Unidad 5

Seguridad activa: sistema operativo y aplicaciones

En esta unidad aprenderemos a:

- Proteger el software del ordenador frente a ataques de software malicioso.
- Aplicar parches de seguridad que corrigen vulnerabilidades.
- Diseñar planes de contingencia ante fallos de seguridad.
- Verificar el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.

Y estudiaremos:

- El software malicioso.
- Las herramientas de protección y desinfección.
- La política de contraseñas.
- La biometría.

1. Carrera de obstáculos

Por muchas medidas de control de acceso que pongamos, un hacker puede sentarse delante de un equipo de nuestra empresa. O directamente robar un portátil a uno de nuestros directivos. Vamos a intentar ponérselo difícil para que su «trabajo» sea una carrera de obstáculos y, seguramente, ante alguna barrera, desista.

1.1. La caja del ordenador

Lo primero es evitar que pueda abrir la **caja** del ordenador para llevarse el disco duro y «destriparlo» tranquilamente en casa. La mayoría de las cajas de los ordenadores de sobremesa llevan un par de **anclajes** donde colocar un **candado** normal. También está la opción de cambiar un tornillo normal por un tornillo con llave.

Fig. 5.1. *Candado de portátil.*

Para los portátiles tenemos el famoso candado **Kensington** (Fig. 5.1), que tiene una cabeza que se introduce por una ranura especial de la caja del portátil. La cabeza continúa en un cable de acero para que lo enrollemos en alguna parte fija (la mesa o algún anclaje especial). La cabeza puede utilizar una llave o una combinación de números.

Los candados son poco efectivos, pero por lo menos obligamos al ladrón a traer alguna herramienta más y le hacemos perder un tiempo precioso. Incluso si lo abre, la mayoría de las cajas de ordenador profesionales llevan un **detector** que graba en la memoria de la BIOS la fecha y hora en que se ha producido la apertura. Al día siguiente, cuando el empleado encienda el ordenador, aparecerá un mensaje en pantalla avisándole.

1.2. La BIOS del ordenador

Con el candado, el hacker ya no se podrá llevar el disco. Pero en la Unidad 4 hemos visto que, utilizando la técnica del arranque con **LiveCD,** montábamos tranquilamente el disco duro local y hacíamos una copia del mismo en un dispositivo externo.

Para evitar que un hacker haga lo mismo, hay que entrar en la BIOS para modificar el **orden de arranque.** Por defecto suele estar puesto primero el CD/DVD y después el disco duro local HDD (Hard Disk Drive). Debemos cambiarlo para que el primero y único sea el HDD (si algún día hace falta otra cosa, siempre podremos volver aquí).

Esta tarea se suele hacer cuando llega un nuevo equipo a la empresa. Tampoco hay que olvidar cambiar las **contraseñas del administrador,** porque si no ponemos ninguna o dejamos los valores por defecto, el hacker puede entrar a la BIOS y modificar el orden de arranque.

En algunas empresas incluso activan una **contraseña de uso** del ordenador. Es decir, al arrancar la BIOS siempre pide una contraseña, no solo cuando queremos acceder a su configuración.

Si hemos olvidado las contraseñas de la BIOS, la solución típica es retirar la **pila** que mantiene esos valores en memoria. En las placas base modernas directamente hay un **jumper** que, si está cerrado cuando el ordenador arranca, borra esos valores. Por ambos motivos (pila o jumper) hay que seguir evitando el acceso al interior de la caja del ordenador.

Actividades

1. Busca ejemplos de películas donde el espía consigue llegar hasta el ordenador del enemigo superando múltiples barreras.
2. Instala un candado Kensington.
3. Borra las contraseñas de la BIOS en algún ordenador del laboratorio.

Caso práctico 1

Poner contraseñas en la BIOS

■ **Duración:** ◷ 15 minutos ■ **Dificultad:** ☺ Fácil

Objetivo. Vamos a poner contraseña de administrador y contraseña de usuario.

Material. Ordenador con BIOS con capacidad de fijar claves para administración y usuario.

1. Arrancamos el ordenador y pulsamos la tecla que nos da acceso a la configuración de la BIOS. Dependiendo del ordenador, puede ser **Esc, Supr, F2,** etc.
2. Una vez dentro, buscamos el menú donde se gestionan las contraseñas. En este caso está bajo *Security* (Fig. 5.2).

Fig. 5.2. *Menú de seguridad de la BIOS.*

3. Entramos en *Admin Password* para cambiar la clave de administrador (Fig. 5.3). Esta clave bloquea toda la configuración: para cambiar cualquier cosa importante habrá que introducirla.

Fig. 5.3. *Clave de administrador.*

4. Vamos a cambiar también la clave de usuario, aquí llamada *System Password* (Fig. 5.4). Esta clave permite utilizar el ordenador pero no modificar la configuración de la BIOS.

Fig. 5.4. *Clave de usuario.*

5. Aplicamos los cambios y la máquina se reinicia. Desde ahora nos aparecerá una pantalla donde se nos solicita la clave de usuario o clave de administrador para poder seguir (Fig. 5.5).

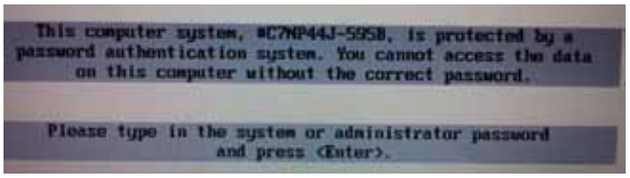

Fig. 5.5. *Nos pide la clave.*

Caso práctico 2

Fijar orden de dispositivos de arranque

■ **Duración:** ◷ 10 minutos ■ **Dificultad:** ☺ Fácil

Objetivo. Aprender a establecer la lista de dispositivos de arranque que nos convenga en cada momento.

Material. Ordenador con BIOS con capacidad de cambiar el orden de arranque.

1. Entramos en la BIOS pulsando la tecla adecuada y buscamos la opción del menú que se refiere al orden de dispositivos de arranque. En nuestro caso es *Boot sequence*. Seguimos las instrucciones para dejar únicamente el disco duro y así evitar los LiveCD (Fig. 5.6).

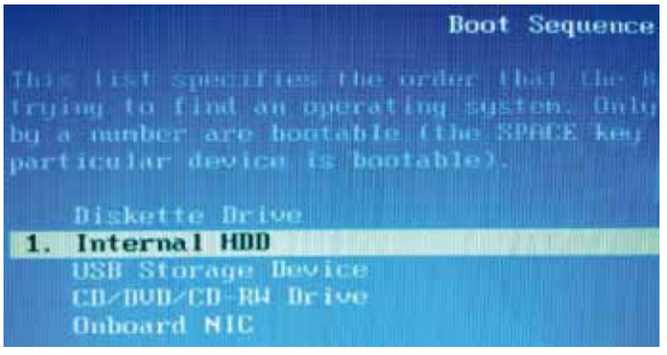

Fig. 5.6. *Dejamos únicamente el disco duro.*

(Continúa)

Caso práctico 2

(Continuación)

2. Podemos arrancar y, efectivamente, no busca en otros dispositivos, sino que va directamente al disco. Pero en las BIOS hay una opción para, puntualmente, evitar la lista de dispositivos de arranque. En nuestro ejemplo se consigue pulsando **F12** durante el arranque de la máquina. Aparece un menú que nos ofrece todos los dispositivos disponibles (Fig. 5.7).

Fig. 5.7. *Podemos arrancar desde cualquiera.*

3. Por tanto, nuestro deseo de evitar los LiveCD no se ha cumplido. Pero en esta BIOS, si activamos una clave de administrador (siguiendo los pasos del caso práctico 1), la lista de dispositivos de **F12** se limita a los fijados en la lista normal (Fig. 5.8).

Fig. 5.8. *Únicamente la lista normal.*

4. Si en este menú alguien elige *BIOS Setup* e intenta cambiar el orden de arranque, se lo impide la protección de la contraseña de administrador (Fig. 5.9).

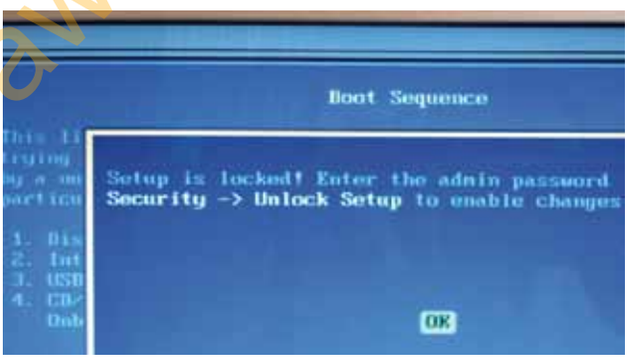

Fig. 5.9. *Protegida la secuencia de arranque.*

Actividades

4. Las contraseñas nunca deben estar en claro en un fichero de texto. Repite el caso del boot manager utilizando cifrado.

1.3. El boot manager

Ya hemos conseguido que el hacker no se pueda llevar nada y solo arranque la máquina desde nuestro disco local. En este disco puede ocurrir que tengamos instalados varios sistemas operativos (o varias versiones del mismo sistema, como suele ocurrir en Linux), de manera que, al arrancar, un programa llamado **boot manager** (gestor de arranque) nos permite elegir uno de ellos. Ahora hay que establecer quién accede a cada opción.

Caso práctico 3

Proteger el boot manager en Linux

■ **Duración:** 🕒 20 minutos ■ **Dificultad:** 😐 Media

Objetivo. Configurar el boot manager de Linux para protegerlo.

Material. Ordenador con Linux.

1. Generalmente, los sistemas Linux se instalan con un gestor de arranque. Si no es nuestro caso, lo instalaremos con `apt-get install grub2`. El gestor de arranque nos ofrecerá varias opciones (Fig. 5.10).

(Continúa)

Caso práctico 3

(Continuación)

Fig. 5.10. *Gestor de arranque.*

2. Podemos utilizar las flechas del teclado para elegir una opción. Entonces pulsaremos **Enter** para ejecutarla. Si no pulsamos nada, a los pocos segundos se lanza una de ellas que ha sido configurada como opción por defecto.

3. Como aparece en el mensaje de la parte inferior de la pantalla, pulsando e podemos entrar en el detalle de los comandos que se van a ejecutar para arrancar con esa opción (Fig. 5.11). Esto es un primer defecto de seguridad, porque el hacker puede alterarlo como quiera para evitar la seguridad del sistema operativo que arrancará.

Fig. 5.11. *Opciones de arranque.*

4. Vamos a proteger las dos primeras entradas referidas al sistema Ubuntu. Entramos en el Linux con privilegios de administrador y editamos el fichero /etc/grub.d/10_linux. Vemos que es un shell script y buscamos la línea que tenía el nombre del sistema (texto `Ubuntu, con Linux`). Donde pone `menuentry` añadimos `--users profesor` para la opción `recovery _ mode` y `--users profesor,alumno` para la opción normal (Fig. 5.12).

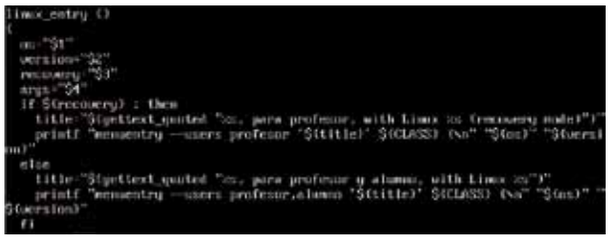

Fig. 5.12. *Modificamos opciones del menú.*

5. Esto hace que las opciones solo puedan ser ejecutadas por los usuarios profesor y alumno. Estos usuarios los definimos en el fichero /etc/grub.d/40_custom. Ponemos en cada línea el comando `password` junto con el nombre del usuario y la contraseña. Vamos a crear tres: `profesor`, `alumno` y `hacker`. También creamos una variable `superusers` que contiene el nombre de los usuarios con permisos para modificar las entradas del menú (Fig. 5.13).

Fig. 5.13. *Usuarios definidos.*

6. Salvamos los ficheros modificados y ejecutamos el comando `update-grub` para reflejar los cambios en el fichero /boot/grub/grub.cfg. Al arrancar de nuevo, el menú ha cambiado y el control de acceso está activado (Fig. 5.14). En la primera opción podrán entrar `profesor` y `alumno`, y en la segunda, solo `profesor`. El tercer usuario, `hacker`, no puede entrar en ninguna.

Fig. 5.14. *Menú modificado.*

7. Por si nos hemos equivocado y el sistema no arranca, conviene tener a mano un LiveCD para entrar a la máquina, montar el disco duro y modificar el `grub.cfg` para recuperar el control.

1.4. Cifrado de particiones

Con las barreras que hemos puesto hasta ahora, el hacker no se puede llevar nada; solo puede arrancar desde el disco local y solo puede elegir alguna de las entradas del boot manager. Pero si alguna de estas medidas falla, todavía podemos evitar que acceda a nuestros datos: vamos a **cifrar el contenido,** de manera que sea ilegible.

Caso práctico 4

Cifrar la partición de arranque con TrueCrypt

■ **Duración:** 🕒 45 minutos ■ **Dificultad:** ☺ Fácil

Objetivo. Utilizar cifrado en la partición de arranque para evitar el acceso no autorizado.

Material. Ordenador con Windows 2008 Server.

1. Entramos al servidor y descargamos el software desde la web de TrueCrypt **(www.truecrypt.org).** Una vez descargado, procedemos a instalarlo (Fig. 5.15).

