellas dactilares, geometría, venas.
  - Rostro: geometría.
  - Patrones oculares: retina, iris.
- Verificación del comportamiento:
  - Timbre de la voz.
  - Escritura: uso del teclado, escritura manual de un texto predefinido, firma del usuario.
  - Longitud y cadencia del paso.

3.3. Listas de control de acceso

Las listas de control de acceso, también conocidas por su sigla en inglés ACL, mejoran la seguridad de los archivos de nuestro sistema. En dichas listas, se definen los privilegios que tiene un usuario de forma individual sobre un determinado fichero, es decir, permiten o limitan el acceso a los archivos de manera individual sin tener en cuenta el grupo al que pertenece el usuario.

Caso práctico 8

Definir listas de control de acceso en Ubuntu 9.04 para restringir el acceso a los archivos

1. Para poder hacer uso de las listas de control de acceso debemos comunicarle al sistema en qué particiones vamos a querer usarlas. Para ello, necesitamos configurar el fichero `/etc/fstab`.

   Los sistemas de ficheros montados con ACL, tendrán la palabra clave «acl» en las opciones de montaje de dicho fichero.

2. En nuestro caso, además de las particiones de root y swap, tenemos una tercera dedicada al almacenamiento de datos; en esta última, vamos a configurar la lista de control de acceso; para ello modificamos el fichero `fstab` (Fig. 5.43), añadiendo la línea correspondiente a dicha partición (Fig. 5.44.)

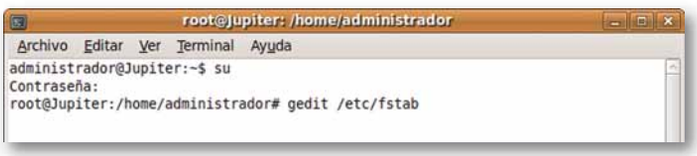


Fig. 5.43. *Edición de fichero* `fstab`.

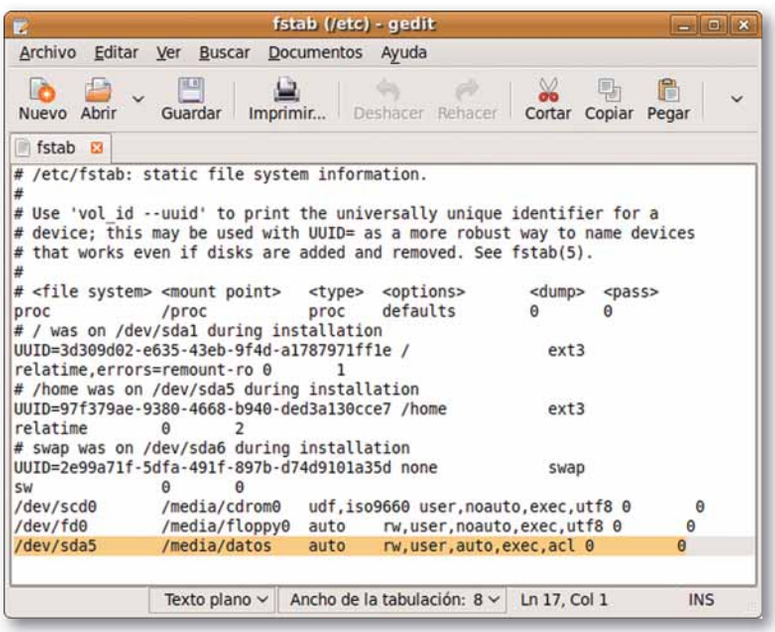


Fig. 5.44. *Fichero* `fstab`.

Claves y consejos

Para comprobar que la distribución de LINUX sobre la que vas a trabajar soporta ACL, debes utilizar el comando *grep,* como se muestra en la imagen.

Fig. 5.46. *Comprobación ACL.*

Importante

Para configurar las listas de control de acceso (ACL) debemos realizarlo bajo el perfil de administrador.

3. A continuación, procederemos a montar la partición nuevamente (Fig. 5.45).

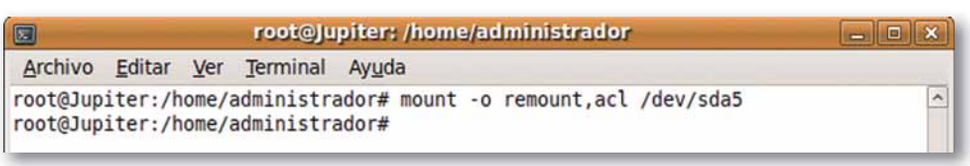


Fig. 5.45. *Remontar unidad.*

Actividades

9. ¿Qué diferencias hay entre el uso de las ACL y el de la orden *chmod*?

(Continúa)

Caso práctico 8

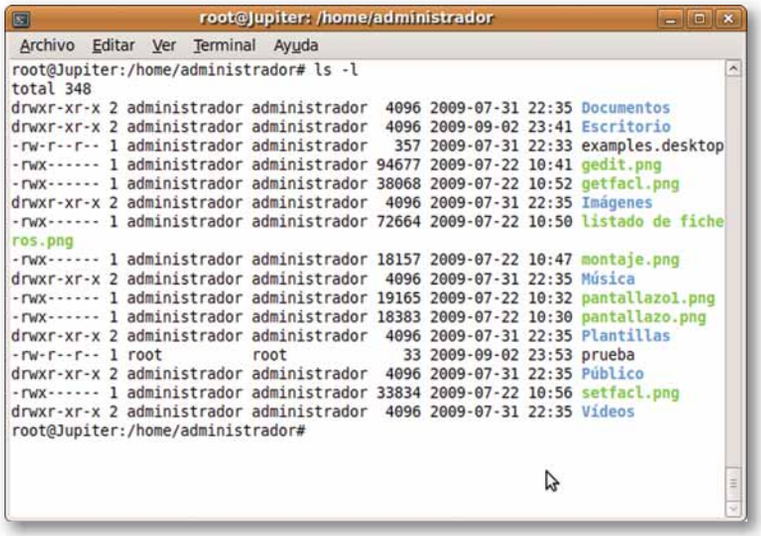


Fig. 5.47. *Ficheros de un directorio.*

(Continuación)

Para realizar el ejemplo, root ha creado un fichero llamado prueba.

Fig. 5.48. *Resultado comando* `getfacl`.

4. A continuación, mediante el comando `getfacl`, vamos a ver la información que almacena la lista de control de acceso del fichero prueba y del directorio actual.

Nos informa del nombre del fichero, del propietario, del grupo y lo que más nos interesa, los permisos del propietario (user::rw-), del grupo (group::r--) y del mundo (other::r--). Lo mismo para el directorio actual (Fig. 5.48).

Fig. 5.49. *Resultado comando* `setfacl`.

5. A continuación, vamos a darle permisos a Fernando, para que pueda leer y modificar el fichero prueba. Para ello, debemos utilizar el comando `setfacl` con la opción «-m», que nos permite modificar la ACL, y por último, comprobamos que se ha realizado la modificación solicitada (Fig. 5. 49).

Caso práctico 9

Definir listas de control de acceso en Windows utilizando el comando `cacls` para evitar el acceso a los ficheros a usuarios no autorizados

1. Para la realización de esta actividad debemos tener creados al menos dos usuarios: Usuario1 y Usuario2.
2. En la carpeta *Mis Documentos* del Usuario1, crearemos otros dos directorios: Confidencial y Datos compartidos.
3. El Usuario1 quiere permitir que Usuario2 pueda leer documentos que hay almacenados en Datos compartidos. En estos momentos eso es imposible, el Usuario2 no tiene permisos para acceder a Datos compartidos. ¿Qué podemos hacer? Modificar la lista de control de acceso para permitirle entrar a la carpeta Datos compartidos. Además, debemos permitir el acceso a la carpeta Usuario1 de *Documents and Settings* y al directorio *Mis Documentos.*

   Para ello debemos ejecutar la instrucción `cacls`, cuya sintaxis es:

   ```
   Cacls fichero /parámetros
   ```

   Los parámetros son:

   /t.- Cambia las ACLS de los archivos especificados en el directorio actual y en todos sus subdirectorios.
   /e.- Modifica la ACL en vez de reemplazarla. Este parámetro es muy importante, supongamos que queremos darle permisos al Usuario2 y no utilizamos este modificador; entonces se reemplaza la ACL antigua por la nueva, no permitiendo al Usuario1 acceder a su información.
   /c.- Fuerza la modificación aunque encuentre errores.
   /g usuario:permisos; R (lectura); E (escritura); C (cambiar), y F (control total).- Concede derechos de acceso al usuario.
   /R usuario.- Suspende los derechos al usuario.
   /p usuario:perm.- Sustituye los derechos del usuario especificado.
   /d usuario.- Deniega el acceso al usuario especificado.

   La instrucción `cacls` permite modificar las listas de control de acceso a los ficheros.

   Según la sintaxis anterior, debemos ejecutar el comando que aparece en la Figura 5.50.

