Unidades de competencia
Certificados de profesionalidad

Ciclo Formativo Grado Medio

https://www.yolibrospdf.com

Seguridad informática

Jose Fabián Roa Buendía



Mc Graw Hill Education

www.mhe.es/cf/informatica

Seguridad informática

José Fabián Roa Buendía

Revisión Técnica
Francisco Javier Sanz

Mc Graw Hill Education

MADRID - BARCELONA - BOGOTÁ - BUENOS AIRES - CARACAS - GUATEMALA
MÉXICO - NUEVA YORK - PANAMÁ - SAN JUAN - SANTIAGO - SÃO PAULO
AUCKLAND - HAMBURGO - LONDRES - MILÁN - MONTREAL - NUEVA DELHI - PARÍS
SAN FRANCISCO - SIDNEY - SINGAPUR - ST. LOUIS - TOKIO - TORONTO

Seguridad informática • Ciclo Formativo Grado Medio

No está permitida la reproducción total o parcial de este libro, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares del Copyright.

Si necesita fotocopiar o escanear algún fragmento de esta obra, diríjase a CEDRO (Centro Español de Derechos Reprográficos, www.conlicencia.org).

Nota: Este libro se atiene al artículo 32 del derecho de cita de la Ley de Propiedad Intelectual de 1996 (R. D. Leg. 1/1996, de 12 de abril).

Derechos reservados © 2013, respecto a la primera edición en español, por:

McGraw-Hill/Interamericana de España, S. L.
Edificio Valrealty, 1.ª planta
Basauri, 17
28023 Aravaca (Madrid)

ISBN: 978-84-481-8569-5

© José Fabián Roa Buendía

Obra original: *Seguridad informática* © 2013,
respecto a la segunda edición en español, por McGraw-Hill Interamericana de España, S.L.

ISBN edición original: 978-84-481-8396-7

Autores del material complementario: José Fabián Roa Buendía, Gopal Bijani Chiquero
Equipo editorial: Ariadna Allés, Paloma Sánchez, María Dolores Crispín
Diseño de cubierta: rload.es
Diseño interior: dfrente.es
Fotografías: 123RF, iStockphoto
Ilustraciones: M.ª Carmen Fuente Canalda
Composición: Diseño y Control Gráfico, S. L. U.

Presentación

Cuando alguien me pregunta qué estudiamos en SMR **(Sistemas Microinformáticos y Redes),** yo les planteo esta analogía: a muchos nos gustan los coches, pero conducirlos. Si aparece alguna avería, o tenemos que pasar una revisión, lo llevamos a un mecánico. Pues bien, en SMR formamos **mecánicos de sistemas, ordenadores y redes.**

Este libro cubre el módulo de **Seguridad Informática** dentro del currículo de este ciclo formativo de Formación Profesional. Es un tema imprescindible, puesto que el mundo está digitalizado a todos los niveles: personal, empresarial y gubernamental. La era de la información, con Internet como principal exponente, ha mejorado el nivel de vida y la convivencia en este planeta. La información es poder, luego hay que protegerla.

Todos los servicios avanzados que disfrutamos están implementados sobre sistemas informáticos que utilizan ordenadores con un hardware y un software concretos, configurados adecuadamente y conectados entre sí y con los clientes mediantes redes de comunicaciones. Cualquiera de estos elementos es susceptible de ser atacado por un saboteador o, simplemente, fallar. La seguridad informática intenta evitarlo y, en caso de que ocurra, minimizar los daños para recuperar el servicio lo antes posible. Al usuario final no le importa si ha sido un ataque de un equipo de hackers contratado por la competencia o un simple apagón en la sala de servidores: él contaba con utilizar un servicio que nuestra empresa ha dejado de prestarle.

Pero tenemos que asumir que la seguridad total es imposible. Ante cualquier barrera física o lógica, el atacante buscará una forma de romperla o rodearla. Así ha sido hasta ahora y seguirá ocurriendo. Debemos tomar todas las medidas que estén a nuestro alcance y entren en nuestro presupuesto, pero su eficacia dependerá del interés que otros tengan por acceder a nuestros datos y sistemas. No se protege igual la caja de un banco que la hucha de un niño.

Quiero agradecer la total colaboración material y humana por parte del Colegio Valle del Miro, tanto de mis compañeros informáticos como, sobre todo, de la jefatura de estudios, la dirección y la presidencia del centro. Nos quedan muchos años juntos, y los vamos a disfrutar.

Muchas gracias también a la editorial McGraw-Hill, a mis dos editoras, Ariadna y Loly, y a mi revisor, Francisco Javier, por toda la paciencia que han derrochado conmigo.

Pero este libro va dedicado a los que cada día me dan todo su amor y cariño: mi mujer, Tote; mis hijos, Daniel y Enrique; mis padres, Fabián y Amparo, y todos los miembros de mi familia.

Volviendo a la analogía del coche, el piloto y el mecánico, tienen algo en común, además del vehículo: les gusta su trabajo. Y encima les pagan por hacerlo. Si vas a trabajar ocho horas de lunes a viernes, durante muchos años, intenta que sea haciendo algo que te guste de verdad. Y fórmate para conseguirlo.

El autor

Índice

Conceptos sobre seguridad informática

1

1. ¿Por qué proteger? 8
2. ¿Qué proteger? 10
3. Definiciones 14
4. Tipos de ataques 19
5. Buenas prácticas 21
6. Legislación 22

Síntesis 24
Test de repaso 25
Comprueba tu aprendizaje 26

Criptografía

2

1. ¿Por qué cifrar? 28
2. Criptografía 29
3. Criptografía simétrica y asimétrica 30
4. Cifrar y firmar 40
5. PKI. DNIe 48

Síntesis 58
Test de repaso 59
Comprueba tu aprendizaje 60

Seguridad pasiva: equipos

3

1. Ubicación del CPD 62
2. Centro de respaldo 67
3. SAI/UPS 68

Síntesis 72
Test de repaso 73
Comprueba tu aprendizaje 74

Seguridad pasiva: almacenamiento

4

1. Estrategias de almacenamiento 76
2. Backup de datos 94
3. Imagen del sistema 101

Síntesis 108
Test de repaso 109
Comprueba tu aprendizaje 110

Índice

Seguridad activa: sistema operativo y aplicaciones

5

1. Carrera de obstáculos 112
2. Autenticación en el sistema operativo 121
3. Cuotas 129
4. Actualizaciones y parches 131
5. Antivirus 132
6. Monitorización 133
7. Aplicaciones web 138
8. Cloud computing 139

Síntesis 140
Test de repaso 141
Comprueba tu aprendizaje 142

Seguridad activa: acceso a redes

6

1. Redes cableadas 144
2. Redes inalámbricas 154
3. VPN 162
4. Servicios de red. Nmap y netstat 164

Síntesis 166
Test de repaso 167
Comprueba tu aprendizaje 168

Seguridad activa: control de redes

7

1. Espiar nuestra red 170
2. Firewall 183
3. Proxy 194
4. Spam 200

Síntesis 204
Test de repaso 205
Comprueba tu aprendizaje 206

Ataques y contramedidas

8

1. Ataques TCP/IP. MITM 208
2. Ataques wifi. Aircrack-ng 214
3. Ataques web. WebGoat 216
4. Ataques proxy. Ultrasurf 219

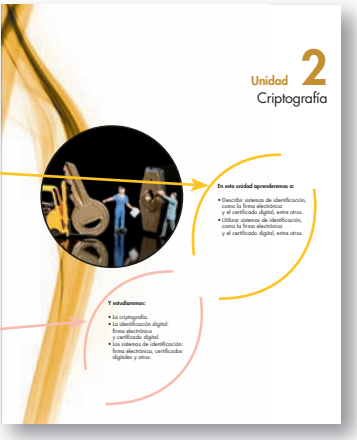
Síntesis 222
Test de repaso 223
Comprueba tu aprendizaje 224

Cómo se utiliza este libro

Presentación de la unidad

Aquí encontrarás los **criterios de evaluación** de la unidad.

Además, te avanzamos los **contenidos** que se van a desarrollar.



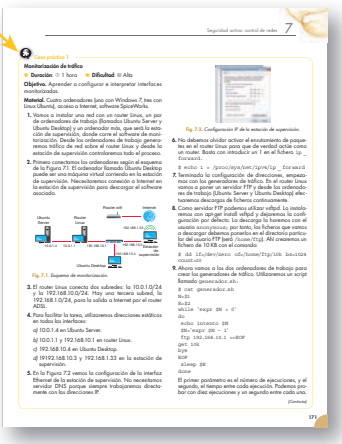
Desarrollo de los contenidos

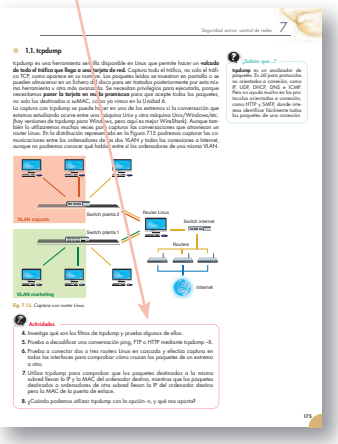
CASOS PRÁCTICOS
Aplican los conocimientos aprendidos a problemas y situaciones reales del entorno profesional.

ACTIVIDADES
Permiten trabajar los contenidos a medida que se van explicando, y aseguran un aprendizaje progresivo.

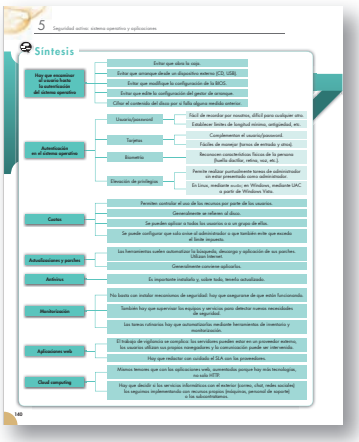
Una exposición clara y concisa de la teoría, acompañada de recuadros que ayudan a la comprensión de los aspectos más importantes:

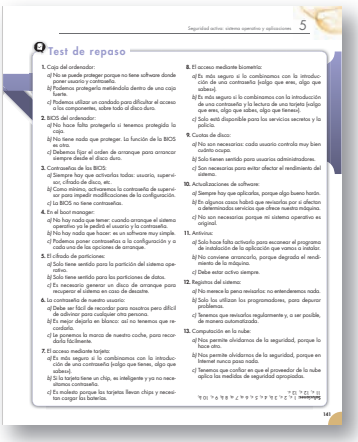
- **¿Sabías que...?**
- **Ten cuidado**
- **Importante**
- **Vocabulario**
- **Web**





Cierre de la unidad





Síntesis: esquema-resumen de los contenidos estudiados en la unidad.

Test: ayuda a detectar cualquier laguna de conocimientos.

Comprueba tu aprendizaje: actividades finales agrupadas por criterios de evaluación.

Unidad 1

Conceptos sobre seguridad informática



En esta unidad aprenderemos a:

- Valorar la importancia de mantener la información segura.
- Conocer las diferencias entre seguridad física y lógica.
- Contrastar la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
- Conocer la legislación sobre protección de datos de carácter personal.
- Conocer la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Contrastar las normas sobre gestión de seguridad de la información.

Y estudiaremos:

- La aplicación de medidas de seguridad activa y pasiva.
- Los métodos para asegurar la privacidad de la información transmitida.
- Los fraudes informáticos y robos de información.
- La legislación sobre protección de datos.
- La legislación sobre los servicios de la sociedad de la información y el correo electrónico.

1. ¿Por qué proteger?

Una experiencia personal: una persona me trae su portátil porque dice que va lento. Le extraña que haya entrado algún troyano porque le puso un antivirus.

Recojo el ordenador y le pregunto por la contraseña del administrador. Dice que no tiene ningún usuario que se llame así, solo el usuario con su nombre. Y no tiene contraseña, entra directamente al pinchar sobre el icono.

—¿No temes que alguien pueda usar tu ordenador sin tu permiso?

—¿Por qué? Mi portátil solo lo uso yo.

—Pero sí lo conectas a Internet. ¿No sabes que pueden entrar por ahí?

—Imposible: sí que tengo contraseña en la wifi de casa.

No insisto más y cojo el ordenador. En efecto, tenía un antivirus, pero estaba caducado. Lo quito, instalo otro y encuentra un troyano. El antivirus lo quita y devuelvo el ordenador a su dueño. Le volveré a ver pronto, me temo.

Así es la inmensa mayoría de los usuarios de ordenadores, tabletas, móviles… Deberían saber que sus máquinas son muy **poderosas,** pero también muy **vulnerables.** Es importante reconocerlo, dado que **nuestra vida es digital:**

- Hablamos por teléfonos móviles.
- Enviamos mensajes con aplicaciones IP, como e-mail, WhatsApp, etc.
- Hacemos compras por Internet. De todo tipo: libros, viajes, comida.
- Estudiamos por Internet, desde una simple búsqueda de información en la Wikipedia hasta clases en directo en un campus virtual.
- Entramos en contacto con determinadas empresas y organizaciones a través de su página web para conocer las novedades de su último lanzamiento, pedir ayuda con un problema, etc.
- Las empresas realizan entre sí contratos electrónicos sin necesitar una firma en un papel.

No hay marcha atrás. La era de la información es el presente y el futuro de nuestra civilización. Por eso hay que estar preparados para evitar estas situaciones:

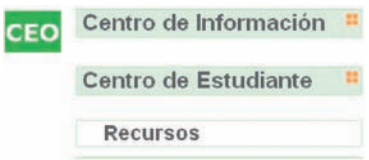
- Nuestras conversaciones son personales: nadie más debería poder escucharlas.
- Nuestros mensajes son privados: nadie debería tener acceso a ellos.
- Una compra solo interesa al vendedor y al comprador. Y debe asegurarse que el vendedor proporcionará los productos elegidos y el comprador pagará el precio acordado.
- La información pública en Internet debe estar al alcance de todos.
- Las empresas deben cuidar su imagen: no pueden consentir un ataque a su página web que modifique el contenido, engañando a sus clientes y usuarios.
- Los contratos entre empresas son privados en muchos casos, y en todos los casos les comprometen a llevarlos a cabo. Nadie externo debe poder alterarlos, ni siquiera conocerlos.

La **seguridad informática** intenta **proteger el almacenamiento, procesamiento y transmisión de información digital.** En los ejemplos anteriores:

- Las conversaciones por teléfono móvil van cifradas: aunque otro móvil pueda recibir la misma señal, no puede entender qué están transmitiendo.
- Los mensajes se almacenan en el servidor de correo y, opcionalmente, en el cliente de correo que ejecuta en mi ordenador. Debemos proteger esos equipos, así como la comunicación entre ambos (como veremos en la Unidad 6). Por ejemplo, podemos cifrar el mensaje y enviarlo al servidor por una conexión cifrada.
- La navegación por la web del vendedor puede ser una conexión no cifrada, pero cuando se utiliza el carrito debemos pasar a servidor seguro. Por otra parte, la web del vendedor debe estar disponible a todas horas: hay que protegerla frente a caídas de tensión, cortes de red, accidentes o sabotajes de sus instalaciones (inundaciones, incendios, etc.).
- Los servidores de información de una red mundial deben estar disponibles a todas horas.

CEO

En el Centro de Enseñanza Online de este libro **(http://www.mhe.es/cf/informatica)** encontrarás todos los documentos mencionados en los cuadros CEO.



¿Sabías que…?

En agosto de 2012 algunos futbolistas famosos sufrieron un ataque en sus cuentas de Twitter: un hacker podía incluir mensajes falsos, que aparecían en sus cuentas, pero no los habían escrito ellos:

http://goo.gl/1Gf6O

El 8 de julio de 2008 hubo una actuación coordinada de la mayoría de los fabricantes de software y hardware para resolver una vulnerabilidad descubierta en el protocolo DNS, el responsable de traducir nombres a direcciones IP. Toda la red Internet estaba en peligro:

http://goo.gl/5Eryq

Actividades

1. Encuentra los defectos de seguridad del ejemplo del portátil contaminado. ¿Cómo los resolverías?

- Las empresas deben restringir el acceso a las partes protegidas de su web, como la administración y la edición de contenidos (Unidad 5).
- Los contratos deben llevar la firma digital de las empresas interesadas (Unidad 2) y deben almacenarse en discos cifrados con almacenamiento redundante (Unidad 4), cuya copia de seguridad irá también cifrada (Unidad 4), y se dejará en un edificio diferente, a ser posible en otra ciudad (Unidad 3).

A pesar de toda nuestra preocupación y todas las medidas que tomemos, la seguridad completa es **imposible.** Debemos asumir que hemos desplegado la máxima seguridad posible con el **presupuesto** asignado y la **formación** actual de nuestros técnicos y usuarios:

- Con más dinero podríamos replicar los servidores, las conexiones, el suministro eléctrico o todo a la vez (Unidad 3).
- Con más formación en los técnicos podríamos desplegar sistemas avanzados de protección, como los NIPS (Network Intrusion Prevention System), que veremos en la Unidad 7.
- Con más formación en los usuarios podríamos estar tranquilos porque no compartirían su contraseña con otros usuarios, no entrarían en páginas potencialmente peligrosas y, cuando llegaran a casa, el portátil o el móvil de empresa no lo usaría cualquier otro componente de su familia.

Por otra parte, podemos estar seguros de que en nuestra casa o en nuestra empresa estamos aplicando todas las medidas; pero **no sabemos qué hacen las otras personas con las que nos comunicamos.** En el ámbito personal, posiblemente enviamos imágenes a alguien que no sabe que tiene un troyano en su ordenador, y que ese troyano está especializado en difundir en Internet cualquier imagen que encuentra.

En el fondo, todo es información: sean los escasos 140 caracteres de un tweet, sean ficheros de varios megabytes, están en nuestro equipo y alguien puede intentar obtenerlos. La clave es la motivación: **quién está interesado en nuestra información.** Es poco probable que algún superhacker intente entrar en nuestro ordenador portátil a por nuestras fotos descargadas de la cámara o nuestros apuntes de clase; seguramente no le costaría mucho, pero el esfuerzo no le merece la pena.

En cambio, las empresas sí son mucho más atractivas para estas actividades delictivas. Hasta tal punto que existen las **auditorías de seguridad:** contratamos a una empresa externa especializada en seguridad informática para que revise nuestros equipos y nuestros procedimientos. Un ejemplo de estas empresas son los tiger teams (equipos tigre): intentan acceder a nuestras instalaciones como lo haría un hacker, para confirmar si podemos estar tranquilos.

Por otro lado, los **mecanismos de seguridad deben estar adaptados** a cada caso particular: una contraseña de 20 caracteres que utiliza mayúsculas, minúsculas, números y signos de puntuación es muy segura; pero si obligamos a que sean así las contraseñas de todos los empleados, la mayoría la apuntará en un papel y la pegará con celofán en el monitor. Cualquiera que se siente en el ordenador tendrá acceso a los recursos de ese usuario.

Un caso real donde se mezcla lo profesional y lo personal: una persona regala a su pareja un teléfono móvil de la empresa. La pareja no lo sabe, pero el equipo lleva preinstalado un troyano que registra todas las llamadas y mensajes efectuados con ese teléfono. Con esa información, el programa elabora un informe que luego cuelga en una web, donde se puede consultar introduciendo el usuario y la contraseña adecuados.

Por este medio descubre que su pareja mantiene una relación paralela con otra persona, que es amigo de la pareja y también trabaja en la misma empresa. El siguiente paso es regalar otro móvil a ese amigo con el mismo troyano, para así espiar la vida de ambos.

Afortunadamente, la empresa de telefonía que da servicio a la empresa tiene un equipo de vigilancia que detecta ese tráfico extraño de informes espontáneos. Avisa a los directivos de la empresa y se denuncia al empleado.

Este último ejemplo también muestra que, aunque los ataques necesitan un componente técnico informático más o menos avanzado, muchas veces hay un factor humano que facilita enormemente la tarea del atacante y contra el que los administradores de los sistemas poco pueden hacer.



¿Sabías que...?

En las empresas es habitual encontrar carteles en los pasillos que recuerdan a los empleados que los datos que manejan son importantes y deben protegerlos.

Web

El número de ataques aumenta, y las consiguientes pérdidas económicas también:

http://goo.gl/sJQFI

Para lanzar un ataque no hacen falta muchos conocimientos de informática: simplemente podemos comprarlo:

http://goo.gl/R66r1

Los principales objetivos de los hackers son compañías de seguridad y bancos:

http://goo.gl/ET69Q

2. ¿Qué proteger?

Debido al presupuesto, no podemos aplicar todas las medidas de seguridad posibles a todos los equipos de la empresa. Debemos **identificar los activos que hay que proteger:** qué equipos son más importantes y qué medidas aplicamos en cada uno. Por ejemplo, todos los equipos deben llevar antivirus y firewall; sin embargo, la ocupación del disco duro solo nos preocupará en los servidores, no en los puestos de trabajo. Del mismo modo, el control del software instalado es mucho más exhaustivo en un servidor que en un ordenador personal.

Sin embargo, **el mayor activo es la información** contenida en los equipos, porque un equipo dañado o perdido se puede volver a comprar y podemos volver a instalar y configurar todas las aplicaciones que tenía. Es caro, pero tenemos el mismo ordenador o mejor; sin embargo, los datos de nuestra empresa son nuestros, nadie nos los puede devolver si se pierden. En este punto nuestra única esperanza son las copias de seguridad y el almacenamiento redundante, que veremos en la Unidad 4.

2.1. Equipos

En cuanto a la seguridad física de los equipos:

- Es fundamental que no se puedan **sustraer,** ni el equipo entero ni alguna pieza del mismo (principalmente el disco duro, pero también el dispositivo donde se hace la copia de seguridad de ese disco).
- En el caso de los portátiles no podemos evitar que salgan de la empresa, porque los trabajadores visitan las dependencias del cliente o se llevan trabajo a casa. Pero sí debemos vigilar que esos ordenadores apliquen **cifrado en el disco duro** y tengan contraseñas actualizadas, sobre todo en los usuarios con perfil de administrador.
- Es importante que no se puedan introducir nuevos **equipos no autorizados.** Un hacker no necesita romper la seguridad de un servidor si puede conectar a la red de la empresa un equipo suyo con el software adecuado para realizar el ataque. O si puede introducir un troyano en algún ordenador de un empleado.
- Aplicaremos **mantenimiento preventivo** para evitar averías. Por ejemplo, en cada ordenador, una vez al año, abrir la caja para limpiar los disipadores y los ventiladores, porque el polvo acumulado puede anular su función de rebajar la temperatura del sistema.

2.2. Aplicaciones

Los ordenadores de una empresa deben tener **las aplicaciones estrictamente necesarias** para llevar a cabo el trabajo asignado: ni más ni menos. Menos es evidente porque impediría cumplir la tarea; pero también debemos evitar instalar software extra porque puede tener **vulnerabilidades** que puedan dañar al sistema completo.

Cuando una empresa adquiere un nuevo equipo, el personal de sistemas procede a **maquetarlo:** instala las aplicaciones utilizadas en esa empresa, cada una en la versión adecuada para esa empresa, con la configuración particular de esa empresa. Incluso puede llegar a sustituir el sistema operativo que traía el equipo por la versión que se utiliza en la empresa. El objetivo perseguido es múltiple:

- Ahorrar al usuario la tarea de instalar y configurar cada aplicación (y de paso evitamos darle demasiados privilegios).
- Asegurar que el software instalado responde a las licencias compradas en la empresa.
- Homogeneizar el equipamiento, de manera que solo tendremos que enfrentarnos a los problemas en una lista reducida de configuraciones de hardware. La solución encontrada se aplica rápidamente a todos los equipos afectados.

Pero debemos estar preparados porque otras aplicaciones intentarán instalarse:

- **Intencionadamente.** El usuario lanza un instalador del programa que ha descargado de Internet o lo trae de casa en un CD/USB.
- **Inocentemente.** El usuario entra en una página pirata que hace la descarga sin que lo sepa, o introduce un CD/USB que desconoce que está infectado por un virus.

En ambos casos, el antivirus será una barrera y la ausencia de privilegios de administración también ayudará. Pero conviene aplicar otras medidas para no ponerlos a prueba:

- A la hora de crear un usuario, evitar que tenga privilegios de administración del sistema. Aunque todavía puede instalar determinadas aplicaciones, solo afectarán a ese usuario, no a todos los de esa máquina.
- Desactivar el mecanismo de autoarranque de aplicaciones desde CD o USB (en algunas empresas, al maquetar los equipos de usuario, incluso quitan los lectores de CD y desactivan los USB de la máquina).

Caso práctico 1

Autoarranque de aplicaciones en sistema Windows

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

Objetivo. Conocer el mecanismo de autoarranque de aplicaciones y los riesgos que conlleva.

Material. Ordenadores con distintas versiones de Windows, pendrive USB.

1. En Windows 95, Microsoft introdujo la funcionalidad llamada AutoRun. El objetivo era facilitar al usuario la instalación de aplicaciones en los ordenadores: bastaba con introducir el CD del programa y automáticamente arrancaba el asistente de instalación.
2. Para que ocurriera así, debía existir un fichero llamado `autorun.inf` en la raíz del CD. En este fichero se indicaba el programa que había que lanzar cuando se insertaba el CD.
3. Sin embargo, un virus puede aprovechar este mecanismo para reproducirse fácilmente, introduciéndose en cada CD que se grabe en esa máquina.
4. Por desgracia, también funciona con los USB. Y utilizamos mucho más los USB que los CD.
5. Vamos a comprobarlo. En un ordenador con XP SP2 insertamos el USB. El sistema lo reconoce y nos pregunta qué queremos hacer con esa unidad (Fig. 1.1). No elegimos nada especial.
6. Ahora nos vamos a la raíz de esa unidad para crear dos ficheros. Uno será una copia del bloc de notas (le llamaremos `bloc.exe`); el otro será un `autorun.inf` que simplemente lanzará ese bloc de notas. El contenido del fichero será (Fig. 1.2):

```
[autorun]
shellexecute=bloc.exe
```

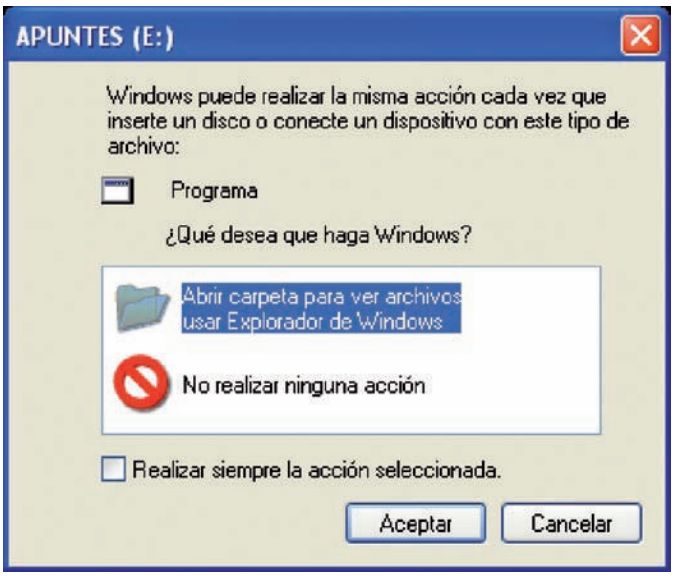


Fig. 1.1. *Acciones posibles.*

```
E:\>copy %windir%\notepad.exe bloc.exe
        1 archivos copiados.

E:\>dir
 El volumen de la unidad E es APUNTES
 El número de serie del volumen es: 4487-EAA9

 Directorio de E:\

21/09/2012  23:07                38 autorun.inf
20/08/2004  12:00            70.144 bloc.exe
               2 archivos         70.182 bytes
               0 dirs   1.001.394.176 bytes libres

E:\>type autorun.inf
[autorun]
shellexecute=bloc.exe
```

Fig. 1.2. *Preparamos la trampa.*

(Continúa)

Caso práctico 1

(Continuación)

7. Listo. Sacamos y volvemos a meter el USB. De nuevo, no elegimos ninguna acción y vamos *Inicio* > *Mi PC* para localizar la unidad correspondiente (Fig. 1.3).

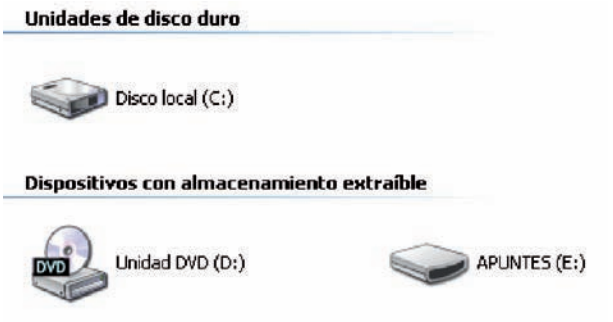


Fig. 1.3. *Localizamos la unidad.*

8. Si hacemos doble clic sobre la unidad E: no aparecerán los ficheros de la unidad, sino que se ejecutará el bloc de notas. Si ese ejecutable tuviera un virus, ya estaríamos infectados.

9. Ahora vamos a un Windows Vista y repetimos la prueba. Al conectar el USB también aparece una ventana de acciones posibles (Fig. 1.4).

10. De nuevo evitamos elegir nada y vamos a *Inicio* > *Equipo* para intentar el doble clic en la unidad. Afortunadamente, se ignora nuestro `autorun.inf` y aparecen los ficheros sin ningún riesgo (Fig. 1.5).



Fig. 1.4. *Acciones en Windows Vista.*

11. Este cambio de comportamiento con los USB ha sido una decisión de Microsoft que afecta a Windows 7, Vista y XP SP3. Está explicado en esta web: **http://goo.gl/NXXVt**.

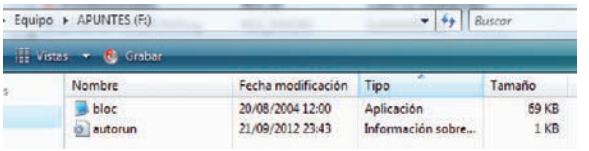


Fig. 1.5. *Lista de ficheros.*

Actividades

2. Discute en clase si resulta conveniente desactivar los USB de los ordenadores de los empleados.

3. Aunque un usuario tenga privilegios limitados en una máquina, ¿todavía es un peligro potencial?

4. ¿Resulta totalmente fiable utilizar las aplicaciones descargadas de Google Play?

La primera garantía que debemos tener a la hora de instalar una aplicación es su **origen:** si ha llegado en un CD del fabricante o si la descargamos de su web, o si está incluida en el mecanismo de actualizaciones automáticas de la versión actual. Si el CD no es original, o si descargamos de la web de otro, debemos desconfiar.

Por ejemplo, en los teléfonos móviles y tabletas la mayoría de las aplicaciones procede de la aplicación oficial del fabricante (Google Play en Android, App Store en iPhone). Utilizamos su opción de búsqueda, miramos que el número de descargas sea elevado y la bajamos. Durante la instalación nos pide permiso para hacer algunas cosas en el equipo, aunque no tiene mucho sentido porque el 99 % de los usuarios no sabe qué le está preguntando y siempre acepta. En el fondo, confiamos en que la aplicación no es peligrosa porque la hemos encontrado en el sitio oficial, donde se supone que la prueban antes de colgarla.

2.3. Datos

Como hemos dicho antes, las máquinas y las aplicaciones se compran; pero los datos de nuestra empresa son exclusivamente suyos. Hay que protegerlos por dos aspectos:

- Si desaparecen, la empresa no puede funcionar con normalidad.
- Si llegan a manos de la competencia, la estrategia empresarial y el futuro de la compañía están en riesgo.

Las empresas modernas responden al esquema de «oficina sin papeles»: están informatizados todos los datos que entran, los generados internamente y los que comunicamos al exterior. La infraestructura necesaria es amplia y compleja porque los niveles de seguridad son elevados:

- Todos los equipos deben estar especialmente **protegidos contra software malicioso** que pueda robar datos o alterarlos.
- El almacenamiento debe ser **redundante:** grabamos el mismo dato en más de un dispositivo. En caso de que ocurra un fallo de hardware en cualquier dispositivo, no hemos perdido la información.
- El almacenamiento debe ser **cifrado.** Las empresas manejan información muy sensible, tanto los datos personales de clientes o proveedores como sus propios informes, que pueden ser interesantes para la competencia. Si, por cualquier circunstancia, perdemos un dispositivo de almacenamiento (disco duro, pendrive USB, cinta de backup), los datos que contenga deben ser inútiles para cualquiera que no pueda descifrarlos.

2.4. Comunicaciones

Los datos no suelen estar recluidos siempre en la misma máquina: en muchos casos salen con destino a otro usuario que los necesita. Esa transferencia (correo electrónico, mensajería instantánea, disco en red, servidor web) también hay que protegerla. Debemos utilizar **canales cifrados,** incluso aunque el fichero de datos que estamos transfiriendo ya esté cifrado (doble cifrado es doble obstáculo para el atacante).

Además de proteger las comunicaciones de datos, también es tarea de la seguridad informática **controlar las conexiones** a la red de la empresa. Sobre todo con la expansión del **teletrabajo,** que permite aprovechar Internet para trabajar en la red interna como si estuviéramos sentados en una mesa de la oficina. Ahora las redes de las empresas necesitan estar más abiertas al exterior, luego estarán más expuestas a ataques desde cualquier parte del mundo.

El peligro también está **en la propia oficina:** no puede ser que cualquier visitante entre en nuestra red con solo conectar su portátil a una toma de la pared o a través del wifi de la sala de espera. Un hacker seguramente no conoce los usuarios y contraseñas de los administradores de cada máquina; pero puede introducir software malicioso que intente adivinarlo, aprovechar vulnerabilidades no resueltas en nuestras aplicaciones para desplegar gusanos que ralenticen el rendimiento de la red, etc.

Un segundo objetivo de la supervisión de las comunicaciones es evitar la llegada de correo no deseado **(spam)** y **publicidad** en general. Con ello liberamos parte de la ocupación de la conexión a Internet, reducimos la carga de los servidores de correo (así como la ocupación de disco), nuestros usuarios no sufrirán distracciones y finalmente evitamos ataques camuflados en esos correos.

La tendencia actual en las empresas es migrar sus sistemas a Internet. Es el llamado **cloud computing.** Las más atrasadas todavía se limitan a disponer del servicio de correo electrónico con su propio dominio (@miempresa.es) y colgar la página web en algún servidor compartido (hosting); pero muchas ya utilizan el almacenamiento en web (por ejemplo, Dropbox y Google Drive para usuarios individuales; S3 de Amazon para empresas) y algunas están desplazando toda su infraestructura informática a servidores virtuales situados en algún punto del planeta con conexión a Internet (de nuevo Amazon con su EC2).

Realmente hace mucho que utilizamos cloud computing: todos los webmail (Gmail, Hotmail, etc.) son servicios de correo electrónico que no están en nuestros ordenadores, sino que nos conectamos a ellos mediante un navegador para enviar, recibir y leer los mensajes, sin importarnos cuántos servidores o equipos de red ha necesitado desplegar esa empresa para que todo funcione con normalidad.

Sea cual sea el grado de adopción de cloud computing en una empresa, la primera premisa debe ser la seguridad en las comunicaciones, porque todos esos servicios están en máquinas remotas a las que llegamos atravesando redes de terceros.



Web

Las redes de telefonía móvil no son inmunes a los ataques:
http://goo.gl/7Xt6r
Los teléfonos por satélite, tampoco:
http://goo.gl/KpZYu

3. Definiciones

Para fijar los conceptos relacionados con la seguridad informática vamos a intentar elaborar un pequeño diccionario. Utilizaremos ejemplos de la vida real para comprobar que la seguridad está en todas partes, no solo en los ordenadores.

3.1. Seguridad física/lógica, activa/pasiva

La **seguridad física** cubre todo lo referido a los **equipos** informáticos: ordenadores de propósito general, servidores especializados y equipamiento de red. La **seguridad lógica** se refiere a las distintas **aplicaciones** que ejecutan en cada uno de estos equipos.

Las **amenazas contra la seguridad física** son:

- **Desastres naturales** (incendios, inundaciones, hundimientos, terremotos). Los tenemos en cuenta a la hora de ubicar el emplazamiento del centro de proceso de datos (CPD), donde alojamos los principales servidores de la empresa; pero, aunque tengamos el mejor sistema de extinción de incendios o la sala esté perfectamente sellada, siempre deberíamos tener un segundo CPD para que la actividad no pare.
- **Robos.** Nuestros equipos, y sobre todo la información que contienen, resultan valiosos para otros individuos u organizaciones. Debemos proteger el acceso a la sala del CPD mediante múltiples medidas de seguridad: vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc.
- **Fallos de suministro.** Los ordenadores utilizan corriente eléctrica para funcionar y necesitan redes externas para comunicar con otras empresas y con los clientes. Estos servicios los contrataremos con determinados suministradores, pero debemos estar preparados para las ocasiones en que no puedan proporcionarlo: unas baterías o un grupo electrógeno por si falla la corriente, una segunda conexión a Internet como línea de backup —incluso podemos optar por una solución inalámbrica— para estar protegidos ante un corte en la calle.

Las **amenazas contra la seguridad lógica** son:

- **Virus, troyanos y malware** en general. Como ocurre con el spam en el correo electrónico, el malware es software no deseado y que debemos **eliminar.**
- **Pérdida de datos.** Un defecto en el código fuente de una aplicación, o una configuración defectuosa de la misma, puede ocasionar modificaciones inexplicables en la información almacenada, incluso la pérdida de datos. Para reducir este riesgo, las empresas prueban muy bien una aplicación antes de decidir utilizarla y, sobre todo, realizan copias de seguridad en varios puntos del procesamiento de la información para poder recuperarse sin perderlo todo.
- **Ataques a las aplicaciones de los servidores.** Los hackers intentarán entrar a por los datos aprovechando cualquier vulnerabilidad del sistema operativo o de las aplicaciones que ejecutan en esa máquina (por eso conviene tener instalado el software mínimo imprescindible).

Por otro lado, podemos hablar de seguridad activa y seguridad pasiva.

La **seguridad pasiva** son todos los mecanismos que, cuando sufrimos un ataque, nos permiten **recuperarnos** razonablemente bien. Por ejemplo, las baterías ante una caída de tensión o la copia de seguridad cuando se ha estropeado la información de un disco.

La **seguridad activa** intenta **protegernos de los ataques** mediante la adopción de medidas que protejan los activos de la empresa, como vimos en el epígrafe anterior: equipos, aplicaciones, datos y comunicaciones.

Vocabulario

Malware se refiere al software que se diseña e implementa para causar daño a quien, inocentemente, lo instale. Los antivirus intentan detectar y eliminar estos programas antes de que infecten el sistema.

3.2. Confidencialidad, disponibilidad, integridad y no repudio

La **confidencialidad** intenta que la información solo sea utilizada por las personas o máquinas debidamente **autorizadas.** Para garantizar la confidencialidad necesitamos disponer de tres tipos de mecanismos:

- **Autenticación.** La autenticación intenta confirmar que una persona o máquina es quien dice ser, que no estamos hablando con un impostor.
- **Autorización.** Una vez autenticado, los distintos usuarios de la información tendrán distintos privilegios sobre ella. Básicamente dos: solo lectura, o lectura y modificación.
- **Cifrado.** La información estará cifrada para que sea inútil para cualquiera que no supere la autenticación.

Veamos algunos ejemplos del mundo real:

- Para entrar a un estadio de fútbol se necesita una entrada (autenticación); pero unos irán a tribuna y otros a un palco VIP (autorización).
- Para sacar dinero de un cajero necesitas una tarjeta y el PIN de esa tarjeta (autenticación).
- Al recoger un envío certificado necesitas llevar el DNI, para que comprueben que eres tú (autenticación).
- En los parques temáticos hay que llevar una entrada (autenticación) y, si pagas un poco más, tienes un fast-pass para no hacer cola en las atracciones (autorización).

El objetivo de la **integridad** es que los datos queden almacenados tal y como espera el usuario: que no sean alterados sin su **consentimiento.** Un ejemplo sería el identificador de la cuenta bancaria, que tiene cuatro grupos de números:

- Cuatro dígitos del código del banco.
- Cuatro dígitos del código de la sucursal del banco donde hemos abierto la cuenta.
- Dos dígitos de control.
- Diez dígitos para el código de la cuenta, dentro de todas las abiertas en esa sucursal.

Los dígitos de control se obtienen por combinación numérica de los otros 18 números. Esa combinación es una operación matemática que nos asegura que cualquier pequeño cambio en alguno de los 18 números generaría unos dígitos de control distintos. Es decir, si queremos hacer una transferencia bancaria por teléfono y, al dictar el número de cuenta, cambiamos sin querer alguno de los dígitos (da igual cualquiera de los 20), quien apunta ese número de cuenta no podrá operar con ella porque es un número inválido, ya que los dígitos de control no corresponden a los otros 18.

La **disponibilidad** intenta que los usuarios puedan acceder a los servicios con **normalidad** en el horario establecido. Para ello se invierte en sobredimensionar los recursos:

- Una tienda tiene dos datáfonos con dos bancos distintos. Así siempre puede ofrecer el cobro por tarjeta.
- Un equipo de fútbol tiene varios suplentes en el banquillo. Así siempre puede intentar mantener once jugadores cuando alguno se lesiona.
- Los aviones llevan piloto y copiloto.
- Cuando se hacen obras entre dos estaciones de metro, hay una línea de autobuses que lleva de una a otra por superficie, y el ticket es el mismo.

El **no repudio** se refiere a que, ante una relación entre dos partes, intentaremos evitar que cualquiera de ellas pueda **negar** que participara en esa relación. Hay muchos ejemplos de la vida real:

- Los contratos se firman por las dos partes. Por ejemplo, la hipoteca de una casa.
- Firmamos el impreso de matriculación en un ciclo formativo.
- En algunas tarjetas de crédito hay que firmar un papel con los datos de la compra, y la tienda se queda una copia.

Actividades

5. Busca el algoritmo matemático que permite obtener la letra del DNI a partir de los números del mismo. Compruébalo con tu DNI y el de algún compañero.

- Conservamos el ticket de compra para poder solicitar la devolución.
- Cuando hacemos una reserva de vuelo obtenemos un localizador; a la hora de retirar el billete no pueden negar que hicimos la reserva.

Caso práctico 2

Comprobación de integridad en Linux

Duración: 10 minutos **Dificultad**: Fácil

Objetivo. Utilizar la suma de comprobación de ficheros.

Material. Ordenador con Linux Ubuntu 12.04.

1. En Linux el comando `sum` permite obtener de un fichero el equivalente al dígito de control de la cuenta bancaria. Si modificamos el fichero, el valor devuelto por `sum` cambia. La secuencia de comandos sería (Fig. 1.6):

```
alumno@alumno-VirtualBox:~$ echo esto es una prueba >a
alumno@alumno-VirtualBox:~$ cat a
esto es una prueba
alumno@alumno-VirtualBox:~$ sum a
01578     1
alumno@alumno-VirtualBox:~$ echo mas >>a
alumno@alumno-VirtualBox:~$ cat a
esto es una prueba
mas
alumno@alumno-VirtualBox:~$ sum a
00204     1
```

Fig. 1.6. *Ejemplo de sum.*

```
$ echo esto es una prueba > a
$ sum a
01578 1
$ echo mas >>a
$ sum a
00204 1
```

2. Por tanto, si nos han enviado un fichero, para comprobar que ha llegado bien deberíamos preguntar al emisor cuál es el sum en su máquina, y compararlo con el sum del fichero que hemos recibido.
3. En algunos ficheros pequeños, el comando `sum` puede fallar y generar el mismo par de números, aunque efectivamente se hayan producido algunos cambios. Es más fiable el comando `cksum` (Fig. 1.7).

```
alumno@alumno-VirtualBox:~$ echo esto es una prueba >a
alumno@alumno-VirtualBox:~$ cat a
esto es una prueba
alumno@alumno-VirtualBox:~$ cksum a
3690535080 19 a
alumno@alumno-VirtualBox:~$ echo mas >>a
alumno@alumno-VirtualBox:~$ cksum a
1738197011 23 a
alumno@alumno-VirtualBox:~$
```

Fig. 1.7. *Ejemplo de cksum.*

Actividades

6. En los primeros Unix el usuario root estaba disponible para entrar al sistema; actualmente no. ¿Por qué?
7. En las webs de los bancos puedes entrar con un usuario y contraseña. Pero para realizar transferencias a otras cuentas solicitan una nueva autenticación. ¿Cuál?
8. En la película *La amenaza de Andrómeda*, la autodestrucción del laboratorio solo se podía detener de una forma. ¿Cómo?

3.3. Sabes-tienes-eres

La autenticación es especialmente importante en temas de seguridad. Debemos estar muy seguros de la identidad de la persona o sistema que solicita acceder a nuestra información. Un esquema muy utilizado para analizar la autenticación es clasificar las medidas adoptadas según tres criterios:

- **Algo que sabes.** Para acceder al sistema necesitas conocer alguna palabra secreta: la típica contraseña.
- **Algo que tienes.** En este caso es imprescindible aportar algún elemento material: generalmente una tarjeta.
- **Algo que eres.** El sistema solicita reconocer alguna característica física del individuo (biometría): huella dactilar, escáner de retina, reconocimiento de voz, etc.

La autenticación será más fiable cuantos más criterios distintos cumpla:

- Para entrar en casa solamente nos hace falta una llave (algo que tienes). Pero en algunos países europeos los portales tienen un código (algo que sabes).
- Para entrar a un ordenador, generalmente necesitamos un usuario (algo que sabes) y una contraseña (algo que sabes).
- Para sacar dinero de un cajero necesitamos una tarjeta (algo que tienes) e introducir un PIN (algo que sabes). En cambio, en la web del banco solo necesitamos un usuario (que suele ser nuestro DNI, relativamente fácil de localizar) y un PIN (algo que sabes).

- Para recoger en Correos un envío certificado o para identificarte a la Policía, necesitas llevar tu DNI (algo que tienes) y que sea tu cara la que aparece (algo que eres).

Los sistemas biométricos no siempre se aplican en entornos de muy alta seguridad. Por ejemplo, pueden estar en el comedor de la empresa, comprobando quién es empleado y quién no para decidir solicitar el pago del menú.

3.4. AAA

La sigla **AAA** se refiere a **autenticación, autorización y accounting.** Las dos primeras ya las hemos visto con anterioridad; la tercera se refiere a la información interna que los sistemas generan acerca de sí mismos. Concretamente, el uso que se hace de sus servicios. Esta información sirve para revisar el dimensionado de los equipos y, debidamente asociada a cada departamento de la empresa, permite establecer limitaciones y penalizaciones.

Pero la información del accounting también permite comprobar la eficacia de las medidas de autenticación y autorización, sobre todo en un **análisis forense** tras un ataque. Siguiendo el rastro podremos localizar por dónde ha entrado e intentar resolverlo.

Por este motivo, es importante que el registro del accounting se haga en una **máquina distinta:** si el hacker ha conseguido entrar, puede fácilmente borrar sus huellas. Sin embargo, si el registro se hace simultáneamente en otra máquina, ya son dos las máquinas que debe atacar (y generalmente la máquina de registro se carga con el mínimo software posible, para reducir las opciones de entrada).

3.5. e2e

e2e significa **extremo a extremo:** la seguridad debe controlarse en el origen de los datos, en el destino de los datos y en el canal de comunicación utilizado entre origen y destino:

- En el origen y en el destino intentaremos que el equipo y las aplicaciones no hayan sido modificados. Si alguno no está bajo nuestro control, debemos desconfiar.
- En el canal intentaremos limitar quién accede y, sobre todo, cifraremos, porque nuestros datos atravesarán las redes de otras compañías. Sobre sus equipos y el personal que opera con ellos no tenemos ningún control, luego debemos desconfiar.

Web

Podemos convertirnos en peritos informáticos forenses con este curso:

http://goo.gl/TgCyA

En este artículo podemos ampliar la información sobre seguridad extremo a extremo:

http://goo.gl/qi0Br

3.6. Vulnerabilidad, malware, exploit

El software está hecho por humanos, luego debemos estar preparados para sufrir los errores introducidos durante su programación. Pueden ser leves (algún mensaje mal traducido), graves (corrupción de datos) y críticos (un agujero de seguridad da acceso libre a datos confidenciales).

Una **vulnerabilidad** es un defecto de una aplicación que puede ser aprovechado por un atacante. Si lo descubre, el atacante programará un software (llamado **malware**) que utiliza esa vulnerabilidad para tomar el control de la máquina **(exploit)** o realizar cualquier operación no autorizada.

Hay tres tipos de vulnerabilidades:

- **Vulnerabilidades reconocidas** por el suministrador de la aplicación y para las cuales ya tiene un **parche** que las corrige. Si nuestra empresa utiliza esa aplicación, debemos aplicar el parche inmediatamente.
- **Vulnerabilidades reconocidas** por el suministrador, pero todavía **no hay un parche.** En algunos casos sí se proporciona una solución temporal **(workaround),** pero, generalmente, lo mejor es desactivar el servicio hasta haber aplicado el parche.
- **Vulnerabilidades no reconocidas** por el suministrador. Es el peor caso, porque podemos estar expuestos a un ataque durante un tiempo largo sin saberlo.

Web

Aquí tenemos un exploit contra Joomla!

http://goo.gl/Ek4vA

En este vídeo nos hablan sobre la importancia del malware:

http://goo.gl/BfcJw

Los fabricantes de software intentan reaccionar rápidamente ante cualquier informe que demuestre una vulnerabilidad en sus programas. Gracias a Internet, de manera programada, los programas conectan con la web de su suministrador para comprobar si hay algún parche pendiente de aplicar **(actualizaciones automáticas).** Es decir, no esperan a que el administrador de la máquina compruebe uno a uno el estado de todos los programas instalados, porque puede pasar un tiempo precioso desde que se libera el parche hasta que el administrador se entera, lo descarga y lo aplica.

Hay muchos tipos de malware:

- **Virus.** Intentan dejar inservible el ordenador infectado. Pueden actuar aleatoriamente o esperar una fecha concreta (por ejemplo, Viernes 13).
- **Gusanos.** Van acaparando todos los recursos del ordenador: disco, memoria, red. El usuario nota que el sistema va cada vez más lento, hasta que no hay forma de trabajar.
- **Troyanos.** Suelen habilitar puertas traseras en los equipos: desde otro ordenador podemos conectar con el troyano para ejecutar programas en el ordenador infectado.

Realmente no es tan importante qué malware nos ha entrado: hay que **eliminarlo** de todas formas porque es una aplicación que no hemos querido instalar y que no nos traerá nada bueno (incluso puede mutar: un gusano convertirse en troyano, etc.).

Todos tienen en común su afán de **replicación:** intentan contaminar el máximo número de ordenadores posible para continuar la infección.

También hay que tener cuidado con los **falsos antivirus.** En algunas páginas web peligrosas (servicios de descargas ilegales, por ejemplo) aparece un mensaje que nos avisa de que estamos infectados y se ofrecen amablemente para descargar un antivirus que nos limpiará el ordenador.

Si pulsamos en el enlace y descargamos e instalamos ese programa, lo que realmente ocurre es que hemos dejado entrar un malware que, desde ese instante, puede hacer cualquier cosa: lanzar anuncios sin parar, instalar otros virus, abrir una puerta trasera para convertirnos en ordenador zombi en algún ataque organizado, robar datos personales (imágenes, vídeos), etc.

En algunos casos, el virus da la cara y directamente nos dice que ha **secuestrado** nuestro ordenador. Efectivamente: ya no podemos hacer nada con el teclado ni el ratón. Para recuperar la máquina hay que introducir una contraseña que solo nos la proporcionan tras efectuar un pago económico (es decir, piden un rescate).

Por supuesto, el primer aviso era falso; seguramente, al entrar de nuevo en esa página, seguirá apareciendo. Si bien es cierto que los navegadores pueden realizar análisis del disco duro buscando virus (los llamados **antivirus on-line,** como Panda Activescan), para ello necesitan la **instalación previa** de un software específico para esa tarea de buscar virus. Después podrán avisar o no, dependiendo de lo que encuentren; pero nunca aparecerá un aviso solo por entrar a una página.

Lo mismo puede ocurrir con programas que nos aseguran que acelerarán el rendimiento del ordenador, o el disco duro, o la conexión a Internet. Estos programas existen, pero debemos descargarlos desde **fuentes de toda confianza,** como las webs de los autores de ese software o un sitio con buena reputación (Softonic, CNET, etc.).

Para evitar que ocurra, lo mejor es tener siempre activado el antivirus (y tenerlo actualizado, claro). Y, si por cualquier razón, el ordenador ya está secuestrado, algunos antivirus tienen la opción de ejecutarse desde un **LiveCD.** Es decir, descargamos desde la web del fabricante del antivirus una imagen que grabamos en un CD. Esa imagen lleva un minisistema operativo y el programa del antivirus. Arrancamos el ordenador desde ese CD y podemos hacer una limpieza a fondo, con la tranquilidad de que el virus no se ha activado porque no está funcionando el sistema operativo del disco duro.

4. Tipos de ataques

Una vez que alguien está decidido a atacarnos, puede elegir alguna de estas formas:

- **Interrupción.** El ataque consigue provocar un corte en la prestación de un servicio: el servidor web no está disponible, el disco en red no aparece o solo podemos leer (no escribir), etc.
- **Interceptación.** El atacante ha logrado acceder a nuestras comunicaciones y ha copiado la información que estábamos transmitiendo.
- **Modificación.** Ha conseguido acceder, pero, en lugar de copiar la información, la está modificando para que llegue alterada hasta el destino y provoque alguna reacción anormal. Por ejemplo, cambia las cifras de una transacción bancaria.
- **Fabricación.** El atacante se hace pasar por el destino de la transmisión, por lo que puede tranquilamente conocer el objeto de nuestra comunicación, engañarnos para obtener información valiosa, etc.

Para conseguir su objetivo puede aplicar una o varias de estas técnicas:

- **Ingeniería social.** A la hora de poner una contraseña, los usuarios no suelen utilizar combinaciones aleatorias de caracteres. En cambio, recurren a palabras conocidas para ellos: el mes de su cumpleaños, el nombre de su calle, su mascota, su futbolista favorito, etc. Si conocemos bien a esa persona, podemos intentar adivinar su contraseña.

  También constituye ingeniería social pedir por favor a un compañero de trabajo que introduzca su usuario y contraseña, que el nuestro parece que no funciona. En esa sesión podemos aprovechar para introducir un troyano, por ejemplo.
- **Phishing.** El atacante se pone en contacto con la víctima (generalmente, un correo electrónico) haciéndose pasar por una empresa con la que tenga alguna relación (su banco, su empresa de telefonía, etc.). En el contenido del mensaje intenta convencerle para que pulse un enlace que le llevará a una (falsa) web de la empresa. En esa web le solicitarán su identificación habitual y desde ese momento el atacante podrá utilizarla.
- **Keyloggers.** Un troyano en nuestra máquina puede tomar nota de todas las teclas que pulsamos, buscando el momento en que introducimos un usuario y contraseña. Si lo consigue, los envía al atacante.
- **Fuerza bruta.** Las contraseñas son un número limitado de caracteres (letras, números y signos de puntuación). Una aplicación malware puede ir generando todas las combinaciones posibles y probarlas una a una; tarde o temprano, acertará. Incluso puede ahorrar tiempo si utiliza un diccionario de palabras comunes y aplica combinaciones de esas palabras con números y signos de puntuación.

  Contra los ataques de fuerza bruta hay varias medidas:

  – Utilizar contraseñas no triviales. No utilizar nada personal e insertar en medio de la palabra o al final un número o un signo de puntuación. En algunos sistemas nos avisan de la fortaleza de la contraseña elegida (Fig. 1.8).

  – Cambiar la contraseña con frecuencia (un mes, una semana). Dependiendo del hardware utilizado, los ataques pueden tardar bastante; si antes hemos cambiado la clave, se lo ponemos difícil.

  – Impedir ráfagas de intentos repetidos. Nuestro software de autenticación que solicita usuario y contraseña fácilmente puede detectar varios intentos consecutivos en muy poco tiempo. No puede ser un humano: debemos responder introduciendo una espera. En Windows se hace: tras cuatro intentos fallidos, el sistema deja pasar varios minutos antes de dejarnos repetir. Esta demora alarga muchísimo el tiempo necesario para completar el ataque de fuerza bruta.

Actividades

9. Busca información sobre la iniciativa *Confianza online*. ¿Qué te parece?

10. ¿Cómo detectarías un ataque DoS? ¿Qué harías para defenderte?

– Establecer un máximo de fallos y después bloquear el acceso. Es el caso de las tarjetas SIM que llevan los móviles GSM/UMTS: al tercer intento fallido de introducir el PIN para desbloquear la SIM, ya no permite ninguno más. Como el PIN es un número de cuatro cifras, la probabilidad de acertar un número entre 10 000 en tres intentos es muy baja.

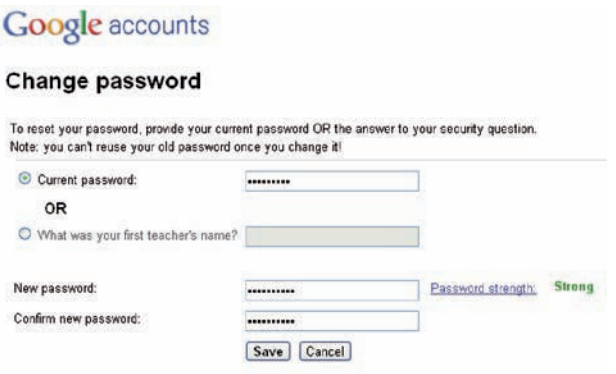


Fig. 1.8. *Fortaleza de contraseña.*

- **Spoofing.** Alteramos algún elemento de la máquina para hacernos pasar por otra máquina. Por ejemplo, generamos mensajes con la misma dirección que la máquina auténtica.
- **Sniffing.** El atacante consigue conectarse en el mismo tramo de red que el equipo atacado. De esta manera tiene acceso directo a todas sus conversaciones.
- **DoS** (Denial of Service, denegación de servicio). Consiste en tumbar un servidor saturándolo con falsas peticiones de conexión. Es decir, intenta simular el efecto de una carga de trabajo varias veces superior a la normal.
- **DDoS** (Distributed Denial of Service, denegación de servicio distribuida). Es el mismo ataque DoS, pero ahora no es una única máquina la que genera las peticiones falsas (que es fácilmente localizable y permite actuar contra ella), sino muchas máquinas repartidas por distintos puntos del planeta. Esto es posible porque todas esas máquinas han sido infectadas por un troyano que las ha convertido en ordenadores zombis (obedecen las órdenes del atacante).

4.1. Tipos de atacantes

Se suele hablar de hacker de manera genérica para referirse a un individuo que se salta las protecciones de un sistema. A partir de ahí podemos distinguir entre:

- **Hacker.** Ataca la defensa informática de un sistema solo por el reto que supone hacerlo. Si tiene éxito, moralmente debería avisar a los administradores sobre los agujeros de seguridad que ha utilizado, porque están disponibles para cualquiera.
- **Cracker.** También ataca la defensa, pero esta vez sí quiere hacer daño: robar datos, desactivar servicios, alterar información, etc.
- **Script kiddie.** Son aprendices de hacker y cracker que encuentran en Internet cualquier ataque y lo lanzan sin conocer muy bien qué están haciendo y, sobre todo, las consecuencias derivadas de su actuación (esto les hace especialmente peligrosos).
- **Programadores de malware.** Expertos en programación de sistemas operativos y aplicaciones capaces de aprovechar las vulnerabilidades de alguna versión concreta de un software conocido para generar un programa que les permita atacar.
- **Sniffers.** Expertos en protocolos de comunicaciones capaces de procesar una captura de tráfico de red para localizar la información interesante.
- **Ciberterrorista.** Cracker con intereses políticos y económicos a gran escala.

Web

En esta web puedes probar la fortaleza de las contraseñas que usas habitualmente:

http://goo.gl/bzsne

A veces, un hacker es contratado por la compañía a la que ha perjudicado. Aunque esa relación no suele durar mucho tiempo:

http://goo.gl/zuyja

Algún ayuntamiento ha sufrido robos de hackers en sus cuentas bancarias:

http://goo.gl/0x8EW

5. Buenas prácticas

Es muy dura la tarea del responsable de seguridad informática en una empresa grande: hay mucha información que proteger y múltiples puertas por donde sufrir intrusiones. Sus funciones son:

- **Localizar los activos que hay que proteger:** equipos, aplicaciones, datos y comunicaciones. Sobre todo, revisar la **política de copias de seguridad:** qué copiamos, cuándo copiamos, dónde lo copiamos, dónde guardamos de manera segura los dispositivos de copia, cómo verificamos que la copia se ha hecho bien, cuándo hacemos una prueba de recuperación de una copia, etc.
- Redactar y revisar regularmente los **planes de actuación ante catástrofes,** contemplando todas las posibilidades: ataque intencionado, desastre natural, arranque parcial de servicios (pocos servicios o todos los servicios pero con menor capacidad).
- No instalar nada que no sea **estrictamente necesario,** y **revisar la configuración** de los sistemas y aplicaciones por si estamos otorgando más permisos de los imprescindibles.
- Estar al día de todos los informes de seguridad que aparezcan. Para ello hay que registrarse en **listas de correo** sobre seguridad y, además, en las listas de nuestros proveedores (tanto de hardware como de software) para recibir sus noticias directamente.
- Activar los mecanismos de **actualización automática** de las aplicaciones que tenemos instaladas. Salvo sistemas delicados (tenemos que probar muy bien cada actualización antes de aplicarla), en general los fabricantes liberan actualizaciones que no dan problemas.
- Dar **formación a los usuarios** para que utilicen la seguridad y la vean como una ayuda, no como un estorbo.
- **Revisar los log** del sistema (el accounting que hemos visto antes). Algunas herramientas nos ayudan porque recogen los ficheros de log y aplican fácilmente muchos patrones conocidos (buscar la palabra *error* o *warning,* etc.).
- Considerar la opción de contratar una **auditoría externa,** porque si hemos cometido un error de concepto, es muy difícil que lo encontremos por nosotros mismos.
- Revisar la **lista de equipos conectados:** pueden haber introducido equipos no autorizados.
- Revisar la **lista de usuarios activos:** puede que algún empleado ya no esté en la empresa pero su usuario y todos los privilegios asociados siguen disponibles para él o para alguien de su confianza.
- En aquellos sistemas que lo permitan, configurar el **aviso por SMS o correo electrónico** para que nos enteremos los primeros de cualquier problema. Por ejemplo, los sistemas de baterías (SAI [sistema de alimentación ininterrumpida]) suelen tener esta funcionalidad.

Formalmente hay una serie de **estándares** sobre la seguridad informática. La normativa **ISO/IEC 27002:2009** trata sobre la gestión de la seguridad de la información. En ella se propone implantar controles para afrontar los riesgos inherentes a los sistemas informáticos. Los controles incluyen políticas de empresa, estructura de la organización y procedimientos. Los controles se aplican a todas las partes afectadas: gestión de activos, seguridad sobre los recursos humanos (antes, durante y después de pertenecer a la empresa), seguridad física y ambiental, gestión de comunicaciones y operaciones, control de acceso, etc.

La segunda referencia mundial son las normas **ITIL** (Information Technology Infrastructure Library), que están orientadas a la gestión de servicios de tecnologías de la información, y uno de los aspectos que cubren es la seguridad.



Web

Visita alguna web de avisos de seguridad, como CERT o INTECO.



Importante

Aunque los navegadores nos intentan facilitar la vida ofreciendo recordar la contraseña que introducimos en una página web, no es recomendable hacerlo porque, si alguien se sienta a nuestro ordenador, entrará directamente en esas páginas con nuestra identidad y privilegios.

6. Legislación

Como en el mundo real, romper la seguridad informática de una empresa para robar sus datos es un delito perseguido por la ley. También el desarrollo de Internet ha impulsado la aparición de leyes completamente nuevas, como la que regula el comercio electrónico.

6.1. LOPD

La Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999, de 13 de diciembre) establece las bases para proteger el **tratamiento de los datos de carácter personal de las personas físicas.** Estos datos pueden estar en cualquier tipo de soporte, digitalizado o no. La ley establece cómo se pueden tomar los datos, qué tipo de almacenamiento protegido necesitan y qué derecho y obligaciones tiene el ciudadano sobre esos datos suyos en manos de terceros.

El Real Decreto 1720/2007, de 21 de diciembre, desarrolla la LOPD para **ficheros** (automatizados y no automatizados). Define tres tipos de medidas en función de la sensibilidad de los datos tratados:

- **Nivel básico.** Cualquier fichero de datos de carácter personal. Las medidas de seguridad con estos datos son:
  - Identificar y autenticar a los usuarios que pueden trabajar con esos datos.
  - Llevar un registro de incidencias acontecidas en el fichero.
  - Realizar copia de seguridad como mínimo semanalmente.
- **Nivel medio.** Cuando los datos incluyen información sobre infracciones administrativas o penales, informes financieros y de gestión tributaria y datos sobre la personalidad del sujeto. Las medidas de seguridad incluyen las del nivel básico más:
  - Al menos una vez cada dos años una auditoría externa verificará los procedimientos de seguridad.
  - Debe existir control de acceso físico a los medios de almacenamiento de los datos.
- **Nivel alto.** Son los datos especialmente protegidos: ideología, vida sexual, origen racial, afiliación sindical o política, historial médico, etc. Las medidas de seguridad amplían las de nivel medio:
  - Cifrado de las comunicaciones.
  - Registro detallado de todas las operaciones sobre el fichero, incluyendo usuario, fecha y hora, tipo de operación y resultado de la autenticación y autorización.

6.2. LSSI-CE

La Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE 34/2002, de 11 de julio) intenta cubrir el hueco legal que había con las empresas que prestan **servicios de la sociedad de la información:**

- Las obligaciones de los prestadores de servicio, incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones.
- Las comunicaciones comerciales por vía electrónica.
- La información previa y posterior a la celebración de contratos electrónicos.
- Las condiciones relativas a su validez y eficacia.
- El régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

Actividades

11. En algún documento oficial de toma de datos personales, busca el aviso que detalla tus derechos sobre los datos que estás aportando.

12. Esta misma información está disponible junto a las cámaras de seguridad que graban espacios públicos. Busca alguna y trae una foto a clase.

13. ¿Cuáles son las funciones de la Agencia de Protección de Datos (APD)?

Web

Las sanciones por no cumplir la LOPD son elevadas multas. Son frecuentes entre las empresas del sector de las telecomunicaciones.

http://goo.gl/HdvBr

La ley es de obligado cumplimiento para todas las webs que consiguen algún tipo de ingreso, bien directo (pago de cuotas, venta de productos y servicios), bien indirecto (publicidad). La primera obligación que tienen es incluir en su página **información de la persona o empresa** que está detrás de esa página: nombre o denominación social, dirección postal, datos de inscripción en el registro de la propiedad mercantil, etc.

6.3. LPI

La Ley de Propiedad Intelectual (LPI) establece los **derechos de autor en los entornos digitales.** Considera la digitalización de un contenido como un acto de reproducción, luego se necesita autorización expresa del titular del contenido.

Como excepción incluye la **copia privada,** que es para uso personal del dueño de ese contenido legalmente adquirido. La copia, al igual que el original, no se puede utilizar de manera colectiva ni lucrativa.

Para compensar a los autores por estas copias no controladas, se establece un **canon** sobre los distintos dispositivos de almacenamiento. Este canon revierte en las sociedades de autores.

6.4. Administración electrónica

La Administración electrónica hace referencia al esfuerzo de todos los estamentos públicos para adaptar sus procedimientos a las nuevas tecnologías. Así evitan seguir manejando papeles, y los ciudadanos y empresas pueden relacionarse con la Administración de manera telemática.

Poder resolver los trámites por Internet tiene múltiples ventajas:

- Disponibilidad las 24 horas del día. No hace falta pedir permiso en el trabajo; incluso podemos hacerlo en días festivos y fines de semana.
- Facilidad de acceso. Los portales de la Administración incorporan múltiples asistentes que proporcionan toda la ayuda necesaria.
- Ahorro de tiempo. No hay que desplazarse hasta una oficina y esperar turno para ser atendido.
- Fiabilidad. Los procedimientos ya no dependen de personas, sino de sistemas.

La realidad es que muchas webs todavía se limitan a ofrecer la descarga del PDF del mismo formulario para que lo pasemos a papel y lo entreguemos en mano o por correo certificado. En contadas excepciones se completa el procedimiento: rellenar un formulario y enviarlo a un servidor donde nos acepten la solicitud y nos proporcionen información puntual sobre el estado de su tramitación.

El DNI electrónico (DNIe) supuso un punto de inflexión porque ahora el ciudadano sí dispone de una autenticación fiable. Pero todavía está lejos de ser ampliamente utilizado, sobre todo en el sector privado.

Web

La implantación de administración electrónica supone un importante ahorro:
http://goo.gl/gBbhv

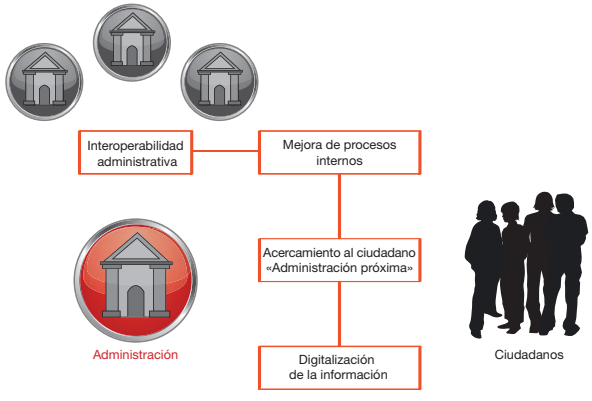


Fig. 1.9. *Ventajas de la Administración electrónica.*

Síntesis

Nuestra sociedad se basa en información procesada digitalmente: hay que protegerla porque la información es poder.

La seguridad completa es imposible de alcanzar:

- Los equipos son máquinas y pueden fallar. Nos interesan particularmente los dispositivos de almacenamiento: discos duros y memorias externas. Nos protegeremos con almacenamiento redundante y copias de seguridad.
- Los sistemas operativos y las aplicaciones los programan personas y pueden fallar. Las consecuencias más importantes son una caída del servicio, una pérdida de datos o una vulnerabilidad que permite la intrusión de un atacante. Nos protegeremos mediante servidores redundantes, antivirus y activando las actualizaciones automáticas.
- Los usuarios son personas y pueden fallar: descargan software no permitido o revelan sus contraseñas a terceras personas. Nos protegeremos limitando privilegios, dando cursos de formación y estableciendo una política de contraseñas (caducidad, complejidad mínima).
- En nuestras comunicaciones con otras personas desconocemos el nivel de seguridad que aplican. Incluso generalmente atravesamos redes públicas operadas por otras empresas, de las que también desconocemos el nivel de seguridad que aplican. Debemos aplicar protección extremo a extremo.

La inversión en seguridad depende del interés de otros en nuestros equipos y, sobre todo, nuestros datos.

Las auditorías de seguridad son revisiones de la seguridad de nuestra empresa. Para ello se suele contratar a empresas especializadas, como los tiger teams.

La complejidad de la seguridad debe estar equilibrada con la formación del personal que la tiene que aplicar: una contraseña de 20 caracteres terminará apuntada en un papel bajo el teclado.

La seguridad informática comprende:

- **Equipos.** Robo; evitar intentos de conectar equipos externos a la empresa, mantenimiento preventivo.
- **Aplicaciones.** Limitar privilegios, revisar vulnerabilidades conocidas, descargar aplicaciones de fuentes fiables.
- **Datos**. Almacenamiento redundante, copias de seguridad y cifrado.
- **Comunicaciones.** Utilizaremos canales cifrados para proteger la información cuando es transmitida por nuestra red interna y, sobre todo, por Internet.

La seguridad física se ocupa de los equipos; la seguridad lógica, de los programas que se ejecutan en esos equipos.

La seguridad activa intenta impedir una catástrofe; la seguridad pasiva intenta que, si ocurre, la recuperación sea posible.

La confidencialidad busca garantizar que una información solo sea utilizada por los usuarios y máquinas que lo necesitan. Se materializa en:

- **Autenticación.** Cómo confirmamos que el usuario es quien dice ser. Aplicaremos el esquema **sabes-tienes-eres.**
- **Autorización.** Qué operaciones puede efectuar.
- **Cifrado.** Los datos se almacenan cifrados para que no puedan ser aprovechados por nadie que no esté debidamente autenticado y autorizado.

La integridad intenta que los datos almacenados por un usuario no sufran ninguna alteración sin su consentimiento.

La disponibilidad se refiere a todas las técnicas dirigidas a mantener activo un servicio. Generalmente supone añadir equipamiento adicional.

No repudio: que ninguna de las partes que intervienen en una relación pueda negarlo.

Los tipos de ataques son: interrupción, interceptación, modificación y fabricación.

Test de repaso

1. Hablar por teléfono móvil es seguro:

a) Es más seguro que hablar por teléfono fijo.

b) Es más seguro que hablar por teléfono fijo, salvo cuando utilizamos un terminal DECT.

c) Es más inseguro porque las ondas se transmiten por el aire y cualquier otro teléfono puede recibirlas.

2. ¿Es seguro utilizar el WhatsApp?

a) Es más seguro enviar un SMS, porque utiliza telefonía móvil, que es muy segura.

b) Es igual de seguro que el SMS, porque la conexión al servidor de WhatsApp también utiliza telefonía móvil.

c) Es menos seguro que el SMS, porque para llegar a su servidor atraviesa Internet, que es una red poco segura.

3. ¿Es seguro comprar por Internet?

a) No: cualquiera puede saber nuestro número de tarjeta de crédito y comprar con ella.

b) No: cualquiera puede saber nuestro número de cuenta corriente y comprar con ella.

c) Sí: además de la tarjeta (algo que tienes), la mayoría de los bancos solicitan un PIN (algo que sabes).

4. Tengo una cuenta corriente en MiBanco y me llega un correo de info@mibanco.es donde me avisan de que hay una nueva web donde cambiar las claves:

a) Imposible. Los bancos nunca utilizan el correo electrónico para ese tipo de notificaciones.

b) Agradezco el aviso y pincho para probarlo.

c) Pincho en el enlace y envío este correo a mis conocidos.

5. Queremos enviar fotos personales a un amigo:

a) Las subo a Facebook, porque es más cómodo y seguramente nadie las verá.

b) Las envío a su dirección de correo electrónico del trabajo.

c) Las grabo en un CD y se las llevo a casa.

6. Un tiger team:

a) Es un nuevo espectáculo de lucha libre americana.

b) Es un equipo de expertos en seguridad que ofrecen sus servicios a empresas.

c) Es un grupo de becarios del departamento de informática que revisan los log de los sistemas.

7. Los portátiles que una empresa proporciona para algunos empleados:

a) Nunca salen de las oficinas. Los tienen para poder trabajar en las salas de reunión.

b) Como los utilizarán fuera de las oficinas, el usuario del empleado tiene privilegios de administración, por si necesita instalar algo.

c) Los discos duros aplican cifrado de la información almacenada por si el portátil resulta extraviado.

8. En los ordenadores de la empresa:

a) Todos llevan el mismo software, por si alguna vez necesitamos sustituir unos por otros.

b) En cada uno instalamos las aplicaciones estrictamente necesarias.

c) Dejamos que cada usuario instale lo que quiera.

9. Cuando un usuario nos pide instalar una nueva aplicación:

a) Aceptamos el CD que nos ofrece.

b) Aceptamos el USB que nos ofrece.

c) Buscamos el suministrador de esa aplicación y contactamos para conseguir una copia oficial.

10. Durante la descarga de un programa, el antivirus detecta que tiene un troyano:

a) Lo dejamos estar: peor sería tener un virus.

b) Lo ejecutamos para confirmar que es un troyano.

c) Lo borramos y buscamos ese software en otra parte más fiable.

11. Para facilitar el acceso de un empleado a su nómina, la empresa quiere ponerla en un disco compartido en la red interna:

a) Mejor colgarla en la web para que pueda consultarla desde casa.

b) Utilizaremos una carpeta distinta para cada usuario, con permisos exclusivos para ese usuario.

c) No hay problema: como la transferencia va cifrada, nadie que escuche en la red podrá obtener esa información.

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

Comprueba tu aprendizaje

Aplicar medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades

1. Trabajas en una auditoría de seguridad informática. Llega un nuevo cliente que desea conocer la situación de su empresa y si es aceptable o podría mejorar. Durante la entrevista tomas las siguientes notas:

- El edificio tiene un servicio de vigilancia a través de una empresa externa. Por reducción del presupuesto, ahora solo hay un vigilante que también atiende el edificio del otro lado de la calle.
- El CPD tiene otro vigilante, de otra compañía, que también atiende el teléfono de la centralita a partir de las tres, cuando termina el turno del recepcionista.
- Para entrar al CPD, cada informático tiene una tarjeta particular, si bien hay una en el cajón de la mesa del vigilante para el personal de limpieza o por si ocurre una emergencia.
- Una vez a la semana se hace la copia de seguridad. Como solo disponen de un dispositivo de cinta, los cuatro servidores se reparten cada semana del mes. Dado que solo hay un vigilante para el CPD, las cintas se dejan dentro de la sala, cada una encima de su servidor (cada servidor tiene una cinta en exclusiva).
- El edificio pertenece al patrimonio histórico y no admite reformas en la fachada. Por tanto, no ha sido posible instalar equipos de aire acondicionado en el CPD. Para combatir el calor que desprenden los ordenadores, las ventanas están siempre abiertas.
- Cada servidor tiene un disco duro de alta gama, que no ha fallado nunca.
- Los servidores tienen doble fuente de alimentación, por si se estropea alguna.
- El presidente y el contable tienen cada uno un portátil de la empresa. El disco duro de estas máquinas no está cifrado porque no se arriesgan al desastre que supondría olvidar la contraseña.
- Los ordenadores tienen dos usuarios: uno para las tareas normales y otro para cuando necesitan realizar alguna instalación o modificar un parámetro del sistema operativo. Los empleados saben cuándo deben usar cada uno.

Termináis por hoy la entrevista porque ha sido una reunión muy larga. Todavía no has redactado el informe final, pero ¿encuentras algo que mejorar? ¿Qué alternativa le puedes proponer?

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

2. Al día siguiente continúa la entrevista. Tus nuevas notas son:

- Hay una red wifi en la oficina que permite entrar en la red de ordenadores y salir a Internet. No tiene contraseña para que los clientes puedan utilizarla con total comodidad.
- La mayoría de los ordenadores utilizan Windows XP, pero algunos empleados necesitan Windows 7. Como la empresa no puede afrontar la compra de nuevas licencias, están utilizando software pirata.
- En cuanto al antivirus, cada empleado pone el que más le gusta y se los pasan entre ellos mediante discos USB.
- Los ordenadores que hacen de servidores tienen activadas las actualizaciones automáticas de todas las aplicaciones y el sistema operativo, pero en los ordenadores de los empleados no se hace porque han visto que se satura la conexión a Internet.
- La mayoría de los equipos de red son switch y routers, pero algunos despachos todavía tienen hubs porque son fiables y el ancho de banda es suficiente.
- Para entrar a la red desde Internet utilizan Hamachi, un servicio gratuito y muy sencillo de instalar.
- El servidor web está instalado sobre una máquina con sistema operativo Linux Ubuntu Server 9.04.

Termina la entrevista del segundo día porque el cliente tiene otro compromiso. De nuevo, ¿encuentras algo que mejorar? ¿Qué le puedes proponer?

Reconocer la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento

3. Tus notas del tercer y último día son las siguientes:

- Los clientes rellenan una ficha con su nombre, dirección, teléfono, correo electrónico y la medicación que están tomando en ese momento.
- Después, una secretaria introduce la ficha en una hoja Excel de su ordenador.

Finalmente, ¿tienes algo que aportar sobre la seguridad que necesitan estos datos?

Unidad 2
Criptografía



En esta unidad aprenderemos a:

- Describir sistemas de identificación, como la firma electrónica y el certificado digital, entre otros.
- Utilizar sistemas de identificación, como la firma electrónica y el certificado digital, entre otros.

Y estudiaremos:

- La criptografía.
- La identificación digital: firma electrónica y certificado digital.
- Los sistemas de identificación: firma electrónica, certificados digitales y otros.

1. ¿Por qué cifrar?

La información es poder: los planos de un nuevo motor de coche eléctrico, la estrategia electoral de un partido político o la fórmula de un nuevo medicamento. Todos son ejemplos de información que interesa a terceras personas: una empresa de la competencia, un partido rival.

Para sacar el máximo partido de una información hay que compartirla con otros individuos: el plano del motor o la fórmula deben llegar a la fábrica, y la estrategia electoral se discutirá en algún comité regional. En todos estos casos, el autor del documento **(emisor)** debe transferirlo a algún **soporte** (disco duro, CD, pendrive USB, impresión en papel, cuenta de correo electrónico, upload a un servidor web, etc.) y hacer llegar ese soporte hasta el destino **(receptor)** mediante algún **canal** de comunicación (empresa de mensajería, fax, Internet, etc.).

En ese canal pueden estar acechando **terceras personas** con la intención de **interceptarlo:** sobornarán al mensajero para hacer una copia del disco duro/CD/USB o una fotocopia del papel, «hackearán» el servidor de correo, capturarán el tráfico de red en el servidor web. Es imposible asegurar que nunca conseguirán el documento. Nuestra esperanza es que, aunque lo tengan y lo puedan leer, no entiendan nada porque **el contenido estará cifrado.** Aquí nos ayuda la **criptografía.**

Nuestra era de la información y las comunicaciones necesita el cifrado más que nunca, porque cada vez existen más medios de almacenamiento (memorias portables de todo tipo) y, sobre todo, más mecanismos de comunicación (Fig. 2.1):

- Voz mediante teléfono (fijo/móvil) con tecnología analógica (fijo) y digital (GSM, UMTS, RDSI, VoIP), así como el aumento constante de videoconferencias.
- Mensajería electrónica breve (SMS, Skype, WhatsApp) o completa (correo electrónico, burofax).
- Datos por línea digital (ADSL, fibra, HFC) o inalámbrica (wifi, UMTS, LTE).
- Apertura de las redes internas de las empresas para que puedan trabajar sus trabajadores (VPN de teletrabajo), sus clientes (acceso web) y otras empresas (VPN de empresas), todo a través de Internet.

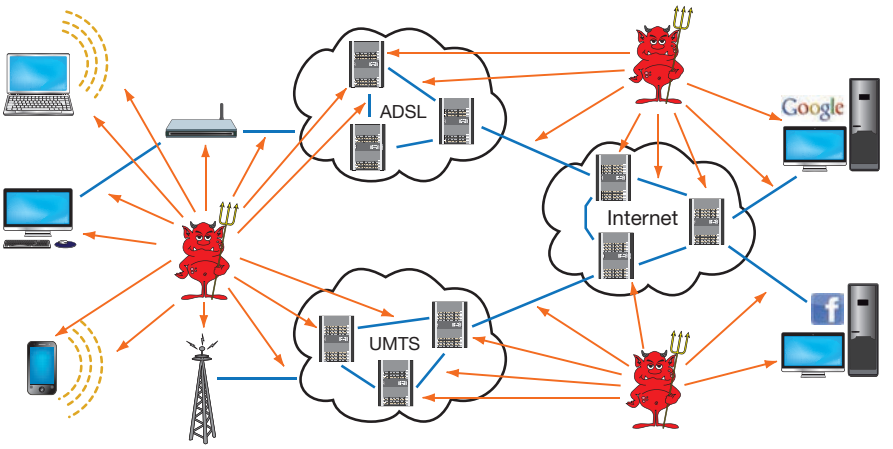


Fig. 2.1. *Posibles ataques.*

Todas esas conversaciones utilizan **redes compartidas** con otros usuarios que no somos nosotros y administradas por otras **empresas que no son la nuestra.** Las operadoras de telecomunicaciones pueden darnos confianza utilizando protocolos seguros; pero para las empresas no es suficiente (las operadoras de telecomunicaciones también son sobornables y «hackeables») y por eso aplican cifrado en todas partes (incluso dentro: podemos tener empleados «traidores»); también los usuarios particulares deberían preocuparse de hacerlo porque su privacidad les pertenece (llamadas personales, correos intercambiados con sus contactos, movimientos bancarios, etc.).

Actividades

1. Investiga el cifrado utilizado por Julio César y haz una prueba con tu compañero.
2. Investiga en qué consiste el voto electrónico.
3. Repasa todas las veces que se utiliza criptografía en la película *El Código Da Vinci* (2006).
4. Discute las ventajas e inconvenientes de los algoritmos de cifrado abiertos (se conocen todos los pasos, incluso hay estándares) frente a los privados (la empresa dueña del equipo de cifrado no lo publica).
5. Investiga el cifrado del programa Skype.
6. Investiga cómo y dónde se guardan las claves de los usuarios en Linux.

2. Criptografía

La palabra *criptografía* viene del griego *cripto* (que significa «ocultar») y *graphos* (que significa «escribir»). Se podría traducir por: **cómo escribir mensajes ocultos.** En la antigüedad se utilizaba sobre todo durante las guerras, para comunicar estrategias, de manera que, aunque el mensajero fuera interceptado por el enemigo, el contenido del mensaje estaba a salvo.

La criptografía consiste en tomar el documento original y aplicarle un **algoritmo** cuyo resultado es un nuevo documento. Ese documento está cifrado: no se puede entender nada al leerlo directamente. Podemos, tranquilamente, hacerlo llegar hasta el destinatario, que sabrá aplicar el algoritmo para recuperar el documento original.

Realmente, hace falta algo más que el algoritmo, porque el enemigo también puede conocerlo (incluso lo utiliza en sus propias comunicaciones). Por ejemplo, nosotros tenemos una red wifi con cifrado WPA, pero el vecino también. La privacidad la conseguimos gracias a la **clave del algoritmo** (Fig. 2.2): un conjunto de valores que, combinados con el documento original tal y como se indica en el algoritmo, generan un documento cifrado de tal forma que, solo con ese documento, es imposible deducir ni el documento original ni la clave utilizada. Por supuesto, debemos evitar que el enemigo pueda llegar a conocer nuestra clave.

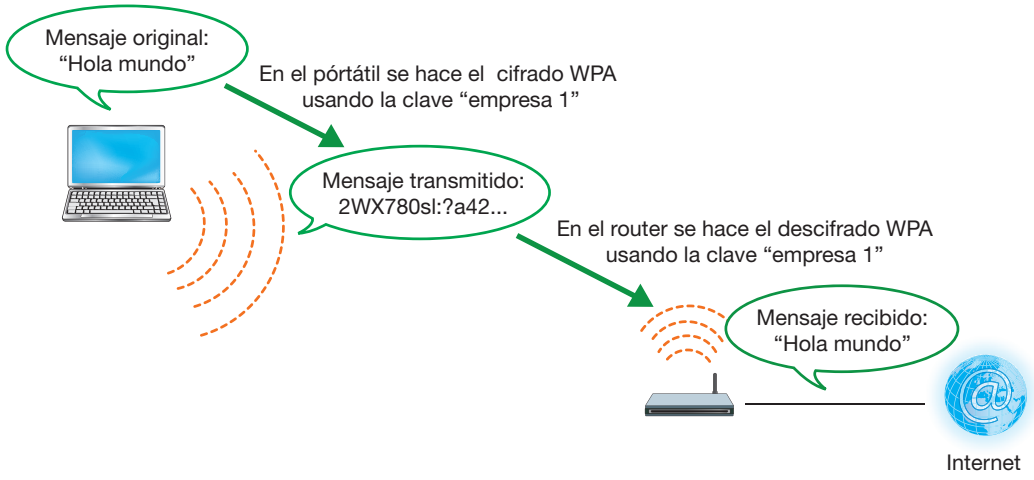


Fig. 2.2. *Cifrado WPA en redes wifi.*

Las claves son combinaciones de símbolos (letras, números, signos de puntuación, etc.). Por tanto, nuestra seguridad está expuesta a los **ataques de fuerza bruta:** probar todas las combinaciones posibles de símbolos. Para evitarlo tomaremos estas medidas:

- **Utilizar claves de gran longitud** (512-1024-2048-4096 bytes), de manera que el atacante necesite muchos recursos computacionales para cubrir todo el rango rápidamente.
- **Cambiar regularmente la clave.** De esta forma, si alguien quiere intentar cubrir todo el rango de claves, le limitamos el tiempo para hacerlo.
- **Utilizar todos los tipos de caracteres posibles:** una clave compuesta solo de números (diez valores posibles) es más fácil de adivinar que una con números y letras (36 valores posibles).
- **No utilizar palabras fácilmente identificables:** palabras de diccionario, nombres propios, etc.
- **Detectar repetidos intentos fallidos en un corto intervalo de tiempo.** Por ejemplo, la tarjeta del móvil se bloquea si fallamos tres veces al introducir el PIN.

Las claves no son el único punto débil de la criptografía; pueden existir **vulnerabilidades** en el propio algoritmo o en la implementación del algoritmo en alguna versión de un sistema operativo o un driver concreto. Estas vulnerabilidades las estudia el **criptoanálisis.**

Web

En este artículo se estudia el tiempo necesario para probar todas las claves del algoritmo AES:
http://goo.gl/OeYtK
El ataque al cifrado de la máquina Enigma fue clave para el desenlace de la Segunda Guerra Mundial:
http://goo.gl/NtBiQ

3. Criptografía simétrica y asimétrica

Los **algoritmos de criptografía simétrica** utilizan la **misma clave** para los dos procesos: cifrar y descifrar. Son sencillos de utilizar y, en general, resultan bastante **eficientes** (tardan poco tiempo en cifrar o descifrar). Por este motivo, todos los algoritmos, desde la antigüedad hasta los años setenta, eran simétricos. Los más utilizados actualmente son DES, 3DES, AES, Blowfish e IDEA.

El funcionamiento es simple: en la Figura 2.3 el emisor quiere hacer llegar un documento al receptor. Toma ese documento y le aplica el algoritmo simétrico, usando la clave única, que también conoce el receptor. El resultado es un documento cifrado que ya podemos enviar tranquilamente.

Cuando el receptor recibe este documento cifrado, le aplica el mismo algoritmo con la misma clave, pero ahora en función de descifrar. Si el documento cifrado no ha sido alterado en el camino y la clave es la misma, el resultado será el documento original.

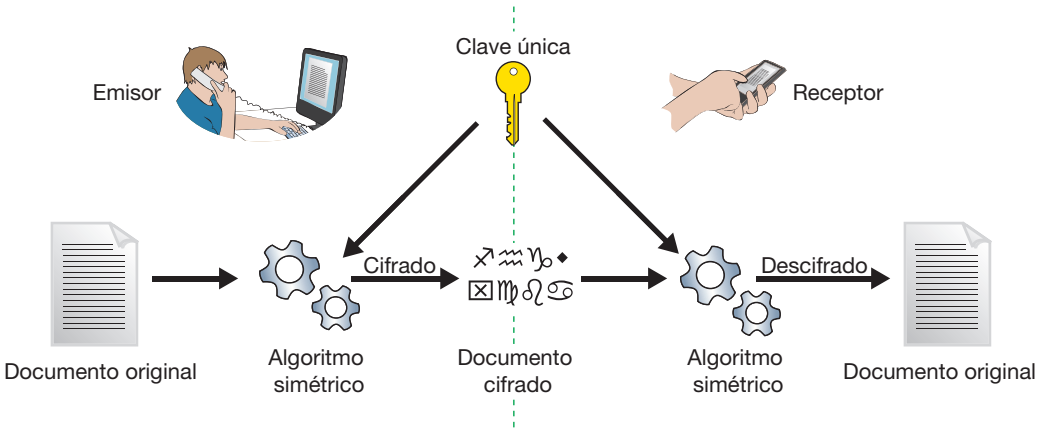


Fig. 2.3. *Criptografía simétrica.*

Un ejemplo de criptografía simétrica es la **autenticación de un móvil GSM:** por qué sabe que es nuestro número, aunque metamos la tarjeta SIM en otro teléfono. El procedimiento es el siguiente:

- Nuestra tarjeta SIM contiene un identificador T y una clave K.
- Ese identificador T y la clave K aparecen asociados a nuestro contrato en los servidores de autenticación de la operadora de la que somos clientes.
- Cuando encendemos el teléfono, se conecta a la red de la operadora y solicita entrar con el identificador T. Su servidor de autenticación recibe la petición y genera un número aleatorio A (llamado desafío), que nos lo envía.
- Una vez recibido, en nuestro teléfono aplicamos un determinado algoritmo simétrico sobre ese número A, utilizando la clave K. El resultado es el número B. Enviamos el número B al servidor de autenticación.
- Cuando lo recibe, él también aplica el mismo algoritmo con la misma clave. Si el resultado es igual a B, se confirma que somos los dueños del identificador T. Nos asigna nuestro número 6XX, y ya podemos hacer y recibir llamadas.
- Si cambiamos de teléfono, no importa porque el número va asociado a la SIM.

Con esta solución estamos protegidos de una posible captura de tráfico inalámbrico mediante un sniffer de red:

- Podría capturar el número A. Pero es un simple número aleatorio: sin el algoritmo y la clave, el atacante no podrá generar la respuesta correcta B.
- Podría capturar también el número B y ya tendría la respuesta correcta cuando el servidor envía el número A. Pero la probabilidad de que el servidor repita el mismo número A para este abonado es muy baja. Es decir, si el atacante elabora una tarjeta SIM preparada para responder B cuando le pregunten A, es muy poco probable que tenga éxito.

Web

Alicia y Bernardo nos explican la criptografía simétrica:
http://goo.gl/L6jzs

Actividades

7. Busca información sobre algoritmos de cifrado de tipo bloque y de flujo.

8. Idea mecanismos para hacer llegar la clave simétrica a los participantes de una comunicación.

9. Un método sencillo de cambiar la clave simétrica sería avisarlo en el último mensaje intercambiado. ¿Te parece adecuado?

Vocabulario

Sniffer de red. Dispositivo con acceso a un medio físico de transmisión de datos que es capaz de capturar todos los paquetes, aunque no vayan destinados a él.

Caso práctico 1

Cifrado simétrico en Windows

Objetivo. Cifrar ficheros con algoritmos simétricos mediante la herramienta IZArc.

Material. Dos ordenadores con Windows.

Duración: 10 minutos **Dificultad:** Fácil

1. En un ordenador con Windows 7 descargamos la herramienta de la web oficial **www.izarc.org**. Realmente es un compresor de ficheros, pero como además tiene la opción de cifrar el fichero comprimido, podemos utilizarlo para las dos cosas. Por ejemplo, podemos cifrar muchos ficheros, incluso una estructura de carpetas, en un solo fichero fácil de transportar.
2. Durante la instalación nos indicará qué tipos de cifrado queremos manejar con IZArc. Están los habituales (.zip, .rar) y algunos interesantes (.tar, .7z).
3. Una vez instalado, podemos situarnos sobre cualquier fichero o carpeta y acceder al menú del botón derecho. En este ejemplo hemos creado el fichero de texto top secret y en la opción *IZArc* elegiremos la operación *Agregar a top secret.zip* (el nombre se genera automáticamente). Aparecerá la ventana de la herramienta, donde podremos elegir el algoritmo de encriptación. En nuestro caso será AES de 128 bits (Fig. 2.4).

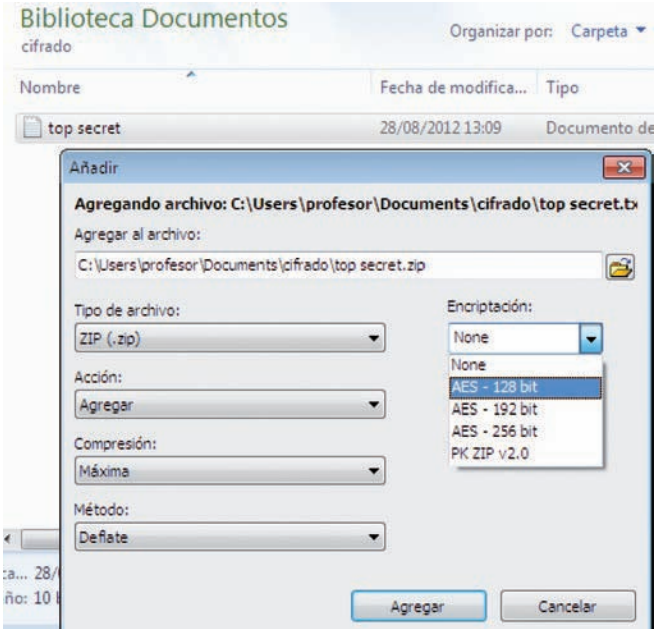


Fig. 2.4. *Cifrado de un fichero.*

4. La opción por defecto es *None* porque estamos trabajando con un programa que es fundamentalmente un compresor de ficheros. Terminaremos pulsando en *Agregar*. En ese momento nos preguntará la clave que queremos utilizar en el cifrado. La preguntará una segunda vez para confirmar que la hemos tecleado bien. Si es así, estará disponible el fichero cifrado top secret.zip.
5. Ese fichero .zip lo podemos llevar a otra máquina que también tenga IZArc y descifrarlo allí (en este ejemplo, un XP). Nos situamos sobre el fichero .zip y desde el menú del botón derecho recuperamos los ficheros pulsando en *Extract Here* (Fig. 2.5).

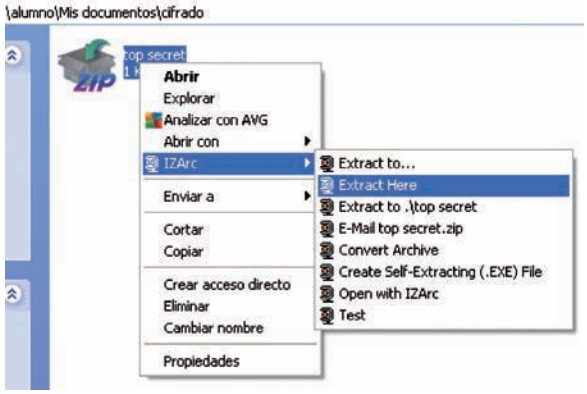


Fig. 2.5. *Descifrado de un fichero.*

6. Nos preguntará la clave (Fig. 2.6). Si la introducimos bien, habremos conseguido el fichero de texto que almacenaba el fichero .zip.

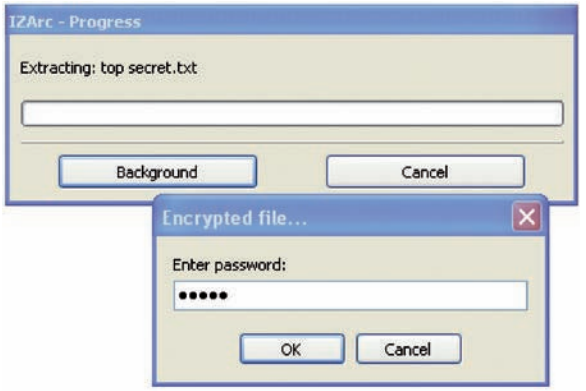


Fig. 2.6. *Introducimos la clave de cifrado.*

7. El programa ofrece más funciones, como elegir el directorio donde almacenar los ficheros recuperados *(Extract to...)*, comprobar la integridad del fichero *(Test)*, cambiar de formato de compresión *(Convert Archive)* o crear un ejecutable *(Create Self-Extracting [.EXE] File)*. Esta última opción es particularmente útil si la máquina donde llevamos el fichero comprimido no tiene instalado ningún descompresor compatible con el formato utilizado.
8. En todos los casos, como era de esperar, cuando el fichero utilizado está cifrado, antes de realizar la operación nos preguntará por la contraseña correcta.