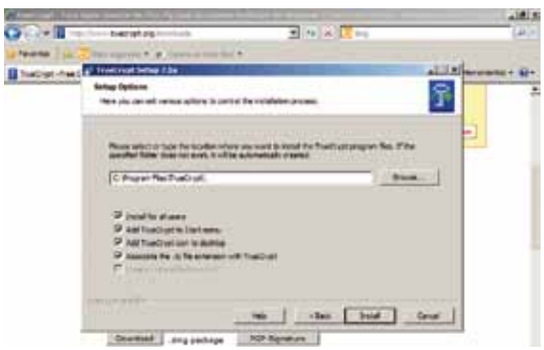

Fig. 5.15. *Instalación de TrueCrypt.*

2. En la ventana principal de la herramienta se nos permite crear un nuevo volumen. Al pulsarlo aparece un asistente. El primer paso consiste en decidir si vamos a crear un contenedor (una unidad completa en un solo fichero cifrado), si queremos cifrar un disco duro que no tiene el sistema operativo o cifrar el disco del sistema operativo. Elegimos la tercera opción (Fig. 5.16).

Fig. 5.16. *Elegimos cifrar el disco del sistema.*

3. El siguiente paso nos pregunta si queremos un cifrado de sistema normal u oculto. No necesitamos tanta seguridad: elegimos normal (Fig. 5.17).

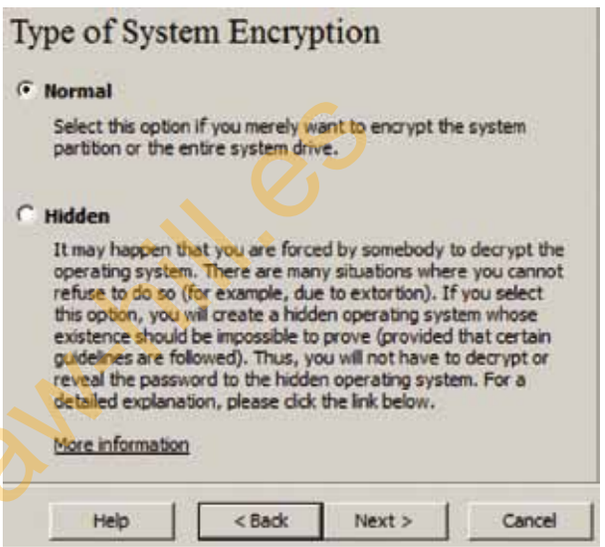

Fig. 5.17. *Cifrado de sistema normal.*

4. Después nos pregunta si queremos cifrar solo la partición de Windows o todo el disco. Para tener control total, elegimos el disco (Fig. 5.18)

Fig. 5.18. *Ciframos todo el disco.*

5. La siguiente pregunta nos avisa de que en el final del disco algunos controladores dejan información importante. Por precaución, elegimos no cifrarlo (Fig. 5.19).

(Continúa)

Caso práctico 4

(Continuación)

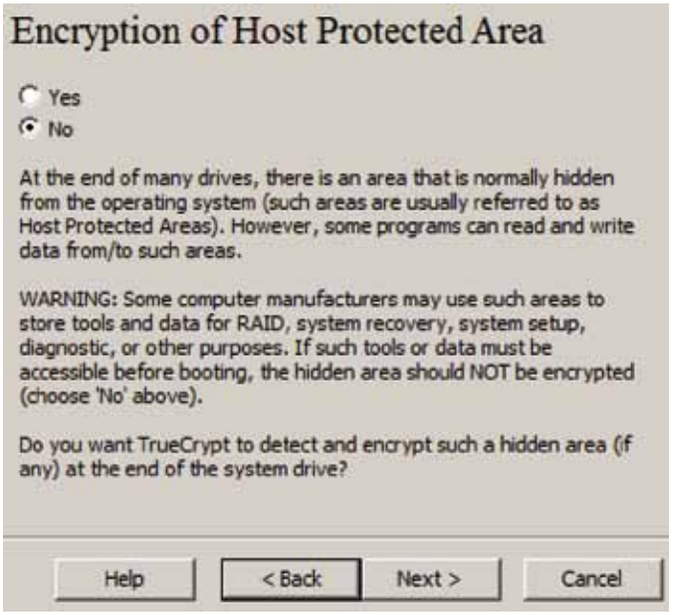

Fig. 5.19. *No cifraremos el final del disco.*

6. Ahora nos pregunta por el tipo de arranque de ese disco. En nuestro caso es un único sistema operativo (Fig. 5.20).

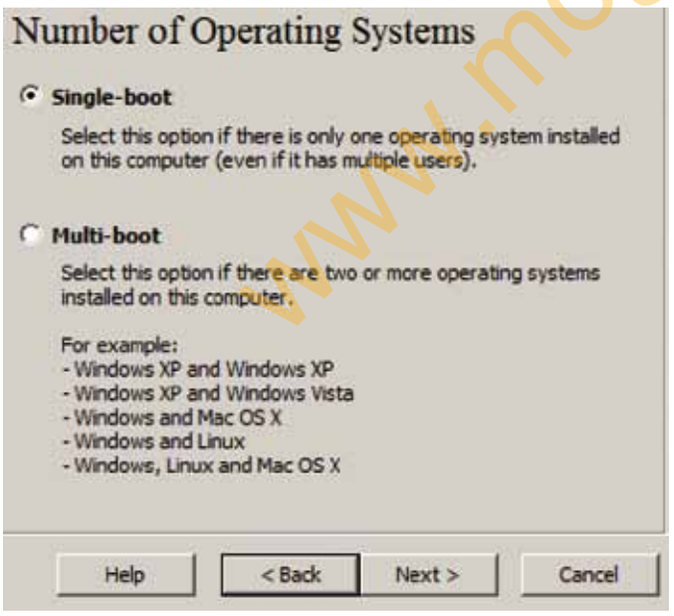

Fig. 5.20. *Tipo de arranque.*

7. Por fin llegamos a las opciones de cifrado. Según las necesidades de la empresa, elegiremos un algoritmo más potente. En nuestro caso lo dejamos en AES y RIPEMD-160 (Fig. 5.21).

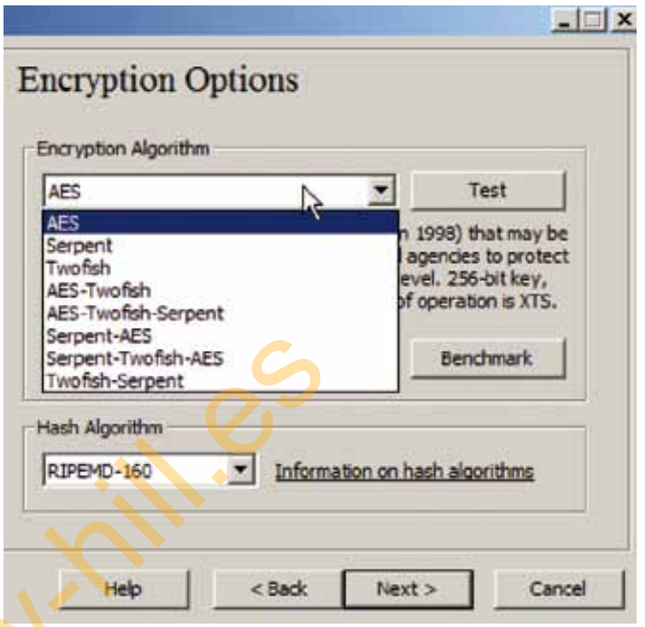

Fig. 5.21. *Opciones de cifrado.*

8. La siguiente pregunta es importante porque nos pide la clave de cifrado (Fig. 5.22). Esta clave será la que nos pedirá la máquina en cada arranque. Como ya sabemos, debe ser fácil de recordar para nosotros y difícil de adivinar para cualquier otra persona.

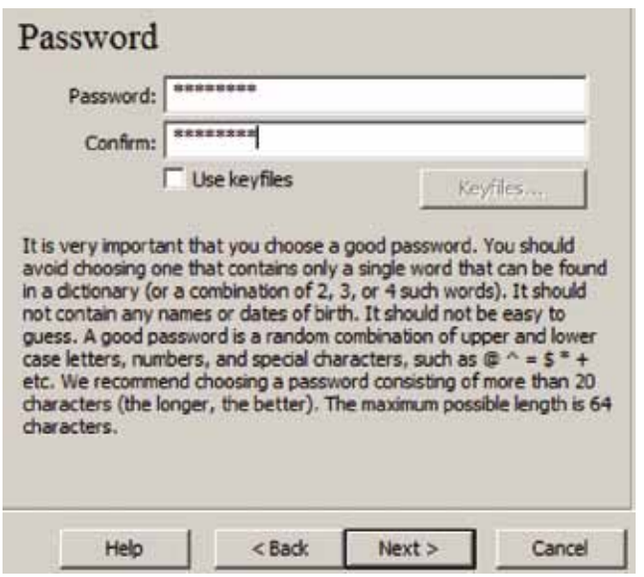

Fig. 5.22. *Clave de cifrado.*

9. El siguiente paso genera aleatoriedad en las claves del algoritmo criptográfico para mejorar la seguridad (Fig. 5.23).

(Continúa)

Caso práctico 4

(Continuación)

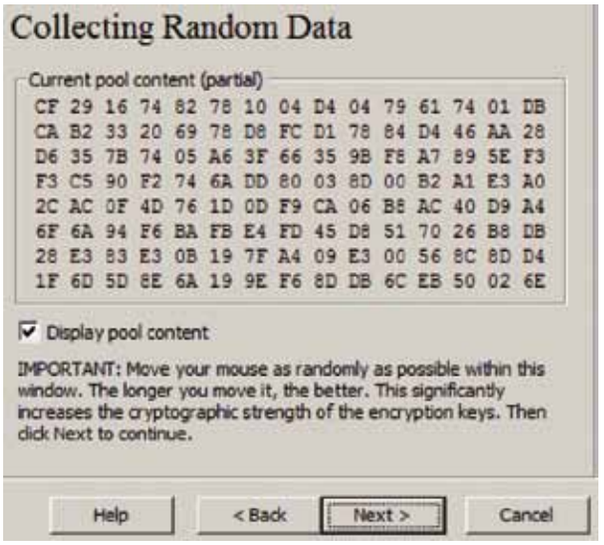

Fig. 5.23. *Generación de aleatoriedad.*

10. El siguiente paso nos muestra las claves obtenidas con la aleatoriedad generada en el paso anterior (Fig. 5.24). Si aparece vacío, habría que volver al paso anterior para repetirlo.

Fig. 5.24. *Claves generadas.*

11. Pulsando *Next* aparece la siguiente ventana, que es muy importante porque nos genera el disco de rescate. Estamos a punto de cifrar todo el disco e instalar un programa en el arranque para descifrar y acceder al sistema. Si el arranque del disco duro se dañara, no podríamos acceder al programa que descifra y tampoco al sistema. Para remediarlo, en este momento el TrueCrypt nos genera un fichero .iso para que lo grabemos en un CD con el que arrancar el sistema (Fig. 5.25).

Fig. 5.25. *Disco de rescate.*

12. Una vez creado, nos avisa de que debemos grabarlo (Fig. 5.26), y el programa no continúa hasta que detecte que hemos utilizado la grabadora de CD.

Fig. 5.26. *Debemos grabar el disco de rescate.*

13. Si vamos a ese directorio, podemos comprobar que el fichero está ahí (Fig. 5.27).

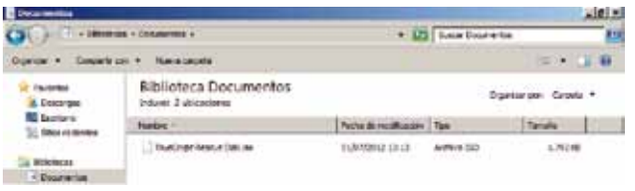

Fig. 5.27. *Fichero .iso del disco de rescate.*

(Continúa)

Caso práctico 4

(Continuación)

14. Cuando terminamos la grabación, el programa nos permite seguir (Fig. 5.28).

Fig. 5.28. *Podemos seguir.*

15. La siguiente opción se refiere al proceso de cifrado inicial. Como estamos hablando de alta seguridad, TrueCrypt permite reforzar este proceso. En nuestro caso no necesitamos seguridad militar y elegimos *None* (Fig. 5.29).

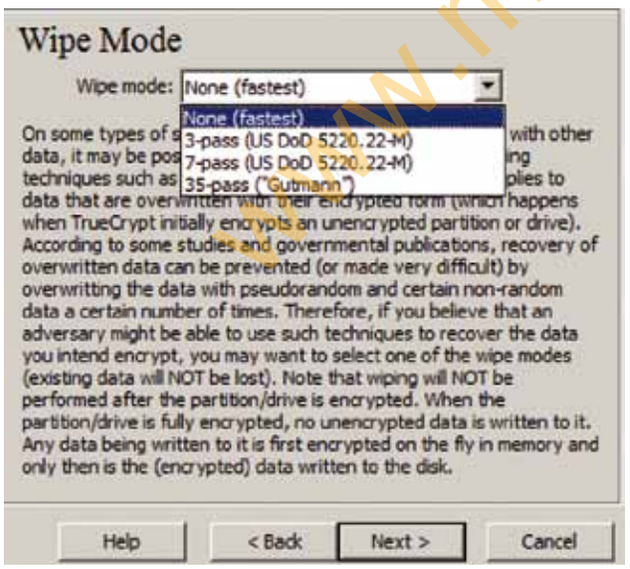

Fig. 5.29. *Tipo de cifrado inicial.*

16. Como estamos cifrando la unidad del sistema, para estar seguros de que todo va a ir bien, el siguiente paso hace una simulación del nuevo gesto de arranque (Fig. 5.30).