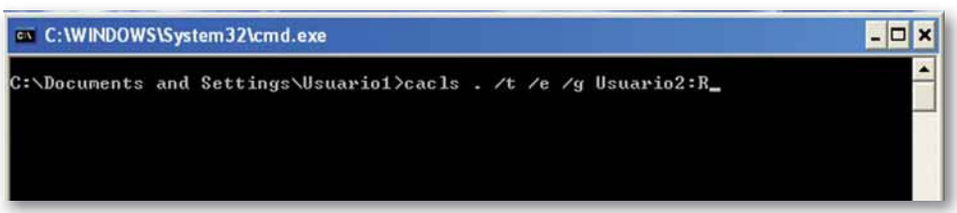


Fig. 5.50. *Modificación ACL del directorio actual y subdirectorios.*

El resultado es que el Usuario2 puede entrar a todos los directorios y ficheros que cuelguen del directorio Usuario1, o lo que es lo mismo, puede visualizar cualquier documento de dicho usuario.

Como toda la información del Usuario1 está almacenada en dos carpetas, Confidencial y Datos Compartidos, para que no tenga acceso el Usuario2 al directorio Confidencial del Usuario1, debemos ejecutar la orden de la Figura 5.51.

Fig. 5.51. *Denegación de acceso a carpeta confidencial.*

4. Vulnerabilidades del sistema

Los sistemas operativos son programados y sometidos a numerosas pruebas antes de ser lanzados al mercado, pero no se descubren sus verdaderas vulnerabilidades hasta que los «expertos en seguridad» (hackers, crackers, virus…), lo someten a sus duras pruebas. Entonces, esos agujeros son corregidos con la mayor celeridad posible por los programadores del sistema.

Por ello, siempre debemos mantener el sistema actualizado.

¿Sabías que…?

Windows publica las actualizaciones los segundos martes de cada mes, conocido como Patch Tuesday (martes de correcciones), a no ser que sea una actualización crítica, en ese caso se publica según se termine.

4.1. Evitar vulnerabilidades en Windows

Para evitar las vulnerabilidades en Windows, debemos mantener el sistema actualizado con los últimos parches. Esto lo podemos realizar de distintas maneras:

Windows proporciona un servicio de actualizaciones automáticas a través de la Web, denominado Windows Update, ubicado en windowsupdate.microsoft.com. Si nos conectamos a esta página, el servicio analiza el sistema operativo y determina las actualizaciones que es necesario descargar.

Otra manera es configurar el sistema operativo para que realice las descargas de las actualizaciones automáticamente. Para ello debemos pulsar el botón Inicio de Windows Vista, hacer clic sobre el *Panel de Control* y seleccionar la opción de *Windows Update* (Fig. 5.52).

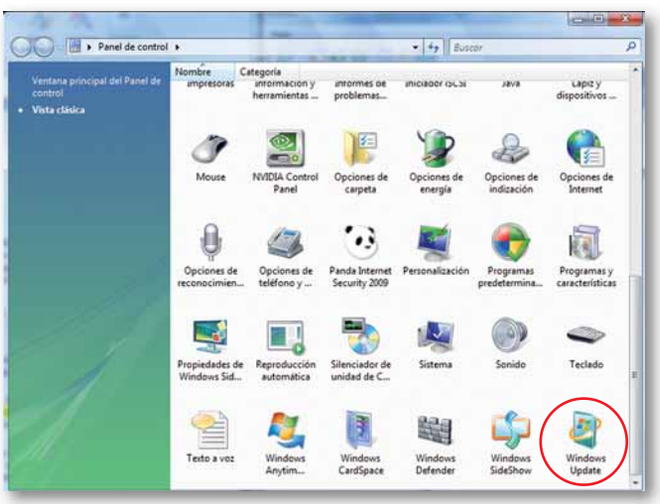


Fig. 5.52. *Panel de control.*

A continuación, se abre una nueva ventana similar a la que se muestra en la Figura 5.53.

Fig. 5.53. *Windows Update en Windows Vista.*

En esa ventana podemos buscar actualizaciones, cambiar la configuración, consultar el historial de actualizaciones, restaurar actualizaciones ocultas y ver las preguntas frecuentes sobre el proceso de actualizar el sistema.

Como estamos intentando configurar las actualizaciones automáticamente, debemos hacer clic en la opción *Cambiar configuración*, que se muestra en el marco izquierdo de la Figura 5.53.

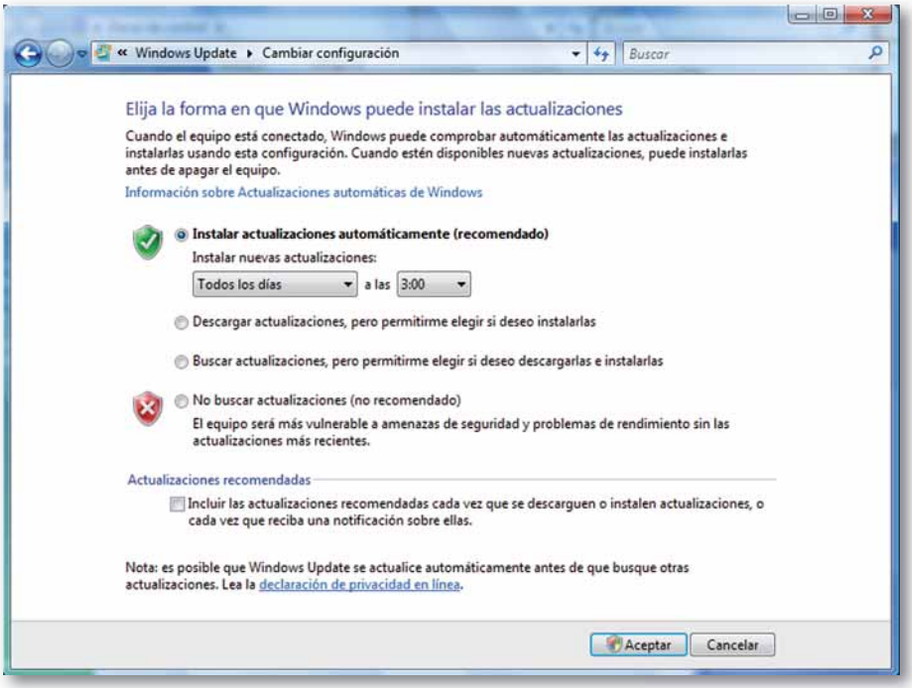


Fig. 5.54. *Configuración Actualizaciones.*

En la nueva ventana (Fig. 5.54), seleccionamos la primera opción, *Instalar actualizaciones automáticamente (recomendado),* definiendo cuándo queremos que se instalen las nuevas actualizaciones. Como sabemos que Windows suele publicar las actualizaciones los martes, lo podemos configurar para que se instalen los viernes a las 20:00 horas, de esta manera, nos aseguramos que no han dado problemas los parches publicados.

Otra opción que podemos seleccionar en la misma ventana es *Descargar actualizaciones, pero permitirme elegir si deseo instalarlas;* como su nombre indica se descargan las actualizaciones, pero no son instaladas hasta que no demos la oportuna orden.

Otra selección posible es *Buscar las actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas;* de esta manera, no se descargan las actualizaciones, ocupando espacio en el disco duro hasta el momento en que las instalamos.

Por último, podemos optar por no buscar las actualizaciones; en ese caso somos los responsables de acceder a la página de Windows Update y determinar las actualizaciones que necesitamos para mantener nuestro equipo sin vulnerabilidades.

De la misma manera que mantenemos actualizado el sistema operativo, debemos mantener actualizado los programas que tenemos instalados y, por supuesto, el firmware de los distintos periféricos que conectamos al equipo: router, switch, etc.

Como perderíamos mucho tiempo consultando la página de cada fabricante para ver si han publicado nuevas actualizaciones de las aplicaciones instaladas, podemos utilizar algunos de los numerosos programas gratuitos que existen. Estos se conectan a Internet y nos informan de si hay nuevas actualizaciones publicadas que aún no tengamos instaladas.

Algunos ejemplos de dichos programas son APPGET, SUMO, LOGICIEIMAC.COM, APPFRESH, UPDATE NOTIFIER **(http://cleansofts.org),** etc.

5. Monitorización del sistema

Con la monitorización del sistema vamos a poder auditar los eventos que se han producido en nuestro equipo.

5.1. Monitorización en Windows

Como ya estudiamos, podemos abrir el visor de sucesos mediante la orden *eventvwr.msc*. En la Figura 5.55, podemos ver que guarda información de los sucesos de aplicación, seguridad y sistema.

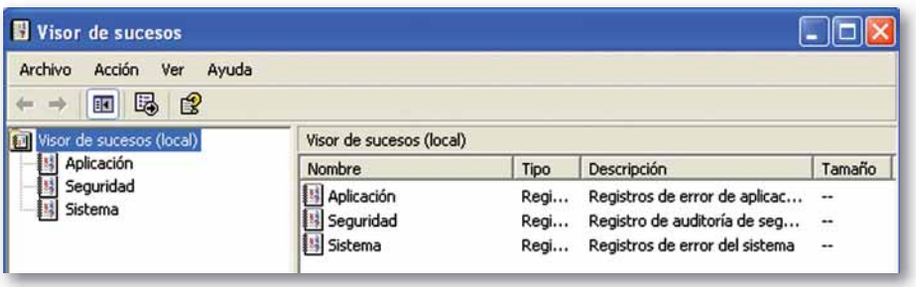


Fig. 5.55. *Visor de sucesos Windows.*

Esta información es guardada en los archivos AppEvent.Evt, SecEvent.Evt y SysEvent.Evt, ubicados todos ellos en el directorio %SystemRoot%\system32\config.