Caso práctico 2

Cifrado simétrico en Linux

Objetivo. Cifrar ficheros con algoritmos simétricos mediante la herramienta gpg.

Material. Ordenador con Ubuntu 12.04.

- **Duración:** 20 minutos
- **Dificultad:** Fácil

1. La herramienta gpg nos permite utilizar tanto criptografía simétrica como asimétrica. En este ejemplo veremos la simétrica.

2. Nos presentamos en Ubuntu y creamos un directorio llamado `cifrado` donde vamos a trabajar. Lo primero será crear un fichero de prueba. Podemos utilizar la herramienta fortune, que ofrece aleatoriamente refranes, chistes, etc. En este ejemplo ejecutamos (Fig. 2.7):

```
$ fortune > mensaje
```

```
alumno@alumno-VirtualBox:~/cifrado$ fortune > mensaje
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 4
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:35 mensaje
alumno@alumno-VirtualBox:~/cifrado$ cat mensaje
Q:      Why did the chicken cross the road?
A:      To see his friend Gregory peck.

Q:      Why did the chicken cross the playground?
A:      To get to the other slide.
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.7. *Creamos un fichero de prueba.*

3. Para cifrarlo con clave simétrica el comando es:

```
$ gpg --symmetric mensaje
```

El comando nos pedirá la clave que queremos utilizar (Fig. 2.8). La pedirá de nuevo para confirmarla.

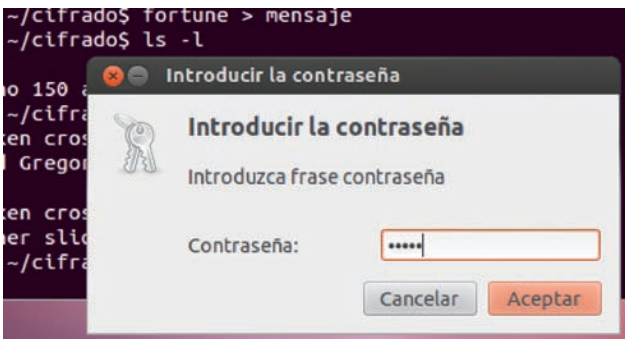


Fig. 2.8. *Ciframos el fichero con clave simétrica.*

4. El resultado del comando es un nuevo fichero con la extensión .gpg. Es un fichero cifrado: si intentamos ver qué hay dentro con el comando `strings`, no aparece nada inteligible (Fig. 2.9). No es recomendable utilizar directamente cat porque es un fichero binario y podríamos inutilizar la sesión.

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --symmetric mensaje
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 8
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:35 mensaje
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:39 mensaje.gpg
alumno@alumno-VirtualBox:~/cifrado$ strings mensaje.gpg
Nr{k`
~_?d
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.9. *Fichero cifrado.*

5. Ahora ya podríamos eliminar el fichero `mensaje`, porque su contenido está protegido en el fichero `mensaje.gpg`. Para hacer llegar este fichero .gpg a las personas interesadas, podemos utilizar cualquier mecanismo normal de gestión de ficheros (disco duro, USB, upload web, FTP, etc.). Cuando necesiten leerlo, lo descifrarán con el comando (Fig. 2.10):

```
$ gpg --decrypt mensaje.gpg
```

El comando pedirá la clave que habíamos utilizado para cifrar (y que haremos llegar al interesado a través de un medio seguro). Si la introducimos correctamente, aparecerá en pantalla el contenido del fichero (Fig. 2.10).

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --decrypt mensaje.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 frase contraseña
Q:      Why did the chicken cross the road?
A:      To see his friend Gregory peck.

Q:      Why did the chicken cross the playground?
A:      To get to the other slide.
gpg: AVISO: la integridad del mensaje no está protegida
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.10. *Desciframos.*

6. Si no queremos verlo por pantalla, sino volcarlo a un fichero, podemos redirigir la salida estándar (Fig. 2.11):

```
$ gpg --decrypt mensaje.gpg > mensaje2
```

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --decrypt mensaje.gpg >mensaje2
gpg: datos cifrados CAST5
gpg: cifrado con 1 frase contraseña
gpg: AVISO: la integridad del mensaje no está protegida
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 12
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:35 mensaje
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:42 mensaje2
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:39 mensaje.gpg
alumno@alumno-VirtualBox:~/cifrado$ diff mensaje mensaje2
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.11. *Desciframos y volcamos a fichero.*

7. Los ficheros binarios .gpg no siempre son adecuados. No sirven para incluirlos dentro de un texto (por ejemplo, en un script o un correo electrónico). Para resolverlo tenemos el parámetro `-a`, que genera un fichero cifrado pero compuesto solo de caracteres ASCII. Estos ficheros ya no tienen extensión .gpg, sino .asc. Dentro está el contenido cifrado y alrededor un par de cabeceras informativas. En nuestro ejemplo el comando sería (Fig. 2.12):

(Continúa)

Caso práctico 2

(Continuación)

```
$ gpg -a --symmetric mensaje
```

```
alumno@alumno-VirtualBox:~/cifrado$ gpg -a --symmetric mensaje
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 16
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:35 mensaje
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:42 mensaje2
-rw-rw-r-- 1 alumno alumno 304 ago 28 19:45 mensaje.asc
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:39 mensaje.gpg
alumno@alumno-VirtualBox:~/cifrado$ cat mensaje.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAwMC8HG1mISwUYxgyYayrsJ4URD7PsLQ8biXeoP4pzETPAXVGts0pmz3v5bn
gi804NbKNk8Nn5v1w5GxLX/2GxIX5LJhSXitBu7NScmDj5p6IRAdjFPJk6ge+cPI
EYioy8SOkfN23QgI04E7PgaOJ6wFpf9rP1rLWsDAICd+tuppWPS6MUAy80+zHH4+
zQ5ZJG58kA==
=iHQ4
-----END PGP MESSAGE-----
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.12. *Ciframos en modo ASCII.*

8. El fichero .asc ofrece las mismas garantías que el .gpg y se utiliza igual. Para descifrar sería (Fig. 2.13):

```
$ gpg --decrypt mensaje.asc
```

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --decrypt mensaje.asc
gpg: datos cifrados CAST5
gpg: cifrado con 1 frase contraseña
Q:      Why did the chicken cross the road?
A:      To see his friend Gregory peck.

Q:      Why did the chicken cross the playground?
A:      To get to the other slide.
gpg: AVISO: la integridad del mensaje no está protegida
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.13. *Desciframos desde modo ASCII.*

9. La herramienta por defecto utiliza el algoritmo de cifrado `CAST5` (en pantalla nos lo informa al descifrar). Podemos cambiarlo con el parámetro `cipher-alg`. Por ejemplo, para utilizar AES ejecutaríamos (Fig. 2.14):

```
$ gpg -a --symmetric --cipher-alg AES -o
mensaje.aes mensaje
```

En este ejemplo hemos utilizado `-a` para tener el fichero en ASCII y el parámetro `-o` para indicar el fichero de salida (es equivalente a redirigir la salida estándar).

```
alumno@alumno-VirtualBox:~/cifrado$ gpg -a --symmetric --cipher-alg AES -o mensa
je.aes mensaje
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 20
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:35 mensaje
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:42 mensaje2
-rw-rw-r-- 1 alumno alumno 344 ago 28 19:49 mensaje.aes
-rw-rw-r-- 1 alumno alumno 304 ago 28 19:45 mensaje.asc
-rw-rw-r-- 1 alumno alumno 150 ago 28 19:39 mensaje.gpg
alumno@alumno-VirtualBox:~/cifrado$ cat mensaje.aes
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EBwMC+zQD8Y1j0tNg0qQBPAGRmFj21AAsyXb+ZNvx6WU+RntTDQ2Y9fk56tWe
tYAinszGr8KRGV0QMDx2SSN4kCoIH4dt7P8cYvLYxzX9Q48WU1uRCpNFqpmkKvO9
HAG3TD1H1gOCeYeKNJgFIwYxNShktiKFjVlsK0kJHVtkf9LfoGMKLs0R7cjHKmxn
364w0wPKBeVewhJ8fXQOHsF9lGFZoc6RKEQ8Nh/6S/pGi7ftcw==
=lfvz
-----END PGP MESSAGE-----
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.14. *Elegimos el algoritmo de cifrado AES.*

10. El descifrado se hace como siempre (Fig. 2.15):

```
$ gpg --decrypt mensaje.aes
```

Ahora, el mensaje de la pantalla nos avisa de que el fichero estaba cifrado con `AES` (ya no es CAST5).

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --decrypt mensaje.aes
gpg: datos cifrados AES
gpg: cifrado con 1 frase contraseña
Q:      Why did the chicken cross the road?
A:      To see his friend Gregory peck.

Q:      Why did the chicken cross the playground?
A:      To get to the other slide.
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.15. *Desciframos el fichero AES.*

11. Con esta herramienta podemos cifrar ficheros binarios, no solo ficheros de texto. Vamos a trabajar sobre una copia del propio ejecutable `fortune` y le llamaremos `refranes`. Los comandos serían (Fig. 2.16):

```
$ cp /usr/games/fortune refranes
$ ./refranes
```

```
alumno@alumno-VirtualBox:~/cifrado$ which fortune
/usr/games/fortune
alumno@alumno-VirtualBox:~/cifrado$ cp /usr/games/fortune refranes
alumno@alumno-VirtualBox:~/cifrado$ ./refranes
Persons attempting to find a motive in this narrative will be prosecuted;
persons attempting to find a moral in it will be banished; persons attempting
to find a plot in it will be shot.  By Order of the Author
                -- Mark Twain, "The Adventures of Huckleberry Finn"
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.16. *Traemos un ejecutable.*

12. Lo ciframos en modo ASCII para verlo mejor (Fig. 2.17):

```
$ gpg -a --symmetric refranes
```

```
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 24
-rwxr-xr-x 1 alumno alumno 22012 ago 28 19:57 refranes
alumno@alumno-VirtualBox:~/cifrado$ gpg -a --symmetric refranes
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 40
-rwxr-xr-x 1 alumno alumno 22012 ago 28 19:57 refranes
-rw-rw-r-- 1 alumno alumno 12918 ago 28 20:45 refranes.asc
alumno@alumno-VirtualBox:~/cifrado$ head refranes.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

jA0EAwMClctB7Cs19Vhgye0t0nSmLz2lucCzGQD437TOiCoADVe0nWEVkq+9l43x
j6gTubuwghX2BcrqgI6QO1yvIqZjBIQUU4n2Gu8KA1HfXU76fzsRqyf0tzEhTkO3
UV6NzHP8banr/Cq6Nq1fskUR97/wqqyJ5nvPJjOnsIGR7dZX1sSYq27/RCL80BsS
u4ujuA2h70/eS57jo/yBoMw7SW6aPj6gMS8e6c7dvOM+Y8L59FhXCS43z4m2EZfs
/qcdEjGjf13viC8MmS+0aTWwCxk6Kkj61ZUOlCFc7FY4LR0eyM6qUCKPhmOMHvIW
uciZwyfIt4bUrfHsCak0cNFaJkA0TmmaDlDKjSPC4ksbqQymNVQY4XStP09PcCFB
JIru7ETBp4ggPQIGJ+YOmuUWvf+O2BeUOJXsLuJc+dH3wQagS0esUD8eoJqnu2ad
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.17. *Ciframos el ejecutable.*

13. Podemos recuperarlo descifrando el fichero `refranes.asc` con las opciones conocidas. Por ejemplo, podemos dejar el resultado en un nuevo fichero `dichos`. Después de introducir la contraseña, solo necesitamos darle permisos de ejecución y estará disponible. Los comandos son:

```
$ gpg --decrypt -o dichos refranes.asc
$ chmod 755 dichos
$ ./dichos
```

Actividades

10. Para cifrar y descifrar no necesitamos privilegios especiales en Linux. ¿Por qué?

11. Prueba a intentar cifrar un fichero con IZArc aplicando el algoritmo AES256 y después llévalo a un Linux Ubuntu e intenta descifrarlo con gpg. ¿Funcionará?

El **problema principal** de la criptografía simétrica es la **circulación de las claves:** cómo conseguimos que el emisor y el receptor tengan la clave buena. No podemos utilizar el mismo canal inseguro por el que enviaremos el mensaje (la inseguridad nos ha llevado a cifrar). Hay que utilizar un **segundo canal de comunicación,** que también habría que proteger, y así sucesivamente. Por ejemplo, en el correo de bienvenida a una empresa puede aparecer la contraseña de la wifi de la oficina; cuando se cambie, se envía otro correo, etc.

El **segundo problema** es la **gestión de las claves almacenadas.** Si en una empresa hay diez trabajadores y todos tienen conversaciones privadas con todos, cada uno necesita establecer nueve claves distintas y encontrar nueve canales seguros para actualizarlas cada vez (en total 81 claves y 81 canales). Si aparece un trabajador nuevo, ahora son 100 claves y 100 canales. Y las empresas pueden tener muchos trabajadores: 500, 5 000, 50 000... ¿Cada vez que cambie mi clave tengo que avisar a 49 999 compañeros? Es poco manejable.

En los años setenta, los criptógrafos Diffie y Hellman publicaron sus investigaciones sobre **criptografía asimétrica.** Su algoritmo de cifrado utiliza **dos claves matemáticamente relacionadas** de manera que **lo que cifras con una solo lo puedes descifrar con la otra.** Comparado con la clave simétrica, ahora el emisor no necesita conocer y proteger una clave propia; es el receptor quien tiene el par de claves. Elige una de ellas (llamada **clave pública**) para comunicarla al emisor por si quiere enviarle algo cifrado. Pero ya no hace falta buscar canales protegidos para enviarla porque, aunque un tercer individuo la conozca, todo lo que se cifre con esa clave solo se podrá descifrar con la otra clave de la pareja (la **clave privada**), que nunca es comunicada. Y matemáticamente es imposible deducir la clave privada conociendo solo la clave pública.

Web

Alicia y Bernardo nos explican la criptografía asimétrica:
http://goo.gl/qM51P

Como se ilustra en la Figura 2.18, cuando el emisor quiere hacer llegar un mensaje confidencial al receptor, primero consigue la clave pública del receptor. Con esa clave y el documento original, aplica el algoritmo asimétrico. El resultado es un documento cifrado que puede enviar al receptor por cualquier canal. Cuando el mensaje cifrado llega al receptor, él recupera el documento original aplicando el algoritmo asimétrico con su clave privada.

Si el receptor quiere enviar al emisor una respuesta cifrada, debería conseguir la clave pública del emisor y seguir el mismo procedimiento.

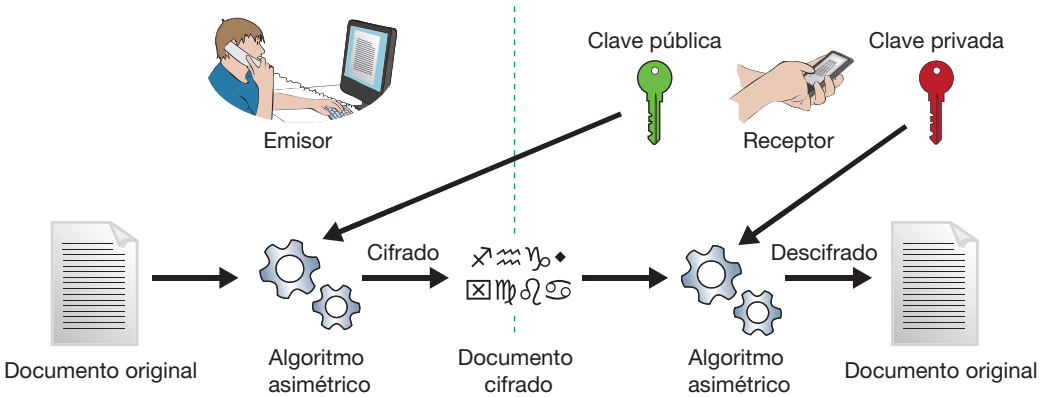


Fig. 2.18. *Criptografía asimétrica.*

La criptografía asimétrica resuelve los dos problemas de la clave simétrica:

- No necesitamos canales seguros para comunicar la clave que utilizaremos en el cifrado. Podemos adjuntarla en nuestros correos, añadirla al perfil de nuestras redes sociales, «postearla» en un blog, incluso repartirla en octavillas por la calle.
- No hay desbordamiento en el tratamiento de claves y canales. Si somos nueve empleados, solo necesitamos nueve claves y un solo canal: la intranet de la empresa, un correo destinado a toda la empresa, etc. Y si aparece un empleado nuevo, serán diez claves y el mismo canal.

Sin embargo, los algoritmos asimétricos tienen sus propios problemas:

- Son **poco eficientes:** tardan bastante en aplicar las claves para generar los documentos cifrados, sobre todo porque las claves deben ser largas para asegurar la independencia matemática entre ellas.
- Utilizar las claves privadas repetidamente es arriesgado porque algunos **ataques criptográficos** se basan en analizar paquetes cifrados. Estos paquetes serían capturados en la red o directamente el atacante podría elaborar un software malicioso que generase paquetes de tamaño y contenido elegidos cuidadosamente y conseguir enviarlos a nuestro servidor para que los devolviera cifrados con su clave privada.
- Hay que **proteger la clave privada.** No basta con dejarla en un fichero de una carpeta del disco duro en la cuenta de nuestro usuario; cualquier otro usuario con permisos de administrador podría llegar hasta él. Por este motivo, las claves privadas se guardan todas juntas en un fichero llamado **keyring** (archivo de llaves, llavero), y este fichero está protegido mediante **cifrado simétrico.** Es decir, para poder usar la clave privada, hay que introducir una clave que descifra el llavero y permite leerla.

  Necesitamos una segunda medida de protección de la clave privada: la **copia de seguridad del llavero.** Si el disco duro se estropea, perderemos el fichero que contiene la clave privada y no podremos volver a utilizarla. Por tanto, debemos incluirlo en la política de backup de la empresa, y confiamos en que, aunque alguien más tenga acceso al backup (cintas, discos, etc.), la clave simétrica todavía protege el llavero.
- Hay que **transportar la clave privada.** En cifrado simétrico, si hemos enviado el fichero cifrado a otra máquina y queremos descifrarlo, basta con recordar la clave e introducirla. Pero en la clave privada esto es imposible (son cientos de símbolos sin sentido). Debemos transportar el llavero, con el riesgo que supone (si lo perdemos, podrían intentar un ataque de fuerza bruta contra el cifrado simétrico).

Caso práctico 3

Cifrado asimétrico en Linux

Objetivo. Cifrar ficheros con algoritmos asimétricos mediante la herramienta gpg.

Material. Ordenador con Ubuntu 12.04.

■ **Duración:** 🕒 30 minutos ■ **Dificultad:** 😐 Media

1. En el caso práctico 2 hemos utilizado la herramienta gpg para el cifrado simétrico. Esta misma herramienta sirve para el cifrado asimétrico.
2. Entramos con un usuario de la máquina (en este ejemplo, `alumno`). Lo primero será generar un par de claves de criptografía asimétrica, nuestra propia clave pública y clave privada. El comando es (Fig. 2.19):

   ```
   alumno$ gpg --gen-key
   ```
3. En el proceso de generación de la clave nos preguntarán varios detalles. El primero es el tipo de clave. La herramienta nos ofrece cuatro opciones. Los nombres se corresponden con el tipo de algoritmo asimétrico asociado (hay varios tipos, como también ocurría en criptografía simétrica: DES, AES, etc.). Es decir, una clave de tipo DSA se utiliza en un algoritmo DSA, y una clave Elgamal, en un algoritmo Elgamal. Las dos primeras opciones ofrecen dos algoritmos, luego generan dos pares de claves: en total, cuatro claves, dos públicas y dos privadas. El motivo es que generalmente se utiliza una clave (un par) para cifrar y otra diferente (otro par) para firmar, como veremos en el siguiente apartado de esta unidad. Elegimos la opción 2, que tiene algoritmos distintos, y así veremos claramente cuándo se utiliza cada clave.

```
alumno@alumno-VirtualBox:~$ gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Por favor seleccione tipo de clave deseado:
   (1) RSA y RSA (predeterminado)
   (2) DSA y Elgamal
   (3) DSA (sólo firmar)
   (4) RSA (sólo firmar)
¿Su selección?: 2
```

Fig. 2.19. *Generamos un par de claves.*

(Continúa)

Caso práctico 3

(Continuación)

4. A continuación nos pregunta el tamaño de la clave del algoritmo DSA. Por defecto ofrece 2 048, pero en este ejemplo elegimos el mínimo, 1 024, para tardar menos en generarla (Fig. 2.20).

```
las claves DSA pueden tener entre 1024 y 3072 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 1024
```

Fig. 2.20. *Elegimos el tamaño de la clave.*

5. La siguiente pregunta es el periodo de validez de la clave. Ya estamos advertidos de los problemas que supone proteger la clave privada. Por si la perdemos, conviene fijar una fecha de caducidad para que no se pueda usar más allá de ese día. En nuestro ejemplo no hace falta tanta seguridad y elegiremos que nunca caduque (Fig. 2.21).

```
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
      <n>  = la clave caduca en n días
      <n>w = la clave caduca en n semanas
      <n>m = la clave caduca en n meses
      <n>y = la clave caduca en n años
¿Validez de la clave (0)? 0
```

Fig. 2.21. *Fijamos la caducidad de la clave.*

6. A continuación nos pide algunos datos para identificar la clave. Ya sabemos que en el llavero se pueden almacenar varias claves (de hecho, estamos generando dos pares ahora mismo). Para elegir una u otra en cada ocasión, tenemos que identificarlas fácilmente. En este caso nos pedirá un nombre, una dirección de correo y un comentario (Fig. 2.22). La herramienta gpg nunca nos enviará un correo; pero es una forma de contactar con el dueño de la clave (entregaremos nuestra clave pública a mucha gente, y ellos tendrán las claves públicas de otras personas).

```
Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo electrónico de esta forma:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: alumno
Dirección de correo electrónico: alumno@gmail.com
Comentario: seguridad 2012
Ha seleccionado este ID de usuario:
    «alumno (seguridad 2012) <alumno@gmail.com>»

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir?
```

Fig. 2.22. *Identificamos la clave.*

7. El siguiente paso es elegir la clave simétrica que protegerá nuestras claves (Fig. 2.23). Como siempre, debe ser una clave fácil de recordar para nosotros y difícil de averiguar para cualquier otra persona. Si la olvidamos, no podremos utilizar nuestras claves asimétricas.

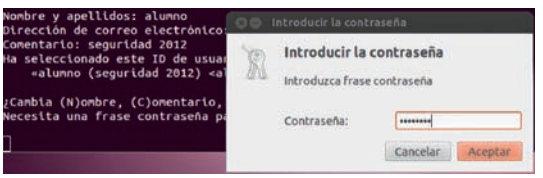


Fig. 2.23. *Elegimos la clave simétrica que protege la clave privada.*

8. Ya no hay más preguntas. Ahora la herramienta ejecuta los procedimientos matemáticos para obtener las claves asimétricas que hemos solicitado. Estos procedimientos necesitan muchos datos aleatorios, por lo que nos pide que generemos actividad en el sistema para ayudarle (Fig. 2.24).

```
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
+++++++++++++++++++++++.+++++.+++++++++++++..++++++++++.+++++++++++++++.++++
++++++..++++++++++.+++++++++++++++++++.+++++.++++++++++++++>++++++++++.......
.....................................+++++
```

Fig. 2.24. *Entropía.*

9. En poco tiempo el proceso termina y ya tenemos nuestras claves creadas (Fig. 2.25).

```
gpg: clave EC2B0C7F marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n, 0m, 0f, 1u
pub   1024D/EC2B0C7F 2012-08-29
      Huella de clave = 73F5 E556 FF38 9BB8 98C5  88B4 E203 B191 EC2B 0C7F
uid                  alumno (seguridad 2012) <alumno@gmail.com>
sub   1024g/EC40F46E 2012-08-29

alumno@alumno-VirtualBox:~$
```

Fig. 2.25. *Claves creadas.*

10. Si nos fijamos, veremos una clave primaria (`pub`) de tipo DSA con tamaño de clave 1 024 (`1024D`). Debajo hay una clave subordinada de tipo Elgamal con tamaño de clave 1 024 (`1024g`).

11. En el directorio HOME del usuario se ha creado un directorio oculto llamado `.gnupg`, donde se guardan los ficheros internos que utiliza la herramienta (Fig. 2.26). El fichero `pubring.gpg` contiene las claves públicas y el fichero `secring.gpg`, las claves privadas. Por supuesto, ambos están cifrados.

```
alumno@alumno-VirtualBox:~$ ls -l .gnupg/
total 32
-rw------- 1 alumno alumno 9398 ago 28 12:46 gpg.conf
-rw------- 1 alumno alumno  920 ago 29 12:33 pubring.gpg
-rw------- 1 alumno alumno  920 ago 29 12:33 pubring.gpg~
-rw------- 1 alumno alumno  600 ago 29 12:33 random_seed
-rw------- 1 alumno alumno 1057 ago 29 12:33 secring.gpg
-rw------- 1 alumno alumno 1360 ago 29 12:33 trustdb.gpg
alumno@alumno-VirtualBox:~$ strings .gnupg/pubring.gpg
C-NVFI
(zpt
7qCNs&
*alumno (seguridad 2012) <alumno@gmail.com>
v2=?
alumno@alumno-VirtualBox:~$
```

Fig. 2.26. *Ficheros internos.*

12. Para trabajar con las claves debemos utilizar la propia herramienta. La lista de claves la obtenemos con el parámetro `list-keys` (Fig. 2.27). En pantalla aparecerá nuestra clave principal y la subordinada.

```
alumno$ gpg --list-keys
```

(Continúa)

Caso práctico 3

(Continuación)

```
alumno@alumno-VirtualBox:~$ gpg --list-keys
/home/alumno/.gnupg/pubring.gpg
--------------------------------
pub   1024D/EC2B0C7F 2012-08-29
uid                  alumno (seguridad 2012) <alumno@gmail.com>
sub   1024g/EC40F46E 2012-08-29

alumno@alumno-VirtualBox:~$
```

Fig. 2.27. *Lista de claves.*

13. Comparado con el caso práctico del cifrado simétrico, estamos en el paso 13 y todavía no hemos cifrado nada: como ya suponíamos, la criptografía asimétrica es un poco más complicada. Ahora tenemos que comunicar nuestra clave pública a quien esté interesado en enviarnos un mensaje cifrado. Primero tenemos que sacarla del llavero. El parámetro es `export` (Fig. 2.28):

```
alumno$ gpg -a --export -o /tmp/alumno.pub alumno
```

```
alumno@alumno-VirtualBox:~$ gpg -a --export -o /tmp/alumno.pub alumno
alumno@alumno-VirtualBox:~$ head /tmp/alumno.pub
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQGiBFA978oRBAC3OTLZhZeEG8lDO7pb7NdNAh3Kjbc1Mq9ZwmymVPVC9HQzhCny
hQz94I3WgAkaAiIPwnZy8kIVOHwvtRegI6twGCMxzO97S5V30jZDrGgMAbdStAK6
uDZfHLrYd53ug5oJyBZp9/L38HJsuSH/O1SrwqFhGNnSbQjBOBGWOyDvKwCgpV/t
S4UUQy1OVkZJ9hM6v3+JBh0D/1kjbKYz0+nyb+4Ofpl93Fwb3gVeq+ktAZdqUbi+
NTjMLGpb84Z0vYSr9K9ePoBEU/LfsA8ijpdDD5uRQ99iB6LtlDX043vCAP4XpRz+
o1VHm6XKKHpwdJz6HVNBfLwfEG1CByacz1BRAQ7BVIxfuh83cUNOcyaQYAkBkLnA
w/liA/wM61J9fbMcp/JvEqyFS5KL9/s91U/p3ZvW2KE2Y0rvj/2ICJyM6/AE6LrK
alumno@alumno-VirtualBox:~$
```

Fig. 2.28. *Exportamos la clave pública.*

Hemos utilizado los parámetros `a` (armor) para que el resultado no sea binario y `o` (output) para guardarlo directamente en un fichero (si no, aparece por la salida estándar). El fichero lo ponemos tranquilamente en `/tmp` porque no nos importa que otros usuarios lo copien.

14. En la máquina tenemos un segundo usuario llamado `profesor`. Entramos con este usuario para enviar un mensaje cifrado al usuario `alumno` con la misma herramienta gpg. Para coger las claves públicas de `alumno` utilizamos el parámetro `import` (Fig. 2.29):

```
profesor$ gpg --import /tmp/alumno.pub
```

```
profesor$ gpg --import /tmp/alumno.pub
gpg: /home/profesor/.gnupg: directorio creado
gpg: creado un nuevo archivo de configuraciÃ³n '/home/profesor/.gnupg/gpg.conf'
gpg: AVISO: las opciones en '/home/profesor/.gnupg/gpg.conf' no estÃ¡n aÃºn acti
vas en esta ejecuciÃ³n
gpg: anillo Â«/home/profesor/.gnupg/secring.gpgÂ» creado
gpg: anillo Â«/home/profesor/.gnupg/pubring.gpgÂ» creado
gpg: /home/profesor/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave EC2B0C7F: clave pÃºblica "alumno (seguridad 2012) <alumno@gmail.com>"
 importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
profesor$
```

Fig. 2.29. *Importamos la clave pública.*

15. En nuestro ejemplo el usuario `profesor` es la primera vez que utiliza la herramienta gpg, por lo que se le informa que se crea el directorio `.gnupg` y los ficheros internos.

16. Podemos consultar las claves disponibles en el llavero con el mismo parámetro `list-keys` que vimos anteriormente (Fig. 2.30):

```
profesor$ gpg --list-keys
```

```
profesor$ gpg --list-keys
/home/profesor/.gnupg/pubring.gpg
---------------------------------
pub   1024D/EC2B0C7F 2012-08-29
uid                  alumno (seguridad 2012) <alumno@gmail.com>
sub   1024g/EC40F46E 2012-08-29

profesor$
```

Fig. 2.30. *Claves disponibles.*

17. Vamos a crear un fichero llamado `mensaje` y lo cifraremos para enviárselo al usuario `alumno`. Los comandos serían (Fig. 2.31):

```
profesor$ fortune > mensaje

profesor$ gpg -v -a -o /tmp/mensaje.cifrado
--encrypt --recipient alumno mensaje
```

```
profesor$ gpg -v -a -o /tmp/mensaje.cifrado --encrypt --recipient alumno mensaje

gpg: usando PGP como modelo de confianza
gpg: usando subclave EC40F46E en vez de clave primaria EC2B0C7F
gpg: EC40F46E: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub  1024g/EC40F46E 2012-08-29 alumno (seguridad 2012) <alumno@gmail.com>
 Huella de clave primaria: 73F5 E556 FF38 9BB8 98C5  80B4 E203 B191 EC2B 0C7F
      Huella de subclave: DBFE B53F 0B0B B8B1 8473  BC17 6276 F32E EC40 F46E

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si "realmente" sabe lo que estÃ¡ haciendo,
puede contestar sÃ- a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N)
```

Fig. 2.31. *Ciframos un fichero.*

Los parámetros `a` y `o` ya los conocemos (dejamos el fichero en `/tmp` porque no nos importa que otros usuarios puedan leerlo: sin la clave privada, el contenido es ininteligible). Hemos añadido el parámetro `v` (verbose) para obtener más información. En este caso, nos sirve para conocer que utilizará la clave subordinada (Elgamal), en lugar de la clave primaria (DSA).

El parámetro `encrypt` indica que deseamos cifrado asimétrico y el parámetro `recipient` va seguido del identificador de la clave pública que queremos utilizar. Como ya sabemos, el cifrado utiliza la clave pública del receptor.

18. Una vez introducido ese comando, la respuesta es una advertencia: no hay seguridad de que esa clave pública sea realmente la clave pública de `alumno`. Cualquiera podría haber cambiado el fichero `/tmp/alumno.pub` antes de que `profesor` hiciera el `import` de las claves. Como ayuda, el comando nos

(Continúa)

Caso práctico 3

(Continuación)

ofrece la huella (fingerprint) de la clave y nos pide la confirmación de que es la clave que queremos utilizar.

19. Podemos volver a la sesión del usuario `alumno`, obtener la huella de su clave pública y compararla con la que aparece en la sesión de `profesor`. El parámetro para obtener la huella es `fingerprint` (Fig. 2.32):

```
alumno$ gpg --fingerprint
```

```
alumno@alumno-VirtualBox:~$ gpg --fingerprint
/home/alumno/.gnupg/pubring.gpg
------------------------------
pub   1024D/EC2B0C7F 2012-08-29
      Huella de clave = 73F5 E556 FF38 9B88 98C5  88B4 E203 B191 EC2B 0C7F
uid                  alumno (seguridad 2012) <alumno@gmail.com>
sub   1024g/EC40F46E 2012-08-29

alumno@alumno-VirtualBox:~$
```

Fig. 2.32. *Obtenemos la huella de la clave.*

20. Efectivamente, las huellas coinciden y podemos confiar en que la clave importada en `profesor` es correcta. Confirmamos que queremos usar esa clave y se crea el fichero cifrado. Ahora podemos volver a la sesión del usuario `alumno` e intentar descifrarlo. El parámetro es `decrypt`:

```
alumno$ gpg --decrypt /tmp/mensaje.
cifrado
```

Como esperábamos, el comando nos solicita la contraseña que da acceso a la clave privada. En la ventana aparece qué clave necesita (en nuestro caso, la clave del algoritmo Elgamal), con toda su identificación (Fig. 2.33).

Si pulsamos en *Detalles* podemos elegir que el sistema recuerde esta clave; así ahorraremos volver a teclearla. Como vimos en la Unidad 1, no es recomendable que la recuerde para siempre, porque cualquiera podría coger nuestro ordenador y descifrar nuestros mensajes.

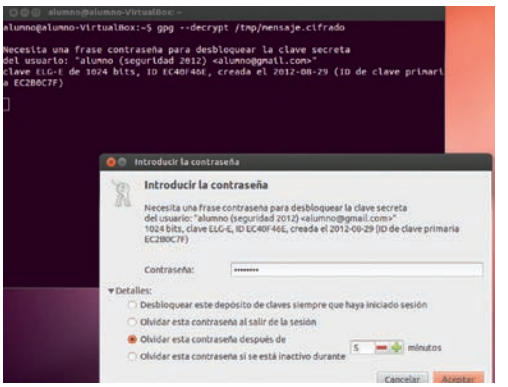


Fig. 2.33. *Desciframos el fichero.*

21. Si hemos introducido bien la contraseña aparecerá el mensaje que nos ha enviado el usuario `profesor` (Fig. 2.34).

```
gpg: cifrado con clave ELG-E de 1024 bits, ID EC40F46E, creada el 2012-08-29
      «alumno (seguridad 2012) <alumno@gmail.com>»
"Not Hercules could have knock'd out his brains, for he had none."
                -- Shakespeare
alumno@alumno-VirtualBox:~$
```

Fig. 2.34. *Contenido recuperado.*

22. Podemos comprobar qué pasa si el fichero, por cualquier razón, resulta dañado (defecto físico del disco duro, error en la transmisión, etc.). En el usuario `alumno` hacemos una copia del fichero y lo editamos para cambiar cualquier letra. Si después lo intentamos descifrar, aparecerá un error (Fig. 2.35).

```
alumno@alumno-VirtualBox:~$ cp /tmp/mensaje.cifrado a
alumno@alumno-VirtualBox:~$ vi a
alumno@alumno-VirtualBox:~$ gpg --decrypt a
gpg: Error en suma de comprobación: F2AB33 - 69C517
alumno@alumno-VirtualBox:~$
```

Fig. 2.35. *Detectamos error en el fichero cifrado.*

23. Si ahora el usuario `alumno` quisiera enviar un fichero cifrado a `profesor`, primero `profesor` debería generar su propio par de claves, después exportar la clave pública, hacerla llegar hasta `alumno` para que la importe, etc.



Fig. 2.36. *Tarjeta inteligente.*

La solución más común a los problemas de proteger y transportar la clave privada es la **tarjeta inteligente** (Fig. 2.36). Es una tarjeta de plástico que contiene un **chip** electrónico. Hay dos tipos:

- Tarjeta de **memoria.** Es equivalente a una memoria Flash y se limita a almacenar el llavero. Cuando se introduce en el lector, el ordenador hace una copia temporal del llavero y trabaja con él introduciendo la clave simétrica, etc.
- Tarjeta **procesadora.** La tarjeta de memoria es peligrosa porque hemos expuesto nuestro llavero. En cambio, en las tarjetas procesadoras las claves también están almacenadas, pero nunca salen de la tarjeta. Cualquier cifrado que necesite nuestra clave privada es **realizado por el propio chip** porque incluye una CPU, memoria RAM, etc. Por supuesto, sigue siendo necesario introducir la clave simétrica que abre el llavero.

El ejemplo más sencillo es la tarjeta SIM de los teléfonos móviles: para poder usarla necesitamos introducir el número PIN. Aunque la usemos en otro teléfono, el PIN es el mismo porque está asociado a la tarjeta. En la sección final de esta unidad veremos otro ejemplo de tarjeta inteligente: el DNI electrónico.

Las tarjetas inteligentes también se pueden clasificar por su tipo de interfaz:

- Tarjeta de **contacto.** El lector necesita tocar los contactos metálicos del chip para interactuar con él. Son las más utilizadas, sobre todo en entornos de alta seguridad, como el sector bancario, Administración electrónica, etc.
- Tarjeta **sin contacto.** El lector utiliza tecnologías inalámbricas para interactuar con el chip. Se utilizan en situaciones donde se necesitan transacciones rápidas, como el acceso al transporte público.

El cifrado asimétrico no se puede utilizar para cifrar todos los paquetes intercambiados en una red local porque el bajo rendimiento del algoritmo ralentizaría el tráfico. En su lugar se adopta un **esquema híbrido:**

- Criptografía **asimétrica solo para el inicio de la sesión,** cuando hay que generar un canal seguro donde acordar la clave simétrica aleatoria que se utilizará en esa conversación.
- Criptografía **simétrica durante la transmisión,** utilizando la clave simétrica acordada durante el inicio de sesión. Generalmente se suele cambiar la clave simétrica cada cierto tiempo (minutos) para dificultar más el espionaje de la conversación.

Es decir, cuando A quiere establecer una conversación con B, en A se genera en ese instante una nueva clave simétrica (CS). Para enviársela a B de modo seguro, A la cifra utilizando un algoritmo asimétrico con la clave pública de B. Cuando B recibe la CS cifrada, la descifra con su clave privada y desde ese momento pueden seguir el diálogo cifrando con el algoritmo simétrico acordado y la CS recibida. En la Figura 2.37 vemos un ejemplo con el protocolo SSH.

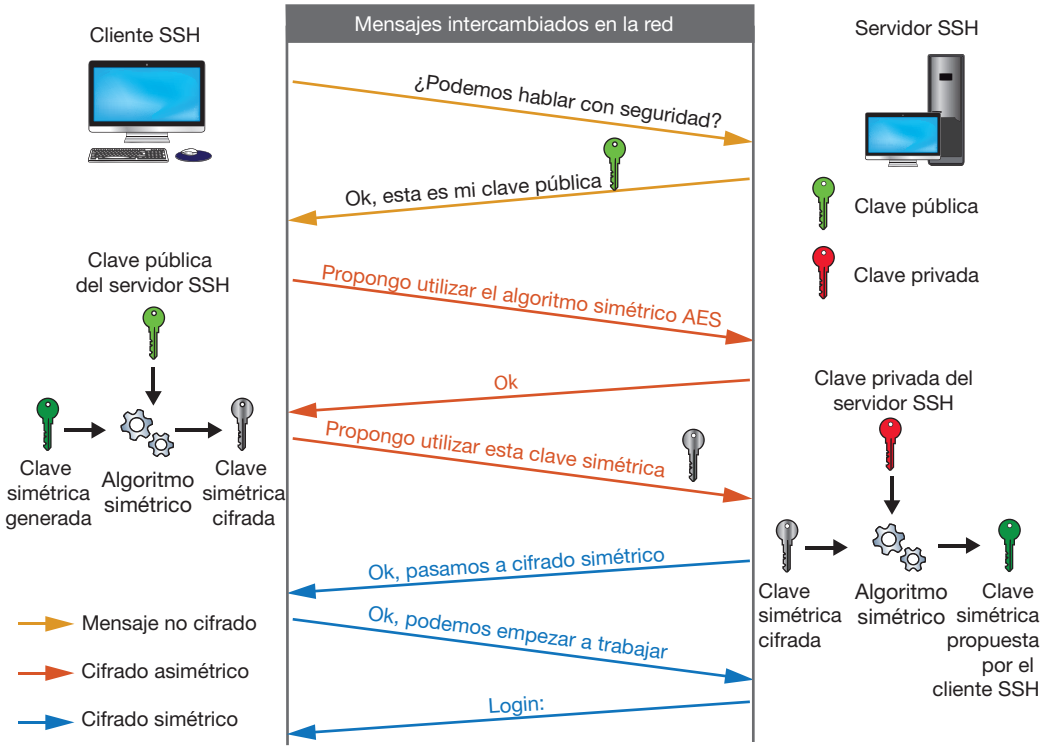


Fig. 2.37. *Esquema híbrido de cifrado en SSH.*

Actividades

12. Entre dos compañeros, utilizad gpg en modo asimétrico para enviar un correo electrónico que dentro lleve un mensaje cifrado.

13. ¿Podríamos proteger el archivo de llaves con un algoritmo asimétrico?

14. ¿Para qué sirve el parámetro gen-revoke en la herramienta gpg?

15. Investiga si la tarjeta SIM es de tipo procesadora o memoria.

16. Las primeras tarjetas de crédito utilizaban una banda magnética; después cambiaron a chip. ¿Por qué?

17. Busca cómo se puede establecer un túnel seguro con un servidor FTP mediante SSH.

Vocabulario

SSH (Secure SHell). Protocolo de comunicaciones que permite cifrar la conversación extremo a extremo. Se utiliza para sesiones interactivas de comandos (es un buen sustituto de telnet), transferencias de archivos (sustituto de FTP), túneles seguros entre aplicaciones, etc.

4. Cifrar y firmar

Vocabulario

La función hash se utiliza también para comprobar que un fichero no ha sido alterado. Es importante sobre todo si el fichero es un ejecutable, que puede haber sido modificado por un virus para intentar replicarse. Las funciones más utilizadas son MD5 y las distintas versiones de SHA.

La primera utilidad de la criptografía es ocultar el mensaje para aquellos que no son destinatarios del mismo. Es decir, garantizar la **confidencialidad de la comunicación** cifrando el documento original.

La segunda utilidad es conseguir determinar la **autenticidad del emisor.** ¿Cómo podía estar seguro el general romano de que ese mensaje con las nuevas órdenes venía de otro general romano, y no de algún enemigo? Si el enemigo conocía el algoritmo de cifrado y la clave actual, podía intentar engañarle mediante un mensaje falso pero correctamente cifrado.

En el paso 18 del caso práctico 3 nos ha ocurrido lo mismo: hemos tenido que recurrir a una comprobación más (entrar al usuario alumno para comparar la huella de su clave) para estar seguros de que estábamos cifrando el mensaje para el destinatario correcto.

En criptografía asimétrica, el **mecanismo de firma** garantiza que el emisor es quien dice ser. Supongamos que vamos a enviar un documento y queremos que el receptor confíe en que somos nosotros (Fig. 2.38). Para conseguirlo, el emisor aplica al documento una función resumen (función **hash**). El resultado de esta función es una lista de caracteres, el **resumen,** que la función garantiza que solo se pueden haber obtenido con el documento original (el algoritmo de la función hash no necesita una clave extra como los algoritmos de cifrado). Ahora **el emisor cifra ese resumen con su clave privada** y lo envía al destino, junto con el documento original.

En el destino se hacen dos operaciones:

- Aplicar la misma función hash al documento para obtener su resumen.
- Descifrar el resumen recibido, utilizando la clave pública del emisor.

Si ambos resúmenes coinciden, el destino puede estar seguro de que el emisor del documento es el mismo que el dueño de la clave pública que acaba de aplicar para descifrar el resumen recibido.

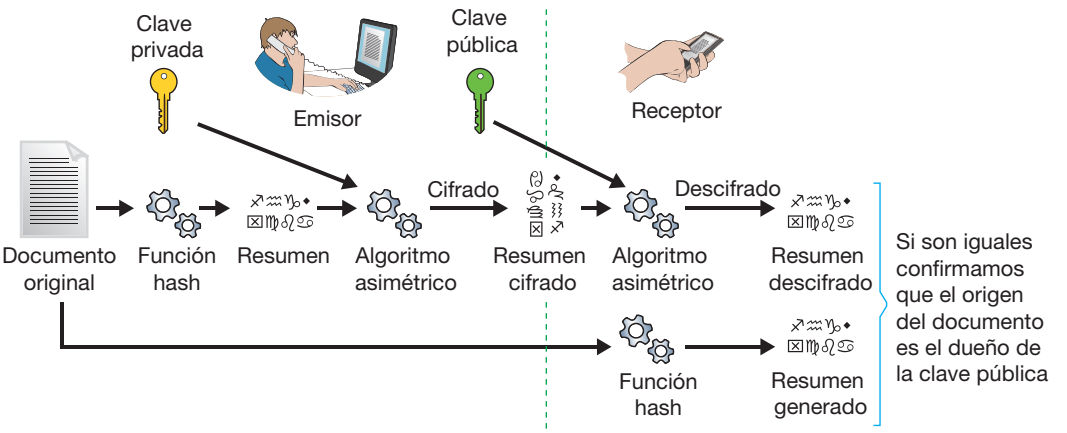


Fig. 2.38. *Mecanismo de firma.*

Actividades

18. ¿Cómo harías llegar al servidor, de manera segura, las claves públicas de los clientes?

19. Investiga cómo confirma un cliente que el servidor al que se conecta es el auténtico y no un impostor.

20. Envía a un compañero un fichero ejecutable firmado. Él deberá comprobar la firma, extraer el fichero y ejecutarlo para confirmar que ha llegado bien.

21. ¿Por qué se firma solo el resumen del documento, y no el documento completo?

Por supuesto, si queremos que el documento original no pueda ser interceptado en la transmisión desde el emisor al receptor, debemos cifrarlo. Para ello usaremos la clave pública del receptor. El procedimiento completo sería:

- El emisor **aplica la función hash al original** para generar el resumen.
- El emisor toma **su clave privada** para aplicar el algoritmo asimétrico al documento resumen. El resultado es un documento resumen cifrado.
- El emisor toma **la clave pública del receptor** para aplicar el algoritmo asimétrico al documento original y al documento resumen. El resultado es un documento conjunto cifrado que se envía al receptor.

En el receptor, utiliza **su clave privada** para descifrar los documentos y **la clave pública del origen** para comprobar la firma.

Caso práctico 4

Firma digital en Linux

Objetivo. Utilizar la herramienta gpg para firmar ficheros.

Material. Ordenador con Linux Ubuntu 12.04.

■ **Duración:** 15 minutos ■ **Dificultad:** Media

1. Seguimos con el usuario `alumno` del caso práctico 3. Recordemos que habíamos generado dos parejas de claves, una pareja DSA y una pareja Elgamal. En el cifrado del fichero habíamos utilizado la clave Elgamal.
2. En la sesión de `alumno` creamos un fichero `mensaje` y lo firmamos con nuestra clave privada para que cualquiera pueda confirmar que es nuestro. Usaremos el parámetro `detach-sign`, que crea un fichero nuevo solo con la firma (el cifrado del resultado de aplicar el hash al fichero original). Utilizaremos también el parámetro `a` para observar ese fichero. Los comandos son:

```
alumno$ fortune > mensaje
alumno$ gpg -a --detach-sign mensaje
```

3. En la Figura 2.39 vemos que la herramienta nos pide la contraseña de nuestra clave secreta de tipo DSA (directamente utiliza esa, no Elgamal). Como al cifrar, es recomendable evitar que recuerde la contraseña.

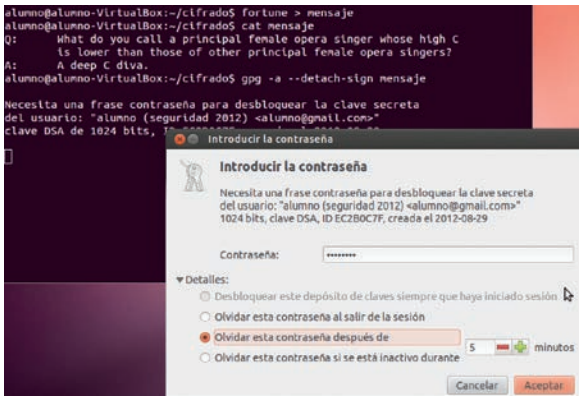


Fig. 2.39. *Firma separada.*

4. El resultado del cifrado será un nuevo fichero `mensaje.asc` (Fig. 2.40). La primera línea indica que es una firma `(PGP SIGNATURE)`.

```
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 8
-rw-rw-r-- 1 alumno alumno 145 ago 30 18:05 mensaje
-rw-rw-r-- 1 alumno alumno 198 ago 30 18:06 mensaje.asc
alumno@alumno-VirtualBox:~/cifrado$ cat mensaje.asc
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iEYEABECAAYFAlA/j0YACgkQ4gOxkewrDH9imwCfWmsuenJcfHP/eh/FH8S5ZAlB
m30Amwc1/ld6x/7XcvskH7WQIXU0z+UQ
=tXFJ
-----END PGP SIGNATURE-----
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.40. *Fichero de firma.*

5. Ahora realizamos el envío al usuario `profesor` (por ejemplo, podríamos estar entregando un trabajo). En este caso simplemente lo copiaremos en `/tmp`. Hay que copiar los dos ficheros: `mensaje`, que no lleva la firma, y `mensaje.asc`, que solo es una firma. Los comandos serían:

```
alumno$ cp mensaje /tmp
alumno$ cp mensaje.asc /tmp
```

6. Iniciamos una sesión con el usuario `profesor`, copiamos los ficheros a nuestro directorio y comprobamos la firma. El parámetro es `verify` junto con el nombre del fichero que lleva la firma (en nuestro caso, `mensaje.asc`). Los comandos son (Fig. 2.41):

```
profesor$ cp /tmp/mensaje* .
profesor$ gpg --verify mensaje.asc
```

```
profesor@alumno-VirtualBox:~/trabajos$ cp /tmp/mensaje* .
profesor@alumno-VirtualBox:~/trabajos$ gpg --verify mensaje.asc
gpg: Firmado el jue 30 ago 2012 18:05:26 CEST usando clave DSA ID EC2B0C7F
gpg: Firma correcta de Â«alumno (seguridad 2012) <alumno@gmail.com>Â»
gpg: AVISO: Â¡Esta clave no estÃ¡ certificada por una firma de confianza!
gpg:         No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 73F5 E556 FF38 9B88 98C5  88B4 E203 B19
1 EC2B 0C7F
profesor@alumno-VirtualBox:~/trabajos$
```

Fig. 2.41. *Comprobamos la firma.*

7. El mensaje de la herramienta dice que, efectivamente, el fichero `mensaje` ha sido firmado por el dueño de la clave privada cuya clave pública tenemos almacenada con esa misma identificación (nombre, huella, etc.). También insiste en que no está confirmado que efectivamente esa sea su clave; pero esto lo resolveremos pronto.
8. Podemos probar a alterar algún carácter dentro del fichero original o dentro del fichero cifrado; la verificación fallará (Fig. 2.42).

```
profesor@alumno-VirtualBox:~/trabajos$ echo a >>mensaje
profesor@alumno-VirtualBox:~/trabajos$ gpg --verify mensaje.asc
gpg: Firmado el jue 30 ago 2012 18:05:26 CEST usando clave DSA ID EC2B0C7F
gpg: Firma INCORRECTA de Â«alumno (seguridad 2012) <alumno@gmail.com>Â»
profesor@alumno-VirtualBox:~/trabajos$
```

Fig. 2.42. *Detectamos modificaciones.*

9. Para evitar enviar dos ficheros, podemos incluirlo todo en el mismo. Volvemos a la sesión del usuario `alumno` y ahora firmamos con el parámetro `clearsign`. El comando sería:

```
alumno$ gpg -a --clearsign mensaje
```

10. De nuevo hay un fichero `mensaje.asc` pero ahora contiene tanto la firma como el texto del mensaje (Fig. 2.43).

(Continúa)

Caso práctico 4

(Continuación)

```
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 8
-rw-rw-r-- 1 alumno alumno 145 ago 30 18:05 mensaje
-rw-rw-r-- 1 alumno alumno 390 ago 30 18:39 mensaje.asc
alumno@alumno-VirtualBox:~/cifrado$ cat mensaje.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Q:      What do you call a principal female opera singer whose high C
        is lower than those of other principal female opera singers?
A:      A deep C diva.
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iEYEARECAAYFAlA/lx0ACgkQ4gOxkewrDH/fIgCfT1Z2qdF+tUFKRwZalfdMro76
YSkAn1nO/2ApugH/ziS5a3hk5uUX2cYS
=oYEd
-----END PGP SIGNATURE-----
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.43. *Firma y contenido en el mismo fichero.*

11. Podemos copiarlo de nuevo a `/tmp` y tomarlo desde la sesión del `profesor`. El comando de verificación es el mismo que en el caso del fichero separado (Fig. 2.44).

```
profesor@alumno-VirtualBox:~/trabajos$ rm *
profesor@alumno-VirtualBox:~/trabajos$ cp /tmp/mensaje.asc .
profesor@alumno-VirtualBox:~/trabajos$ gpg --verify mensaje.asc
gpg: Firmado el jue 30 ago 2012 18:38:53 CEST usando clave DSA ID EC2B0C7F
gpg: Firma correcta de Â«alumno (seguridad 2012) <alumno@gmail.com>Â»
gpg: AVISO: Â¡Esta clave no estÃ¡ certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 73F5 E556 FF38 9BB8 98C5  88B4 E203 B19
1 EC2B 0C7F
profesor@alumno-VirtualBox:~/trabajos$
```

Fig. 2.44. *Comprobamos la firma del fichero conjunto.*

12. Hasta ahora, el fichero `mensaje` estaba accesible, bien porque estaba separado de la firma, bien porque estaba junto a ella pero en texto claro. Si utilizamos la opción `sign` tendremos un fichero único con el texto y la firma, e ilegible. El comando sería (Fig. 2.45):

```
alumno$ gpg -a --sign mensaje
```

```
alumno@alumno-VirtualBox:~/cifrado$ gpg -a --sign mensaje

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "alumno (seguridad 2012) <alumno@gmail.com>"
clave DSA de 1024 bits, ID EC2B0C7F, creada el 2012-08-29

alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 8
-rw-rw-r-- 1 alumno alumno 145 ago 30 18:05 mensaje
-rw-rw-r-- 1 alumno alumno 389 ago 30 19:04 mensaje.asc
alumno@alumno-VirtualBox:~/cifrado$ cat mensaje.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.11 (GNU/Linux)

owGbwMvMwCT4iHnjxDfaPPWMa+Ylseem5hUnZqUG2M9lCrTiDM9ILFFIyVeozC9V
SE7MyVFIVCgoysxLzixIzFFIS81NzElVyC9ILUpUKM7MS08tUijPyC9OVcjITM9Q
cObizCxWyMkvBwqXZCTmAQmQXH6aQn5JBlAMr0HF9lyOVpyOCimpqQUKzgopmWWJ
elwdbiwMgkwMbKxMIOcxcHEKwJyeEcEwV2iKlcPhQJ/INXuLFu2x+MUn85w3mGGe
0oGak9Urb9RtaF7yPFhfM2zS0ZflAA==
=+owa
-----END PGP MESSAGE-----
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.45. *Firma protegida.*

13. De nuevo podemos llevarlo al directorio `/tmp` para que el usuario `profesor` haga una copia y lo verifique. Si además queremos extraer el fichero (Fig. 2.46) utilizaremos `decrypt`:

```
profesor$ rm mensaje.*
profesor$ cp /tmp/mensaje.asc .
profesor$ gpg --verify mensaje.asc
profesor$ gpg --decrypt -o mensaje men-
saje.asc
```

```
profesor@alumno-VirtualBox:~/trabajos$ rm mensaje*
profesor@alumno-VirtualBox:~/trabajos$ cp /tmp/mensaje.asc .
profesor@alumno-VirtualBox:~/trabajos$ gpg --verify mensaje.asc
gpg: Firmado el jue 30 ago 2012 19:04:02 CEST usando clave DSA ID EC2B0C7F
gpg: Firma correcta de Â«alumno (seguridad 2012) <alumno@gmail.com>Â»
gpg: AVISO: Â¡Esta clave no estÃ¡ certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 73F5 E556 FF38 9BB8 98C5  88B4 E203 B19
1 EC2B 0C7F
profesor@alumno-VirtualBox:~/trabajos$ gpg --decrypt -o mensaje mensaje.asc
gpg: Firmado el jue 30 ago 2012 19:04:02 CEST usando clave DSA ID EC2B0C7F
gpg: Firma correcta de Â«alumno (seguridad 2012) <alumno@gmail.com>Â»
gpg: AVISO: Â¡Esta clave no estÃ¡ certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 73F5 E556 FF38 9BB8 98C5  88B4 E203 B19
1 EC2B 0C7F
profesor@alumno-VirtualBox:~/trabajos$ cat mensaje
Q:      What do you call a principal female opera singer whose high C
        is lower than those of other principal female opera singers?
A:      A deep C diva.
profesor@alumno-VirtualBox:~/trabajos$
```

Fig. 2.46. *Comprobamos la firma y extraemos el fichero.*

14. Aunque esta protección es bastante débil, porque cualquiera que tenga la clave pública de `alumno` tendrá acceso al contenido del fichero. Debemos utilizar el cifrado normal, lo que nos lleva a que el usuario `profesor` genere su par de claves (hasta ahora no ha sido necesario). Utilizaremos el parámetro `gen-key` (Fig. 2.47) con parámetros similares al caso práctico 3 (claves DSA y Elgamal, duración ilimitada, etc.):

```
profesor$ gpg --gen-key
```

```
gpg: clave 7D6D535B marcada como de confianza absoluta
claves pÃºblica y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n, 0m, 0f, 1u
pub   1024D/7D6D535B 2012-08-30
      Huella de clave = 3396 9D3D D9D8 8396 A523  529B 0675 0790 7D6D 535B
uid                  profesor (seguridad 2012) <profesor.si2012@gmail.com>
sub   1024g/941A6CDB 2012-08-30

profesor@alumno-VirtualBox:~/trabajos$
```

Fig. 2.47. *Generamos las claves de profesor.*

15. Con `list-keys` podemos comprobar que tenemos dos claves: las nuestras y las de `alumno` (Fig. 2.48).

```
profesor@alumno-VirtualBox:~/trabajos$ gpg --list-keys
/home/profesor/.gnupg/pubring.gpg
---------------------------------
pub   1024D/EC2B0C7F 2012-08-29
uid                  alumno (seguridad 2012) <alumno@gmail.com>
sub   1024g/EC40F46E 2012-08-29

pub   1024D/7D6D535B 2012-08-30
uid                  profesor (seguridad 2012) <profesor.si2012@gmail.com>
sub   1024g/941A6CDB 2012-08-30

profesor@alumno-VirtualBox:~/trabajos$
```

Fig. 2.48. *Todas las claves de profesor.*

16. Ahora por fin podemos confirmar que la clave pública del usuario `alumno` es auténtica. Utilizaremos el parámetro `sign-key` y el identificador de la clave (Fig. 2.49):

```
profesor$ gpg --sign-key alumno
```

(Continúa)

Caso práctico 4

(Continuación)

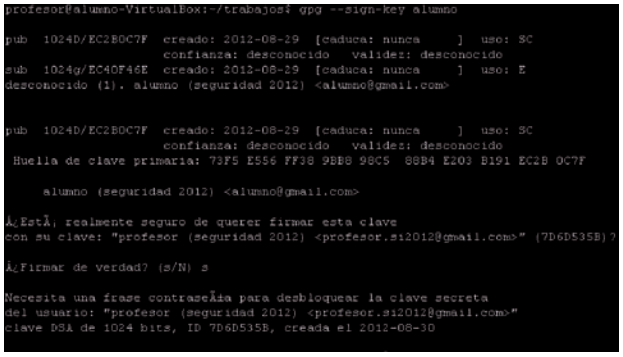


Fig. 2.49. *Confirmamos la clave de alumno.*

17. Desde ahora las verificaciones ya no emitirán el aviso de que la clave es sospechosa (Fig. 2.50).

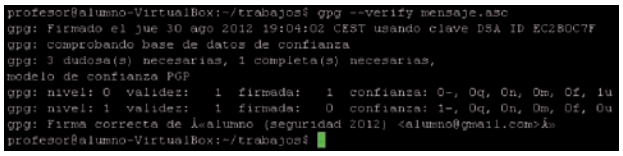


Fig. 2.50. *Ahora la firma es fiable.*

18. Para que `alumno` nos pueda cifrar el fichero firmado, debemos seguir el procedimiento conocido: exportar la clave pública de `profesor` e importarla en `alumno`. Los comandos a introducir en cada sesión serían:

```
profesor$ gpg -a --export /tmp/profesor.pub profesor
alumno$ gpg --import /tmp/profesor.pub
```

19. En la sesión de `alumno` podemos usar `list-key` para consultar todas las claves que tiene almacenadas (Fig. 2.51).



Fig. 2.51. *Todas las claves de alumno.*

20. En la sesión de `alumno` vamos a generar un nuevo fichero, lo cifraremos para que solo `profesor` pueda recuperarlo y lo firmaremos para que sepa que es nuestro. Primero firmaremos la clave pública de `profesor` para evitar mensajes de error. Después ejecutaremos conjuntamente `sign` y `encript` (Fig. 2.52):

```
Alumno$ gpg --sign-key profesor
Alumno$ fortune > mensaje
Alumno$ gpg -a --sign --encrypt --recipient profesor mensaje
Alumno$ cp mensaje.asc /tmp
```



Fig. 2.52. *Firmamos y ciframos.*

21. El fichero `mensaje.asc` es ilegible y lleva dentro el contenido del fichero `mensaje` y la firma. Lo copiamos en `/tmp` para recuperarlo desde la sesión de `profesor`, descifrarlo, verificar la firma y recuperar el fichero `mensaje`. El parámetro será `decrypt`, porque también nos ofrece la confirmación de la firma (Fig. 2.53). Nos pedirá la contraseña que protege la clave privada de `profesor`, necesaria para descifrar el fichero. Los comandos serían:

```
profesor$ cp /tmp/mensaje.asc
profesor$ gpg --decrypt -o mensaje mensaje.asc
profesor$ cat mensaje
```

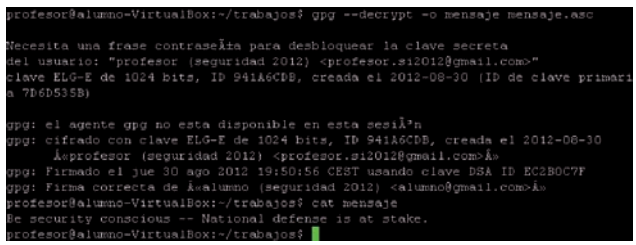


Fig. 2.53. *Recuperamos el fichero destinado a profesor.*

22. Si no tenemos la clave privada de `profesor`, no podemos descifrar ni, por tanto, recuperar el fichero ni comprobar la firma. Por ejemplo, podemos borrar nuestras propias claves con los parámetros `delete-secret-key` y `delete-key`. Después ya no funcionará ni descifrar ni verificar. El mensaje de error indicará que el fichero fue cifrado con una clave Elgamal que ya no tenemos (Fig. 2.54). Los comandos son:

```
profesor$ gpg --delete-secret-key profesor
profesor$ gpg --delete-key profesor
profesor$ gpg --list-key
profesor$ gpg --decrypt mensaje.asc
profesor$ gpg --verify mensaje.asc
```

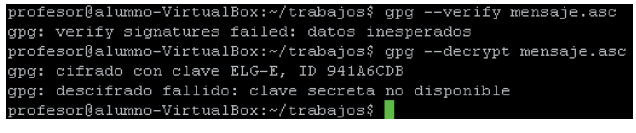


Fig. 2.54. *Mensaje irrecuperable.*

Caso práctico 5

Firma digital en Windows

Objetivo. Realizar una firma digital sobre un fichero utilizando Windows.

Material. Ordenador con Windows, ordenador con Linux Ubuntu 12.04, conexión a Internet.

■ **Duración:** ◷ 30 minutos ■ **Dificultad:** ☺ Media

1. Instalaremos el software Gpg4win. Es una adaptación a Windows de la utilidad gpg que hemos venido utilizando en Linux, aunque el entorno es bastante diferente. Lo descargamos de la página web y lanzamos el asistente de instalación (Fig. 2.55).



Fig. 2.55. *Asistente de instalación de Gpg4win.*

2. Al final de la instalación nos pedirá realizar una serie de pasos para establecer las autoridades de certificación raíz de confianza (root CA). La utilidad de una CA la veremos en el apartado siguiente al hablar de PKI. Pero en este ejemplo no lo necesitamos, así que podemos omitir este paso activando skip configuration (Fig. 2.56).



Fig. 2.56. *Certificados de confianza.*

3. Terminada la instalación, abrimos el programa. La aplicación principal se llama Kleopatra y es el administrador de certificados. Como hicimos en el caso práctico de Linux, primero vamos a generar un certificado nuevo. Entraremos en *File > New certificate* (Fig. 2.57).

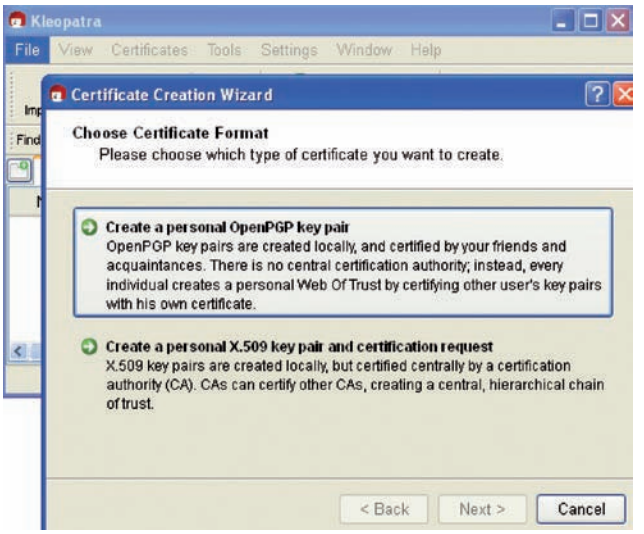


Fig. 2.57. *Nuevo certificado.*

4. La primera pregunta nos deja elegir el tipo de certificado: el simple par de claves o utilizar una CA. Como hicimos en el caso Linux, nos limitaremos a las claves, para posteriormente exportarlas, importarlas, etc.

5. El siguiente paso es introducir los datos identificativos del certificado (Fig. 2.58), que nos permiten elegirlo entre todos los disponibles en el almacén.



Fig. 2.58. *Datos identificativos.*

6. Pulsando en *Advanced Settings* podemos cambiar el tipo de algoritmo asimétrico (Fig. 2.59). Elegimos DSA y Elgamal. También podemos limitar el uso (cifrar, firmar, etc.) y la validez.

(Continúa)

Caso práctico 5

(Continuación)

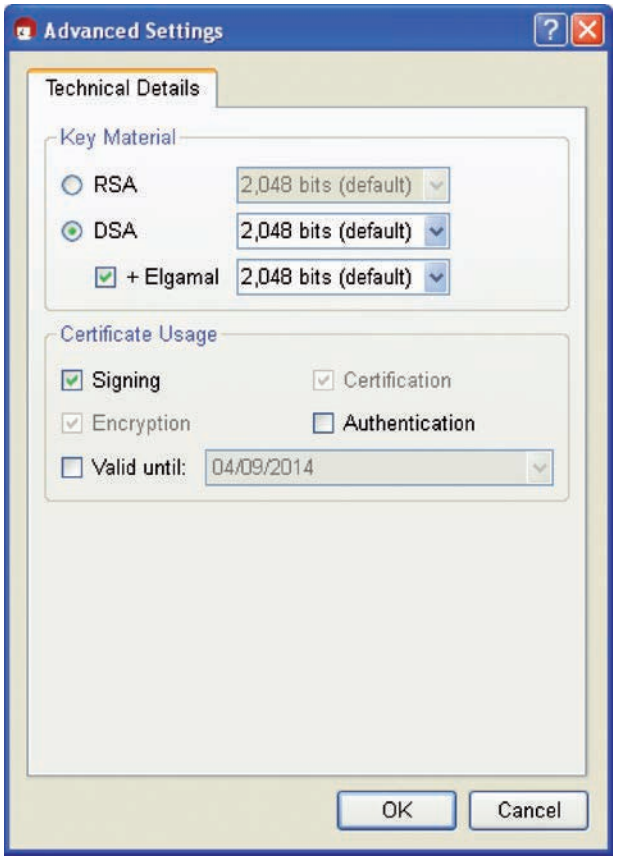


Fig. 2.59. *Ajustes del certificado.*

7. En el último paso nos pedirán confirmar los parámetros del certificado que estamos a punto de crear (Fig. 2.60).

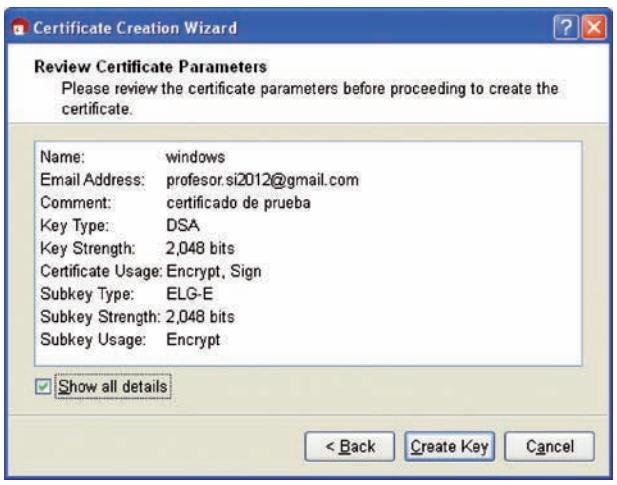


Fig. 2.60. *Parámetros del certificado.*

8. Si seguimos adelante pulsando *Create Key*, nos pedirá la contraseña simétrica que protege el certificado (Fig. 2.61).



Fig. 2.61. *Contraseña que protege el certificado.*

9. Una vez introducida la contraseña y su verificación, la herramienta necesita un tiempo para conseguir generar buenos números aleatorios que aseguren la calidad de las claves (Fig. 2.62).

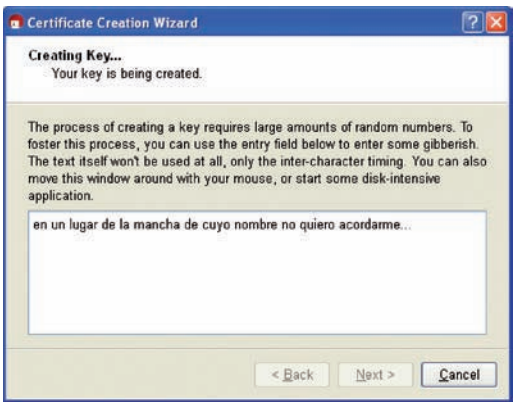


Fig. 2.62. *Generando las claves.*

10. En poco tiempo aparecerá la ventana de confirmación (Fig. 2.63). En ella aparece la huella de la clave pública (fingerprint) y nos permite terminar en este punto o hacer alguna otra operación, como un backup de las claves (el ordenador donde está Kleopatra podría estropearse), enviar el certificado por correo o subirlo a un servidor.

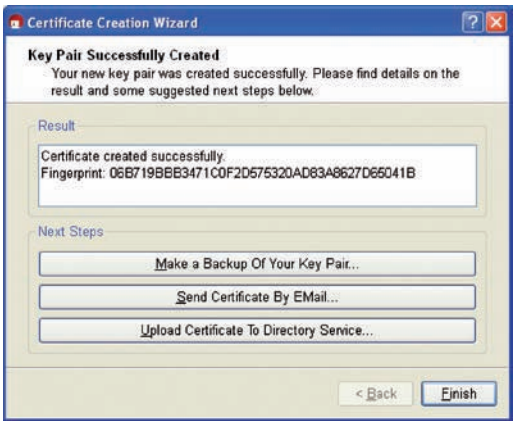


Fig. 2.63. *Claves generadas.*

(Continúa)

Caso práctico 5

(Continuación)

11. Pulsamos *Finish* y ahora en la ventana principal aparece nuestro certificado, con los identificadores utilizados y el tipo OpenPGP que habíamos elegido (Fig. 2.64).

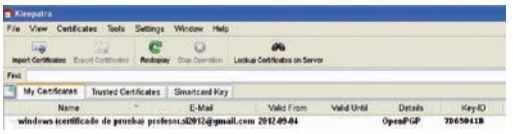


Fig. 2.64. *Certificado creado.*

12. Vamos a probar nuestras claves. Creamos un fichero de texto llamado top secret.txt, nos situamos sobre él y desplegamos al menú del botón derecho. En el nuevo menú, llamado *Más opciones de GgpEX*, elegimos *Firmar* (Fig. 2.65).

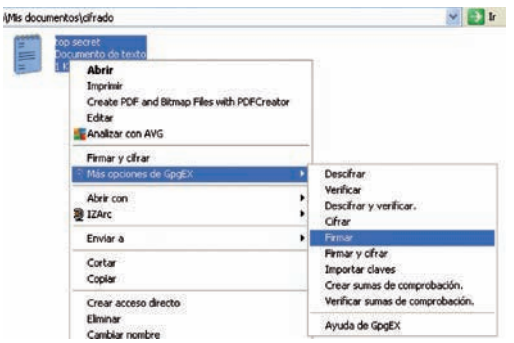


Fig. 2.65. *Menú contextual.*

13. Aparecerá un asistente del proceso de firma digital (Fig. 2.66). En el primer paso podemos elegir incluir todos los ficheros en un único fichero de tipo .tar. También optaremos entre firmar y cifrar o solo firmar. En este ejemplo elegimos solo firmar y marcamos la opción de que el fichero de salida sea legible (la conocida opción -a de la herramienta Linux).

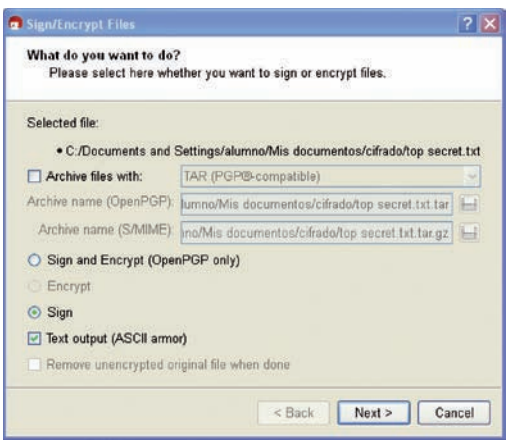


Fig. 2.66. *Asistente de firma.*

14. El siguiente paso es elegir el certificado que vamos a utilizar para firmar (Fig. 2.67).

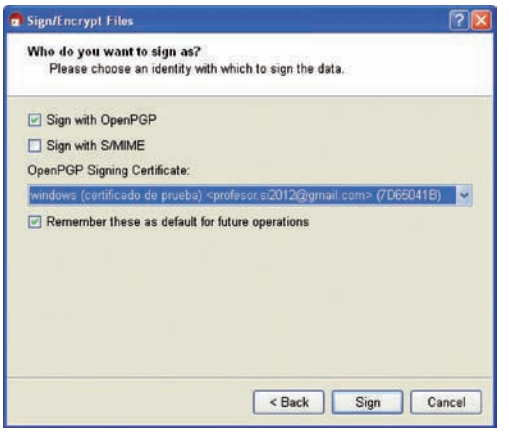


Fig. 2.67. *Elegimos el certificado.*

15. Finalmente, nos solicita la contraseña para poder trabajar con la clave privada (Fig. 2.68). En la ventana aparece que estamos firmando con la clave DSA (ya sabemos que el cifrado se hace con la clave Elgamal).

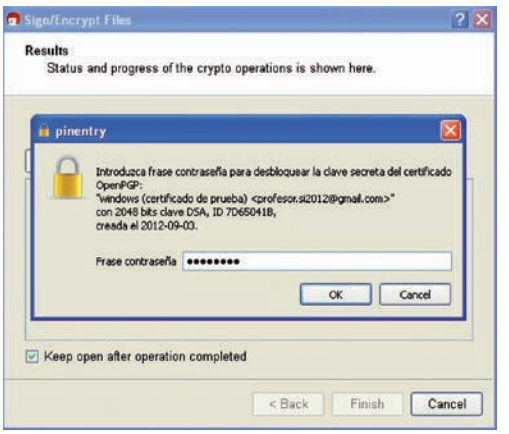


Fig. 2.68. *Introducimos la contraseña.*

16. Si todo va bien, la firma se completa y el resultado es un fichero top secret.txt.asc (Fig. 2.69).

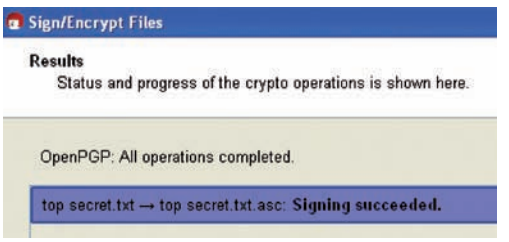


Fig. 2.69. *Firma completada.*

17. Ahora podemos llevar el fichero original junto con el fichero de firma hasta otra máquina y comprobar la firma. Previamente necesitamos un tercer fichero: la clave pública del certificado, para poder importarlo en la otra máquina. Para conseguirlo nos situamos sobre

(Continúa)

Caso práctico 5

(Continuación)

el certificado y en el menú del botón derecho elegimos *Export Certificates* (Fig. 2.70).

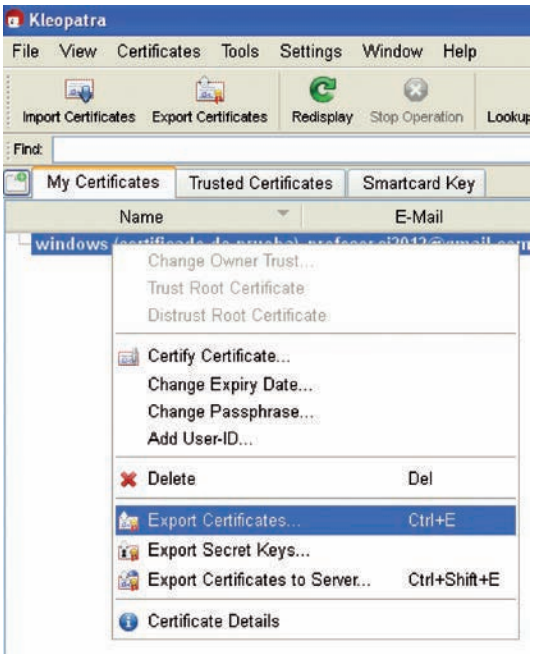


Fig. 2.70. *Exportamos el certificado.*

18. Lo exportamos al fichero windows.asc. Como es un fichero ASCII, lo podemos mirar con un editor de textos (Fig. 2.71). La cabecera PGP PUBLIC KEY indica que es una clave pública, como esperábamos.

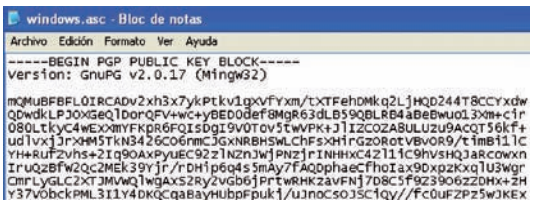


Fig. 2.71. *Contenido del certificado.*

19. Transferimos los tres ficheros a una máquina Linux (Fig. 2.72). En este ejemplo utilizamos la misma máquina del caso práctico 4. Podemos utilizar cualquier mecanismo: disco compartido, servidor FTP, pendrive USB, etc.

```
alumno@alumno-VirtualBox:~/cifrado$ ls -l
total 12
-rw-r--r-- 1 alumno alumno   10 sep  4 00:40 top secret.txt
-rw-r--r-- 1 alumno alumno  235 sep  4 00:40 top secret.txt.asc
-rw-r--r-- 1 alumno alumno 2357 sep  4 00:40 windows.asc
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.72. *Ficheros transferidos.*

20. El resto del procedimiento ya lo conocemos: primero hay que importar la clave pública con el comando (Fig. 2.73):

```
alumno$ gpg --import windows.asc
```

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --import windows.asc
gpg: clave 7D65041B: clave pública "windows (certificado de prueba) <profesor.si
2012@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.73. *Importamos la clave pública.*

21. Ya podemos comprobar la firma con el comando (Fig. 2.74):