Fig. 5.30. *Simulación de nuevo arranque.*

17. Si todo ha ido bien, estamos listos para hacer el cifrado (Fig. 5.31). Nos avisa de que una pérdida de alimentación eléctrica puede dejar inservible el disco.

Fig. 5.31. *Listos para cifrar.*

18. Pulsamos *Encrypt* y empieza el cifrado (Fig. 5.32). La duración de este proceso depende del tamaño del disco y su velocidad.

Fig. 5.32. *Cifrado en curso.*

(Continúa)

Caso práctico 4

(Continuación)

19. Al final aparecerá una ventana de confirmación (Fig. 5.33).

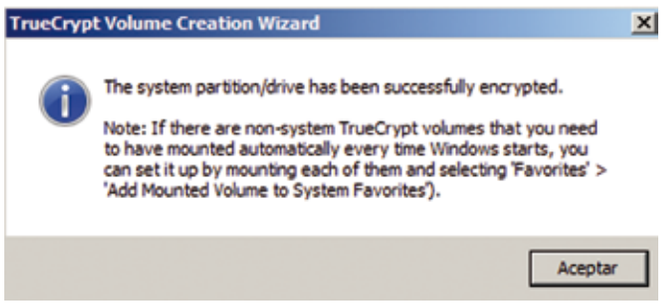

Fig. 5.33. *Cifrado completado.*

20. Ahora, cada vez que arranquemos el sistema, nos aparecerá el boot loader de TrueCrypt, que nos pide la contraseña para descifrar la unidad y acceder al sistema operativo (Fig. 5.34).

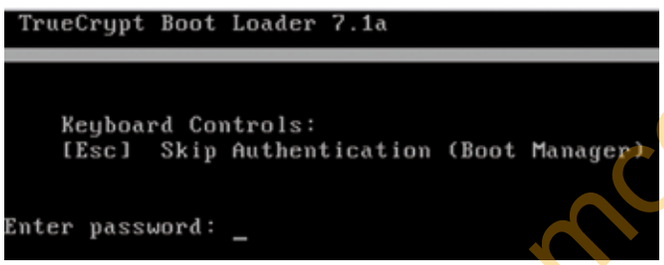

Fig. 5.34. *Boot loader de TrueCrypt.*

21. Si nos equivocamos, no tenemos acceso al sistema (Fig. 5.35).

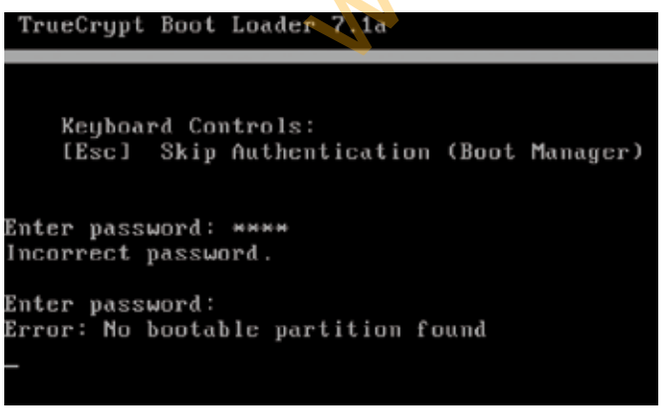

Fig. 5.35. *Acceso incorrecto.*

22. Si arrancamos con un LiveCD e intentamos montar alguna de las particiones del disco duro, no podemos (Fig. 5.36).

Fig. 5.36. *Particiones protegidas.*

23. Vamos a arrancar desde CD, pero ahora con el disco de rescate. Nos aparece un menú (Fig. 5.37).

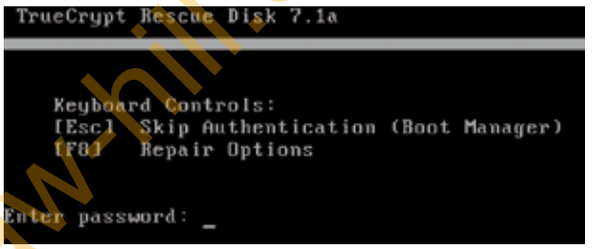

Fig. 5.37. *Menú del disco de rescate.*

24. En las opciones de reparación podemos descifrar o intentar reparar el gestor de arranque (Fig. 5.38).

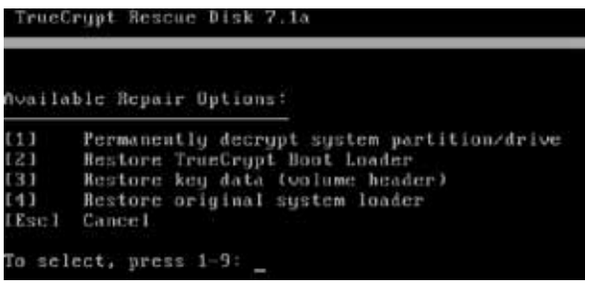

Fig. 5.38. *Opciones de reparación.*

25. En cualquier caso, siguiendo la estrategia «algo que tienes, algo que sabes», siempre nos pedirá la contraseña de cifrado (Fig. 5.39).

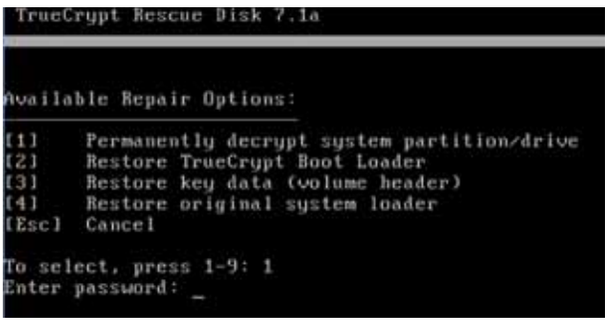

Fig. 5.39. *Pide la contraseña de cifrado.*

2. Autenticación en el sistema operativo

Hemos conseguido que nuestro hacker no pueda evitar que la máquina arranque con un sistema operativo instalado por nosotros. Comparado con lo que hemos visto hasta ahora (BIOS, boot manager), los sistemas operativos permiten incluir mucho más **software de autenticación** y más complejo. Veremos múltiples mecanismos para asegurarnos de que nuestro sistema solo lo usa quien está autorizado para ello.

Importante

No hay que hacer la vida imposible a los usuarios. Poner muchas contraseñas (BIOS, cifrado de partición, gestor de arranque, usuario del sistema operativo) y ponerlas difíciles (muchos caracteres, caracteres especiales) probablemente les lleve a tenerlas todas apuntadas en un papel sobre el teclado.

2.1. Usuario/password

Es el mecanismo más típico. Aplicando la estrategia «algo que sabes», la pantalla inicial del sistema espera que la persona introduzca el nombre de un **usuario** y la **contraseña** asociada a ese usuario. Mientras lo teclea, el nombre del usuario es visible pero la contraseña no (se suele sustituir por asteriscos, guiones, etc.), para evitar que la vea alguien que se encuentre a nuestra espalda.

Si nos equivocamos, bien porque el usuario no existe, bien porque la contraseña no es la correcta, el sistema nos impide la entrada y nos deja intentarlo de nuevo. En algunos sistemas nos ofrece una **pista** sobre la contraseña (si la pusimos la última vez que cambiamos la contraseña), y la mayoría tiene un **límite de intentos.** Alcanzado ese límite, el sistema se puede bloquear durante un tiempo o definitivamente (por ejemplo, los móviles tienen un límite de tres intentos para introducir el PIN). Con este límite evitamos ataques de fuerza bruta que prueben una a una todas las combinaciones de letras, números y caracteres especiales.

Caso práctico 5

Cambiar contraseña del propio usuario y de otros en Windows y Linux

■ **Duración:** 10 minutos ■ **Dificultad:** Fácil

Objetivo. Manejar el cambio de contraseñas.

Material. Ordenador con Windows 7 y Linux.

1. En Windows 7 entramos en una cuenta de administrador y vamos al panel de control. Una vez allí elegimos *Cuentas de usuario* y aparecerá nuestra cuenta. Elegimos *Cambiar la contraseña* (Fig. 5.40).

Fig. 5.40. *Cambiar la contraseña propia en W7.*

2. Nos pide la contraseña actual (puede que hayamos salido sin cerrar la sesión y alguien se ha sentado en nuestro sitio) y la nueva dos veces. También podemos añadir un indicio de contraseña, que es una pregunta que, si damos la respuesta correcta, nos recupera la contraseña cuando la hemos olvidado.
3. Como somos administradores podemos cambiar la contraseña de otros usuarios (Fig. 5.41). En este caso no nos pregunta la clave anterior porque podemos (y debemos) ignorarla. De nuevo, hay que introducirla dos veces para reducir la posibilidad de error y podemos introducir un indicio de contraseña para recuperarla fácilmente.

Fig. 5.41. *Cambiar la contraseña de otro usuario.*

4. En un sistema Linux podemos usar el comando `passwd`. Si no ponemos ningún parámetro, cambia la contraseña de nuestro usuario; si ponemos como parámetro el nombre de otro usuario, cambia su contraseña (por supuesto, necesitamos hacerlo desde un usuario con privilegios de administración del sistema).

Para poner las cosas más difíciles a los hackers, una buena medida es **cambiar el nombre por defecto** de los usuarios con más privilegios sobre el sistema. Así no solo tendrán que aplicar la fuerza bruta sobre la contraseña, sino también sobre el nombre del usuario. Por ejemplo, en los primeros sistemas Unix se trabajaba desde el usuario root con todos los privilegios (superusuario); en la actualidad, aunque el usuario root sigue existiendo, el sistema no permite usarlo para entrar al sistema; en cambio, los privilegios se administran mediante el mecanismo sudo, como veremos más adelante.

Aun así, siempre conviene utilizar **contraseñas no triviales:** palabras que no aparezcan en el diccionario de ninguna lengua, combinar letras mayúsculas con minúsculas, números, signos de puntuación, etc. Y **cambiar la contraseña regularmente,** porque no sabemos cuánto tiempo llevan intentando atacarla. Los sistemas operativos permiten obligar al usuario a cumplir todas estas normas, como veremos en el caso práctico 6.

Caso práctico 6

Cambiar restricciones de contraseñas en Windows 2008

■ **Duración:** 15 minutos ■ **Dificultad:** Fácil

Objetivo. Aprender a adaptar las restricciones de contraseñas.

Material. Ordenador con Windows 2008.

1. Entramos en el sistema con un usuario administrador. Pulsamos **Inicio** y buscamos las directivas de seguridad local introduciendo la palabra *dire* (Fig. 5.42).

Fig. 5.42. *Buscamos la herramienta de directivas de seguridad local.*

2. Una vez dentro, en el menú de la derecha navegamos por *Configuración de seguridad > Directivas de cuentas > Directivas de contraseñas*. En la parte derecha aparecen los valores que podemos cambiar (Fig. 5.43).

Fig. 5.43. *Directivas sobre contraseñas.*

3. Vamos a probar a cambiar la longitud mínima. La ponemos en ocho, aplicamos el cambio y a continuación intentamos poner una contraseña de siete caracteres. El sistema nos lo impide (Fig. 5.44).

Fig. 5.44. *Control de longitud de contraseña.*

Actividades

5. Busca alguna web para medir la fortaleza de una contraseña.

6. Investiga qué es un keylogger y cómo nos puede afectar.

7. ¿Por qué, para entrar, los sistemas Windows obligan a pulsar **Ctrl+Alt+Supr,** y por qué son precisamente esas teclas?

2.2. Tarjetas

En algunas ocasiones, el mecanismo de usuario y contraseña no es suficiente: es **inseguro** (alguien puede espiar qué teclas pulsamos) o simplemente **molesto** (por ejemplo, en los tornos de acceso a la entrada de la empresa no podemos perder el tiempo tecleando). Para estos casos aplicaremos la estrategia «algo que tienes» y repartiremos tarjetas entre los usuarios. Por ejemplo, los cajeros automáticos de los bancos aplican una seguridad doble: la tarjeta más un número PIN.

Las tarjetas son de dos tipos: sencillas (magnéticas, RFID) o complejas (chip). Las magnéticas van desapareciendo porque las RFID son igual de baratas y no sufren borrados accidentales (en Londres y Madrid ya se utilizan para el abono de transporte).

Las tarjetas con chip son más seguras pero más caras, por lo que se utilizan en ocasiones especiales. 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.

2.3. Biometría

La seguridad del mecanismo usuario/contraseña es suficiente para la mayoría de las aplicaciones. La tarjeta es cómoda. Pero cualquiera podría sentarse en nuestro ordenador, insertar nuestra tarjeta (robada o duplicada), introducir nuestro usuario y contraseña (nos puede haber espiado, o se la dijimos al irnos de vacaciones) y acceder al sistema como si fuéramos nosotros mismos. Si la información que manejamos es importante, aplicaremos la estrategia «algo que eres», para complementar el mecanismo usuario/contraseña con un control más: la biometría.

La **biometría** consiste en identificar alguna característica **física** del sujeto: la huella dactilar, el ojo, la voz (Fig. 5.45). La persona o personas autorizadas deben grabar primero su característica física. Por ejemplo, en la huella se graban dedos de las dos manos, por si se sufre un accidente en una de ellas. Después, cada vez que quieran utilizar el ordenador, deberán situar el dedo encima del sensor.

Como hemos dicho antes, el control biométrico no es sustitutivo del usuario/contraseña, sino complementario: conviene tener los dos para **aumentar la seguridad** (estrategia «algo que sabes, algo que eres»). Aunque en algunas ocasiones sí se utiliza individualmente para ahorrar la molestia de estar pulsando teclas: por ejemplo, para acceder a alguna zona vip de la empresa.