Es muy importante configurar correctamente el tamaño y el acceso a los mismos. El tamaño debe ser lo suficientemente grande para albergar los sucesos producidos en el sistema hasta que lo auditemos. Y como es lógico, para evitar que los intrusos borren sus huellas sólo deberán tener permisos de control total el técnico o técnicos encargados de la seguridad del sistema.

5.2. Monitorización en Linux

Linux tiene un complejo visor de sucesos (Fig. 5.56) que podemos arrancar desde *Sistema > Administración > Visor de archivos de sucesos.*

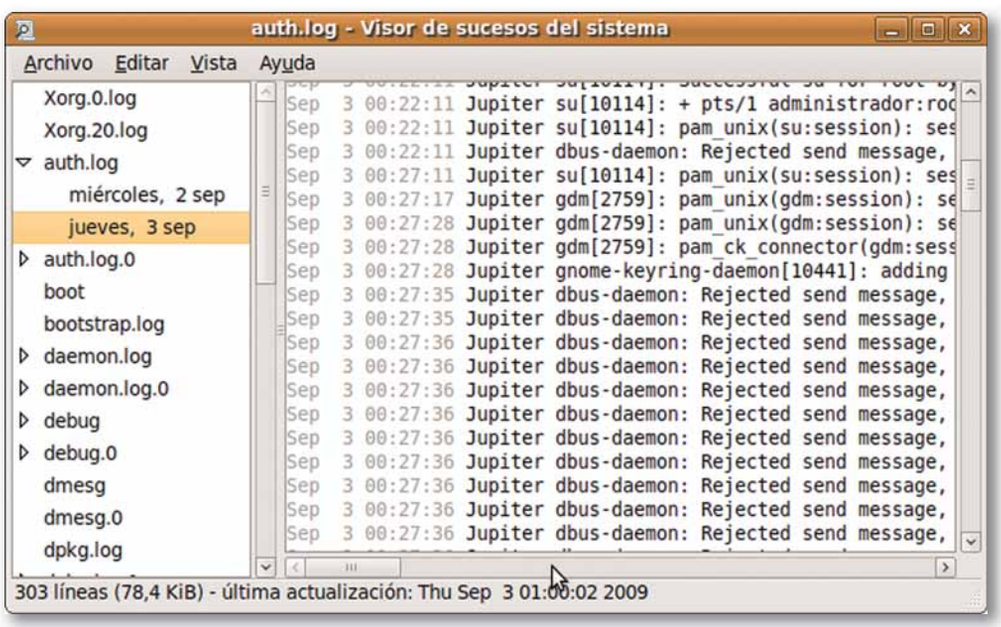


Fig. 5.56. *Visor de sucesos Linux.*

Para simplificar la auditoría, Linux tiene un conjunto de comandos, que se especializan en el registro de los distintos eventos. Para auditar las entradas al sistema utilizaremos el comando `last` (Fig. 5.58), para auditar las accesos fallidos usaremos el comando `lastb` (Fig. 5.59) y para las conexiones al sistema por red utilizaremos el comando `lastlog` (Fig. 5.60).

Los ficheros donde se guarda la información se encuentran ubicados en el directorio */var/log* (Fig. 5.57).

Vocabulario

Log. Es el registro de un evento que se produce en el sistema.

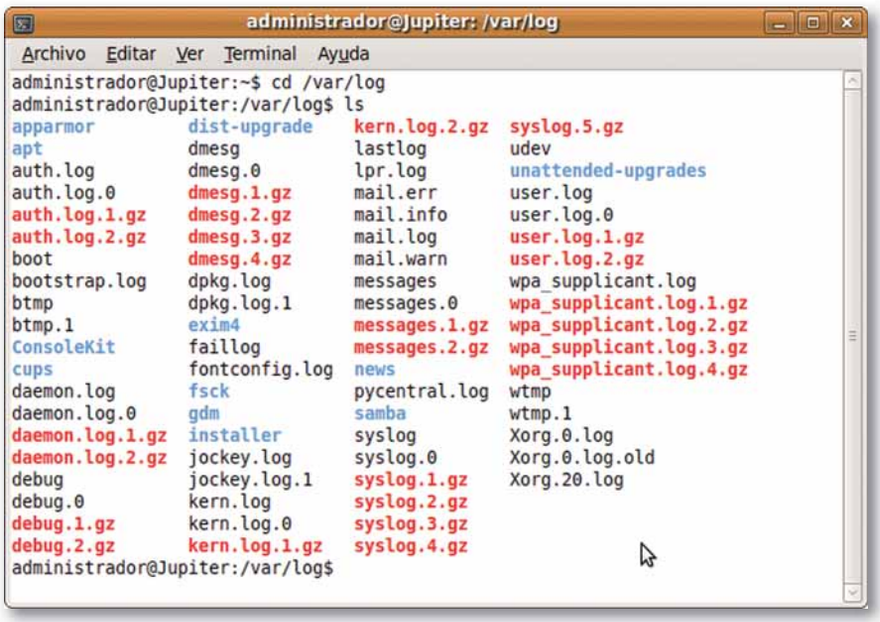


Fig. 5.57. *Ubicación logs de Linux.*

¿Sabías que...?

Blog viene de weB LOG.

A continuación, vamos a ver unos ejemplos de los comandos vistos anteriormente.

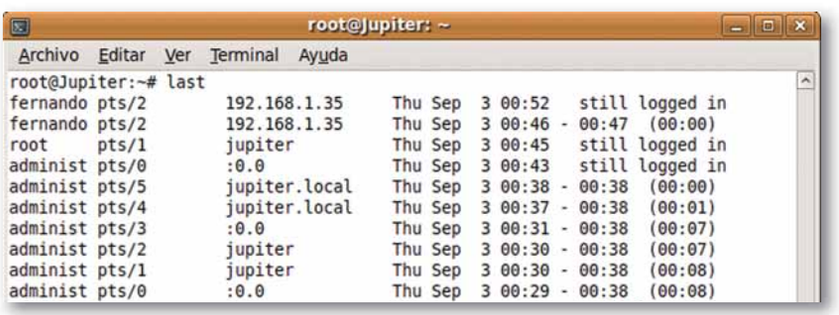


Fig. 5.58. *Resultado comando* `last`.

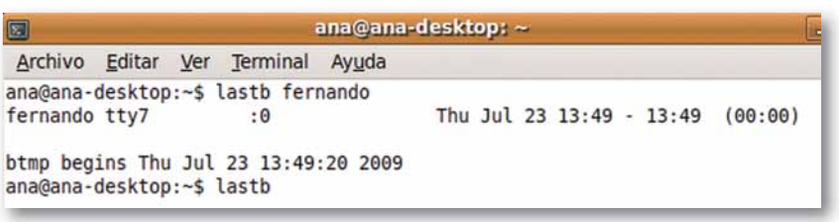


Fig. 5.59. *Salida comando* `lastb`.

Fig. 5.60. *Resultado comando* `lastlog`.

6. Software que vulnera la seguridad del sistema

En este apartado vamos a estudiar tanto las aplicaciones (virus, gusanos, snifadores…) como el tipo de intrusos que mediante el uso de las mismas amenazan la seguridad del sistema.

6.1. Clasificación de los atacantes

Los atacantes se pueden clasificar según el tipo de ataque:

- **Hackers:** son personas con grandes conocimientos informáticos y telemáticos (expertos programadores). Por su infinita curiosidad dedican un gran esfuerzo a investigar los sistemas operativos y los sistemas de seguridad para descubrir todas sus vulnerabilidades. La principal motivación de los hackers es seguir aprendiendo y mostrar las vulnerabilidades de los sistemas al mundo. En ningún caso buscan un beneficio económico o dañar la estructura del sistema. Podríamos hacer un símil con una persona que ha sido capaz de acceder al interior de una caja fuerte, pero no se ha llevado nada, simplemente ha dejado una nota informativa diciendo que ha estado allí, para informar de la vulnerabilidad de la misma. También son conocidos como hackers de sombrero blanco.
- **Crackers o hackers de sombrero negro:** el término *hacker* fue utilizado por los medios de comunicación de forma genérica, para referirse a cualquier intruso en un sistema, sin tener en cuenta la finalidad del ataque. Por este motivo, los propios hackers inventaron una nueva palabra para designar a aquellas personas que rompían las barreras de seguridad de los sistemas con fines maliciosos, bien porque buscaban un beneficio económico o bien porque por venganza dañaban las estructuras de los sistemas, etc. La palabra cracker proviene de CRiminal hACKER, es decir hackers criminales, hackers cuyas intenciones son maliciosas.
- **Phreakers:** son expertos en telefonía. Son conocidos como los phone crackers, los crackers de la telefonía, buscan un beneficio económico saboteando las redes telefónicas para realizar llamadas gratuitas.
- **Ciberterroristas:** son expertos en informática y en intrusismo en la red, que ponen sus conocimientos al servicio de países y organizaciones para el espionaje o sabotaje informático.
- **Programadores de virus:** son expertos en programación, en sistemas y en redes, que crean pequeños programas dañinos, que por uno u otro motivo llegan a la red y se distribuyen con rapidez ocasionando daños en los sistemas o en la información almacenada en los mismos.
- **Carders:** atacan los sistemas de tarjetas, especialmente los cajeros automáticos.
- **Sniffers:** lo podríamos traducir como *cotilla,* son las personas que se dedican a escuchar el tráfico de la red, para intentar recomponer y descifrar los mensajes que circulan por la misma.
- **Lammers:** también conocidos como **wannabes** o **script-kiddies** o **click-kiddies,** son chicos jóvenes que sin grandes conocimientos informáticos, se creen verdaderos hackers y se lo hacen creer a los miembros de sus pandillas. Estos sólo se han descargado herramientas o programas de Internet para realizar ataques informáticos y los han puesto en marcha sin saber cómo funcionan. Los verdaderos hackers muestran una gran repulsa hacia los lammers.
- **Newbie:** son los hackers novatos, empiezan a aprender y van superando los primeros retos para llegar a ser verdaderos hackers.