```
alumno$ gpg --verify top secret.txt.asc
```

```
alumno@alumno-VirtualBox:~/cifrado$ gpg --verify top\ secret.txt.asc
gpg: Firmado el mar 04 sep 2012 00:34:15 CEST usando clave DSA ID 7D65041B
gpg: Firma correcta de «windows (certificado de prueba) <profesor.si2012@gmail.c
om>»
gpg: AVISO: ¡Esta clave no está certificada por una firma de confianza!
gpg:          No hay indicios de que la firma pertenezca al propietario.
Huellas dactilares de la clave primaria: 06B7 19BB B347 1C0F 2D57  5320 AD83 A86
2 7D65 041B
alumno@alumno-VirtualBox:~/cifrado$
```

Fig. 2.74. *Comprobamos la firma.*

22. Podemos comprobar también que, alterando un solo carácter del fichero de texto o de su firma, la verificación ya no es posible.

El mecanismo de firma también se utiliza en las comunicaciones de datos para garantizar al servidor que somos un cliente de confianza, y así podemos evitar introducir usuario y contraseña **(autenticación sin contraseña).** Previamente, el servidor debe tener almacenada la clave pública del cliente (que habrá llegado hasta allí de manera segura). Cuando el cliente empieza una sesión y solicita autenticación sin contraseña, el servidor genera en ese momento un documento especial, llamado **desafío,** compuesto de cifras y letras elegidas aleatoriamente. Busca en sus ficheros la clave pública del cliente, cifra con ella ese desafío y se lo envía al cliente.

El cliente lo recibe, lo intenta descifrar con su clave privada y el resultado lo devuelve al servidor. Entonces el servidor compara la secuencia de caracteres recibida con el desafío que generó; si son iguales, efectivamente el cliente es de confianza y puede conectar directamente. Todo este diálogo puede quedar a salvo de miradas ajenas si usamos una conexión cifrada mediante la clave pública del servidor.

5. PKI. DNIe

Hasta ahora hemos aprendido a enviar documentos a un destinatario de manera que solo él pueda aprovecharlos (cifrado), y garantizando que el documento es nuestro (firmado). Pero en todos los casos hemos necesitado una comprobación extra sobre la clave pública: comparar la huella de esa clave importada con la huella de la clave original, para estar seguros de que vamos a comunicarnos con la persona correcta.

En nuestros casos prácticos ha sido sencillo porque estamos trabajando en la misma máquina o, como mucho, en la máquina del compañero. Pero la mayoría de las comunicaciones seguras ocurren entre máquinas muy alejadas entre sí que seguramente pertenecen a otras empresas. Por ejemplo, las oficinas virtuales de los bancos o el correo web (Gmail, Hotmail, etc.). No podemos entrar en sus máquinas para ver las huellas ni negociar con cada uno otro canal seguro donde poder consultarlas.

La solución a este problema es la implantación de una **PKI** (Public Key Infrastructure, infraestructura de clave pública). Ahora, en la comunicación segura entre cliente y servidor aparecen nuevos interlocutores:

- La Autoridad de Certificación (**CA** [Certificate Authority]), cuya misión es emitir certificados. Hasta ahora los generábamos nosotros mismos con una herramienta en el ordenador.
- La Autoridad de Registro (**RA** [Registration Authority]), que es la responsable de asegurar que el solicitante del certificado es quien dice ser. Por ejemplo, en los certificados necesarios para presentar la declaración de la renta, la solicitud se puede hacer por Internet, pero para recogerlos hay que presentarse con el DNI en una oficina de la Administración.
- La Autoridad de Validación (**VA** [Validation Authority]) es la responsable de comprobar la validez de los certificados digitales emitidos. En la práctica suele coincidir con la CA.
- Los **repositorios.** Son almacenes de certificados. Los principales son el repositorio de certificados activos y el repositorio de listas de revocación de certificados (certificados que, por cualquier motivo, fueron expresamente desactivados antes de caducar).

El funcionamiento es el siguiente:

- Durante el inicio de la sesión, el servidor envía su clave pública al cliente para que cifre el diálogo que van comenzar (autenticación usuario/contraseña, etc.); pero el cliente, antes de utilizarla, desconfía: necesita comprobar que el servidor es quien dice ser.
- El servidor lo ha supuesto y ha enviado, junto con su clave pública, la firma digital de esa clave. Esa firma digital ha sido realizada por una CA oficial utilizando la clave privada de esa CA.
- El cliente puede verificar la firma recibida utilizando la clave pública de la CA (en este punto puede necesitar conectar con la VA). Si la firma es correcta, la clave pública del servidor también lo es y podemos iniciar la sesión segura con toda confianza.

Por tanto, para que funcione la autenticación de una clave pública mediante PKI, se necesitan dos pasos previos:

- El servidor ha conseguido que una CA le firme su clave pública. Por ejemplo: VeriSign, FNMT, etc.
- El cliente dispone de la clave pública de esa CA dentro de su llavero de claves asimétricas.

En la Figura 2.75 hemos añadido estos dos pasos al ejemplo de la Figura 2.37 acerca del protocolo SSH. En algún momento el servidor SSH consigue que una CA le firme la clave pública, y en algún momento el cliente SSH instala la clave pública de esa CA. Desde ese instante ya pueden establecerse conversaciones seguras entre cliente y servidor SSH, porque el cliente puede autentificar la clave pública ofrecida por el servidor.

Web

Este vídeo sobre navegación segura en SSL ilustra el concepto de PKI:
http://goo.gl/aFO0L

Actividades

22. Investiga precios y requisitos para conseguir un certificado de una empresa de PKI.

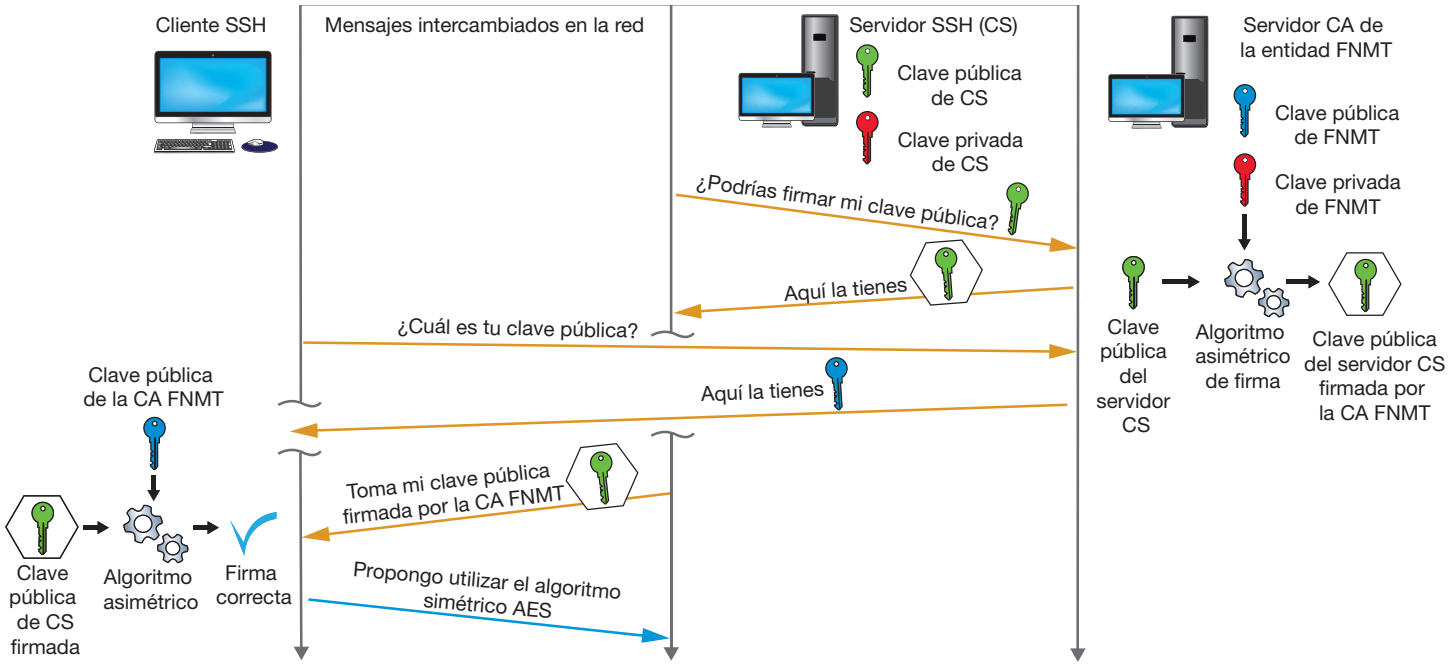


Fig. 2.75. *Funcionamiento de una PKI.*

Realmente, las CA no emiten un simple fichero con la firma, como hemos visto hasta ahora en los casos prácticos (ficheros .gpg o .asc); ni encontramos suelta la clave pública de una CA para importarla. Es importante la información complementaria: quién firma, para quién firma, qué usos tiene la clave (cifrado y firmado, solo firmado, etc.), en qué fecha se firmó, cuándo caduca esa firma, qué algoritmos se han utilizado, etc. Esta información se recoge en una estructura que constituye el **certificado digital,** según el estándar X.509. Por tanto, en el funcionamiento de una PKI los usuarios importan certificados de CA y los servidores envían sus claves públicas dentro de certificados.

Ahora bien, ¿cómo podemos estar seguros de que la clave pública de la CA es auténtica? Porque se ha instalado en nuestro ordenador de manera segura: bien porque forma parte de la instalación del sistema operativo, bien porque en algún momento la hemos importado voluntariamente. Se suelen llamar **certificados raíz** (root certificates).

Hay muchas empresas públicas y privadas que disponen de una PKI y se dedican a emitir certificados. Los usuarios que desean un certificado de esa empresa visitarán solo una vez su RA y su CA para obtenerlo, aunque después usarán muchas veces la VA y los repositorios. Solo volverán a la CA para renovar el certificado cuando esté próximo a caducar.

Además de las comunicaciones por Internet, las empresas también necesitan cifrar la información interna que circula por sus sistemas y sus redes. Para reducir el coste que supone contratar los certificados con una empresa externa, suelen crear una **PKI propia** que no emita certificados al público en general, sino solo a sus empleados y sus sistemas. La instalación consiste en configurar un servidor de la empresa con el software necesario para ejercer las funciones de CA y VA, y poner la clave pública de la CA en todos los equipos, uno a uno. La RA es asumida por el departamento de informática.

Como casi todo en seguridad informática, la PKI no es perfecta. Todavía tenemos dos **vulnerabilidades:**

- Un virus en nuestro ordenador puede alterar el depósito de claves, e importar sin nuestro consentimiento claves públicas de **CA fraudulentas.** Una conexión segura a servidores respaldados por esas CA no es fiable.
- Un **ataque a los servidores de una CA** podría robar su clave privada. Desde ese momento, el atacante puede firmar las claves públicas de servidores peligrosos y los clientes se conectarían a ellos confiando en que es una firma legal.

Actividades

23. En un certificado X.509 se pueden indicar otros usos de la clave del cliente, además de cifrar y firmar. ¿Cuáles son?

24. ¿Qué son los ficheros con extensión .pem, .cer, .p7b, .p12, etc.?

Caso práctico 6

Uso de certificados en Windows

Objetivo. Confirmar que la navegación es segura.

Material. Ordenador con Windows 7 con conexión a Internet.

- **Duración:** 15 minutos
- **Dificultad:** Fácil

1. Abrimos el navegador y nos conectamos a **gmail.com**. Aparecerá la página para introducir usuario y contraseña. Esta es una página segura y vamos a comprobarlo. Buscamos en el navegador el icono asociado. En la versión de Chrome de la Figura 2.76 es un candado verde junto a la URL (que ya vemos que utiliza el protocolo seguro HTTPS).



Fig. 2.76. *Navegación segura.*

2. Al pulsar sobre el candado aparecen las características de seguridad. En este ejemplo dice que la web **accounts.google.com** es quien dice ser, según la CA de la empresa Thawte. También dice que en la comunicación se está utilizando el algoritmo de cifrado RC4_128 con una clave de 128 bits. Esa clave se acordó en un canal asegurado mediante ECDHE_RSA. La autenticación utiliza el algoritmo SHA1.

3. Si pulsamos en *Datos del certificado* aparece la información general del mismo (Fig. 2.77): usos posibles de la clave pública que están firmando, identificador del solicitante y de la CA, y caducidad. En los usos podemos ver que sirve tanto para un servidor que quiere demostrar a un cliente que es quien dice ser como para un cliente que necesita demostrar al servidor que es quien dice ser. El intervalo de validez no es demasiado amplio (dos años), pero es más que suficiente para el uso que estamos haciendo (abrir el correo). En general, las operaciones en la web suelen durar muy poco tiempo.



Fig. 2.77. *Datos del certificado.*

4. Si vamos a la pestaña *Detalles* podemos consultar todos los campos del certificado según el estándar X.509 (Fig. 2.78): versión, algoritmos, emisor, sujeto, etc.



Fig. 2.78. *Detalles del certificado.*

5. Finalmente, en la pestaña *Ruta de certificación* tenemos quién respalda a quién (Fig. 2.79). Vemos que **accounts.google.com** está autentificado por Thawte, y que a su vez Thawte está autentificado por VeriSign.

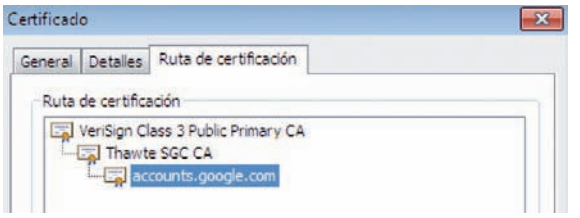


Fig. 2.79. *Ruta de certificación.*

(Continúa)

Caso práctico 6

(Continuación)

6. Si hacemos doble clic en *Thawte SGC CA* veremos su certificado (Fig. 2.80). En los datos generales tenemos el destinatario (Thawte) y el emisor, así como la caducidad y los usos posibles.

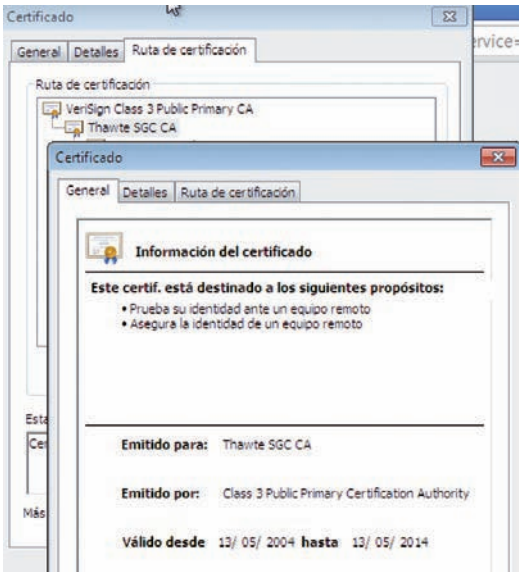


Fig. 2.80. *Certificado de Thawte.*

7. Haciendo doble clic sobre el tercer certificado veremos la información de un certificado raíz (Fig. 2.81). Es muy diferente a los anteriores: más usos, más duración de la validez y, sobre todo, está firmado por sí mismo (el destinatario y el emisor son el mismo). Por tanto, es un certificado que venía con el sistema operativo o lo hemos instalado nosotros mismos.



Fig. 2.81. *Certificado raíz.*

La mayor duración de la validez (diez años) refleja que esa CA firma claves para procesos mucho más duraderos que una simple sesión web. Por ejemplo, contratos entre compañías, entre una compañía y un cliente o incluso entre una compañía y un empleado.

El equivalente en el mundo real es el notario, donde acuden los interesados para asegurar que no existirá repudio por ninguno de ellos sobre el acuerdo alcanzado y formulado en un contrato o cualquier otro documento.

8. La lista de certificados que tenemos almacenados en la máquina está en *Propiedades de Internet* (esta herramienta también suele estar accesible al entrar en la configuración de los navegadores). Vamos a la pestaña *Contenido* y pulsamos el botón *Certificados*. Aparece una ventana con varias pestañas (Fig. 2.82).

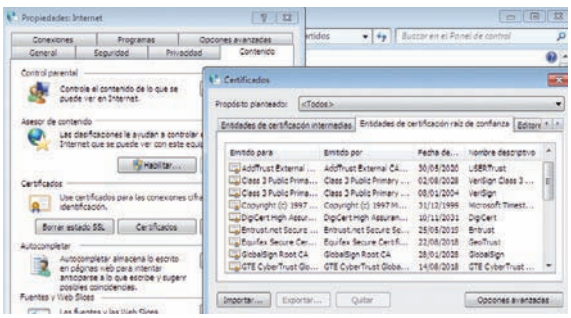


Fig. 2.82. *Lista de certificados.*

9. Pulsando en *Entidades de certificación raíz de confianza*, la tabla ofrece la identidad del solicitante del certificado, la identidad del emisor del certificado y la fecha de emisión. Ahora podemos encontrar la entidad del paso anterior. Un doble clic sobre ella nos muestra los datos que esperábamos (Fig. 2.83).

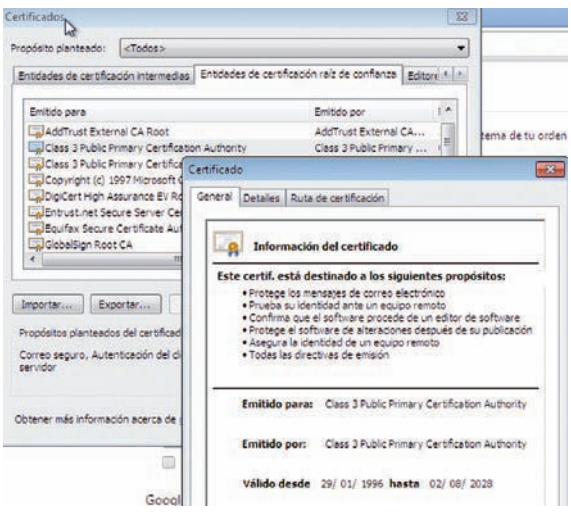


Fig. 2.83. *Datos del certificado raíz.*



Fig. 2.84. *Lector de tarjetas inteligentes.*

A modo de ejemplo de PKI vamos a estudiar el DNI electrónico **(DNIe),** recientemente implantado en nuestro país. Tiene el mismo tamaño que el DNI anterior y también aparecen escritos los datos de identificación de la persona. La diferencia es un pequeño chip que lo convierte en una tarjeta inteligente. El chip permite conocer:

- **Datos generales de la persona,** los mismos que están impresos en la tarjeta.
- **Datos biométricos de la persona,** como su huella dactilar digitalizada.
- **Claves de cifrado asimétrico.** El DNIe incluye claves distintas para firmar y para cifrar, por los motivos que ya conocemos: utilizar mucho una clave la expone a análisis criptográficos. Si al final alguien consigue nuestra clave de cifrado, por lo menos que no pueda firmar contratos en nuestro nombre.

Para conseguirlo hay que ir a una comisaría de Policía especializada en DNI. Si ya teníamos DNI anteriormente, solo llevaremos la fotografía. Tras identificarnos, aportar las huellas dactilares y pagar las tasas correspondientes, nos entregan dos cosas: el DNIe y un sobre ciego (su contenido no es visible al trasluz, sino que hay que abrirlo). Según el esquema PKI, la misma comisaría (en general, la Policía) hace de CA (emite el certificado) y también de RA (ha confirmado quiénes somos). El sobre ciego contiene la clave simétrica que permite utilizar la clave privada para descifrar o firmar.

Para usarlo necesitaremos un lector de tarjetas inteligentes como el de la Figura 2.84. La contraseña la podemos cambiar desde casa o en unos quioscos especiales instalados en la misma comisaría. También acudiremos a los quioscos para renovar los certificados, porque tienen una validez de 30 meses.

Caso práctico 7

Identificación mediante DNIe

Objetivo. Utilizar el DNIe para identificarnos.

Material. Ordenador con Windows, DNI electrónico con certificados en vigor y PIN válido, lector de tarjetas inteligentes, conexión a Internet.

■ **Duración:** ◷ 30 minutos ■ **Dificultad:** ☺ Media

1. Conectamos al ordenador el lector de tarjetas inteligentes. En este ejemplo utiliza una conexión USB. Automáticamente es reconocido por el sistema operativo (Fig. 2.85).

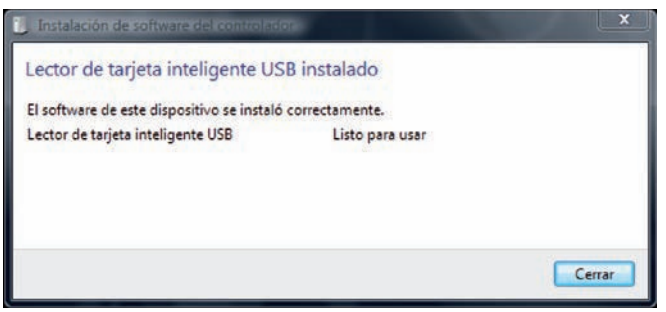


Fig. 2.85. *Lector disponible.*

2. Introducimos el DNIe y abrimos el navegador para comprobar que funciona. Por ejemplo, vamos a la web de la DGT (Dirección General de Tráfico). En esta web se puede utilizar el DNIe para consultar los puntos del carné de conducir. Pulsamos en esa opción, pero no podemos acceder a esa información (Fig. 2.86).



Fig. 2.86. *DNIe no reconocido.*

3. Efectivamente, no es suficiente con tener el lector y el DNIe. El lector sabe trabajar con tarjetas inteligentes, pero en este caso necesitamos un software más para realizar las operaciones criptográficas (cifrar, firmar, etcétera). Este software lo podemos descargar de la web oficial **www.dnielectronico.es**. Elegiremos la versión adecuada para nuestro sistema operativo: en nuestro caso, Windows (Fig. 2.87).



Fig. 2.87. *Descarga del software criptográfico.*

4. Descargamos y lanzamos la instalación. Una vez terminada, nos pide reiniciar la máquina (Fig. 2.88). Es necesario porque hemos introducido una nueva CA raíz, la CA del DNIe de la Policía, que debe estar instalada como CA de confianza dado que las claves de

(Continúa)

Caso práctico 7

(Continuación)

nuestra nueva tarjeta inteligente van firmadas por ella. Aunque los sistemas operativos traen varias CA como VeriSign, es poco probable que traigan esta CA particular. Y la Policía tiene su propia CA porque la información que firman es muy valiosa y no conviene que esté en manos de empresas privadas.

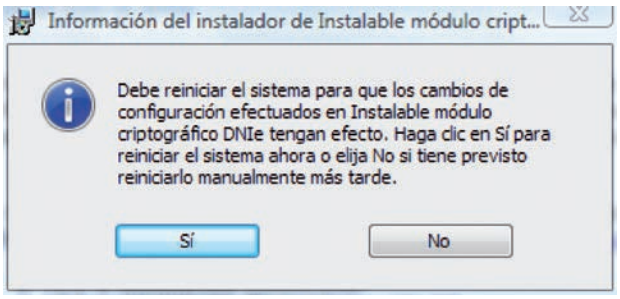


Fig. 2.88. *Fin de la instalación.*

5. En Windows Vista y Windows 7 la instalación de la nueva CA pasa desapercibida; en Windows XP sí aparece una ventana de confirmación (Fig. 2.89). Como era de esperar, el destinatario y el emisor coinciden.

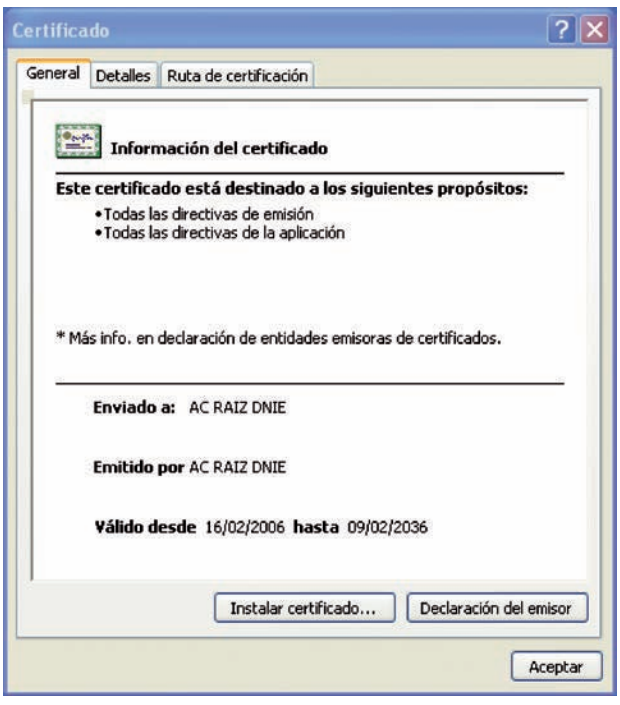


Fig. 2.89. *Instalación de la nueva CA.*

6. Tras arrancar, podemos consultar la lista de certificados en la herramienta de opciones de Internet para comprobar que se ha introducido con éxito (Fig. 2.90). Se llama AC RAIZ DNIE (certificado raíz de la Autoridad de Certificación del DNIe).

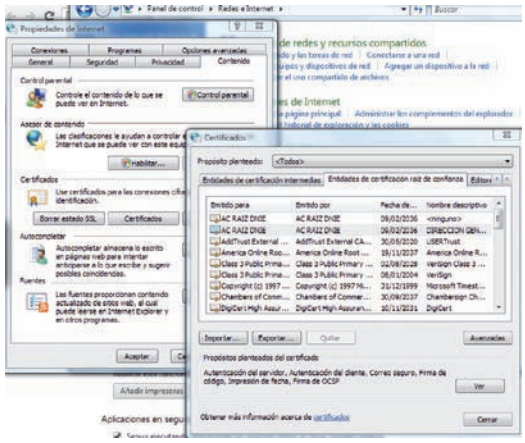


Fig. 2.90. *Nuevo certificado de CA.*

7. Ahora introducimos nuestro DNIe en el lector. Aparecerá una ventana informativa (Fig. 2.91) que nos recuerda que solo debemos introducir el DNIe en el lector cuando estemos a punto de realizar una operación de identificación o firma. Es decir, que no lo tengamos siempre conectado. Esto sirve para dificultar que un troyano realice múltiples intentos de obtener nuestras claves.



Fig. 2.91. *Advertencia de uso del DNIe.*

8. Cerramos esa ventana y, en la misma ventana de certificados, vamos a la pestaña *Personal*. Ahí deberían estar los dos certificados de nuestro DNIe: el de autenticación y el de firma (Fig. 2.92). Si extraemos el DNIe del lector, esos certificados desaparecen de la ventana.

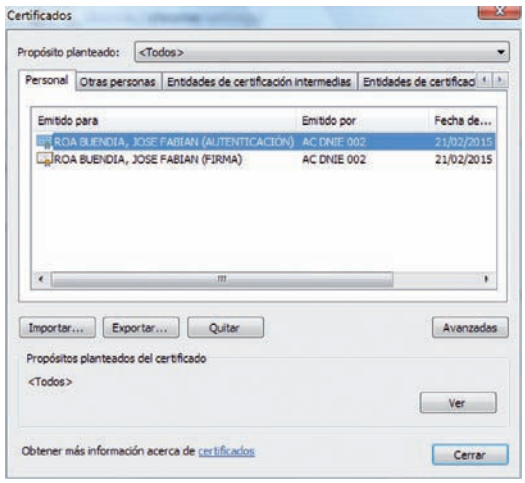


Fig. 2.92. *Encontramos nuestros certificados.*

(Continúa)

Caso práctico 7

(Continuación)

9. Ahora podemos volver a la página web de la DGT. Al entrar en la opción de consultar los puntos, la tarjeta empieza a trabajar y el navegador nos pregunta qué identificación queremos utilizar (Fig. 2.93). La lista que aparece son los certificados personales que hemos visto en el punto anterior (en este caso, el de autenticación, porque no estamos firmando). En el mensaje aparece la URL de la web que nos lo pide: en este caso, **aplcr.dgt.es:443**.

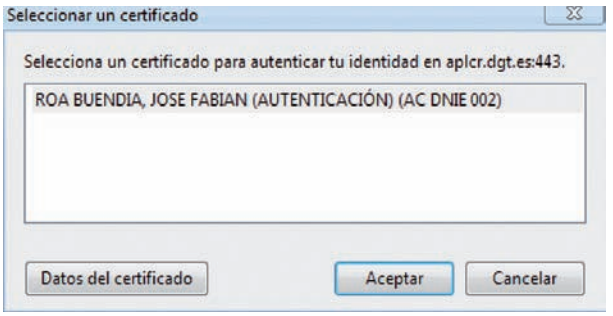


Fig. 2.93. *Elegimos el certificado de identificación.*

10. Lo seleccionamos y pulsamos en *Aceptar*. Ahora nos pedirá el PIN de la tarjeta (Fig. 2.94), que es la contraseña que viene en el sobre ciego que nos entregaron junto al DNIe. Esta contraseña autoriza el procesamiento de datos (en este caso, el desafío) con la clave privada del certificado de autenticación que hemos elegido. Por tanto, cualquiera que tenga nuestro DNIe necesitará también conocer esta contraseña para utilizarlo.



Fig. 2.94. *Contraseña de acceso a la clave privada.*

11. Si lo hemos hecho bien, aparecerá la información asociada a ese conductor (Fig. 2.95).

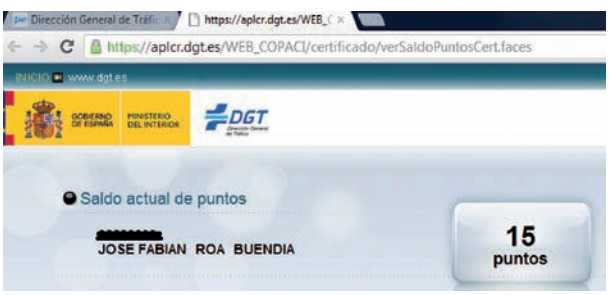


Fig. 2.95. *Información de la DGT.*

12. Lo normal es validar el funcionamiento del DNIe entrando en una página de validación de la propia web **www.dnielectronico.es**. Iremos a la página llamada *Comprobación de certificados* y de nuevo nos pedirá elegir identificación (Fig. 2.96). La ventana informa sobre qué URL lo está solicitando: **av-dnie.cert.fnmt.es:443**.

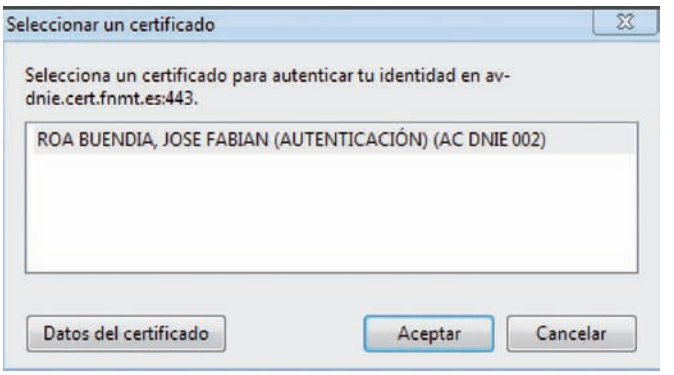


Fig. 2.96. *Elegimos el certificado de identificación.*

13. Si todo va bien, aparecerá una página con nuestros datos personales almacenados en el DNIe (Fig. 2.97).



Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD	(Valores Personales)
Nombre	JOSE FABIAN (AUTENTICACIÓN)
Apellidos	ROA BUENDIA
NIF	[redacted]
Número de Serie del Certificado de Autenticación	[redacted]
Autoridad Emisora	AC DNIE 002
Propietario	CN="ROA BUENDIA, JOSE FABIAN (AUTENTICACIÓN)", GIVENNAME=JOSE FABIAN, SURNAME=ROA, SERIALNUMBER=[redacted], C=ES
Comienzo de la Validez del Certificado	21 de agosto de 2012
Fin de la Validez del Certificado	21 de febrero de 2015
Estado del Certificado de Autenticación	Activo

Fig. 2.97. *Datos personales del DNIe.*

Caso práctico 8

Firma con DNIe

Objetivo. Utilizar el DNIe para firmar documentos.

Material. Ordenador con Windows, DNI electrónico con certificados en vigor y PIN válido, lector de tarjetas inteligentes, conexión a Internet.

■ **Duración:** 30 minutos ■ **Dificultad:** Media

1. Ahora vamos a probar la firma de nuestro DNIe. Hay una aplicación llamada eCoFirma disponible en la web del Ministerio de Industria. Está hecha en Java. Nos conectamos y la descargamos para instalarla.

2. La instalación consiste en un asistente de varios pasos (Fig. 2.98).



Fig. 2.98. *Asistente de instalación de eCoFirma.*

3. En el segundo paso nos pide crear una contraseña que proteja nuestra configuración de la herramienta (Fig. 2.99). Es una contraseña particular de esta herramienta, no tiene nada que ver con la contraseña de nuestros certificados del DNIe.

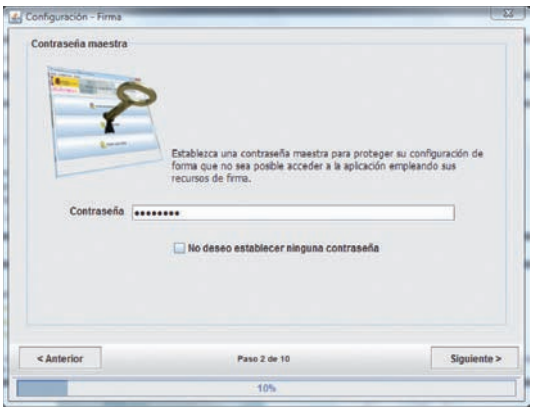


Fig. 2.99. *Contraseña de eCoFirma.*

4. Más adelante nos preguntará dónde están nuestros certificados (Fig. 2.100). Hasta ahora siempre hemos trabajado con los certificados de Windows, que también los utiliza Internet Explorer; pero en el ordenador podemos tener otros almacenes (Firefox, etc.). Elegimos el almacén de Windows porque ya lo conocemos, aunque la herramienta de instalación del DNIe debería haber actualizado también el almacén de Firefox.

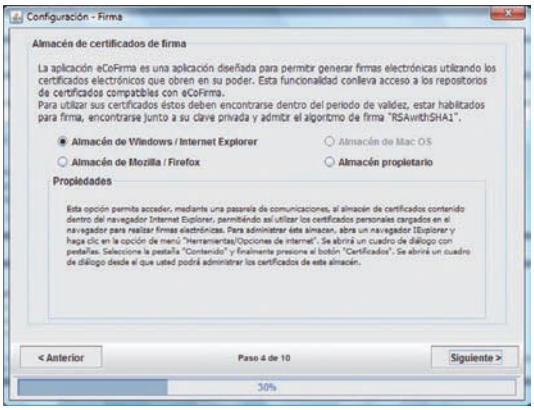


Fig. 2.100. *Almacenes de certificados.*

5. El siguiente paso es elegir el tipo de firma (Fig. 2.101). Dejamos el valor por defecto XAdES-BES. En esta ventana también podemos seleccionar que la herramienta genere un documento firmado por cada documento original, o que haga un único documento firmado con todos los documentos originales.

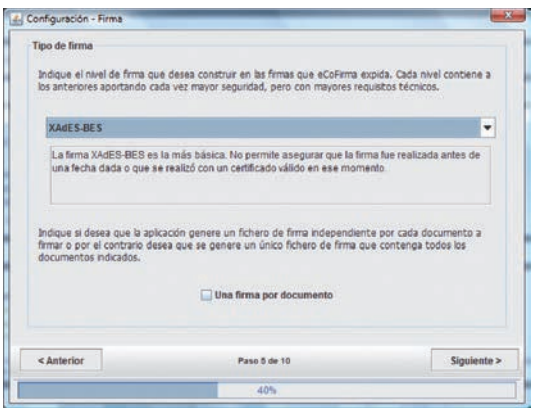


Fig. 2.101. *Tipo de firma.*

6. El siguiente paso nos permite cambiar los servidores OCSP (Online Certificate Status Protocol). Los certificados de nuestro DNIe están firmados con la clave privada de una CA de confianza; pero puede que estén revocados. Por ejemplo, si nos quitan el DNIe y tienen nuestra contraseña de uso, debemos denunciarlo inmediatamente y la Policía procederá a invalidar ese certificado en su servidor OCSP. Esto anula cualquier intento de firma con los certificados de ese DNIe robado. Así introducimos un nivel más de seguridad: se necesita la tarjeta, el PIN y, además, en directo se comprueba que los certificados de esa tarjeta son válidos.

(Continúa)

Caso práctico 8

(Continuación)

En nuestro caso, pasamos a la siguiente ventana sin cambiar nada (Fig. 2.102).

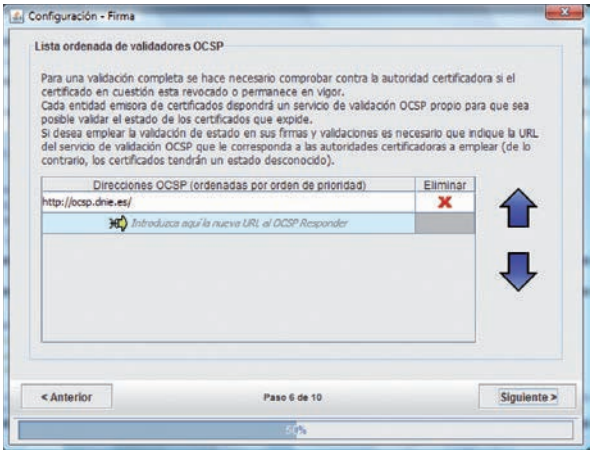


Fig. 2.102. *Lista de servidores OCSP.*

7. Más adelante nos pide confirmación para cambiar la asociación de la extensión de fichero .xsig, de manera que haciendo doble clic sobre ellos directamente abre el programa eCoFirma. Aceptamos.

8. El siguiente paso es comprobar la lista de CA de confianza (Fig. 2.103). Comprobamos que ahí está nuestra CA DNIE y seguimos.



Fig. 2.103. *Lista de CA de confianza.*

9. Finalmente efectúa un test de la configuración que hemos elegido. Como siempre, nos pide el PIN de la tarjeta para operar con ella. Si todo va bien, la herramienta nos lo confirma.

10. Terminada la configuración, aparece la ventana principal de la herramienta eCoFirma (Fig. 2.104). Hay tres opciones: firmar, validar firma y añadir una firma (un documento original puede ser firmado varias veces por distintos responsables).

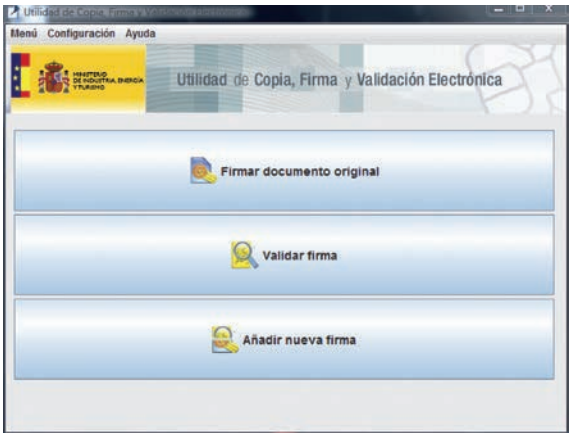


Fig. 2.104. *Herramienta eCoFirma.*

11. Entramos en la primera opción y aparece un asistente. El primer paso es elegir el documento que queremos firmar. En este ejemplo, es un PDF de nuestro disco (Fig. 2.105).

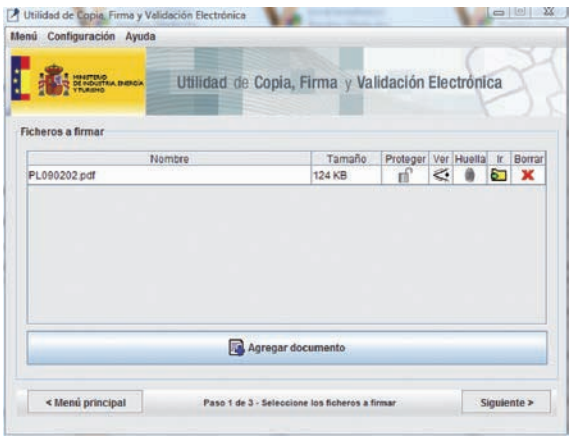


Fig. 2.105. *Elegimos el fichero que queremos firmar.*

12. Pulsamos *Siguiente* y la herramienta busca nuestros certificados. Como siempre, nos pedirá el PIN (Fig. 2.106).



Fig. 2.106. *PIN del DNIe.*

(Continúa)

Caso práctico 8

(Continuación)

13. En la ventana (Fig. 2.107) aparecerá directamente nuestro certificado de firma (en las operaciones anteriores aparecía el certificado de autenticación).

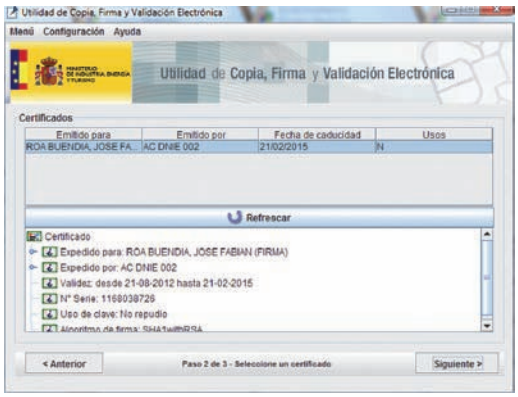


Fig. 2.107. *Nuestro certificado de firma.*

14. El paso siguiente es la firma. En este proceso aparecerá una ventana para confirmar que vamos a firmar (Fig. 2.108). Esta ventana no pertenece a eCoFirma, sino al software del DNIe.



Fig. 2.108. *Confirmación de firma.*

15. Si todo va bien, ya tendremos el fichero firmado. En la pestaña *Información* aparecerá nuestro certificado de firma (Fig. 2.109).

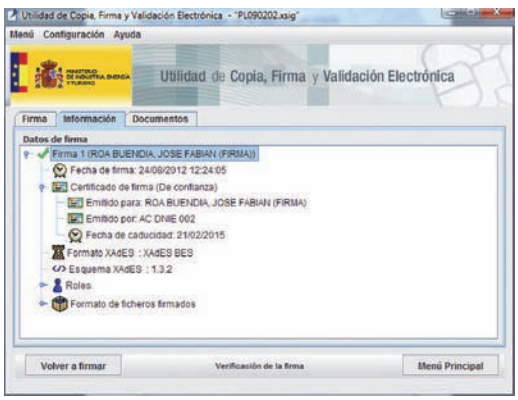


Fig. 2.109. *Datos de la firma.*

16. En el disco se habrá creado un fichero con el mismo nombre que el PDF pero con extensión .xsig. Ahora podemos copiar el fichero en un USB, ir a otra máquina (en este ejemplo un XP), copiar el fichero e instalar allí el software eCoFirma para proceder a validar la firma. Por supuesto, en esta nueva máquina no necesitamos el DNIe porque solo vamos a validar, no vamos a cifrar ni firmar.

Entramos en la opción *Validar firma* y elegimos el fichero .xsig copiado.

17. Si todo va bien, la firma debe ser correcta (Fig. 2.110).

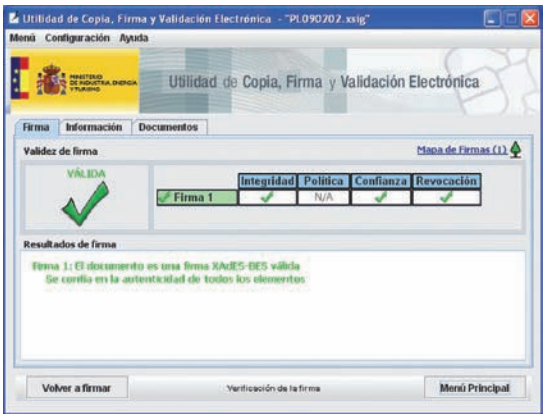


Fig. 2.110. *Firma correcta.*

18. En la pestaña *Documentos* aparece la lista de documentos asociados a este documento de firma (podríamos haber firmado varios). En el último icono de la derecha podemos acceder a la descarga del documento original (Fig. 2.111). Pulsándolo recuperamos el PDF que estaba cifrado dentro del fichero .xsig.



Fig. 2.111. *Podemos descargar el fichero.*

19. Si abrimos el fichero .xsig con un editor de texto, comprobamos que es un XML que sigue el estándar de firma que elegimos con anterioridad (Fig. 2.112).

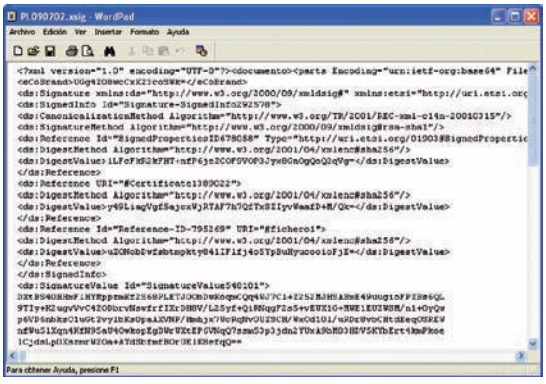


Fig. 2.112. *XML del fichero de firma.*

Síntesis

La información importante debe permanecer inaccesible para quien no esté debidamente autorizado. Por supuesto, protegeremos el medio físico donde está almacenada (disco duro, CD, USB) o por donde circula (redes de voz y datos, cableadas e inalámbricas); pero, por si acaso, el contenido estará cifrado para que no puedan aprovecharlo si cae en sus manos.

Las técnicas criptográficas permiten generar mensajes que ocultan el mensaje original. Cada técnica se caracteriza por:

- Un **algoritmo:** es el procedimiento paso a paso que convierte el mensaje original en un mensaje cifrado.
- Una **clave:** es un dato para el algoritmo gracias al cual se genera un mensaje cifrado tan complejo que es imposible deducir el mensaje original. Necesitaremos una clave para descifrarlo.

Si el algoritmo utiliza la misma clave para cifrar y descifrar, es un algoritmo simétrico (DES, 3DES, AES); si utiliza claves distintas, es asimétrico (RSA, DSA, Elgamal).

En los algoritmos simétricos la clave debe ser conocida por el emisor y por el receptor del mensaje cifrado. Por tanto, necesitamos un canal seguro para comunicársela.

Los algoritmos simétricos cifran así:

- El emisor utiliza el algoritmo simétrico y la clave compartida para cifrar el documento.
- El documento cifrado se transmite al receptor por cualquier medio.
- El receptor utiliza el algoritmo simétrico y la clave compartida para descifrarlo y así recuperar el documento original.

Los algoritmos asimétricos trabajan con dos claves:

- Una **clave pública,** que se puede difundir por cualquier medio sin ningún problema.
- Una **clave privada,** que solo debe conocer el dueño de la clave pública.

Los algoritmos asimétricos cifran así:

- El **emisor** utiliza el algoritmo asimétrico y la **clave pública del receptor para cifrar** el documento.
- El documento cifrado se transmite al receptor por cualquier medio.
- El **receptor** utiliza el algoritmo asimétrico y **su clave privada para descifrarlo** y así recuperar el documento original.

Los algoritmos asimétricos evitan el canal seguro de intercambio de claves, pero no son perfectos: son poco eficientes y necesitan proteger la clave privada (generalmente con una clave simétrica).

Las claves privadas suelen viajar dentro de tarjetas inteligentes. Estas tarjetas incorporan un chip capaz de ejecutar las operaciones de cifrado con esas claves.

Los algoritmos asimétricos, además de cifrar, permiten firmar un documento para garantizar el origen del mismo. La firma consiste en:

- El **emisor** utiliza el algoritmo asimétrico y **su clave privada** para cifrar un resumen del documento. El resumen se genera con una función hash.
- El documento firmado se transmite al receptor por cualquier medio.
- El **receptor** utiliza el algoritmo asimétrico y **la clave pública del emisor** para verificar la firma.

Generalmente se combinan las dos operaciones: firmamos un documento y ciframos el resultado para que nadie extraño pueda utilizarlo.

Las claves públicas de los individuos e instituciones pueden ser autentificadas por una CA (Certificate Authority), dentro de un esquema PKI (Private Key Infrastructure). Otros elementos son la RA (Autoridad de Registro) y la VA (Autoridad de Validación).

Test de repaso

1. Una agente del FBI necesita enviar un fichero top secret a su jefe, que está en Langley (Virginia):

a) Lo imprime y envía los folios por correo certificado.

b) Lo imprime y envía los folios por mensajero.

c) Lo cifra con IZArc utilizando la contraseña habitual y el resultado lo graba en un CD. El CD lo manda por correo ordinario.

2. El jefe lo necesita con urgencia. Como el agente tiene acceso a Internet, decide transferir el fichero:

a) Se conecta al servidor FTP de su departamento. Se identifica con su usuario y contraseña y completa la transferencia.

b) Se conecta al servidor HTTPS de su departamento. Se identifica con su usuario y contraseña y efectúa el upload.

c) Se conecta al servidor HTTP de su departamento. Se identifica con su usuario y contraseña y efectúa el upload.

3. Todos los servidores del departamento están caídos. El agente y el jefe acuerdan un mecanismo alternativo:

a) El agente envía el fichero a la cuenta de correo jefe@fbi.com.

b) El agente envía el fichero cifrado a la cuenta de correo jefe_fbi@hotmail.com.

c) El agente envía el fichero cifrado a la cuenta de correo jefe@fbi.com.

4. Si podemos elegir entre algoritmo simétrico y asimétrico:

a) Siempre simétrico, porque son más eficientes.

b) Siempre asimétrico, porque son más seguros.

c) Depende de la situación: si necesitamos rendimiento, simétrico; si necesitamos seguridad, asimétrico.

5. Tenemos que elegir entre un algoritmo simétrico con clave de 512 bits y un algoritmo asimétrico con clave de 32 bits:

a) El simétrico, porque la clave es larga, luego segura.

b) El asimétrico, porque son más modernos.

c) Da igual, porque la información que enviamos no es muy importante.

6. Hemos cifrado un fichero con un algoritmo simétrico:

a) Lo enviamos en un CD y en la carátula escribimos la clave, por si nuestro destinatario la ha olvidado.

b) Lo enviamos en un CD y en la carátula ponemos nuestro teléfono móvil, por si el destinatario ha olvidado la clave.

c) Lo enviamos en un CD sin ninguna indicación especial en la carátula. Confiamos en que el destinatario sabe la clave y, si no, sabrá cómo preguntárnosla.

7. En una operación de cifrado con un algoritmo asimétrico:

a) Necesitamos la clave pública y privada del receptor del mensaje.

b) Necesitamos la clave pública y privada del emisor del mensaje.

c) Necesitamos la clave pública del emisor y la clave privada del receptor del mensaje.

8. En una operación de firma con un algoritmo asimétrico:

a) Necesitamos la clave pública y privada del receptor del mensaje.

b) Necesitamos la clave pública y privada del emisor del mensaje.

c) Necesitamos la clave pública del emisor y la clave privada del receptor del mensaje.

9. Las tarjetas inteligentes:

a) Contienen la clave simétrica del dueño de la tarjeta, como si fuera un pendrive USB.

b) Contienen la clave pública del dueño de la tarjeta, porque la privada siempre está en su ordenador.

c) Contienen la clave privada del dueño de la tarjeta, porque la pública puede estar en cualquier otra parte.

10. La tarjeta electrónica del DNIe:

a) Contiene dos parejas de claves asimétricas asociadas al ciudadano: una para identificarse y otra para firmar.

b) Contiene la clave pública del ciudadano.

c) Contiene la clave privada del ciudadano.

11. La tarjeta electrónica del DNIe:

a) Se puede grabar en casa como un USB.

b) Solo puede emitirla la Policía, que hace de CA dentro de un esquema PKI.

c) Podemos pedirla en cualquier banco, porque tienen experiencia en tarjetas.

12. En una comunicación, ¿podemos utilizar algoritmos simétricos y asimétricos?

a) Sí. El simétrico para cifrar y el asimétrico para intercambiar la clave.

b) Sí. El asimétrico para cifrar y el simétrico para intercambiar las claves públicas y privadas.

c) Nunca. Son incompatibles.

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

Comprueba tu aprendizaje

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

1. Utiliza dos máquinas conectadas entre sí:

Una debe ser un sistema Windows. En ella instala un servidor FTP. En ese servidor crea un usuario james con contraseña bond007 y permisos para subir y bajar ficheros.

La otra debe ser un sistema Linux. Puedes utilizar el cliente nativo ftp desde la shell o algún cliente gráfico, como un navegador.

a) Comprueba que el esquema funciona: desde el sistema Linux, ese usuario puede trabajar con el servidor FTP de la máquina Windows.

b) Ahora, en la máquina Windows instala el software de captura de paquetes wireshark (lo veremos en detalle en la Unidad 7).

c) Inicia una captura de tráfico. Conéctate al servidor para realizar la transferencia de un fichero de texto.

d) Termina la captura y demuestra que eres capaz de localizar los paquetes donde va el usuario y la contraseña y algunos paquetes del contenido.

Como has visto, las transferencias FTP son fáciles de espiar.

Una primera solución: cifrar el contenido transmitido

e) En el sistema Linux utiliza la herramienta gpg para realizar un cifrado simétrico del mismo fichero de texto del punto anterior.

f) Activa la captura de tráfico en el servidor y realiza la transferencia del fichero cifrado.

g) Detén la captura y demuestra que, aunque todavía eres capaz de conocer el usuario y la contraseña, los paquetes que llevan el contenido del fichero son ilegibles.

Una segunda solución: instalar un servidor FTPS

h) En el sistema Windows instala un servidor FTPS. Habilita el mismo usuario james con contraseña bond007.

i) Activa la captura de tráfico en el servidor y realiza la transferencia del fichero de texto (normal, sin cifrar).

j) Detén la captura y demuestra que en los paquetes ya no puedes identificar ni el usuario ni el contenido del fichero.

Utilizar sistemas de identificación, como la firma electrónica y el certificado digital, entre otros

2. En las dos máquinas del ejercicio 1, realiza estas operaciones:

a) En la máquina Windows instala Gpg4win y crea un par de claves DSA-Elgamal identificadas como bill gates.

b) En la máquina Linux crea un usuario linus y utiliza la herramienta gpg para crearle un par de claves DSA-Elgamal identificadas como linus torvalds.

c) En la máquina Windows crea un fichero de texto y envíalo cifrado y firmado por bill gates para que lo reciba linus torvalds. Al recibirlo linus torvalds deberá comprobar la firma y recuperar el fichero.

d) En la máquina Linux crea un fichero de texto y envíalo cifrado y firmado por linus torvalds para que lo reciba bill gates. Al recibirlo bill gates deberá comprobar la firma y recuperar el fichero.

e) Repite las dos operaciones de cifrado y firmado, pero utilizando el correo electrónico como mecanismo de transferencia entre máquinas.

f) Repite las dos operaciones, pero utilizando una imagen en lugar del fichero de texto.

g) Repite las dos operaciones con la imagen y enviando mediante correo electrónico.

h) En la máquina Linux crea un nuevo usuario larry y créale un nuevo par de claves identificadas como larry ellison.

i) En la máquina Windows crea un nuevo fichero de texto y envíalo cifrado y firmado por bill gates para larry ellison. Al recibirlo, deberá comprobar la firma y recuperar el fichero.

j) En la máquina Linux elige un archivo de sonido y envíalo cifrado y firmado por larry ellison para que lo reciba bill gates. Al recibirlo, deberá comprobar la firma.

k) En la máquina Linux crea un archivo de texto y déjalo en /tmp cifrado y firmado por larry ellison para linus torvalds. Entra con el usuario linus para comprobar la firma y recuperar el fichero.

l) En todos los casos, documenta el procedimiento llevado a cabo.

Unidad 3

Seguridad pasiva: equipos



En esta unidad aprenderemos a:

- Definir las características de la ubicación física y condiciones ambientales de los equipos y servidores.
- Verificar el funcionamiento de los sistemas de alimentación ininterrumpida.
- Seleccionar los puntos de aplicación de los sistemas de alimentación ininterrumpida.
- Valorar las ventajas que supone la utilización de sistemas biométricos.

Y estudiaremos:

- La ubicación y la protección física de los equipos y servidores.
- Los sistemas de alimentación ininterrumpida.

Actividades

1. Investiga la reacción de la empresa Deloitte ante la pérdida de su CPD en el incendio del edificio Windsor de Madrid.
2. Discute en clase las ventajas e inconvenientes que tiene para la seguridad pasiva utilizar servidores de otras empresas (cloud computing).
3. Busca la clasificación de infraestructuras TIER 1 a 4 en las especificaciones del estándar ANSI\TIA-942.

1. Ubicación del CPD

Las empresas colocan los equipos de usuario cerca del usuario (un ordenador sobre su mesa, un portátil que se lleva a casa); pero los servidores están todos juntos en una misma sala. Esa sala tiene varios nombres: CPD (centro de proceso de datos), centro de cálculo, DataCenter, sala fría, «pecera», etc. Centralizando se consigue:

- **Ahorrar en costes de protección y mantenimiento.** No necesitan duplicar la vigilancia, la refrigeración, etc.
- **Optimizar las comunicaciones entre servidores.** Al estar unos cerca de otros no necesitan utilizar cables largos o demasiados elementos intermedios que reducen el rendimiento.
- **Aprovechar mejor los recursos humanos del departamento de informática.** No tienen que desplazarse a distintos edificios para realizar instalaciones, sustituir tarjetas, etc.

Tan importante como tomar medidas para proteger los equipos es tener en cuenta qué hacer cuando esas medidas fallan. Todas las empresas deben tener documentado un **plan de recuperación ante desastres,** donde se describa con el máximo detalle (en una crisis no hay tiempo para reflexionar) qué hacer ante una caída de cualquiera de los servicios que presta el CPD. Este plan debe ser **actualizado** cuando se efectúe un cambio en el CPD (nuevo servicio, nuevo equipo). El plan debe incluir:

- **Hardware.** Qué modelos de máquinas tenemos instalados (tanto servidores como equipamiento de red), qué modelos alternativos podemos utilizar y cómo se instalarán (conexiones, configuración).
- **Software.** Qué sistema operativo y aplicaciones están instalados, con el número de versión actualizado y todas las opciones de configuración (permisos, usuarios, etc.).
- **Datos.** Qué sistemas de almacenamiento utilizamos (discos locales, armario de discos), con qué configuración y cómo se hace el respaldo de datos (copias de seguridad).

Web

Este vídeo describe el funcionamiento de los CPD de Google:
http://goo.gl/TeGHY
Y este, el CPD de una universidad española:
http://goo.gl/TcUHQ

1.1. Protección

La informática es vital para la empresa: si los servidores se paran, la empresa se para. Sucede en todos los sectores: en una empresa de telefonía, en una compañía aérea, en unos grandes almacenes...

El CPD debe estar protegido al máximo:

- Elegiremos un edificio en una zona con **baja probabilidad de accidentes naturales** (terremotos, ciclones, inundaciones).
- También evitaremos la proximidad de ríos, playas, presas, aeropuertos, autopistas, bases militares, centrales nucleares, etc.
- Evitaremos ubicaciones donde los edificios vecinos al nuestro pertenezcan a empresas dedicadas a **actividades potencialmente peligrosas:** gases inflamables, explosivos, etc.
- Preferentemente **seleccionaremos las primeras plantas del edificio.**
  - La planta baja está expuesta a sabotajes desde el exterior (impacto de vehículos, asaltos, etc.).
  - Las plantas subterráneas serían las primeras afectadas por una inundación.
  - Las plantas superiores están expuestas a un accidente aéreo y, en caso de incendio iniciado en plantas inferiores, es seguro que nos afectará.
- Se recomienda que el edificio tenga **dos accesos y por calles diferentes.** Así siempre podremos entrar en caso de que una entrada quede inaccesible (obras, incidente, etc.).

¿Sabías que...?

El término CPD (centro de proceso de datos) es una evolución de la primera denominación: centro de cálculo (la primera utilidad de los ordenadores fue realizar cálculos matemáticos).

- Es recomendable **evitar señalizar la ubicación del CPD** para dificultar su localización a posibles atacantes. La lista de empleados que entran a esa sala es muy reducida y saben perfectamente dónde está.
- **Los pasillos que llevan hasta el CPD deben ser anchos** porque algunos equipos son bastante voluminosos. Incluso conviene dotarlo de un muelle de descarga.
- **El acceso a la sala debe estar muy controlado.** Los servidores solo interesan al personal del CPD.
- En las paredes de la sala se deberá **utilizar pintura plástica** porque facilita su limpieza y se evita la generación de polvo.
- En la sala se **utilizará falso suelo y falso techo** (Fig. 3.1) porque facilita la distribución del cableado (para electricidad y comunicaciones) y la ventilación.
- **La altura de la sala será elevada** tanto para permitir el despliegue de falso suelo y falso techo como para acumular muchos equipos en vertical (Fig. 3.1), porque el espacio de esta sala es muy valioso.
- En empresas de alta seguridad, la sala del CPD se recubre con un **cofre de hormigón** para protegerla de intrusiones desde el exterior.
- Instalaremos **equipos de detección de humos y sistemas automáticos de extinción de incendios,** como los elementos del techo de la Figura 3.1.
- El mobiliario de la sala debe utilizar **materiales ignífugos.**



Fig. 3.1. *Equipos en un CPD.*

1.2. Aislamiento

Las máquinas que situamos en el CPD utilizan circuitos electrónicos. Por tanto, hay que protegerlas ante:

- **Temperatura.** Los circuitos de los equipos, en especial los procesadores, trabajan a alta velocidad, por lo que generan mucho calor. Si además le sumamos la temperatura del aire, los equipos pueden tener problemas.
- **Humedad.** No solo el agua, también un alto porcentaje de humedad en el ambiente puede dañarnos. Para evitarlo utilizaremos deshumidificadores.
- **Interferencias electromagnéticas.** El CPD debe estar alejado de equipos que generen estas interferencias, como material industrial o generadores de electricidad, sean nuestros o de alguna empresa vecina.
- **Ruido.** Los ventiladores de las máquinas del CPD generan mucho ruido (son muchas máquinas trabajando en alto rendimiento), tanto que conviene introducir aislamiento acústico para no afectar a los trabajadores de las salas adyacentes.

Web

Este vídeo muestra el proceso de instalación de un sistema de detección y extinción automática de incendios:

http://goo.gl/Xt9hC

Y este vídeo es una demostración práctica:

http://goo.gl/h1Ft3

Vocabulario

Sala fría. Al CPD también se le suele llamar sala fría porque tiene una refrigeración especial para combatir el calor generado por todos los ordenadores que hay dentro.

Actividades

4. ¿Qué se utiliza para apagar un incendio en un CPD?

5. Busca las especificaciones de tu placa base y el disco duro, y localiza la temperatura y humedad recomendadas.

6. Las CPU modernas miden la temperatura y reaccionan ante un exceso de calor. ¿Qué hacen?

7. El elevado calor generado en un CPD puede aprovecharse. Investiga las soluciones adoptadas en algunas empresas.

Caso práctico 1

Control de temperatura en Windows

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

Objetivo. Vigilar la temperatura de la máquina.

Material. Ordenador con Windows.

1. El ordenador tiene varios sensores de temperatura: en la CPU, en la tarjeta gráfica, en el disco duro, etc. El principal es el de la CPU, porque es la parte crítica del sistema que funciona a más velocidad, lo cual genera mucho calor. Por eso la CPU siempre dispone de ventilación especial (disipador más ventilador).
2. Podemos conocer la temperatura instalando alguna utilidad software, como RealTemp. En la Figura 3.2 tenemos la ventana principal de la herramienta. Por desgracia, estas herramientas no funcionan bien en todos los equipos porque dependen mucho del API (Application Programming Interface) ofrecido por el fabricante de la CPU, la tarjeta gráfica, la placa base, etc. Es decir, el sensor está, pero no siempre resulta fácil que cualquier software lo consulte.

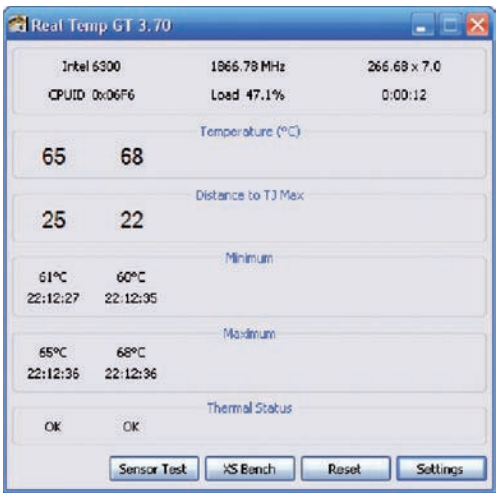


Fig. 3.2. *Utilidad RealTemp.*

La primera parte de la ventana muestra el tipo de CPU y la velocidad actual (en Mhz), así como la carga del sistema operativo (Load: una alta carga supone que la CPU trabaja más y genera más calor). Debajo tiene la temperatura de la CPU. En este caso ofrece dos valores porque es un procesador de doble núcleo. La siguiente fila es la diferencia con el máximo que admitimos (este valor lo podemos configurar), es decir: cuántos grados más se puede calentar antes de que sea importante. Finalmente, hay dos filas donde aparecen los valores mínimo y máximo que ha registrado la herramienta desde que está arrancada. Esto nos sirve para comprobar si la máquina está siempre trabajando al mismo ritmo o tiene altibajos.

3. Pulsando en *Settings* accedemos a la configuración (Fig. 3.3). Si nuestra tarjeta gráfica es ATI o Nvidia, podemos activar la casilla correspondiente para disponer de su temperatura. Para verla activaremos su casilla en la zona central bajo GPU (Graphics Processing Unit, el procesador gráfico).



Fig. 3.3. *Configuración de RealTemp.*

4. Si pulsamos *OK*, ahora la ventana principal nos ofrece la temperatura de la tarjeta gráfica (Fig. 3.4).



Fig. 3.4. *Temperatura de la tarjeta gráfica.*

5. Esta misma información está disponible en la barra de tareas (Fig. 3.5).



Fig. 3.5. *Temperaturas en la barra de tareas.*

6. Finalmente, esta herramienta incorpora un mecanismo de aviso de sobrecalentamiento. En la ventana de configuración activaremos la casilla *Alarm* (Fig. 3.6). A la derecha podemos asignar valores para la temperatura de CPU y GPU. Si se superan, oiremos una sirena. También podemos ejecutar un programa cualquiera (enviar un correo, registrar un evento, avisar a un sistema de monitorización como los que veremos en la Unidad 5): basta elegirlo pulsando en *Alarm EXE*. En el ejemplo, como la temperatura de la CPU estaba por encima de 60, poniendo un valor de 60 y pulsando Apply se activa la alarma.

(Continúa)

Caso práctico 1

(Continuación)

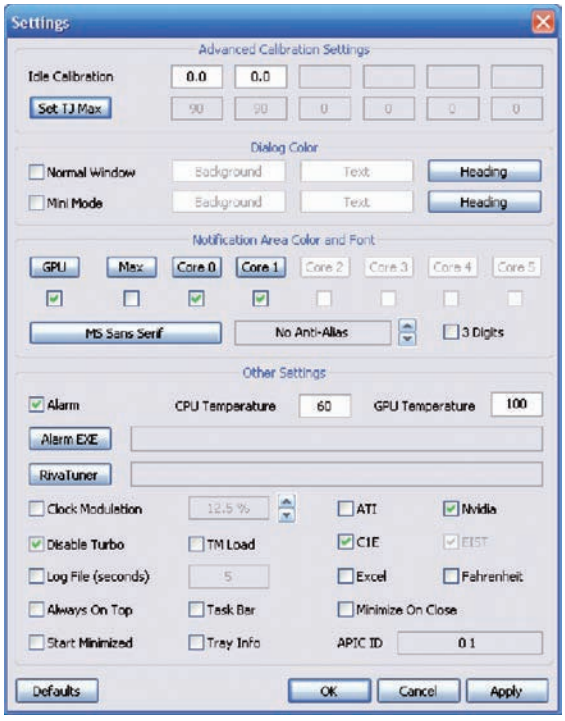


Fig. 3.6. *Alarma de sobrecalentamiento.*

7. Algunas utilidades, además de la temperatura, saben cómo hablar con la placa base para obtener la velocidad de los ventiladores. Por ejemplo, SpeedFan. En la Figura 3.7 vemos que aparece la velocidad en RPM (revoluciones por minuto) de los ventiladores Fan1 y Fan2 (mirando en el manual de la placa, uno corresponde a la CPU y el otro, al chipset). Hay un tercero, Fan3, que no está siendo utilizado. Si la velocidad de Fan1 o Fan2 baja repentinamente, debemos averiguar qué pasa, porque en poco tiempo subirá la temperatura.

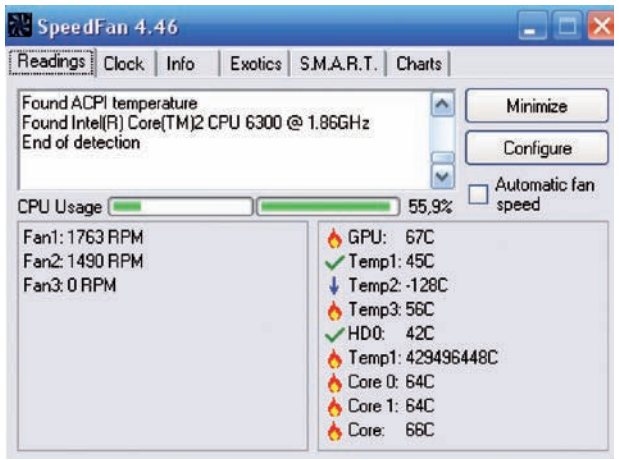


Fig. 3.7. *Ventana principal de SpeedFan.*

8. Un ventilador se puede parar por un fallo interno o por un uso excesivo; pero la causa más frecuente de problemas con los ventiladores es la acumulación de polvo y otras partículas. Por este motivo, conviene abrir la caja del ordenador para limpiarla con un aspirador. Nos centraremos especialmente en los ventiladores y disipadores. Dependiendo del ambiente de la sala, esta tarea se hará una vez al año (oficina) o una vez al mes (ordenador en contacto con el exterior).

1.3. Ventilación

Los CPD **no suelen tener ventanas.** La ventilación que conseguiríamos con ellas sería mínima para todo el calor que se genera, y el riesgo de intrusiones desde el exterior (o simplemente la lluvia) no es admisible en una instalación de tanta importancia.

La temperatura recomendable en la sala estaría alrededor de los **22 grados.** Las máquinas no lo necesitan, pero hay que pensar que ahí también van a trabajar personas. Para conseguirlo instalaremos **equipos de climatización.** Se suelen instalar por duplicado, para estar cubiertos ante el fallo de uno de los equipos.

En los CPD grandes se adopta la **configuración de pasillos calientes y pasillos fríos** (Fig. 3.8). Las filas de equipos se colocan en bloques formando pasillos, de manera que todos los ventiladores que extraen el calor de la máquina (fuente de alimentación, caja de la CPU) apunten hacia el mismo pasillo. En este pasillo se colocan los extractores de calor del equipo de climatización.

Ese mismo equipo introduce aire frío en los pasillos fríos, generalmente a través del falso suelo utilizando baldosas perforadas.

Web

Este vídeo muestra el proceso de construcción de un CPD, donde se cuida especialmente la ventilación:

http://goo.gl/bT6hj

Y este vídeo muestra un CPD ya construido:

http://goo.gl/GvmGL

Si es posible, todo el cableado de potencia irá en los pasillos fríos (es peligroso sobrecalentarlos) y el cableado de datos en los pasillos calientes.

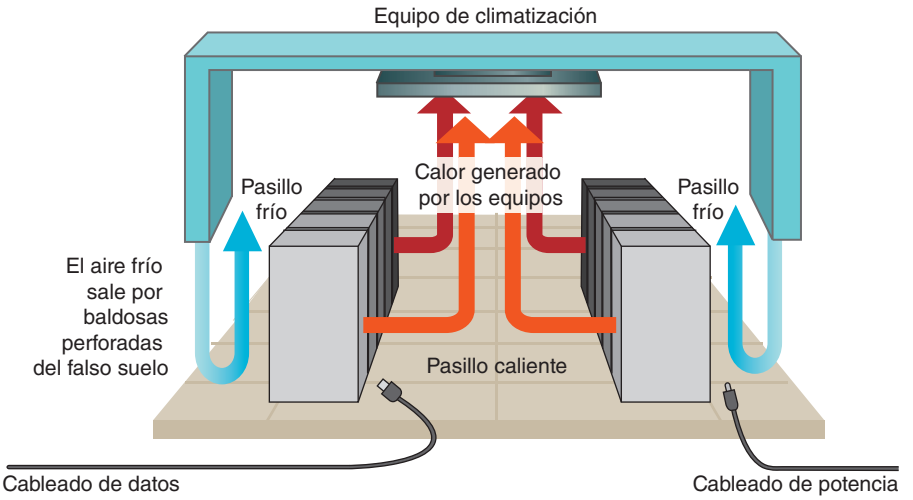


Fig. 3.8. *Pasillos calientes y fríos.*

1.4. Suministro eléctrico y comunicaciones

Nuestro CPD no está aislado: necesita ciertos servicios del exterior. Los principales son la alimentación eléctrica y las comunicaciones. En ambos casos **conviene contratar con dos empresas distintas,** de manera que un fallo en una compañía suministradora no nos impida seguir trabajando.

El **suministro eléctrico** del CPD debería estar **separado del que alimenta al resto de la empresa** para evitar que un problema en cualquier despacho de ese edificio afecte a los servidores, porque están siendo utilizados por empleados de otros edificios, incluso por clientes y proveedores.

Para los sistemas críticos, en los que la empresa no puede permitirse ninguna interrupción del servicio, deberemos instalar **generadores eléctricos** alimentados por combustible.

En cuanto a las **comunicaciones,** conviene que el **segundo suministrador utilice una tecnología diferente al primero.** Por ejemplo, si tenemos una conexión ADSL, el segundo no debería ser ADSL también, porque comparten el mismo cable hasta llegar a la central: un fallo en ese cable nos desconectaría de los dos suministradores. En cualquier caso, siempre conviene tener una tercera opción de conexión inalámbrica, por si el problema ocurre en la calle (obras en la acera, etc.).

Web

Algunos routers ADSL incorporan un puerto USB donde podemos conectar un módem 3G. Esto permite mantener la conexión a Internet aunque falle el ADSL:
http://goo.gl/fvYLl

1.5. Control de acceso

Las máquinas del CPD son vitales para la empresa y solo necesitan ser utilizadas por un reducido grupo de especialistas. El acceso a esta sala de máquinas debe estar especialmente controlado. No podemos consentir que alguien se lleve ninguna máquina o algún componente de ella (discos duros, cintas de backup) ni dejarle dentro intentando tener acceso desde las consolas de los servidores.

Las identificaciones habituales (contraseñas, tarjetas de acceso) se complementan con medidas más seguras, como la biometría, que veremos en la Unidad 5. En instalaciones importantes, el CPD puede tener su **propio equipo de vigilantes de seguridad.** En la sala se suele instalar también una red de **sensores de presencia y cámaras de vídeo** para detectar visitas inesperadas.

Actividades

8. Haz una lista con todos los controles que había para acceder al computador principal en la película *Misión: Imposible* (1996). A pesar de todo, los superaron. ¿Cómo lo hubieras evitado?

2. Centro de respaldo

A pesar de tanta protección, debemos pensar en la posibilidad de que ocurra una catástrofe en nuestro CPD y quede inservible (inundación, terremoto, sabotaje). La continuidad de la empresa no puede depender de un **punto único de fallo;** si disponemos de presupuesto suficiente, debemos **instalar un segundo CPD.**

Este segundo CPD, también llamado **centro de respaldo** (CR), **ofrece los mismos servicios** del centro principal (CP). Aunque, si la inversión en hardware resulta demasiado elevada, puede limitarse a los servicios principales, o a los mismos servicios pero con menos prestaciones. Por supuesto, **debe estar físicamente alejado del CP;** cuantos más kilómetros entre ambos, mejor (Fig. 3.9).

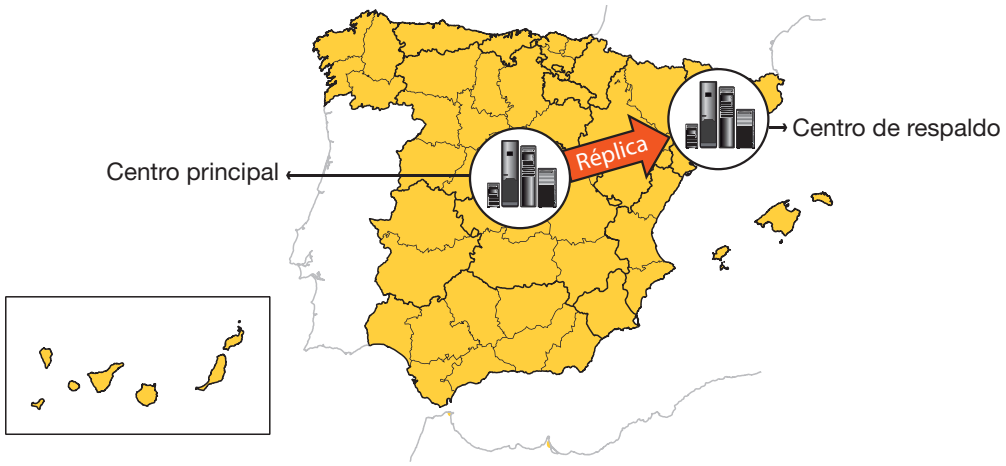


Fig. 3.9. *Centro de respaldo alejado del centro principal.*

En condiciones normales, el CR está parado **(stand-by)** esperando que, en cualquier momento, la empresa pueda necesitar detener el CP y activar el CR como nuevo CP. Los usuarios (empleados, clientes, proveedores) no deberían notar el cambio. Para ello, **la información del CP también está en el CR.** Esto incluye la configuración de los servicios; pero, sobre todo, los datos que han sido modificados en el último instante, antes de la conmutación de centros. Por tanto, no es suficiente con recuperar la última copia de seguridad del CP (sobre todo, porque la configuración puede ser distinta): debemos habilitar **mecanismos especiales de réplica,** en especial para las **bases de datos,** que son más complejas que los sistemas de ficheros. Pero esto necesita de **muy buenas comunicaciones entre el CP y el CR,** con lo que la distancia que los separa puede ser un problema.

Como hemos señalado con anterioridad en el plan de recuperación ante desastres, puede que las circunstancias que nos lleven a conmutar el CR al CP sean muy urgentes y no haya tiempo para descubrir cómo se hace: todo **el procedimiento de conmutación debe estar documentado** con el máximo detalle, así como la posterior recuperación del CP, asumiendo los cambios ocurridos mientras estaba inactivo. Incluso conviene **probarlo una vez al año** para confirmar que los pasos están bien descritos y el personal está capacitado para ejecutarlos bien.

Los equipos del centro principal y el centro de respaldo constituyen los **centros de producción** de la empresa: están en funcionamiento para dar servicio a los empleados, clientes y proveedores de la misma. Pero no son las únicas salas con servidores y equipamiento de red. Cualquier cambio en las aplicaciones corporativas o la nueva web de la empresa no puede instalarse directamente en las máquinas de producción, porque un fallo no detectado puede bloquear algunas áreas de la empresa. Primero se prueba en un entorno controlado, llamado **maqueta de preproducción,** donde el personal de la empresa aplica el cambio. En esta fase hay un contacto directo con el suministrador del software para resolver inmediatamente cualquier contingencia.

¿Sabías que...?

Las empresas de desarrollo de software tienen sus propias salas de ordenadores para montar varias maquetas de la aplicación que están desarrollando. Como mínimo hay dos: maqueta de desarrollo (para programadores) y maqueta de pruebas de sistema (prueba final antes de la entrega al cliente).

Actividades

9. La conmutación del CR al CP no siempre se debe a desastres en el CP. También puede ser una parada ordenada y planificada. ¿Se te ocurre algún ejemplo?

10. En algunas empresas, el CR no está parado, sino que funciona al 100 %, en paralelo con el CP. Cuando uno falla, el otro asume toda la carga. Discute las ventajas y los inconvenientes de esta solución.

3. SAI/UPS

La corriente eléctrica es vital en cualquier ordenador. Como no podemos confiar en que nunca va a fallar la empresa con la que hemos contratado el suministro eléctrico, tenemos que pensar en alternativas. En esta misma unidad hemos sugerido contratar un **segundo suministrador** o disponer de un **generador propio** (grupo electrógeno). Sin abandonar estas soluciones, en un CPD nunca debe faltar un SAI **(sistema de alimentación ininterrumpida),** en inglés UPS (Uninterruptible Power Supply).

Un SAI es un conjunto de **baterías** que alimentan una instalación eléctrica (en nuestro caso, equipos informáticos). La Figura 3.10 corresponde a la vista trasera de un SAI. Lo enchufamos a la corriente eléctrica por la toma de la izquierda y ofrece cuatro enchufes en la derecha.



Fig. 3.10. *Vista trasera de un SAI con todas sus conexiones.*

En caso de corte de la corriente, los equipos conectados al SAI siguen funcionando porque consigue electricidad de las baterías. **La capacidad de estas baterías es reducida** depende del SAI elegido y del consumo de los equipos, aunque el mínimo garantizado suele ser diez minutos. Este es el factor más importante a la hora de adquirir un SAI: cuántos vatios consumen los equipos que debe proteger y cuánto tiempo necesitamos que los proteja.

Al igual que ocurría con los equipos de climatización, si el presupuesto lo permite, conviene aplicar redundancia e instalar un **doble juego de equipos SAI,** para estar cubiertos en caso de que uno fallara. Esto es posible porque la mayoría de los servidores vienen con doble fuente de alimentación y conectaríamos una fuente a cada grupo de SAI.

Cuando ocurre un corte de luz, el SAI procede de esta manera:

- Espera unos minutos por si el corte ha sido puntual y el suministro se recupera inmediatamente por sí solo.
- Si no es así, ejecuta una **parada ordenada** de los equipos conectados al SAI. Siempre es mejor solicitar una parada al sistema operativo y las aplicaciones que ejecuta que perder la corriente y confiar en que no se genere ninguna inconsistencia.

¿Sabías que...?

Para elegir el SAI debes conocer el consumo eléctrico de tus equipos; si no tienes su ficha técnica, puedes utilizar un medidor de consumo como este:



Fig. 3.11. *Medidor de consumo.*

Actividades

11. Busca características y precios de algunos SAI para uso doméstico y empresarial.

12. Si tienes acceso a un SAI, conéctale dos máquinas y configúralo para que, cuando se corte la luz, lance una parada ordenada de las dos. Compruébalo.

Conectar los equipos al SAI tiene otras ventajas:

- Suelen llevar un **estabilizador de corriente** que quita los picos, que también pueden ser muy dañinos.
- En algunos SAI también se incluye una entrada y salida de **cable telefónico** (conectores a la izquierda del ventilador en la Figura 3.10), que sirve para proteger nuestra conexión, porque las comunicaciones por línea telefónica también utilizan corriente eléctrica, luego también estamos expuestos a picos de tensión.

3.1. Tipos

Tradicionalmente, se han considerado dos tipos de equipos SAI:

- **SAI en estado de espera** (stand-by). Los equipos informáticos toman corriente del suministro principal, mientras el SAI se limita a vigilar que ese suministro fluya (Fig. 3.12). Cuando ocurre un corte, el SAI activa inmediatamente sus baterías para que los equipos no se vean afectados (el tiempo de respuesta suele ser suficiente). A partir de ese momento, el SAI aplica los tiempos de espera señalados en el punto anterior. Cuando vuelve la corriente, desactiva la generación de corriente propia y empieza a cargar las baterías.
- **SAI en línea** (on-line). Los equipos siempre están tomando corriente de las baterías del SAI. Cuando ocurre un corte, el SAI se limita a aplicar los tiempos de espera. Cuando vuelve la corriente, empieza a cargar las baterías.

La ventaja del SAI en línea es que no dependemos del tiempo de respuesta para activar las baterías; en cambio, la ventaja del SAI en espera es que podemos sustituir las baterías sin detener el suministro a los equipos conectados.

Ten cuidado

Las impresoras láser no deben formar parte de los equipos protegidos en un SAI porque utilizan resistencias de alto consumo para calentar el rodillo del tóner. Este elevado consumo instantáneo genera ruido a los otros equipos protegidos, que esperaban que el SAI les librara de estos problemas.

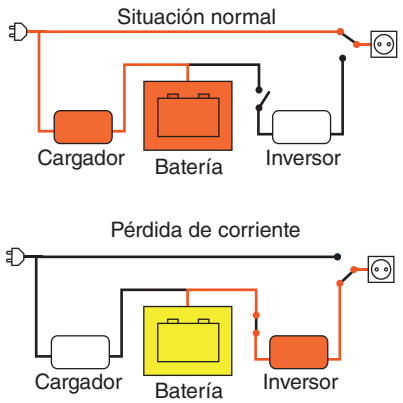


Fig. 3.12. *Esquema de un SAI en stand-by.*

3.2. Monitorización

Cuando tenemos un SAI confiamos en que está bien y que responderá cuando sea necesaria su intervención. Pero conviene revisar regularmente el estado del SAI. Estos equipos suelen incorporar unos **indicadores luminosos en el frontal** (Fig. 3.13): si está cargando o descargando las baterías, porcentaje de batería restante, etc.

Sin embargo, es una información puntual y solo disponible si se está delante del equipo. Para mejorar su gestión, los SAI suelen incorporar un **puerto de conexión con un ordenador.** En la Figura 3.10 vemos dos: un puerto serie y un USB. En ese ordenador instalaremos el software adecuado para comunicarse con el SAI y conocer no solo el estado actual, sino todas las veces que ha actuado en el pasado reciente. Por supuesto, ese ordenador debe estar protegido, sea por este SAI o por cualquier otro.

En la Figura 3.14 vemos una ventana del log de un SAI. Muestra una lista de los eventos que ha registrado:

- La primera columna señala el **tipo de evento.** Puede ser informativo o una alerta.
- Las dos siguientes indican la **fecha y hora** en que ocurrió el evento. Es importante para asociarlo a otros sucesos ocurridos: caída de alguna máquina, corte de líneas de comunicaciones, etc.
- La cuarta es la **descripción del evento.** Hay algunos sencillos, como Agent Start, que indican que ha arrancado el agente (el software que corre en el ordenador). Vemos que minutos antes ha ocurrido un USB Communication with device lost, lo que significa que el ordenador se ha reiniciado.

Los más graves son los eventos AC power failure, que es un corte de luz. En la imagen se aprecia que después ocurre un AC power restored, que indica que se ha recuperado el suministro. Observar el tiempo transcurrido entre ambos eventos nos servirá para ajustar la espera del SAI antes de lanzar la parada de equipos (y para reclamar a la compañía eléctrica, por supuesto).



Fig. 3.13. *LED en el frontal de un SAI.*

Web

Los SAI manejan baterías sometidas a fuertes cargas eléctricas y pueden explotar:
http://goo.gl/AacRZ

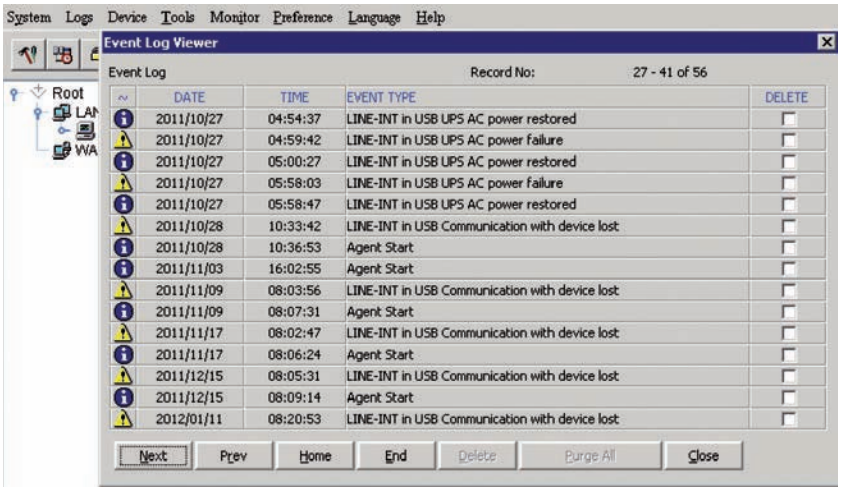


Fig. 3.14. *Log de un SAI.*

¿Sabías que...?

Para conocer el estado del SAI, además de revisar el log y programar los trigger, podemos incluirlo como un equipo más dentro de los sistemas de inventario que veremos en la Unidad 5.

3.3. Triggers

El software del SAI, además de la monitorización, incluye la configuración de los comandos para **responder ante un corte de corriente.** En general, la respuesta consistirá en realizar la parada ordenada de los equipos protegidos. En la Figura 3.15 vemos un ejemplo de la interfaz asociada. Las opciones principales son:

- **Cuándo hacerlo:** en un instante concreto (cuando se alcance Battery Backup Time) o cuando detecte que la carga de la batería está baja.
- **Qué hacer** con el sistema: suspenderlo o apagarlo.
- **Qué comando ejecutar antes de empezar el apagado** (Run Command File Before Shutdown). En este apartado aprovecharemos para apagar las otras máquinas conectadas a este SAI.

Ten cuidado

Si queremos que el SAI pueda desconectar otras máquinas, incluso avisarnos mediante un correo electrónico, debemos acordarnos de enchufar al SAI también los equipos de red asociados (switch, router ADSL).

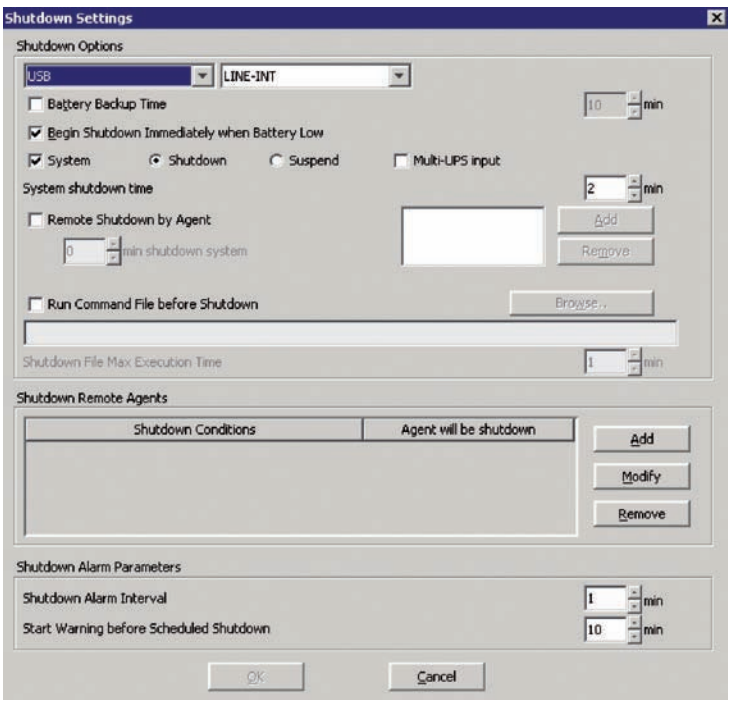


Fig. 3.15. *Configuración de acciones de respuesta en un SAI.*

Importante

El SAI casi nunca entra en acción; pero cuando lo hace, es extremadamente importante que todo funcione a la perfección, porque hay poco tiempo de maniobra. Por ejemplo, deben estar actualizadas las contraseñas de acceso a los servidores remotos para lanzar la parada, o el usuario y la contraseña del servidor de correo que nos tiene que hacer llegar el aviso.

Además de la parada, se puede configurar un **aviso por correo** a los administradores del sistema. En la ventana de la Figura 3.16 introduciremos los datos del servidor de correo donde tenemos cuenta (dirección y usuario/contraseña), las direcciones destino del aviso y la lista de eventos de los que queremos informarles.

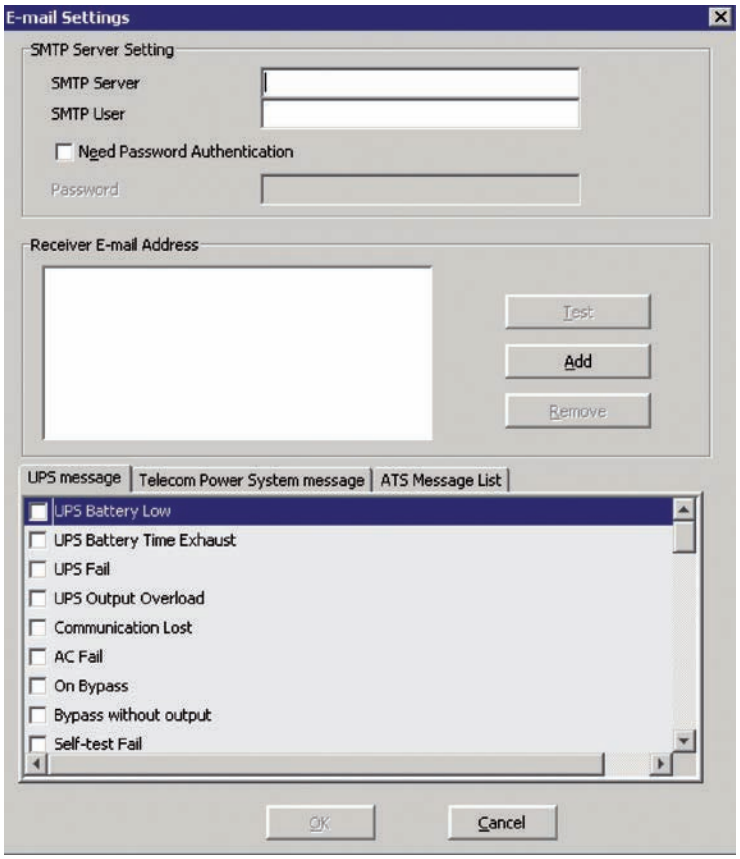


Fig. 3.16. *Aviso por correo.*

¿Sabías que...?

La capacidad de un SAI se suele medir en voltiamperios (VA) y está relacionada con el consumo eléctrico en watios (W). En general, las fuentes de alimentación utilizan un factor 0.6, de manera que un SAI de 1 000 VA solo puede alimentar equipos de hasta 600 W.

3.4. Mantenimiento

Las baterías se desgastan con el tiempo y ofrecen cada vez menos rendimiento. El software del SAI nos ayuda en este aspecto:

- Permite lanzar determinados test para comprobar la degradación actual de las baterías. Si no es suficiente para garantizar la parada ordenada de los equipos protegidos, debemos cambiarlas (Fig. 3.17). Para cambiar las baterías acudiremos al personal especializado, porque las baterías utilizan componentes químicos muy peligrosos.
- Incluye operaciones automáticas de descarga controlada, que alargan la vida de las baterías.

Como hemos visto antes, la operación de cambiar las baterías será relativamente sencilla en un SAI de tipo stand-by porque mientras tanto los equipos seguirán alimentados; pero en un SAI on-line perderemos la alimentación, por lo que es necesario detener los equipos. Este aspecto puede ser crítico en una empresa que no pueda permitirse ninguna parada.

Los SAI empresariales suelen adoptar una **configuración modular:** no utilizan pocas baterías grandes, sino muchas baterías pequeñas. Con este diseño podemos reemplazar fácilmente una batería sin afectar demasiado a la carga total ofrecida por el equipo, y a la vez conseguimos **escalabilidad:** el cliente compra un bastidor con capacidad de alojar muchas baterías, y lo va rellenando según aumenta el número de equipos protegidos.



Fig. 3.17. *Batería de repuesto.*

Síntesis

Los equipos informáticos más importantes para la empresa se sitúan en una sala especial llamada CPD (centro de proceso de datos). Se busca centralizarlos porque:

- Es más fácil protegerlos.
- Es más fácil controlar el acceso.
- Hay mejor rendimiento de sus interconexiones.
- Resulta más fácil administrarlos.

La empresa debe tener por escrito un plan de recuperación ante cualquier problema que pueda ocurrir en el CPD y afecte a uno o varios servicios.

La ubicación de esta sala se elige con especial cuidado:

- Alejada de posibles desastres naturales.
- Alejada de otras empresas potencialmente peligrosas.
- Preferentemente en las primeras plantas:
  - Ni planta baja ni sótanos, expuestas a ataques del exterior o inundaciones.
  - Las plantas superiores serán difíciles de salvar en un incendio.
- Deberá disponer de un acceso desde la calle, con pasillos anchos, por el tipo de máquinas que pueden llegar.
- Acceso muy controlado, superior a cualquier otra zona de trabajo.
- Dotada de detectores de humo y extintores automáticos.

El aislamiento de esta sala incluye:

- Temperatura.
- Humedad.
- Interferencias electromagnéticas.
- Ruido.

La ventilación será forzada, utilizando el esquema de pasillos fríos y calientes.

El suministro eléctrico y comunicaciones al CPD estará separado del utilizado por el resto de la empresa, para estar aislados de sus problemas y poder conectar fácilmente proveedores alternativos.

El control de acceso es superior a otras zonas de trabajo:

- Mecanismos de alta seguridad, como reconocimiento biométrico.
- Mecanismos de uso exclusivo del CPD, como vigilantes de seguridad.

El centro de respaldo es un CPD similar al centro principal pero alejado en muchos kilómetros. Está sincronizado al máximo para poder asumir sus funciones en cualquier momento.

Los equipos SAI (sistema de alimentación ininterrumpida) disponen de baterías para alimentar un conjunto de máquinas en caso de que la corriente eléctrica general sufra un corte. Hay dos tipos:

- SAI en espera (stand-by). Las baterías entran en acción cuando el SAI detecta el corte.
- SAI en línea (on-line). Las baterías siempre están alimentando a los equipos protegidos.

Un SAI posee cierta inteligencia y es capaz de conectar con un ordenador por una interfaz serie o USB. Mediante esta conexión podemos:

- Conocer el estado de las baterías del SAI.
- Conocer la actividad reciente del SAI (cortes ocurridos, etc.).
- Ejecutar determinadas acciones, cuando aparezca un corte, que permitan la parada ordenada de los sistemas si el suministro no se recupera en un tiempo prudencial.

Las baterías de un SAI se degradan con el tiempo, por lo que en algún momento necesitarán ser sustituidas. Esta tarea debe realizarla personal especializado, por la presencia de componentes químicos peligrosos.

Test de repaso

1. En una empresa tenemos varios servidores importantes y queremos protegerlos:

a) Los dejamos desperdigados por las salas de trabajadores para que pasen desapercibidos.

b) Los separamos en dos grupos y llevamos un grupo a una sala protegida del edificio de Madrid y el otro a una sala protegida del edificio de Barcelona.

c) Los reunimos en una única sala protegida de uno de los edificios de la compañía (Madrid o Barcelona).

2. Colocar todos los servidores en una sala:

a) Es malo porque generan más calor y se estropearán.

b) Es bueno porque controlamos mejor el calor.

c) No es bueno porque conviene mezclarlos con los ordenadores de los puestos de usuario, que se calientan menos.

3. El plan de recuperación de un desastre ocurrido en el CPD:

a) No es necesario elaborarlo: como no sabemos qué pasará, cuando ocurra ya pensaremos alguna solución.

b) Lo redactamos durante la instalación del CPD, porque tenemos más reciente la motivación de cada decisión.

c) Lo revisamos en cada cambio importante en los servicios ofrecidos por las máquinas del CPD.

4. La sala donde instalaremos las máquinas del CPD de la empresa:

a) Será una sala de nuestro edificio o el de otra empresa, lo que salga más barato.

b) Será una sala de nuestro edificio, con una protección superior a cualquier otra sala de trabajo.

c) Utilizaremos cualquier almacén del sótano, porque allí apenas hace calor.

5. Somos una empresa multinacional con sedes en varios países de varios continentes. En este caso instalaremos el CPD:

a) En un país de África, porque la mano de obra es más barata.

b) En un país de Asia, porque saben más de ordenadores.

c) En un país donde tengamos la mejor combinación de recursos materiales y recursos humanos.

6. Una empresa multinacional decide instalar dos CPD iguales, uno en Indonesia y otro en Brasil:

a) Buena idea: así siempre podemos tener uno funcionando solamente por la noche, cuando hace menos calor. Mientras, el otro estará parado, y viceversa.

b) Es mejor poner todas las máquinas en Indonesia.

c) Es mejor poner todas las máquinas en Brasil.

7. Si se declara un incendio en un CPD:

a) El personal de informática debe acudir con los extintores de mano.

b) Los vigilantes de seguridad acudirán con las mangueras de agua a presión.

c) Se dispara el sistema automático de extinción, que utiliza un compuesto especial que no afecta ni a personas ni a máquinas.

8. La ventilación de la sala del CPD:

a) Basta con abrir las ventanas para que el calor escape al exterior.

b) Utiliza un equipo de climatización especial, en cuya instalación se aprovechan los pasillos fríos y calientes que dejan las máquinas.

c) Debe priorizar el confort de los administradores de las máquinas.

9. El suministro eléctrico de las máquinas del CPD:

a) Puede ser el mismo que utilizamos para los empleados porque, si se va la luz, todos dejan de trabajar.

b) Utilizamos un suministrador diferente al del resto de la empresa.

c) Contratamos un segundo suministrador, además del que compartimos con el resto de la empresa.

10. El acceso a la sala del CPD:

a) Está permitido a cualquier empleado de la empresa, porque puede necesitar entrar a buscar un listado de la impresora.

b) Está permitido a cualquier persona, porque se suele enseñar a las visitas.

c) Está más restringido que cualquier otra sala de trabajo.

11. Un centro de respaldo:

a) Siempre tiene la misma configuración que el centro principal.

b) Siempre tiene menos capacidad que el centro principal.

c) Tiene la configuración adecuada al presupuesto de la empresa.

12. Un SAI:

a) Protege todas las máquinas de la empresa.

b) Protege solo los servidores.

c) Protege las máquinas del CPD.

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

Comprueba tu aprendizaje

Aplicar medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades

1. Una empresa está experimentando un fuerte crecimiento y necesita incluir nuevas máquinas en el CPD. Se están planteando cambiarlo a una nueva ubicación. Indica qué harías ante cada situación:

a) La instalación eléctrica está al máximo de su capacidad. No se puede conectar ningún nuevo servidor de alto consumo.

b) Hasta ahora, el CPD no tiene climatización específica porque la sala está en una zona del edificio orientada hacia el norte.

c) Carecen de grupo electrógeno porque, hasta la fecha, la compañía eléctrica nunca ha tenido una avería en su zona.

d) No hay sensores de humo porque, si en el CPD se declara un incendio, se vería en la cámara de seguridad, que está conectada al panel de control del servicio de vigilancia de la entrada de la empresa.

e) La cámara de seguridad del CPD carece de sistema de grabación automático. Solo se utiliza para vigilancias rutinarias.

f) La sala con los SAI y los cuadros eléctricos está separada de la sala de servidores, para que el personal de mantenimiento no tenga acceso a las consolas de los ordenadores.

g) Para el acceso a la sala de ordenadores solamente se necesita una llave, que está custodiada por el servicio de vigilancia.

h) La operativa de la empresa se desarrolla principalmente en horario de nueve a cinco, de lunes a viernes. Pero durante ese tiempo no se puede parar ningún servicio del CPD.

2. Una empresa se traslada a una nueva ciudad y busca un edificio adecuado para instalar el CPD. Está dudando entre unas oficinas en el interior de la ciudad, un parque empresarial o un parque industrial. Indica qué recomendarías en cada situación:

a) El CPD posee varias máquinas antiguas que hacen mucho ruido.

b) Por la noche, el parque empresarial es una zona de copas muy animada.

c) El parque industrial solamente proporciona la nave, mientras que el edificio de la ciudad y el parque empresarial tienen varias instalaciones disponibles.

d) El parque industrial carece de seguridad centralizada: cada nave contrata su servicio particular.

e) La mayoría de las empresas del parque industrial se dedican al almacenaje de maderas y pinturas.

f) En el parque empresarial ya dispone de oficina alguna de las empresas que le suministran material informático y comunicaciones.

g) En el edificio de la ciudad solo tienen disponible la última planta o alguna de las plantas subterráneas.

3. Una consultora realiza una auditoría al CPD de una empresa. Elabora un informe con las principales conclusiones. Para cada punto, evalúa si es correcto o, en cambio, tú propones alguna modificación:

a) Las paredes del CPD son módulos de madera, como el utilizado para habilitar salas de reunión dentro de la planta.

b) El sistema de extinción de incendios es el mismo para todas las salas de trabajo: aspersores de agua desde el techo.

c) Varias salas próximas al CPD se utilizan como almacenes de papel.

d) La cubierta del techo suele tener goteras en invierno.

e) La sala del CPD tiene sensores de temperatura y humedad conectados al mismo sistema que supervisa los servidores.

f) La puerta del CPD está abierta a cualquiera, porque nunca han tenido problemas de sabotaje en la historia de la empresa. Por la misma razón, no hay ningún detector de presencia.

g) El sistema de SAI instalado permite una autonomía de 30 minutos.

h) Una pared del CPD tiene un gran ventanal a pie de calle.

i) La sala del CPD dispone de un conjunto de cámaras conectadas por IP con el ordenador del responsable de informática.

j) La colocación de ordenadores es caótica, sin respetar ningún pasillo de ventilación.

k) En la planta superior está el laboratorio de I+D de una empresa de telecomunicaciones.

Unidad 4

Seguridad pasiva: almacenamiento



En esta unidad aprenderemos a:

- Preocuparnos por la información almacenada: rendimiento, disponibilidad, accesibilidad.
- Realizar copias de seguridad en dispositivos locales y remotos, fijos y extraíbles.
- Interpretar documentación técnica sobre soluciones de almacenamiento.
- Hacer imágenes completas o parciales del sistema operativo instalado.

Y estudiaremos:

- El almacenamiento redundante y distribuido.
- El almacenamiento en la red local y en Internet.
- Las copias de seguridad y las imágenes de respaldo.
- El almacenamiento remoto y extraíble.
- Los medios de almacenamiento.

1. Estrategias de almacenamiento

Vocabulario

BSOD (Blue Screen of Death). Es el típico pantallazo azul de los sistemas operativos Windows cuando ocurre un error grave.

MTBF (Mean Time Before Failure). Es el tiempo medio entre fallos de un sistema. En los discos duros estamos hablando de 1,4 millones de horas.

SSD (Solid State Drive). Unidad de almacenamiento tipo pendrive USB pero con comportamiento de disco duro.

Para una empresa, la parte más importante de la informática son los datos: sus datos. Porque:

- El hardware es caro, pero se puede volver a comprar.
- Un informático muy bueno puede despedirse, pero es posible contratar otro.
- Si una máquina no arranca porque se ha corrompido el sistema de ficheros (el típico BSOD), puedes instalar de nuevo el sistema operativo y las aplicaciones desde los CD o DVD originales.

En todos los casos anteriores se recupera la normalidad en un plazo de tiempo razonable.

Sin embargo, los datos de esa empresa son únicos: no se pueden comprar, no se pueden contratar, no hay originales. Si se pierden, no los podemos recuperar (por lo menos, ni fácil ni rápidamente).

Bien, puesto que los datos son tan importantes, hay que esforzarse especialmente en mejorar su integridad y disponibilidad (estos conceptos los aprendimos en la Unidad 1):

- Podemos comprar los mejores discos del mercado en calidad (MTBF) y velocidad; aunque nunca debemos olvidar que son máquinas y pueden fallar (salvo los SSD, todos los discos tienen partes móviles). En un puesto de usuario nos lo podemos permitir (lo cambiamos y listo): en un servidor hemos visto que no.
- Podemos concentrar los discos en unos servidores especializados en almacenamiento.
- Podemos replicar la información varias veces y repartirla por ciudades distintas.
- Podemos contratar el servicio de respaldo de datos a otra empresa, conectados por Internet, para no depender de nuestros equipos y personal.

A continuación estudiaremos cada una de estas alternativas.

Cada empresa elegirá implementar una o varias, según sus necesidades y posibilidades.

Actividades

Vamos a suponer que trabajamos en el departamento de informática de una cadena de restaurantes. Tenemos establecimientos en España y en el extranjero. Nuestras bases de datos almacenan información acerca de reservas, facturas, proveedores, pedidos, bancos, empleados, etc.

1. Hay una sede central en la que están los servidores principales donde corren esas bases de datos. Si ocurre un incendio y se destruyen esos ordenadores, ¿qué consecuencias tendría para la empresa?
2. ¿Y si solo se hubiera perdido alguna de las tablas (pedidos, facturas, empleados), no todas?
3. Razona si cada una de las actuaciones referidas (comprar discos mejores, utilizar servidores especializados, etc.) mejora la integridad, la disponibilidad o ambas.
4. Busca las características del disco duro de tu ordenador de clase y localiza el tiempo medio de fallo.

1.1. Rendimiento y redundancia. RAID en Windows y Linux

Los ordenadores pueden conectar varios discos internos porque las placas base suelen traer integrada una controladora de discos para dos o tres conexiones. Y si pinchamos más controladoras (Fig. 4.1), podremos conectar más dispositivos. Pero ¿para qué queremos varios discos en un ordenador? Por la misma razón por la que compramos CPU de varios núcleos o placas base con varias CPU.

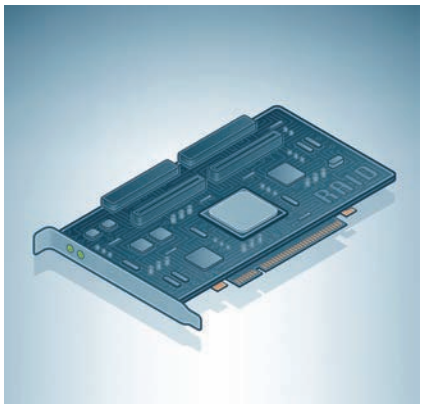


Fig. 4.1. *Tarjeta RAID.*

Podemos aprovechar varios discos de un ordenador para:

- **Crear unidades más grandes.** Dos discos de 500 GB juntos nos pueden dar una unidad de 1 TB. Con tres discos tenemos 1,5 TB, etc. Por ejemplo, si queremos ripear un Blu-ray de 25 GB y solo tenemos discos de 20 GB, necesitamos juntar dos en una unidad de 40 GB. O, si queremos darle al `/home` 2 TB y solo tenemos discos de 640 GB, podemos juntar tres.
- **Crear unidades más rápidas.** Si tenemos dos discos de 500 GB y configuramos el sistema para que, en cada fichero, los bloques pares se escriban en un disco y los impares en otro, después podremos hacer lecturas y escrituras en paralelo (en el mejor caso, ahorramos la mitad de tiempo). Con un único disco de 1 TB tenemos la misma capacidad, pero cada lectura o escritura debe esperar que termine la operación anterior. La diferencia es más notable si ponemos tres discos, cuatro, etc.
- **Crear unidades más fiables.** Si configuramos los dos discos anteriores para que, en cada fichero, los bloques se escriban a la vez en ambos discos, podemos estar tranquilos porque, si falla un disco, los datos estarán a salvo en el otro.

Pues una de las tecnologías que lo consigue se llama RAID. Hay varios niveles de RAID. Los más importantes son:

- **RAID 0.** Agrupamos discos para tener un disco más grande, incluso más rápido. Desde ese momento, los bloques que lleguen al disco RAID 0 se escribirán en alguno de los discos del grupo. Por supuesto, para el usuario este proceso es transparente: él solo ve un disco de 1 TB donde antes había dos discos de 500 GB. En el RAID 0 podemos elegir entre spanning y striping (que es lo más común). En cualquier caso, si falla uno de los discos, lo perdemos todo.
- **RAID 1.** Se le suele llamar **mirror** o **espejo.** Agrupamos discos por parejas, de manera que cada bloque que llegue al disco RAID 1 se escribirá en los dos discos a la vez. Si falla uno de los discos, no perdemos la información, porque estará en el otro. A cambio, sacrificamos la mitad de la capacidad (el usuario ha conectado dos discos de 500 GB y solo tiene disponibles 500 GB, en lugar de 1 TB) y no ganamos rendimiento.
- **RAID 5.** Hemos visto que el RAID 0 es más rápido que cada uno de los discos, pero tan seguro como cualquiera de ellos. El RAID 1 es más seguro que los discos por separado, pero con el mismo rendimiento. El RAID 5 consigue ambas cosas aplicando dos mecanismos:
  - Para cada dato que el sistema quiere almacenar en el RAID, este aplica un procedimiento matemático (en general, la paridad) para obtener información complementaria a ese dato, de tal manera que se puede recuperar el dato en caso de perder cualquier disco (sea disco de datos o paridad).
  - Una vez obtenida la paridad, se hace striping para repartir el dato y su paridad por los discos conectados al RAID.

Importante

Hablamos de ficheros, pero en los bloques de los discos se escribe cualquier cosa que necesite el sistema operativo o las aplicaciones instaladas. Por ejemplo, el sector de arranque (MBR [Master Boot Record]).

Vocabulario

RAID (Redundant Array of Independent Disks). Es un grupo de discos configurados para trabajar en conjunto, con el fin de lograr más rendimiento, más fiabilidad o ambas cosas.

Spanning. Los bloques se escriben en el primer disco hasta que lo llenan; entonces pasan al siguiente, y así sucesivamente. Por tanto, la lectura o escritura de cada bloque tiene que esperar hasta que el disco haya terminado la anterior.

Striping. Los bloques se escriben cada vez en un disco distinto. Es más rápido que el spanning porque hace trabajar a todos los discos a la vez.

Actividades

5. Busca en Internet precios y características de una tarjeta controladora SATA para pinchar en un equipo con slots PCI.

6. Investiga en qué consiste la técnica XOR para obtener la información redundante en RAID 5 y explícalo a tus compañeros.

Web

Algunas empresas han construido sus propios servidores en RAID:
http://goo.gl/4uPCi

Por tanto, necesitamos un disco más para almacenar la paridad. Por ejemplo, si queremos una capacidad de 1 TB, necesitamos tres discos de 500 GB (o cinco discos de 250 GB).

Gracias al striping hemos conseguido mejor rendimiento que el disco individual, y gracias a la paridad estamos más seguros que en RAID 0. A cambio, sacrificamos la capacidad de un disco (aunque cuantos más discos, menos porcentaje de capacidad perdida).

Estamos viendo que el RAID para el sistema operativo es una especie de disco «virtual», que está organizado en stripes (bandas, filas). Al igual que el tamaño del bloque en los discos «físicos» (512 bytes, 4 096 bytes) y el tamaño del bloque del sistema de ficheros (4 096 bytes en NTFS), en el RAID es importante el tamaño de stripe. El valor recomendado es 64 KB.

Veamos un ejemplo (Fig. 4.2). Tenemos tres ficheros y queremos almacenarlos en un RAID donde, por simplificar, el tamaño de stripe es el mismo que el tamaño de bloque del sistema operativo.

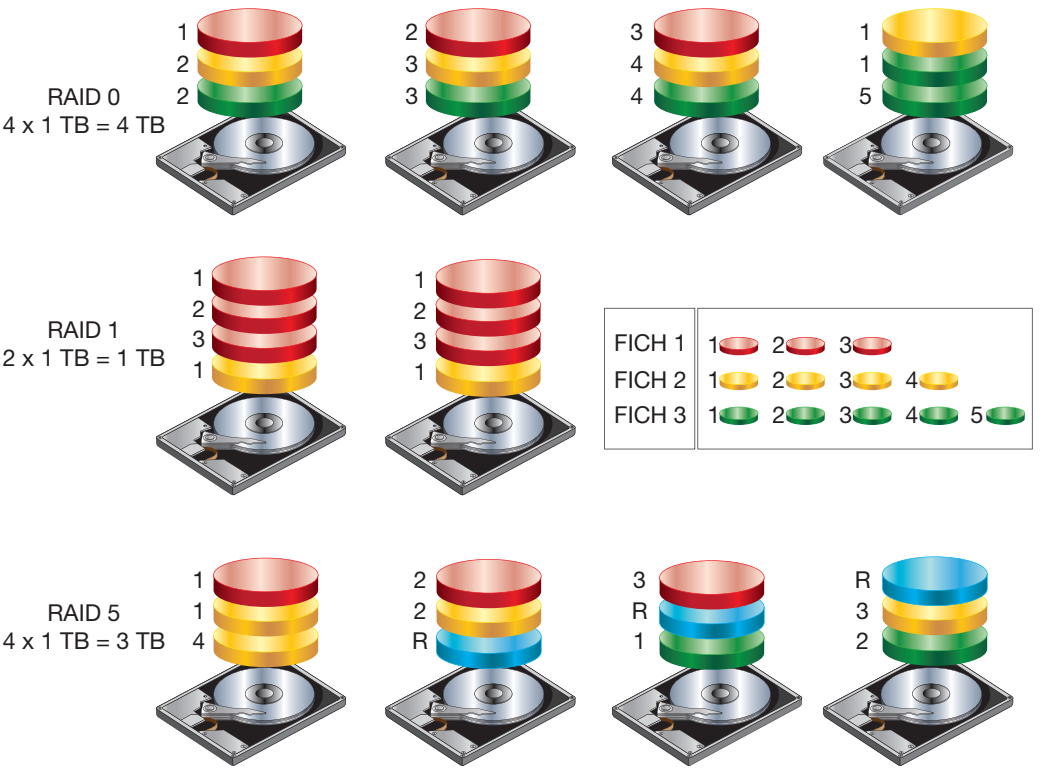


Fig. 4.2. *Almacenamiento en RAID 0, RAID 1 y RAID 5.*

El primer fichero ocupa tres bloques; el segundo, cuatro, y el tercero, cinco. Todos los discos son de 1 TB.

- Si tenemos cuatro discos y los configuramos en RAID 0, los bloques de los ficheros se reparten por los cuatro discos. La capacidad total es de 4 TB, y los bloques de un fichero se pueden recuperar simultáneamente por varios discos.
- Si ponemos dos discos en RAID 1, los bloques de los ficheros se copian en los dos. La capacidad total es de 1 TB.
- Si ponemos los cuatro discos en RAID 5, los bloques de los ficheros se reparten por los cuatro discos, pero hay que incluir un bloque R que representa la redundancia (la paridad). La paridad se calcula para cada fila (el stripe que hemos visto). Este bloque no se usa durante la lectura (salvo fallo de un disco), pero sí durante la escritura, porque hay que actualizarlo. Los bloques R no se dejan en el mismo disco para evitar cuellos de botella.

Actividades

7. ¿El tamaño del stripe es importante? ¿De qué depende?

8. ¿Los discos de un RAID tienen que ser todos iguales? ¿O incluso conviene que sean diferentes?

9. Cuando cae un disco en un RAID 5, hay que sustituirlo y regenerar el RAID. Y hay que hacerlo con el sistema arrancado, porque la información sigue disponible y la empresa no puede parar. ¿Qué ocurre cuando utilizamos discos muy grandes (varios terabytes)?

10. Investiga otros tipos de RAID, como el RAID 6 (doble paridad), RAID 10 (hacer mirror de un RAID 0), etcétera.

11. La tarea de repartir la información por los discos del RAID puede ser asumida por el sistema operativo o por la tarjeta controladora. Investiga y debate sobre las ventajas e inconvenientes de cada método.

Caso práctico 1

RAID en Linux

■ **Duración**: 🕒 15 minutos ■ **Dificultad**: 😐 Media

Objetivo. Crear discos RAID 1 por software en Linux. También sustituiremos un disco fallido.

Material. Ubuntu Server 12.04 sobre VirtualBox 4. Lo haremos en máquina virtual para añadir discos con facilidad; todos los pasos son válidos para una máquina real, porque el sistema operativo no sabe que se está ejecutando en una máquina virtual.

1. Crear una máquina virtual e instalar Ubuntu Server 12.04.

CEO

En el CEO del proyecto tienes una exhaustiva explicación y los ficheros necesarios para realizar la instalación de la máquina virtual Ubuntu Server.

2. Antes de arrancarla, crearemos los discos que queremos conectar. Entramos en VirtualBox, seleccionamos nuestra máquina UbuntuServer y pulsamos en *Almacenamiento*. Sobre el controlador SATA pulsamos el botón derecho y elegimos *Agregar disco duro*. Nos preguntará si ya lo tenemos o hay que crearlo (Fig. 4.3).

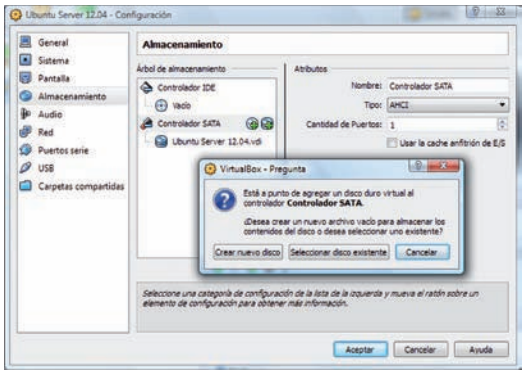


Fig. 4.3. *Añadimos disco nuevo.*

3. Seleccionamos *Crear* y aparece un asistente. Elegiremos el tipo VDI, tipo dinámico y tamaño de 100 MB. Lo llamaremos *disco1*.

4. Repetimos los pasos para *disco2*.

5. Arrancamos la máquina virtual y nos ponemos con privilegios de administrador.