Fig. 5.45. *Sistemas de biometría.*

Actividades

8. Investiga cómo funcionan las tarjetas RFID.

9. En la película *Gattaca* (1997) el acceso a la academia aplicaba un control biométrico. Investiga en qué consistía y qué hacía el protagonista para engañarlo.

10. En la película *Los vengadores* (2012) también había un control biométrico. Investiga cómo consiguió evitarlo Loki.

11. Busca aplicaciones de control de acceso biométrico en Android. ¿Son reales?

Caso práctico 7

Control de acceso biométrico en Windows 7

■ **Duración:** 15 minutos ■ **Dificultad:** Fácil

Objetivo. Configurar el control de acceso por huella digital.

Material. Ordenador HP con Windows 7 y dispositivo lector de huellas digitales.

1. Identificamos en el ordenador el lector de huellas digitales. En este ejemplo es un portátil (Fig. 5.46).

Fig. 5.46. *Lector de huellas digitales.*

2. En la pantalla inicial el sistema nos avisa de que todavía no está preparado para reconocer ninguna huella (Fig. 5.47).

Fig. 5.47. *El sistema todavía no está preparado.*

3. Vamos a configurarlo. Entramos al sistema con el mecanismo habitual (usuario/clave) y lanzamos la herramienta HP Security Manager (Fig. 5.48).

Fig. 5.48. *Herramienta HP Security Manager.*

4. En la ventana principal elegimos *Registrar credenciales* (Fig. 5.49). Nos aparece un gestor de credenciales.

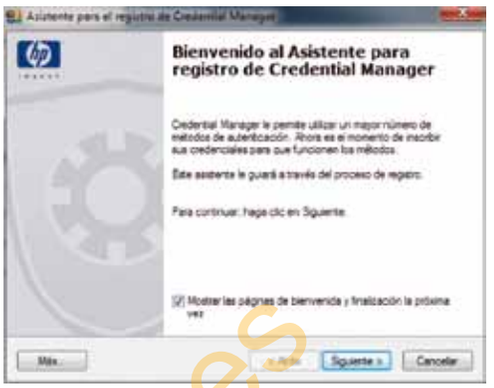

Fig. 5.49. *Registrar credenciales.*

5. Empieza un asistente cuyo primer paso es pedirnos que establezcamos una contraseña para proteger el acceso al propio gestor (Fig. 5.50).

Fig. 5.50. *Protegemos el acceso al gestor.*

6. A continuación nos pide que pasemos el dedo por el lector para grabar nuestras huellas (Fig. 5.51). La herramienta nos permite elegir el dedo que queremos registrar.

Fig. 5.51. *Grabamos las huellas.*

(Continúa)

Caso práctico 7

(Continuación)

7. Debemos registrar dos dedos. Si todo ha ido bien, aparecerá una ventana de confirmación (Fig. 5.52).

Fig. 5.52. *Grabado completado.*

8. Finalmente nos pregunta si queremos utilizar esta credencial para acceder a Windows (Fig. 5.53). Si aceptamos, bastará con deslizar nuestro dedo por el lector para entrar sin introducir usuario ni contraseña.

Fig. 5.53. *Usar huellas para entrar a Windows.*

2.4. 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 permiso 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.

Pero hay determinadas situaciones (instalación de nuevos programas, modificación de parámetros del sistema) 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.

En cuanto al usuario, dependiendo de la configuración del sistema, simplemente aparecerá una ventana de confirmación o nos pedirá una nueva autenticación.

Actividades

12. ¿Se te ocurre algún peligro en el mecanismo de elevación de privilegios de Windows?

13. En Windows, los usuarios limitados pueden instalar algunos programas, como Google Chrome, pero cuando lo hacen en Windows 7, en un momento concreto del proceso de instalación el sistema solicita elevación de privilegios. En cambio, con XP no ocurre. ¿Por qué?

Caso práctico 8

Elevación de privilegios en Windows 7

■ **Duración:** 10 minutos ■ **Dificultad:** Fácil

Objetivo. Ejecutar una aplicación con elevación de privilegios.

Material. Ordenador con Windows 7.

1. Nos presentamos en el sistema con un usuario limitado (no administrador) y lanzamos una ventana de comandos (*Inicio > cmd* o *Inicio > Todos los programas > Accesorios > Símbolo del sistema*). Si introducimos el comando `netstat -an` para ver todas las conexiones, se ejecuta con normalidad. Pero si añadimos el parámetro `b` para mostrar el programa asociado a cada conexión, el sistema nos avisa de que necesitamos más privilegios (Fig. 5.54).

Fig. 5.54. *Necesitamos privilegios.*

2. Salimos de esa ventana y volvemos a lanzar la ventana de comandos, pero ahora no pulsamos directamente el botón izquierdo, sino el derecho, para poder elegir *Ejecutar como administrador* (Fig. 5.55).

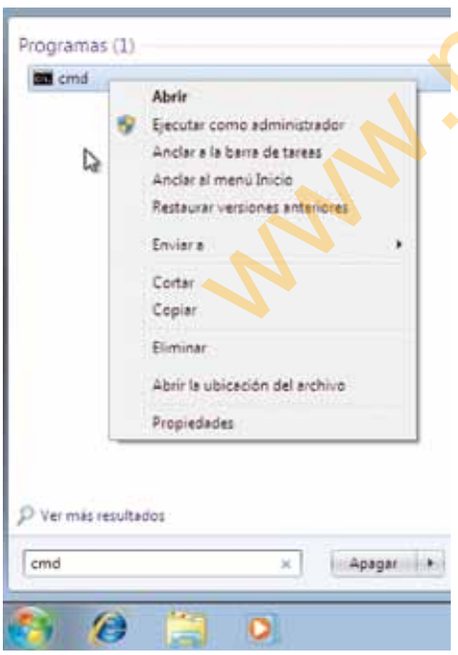

Fig. 5.55. *Solicitamos elevación.*

3. El sistema nos contesta solicitando una nueva autenticación para proceder a la ejecución. Nos ofrece el nombre de un usuario administrador y nos pregunta por su clave (Fig. 5.56).

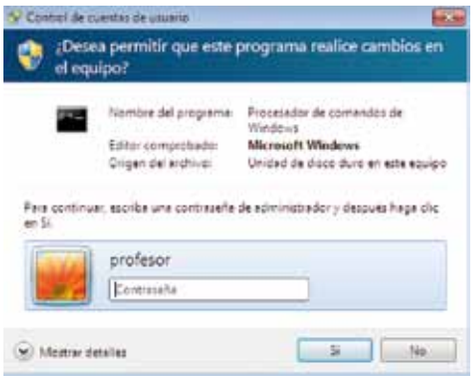

Fig. 5.56. *Autenticación puntual.*

4. Si la introducimos correctamente, aparecerá la ventana de comandos y podremos ejecutar el comando `netstat -abn` y cualquier otro, como `chkdsk`. Pero si cerramos esa ventana y la intentamos abrir de nuevo como administrador, nos pedirá de nuevo la contraseña.

5. Este proceso se repite en cualquier menú o botón de Windows donde aparezca un escudo a la izquierda; indica que esa operación necesita elevación de privilegios. Por ejemplo, si abrimos el desfragmentador de disco *(Inicio > desfrag)* la ventana se abre, pero cualquier operación posterior solicitará elevación (Fig. 5.57).

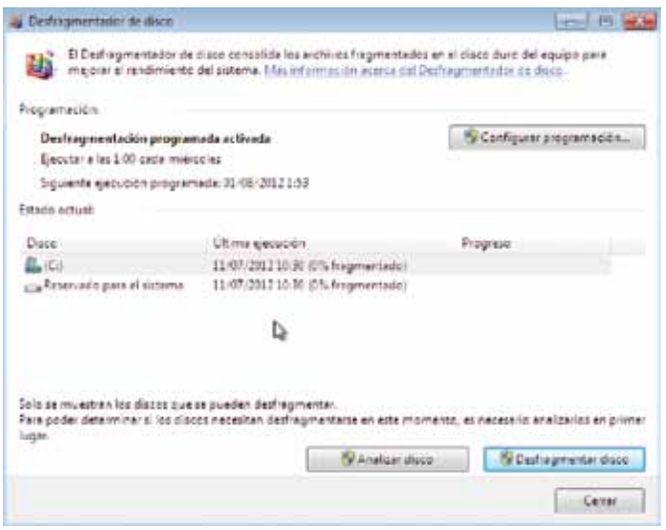

Fig. 5.57. *Operaciones con elevación.*

6. Salgamos del usuario limitado y entremos con el usuario administrador. Podemos repetir los pasos anteriores y la única diferencia será que ya no nos pregunta por la contraseña (hemos entrado con un usuario administrador). Simplemente nos avisa de que vamos a realizar algo potencialmente peligroso.

Caso práctico 9

Elevación de privilegios en Linux

■ **Duración:** 🕒 10 minutos ■ **Dificultad:** 😐 Media

Objetivo. Elevar privilegios de un usuario normal usando `sudo`.

Material. Ordenador con Linux Ubuntu Server 12.04.

1. Entramos al sistema con un usuario registrado (por ejemplo, el usuario al que dimos nombre durante la instalación del sistema). Abrimos una shell y ejecutamos el comando `fdisk -l /dev/sda`. Nos aparecerá un mensaje de error porque no tenemos privilegios suficientes.
2. Ejecutamos el comando `sudo -i`. Seguramente nos pedirá de nuevo nuestra contraseña. Si la introducimos correctamente, estaremos ejecutando una nueva shell con permisos de administrador (Fig. 5.58). Ahora sí funciona el comando anterior.

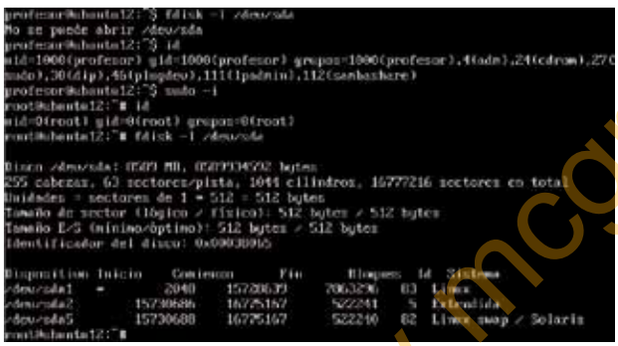

Fig. 5.58. *Elevación de privilegios mediante sudo.*

3. El comando `sudo` permite ejecutar con privilegios el comando que pongamos a continuación (por ejemplo, `sudo fdisk -l /dev/sda`). Si vamos a ejecutar varios comandos, es más cómodo utilizar `sudo -i`.
4. Esto ha funcionado porque nuestro usuario cumple alguna de las condiciones que se configuran en el fichero /etc/sudoers. En este fichero se pueden establecer limitaciones para un usuario concreto o para un grupo de usuarios. Las limitaciones pueden ser comandos concretos o todos. En nuestro caso se ha aplicado que nuestro usuario pertenece al grupo `sudo`, y este grupo tiene todos los comandos disponibles. En el fichero aparece esta línea:

   ```
   %sudo ALL=(ALL:ALL) ALL
   ```

5. Vamos a crear un usuario nuevo llamado `limitado`. Lo podemos hacer desde la misma ventana donde tenemos el `sudo -i` con los comandos:

   ```
   # useradd limitado
   # passwd limitado
   ```

6. Si entramos en el sistema con el nuevo usuario e intentamos el `fdisk -l /dev/sda`, fallará. Pero si intentamos el `sudo -i`, no solo falla, sino que advierte de que avisará al administrador (Fig. 5.59).

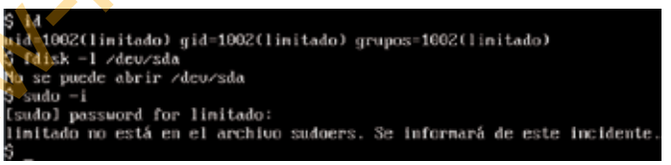

Fig. 5.59. *Elevación no permitida.*

7. En efecto, si volvemos a la sesión con privilegios y vemos las últimas líneas del fichero /var/log/auth.log, ahí aparecerá el intento fallido, junto con la fecha y la hora en la que lo hemos hecho.
8. Podemos permitir que el usuario `limitado` pueda hacer `sudo` solo con incluirlo en el grupo `sudo`. Por ejemplo, en la sesión de administrador ejecutamos el comando:

   ```
   # usermod -G sudo limitado
   ```

   La próxima vez que `limitado` entre al sistema ya podrá utilizar el mecanismo `sudo`.

En el caso práctico 8 hemos visto que, aunque estábamos presentados como administradores, antes de realizar la elevación de privilegios, el sistema nos pedía confirmación. Tradicionalmente esto no ocurría en los sistemas Windows, hasta XP inclusive: una vez entrábamos como administrador, no había **ningún control más.** Como consecuencia, cualquier virus podía dominar la máquina. Y como en los ordenadores de uso personal se suele utilizar siempre el usuario administrador porque es el propio usuario el que realiza las tareas de mantenimiento de su máquina, aquí tenemos la principal causa de la **mala fama** de los sistemas Windows en cuanto a seguridad.

Para mitigarlo, en la versión Vista se añadió el famoso UAC **(User Access Control).** Ahora el sistema avisa al usuario cuando un programa solicita ejecutar una operación de administración. Si no estábamos haciendo nada especial, como una instalación de nuevo software, podemos suponer que es un ataque y detenerlo ahí.

Pero al final resultó ser muy **molesto,** porque muchas herramientas necesitan hacer operaciones especiales en el sistema y no por eso son peligrosas (por ejemplo, cambiar la hora).