¿Sabías que…?

Luser es el término que utilizan los atacantes para referirse al usuario que va a ser atacado. Es la abreviatura de Local USER.

¿Sabías que…?

La palabra *hacker* ha sido utilizada erróneamente por la prensa para referirse a aquellas personas involucradas en cualquier acto que ataque la seguridad informática, sin tener en cuenta el fin del mismo.

6.2. Tipos de ataques

Podemos hacer una primera clasificación de los tipos de ataques **según los objetivos** de seguridad que vulneran.

- **Interrupción,** este tipo de ataque vulnera la disponibilidad de un recurso del sistema o de la red. El recurso no podrá ser utilizado. Ejemplos, denegación del servicio, el apagado manual de cualquier recurso (equipo, servidor, impresoras), el robo de un disco duro, cortar una línea de comunicación, deshabilitación de un sistema de ficheros (umount).

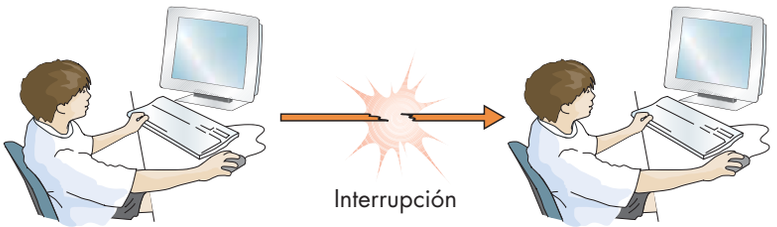


Fig. 5.61. *Interrupción.*

- **Intercepción,** ataca la confidencialidad. Un intruso accede a información almacenada en nuestro sistema o al que hemos trasmitido por la red, es decir, la información ha caído en manos de personal no autorizado. Ejemplos, captura de información en la red o copia de archivos no autorizada.

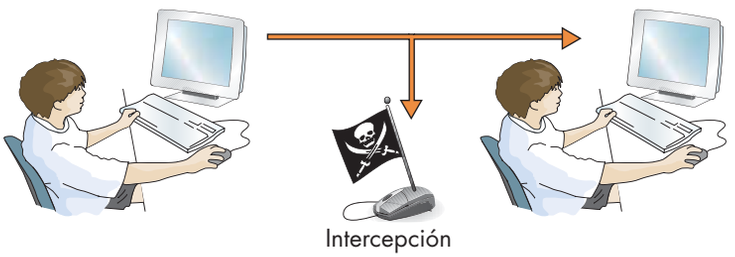


Fig. 5.62. *Intercepción.*

- **Modificación,** ataca el objetivo de integridad. Los datos han sido manipulados por personal no autorizado en algún momento entre su creación y su llegada al destinatario. La información que se dispone después de un ataque de estas características no es válida ni consistente. Ejemplos, las modificaciones de programas para que realicen acciones diferentes a las propuestas originalmente, modificar un mensaje transmitido por la red, DNS spoofing,…

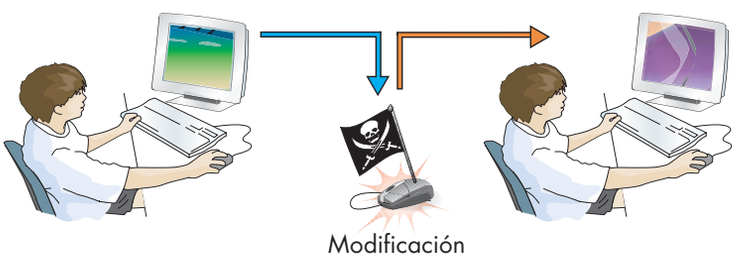


Fig. 5.63. *Modificación.*

- **Fabricación,** este tipo de ataque vulnera la autenticidad. Se trata de modificaciones destinadas a conseguir que el producto final sea similar al atacado de forma que sea difícil distinguirlo del original. Por ejemplo, el phising.

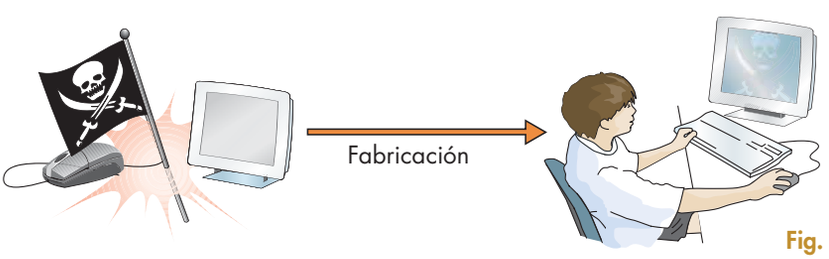


Fig. 5.64. *Fabricación.*

Otro tipo de clasificación se puede realizar **en función de la forma de actuar** de los ataques:

- **Spoofing o suplantación de la identidad:** la técnica de spoofing (engaño o falseamiento) se usa en redes ethernet conmutadas, es decir, en redes que hacen uso de switch como elemento de interconexión entre los diferentes PC.

  Este ataque consiste en falsear algún dato de un PC atacado. Existen distintos tipos de spoofing, como puede ser el arp spoofing o arp poisoning, que consiste en engañar a la tabla arp que los equipos guardan en memoria, tabla que simplemente asocia una dirección física o mac de una tarjeta de red con su IP (Fig. 5.65).

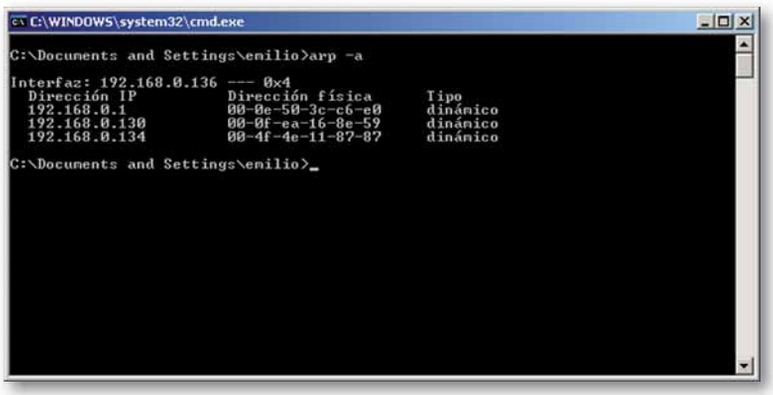


Fig. 5.65. *Tabla ARP de PC atacado antes de realizar ARP Spoofing.*

Ten cuidado

El comando ARP permite ver o modificar las entradas de la tabla de IP-MAC.

Con esta técnica de engaño podemos hacer creer a un PC atacado que la dirección física de otro PC, también atacado de la red, es la del PC del atacante, consiguiendo con ello que todo el tráfico de red entre los dos PC atacados pase por el PC del atacante (Fig. 5.65); es lo que se conoce como *man in the middle* (hombre en medio).

En la Figura 5.66 podemos ver como la MAC de la dirección del PC atacado (192.168.0.134) ha sido modificada con la dirección física (00-0f-ea-16-8e-59) que es la dirección física del atacante.

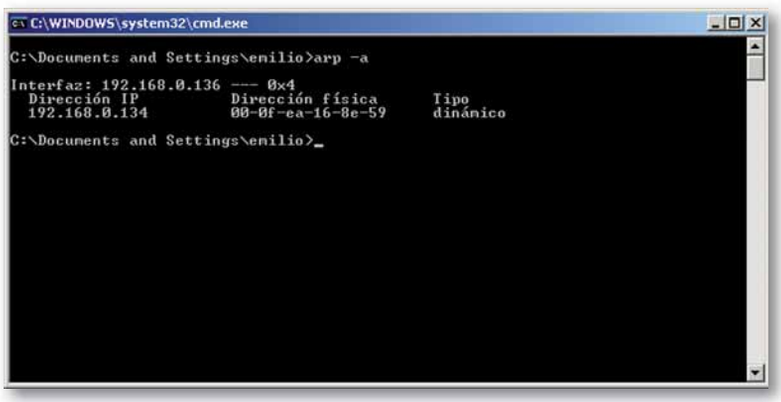


Fig. 5.66. *Tabla ARP del PC atacado tras el ARP Spoofing.*

Otra versión de este tipo de ataques es el DNS spoofing o engaño de DNS, que consiste en falsear la respuesta del servidor DNS sobre una petición y darle una dirección IP diferente a la real. Es decir, que cuando un PC atacado pide por ejemplo la IP de www.mibanco.es a su servidor DNS, el equipo atacante falseará el paquete de datos de los DNS con la respuesta y le puede engañar dándole la IP de otro equipo cualquiera. Así en vez de conectarse a su banco se conectaría a otro PC diferente pudiendo falsear la pagina de entrada de su banca electrónica y capturando sus claves de acceso a la misma.