```
$ sudo –i
#
```

6. Comprobamos que los discos están ahí (Fig. 4.4).

```
# fdisk -l
```

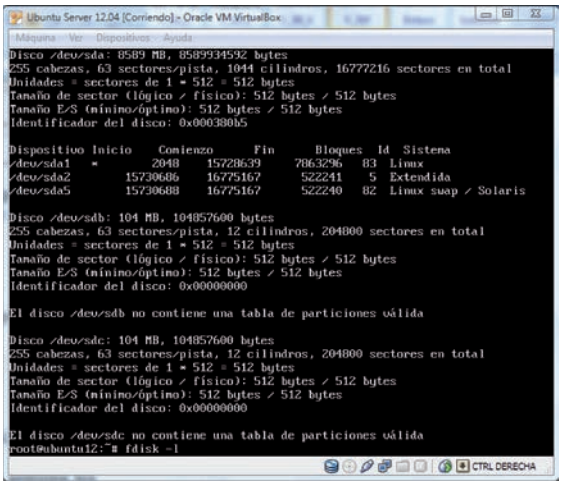


Fig. 4.4. *Comprobamos discos conectados.*

7. Instalamos el paquete `mdadm`, que gestiona los dispositivos RAID por software.

```
# apt-get install mdadm
```

Veremos que, además del mdadm, vamos a instalar el servidor de correo `postfix`. Esto se debe a que el RAID se puede configurar para que avise por correo cuando ocurra un fallo.

8. Creamos el RAID 1 con el comando:

```
# mdadm --create /dev/md0 --level=1
--raid-devices=2 /dev/sdb /dev/sdc
```

Donde `/dev/md0` es el nombre del nuevo dispositivo RAID, `level=1` indica un RAID 1, `raid-devices=2` indica que son dos discos.

9. Comprobamos que el nuevo dispositivo está disponible y tiene 100 MB, como los originales (Fig. 4.5).

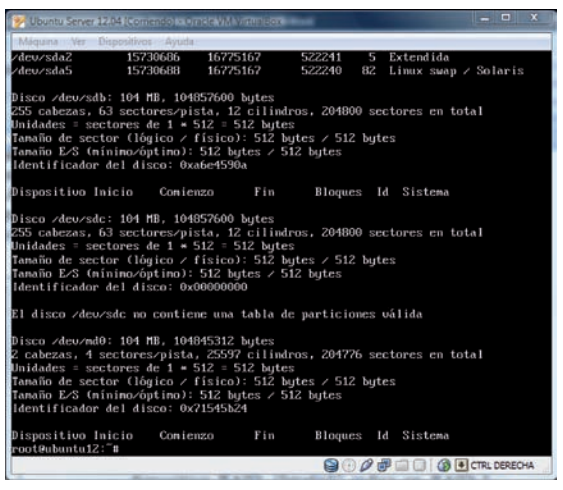


Fig. 4.5. *Comprobamos nuevo disco RAID.*

(Continúa)

Caso práctico 1

(Continuación)

10. Ya podemos trabajar con él como un disco cualquiera: crear particiones con `fdisk`, formatearlo con `mkfs`, etc. Vamos a crear una partición, la formatearemos y meteremos un fichero de 50 MB. Para crear la partición usamos:

```
# fdisk /dev/md0
```

Este comando nos ofrece un menú con múltiples operaciones. Elegimos `n` para crear la nueva partición y en las opciones dejamos los valores por defecto (tipo `p` [primaria], número 1 y todos los sectores disponibles). Finalmente ejecutamos `w` para escribir los cambios al disco.

```
# mkfs /dev/md0p1
# mkdir /mnt/raid1
# mount /dev/md0p1 /mnt/raid1
```

Con estos tres comandos creamos el sistema de ficheros y lo montamos para empezar a usarlo.

```
# dd if=/dev/zero
of=/mnt/raid1/fich bs=512
count=100000
# ls -l /mnt/raid1
```

El primer comando crea el fichero de 50 MB aproximadamente (10 000 bloques de 512 bytes). Con el segundo comprobamos el resultado.

11. Para comprobar el estado del RAID tenemos el fichero `/proc/mdstat` (Fig. 4.6).

En nuestro caso nos muestra que tenemos un RAID `md0`, que está activo, de tipo `raid1`, cuyos componentes son `sdc` y `sdb`.

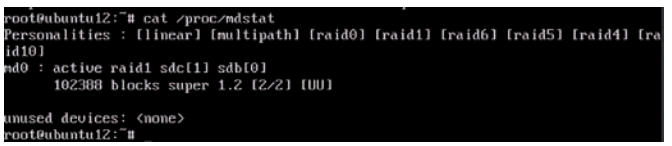


Fig. 4.6. *Comprobamos el estado del RAID.*

12. Si un disco falla, podemos quitarlo y el RAID se mantiene porque espera que lo sustituyamos por otro. Para ello primero hay que marcarlo como disco fallido y luego quitarlo del RAID. Vamos a hacerlo con el disco `sdb`. Los comandos son:

```
# mdadm /dev/md0 --fail /dev/sdb
# mdadm /dev/md0 --remove /dev/sdb
```

Después de cada comando consultamos el `mdstat` para comprobar qué ha ocurrido (Fig. 4.7). En el primer caso se indica que el disco `sdb` ha fallado (*F* de *Failed*); en el segundo comando ya no aparece `sdb`. En ambos casos la composición del RAID 1 aparece incompleta `[_U]`.

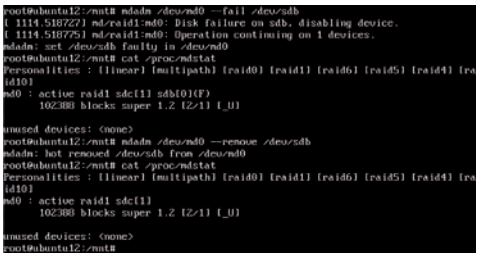


Fig. 4.7. *Eliminamos un disco del array.*

13. Sin embargo, los datos siguen ahí.

14. Si quisiéramos que el disco `sdb` volviera al RAID, primero habría que eliminar su configuración anterior (borrar el superbloque) y luego añadirlo. Los comandos son:

```
# mdadm --zero-superblock /dev/sdb
# mdadm /dev/md0 --add /dev/sdb
```

Como se ve en la Figura 4.8, después de añadir el disco se inicia un proceso de sincronización (recovery). Hasta que no ha terminado el RAID no recupera el estado `[UU]`.

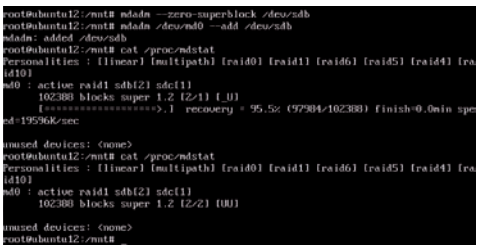


Fig. 4.8. *Recuperamos el disco.*

15. Si queremos que los sistemas de ficheros creados en un RAID estén disponibles al arrancar, debemos incluirlos en el `fstab`, como es habitual.

16. Podemos desactivar temporalmente un RAID con el comando:

```
# mdadm /dev/md0 --stop
```

El comando anterior necesita que el disco no esté siendo utilizado en ningún sistema de ficheros.

17. Para activar el RAID tenemos (Fig. 4.9):

```
# mdadm --assemble --scan
```

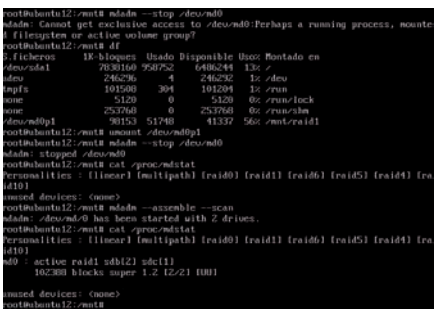


Fig. 4.9. *Reconectamos el RAID.*

Caso práctico 2

RAID en Windows

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

Objetivo. Crear un RAID 1 y un RAID 0 en Windows, donde se llaman volumen reflejado y volumen distribuido, respectivamente. En el caso del RAID 1, romperemos el espejo para obtener dos discos iguales.

Material. Windows Server 2008 R2 corriendo sobre VirtualBox 4. El procedimiento es similar para Windows 7 y anteriores, aunque no todas las versiones permiten todos los tipos de RAID (por ejemplo, RAID 5 solo está para servidores, como es normal).

1. Crear una máquina virtual e instalar Windows Server 2008.

CEO

En el CEO del proyecto tienes una exhaustiva explicación y los ficheros necesarios para realizar la instalación de máquina virtual Windows Server 2008.

2. Antes de arrancarla, crearemos los discos que queremos conectar. Como en el caso práctico 1, serán dos discos muy pequeños, de 100 MB, para que las pruebas sean rápidas.
3. Arrancamos nuestra máquina W2008. Nos logueamos como administrador y entramos a la herramienta de gestión de discos. Hay varias formas de hacerlo. Por ejemplo, pulsar en *Inicio*; sobre la opción *Equipo* activamos el menú de botón derecho y elegimos *Administrar*. Aparecerá una ventana donde seleccionaremos *Administración de discos*.
4. Como se ve en la Figura 4.10, el sistema ha detectado que hay discos nuevos. Nos solicita inicializarlos y aceptamos.

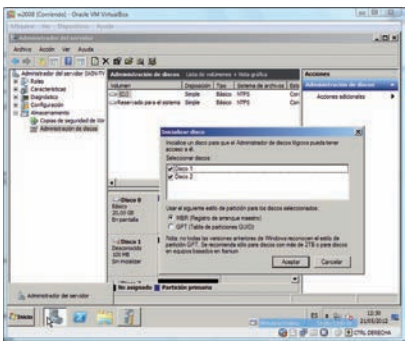


Fig. 4.10. *Detectados discos nuevos.*

5. Ahora tenemos dos discos nuevos y vamos a crear un RAID 1 con ellos. Nos ponemos sobre cualquiera de ellos y pulsamos el botón derecho. En el menú que aparece elegimos *Nuevo volumen reflejado*.
6. Se inicia un asistente que nos pregunta qué discos queremos incluir. Seleccionamos los dos discos libres. Como ya sabemos, el tamaño final serán 100 MB (Fig. 4.11).

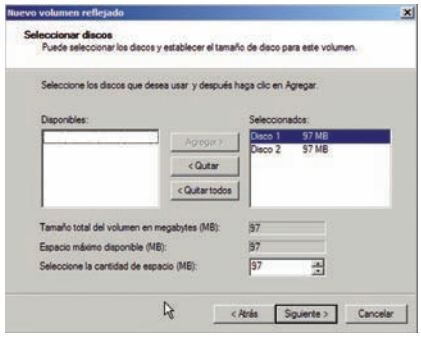


Fig. 4.11. *Componentes del espejo.*

7. Al terminar el asistente tenemos el espejo creado. En el administrador de discos aparecen marcados en rojo (Fig. 4.12).

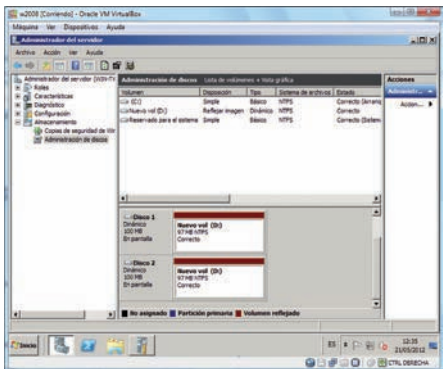


Fig. 4.12. *Espejo creado.*

8. Pero para el usuario es una unidad normal y corriente de 100 MB (Fig. 4.13).



Fig. 4.13. *Nueva unidad en espejo.*

9. En la nueva unidad vamos a crear un fichero de texto llamado prueba (Fig. 4.14).

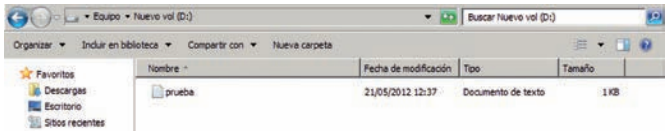


Fig. 4.14. *Fichero de prueba.*

(Continúa)

Caso práctico 2

(Continuación)

10. Para comprobar que efectivamente es un espejo y los dos discos tienen el mismo contenido, vamos a romper el espejo. Volvemos al administrador de discos, nos situamos sobre uno de los discos rojos y pulsamos el botón derecho. Elegimos *Romper volumen reflejado* (Fig. 4.15).

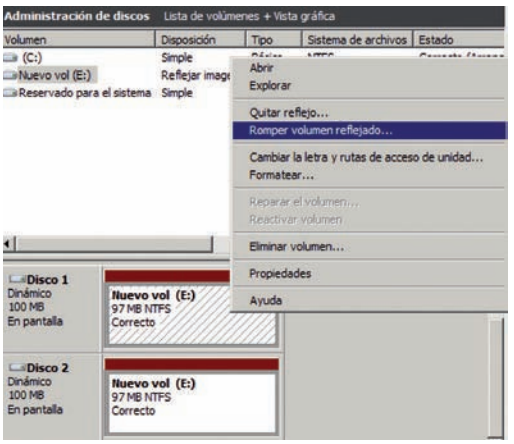


Fig. 4.15. *Romper volumen reflejado.*

11. El resultado es que nuestros discos ya no tienen el color rojo que indica que están reflejados, sino el verde de disco normal (Fig. 4.16).

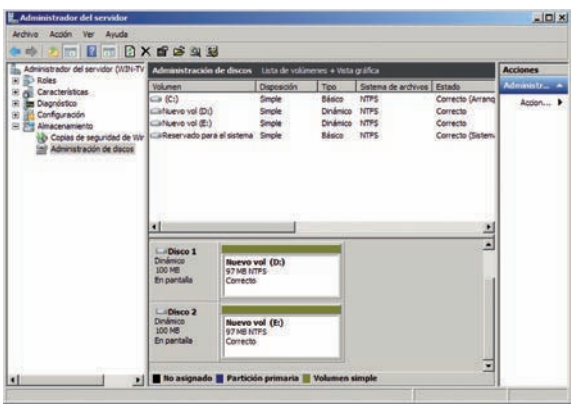


Fig. 4.16. *Espejo roto.*

12. Para el usuario, de repente, han aparecido dos unidades de 100 MB, con el mismo contenido cada una (Figs. 4.17 y 4.18).

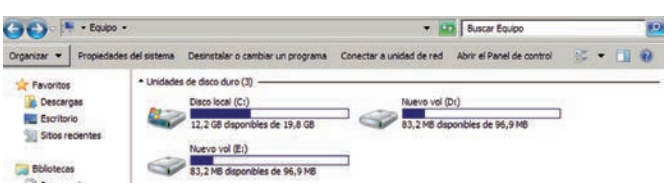


Fig. 4.17. *Dos unidades nuevas e iguales.*

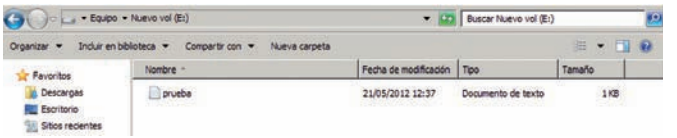


Fig. 4.18. *Contenido replicado.*

13. Ahora vamos a montar un RAID 0 con esos mismos discos. En el administrador de discos nos ponemos sobre cualquiera de ellos, y en el menú de botón derecho primero ejecutamos *Eliminar volumen* (ahora están en uso como mirror) y después *Nuevo volumen seccionado*. De nuevo, el asistente nos permite elegir los discos y formatearlos. En el administrador de discos aparecen con un verde distinto (Fig. 4.19).

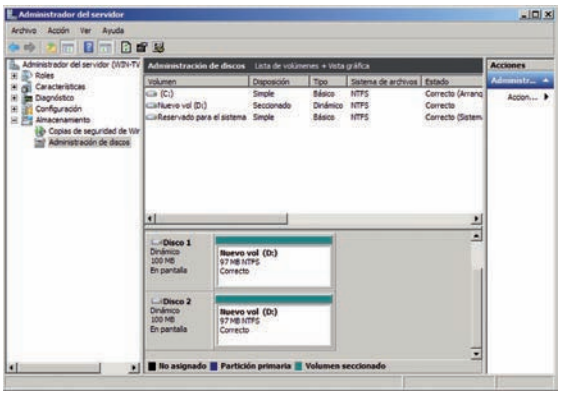


Fig. 4.19. *Discos seccionados.*

14. Para el usuario es una nueva unidad de 200 MB (Fig. 4.20).

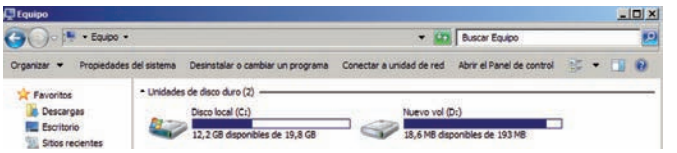


Fig. 4.20. *Unidad seccionada.*

15. Podemos usarla para guardar un fichero de 160 MB, lo que no podríamos hacer con los discos de 100 MB (Fig. 4.21).

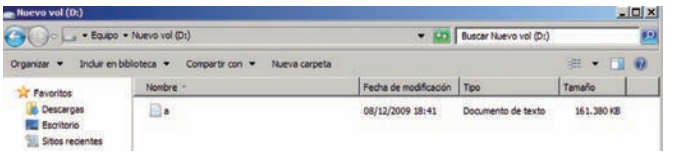


Fig. 4.21. *Usamos la unidad seccionada.*

16. Podemos comprobar que, si rompiéramos el volumen seccionado, perderíamos todos los datos.

Caso práctico 3

RAID en hardware

■ **Duración**: ◷ 15 minutos ■ **Dificultad**: ☹ Alta

Objetivo. Vamos a crear un RAID 1 soportado por la tarjeta controladora, no por el sistema operativo.

Material. Ordenador con BIOS compatible con Intel Matrix Storage, dos discos duros SATA (160 GB en este ejemplo) y el CD de instalación de Windows XP.

1. Conectamos los dos discos duros SATA (Fig. 4.22).

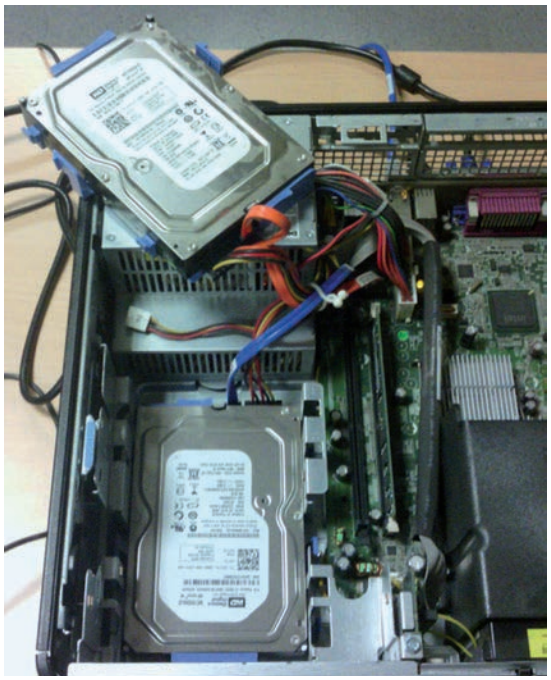


Fig. 4.22. *Conectamos dos discos duros.*

2. Encendemos el ordenador y entramos en la BIOS (típicamente pulsando **F2** durante el arranque). Buscamos la opción que activa la funcionalidad RAID y la seleccionamos (Fig. 4.23).

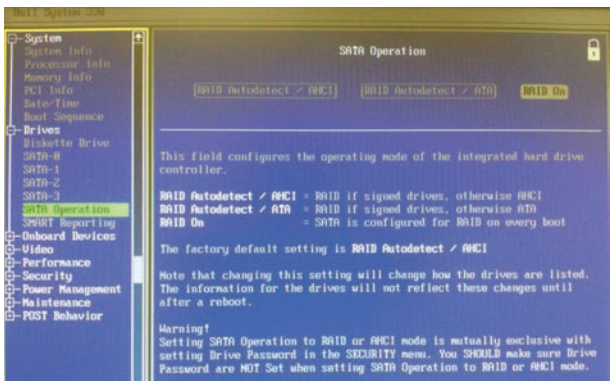


Fig. 4.23. *Activamos RAID en BIOS.*

3. Guardamos los cambios y al arrancar de nuevo aparecen las opciones de configuración RAID. En nuestro caso, es la herramienta ROM del Intel Matrix Manager y se accede al menú principal pulsando **Ctrl+I** (Fig. 4.24).

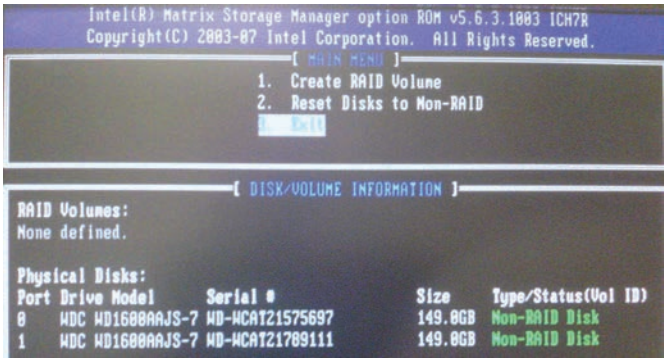


Fig. 4.24. *Menú principal.*

4. Vemos los dos discos y ningún volumen creado. Pulsamos **1** para crearlo (Fig. 4.25). Le damos nombre (*espejo*, por ejemplo), elegimos el tipo de RAID y los discos afectados. Finalmente seleccionamos *Create Volume*.



Fig. 4.25. *Nuevo volumen.*

5. Si todo ha ido bien, volvemos al menú principal con la nueva configuración (Fig. 4.26).

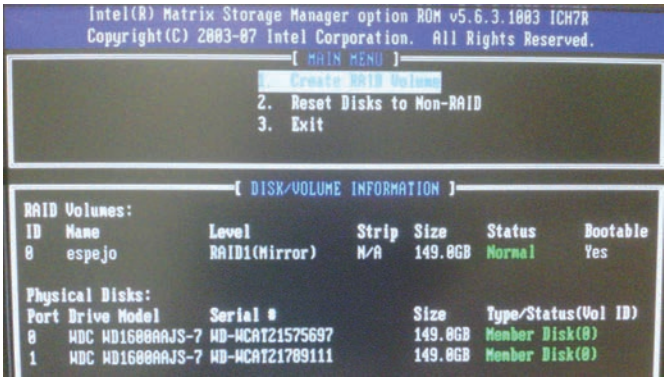


Fig. 4.26. *Volumen RAID 1 creado.*

6. Salimos de la herramienta y al arrancar de nuevo vemos nuestro mirror, pero no hay ningún sistema operativo (Fig. 4.27). La herramienta ya nos advirtió de que el RAID 1 se crearía vacío.

(Continúa)

Caso práctico 3

(Continuación)

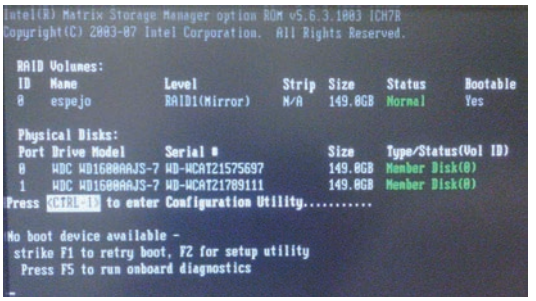


Fig. 4.27. *Arranque con mirror vacío.*

7. En este punto introducimos el CD de instalación de XP. Elegimos XP porque tarda muy poco en instalarse. Si el CD no viene preconfigurado con los drivers para Intel Matrix, habrá que interrumpir la instalación pulsando **F6** cuando llegue el momento.

8. Si todo ha ido bien, Windows nos ofrecerá instalarse en un disco de 160 GB, aunque físicamente tenemos dos (Fig. 4.28).

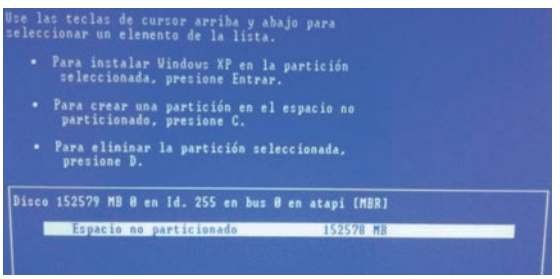


Fig. 4.28. *Instalación de Windows en volumen espejado.*

9. Creamos una partición de 40 GB (suficiente para XP) y, una vez terminada la instalación, en el administrador de dispositivos podemos ver la controladora RAID (Fig. 4.29).

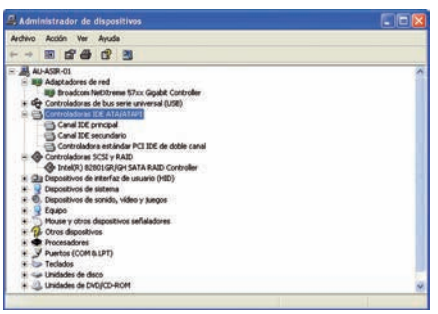


Fig. 4.29. *Controladora RAID.*

10. En el administrador de discos (Fig. 4.30) aparece como un único disco (en el caso práctico 2 se veían dos discos marcados en verde).

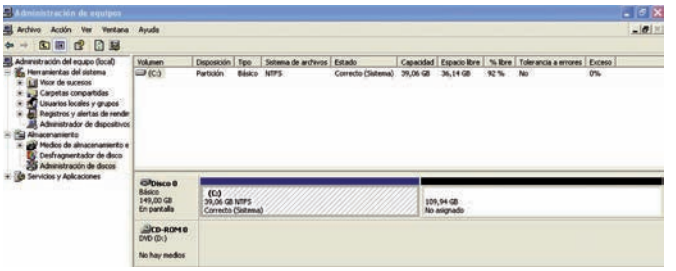


Fig. 4.30. *Un único disco.*

11. Para trabajar con la configuración del RAID podemos seguir utilizando el arranque, pero también hay una aplicación llamada Intel Matrix Console. La podemos descargar de la web de Intel. Al arrancarla veremos el estado de nuestro RAID (Fig. 4.31).

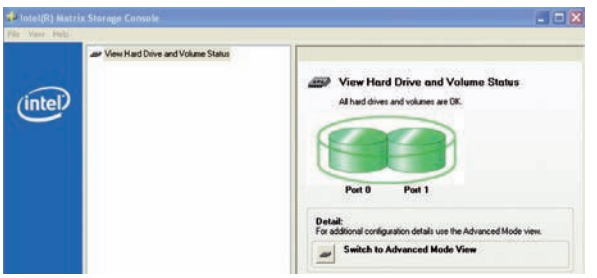


Fig. 4.31. *Intel Matrix Console.*

12. Podemos verlo en modo avanzado para tener los detalles de nuestro volumen (Fig. 4.32). Aparece nuestro volumen y los discos que lo componen.

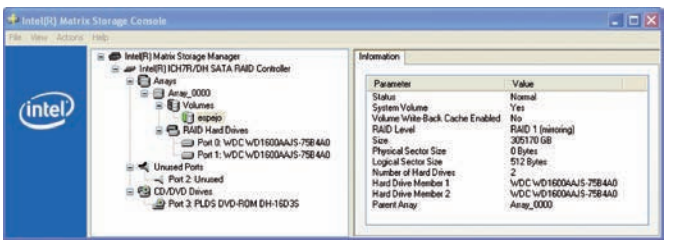


Fig. 4.32. *Modo avanzado.*

13. Si nos situamos en el volumen, podemos lanzar las operaciones asociadas (Fig. 4.33).

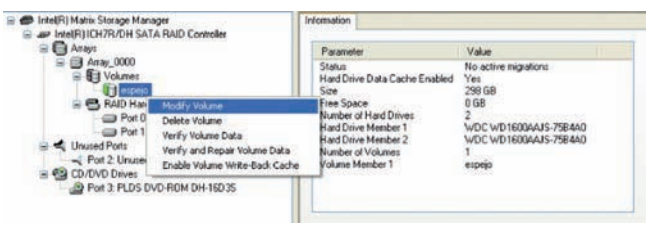


Fig. 4.33. *Operaciones.*

(Continúa)

Caso práctico 3

(Continuación)

14. Vamos a probar a romper el volumen. Arrancamos y pulsamos **Ctrl+I** para entrar a la herramienta. Ahora elegimos la opción 2 para recuperar uno de los discos (Fig. 4.34).

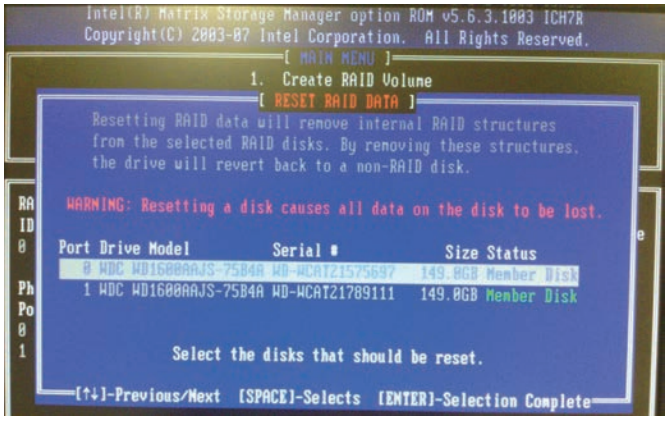


Fig. 4.34. *Rompemos el espejo.*

15. Nos situamos en el segundo y pulsamos la tecla **Space.** Ahora pulsamos **Enter** para confirmar la operación. El RAID 1 ha quedado degradado (Fig. 4.35), pero no se ha perdido todo: los datos siguen en el único disco que todavía forma parte del espejo.

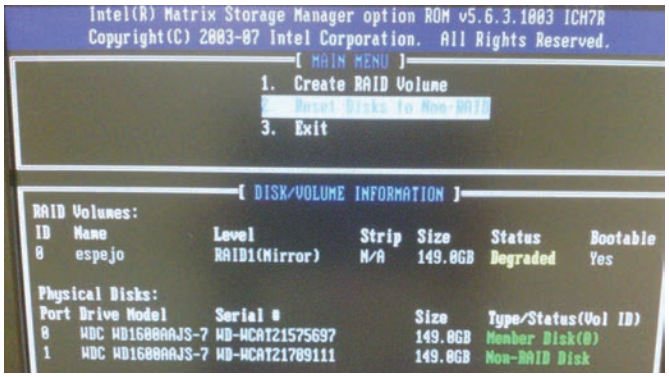


Fig. 4.35. *Espejo degradado.*

16. Podemos arrancar la máquina y comprobaremos que ahora hay dos discos (Fig. 4.36).

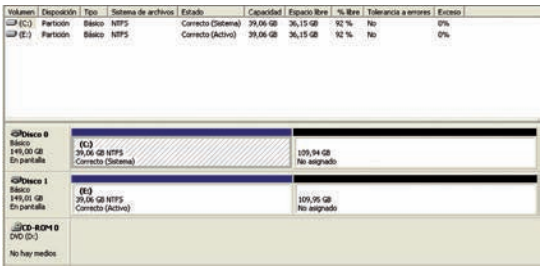


Fig. 4.36. *Dos discos.*

17. Incluso en el nuevo disco `E:` están los mismos contenidos que en `C:` (Fig. 4.37). Es decir, al romper el espejo no se ha perdido nada en ninguno.

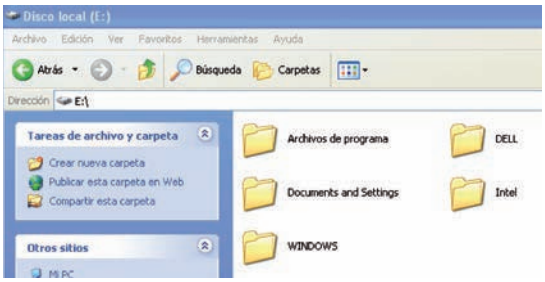


Fig. 4.37. *Contenido intacto.*

18. Si arrancamos la Intel Matrix Console, nos avisará del problema (Fig. 4.38).



Fig. 4.38. *Problema detectado.*

19. Podríamos regenerar el RAID con el disco disponible o eliminar definitivamente el volumen. Aunque, como es el disco de Windows, habría que hacerlo desde la herramienta ROM.

Actividades

12. El profesor encarga una presentación en PowerPoint a un grupo de alumnos. Ellos se reparten el trabajo: uno busca las imágenes, otro los vídeos, otro los sonidos, etc. ¿Cómo organizaríais el traspaso de ficheros?

1.2. Almacenamiento en red: NAS y SAN. Clústers

Hemos visto que podemos mejorar el rendimiento y la fiabilidad del almacenamiento de un ordenador conectando varios discos y configurándolos en RAID.

Pero en las empresas se suele trabajar en equipo, compartiendo ficheros entre varios ordenadores. Tenemos que pensar cómo compartir ficheros y cómo hacerlo con seguridad (quién puede leer esos ficheros y quién puede modificarlos, borrarlos o incluir nuevos).

Aunque en el caso práctico 4 veremos cómo se hace en un ordenador de un puesto de trabajo, no es la solución más recomendable porque:

- Hacer de servidor de ficheros afectará al rendimiento de sus aplicaciones (Office, Chrome), y viceversa.
- Estaríamos pendientes de si la otra persona lo ha apagado al salir de la oficina (y puede que estemos en edificios diferentes).
- Es un ordenador personal, luego es probable que no disponga de RAID ni copias de seguridad.
- Estamos expuestos a que un virus entre en ese ordenador y borre todo.

Por tanto, lo mejor es ponerlo en un servidor dedicado y, a ser posible, especializado en almacenamiento. De esta manera:

- Podemos instalar el software estrictamente necesario y tenerlo actualizado (menor riesgo de infecciones).
- Estará bajo la supervisión del personal del CPD (centro de proceso de datos), lo que garantiza estar encendido todo el tiempo, formar parte de la política de copias de seguridad de la empresa, detectar cuando el disco está próximo a llenarse, etc.
- Si, además, es un servidor especializado en almacenamiento, dispondrá de hardware suficiente para desplegar configuraciones RAID, una memoria caché de alto rendimiento, etc.

Caso práctico 4

Compartir carpetas en Windows

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

Objetivo. Compartir una carpeta en Windows para que se vea desde otros Windows y también desde Linux.

Material. Varios sistemas operativos (XP, Vista, 7, Ubuntu).

Empezaremos por lo más sencillo: compartir en modo solo lectura (cualquiera puede leer pero nadie puede escribir).

1. Arrancamos un Windows XP Professional y entramos como administrador.
2. En el escritorio creamos una carpeta llamada compartida y dentro un fichero.
3. Sobre la carpeta pulsamos el botón derecho y elegimos la opción *Compartir y seguridad* (Fig. 4.39).



Fig. 4.39. *Compartir una carpeta.*

4. La primera vez que lo hagamos Windows nos preguntará si queremos ejecutar un asistente o solo buscamos compartir archivos. Elegimos esta segunda opción.
5. En la ventana que aparece vamos a las opciones centrales (la primera opción solo permite compartir con otros usuarios de esa máquina). Activamos la casilla *Compartir esta carpeta en la red*, dejamos desactivada la casilla *Permitir que los usuarios de la red cambien mis archivos* y pulsamos *Aceptar* (Fig. 4.40).

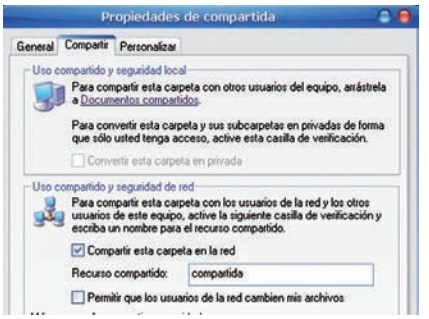


Fig. 4.40. *Compartir en red.*

(Continúa)

Caso práctico 4

(Continuación)

6. Desde ese momento la carpeta cambia su icono (aparece una mano por debajo) y estará disponible para cualquier equipo conectado a nuestra red. Por ejemplo, si en nuestro ordenador servidor utilizamos el comando `ipconfig` para conocer que su dirección IP es `192.168.1.38`, desde otro Windows cliente pueden hacer *Inicio > Ejecutar* y en la ventana que aparece introducir `\\192.168.1.38`. Esto abrirá una ventana del explorador con la carpeta compartida para que podamos trabajar con ella (Fig. 4.41).

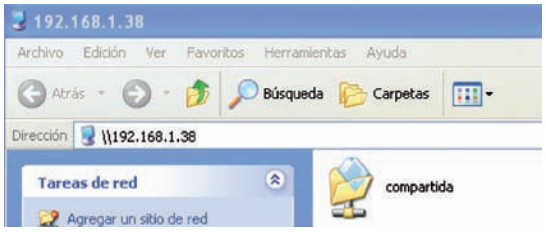


Fig. 4.41. *Conectamos desde XP.*

7. En el XP cliente podemos asociarlo a una unidad (Z:, Y:) mediante *Herramientas > Conectar a una unidad de red*. También podemos asociar desde el menú del botón derecho de la carpeta compartida.

8. Finalmente, podemos hacer esa asociación desde la línea de comandos. En el ordenador XP cliente ejecutamos *Inicio > Ejecutar > cmd* y en la ventana que aparece introducimos el comando `net use z: \\192.168.1.38\compartida`. Desde ese momento tenemos una nueva unidad Z: con los archivos de la máquina servidora (Fig. 4.42).



Fig. 4.42. *Conectamos con comandos XP.*

9. Los dos mecanismos anteriores sirven para cualquier versión superior de Windows (Vista, 7, Windows Server). Hay otras formas de conseguirlo. Por ejemplo, en Windows Vista podemos hacer *Inicio > Red* y aparecerán las máquinas que están accesibles. En Windows 7 hacemos *Inicio > Equipo > Conectar a unidad de red* y aparece un asistente (Fig. 4.43).

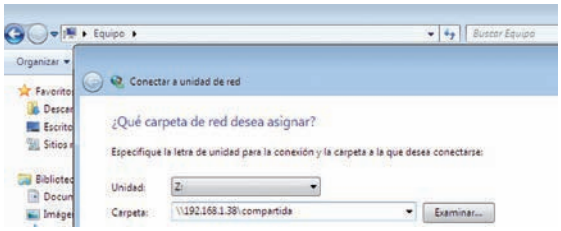


Fig. 4.43. *Conectamos desde W7.*

10. En *Carpeta* introducimos la dirección ya conocida y pulsamos el botón *Aceptar*. Nuestra nueva unidad Z: está disponible (Fig. 4.44).

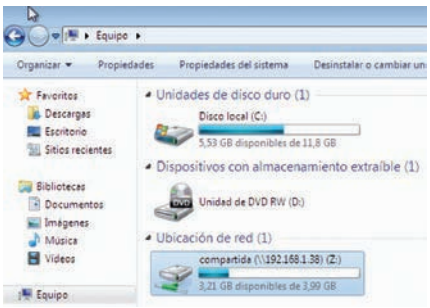


Fig. 4.44. *Nueva unidad de red W7.*

11. Desde Linux también podemos acceder a la carpeta compartida. En un Ubuntu Desktop 12.04 nos situamos en el escritorio y en el botón *Inicio* introducimos `smb://192.168.1.38/compartida`, donde smb es el protocolo de sistema de ficheros en red (Fig. 4.45).

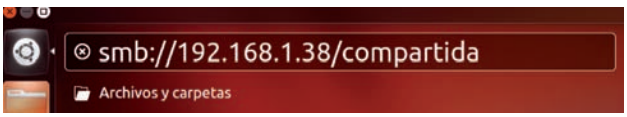


Fig. 4.45. *Conectamos desde Ubuntu Desktop.*

12. Al pulsar la tecla **Enter** aparece el contenido de la carpeta compartida. También podemos hacer lo mismo desde cualquier carpeta entrando en el menú *Ir > Lugar* (Fig. 4.46).

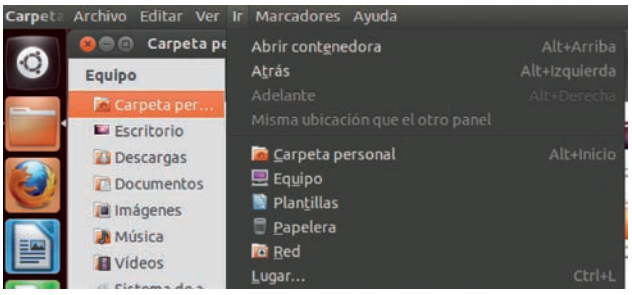


Fig. 4.46. *Conectamos carpetas desde Ubuntu Desktop.*

(Continúa)

Caso práctico 4

(Continuación)

13. En un Ubuntu Server podemos montar directamente la carpeta compartida como un sistema de ficheros. Usaremos el comando `mount.cifs` (Fig. 4.47).

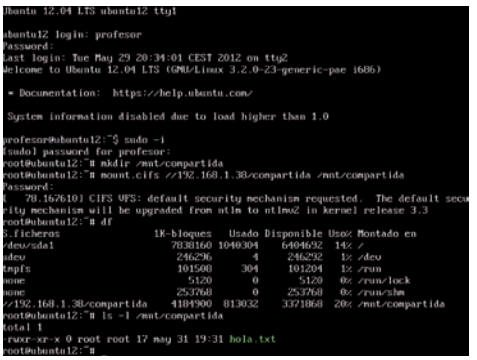


Fig. 4.47. *Conectamos desde Ubuntu Server.*

14. En cuanto a la seguridad, nos interesa poder consultar quién está conectado a nuestro servidor XP. Podemos utilizar *Inicio > Ejecutar > compmgmt.msc > Carpetas compartidas,* o también el comando `netstat -an`. En la Figura 4.48 podemos ver que hay conexiones desde las máquinas 35, 36 y 41 al puerto 445, que es el puerto para compartir ficheros en Windows.



Fig. 4.48. *Conexiones activas en el servidor.*

En el caso práctico 4 hemos visto que un equipo de la red ofrece disco a otros equipos conectados a ella. Es lo que se conoce como **NAS** (Network Attached Storage, almacenamiento conectado a la red). En ese esquema tenemos un equipo con almacenamiento local (una carpeta del escritorio, como hemos visto) que desea ofrecerlo a otros equipos de la red. Este equipo servidor ejecutará un determinado software servidor que responde a un determinado protocolo. Aquel equipo que necesite acceder a esa carpeta compartida, ejecutará un software cliente capaz de interactuar con el servidor de acuerdo con el protocolo del servidor (Fig. 4.49). Como la mayoría de los equipos de usuario son Windows, el protocolo más común es CIFS (Common Internet File System), que es una evolución de SMB (Server Message Block). En el caso práctico 5 probaremos distintos servidores CIFS.

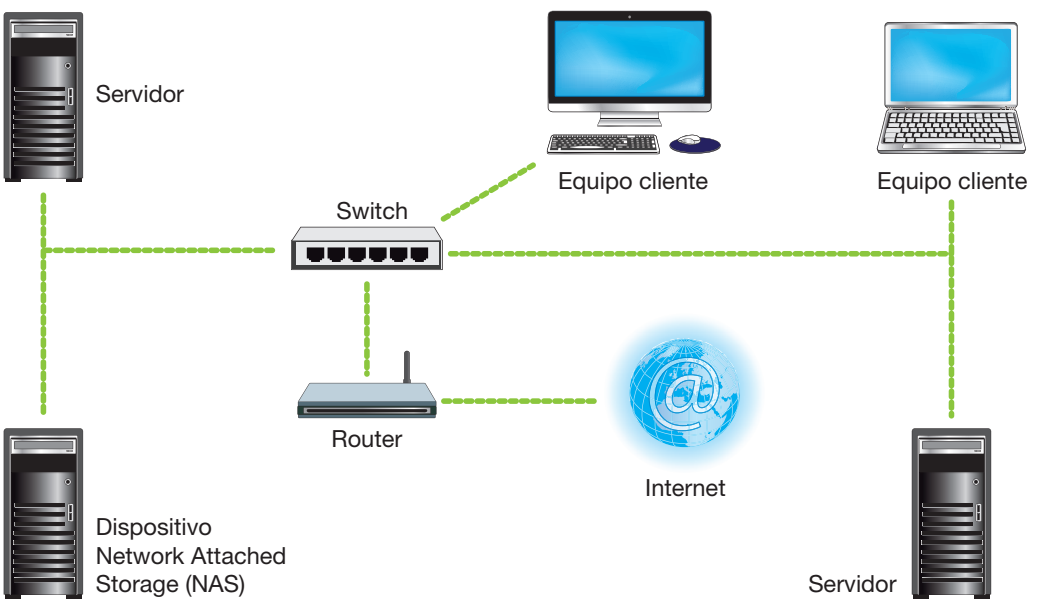


Fig. 4.49. *Solución NAS utilizando protocolos CIFS.*

Actividades

13. En el servidor del caso práctico 4 activa ahora la casilla que permite cambiar los archivos. ¿Qué ocurre?

14. Repite ese caso práctico pero ahora el servidor SMB es un Linux.

En un entorno privado puede ser suficiente con un pequeño equipo que haga de servidor NAS; pero en un entorno empresarial necesitamos mucho más rendimiento y seguridad, por lo que el equipo servidor necesitará potencia de procesamiento, amplia memoria caché, tarjetas de red de alta capacidad y configuraciones RAID. Si otros servidores también lo necesitan, seguramente optaremos por una solución **SAN** (Storage Area Network). En un SAN los discos están en lo que se llama un «armario», donde se realiza la configuración RAID. El armario dispone de cachés de alto rendimiento para reducir los tiempos de operación (Fig. 4.50). Los servidores se conectan al armario mediante conmutadores de fibra óptica (por eso hablamos de network). La configuración de los armarios es flexible: para cada equipo se pueden asignar unos discos concretos y reservarle cierta cantidad de caché. Y cambiarlo cuando sea necesario.

Importante

La solución SAN sirve para cualquier tipo de servidores, no exclusivamente para servidores de disco NAS.

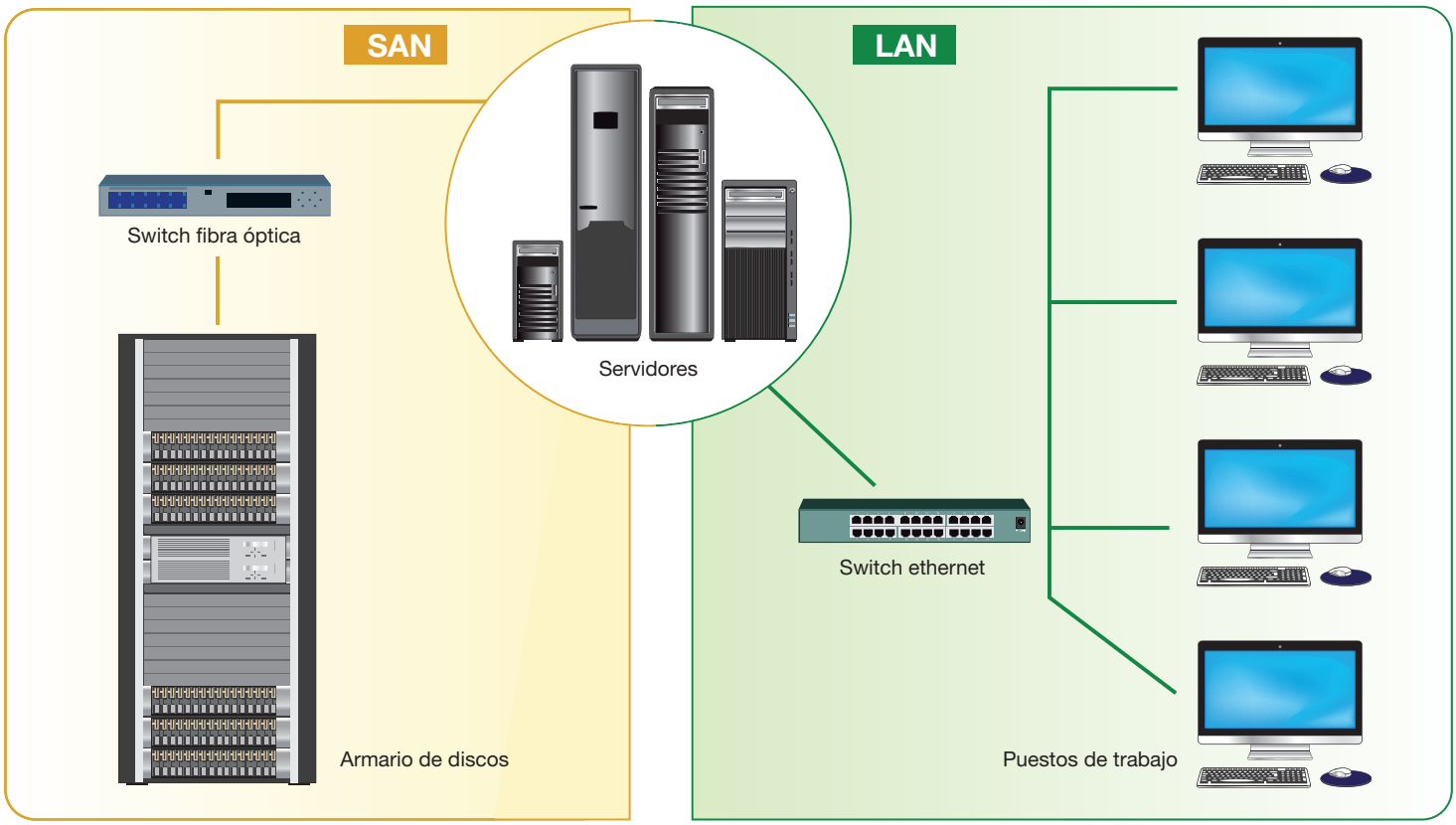


Fig. 4.50. *Solución SAN en un entorno empresarial.*

El almacenamiento compartido es especialmente importante en los clústers. Un **clúster** es un conjunto de máquinas (llamadas nodos) coordinadas para realizar una tarea en común. Puede ser una base de datos, un servidor web, un sistema de gestión de redes, búsqueda de vida extraterrestre (SETI), almacenamiento compartido en Internet (P2P, como eMule, que veremos en el siguiente apartado), etc.

Cada máquina ejecuta una parte de la funcionalidad y está coordinada con el resto de las máquinas. Para ello necesitan un determinado software de clúster instalado en todas ellas y, sobre todo, un almacenamiento fiable y de alto rendimiento, porque los nodos intercambian mucha información.

Actividades

15. Analiza las prestaciones de un equipo SAN.

16. Compara las ventajas y los inconvenientes de utilizar un disco grande o un clúster de discos pequeños.

Vocabulario

SETI (Search for Extraterrestrial Intelligence). Proyecto de investigación espacial que permite contribuir a cualquiera conectado a Internet. Basta descargar su salvapantallas, que además de cumplir su función, analiza información recibida en los radiotelescopios.

P2P (Peer to Peer). Arquitectura distribuida donde todos los nodos ofrecen algo a los demás nodos y necesitan algo de los demás nodos.

Caso práctico 5

NAS en routers domésticos

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

Objetivo. Comprobar que para ofrecer disco en red no es imprescindible un ordenador personal, como el utilizado en el caso práctico 4. Los routers que tenemos en casa ya ofrecen estas funciones.

Material. Router ADSL Livebox, Cisco WRT160NL y cliente Windows.

1. Tenemos un router ADSL Livebox y le pinchamos un pendrive USB. Nos conectamos a su servidor web para entrar como administrador. Generalmente estará en la 192.168.1.1 (Fig. 4.51).

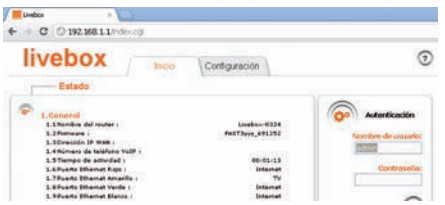


Fig. 4.51. *Login Livebox.*

2. Una vez dentro vamos a la pestaña *Configuración*, donde deberá aparecer nuestro USB. Haciendo clic sobre él accedemos a su configuración (Fig. 4.52).

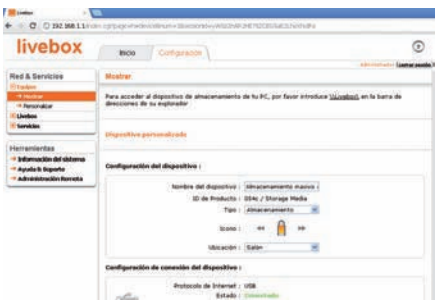


Fig. 4.52. *USB Livebox.*

3. Ya podemos conectarnos desde cualquier ordenador. Por ejemplo, en un XP vamos a *Inicio* > *MiPC* y en la barra de direcciones ponemos \\Livebox o bien \\192.168.1.1 (Fig. 4.53).



Fig. 4.53. *Disco en red Livebox.*

4. En este caso, cualquier equipo que se conecte al router podría leer y escribir en ese disco. Esto puede ser aceptable en un entorno doméstico, pero no en una empresa.

5. Otros routers sí permiten establecer permisos. Por ejemplo, el Cisco WRT160NL. Pinchamos nuestro USB en el router Cisco. Entramos al servidor HTTP (suele estar en la dirección 192.168.1.1) y nos presentamos como administradores.

6. Una vez dentro, vamos a la pestaña *Storage* (Fig. 4.54).



Fig. 4.54. *USB Cisco.*

7. Para compartirlo pulsamos en el botón *Create share*. Aparece un formulario donde daremos nombre al disco en red y elegiremos qué carpeta del USB queremos ofrecer (Fig. 4.55).



Fig. 4.55. *Compartimos en Cisco.*

8. Debajo de la carpeta podemos elegir quién puede hacer qué sobre esa carpeta. En general los admin podrán leer y escribir y los guest solo leer.

9. Cuando hemos terminado la configuración, esa carpeta está disponible para otros equipos. Por ejemplo, un XP podría localizarla con \\wrt160nl (Fig. 4.56).



Fig. 4.56. *Disco en red Cisco.*

10. Nos pedirá usuario y contraseña. Si entramos con admin, podremos navegar por las carpetas, leer los ficheros y modificarlos y crear nuevos ficheros y carpetas; con guest, solo navegar por las carpetas y leer los ficheros.

1.3. Almacenamiento en la nube y P2P

Supongamos que nuestra empresa ya tiene en sus instalaciones NAS (disco en red) y SAN (discos de alto rendimiento, capacidad y seguridad). Pero hay más necesidades:

- Queremos colgar ficheros para nuestros clientes y proveedores.
- Cuando estamos fuera de la oficina podemos necesitar algún fichero (un presupuesto, un contrato).
- Vamos a continuar en casa un trabajo que tenemos a medias.
- Simplemente queremos una copia de unos documentos importantes en otro lugar que no sea la oficina.

Para un empleado, una solución simple es guardarlo todo en un pendrive USB. Pero se pierden con demasiada facilidad (y la información que va puede ser muy importante: conviene haberla cifrado) y además no podríamos trabajar simultáneamente con otros compañeros (aunque cada uno lleve su pendrive, los siguientes cambios no estarían sincronizados).

La solución habitual era abrir un acceso directo desde Internet hasta los discos de la empresa. Funciona, aunque es delicado, porque al final es una «puerta trasera» por donde pueden intentar entrar hackers, y llegar hasta esos discos o cualquier otro servidor nuestro.

Como alternativa, en los últimos años han aparecido multitud de servicios de almacenamiento en la nube:

- La primera generación (Megaupload, FileServe, etc.) consiste en que un usuario sube un fichero a una web para que lo descarguen otros usuarios conectados a esa web. Pero resulta incómodo, primero porque solo almacena ficheros, sin una estructura de carpetas; y, segundo, porque si queremos todos los ficheros de una carpeta, hay que ir uno por uno, o comprimirlos en un zip y subirlo.
- La segunda generación (Dropbox, iCloud, Box.net, Skydrive, GoogleDrive) es más simple: directamente sincronizan carpetas de los dispositivos (ordenador personal, móvil, tableta) entre sí y con los servidores del proveedor (Fig. 4.57). Cualquier cambio que hagas en cualquier dispositivo automáticamente ocurre en los demás dispositivos y en el disco del proveedor, sin necesidad de acordarse de conectar a una web y hacer la descarga (aunque también está disponible).



Fig. 4.57. *Almacenamiento en la nube.*

Vocabulario

Puerta trasera. Mecanismo que da acceso a un sistema y que es desconocido por los administradores de dicho sistema.

Actividades

17. Investiga y discute en clase sobre el cierre de Megaupload.

18. Busca un servicio de almacenamiento en la nube para servidores.

19. Investiga las diferencias entre las arquitecturas de Pando y Akamai.

Todos estos servicios tienen ventajas e inconvenientes:

- Nuestros datos están fuera de nuestras instalaciones, por lo que podemos acceder a ellos a cualquier hora, sin estar allí, y con la tranquilidad de que cualquier desastre que ocurra en la oficina no les afectará.
- La empresa proveedora del servicio de almacenamiento en la nube se preocupa por hacer copias de seguridad de los datos que subimos; incluso suelen conservar versiones anteriores de cada fichero que modificamos.
- La conectividad a Internet de estas empresas suele ser muy superior a la nuestra, por lo que el acceso es rápido. Y al mismo tiempo no ocupamos ancho de banda de nuestra conexión.
- Sin embargo, perdemos el control sobre el acceso a nuestra información. Tenemos que confiar en la capacidad técnica y humana del proveedor de almacenamiento en la nube para evitar ataques sobre sus servidores (de nuevo, conviene cifrar los archivos que subimos a la nube). Y confiar también en que no incurre en prácticas delictivas, como el caso Megaupload, que cierra el servicio a todos los clientes, inocentes o no.

Las soluciones **P2P** (peer to peer) están muy extendidas entre particulares (eMule, Torrent); las empresas no suelen recurrir a ellas para información confidencial porque, si en almacenamiento en la nube teníamos que desconfiar de un proveedor, en P2P son miles. Pero sí son interesantes para difusión de contenidos, como hace PandoNetworks.

Caso práctico 6

Almacenamiento en la nube mediante Dropbox

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

Objetivo. Abrir una cuenta en Dropbox e instalar el cliente en varios dispositivos, para comprobar que las carpetas se sincronizan entre sí y con la web.

Materiales: Windows 7 y tableta Android.

1. En el Windows 7 descargamos el software cliente desde **www.dropbox.com** y lo instalamos.
2. Durante la instalación nos preguntará si ya tenemos una cuenta. Como no es así, la creamos en el momento. Nos pedirá un nombre, una dirección de correo, una contraseña y un identificador para la máquina en la que estamos instalando (Fig. 4.58).

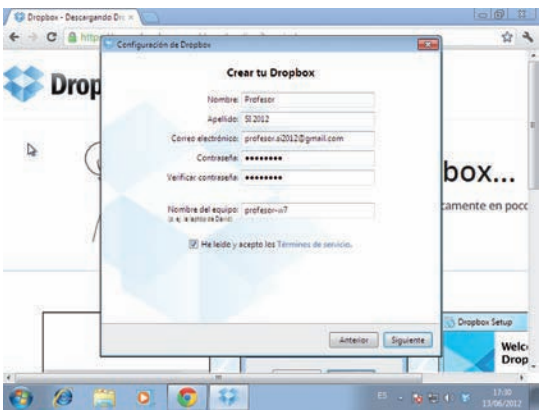


Fig. 4.58. *Nueva cuenta en Dropbox.*

3. Después nos pregunta cuánto disco queremos utilizar (para esta prueba, nos quedamos con los 2 GB gratuitos) y qué configuración queremos. Aquí elegiremos la opción típica, que crea una carpeta Dropbox en el directorio del usuario (Fig. 4.59).

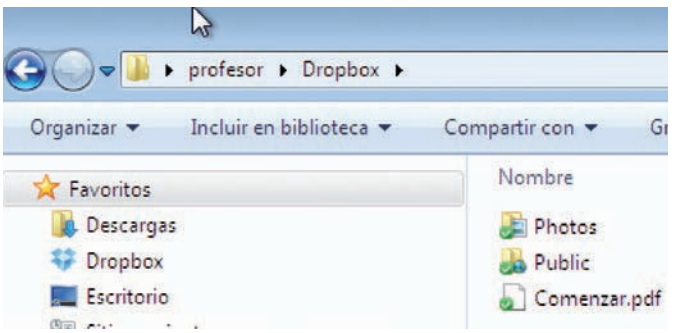


Fig. 4.59. *Carpeta local.*

4. Vamos a crear un documento en esa carpeta. Si nos fijamos, las carpetas y ficheros de esta carpeta tienen un icono en la esquina inferior izquierda. Si está en verde, significa que el fichero ha subido al servidor de Dropbox; si está en azul, significa que todavía está subiendo.
5. Una vez creado, comprobamos que está en la web. Desde el navegador entramos en **www.dropbox.com** y en *Iniciar sesión*. Nos pide nuestro usuario (que es el correo electrónico que pusimos al crear la cuenta en el paso 2) y la contraseña.

(Continúa)

Caso práctico 6

(Continuación)

6. Nos aparecerá un asistente para aumentar nuestra capacidad, pero vamos a la opción *Dropbox* del menú de la izquierda. Al pulsar sobre ella aparece el mismo contenido de la carpeta del ordenador (Fig. 4.60).

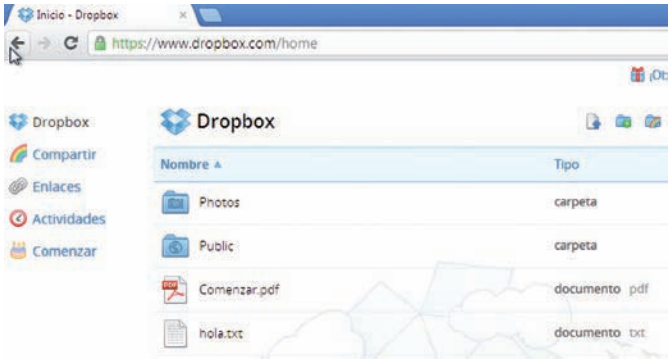


Fig. 4.60. *Carpeta en la web de Dropbox.*

7. Por tanto, tenemos nuestros archivos accesibles desde Internet. Cualquier cambio que hagamos en una parte (ordenador o web), se actualiza en la otra. Por ejemplo, vamos a crear una carpeta en la web pulsando en el icono *Carpeta nueva* y comprobamos que aparece en el disco (Fig. 4.61).



Fig. 4.61. *Nueva carpeta en local.*

8. Ahora vamos a una tableta Android e instalamos el Dropbox desde Google Play Store. En el proceso de instalación, cuando nos pregunte si tenemos cuenta, le daremos la que hemos creado en el paso 2. Si todo va bien, tendremos acceso a la misma carpeta (Fig. 4.62).



Fig. 4.62. *Dropbox en tableta Android.*

9. Sin embargo, hay una diferencia. Dadas las limitaciones de capacidad y autonomía de los móviles y las tabletas, por defecto no se sincronizan todos los ficheros, sino solo los que has abierto hasta entonces. Internamente se guardan en una carpeta scratch (Fig. 4.63).

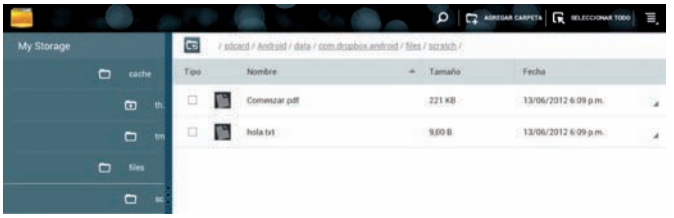


Fig. 4.63. *Almacenamiento interno en Android.*

10. Publicar un fichero o una carpeta en Internet es tan sencillo como entrar en la web con nuestro usuario, seleccionar el elemento y pulsar en *Obtener el enlace* (Fig. 4.64). La URL que aparece la podemos difundir por cualquier medio (correo electrónico, Twitter, perfil) para que cualquiera vea nuestros archivos; aunque para poder modificarlos hay que elegir *Compartir carpeta* y solo funcionará entre usuarios Dropbox.

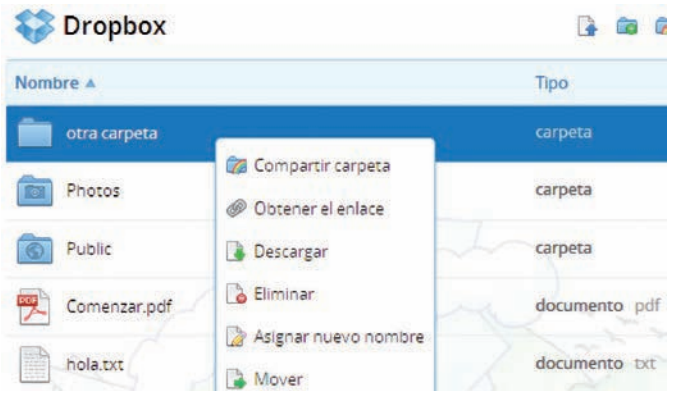


Fig. 4.64. *Compartir ficheros y carpetas.*

2. Backup de datos

Ni el RAID 1 ni el RAID 5 nos permiten dormir tranquilos. Estamos protegidos ante el fallo de uno de los discos, pero no si fallan dos. O si se incendia la sala y arde el servidor. O si alguien accede a la máquina y la formatea.

Podemos ver el RAID como una forma de seguir funcionando, aunque haya fallecido uno de los discos. Pero nuestros datos son más importantes y hay que seguir protegiéndolos. Por eso haremos copias y las llevaremos lo más lejos posible.

- Primero vamos a distinguir entre:
  - **Backup de datos.** Copia de seguridad de los datos del usuario o empresa que están almacenados en un ordenador.
  - **Imagen del sistema.** Copia de seguridad de los programas (sistema operativo y aplicaciones) que están instalados en un ordenador.

Normalmente se hace una imagen del sistema justo después de instalarlo y configurarlo, o después de la instalación de una aplicación importante. En cambio, el backup de datos hay que hacerlo diariamente, incluso con más frecuencia, dependiendo de la actividad de la empresa.

- El segundo paso es identificar los datos que tenemos que salvar. Aquí tenemos que distinguir entre:
  - **Ficheros.** Pueden ser unidades enteras, la típica carpeta Mis Documentos, etc. Existe la complicación de detectar los ficheros que están siendo modificados precisamente cuando se ha lanzado la copia.
  - **Sistemas complejos,** como las bases de datos, donde la concurrencia de cambios suele ser mucho más alta que con ficheros, porque una operación afecta a varias tablas. Por este motivo, los servidores de base de datos tienen sus propios mecanismos de exportación del contenido de las tablas.
- Finalmente, para cada tipo de información identificada en el paso anterior, hay que **acordar la frecuencia** de respaldo. En un supermercado, para la base de datos de empleados puede ser suficiente efectuar una copia diaria o semanal; pero la base de datos de ventas no puede esperar tanto.

Actividades

20. Por tranquilidad, podríamos hacer imagen del sistema todos los días, porque ahí van los programas y los datos. ¿Es recomendable?

21. Además de hacer backup regularmente, también hay que probar a recuperarlo regularmente. ¿Por qué?



Fig. 4.65. *Dispositivo LTO.*

2.1. Tipos de dispositivos locales y remotos. Robot de cintas

Una vez hemos confirmado qué información del disco duro queremos conservar y con qué frecuencia, hay que decidir dónde hacemos la copia: soporte físico y ubicación de este soporte físico. En cuanto al soporte físico, podemos pensar en:

- Usar **otra partición** del mismo disco duro. No es buena idea, porque si falla el disco, lo perdemos todo. Por cierto, esta es la solución de los ordenadores personales para evitar entregar DVD de instalación del sistema operativo.
- Usar **otro disco** de esa máquina; pero si se destruye la máquina, lo perdemos todo.
- Pasarlo a un disco duro extraíble para llevárnoslo, o quizá el disco duro de otra máquina al que accedemos por FTP. Sería aceptable, pero los discos duros son relativamente caros; por lo menos, mucho más que otras tecnologías de almacenamiento, como las cintas o los discos ópticos (CD/DVD/BR), que además son fáciles de transportar y realmente no necesitamos las elevadas prestaciones de un disco duro (no vamos a estar leyendo y escribiendo continuamente; solo durante la copia).
- Si podemos elegir entre cintas y discos, **mejor las cintas** porque tienen más capacidad y son más fiables y reutilizables. Las cintas más usadas son las LTO (Linear Tape-Open, Fig. 4.66).



Fig. 4.66. *Cartucho LTO.*

En cualquier caso, y sobre todo si vamos a utilizar soportes extraíbles, que se pueden extraviar, debemos preocuparnos por **cifrar el contenido.** Esto ya lo hace la mayoría de los programas de backup, incluso se puede hacer en el hardware, en el dispositivo de escritura.

La facilidad de extraer un soporte y poner otro es vital. Primero porque evitamos estar siempre utilizando el mismo elemento, lo que acelera su deterioro, y sobre todo porque las copias de seguridad, si podemos, hay que conservarlas lo más alejadas posible del disco copiado, para evitar que un desastre en la sala de ordenadores también termine con las copias. Por ello:

- Si nuestra empresa tiene dos sedes, conviene que las cintas de una sede se intercambien con las cintas de la otra por mensajería.
- Si solo hay un edificio, en la parte opuesta al CPD.
- Deben estar siempre en una sala con control de acceso, para evitar que cualquiera llegue hasta nuestros datos.
- Dentro de la sala, hay que meterlas en un armario ignífugo.

Una vez elegido el soporte, hay que decidir dónde ponerlo. Podríamos comprar uno para cada servidor como dispositivo local (Fig. 4.65), pero resulta caro y laborioso, dado que vamos a utilizar varias cintas (por ejemplo, una para cada día de la semana) y alguien debería ir máquina por máquina cambiando las cintas, y etiquetando perfectamente de qué máquina son y a qué día corresponden.

Interesa centralizar estas tareas repetitivas y que las hagan máquinas, no personas. En las empresas se suele instalar una librería de cintas (robot de cintas), donde se hace el backup de todos los servidores de la empresa y también aquellos puestos de trabajo que lo necesiten. Cada cinta está etiquetada y el robot mantiene una base de datos donde registra qué cinta utilizó en cada momento. Las etiquetas suelen ser códigos de barras y también RFID.

Este dispositivo remoto está conectado a la LAN de la empresa o directamente a los servidores mediante SAN. Ejecuta un software servidor que conecta con un software cliente instalado en cada equipo seleccionado. Normalmente, la red que utiliza es una LAN o VLAN distinta a la LAN de trabajo (los ordenadores con función de servidor suelen llevar dos interfaces de red). Al utilizar una LAN diferente, la actividad de la empresa no se ve afectada por el tráfico de backup, y viceversa (Fig. 4.67).

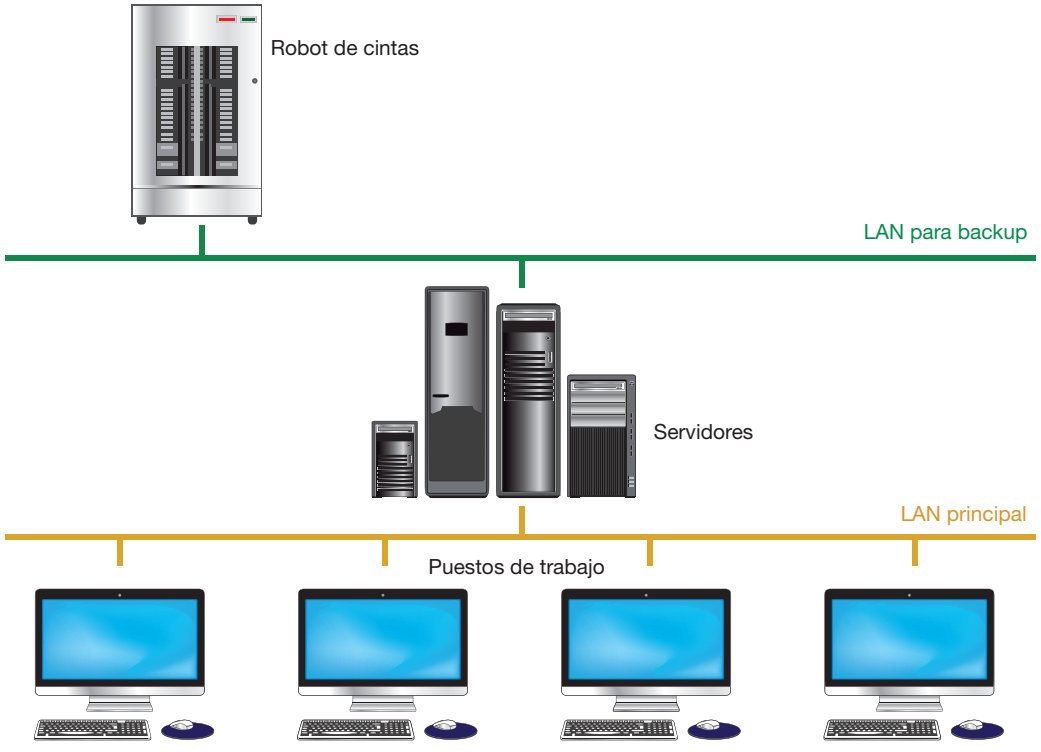


Fig. 4.67. *Funcionamiento de una LAN exclusiva para backup.*

Actividades

22. Busca precios y características de cartuchos de cinta, junto con sus grabadores.

23. Busca precios y características de librerías de cintas.

Vocabulario

RFID. Tecnología de identificación a distancia mediante radiofrecuencia, muy utilizada en tarjetas y etiquetas. La principal aportación es que no necesita alimentación eléctrica, porque cuando un aparato le pregunta, puede contestar aprovechando la energía de las ondas donde recibió la pregunta.

Vocabulario

Copia consistente. Mientras se hace la copia, el sistema sigue funcionando. Esto es importante porque se pueden introducir inconsistencias en la copia: en una operación que afecta a dos ficheros, puede ocurrir que en la cinta se guarde uno actualizado y el otro no. Las bases de datos son especialmente sensibles a la copia consistente y proporcionan mecanismos específicos orientados a conseguirla.

2.2. Tipos de copias

Como hemos visto antes, cada empresa debe identificar qué datos quiere proteger mediante copia de seguridad. Hay tres tipos de copia:

- **Completa.** Incluye toda la información identificada. Si era una unidad de disco, todos los archivos y carpetas que contiene; si era una base de datos, la exportación de todas sus tablas.
- **Diferencial.** Incluye toda la información que ha cambiado desde la última vez que se hizo una copia de seguridad completa. Por ejemplo, si el lunes se hizo una completa y el martes solo ha cambiado el fichero a.txt, en la cinta del martes solo se escribe ese fichero. Si el miércoles solo ha cambiado el fichero b.doc, en la cinta del miércoles se escribirán a.txt y b.doc.
- **Incremental.** Incluye toda la información que ha cambiado desde la última copia de seguridad, sea completa o incremental. En el ejemplo anterior, la cinta del martes llevará el fichero a.txt, pero la cinta del miércoles solo b.doc.

Una empresa podría decidir hacer todos los días copia completa. Pero, si hay muchos datos, es un proceso lento y algo arriesgado, porque hay que vigilar que se esté haciendo una **copia consistente** de la información (mientras se hace la copia, el sistema sigue funcionando y en cualquier momento alguien puede introducir cambios). Con la copia diferencial o incremental tenemos las mismas garantías, porque recuperamos la información aplicando la última cinta completa y la última diferencial (o la última completa y todas las incrementales).

En una empresa mediana es habitual el esquema de diez cintas:

- Una para un backup completo (los viernes).
- Cuatro para un backup parcial diario (diferencial o incremental) de lunes a jueves.
- Cinco para backups completos anteriores: quincenal, mensual, trimestral, semestral y anual.

Elegir entre diferencial o incremental para el backup diario depende de cada empresa. Si hay poca actividad diaria, se puede permitir el diferencial, porque aporta la ventaja de que cada cinta diaria tiene toda la información necesaria para recuperar ese día (en el incremental, si perdemos la cinta de un día, puede que tenga ficheros que no estén en las cintas siguientes). Pero si hay mucha actividad, estamos de nuevo ante el problema de mantener la consistencia de la copia.

2.3. Copia y recuperación en Windows y Linux

Vamos a practicar la copia y recuperación de datos en los sistemas habituales: Windows y Linux.

Caso práctico 7

Backup en Windows

Duración: 20 minutos **Dificultad**: Fácil

Objetivo. Utilizar un programa de backup para probar los tipos de copia completa e incremental.

Material. Windows 7, XP y Lynux Ubuntu.

Vamos a utilizar el programa Backup4all para hacer copias de seguridad locales y remotas, completas y parciales. Para las copias remotas utilizaremos un servidor FTP en un Linux Ubuntu.

1. Instalamos en un Windows 7 la herramienta Backup4all, que descargamos de su página oficial. Elegiremos la versión Professional, que nos permite hacer copias parciales. En el proceso de instalación elegiremos la configuración típica. Si todo ha ido bien, al arrancar aparecerá un asistente (Fig. 4.68).

(Continúa)

Caso práctico 7

(Continuación)

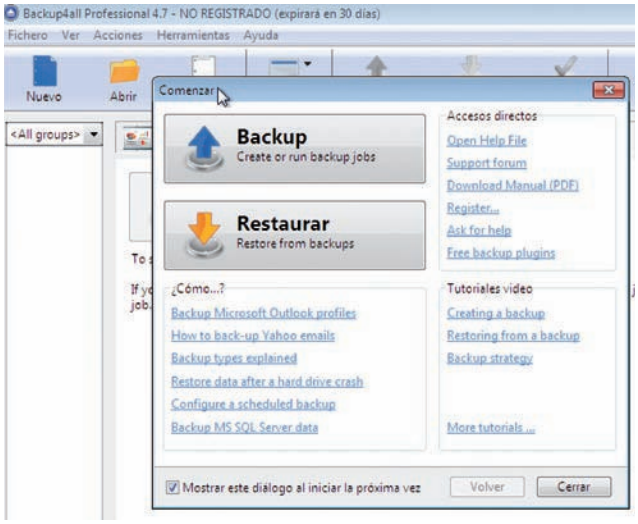


Fig. 4.68. *Asistente Backup4all.*

2. El asistente nos ofrece crear una tarea de backup o restaurar un backup anterior. En esta misma ventana nos propone enlaces a documentación sobre temas avanzados; por ejemplo, hacer backup de una base de datos SQLServer.

3. Como es la primera vez que lo usamos, pulsaremos en *Crear una tarea.* A continuación nos pedirá un nombre para la tarea, que debe ser explicativo de qué estamos guardando, para cuando haya que recuperarlo. También nos pregunta dónde dejaremos la copia. Como hemos visto antes, puede ser local (disco de nuestra máquina) o remoto (disco en red o un servidor FTP/SFTP). Para nuestra prueba sencilla elegiremos local en una carpeta de Documentos de nuestro usuario (Fig. 4.69).

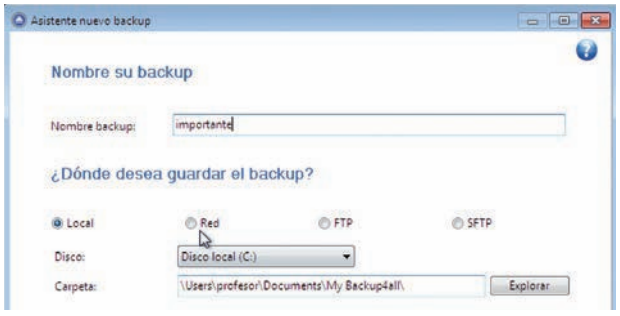


Fig. 4.69. *Características del backup.*

4. El siguiente paso es elegir qué queremos salvaguardar. El desplegable ofrece objetos típicos, como el archivo de correo de Outlook; en nuestro caso elegiremos una carpeta llamada top secret (Fig. 4.70). Si nos fijamos en el lado derecho, el programa permite filtrar ficheros temporales o los ficheros de hibernación y paginación de Windows (no tiene sentido copiarlos).

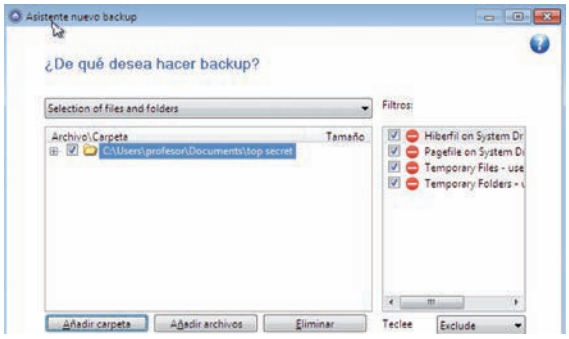


Fig. 4.70. *Carpetas para backup.*

5. A continuación podemos elegir cuándo queremos hacer el backup (Fig. 4.71). Para una prueba elegiremos la ejecución manual, pero los backups solo tienen sentido si se hacen regularmente.



Fig. 4.71. *Frecuencia del backup.*

6. Finalmente nos deja elegir el tipo de backup, como ya hemos visto: completo (full), diferencial o incremental (Fig. 4.72). También nos permite encriptar con una contraseña.



Fig. 4.72. *Tipo de backup.*

(Continúa)

Caso práctico 7

(Continuación)

7. Hemos terminado. La tarea ha quedado creada (Fig. 4.73). Ahora podemos editar, ejecutar inmediatamente o de manera programada. En la información relevante aparece cuándo se hizo el último backup, cómo terminó (éxito/fracaso) y cuándo es el siguiente. Como hemos elegido ejecución manual, no aparece ninguna fecha.

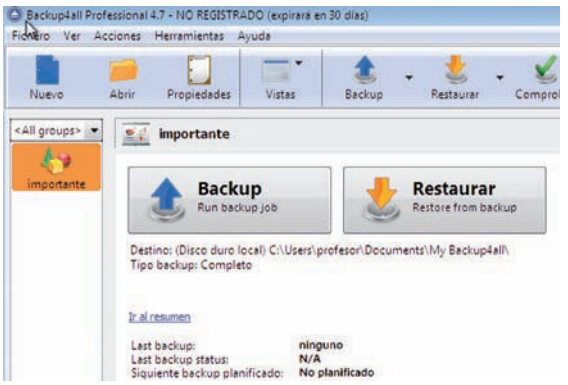


Fig. 4.73. *Tarea de backup creada.*

8. Lanzamos una ejecución pulsando en *Backup Run backup job*. Si todo ha ido bien, como hemos elegido destino local, dentro de la carpeta *Mis documentos* > *My Backup4all* tendremos una carpeta llamada importante (el nombre de la tarea) y dentro de ella hay un fichero 1_C.zip. Si queremos llevar este backup a un dispositivo extraíble, habría que copiar esa carpeta (la carpeta completa, porque hay más ficheros con la configuración de la tarea). El fichero .zip tiene exactamente los ficheros guardados, con todas las carpetas necesarias (Fig. 4.74).

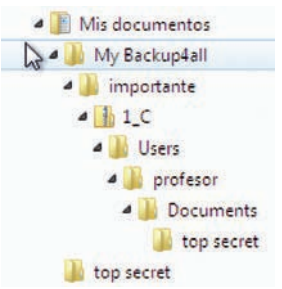


Fig. 4.74. *Backup ejecutado.*

9. Ahora vamos a editar nuestra tarea para cambiar el destino. Ya no será local, sino una unidad de red. Como aprendimos en el caso práctico 4, en una máquina XP creamos un usuario de tipo administrador llamado backup y le ponemos contraseña. Entramos con ese usuario y creamos una carpeta en el escritorio llamada backup remoto. A continuación la compartimos y activamos que se pueda escribir en ella.

10. Volvemos a nuestro W7, y en las propiedades de la tarea ponemos destino Red. Nos pedirá la ruta UNC (IP del XP más backup remoto) y el usuario (backup) y la contraseña. Pulsamos en *Comprobar conexión* de red para confirmar que está todo bien (Fig. 4.75).

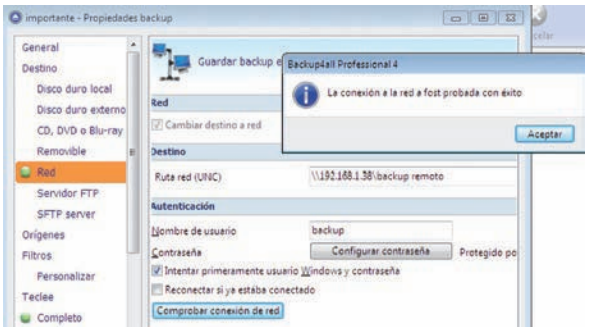


Fig. 4.75. *Backup a unidad compartida.*

11. Con la nueva configuración de la tarea podemos volver a lanzar el backup. Si todo va bien, de nuevo se habrá creado una carpeta llamada importante que contiene el fichero 1_C.zip (Fig. 4.76).

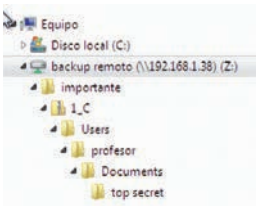


Fig. 4.76. *Comprobamos backup a unidad compartida.*

12. Para probar el backup incremental crearemos una tarea nueva. La configuraremos igual que la anterior; solo que al elegir el tipo de backup ahora marcamos *Incremental*. Lanzamos una primera ejecución (Fig. 4.77) y podemos comprobar que se ha creado la carpeta nueva y dentro tiene el fichero 1_C.zip con el mismo contenido que el backup completo, como era de esperar (no hay backup anterior para comparar).

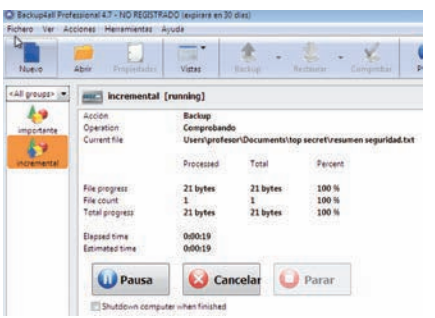


Fig. 4.77. *Backup en acción.*

(Continúa)

Caso práctico 7

(Continuación)

13. Si ahora creamos en top secret un fichero nuevo llamado resumen seguridad.txt y ejecutamos de nuevo el backup, podemos comprobar que aparece un fichero 2_C.zip con la estructura de directorios pero solo el nuevo fichero (Fig. 4.78).

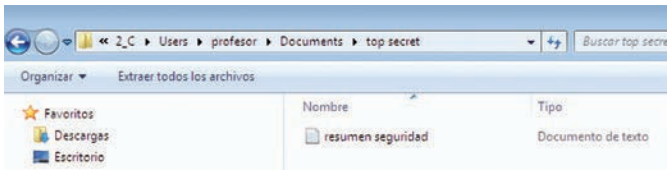


Fig. 4.78. *Backup incremental.*

14. Una vez que entendemos en qué consiste el backup, podemos probar las posibilidades de ejecución programada, que son las realmente interesantes para la empresa. Si en las propiedades de la tarea vamos a Planificador, nos aparecerá la lista de planificaciones (podemos tener más de una, como hemos visto en el esquema de diez cintas). El programa nos permite elegir entre el planificador de tareas de Windows o uno interno del propio Backup4all. En la pestaña *Configuración* podemos ajustar la ejecución (Fig. 4.79) porque, como no vamos a estar delante cada día que se ejecute, hay que decidir qué hacer si el backup tarda demasiado, si el equipo está funcionando con baterías, etc.

15. Finalmente, podemos consultar las opciones avanzadas del backup (Fig. 4.80). La más importante es asociar la ejecución de un script antes y después del backup. En el punto 2 de este caso práctico vimos que el programa ofrecía enlaces a información sobre cómo hacer backup de una base de datos SQL Server. Si consultamos esa página, veremos que proporciona dos scripts: uno para parar la base de datos (lo lanzaríamos antes del backup), y otro para arrancarla después del backup. Por tanto, durante la copia, la base de datos no estará disponible, por lo que la empresa debe estudiar alternativas (base de datos de un centro de respaldo, hacer siempre rápidos backups incrementales, etc.).

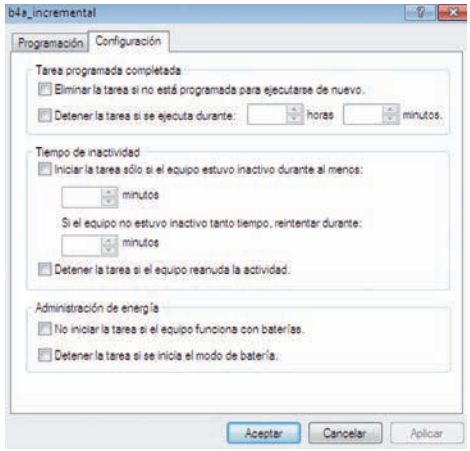


Fig. 4.79. *Backup programado.*

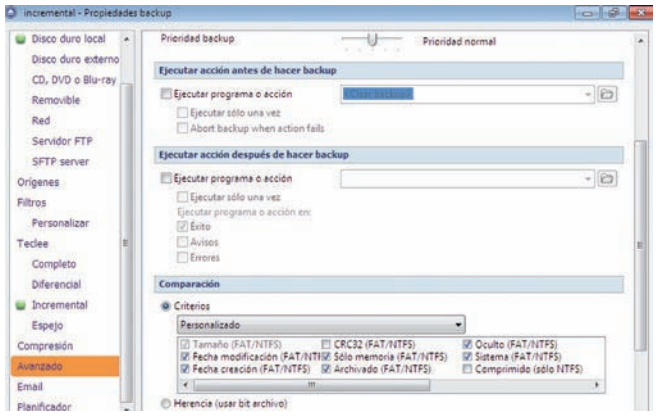


Fig. 4.80. *Opciones avanzadas de backup.*

Actividades

24. Mediante la herramienta Backup4all, crea un backup incremental programado para los próximos cinco minutos, ejecutándose una vez al minuto. En ese tiempo crea manualmente más ficheros. Al final de la ejecución comprueba los ficheros .zip creados.

25. Repite la actividad 21, pero con backup diferencial. Comprueba que los ficheros .zip tienen distinto contenido que en la actividad anterior.

26. Mediante la herramienta Backup4all, prueba un backup completo cifrado. Intenta abrir el fichero .zip creado.

27. Investiga cómo saben las herramientas de backup si un fichero ha cambiado, para decidir incluirlo en un backup parcial.

Caso práctico 8

Backup en Linux

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

Objetivo. Hacer backup mediante comandos.

Material. Servidor Ubuntu 12.04.

Para Linux vamos a probar la herramienta rsync. Es una herramienta sencilla pero muy potente. Básicamente nos permite sincronizar directorios en una misma máquina o entre dos máquinas.

1. Entramos en nuestro Ubuntu Server 12.04 y nos ponemos en modo super-usuario con `sudo -i`.
2. Nos vamos al `/tmp` y creamos un directorio llamado `original` con un fichero `hola.txt`.
3. Ahora creamos una copia de `original` mediante el comando:

   ```
   # rsync -av /tmp/original /tmp/copia
   ```

   Como se ve en la Figura 4.81, la herramienta nos avisa de que va a crear el directorio `/tmp/copia` (no lo habíamos creado) y muestra los ficheros que ha traspasado y un resumen de bytes transferidos. El directorio `copia` reproduce la estructura de carpetas de `original`, no solo los ficheros.

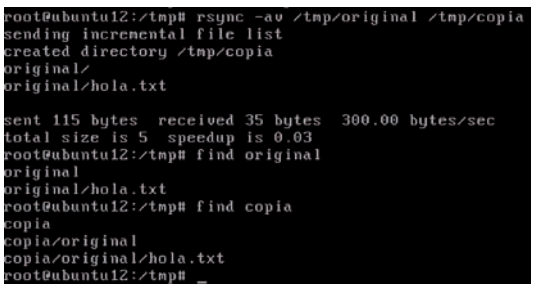


Fig. 4.81. *rsync de directorios.*

4. ¿En qué se diferencia de hacer una copia normal mediante cp? Pues en que rsync no copia todo, sino solo los ficheros nuevos o los que han cambiado. Por ejemplo, creamos un fichero nuevo y sincronizamos. Solo se traspasa ese fichero (Fig. 4.82).

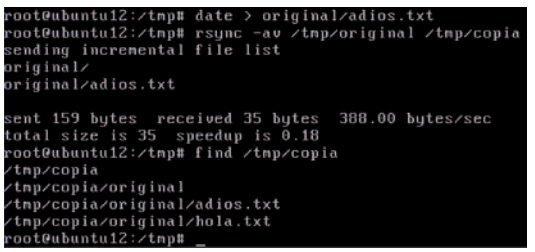


Fig. 4.82. *Solo copiamos los cambios.*

5. Si hemos borrado un fichero en el original y queremos que se actualice la copia, hay que incluir el parámetro `--delete`.
6. Con lo que hemos visto hasta ahora solo podemos hacer backups completos. El directorio `copia` lo podemos llevar a cualquier dispositivo extraíble o podría ser un disco en red. Para hacer backups incrementales ejecutaremos esto:

   ```
   # rsync --avvb --delete --backup dir=/tmp/
   backup1 /tmp/original /tmp/copia
   ```

   Esta vez la sincronización deja en el directorio `/tmp/backup1` los ficheros que resultan modificados o eliminados; en `/tmp/copia` siempre está la versión actual. En nuestro ejemplo vamos a borrar el fichero `adios.txt` y al sincronizar vemos que ya no está en `original` ni en `copia`, pero sí en `backup1` (Fig. 4.83).

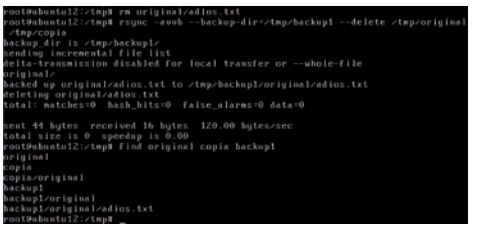


Fig. 4.83. *Backup incremental.*

7. Lo mismo ocurre para ficheros modificados. Vamos a crear un fichero en `original`, sincronizamos, modificamos ese fichero y al volver a sincronizar, además de actualizar `copia`, se guarda la versión anterior en `backup1`.
8. Finalmente, como es imprescindible que el backup se ejecute con regularidad, vamos a probar a meterlo en el cron. Le pondremos que se ejecute cada minuto (lo normal sería una vez al día), y en ese tiempo haremos cambios para comprobar el funcionamiento.

   Como se ve en la Figura 4.84, hemos creado un script `mibackup.sh` que se invoca desde el cron. Para distinguir las distintas copias incrementales, el script utiliza la fecha en que se ejecuta. Dejamos un log para comprobar diariamente que todo ha ido bien.

   ```
   # cat mibackup.sh
   FECHA=`date +%y%m%d%H%M`
   rsync -avvb --backup-dir=/tmp/backup _
   $FECHA --delete
   /tmp/original /tmp/copia >> /tmp/log _
   $FECHA
   # crontab -l
   # m h dom mon dow command
   * * * * * /tmp/mibackup.sh
   ```

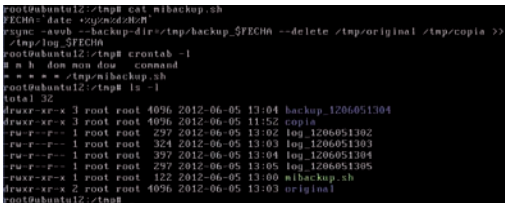


Fig. 4.84. *Backup incremental programado.*

3. Imagen del sistema

La imagen del sistema no es tan importante como los datos, porque en último extremo podríamos instalar desde cero, con el CD/DVD del sistema operativo y las aplicaciones necesarias, y después aplicaríamos a ambos las opciones de configuración que tenemos documentadas. Pero este proceso es lento y generalmente necesita que un técnico esté presente (y también se puede equivocar); una imagen nos ayudará a recuperar el sistema rápidamente y sin errores.

La imagen de un sistema es un **volcado del contenido del disco duro.** Con todo: ejecutables y datos del sistema operativo, ejecutables y datos de las aplicaciones instaladas y datos personales de los usuarios. Generalmente se comprime en un único fichero que ocupa muchos gigabytes, dependiendo del tamaño del disco, la ocupación y el tipo de contenidos. Ese fichero suele estar cifrado y se almacena lejos del sistema original, como hacemos con las cintas del backup.

Como hemos explicado antes, la imagen no es un método adecuado de hacer copias de seguridad en una empresa. Es cierto que copiamos todo, programas y datos, pero es un proceso lento durante el cual el sistema no está operativo, lo que es incompatible con la misión crítica que la informática desempeña en una empresa.

Vocabulario

LiveCD. Es un almacenamiento extraíble (CD/DVD/USB) que contiene un sistema operativo configurado de tal manera que puede funcionar inmediatamente, sin pasar por una instalación previa en el disco duro de la máquina. Se suele utilizar para probar ese sistema antes de tomar la decisión de adquirirlo. En algunas ocasiones, el LiveCD consiste en un sistema operativo que acompaña a una aplicación concreta, como un antivirus, que también está lista para ejecutar sin instalación.

3.1. Creación y recuperación. LiveCD

Existen varias herramientas en los distintos sistemas operativos para crear y recuperar imágenes (Norton Ghost, Acronis True Image), pero presentan el inconveniente de ser formatos propietarios, de manera que para recuperarlas necesitas el mismo programa (incluso la misma versión), lo cual puede ser un problema en determinadas circunstancias.

Nosotros vamos a estudiar una solución sencilla y genérica, disponible para cualquier plataforma hardware habitual. Consiste en la utilización de un LiveCD Linux, con el cual arrancaremos el ordenador cuyo disco queremos clonar. Una vez dentro, elegiremos el dispositivo local o remoto donde almacenar la imagen (generalmente, un disco USB) y procederemos a ejecutar la copia.

Por supuesto, una solución alternativa es apagar el ordenador, extraer el disco duro, pincharlo en otro ordenador y hacer la copia allí. El LiveCD nos ahorra esas manipulaciones.

Las **ventajas** del LiveCD son:

- Es una solución válida para clonar sistemas Windows o Linux en cualquiera de sus versiones, porque trabajamos directamente con el disco, sin importar qué hay dentro.
- Es una solución válida para cualquier hardware convencional, porque Linux funciona en casi todas las plataformas.
- Es una solución interoperable: el formato del fichero es estándar, de manera que un fichero creado con un LiveCD se puede recuperar con otro LiveCD diferente.

Los **inconvenientes** son:

- Como cualquier imagen, hay que recuperarla entera, no hay opción de elegir carpetas o ficheros.
- Durante la recuperación estamos escribiendo en todo el disco; un error en un sector puede interrumpir la operación.
- El tamaño del disco donde recuperamos debe ser el mismo o superior al del disco original.
- No incluye opciones avanzadas, como dejar la imagen en el mismo disco e instalar un gestor de arranque que permita recuperarla fácilmente, como ocurre en los ordenadores actuales. Aunque es una opción poco fiable, porque el daño del disco que nos lleva a recuperar la imagen le puede haber afectado a ella.

Caso práctico 9

Creación de una imagen del sistema mediante LiveCD

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

Objetivo. Crear una imagen del disco de un Linux.

Material. Linux Desktop 12.04 sobre VirtualBox 4, LiveCD Linux Slax 6.0.9.

Como siempre, utilizaremos máquinas virtuales porque es fácil acumular discos. Necesitamos un disco extra porque la imagen la conservamos fuera de la máquina que vamos a proteger.

1. En la configuración de la máquina virtual del Linux Desktop vamos a las opciones de almacenamiento. Comprobamos el tamaño del disco actual y en el mismo controlador SATA agregamos un disco duro nuevo. En el asistente elegimos tipo VDI, tipo dinámico, le llamamos imagen y le damos la misma capacidad (aunque la imagen comprimida ocupará menos, como tenemos reserva dinámica de espacio, no nos importa).
2. En esta misma ventana de almacenamiento añadimos un CD en el controlador IDE. Como CD ponemos el fichero .iso de un LiveCD. En este ejemplo ponemos un Slax 6.0.9, que, aunque es antiguo, reconoce bien los distintos discos duros posibles (IDE, SATA). Además, una versión simple tarda menos en arrancar porque no necesitamos los servicios de versiones superiores (Fig. 4.85).

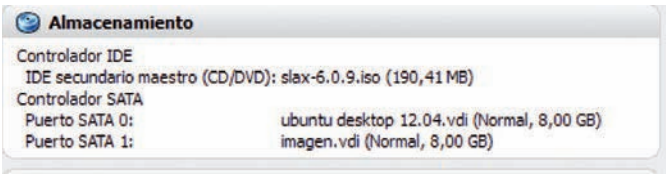


Fig. 4.85. *Añadimos dispositivos.*

3. Arrancamos la máquina virtual y aparece el menú del Slax. Elegimos la opción de arrancar en modo Slax Text Mode, porque solo utilizaremos comandos de Shell.
4. Entramos con `root/toor`. Como se ve en la Figura 4.86, comprobamos los dispositivos conectados (con `fdisk -l`) y los sistemas de ficheros montados (con `df`).

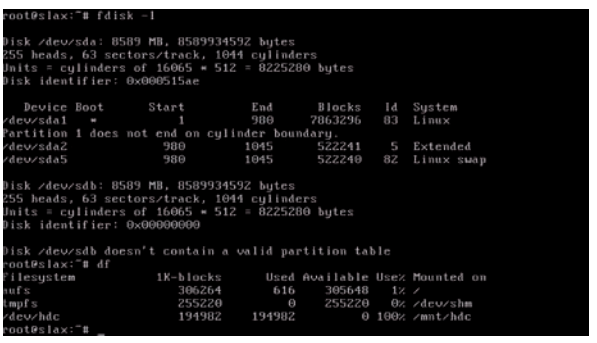


Fig. 4.86. *Comprobamos dispositivos.*

5. Comprobamos que hay un disco `sda` de 8 GB, que tiene las particiones del Linux Desktop. El disco `sdb` no tiene nada (es nuevo) y solo está montado el `hdc` (el propio CD de Slax). Si alguna partición del `sda` estuviera montada, habría que desmontarla para asegurarnos la integridad de la copia.
6. La imagen será un fichero que debe estar en un sistema de ficheros, por lo que creamos una partición en `sdb`, la formateamos y la montamos. La secuencia de comandos es:

```
# fdisk /dev/sdb

# mkfs /dev/sdb1

# mkdir /mnt/sdb1

# mount /dev/sdb1 /mnt/sdb1
```

7. Nos situamos en ese directorio y ejecutamos el comando que genera la imagen.

```
# cd /mnt/sdb1

# dd if=/dev/sda | gzip -c > imagen-sda.gz
```

   Es sencillo: un volcado completo del dispositivo `sda` que se pasa mediante un pipe a un compresor. Al final tenemos un fichero comprimido llamado `imagen-sda.gz` con el contenido de todo el disco.
8. Ahora solo queda esperar. Será más o menos tiempo dependiendo de las prestaciones del ordenador donde corre la máquina virtual. Si somos impacientes, podemos entrar en otra consola con **Alt+F2** y hacer un `ls -l` en ese directorio para comprobar que el fichero está creciendo.
9. Cuando termina el comando vemos que nuestro disco de 8 GB se puede comprimir en un fichero de poco más de 1 GB (Fig. 4.87).



Fig. 4.87. *Imagen completada.*

10. Ahora ya podemos apagar la máquina y llevarnos el disco `hdb` a otra máquina para sacarlo a un USB, guardarlo en cinta, etc.

Caso práctico 10

Recuperación de una imagen de un sistema creada mediante LiveCD

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

Objetivo. Recuperar en un disco nuevo la imagen creada en el caso práctico 9.

Material. LiveCD Linux Slax 6.0.9, VirtualBox 4.

Supongamos que se ha roto el disco o se ha dañado irreversiblemente la instalación de Ubuntu Desktop que hemos usado en el caso práctico 9. Como tenemos la imagen, vamos a recuperarla. Necesitaremos los mismos ingredientes: una imagen .iso de un LiveCD (en nuestro caso el mismo Slax 6.0.9, pero podría ser otro) y un disco duro nuevo de 8 GB, donde vamos recuperar la imagen (podría ser el mismo disco, si no hay fallo hardware).

1. En la máquina virtual del Ubuntu Desktop vamos a la opción de almacenamiento. Desconectamos el disco fallido, pinchamos el LiveCD y el disco con la imagen y añadimos un disco nuevo de 8 GB (tipo VDI con crecimiento dinámico, como siempre) y le llamamos *recuperado* (Fig. 4.88).



Fig. 4.88. *Discos para la recuperación.*

2. Arrancamos y elegimos Slax Text Mode, porque solo vamos a trabajar en la shell.
3. Entramos como `root/toor` y comprobamos que los discos están ahí (`fdisk -l`) y cuál está montado (`df`). La imagen debe estar ahí y el disco nuevo no debería tener nada (Fig. 4.89).

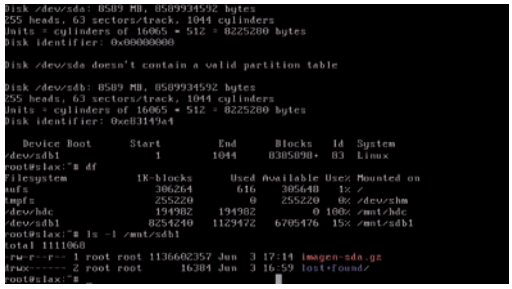


Fig. 4.89. *Comprobamos dispositivos.*

4. Todo está listo para el comando de recuperación:

```
# cd /mnt/sdb1
# gzip -d -c imagen-sda.gz | dd of=/dev/sda
```

Como era de esperar, es el proceso inverso: descomprimimos el fichero y lo volcamos directamente al disco, sin pasar por ningún sistema de ficheros. Esto nos permite recuperar todo: la tabla de particiones, el sector de arranque, etc.

5. Después de una larga espera, en función de la capacidad del disco y la potencia del ordenador que ejecuta nuestra máquina virtual, el proceso termina (Fig. 4.90).



Fig. 4.90. *Recuperación completada.*

6. Ya podemos apagar el LiveCD, desconectar el CD y el disco con la imagen y arrancar con el sistema recuperado en el nuevo disco.

3.2. Congelación

En algunos entornos interesa dar una configuración estable al ordenador y después impedir cualquier cambio, venga del usuario o de algún intruso (virus, troyano, etc.). El ejemplo más típico son las salas de ordenadores de un cibercafé: cuando se acaba el tiempo de alquiler del puesto, hay que borrar cualquier rastro (ficheros personales, programas instalados) para que el siguiente cliente encuentre el ordenador «limpio».

Esta es la misión del software de congelación: una vez instalado, toma nota de cómo está el sistema (snapshot) y, desde ese instante, cualquier cambio que ocurra en el sistema podrá ser anulado cuando el administrador lo solicite (en el caso del cibercafé se configura para que ocurra de manera automática en el próximo arranque).

Los sistemas Windows también incluyen esta funcionalidad de crear puntos de restauración, pero la funcionalidad es limitada, porque solo se preocupan de programas, no de datos.

Las herramientas de congelación suelen permitir mantener varios snapshots, para facilitar volver a otras situaciones pasadas; aunque el espacio ocupado en el disco puede llegar a ser un problema.

Actividades

28. El concepto de congelación de un sistema suele confundirse con la imagen. Discute las semejanzas y diferencias.

29. Investiga cómo saben estos programas qué ficheros han cambiado para proceder a su restauración.

Vocabulario

Patch Tuesday. El segundo martes de cada mes Microsoft suele liberar parches para sus sistemas operativos y aplicaciones.

El principal inconveniente de esta solución aparece cuando queremos instalar un programa nuevo.

En algunos programas hay que descongelar, instalar y volver a congelar; en otros simplemente recordar que, si alguna vez recuperamos un snapshot anterior, habría que volver a instalarlo. Y esto se agrava con el hecho de que la mayoría de los sistemas operativos y las aplicaciones se actualizan con mucha frecuencia (el famoso Patch Tuesday). Por tanto, las soluciones de congelación tienen una aplicabilidad bastante limitada porque es difícil administrar los distintos snapshots (nos pueden interesar unos ficheros de uno y otros de otro).

Caso práctico 11

Congelación en Windows 7

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

Objetivo. Probar la congelación en un Windows *7*.

Material. Windows *7*.

Vamos a probar la congelación de un Windows *7* usando el software Comodo Time Machine.

1. Nos descargamos el software de su página web y lo instalamos. En un momento dado nos preguntará a qué unidades queremos aplicar la congelación (Fig. 4.91). Nos aconseja dejar al menos 10 GB libres, porque ahí necesita ir guardando cada fichero añadido o modificado.

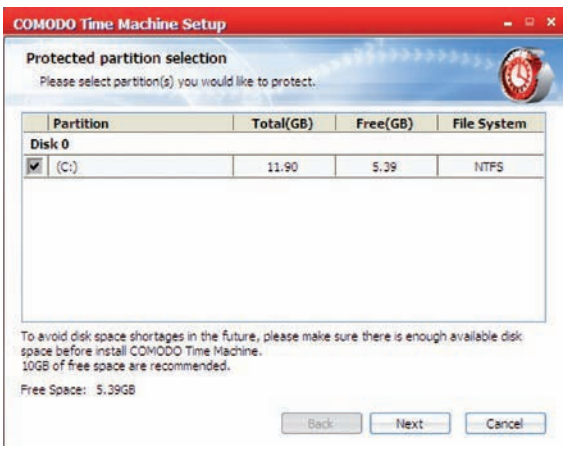


Fig. 4.91. *Unidad que vamos a congelar.*

2. Después de reiniciar el ordenador ya podemos probarlo. Tenemos un icono en la barra de tareas para lanzar la herramienta en modo simple (Fig. 4.92).



Fig. 4.92. *Menú simple.*

3. Vamos a hacer una primera prueba simple: haremos una «foto» del sistema actual, crearemos un fichero nuevo y después recuperaremos la «foto» guardada. El fichero debería desaparecer.

4. Pinchamos en *Take Snapshot* y nos pedirá un nombre. Lo llamaremos fichero fantasma. Es importante darle un nombre significativo si vamos a crear muchos snapshots.

5. Una vez terminado el snapshot, creamos un fichero en la carpeta Documentos. Después volvemos a la herramienta y pulsamos en *Restore System*. Nos ofrecerá los snapshots creados. Seleccionamos el nuestro y pulsamos *Next*. Nos pedirá confirmación de lo que vamos a hacer; pulsamos *Restore* y a continuación el sistema arranca de nuevo para aplicar la restauración (Fig. 4.93). Si todo ha ido bien, el fichero habrá desaparecido.



Fig. 4.93. *Confirmación de restauración.*

6. Volvemos a la herramienta y ahora elegimos el modo avanzado (Fig. 4.94).

7. Aparecen los snapshots organizados en un árbol, para que veamos de dónde viene cada foto que hemos creado. Veréis que hay uno más, porque por defecto hace un snapshot antes de aplicar una restauración. Este comportamiento lo podemos anular en *Settings > Advanced Settings > Always take…*

(Continúa)

Caso práctico 11

(Continuación)

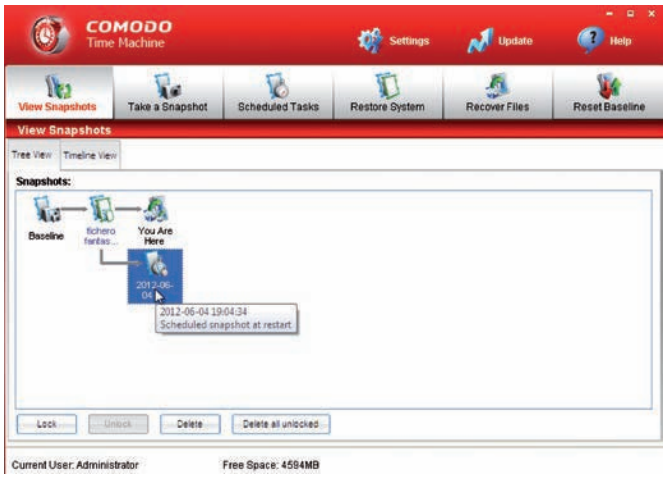


Fig. 4.94. *Menú avanzado.*

8. Vamos a probar algo más arriesgado. Desinstalaremos el Backup4all del caso práctico *7*. Cuando termine, comprobamos que no está disponible. Si es así, volvemos al Comodo y hacemos la restauración a fichero fantasma. Al arrancar otra vez, el programa ha vuelto (y tenemos un nuevo snapshot por haber hecho una restauración, claro).

9. La herramienta tiene funciones bastante interesantes, como Recover files, que permite buscar un fichero en cualquiera de nuestros snapshots. Así evitamos restaurar el sistema completo solo porque necesitamos un fichero antiguo.

10. Otra funcionalidad importante es la consola de restauración: si no podemos entrar a Windows, pulsando la tecla **Inicio** durante el arranque de la máquina podemos ejecutar la herramienta Comodo e intentar restaurar un snapshot anterior (Fig. 4.95).

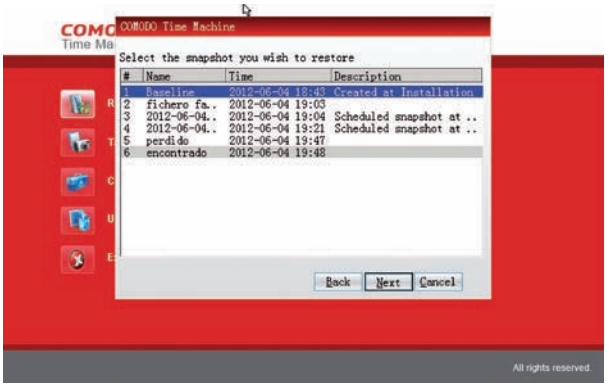


Fig. 4.95. *Consola de restauración.*

3.3. Registro de Windows y puntos de restauración

Los sistemas Windows incluyen una funcionalidad similar al software de congelación del apartado anterior: se llaman puntos de restauración y recogen el estado de los ejecutables y la configuración del sistema operativo (no se incluyen los documentos de los usuarios). Es importante crear un punto de restauración antes de efectuar cambios importantes en el sistema, como la instalación o sustitución de drivers o la aplicación de parches. De hecho, las actualizaciones automáticas de Windows siempre crean primero un punto de restauración.

Si el cambio aplicado ha sido un desastre, podemos volver a la situación anterior utilizando el punto de restauración. Es una operación irreversible: una vez lanzado, no podemos interrumpirlo y el sistema quedará con esa configuración. Por este motivo, en las versiones modernas, como Windows *7*, podemos consultar exactamente los ficheros que se van a modificar.

Si el cambio solo afecta a la configuración, entonces nos podemos limitar a proteger el registro. El registro es una base de datos interna donde el sistema operativo y las aplicaciones anotan información de configuración. Si sufre algún daño o se manipula indebidamente, las aplicaciones afectadas pueden dejar de funcionar y necesitar ser instaladas de nuevo.

Por este motivo, antes de la instalación de un parche complejo o si necesitamos modificar manualmente algún valor del registro, conviene hacer una copia del mismo. Para ello ejecutaremos la aplicación regedit (desde *Inicio* > *Buscar,* en Vista/Windows *7*; *Inicio* > *Ejecutar,* en XP). En la ventana que aparece vamos a *Archivo* > *Exportar.*

Actividades

30. Compara la copia del registro de Windows con las soluciones que hemos visto antes: congelación, imagen, etc.

Importante

La información de recuperación suele ocupar mucho disco, por eso conviene eliminar los puntos de restauración antiguos. Están en un directorio oculto en la raíz de la unidad llamado System Volume Information, aunque siempre conviene eliminarlos desde la propia herramienta.

Podemos elegir salvar una clave, una rama o todo el registro (si no sabemos qué va a cambiar, debemos salvar todo). Nos pedirá el nombre que le daremos al fichero, que tendrá la extensión .reg (Fig. 4.96).

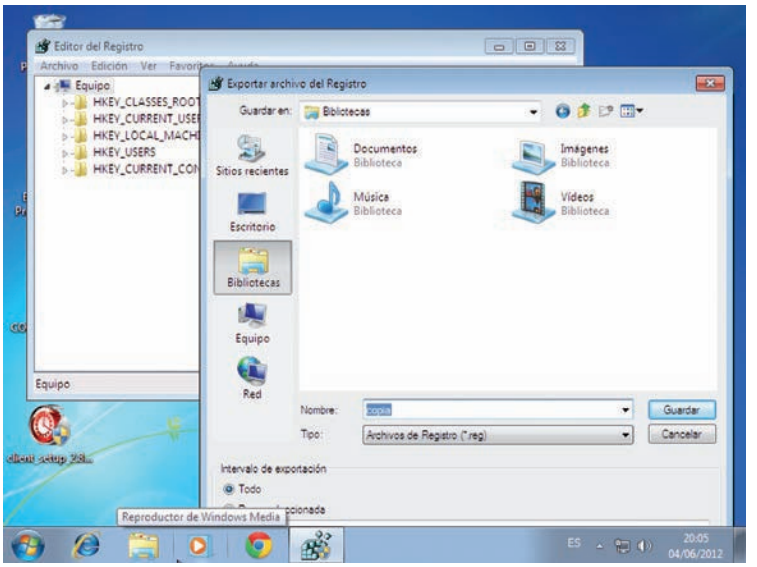


Fig. 4.96. *Copia del registro.*

Si queremos recuperar esta configuración, abriremos la misma herramienta pero ahora elegiremos la opción *Importar*.

3.4. Herramientas de chequeo de discos

Ya sabemos cómo proteger nuestros datos frente a un fallo en un disco (RAID, backup, almacenamiento en la nube, etc.). Pero no deberíamos esperar sentados hasta que un disco falle y confiar en que entrará en funcionamiento el mecanismo de respaldo. Siempre es aconsejable tomar medidas preventivas, en este caso la detección temprana del fallo.

En Windows 7 nos situamos sobre la unidad y, en el menú de botón derecho, elegimos *Propiedades*. Aparece una ventana y pinchamos en la pestaña *Herramientas*. Ahí tenemos la herramienta de comprobación de errores (Fig. 4.97).

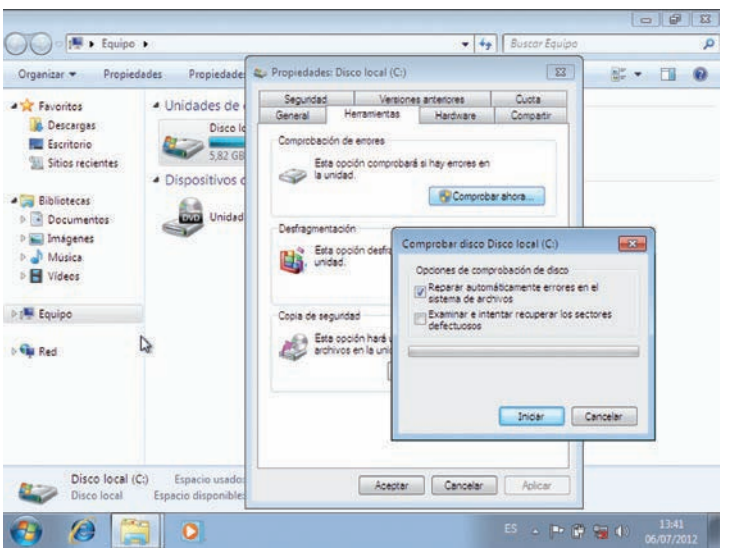


Fig. 4.97. *Chequeo de disco en W7.*

Como estamos usando esa unidad para el sistema operativo, nos encontramos ante un problema similar a la copia consistente que vimos con anterioridad. La herramienta nos advierte de que no puede hacer los cambios y que lo prepara todo para hacerlo en el siguiente arranque. Se consigue lo mismo ejecutando el comando `chkdsk /f` desde el `cmd`.

En Linux tenemos el comando `fsck` para comprobar la integridad del sistema de ficheros. Para comprobar el disco podemos utilizar la utilidad de discos (Fig. 4.98).

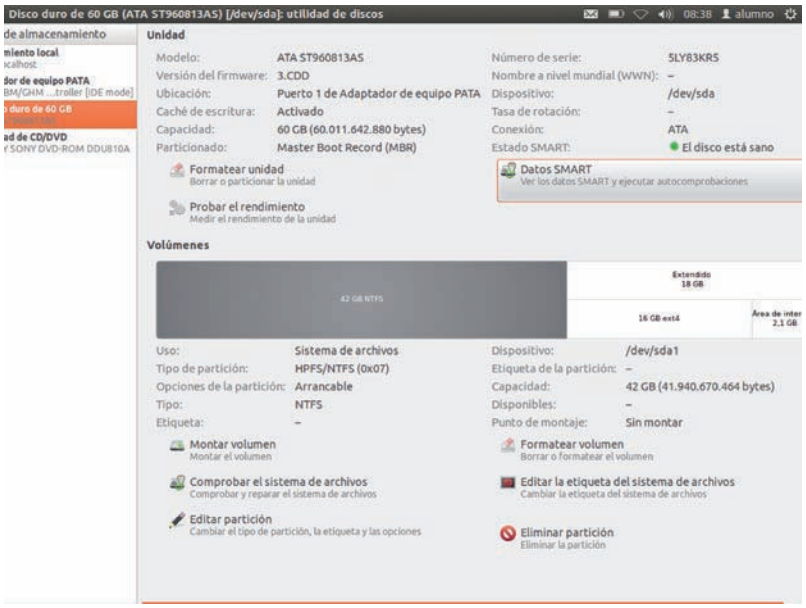


Fig. 4.98. *Utilidad de discos en Ubuntu 12.*

En esta herramienta aparecen en el lado izquierdo todas las unidades conectadas al equipo. Al seleccionar alguna, en el lado derecho obtenemos toda la información (modelo, capacidad, volúmenes) y podemos lanzar varias operaciones (formatear, editar particiones, comprobar el sistema de archivos).

Hay una operación especial llamada Datos SMART. Se refiere a un estándar utilizado en los discos duros para analizar en detalle su estado (Fig. 4.99). Si en esta herramienta la estimación general es que el disco no está sano, debemos sustituirlo cuanto antes.



Fig. 4.99. *Herramienta SMART.*

Actividades

31. Investiga si en Windows se puede comprobar la integridad de un sistema de ficheros Linux, y viceversa.

32. Busca una herramienta SMART para Windows, ejecútala y compara el resultado con lo que aparece en la herramienta Linux. ¿Debería ser lo mismo?

33. En Windows, prueba el chkdsk /f en un disco que no tenga instalado el sistema operativo. ¿Se hace inmediatamente o se programa para el próximo arranque?

Síntesis

Conectar varios discos en RAID

- RAID 0: juntamos discos en una unidad más grande.
  - Mejor rendimiento.
  - Igual seguridad.
- RAID 1: dos discos, uno espejo del otro.
  - Igual rendimiento.
  - Mejor seguridad.
- RAID 5: juntamos varios discos e incluimos la paridad.
  - Mejor rendimiento.
  - Mejor seguridad.

Almacenamiento en red

- NAS: un equipo ofrece disco a los equipos conectados a su misma red.
  - Arquitectura cliente/servidor.
  - Protocolo CIFS. Precio elevado.
- SAN: armario de discos conectado a uno o varios servidores.
  - Altas prestaciones, fiabilidad, flexibilidad.
  - Precio elevado.

Almacenamiento en la nube

- Generaciones
  - Primera: servidor web con upload/download.
  - Segunda: carpeta actualizada automáticamente entre varios equipos.
- P2P
  - Mejor rendimiento cuanto más se usa.
  - Seguridad baja.

Tipos de copia

- Completa
  - Todos los archivos.
  - Necesaria para poder aplicar diferencial o incremental.
- Diferencial
  - Solo los archivos cambiados desde la última copia completa.
  - Ocupa más que la copia incremental.
  - Para recuperar solo necesitamos la completa y la última diferencial.
- Incremental
  - Solo los archivos cambiados desde la última copia: completa o incremental.
  - Ocupa menos que la copia diferencial.
  - Para recuperar una copia necesitamos la completa y todas las incrementales.

Backup del registro de Windows y puntos de restauración

- La herramienta que sirve para manipular el registro permite hacer una copia a fichero.
- Los puntos de restauración recuperan el disco tal y como estaba en un momento anterior, pero solo los programas, no los documentos del usuario.

Herramientas de chequeo de disco

- Son tareas preventivas para anticiparse a un fallo del dispositivo.
- Operan sobre:
  - La integridad del sistema de ficheros.
  - La capacidad del disco para auto-diagnosticarse (SMART).

Test de repaso

1. ¿Cómo se mide la calidad de un disco duro?
a) MTS.
b) AMD.
c) MTBF.

2. ¿Qué discos duros carecen de partes móviles?
a) USB.
b) IDE.
c) SSD.

3. ¿Por qué hay que proteger los datos de la empresa?
a) Porque son irrepetibles.
b) Porque son mejores que los de la competencia.
c) Porque hay que dar trabajo al departamento de informática.

4. Si ponemos seis discos duros de 1 TB en RAID 1, el usuario ve:
a) 6 TB.
b) 3 TB.
c) 5 TB.

5. Si tenemos cuatro discos de 1 TB en RAID 0 y falla uno de ellos:
a) El usuario todavía puede acceder a 3 TB de ficheros.
b) El RAID se ha roto, pero reponiendo el disco podemos recuperarlo.
c) Hemos perdido todo.

6. Si tenemos cuatro discos de 1 TB en RAID 5 y falla uno de ellos:
a) El usuario todavía puede acceder a 3 TB de ficheros.
b) El usuario solo puede acceder a la mitad de los discos.
c) Hemos perdido todo.

7. Un miembro del equipo ofrece su ordenador para almacenar los ficheros comunes a todos:
a) Se lo aceptamos, porque es muy amable.
b) No se lo aceptamos, porque tememos que pueda borrarse todo.
c) Preguntamos al departamento de informática qué servicios de almacenamiento compartido están soportados en la empresa.

8. Un miembro del equipo propone abrir una cuenta en Dropbox para almacenar los ficheros comunes a todos:
a) Lo aceptamos, porque se ofrece a gestionarlo.
b) No lo aceptamos, porque es una violación de seguridad.
c) Preguntamos al departamento de informática qué servicios de almacenamiento compartido están soportados en la empresa.

9. El jefe del departamento de informática nos propone que, a partir de hoy, hagamos una imagen de todos los equipos el viernes por la tarde.
a) Nos oponemos, porque nos queremos ir pronto de fin de semana.
b) Aceptamos, porque es el jefe.
c) Empezamos una discusión sobre las diferencias entre backup e imagen.

10. Nuestro jefe nos pide que estudiemos la posibilidad de configurar uno de los servidores conectados al SAN para ofrecer disco en red mediante NAS.
a) No tiene sentido: el servidor puede tener NAS o SAN, pero no las dos cosas.
b) No hay problema: utilizaremos un servidor con Windows XP para que sea más fácil.
c) No hay problema: buscaremos el software más adecuado para los distintos sistemas operativos de los equipos de nuestra empresa.

11. En general, la copia incremental:
a) Ocupa más que la copia completa.
b) Ocupa más que la copia diferencial.
c) Ocupa menos que la copia diferencial.

12. Durante la configuración del backup de datos:
a) Fijamos la periodicidad.
b) Fijamos la periodicidad y activamos el cifrado.
c) Lo programamos para que se ejecute una vez al mes.

13. ¿Para qué necesitamos una LAN destinada al backup de datos?
a) Para dar trabajo al departamento de redes.
b) Para evitar sobrecarga de tráfico en la red principal.
c) Para evitar que algún hacker espíe los backup remotos.

14. Hacer una imagen del sistema con un LiveCD Linux:
a) Funciona para cualquier sistema instalado y para cualquier LiveCD.
b) No funciona en un sistema que ya tiene Windows.
c) Solo se puede recuperar con el mismo LiveCD.

15. Estamos dudando entre hacer congelación o imagen:
a) No hay duda: es mejor hacer congelación siempre.
b) No hay duda: es mejor hacer imagen siempre.
c) Son complementarias.

16. El registro de Windows:
a) Se salva automáticamente en cualquier backup.
b) Se puede salvar a un fichero y luego meter ese fichero en el backup.
c) No se puede salvar, porque es interno al sistema.

Soluciones: 1 c, 2 c, 3 a, 4 b, 5 c, 6 a, 7 c, 8 c, 9 c, 10 c, 11 c, 12 b, 13 b, 14 a, 15 c, 16 b.

Comprueba tu aprendizaje

Implantar y documentar políticas de almacenamiento redundante y distribuido

1. Sobre una máquina virtual de Windows Server 2008, añade dos discos duros virtuales de 200 MB cada uno.

a) Configura los discos en RAID 1.

b) Configura de nuevo los discos en RAID 0.

c) Añade un disco más y configúralo en RAID 5.

d) Resume en una tabla las ventajas e inconvenientes de las configuraciones anteriores.

e) Documenta todos los procedimientos llevados a cabo.

Instalar y configurar un servicio de almacenamiento en red

2. Instala una maqueta con tres máquinas: dos Windows y un Linux.

a) En uno de los sistemas Windows debes compartir una carpeta que sea accesible desde las otras dos máquinas. El acceso será solo de lectura. Comprueba que funciona así.

b) En el segundo sistema Windows debes compartir una carpeta que sea accesible desde las otras dos máquinas. El acceso será de lectura y escritura. Comprueba que se pueden coger y dejar archivos.

c) En el sistema Linux debes compartir dos carpetas que sean accesibles desde las otras dos máquinas. Una carpeta tendrá acceso de solo lectura y la otra de lectura y escritura. Comprueba que es así.

d) Documenta los procedimientos ejecutados.

Realización de copias de seguridad en dispositivos extraíbles y remotos

3. Instala una maqueta con dos máquinas: un sistema Windows y uno Linux.

a) Instala en el sistema Windows una herramienta de backup.

b) Instala en el sistema Linux un servidor FTP. Crea un usuario backup en ese servidor.

c) En el sistema Windows entra con el usuario administrador, crea una carpeta en el escritorio y llámala Importante. Copia varios ficheros dentro de esa carpeta y alguna subcarpeta.

d) Realiza un backup completo de la carpeta Importante. El destino del backup será un pendrive USB.

e) Borra un fichero de la carpeta Importante. Intenta recuperarlo con una herramienta como FileScavenger.

f) Bórralo de nuevo y ahora intenta recuperarlo desde el backup residente en el pendrive.

g) Realiza un backup completo de la carpeta Importante en la cuenta backup del servidor FTP.

h) Borra la carpeta Importante y después intenta recuperarla desde el backup del FTP.

i) Elabora una tabla resumen con las ventajas e inconvenientes de los dos dispositivos de almacenamiento de backup que hemos utilizado.

j) Documenta los procedimientos ejecutados.

Utilizar distintas estrategias de ejecución de copias de seguridad

4. Instala en una maqueta dos máquinas Windows.

a) Instala en una de ellas (la llamaremos M1) una herramienta de backup y en la otra (M2) un servicio de almacenamiento en red. En M2 crea un usuario backup.

b) En M1 entra con un usuario administrador, crea una carpeta en el escritorio y llámala Seguridad. Dentro de ella debes copiar varios ficheros.

c) En M1 ejecuta un backup incremental sobre el almacenamiento en red ofrecido por M2.

d) A continuación modifica un fichero, borra otro y añade uno nuevo. Repite la ejecución del backup incremental y comprueba qué ha ocurrido en M2.

e) Repite el ejercicio utilizando backup diferencial.

f) Repite el ejercicio aplicando una programación de cinco ejecuciones separadas por un minuto. Durante ese tiempo debes realizar modificaciones en la carpeta.

g) Documenta los procedimientos ejecutados.

Crear y restaurar imágenes de sistemas

5. Genera una imagen de una máquina virtual de un sistema Linux Ubuntu Desktop.

a) Recupera esa imagen en un disco nuevo y comprueba que el sistema funciona.

b) Documenta los procedimientos llevados a cabo.

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.

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.



Fig. 5.1. *Candado de portátil.*

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.

Web

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.



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.

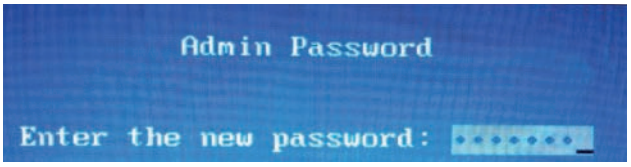


Fig. 5.3. *Clave de administrador.*

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).

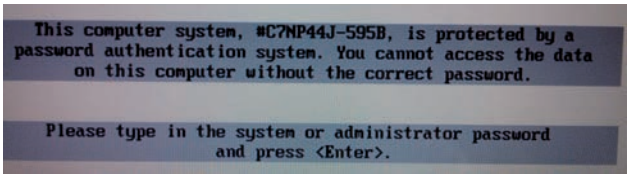


Fig. 5.5. *Nos pide la clave.*

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).

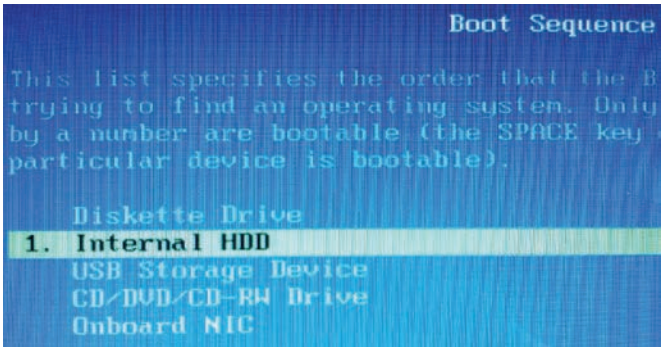


Fig. 5.6. *Dejamos únicamente el disco duro.*

(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).

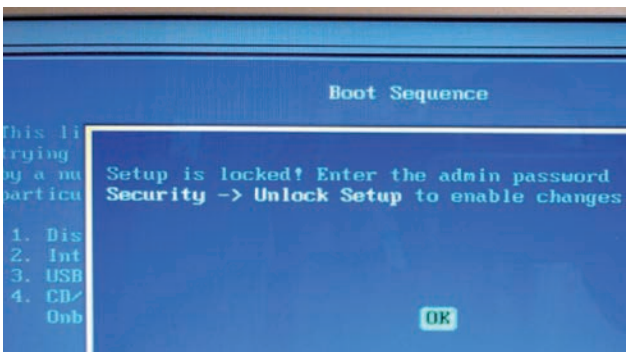


Fig. 5.9. *Protegida la secuencia de arranque.*

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.

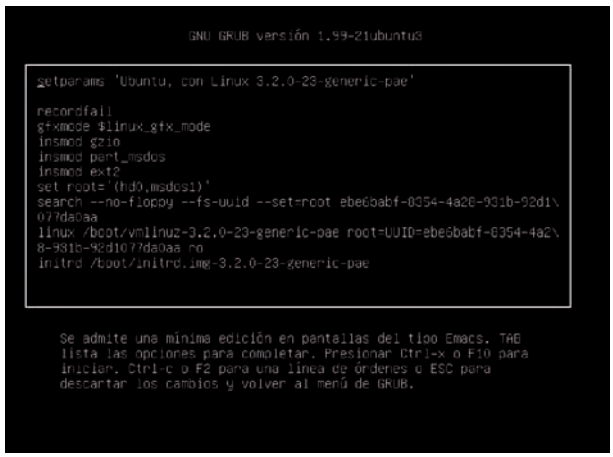


Fig. 5.11. *Opciones de arranque.*

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).

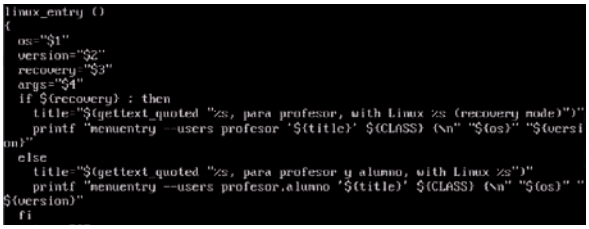


Fig. 5.12. *Modificamos opciones del menú.*

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).

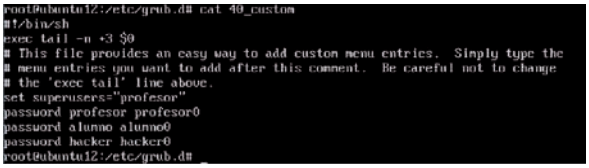


Fig. 5.13. *Usuarios definidos.*

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).

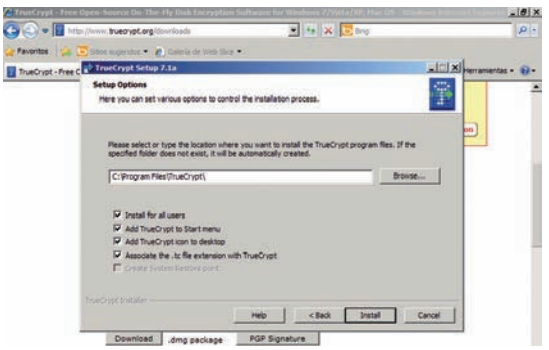


Fig. 5.15. *Instalación de TrueCrypt.*

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).

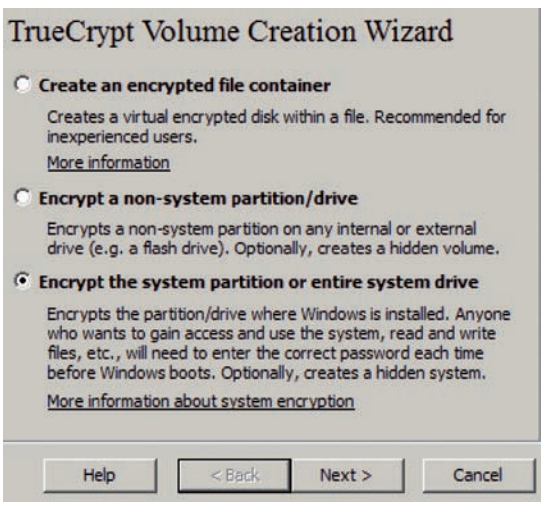


Fig. 5.16. *Elegimos cifrar el disco del sistema.*

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

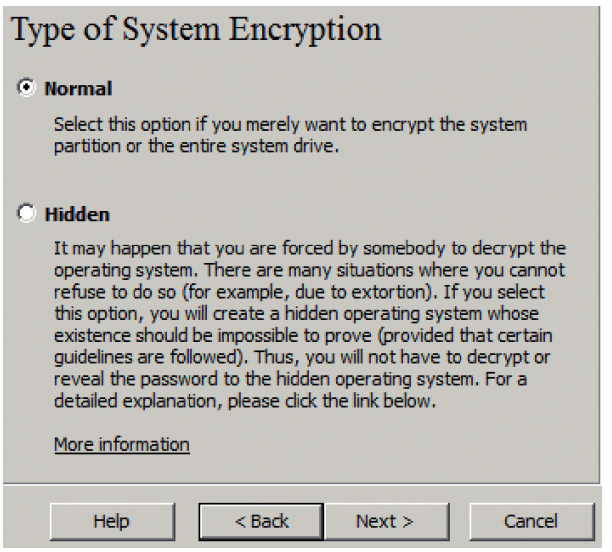


Fig. 5.17. *Cifrado de sistema normal.*

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)

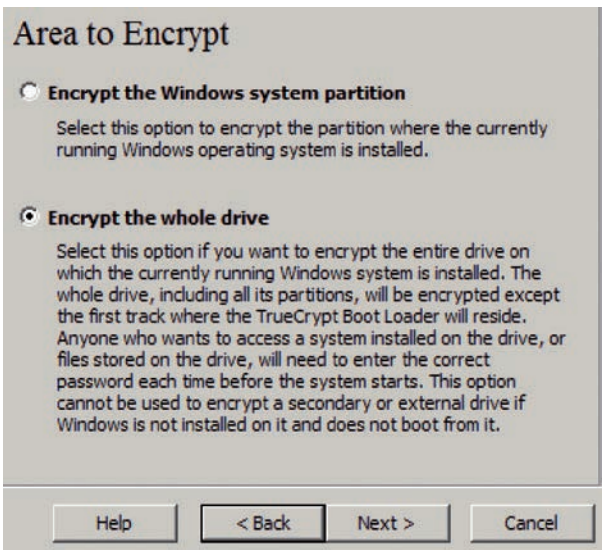


Fig. 5.18. *Ciframos todo el disco.*

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)

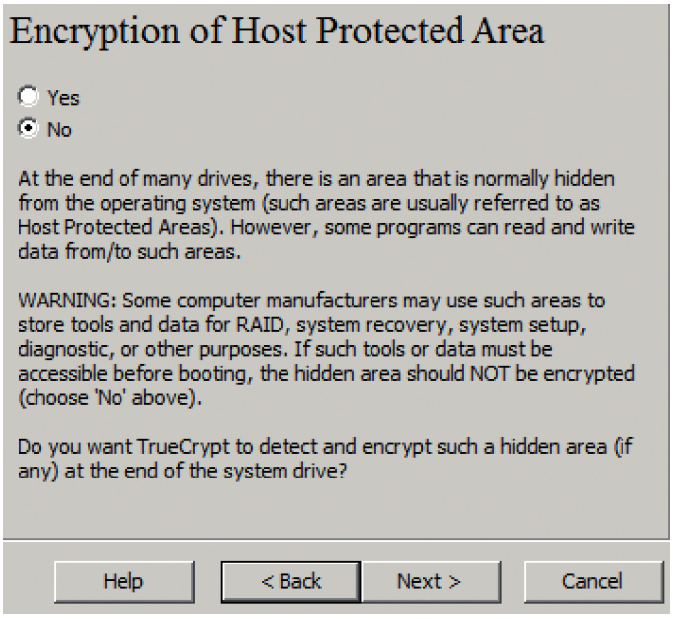


Fig. 5.19. *No ciframos el final del disco.*

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

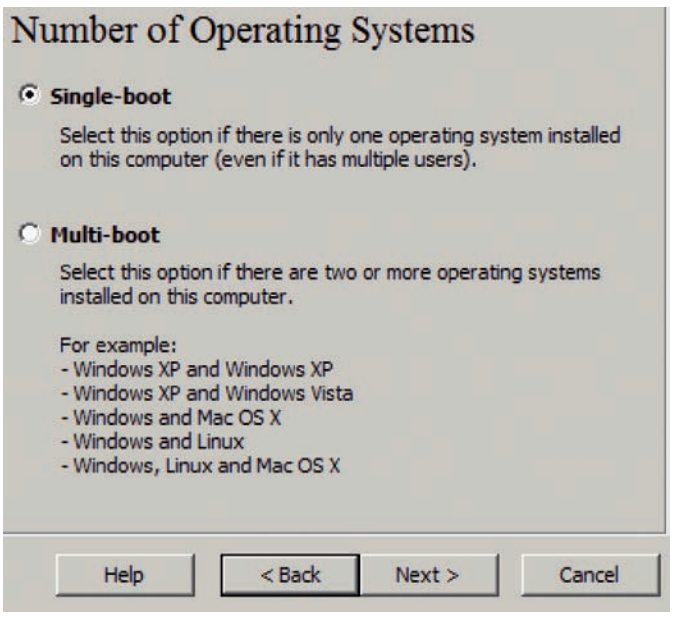


Fig. 5.20. *Tipo de arranque.*

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).

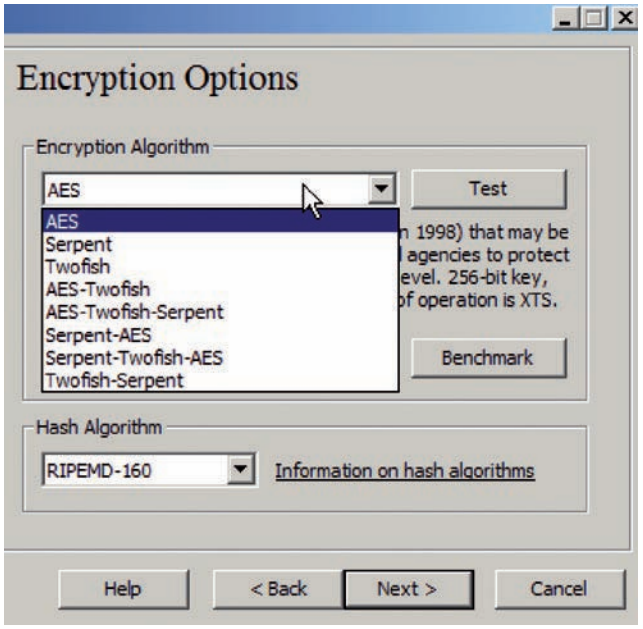


Fig. 5.21. *Opciones de cifrado.*

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.

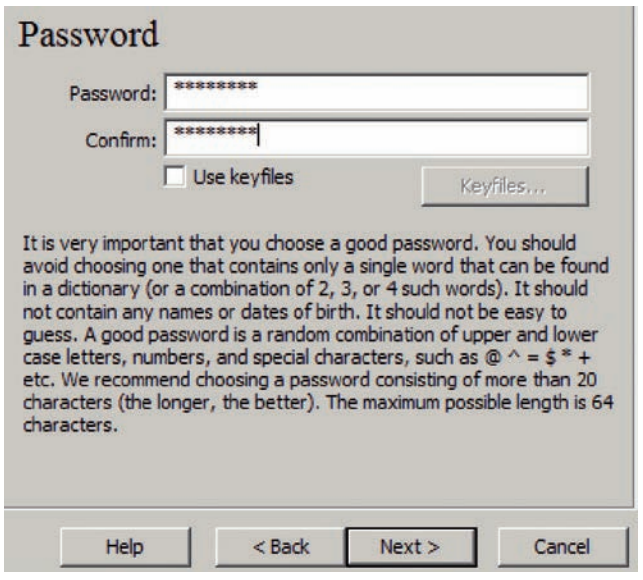


Fig. 5.22. *Clave de cifrado.*

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

(Continúa)

Caso práctico 4

(Continuación)

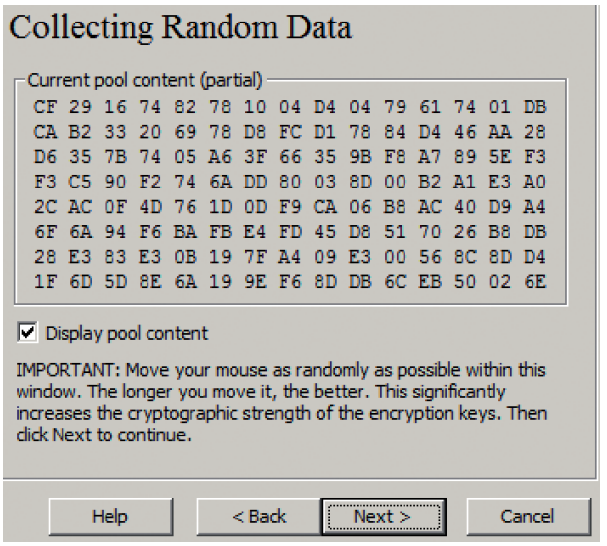


Fig. 5.23. *Generación de aleatoriedad.*

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.

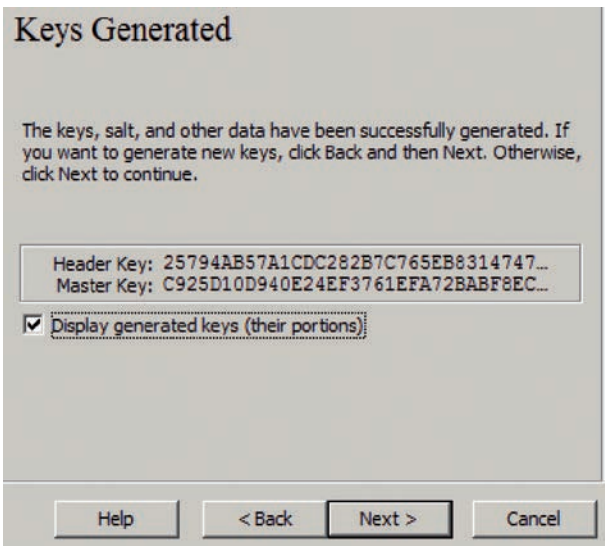


Fig. 5.24. *Claves generadas.*

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).

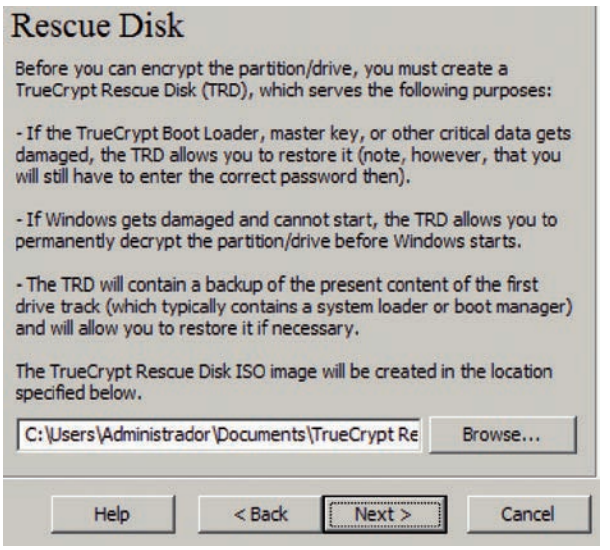


Fig. 5.25. *Disco de rescate.*

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.

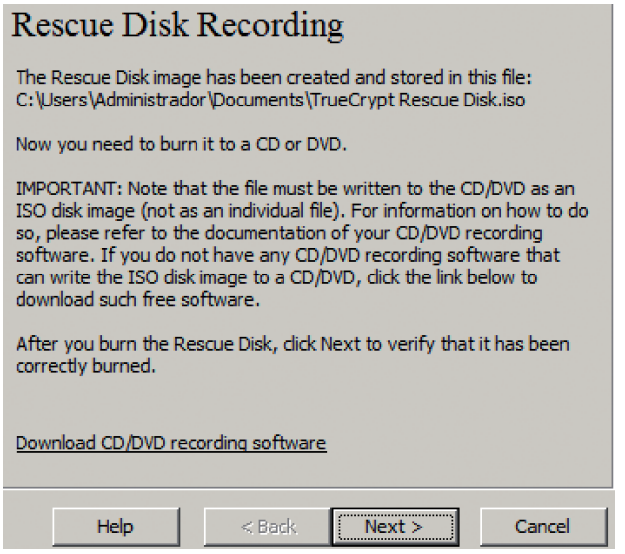


Fig. 5.26. *Debemos grabar el disco de rescate.*

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

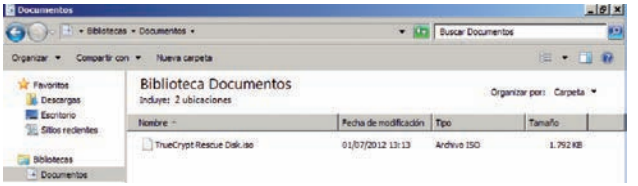


Fig. 5.27. *Fichero .iso del disco de rescate.*

(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).

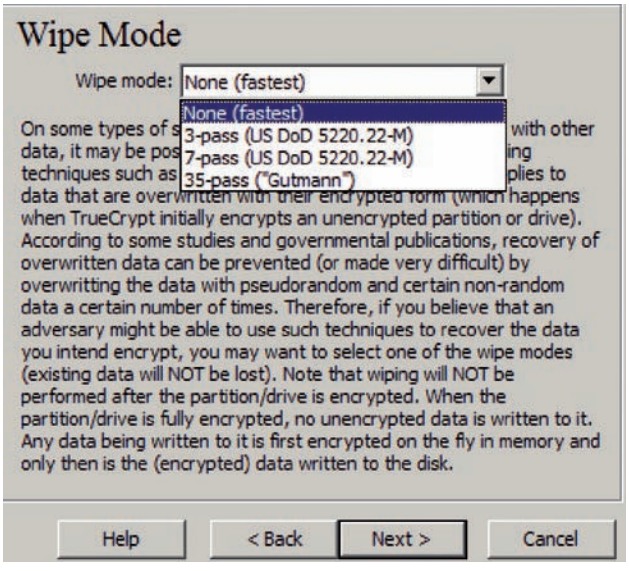


Fig. 5.29. *Tipo de cifrado inicial.*

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.

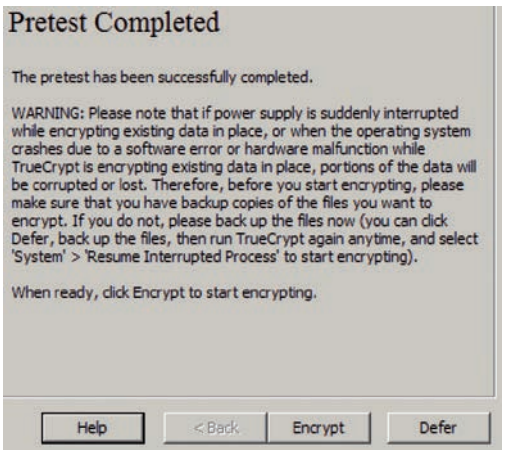


Fig. 5.31. *Listos para cifrar.*

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

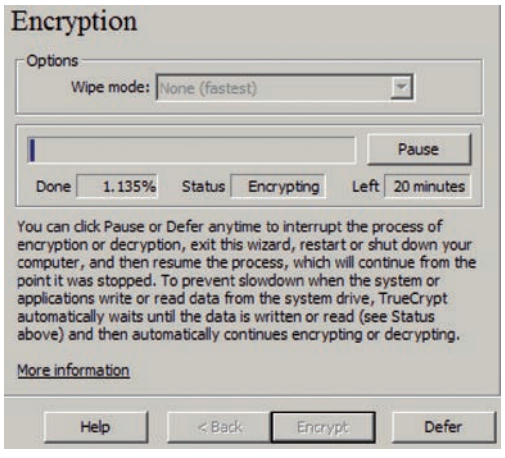


Fig. 5.32. *Cifrado en curso.*

(Continúa)

Caso práctico 4

(Continuación)

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

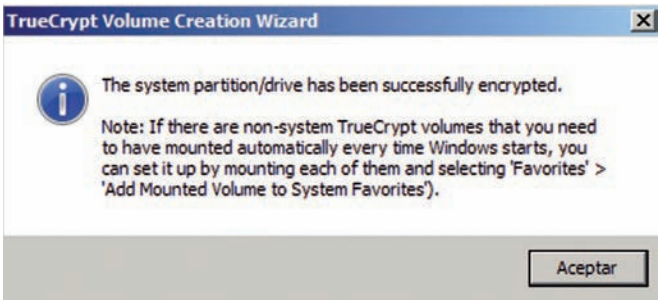


Fig. 5.33. *Cifrado completado.*

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).

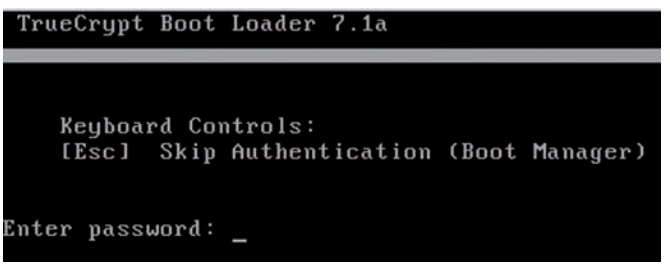


Fig. 5.34. *Boot loader de TrueCrypt.*

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

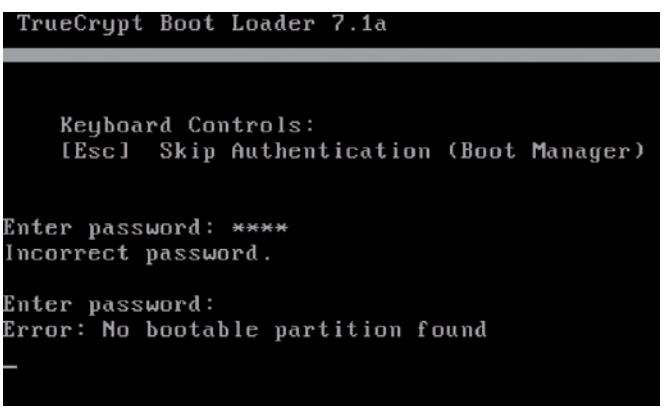


Fig. 5.35. *Acceso incorrecto.*

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

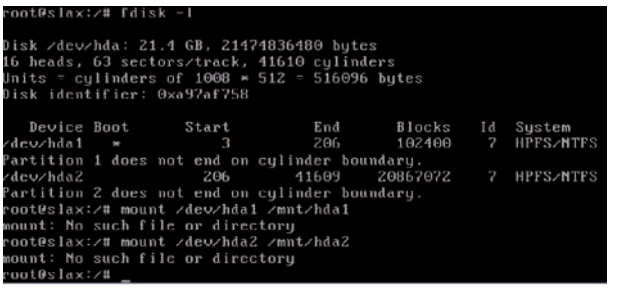


Fig. 5.36. *Particiones protegidas.*

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

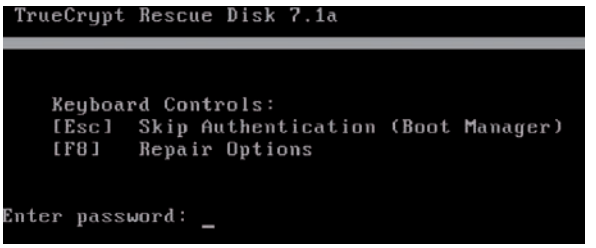


Fig. 5.37. *Menú del disco de rescate.*

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

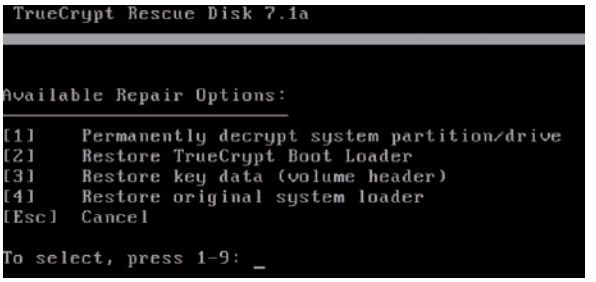


Fig. 5.38. *Opciones de reparación.*

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

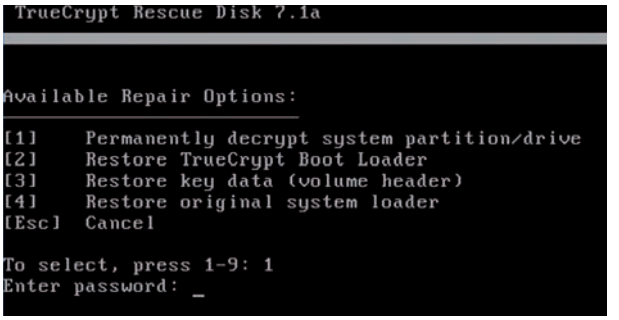


Fig. 5.39. *Pide la contraseña de cifrado.*

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.

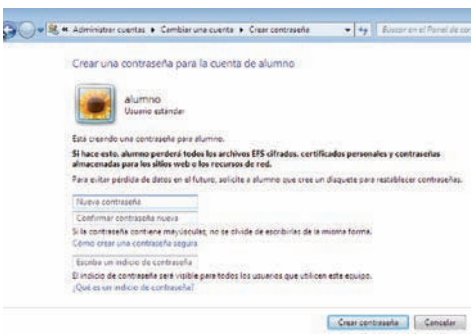


Fig. 5.41. *Cambiar la contraseña de otro usuario.*

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).

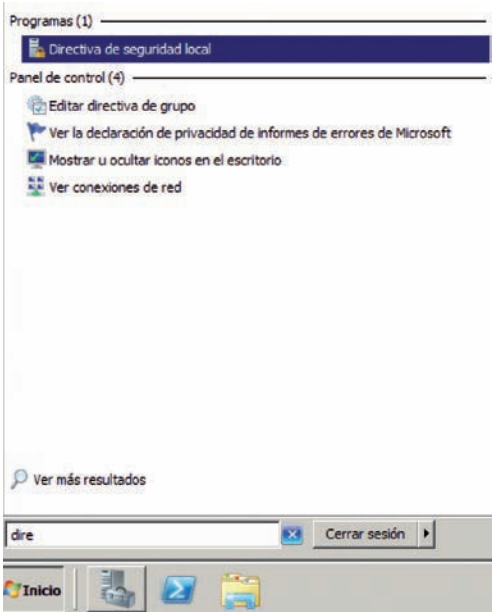


Fig. 5.42. *Buscamos la herramienta de directivas de seguridad local.*

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).

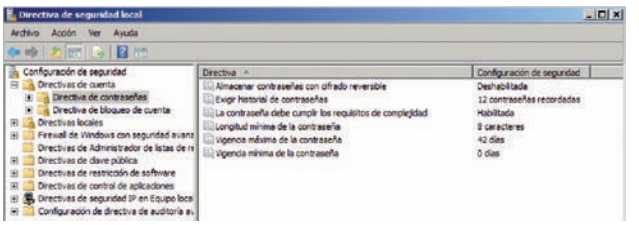


Fig. 5.43. *Directivas sobre contraseñas.*

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).

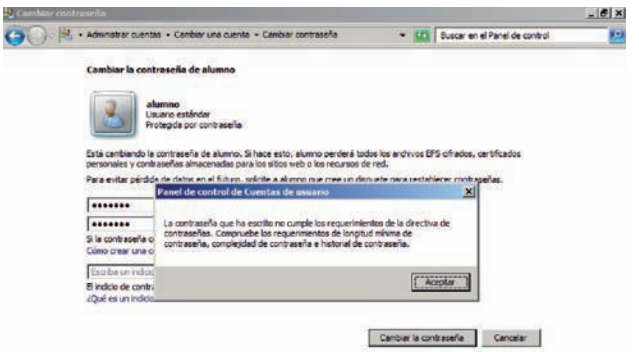


Fig. 5.44. *Control de longitud de contraseña.*

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).

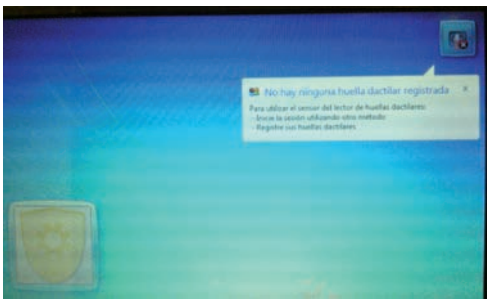


Fig. 5.47. *El sistema todavía no está preparado.*

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

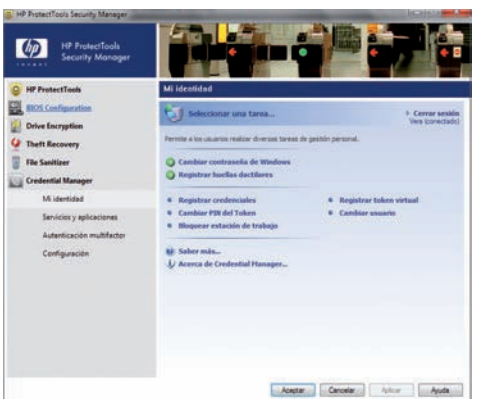


Fig. 5.48. *Herramienta HP Security Manager.*

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).

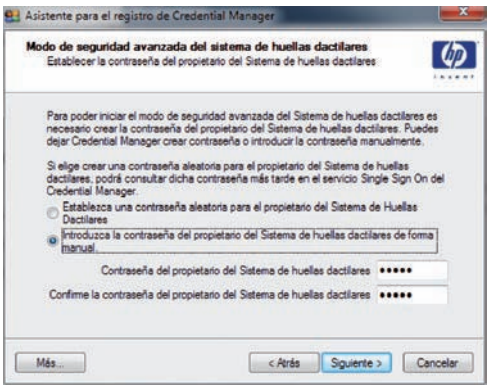


Fig. 5.50. *Protegemos el acceso al gestor.*

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).

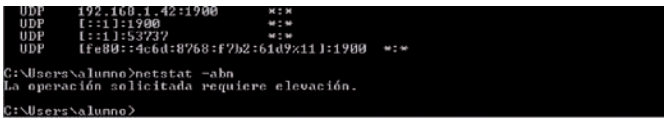


Fig. 5.54. *Necesitamos privilegios.*

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).

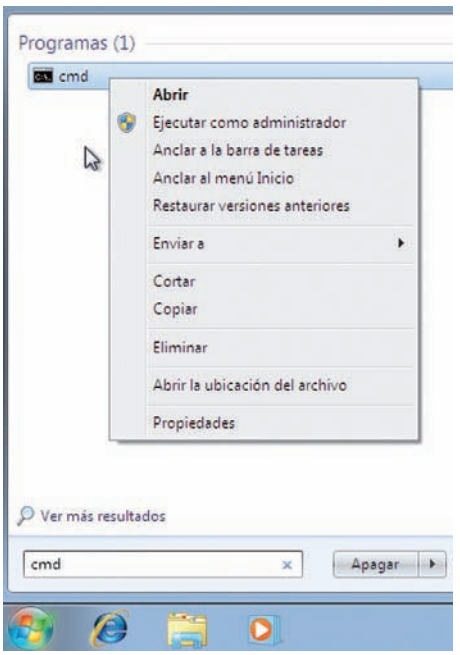


Fig. 5.55. *Solicitamos elevación.*

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).

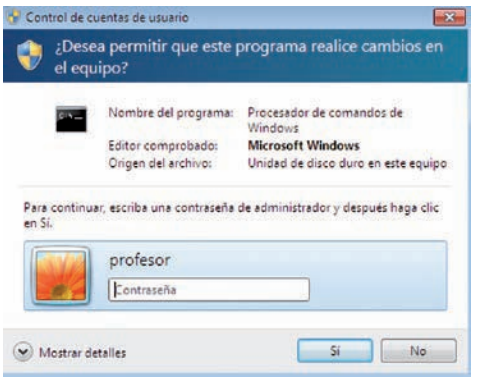


Fig. 5.56. *Autenticación puntual.*

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).

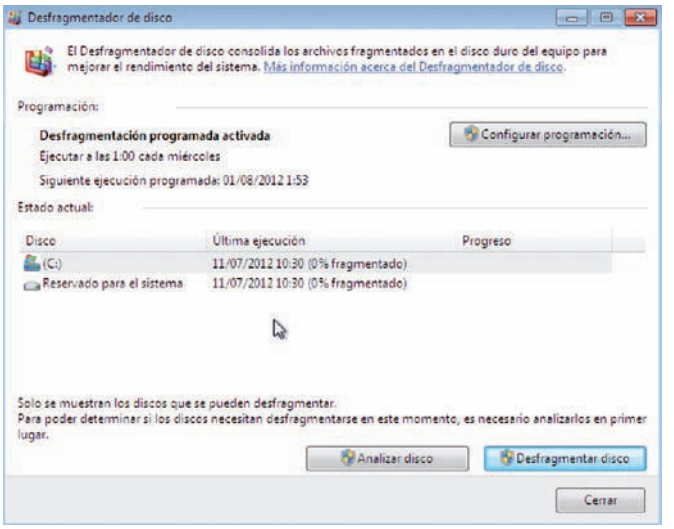


Fig. 5.57. *Operaciones con elevación.*

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.

```
profesor@ubuntu12:~$ fdisk -l /dev/sda
No se puede abrir /dev/sda
profesor@ubuntu12:~$ id
uid=1000(profesor) gid=1000(profesor) grupos=1000(profesor),4(adm),24(cdrom),27(
sudo),30(dip),46(plugdev),111(lpadmin),112(sambashare)
profesor@ubuntu12:~$ sudo -i
root@ubuntu12:~# id
uid=0(root) gid=0(root) grupos=0(root)
root@ubuntu12:~# fdisk -l /dev/sda

Disco /dev/sda: 8589 MB, 8589934592 bytes
255 cabezas, 63 sectores/pista, 1044 cilindros, 16777216 sectores en total
Unidades = sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico / físico): 512 bytes / 512 bytes
Tamaño E/S (mínimo/óptimo): 512 bytes / 512 bytes
Identificador del disco: 0x000380b5

Dispositivo Inicio    Comienzo       Fin     Bloques  Id  Sistema
/dev/sda1   *          2048    15720639     7063296   83  Linux
/dev/sda2        15730686    16775167      522241    5  Extendida
/dev/sda5        15730688    16775167      522240   82  Linux swap / Solaris
root@ubuntu12:~#
```

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).

```
$ id
uid=1002(limitado) gid=1002(limitado) grupos=1002(limitado)
$ fdisk -l /dev/sda
No se puede abrir /dev/sda
$ sudo -i
[sudo] password for limitado:
limitado no está en el archivo sudoers. Se informará de este incidente.
$
```

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.

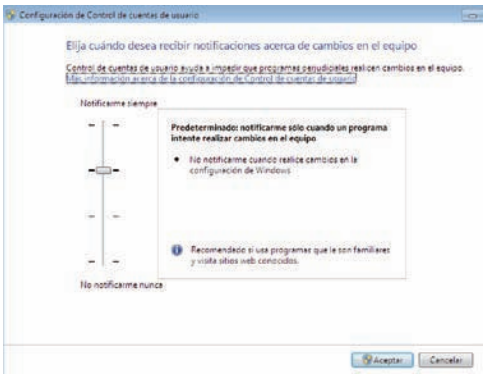


Fig. 5.60. *Configuración de UAC.*

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.).

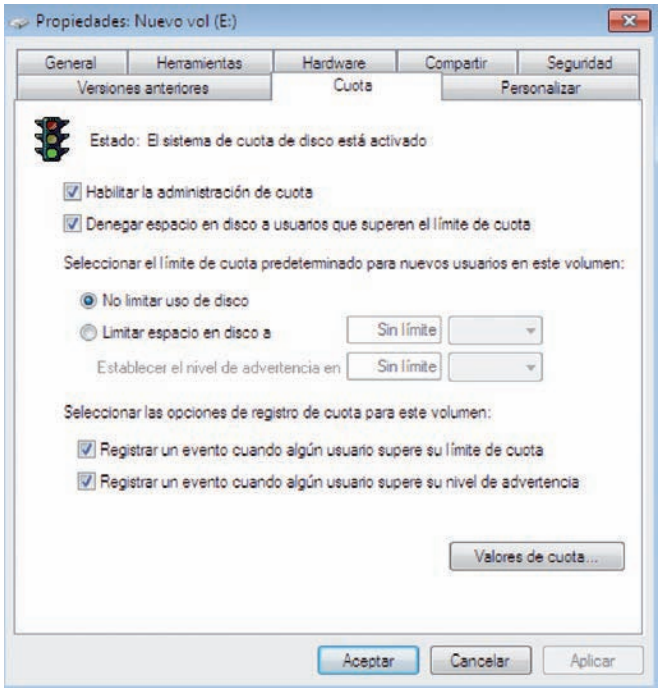


Fig. 5.61. *Cuotas de disco en W7.*

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).

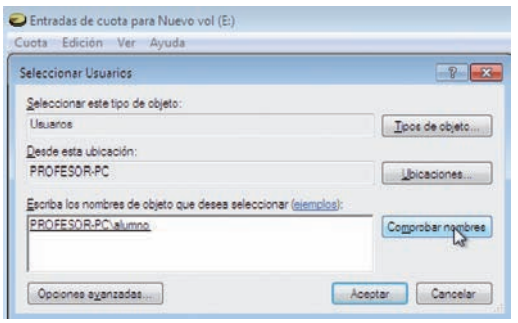


Fig. 5.62. *Elegimos usuario para cuota.*

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).

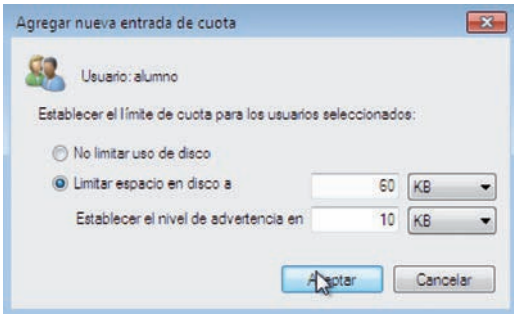


Fig. 5.63. *Valores de cuota.*

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).

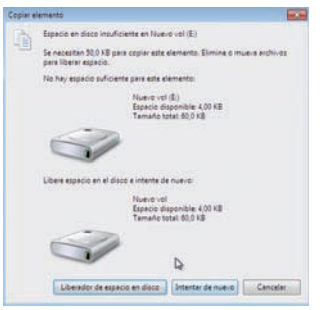


Fig. 5.64. *Cuota excedida.*

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

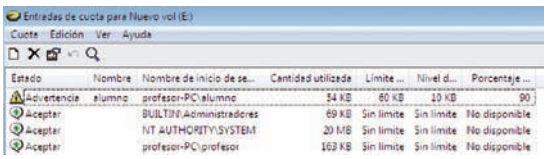


Fig. 5.65. *Estado de cuotas.*

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).

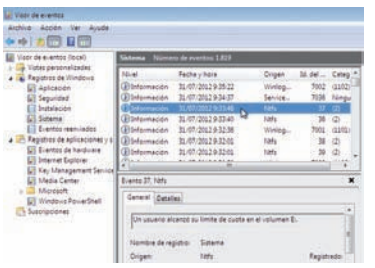


Fig. 5.66. *Evento registrado.*

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).

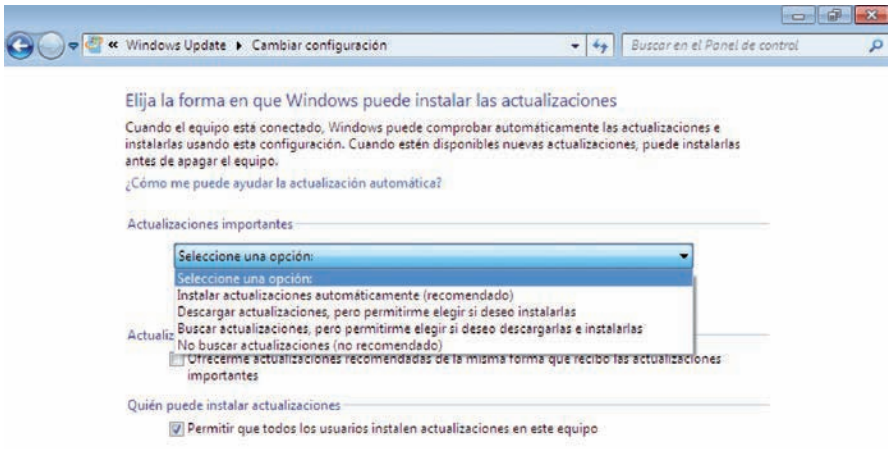


Fig. 5.67. *Actualizaciones W7.*

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).

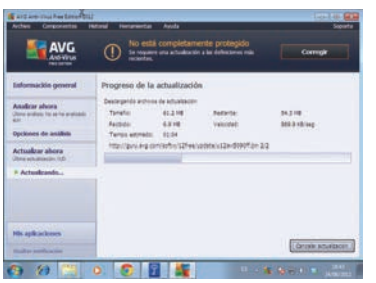


Fig. 5.70. *Actualización tras instalación.*

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.

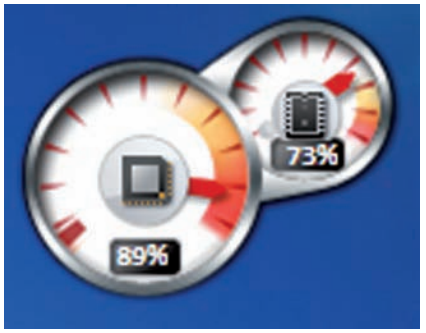


Fig. 5.72. *Gadget de rendimiento W7.*

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.

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 1?

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.

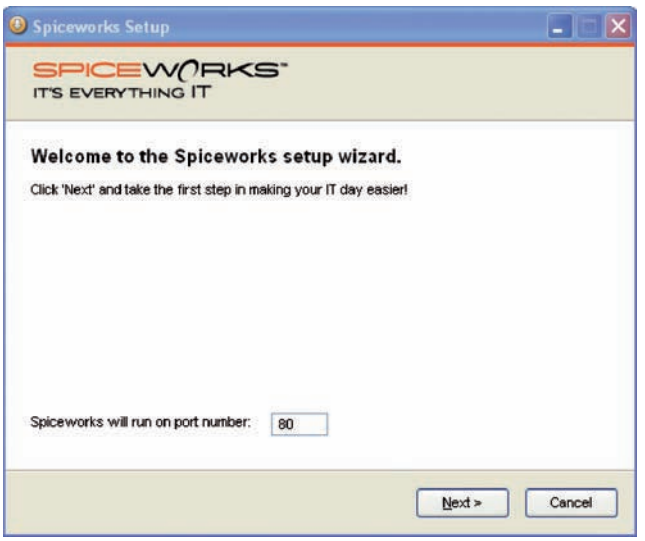


Fig. 5.73. *Puerto del servidor web de la herramienta.*

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).

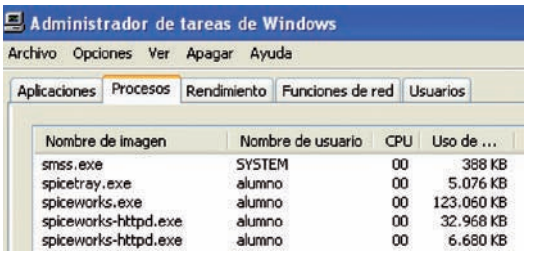


Fig. 5.74. *Procesos de la herramienta.*

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.

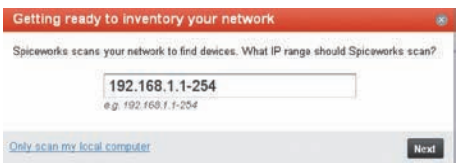


Fig. 5.75. *Rastreará la red de nuestros equipos.*

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.

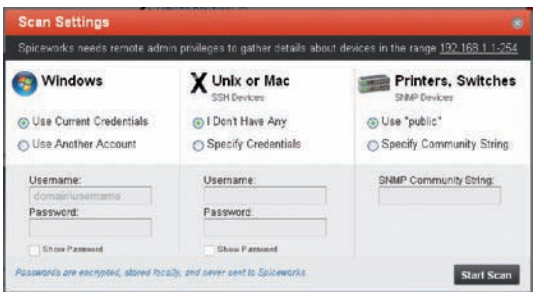


Fig. 5.76. *Credenciales disponibles.*

(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*.

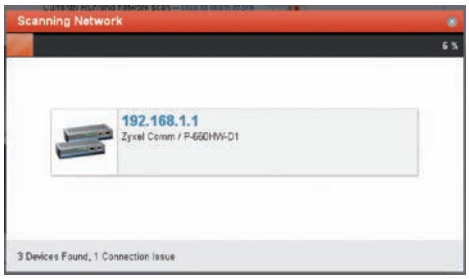


Fig. 5.77. *Escaneo en curso.*

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.

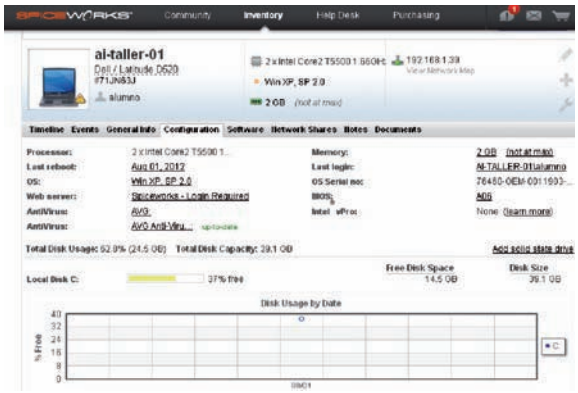


Fig. 5.80. *Configuración de la workstation detectada.*

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.

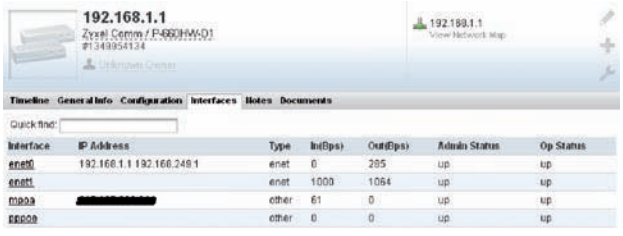


Fig. 5.82. *Configuración del router.*

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).

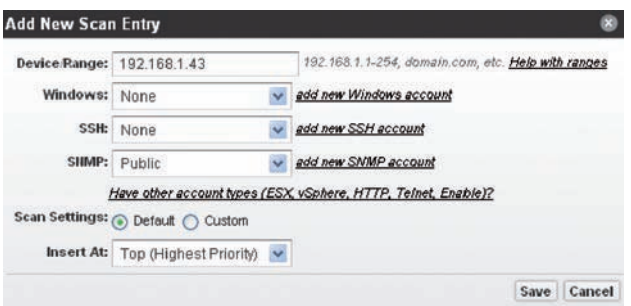


Fig. 5.84. *Escaneo particular.*

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).

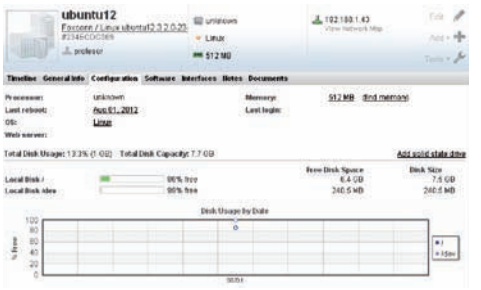


Fig. 5.85. *Configuración del servidor Linux detectado.*

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).

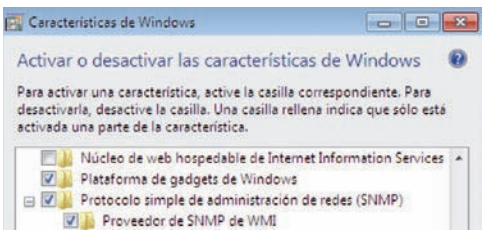


Fig. 5.86. *Activamos SNMP en W7.*

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).

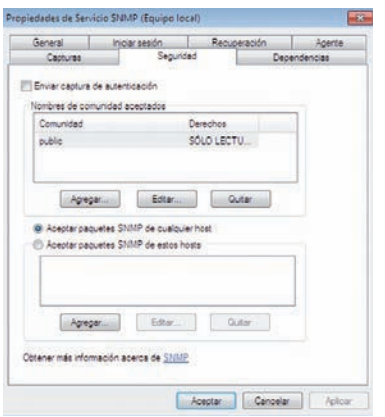


Fig. 5.87. *Configuramos SNMP en W7.*

(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).

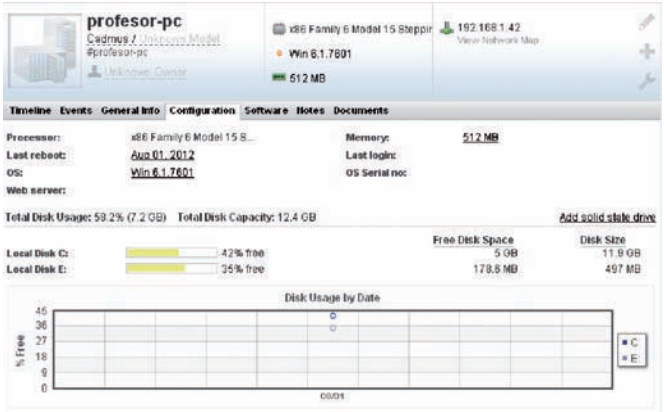


Fig. 5.88. *Configuración del W7 detectado.*

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).

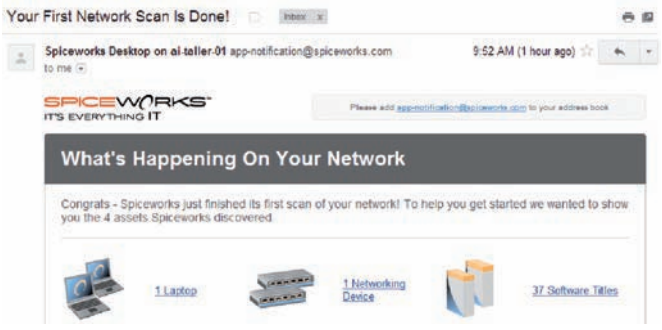


Fig. 5.89. *Correo enviado por la herramienta.*

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.

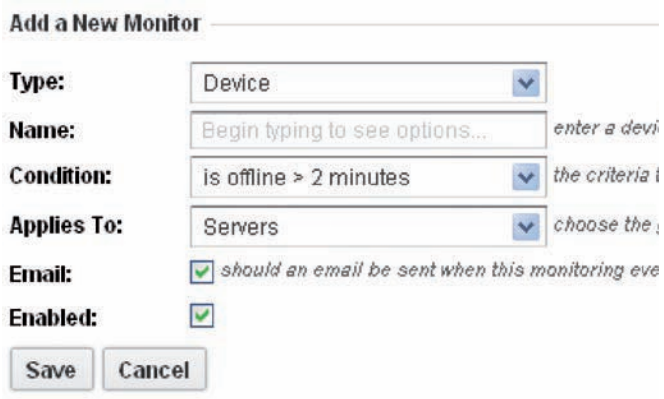


Fig. 5.90. *Nuevo monitor.*

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).

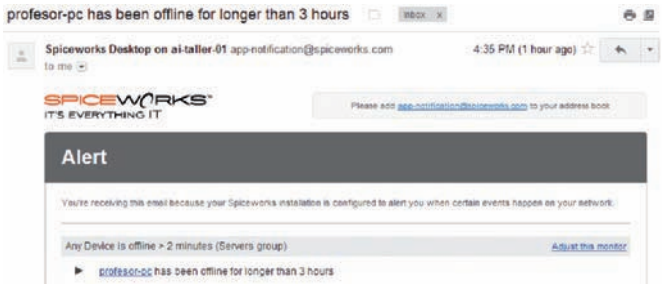


Fig. 5.92. *Correo con la alerta generada.*

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 wifi 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.

Unidad 6

Seguridad activa: acceso a redes



En esta unidad aprenderemos a:

- Identificar la necesidad de inventariar y controlar los servicios de red.
- Aplicar medidas para evitar la monitorización de redes cableadas.
- Clasificar y valorar las propiedades de seguridad de los protocolos usados en redes inalámbricas.

Y estudiaremos:

- El control de la monitorización en redes cableadas.
- Las listas de control de acceso.
- La seguridad en redes inalámbricas.
- La seguridad en los protocolos para comunicaciones inalámbricas.

1. Redes cableadas

Importante

Si los equipos conectados a la red utilizan entre sí protocolos seguros (HTTPS, SSH), la seguridad o inseguridad de la red es menos crítica. Pero todavía hay una mayoría de protocolos inseguros (DHCP, DNS, HTTP, etc.).

En las dos unidades anteriores hemos estudiado a fondo cómo proteger nuestra máquina junto con los datos y el software que ejecuta en ella. Pero en una empresa es raro encontrar una **máquina aislada.** Generalmente están **conectadas a una red** de área local (LAN [Local Area Network]) para utilizar los recursos de otras máquinas y para que otras máquinas aprovechen los suyos (por ejemplo, el disco en red NAS que vimos en la Unidad 4). El mismo celo que hemos puesto en vigilar la actividad que ocurre dentro de la máquina hay que mantenerlo cuando **los datos salen y entran** por alguna de sus interfaces de red.

También hay que **protegerse de los ataques que vengan por la red.** Una máquina que ofrece servicios TCP/IP debe abrir ciertos puertos. A estos puertos pueden solicitar conexión máquinas fiables siguiendo el protocolo estándar, o máquinas maliciosas siguiendo una variación del protocolo que provoca un fallo en nuestro servidor. Las consecuencias de este fallo serán, como mínimo, que el servicio queda interrumpido; pero en algunos casos el atacante puede tomar el control de la máquina (por eso cada vez más los servicios se ejecutan con el mínimo de privilegios).

Caso práctico 1

Conexiones establecidas en Windows 7

Duración: 10 minutos **Dificultad**: Fácil

Objetivo. Vamos a conocer cómo se sabe si un ordenador con Windows 7 está conectado a otra máquina.

Material. Ordenador con Windows 7, conexión a Internet, otro ordenador que ofrece un disco en red.

1. En Windows 7 lanzamos la herramienta del monitor de recursos. Podemos llegar a ella, por ejemplo, pulsando **Inicio** y tecleando *Monitor*. Nos aparecerán varias opciones (Fig. 6.1) y elegimos *Monitor de recursos*.

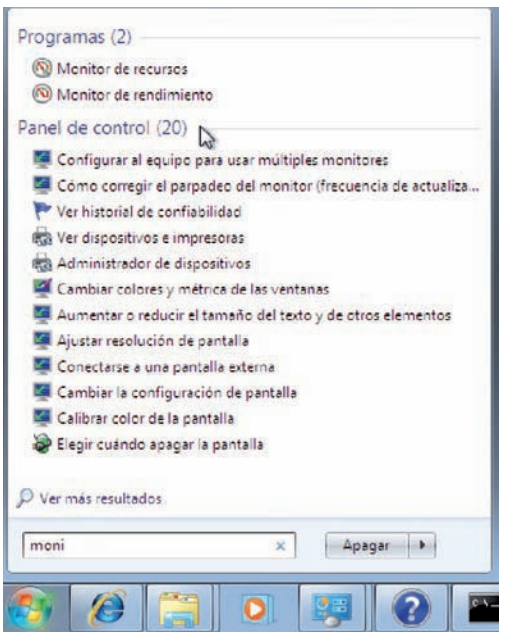


Fig. 6.1. *Buscamos el monitor de recursos.*

2. En la ventana del monitor de recursos nos vamos a la pestaña *Red* (Fig. 6.2). En la parte derecha tenemos unas gráficas de la evolución del uso de la red, y en la parte izquierda, unas listas. En este caso práctico nos centraremos en la primera, que son los procesos que están corriendo en la máquina y que tienen alguna actividad en la red, y la tercera, que son las conexiones TCP establecidas.

Si nos fijamos, aunque todavía no nos hemos conectado a nada, el sistema sí tiene actividad en la red: está buscando servicios, renovando la dirección recibida por DHCP, etc.

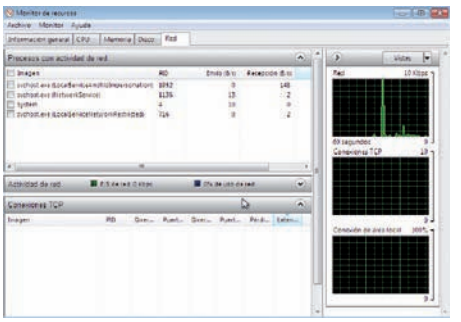


Fig. 6.2. *Monitor de recursos.*

3. Vamos a arrancar Internet Explorer para conectar con un servidor web. Puede ser una máquina de Internet o, como en el ejemplo, un servidor de nuestra red local en la dirección 10.0.1.1. En el monitor de recursos (Fig. 6.3) aparece el proceso iexplore con PID 1052 en la lista de procesos con actividad en la red, y en la lista de conexiones TCP una conexión del mismo proceso 1052 entre el puerto local 49157 de la dirección de nuestra máquina 10.0.1.10 y el puerto remoto 80 de la dirección del servidor 10.0.1.1.

(Continúa)

Caso práctico 1

(Continuación)

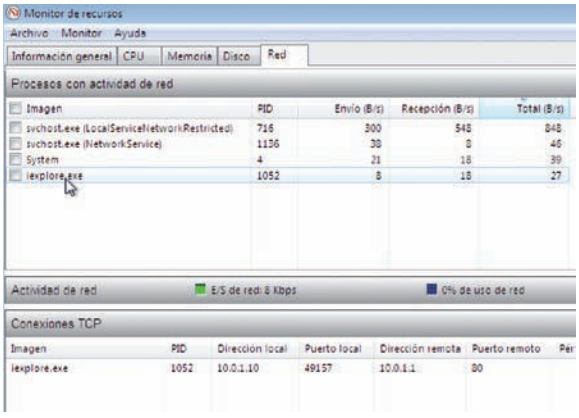


Fig. 6.3. *Conexión a servidor web.*

4. Sin cerrar el navegador, conectamos con la unidad de red (suponemos que está en el servidor 10.0.1.11). Aparecen nuevas conexiones (Fig. 6.4) entre puertos locales y los puertos 139 y 445 del servidor. Estos puertos son habituales en el protocolo SMB para acceso a discos en red.

5. Recurriremos a esta herramienta cuando la conexión a la red vaya sorprendentemente lenta. Si aparecen procesos extraños con altas tasas de transferencia (columnas de B/s, bytes por segundo), debemos sospechar que el ordenador tiene un troyano y deberíamos pasar un antivirus; si es un proceso conocido pero que no debería estar ahí (Torrent, por ejemplo), debemos pararlo. En ambos casos, podemos detenerlo inmediatamente: nos fijamos en su PID y vamos a la pestaña *CPU* para matarlo. Por ejemplo, vamos a matar el proceso del navegador web, que es el 1052.

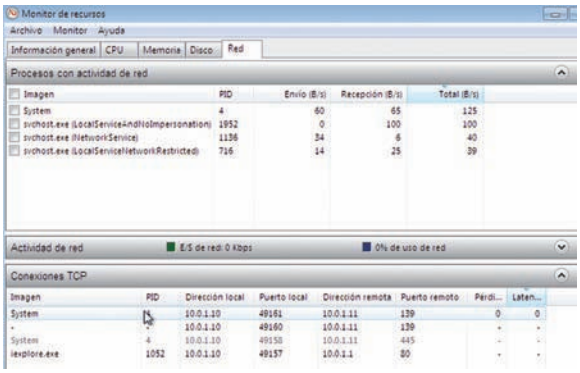


Fig. 6.4. *Conexión a disco en red.*

Las primeras redes LAN cableadas eran muy inseguras, porque todos los ordenadores estaban conectados al mismo cable (arquitectura en bus), de manera que cualquiera podía poner su tarjeta de red en modo promiscuo y escuchar todas las conversaciones, no solo aquellas en las que participaba.

Actualmente, este miedo prácticamente ha desaparecido, porque utilizamos la **arquitectura en estrella:** cada equipo tiene un cable directo a un puerto de un conmutador de red (switch) y por ahí envían sus paquetes; el switch los recibe y decide por qué puerto va a enviarlos para que lleguen al destino (Fig. 6.5). Además de mejorar la seguridad, estamos mejorando el rendimiento, porque no malgastamos recursos en enviar paquetes a equipos que no les interesan.

Vocabulario

Modo promiscuo. Por defecto, una tarjeta de red procesa solo los paquetes que van dirigidos a ella; al ponerla en modo promiscuo, procesa cualquier paquete que pasa por su interfaz.

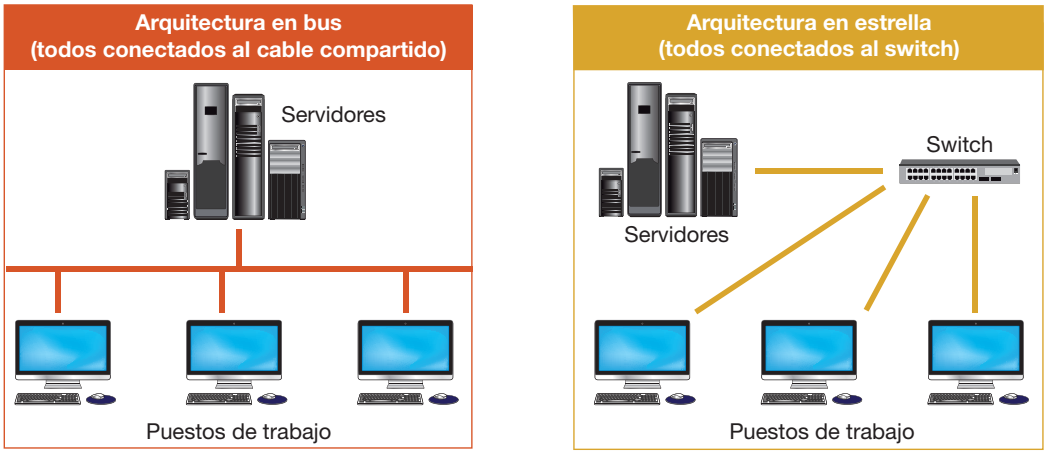


Fig. 6.5. *Arquitectura en bus y en estrella.*

Vocabulario

Switch gestionable. Conmutador de red con funcionalidades avanzadas de gestión: VLAN, autenticación en el puerto, estadísticas de tráfico, etc.

Actividades

1. Investiga el ataque de inundación contra un switch y cómo evitarlo.
2. Busca herramientas para detectar tarjetas en modo promiscuo.
3. Alguien podría directamente espiar nuestro cable (conectarlo a un hub propio y escuchar todas nuestras comunicaciones). Para protegernos, ¿tiene sentido hacer cifrado en los puertos del switch?

Sin embargo, las redes conmutadas tienen sus propias **vulnerabilidades:**

- Hay que **proteger el switch físicamente:** encerrarlo en un armario/rack con llave dentro de una sala con control de acceso. Así evitamos no solo el robo, sino que alguien acceda al botón de reset y lo configure a su modo.
- Hay que **proteger el switch lógicamente:** poner usuario/contraseña para acceder a su configuración.
- Hay que **hacer grupos de puertos,** porque en un switch suelen estar conectados grupos de máquinas que nunca necesitan comunicarse entre sí (por ejemplo, el departamento de marketing con el departamento de soporte). Debemos aislarlas para evitar problemas de rendimiento y seguridad.
- Hay que **controlar** qué equipos se pueden conectar y a qué puertos. Por el motivo anterior, al grupo de marketing solo deberían entrar máquinas de marketing.

En los capítulos siguientes profundizamos en estos problemas y las soluciones disponibles.

1.1. VLAN

Los grupos de puertos que hacemos en un switch gestionable para aislar un conjunto de máquinas constituyen una VLAN **(LAN virtual).** Se le llama virtual porque parece que están en una LAN propia, que la red está montada para ellos solos. Como hemos dicho antes, **utilizar VLAN mejora el rendimiento y la seguridad,** porque esas máquinas solo hablan entre ellas y nadie extraño las escucha. Al mismo tiempo, si ocurre un problema en una VLAN (un ataque, un problema de un servidor DHCP descontrolado), las otras VLAN no se ven afectadas. Pero un exceso de tráfico en una VLAN sí afectaría a todos porque, al fin y al cabo, comparten el switch.

Caso práctico 2

Configurar VLAN

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

Objetivo. Configurar VLAN en un switch.

Material. Switch con capacidad VLAN (en nuestro caso, un DLink DGS-1216T) y cuatro ordenadores.

1. Conectamos los cuatro ordenadores al switch. Uno de los ordenadores será la consola desde donde aplicaremos los cambios de configuración. Conviene recordar el puerto donde hemos pinchado cada uno, para evitar aislar la consola y perder el control del switch (habría que resetearlo).
2. En el ordenador de la consola abrimos el navegador y nos conectamos con el servidor web que gestiona la configuración del switch. En nuestro caso es la dirección 192.168.10.34. Si no recordamos la dirección o la contraseña, podemos resetear el router para que vuelva a la dirección por defecto y la contraseña por defecto.
3. Introducimos la contraseña (no hay más usuario que el administrador) para acceder a la página principal. En el menú de la izquierda podemos cambiar la contraseña en *System > Password Access Control* (Fig. 6.6).

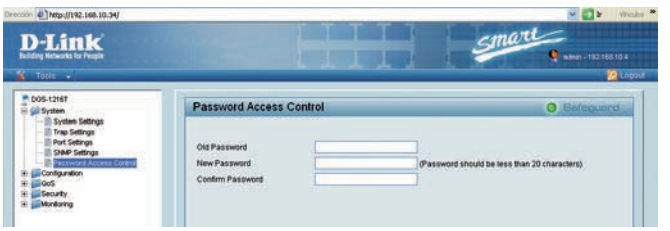


Fig. 6.6. *Cambio de clave en el switch.*

4. La configuración de las VLAN está bajo *Configuration > 802.1Q VLAN* (Fig. 6.7). Hay una VLAN por defecto en la que están incluidos todos los puertos (16). En nuestro caso tiene el VID (identificador de VLAN) con valor 01.

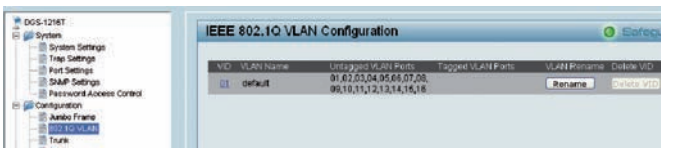


Fig. 6.7. *VLAN por defecto.*

(Continúa)

Caso práctico 2

(Continuación)

5. Vamos a uno de los ordenadores (lo llamaremos PC1 con dirección IP `10.0.1.1`) y probamos la conectividad con los otros dos (PC2 con dirección `10.0.1.2` y PC3 con dirección `10.0.1.3`). Para ello utilizamos el comando `ping` (Fig. 6.8).