Además, la mayoría de **los usuarios no saben** a priori si lo que va a hacer la aplicación es dañino o no y, por defecto, siempre aceptan (con la posible entrada de virus) o siempre niegan (entonces, las nuevas aplicaciones no se instalan bien).

El resultado final fue que mucha gente no lo entendió como una mejora y se quejó. Microsoft se vio obligado entonces a introducir una modificación en Vista que permitía desactivar el UAC, de manera que volvíamos al funcionamiento de XP. En Windows 7 y Windows 2008 se ha mejorado el UAC al permitir cierta configuración. Lo detallamos en el caso práctico 10.

Caso práctico 10

Configuración del UAC en Windows 7

■ **Duración:** 15 minutos ■ **Dificultad:** Fácil

Objetivo. Utilizar las distintas configuraciones del UAC.

Material. Ordenador con Windows 7.

1. Entramos a Windows 7 como administrador y comprobamos cómo está la configuración del UAC. Para ello ejecutamos la herramienta correspondiente. Por ejemplo, en *Inicio* buscamos *UAC* y ejecutamos el programa que nos ofrece.
2. En la ventana (Fig. 5.60) vemos que hay una escala. Esta escala va desde *Notificarme siempre* (configuración Vista) hasta *No notificarme nunca* (configuración XP), con dos valores intermedios. El valor por defecto es el inmediatamente inferior a *Notificarme siempre*, porque permite operaciones sencillas, como cambiar la hora.
3. Podemos probar a ponerlo en *Notificarme siempre* y veremos que, tras cerrar la ventana, el cambio de hora nos pide confirmación.

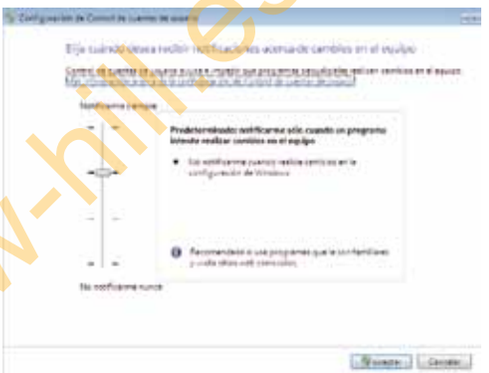

Fig. 5.60. *Configuración de UAC.*

4. Podemos probar a bajarlo hasta *No notificarme nunca* y comprobaremos que, después de reiniciar la máquina, el cambio de hora ya no pide confirmación.
5. Aunque no pida confirmación, no quiere decir que ya no sea una operación privilegiada. Si entramos con un usuario no administrador, seguimos sin poder cambiar la hora (con la diferencia de que ni siquiera nos ofrece la elevación de privilegios).

Actividades

14. Cuando entramos en una máquina Linux y ejecutamos inmediatamente el comando `sudo -i`, ¿por qué nos pide la contraseña, si la acabamos de introducir?

15. Investiga las opciones de configuración del fichero /etc/sudoers para dar privilegios a un usuario concreto y una lista de usuarios concreta.

16. Ventajas e inconvenientes del mecanismo de elevación de privilegios de Linux y Windows.

17. En una empresa donde la mayoría de los trabajadores son licenciados universitarios, ¿conviene que cada usuario tenga privilegios de administrador para que solucionen sus problemas sin molestar al departamento de soporte?

3. Cuotas

Hasta ahora hemos protegido nuestros sistemas evitando el acceso de personas no autorizadas; ahora vamos a protegerlos de las personas que sí están autorizadas. Porque nuestros usuarios, con intención o no, **también pueden dañar el sistema.** Por ejemplo, pueden descargar muchos archivos pesados, de manera que llenan el disco y el sistema empieza a fallar porque siempre necesita escribir en algunos ficheros (el típico error *filesystem full*); también pueden lanzar procesos muy pesados, que ralentizan la CPU y no permiten trabajar a los demás usuarios.

Para evitarlo, los sistemas se configuran para aplicar **cuotas.** Para el disco, se establece que cada usuario puede ocupar un número determinado de bytes (megabytes, gigabytes). Cuando excede ese límite, podemos configurar de modo que el sistema no le permita 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 especial cuidado con los usuarios que se crean porque son necesarios para arrancar una aplicación, como el www-data del servidor web Apache: si exceden la cuota, la aplicación se parará.
- Si son **muy altas,** no tendrán el efecto disuasorio que se espera de ellas y, al final, terminaremos comprando más disco.

Caso práctico 11

Cuotas de disco en Windows 7

■ **Duración:** 15 minutos ■ **Dificultad:** Fácil

Objetivo. Aplicar cuotas a un usuario concreto sobre un disco concreto.

Material. Windows 7 sobre VirtualBox 4.

1. Utilizaremos una máquina virtual para añadir un nuevo disco con facilidad, como ya vimos en la Unidad 4. En este caso utilizaremos un disco pequeño, de 500 MB. Arrancamos la máquina virtual y entramos con un usuario administrador para crear la nueva unidad: en *Inicio* buscamos *admin* y elegimos *Administración de equipos*. Una vez dentro vamos a *Administración de discos* dentro de *Almacenamiento*. En el nuevo disco creamos un volumen y lo formateamos en NTFS.
2. En esa misma ventana o en *Inicio* > *Equipo* nos situamos sobre la nueva unidad E: y en el menú del botón derecho elegimos *Propiedades*. En la ventana que aparece vamos a la pestaña *Cuota* (Fig. 5.61).
3. En la figura aparece activado, pero en general no lo está y tenemos que pulsar en *Habilitar la administración de cuota*. En ese momento se activan todas las opciones.
4. La primera opción es para decidir qué pasa cuando un usuario intenta utilizar más espacio del que tiene asignado. Podemos denegar la operación o permitirla. Si es un disco donde los usuarios dejan archivos personales, lo normal es denegarla y forzar el borrado de archivos antiguos; si es un disco utilizado por una aplicación, lo normal es permitir que siga; cuando el administrador revise los log del sistema, procederá a corregir la situación (aumentar cuota, reconfigurar la aplicación, etc.).

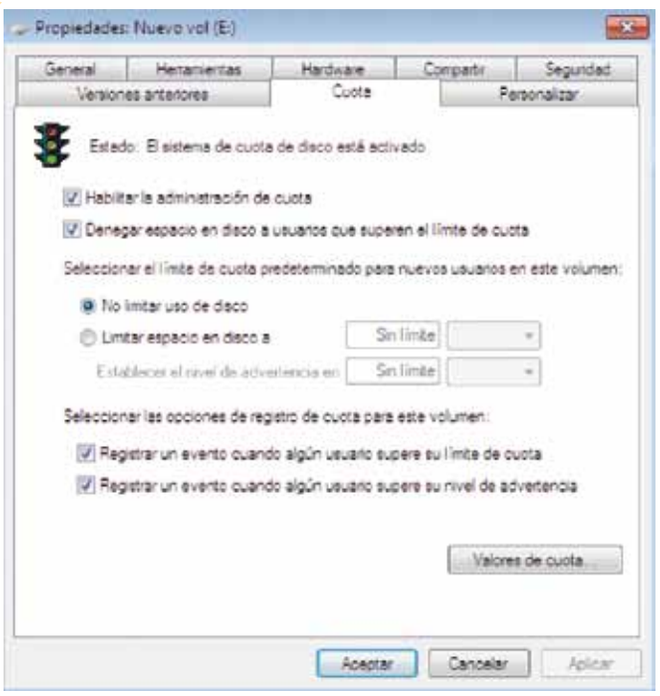

Fig. 5.61. *Cuotas de disco en W7.*

En nuestro ejemplo lo dejaremos activado.

(Continúa)

Caso práctico 11

(Continuación)

5. Después podemos establecer cuotas de manera general para todos los usuarios. Si activamos *Limitar espacio en disco a,* nos ofrece establecer dos límites. El primero es el espacio total que le dejaremos usar; el segundo es un nivel de advertencia que se pone a un valor inferior al espacio total para que el administrador pueda anticiparse a la situación en que el usuario se quede sin disco.

En nuestro ejemplo no vamos a utilizar esta opción porque lo haremos para un usuario en concreto.

6. Las últimas opciones permiten elegir si queremos registrar un evento cuando ocurra alguna de las situaciones anteriores: superar el nivel de advertencia o el nivel de cuota.

En nuestro ejemplo activaremos los dos avisos.

7. Ahora pulsamos el botón *Valores de cuota* para establecer la cuota de un usuario concreto. Vamos a hacerlo para el usuario alumno. En la ventana que aparece entramos al menú *Cuota* y elegimos *Nueva entrada de cuota*. Nos preguntará el usuario al que se aplica. Introducimos alumno y pulsamos en *Comprobar nombres* para completar el nombre (Fig. 5.62).

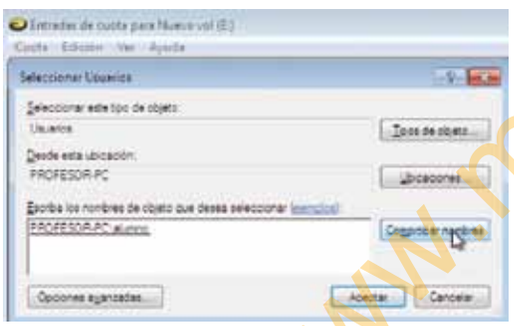

Fig. 5.62. *Elegimos usuario para cuota.*

8. Pulsamos *Aceptar* y la siguiente ventana permite establecer los valores de espacio total y nivel de advertencia. En nuestro ejemplo asignaremos 60 y 10 KB, respectivamente. Son muy bajas, para poder superarlas fácilmente, pero en un sistema normal estaremos hablando de megas o gigas (Fig. 5.63).

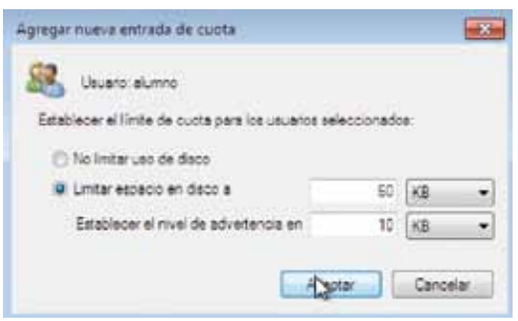

Fig. 5.63. *Valores de cuota.*

9. Pulsamos en *Aceptar* y ahora la ventana refleja el estado de la cuota del usuario alumno. Vamos a probar qué ocurre cuando se aplica. Cerramos todas las ventanas y entramos con el usuario alumno. Nos situamos en el nuevo disco y copiamos el fichero C:\WINDOWS\twain_32.dll, que tiene aproximadamente 50 KB. La primera copia funciona bien, pero en la segunda el sistema ya no nos deja (Fig. 5.64).

Fig. 5.64. *Cuota excedida.*

10. Efectivamente, si volvemos al usuario administrador y abrimos la ventana de cuotas, vemos el aviso (Fig. 5.65).

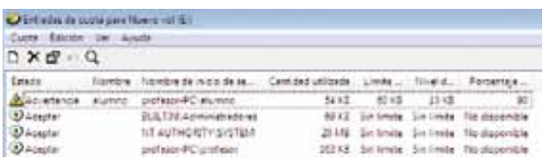

Fig. 5.65. *Estado de cuotas.*

11. Como tenemos activado que se genere un evento cuando se superen los umbrales, vamos a verlo. En el visor de eventos (pulsamos **Inicio,** introducimos evento y, entre las opciones que ofrece, elegimos *Visor de eventos*) entramos en *Sistema* dentro de *Registros de Windows*. Los identificaremos porque el origen es NTFS (Fig. 5.66).

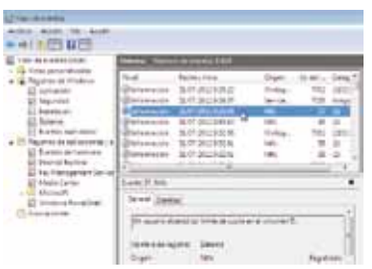

Fig. 5.66. *Evento registrado.*

12. Podemos comprobar que la cuota está funcionando solo para este usuario y solo para este disco. El usuario administrador puede superar ese límite en el disco E, y el usuario alumno puede superarlo en el disco C:, en su carpeta Documentos, por ejemplo.

4. Actualizaciones y parches

Ya tenemos el sistema protegido contra el acceso de extraños y contra el mal uso de los propios. Pero estamos hablando de software: hecho por humanos y, por tanto, sujeto a errores.

El CD/DVD que hemos 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, sobre todo, **corrigen defectos.**

Como administradores responsables del sistema, debemos instalar esas actualizaciones. Por suerte, no hace falta esperar a que nos llegue otro CD con cada actualización: **se descarga automáticamente desde Internet.**

Microsoft libera actualizaciones de forma rutinaria, y Service Pack, cada dos semanas, los martes por la noche; pero si encuentran la solución a un problema urgente, lo liberan inmediatamente, sin esperar al siguiente martes.

Las actualizaciones se configuran desde el panel de control (Fig. 5.67).