Veamos estas dos técnicas mediante una práctica realizada con el programa CAIN que te puedes descargar de la página **http://www.oxid.it/cain.html.**

Caso práctico 10

ARP spoofing y DNS spoofing

En esta práctica, vamos a hacer que cuando un usuario desde un PC atacado resuelva la IP asociada al nombre www.google.com, en vez de contestarle con la dirección real, obtendrá como repuesta la IP de un equipo de nuestra red.

Antes de hacer el DNS spoofing tendremos que realizar un envenenamiento de la tabla ARP, para así cambiar las tablas IP-MAC del PC atacado y del router y redirigir todo el tráfico que va desde el PC atacado hacia el router a través del PC del atacante.

Como vemos en la Figura 5.67 antes del ataque, el DNS resuelve la dirección de Google con su dirección IP real (209.85.229.147).

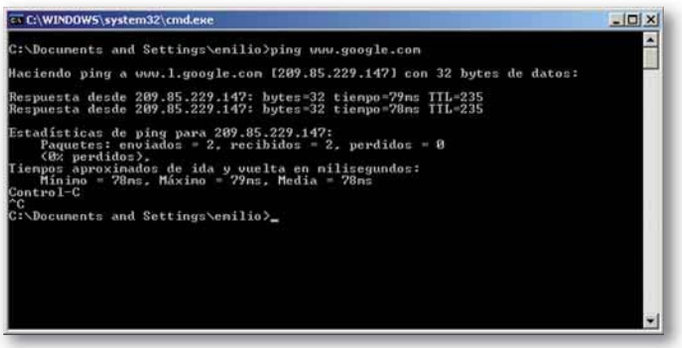


Fig. 5.67. *Ping a la dirección www.google.com.*

Después del ataque, el atacante modifica la dirección devuelta por el DNS por una dirección que el atacante configura a través de la aplicación CAIN. Para realizar esta práctica debemos seguir dos sencillos pasos:

1. El primero, crear una entrada de envenenamiento ARP (Fig. 5.68). Con esto conseguiremos que todo el tráfico entre PC atacado y el router sea redireccionado al PC del atacante.

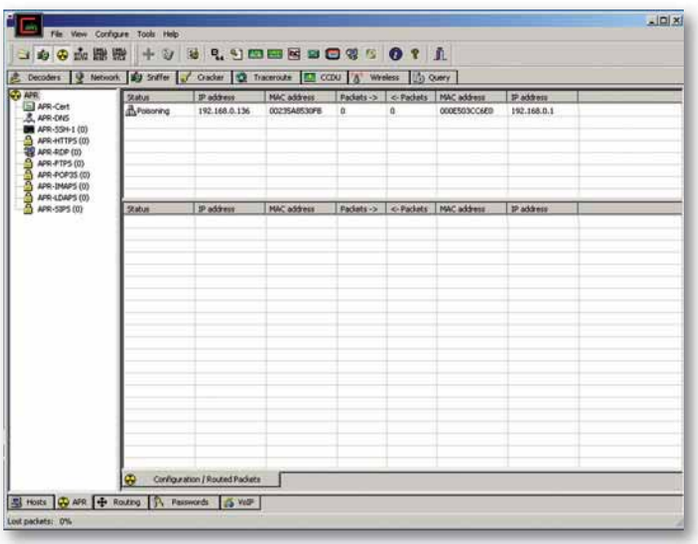


Fig. 5.68. *Entrada de envenenamiento.*

2. El segundo paso, consiste en introducir una entrada de DNS spoofing (Fig. 5.69) consiguiendo que cuando el atacado se quiera conectar a Google realmente se conectará al equipo con la IP 192.168.0.134.

(Continúa)

Caso práctico 10

(Continuación)

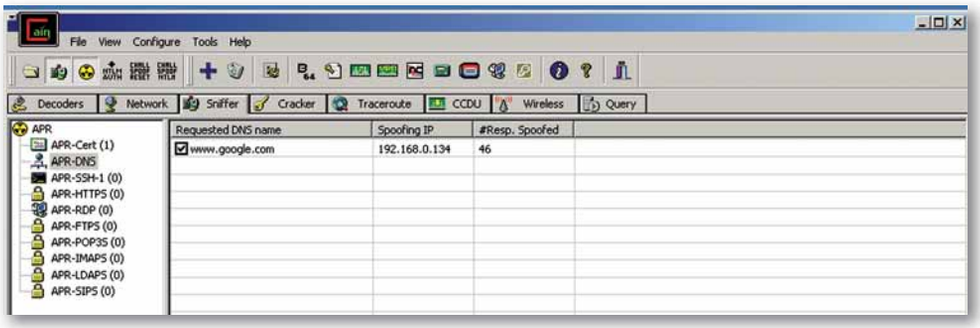


Fig. 5.69. *Entrada de DNS spoofing.*

Como se puede ver en la siguiente imagen, cuando hacemos un ping a Google desde el equipo atacado devuelve la dirección que ha configurado el atacante (192.268.0.134).

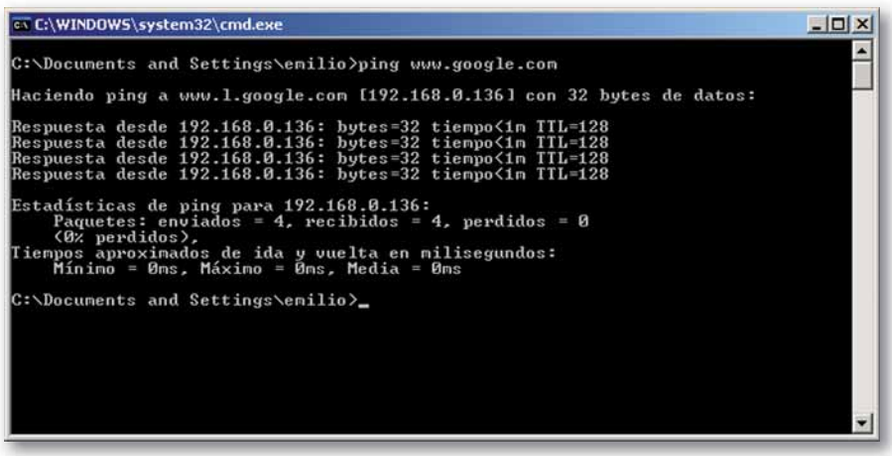


Fig. 5.70. *Resultado de la entrada de DNS spooting.*

Como es lógico pensar, esta técnica se puede utilizar para cometer fraudes en intranets o redes corporativas reenviando al atacado a una página muy similar a la original, pero falsa, por lo que el intruso podrá ver sus claves.

Contra este tipo de ataques podemos luchar creando las tablas ARP de los equipos expuestos de forma estática mediante el comando ARP.

Vocabulario

MAC. Media Access Control, es un número de 48 bits que generalmente se expresa como 12 dígitos hexadecimales, y que identifica de forma única a cada tarjeta de red ethernet.

Sniffing o análisis de tráfico: como hemos comentado en el epígrafe de tipos de atacantes, este tipo de ataques consiste en escuchar el tráfico de la red.

En las redes de área local que utilizan el HUB como medio de interconexión entre los equipos, esta técnica se convierte en un juego de niños; como sabemos, los hubs o concentradores repiten toda la información recibida por cada uno de sus puertos. Para dificultar el uso de esta técnica, debemos sustituir los concentradores por switchs o conmutadores, ya que estos últimos al tener definidas las tablas de direccionamiento (CAM Control Addressable Memory) sólo mandan la información recibida por el puerto adecuado. Pero es tan fácil como utilizar una técnica de MAC flooding, que consiste en saturar la memoria de los conmutadores para que pierdan la tabla de direccionamiento y terminen funcionando como concentradores, es decir, que reenvían la información recibida por todos los puertos por no saber por cuál de ellos debe enviarla.

Caso práctico 11

Comprometer una sesión telnet entre dos equipos atacados

Para la realización de esta práctica hemos utilizado tres equipos conectados a la misma red mediante un switch. Volveremos a utilizar la misma aplicación que en el caso práctico anterior, CAIN, con la que envenenaremos mediante la técnica del ARP spoofing el tráfico generado entre los dos PC atacados consiguiendo visualizar el contenido de la sesión telnet entre los mismos.