```
C:\Documents and Settings\tic>ping -n 2 10.0.1.2

Haciendo ping a 10.0.1.2 con 32 bytes de datos:

Respuesta desde 10.0.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.1.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.0.1.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\tic>ping -n 2 10.0.1.3

Haciendo ping a 10.0.1.3 con 32 bytes de datos:

Respuesta desde 10.0.1.3: bytes=32 tiempo=2ms TTL=64
Respuesta desde 10.0.1.3: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 10.0.1.3:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Documents and Settings\tic>
```

Fig. 6.8. *Conectividad desde PC1.*

6. Para asegurarnos, hacemos lo mismo de PC3.

7. Vamos a crear una VLAN que incluya solo a PC1 y PC2 y deje fuera a PC3. Primero hay que sacar esos puertos de la VLAN por defecto. En el ordenador de consola pulsamos sobre su VID y sacamos los puertos 7 y 8, que corresponden a PC1 y PC2, respectivamente (Fig. 6.9).

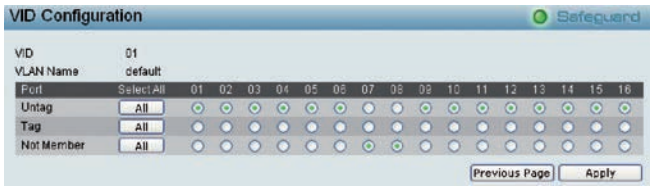


Fig. 6.9. *Sacamos puertos de VLAN por defecto.*

8. Pulsamos *Apply* para aplicar los cambios. Ahora esos puertos no tienen conexión con nadie: ni siquiera entre ellos. Para comprobarlo, vamos de nuevo a PC1 y miramos su conectividad. Ya no encuentra a nadie.

9. Ahora creamos la nueva VLAN. En la página de las VLAN pulsamos el botón *Add VID*. Le ponemos 02 como VID, le llamamos prueba y de la lista de puertos *Not Member* elegimos el 7 y el 8 (Fig. 6.10) y los marcamos como *Untagged* (sin etiqueta: las etiquetas las veremos más adelante).

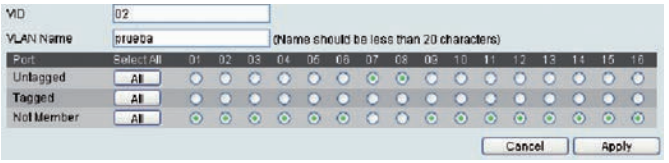


Fig. 6.10. *Creamos VLAN nueva.*

10. Pulsamos *Apply* y ya tenemos la VLAN lista. En la Fig. 6.11 vemos las dos VLAN con los puertos que les pertenecen a cada una.



Fig. 6.11. *VLAN creada.*

11. Para comprobarlo, volvemos a PC1 y comprobamos que ve a PC2 pero no a PC3 (Fig. 6.12).

```
C:\Documents and Settings\tic>ping -n 2 10.0.1.2

Haciendo ping a 10.0.1.2 con 32 bytes de datos:

Respuesta desde 10.0.1.2: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.1.2: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 10.0.1.2:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\tic>ping -n 2 10.0.1.3

Haciendo ping a 10.0.1.3 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 10.0.1.3:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),

C:\Documents and Settings\tic>_
```

Fig. 6.12. *PC1 ve a PC2 pero no a PC3.*

12. Si nos vamos a PC3, no tiene conectividad con ninguno (Fig. 6.13).

```
root@profesor-VirtualBox:~# ping -c 2 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.

--- 10.0.1.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1000ms

root@profesor-VirtualBox:~# ping -c 2 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.

--- 10.0.1.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1003ms

root@profesor-VirtualBox:~#
```

Fig. 6.13. *PC aislado.*

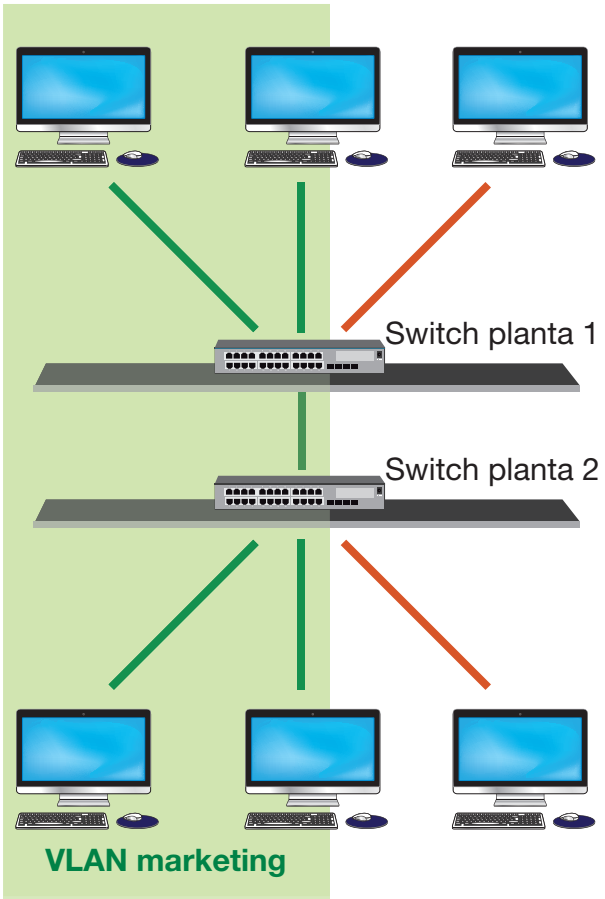


Fig. 6.14. *VLAN entre dos switch.*

Una VLAN basada en grupos de puertos no queda limitada a un switch; uno de los puertos puede estar conectado al puerto de otro switch, y, a su vez, ese puerto forma parte de otro grupo de puertos, etc. Por ejemplo, cuando el departamento de marketing tiene parte de su personal en la primera planta y parte en la segunda, hay que dejar un puerto en cada switch para interconectarlos. En la Figura 6.14 tenemos dos equipos en cada planta, por lo que ocuparían tres puertos en cada switch.

Sin embargo, es raro que las VLAN estén completamente aisladas del resto del mundo. Como mínimo, necesitarán acceso a Internet, así como conectar con otros servidores internos de la empresa (intranet, disco, backup, correo, etc.). **Para interconectar VLAN (capa 2) generalmente utilizaremos un router (capa 3).**

Capa 2. En el modelo TCP/IP la capa 2 o capa de enlace tiene una visión local de la red: sabe cómo intercambiar paquetes de datos (llamados tramas) con los equipos que están en su misma red. La comunicación es directa entre origen y destino (aunque cruce uno o varios switch).

Capa 3. La capa 3 o capa de red tiene una visión global de la red: sabe cómo hacer llegar paquetes de datos hasta equipos que no están en su misma red. La comunicación es indirecta, necesita pasar por una máquina más: el router.

El router necesitará conectividad con cada una de las VLAN que interconecta. Una forma de conseguirlo es reservarle un puerto en cada una, pero nos llevaría a instalar muchas tarjetas en el router. Una solución alternativa es utilizar el segundo tipo de VLAN: **VLAN etiquetada** (tag).

La configuración más simple de VLAN etiquetada mantiene los grupos de puertos, pero el que los conectará con el router tiene una configuración distinta: **el switch añadirá una etiqueta** (un número) a los paquetes de datos (tramas) que salen por ese puerto. Estos paquetes ya pueden viajar por el mismo cable que los paquetes de otras VLAN sin interferirse entre ellos (conservamos el aislamiento entre VLAN), porque llegarán solo a los puertos donde la interfaz de red sea capaz de interpretar ese tag. En la Figura 6.15, el tráfico azul (VLAN de soporte) sale por el mismo puerto que el tráfico verde, y lo mismo para la VLAN de marketing (todas las conexiones son un único cable, aunque transporten distintos tráficos). El router solo necesita un cable hasta el switch donde llegan todos los flujos, porque internamente utiliza subinterfaces para tratar el tráfico de las distintas VLAN, como veremos en el caso práctico 3.

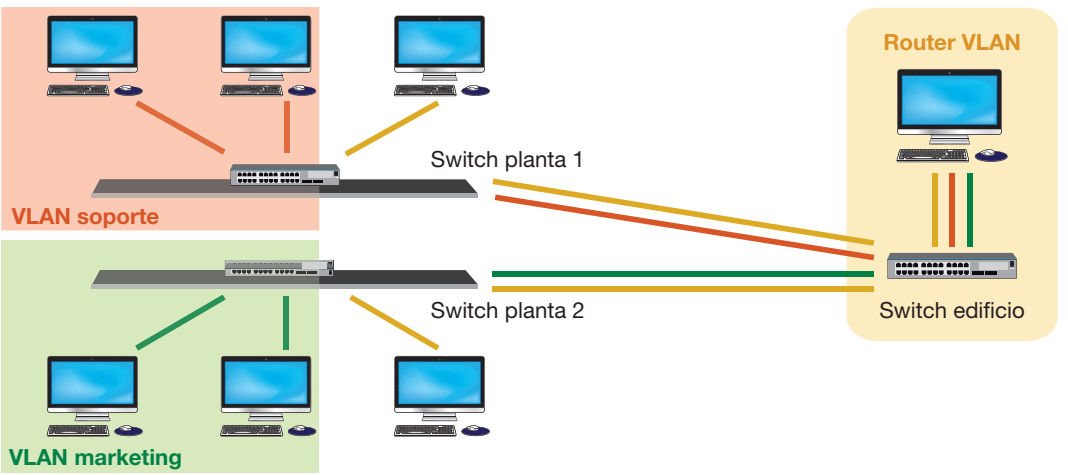


Fig. 6.15. *VLAN etiquetada.*

Caso práctico 3

Trabajar con VLAN etiquetadas en un router Linux

■ **Duración**: 30 minutos ■ **Dificultad**: Media

Objetivo. Configurar la interconexión de dos VLAN mediante un router utilizando VLAN etiquetadas.

Material. Switch gestionable con capacidad de VLAN etiquetada (en nuestro caso, un DLink DGS-1216T), switch no gestionable y seis ordenadores (uno con Linux; el resto pueden ser Windows o Linux).

1. De los seis ordenadores, reservamos uno con Linux para que haga de router. El resto los conectamos al switch gestionable. Es importante apuntar en qué puerto ponemos cada uno para no confundirnos más adelante.
2. Como en el caso práctico 2, uno de los ordenadores estará reservado para los cambios de configuración en el switch. En ese ordenador, abrimos un navegador para conectar con el servidor web del switch. Introducimos la contraseña y comprobamos que todos los puertos están en la VLAN por defecto (Fig. 6.16).

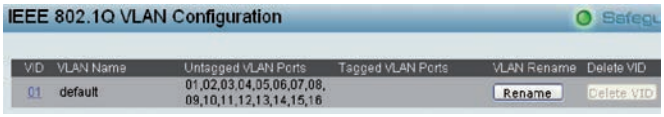


Fig. 6.16. *Todos en VLAN por defecto.*

3. Vamos a asignar direcciones a los ordenadores. De los cinco que quedan, cuatro serán los equipos de las VLAN, y el último será el router que las conecta. Pondremos dos equipos en cada VLAN. Las direcciones serán `10.0.1.2/8` para PC12, `10.0.1.3/8` para PC13, `10.0.2.2/8` para PC22 y `10.0.2.3/8` para PC23. Con esa máscara de red se pueden ver entre ellos; lo comprobamos desde PC12 (Fig. 6.17).

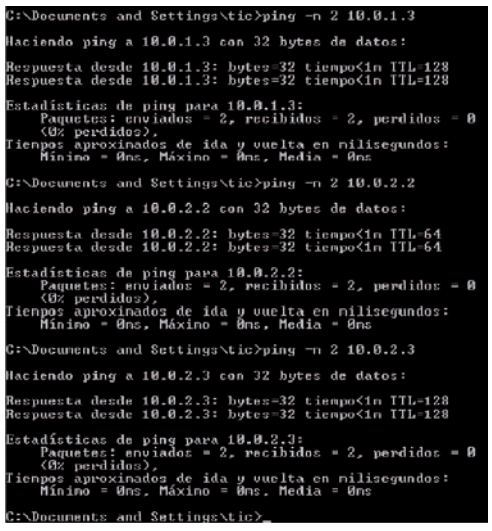


Fig. 6.17. *PC12 ve a todos.*

4. Como ya sabemos, para crear las VLAN primero hay que quitar los puertos de la VLAN por defecto. En este ejemplo PC12 y PC13 están en los puertos 7 y 8, y PC22 y PC23 en los 15 y 16 (Fig. 6.18).

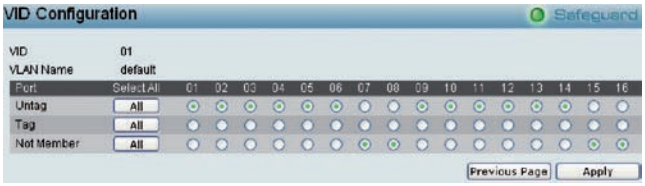


Fig. 6.18. *Sacamos los puertos para crear dos VLAN.*

5. Creamos las dos VLAN de puertos: una la identificamos como *VLAN11* con VID 11 y le ponemos los puertos 6, 7 y 8 (añadimos el 6 para conectar al router); la otra será *VLAN12* con VID 12 y los puertos 14, 15 y 16 (el 14 lo utilizaremos para conectar al router).
6. Podemos repetir el paso 3 para comprobar que se han creado bien (Fig. 6.19).

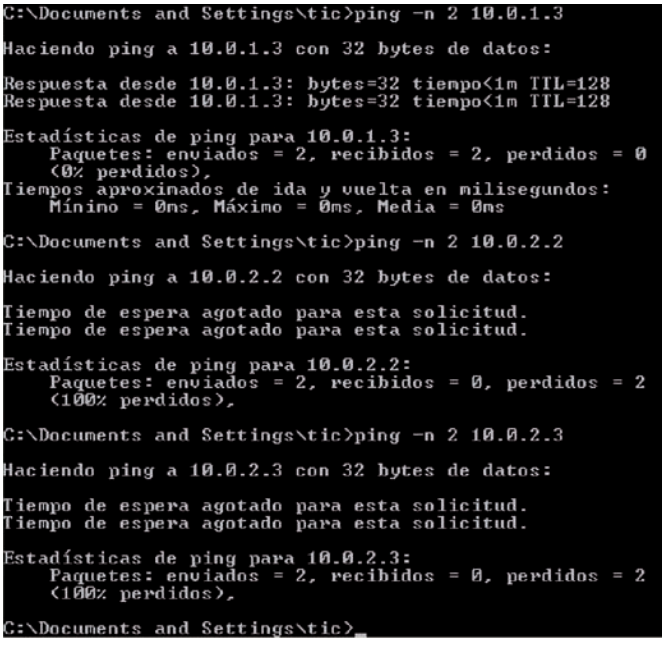


Fig. 6.19. *PC12 solo ve a PC13.*

7. Podemos probar a conectar las dos VLAN mediante un cable entre los puertos 6 y 14, y volveríamos a la situación inicial en que todos los ordenadores estaban accesibles, aunque aislados del resto de los puertos del switch.
8. Seguimos con nuestra práctica de VLAN etiquetada. Vamos a marcar el puerto que llevará la etiqueta. Entramos en la configuración de *VLAN11*, y el puerto 6 lo pasamos de *Untag* a *Tag* (Fig. 6.20).

(Continúa)

Caso práctico 3

(Continuación)

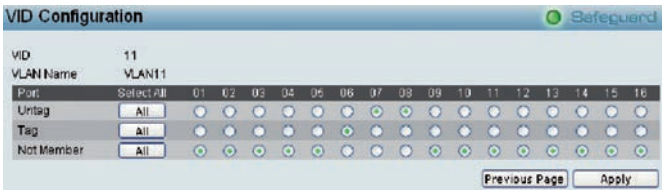


Fig. 6.20. *Marcamos puertos.*

9. Hacemos lo mismo con el puerto 14 de *VLAN12*. La Figura 6.21 nos muestra la configuración final.

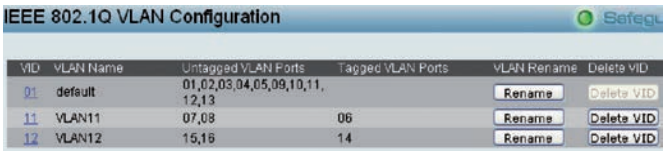


Fig. 6.21. *Puertos marcados.*

10. Ahora vamos a conectar y configurar el último ordenador con Linux para que vea las VLAN como router. Para ello utilizamos el switch no gestionable. Enchufamos en este switch tres cables: uno al router, uno al puerto 6 y otro al puerto 14.

11. En el router instalamos el soporte a VLAN mediante `apt-get install vlan` (si necesitamos conexión a Internet para descargarlo, podemos desconectar y volver a conectar al switch). A continuación configuramos las subinterfaces (Fig. 6.22):

```
# modprobe 8021q
# vconfig add eth0 11
# ifconfig eth0.11 10.0.1.1/24
# vconfig add eth0 21
# ifconfig eth0.21 10.0.2.1/24
```

El comando `modprobe 8021q` instala el módulo que entiende las VLAN del estándar 802.1Q, que es el referente para VLAN etiquetadas.

```
root@alumno-Latitude-D520:~# vconfig add eth0 11
Added VLAN with VID == 11 to IF -:eth0:-
root@alumno-Latitude-D520:~# ifconfig eth0.11 10.0.1.1/24
root@alumno-Latitude-D520:~# vconfig add eth0 21
Added VLAN with VID == 21 to IF -:eth0:-
root@alumno-Latitude-D520:~# ifconfig eth0.21 10.0.2.1/24
root@alumno-Latitude-D520:~#
```

Fig. 6.22. *Interfaces VLAN en el router.*

El comando `vconfig` crea una subinterfaz que entiende una VLAN. El primer parámetro es la operación (`add` añade, `rem` elimina), el segundo es la interfaz donde llega el tráfico (`eth0` en nuestro caso) y el tercero es el VID (11 y 12, como hemos definido en el switch).

Finalmente, asignamos direcciones a las nuevas interfaces `eth0.11` y `eth0.21` (son interfaces normales: aparecen en `ifconfig`). Les ponemos máscara `/24` para que el router vea cada red por separado.

12. Si lo hemos hecho bien, el router debería ver los equipos de las dos VLAN (Fig. 6.23).

```
root@alumno-Latitude-D520:~# ping -c 2 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
64 bytes from 10.0.1.2: icmp_req=1 ttl=128 time=0.399 ms
64 bytes from 10.0.1.2: icmp_req=2 ttl=128 time=0.275 ms

--- 10.0.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.275/0.337/0.399/0.062 ms
root@alumno-Latitude-D520:~# ping -c 2 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_req=1 ttl=64 time=0.518 ms
64 bytes from 10.0.2.2: icmp_req=2 ttl=64 time=0.359 ms

--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.359/0.438/0.518/0.082 ms
root@alumno-Latitude-D520:~#
```

Fig. 6.23. *El router ve a todos.*

13. Para conseguir intercambiar tráfico entre ellas solo hay que activar el `ip _ forward` en el router, y en los equipos cambiar las máscaras de red para que sean /24 en lugar de /8 y poner como puerta de enlace la interfaz correspondiente del router (`10.0.1.1` para PC12 y PC13, `10.0.2.1` para PC22 y PC23).

Vocabulario

Dirección MAC (Medium Access Control). Dirección de nivel 2 (nivel de enlace) de una tarjeta de red. En Ethernet son 48 bits que se representan como seis parejas de números hexadecimales (1A-2B-3C-4D-5E-6F). Esta dirección es asignada por el fabricante, por lo que no hay dos tarjetas con la misma MAC.

1.2. Autenticación en el puerto. MAC y 802.1X

Hemos protegido el acceso al switch y repartido las máquinas de la empresa en varias VLAN, interconectadas por routers. Pero cualquiera puede meterse en un despacho, desconectar el cable RJ45 del ordenador del empleado, conectarlo a su portátil y ya estaría en esa VLAN. Como sigue siendo un switch, no podrá escuchar el tráfico normal de los demás ordenadores de la VLAN, pero sí lanzar ataques contra ellos.

Para evitarlo, los switch permiten establecer **autenticación en el puerto:** solo podrá conectar aquel cuya MAC esté dentro de una lista definida en el propio switch, o, dado que las MAC son fácilmente falsificables (las tarjetas emiten los paquetes que genera el software de red del sistema operativo), el que sea autentificado mediante RADIUS en el estándar 802.1X.

Caso práctico 4

Autenticación en el puerto

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

Objetivo. Limitar los equipos que pueden conectar a un switch.

Material. Cuatro ordenadores (uno con Linux), un switch no gestionable y un switch gestionable con autenticación en el puerto mediante MAC y 802.1X (en este ejemplo, DLink DGS-1216T).

1. Como en los casos anteriores, uno de los ordenadores estará conectado al switch para aplicar los cambios de configuración. Reservamos un ordenador con Linux para el servidor RADIUS de la configuración 802.1X. Los otros dos ordenadores hacen de equipos cliente y los conectamos a un switch no gestionable, y un tercer puerto de este switch lo conectamos a un puerto del switch gestionable (en este ejemplo, el puerto 9). El switch gestionable tiene salida a Internet. Probamos esa conectividad desde alguno de los equipos (Fig. 6.24).

```
C:\Documents and Settings\tic>ping -n 2 terra.es

Haciendo ping a terra.es [208.84.244.10] con 32 bytes de datos:

Respuesta desde 208.84.244.10: bytes=32 tiempo=593ms TTL=243
Respuesta desde 208.84.244.10: bytes=32 tiempo=620ms TTL=243

Estadísticas de ping para 208.84.244.10:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 593ms, Máximo = 620ms, Media = 606ms

C:\Documents and Settings\tic>
```

Fig. 6.24. *Conectividad disponible.*

2. Entramos en el switch y comprobamos que los equipos cliente están conectados. Para ello entramos en *Security > MAC Address Table > Dynamic Forwarding Table* y miramos el puerto 9. Aparecerán las MAC de los dos equipos (Fig. 6.25).

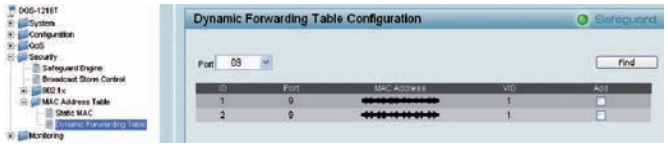


Fig. 6.25. *Dos PC en el mismo puerto.*

En esta tabla se guardan las direcciones que el switch va aprendiendo según se conectan equipos a sus puertos; así sabe por dónde enviar cada paquete.

3. Para limitar los equipos que se pueden conectar vamos a desactivar el mecanismo de autoaprendizaje de direcciones MAC y fijaremos la lista de direcciones autorizadas. En ese mismo menú entramos en *Static MAC*. Deshabilitamos el *Auto Learning* (salvo el puerto que nos conecta a Internet, en nuestro caso el 5, porque ahí hay muchas máquinas y ya está ocupado) y añadimos dos direcciones a la lista: la dirección de uno de los equipos cliente en el puerto 9 y la dirección de nuestra consola en puerto 13 (así podemos seguir aplicando cambios). En la Figura 6.26 tenemos la nueva configuración.

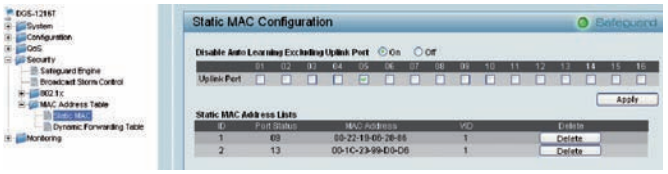


Fig. 6.26. *Fijamos MAC en cada puerto.*

4. Aplicamos los cambios y podemos comprobar que, aunque el equipo cliente que hemos excluido (dirección IP terminada en 36.82) puede conectar con el otro equipo (dirección 36.42), pues comparten el switch no gestionable, no puede ir más allá (Fig. 6.27).

```
C:\Documents and Settings\alumno>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local          :

        Sufijo de conexión específica DNS :
        Dirección IP. . . . . . . . . . . . : 192.168.36.82
        Máscara de subred . . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada     : 192.168.36.1

Adaptador Ethernet Conexiones de red inalámbricas          :

        Estado de los medios. . . .: medios desconectados

C:\Documents and Settings\alumno>ping -n 2 192.168.36.42

Haciendo ping a 192.168.36.42 con 32 bytes de datos:

Respuesta desde 192.168.36.42: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.36.42: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.36.42:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\alumno>ping -n 2 192.168.36.1

Haciendo ping a 192.168.36.1 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.36.1:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),

C:\Documents and Settings\alumno>
```

Fig. 6.27. *Equipo excluido.*

5. Deshacemos los cambios para probar la configuración 802.1X. En esta configuración el switch pedirá usuario y contraseña para dejar conectar a sus puertos. Y estas contraseñas no las tiene él, sino que se almacenan en una base de datos gestionada mediante RADIUS. Cuando un ordenador se enchufa a un puerto, el switch le pide la identificación y lo que reciba lo consulta en el RADIUS. Si no está autorizado, no podrá conectar en ese puerto.

(Continúa)

Caso práctico 4

(Continuación)

6. Nos vamos al ordenador Linux para instalar el servidor RADIUS. Instalaremos el software mediante `apt-get install freeradius`.

7. Hay que configurar tres ficheros. Primero, la lista de clientes «preguntones», porque el servidor solo atenderá preguntas que vengan de ellos. La configuración del cliente incluye una contraseña porque cualquiera podría falsificar su IP con la de un cliente auténtico. Está en el fichero `/etc/freeradius/clients.conf` y en nuestro caso habría que añadir estas líneas:

```
client 192.168.10.34 {
secret nolasabes1
}
```

Lo segundo es la lista de usuarios y contraseñas que queremos comprobar. Está en el fichero `/etc/freeradius/users`. En nuestro caso añadiremos una línea con el usuario `profe` y la contraseña `test1234`. La línea sería:

```
profe Cleartext-Password := «test1234»
```

Tanto en ese caso como en el anterior, no es demasiado problema que las contraseñas estén en texto claro, porque al directorio `/etc/freeradius` solo tiene acceso `root`.

En la Figura 6.28 vemos la configuración elegida.

```
druxr-s--x 2 freerad freerad  4096 jul 11 17:31 sites-available
druxr-xr-x 2 root    root     4096 jul 11 17:31 modules
druxr-s--x 2 freerad freerad  4096 jul 11 17:32 sites-enabled
druxr-s--x 2 freerad freerad  4096 jul 11 17:33 certs
-rw-r----- 1 root    freerad 18085 jul 12 13:47 eap.conf
-rw-r----- 1 root    freerad  6748 jul 12 14:12 clients.conf
-rw-r--r-- 1 root    root     6563 jul 12 14:13 users
root@ubuntu12:/etc/freeradius# tail clients.conf
#  will then accept ONLY the clients listed in this section.
#
#clients per_socket_clients {
#       client 192.168.3.4 {
#               secret = testing123
#       }
#}
client 192.168.10.34 {
secret = nolasabes1
}
root@ubuntu12:/etc/freeradius# tail users
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User

# On no match, the user is denied access.
profe Cleartext-Password := "test1234"
root@ubuntu12:/etc/freeradius#
```

Fig. 6.28. *Configuración de clientes y usuarios.*

8. El tercer fichero es el tipo de autenticación. Como estamos usando contraseñas en texto plano, debemos modificar el fichero `/etc/freeradius/eap.conf` para utilizar `PEAP`. Hay que sustituir `md5` por `peap` en la línea que asigna `default _ eap _ type` (Fig. 6.29).

```
        eap {
                #default_eap_type = md5
                default_eap_type = peap
```

Fig. 6.29. *Configuración del tipo de autenticación.*

9. A continuación paramos el servidor y lo arrancamos de nuevo desde la shell, para ver las peticiones que recibe (Fig. 6.30).

```
# server freeradius stop
# freeradius -X
```

```
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
Listening on proxy address * port 1814
Ready to process requests.
```

Fig. 6.30. *Arrancamos freeradius en la shell.*

10. Volvemos a la configuración del switch. Entramos en *Security > 802.1x > 802.1x Settings*. Aquí podemos activar este control y configurarlo. La configuración tiene dos partes: una parte con los datos del servidor RADIUS y la contraseña de nuestro cliente, y otra parte con los puertos concretos donde queremos activarlo. En nuestro ejemplo (Fig. 6.31) pondremos la dirección del servidor Linux (`192.168.10.4`) y la contraseña nolasabes1 (como es habitual, la introducimos dos veces, para reducir la posibilidad de error).

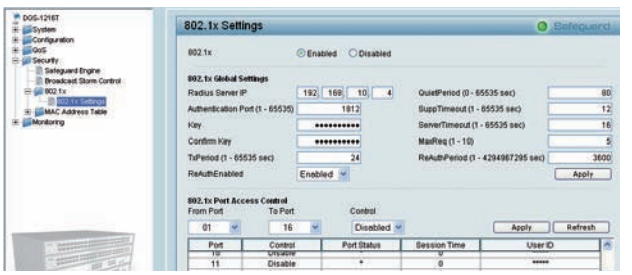


Fig. 6.31. *Configuración RADIUS en el switch.*

11. En la lista de los puertos activaremos el control en el puerto 13, donde tenemos conectados los ordenadores cliente (Fig. 6.32).

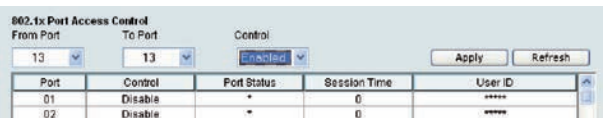


Fig. 6.32. *Control en el puerto 13.*

12. Pulsamos *Apply* y ya está listo para aplicar la autorización mediante usuario y contraseña.

(Continúa)

Caso práctico 4

(Continuación)

13. Los equipos conectados al puerto 13 ahora deben aportar la identificación. Si tenemos un XP, la tarjeta de red avisa como en la Figura 6.33.



Fig. 6.33. *La tarjeta avisa del problema.*

14. Tenemos que ajustar algún parámetro en la configuración de la tarjeta para que dialogue correctamente con el switch. Pulsamos en *Propiedades* y después en la pestaña *Autenticación*. Activamos la primera opción y elegimos `PEAP`. Pulsamos en *Propiedades* y desactivamos *Validar un certificado de servidor* (estamos utilizando la validación más simple). En la parte inferior de esa ventana elegimos *EAP-MSCHAP v2,* y pulsando en *Propiedades* desactivamos que utilice el mismo usuario y contraseña con el que estamos presentados en Windows (en RADIUS hemos configurado `profe`). La secuencia de ventanas aparece en la Figura 6.34.

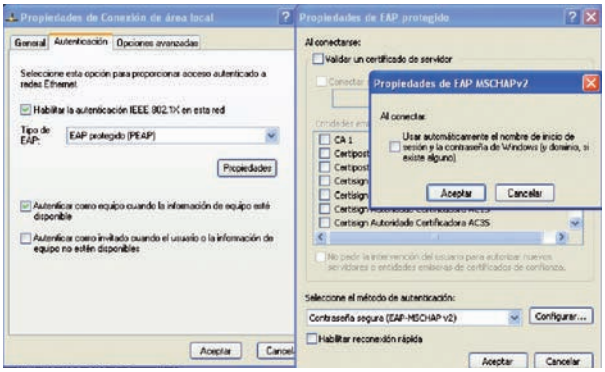


Fig. 6.34. *Ajustamos la configuración de la tarjeta.*

15. Salimos de todas las ventanas pulsando en *Aceptar*. Ahora, pulsando en la tarjeta, por fin nos solicita el usuario y la contraseña (Fig. 6.35).



Fig. 6.35. *Introducimos usuario.*

16. En el servidor RADIUS aparece el procesamiento de nuestra autenticación.

17. Ahora el ordenador puede conectar con normalidad. En el switch podemos consultar las autorizaciones conseguidas (Fig. 6.36).

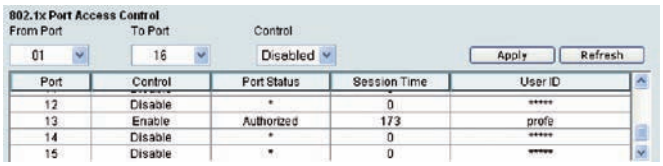


Fig. 6.36. *Autorizado en el switch.*

Actividades

4. Prueba a cambiar la MAC de tu tarjeta para saltarte una autenticación por MAC en el puerto.

2. Redes inalámbricas

Vocabulario

SSID. Es el identificador de una red inalámbrica. En las ciudades es muy habitual activar la interfaz wifi y poder elegir entre varias redes a tu alcance. Cada nombre que aparece es el SSID de una red servida por un AP.

Los miedos a que las comunicaciones sean escuchadas por terceros no autorizados han desaparecido en las redes cableadas, pero están plenamente justificados en redes inalámbricas o WLAN (Wireless LAN), porque de nuevo **el medio de transmisión (el aire) es compartido por todos los equipos** y cualquier tarjeta en modo promiscuo puede perfectamente escuchar lo que no debe.

Aunque se pueden hacer redes inalámbricas entre equipos (redes ad hoc), lo más habitual son las **redes de tipo infraestructura:** un equipo llamado **access point** (AP, punto de acceso) hace de switch, de manera que los demás ordenadores se conectan a él, le envían sus paquetes y él decide cómo hacerlos llegar al destino, que puede ser enviarlo de nuevo al aire o sacarlo por el cable que le lleva al resto de la red (Fig. 6.37). Salir por el cable es la configuración más habitual en las empresas, donde la WLAN se considera **una extensión de la red cableada.**

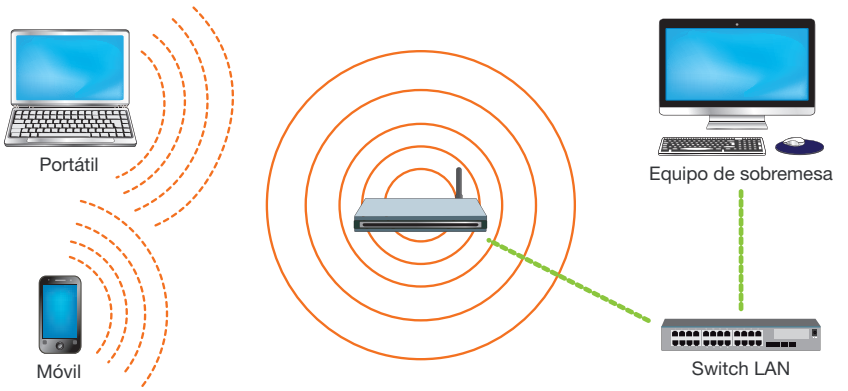


Fig. 6.37. *WLAN en modo infraestructura.*

Como ocurría con el switch en las redes cableadas, hemos de:

- **Proteger el access point físicamente.** La protección física es más complicada que en el caso del switch, porque el AP tiene que estar cerca de los usuarios para que puedan captar la señal inalámbrica, mientras que para conectar la toma de red de la mesa con el switch podemos utilizar cable de varias decenas de metros.
- **Proteger el access point lógicamente** (usuario/contraseña).
- **Controlar qué clientes pueden conectarse a él** (autenticación).
- Podemos **separar dos grupos de usuarios,** haciendo que el mismo AP emita varias SSID distintas, con autenticaciones distintas. Estas distintas SSID suelen tener asociada una VLAN etiquetada.
- Sobre todo, hay que **encriptar la transmisión** entre el ordenador y el AP. Así, aunque alguien capture nuestras comunicaciones, no podrá sacar nada en claro.

Web

Este vídeo expone el funcionamiento de wifi y los distintos estándares:

http://goo.gl/7btcD

En este vídeo nos presentan distintas tarjetas y antenas para conectarse a una red wifi:

http://goo.gl/WuIbv

Compartir wifi es una práctica muy extendida:

http://goo.gl/50N2i

2.1. Asociación y transmisión

Para que un ordenador pueda trabajar en una red cableada normal (sin autenticación en el puerto), basta con enchufar un cable Ethernet entre la tarjeta de red del equipo y la toma de red en la pared, por ejemplo. En wifi se establecen dos fases: asociación y transmisión.

Durante la **asociación** el usuario elige la SSID a la que se quiere conectar y entonces su tarjeta inalámbrica contacta con el AP que ofrece esa SSID. Negocian varias características de la comunicación (protocolo b/g/n, velocidad, etc.), pero sobre todo el AP puede solicitar algún tipo de **autenticación** para decidir si debe dejarle asociarse o no. Generalmente es una clave alfanumérica que se registra en la configuración del AP y que el usuario debe introducir para poder trabajar con él.

La autenticación es más habitual en redes inalámbricas que en redes cableadas porque, para poder llegar a conectar un cable, primero tenemos que entrar en la empresa, y se supone que no dejan pasar a cualquiera; en cambio, podemos captar la señal inalámbrica desde un coche aparcado junto a la fachada, sentados en un bar en la planta baja, etc. Aunque la empresa intente evitarlo limitando la potencia de emisión de sus AP, es imposible que no salga nada.

Las AP admiten varios **tipos de autenticación:**

- **Abierta:** no hay autenticación, cualquier equipo puede asociarse con el AP.
- **Compartida:** la misma clave que utilizamos para cifrar la usamos para autenticar.
- **Acceso seguro:** usamos distintas claves para autenticar y cifrar. El usuario solo necesita saber una, la clave de autenticación: la clave de cifrado se genera automáticamente durante la asociación.
- **Autenticación por MAC:** el AP mantiene una lista de MAC autorizadas y solo ellas pueden asociarse.

Una vez asociados al AP, podemos empezar la **fase de transmisión,** durante la cual estableceremos conversaciones con el AP. Si queremos evitar que un tercero capture los paquetes intercambiados e intente conocer lo que transmitimos, el cliente y el AP deberán activar el cifrado de cada paquete. El tipo de cifrado (algoritmo, longitud de la clave, etc.) se negocia durante la asociación.

Por tanto, **el AP admite varias combinaciones:**

- **Autenticación abierta y sin cifrado:** se utiliza en **lugares públicos** (bibliotecas, cafeterías, etc.). La intención es no molestar al usuario introduciendo claves; además, si las ponemos, habría que dar a conocer la clave mediante un cartel en el interior del establecimiento, por lo que la tendrían todos, usuarios y atacantes. En estos casos, **el sistema operativo nos avisa** de que vamos a conectarnos a una red sin seguridad.
- **Autenticación abierta y transmisión cifrada:** es el esquema habitual de las primeras redes wifi.
- **Autenticación compartida y transmisión cifrada:** es una mala combinación (en Windows 7 ni siquiera se contempla), porque la autenticación es muy vulnerable y, conocida esa clave, tendrán acceso a descifrar las comunicaciones de cualquier ordenador conectado a ese AP.
- **Autenticación segura y transmisión cifrada:** es la mejor solución porque utiliza una clave distinta para cada cosa. La más conocida es WPA, como veremos en el siguiente apartado de esta unidad.

Web

Alicia y Bernardo nos hablan de seguridad wifi:
http://goo.gl/KXQdL

Aquí tienes una conferencia sobre seguridad muy divertida y muy seria, a partes iguales:
http://goo.gl/UeAWX

Actividades

5. Hay otras arquitecturas de redes inalámbricas, como las redes malladas. Discute en clase los problemas de seguridad asociados.

6. En una empresa hay cuatro trabajadores en un despacho. Hartos de pedir a la empresa que ponga wifi en su zona, sin avisar a nadie deciden traer un router ADSL de su casa y enchufarlo. Analiza los problemas que puede causar.

7. ¿Por qué es peligrosa la autenticación compartida?

8. ¿Mejora la seguridad si desactivamos la difusión del SSID?

9. Investiga por qué hay dos versiones: WPA y WPA2.

10. Busca un programa para revelar las contraseñas wifi almacenadas en tu ordenador.

11. Investiga el origen de los servidores RADIUS.

Caso práctico 5

Configurar un AP con autenticación

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

Objetivo. Probar distintos tipos de autenticación en redes inalámbricas.

Material. Un ordenador, un equipo con wifi (ordenador, móvil, tableta) y un router inalámbrico Linksys WRT160NL.

1. Conectamos el ordenador al router mediante un cable Ethernet (usamos cable porque vamos a cambiar varias veces la autenticación wifi, y en cada cambio perderíamos la conexión). Debemos introducirlo por alguno de los cuatro puertos azules, no por el puerto amarillo porque este es el que sale a otras redes (generalmente Internet).
2. Si tenemos activado DHCP en el router, el ordenador habrá tomado una configuración IP válida (si no, podemos resetear el router). Para empezar nuestras pruebas debemos entrar al servidor web que gestiona el router. Para conocer la dirección del router, lo más sencillo es ejecutar el comando `ipconfig` y fijarnos en la dirección de la puerta de enlace (Fig. 6.38). En nuestro caso es la `10.0.1.1`.

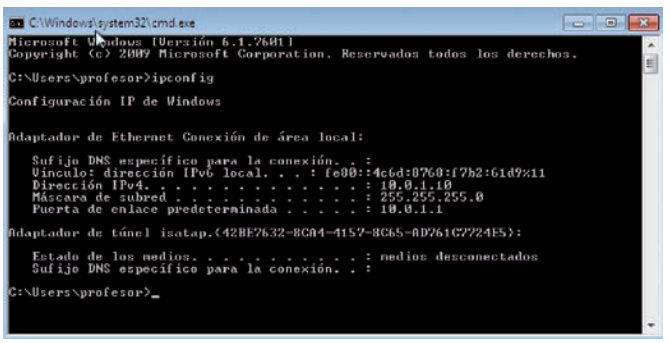


Fig. 6.38. *Localizar la IP del router.*

3. Con el navegador vamos a esa dirección y seguramente nos aparecerá una ventana para introducir el usuario y la contraseña.
4. El nombre de usuario y la clave por defecto los podemos buscar en Internet, aunque siempre aparecen en la documentación y, en algunos casos, en una pegatina en la parte inferior del equipo. En nuestro caso, el usuario es admin, pero la contraseña no es admin, ya está cambiada, como sabemos que hay que hacer. Tampoco conviene activar *Recordar mis credenciales*, porque cualquiera sentado en nuestro ordenador podría entrar a esa máquina.
5. Una vez dentro, vamos a crear una red inalámbrica. Nos vamos a la pestaña *Wireless* y, dentro de ella, *Basic Wireless Settings*. Elegiremos configuración manual, modo mixto (Mixed: admitiremos clientes b/g/n) y en el nombre de la red (el SSID) ponemos ALUMNOS. Los selectores del canal los dejamos en automático y activamos la difusión del SSID para que sea fácil encontrarnos (si lo quitamos, apenas ganamos en seguridad). Pulsamos en *Save Settings* para aplicar esta configuración (Fig. 6.39).

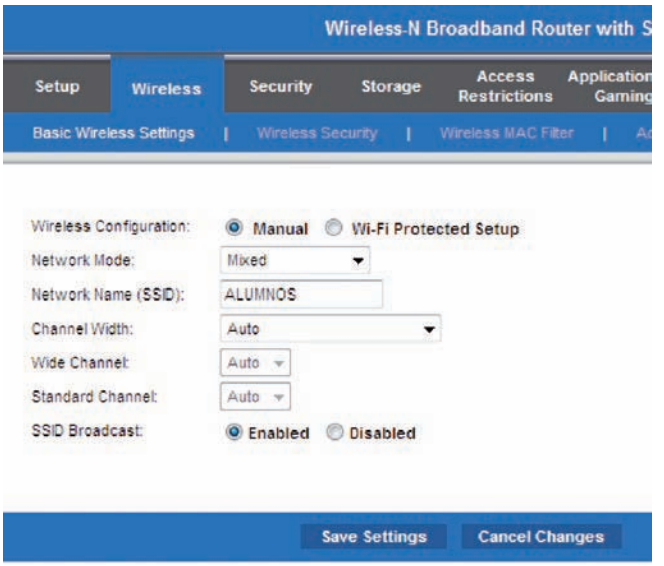


Fig. 6.39. *Definimos la wifi.*

6. Ahora vamos a la pestaña *Wireless Security* y en *Security Mode* elegimos *Disabled* (Fig. 6.40), para probar la asociación sin autenticación (red abierta).

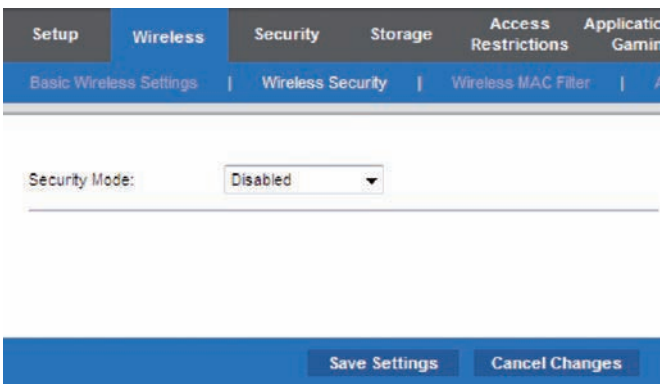


Fig. 6.40. *Red abierta.*

7. Tras pulsar en *Save Settings,* el AP está listo para aceptar conexiones de cualquiera. Probamos con nuestro equipo cliente. Activando la wifi debería encontrar nuestra red ALUMNOS y conectar a ella. Si todo va bien, podríamos hacer ping al router o entrar a su servidor web. En el router lo podemos saber entrando en la pestaña *Status* y dentro de ella *Local Network*. Al pulsar en el botón *DHCP Client Table* de esa página aparecerá una lista

(Continúa)

Caso práctico 5

(Continuación)

con dos equipos: el PC que estamos usando para configurar y el dispositivo conectado por wifi (Fig. 6.41).

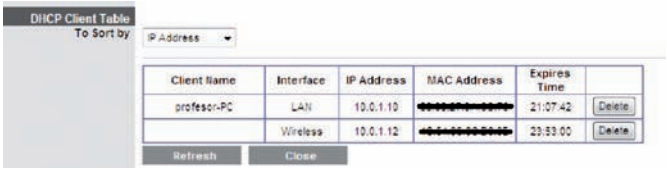


Fig. 6.41. *Lista de clientes conectados.*

8. Revisar esa lista es útil cuando queremos saber quién está conectado a nuestra wifi. Por ejemplo, vamos a prohibir que ese equipo se vuelva a conectar. Para eso vamos a la pestaña *Wireless* y dentro de ella *Wireless MAC Filter*. Activamos el filtro pulsando *Enabled*, seleccionamos la opción *Prevent* (la otra es para permitir) y ponemos la MAC del equipo en la primera posición de la lista (Fig. 6.42).

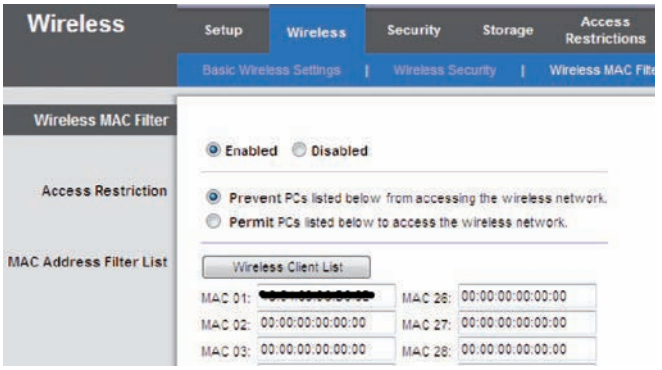


Fig. 6.42. *Acceso restringido.*

9. Al pulsar *Save Settings*, el móvil ya no podrá conectar con nosotros, pero cualquier otro sí. Si lo cambiamos a *Permit* y pulsamos de nuevo *Save Settings*, ocurre lo contrario: solo el móvil podrá conectar.

2.2. Cifrado: WEP, WPA, WPA2

La necesidad de encriptar las comunicaciones inalámbricas apareció desde el primer momento. Había que dar a los usuarios la **confianza** de que su información viajaba segura. El primer estándar se llamó **WEP** (Wireline Equivalent Privacy, privacidad equivalente al cable), intentando compensar las dos realidades:

- En redes cableadas es difícil el acceso al cable, pero si alguien lo consigue, puede capturar cualquier comunicación que pase por ahí.
- En redes inalámbricas cualquiera puede capturar las comunicaciones, pero, como van cifradas, no le servirá de nada.

Sin embargo, en poco tiempo se encontraron **debilidades** al algoritmo de cifrado utilizado en WEP. Capturando cierto número de tramas, en poco tiempo (cada vez menos, con el aumento de la capacidad de proceso de los ordenadores personales) cualquiera podía obtener la clave WEP.

Las autoridades de estandarización empezaron a trabajar en un nuevo estándar. Se llamó **WPA** (Wi-Fi Protected Access) e introduce muchas **mejoras:**

- Nuevos **algoritmos más seguros** (TKIP, AES), tanto por el algoritmo en sí como por el aumento de longitud de las claves, lo que dificulta los ataques.
- **Rotación automática de claves.** Cada cierto tiempo (varios minutos) el AP y el cliente negocian una nueva clave. Por tanto, si algún atacante lograra acertar con la clave de una comunicación, solo le serviría para descifrar la información intercambiada durante ese intervalo de tiempo, pero no la anterior ni la siguiente.
- Por primera vez se **distingue entre los ámbitos personal y empresarial.** En el ámbito personal es suficiente con el esquema habitual de una única clave que conocen todos (WPA le llama **PSK** [Pre-Shared Key]); en el ámbito empresarial no tiene sentido, porque si una persona abandona la empresa, habría que cambiar la clave y comunicarlo de nuevo a todos los empleados. Para resolverlo, **WPA empresarial** introduce un servidor **RADIUS** donde poder almacenar un usuario y una clave para cada empleado.

Web

Las empresas de telecomunicaciones deben tener cuidado a la hora de elegir la clave que ponen en la wifi de sus clientes:
http://goo.gl/YRgQy

Caso práctico 6

Configurar seguridad WPA-PSK en un AP

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

Objetivo. Utilizar WPA-PSK para autenticar y cifrar.

Material. Un ordenador, un equipo con wifi (ordenador, móvil, tablet) y un router inalámbrico Linksys WRT160NL.

1. Los primeros pasos son similares a los del caso práctico 5: conectamos el ordenador al router mediante cable y abrimos el navegador conectándonos al servidor web del router (dirección 10.0.1.1 en nuestro ejemplo).
2. Creamos la nueva red entrando en la pestaña *Wireless*. Ahora la llamaremos ALUMNOS-WPA (Fig. 6.43).

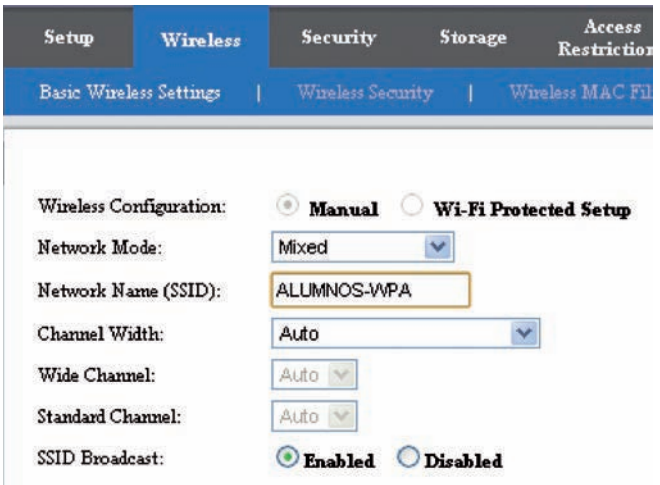


Fig. 6.43. *Creamos la nueva red.*

3. Aplicamos los cambios y vamos a la pestaña *Wireless Security*. Aquí elegimos WPA2 Personal, encriptación AES, dejamos la renovación de claves de cifrado cada hora y ponemos la clave que queremos para autenticarnos en nuestra red (Fig. 6.44).

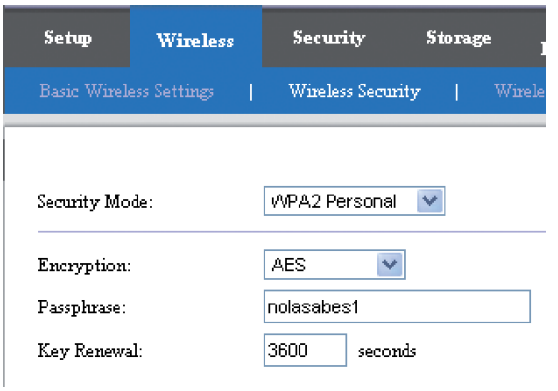


Fig. 6.44. *Activamos seguridad WPA2-PSK.*

4. Aplicamos los cambios y vamos a probarlo. En nuestro móvil con wifi buscamos la nueva red y solicitamos conexión. Nos pedirá la contraseña y la introducimos. Una vez conectados, aparecemos en la lista de direcciones prestadas por el router, que se encuentra en la pestaña *Local Network* dentro de *Status* (Fig. 6.45). La primera entra por LAN y es la dirección del ordenador con el que estamos configurando el router; la segunda entra por wifi y es la dirección del móvil.

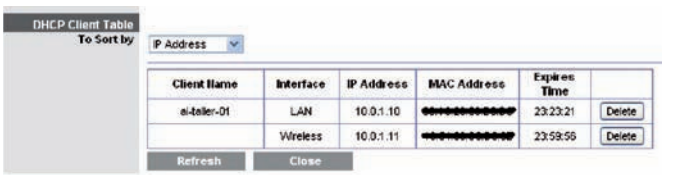


Fig. 6.45. *Cliente asociado.*

5. Esta autenticación es compatible con el mecanismo de lista de MAC que vimos en el caso práctico anterior. Si está activada la lista *Prevent* y la MAC de nuestro móvil está ahí, ni siquiera nos aparece la ventana que solicita la clave.

En general conviene tener todas las redes en WPA; pero en cada caso habrá que estudiar si el AP lo tiene y si todos los posibles equipos que queremos conectarle lo permiten, tanto en hardware (el cifrado se hace en la tarjeta) como en software (el sistema operativo y el driver deben contemplarlo). Puede ocurrir que equipos viejos solo admitan WEP, en cuyo caso hay que decidir entre actualizarlos o bajar la seguridad de todos los demás.

2.3. WPA empresarial: RADIUS

Como acabamos de destacar, para las necesidades de seguridad de una empresa no es suficiente con la solución de clave única compartida por todos. Además de la salida de empleados, ya sabemos que es una buena práctica cambiar las claves regularmente (no sabemos cuánto tiempo llevan intentando conocerla), se puede extraviar el portátil o el móvil de un empleado y quien lo encuentre puede sacar las claves almacenadas en el dispositivo, etc.

El esquema de funcionamiento de WPA empresarial es el siguiente:

- Dentro de la LAN de la empresa hay un ordenador que ejecuta un **software servidor RADIUS.** En este servidor hay una **base de datos de usuarios y contraseñas,** y el servidor admite preguntas sobre ellos.
- Los AP de la empresa tienen conexión con ese ordenador.
- Los AP ejecutan un **software cliente RADIUS.** Este software es capaz de formular las preguntas y analizar las respuestas.
- El servidor RADIUS tiene la lista de las direcciones IP de los **AP que le pueden preguntar.** Además de estar en la lista, el AP necesita que le configuremos una **contraseña** definida en el servidor (una dirección IP es fácilmente falsificable).
- Cuando un cliente quiere asociarse a un AP, le solicita usuario y contraseña. Pero no las comprueba él mismo, sino que formula la pregunta al servidor RADIUS utilizando la contraseña configurada para ese servidor. Dependiendo de la respuesta, el AP acepta la asociación o no.

Además de mejorar la seguridad, porque **cada usuario tiene su contraseña** (con su caducidad) y en cualquier momento podemos añadir o eliminar un usuario, con WPA empresarial podemos **llevar un registro** de quién entra a la red en cada momento.

Importante

En una empresa conviene centralizar la base de datos de usuarios y contraseñas para añadir o eliminar usuarios fácilmente. En el caso de RADIUS, algunos servidores admiten la integración con LDAP (Lightweight Directory Access Protocol).

Caso práctico 7

Configuración de WPA Empresarial

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

Objetivo. Instalar y configurar el equipamiento necesario para disponer de autenticación WPA Empresarial.

Material. Un ordenador, un ordenador Windows Vista con wifi y un router inalámbrico Linksys WRT160NL.

1. Primero instalamos el servidor RADIUS siguiendo los pasos del caso práctico 4. La única diferencia es que pondremos el servidor en la dirección 10.0.1.4, porque nuestro AP está en la 10.0.1.1 (por tanto, habrá que modificar el clients.conf). Mantenemos la misma contraseña nolasabes1 y el mismo usuario profe con la clave test1234.

2. Para configurar el AP seguimos los primeros pasos del caso práctico 5: conectamos el ordenador al router mediante cable y abrimos el navegador conectándonos al servidor web del router (dirección 10.0.1.1 en nuestro ejemplo).

3. Creamos la nueva red entrando en la pestaña *Wireless*. Ahora le llamaremos ALUMNOS-RADIUS (Fig. 6.46).

4. Pulsamos *Save Settings* y nos vamos a *Wireless Security*. Aquí elegimos WPA Enterprise, cifrado AES y ponemos la dirección y la clave del RADIUS (Fig. 6.47).

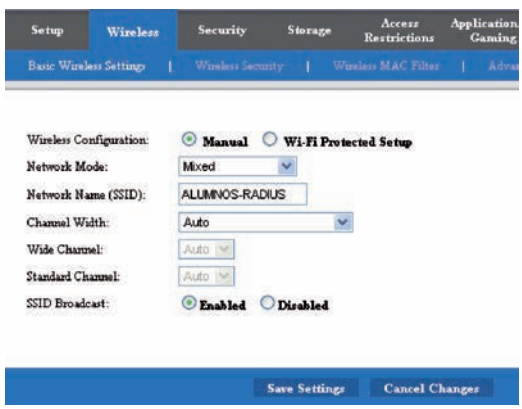


Fig. 6.46. *Nueva wifi.*

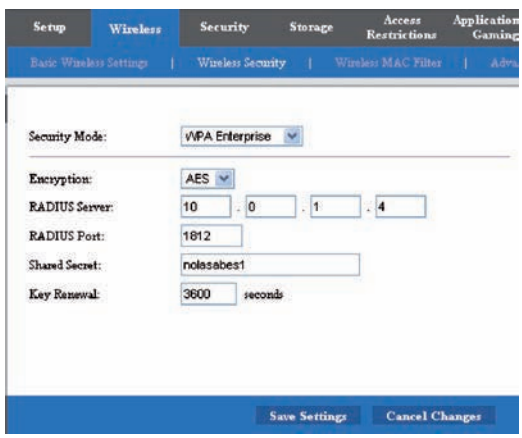


Fig. 6.47. *Seguridad RADIUS.*

(Continúa)

Caso práctico 7

(Continuación)

5. Pulsamos *Save Settings* y ya estamos listos para recibir las conexiones. En el caso práctico 4 lo hicimos con XP; ahora lo intentamos con Vista. Ya vimos que antes de conectar tenemos que modificar el tipo de autenticación para que admita EAP en texto plano. Para conseguirlo vamos a crear la conexión desde cero. Hacemos *Inicio > Panel de Control > Ver el estado y las tareas de red > Administrar redes inalámbricas* (Fig. 6.48).

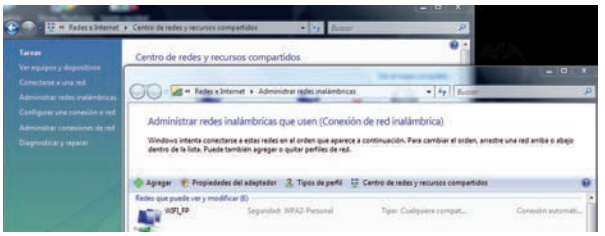


Fig. 6.48. *Redes configuradas.*

6. Pulsamos *Agregar* y elegimos *Crear un perfil de red manualmente*. En la ventana que aparece introducimos el SSID, elegimos seguridad WPA Enterprise y cifrado AES (Fig. 6.49). También desmarcamos el *Iniciar esta conexión automáticamente* para que se vea mejor la petición de usuario y contraseña.

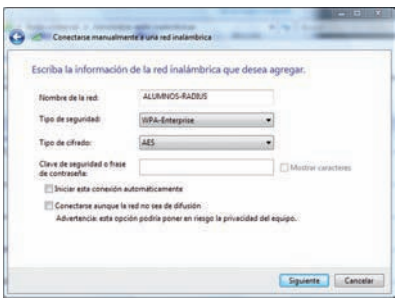


Fig. 6.49. *Configuración manual.*

7. Pulsamos *Siguiente* y elegimos *Cambiar la configuración de conexión*. En la ventana que aparece vamos a la pestaña *Seguridad* y elegimos *PEAP* (Fig. 6.50).

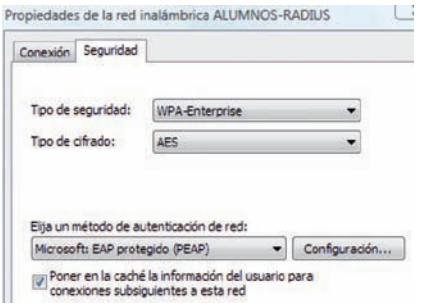


Fig. 6.50. *Propiedades de seguridad.*

8. Pulsamos en *Configuración…* y desmarcamos *Validar un certificado de servidor*. En el método de autenticación ponemos EAP-MSCHAP v2 y pulsando en *Configurar…* desactivamos que utilice nuestro usuario de Windows (Fig. 6.51).

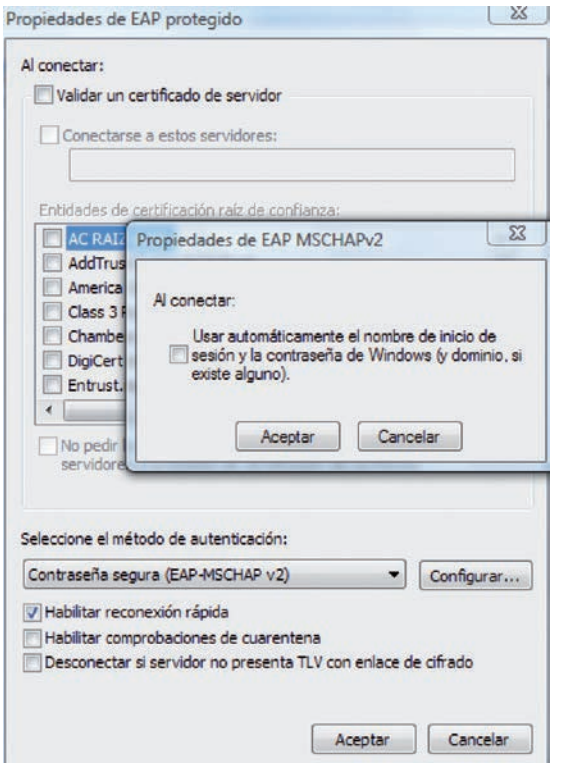


Fig. 6.51. *Propiedades de EAP.*

9. Salimos de todas las ventanas pulsando en *Aceptar* hasta llegar a la ventana donde elegimos cambiar la configuración. Ahora sí podemos pulsar en *Conectar*. Aparecerá la lista de redes que capta nuestro adaptador wifi (Fig. 6.52).

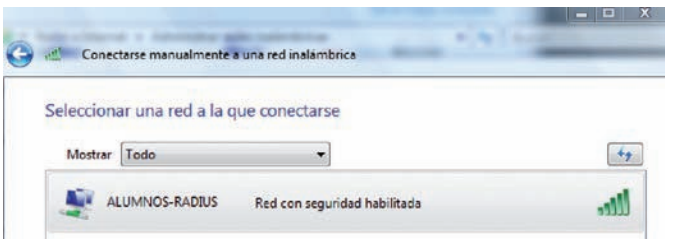


Fig. 6.52. *Lista de redes disponibles.*

10. Hacemos doble clic en ALUMNOS-RADIUS y aparecerá una ventana que nos anuncia que necesitamos autenticarnos o podemos conectar a otra red (Fig. 6.53).

(Continúa)

Caso práctico 7

(Continuación)

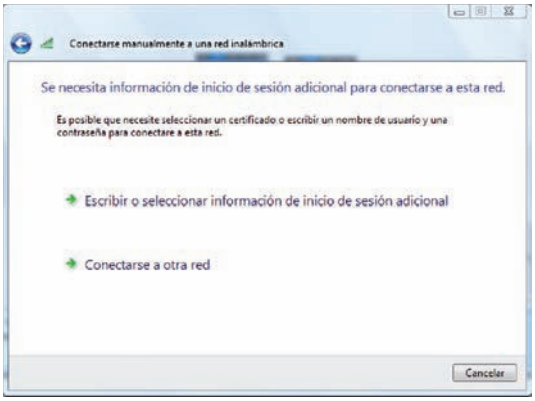


Fig. 6.53. *Aviso de autenticación.*

11. Elegimos autenticarnos y rellenamos el usuario y la contraseña que hemos configurado en RADIUS (Fig. 6.54).

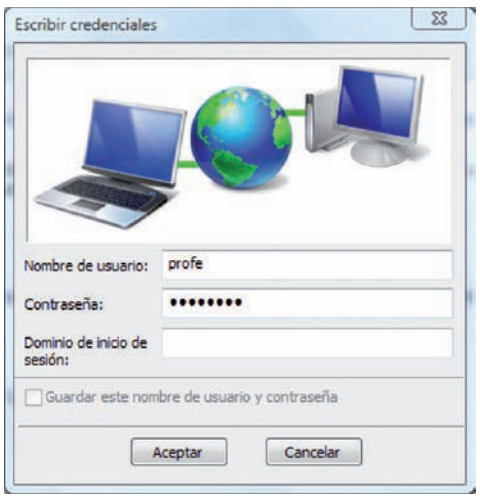


Fig. 6.54. *Introducimos usuario y clave.*

12. Si todo va bien, estaremos conectados (Fig. 6.55).

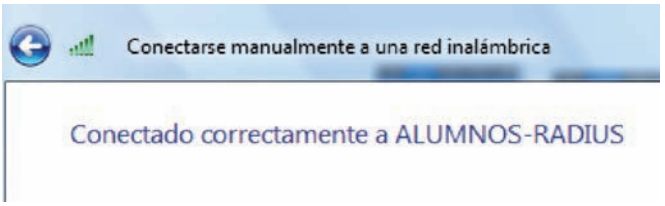


Fig. 6.55. *Conexión conseguida.*

13. En el servidor freeradius podemos confirmar que se ha efectuado la autorización (Fig. 6.56).

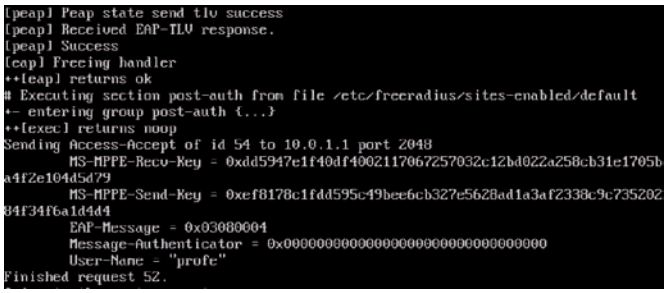


Fig. 6.56. *Log del freeradius.*

14. En el router lo podemos ver en la lista de préstamos: *Status > Local Network > DHCP Client Table* (Fig. 6.57).

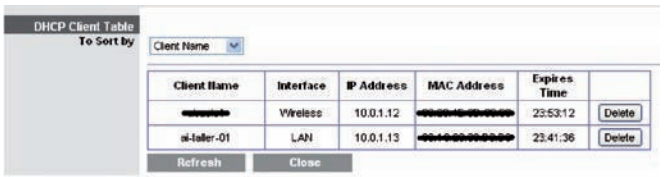


Fig. 6.57. *Registro en el router.*

La rotación de claves que introdujo WPA fue un paso importante para disuadir a los hackers de intentar obtener la clave mediante el análisis de la captura de tramas de tráfico de equipos ya conectados al AP.

Entonces los hackers concentraron su trabajo en la clave PSK de la fase de asociación.

Utilizaron la fuerza bruta de dos formas:

- Probando contraseñas una tras otra. Las contraseñas serían todas las combinaciones posibles de letras y números, o una selección mediante un diccionario. Por desgracia, los AP no suelen tener un control del número de intentos fallidos, como sí ocurre en otros sistemas de autenticación que hemos visto en este libro (login de Windows, tarjetas SIM).
- Si consiguieran capturar las tramas de inicio de conexión de un cliente, podrían aplicar un ataque de diccionario sobre la información de esas tramas. Si no queremos esperar a que aparezca un cliente nuevo, podemos forzar la desconexión de alguno.

3. VPN

Las empresas tienen redes LAN y WLAN para sus oficinas, pero también suelen necesitar que los empleados puedan entrar a esa misma red **desde cualquier otro lugar de Internet** (su casa, la sede de otra empresa, etc.), por cualquier motivo (buscar información en la intranet, recuperar un fichero del disco compartido, actualizar un pedido, etc.). Algo como establecer una VLAN entre el ordenador del empleado y la LAN de la empresa, utilizando Internet como transporte. Estamos hablando de montar una **VPN** (Virtual Private Network, red privada virtual).

El objetivo final de la VPN es que el empleado (más bien, su ordenador) **no note si está en la empresa o fuera de ella.** En ambos casos recibe una configuración IP privada (direcciones 10.X.X.X, por ejemplo), por lo que no necesita cambiar nada en la configuración de sus aplicaciones (correo, intranet, etc.).

Web

Este videotutorial enseña cómo crear VPN en Windows:
http://goo.gl/yCpsh

El responsable de conseguir esta transparencia es el software de la VPN. En el ordenador del empleado hay que instalar un **software cliente VPN.** Este software instala un **driver de red,** de manera que para el sistema operativo es una tarjeta más. Ese driver se encarga de contactar con una máquina de la empresa, donde ejecuta un **software servidor VPN** que gestiona la conexión, para introducir los paquetes en la LAN. La gestión consiste en:

- **Autentificar al cliente VPN.** No podemos dejar que entre cualquiera, por lo que se utiliza el típico usuario/contraseña, tarjetas inteligentes, etc.
- **Establecer un túnel** a través de Internet. El driver de la VPN en el cliente le ofrece una dirección privada de la LAN de la empresa (la 10.0.1.45, por ejemplo), pero cualquier paquete que intente salir por esa tarjeta es **encapsulado** dentro de otro paquete. Este segundo paquete viaja por Internet desde la IP pública del empleado hasta la IP pública del servidor VPN en la empresa. Una vez allí, se extrae el paquete y **se inyecta en la LAN.** Para que alguien de la LAN envíe un paquete a la 10.0.1.45 el proceso es similar.
- **Proteger el túnel.** Como estamos atravesando Internet, hay que encriptar las comunicaciones (sobre todo si somos una empresa). Los paquetes encapsulados irán cifrados.
- **Liberar el túnel.** El cliente o el servidor pueden interrumpir la conexión cuando lo consideren necesario.

Actividades

12. Analiza la validez de la VPN Hamachi en un entorno empresarial.

El software VPN en el cliente suele llevar una opción para que las conexiones a Internet se hagan directamente en la conexión del usuario, sin tener que pasar por el túnel y salir por la conexión a Internet de la empresa. Es decir, el túnel se usa solo para comunicaciones internas.

Caso práctico 8

Establecer una VPN

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

Objetivo. Construir una VLAN con dos equipos utilizando el software Hamachi.

Material. Dos ordenadores con conexión a Internet (uno con Windows XP y otro con Vista).

1. En cada equipo descargamos el software de Hamachi. Como lo bajamos de Internet hay que asegurarse de que la web es fiable. En este ejemplo utilizaremos **softonic.com** (Fig. 6.58).



Fig. 6.58. *Descargar software Hamachi.*

(Continúa)

Caso práctico 8

(Continuación)

2. Una vez descargado, lo instalamos. Si nos fijamos, durante la instalación nos avisa de que va a instalar un driver de red.

3. Una vez instalado, aparece la ventana principal de la herramienta. Pulsamos en el botón inicial para crear nuestra identidad en la red (Fig. 6.59). En el XP nos hacemos llamar ai-taller-01.

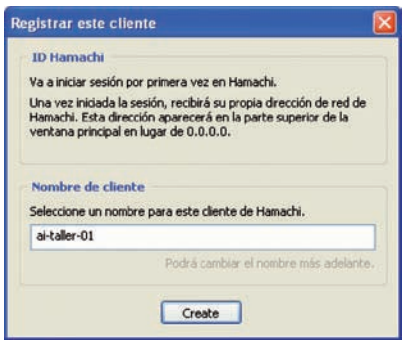


Fig. 6.59. *Nuevo equipo Hamachi.*

4. Hacemos lo mismo en el Vista, esta vez con el identificador profesor. Completado este paso, la ventana principal nos informa de nuestra IP en la red Hamachi: en el ejemplo es la 5.117.67.96 (Fig. 6.60). Utilizaremos esa IP para comunicarnos con los otros componentes de la VPN.



Fig. 6.60. *Equipo Hamachi conectado.*

5. Si vamos a las conexiones de red, veremos la nueva interfaz de red llamada Hamachi (Fig. 6.61).



Fig. 6.61. *Tarjeta de red Hamachi.*

6. Para conectar los dos equipos debemos crear una red en uno, y asociarse a esa red en el otro. En el ordenador del profesor pulsamos el botón *Crear una nueva red*. Nos pedirá un nombre y una contraseña (Fig. 6.62).

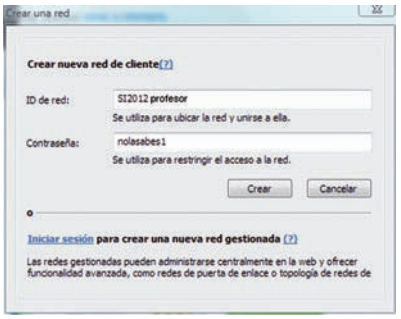


Fig. 6.62. *Nueva red Hamachi.*

7. Si el nombre de la red no coincide con ningún nombre de red de otros usuarios de Hamachi, la red está creada. Vamos al XP y pulsamos en *Unirse a una red existente*. Introducimos el nombre y la contraseña.

8. En la ventana principal del XP aparece que estamos conectados a esa red, donde está el equipo llamado profesor con su IP (Fig. 6.63).



Fig. 6.63. *Cliente unido a la red.*

9. En la ventana del Vista aparece el nuevo miembro de la red con su IP.

10. Para comprobar la conectividad podemos entrar al XP para hacer un `ping` a la IP del Vista (Fig. 6.64).

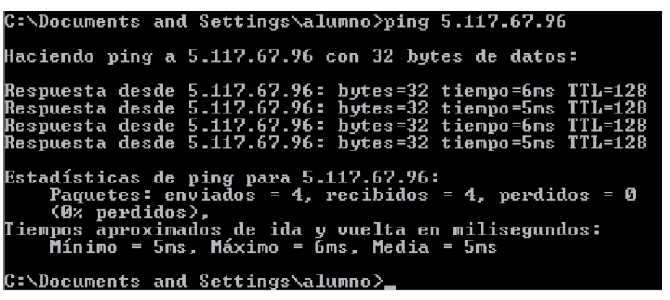


Fig. 6.64. *Accesibles a través de la VPN.*

4. Servicios de red. Nmap y netstat

Empezamos esta unidad hablando de los riesgos de conectar un equipo a una red. Habrá una parte del software instalado en ese equipo (los llamados servicios de red) que quiere conectar con unos equipos y que espera conexiones de esos equipos u otros. Pero pueden llegar conexiones de un cliente atacante, o nos podemos estar conectando erróneamente a un servidor atacante.

El software de los servicios de red es especialmente delicado. Debemos vigilar qué software tenemos activo y qué actualizaciones tiene pendientes.

Las actualizaciones llegarán por el mecanismo habitual del sistema operativo; el software que tenemos activo (haciendo conexiones o esperándolas) lo podemos conocer mediante un par de herramientas sencillas: Nmap y netstat.

Caso práctico 9

Utilidad netstat en Windows y Linux

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

Objetivo. Identificar las conexiones de red abiertas en un equipo.

Material. Ordenador Windows 7 y Linux.

1. En el primer caso práctico de esta unidad utilizamos el monitor de recursos de Windows 7 para saber quién estaba conectado. Lo podemos hacer con un simple comando. Entramos al Windows 7 y abrimos el navegador para conectar con alguna web. Sin cerrar el navegador, desde otra ventana abrimos un cmd con privilegios (sobre el icono *Símbolo de sistema,* pulsar el botón derecho y elegir *Ejecutar como administrador*). Lanzamos el comando `netstat –an` (Fig. 6.65).

```
Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    192.168.43.176:139     0.0.0.0:0              LISTENING
  TCP    192.168.43.176:49217   192.168.43.86:80       ESTABLISHED
  TCP    192.168.43.176:49218   192.168.43.86:80       ESTABLISHED
  TCP    192.168.43.176:49219   192.168.43.86:80       ESTABLISHED
  TCP    192.168.43.176:49220   192.168.43.86:80       ESTABLISHED
  TCP    192.168.43.176:49221   192.168.43.86:80       ESTABLISHED
  TCP    192.168.43.176:49222   192.168.43.86:80       ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
-- Más  --
```

Fig. 6.65. *Netstat en Windows.*

2. Hay una fila por cada conexión. La primera columna es el protocolo (TCP, UDP). La segunda es la dirección y puerto de nuestra máquina que está conectado con la dirección y puerto de la otra máquina (tercera columna). La cuarta columna es el estado de la conexión: `LISTENING` significa que el puerto está abierto, está esperando una conexión; y `ESTABLISHED`, que se ha hecho la conexión. En nuestro ejemplo vemos que hay conexiones establecidas con un servidor web (puerto 80) y que tenemos abiertos varios puertos (135 y 445, los típicos de conexiones de disco compartido).

3. Si ejecutamos `netstat –abn` aparece una quinta columna con el ejecutable de nuestra máquina que está detrás de esa conexión (Fig. 6.66). Podemos confirmar que la conexión al puerto 80 la ha hecho un Internet Explorer y que los servicios de disco en red los lleva el `svchost.exe`.

```
Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
No se puede obtener información de propiedad
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
 [wininit.exe]
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  eventlog
 [svchost.exe]
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
 [services.exe]
  TCP    192.168.43.176:139     0.0.0.0:0              LISTENING
No se puede obtener información de propiedad
  TCP    192.168.43.176:49223   192.168.43.86:80       ESTABLISHED
 [iexplore.exe]
-- Más  --
```

Fig. 6.66. *Ejecutables de cada conexión Windows.*

4. Podemos probar el mismo comando en la máquina Unix que hemos utilizado en los servidores RADIUS de los casos prácticos anteriores. Entramos con privilegios de administrador y ejecutamos `netstat –an` (Fig. 6.67).

```
root@ubuntu12:~# netstat -an | head
Conexiones activas de Internet (servidores y establecidos)
Proto  Recib Enviad Dirección local        Dirección remota       Estado
tcp        0      0 0.0.0.0:22             0.0.0.0:*              ESCUCHAR
tcp6       0      0 :::22                  :::*                   ESCUCHAR
udp        0      0 127.0.0.1:18120        0.0.0.0:*
udp        0      0 0.0.0.0:1812           0.0.0.0:*
udp        0      0 0.0.0.0:1813           0.0.0.0:*
udp        0      0 0.0.0.0:1814           0.0.0.0:*
udp        0      0 0.0.0.0:68             0.0.0.0:*
```

Fig. 6.67. *Netstat en Linux.*

(Continúa)

Caso práctico 9

(Continuación)

5. En este caso vemos que está escuchando en el puerto 22 de TCP (un servidor SSH) y en el puerto 1812 de UDP (el servidor freeradius). Lo podemos confirmar con `netstat -apn` (Fig. 6.68). Cuidado: en Windows era `-abn` y en Linux es `-apn`. Hemos invocado el comando con la opción a para ver todos los puertos abiertos (sin ella, solo aparecen las conexiones establecidas). La opción n sirve para ver los datos numéricos de direcciones y puertos (sin ella, el comando intenta conseguir la traducción DNS inversa y el nombre común del puerto: http, https).

```
root@ubuntu12:~# netstat -apn | head
Conexiones activas de Internet (servidores y establecidos)
Proto  Recib Enviad Dirección local          Dirección remota        Estado
PID/Program name
tcp        0      0 0.0.0.0:22               0.0.0.0:*               ESCUCHAR
1291/sshd
tcp6       0      0 :::22                    :::*                    ESCUCHAR
1291/sshd
udp        0      0 127.0.0.1:18120          0.0.0.0:*
839/freeradius
udp        0      0 0.0.0.0:1812             0.0.0.0:*
839/freeradius
udp        0      0 0.0.0.0:1813             0.0.0.0:*
839/freeradius
udp        0      0 0.0.0.0:1814             0.0.0.0:*
839/freeradius
udp        0      0 0.0.0.0:68               0.0.0.0:*
1269/dhclient3
```

Fig. 6.68. *Ejecutables de cada conexión Linux.*

Caso práctico 10

Utilidad Nmap en Linux

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

Objetivo. Explorar los servicios ofrecidos por un equipo.

Material. Ordenador Linux conectado en red con otros equipos.

1. Con el comando `netstat` podemos conocer los puertos abiertos en nuestra máquina; para conocer los de otras máquinas utilizamos `nmap`. Entramos a la máquina Linux y lo instalamos con `apt-get install nmap`.

2. Ahora podemos lanzarlo pasando como parámetro la IP de la máquina que queremos analizar. En el ejemplo de la Figura 6.69 vemos que la `192.168.43.86` está ofreciendo un servicio web y un servicio de disco en red.

```
root@ubuntu12:~# nmap 192.168.43.86

Starting Nmap 5.21 ( http://nmap.org ) at 2012-07-14 17:18 CEST
Nmap scan report for ai-taller-01 (192.168.43.86)
Host is up (0.050s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:1B:77:C8:28:6B (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 9.63 seconds
root@ubuntu12:~#
```

Fig. 6.69. *Nmap.*

La herramienta **Nmap,** disponible para sistemas Linux y Windows, se ha convertido en la navaja suiza de los hackers de red. Además del escaneo de puertos para determinar los servicios disponibles en una máquina, podemos pedir a la herramienta que intente la conexión a cada uno de ellos. Después analiza los mensajes que generan estos servidores para identificar la versión concreta del sistema operativo y la versión concreta del software de servidor (server fingerprint) que está escuchando en cada puerto.

Es decir, aunque intentemos despistar arrancando servicios en puertos que no son los esperados (80 para HTTP y otros), la herramienta reconoce el puerto como abierto y consigue identificar el servicio.

La información de versión es muy útil para un atacante porque puede consultar en su base de datos las vulnerabilidades de cada versión de un servicio y así elegir mejor el tipo de ataque que puede lanzar contra la máquina.

Para cada puerto, la herramienta ofrece cuatro posibles estados:

- **open** (abierto): la máquina acepta paquetes dirigidos a ese puerto, donde algún servidor está escuchando y los procesará adecuadamente.
- **closed** (cerrado): no hay ningún servidor escuchando.
- **filtered:** Nmap no puede decir si ese puerto está abierto o cerrado porque alguien está bloqueando el intento de conexión (router, firewall).
- **unfiltered:** el puerto no está bloqueado, pero no se puede concluir si está abierto o cerrado.

Síntesis

Los equipos utilizan protocolos inseguros sobre redes inseguras

En redes cableadas la seguridad se centra en el switch
- Guardarlo en un rack, fuera del alcance de los usuarios.
- Proteger su configuración con usuario/contraseña.
- Establecer VLAN siempre que sea razonable.
- Configurar autenticación en el puerto siempre que sea razonable.

Tipos de VLAN
- Grupos de puertos en uno o más switch.
- VLAN etiquetada (tag). Permite compartir enlaces entre varias VLAN.

Autenticación en el puerto
- Lista de MAC autorizadas.
- Certificados 802.1X.

En redes inalámbricas la seguridad se centra en el access point y el cifrado de las comunicaciones con las estaciones conectadas a él
- No podemos poner el AP lejos de los usuarios, pero sí que no lo tengan fácil.
- Proteger su configuración con usuario/contraseña.
- Autenticar quién se puede conectar.
- Encriptar las comunicaciones.

Tipos de autenticación
- Abierta. No hay autenticación.
- Compartida. Misma clave que el cifrado. No recomendable.
- Acceso seguro. Distinta clave que el cifrado.
- Lista de MAC autorizadas.

Tipos de cifrado
- WEP. No recomendable.
- WPA. Buenos algoritmos de cifrado (TKIP, AES). Rotación automática de claves.
  - WPA personal. Clave de autenticación única.
  - WPA empresarial. Claves de autenticación para cada usuario en servidor RADIUS.

VPN es una extensión de la LAN de la empresa a través de Internet

Supervisión de servicios de red activos mediante nmap y netstat

Test de repaso

1. En una LAN hay que vigilar las comunicaciones:
a) Nunca, porque son nuestras máquinas y sabemos qué tienen dentro.
b) Siempre, porque nuestras máquinas pueden haber sido atacadas, o cada día vienen máquinas distintas (portátiles de clientes y otras).
c) Solo cuando conectamos a Internet.

2. Si todas nuestras máquinas utilizan entre sí protocolos seguros:
a) No es tan importante la seguridad de la red, porque ya la tenemos en los extremos.
b) Seguimos asegurando la red porque no existen los protocolos seguros.
c) No podemos asegurar la red porque es incompatible con la seguridad en los equipos.

3. Una tarjeta de red en modo promiscuo:
a) Nos permite ahorrar energía porque utiliza menos recursos.
b) Procesa todos los paquetes de datos, no únicamente los dirigidos a su MAC.
c) En este modo podemos unirnos con otra tarjeta para tener más ancho de banda.

4. Los switch:
a) Podemos dejarlos encima de la mesa de los usuarios, porque no saben para qué sirven.
b) No tocamos la configuración de fábrica, por si estropeamos algo.
c) Hay que instalarlos fuera del alcance de los usuarios y modificar la contraseña de acceso a la configuración.

5. Queremos conectar los equipos de tres departamentos y tenemos un switch de 16 puertos con capacidad VLAN:
a) No se puede hacer: necesitamos tres switch.
b) Para que funcione, debemos conectar todos en la VLAN por defecto.
c) Podemos crear tres VLAN, una para cada departamento.

6. Una VLAN basada en grupos de puertos:
a) Solo funciona dentro del mismo switch.
b) Podemos conectarla con otra VLAN de grupo de puertos en otro switch.
c) Esos equipos quedarán aislados del resto de la red.

7. Las VLAN etiquetadas:
a) Permiten meter en un mismo enlace el tráfico de distintas VLAN.
b) No pueden mezclarse con VLAN de grupos de puertos.
c) No existen: solo podemos hacer grupos de puertos.

8. La autenticación en el puerto de un switch:
a) Consiste en utilizar siempre el mismo cable.
b) Solo funciona con tarjetas del mismo fabricante que el switch al que nos queremos conectar.
c) El switch identifica al equipo que se quiere conectar por ese puerto.

9. La seguridad en redes inalámbricas:
a) Ya no hace falta preocuparse, porque son más modernas que las redes cableadas.
b) Hemos dado un paso atrás: cualquiera puede escuchar en el medio de transmisión.
c) Solo funciona con tarjetas del mismo fabricante que el access point al que nos queremos conectar.

10. Para proteger el access point:
a) Lo guardamos en un armario, como hacemos con los switch.
b) Modificamos la contraseña de acceso a la configuración.
c) Dejamos la contraseña por defecto, porque si la olvidamos, la podemos buscar en Internet.

11. Entre seguridad WEP y WPA:
a) Nos quedamos con WEP, que lleva más tiempo en el mercado y es más fiable.
b) Nos quedamos con WPA, porque utiliza algoritmos más seguros.
c) No necesitamos elegir porque podemos usar las dos a la vez.

12. La configuración WPA-PSK:
a) Es suficiente en un entorno doméstico o pequeña empresa.
b) Es suficiente en todas las circunstancias.
c) Todavía no está disponible.

13. En una VPN:
a) No importa la seguridad, porque en Internet, ¿quién puede saber que estamos conectando con una empresa?
b) La seguridad es vital, porque atravesamos redes que no controlamos.
c) Nos vale cualquier software VPN.

14. Con el comando netstat:
a) Comprobamos las estadísticas de la red.
b) Comprobamos las conexiones anteriores.
c) Comprobamos las conexiones establecidas en este momento.

Soluciones: 1 b, 2 a, 3 b, 4 c, 5 c, 6 b, 7 a, 8 c, 9 b, 10 b, 11 b, 12 a, 13 b, 14 c.

Comprueba tu aprendizaje

Inventariar y controlar los servicios de red

1. En una máquina del laboratorio, instala varios servicios: FTP, HTTP, DNS, SSH, etc.

a) Comprueba que los puedes identificar utilizando:

- netstat.
- Nmap.
- Spiceworks.

b) Documenta el procedimiento, así como las diferencias que puedan aparecer entre los resultados ofrecidos.

Medidas para evitar la monitorización de redes cableadas: VLAN de grupos de puertos

2. En el laboratorio, configura un switch gestionable para que cumpla estas especificaciones:

a) La contraseña de acceso al switch será vlan2puerto.

b) Crea dos VLAN de grupos de puertos con los identificadores 11 y 12. Cada VLAN incluye al menos dos puertos.

c) Conecta cuatro equipos al switch, dos en cada VLAN, según el esquema de la Figura 6.71.

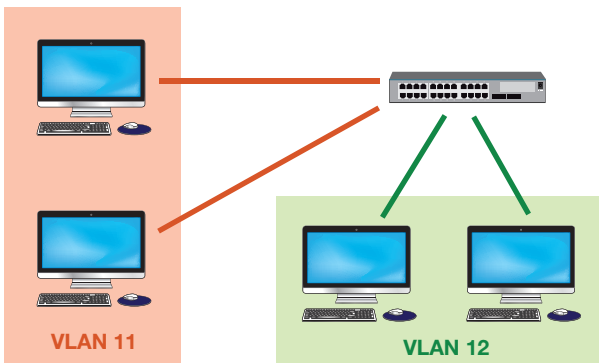


Fig. 6.70. *Ejercicio 2.*

d) Comprueba mediante ping que hay conectividad entre los equipos de la misma VLAN, pero no con los de la otra VLAN.

e) Documenta todo el proceso.

Medidas para evitar la monitorización de redes cableadas: VLAN etiquetadas

3. En el laboratorio, configura un switch gestionable para que cumpla estas especificaciones:

a) La contraseña de acceso al switch será vlan2tag.

b) Crea dos VLAN de grupos de puertos con los identificadores 21 y 22. Cada VLAN incluye al menos tres puertos.

c) Un puerto de cada VLAN está etiquetado y su cable va a otro switch.

d) En ese switch, conecta un router. En cada VLAN, conecta dos equipos según el esquema de la Figura 6.72.

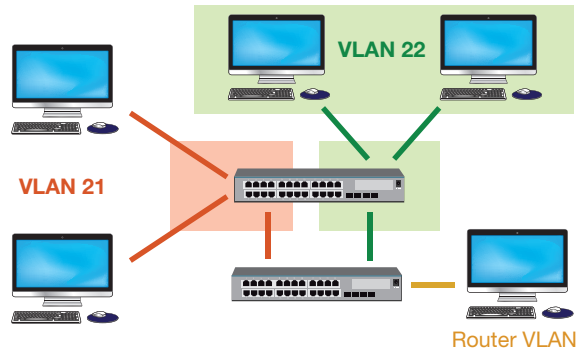


Fig. 6.71. *Ejercicio 3.*

e) Configura el router para que tenga conectividad con los equipos de las VLAN.

f) Documenta todo el procedimiento realizado.

Medidas para evitar la monitorización de redes cableadas: autenticación en el puerto

4. En el laboratorio, configura un switch gestionable para que cumpla estas especificaciones:

a) La contraseña de acceso al switch será mac2puerto.

b) Configura de modo que al puerto 1 solo pueda conectar la tarjeta de uno de los equipos.

c) Comprueba que, conectando otro equipo en ese puerto, no hay conectividad con el switch, pero que sí la hay si lo ponemos en otro puerto no modificado.

d) Documenta todo el procedimiento realizado.

Seguridad en redes inalámbricas

5. Configura el access point del laboratorio para que:

a) La contraseña sea wpa2radius.

b) Utilice el canal 5.

c) El SSID sea wifi5.

d) Esté conectado a un servidor RADIUS cuya contraseña es seguridad5.

e) En el RADIUS haya dos usuarios creados: invitado y soporte, con contraseñas gracias y seguridad55, respectivamente.

f) Comprueba que funciona y documenta el procedimiento.

Unidad 7

Seguridad activa: control de redes



En esta unidad aprenderemos a:

- Aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
- Asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

Y estudiaremos:

- El cortafuegos en equipos o servidores.
- Las listas de control de acceso.
- Las herramientas de protección y desinfección.
- El control de la monitorización en redes cableadas.

1. Espiar nuestra red

En la unidad anterior hemos aprendido a delimitar quién puede usar nuestra red. Para ello establecemos controles en los puntos de conexión, tanto cableados como inalámbricos o en una VPN a través de Internet. En esta unidad vamos a aprender a conocer qué está pasando en nuestra red, qué están haciendo esos usuarios autorizados. Para este fin necesitaremos **espiarnos a nosotros mismos,** buscando garantizar la disponibilidad de la red (localizaremos enlaces saturados) y detectar ataques en curso.

Vamos a **procesar el tráfico** de nuestra red mediante dos tipos de técnicas:

- La **monitorización** del tráfico. Trabaja a **alto nivel:** se limita a tomar **medidas agregadas,** los llamados **contadores.** Por ejemplo, total de bytes enviados o recibidos en un interfaz, agrupados por puerto de origen o destino. La monitorización es habitual en las empresas porque:
  - Resulta **fácil de activar** en toda la red dado que son los propios equipos los que facilitan esta información sobre sus interfaces.
  - Genera relativamente poca información para transmitir y procesar.
  - Es suficiente para conocer la disponibilidad de la red o el tipo de tráfico que transita. Por ejemplo, conocer el porcentaje de tráfico HTTP de nuestra red nos puede llevar a instalar un proxy, como veremos en el apartado 7.3.
- El **análisis** del tráfico. Trabaja a **bajo nivel:** captura todos los paquetes que transitan por una interfaz (los conocidos **sniffer de red**). Los paquetes solo son leídos, no interceptados: el paquete continúa su camino. El procesamiento de estos paquetes leídos permite generar **medidas agregadas,** pero sobre todo interesa analizar las conversaciones entre los equipos, comprobando que se ajustan al comportamiento esperado en el protocolo estándar **(analizador de protocolos).** Aunque esta información es mucho más rica que los simples contadores, la captura es **muy costosa de activar en toda la red,** porque se dispara la cantidad de información que hay que transmitir y procesar (la mayoría de los puertos ya tienen velocidad gigabit); por este motivo, solo se utiliza en situaciones concretas que no se pueden abordar con el estudio de contadores, como es la **detección de ataques.**

En ambos casos, como las redes de las empresas tienen muchos equipos utilizando distintos protocolos, **necesitaremos herramientas** que nos ayuden a recoger, procesar, analizar y presentar toda la información disponible.

Con estas herramientas hay que tener cuidado para conseguir un **equilibrio** entre los objetivos de seguridad y la carga extra que supone tratar esta información (CPU de los equipos de red, tráfico que ocupa en la red enviar los contadores o capturas hasta la herramienta, CPU del servidor de la herramienta, coste del software especializado, dedicación de personal de soporte a consultar los informes y tomar decisiones, etc.).

Los problemas típicos que nos harán aplicar estas técnicas pueden ser tan sencillos como una tormenta de broadcast (demasiados paquetes de tipo broadcast), que podemos detectar en las estadísticas de una interfaz. Y tan complejos como un DoS (Denial of Service, **denegación de servicio**).

Como vimos en la primera unidad de este libro, los DoS son un intento de sobrecarga de un servidor saturándolo de peticiones. Nuestra misión será averiguar si esas peticiones corresponden a clientes reales o a falsos clientes (dirigidos por el atacante). Para ello haremos una captura puntual en un tramo de la red y trataremos de analizar los intentos de conexión a ese servidor: origen, tipo de petición, número de peticiones, etc.

Además de la monitorización del tráfico y el análisis del mismo, hay un tercer elemento para el control de la red: la **sonda.** Una sonda (en inglés probe) es un equipo de la red que está programado para comportarse como un cliente normal de alguno de los servicios que tenemos desplegados. La sonda ejecuta sus operaciones periódicamente, de manera que, si alguna falla, podemos suponer que también le fallará al usuario y debemos corregir el problema.

Web

En este vídeo nos enseñan una herramienta de control de velocidad de conexión:

http://goo.gl/WaOBC

En la segunda parte permiten elegir las aplicaciones que sufren la limitación:

http://goo.gl/Q3Z6A

Actividades

1. ¿Qué tenemos que vigilar más, Internet o nuestra propia LAN?
2. Busca precios y especificaciones sobre hubs (no switch) de altas velocidades (100/1 000 Mbps).
3. Busca información sobre lo que hace un traffic shaper.

Caso práctico 1

Monitorización de tráfico

■ **Duración**: 1 hora ■ **Dificultad**: Alta

Objetivo. Aprender a configurar e interpretar interfaces monitorizadas.

Material. Cuatro ordenadores (uno con Windows 7, tres con Linux Ubuntu), acceso a Internet, software SpiceWorks.

1. Vamos a instalar una red con un router Linux, un par de ordenadores de trabajo (llamados Ubuntu Server y Ubuntu Desktop) y un ordenador más, que será la estación de supervisión, donde corre el software de monitorización. Desde los ordenadores de trabajo generaremos tráfico de red sobre el router Linux y desde la estación de supervisión controlaremos todo el proceso.
2. Primero conectamos los ordenadores según el esquema de la Figura 7.1. El ordenador llamado Ubuntu Desktop puede ser una máquina virtual corriendo en la estación de supervisión. Necesitaremos conexión a Internet en la estación de supervisión para descargar el software asociado.

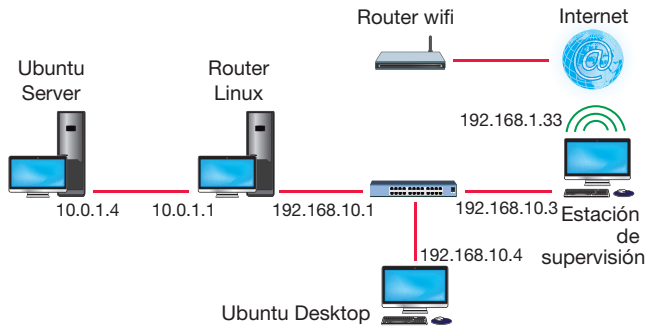


Fig. 7.1. *Esquema de monitorización.*

3. El router Linux conecta dos subredes: la 10.0.1.0/24 y la 192.168.10.0/24. Hay una tercera subred, la 192.168.1.0/24, para la salida a Internet por el router ADSL.
4. Para facilitar la tarea, utilizaremos direcciones estáticas en todas las interfaces:
   a) 10.0.1.4 en Ubuntu Server.
   b) 10.0.1.1 y 192.168.10.1 en router Linux.
   c) 192.168.10.4 en Ubuntu Desktop.
   d) 19192.168.10.3 y 192.168.1.33 en la estación de supervisión.
5. En la Figura 7.2 vemos la configuración de la interfaz Ethernet de la estación de supervisión. No necesitamos servidor DNS porque siempre trabajaremos directamente con las direcciones IP.

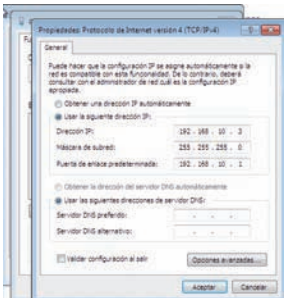


Fig. 7.2. *Configuración IP de la estación de supervisión.*

6. No debemos olvidar activar el enrutamiento de paquetes en el router Linux para que de verdad actúe como un router. Basta con introducir un 1 en el fichero `ip _ forward`.