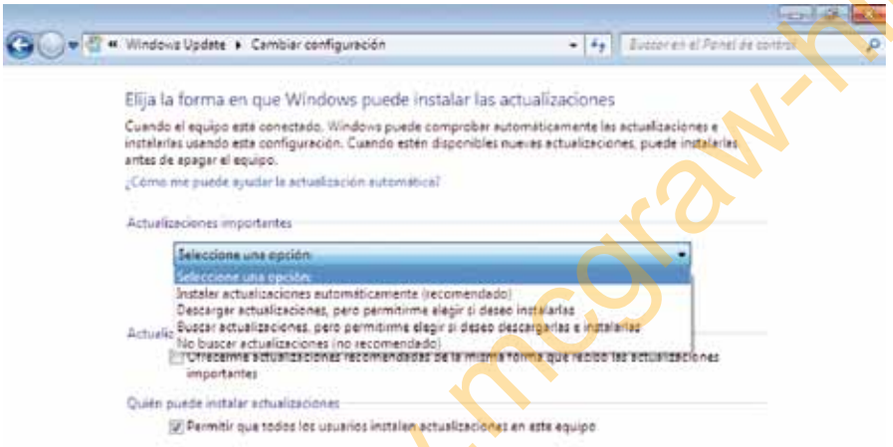

Fig. 5.67. *Actualizaciones W7.*

Podemos elegir entre:

- No buscar actualizaciones ni instalarlas (no recomendable).
- Comprobar si hay actualizaciones, pero no descargarlas ni instalarlas. Esto solo tiene sentido en equipos con poco disco o acceso limitado a Internet.
- 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 los puestos de usuario.

Este comportamiento no es único de Microsoft; todos los fabricantes de aplicaciones necesitan actualizar su software porque desde que lo descargamos han seguido trabajando. Esto nos ocurre con Adobe Reader, Adobe Flash Player, Dropbox, los antivirus, etc.

Los **parches** son parecidos a las actualizaciones, pero se utilizan solo para corregir defectos y suelen necesitar que el usuario lo descargue y lo instale. Es decir, cuando alguien (el propio fabricante o algún cliente) detecta un problema en una aplicación, el fabricante avisa a todos los clientes afectados, les describe un **workaround** (si lo hay) y, cuando tiene el parche que lo arregla, les avisa para que lo descarguen de su web. Por este motivo es importante tener **copias originales** de las aplicaciones y **registrarse** en la web del fabricante para estar al día de los problemas que aparezcan.

Vocabulario

Service Pack (SP). En los sistemas Windows, reúne las actualizaciones generadas desde que se distribuyó el sistema (SP1) o desde el anterior Service Pack (SP2, SP3…).

Workaround. Cuando una aplicación tiene un problema y todavía no existe la solución definitiva, podemos aplicar una solución temporal. En general, consiste en desactivar la funcionalidad que falla.

Actividades

18. Algunas aplicaciones, tras recibir y aplicar su actualización, solicitan reiniciar el sistema. ¿Por qué?

19. Las actualizaciones de Windows se suelen aplicar al cerrar el sistema. ¿Por qué?

20. Un usuario normal, sin privilegios, no puede instalar una aplicación. Sin embargo, en algunos casos sí puede actualizarla. ¿Por qué?

5. Antivirus

Actividades

21. ¿Tiene sentido un antivirus en un móvil? ¿Y en una tableta?

22. ¿Hay virus en otros sistemas operativos: Linux, Mac OS? ¿Por qué?

23. ¿Qué es un exploit?

24. En un antivirus, ¿qué es un heurístico?

25. En las primeras versiones beta de Windows Vista se bloqueaban los antivirus. ¿Qué ocurrió?

Podemos tener el sistema actualizado, pero hay mucho programador malicioso que quiere instalar software en nuestro sistema para su provecho (diversión, espionaje industrial, etc.). Son los llamados **virus informáticos,** que son de muchos tipos (gusanos, troyanos, etc.), pero, en cualquier caso, estamos hablando de **malware** (software maligno) y hay que evitarlos.

Los virus pueden instalarse en nuestra máquina sin que lo sepamos, aprovechando algún defecto del sistema operativo o las aplicaciones instaladas (defectos que todavía no se han resuelto, o se han resuelto y no nos hemos enterado). Pero también les podemos «abrir la puerta» porque estamos haciendo la instalación de una aplicación que hemos conseguido de algún sitio no oficial. Para combatir ambos casos tenemos que instalar un antivirus.

El **antivirus** es un programa que está vigilando continuamente lo que ocurre en nuestra máquina. Concretamente, cualquier software que se intenta ejecutar (ejecutables .exe, librerías .dll) primero pasa por el antivirus. Él lo compara con su **base de datos** de virus y, si lo encuentra, impide que se ejecute y avisa al usuario.

Aunque el antivirus siempre va por detrás del virus, es importante tenerlo actualizado. La actualización afecta tanto a la base de datos de virus conocidos como al software del propio antivirus.

Caso práctico 12

Antivirus AVG en Windows 7

■ **Duración:** ◷ 20 minutos ■ **Dificultad:** ☺ Fácil

Objetivo. Instalar y configurar un antivirus.

Material. Ordenador Windows 7 con conexión a Internet.

1. Nos descargamos el antivirus AVG de su web oficial: **www.avg.com.** Elegimos la opción gratuita. El instalador inicia un asistente (Fig. 5.68).

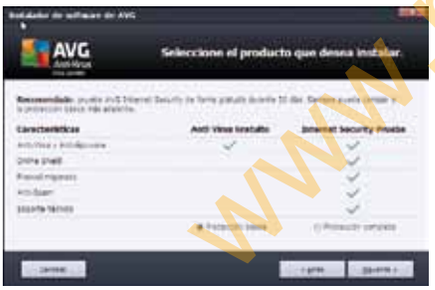

Fig. 5.68. *Instalación de AVG.*

2. Cuando nos pregunte por el tipo de instalación, podemos elegir la instalación personalizada para evitar una nueva barra en el navegador (Fig. 5.69).

Fig. 5.69. *Instalación personalizada.*

3. Entre los componentes podemos quitar el correo electrónico si no usamos Outlook, así como el LinkScanner si ya lo hace nuestro navegador, como en el caso de Google Chrome.

4. El proceso de instalación termina, pero después hay que esperar a que se complete la actualización (Fig. 5.70).

Fig. 5.70. *Actualización tras instalación.*

5. Cuando detecte un virus nos avisará con una ventana como la que aparece en la Figura 5.71. Podemos elegir entre eliminarlo de su ubicación actual o dejarlo estar. Lo normal es eliminarlo.

Fig. 5.71. *Virus detectado.*

6. Monitorización

Hemos evitado el acceso de externos, hemos aplicado cuotas a los internos, tenemos activadas las actualizaciones automáticas del sistema operativo y todas las aplicaciones instaladas, tenemos antivirus actualizado… ¿Estamos tranquilos?

Pues no. 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 dónde lo hace (fichero, base de datos).
- 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 otra. De esta forma podremos analizar un desastre, evitaremos que un hacker borre sus huellas, etc.
- Revisar la **ocupación del sistema,** principalmente el disco y la CPU. Lo habitual es programar una tarea para revisarlo regularmente (cada cinco minutos, por ejemplo) y generar una alarma que alerte al administrador cuando se supere algún límite (90 % del disco, por ejemplo).
- Suscribirse a las **newsletters** de los fabricantes de nuestro hardware y software para tener a mano la información oficial: actualizaciones, parches, nueva funcionalidad, workarounds, etc.
- Participar en **foros de usuarios** de las mismas aplicaciones que nosotros, para estar al día de los problemas que aparecen (puede que nos pase lo mismo) y para poder pedir ayuda si algo nos sobrepasa (en paralelo con la consulta al soporte oficial).

La monitorización de los log consiste primero en diferenciar qué es un problema y qué no lo es. El texto de log ayuda porque suele tener un **indicador de gravedad** (crítica, alto, medio, bajo o simple aviso), aunque es la clasificación del fabricante: solo nosotros conocemos nuestro sistema y sabemos las consecuencias de cada aviso.

Para conocer la ocupación de recursos de una máquina podemos entrar en ella y lanzar **herramientas locales,** como la que aparece en la Figura 5.72 o el comando `top` en Linux. Pero si tenemos a nuestro cargo la monitorización de muchos equipos, no podemos estar todo el día entrando en cada uno de ellos cada cinco minutos.

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** en todo momento del **estado** de los elementos del inventario. Estas herramientas facilitan mucho el trabajo del administrador porque:

- **Rastrean la red** periódicamente buscando nuevas altas y bajas de equipos en el inventario.
- Son capaces de **identificar** distintos tipos de equipos, no solo ordenadores, sino también equipamiento de red. Para ello es necesario que los equipos ofrezcan **interfaces estándar,** como SNMP (Simple Network Management Protocol).
- Obtienen la configuración para todos los equipos del inventario y la registran en una **base de datos** para generar informes, avisar de cambios, etc.
- Incorporan **alertas** sobre ocupación de disco, inactividad de una interfaz, etc.
- Podemos **monitorizar en directo** la actividad de las interfaces de red, uso de CPU, etc.

La implantación de una de estas herramientas representa la frontera entre una administración artesanal de la red y sistemas, y una administración moderna y profesional. El punto de inflexión suele ser un límite en la proporción entre el número de equipos y el número de integrantes del departamento de soporte informático. Cuando el personal ya está desbordado de trabajo, introducir estas herramientas permite automatizar las tareas rutinarias y así dejar tiempo libre a las personas que atienden los problemas complicados. Por ejemplo, localizar los equipos de la red que tienen un determinado software instalado, detectar nuevos equipos conectados pero no autorizados, etc.

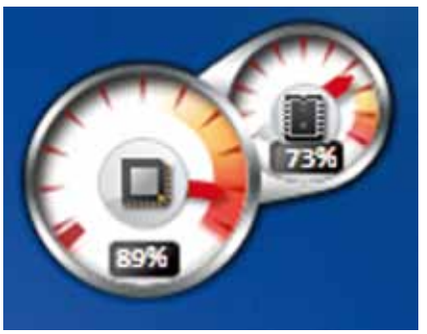

Fig. 5.72. *Gadget de rendimiento W7.*

Actividades

26. Estudia las posibilidades de la herramienta Monitor de rendimiento y Monitor de confiabilidad de Windows 7.

27. ¿Por qué es tan restringida la configuración por defecto del SNMP, como vemos en el caso práctico 13?

Caso práctico 13

Herramienta de Inventario y Monitorización

■ **Duración:** 45 minutos ■ **Dificultad:** Alta

Objetivo. Instalar y configurar la herramienta gratuita SpiceWorks para monitorizar distintos equipos.

Material. Ordenador Windows XP con máquina virtual Windows *7*, ordenador Vista con máquina virtual Linux Ubuntu Server, router ADSL.

1. Vamos a monitorizar una red con tres equipos: un Windows *7* (máquina virtual corriendo en un XP), un Ubuntu Server (máquina virtual corriendo en un Vista) y un router ADSL. Todo desde un único punto: la herramienta SpiceWorks instalada en el XP.
2. Todos los equipos están en la misma red `192.168.1.0/24`. Primero instalamos la herramienta descargándola desde su web **(www.spiceworks.com).** Aparece un asistente de instalación cuya primera pregunta es en qué puerto queremos habilitar la herramienta. Por defecto ofrece el 80: efectivamente, nos va a instalar un servidor web (Apache) para manejar la herramienta (Fig. 5.73). Esto supone una gran ventaja porque podemos utilizarla desde cualquier punto de la red.

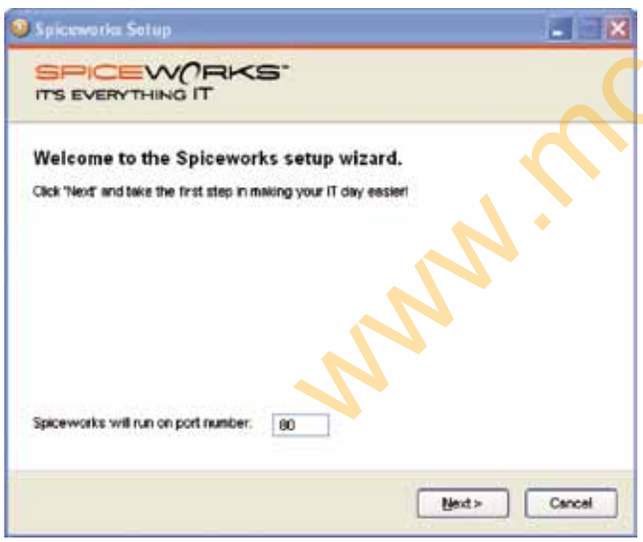

Fig. 5.73. *Puerto del servidor web de la herramienta.*

3. En los siguientes pasos nos pide la típica confirmación de la licencia y nos permite cambiar el directorio destino. Dejamos los valores por defecto.
4. Terminada la instalación, la herramienta arranca el servidor web (interfaz de usuario) y el servidor de la herramienta, y nos abre el navegador para empezar a trabajar. Si consultamos la lista de procesos mediante taskmgr veremos un spiceworks.exe y un spiceworks-httpd.exe (Fig. 5.74).

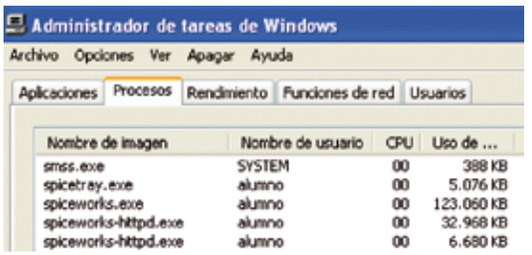

Fig. 5.74. *Procesos de la herramienta.*

5. Para empezar a trabajar, nos solicita crear una cuenta. Con esta cuenta podremos autenticarnos en el servidor web y, sobre todo, podremos acceder a la comunidad de usuarios de SpiceWorks.
6. Terminado el registro, nos ofrece varias tareas. Elegimos el inventario. A continuación nos pide confirmación para el rango de IP de nuestra red donde aplicará el rastreo (Fig. 5.75). El rastreo consiste en probar con cada IP de nuestra subred y, para aquellas que contestan, aplicar varios algoritmos destinados a deducir qué tipo de equipo es. Puede tardar varios minutos dependiendo de cuántos equipos tengamos conectados, la velocidad de la red, la potencia del servidor, etc.