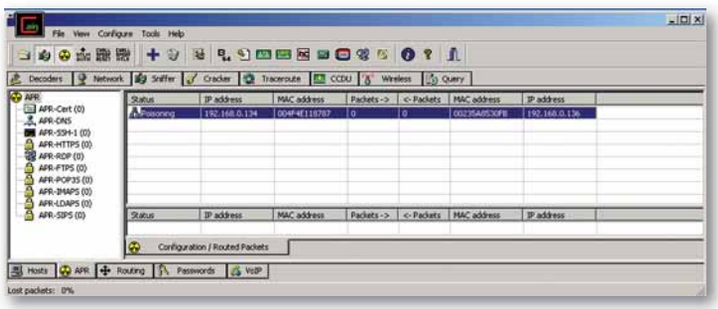


Fig. 5.71. *Envenenamiento del tráfico entre dos PC.*

1. Como puedes ver en la siguiente imagen (Fig. 5.71), se está envenenando el tráfico entre dos PC; uno con la dirección IP 192.168.0.134, que será el que inicie la sesión telnet, y otro con dirección IP 192.168.0.136 que es quien tiene en ejecución un servidor telnet.
2. En el siguiente paso, vamos a ver como el sniffer escucha el tráfico generado entre los dos PC atacados durante una sesión de acceso remoto.

En primer lugar Emilio inicia una sesión telnet autenticándose mediante su nombre y usando como contraseña patata (Fig. 5.72).

En la siguiente imagen, vemos como el sniffer mediante la aplicación CAIN ha sido capaz de comprometer nuestra sesión telnet (Fig. 5.73). El intruso ve el nombre de usuario y la contraseña utilizados para la conexión y posteriormente la ejecución del comando `dir` realizada durante la sesión por el atacado.

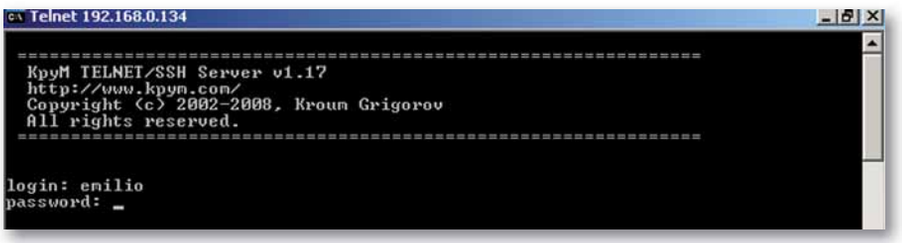


Fig. 5.72. *Inicio sesión telnet.*

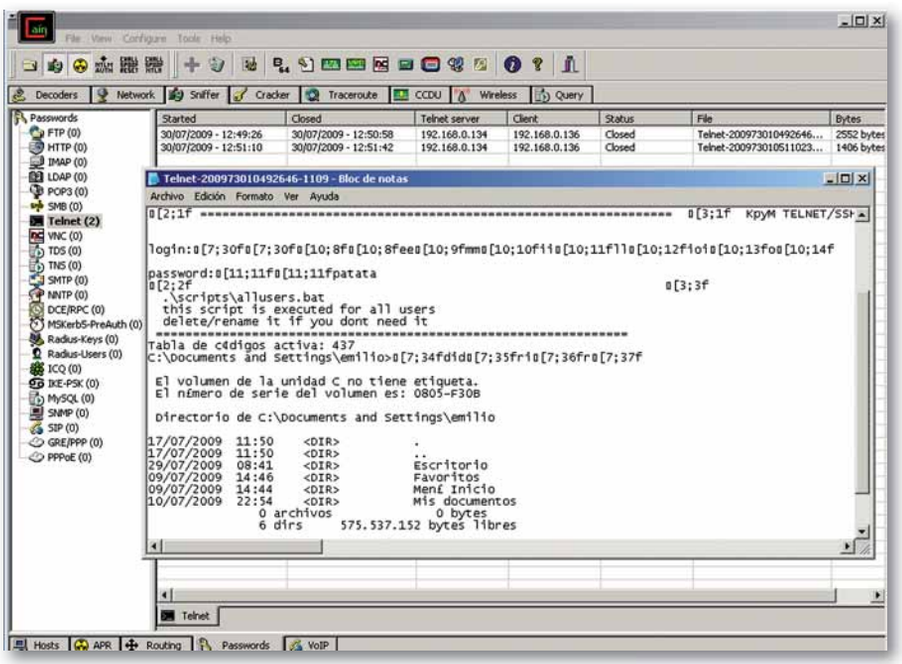


Fig. 5.73. *Telnet comprometido.*

- **Conexión no autorizada a equipos y servidores:** este tipo de ataque consiste en descubrir distintos agujeros en la seguridad de un sistema informático y establecer con el mismo una conexión no autorizada. Ya sea porque hemos descubierto las contraseñas de algunos usuarios, como en el caso práctico anterior, o bien utilizando aplicaciones malware que aprovechan las puertas traseras o agujeros para permitir el acceso al equipo desde el exterior.
- **Introducción en el sistema de malware. Virus, troyanos y gusanos:** los virus, troyanos o gusanos son conocidos como malware, programas malintencionados, que infectan nuestro equipo dañando de múltiples formas nuestro sistema.
  - Los **virus** son programas que se propagan entre los equipos. Su código se adjunta al de otro programa existente en el sistema para facilitar la propagación del mismo y causar los daños para los que han sido diseñados por el creador. La característica principal es que su código ha sido escrito con la intención de que se vaya replicando para así infectar el mayor número de equipos posibles. Ejemplos famosos de virus son Barrotes, Viernes 13…
  - Los **gusanos** son diseñados con el mismo fin que los virus, que se propaguen por la red. Se diferencian en que éstos no necesitan la intervención del usuario, ya que no se adjuntan a ningún otro programa, sino que son distribuidos de manera completa por la red consumiendo en la gran mayoría de los casos un gran ancho de banda de la red o pueden llegar a bloquear el equipo infectado. Algunos ejemplos famosos de este tipo de programas son Sasser y Blaster.
  - Los **troyanos** son aplicaciones aparentemente inofensivas que facilitan en la mayoría de los casos el acceso remoto a los equipos infectados. Estas aplicaciones se pueden esconder en archivos adjuntos en los mensajes que enviamos por la red.

Estos daños varían desde aquellos que no realizan ningún perjuicio al equipo infectado hasta otros que realizan verdaderos destrozos irreversibles en nuestro sistema.

Para evitar el ataque de este tipo de programas se han comercializado aplicaciones denominadas antivirus que mantienen actualizadas sus ficheros de firmas para detectar y eliminar los programas con código malicioso. Ejemplos de antivirus son Panda, Norton, AVG, etc. Todos ellos tienen antivirus *on-line* (en línea) que en la mayoría de los casos sólo permiten detectar si nuestra máquina está infectada.

Es aconsejable tener instalado un antivirus, teniendo en cuenta que todos ellos ralentizan tanto el arranque como el normal funcionamiento del equipo por consumir recursos del equipo.

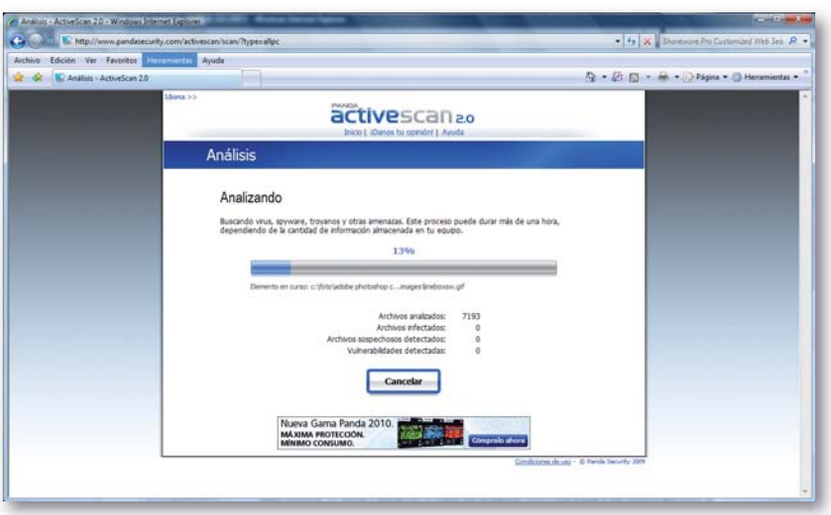


Fig. 5.74. *Antivirus online de Panda.*

Software

Puedes descargarte una versión demo de 30 días del antivirus ESET en **http://demos.eset.es/.** En el sitio podrás elegir entre ESET NOD32 Antivirus o ESET Smart Security. Puedes solicitar más información a tu profesor.

Importante

Debes cambiar las contraseñas que ponen por defecto los fabricantes a los distintos periféricos que nos permiten la conexión a Internet para evitar conexiones no autorizadas a los mismos.

¿Sabías que…?

Algunos virus famosos:

- El virus FORM hace sonar los días 18 de cada mes un pitido por cada tecla pulsada. Esto simplemente se puede considerar una broma más o menos incómoda.
- El virus VIERNES 13 borra los programas utilizados en dicho día afectando exclusivamente a los archivos ejecutables.
- Generic Backdoor, permite a los intrusos acceder de manera remota al ordenador afectado, por lo que compromete la confidencialidad de la información almacenada en el equipo.
- Sasser, es un gusano que aprovechando una vulnerabilidad de Windows, apagaba el equipo.
- Elk Cloner, programado por Rich Skrenta a los quince años de edad, es considerado el primer virus desarrollado y expandido por la red. Afectaba a los equipos con sistemas MAC instalado.