```
# echo 1 > /proc/sys/net/ipv4/ip _ forward
```

7. Terminada la configuración de direcciones, empezamos con los generadores de tráfico. En el router Linux vamos a poner un servidor FTP y desde los ordenadores de trabajo (Ubuntu Server y Ubuntu Desktop) efectuaremos descargas de ficheros continuamente.
8. Como servidor FTP podemos utilizar vsftpd. Lo instalaremos con apt-get install vsftpd y dejaremos la configuración por defecto. La descarga la haremos con el usuario anonymous; por tanto, los ficheros que vamos a descargar debemos ponerlos en el directorio particular del usuario FTP (será `/home/ftp`). Ahí crearemos un fichero de 10 KB con el comando:

```
# dd if=/dev/zero of=/home/ftp/10k bs=1024
count=10
```

9. Ahora vamos a los dos ordenadores de trabajo para crear los generadores de tráfico. Utilizaremos un script llamado `generador.sh`:

```
# cat generador.sh
N=$1
E=$2
while `expr $N > 0`
do
 echo intento $N
 $N=`expr $N - 1`
 ftp 192.168.10.1 <<EOF
get 10k
bye
EOF
 sleep $E
done
```

El primer parámetro es el número de ejecuciones, y el segundo, el tiempo entre cada ejecución. Podemos probar con diez ejecuciones y un segundo entre cada una.

(Continúa)

Caso práctico 1

(Continuación)

La dirección IP del servidor FTP será la `192.168.10.1` para Ubuntu Desktop y `10.0.1.1` para Ubuntu Server.

Para que funcione correctamente necesitamos evitar que el comando FTP nos pida usuario y contraseña en cada intento. Esto se consigue introduciendo esta línea en el fichero `.netrc` del directorio personal del usuario en los ordenadores de trabajo:

```
# cat $HOME/.netrc
default login anonymous password a@b.com
```

10. Listos los generadores, vamos a la estación de supervisión e instalamos el software SpiceWorks. El procedimiento se explicó en la Unidad 5, en el caso práctico 13. Para ahorrar tiempo podemos directamente escanear los equipos que nos interesan: router Linux y Ubuntu Server. Utilizaremos consultas SNMP en los dos casos.

11. Si todo va bien, la herramienta localizará el router Linux. En la Figura 7.3 vemos que tiene cuatro interfaces: el loopback, un Ethernet en la red 192.168.10.X y otro en la 10.0.1.X. Hay una cuarta interfaz wifi que no es necesaria en ese momento y la dejamos desactivada.

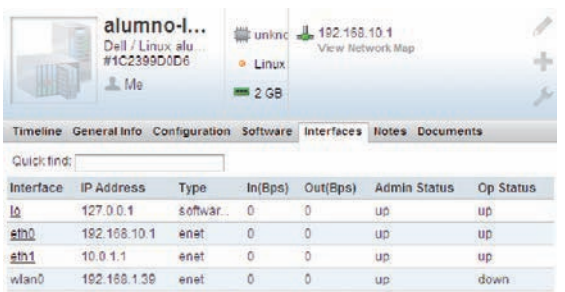


Fig. 7.3. *Localizado router Linux.*

12. También debería aparecer Ubuntu Server. En la Figura 7.4 se aprecian tres interfaces: loopback, un Ethernet en la red 10.0.1.X y un Ethernet más en la red del router wifi (de nuevo, no es necesario y está desactivado).

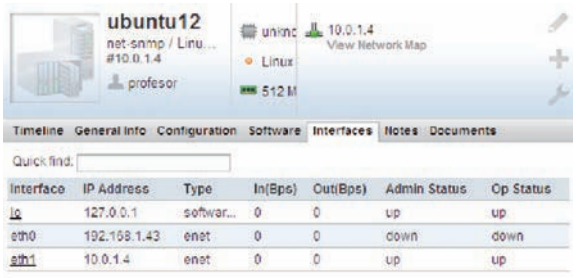


Fig. 7.4. *Localizado Ubuntu Server.*

13. Para ayudarnos a la monitorización vamos a instalar un componente nuevo en SpiceWorks. Se llama Bandwidth Monitor. Lo buscaremos entrando en la pestaña *Community* (Fig. 7.5). En la comunidad contactaremos con otros usuarios del producto para pedir ayuda, compartir experiencias, etc. La primera vez nos pedirá crear una cuenta, que puede ser distinta a la utilizada durante la instalación, porque podemos tener varias instalaciones de SpiceWorks pero solo una cuenta de comunidad.

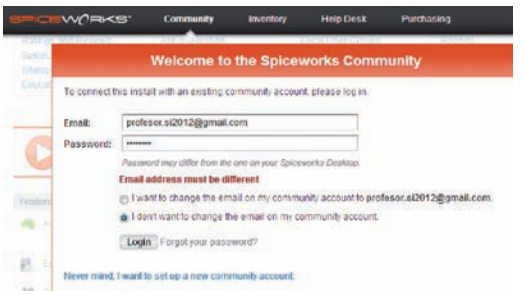


Fig. 7.5. *Entramos en la comunidad de SpiceWorks.*

14. Dentro del menú *Community* vamos a la opción *Extensions Center* y elegimos *Plugins* (Fig. 7.6).

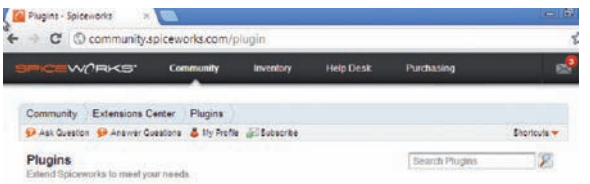


Fig. 7.6. *Buscamos entre los plugins.*

15. Lo buscamos por su nombre: Bandwidth Monitor (Fig. 7.7).

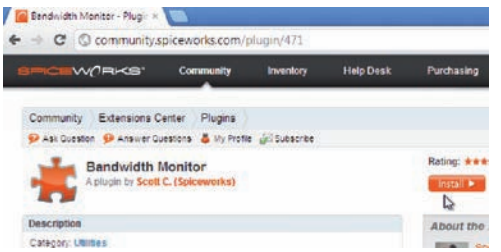


Fig. 7.7. *Encontramos el Bandwidth Monitor.*

16. Lo instalamos. Al final de la instalación nos pregunta si lo queremos añadir al dashboard (panel de control). En este ejercicio no lo haremos porque en ese panel solo muestra una gráfica, y necesitamos dos.

(Continúa)

Caso práctico 1

(Continuación)

17. Entramos en la ventana del plugin. Podemos hacerlo desde *Inventory > My tools*. La herramienta nos ofrece cuatro zonas desde donde controlar la actividad de red de las máquinas del inventario. Elegiremos el router Linux y el Ubuntu Server. Una vez seleccionados, no hace falta tener siempre abierta esta página: la herramienta sigue recogiendo datos, los estemos consultando o no.

18. Ahora activamos el generador de tráfico en Ubuntu Server. Al poco tiempo veremos unas gráficas similares a las de la Figura 7.8.

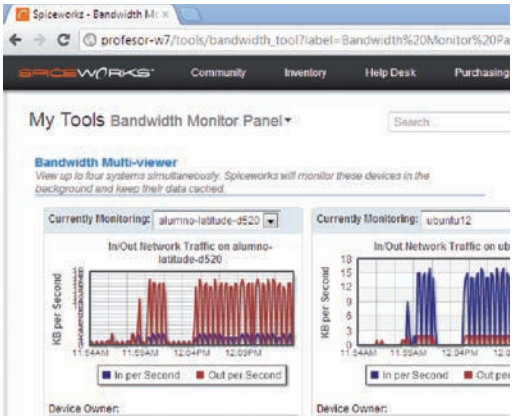


Fig. 7.8. *Ocupación de red con un FTP.*

19. La gráfica de la izquierda muestra la ocupación de las interfaces de red en el router Linux. La línea roja representa el tráfico saliente, y la línea azul, el tráfico entrante. El tráfico saliente es mucho mayor porque nuestro generador de tráfico descarga el fichero; el tráfico entrante se limita a los paquetes ACK del protocolo. Si el generador subiera ficheros en lugar de bajarlos, el comportamiento de las líneas sería el contrario (mucho más azul que rojo).

20. La gráfica de la derecha muestra la ocupación de las interfaces de red en el Ubuntu Server. Como era de esperar, el tráfico entrante es muy superior porque estamos recibiendo el fichero. Los valores de ambas gráficas son similares (entre 15 y 18 KBps), lo que indica que todo el tráfico del router Linux se debe al generador del Ubuntu Server.

21. Activamos ahora el segundo generador en la máquina Ubuntu Desktop. Veremos que la gráfica de Ubuntu Server no cambia (no hemos hecho nada en ella), pero la correspondiente al router Linux duplica su tráfico (Fig. 7.9). Ahora procesa unos 32 KBps de tráfico saliente.

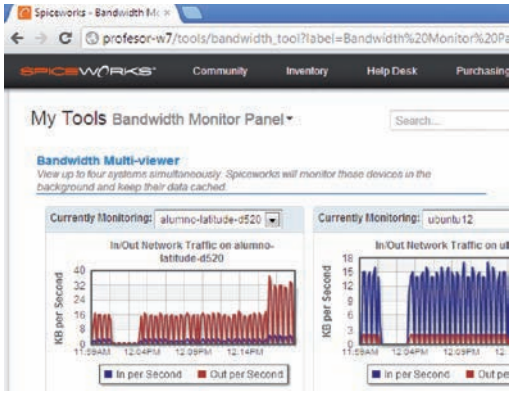


Fig. 7.9. *Ocupación de red con dos FTP.*

22. Estas gráficas ayudan a conocer el estado de ocupación de las interfaces de red. Unos valores anormalmente altos nos deben alertar de que puede estar saturada, por lo que el rendimiento será menor al habitual; unos valores anormalmente bajos nos deben alertar de que algo ha dejado de funcionar.

23. Para detectar estas situaciones no tiene sentido tener abiertas todas las gráficas de todas las máquinas de la red. Como vimos en el caso práctico de la Unidad 5, podemos utilizar los monitores para generar alertas que nos avisen. Cuando nos llegue una alerta, sí tiene sentido consultar las gráficas de las máquinas relacionadas con ese problema concreto.

24. Vamos a simular un problema en la red: desconectamos el cable que hay entre Ubuntu Server y el router Linux. Además de generarse la alerta, es fácil detectarlo en nuestras gráficas por dos razones: la gráfica del router Linux muestra menos tráfico y la gráfica de Ubuntu Server se congela: ya no introduce más datos, se queda con las fechas de la última recolección (Fig. 7.10).

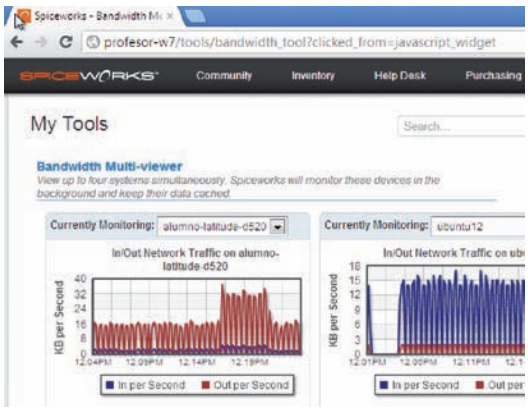


Fig. 7.10. *Quitamos un cable.*

(Continúa)

Caso práctico 1

(Continuación)

25. Por supuesto, el problema aparece en el inventario (recordemos que el bandwidth monitor es un plugin opcional). En la Figura 7.11 se ve el aviso de la pérdida de conexión con un servidor.



Fig. 7.11. *Aviso de pérdida de conexión.*

26. Pulsamos sobre esa máquina y vemos que ya no llegamos a la interfaz 10.0.1.4 (Fig. 7.12).



Fig. 7.12. *Interfaz inalcanzable.*

27. Si reconectamos el cable, el generador vuelve a cargar el router Linux y las gráficas recuperan la normalidad (Fig. 7.13). La gráfica de Ubuntu Server empezará a mostrar datos de la fecha actual.

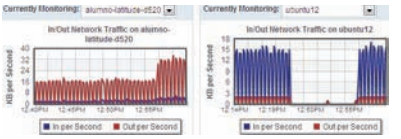


Fig. 7.13. *Conexión recuperada.*

Como hemos señalado con anterioridad, la monitorización del tráfico es relativamente fácil de activar en una red, porque los equipos suelen estar preparados para facilitarnos la información sobre sus contadores y basta con preguntarles periódicamente. En cambio, la captura de conversaciones es más compleja de activar. Las opciones son:

- Conseguir el control sobre alguno de los **extremos de la conexión** para poder utilizar alguna de las herramientas que veremos a continuación (tcpdump, wireshark).
- **Interceptar la conexión** misma desde algún equipo de red por donde pasen los paquetes intercambiados. Si este equipo tiene cierta inteligencia, seguramente incorporará funcionalidades avanzadas, como el port mirroring; incluso puede ser un router Linux, con lo que tendremos a nuestro alcance todas las herramientas que veremos para los extremos.
- Como último recurso podríamos **conectar de manera temporal un hub** en el puerto que queremos vigilar (Fig. 7.14), pero esto supone desplazamientos de personal y equipos que no siempre están disponibles (por ejemplo, el switch de LAN está en Barcelona, pero el departamento de soporte está en Madrid). Utilizamos un hub y no un switch porque el hub repite el tráfico de cada puerto a todos los demás, justo lo que necesitamos.

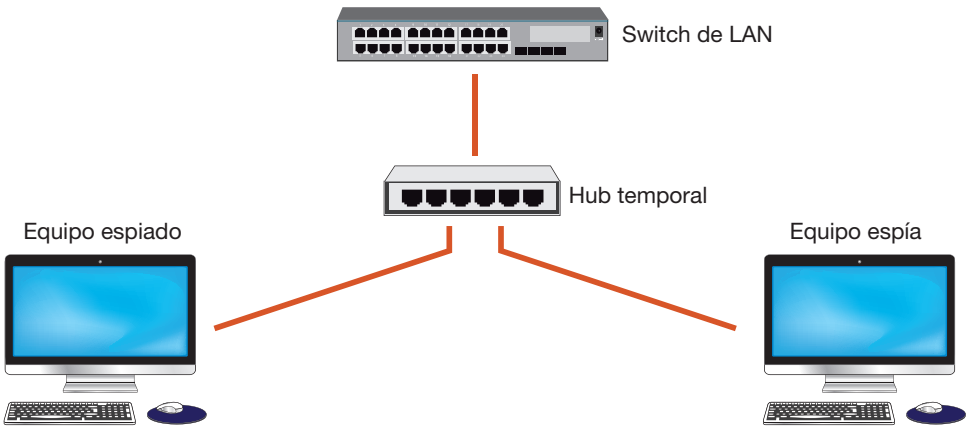


Fig. 7.14. *Espionaje utilizando un hub temporal.*

Vocabulario

Port mirroring. Funcionalidad de los switch que permite enviar a un puerto todo el tráfico de otro puerto.

Router Linux. Ordenador con sistema operativo Linux y varias tarjetas de red que ejecuta el software adecuado para realizar tareas de router (interconexión de VLAN, salida balanceada a Internet, etc.).

1.1. tcpdump

tcpdump es una herramienta sencilla disponible en Linux que permite hacer un **volcado de todo el tráfico que llega a una tarjeta de red.** Captura todo el tráfico, no solo el tráfico TCP, como aparece en su nombre. Los paquetes leídos se muestran en pantalla o se pueden almacenar en un fichero del disco para ser tratados posteriormente por esta misma herramienta u otra más avanzada. Se necesitan privilegios para ejecutarla, porque necesitamos **poner la tarjeta en modo promiscuo** para que acepte todos los paquetes, no solo los destinados a suMAC, como ya vimos en la Unidad 6.

La captura con tcpdump se puede hacer en uno de los extremos si la conversación que estamos estudiando ocurre entre una máquina Unix y otra máquina Unix/Windows/etc. (hay versiones de tcpdump para Windows, pero aquí es mejor WireShark). Aunque también lo utilizaremos muchas veces para capturar las conversaciones que atraviesan un router Linux. En la distribución representada en la Figura 7.15 podremos capturar las comunicaciones entre los ordenadores de las dos VLAN y todas las conexiones a Internet, aunque no podremos conocer qué hablan entre sí los ordenadores de una misma VLAN.

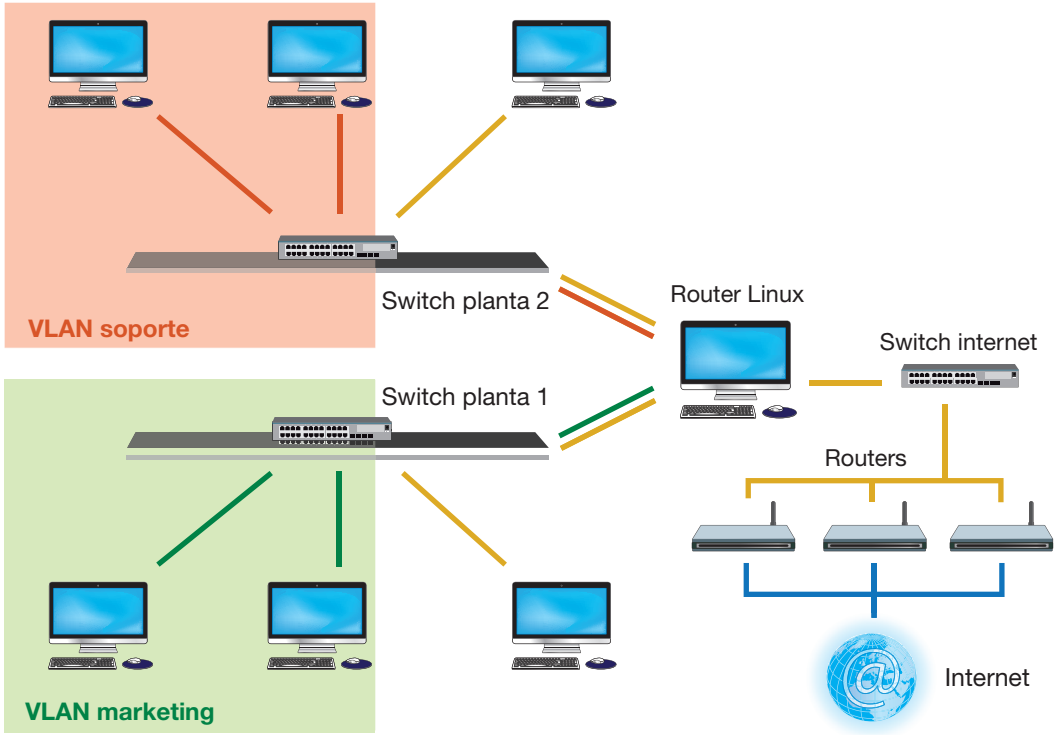


Fig. 7.15. *Captura con router Linux.*

¿Sabías que...?

tcpdump es un analizador de paquetes. Es útil para protocolos no orientados a conexión, como IP, UDP, DHCP, DNS e ICMP. Pero no ayuda mucho en los protocolos orientados a conexión, como HTTP y SMTP, donde interesa identificar fácilmente todos los paquetes de una conexión.

Actividades

4. Investiga qué son los filtros de tcpdump y prueba algunos de ellos.
5. Prueba a decodificar una conversación ping, FTP o HTTP mediante tcpdump –X.
6. Prueba a conectar dos o tres routers Linux en cascada y efectúa captura en todas las interfaces para comprobar cómo cruzan los paquetes de un extremo a otro.
7. Utiliza tcpdump para comprobar que los paquetes destinados a la misma subred llevan la IP y la MAC del ordenador destino, mientras que los paquetes destinados a ordenadores de otra subred llevan la IP del ordenador destino pero la MAC de la puerta de enlace.
8. ¿Cuándo podemos utilizar tcpdump con la opción -n, y qué nos aporta?

Caso práctico 2

Uso de tcpdump

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

Objetivo. Capturar el tráfico que atraviesa un router Linux.

Material. Tres ordenadores, uno de ellos con Linux Ubuntu.

1. Vamos a aprovechar la red desplegada para el caso práctico 1. Reutilizamos el router Linux y los dos ordenadores de trabajo Linux (aunque para estos también se pueden utilizar otras máquinas, mientras conserven la misma configuración IP). El tráfico lo producirá un simple ping entre nuestros equipos.

2. Nos situamos en el router Linux y abrimos un terminal. Incrementamos privilegios con `sudo -i` y ejecutamos el comando:

   ```
   # tcpdump -i eth0 -l -n | grep ICMP
   ```

   El parámetro `-i` indica la interfaz donde queremos escuchar. El parámetro `-l` consigue que las líneas aparezcan en pantalla con fluidez. El parámetro `-n` nos evita intentar traducir las direcciones IP que capturaremos (puede ralentizar la salida, y en nuestro caso no tiene sentido porque son direcciones de prueba). Finalmente, filtramos la salida del comando porque solo nos interesan los paquetes ICMP.

   Para finalizar la captura hay que interrumpir la ejecución **(Control+C).**

3. Ahora vamos al Ubuntu Desktop y hacemos un ping al router Linux. En la ventana del terminal del router Linux aparecen inmediatamente los paquetes capturados (Fig. 7.16).

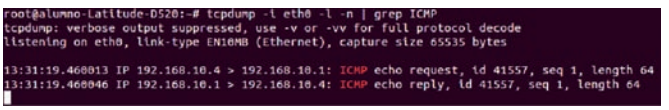


Fig. 7.16. *Captura de ping directo.*

4. El comando muestra una línea por cada paquete. La primera columna es el instante de la captura. Utiliza mucha precisión porque las interfaces son muy rápidas y muchas veces necesitaremos relacionar capturas simultáneas en varias interfaces de la misma máquina (si son otras máquinas habrá que añadir el desfase de sus relojes).

   Después viene el tipo de protocolo (IP) y la dirección de origen y de destino. Comprobamos que el ping consiste en dos paquetes: uno del origen al destino preguntando si está conectado (`echo request`), y otro del destino al origen confirmándolo (`echo reply`).

   El resto de la línea depende de la naturaleza del paquete capturado. Se puede añadir más información utilizando los parámetros `-v` y `-vv`.

5. Hemos capturado un paquete que venía destinado a nosotros. Ahora vamos a capturar un paquete que atraviesa el router camino de su destino: será un ping desde Ubuntu Desktop hasta Ubuntu Server. Como atravesará dos interfaces, necesitamos una segunda ventana donde capturaremos el tráfico en la interfaz `eth1`.

6. La captura en `eth0` se muestra en la Figura 7.17. Aparece el primer paquete con origen Ubuntu Desktop y destino Ubuntu Server, preguntándole si está disponible. El segundo paquete es la respuesta de Ubuntu Server.

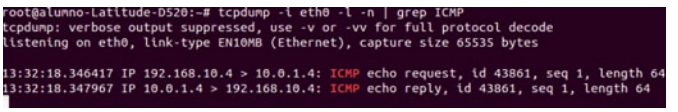


Fig. 7.17. *Captura en primer tramo de ping remoto.*

7. La captura en `eth1` se muestra en la Figura 7.18. Aparecen los mismos paquetes que en la primera interfaz (el router no necesita introducir cambios: se limita a pasarlos de una interfaz a otra). Si nos fijamos en la fecha de cada paquete, podemos confirmar que el primero es el `echo request` en el `eth0`; luego, el mismo `echo request` en el `eth1`. Después, el `echo reply` en el `eth1` y, finalmente, el `echo reply` en `eth0`.

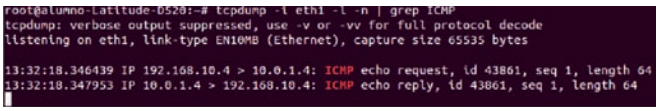


Fig. 7.18. *Captura en segundo tramo de ping remoto.*

8. Finalmente indicamos cómo se consigue que la captura de paquetes se almacene en un fichero (Fig. 7.19). Usaremos el parámetro `-w` junto al nombre del fichero:

   ```
   # tcpdump -i eth0 -w e0
   ```

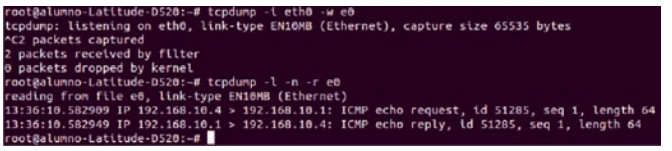


Fig. 7.19. *Volcado de captura a fichero.*

Si la captura va a ser larga, conviene asegurarse de que hay suficiente espacio libre en el disco. El fichero puede ser procesado por el propio `tcpdump` con el parámetro `-r`:

```
# tcpdump -l -n -r e0
```

1.2. WireShark

WireShark es la herramienta más extendida en Windows para realizar capturas de tráfico y analizar los resultados. Es una evolución de una herramienta anterior llamada Ethereal. Para la captura de paquetes utiliza la librería pcap, que también aparece en otros sniffer, como tcpdump. La interfaz de usuario es muy potente, así como el número de protocolos que es capaz de analizar.

Caso práctico 3

Uso de WireShark

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

Objetivo. Capturar y analizar tráfico mediante WireShark.

Material. Dos ordenadores, uno de ellos con Windows 7.

1. Siguiendo con el mismo esquema de red utilizado en el caso práctico 1, en el ordenador con Windows 7 descargamos la herramienta desde **wireshark.org.** Durante la instalación puede que detecte que ya hay una librería pcap (Fig. 7.20). En nuestro caso nos muestra que ha sido instalada por SpiceWorks. Como es la misma versión, la dejamos.

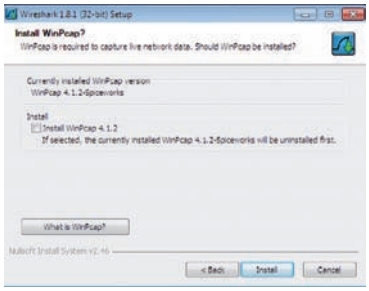


Fig. 7.20. *Librería ya disponible.*

2. Terminada la instalación, abrimos la herramienta. Las operaciones disponibles son muy numerosas, como corresponde a una herramienta muy potente. Vamos a realizar una captura. En el menú *Capture* elegimos *Interfaces* para seleccionar dónde queremos actuar (Fig. 7.21).

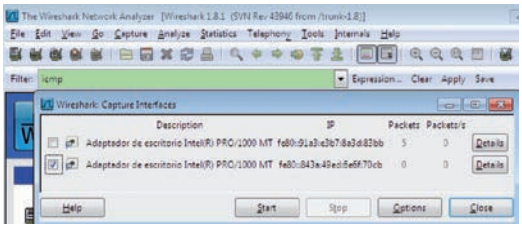


Fig. 7.21. *Elegimos interfaz de captura.*

En nuestro caso elegimos la interfaz que nos conecta con la red 192.168.10.X. También aprovechamos para crear un filtro: como en el caso práctico 2, vamos a capturar el tráfico del comando ping. En *Filter* pondremos icmp.

3. Desde el propio Windows 7 hacemos un ping al router Linux en su dirección 192.168.10.1. La ventana del WireShark se actualiza inmediatamente (Fig. 7.22).

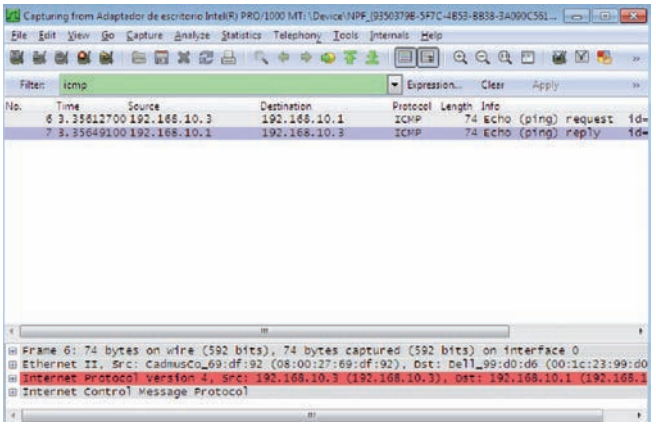


Fig. 7.22. *Capturamos ping saliente.*

En la primera parte de la ventana la información que aparece es muy similar al tcpdump. La primera columna es el número de paquete de la captura. La segunda es el instante en que ha sido capturado. Después vienen las direcciones de origen y de destino, luego el protocolo y el resto de la información particular de ese paquete.

Como esperábamos, hay un `echo request` desde nuestra máquina al router Linux, y un `echo reply` en sentido inverso.

4. La segunda parte de la ventana es mucho más interesante, porque entra en detalles capa por capa: nivel físico, enlace, red y aplicación (según el protocolo correspondiente).

5. Puede ocurrir que no sea 1 el número del primer paquete que vemos; efectivamente, el filtro icmp que hemos puesto es un filtro de visualización. Se aplica tras realizar la captura. Si lo quitamos pulsando en *Clear*, veremos todos los paquetes capturados (Fig. 7.23).

Ahora vemos paquetes de otras máquinas, utilizando protocolos privados, como Dropbox, y protocolos estándares, como ARP.

(Continúa)

Caso práctico 3

(Continuación)

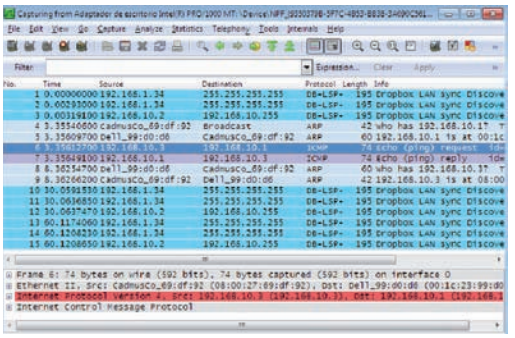


Fig. 7.23. *Captura completa.*

6. Como ya hemos dicho, la herramienta es capaz de analizar multitud de protocolos. Pulsando en *Expression* podemos componer el filtro más adecuado en cada caso. Como se ve en la Figura 7.24, la lista es amplísima.

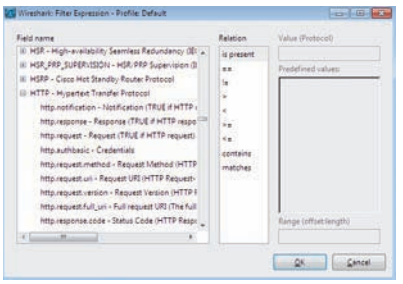


Fig. 7.24. *Multitud de protocolos disponibles.*

7. Vamos a realizar una captura más complicada que un simple ping. En la ventana de filtros introducimos ahora http.request, que es una petición HTTP. Activamos la captura sobre la interfaz con conexión a Internet y abrimos el navegador sobre **google.es.** En la ventana de WireShark aparecen los paquetes capturados (Fig. 7.25). Cuando la página haya terminado de descargarse, detenemos la captura pulsando el icono de *Stop* (o en el menú *Capture* > *Stop*).

8. En la parte inferior de la ventana podemos entrar a ver los detalles del protocolo HTTP. Por ejemplo, en la Figura 7.25 el segundo paquete se refiere a la descarga de una imagen PNG.

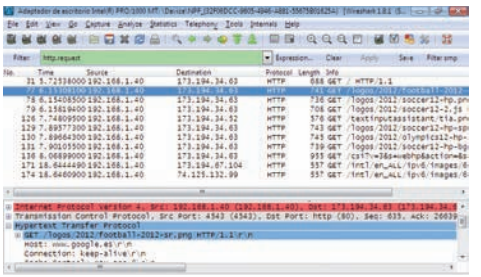


Fig. 7.25. *Captura de peticiones HTTP.*

9. Sin hacer una nueva captura, podemos cambiar el filtro para ver las respuestas. El nuevo filtro será http.response. En la Figura 7.26 se ha destacado el primer paquete, cuyo contenido aparece en la parte inferior: es el código JavaScript de la página de Google.

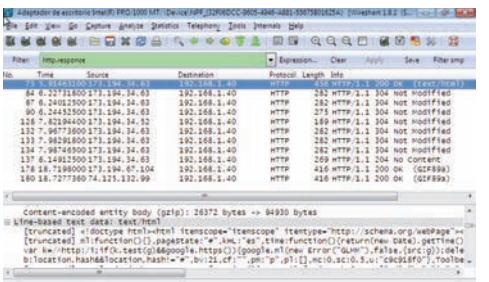


Fig. 7.26. *Captura de respuestas HTTP.*

10. Finalmente, conectamos con una página segura que utilice HTTPS, como la página de un banco. En la captura aparecerán nuevos protocolos como TLS, pero aunque podemos abrir los paquetes capturados, su contenido no se entiende porque va cifrado.

1.3. Port mirroring

Los **switch gestionables** suelen incorporar esta funcionalidad. Consiste en modificar la configuración del switch para que **replique todo el tráfico de un puerto a otro.** En el segundo puerto conectaremos el sniffer. El equipo o equipos conectados en el primer puerto funcionan con normalidad, no saben que están siendo espiados.

Generalmente se puede elegir el tipo de tráfico: entrante (desde el equipo hasta el switch), saliente (desde el switch hasta el equipo) o ambos. En algunos modelos podemos hacer que **varios puertos** vuelquen su tráfico a un mismo puerto, aunque habrá que vigilar las prestaciones del conjunto porque pueden desbordar el ancho de banda de la interfaz o la capacidad de captura del sniffer, lo que ocasionaría la pérdida de paquetes, invalidando el análisis posterior.

Caso práctico 4

Port mirroring

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

Objetivo. Probar el replicado de puertos en un switch.

Material. Switch gestionable (en este ejemplo es un TP-Link TL-SG2216WEB), cuatro ordenadores (al menos uno con Windows), salida a Internet.

1. Uno de los ordenadores servirá para controlar el switch, dos generarán tráfico de trabajo y el cuarto recibirá el tráfico replicado (este ordenador será Windows para poder utilizar WireShark).
2. Primero conectamos en el puerto 5 el ordenador que controla el switch. En el puerto 1 ponemos el ordenador espía, y en el puerto 2, uno de los ordenadores de trabajo. Uno de los puertos estará conectado a un router con salida a Internet.
3. En el ordenador del puerto 1 abrimos el WireShark y lanzamos una captura de la interfaz conectada al switch. En el ordenador de trabajo hacemos un simple ping a una máquina de Internet. Como estamos en un switch, en la ventana del WireShark no debería aparecer ningún paquete de esa comunicación.
4. Nos ponemos ahora en el ordenador del puerto 5 y entramos al servidor web que gestiona la configuración del switch. Tras solicitar autenticación, aparece una página con las opciones disponibles. Nos vamos a *Port mirroring* y configuramos que se copie al puerto 1 todo el tráfico que entra al puerto 2 procedente del ordenador (Fig. 7.27). Para ello elegimos *Ingress* en *Mirror Mode*, 1 en el *Mirror Port* y marcamos el 2 en *Mirrored Port*.

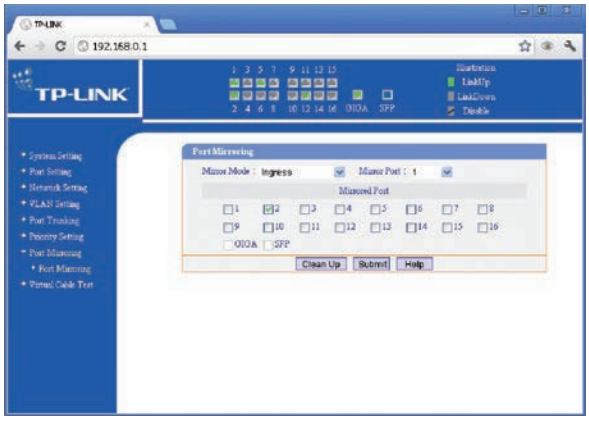


Fig. 7.27. *Activamos Port mirroring.*

5. Pulsamos *Submit* y desde este momento sí podemos capturar el tráfico de ese puerto. En la Figura 7.28 aparecen todos los paquetes echo request que salen de la máquina local (192.168.35.25) hasta la máquina de Internet.

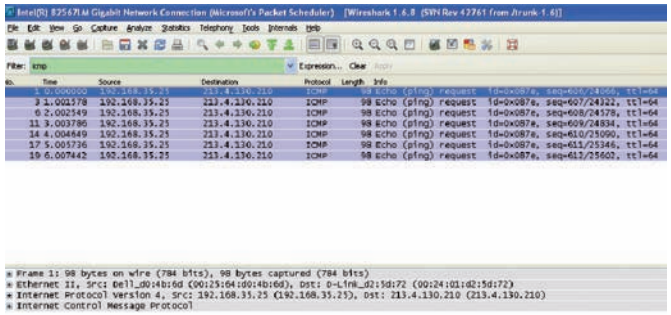


Fig. 7.28. *Tráfico del puerto 2 capturado.*

6. Conectamos ahora en el puerto 3 el segundo ordenador de trabajo. Si en esta máquina hacemos ping, esos paquetes no son capturados (aunque seguimos pudiendo capturar los del puerto 2). Para conseguirlo, volvemos a la configuración del switch y activamos la copia de un segundo puerto sobre el mismo puerto 1 (Fig. 7.29).

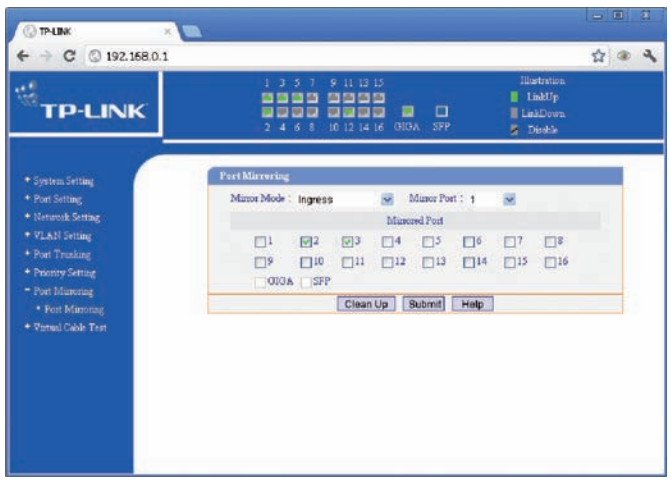


Fig. 7.29. *Doble copiado.*

7. Completamos el cambio de configuración pulsando *Submit* y ahora sí aparecen capturados los paquetes que las dos máquinas envían al switch (Fig. 7.30).

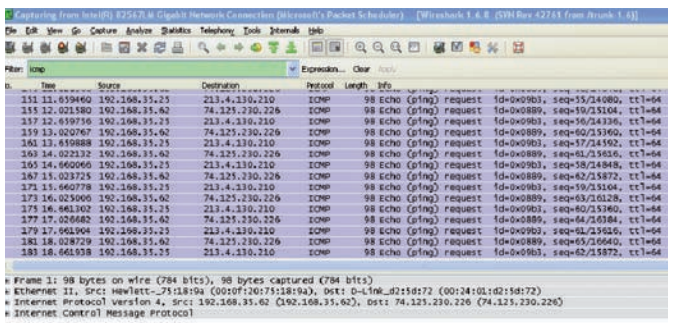


Fig. 7.30. *Tráfico de los puertos 2 y 3 capturado.*

1.4. IDS/IPS. Snort

Las herramientas de análisis de tráfico son más o menos sencillas de instalar y configurar; pero la complicación viene a la hora de interpretar los resultados. Para sacar el máximo partido a estas herramientas se necesitan muchos conocimientos de base y una amplia experiencia en protocolos de comunicaciones.

Hay un segundo problema: aunque dispongamos de personal tan cualificado, no es humanamente posible revisar una a una todas las conversaciones que ocurren a diario en una red normal. Sobre todo porque la mayoría son interacciones normales, libres de toda sospecha. Los expertos hay que reservarlos para los casos difíciles.

Para solucionar ambos problemas existen los sistemas IDS/IPS (Intrusion Detection System / Intrusion Prevention System). Los **IDS detectan** los ataques y los **IPS actúan** contra ellos. Tenemos dos tipos de IDS/IPS:

- NIDS/NIPS **(Network Intrusion y Network Prevention).** Buscan ataques sobre servicios de comunicaciones. Se basan en el análisis de los paquetes que forman parte de la comunicación entre dos máquinas, comprobando que se ajustan al protocolo estándar.
- HIDS/HIPS **(Host Intrusion y Host Prevention).** Buscan ataques sobre las aplicaciones y el sistema operativo de la máquina. Se basan en el análisis de los procesos actuales (ocupación de CPU y memoria, puertos abiertos) y la configuración y el log de cada uno de los servicios.

En este tema vamos a referirnos a los NIDS/NIPS. Estos sistemas procesan un fichero de captura de tráfico (o la realizan ellos mismos) y **buscan patrones de comportamiento** en los paquetes intercambiados entre los equipos. No se limitan a revisar las cabeceras del protocolo, sino que también miran en el contenido del paquete (payload). Cuando detectan un posible ataque, si es un IDS solo avisa al usuario (como mínimo, fichero de log) y si es un IPS solo responde al ataque (también se puede hacer que los IPS avisen).

La respuesta de un IPS puede ser impedir que ese paquete y los siguientes de esa conexión lleguen a su destino. En los más avanzados se puede configurar que permitan que el paquete llegue, pero adecuadamente modificado para que no prospere el ataque.

La inteligencia de estas herramientas suele residir en un **conjunto de reglas** que se cargan en el programa desde un fichero de configuración. Las reglas son elaboradas por expertos en seguridad que, cuando han identificado un nuevo tipo de ataque, escriben la regla que permitirá al IDS detectarlo.

Los problemas de los IDS son dos:

- **Rendimiento.** El número de reglas es creciente (hay nuevos ataques y no podemos descartar los antiguos) y el volumen de tráfico también, por lo que necesitamos un **hardware muy potente** para tener funcionando un IDS sobre capturas de tráfico en **tiempo real.** En determinados momentos, la cola de paquetes pendientes de examinar será tan larga que la interfaz estará a punto de empezar a descartarlos; para evitarlo, el IDS los dejará pasar, a sabiendas de que puede ser un ataque (si no los deja pasar, nosotros mismos estaremos ejecutando un ataque). Pero si nos limitamos a procesar ficheros de captura antiguos, puede que encontremos ataques que ya han ocurrido y sea tarde para reaccionar.
- **Falsos positivos.** Las reglas no son perfectas y puede que estemos alertando sobre comunicaciones que son perfectamente legales. Conviene probar muy bien una regla antes de meterla en un IPS.

Web

En este vídeo nos enseñan la instalación de Snort en Windows:
http://goo.gl/n64TM
Hay herramientas mucho más simples, pero mucho menos potentes:
http://goo.gl/XRm7G

Actividades

9. Prueba a generar algún ataque contra las reglas conocidas en Snort.

10. Investiga qué es el modo inline de Snort y pruébalo.

Caso práctico 5

Snort

■ **Duración**: 🕒 30 minutos ■ **Dificultad**: ☹ Alta

Objetivo. Configurar Snort para detectar ataques.

Material. Dos ordenadores con Linux Ubuntu.

1. La herramienta Snort es un IDS/IPS ampliamente utilizado. Incluye multitud de reglas preconfiguradas para los ataques conocidos y periódicamente se publican actualizaciones. Además, es sencillo añadir las reglas que necesitemos.

2. Necesitaremos el ordenador Ubuntu Server (dirección 10.0.1.4) y el Ubuntu Desktop (dirección 10.0.1.3) de la maqueta de red que estamos utilizando a lo largo de esta unidad. En el Ubuntu Server instalaremos la herramienta mediante:

```
# apt-get install snort
```

   Durante la instalación nos preguntará algunos parámetros, como la red que queremos controlar. Más adelante podremos cambiar esta primera configuración.

3. Los ficheros de configuración están en el directorio `/etc/snort`, y los ficheros de log en `/var/log/snort`. La herramienta admite varios modos de funcionamiento. Puede ser un simple sniffer ejecutando:

```
# snort –i eth1
```

   Desde este momento estamos capturando paquetes de la interfaz `eth1`. Por ejemplo, si entramos en el Ubuntu Desktop y hacemos un ping al Ubuntu Server, veremos los paquetes `echo` (Fig. 7.31). Como ya vimos en el `tcpdump`, por cada paquete aparece la fecha de la captura (con mucha precisión), la IP origen e IP destino del paquete, el tipo de protocolo (en este caso, `ICMP`) y detalles del protocolo (`ECHO`, `ECHO REPLY`).

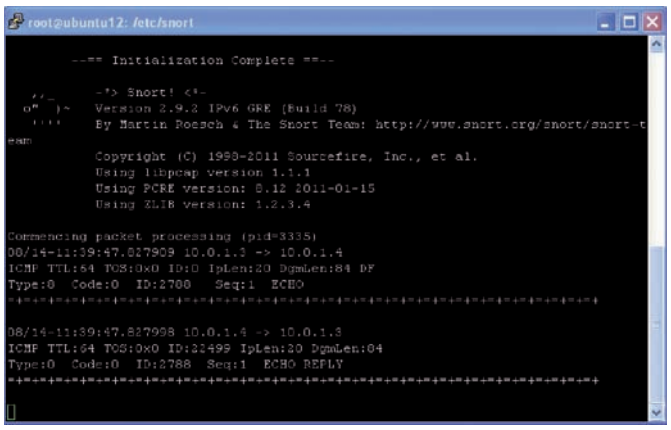


Fig. 7.31. *Capturando tráfico.*

4. Podemos interrumpir la captura pulsando **Control+C.** Aparecerá un resumen de la sesión: total de paquetes capturados y desglosados por protocolo. Pero la potencia de Snort no está en la captura y visualización de paquetes de red, sino en el tratamiento que hace de ellos para detectar ataques. Vamos a probar cómo detecta escaneo de puertos con nmap, que, como vimos en la Unidad 6, se utiliza para conocer los servicios ofrecidos por una máquina. Esta información puede ser utilizada por el atacante para elegir sus herramientas.

5. Una vez capturados, Snort pasa los paquetes por varias etapas de procesamiento. Primero los decodifica para identificar el protocolo que siguen. Después aplica un preprocesamiento que deja la información lista para el analizador. Finalmente, genera el resultado del análisis.

6. La inteligencia de estas operaciones reside en reglas. Para nmap vamos a utilizar las reglas del preprocesador. Estas reglas no están en el paquete binario snort que hemos instalado, sino que hay que bajarse las fuentes de la web del producto **(www.snort.org).** De ese fichero .tar.gz extraemos el directorio `preproc_rules` y lo situamos en `/etc/snort`.

7. Ya tenemos las reglas. Ahora falta activarlas. En el fichero `/etc/snort/snort.conf` hay que modificar dos líneas (las líneas están, pero comentadas: debemos descomentarlas):

```
preprocessor sfportscan: proto { all }
memcap { 10000000 } sense_level { low }
```

```
include $PREPROC_RULE_PATH/preprocessor.rules
```

   La primera activa el preprocesador que vigila el escaneo de puertos. La segunda añade las reglas de preprocesador al conjunto de reglas que serán aplicadas a los paquetes.

8. También cambiaremos esta línea, porque solo nos interesa vigilar nuestra subred:

```
ipvar HOME_NET 10.0.1.0/24
```

9. Guardamos los cambios en el fichero y lanzamos el snort. Pero para que no se limite a capturar paquetes, sino que aplique las reglas de detección, debemos añadir el parámetro `–c` y el path hasta el fichero de configuración:

```
# snort –i eth1 –c /etc/snort/snort.conf
```

   Veremos que la inicialización de la herramienta es mucho más larga porque está cargando las reglas y preparando el analizador.

(Continúa)

Caso práctico 5

(Continuación)

10. Ahora ya podemos ir al Ubuntu Desktop y lanzar un `nmap` sobre Ubuntu Server. El `nmap` se debe completar con normalidad (Fig. 7.32).

```
profesor@profesor-VirtualBox:~$ nmap 10.0.1.4

Starting Nmap 5.21 ( http://nmap.org ) at 2012-08-14 12:09 CEST
Nmap scan report for 10.0.1.4
Host is up (0.0025s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
profesor@profesor-VirtualBox:~$
```

Fig. 7.32. *Nos lanzan un nmap.*

11. En el Ubuntu Server nos situamos en el directorio `/var/log/snort` para comprobar si ha detectado algo. Deberíamos encontrar allí dos ficheros: uno llamado `alert` y otro `tcpdump.log.12345678`. En `alert` se almacenan los avisos de las amenazas detectadas y en el otro fichero se guardan los paquetes correspondientes (así podemos confirmar el ataque y avanzar en su solución). En nuestro caso deberemos tener una alerta de tipo `PORTSCAN` (Fig. 7.33).

```
root@ubuntu12:/var/log/snort# head alert
[**] [122:1:1] PSNG_TCP_PORTSCAN [**]
[Classification: Attempted Information Leak] [Priority: 2]
08/14-12:07:13.697361 10.0.1.3 -> 10.0.1.4
PROTO:255 TTL:64 TOS:0x0 ID:6404 IpLen:20 DgmLen:154 DF
```

Fig. 7.33. *Ataque detectado.*

12. El fichero de los paquetes capturados se puede consultar con `tcpdump -r` (Fig. 7.34).

```
root@ubuntu12:/var/log/snort# tcpdump -r tcpdump.log.1344939356
reading from file tcpdump.log.1344939356, link-type EN10MB (Ethernet)
12:17:42.924885 IP 10.0.1.3 > 10.0.1.4: ip-proto-255 132
12:17:42.956614 IP 10.0.1.3.44672 > 10.0.1.4.snmp: Flags [S], seq 1033160561, wi
n 14600, options [mss 1460,sackOK,TS val 1936486 ecr 0,nop,wscale 3], length 0
12:17:42.985540 IP 10.0.1.3.50085 > 10.0.1.4.bgpd: Flags [S], seq 2329932070, wi
n 14600, options [mss 1460,sackOK,TS val 1936493 ecr 0,nop,wscale 3], length 0
12:17:42.987102 IP 10.0.1.4.9220 > 10.0.1.3.39207: Flags [R.], seq 0, ack 241147
6010, win 0, length 0
12:17:43.022580 IP 10.0.1.3.40187 > 10.0.1.4.705: Flags [S], seq 2716909108, win
 14600, options [mss 1460,sackOK,TS val 1936502 ecr 0,nop,wscale 3], length 0
root@ubuntu12:/var/log/snort#
```

Fig. 7.34. *Paquetes del ataque.*

13. Vamos a crear nuestra propia regla. Por ejemplo, una regla que se active cuando detecte la cadena `hola` en una comunicación TCP. Las reglas están en ficheros dentro del directorio `/etc/snort/rules`. Veremos que están agrupadas por el tipo de ataque que cubren (telnet, exploit, virus, chat, etc.). Nosotros abrimos el fichero `/etc/snort/rules/local.rules`, que es donde van las reglas particulares de nuestro sistema. Introduciremos esta línea:

```
alert tcp any any -> any any (msg:"no te conozco"; content:"hola"; classtype
:shellcode-detect; sid:310; rev:1;)
```

La primera palabra define qué hará snort si un paquete cumple esta regla. Por ahora será `alert`, que se limita a mostrarlo en el fichero de log (comportamiento IDS). La segunda palabra es el protocolo del paquete. Las siguientes son la dirección y el puerto origen y destino (ponemos `any` para aceptar todos).

Después viene el paréntesis. El primer parámetro `msg` es el texto que aparecerá en la alerta. El siguiente es qué estamos buscando: en nuestro caso es la palabra `hola` dentro del paquete. Finalmente, cómo se clasifica la regla, un número de regla y la versión.

14. Guardamos el fichero y reiniciamos la herramienta. Para conseguir ese paquete con la palabra `hola` utilizaremos la herramienta netcat. En una sesión de Ubuntu Server ejecutaremos:

```
# nc -l 1234
```

Este comando se queda esperando que alguien conecte en el puerto 1234.

15. Desde Ubuntu Desktop hacemos esa conexión:

```
# nc 10.0.1.4 1234
```

16. Ahora podemos escribir cualquier palabra, que inmediatamente aparecerá en la otra sesión.

17. Si utilizamos la palabra `hola`, llega al otro lado, pero nuestro snort lo detecta y genera la alerta y el fichero de log de paquetes asociado (Fig. 7.35).

```
profesor@ubuntu12:/var/log/snort$ tail alert
[**] [1:301:1] no te conozco [**]
[Classification: Executable code was detected] [Priority: 1]
08/14-13:00:05.236713 10.0.1.3:34465 -> 10.0.1.4:1234
TCP TTL:64 TOS:0x0 ID:28270 IpLen:20 DgmLen:57 DF
***AP*** Seq: 0x25512594  Ack: 0xD9CB0995  Win: 0x721  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2572057 2782250
```

Fig. 7.35. *Cadena detectada.*

18. Podemos editar de nuevo la regla y cambiar `alert` por `reject` (la convertimos en IPS). Reiniciamos snort y, al repetir la prueba, comprobaremos que el mensaje no llega a la otra ventana y que la conexión se destruye.

19. En un sistema real el snort correrá como un servicio más. Deberemos elegir cuidadosamente las reglas que están activadas para evitar caer en los problemas conocidos: rendimiento, falsos positivos, etc.

2. Firewall

Hemos visto que la tarea de los NIPS es dura: revisar todos los paquetes que transitan por la red buscando patrones de ataques conocidos. Los consiguientes problemas de rendimiento impiden que muchas empresas los utilicen. Pero si efectivamente conocemos las características del ataque (puerto donde intenta conectar, tipo de dirección IP origen inválida, tamaño del paquete utilizado), otra forma de defensa es tomar medidas en las máquinas que tengamos bajo nuestro control para que **reaccionen adecuadamente ante la presencia de estos paquetes sospechosos.** Es decir, los paquetes que consigan entrar en nuestra red, engañar al NIPS (si lo tenemos) y llegar a nuestros equipos, o que intentan salir procedentes de una aplicación no autorizada (por ejemplo, un troyano nos puede convertir en generadores de correo spam), todavía tienen que superar un control más en cada equipo: el firewall o cortafuegos.

Por ejemplo, si tenemos un servidor web en nuestra LAN y no queremos que sea atacado desde la wifi pública que ofrecemos a los clientes en la sala de espera, podemos configurar en el firewall de la máquina del servidor web que no acepte conexiones de las máquinas conectadas a esa wifi (generalmente, las identificaremos porque pertenecen una subred distinta).

2.1. Qué hace

El firewall es un software especializado que se interpone entre las aplicaciones y el software de red para hacer un **filtrado de paquetes:**

- En el tráfico entrante, la tarjeta de red recibe el paquete y lo identifica, pero antes de entregarlo a la aplicación correspondiente, pasa por el firewall para que decida si prospera o no. En el ejemplo del servidor web, la máquina recibe un paquete destinado al puerto 80, pero antes de entregarlo al proceso que tiene abierto ese puerto (un apache.exe), el firewall decide.
- En el tráfico saliente, las aplicaciones elaboran sus paquetes de datos, pero antes de entregarlo al software de red para que lo envíe, pasa por el firewall. Por ejemplo, si sospechamos que una máquina hace spam, podemos bloquear todas las conexiones salientes al puerto 25.

En las máquinas servidor, generalmente el firewall actúa sobre tráfico entrante: los servicios que ejecutan en esa máquina abren determinados puertos y queremos controlar quién se conecta a ellos. En las máquinas cliente es más sencillo: por defecto, todas las conexiones entrantes están prohibidas y todas las salientes permitidas. Esto no quiere decir que no puedan entrar paquetes, porque no habría conversaciones; pero la conversación la tiene que iniciar el equipo cliente.

La inteligencia del firewall se expresa mediante **reglas de configuración.** El administrador de la máquina puede individualmente activarlas, desactivarlas, modificarlas o añadir nuevas. Este proceso puede ser automático: algunos programas que instalan un servidor en la máquina son capaces de configurar algunos programas de firewall, sin necesitar la intervención del administrador.

Las reglas del firewall son mucho más sencillas que las reglas de un IPS y generalmente se aplican solo a las cabeceras TCP/IP de las capas 3 (red) y 4 (transporte): **el firewall básicamente mira direcciones IP y puertos,** aunque también puede reconocer conversaciones entre dos equipos y controlarlas.

No nos podemos permitir aumentar la complejidad de las reglas o mirar el contenido de cada paquete (DPI [Deep Packet Inspection]) porque los recursos de los equipos son limitados. Pero si nuestras necesidades de seguridad son superiores, existe un tipo de firewall más sofisticado, llamado **firewall de nivel de aplicación,** donde sí se entra a mirar en los datos de usuario que hay más allá de las cabeceras. Se utiliza sobre todo en protocolos web (HTTP). Por tanto, es más potente (y más lento) que el firewall normal, pero menos complejo (y más rápido) que todo un IPS.

Actividades

11. ¿Por qué hay que abrir determinados puertos en los programas P2P? ¿En qué máquinas hay que hacerlo?

12. Algunos antivirus también incluyen un firewall. ¿Qué es mejor: usar ese o buscar un producto independiente?

13. ¿Es aconsejable instalar más de un firewall en una máquina?

14. Si ponemos un firewall de red, ¿ya no necesitamos activar el firewall en los servidores? ¿Y en cada máquina de usuario?

15. La arquitectura de firewall presentada es muy completa, pero también es posible realizar distintas simplificaciones: screened subnet, screened host, dual-homed host. Investiga en qué consiste cada una.

16. Investiga para qué puede usar DPI un ISP.

2.2. Dónde situarlo

Todas las máquinas de la empresa conectadas a la red necesitan activar un firewall (elementos 4, 5, 6, 7 y 8 de la Figura 7.36). Incluso aunque no ejecuten ningún servidor: puede que el software de red del sistema operativo tenga una vulnerabilidad. Igual que el malware hay que bloquearlo con el antivirus porque es software no solicitado, el firewall nos ayuda a **bloquear paquetes de red no solicitados.**

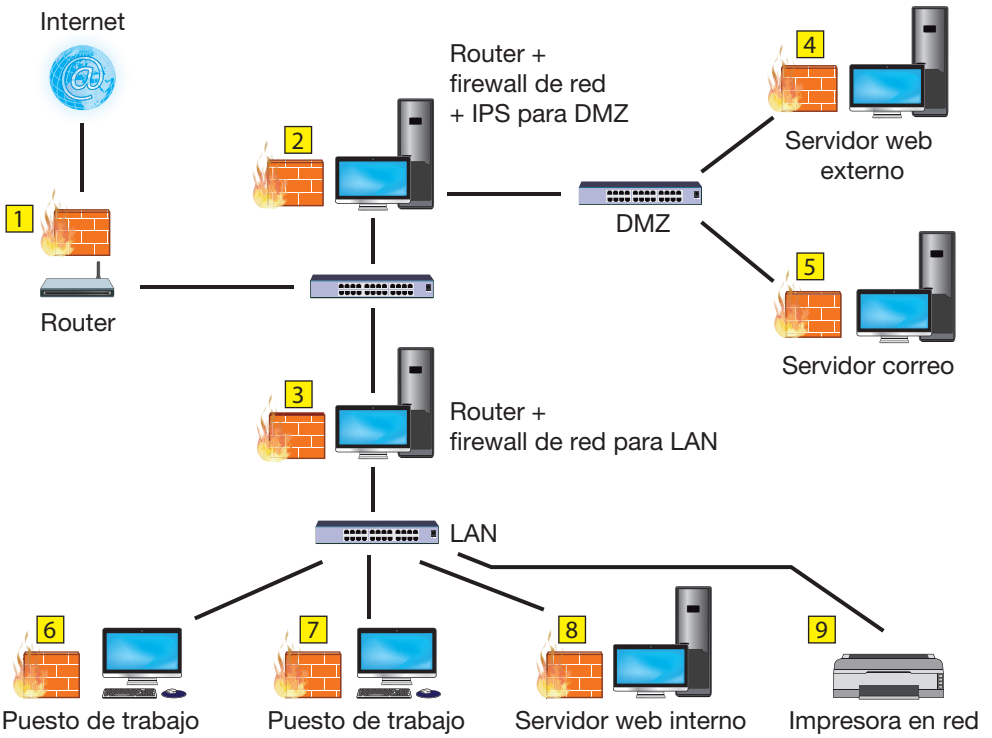


Fig. 7.36. *Despliegue completo de firewall en la empresa.*

Web

Alicia y Bernardo también saben de firewall:
http://goo.gl/gvHL2
En algunas ocasiones hay que abrir agujeros en el cortafuegos:
http://goo.gl/rMJ1h

Esta medida sería suficiente; pero, para evitar que se inunde la red con paquetes que no llegarán a su destino, o para ayudar a máquinas que no tienen firewall (por ejemplo, una impresora en red, como el elemento 9 de la Figura 7.36), en los puntos críticos de la red se suelen colocar máquinas independientes ejecutando tareas de firewall (firewall de red). Por ejemplo, siempre suele estar en la conexión a Internet porque por ahí llegarán muchos ataques.

Los routers domésticos proporcionados por los ISP (Internet Service Provider) hacen funciones de firewall (elemento 1 de la Figura 7.36), porque por defecto se comportan como equipos de usuario y no permiten conexiones entrantes; pero una empresa suele necesitar más configuraciones, por lo que instalará su propio firewall de red.

En empresas pequeñas este firewall de red seguramente ejecutará en una máquina que también hace las funciones de router; incluso puede que también aloje determinados servicios de la empresa en Internet (un servidor web o el servidor de correo). En las empresas grandes hay máquinas distintas para cada servicio, todas situadas en una subred especial llamada DMZ (Demilitarized Zone, **zona desmilitarizada**). El firewall de esta zona (elemento 2 de la Figura 7.36) es menos exigente que el que protege nuestra LAN (elemento 3 de la Figura 7.36), porque tenemos que permitir conexiones a esos servicios; pero, como está expuesto a más ataques, se suele acompañar de un IDS/IPS.

Por ejemplo, si tenemos un servidor web en la DMZ, el firewall de la DMZ debe permitir pasar el puerto 80; pero el firewall de la LAN, no. Sin embargo, conviene poner un IPS en el servidor para protegerlos de múltiples ataques HTTP que puedan venir de Internet.

2.3. Firewall en Linux. Iptables

Cuando llega un paquete a la tarjeta de red, el sistema operativo (más concretamente, el software de red) decide qué hacer con él. El resultado de esa decisión puede ser:

- **Descartarlo.** Si el destinatario del paquete no es nuestra máquina o, aunque lo sea, ningún proceso actual lo espera, el paquete termina aquí. Por ejemplo, llega una petición http a una máquina que no tiene un servidor web arrancado: la máquina lo ignora.
- **Aceptarlo,** porque es para nosotros y hay un **proceso** que sabe qué hacer con ese paquete. Sería el ejemplo anterior, pero ahora sí tenemos un servidor web funcionando.
- **Aceptarlo,** aunque no sea para nosotros, porque somos un **router** y vamos a enviarlo por otra interfaz. En algunos casos llegaremos a modificar las cabeceras del paquete, como veremos más adelante.
- **Aceptarlo,** aunque no es para nosotros y tampoco somos un router: pero estamos escuchando todos los paquetes porque somos un **sniffer** de red.

En el caso de Linux, la utilidad **iptables** permite introducir reglas en cada una de estas fases:

- Cuando llega el paquete para un proceso nuestro pero todavía no se lo hemos entregado, en iptables hablamos de **input.**
- Cuando somos un router y estamos a punto de traspasar el paquete de una interfaz a otra, en iptables hablamos de **forward.**
- Cuando un paquete está listo para salir por una interfaz, en iptables hablamos de **output.**

Hay un par de etapas más:

- **Prerouting.** Se ejecuta antes de input. Sirve para obviar el enrutamiento porque sabemos exactamente qué tratamiento dar a esos paquetes. Veremos un ejemplo en el caso práctico de proxy de esta misma unidad.
- **Postrouting** (después de output y después de forward). Se utiliza para aplicar alguna modificación a los paquetes que están a punto de abandonar la máquina. Veremos un ejemplo, el NAT, en el mismo caso práctico de proxy.

Las **reglas** de iptables tienen una **lista de condiciones** y una **acción,** de manera que, cuando un paquete cumple todas las condiciones de una regla, se ejecuta la acción. En las condiciones podemos utilizar la interfaz por la que entró, la interfaz por la que va a salir, la dirección IP o la subred del paquete, el tipo de protocolo, el puerto origen o destino, etc. Las acciones pueden ser simplemente aceptar o rechazar el paquete, o también modificarlo.

Pero no todas las acciones están disponibles en todas las situaciones. Por esto las reglas se agrupan en **tres tablas principales:**

- **filter.** Es la tabla principal. Su misión es aceptar o rechazar paquetes. Es el firewall propiamente dicho.
- **nat.** Las reglas de esta tabla permiten cambiar la dirección de origen o destino de los paquetes.
- **mangle.** En esta tabla podemos alterar varios campos de la cabecera IP, como el ToS (Type of Service). Se suele usar para aplicar QoS (Quality of Service), marcando los paquetes de determinados servicios para luego priorizarlos.

Dentro de cada tabla, las reglas se agrupan a su vez por la etapa del procesamiento de paquetes donde se aplican (prerouting, input, etc.), aunque no todas las tablas tienen todas las etapas (Figura 7.37). Para cada etapa (también llamada **chain,** porque encadena una regla con otra) hay una lista de reglas que **se recorre secuencialmente hasta que el paquete cumple una regla.** En ese momento se ejecuta la acción asociada a la regla y se deja de aplicar el resto de las reglas de esa etapa (salvo la acción LOG, como veremos más adelante). Si el paquete no cumple ninguna regla de esa etapa, se aplica la **acción por defecto de la etapa.**

¿Sabías que...?

Las reglas de iptables también permiten realizar tareas de NIDS, como reaccionar ante ataques de diccionario a un servidor SSH o detectar algunos Denial of Service.

Web

Este vídeo ilustra una configuración de iptables usando máquinas virtuales:

Primera parte:
http://goo.gl/pCQeL

Segunda parte:
http://goo.gl/uBuA4

Vocabulario

NAT (Network Address Translation). Mecanismo que aplican los routers para cambiar la dirección IP de los paquetes que transitan por ellos. El router pone su propia dirección, ocultando al destinatario que realmente el paquete no es suyo, sino que está haciendo de intermediario. Gracias al NAT, el agotamiento de direcciones IPv4 no ha bloqueado Internet.

QoS (Quality of Service). Es un tratamiento diferenciado que los equipos de la red aplican a los paquetes de datos que procesan, buscando favorecer unos servicios concretos, aunque otros servicios se vean perjudicados. Por ejemplo, VoIP (Voz IP) frente a navegación web.

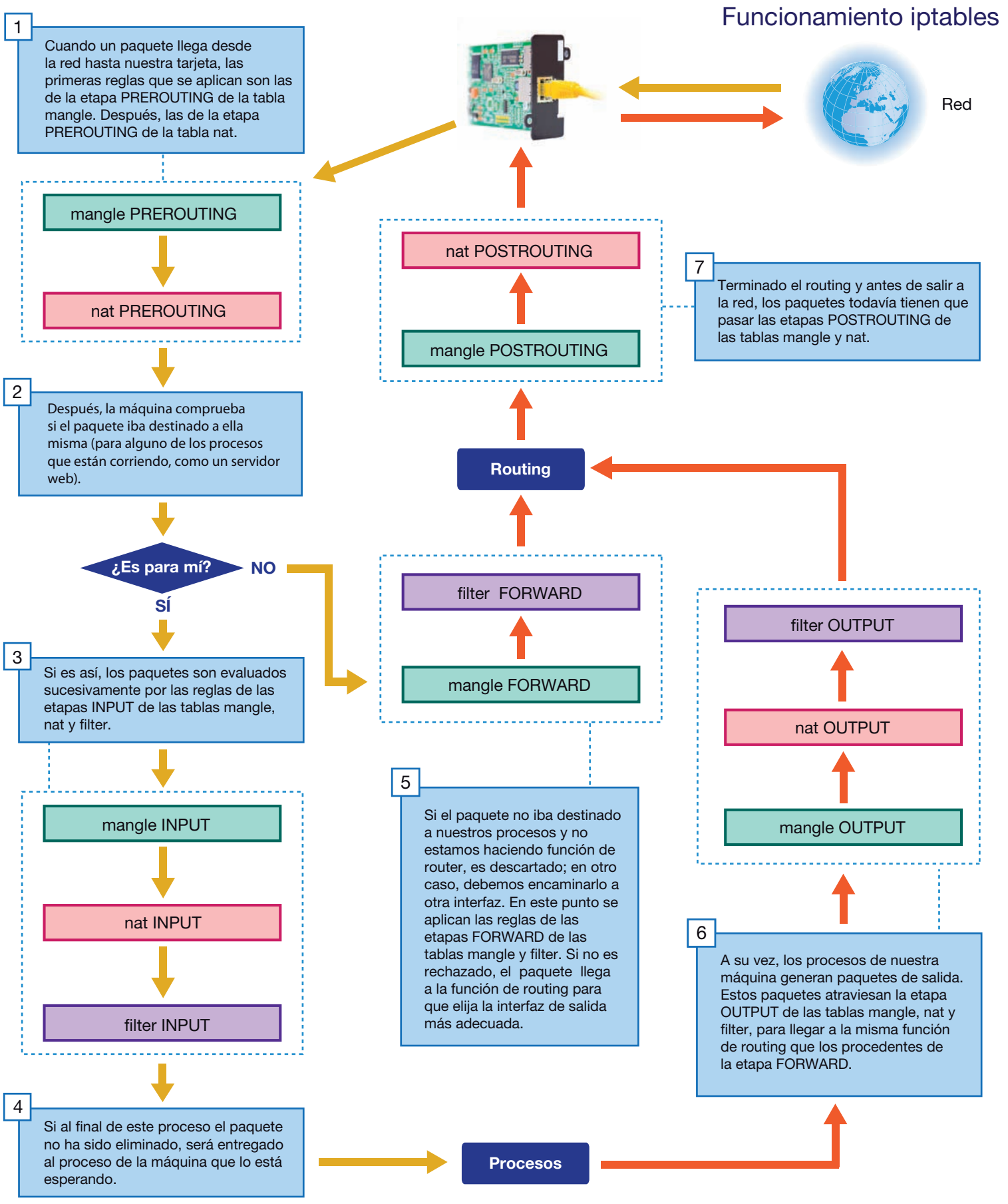


Fig. 7.37. *Esquema iptables.*

Caso práctico 6

Configuración de iptables

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

Objetivo. Configurar el firewall de un router Linux.

Material. Tres ordenadores, uno con Linux Ubuntu.

1. Utilizaremos el mismo esquema de red del caso práctico 1. En concreto nos quedamos con el router Linux, el Windows 7 y el Ubuntu Server.

2. En el router Linux elevamos privilegios para comprobar el estado de las tablas de reglas. El comando es:

   ```
   # iptables -t tabla -L
   ```

   Donde `tabla` es filter, nat o mangle. Si no indicamos la tabla, se muestra la tabla filter (Fig. 7.38). En cada etapa aparece `policy` y la operación por defecto. Lo normal es aceptar siempre.

```
root@alumno-Latitude-D520:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@alumno-Latitude-D520:~#
```

Fig. 7.38. *Tabla filter vacía.*

3. Si la tabla no está vacía, la vaciamos con:

   ```
   # iptables -t tabla -F
   ```

4. Ahora nos vamos al Windows 7 y probamos un `ping` al router Linux. Debería funcionar con normalidad (Fig. 7.39).

```
C:\Users\profesor>ping 192.168.10.1

Haciendo ping a 192.168.10.1 con 32 bytes de datos:
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.10.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.10.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\profesor>_
```

Fig. 7.39. *Ping desde W7.*

5. Volvemos al router Linux para bloquear ese tráfico. El comando sería:

   ```
   # iptables -A INPUT -i eth0 -p icmp -j DROP
   ```

   Este comando añade una regla a la etapa `INPUT` de la tabla filter (como antes, si no ponemos nada, es para esa tabla). Los siguientes parámetros son las condiciones (vienen de la interfaz `eth0` y son del protocolo `icmp`), y finalmente la acción (serán eliminados).

   Para esta regla de esta tabla, otras acciones posibles son `ACCEPT` (paquete aceptado, que es la acción por defecto) y `REJECT` (paquete eliminado, pero avisamos al origen).

6. Una vez introducido este comando, consultamos las reglas para comprobar que está creada (Fig. 7.40).

```
root@alumno-Latitude-D520:~# iptables -A INPUT -i eth0 -p icmp -j DROP
root@alumno-Latitude-D520:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Fig. 7.40. *Regla creada.*

7. Podemos repetir el `ping` desde el Windows 7, pero ya no funciona. En el router Linux comprobaremos que la regla está cumpliendo su cometido. Para ello, borramos las reglas y añadimos de nuevo la regla anterior; pero primero añadimos una regla igual con distinta acción: `LOG` en lugar de `DROP` (Fig. 7.41).

```
root@alumno-Latitude-D520:~# iptables -F
root@alumno-Latitude-D520:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@alumno-Latitude-D520:~# iptables -A INPUT -i eth0 -p icmp -j LOG
root@alumno-Latitude-D520:~# iptables -A INPUT -i eth0 -p icmp -j DROP
root@alumno-Latitude-D520:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
LOG        icmp --  anywhere             anywhere            LOG level warning
DROP       icmp --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@alumno-Latitude-D520:~#
```

Fig. 7.41. *Activamos una regla de log.*

8. Desde el Windows 7, repetimos el intento; y en el router Linux, miramos el `/var/log/syslog` (Fig. 7.42).

```
target     prot opt source               destination
root@alumno-Latitude-D520:~# tail /var/log/syslog
Aug 10 13:47:47 alumno-Latitude-D520 snmpd[1029]: Connection from UDP: [192.168.10.3]:64698->[192.168.10
.1]
Aug 10 13:47:59  snmpd[1029]: last message repeated 18 times
Aug 10 13:47:59 alumno-Latitude-D520 snmpd[1029]: Connection from UDP: [192.168.10.3]:64699->[192.168.10
.1]
Aug 10 13:48:48  snmpd[1029]: last message repeated 18 times
Aug 10 14:17:01 alumno-Latitude-D520 CRON[15989]: (root) CMD (   cd / && run-parts --report /etc/cron.ho
urly)
Aug 10 14:28:42 alumno-Latitude-D520 kernel: [11068.202391] ip_tables: (C) 2000-2006 Netfilter Core Team
Aug 10 14:33:08 alumno-Latitude-D520 kernel: [11334.347290] IN=eth0 OUT= MAC=00:1c:23:99:d0:d6:08:00:27:
69:df:92:08:00 SRC=192.168.10.3 DST=192.168.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=2518 PROTO=ICMP TY
PE=8 CODE=0 ID=1 SEQ=884
Aug 10 14:33:12 alumno-Latitude-D520 kernel: [11338.985076] IN=eth0 OUT= MAC=00:1c:23:99:d0:d6:08:00:27:
69:df:92:08:00 SRC=192.168.10.3 DST=192.168.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=2519 PROTO=ICMP TY
PE=8 CODE=0 ID=1 SEQ=885
Aug 10 14:33:17 alumno-Latitude-D520 kernel: [11344.002219] IN=eth0 OUT= MAC=00:1c:23:99:d0:d6:08:00:27:
69:df:92:08:00 SRC=192.168.10.3 DST=192.168.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=2538 PROTO=ICMP TY
PE=8 CODE=0 ID=1 SEQ=886
Aug 10 14:33:22 alumno-Latitude-D520 kernel: [11349.019766] IN=eth0 OUT= MAC=00:1c:23:99:d0:d6:08:00:27:
69:df:92:08:00 SRC=192.168.10.3 DST=192.168.10.1 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=2545 PROTO=ICMP TY
PE=8 CODE=0 ID=1 SEQ=887
root@alumno-Latitude-D520:~#
```

Fig. 7.42. *Miramos el log.*

(Continúa)

Caso práctico 6

(Continuación)

Veremos una línea por cada paquete bloqueado. Nos aparece la fecha, quién genera el log (`kernel`), la interfaz donde se ha bloqueado (`IN=eth0`) y muchos detalles del paquete (direcciones MAC e IP, protocolo, etc.).

Si consultando el log no aparece nada sobre nuestro firewall, será que tenemos mal las condiciones de la regla o la hemos introducido en una etapa errónea o una tabla errónea.

9. Volvemos al Windows 7 para probar un `ping` al Ubuntu Server. Debería funcionar (Fig. 7.43).

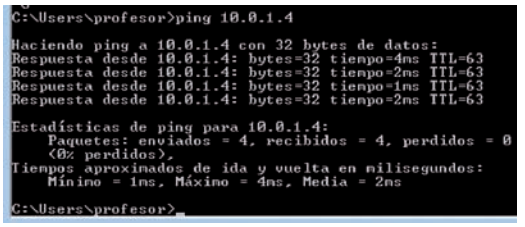


Fig. 7.43. *Ping remoto funciona.*

10. Para bloquearlo también hay que introducir la misma regla, pero ahora en la etapa `FORWARD` de la tabla filter (Fig. 7.44). Si también ponemos la regla de `log` sería:

```
# iptables -A FORWARD -i eth0 -p icmp -j LOG

# iptables -A FORWARD -i eth0 -p icmp -j DROP
```



Fig. 7.44. *Bloqueamos ping remotos.*

11. Podemos repetir el intento en Windows 7, y en el log del router Linux aparecerán los paquetes interceptados (Fig. 7.45).

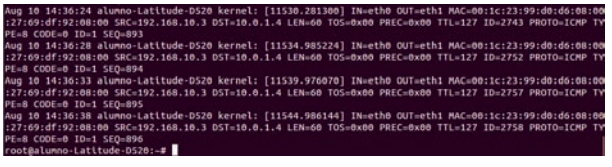


Fig. 7.45. *Comprobamos bloqueo.*

12. En el router Linux teníamos un servidor FTP. Vaciamos las reglas anteriores y vamos a introducir una regla que impida que se conecte a él la máquina Windows 7 (Fig. 7.46):

```
# iptables -A INPUT -i eth0 -p tcp --dport 21 -j LOG

# iptables -A INPUT -i eth0 -p tcp --dport 21 -j DROP
```

La condición de la regla sigue incluyendo la interfaz por donde llega el paquete, pero ahora el protocolo es `tcp` y el puerto de destino es el 21, que es el valor por defecto para los comandos FTP.

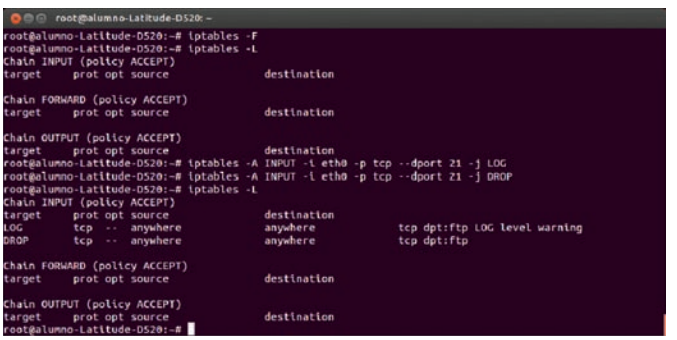


Fig. 7.46. *Bloqueo FTP.*

13. Como hemos añadido la regla de `log` (en una instalación real debemos quitarlas porque reducen el rendimiento del firewall), podemos consultar el resultado (Fig. 7.47).

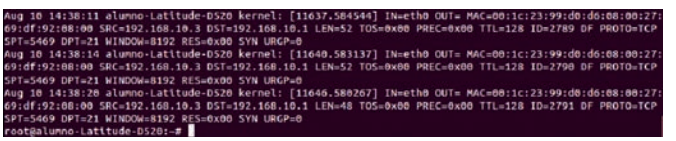


Fig. 7.47. *Comprobamos bloqueo de FTP.*

Ahora los paquetes interceptados incluyen `PROTO=TCP` y `DPT=21`, lo que habíamos indicado.

14. Como solo hemos bloqueado los paquetes que venían por la interfaz `eth0`, el FTP desde Ubuntu Server funciona (Fig. 7.48).

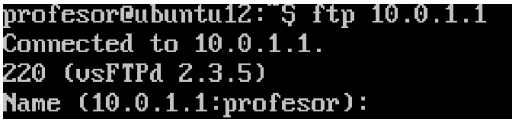


Fig. 7.48. *FTP sigue disponible en la otra red.*

2.4. Firewall en Windows 7

Los sistemas operativos Windows siempre han tenido mala fama en cuanto a seguridad ante malware; sin embargo, la versión **XP introdujo un firewall muy robusto y sencillo.** Las versiones posteriores (Vista, Windows 7) han mantenido la robustez, aunque han sacrificado la sencillez para elaborar **reglas complejas** que permitan cubrir todas las necesidades del usuario.

Comparado con iptables, el firewall de Windows 7 es más sencillo (no hay tantas tablas ni etapas) y más agradable de usar (interfaz de ventanas en lugar de comandos). A diferencia de Linux, **la configuración por defecto para las conexiones entrantes es rechazarlas, no aceptarlas.**

Caso práctico 7

Configuración de firewall en Windows 7

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

Objetivo. Configurar un firewall de usuario en Windows 7.

Material. Tres ordenadores, uno de ellos con Windows 7.

1. Seguimos con el mismo esquema de red elaborado para el caso práctico 1. Usaremos el Windows 7, el Ubuntu Server y el Ubuntu Desktop.
2. En el Windows 7 entramos como administrador y buscamos la configuración del firewall. En *Inicio* introducimos la palabra firewall y elegimos *Firewall de Windows*. Aparecerá la ventana resumen del estado del firewall (Fig. 7.49). En Windows 7, a cada conexión de red se le asigna una categoría (privada, pública o dominio). Esta categoría engloba determinadas medidas de seguridad para las conexiones de esa interfaz (abrir la visibilidad del equipo en la red, etc.). En la Figura 7.49 tenemos activado el firewall para las redes privadas y públicas, aunque la interfaz privada no esté conectada.

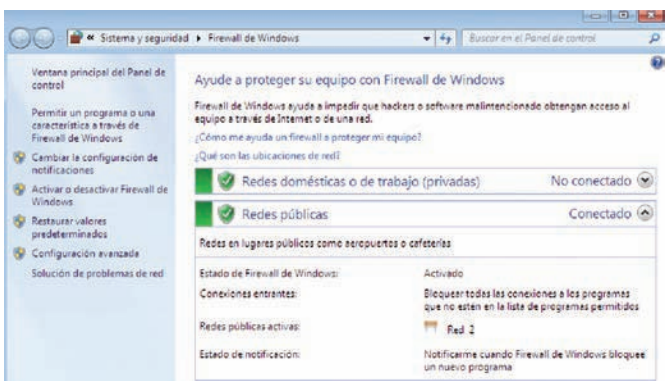


Fig. 7.49. *Estado del firewall.*

3. En la zona izquierda de la ventana tenemos distintas operaciones. Podemos activarlo o desactivarlo (solo lo desactivaremos cuando sea estrictamente necesario). La operación que nos interesa ahora es *Configuración avanzada*, porque ahí tenemos las reglas (Fig. 7.50).

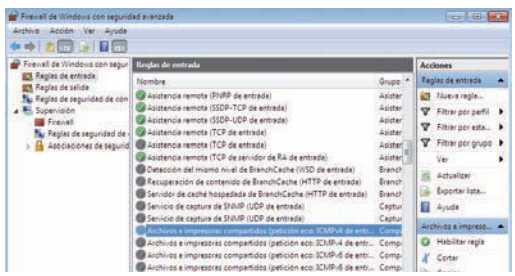


Fig. 7.50. *Configuración avanzada.*

4. Vamos a repetir el primer escenario del caso práctico de iptables. Pulsamos en *Regla de entrada* y buscamos alguna referida al ICMPv4. Las encontraremos deshabilitadas, lo que significa que nuestro equipo acepta ping. Lo podemos comprobar desde el router Linux.
5. Ahora habilitamos esa regla desde el menú del botón derecho o el menú de la derecha *Habilitar regla*. Volvemos al router Linux, repetimos el ping, pero sigue funcionando. Algo ha fallado.
6. Abrimos la configuración de la regla y parece que está bien (Fig. 7.51). La regla permite la conexión y está habilitada.

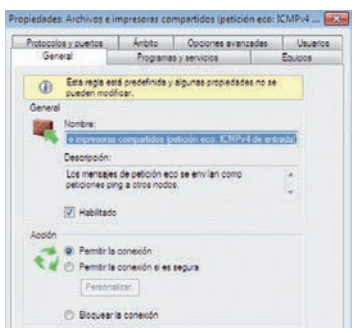


Fig. 7.51. *Configuración regla ICMPv4.*

(Continúa)

Caso práctico 7

(Continuación)

7. Si nos vamos a la pestaña *Protocolos y puertos*, la información es coherente (Fig. 7.52): protocolo ICMP y mensaje de petición de eco (echo request).

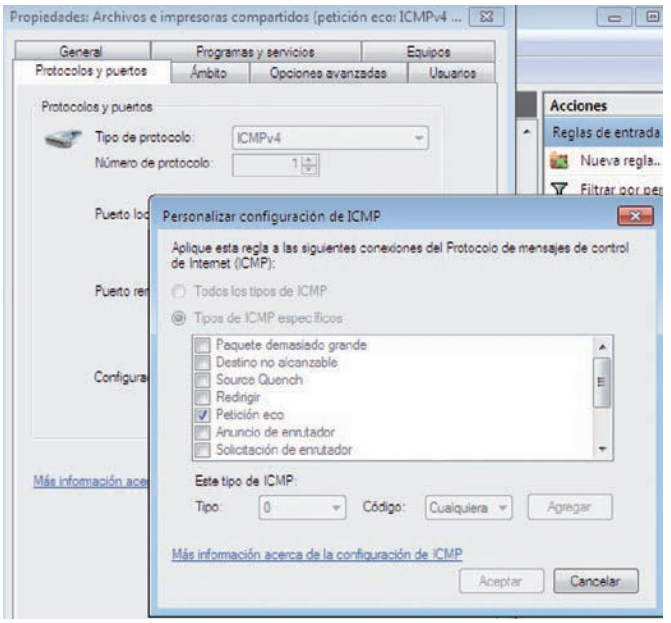


Fig. 7.52. *Configuración de protocolos.*

8. Pero si vamos a *Opciones avanzadas* encontramos el error (Fig. 7.53): esta regla está activada solo para las redes de tipo dominio, y la nuestra era privada.

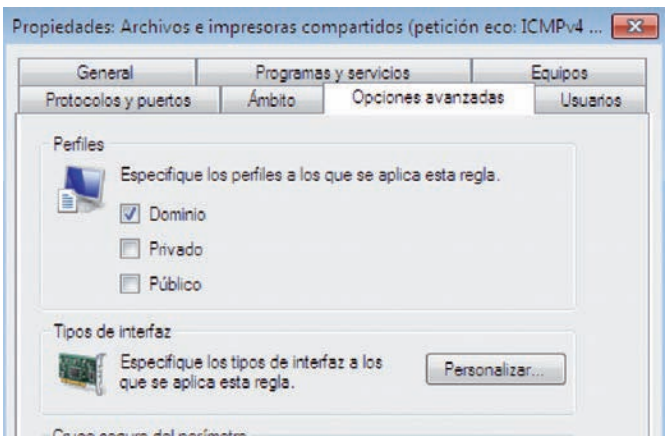


Fig. 7.53. *Configuración del perfil.*

9. Marcamos nuestro perfil, salvamos la regla y ya debería funcionar el bloqueo al ping desde el router Linux.

10. Podemos observar otras reglas, como la referida al servicio SNMP (Fig. 7.54). En el caso práctico 1 activamos este servicio para poder inventariar la máquina. La activación necesitó introducir una regla en el firewall, porque ya hemos dicho que, por defecto, el firewall de Windows rechaza las peticiones de conexiones entrantes.

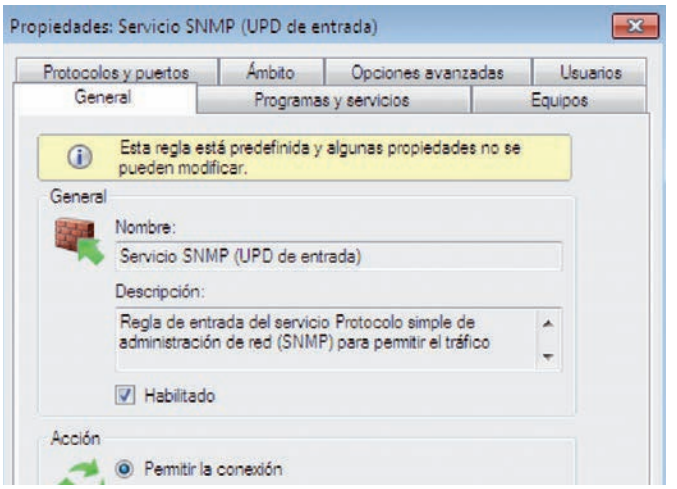


Fig. 7.54. *Regla del SNMP.*

11. En la pestaña de protocolos y puertos aparecen el protocolo UDP y el puerto 161, que son los valores estándares (Fig. 7.55).

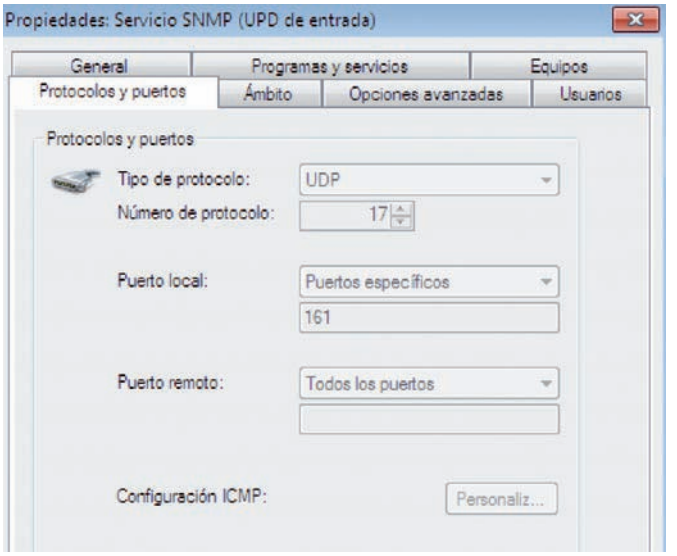


Fig. 7.55. *Configuración del protocolo SNMP.*

12. Otras aplicaciones también introducen sus propias reglas. Por ejemplo, Dropbox necesita conexiones TCP de cualquier puerto (Fig. 7.56).

(Continúa)

Caso práctico 7

(Continuación)

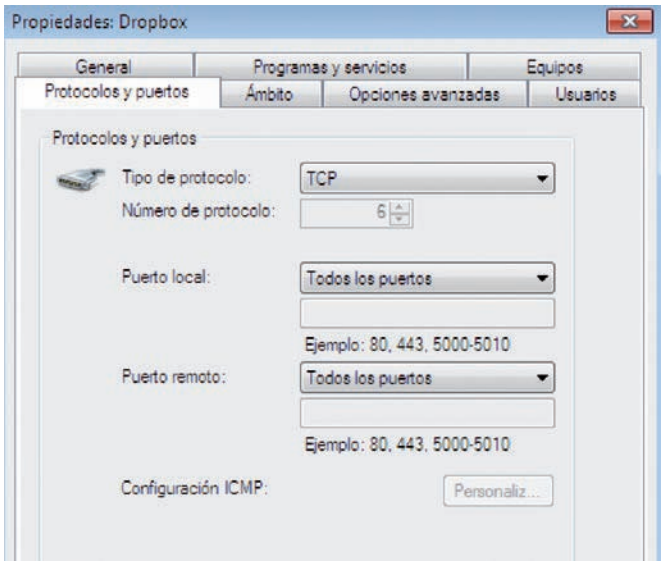


Fig. 7.56. *Regla de Dropbox.*

13. Vamos a instalar un servidor web en nuestro Windows 7. Podemos descargar el software Server2Go, que incluye un servidor web listo para usar. Lo instalamos y nos vamos al directorio donde se descomprime para invocar el ejecutable Server2Go. Si todo va bien, se abrirá un Internet Explorer con la página inicial del servidor (Fig. 7.57). Cuidado: si cerramos esa ventana del navegador, el servidor web se cierra también.



Fig. 7.57. *Servidor web instalado.*

14. Si nos fijamos en el navegador, vemos que el servidor está escuchando en el puerto 4001 de la dirección loopback (127.0.0.1). Como queremos ensayar las reglas contra conexiones desde el exterior, debemos cambiar la dirección. Para ello vamos al directorio donde arrancamos el servidor y editamos el fichero pms_config. En la parte de http ponemos HostName={local_ip} (Fig. 7.58).

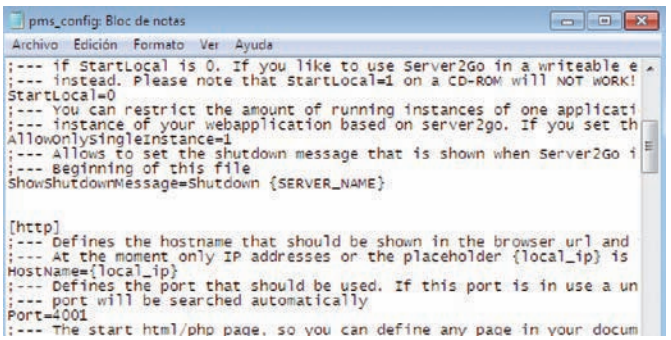


Fig. 7.58. *Cambiamos la dirección de escucha del servidor web.*

15. Cerramos el navegador para detener el servidor y lo volvemos a lanzar. Pero ahora no se abre directamente el IExplorer, sino que nos detiene una ventana del firewall (Fig. 7.59).

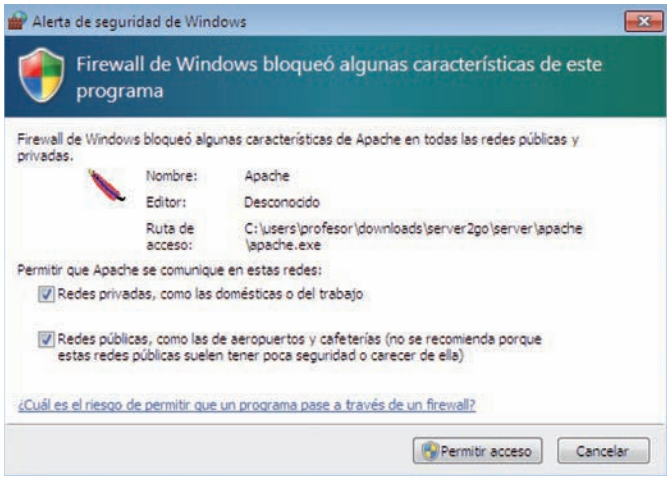


Fig. 7.59. *Bloqueo al servidor web.*

El firewall nos pregunta si debe permitir que el servidor web (en este caso, Apache) acepte conexiones en redes púbicas y privadas. Activamos ambas.