Fig. 5.75. *Rastreará la red de nuestros equipos.*

7. A continuación nos pide credenciales para poder entrar a los equipos y obtener más información (Fig. 5.76). Si estamos utilizando un dominio Windows podemos introducir el usuario y contraseña de un administrador. Si todos o varios de nuestros equipos Unix tienen el mismo usuario privilegiado, podemos introducirlo. Para equipos más sencillos, lo normal es intentarlo por SNMP, cuya contraseña por defecto es public.

   En este primer intento no aportaremos ninguna contraseña especial para ver qué puede hacer.

Fig. 5.76. *Credenciales disponibles.*

(Continúa)

Caso práctico 13

(Continuación)

8. Empieza el escaneo de la red y nos va informando de lo que encuentra. En la Figura 5.77 podemos ver que ha detectado la marca y el modelo del router ADSL y le ha asignado el icono de equipo de red.

Fig. 5.77. *Escaneo en curso.*

9. El resultado del inventario inicial ha sido: cuatro equipos, 37 programas (el software también hay que inventariarlo) y una alerta (Fig. 5.78).

Fig. 5.78. *Resultado del inventario inicial.*

10. Terminado el escaneo, ya podemos empezar a trabajar. La herramienta incluye mucha funcionalidad, por lo que es fácil perderse. En la parte superior está la barra de menú. La opción que más utilizaremos será *Inventory*. Entrando en *Inventory* > *Devices* tenemos la vista de equipos (Fig. 5.79).

Fig. 5.79. *Vista de equipos.*

11. La herramienta los clasifica en varios grupos: workstations (puestos de trabajo), servers (servidores), printers (impresoras), networking (equipo de red), others (teléfonos IP, adaptadores ATA), unknowns (desconocidos), user defined (definidos por el usuario, como móviles o proyectores en red) y SAI. En nuestro caso ha encontrado una workstation (el XP), un equipo de red (el router ADSL) y dos desconocidos (el Vista y el Windows 7). El Ubuntu Server ni siquiera aparece.

12. Para el XP tenemos toda la configuración disponible (Fig. 5.80) porque estamos ejecutando el servidor en esa máquina y, por defecto, utiliza esas credenciales.

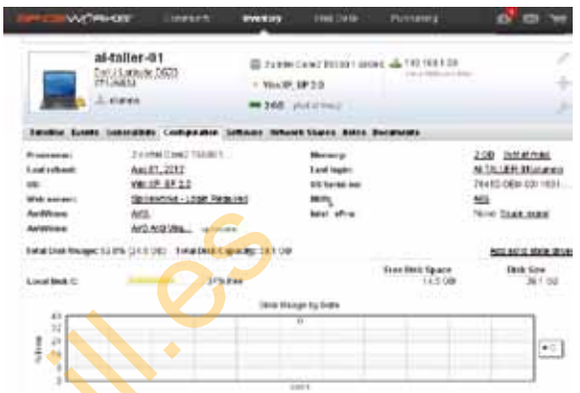

Fig. 5.80. *Configuración de la workstation detectada.*

13. En cambio, para el Windows 7 apenas obtiene nada (Fig. 5.81). Tampoco se lo hemos puesto fácil, porque no le valían las credenciales del XP y no hemos activado SNMP ni WMI (WMI es una evolución de SNMP).

Fig. 5.81. *Configuración incompleta para W7.*

14. El router sí está bien configurado porque tenía activado el SNMP. En la Figura 5.82 vemos las interfaces de red.

Fig. 5.82. *Configuración del router.*

15. Vamos a ayudar un poco a la herramienta. Activaremos SNMP en el Windows 7 y en el Linux Server. En el Linux hay que instalar el paquete snmpd y cambiar la configuración en el fichero /etc/snmp/snmpd.conf. La configuración por defecto es muy restrictiva porque solo

(Continúa)

Caso práctico 13

(Continuación)

admite conexiones desde la máquina local y solo muestra parámetros básicos, como el nombre de la máquina. Como queremos monitorizarla al completo y desde otra máquina, cambiaremos las directivas `agentAddress` y `rocommunity`. Los nuevos valores deben ser:

```
agentAddress udp:161

rocommunity public default
```

16. Salvamos el fichero y reiniciamos el servidor mediante:

```
# service snmpd restart
```

17. Podemos utilizar la herramienta `snmpwalk` para comprobar que está funcionando. Se instala con `apt-get install snmp` y el comando sería (Fig. 5.83):

```
$ snmpwalk -c public -v1 localhost
```

Fig. 5.83. *Prueba con snmpwalk.*

18. Ahora deberíamos repetir el escaneo para inventariar la nueva máquina. Como tarda mucho, vamos a limitar la búsqueda. Entramos en *Inventory > Settings > Network Scan*. Deshabilitamos el escaneo de toda la red y creamos uno nuevo pulsando en *Click here to add a new scan entry*. Introducimos la IP del Linux, le indicamos que no utilice ninguna cuenta Windows ni SSH y elegimos la contraseña Public para el SNMP (Fig. 5.84).

Fig. 5.84. *Escaneo particular.*

19. Salvamos esta configuración y la ejecutamos inmediatamente desde el menú de la derecha *(Scan Now)*. En poco tiempo aparece en el inventario la nueva máquina. La clasifica como servidor y tenemos acceso a toda la configuración (Fig. 5.85).

Fig. 5.85. *Configuración del servidor Linux detectado.*

20. Finalmente configuramos el Windows 7. Como en el Linux, el SNMP tampoco suele estar configurado por defecto. Entramos como administrador y buscamos *Activar o desactivar las características de Windows*. En la ventana que aparece elegimos activar el SNMP con WMI (Fig. 5.86).

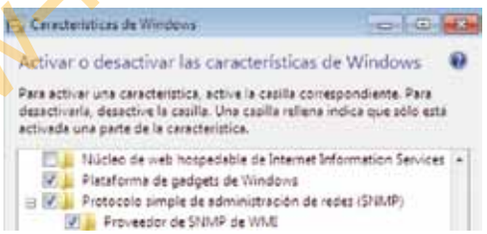

Fig. 5.86. *Activamos SNMP en W7.*

21. Terminamos la instalación y ahora toca configurar. Vamos a la herramienta de servicios (**Inicio** y buscamos *Servicios*). Nos situamos sobre *Servicio SNMP*, y en el menú del botón derecho elegimos *Propiedades*. En la ventana que aparece vamos a la pestaña *Seguridad* y aplicamos varios cambios: desactivar *Enviar captura de autenticación*, agregar el nombre de comunidad public como solo lectura y activar que acepte peticiones SNMP de cualquier host (Fig. 5.87).

Fig. 5.87. *Configuramos SNMP en W7.*

(Continúa)

Caso práctico 13

(Continuación)

22. Cerramos la ventana aceptando la nueva configuración y reiniciamos el servicio. Ahora podemos volver a la herramienta SpiceWorks y, al igual que hicimos en el Linux Server, creamos un escaneo particular para la dirección IP del Windows 7. En poco tiempo lo tendremos disponible en la categoría *Servers* con toda su configuración (Fig. 5.88).

Fig. 5.88. *Configuración del W7 detectado.*

23. Hemos conseguido centralizar en una única herramienta la información de los equipos de nuestra red, aunque sean de distinto tipo (ordenadores, routers) y distintos sistemas operativos (Windows, Linux). Esto nos ahorra entrar en cada máquina, pero todavía tendríamos que pasarnos todo el día delante del SpiceWorks comprobando la configuración uno a uno. Esta tarea pesada se automatiza con las alertas.

24. Las alertas están en *Inventory > Settings > Monitor&Alerts*. Hay varias predefinidas. Las podemos modificar, desactivar y crear nuevas. Las alertas pueden enviar correos cuando ocurra el evento que están vigilando. Por ejemplo, ya deberíamos haber recibido un correo del primer inventario (Fig. 5.89).

Fig. 5.89. *Correo enviado por la herramienta.*

25. Vamos a definir un nuevo monitor. Pulsamos *Click here to add a new monitor* y creamos uno que vigile que ningún servidor esté caído más de dos minutos (Fig. 5.90). Activamos la casilla del correo para recibir el aviso por este canal.

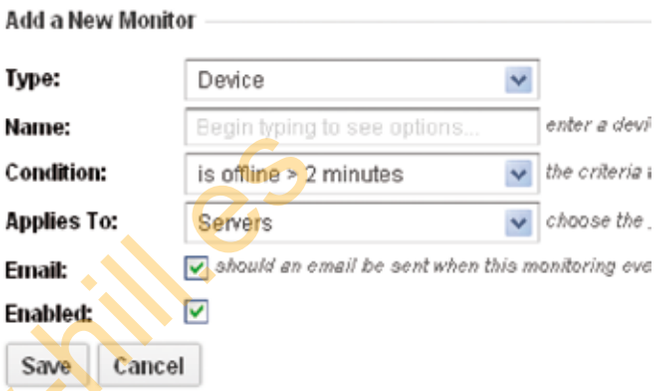

Fig. 5.90. *Nuevo monitor.*

26. Pulsamos *Save* y a continuación paramos la máquina virtual del Windows 7. Se genera una alerta en la herramienta (Fig. 5.91).

Fig. 5.91. *Alerta generada.*

27. También recibiremos el correo (Fig. 5.92).

Fig. 5.92. *Correo con la alerta generada.*

28. Ahora nuestro trabajo se limita a configurar bien los monitores para recibir en el correo las alertas significativas. Para ello hay que conseguir que las condiciones no sean ni demasiado estrictas (muchas alertas para procesar por un humano) ni demasiado laxas (parece que todo está bien, pero puede que el problema esté creciendo mucho y reaccionaremos tarde).

7. Aplicaciones web

La arquitectura de aplicaciones ha evolucionado con el tiempo:

- En los **años sesenta y setenta** eran **monolíticas:** toda la funcionalidad, tanto la interfaz de usuario como la lógica de proceso, estaba en la misma máquina. Los usuarios utilizaban terminales «tontos» conectados al ordenador principal. La protección de una aplicación monolítica se centraba en **proteger la máquina** donde ejecutaban todos los programas.
- En los **años ochenta y noventa** aparecen los ordenadores personales y las redes de comunicaciones dentro de las empresas. Estos dos avances permiten implementar las aplicaciones siguiendo la **arquitectura cliente-servidor:** la interfaz de usuario y parte de la lógica de proceso están en el ordenador del usuario, y el resto de la lógica de proceso está en un ordenador central, al que conectan los ordenadores de usuario mediante la red local. La protección se complica: ahora hay que **proteger a cada cliente, el servidor y la red local de la empresa.**
- A partir de los **años noventa,** el éxito de **Internet** permite extender las aplicaciones web (que siguen el modelo cliente-servidor) a cualquier punto de conexión del planeta. Hay un par de diferencias con los años ochenta: el cliente suele ser siempre el mismo (el **navegador**) y la comunicación utiliza **redes públicas,** sobre las que la empresa tiene nulo control. La protección es más difícil que nunca.

Nadie duda de las ventajas de implementar una aplicación mediante tecnologías web:

- No necesitamos instalar nada en el cliente: solo se necesita el navegador (que se incluye con el sistema operativo y que tiene otros usos, como navegar por Internet). Con esto evitamos instalar un cliente nuevo que pueda entrar en conflicto con otras aplicaciones de la máquina, el usuario no necesita privilegios especiales para instalar programas, etc.
- Cualquier actualización generada por nuestros programadores (más funcionalidad, parches que arreglan defectos) está inmediatamente disponible para los usuarios porque siempre descargan la página actualizada de la última versión. No hay que esperar a que todos los usuarios sean avisados de la actualización, la descarguen, instalen, etc.

Por esta razón 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.**

Veremos un ejemplo de hacking de aplicaciones web en la última unidad de este libro.

Actividades

28. Busca información sobre cómo se hackeaba una conocida plataforma digital de televisión.

29. La aplicación PowerPoint de Microsoft, ¿es una aplicación monolítica o cliente-servidor? ¿Cómo la protegerías?

30. La aplicación SharePoint de Microsoft, ¿es monolítica o cliente-servidor? ¿Cómo la protegerías?

Vocabulario

Intranet. Servidor web dentro de la red de una empresa donde están alojadas algunas herramientas de uso interno (nóminas, gestión de vacaciones, reserva de salas, solicitud de material, etc.).

Hosting web. Servicio de Internet donde una empresa pone sus máquinas y su conexión a Internet para que los clientes instalen sus aplicaciones web. Puede ser hosting dedicado (tenemos una cuenta en la máquina para instalar lo que queramos: servidor web, base de datos, aplicaciones accesorias como el php) o hosting compartido (tenemos servidor web, base de datos y php, pero no podemos configurar nada).

SLA (Service Level Agreement). Son los acuerdos de nivel de servicio: qué vamos a vigilar, cómo lo vamos a vigilar y qué ocurre si no se cumple.

8. Cloud computing

Después de las aplicaciones web, la siguiente evolución de las aplicaciones en Internet es el **cloud computing** (computación en la nube). Conviene diferenciar entre computación en la nube y almacenamiento en la nube (**cloud storage:** iCloud, Dropbox, Amazon S3). El almacenamiento también aporta flexibilidad (número variable de GB reservados, backup automático), pero se limita a guardar archivos y carpetas; la computación es más amplia porque ejecuta programas que trabajan con archivos, bases de datos, otros servidores, etc. Sin embargo, se complementan porque la computación en la nube puede trabajar con archivos de almacenamiento en la nube.