Caso práctico 12

Configurar el análisis en busca de virus y otras amenazas del Antivirus Panda

Como hemos comentado anteriormente, los antivirus ralentizan el arranque de los equipos debido al análisis en busca de malware que realizan en cada uno de los arranques.

Por ello vamos a cambiar la configuración del análisis para que no se realice en todos los arranques sino sólo los viernes.

1. Una vez arrancado el antivirus debemos hacer clic sobre la pestaña *Analizar* (Fig 5.75).

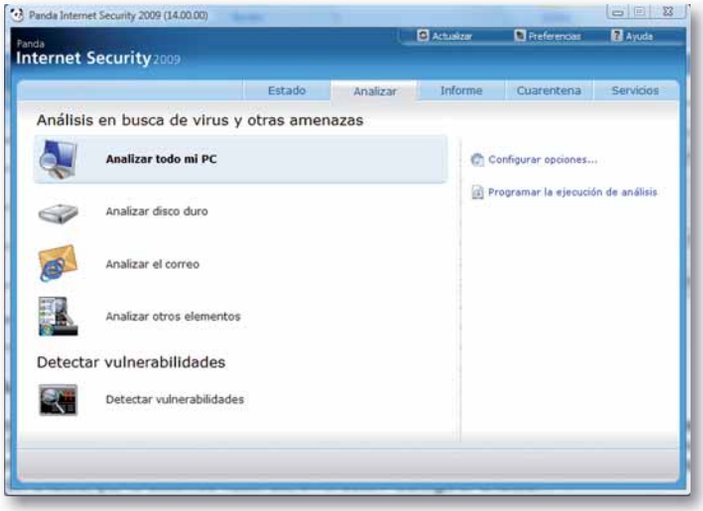


Fig. 5.75. *Análisis Panda.*

Fig. 5.76. *Programar análisis.*

2. En el marco derecho de la Figura 5.76 hacemos clic en *Programar la ejecución de análisis*. Aparece una nueva ventana (Fig 5.77) en la que se nos muestran dos botones; el primero de ellos permite generar un nuevo análisis y el segundo permite modificar la configuración del análisis programado. En nuestro caso queremos modificar la periodicidad del análisis, por lo debemos hacer clic en el botón *Configurar análisis…*

3. En la siguiente pantalla (Fig. 5.77) hacemos clic sobre el botón *Planificación.*

4. Aparece una nueva ventana en la que podemos definir cuándo queremos que se haga el análisis. Como queremos que se realice todos los viernes debemos hacer clic sobre la última opción, seleccionando en el desplegable el día (en nuestro caso Viernes), en el que queremos que se haga la comprobación (Fig. 5.78).

Fig. 5.77. *Configurar análisis.*

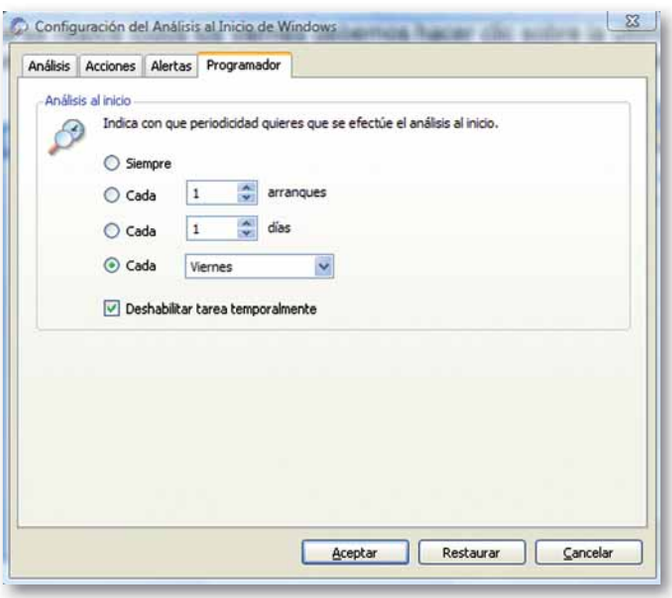


Fig. 5.78. *Configuración de la periodicidad del análisis.*

- **Keyloggers:** la traducción literal de esta palabra, registrador *(logger)* de teclas *(keys),* nos da una idea del tipo de ataque que va a realizar. Se utiliza como herramienta maliciosa para conocer todo lo que un usuario escribe a través del teclado, incluso a veces registran capturas de pantalla del equipo. Para alcanzar estos objetivos existen herramientas hardware y software. Los periféricos diseñados para tal fin pueden ir desde un teclado en apariencia idéntico a uno normal pero que contiene una memoria no volátil donde almacena la información escrita o bien mediante un pequeño dispositivo que se conecta entre el puerto del ordenador (USB o PS2) y un teclado.

- **Denegación del servicio:** este tipo de ataque también es conocido por sus siglas: DoS (Denial Of Service). Se ejecuta contra servidores o redes de ordenadores con el propósito de interrumpir el servicio que están ofreciendo. Es conocido el ataque DoS que realizaron piratas informáticos de la antigua Unión Soviética y que paralizó el acceso a Internet de los estonios, tras la decisión del gobierno del país báltico de retirar una estatua que conmemoraba a los muertos soviéticos durante la Segunda Guerra Mundial. También son conocidos los ataques de este tipo lanzados contra los servidores raíz del sistema de nombres distribuido DNS, con el fin de dejar Internet paralizada al no poder disponer los usuarios del servicio de resolución de nombres. Entre los múltiples tipos de ataque DoS se pueden destacar los siguientes:

  – La mayoría de los ataques de denegación de servicios son realizados al unísono desde múltiples máquinas que han sido convertidas en zombies por crackers de la red, llamándose en este caso DDoS, ataque de Denegación de Servicio Distribuido.

  – Ping de la muerte, consiste en enviar multitud de pings a un ordenador con un tamaño de bytes muy grande, lo que bloqueaba las conexiones en los antiguos sistemas operativos; en los actuales este tipo de ataque está subsanado y por tanto se puede considerar como historia.

- **Inundación de peticiones SYN:** más conocido por SYN Flood, consiste en hacer una petición de establecimiento de conexión a un servidor y no responder a su aceptación de conexión, bien sea porque se falseó el paquete de petición con una IP falsa o por alguna otra causa. Este tipo de ataque provoca una saturación en las conexiones abiertas del servidor, de tal forma que si estas son muy elevadas pueden llegar a producir un colapso del servicio ofrecido con la consiguiente denegación de servicio. Mediante el simple uso del comando `netstat` (comando que nos permite ver el estado de las conexiones) se puede ver si estamos siendo víctimas de un ataque de este tipo y para combatirlo se recomienda el uso de filtros en los routers que paren el tráfico de IP que puedan ser falseadas.

- **Dialers:** también conocidos como marcadores telefónicos, se hicieron muy famosos a principios de los años noventa cuando la mayoría de la gente se conectaba a Internet mediante módem.

  Son programas de conexión a Internet mediante módem, que realizan una llamada a un teléfono con tarificación especial, como aquellos que empezaban por 905. Estos programas actuaban sin la intervención y sin el consentimiento del usuario provocando una factura telefónica desorbitada. Hoy en día con las conexiones ADSL los dialers casi han desaparecido en la mayoría de los hogares.

- **Ingeniería social:** es un ataque que afecta al objetivo de confidencialidad de la seguridad informática. Esta técnica consiste en obtener información secreta de una persona u organismo para utilizarla posteriormente con fines maliciosos. Habitualmente los ingenieros sociales utilizan el correo electrónico, páginas Webs falsas, el correo ordinario o el teléfono para llevar a cabo sus planes. Los ejemplos más llamativos de estos ataques son el phising y el uso de una máquina atacada para la envío de spam.

Vocabulario

Zombie. Ordenador en el que un hacker de sombrero negro ha conseguido instalar software malicioso para hacerse con el control del mismo.

Spam. También conocido como correo basura. Correo habitualmente de publicidad que no ha sido solicitado.

- **Phishing:** es una técnica de engaño al usuario, que intenta adquirir información confidencial del mismo suplantando la identidad de otras personas, organismos o páginas WEB de Internet. Uno de los métodos de Phishing más utilizados hoy en día consiste en colgar en Internet una página que es copia idéntica de alguna otra, como puede ser la de alguna entidad financiera o banco.

  El engaño consiste en que si alguien confunde esta página falsa con la original e introduce en ella sus datos personales como puedan ser el número de tarjeta o el PIN de la misma, estos números se les manda directamente a los creadores de la estafa, que consiguen así tener en su poder información que puede comprometernos.

  La manera de no caer en estas estafas es tener en cuenta que nunca los bancos ni organismos oficiales piden a través de correos electrónicos datos confidenciales. También debemos mirar con cautela las direcciones URL de las páginas visitadas, pues sucede a menudo que si la dirección real es por ejemplo www.mibanca.es, la dirección que utilizan este tipo de delincuentes para diseccionar la página será algo así como www.mibanco.es o www.misbanca.es. Es decir, la URL tiene una pequeña diferencia que a primera vista no se notará pero que obligatoriamente ha de tener.