A las empresas ya no les interesa conectar a Internet un servidor web de su CPD porque necesitan dedicar recursos a proveer QoS (Quality of Service, calidad de servicio), buena conectividad, servidores potentes, administradores eficaces, etc. Además, abrir al exterior las conexiones del CPD es una fuente de problemas por la cantidad de ataques que nos pueden llegar.

Tampoco convence ya alquilar espacio en un hosting porque, si es un servidor web compartido, el rendimiento es bajo; si es un hosting dedicado, suelen ser máquinas individuales de potencia media.

Actividades

31. Busca proveedores de cloud computing que alojen sistemas completos.

32. Investiga los precios de Google Apps y discute en clase las ventajas y los inconvenientes de utilizar un servidor de correo alojado en cloud computing o contratar Google Apps.

33. Piensa en un ejemplo de combinación de cloud storage y cloud computing.

8.1. IaaS: Infrastructure as a Service

Un primera solución de cloud computing es el **IaaS** (Infrastructure as a Service). Nuestra empresa quiere poner una máquina entera (un Linux, por ejemplo) en un proveedor, pero con una diferencia frente al hosting dedicado: esa máquina ejecutará en un entorno **virtualizado,** de manera que podemos regular la potencia. Si la aplicación está ralentizándose por un exceso de carga, contratamos temporalmente más CPU y más RAM (y asumimos el incremento de coste asociado); cuando ya no lo esté, volvemos a la configuración básica. Incluso se puede solicitar que arranquen más máquinas (se llaman **instancias**).

El procedimiento es similar al de las máquinas virtuales: generamos un disco virtual (fichero vdi, por ejemplo), instalamos lo que necesitamos (generalmente Linux RedHat o Ubuntu, pero también Windows Server) y lo subimos a la web del proveedor. Desde un panel de control en esa web modificamos la ejecución de la máquina según nos convenga en cada momento.

Pero en esta opción seguimos necesitando personal especializado para administrar esas instancias, generarlas, actualizarlas, configurar la seguridad, vigilar la virtualización, etc.

Vocabulario

Virtualización. Tecnología hardware y software que permite crear distintas máquinas virtuales dentro de la misma máquina física. Cada máquina virtual tiene su propio sistema operativo y aplicaciones. El hardware disponible (CPU, RAM, interfaces, disco) se reparte entre las máquinas virtuales para que lo utilicen con exclusividad. Este reparto puede modificarse dinámicamente.

8.2. SaaS: Software as a Service

Las empresas que no quieren incurrir en ese gasto (una fábrica de quesos sabe de quesos, no de software) eligen **SaaS** (Software as a Service), aplicaciones completas donde el mismo proveedor se encarga del desarrollo de la aplicación, su mantenimiento y también pone las máquinas y la conectividad (o en las máquinas de un IaaS, pero nunca en las nuestras).

Por ejemplo, para el correo de la fábrica de quesos, en lugar de utilizar una máquina nuestra (lo que supone contratar una buena conexión a Internet y asumir los recursos humanos necesarios para realizar la configuración, administración, monitorización 24 x 7…), podemos simplemente contratar el servicio Google Apps de Google.

De cara a la protección de las aplicaciones, en los dos casos (IaaS, SaaS), como ya ocurría con el hosting, perdemos el control sobre la seguridad de la máquina y el software que ejecuta en ella: tenemos que confiar en la profesionalidad del proveedor y redactar muy bien los **SLA** del contrato del servicio.

Síntesis

Hay que encaminar al usuario hasta la autenticación del sistema operativo
- Evitar que abra la caja.
- Evitar que arranque desde un dispositivo externo (CD, USB).
- Evitar que modifique la configuración de la BIOS.
- Evitar que edite la configuración del gestor de arranque.
- Cifrar el contenido del disco por si falla alguna medida anterior.

Autenticación en el sistema operativo
- Usuario/password
  - Fácil de recordar por nosotros, difícil para cualquier otro.
  - Establecer límites de longitud mínima, antigüedad, etc.
- Tarjetas
  - Complementan el usuario/password.
  - Fáciles de manejar (tornos de entrada y otros).
- Biometría
  - Reconocen características físicas de la persona (huella dactilar, retina, voz, etc.).
- Elevación de privilegios
  - Permite realizar puntualmente tareas de administrador sin estar presentado como administrador.
  - En Linux, mediante `sudo`; en Windows, mediante UAC a partir de Windows Vista.

Cuotas
- Permiten controlar el uso de los recursos por parte de los usuarios.
- Generalmente se refieren al disco.
- Se pueden aplicar a todos los usuarios o a un grupo de ellos.
- Se puede configurar que solo avise al administrador o que también evite que exceda el límite impuesto.

Actualizaciones y parches
- Las herramientas suelen automatizar la búsqueda, descarga y aplicación de sus parches. Utilizan Internet.
- Generalmente conviene aplicarlos.

Antivirus
- Es importante instalarlo y, sobre todo, tenerlo actualizado.

Monitorización
- No basta con instalar mecanismos de seguridad: hay que asegurarse de que están funcionando.
- También hay que supervisar los equipos y servicios para detectar nuevas necesidades de seguridad.
- Las tareas rutinarias hay que automatizarlas mediante herramientas de inventario y monitorización.

Aplicaciones web
- El trabajo de vigilancia se complica: los servidores pueden estar en un proveedor externo, los usuarios utilizan sus propios navegadores y la comunicación puede ser intervenida.
- Hay que redactar con cuidado el SLA con los proveedores.

Cloud computing
- Mismos temores que con las aplicaciones web, aumentados porque hay más tecnologías, no solo HTTP.
- Hay que decidir si los servicios informáticos con el exterior (correo, chat, redes sociales) los seguimos implementando con recursos propios (máquinas, personal de soporte) o los subcontratamos.

Test de repaso

1. Caja del ordenador:

a) No se puede proteger porque no tiene software donde poner usuario y contraseña.

b) Podemos protegerla metiéndola dentro de una caja fuerte.

c) Podemos utilizar un candado para dificultar el acceso a los componentes, sobre todo al disco duro.

2. BIOS del ordenador:

a) No hace falta protegerla si tenemos protegida la caja.

b) No tiene nada que proteger. La función de la BIOS es otra.

c) Debemos fijar el orden de arranque para arrancar siempre desde el disco duro.

3. Contraseñas de las BIOS:

a) Siempre hay que activarlas todas: usuario, supervisor, cifrado de disco, etc.

b) Como mínimo, activaremos la contraseña de supervisor para impedir modificaciones de la configuración.

c) La BIOS no tiene contraseñas.

4. En el boot manager:

a) No hay nada que temer: cuando arranque el sistema operativo ya le pedirá el usuario y la contraseña.

b) No hay nada que hacer: es un software muy simple.

c) Podemos poner contraseñas a la configuración y a cada una de las opciones de arranque.

5. El cifrado de particiones:

a) Solo tiene sentido para la partición del sistema operativo.

b) Solo tiene sentido para las particiones de datos.

c) Es necesario generar un disco de arranque para recuperar el sistema en caso de desastre.

6. La contraseña de nuestro usuario:

a) Debe ser fácil de recordar para nosotros pero difícil de adivinar para cualquier otra persona.

b) Es mejor dejarla en blanco: así no tenemos que recordarla.

c) Le ponemos la marca de nuestro coche, para recordarla fácilmente.

7. El acceso mediante tarjeta:

a) Es más seguro si lo combinamos con la introducción de una contraseña («algo que tienes, algo que sabes»).

b) Si la tarjeta tiene un chip, es inteligente y ya no necesitamos contraseña.

c) Es molesto porque las tarjetas llevan chips y necesitan cargar las baterías.

8. El acceso mediante biometría:

a) Es más seguro si lo combinamos con la introducción de una contraseña («algo que eres, algo que sabes»).

b) Es más seguro si lo combinamos con la introducción de una contraseña y la lectura de una tarjeta («algo que eres, algo que sabes, algo que tienes»).

c) Solo está disponible para los servicios secretos y la policía.

9. Cuotas de disco:

a) No son necesarias: cada usuario controla muy bien cuánto ocupa.

b) Solo tienen sentido para usuarios administradores.

c) Son necesarias para evitar afectar el rendimiento del sistema.

10. Actualizaciones de software:

a) Siempre hay que aplicarlas, porque algo bueno harán.

b) En algunos casos habrá que revisarlas por si afectan a determinados servicios que ofrece nuestra máquina.

c) No son necesarias porque mi sistema operativo es original.

11. Antivirus:

a) Solo hace falta activarlo para escanear el programa de instalación de la aplicación que vamos a instalar.

b) No conviene arrancarlo, porque degrada el rendimiento de la máquina.

c) Debe estar activo siempre.

12. Registros del sistema:

a) No merece la pena revisarlos: no entenderemos nada.

b) Solo los utilizan los programadores, para depurar problemas.

c) Tenemos que revisarlos regularmente y, a ser posible, de manera automatizada.

13. Computación en la nube:

a) Nos permite olvidarnos de la seguridad, porque lo hace otro.

b) Nos permite olvidarnos de la seguridad, porque en Internet nunca pasa nada.

c) Tenemos que confiar en que el proveedor de la nube aplica las medidas de seguridad apropiadas.

Soluciones: 1 c, 2 c, 3 b, 4 c, 5 c, 6 a, 7 a, 8 b, 9 c, 10 b, 11 c, 12 c, 13 c.

Comprueba tu aprendizaje

Seguir planes de contingencia para actuar ante fallos de seguridad

1. En el último boletín de seguridad que te ha llegado por correo aparece una vulnerabilidad en la versión 10 y anteriores de Adobe Reader. Utiliza una herramienta como SpiceWorks para localizar los equipos del aula de ordenadores que están en peligro y actualízalos. Documenta el procedimiento.

2. Mediante la misma herramienta, confirma que todos los equipos del aula de ordenadores tienen antivirus. Documenta el procedimiento.

3. Ha llegado a tus oídos que los de la oficina de al lado conocen la contraseña de la Wi-Fi de tu oficina. ¿Cómo lo podrías comprobar? ¿Es un problema para tu empresa? ¿Qué medidas tomarías para solucionarlo? Documenta las conclusiones a las que has llegado.

Política de contraseñas en la BIOS

4. Busca el manual de la placa base de tu ordenador del aula y localiza cuál es el mecanismo de borrado de contraseñas de la BIOS.

a) Entra en la BIOS de tu ordenador para:

- Poner supervisor1 como contraseña de supervisor.
- Poner usuario1 como contraseña de usuario.
- Cambiar el orden de arranque para que primero lo haga el disco duro y luego el CD.

b) Comprueba la efectividad de la nueva configuración de seguridad y documenta el procedimiento. Al terminar, déjalo todo como estaba.

Política de contraseñas en el gestor de arranque

5. En tu ordenador o en una máquina virtual, instala Windows y Linux, y activa el boot manager de Linux.

a) En ese boot manager, crea dos usuarios, Linus y Bill, con contraseña Linux2 y Windows2, respectivamente.

b) Configura que el Linux solo lo puede arrancar el usuario Linus y el Windows solo el usuario Bill.

c) Comprueba que funciona y documéntalo.

Política de contraseñas en el sistema operativo

6. En un ordenador o una máquina virtual con Windows 2008:

a) Desactiva el control de complejidad de la clave. Comprueba que puedes introducir una contraseña igual al nombre del usuario.

b) Actívalo y comprueba que ya no te deja.

c) Activa el historial de contraseñas para que recuerde las tres últimas. Compruébalo.

d) Documenta el procedimiento. Si has encontrado alguna dificultad, comenta la solución.

Actualizaciones del sistema operativo

7. En un ordenador o máquina virtual Windows.

a) Desactiva la descarga y aplicación inmediata de las actualizaciones del sistema operativo, de manera que solo las notifique.

b) Cuando aparezcan dichas notificaciones, lee una de ellas y búscala en la web de Microsoft. Será fácil identificarla por su código KB (Knowledge Base).

c) Descárgala e instálala.

d) Vuelve a la herramienta de actualizaciones automáticas para que haga una nueva búsqueda. Comprueba que la recién instalada ya no aparece.

e) Documenta todo el procedimiento.

Aplicaciones específicas para la detección y eliminación de software malicioso

8. En un ordenador o máquina virtual Windows.

a) Desinstala el antivirus que tenga en ese momento.

b) Instala el antivirus de otro fabricante.

c) Una vez actualizado, desinstálalo e instala el anterior.

d) Documenta el procedimiento, sobre todo si has tenido que utilizar una herramienta especial para la desinstalación.

Verificar el origen y la autenticidad de las aplicaciones que se instalan en los sistemas

9. Descarga la utilidad putty.exe desde su página oficial, junto con la firma MD5.

10. Descarga alguna utilidad de verificación de firmas MD5 desde una página distinta.

11. Comprueba que son correctas y documenta todo el proceso.

Telf. contacto: 902 656 439 **http://mghlibros.distriforma.es/**

McGraw-Hill te facilita disponer de tus eBooks y libros
¡No esperes más para tenerlos!
Un sistema rápido y cómodo al recibirlo en tu domicilio
Contacta con MGHLibros

www.mcgraw-hill.es / www.mhe.es

Distriforma y MGHLibros: Distribuidor de ebook y venta tradicional

McGraw-Hill y Distriforma colaboran gestionando la librería virtual

En esta página web puedes disponer de nuestro fondo actualmente activo