  Hasta hace poco tiempo, este tipo de ataques solo afectaba a entidades financieras, pero actualmente estos ataques han afectado a otros organismos, como el INEM, Cámaras de Comercios de diferentes ciudades y últimamente a la Agencia Tributaria (Fig. 5.78).

  En este último caso, el ataque consiste en la remisión de un correo electrónico que informa que el receptor del mensaje tiene derecho a un reembolso de impuestos inexistentes. Pero para poder disponer del dinero, el receptor debe enviar los números de cuentas bancarias y tarjetas de crédito.

Actividades

10. El navegador Internet Explorer a partir de la versión 7 incluye la funcionalidad *filtro de suplantación de identidad.*

Para configurarlo debemos acceder a las *Opciones avanzadas* del menú de *Herramientas (Opciones de Internet).*

En la ficha de *Opciones avanzadas* podremos activar la comprobación automática de sitios web en el apartado de seguridad. De esta manera siempre que accedamos a una página comprobará su autenticidad inmediatamente.

Fig. 5.79. *Configuración momento análisis.*

Comprueba tu aprendizaje

Aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático

1. En multitud de noticias podemos leer que el despecho de los empleados dispara el robo de información en las empresas. El 28% de la sustracción de información se produce a través de las memorias externas USB. Para evitar dichos robos podemos deshabilitar estos a través de la BIOS.

   Accede a la BIOS y desactiva los dispositivos USB. Otra forma de protegernos contra dichos robos es desactivando dichos dispositivos USB a través del sistema operativo. Enumera los pasos que has realizado para desactivar dichos dispositivos a través del Sistema Operativo.

2. Spoof Guard es una herramienta que nos ayuda a discernir si estamos siendo víctimas de un ataque malintencionado de spoofing o de phising. Esta aplicación añade un semáforo en la barra de herramientas del navegador que nos indica la peligrosidad de la página.

   Descarga el programa de la página **http://crypto.stanford.edu/SpoofGuard/,** instálalo y comprueba que dependiendo de la luz del semáforo la página que visitas no ha sido atacada o por el contrario es una posible página web fraudulenta.

3. Modifica el fichero de configuración del gestor de arranque (GRUB), `menu.lst`, para que bloquee el arranque del test de memoria.

   Indica los pasos que has realizado para alcanzar el objetivo.

4. Descarga la demo de la aplicación Biopassword de **http://smartadvisors.net/biopassword/demo.php,** instálala, configúrala y comprueba que si escribe otra persona diferente a la que ha realizado el módulo de inscripción lo reconoce y produce un error diciendo que tu forma de escribir no se corresponde con el patrón registrado.

5. Descarga el antivirus AVG de **http://free.avg.com/,** instálalo y haz una comprobación del estado de tus dispositivos de almacenamiento.

Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico

6. En un pequeño colegio es necesario que los alumnos compartan los equipos de un aula de informática. Los perfiles de los alumnos que comparten el aula son:

   - Alumnos de gestión administrativa. Estos utilizan los equipos para aprender mecanografía y el paquete ofimático de Microsoft.
   - Alumnos de construcción que utilizan Autocad para la realización de planos y PRESTO para el cálculo de presupuestos.
   - Alumnos de un curso de JAVA, los cuales utilizan un compilador de dicho programa.

   Se ha observado que los alumnos del curso de JAVA se dedican a instalar juegos en los equipos de manera indiscriminada, por lo que se están viendo perjudicados sus compañeros.

   ¿Cómo podemos solventar la situación? ¿Qué medidas tomarías?

7. Esta actividad se deberá realizar en grupo. Descarga de la página web **http://www.effetech.com/download/** el programa MSN sniffer e instálalo en uno de los equipos de la red.

   Otros dos compañeros deben hacer uso del Messenger manteniendo una conversación entre ellos.

   ¿Puedes ver la conversación mantenida desde tu equipo?

   En caso de que la respuesta sea negativa ¿Por qué no puedes visualizarla? ¿Cómo podrías llegar a visualizar la conversación?

8. Descarga EffeTech HTTP Sniffer de la página Web **http://www.effetech.com/download/** e instálalo en uno de los equipos de la red.

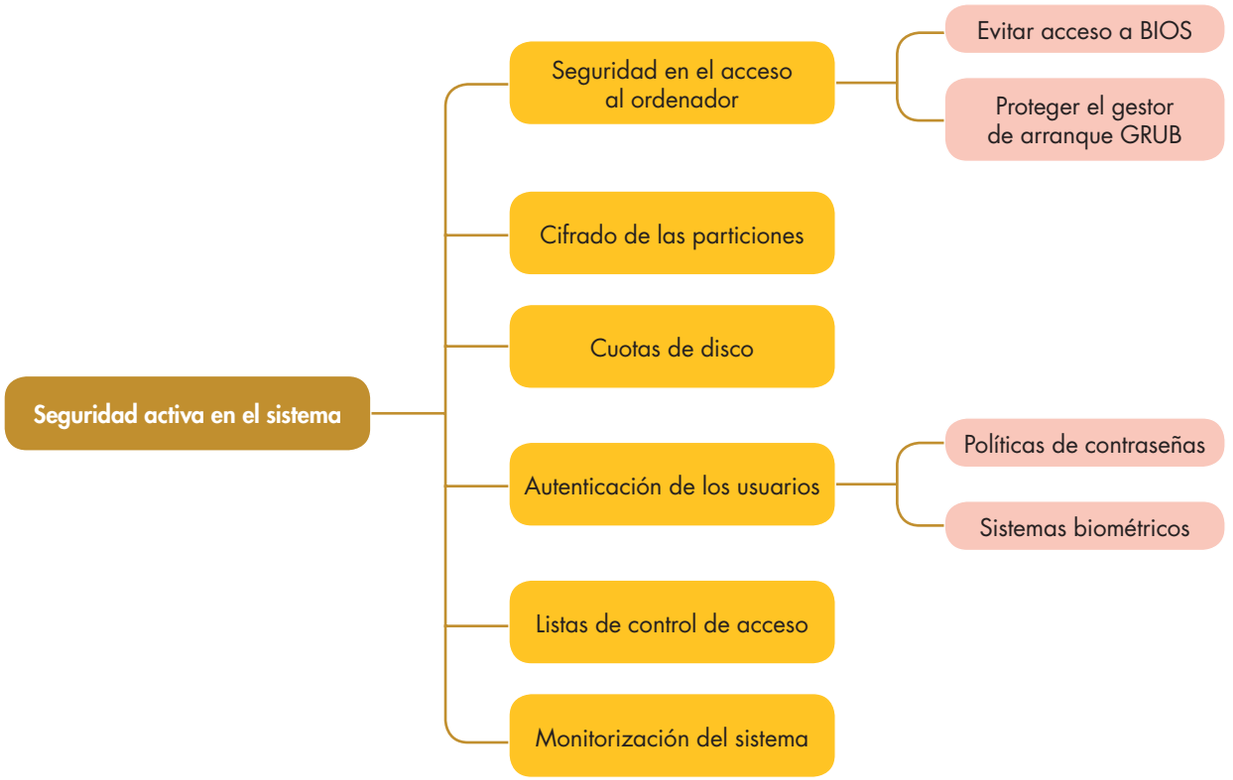
   Otro compañero debe visitar distintas páginas Web.

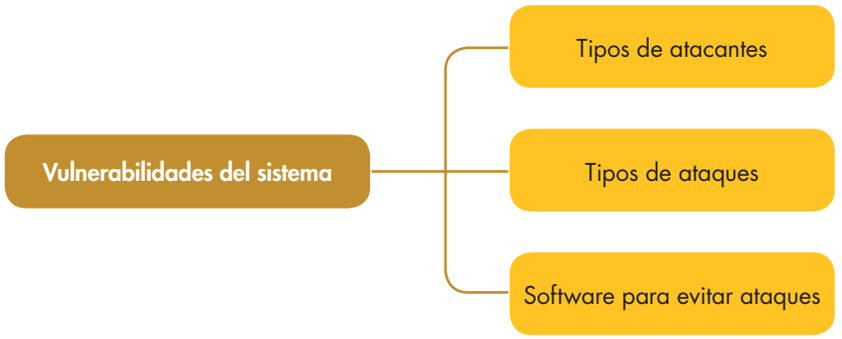
   ¿Puedes ver las páginas que visita tu compañero? En caso de que la respuesta sea negativa, ¿por qué no puedes visualizarlas? ¿Cómo podrías llegar a visualizar las páginas que visita tu compañero?

9. Captura las contraseñas de inicio de sesión de otros usuarios de tu red y envíalas al crackeador de contraseñas para más tarde intentar averiguarlas.

   ¿Qué método utilizas para averiguarlas? ¿Fuerza bruta, diccionario o Rainbow tables?

Síntesis


Seguridad activa en el sistema
Seguridad en el acceso al ordenador
Evitar acceso a BIOS
Proteger el gestor de arranque GRUB
Cifrado de las particiones
Cuotas de disco
Autenticación de los usuarios
Políticas de contraseñas
Sistemas biométricos
Listas de control de acceso
Monitorización del sistema


Vulnerabilidades del sistema
Tipos de atacantes
Tipos de ataques
Software para evitar ataques