16. Ahora podemos entrar en el router Linux y comprobarlo. Abrimos Firefox e intentamos conectar con el servidor web

(Continúa)

Caso práctico 7

(Continuación)

del Windows 7. La URL será **http://192.168.10.3:4001** (Fig. 7.60).

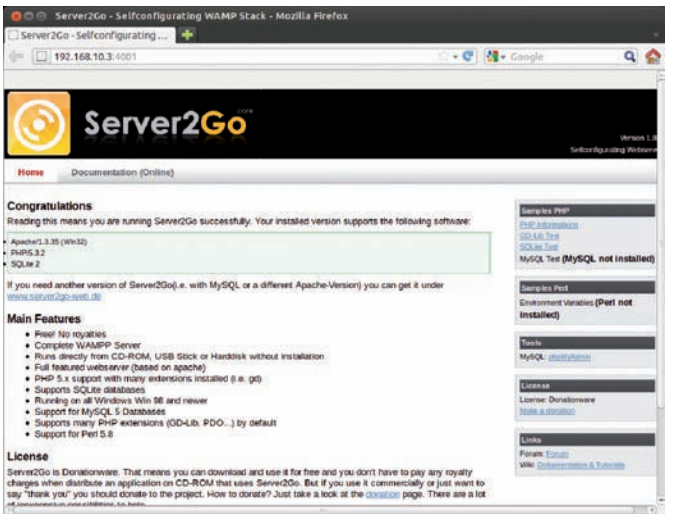


Fig. 7.60. *Conexión desde router Linux.*

17. Volvemos a la ventana de configuración avanzada del firewall de Windows 7. Podemos comprobar que han aparecido reglas nuevas, llamadas Apache (Fig. 7.61), como consecuencia de haber confirmado la consulta del paso 15.

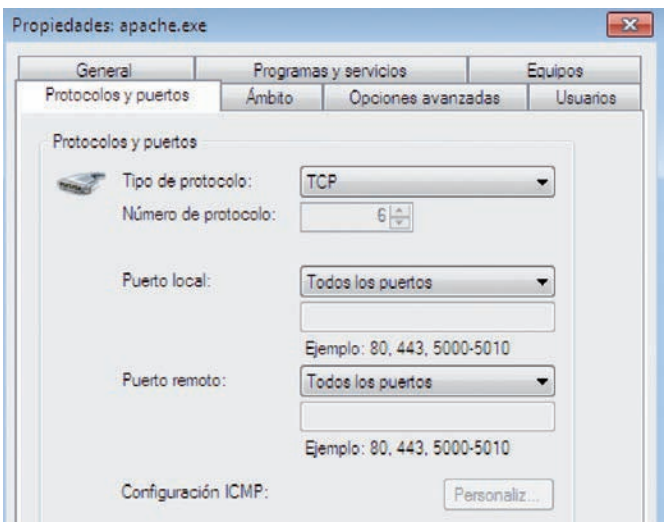


Fig. 7.61. *Nueva regla para Apache.*

18. Procedemos a cambiarla para que ya no se pueda conectar el router Linux. Vamos a la pestaña *Ámbito* y en la dirección IP remota añadimos 192.168.10.2, que es la dirección del Ubuntu Desktop (Fig. 7.62).

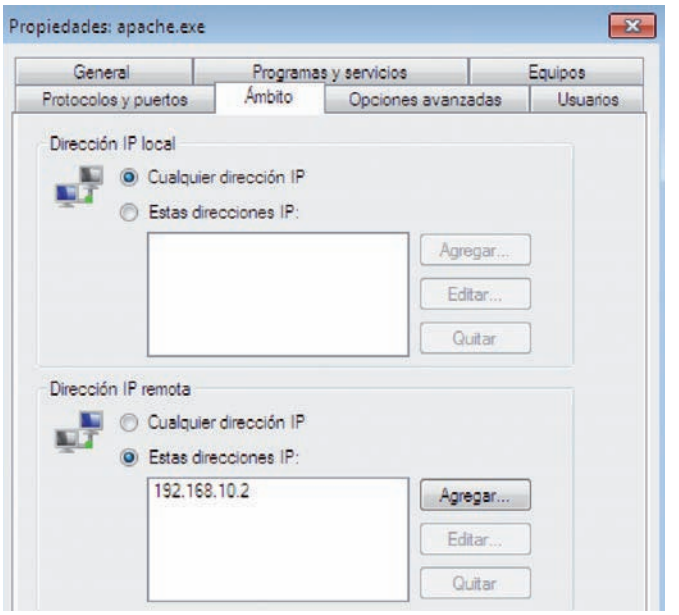


Fig. 7.62. *Cambiamos la regla.*

19. También hay que ir a *Opciones avanzadas* para activar *Permitir cruce seguro del perímetro* (Fig. 7.63).

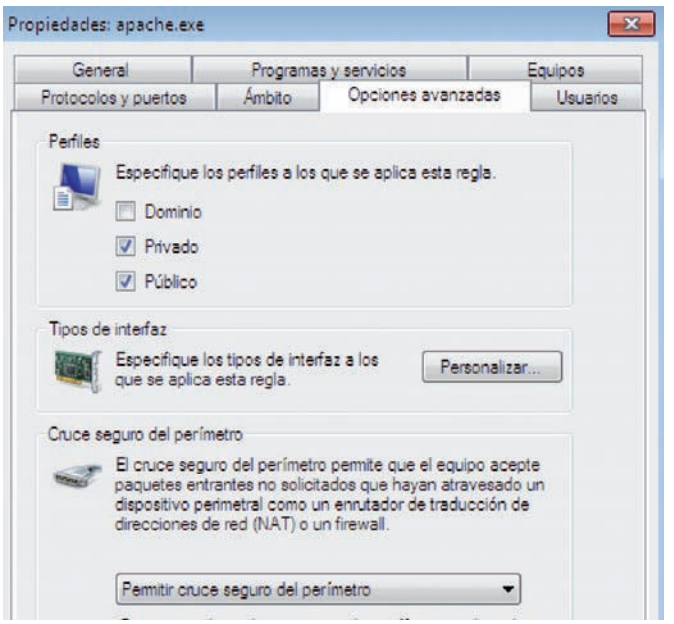


Fig. 7.63. *Configuramos el perímetro.*

20. Tras guardar los cambios, el navegador del Ubuntu Desktop entrará sin problemas; pero el navegador del router Linux, no. En la Figura 7.64 se aprecia que el navegador no consigue conectar, pero el ping sobre la misma máquina funciona con normalidad.

(Continúa)

Caso práctico 7

(Continuación)

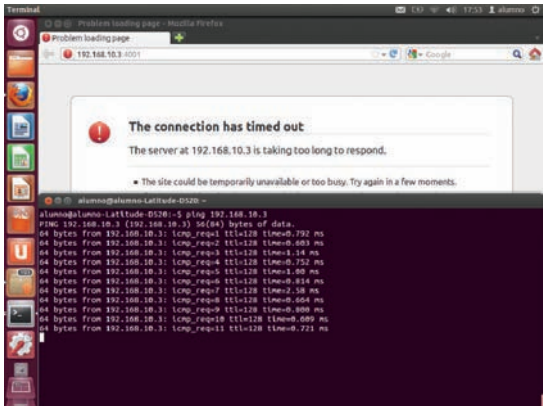


Fig. 7.64. *Acceso bloqueado.*

21. Finalmente, vamos a configurar el log del firewall, para poder confirmar que está siendo efectivo. En la ventana de las reglas pulsamos en la primera opción, la que está sobre *Reglas de entrada*. Ahí tenemos la configuración general. En el menú de la derecha pulsamos en *Propiedades*. Vamos a la pestaña de los perfiles y pulsamos en *Personalizar*. Veremos una opción llamada *Registrar paquetes descartados*, cuyo valor por defecto es *No;* lo cambiamos a *Sí* (Fig. 7.65).

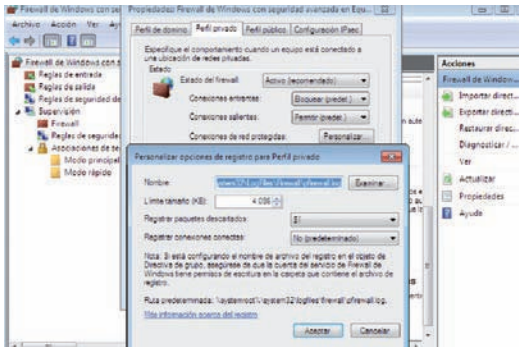


Fig. 7.65. *Propiedades del firewall.*

22. En esta misma ventana nos permite cambiar el fichero donde volcará la información. Por defecto está en el fichero pfirewall.log dentro del directorio *C:\Windows\System32\LogFiles\Firewall.*

23. Si cerramos la ventana aceptando los cambios, desde ese momento quedarán registros de todos los paquetes descartados por nuestro firewall. Podemos repetir el intento de conexión desde el router Linux. Volverá a fallar y ahora podemos confirmarlo mirando el fichero de log. Como es un fichero del sistema necesitaremos elevación de privilegios al abrir el bloc de notas (Fig. 7.66).

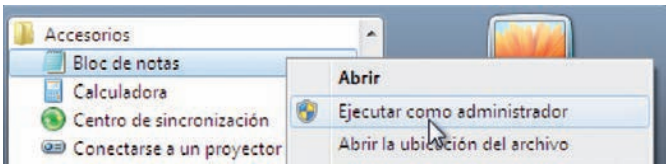


Fig. 7.66. *Bloc de notas con elevación de privilegios.*

24. En el fichero encontraremos una línea por cada paquete (Fig. 7.67). Primero viene la fecha, luego la acción (DROP, tirar el paquete), el protocolo, las direcciones IP origen y destino, etc.

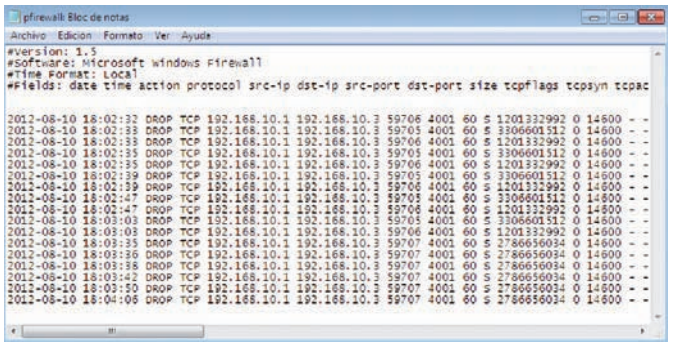


Fig. 7.67. *Lista de rechazos.*

En el paso 15 del caso práctico sobre el firewall de Windows 7 hemos visto que, cuando un programa decide abrir un puerto para recibir conexiones, la decisión por defecto del firewall es bloquear esa conexión. Efectivamente, los equipos de usuario generalmente no ejecutan servidores.

En el ejemplo hemos decidido desbloquear el acceso a nuestro Apache desde redes públicas y privadas. Si más adelante queremos cambiar este comportamiento, podemos buscar la regla en la lista de reglas y editarla; pero resulta más cómodo utilizar una opción de configuración del firewall donde aparece directamente la lista de programas de nuestra máquina y qué pueden hacer en cada red.

3. Proxy

Hemos visto que los firewall normales permiten controlar las conexiones a nivel de red (filtrado de paquetes mirando direcciones y puertos). Si necesitamos algo más, hay que recurrir a un firewall de aplicación o directamente a un IPS.

Pero hay otra forma de enfrentarse al problema de controlar qué están hablando dos máquinas entre sí. Podemos **introducir un nuevo interlocutor en medio de la conversación:** donde antes A hablaba con B, ahora hay un C, de manera que A habla con C y C se lo cuenta a B, y viceversa. Ese nuevo intermediario es un **proxy,** y como tiene acceso a todos los paquetes intercambiados, **puede aplicar medidas de seguridad.**

Un proxy es un servicio de red que hace de intermediario **en un determinado protocolo.** El proxy más habitual es el proxy HTTP: un navegador en una máquina cliente que quiere descargarse una página web de un servidor no lo hace directamente, sino que le pide a un proxy que lo haga por él. El servidor no se ve afectado porque le da igual quién consulta sus páginas.

No hay que ver siempre la seguridad como algo negativo porque nos impide navegar por algunas webs; también puede impedir que entremos en determinados sitios peligrosos donde podemos recibir un ataque. Además, en las empresas hay otros motivos para instalar un proxy:

- **Seguridad para el software del cliente.** Puede ocurrir que el software del ordenador cliente esté hecho para una versión antigua del protocolo o tenga vulnerabilidades. Pasando por un proxy actualizado evitamos estos problemas.
- **Rendimiento.** Si en una LAN varios equipos acceden a la misma página, haciendo que pasen por el proxy podemos conseguir que la conexión al servidor se haga solo la primera vez, y el resto recibe una copia de la página que ha sido almacenada por el proxy.
- **Anonimato.** En determinados países hay censura a las comunicaciones, por lo que utilizar un proxy del extranjero les permite navegar con libertad.
- **Acceso restringido.** Si en nuestra LAN no está activado el routing a Internet, sino que solo puede salir un equipo, podemos dar navegación al resto instalando un proxy en ese equipo.

3.1. Qué hace

El proxy recibe de una máquina origen A un mensaje formateado para el servidor B según un protocolo determinado (petición 1 de la Figura 7.68). Lo procesa y genera un nuevo mensaje para el mismo destino B, pero ahora el origen es P, la máquina del proxy (petición 2). Cuando el servidor B genera la respuesta, la envía a P (respuesta 3). La máquina P procesa ese mensaje y genera su propio mensaje de respuesta con destino A (respuesta 4).

Los usuarios no aprecian la diferencia porque las páginas (en el caso de un servidor web) llegan a su navegador con normalidad; pero realmente el servidor sí puede saber que el origen de la petición no es un ordenador interesado en su servicio, sino un intermediario del ordenador original. Por ejemplo, numerosos servicios de Internet que permiten consultar la IP pública que utiliza nuestro router para conectar a Internet también nos informan de si nuestra conexión está pasando por un proxy.

El procesamiento del proxy puede llevar a decidir no generar ningún mensaje. Es decir, cortar la comunicación. Este comportamiento se decide mediante **reglas.** En estas reglas podemos filtrar determinadas direcciones de origen o destino, algunas directivas del protocolo (por ejemplo, palabras dentro de la URL de una página web), incluso contenidos (por ejemplo, imágenes). Como podemos suponer, cuanto más compleja sea la regla, más tardará el proxy en aplicarla a las peticiones que le llegan, lo que puede ralentizar en exceso la comunicación.

Actividades

17. Diferencias entre un proxy y un router.

18. Busca servidores proxy para protocolos seguros (HTTPS).

19. Prueba algún servidor proxy web.

20. En una red podemos conseguir que los navegadores se autoconfiguren con el proxy de la empresa. Investiga cómo se hace.

21. Discute en clase qué podría hacer un usuario para saltarse el proxy de empresa.

Además de controlar las conexiones web, el proxy mejora el rendimiento global de la navegación porque guarda en disco las páginas que envía a los clientes. En nuestro ejemplo sería la respuesta 4 de la Figura 7.68. Es el llamado **proxy caché.** De esta manera, si esa misma máquina o cualquier otra solicita al proxy la misma página (le envía la misma **petición** 1), no hace falta generar la petición 2 ni esperar la respuesta 3: directamente, el proxy le devuelve la respuesta 4. Hemos ahorrado los dos mensajes que van sobre la red más lenta.

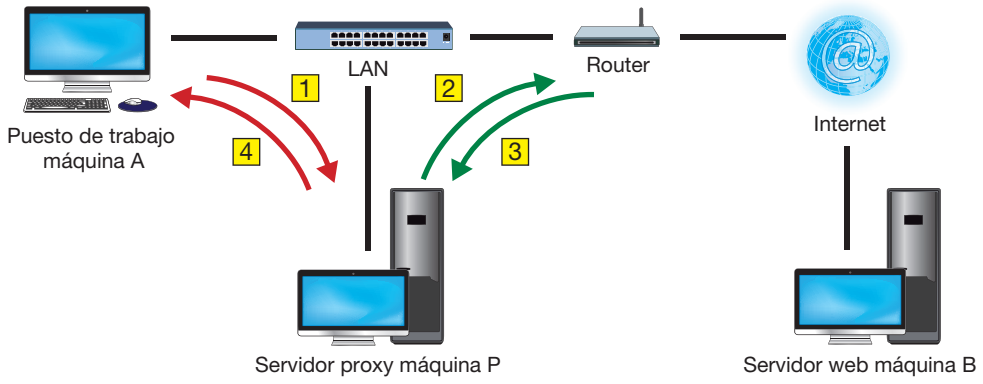


Fig. 7.68. *Funcionamiento de un proxy HTTP.*

3.2. Dónde situarlo

Si el volumen de tráfico que pasará por el proxy es reducido y las reglas definidas son sencillas, el servidor proxy necesitará pocos recursos (CPU, RAM, disco para la caché), por lo cual puede estar incluido en una máquina que ya ofrezca otros servicios (DHCP, DNS, disco en red, correo).

Si el volumen es elevado o las reglas que hemos definido son complejas, no podemos permitirnos afectar a otros servicios: necesitaremos una máquina en exclusividad (incluso más de una, formando un **clúster**). Aunque habrá que dimensionar adecuadamente el ancho de banda en esas máquinas dedicadas, porque van a recibir mucho tráfico.

En cualquier caso, el servidor proxy debe tener la mejor conectividad posible con los servidores para los que hace de intermediario (generalmente, servidores web en Internet).

Web

Aquí tenéis un tutorial para configurar Squid desde Webmin:
http://goo.gl/e6M8H

3.3. Tipos de proxy

Si instalamos un proxy para un determinado protocolo (por ejemplo, HTTP), el siguiente paso es conseguir que el tráfico de nuestros usuarios pase por ese proxy. Tenemos dos opciones:

- **Proxy explícito.** Configuramos los navegadores de los usuarios para que utilicen el proxy de la empresa.
- **Proxy transparente.** En algún punto de la red un router filtrará ese tipo de tráfico (por ejemplo, comprobando que el destino es el puerto 80 de TCP) y lo enviará al proxy, sin que el usuario tenga que hacer nada. Si estamos utilizando un router Linux, la solución óptima es instalarlo ahí, porque ahorramos sacar el tráfico hasta otra máquina.

Una tercera opción de navegación proxy al alcance de los usuarios es utilizar un **proxy web.** Esto es, una página web donde entramos para introducir la URL de la página web que realmente queremos visitar. El servidor del proxy web conecta con esa página y nos muestra el resultado. Este mecanismo es el más utilizado para evitar la censura en algunos países. En una empresa no es aceptable porque el tráfico de nuestros empleados está pasando por la máquina de una empresa desconocida y no sabemos qué puede hacer con esos datos.

En el caso del proxy explícito podemos incluir un mecanismo de **autenticación,** de manera que solo algunos usuarios puedan acceder a Internet y solo a algunas web. En un proxy transparente no tiene sentido porque el usuario no tiene ninguna opción de introducir usuario y contraseña.

3.4. Proxy Squid: configuración y monitorización

El software de servidor proxy más extendido es Squid. Tiene versión para Windows, pero aquí veremos la versión Linux, que es la más utilizada. Vamos a aprender cómo se instala, cómo se configura y cómo se comprueba que está procesando tráfico.

Caso práctico 8

Servidor proxy Squid

■ **Duración**: ◷ 60 minutos ■ **Dificultad**: ☹ Alta

Objetivo. Configurar un servidor proxy Squid, tanto en modo explícito como transparente.

Material. Tres ordenadores (uno con Linux Ubuntu), conexión a Internet.

1. Seguimos con el esquema de red del caso práctico 1. En este caso usaremos el Windows 7 y el router Linux, donde activaremos la interfaz wifi para la conexión a Internet. El tercer ordenador será un Windows en lugar del Ubuntu Desktop.

2. Configuramos el ordenador con Windows 7 para que utilice el router Linux para conectar a Internet (Fig. 7.69).

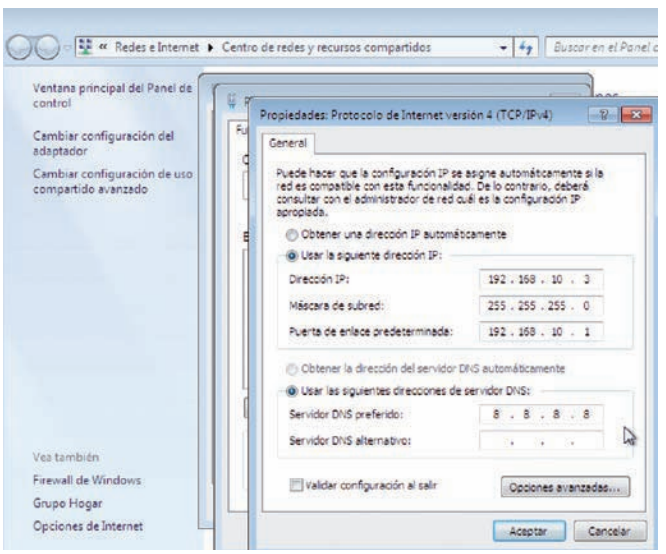


Fig. 7.69. *Configuración del W7.*

3. En el router, además de activar el traspaso de paquetes entre interfaces (ip_forward), debemos hacer NAT (Network Address Translation) para aprovechar la misma dirección de la interfaz wifi (los paquetes enviados por el Windows 7 tienen que saber volver). El NAT se configura mediante una regla de `iptables` sobre la tabla `nat`, que permite modificar la IP de origen, como hemos visto anteriormente en esta misma unidad. Utilizaremos la acción `MASQUERADE`, aunque si tuviéramos varias interfaces es mejor `SNAT`. El comando sería (Fig. 7.70):

```
# iptables -t nat -A POSTROUTING -o wlan0
-j MASQUERADE
```

```
root@alumno-Latitude-D520:~# iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
root@alumno-Latitude-D520:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
root@alumno-Latitude-D520:~#
```

Fig. 7.70. *Configuramos NAT en el router Linux.*

4. En el router Linux instalamos el software del servidor proxy mediante `apt-get install squid3`. Comprobamos que está funcionando mirando los puertos abiertos con `netstat -apn`. Comprobamos que utiliza el puerto 3128 (Fig. 7.71).

```
Seleccionando paquete squid3 previamente no seleccionado
Desempaquetando squid3 (de .../squid3_3.1.19-1ubuntu3.12.04.1_i386.deb) ...
Procesando disparadores para ureadahead ...
ureadahead will be reprofiled on next reboot
Procesando disparadores para ufw ...
Procesando disparadores para man-db ...
Configurando squid-langpack (20111114-1) ...
Configurando squid3-common (3.1.19-1ubuntu3.12.04.1) ...
Configurando squid3 (3.1.19-1ubuntu3.12.04.1) ...
Creating Squid HTTP proxy 3.x spool directory structure
2012/08/10 19:03:42| Creating Swap Directories
squid3 start/running, process 17098
root@alumno-Latitude-D520:~# netstat -apn | grep squid
tcp6       0      0 :::3128                 :::*                    ESCUCHAR    17098/squid3
udp        0      0 0.0.0.0:54235           0.0.0.0:*                           17098/squid3
udp6       0      0 :::35558                :::*                                17098/squid3
```

Fig. 7.71. *Instalamos el servidor proxy.*

5. Vamos al Windows 7 y cambiamos la configuración del navegador para que ahora pase por el nuevo proxy (proxy explícito). En cada navegador se hace en un sitio

(Continúa)

Caso práctico 8

(Continuación)

diferente. Por ejemplo, en Chrome nos lleva hasta la configuración de Internet en el sistema operativo. Entraremos en la pestaña *Conexiones* y pulsaremos el botón *Configuración de LAN*. En la ventana que aparece rellenaremos la información de proxy con nuestros valores: dirección 192.168.10.1 y puerto 3128 (Fig. 7.72).

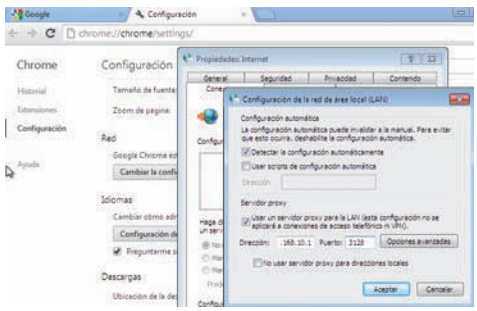


Fig. 7.72. *Proxy explícito.*

6. Guardamos los cambios e intentamos entrar en cualquier página de Internet. Debería aparecer una página de error informando de que no tenemos acceso (Fig. 7.73).



Fig. 7.73. *No tenemos acceso.*

7. Para estar seguros de que ese mensaje viene de nuestro proxy y no de otro que pueda existir más allá de nuestro router Linux, vamos a cambiar el mensaje de error. En el router nos vamos al directorio `/usr/share/squid3/errors/es` (hay un directorio por cada idioma) y buscamos el fichero ERR_ACCESS_DENIED. Lo editamos con cuidado porque es un HTML. Por ejemplo, cambiamos el mensaje principal ERROR por otro. Guardamos los cambios y volvemos al Windows 7 para repetir la conexión. Debería aparecer el nuevo mensaje (Fig. 7.74).

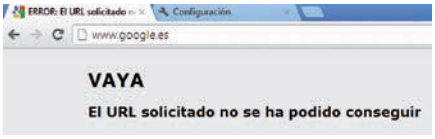


Fig. 7.74. *Nuevo mensaje.*

8. Por tanto, las peticiones del navegador de la máquina Windows 7 sí están pasando por el proxy. Podemos confirmarlo mirando el log del proxy, que está en el directorio `/var/log/squid3`. Hay varios ficheros: un `access.log` con las peticiones y un `cache.log` con información sobre la ocupación de la caché (que era la otra aportación del proxy, no solo la censura). La caché está en el directorio `/var/spool/squid3`, por lo que debemos vigilar la ocupación de ese disco.

En el `access.log` veremos una línea por cada petición (Fig. 7.75).



Fig. 7.75. *Log del Squid.*

La primera columna es el instante en que se registra la petición, la IP que lo solicita y el resultado. Vemos un `TCP _ DENIED`, que significa que hemos rechazado esa petición. Después van los detalles de la petición (URL, MIME, etc.).

9. Por tanto, ha sido el propio Squid quien ha rechazado la petición. Para conocer la causa entramos en el fichero de configuración. Está en `/etc/squid3` y se llama squid.conf. Es un fichero muy largo, con muchas opciones. A nosotros nos interesan las líneas que están bajo `INSERT YOUR OWN RULES`, a partir de la línea número 840. Veremos las reglas:

```
http _ access allow localhost
http _ access deny all
```

Esto significa que permitimos (`allow`) conexiones HTTP (`http _ access`) originadas en nuestra máquina (`localhost`), y las negamos (`deny`) al resto de las direcciones. Intercalamos una regla con `allow all` para que el comportamiento sea el contrario (Fig. 7.76). Aunque debajo siga `deny all`, las reglas se evalúan de manera secuencial, por lo que nunca llegará hasta esa.

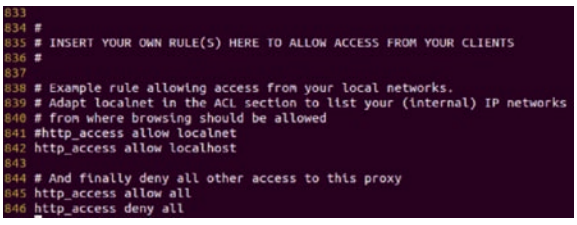


Fig. 7.76. *Cambiamos el comportamiento por defecto.*

(Continúa)

Caso práctico 8

(Continuación)

10. Guardamos los cambios en el fichero y avisamos al servidor mediante el comando:

```
# service squid3 reload
```

Ya deberíamos poder navegar desde el Windows 7 sin problemas.

11. Ahora vamos a conectar el segundo ordenador cliente y configuramos su navegador para que utilice nuestro proxy. En la Figura 7.77 se ha utilizado un Firefox. Guardamos los cambios y deberíamos navegar con normalidad. En el log del Squid veremos las peticiones de los dos navegadores.

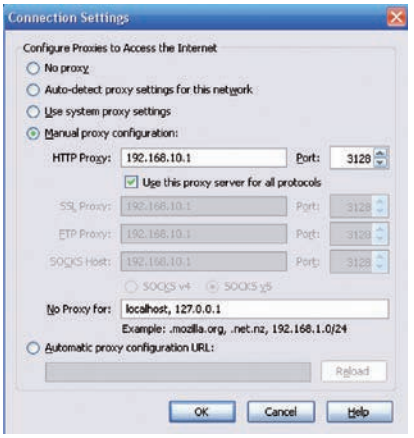


Fig. 7.77. *Configuración en Firefox.*

12. Vamos a configurar en Squid que solo lo pueda usar la máquina del Windows 7 y solo tendrá acceso a una lista reducida de webs. Para especificar estas condiciones Squid utiliza las ACL (Access Control List, listas de control de acceso). Una ACL se compone de la palabra `acl`, un nombre para la ACL y después la condición que representa. En nuestro caso utilizaremos dos (Fig. 7.78):

```
acl w7 src 192.168.10.3/32
acl fiables url_regex -i "/etc/squid/fiables"
```

La primera ACL se llama `w7` y controla que la dirección origen (`src`) sea la de nuestra máquina Windows 7.

La segunda ACL se llama `fiables` y controla que la URL que pasa por el proxy (`url_regex`) contenga alguna de las palabras del fichero `/etc/squid/fiables`. En este fichero pondremos una palabra en cada línea. Por ejemplo:

```
# cat /etc/squid/fiables
google
elpais
```

Cambiamos la regla anterior `http_access allow all` por `http_access allow w7 fiables`, nuestras nuevas ACL. Por supuesto, las ACL deben aparecer antes de la regla, porque tiene que saber qué significa cada ACL (de hecho, `all` es una ACL más).

```
acl w7 src 192.168.10.3/32
acl fiables url_regex -i "/etc/squid3/fiables"
http_access allow w7 fiables
http_access deny all
```

Fig. 7.78. *Nueva configuración.*

13. Guardamos los cambios, avisamos al proxy y comprobamos el efecto. Ahora solo deja pasar las peticiones de la máquina Windows 7 y solo para la URL de ese fichero (Fig. 7.79).



Fig. 7.79. *Acceso limitado.*

Las peticiones del Firefox son bloqueadas, aunque sean para una web de la lista autorizada.

14. Ahora vamos a probar la autenticación en el proxy, de manera que solo pueda usarlo quien introduzca correctamente usuario y contraseña. Squid admite distintos tipos de autenticación, pero usaremos la más sencilla: un fichero con usuarios y sus claves. En el fichero squid.conf tenemos que configurar esa autenticación, crear una ACL y utilizarla en alguna regla (Fig. 7.80):

```
auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/users
auth_param basic children 5
auth_param basic realm proxy de la empresa
acl w7 src 192.168.10.3/32
acl fiables url_regex -i "/etc/squid3/fiables"
acl identificacion proxy_auth REQUIRED
http_access allow w7 fiables identificación
http_access deny all
```

(Continúa)

Caso práctico 8

(Continuación)

La primera línea `auth _ param` indica que usaremos el programa `ncsa _ auth` para comprobar que el usuario y la contraseña están en el fichero `/etc/squid3/users`.

La segunda línea es el número de instancias de ese programa que estarán activas (si tenemos muchos usuarios, habrá que subir ese parámetro para atenderles bien).

La tercera línea es el mensaje que aparecerá en la ventana que solicite el usuario y la contraseña. Así el usuario sabe que le están solicitando la autenticación del proxy, no cualquier otra.

Finalmente, creamos la acl `identificacion` y la añadimos a la regla que ya vigilaba que las peticiones vengan de la máquina Windows 7 y que están en la lista de webs autorizadas.

El orden de las ACL en la regla es importante, porque se evalúan de izquierda a derecha. Por eso ponemos la autenticación al final, para no pedir la contraseña inútilmente.

```
auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/users
auth_param basic children 5
auth_param basic realm proxy de la empresa

acl w7 src 192.168.10.3/32
acl fiables url_regex -i "/etc/squid3/fiables"
acl identificacion proxy_auth REQUIRED
http_access allow w7 fiables identificacion
http_access deny all
```

Fig. 7.80. *Reglas de autenticación.*

15. Guardamos los cambios. Ahora nos falta crear los usuarios del proxy que hemos dicho que estarán en el fichero `users`. Con este tipo de autenticación `ncsa` utilizaremos la herramienta htpasswd. Si no la tenemos, la descargamos con `apt-get install apache2-utils`. Es muy sencilla de usar. En nuestro caso:

```
# htpasswd -c /etc/squid3/users jefe
```

Esto crea el fichero de claves `/etc/squid3/users` e introduce el usuario `jefe`. El comando nos pedirá la contraseña. Si queremos añadir más usuarios hay que ejecutar el mismo comando pero sin la opción `-c`.

16. Ya podemos avisar al servidor proxy y comprobar los cambios. Volvemos al Windows 7 para intentar seguir navegando. Ahora nos pedirá autenticarnos (Fig. 7.81). Nos aparece la IP y el puerto del servidor proxy y el mensaje que pusimos. Si introducimos el valor correcto, podremos navegar como antes (con las mismas limitaciones de URL autorizadas, etc.).

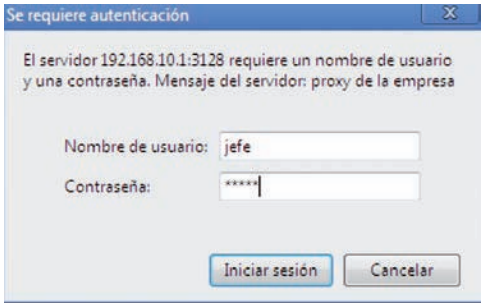


Fig. 7.81. *Autenticación.*

17. Finalmente, vamos a probar la configuración de proxy transparente. Si en los navegadores quitamos el proxy explícito, evitamos el proxy y podremos acceder a cualquier web. Para volver a tomar el control, debemos actuar sobre el tráfico que atraviesa el router. Introduciremos esta regla (Fig. 7.82):

```
# iptables -t nat -A PREROUTING -i eth0
-p tcp --dport 80 -j DNAT --to-destination
192.168.10.1:3128
```

Como ya vimos en el apartado sobre el firewall, el `iptables` permite actuar sobre los paquetes de red que llegan a la máquina. En este caso elegimos la etapa `PREROUTING` y nos fijamos en los paquetes que entran por la interfaz `eth0`, de protocolo `tcp` y destinados al puerto 80 (configuración típica de HTTP). Los paquetes que lo cumplan sufrirán la modificación del destino del paquete: ahora van directamente a nuestro proxy.

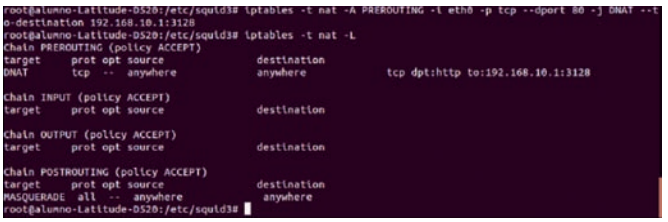


Fig. 7.82. *Desviamos tráfico al proxy.*

18. Hace falta una cosa más: en la configuración del proxy hay que avisarle de que va a llegar este tipo de tráfico. El cambio consiste en localizar en el fichero `squid.conf` la línea `http _ port` y añadir `transparent`.

```
http _ port 3128 transparent
```

Por cierto, ese número es el puerto donde escucha el servidor proxy; podemos cambiarlo por otro para no revelar a nuestros atacantes que tenemos un servidor proxy.

19. Guardamos los cambios y avisamos al servidor. Si volvemos al Windows 7, veremos que ya no podemos navegar por cualquier web, aunque podamos hacerle `ping`.

4. Spam

En las empresas, el correo electrónico es tan importante o más que el teléfono. Los empleados necesitan estar en contacto con otros empleados de la misma empresa, con los proveedores y con los clientes. Como responsables de la infraestructura informática, debemos garantizar que los mensajes se envían y reciben con normalidad, pero también que no hacemos perder el tiempo a nuestros usuarios entregando **correos no deseados (spam).** Estos correos, como mínimo, llevan publicidad, pero también son una fuente de infección de virus y troyanos que pueden venir en un fichero adjunto o que aprovechan una vulnerabilidad del programa de correo.

4.1. Qué hace

Web

El SpamAssasin también está disponible en hosting web:
http://goo.gl/37cMh

El software **antispam colabora con el servidor de correo** para detectar mensajes indeseables. Para determinar si un mensaje entra en esa categoría, el antispam utiliza:

- La **cabecera** del mensaje, buscando si el servidor de correo origen está en alguna lista negra de spammers reconocidos, si la fecha de envío utiliza un formato incorrecto (sugiere que el correo ha sido generado por un software de spam, no por un cliente de correo normal), etc.
- El **contenido** del mensaje, buscando palabras poco relacionadas con la actividad de la empresa (medicinas, etc.), mensajes cuya versión de texto plano es muy diferente de la versión HTML (sugiere de nuevo que ha sido generado con un programa de spam), etc.
- La propia **experiencia** del programa (autoaprendizaje), según el tipo de mensajes que maneja el servidor de correo de nuestra empresa en concreto.

Cuando se detecta un correo spam, tenemos varias opciones:

- Bloquearlo aquí e **impedir que llegue hasta el usuario;** así le ahorramos molestias (leerlo, borrarlo) y evitamos potenciales infecciones. No se suele usar porque nunca tendremos la certeza de que no hemos eliminado algún correo importante.
- Dejarlo pasar, pero **avisando al usuario** de que es un correo sospechoso. Es la opción por defecto. El aviso al usuario consiste en añadir texto en el título del correo (por ejemplo, *** SPAM ***); esto le servirá al usuario para crear sus propios filtros en su programa de correo.
- Dejarlo pasar, pero **convirtiendo el texto del correo en un fichero adjunto,** para que sea más difícil engañar al usuario y solo lo abra si está seguro de que el correo le interesa.

4.2. SpamAssasin: configuración y monitorización

El software SpamAssasin es uno de los más extendidos por su eficacia y la amplia variedad de filtros que puede llegar a aplicar para determinar si un correo es spam. Los filtros se especifican mediante **reglas.** Si un mensaje cumple una regla, se le asigna una **puntuación.** Cuando un mensaje supera un determinado **umbral** (por defecto, 5, aunque lo podemos cambiar), se considera que es spam.

SpamAssasin, además, utiliza técnicas de inteligencia artificial (redes neuronales) para reducir el número de falsos positivos (correo spam que no lo es) y falsos negativos (correo spam que no ha sido detectado como tal).

Actividades

22. En tu programa habitual de correo electrónico, localiza la carpeta de spam. Pídele a un compañero que te envíe un correo censurable y comprueba que llega a esa carpeta. Analiza las cabeceras de ese correo.

Caso práctico 9

SpamAssasin

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

Objetivo. Configurar y probar la detección de correos spam.

Material. Dos ordenadores con Linux Ubuntu, conexión a Internet.

1. Seguimos con el mismo esquema de red que estamos utilizando en toda la unidad. Esta vez usaremos el Ubuntu Server y Ubuntu Desktop. En ambos necesitaremos conexión a Internet para descargar los paquetes que nos falten.
2. La práctica consiste en instalar en Ubuntu Server un servidor de correo capaz de detectar spam. En la otra máquina también instalaremos un servidor de correo, para que el escenario sea similar a un caso real, donde los servidores de correo hablan entre sí.
3. Antes de entrar en detalle, la lista de cambios en Ubuntu Server será la siguiente:

   a) Instalar postfix, mailutils, SpamAssassin y spamc.

   b) Crear el usuario `spamd`.

   c) Modificar los ficheros:

   `/etc/postfix/main.cf`

   `/etc/postfix/master.cf`

   `/etc/hosts`

   `/etc/nsswitch.conf`

   `/etc/spamassassin/local.cf`

   `/etc/default/spamassassin`
4. En la máquina Ubuntu Desktop los cambios serán:

   a) Instalar postfix y mailutils.

   b) Modificar los ficheros:

   `/etc/postfix/master.cf`

   `/etc/hosts`

   `/etc/nsswitch.conf`
5. Primero instalamos el servidor de correo `postfix` en ambas máquinas:

   ```
   # apt-get install postfix
   ```
6. La configuración se realiza en varios ficheros del directorio `/etc/postfix`. Haremos varios cambios sobre la configuración normal, puesto que no seremos servidores de correo oficiales en Internet, dado que estamos en una instalación de laboratorio.
7. Primero copiamos el fichero `/usr/share/postfix/main.cf.debian` en `/etc/postfix/main.cf`. Una vez ahí, introduciremos estas líneas al final:

   ```
   lmtp _ host _ lookup = native
   smtp _ host _ lookup = native
   disable _ dns _ lookups = yes
   ```

   Así evitamos que el servidor de correo intente contactar con otros servidores en Internet. Además de cambiar este fichero, hay que modificar también el `/etc/nsswitch.conf`, de manera que los hosts solo se resuelvan en fichero:

   ```
   hosts: files
   ```

   Modificaremos estos ficheros en las dos máquinas.
8. En el fichero `/etc/postfix/main.cf` introducimos un cambio más para indicar qué direcciones atiende nuestro servidor. Vamos a suponer que el Ubuntu Server es el servidor de correo del dominio `smr.com` y `colegio.net` para el Ubuntu Desktop. Por tanto, en el main.cf de la máquina Ubuntu Server introduciremos:

   ```
   mydestination = smr.com
   ```

   Y en Ubuntu Desktop será:

   ```
   mydestination = colegio.net
   ```
9. Estos nombres necesitan una traducción a dirección IP. En el fichero `/etc/hosts` de las dos máquinas pondremos las direcciones de ambos:

   ```
   192.168.1.38 smr.com
   192.168.1.40 colegio.net
   ```
10. Podemos probar los últimos cambios haciendo un `ping` a esas direcciones (Fig. 7.83).

```
root@profesor-VirtualBox:~# ping smr.com
PING smr.com (192.168.1.38) 56(84) bytes of data.
64 bytes from smr.com (192.168.1.38): icmp_req=1 ttl=64 time=1.43 ms
64 bytes from smr.com (192.168.1.38): icmp_req=2 ttl=64 time=0.222 ms
64 bytes from smr.com (192.168.1.38): icmp_req=3 ttl=64 time=0.000 ms
```

Fig. 7.83. *Probamos conectividad.*

11. Tenemos el servidor de correo configurado en ambas máquinas. Para enviar correos utilizaremos el programa mail, que es muy simple pero suficiente para nuestros intereses. Lo instalaremos con:

    ```
    # apt-get install mailutils
    ```
12. Vamos a confirmar que nuestros servidores funcionan. Entramos en cada uno de ellos y reiniciamos el postfix:

    ```
    # /etc/init.d/postfix restart
    ```
13. En el Ubuntu Server creamos un usuario `profesor` y en el Ubuntu Desktop un usuario `alumno`. Entramos

(Continúa)

Caso práctico 9

(Continuación)

con el usuario `profesor` para enviar un correo al alumno:

```
profesor$ mail alumno@smr.com
Cc:
Subject: prueba uno
texto uno
profesor$
```

El comando `mail` lo acompañamos de la dirección de correo destino. El programa nos pregunta si queremos destinatarios en copia oculta (Cco:), el título del mensaje Subject: y después podemos escribir lo que queramos. Terminamos pulsando **Control+D.**

14. Entramos ahora en la máquina Ubuntu Desktop con el usuario `alumno` para confirmar que ha llegado el correo. Utilizaremos también el comando `mail` (Fig. 7.84).



Fig. 7.84. *Correo recibido.*

15. Hasta aquí, tenemos un servicio de correo normal. Como en Ubuntu Server queremos añadir el control de spam, hay que seguir haciendo cambios. Nos situamos en esa máquina para instalar el software especializado, en nuestro caso el SpamAssassin:

```
# apt-get install spamassasin spamc
```

Son dos programas: `spamassassin` es el detector de spam (analiza un correo aplicando las reglas que tiene configuradas) y `spamc` es una interfaz que sabe hablar con el sistema de correo (SpamAssassin se puede integrar con otros servidores estándares distintos de postfix).

16. Como cualquier servidor, conviene arrancarlo con un usuario que no tenga privilegios, para que, en caso de que sufra un ataque de tipo exploit, los comandos que lance en nuestra máquina causen el mínimo daño. En nuestro caso vamos a crear un usuario `spamd`:

```
# groupadd -g 4001 spamd
# useradd -u 4001 -g spamd -s /sbin/nologin -d /var/lib/spamassassin spamd
# mkdir /var/lib/spamassassin
# chown spamd:spamd /var/lib/spamassassin
```

17. Para la configuración del SpamAssassin utilizaremos dos ficheros. En `/etc/default/spamassassin` debemos poner:

```
ENABLED=1
SAHOME="/var/lib/spamassassin/"
OPTIONS="--create-prefs --max-children 5 --username spamd --helper-home-dir ${SAHOME} -s ${SAHOME}spam.log"
```

La primera variable activa el servidor. La segunda simplemente nos ahorra espacio en la tercera variable, que son las opciones con que arranca el servidor. Entre estas opciones está el usuario (`spamd`, que acabamos de crear) y el fichero de log `spam.log` donde podremos hacer el seguimiento del análisis de correos.

18. El segundo fichero que modificaremos será el `/etc/spamassassin/local.cf`. Introduciremos estas líneas:

```
rewrite _ header Subject *** POSIBLE SPAM ***
required _ score 2.0
```

La primera línea nos permite, cuando detectamos un spam, avisar al usuario modificando el asunto del mensaje.

La segunda línea indica cuántos puntos tiene que alcanzar la anomalía del mensaje para que la herramienta lo clasifique como spam. Por defecto son cinco, pero en este ejemplo usaremos menos.

19. Reiniciamos el servicio y miramos los procesos y puertos que utiliza (Fig. 7.85):

```
# /etc/init.d/spamassassin restart
# ps -ef | grep spamd
# netstat -apn | grep spamd
```

Veremos que hay un proceso `spamd` arrancado, que pertenece al usuario `root`, pero el resto de los procesos `spamd` ya son del usuario `spamd`. El servidor está escuchando en el puerto 783.

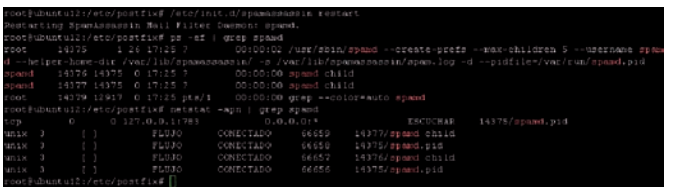


Fig. 7.85. *Servidor SpamAssassin.*

20. Esta información también está disponible en el log (Fig. 7.86).

(Continúa)

Caso práctico 9

(Continuación)



Fig. 7.86. *Log inicial del servidor.*

21. Todavía nos falta lo más importante: conectar el servidor de correo con el detector de spam. Esto se hace en el fichero `/etc/postfix/master.cf`. Hay que añadir esta línea:

```
antispam unix - n n - - pipe user=spamd null_sender= argv=/usr/bin/spamc -f -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

Esta línea le indica al postfix cómo hacer llegar los mensajes al servidor SpamAssassin. Como esperábamos, aparece el usuario `spamd` y el ejecutable `spamc`.

Solo falta modificar la línea del `smtp` para añadir al final `-o content_filter=antispam:dummy`

```
smtp inet n - - - - smtpd -o content_filter=antispam:dummy
```

Con esta línea le estamos diciendo al postfix que siga usando el `smptd` para tráfico SMTP, pero antes de enviar el correo debe pasarlo por un filtro de contenidos, nuestro antispam.

Las líneas hay que introducirlas con cuidado, respetando todos los guiones (-) (Fig. 7.87).



Fig. 7.87. *Conectamos servidores.*

22. Reiniciamos el servidor postfix para que aplique la nueva configuración. Vamos a comprobar que funciona. En el Ubuntu Desktop enviamos un nuevo correo a `alumno@smr.com`, pero esta vez utilizamos alguna palabra prohibida.

23. El correo llega a su destino, pero con nuestro aviso en el título del mensaje (Fig. 7.88).



Fig. 7.88. *Aviso de spam.*

24. Si abrimos el mensaje, podemos apreciar las cabeceras correspondientes al detector (Fig. 7.89).

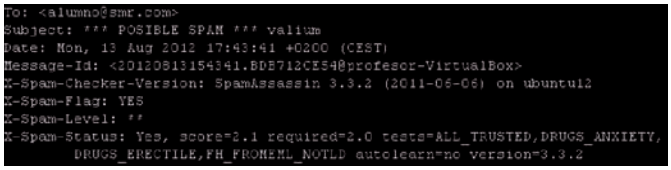


Fig. 7.89. *Cabeceras de spam detectado.*

25. El correo incorpora un aviso para el usuario (Fig. 7.90).

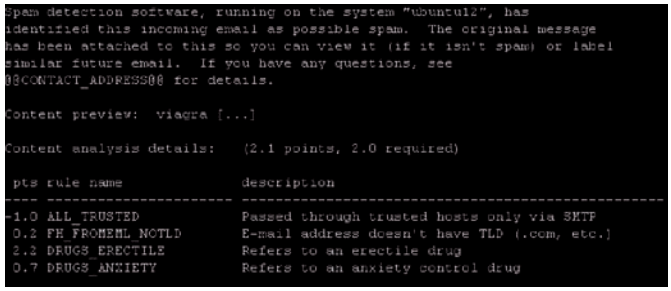


Fig. 7.90. *Mensaje para el usuario.*

26. En el log del SpamAssassin también queda registrado (Fig. 7.91).



Fig. 7.91. *Log del correo detectado.*

La primera línea informa de que le llega una conexión desde nuestro servidor de correo. La segunda línea indica qué mensaje está procesando. La tercera es el veredicto: en este caso, la puntuación es 2.1, superior al límite de 2 que hemos configurado. La cuarta es el resultado de las reglas que han saltado. La última es el estado en que queda el servidor SpamAssassin.

27. En el log del servidor de correo (por defecto, /var/log/syslog) solo aparece que el correo se envió a un filtro llamado antispam (Fig. 7.92).



Fig. 7.92. *Log del servidor de correo.*

Síntesis

Además de vigilar quién entra en nuestra red, debemos controlar para qué la utilizan.

La supervisión del tráfico necesita:

- Alto nivel (monitorización): contadores ofrecidos por los elementos. Simple, ligera y suficiente para detectar saturaciones y pérdidas de conexión.
- Bajo nivel (análisis): captura de paquetes. Compleja, pesada pero imprescindible en situaciones delicadas. Puede necesitar equipamiento adicional (hub temporal, switch gestionable para hacer port mirroring).

La herramienta tcpdump captura el tráfico de una interfaz en Linux.

- Ligera y eficiente.
- Muestra cabeceras de capa 2 y 3.
- Muestra contenido del paquete de red.
- Permite volcar a fichero para un tratamiento posterior.

La herramienta WireShark captura el tráfico y analiza protocolos en Windows.

- Compleja pero potente.
- Muestra cabeceras detalladas de todas las capas.
- Muestra el contenido del paquete.
- Múltiples opciones de filtrado.
- Capaz de analizar muchísimos protocolos de todo tipo (voz, datos, etc.).

La herramienta Snort captura el tráfico y aplica reglas para detectar ataques (NIDS [Network Intrusion Detection System]). También los puede bloquear (NIPS [Network Intrusion Prevention System]).

- Muchas reglas disponibles y actualizadas.
- Capacidad de introducir nuestras propias reglas.

El firewall evita ataques deteniendo paquetes de red no deseados.

- Hay que instalarlo en todos los equipos conectados a la red.
- También conviene controlar los puntos clave de interconexión entre redes locales y con Internet.
- Los firewall de usuario por defecto permiten cualquier conexión saliente y bloquean cualquier conexión entrante. Los routers domésticos de conexión a Internet también funcionan así.
- La inteligencia del firewall reside en sus reglas. Podemos filtrar paquetes en función de su origen, destino, proceso que lo recibe, etc.
- La DMZ es una red donde la empresa sitúa los servidores que tienen presencia en Internet. Está separada de la red local por un router + firewall y protegida de Internet por un firewall + IPS.
- El firewall en Linux se implementa sobre iptables, que permite introducir reglas en cada una de las etapas de procesamiento de los paquetes dentro de la máquina: PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING.
- Las reglas se agrupan en varias tablas (filter, nat, mangle), según el tipo de acción que ejecutarán sobre el paquete (aceptarlo, descartarlo, modificarlo).
- El firewall de Windows 7 es una herramienta muy sencilla para configurar las reglas. Podemos asignar una configuración distinta para cada ámbito de red.

El servidor proxy hace de intermediario en un protocolo. Puede ser explícito o transparente. Se instala porque buscamos:

- Más seguridad.
- Mejor rendimiento gracias a la caché.
- Anonimato.

El spam es correo no deseado. Un servidor antispam analiza el correo y aplica reglas para clasificarlo.

Test de repaso

1. En una LAN de empresa hay que vigilar los paquetes que circulan entre nuestras máquinas:

a) Nunca, si hemos garantizado la autenticación entre ellas.

b) Nunca, porque estamos invadiendo la privacidad de los empleados.

c) Solo para fines administrativos.

2. La monitorización:

a) Es suficiente para controlar todo el tráfico.

b) Es suficiente para controlar el estado de la red.

c) No sirve de nada si no la acompañamos de la captura continua del tráfico en todas las interfaces.

3. La monitorización:

a) La llevan a cabo los elementos de red, por lo que siempre estará disponible y será fiable.

b) La recogemos de los elementos de red y debemos adaptarnos a sus limitaciones (periodo de muestreo, bugs).

c) Hay que ir máquina por máquina mirando los contadores.

4. El análisis de tráfico:

a) Lo llevan a cabo los elementos de red, y nosotros nos limitamos a recoger los resultados.

b) Es difícil de activar, pero luego resulta fácil interpretar los informes del procesamiento de los paquetes capturados en la red.

c) Es costoso de activar en toda la red.

5. El análisis de tráfico:

a) Se puede hacer sobre cualquier interfaz, porque se lo solicitamos al elemento de red al que pertenece.

b) Solo se puede llevar a cabo sobre las interfaces que controlamos totalmente.

c) Necesitamos aislar la interfaz en una VLAN etiquetada.

6. La herramienta tcpdump:

a) Viene incorporada en todos los switch de red.

b) Está disponible solo para Linux.

c) Está disponible para Linux y Windows.

7. La herramienta tcpdump:

a) Solo puede ser ejecutada por un usuario con privilegios de administrador.

b) Puede ser ejecutada por cualquier usuario porque está presentado en la máquina.

c) Puede ser ejecutada por cualquier usuario con privilegios de administrador, pero el ejecutable estará en su directorio personal.

8. La herramienta WireShark:

a) Captura tráfico, pero no es capaz de analizar el protocolo al que pertenece cada paquete.

b) Analiza tráfico, pero necesita ficheros con paquetes capturados por otra herramienta como tcpdump.

c) Es capaz de capturar y analizar.

9. Los filtros de visualización de WireShark:

a) Permiten eliminar de la pantalla los paquetes que no nos interesan.

b) Permiten eliminar de la captura realizada los paquetes que no nos interesan.

c) Permite evitar la captura de los paquetes que no estamos buscando.

10. La herramienta Snort:

a) Sirve para lo mismo que tcpdump.

b) Sirve para lo mismo que WireShark.

c) No tiene nada que ver: es un IDS/IPS.

11. El firewall:

a) Captura tráfico y nos lo muestra en pantalla.

b) Detecta conexiones y evalúa mediante reglas si debe permitirlas o no.

c) Detecta conexiones no deseadas, pero solo puede avisar mediante un fichero de log.

12. En una red local de empresa:

a) Todos los equipos tienen activado el firewall y utilizan el proxy de la empresa.

b) El firewall solo está activado en los equipos servidores, porque son los importantes.

c) El firewall solo está activado en los equipos de los empleados, porque son los más utilizados.

13. Un servidor proxy en una empresa:

a) Se instala solo para mejorar la seguridad.

b) Se instala solo para vigilar a los empleados.

c) Se instala para mejorar la seguridad y el rendimiento de la conexión a Internet.

14. El servidor SpamAssassin:

a) Es un servidor de correo como postfix.

b) Es un detector de correo no deseado que complementa a postfix.

c) Es un cliente de correo capaz de detectar mensajes no deseados.

Soluciones: 1 c, 2 b, 3 b, 4 c, 5 b, 6 c, 7 a, 8 c, 9 a, 10 c, 11 b, 12 a, 13 c, 14 b.

Comprueba tu aprendizaje

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

1. En un ordenador o en una máquina virtual Linux, instala un servidor FTP.

a) En esa misma máquina, instala la herramienta Snort.

b) Descarga algún conjunto de reglas proporcionado por la comunidad de usuarios de Snort. Inclúyelo en la herramienta y comprueba que están disponibles.

c) Configura una nueva regla local para que detecte tres identificaciones erróneas del protocolo FTP.

d) Desde una segunda máquina realiza conexiones correctas y comprueba que no se genera ninguna alerta.

e) Después realiza varias conexiones erróneas hasta conseguir que aparezca la alerta.

f) Utiliza la herramienta tcpdump y WireShark para consultar los paquetes capturados para la detección del ataque.

g) Repite el ejercicio, pero esta vez Snort ejecutará en una tercera máquina, distinta a las anteriores. Tienes que conseguir acceder al tráfico para identificar el ataque.

h) Documenta todo el proceso.

Instalar y configurar cortafuegos en un equipo o servidor

2. Instala un router Linux (máquina RT) entre dos máquinas Linux o Windows (máquinas M1 y M2):

a) Instala un servidor FTP en M1.

b) Instala un servidor HTTP en M2.

c) Configura el firewall de M1 para que acepte conexiones desde M2 pero no desde RT.

d) Configura el firewall de M2 para que acepte conexiones desde RT pero no desde M1.

e) Repite el ejercicio, pero utilizando solo el firewall de RT.

f) Documenta el procedimiento llevado a cabo.

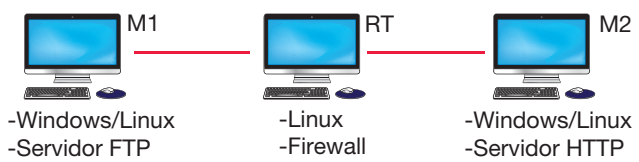


Fig. 7.93. *Esquema ejercicio 2.*

Listas de control de acceso

3. Instala un router Linux (máquina RT) entre una máquina (máquina M1) y la conexión a Internet, de manera que M1 necesite pasar por RT para salir a Internet. Comprueba que M1 puede acceder a cualquier web.

a) Configura el firewall de RT para que M1 no pueda salir a Internet por el puerto 80. Comprueba que ya no puede navegar por ninguna web, autorizada o no; aunque sigue teniendo acceso a las máquinas de esos servidores web (ping).

b) Instala un servidor proxy en RT. Configura en ese servidor proxy una ACL para que la máquina M1 solo puede acceder la web de Google y NASA.

c) Configura el navegador de M1 para que utilice el proxy de RT. Comprueba que ya puede salir a Internet pero solo navegará por esas páginas.

d) Configura en el servidor proxy una nueva regla para que ahora M1, si introduce un usuario y una contraseña adecuados, pueda navegar por cualquier página, salvo algunas páginas de periódicos deportivos.

e) Repite el ejercicio, pero utilizando un proxy transparente.

f) Documenta todos los procedimientos ejecutados.



Fig. 7.94. *Esquema ejercicio 3.*

Herramientas de protección y desinfección

4. Instala en un ordenador o máquina virtual Linux un servidor de correo (máquina M1).

a) En un segundo ordenador o máquina virtual Windows (máquina M2) instala un software cliente de correo que utilice el servidor de correo de M1.

b) En M1 instala el servidor SpamAssassin y configúralo para que interactúe con su servidor de correo.

c) En una tercera máquina M3 instala un segundo servidor de correo. Desde ese servidor envía correos a M1 cuyo contenido les haga merecedores de ser calificados como spam. Comprueba que el correo llega a M2 con tal calificación.

d) Desde M3 envía un correo que tenga adjunto un virus. Comprueba que el antivirus de M2 lo detecta al intentar abrir ese mensaje.

e) Instala en M1 la herramienta Snort y crea nuevas reglas locales que puedan detectar ambos correos peligrosos. Comprueba que funcionan.

f) Elabora una comparativa sobre las ventajas y los inconvenientes de utilizar SpamAssassin o Snort para este tipo de protección de mensajes.

g) Documenta todo el procedimiento.

Unidad 8

Ataques y contramedidas



En esta unidad aprenderemos a:

- Valorar la importancia de mantener la información segura.
- Aplicar medidas para evitar la monitorización de redes cableadas.
- Clasificar y valorar las propiedades de seguridad de los protocolos usados en redes inalámbricas.

Y estudiaremos:

- Los fraudes informáticos y robos de información.
- La seguridad en los protocolos para comunicaciones inalámbricas.
- El control de la monitorización en redes cableadas.
- La seguridad en redes inalámbricas.

Actividades

1. En la película *Un juego de inteligencia* (2007) se realizaba un ataque MITM masivo contra el sistema de medición de audiencias de televisión. ¿En qué consistía?
2. En la película *Speed* (1994) se efectuaba un ataque MITM desde el autobús. ¿En qué consistía?

1. Ataques TCP/IP. MITM

La familia de protocolos TCP/IP se diseñó a principios de los años setenta. Las limitaciones del hardware de esa época orientaron el diseño hacia la fiabilidad más que hacia la seguridad: son muy inseguros (realmente, Internet es un gigante con pies de barro).

Son especialmente peligrosos los ataques MITM (Man-In-The-Middle, intermediario): en una comunicación entre dos equipos aparece un tercero que consigue que los paquetes intercambiados pasen por él. Desde ese momento puede leer todo el tráfico (ataque de interceptación que vimos en la Unidad 1) o, lo que resulta más peligroso, alterar los datos para su beneficio (ataque de modificación).

El atacante puede interponerse en el tráfico entre origen y destino de dos maneras (Fig. 8.1):

- Por **hardware.** El atacante tiene acceso directo a un elemento de red que forma parte del camino entre el origen y el destino. Por ejemplo, el cable que conectaba el origen con su switch de planta ahora pasa por la máquina del atacante.
- Por **software** (engaño). El atacante consigue que el origen crea que él es el destino, y también consigue que el destino crea que él es el origen. Es mucho más simple que el anterior porque no hace falta tener acceso físico a los equipos.

La segunda ventaja del engaño es que es fácil activar y desactivar el ataque a voluntad. Por tanto, es más difícil detectarlo.

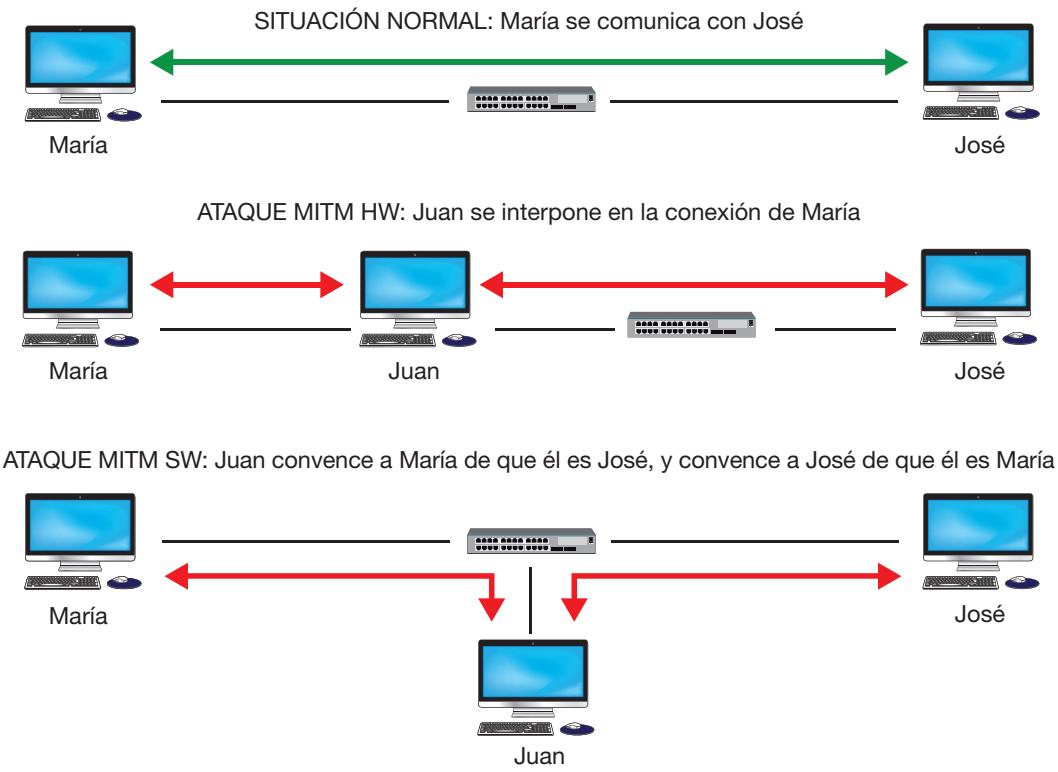


Fig. 8.1. *Tipos de ataque MITM.*

El ejemplo más típico de ataque de engaño es el **envenenamiento ARP** (ARP poisoning). El protocolo ARP (Address Resolution Protocol) se utiliza para obtener la dirección MAC asociada a una IP; es decir, cuando una máquina (llamémosle María) quiere comunicarse con otra máquina (sea José) de la que sabe su dirección IP (nivel 3 de TCP/IP), obtiene la dirección MAC (nivel 2) mediante ARP. Las llamaremos IP-José y MAC-José, respectivamente.

Para ello, María introduce en la red un paquete broadcast (que llegará a todos los equipos de la subred) preguntando la MAC que corresponde a la IP-José. En condiciones normales, solo José debería contestar con su MAC-José.

El ataque consiste en que una máquina Juan, conectada al mismo tramo de red que María y José, en un momento dado empieza a generar paquetes de respuesta ARP. Sin que nadie le pregunte, envía un paquete a María diciendo que la MAC de IP-José es MAC-Juan (la MAC de la máquina Juan), y envía otro paquete a José diciendo que la MAC de IP-María también es MAC-Juan. Es decir, intenta convencer a María de que Juan es José, e intenta convencer a José de que Juan es María.

Por desgracia, estas respuestas espontáneas son aceptadas por María y José. No hay ningún tipo de validación ni correlación con una pregunta anterior, etc.

Caso práctico 1

Ataque MITM leve

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

Objetivo. Interceptaremos las comunicaciones entre dos equipos mediante la técnica de envenenamiento ARP.

Material. Ordenador con Linux Ubuntu 12.04, ordenador con Windows, router ADSL.

1. Tenemos dos ordenadores conectados por wifi a un router ADSL que les da salida a Internet.
2. En el ordenador Linux activamos privilegios e instalamos la aplicación `ettercap`. En este ejemplo utilizaremos la interfaz gráfica, aunque está disponible en modo comando.

```
# sudo –i
# apt-get install ettercap-graphical
```

3. Arrancamos con `ettercap –G` y aparece la ventana principal. Tiene dos partes: la parte superior ofrece listas de elementos (equipos, ataques), mientras la parte inferior informa del resultado de las operaciones solicitadas.

```
# ettercap –G
```

4. Lo primero que haremos es entrar en el menú *Sniff* para elegir la interfaz donde realizaremos el ataque. En nuestro caso es la interfaz inalámbrica (Fig. 8.2).

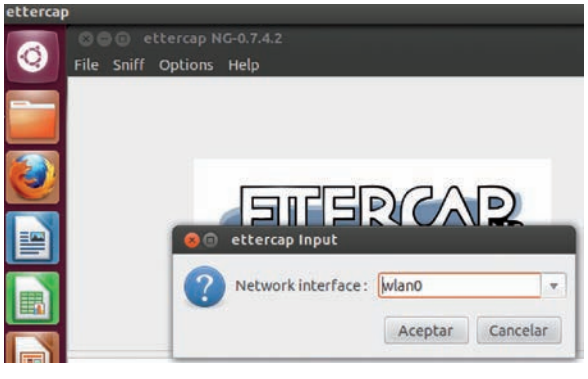


Fig. 8.2. *Elegimos la interfaz donde atacaremos.*

5. Elegida la interfaz, veremos que ahora el menú de la ventana ofrece más opciones, y en la parte de abajo se identifican la MAC y la IP de nuestra tarjeta.
6. El siguiente paso es localizar a las víctimas de nuestro ataque. Por supuesto, deben estar conectadas en este momento, para poder hacer el engaño simultáneo. Las rastrearemos en la opción *Scan for hosts* del menú *Hosts* (Fig. 8.3).

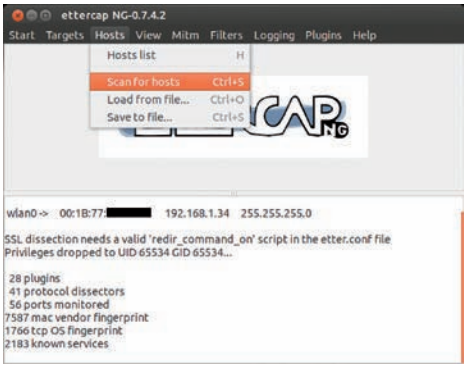


Fig. 8.3. *Buscamos víctimas.*

7. En nuestro caso solo aparecen los dos equipos del ejemplo (el nuestro no aparece, claro). Tenemos su IP y su MAC para confirmar que son ellos (Fig. 8.4). La 192.168.1.1 es el router y la 192.168.1.35 es el ordenador Windows.

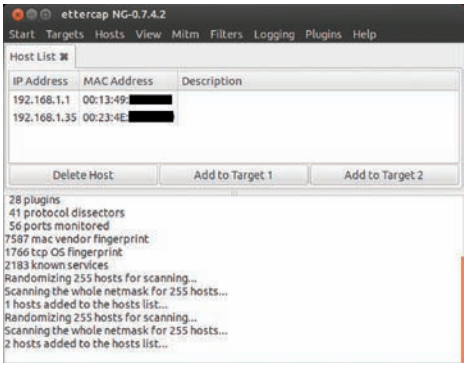


Fig. 8.4. *Encontramos dos.*

(Continúa)

Caso práctico 1

(Continuación)

Una vez identificados, los marcamos como objetivo de nuestro ataque. Seleccionamos la fila de la dirección 1.35 y pulsamos el botón *Add to Target 1*, y seleccionamos la fila de la dirección 1.1 y pulsamos *Add to Target 2*. Podemos ir al menú *Targets* para confirmarlo.

8. Ahora vamos a Windows para comparar la situación normal con la situación anormal que supone estar bajo un ataque (aunque el usuario no notará nada especial). Si abrimos una sesión de comandos, podemos consultar la tabla de traducciones actuales con el comando `arp -a`. En la Figura 8.5 podemos ver que la dirección `1.1` está asociada correctamente a la MAC que empieza por `00-13` y termina en `34`, que es la MAC del router. El ping funciona perfectamente.

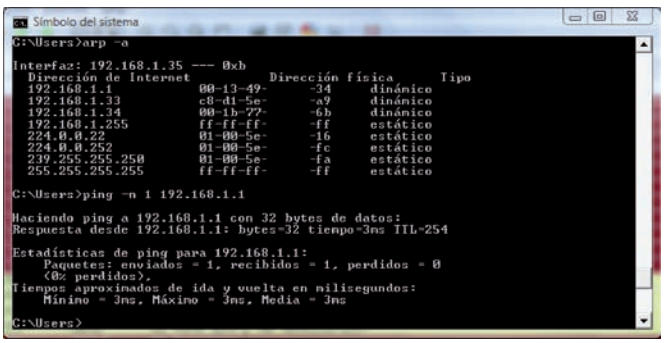


Fig. 8.5. *Situación normal.*

9. Si arrancamos el WireShark en ese equipo, podemos ver los detalles de esta comunicación normal. En la Figura 8.6 vemos cuatro paquetes: el primero es el broadcast ARP por el cual la máquina 192.168.1.35 pregunta por la MAC de la dirección 192.168.1.1. La MAC del emisor es de la marca HonHaiPr y termina en 69.

El segundo paquete es la respuesta normal. La máquina 192.168.1.1 comunica su MAC, que es de la marca ZyxelCom y termina en 34 (como ya sabíamos).

El tercer y cuarto paquete es el ping entre las dos máquinas. Como era de esperar, un paquete con origen 1.35 y destino 1.1, sale de la MAC HonHaiPr con destino la MAC ZyxelCom.

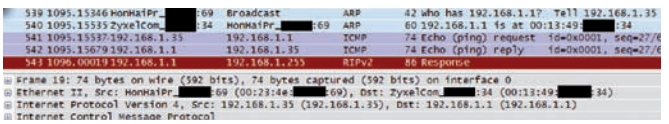


Fig. 8.6. *Captura de tráfico normal.*

10. Volvemos al Linux para activar el ataque. En el menú *Mitm* elegimos *ARP Poisoning*. En la ventana que aparece marcamos la opción *Sniff remote connections* y pulsamos *Aceptar* (Fig. 8.7).

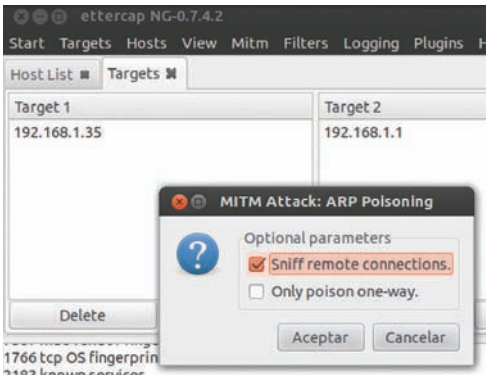


Fig. 8.7. *Activamos el ataque.*

11. La ventana nos informa de las víctimas que están siendo atacadas (Fig. 8.8). Las IP y MAC son las que esperábamos.

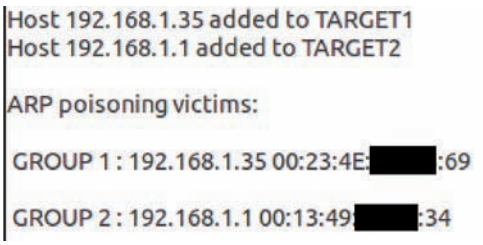


Fig. 8.8. *Ataque activado.*

12. ¿Qué está ocurriendo? Como hemos dicho, el ataque consiste en enviar falsos paquetes ARP de respuesta. En el WireShark lo podemos ver (Fig. 8.9). Cada segundo aparece un paquete ARP de la MAC IntelCor terminada en 6b (la máquina Linux) con destino la MAC HonHaiPr 2 (la máquina Windows). En ese paquete se anuncia que la MAC de la máquina con la dirección 192.168.1.1 es la 00-1b-77 terminada en 6b; pero esta es la MAC del Ubuntu, no el router.



Fig. 8.9. *Ataque en curso.*

13. Comprobamos en la máquina Windows que el engaño ha sido efectivo consultando su tabla ARP (Fig. 8.10). En efecto, la MAC de la dirección `1.1` ya no es la del router, sino la tarjeta de red de la máquina Linux.



Fig. 10. *Ataque efectivo.*

(Continúa)

Caso práctico 1

(Continuación)

14. Pero si probamos un ping a esa dirección, falla. Porque todavía falta un detalle: hemos engañado a las dos máquinas (Windows y router) para que envíen su tráfico al Linux; tenemos que hacer algo con ese tráfico. Volvemos al `ettercap` y en el menú *Start* elegimos *Start sniffing* (Fig. 8.11).

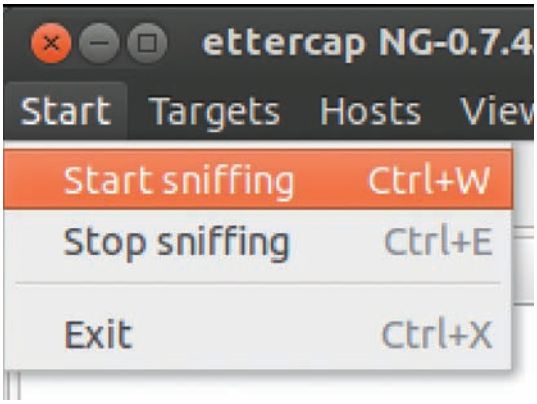


Fig. 8.11. *Activamos tráfico.*

15. Desde ese momento, la máquina Linux simula que no ha pasado nada: el tráfico que recibe de la máquina Windows lo envía el router, y viceversa. Ellos no notan nada porque creen que la MAC del Linux es la MAC correcta. El ping vuelve a funcionar. En la Figura 8.12 tenemos un paquete capturado.

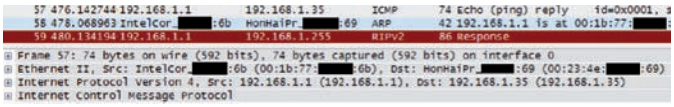


Fig. 8.12. *Engaño.*

El primer paquete es una respuesta de la máquina 1.1 a la 1.35; pero en el detalle se ve que la MAC de la 1.1 es la IntelCor Linux, no la ZyxelCom del router.

16. El engaño persiste en las comunicaciones con el exterior. Si desde la máquina Windows hacemos un ping a una dirección de Internet, el paquete llega, pero pasando primero por la máquina Linux, no por el router. En la Figura 8.13 vemos el detalle de los paquetes intercambiados. El ping con destino 74.125.230.87 utiliza la MAC de InterlCor, no ZyxelCom.

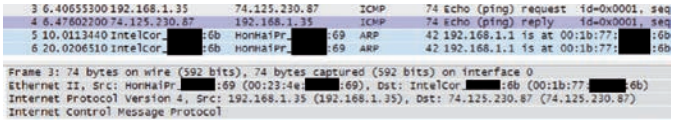


Fig. 8.13. *Falso router.*

17. Cuando terminemos la prueba debemos desactivar el ataque para que la máquina Windows y el router recuperen la normalidad. Para ello entraremos en *Mitm* y elegiremos *Stop Mitm attacks* (Fig. 8.14).

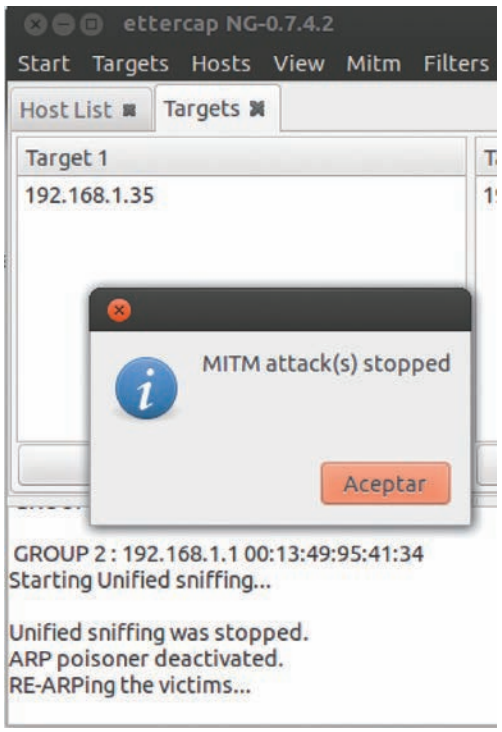


Fig. 8.14. *Detenemos el ataque.*

18. Es la propia herramienta la que se preocupa de generar los paquetes ARP necesarios para corregir la situación. En la Figura 8.15 podemos ver el contenido de la tabla ARP antes y después de parar el ataque. La dirección `192.168.1.1` vuelve a estar asociada a la `00-13`.

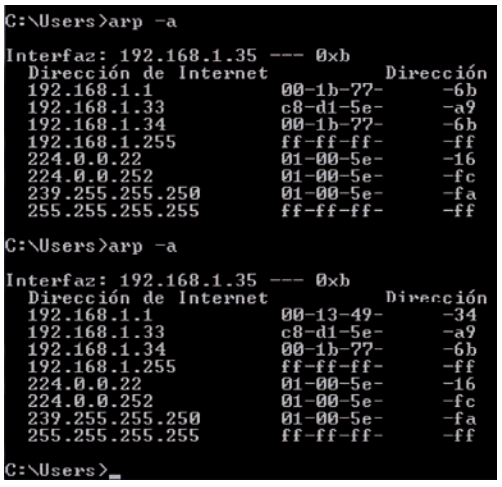


Fig. 8.15. *Normalidad recuperada.*

19. En `ettercap` podemos detener el sniffing porque no es necesario, ya que nadie nos envía tráfico.

Caso práctico 2

Ataque MITM grave

■ **Duración:** 30 minutos ■ **Dificultad:** Alta

Objetivo. Modificaremos las comunicaciones entre dos equipos mediante la técnica de envenenamiento ARP.

Material. Ordenador con Linux Ubuntu 12.04, ordenador con Windows, router ADSL.

1. Ampliamos el caso anterior: además de interceptar las comunicaciones, vamos a modificar alguna conversación. Será una petición DNS (Domain Name System): cuando la máquina Windows pregunte por un nombre concreto que tenemos configurado, la respuesta no será la oficial, sino una arbitraria que ponemos nosotros.

2. Para conseguirlo volvemos al principio. Si la herramienta ettercap está arrancada, salimos de ella (si teníamos un ataque lanzado, lo paramos). Es necesario porque vamos a cambiar la configuración de la herramienta. Editamos el fichero `/usr/share/ettercap/etter.dns` y ponemos estas dos líneas (Fig. 8.16).

```
google.com    A 192.168.1.34
*.google.com  A 192.168.1.34
```

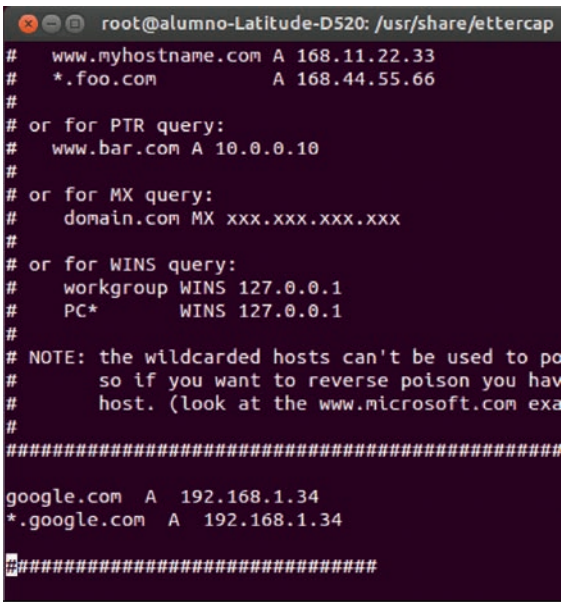


Fig. 8.16. *Respuestas DNS falsas.*

El objetivo es que, cada vez que la máquina Windows pregunte por la traducción de una dirección de **google.com**, la respuesta sea la IP de la máquina Linux.

3. Guardamos los cambios en el fichero y arrancamos la herramienta ettercap. Repetimos los pasos para completar el ataque de envenenamiento ARP.

4. Cuando ya hemos conseguido que pase por el Linux todo el tráfico entre las dos máquinas (sniffing activado), en la herramienta vamos al menú *Plugins*. En la lista que aparece buscamos dns_spoof. Hacemos doble clic para activarlo. En la parte inferior de la ventana aparecerá la confirmación (Fig. 8.17).

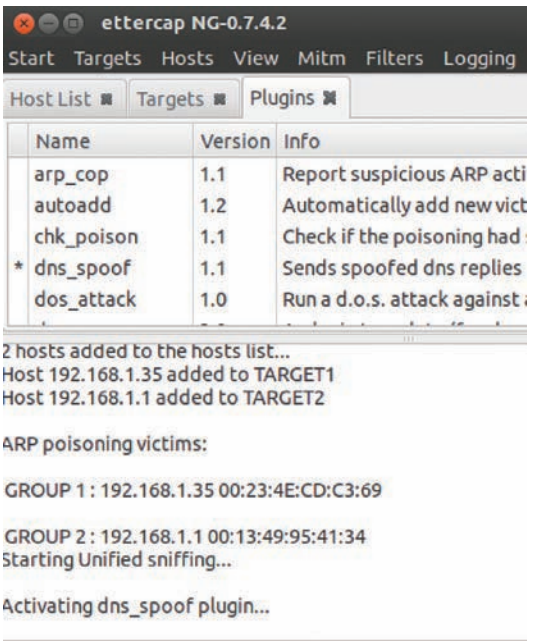


Fig. 8.17. *Activamos plugin de falso DNS.*

La lista de plugins disponibles es relativamente pequeña, pero bastante útil. Internamente, los plugins son ejecutables y la herramienta permite incluir algunos nuevos.

5. Vamos a comprobar si funciona. En Windows hacemos un `nslookup google.com`. En la Figura 8.18 se aprecia la diferencia antes y después de activar el plugin. En ambos casos, el servidor DNS responsable de la respuesta es el mismo `80.58.61.250`.

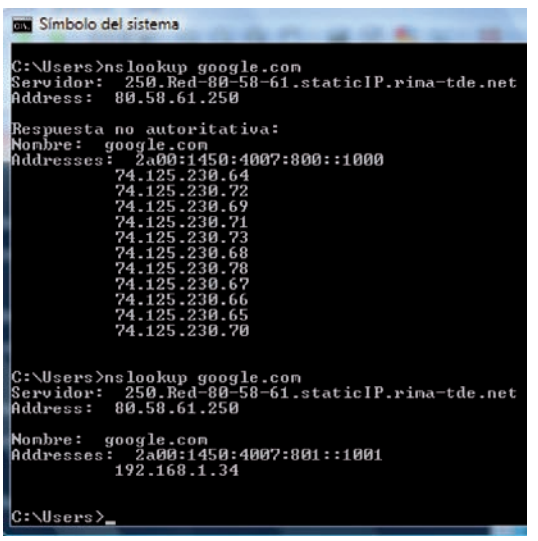


Fig. 8.18. *Respuesta falsa.*

(Continúa)

Caso práctico 2

(Continuación)

6. El engaño está conseguido. Por ejemplo, en la Figura 8.19 la máquina Windows hace un ping a **google.com**, pero nos responde el Linux.

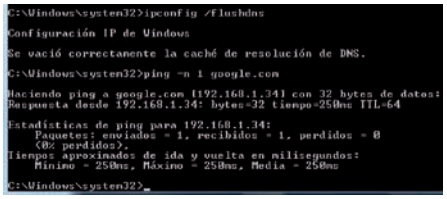


Fig. 8.19. *Ping a la máquina falsa.*

7. Si ese ejemplo no funciona a la primera, puede deberse a que la traducción de **google.com** está en la caché del cliente DNS en la máquina Windows. Podemos vaciar esa caché con el comando (en Vista y Windows 7 necesitaremos ejecutarlo desde una sesión con elevación de privilegios):

```
C:\> ipconfig /flushdns
```

8. Para terminar correctamente este caso práctico debemos interrumpir el ataque MITM y cerrar la herramienta ettercap.

1.1. Contramedidas

Los ataques MITM son difíciles de evitar. Una primera idea es utilizar en todas las máquinas tablas ARP estáticas, renunciando al protocolo dinámico, vista su debilidad. Parece sencillo, pero supone mucho trabajo de mantenimiento: cada vez que llega una nueva máquina, o introducimos una nueva tarjeta de red en una máquina ya existente, hay que actualizar una a una todas las máquinas de la empresa (y pueden ser cientos).

Es más razonable controlar el acceso a nuestra red: si el atacante no puede conectar su equipo, no podrá lanzar paquetes maliciosos. En este punto es importante recordar las medidas que vimos en la Unidad 6.

También es interesante utilizar, siempre que sea posible, protocolos seguros con infraestructura de clave pública (PKI), como vimos en la Unidad 2. Cualquier interceptación de mensajes no será provechosa, y el atacante no tiene las claves privadas de los extremos, por lo que no puede suplantarlos.

Con suficiente presupuesto, la solución definitiva es introducir un NIPS en la red, como vimos en la Unidad 7, que nos alerte de la presencia de respuestas ARP no solicitadas.

Realmente, no necesitamos un NIPS muy potente: el ataque es tan sencillo que un simple sniffer lo detecta durante la captura. En la ejecución de cualquiera de los casos prácticos 1 y 2 sobre ataques MITM, podemos fijarnos en que aparece un aviso del propio WireShark sobre la doble asignación MAC-IP: es normal que una dirección MAC pueda servir a varias direcciones IP, pero no es normal que una IP no aparezca asociada a dos MAC distintas.

Hay una excepción: en algunas soluciones de arquitecturas de alta disponibilidad, la IP de una máquina puede estar en una tarjeta principal o en una tarjeta de respaldo, pero nunca funcionarán las dos a la vez, y cuando se efectúa la conmutación de tarjetas, generalmente el software de red falsea la MAC de la segunda tarjeta para que el resto de los sistemas no se vean afectados por el cambio.

Salvo este caso, la inmensa mayoría de las direcciones IP de los paquetes que circulan por la red de una empresa deben estar asociadas a una única MAC. Encontrar asignaciones duplicadas debe hacernos sospechar.

Por otra parte, aunque puede ser relativamente fácil detectar un ataque MITM de tipo ARP (utiliza paquetes broadcast, que llegan a todos los equipos de la red, entre ellos nuestro sniffer o NIPS), la figura del intermediario se extiende a otros muchos protocolos. En general, son susceptibles de ser atacados todos los protocolos donde no hay autenticación de los equipos que participan en la comunicación. En este punto debemos recordar el concepto de seguridad extremo a extremo, donde no nos importa qué equipamiento de red atraviesan nuestros paquetes, porque estamos seguros de que solo serán aprovechables para el destinatario auténtico.

Web

Hay muchos peligros en la red. En esta web hay una lista detallada:

http://goo.gl/V6fje

Vocabulario

NIPS (Network Intrusion Protection System). Sistema que captura el tráfico de red para analizar los protocolos utilizados y así detectar e impedir determinados ataques.

2. Ataques wifi. Aircrack-ng

Como ya vimos en la Unidad 5, las redes inalámbricas son particularmente interesantes de atacar porque están muy extendidas (tanto en el ámbito personal como en el empresarial) y porque el atacante no necesita entrar en las instalaciones de la víctima: basta con situarse lo suficientemente cerca para entrar en la cobertura del access point.

Los estándares modernos WPA2 lo han puesto más difícil, pero lo siguen intentando. En este apartado veremos el ataque contra WEP mediante la herramienta aircrack-ng, para ilustrar lo fácil que resulta y por qué este cifrado está completamente abandonado.

Caso práctico 3

Cifrado WEP

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

Objetivo. Conseguir la clave WEP de una red wifi.

Material. Ordenador Linux Ubuntu 12.04 con conexión inalámbrica, ordenador Windows con conexión inalámbrica, router wifi.

1. Entramos al sistema Ubuntu y utilizamos `sudo –i` para elevar privilegios; los necesitaremos para instalar la herramienta y para ejecutarla.

2. Intentamos la instalación mediante `apt-get` y falla (Fig. 8.20). En efecto, esta herramienta ya no figura en los repositorios oficiales.

```
root@alumno-Latitude-D520: ~
root@alumno-Latitude-D520:~# apt-get install aircrack-ng
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
El paquete aircrack-ng no está disponible, pero algún otro paquete hac
ia
a él. Esto puede significar que el paquete falta, está obsoleto o sólo
encuentra disponible desde alguna otra fuente
Sin embargo, los siguientes paquetes lo reemplazan:
  iw

E: El paquete «aircrack-ng» no tiene un candidato para la instalación
root@alumno-Latitude-D520:~#
```

Fig. 8.20. *Intento de instalación.*

3. Podríamos descargarnos los fuentes de la página oficial e intentar compilarlos. Por fortuna, sí está disponible un ejecutable en **launchpad.net** (Fig. 8.21).

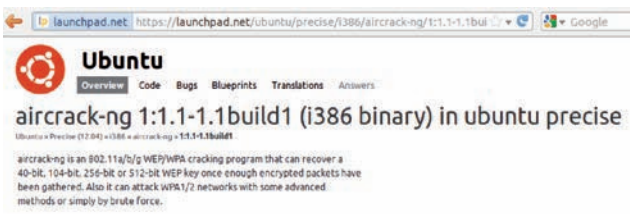


Fig. 8.21. *Encontramos sus binarios.*

Descargamos el fichero .deb y lo instalamos desde la utilidad *Centro de Software*. Como es normal, solicitará autenticación de administrador.

4. Si todo va bien, veremos que se han instalado aircrack-ng y todos los paquetes necesarios (Fig. 8.22).

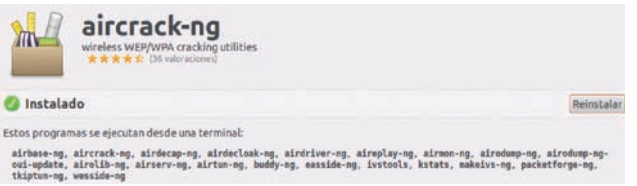


Fig. 8.22. *Instalado.*

5. Volvemos al terminal y ejecutamos `airmon-ng` para poner la tarjeta en modo monitor y así poder escuchar todos los paquetes (el conocido modo promiscuo). El ataque se basa en capturar muchos paquetes y procesarlos para deducir la clave utilizada. En este ejemplo la interfaz es wlan0, luego introducimos (Fig. 8.23):

```
# airmon-ng start wlan0
```

```
root@alumno-Latitude-D520:~# airmon-ng start wlan0

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
904     avahi-daemon
905     avahi-daemon
991     NetworkManager
1130    wpa_supplicant
1535    dhclient
Process with PID 1535 (dhclient) is running on interface wlan0

Interface       Chipset         Driver

wlan0           Intel 3945ABG   iwl3945 - [phy0]
                                (monitor mode enabled on mon0)

root@alumno-Latitude-D520:~#
```

Fig. 8.23. *Iniciamos la tarjeta.*

6. La herramienta nos advierte de que algunos procesos de la máquina pueden interferir con el ataque. Concretamente, tendremos problemas con el NetworkManager, por lo que debemos pararlo:

```
# service network-manager stop
```

7. Una vez que tenemos la tarjeta en modo monitor el siguiente paso es localizar la wifi que queremos atacar. Para eso utilizamos `airodump`:

```
# airodump-ng wlan0
```

Esta herramienta nos muestra todas las redes wifi de nuestra zona (Fig. 8.24). En cada línea aparece la infor-

(Continúa)

Caso práctico 3

(Continuación)

mación del access point (AP) correspondiente. Para el ataque nos interesa la BSSID (que es la MAC del AP), el canal (columna CH), el tipo de codificación (columna ENC) y el nombre de la red (columna ESSID).

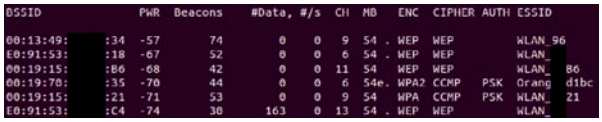


Fig. 8.24. *Redes de nuestra zona.*

8. Este ataque solo funciona con codificaciones WEP. De las cuatro disponibles, intentaremos atacar la primera: WLAN_96, que emite en el canal 9. Pulsamos **Ctrl+C** para terminar el comando.
9. Para continuar con este ejemplo, nos vamos al ordenador Windows y conectamos a esa red (es decir, sí sabemos la clave, pero nunca la hemos introducido en el Linux). Generaremos mucho tráfico accediendo a vídeo on-line, por ejemplo.
10. Con la tarjeta en modo monitor y sabiendo la identificación de la víctima, ya podemos hacer la captura. Lanzamos el mismo comando `airodump`, pero particularizado para esa red:

    ```
    # airodump-ng --ivs --write captura --bssid 00:13:49:XX:XX:34 --channel 9 wlan0
    ```

    El parámetro `ivs` indica que solo cogemos los vectores de inicialización (es lo que necesita el ataque); `write` permite especificar un nombre para los ficheros .ivs. Los parámetros `bssid` y `channel` los hemos obtenido con `airodump-ng`.

    En la ventana se muestra el estado de la captura (Fig. 8.25). La primera línea muestra el canal y el tiempo transcurrido. Después viene la información del AP. Lo más importante es la última lista, donde aparecen todos los equipos conectados actualmente a ese AP (se llaman estaciones). Sobre todo, la columna `Packets` que muestra todos los paquetes de esa estación que hemos conseguido capturar.

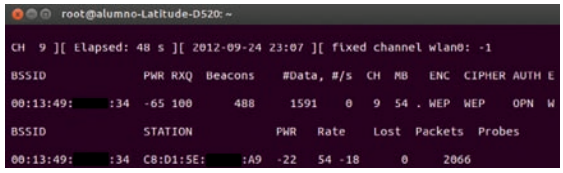


Fig. 8.25. *Captura de paquetes.*

11. Después de aproximadamente 20 000 paquetes detenemos el comando con **Ctrl+C.** La captura está en un fichero con la extensión .ivs. Usando esta información, vamos a intentar descifrar la clave con el comando `aircrack-ng`:

    ```
    # aircrack-ng *.ivs
    ```

12. Sin embargo, resulta insuficiente. La herramienta nos recomienda intentarlo de nuevo con 25 000.
13. Volvemos a lanzar la captura y esperamos hasta superar esa cifra. Después repetimos el comando y ahora lo consigue (Fig. 8.26). Utilizando el comando `time` podemos ver que ha tardado menos de dos segundos para una clave de 13 caracteres alfanuméricos.

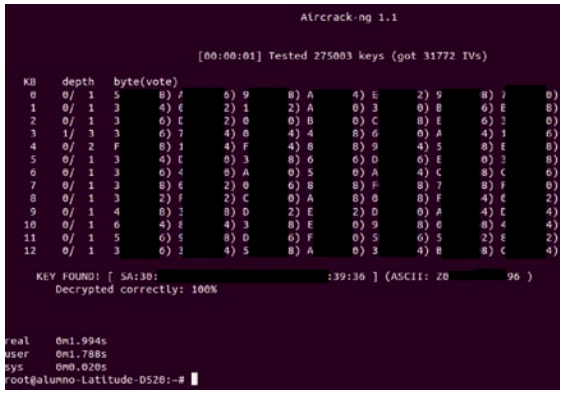


Fig. 8.26. *Tenemos la clave.*

2.1. Contramedidas

La primera solución es evitar utilizar cifrado WEP. Si lo tenemos porque algún dispositivo es incapaz de trabajar con otros protocolos, debemos plantearnos sustituir ese equipo o, si no es técnica o económicamente posible, dejarle un AP WEP para él solo y poner un nuevo AP WPA2 para el resto.

La segunda medida es reducir la potencia de nuestro AP. Así evitaremos que cualquiera de la calle pueda intentar atacarnos: simplemente no le llega la señal.

También se puede intentar activar en el AP la lista de MAC permitidas. Aunque es relativamente fácil para un atacante conocer alguna MAC permitida, ya que puede descifrar el tráfico porque tiene la clave WEP. Después, tranquilamente modifica la MAC de su máquina y ya puede conectar.

Web

Un americano ha sido condenado a 18 años de cárcel por cometer distintos delitos. Utilizaba la wifi de su vecino:

http://goo.gl/9HJ7n

3. Ataques web. WebGoat

Las aplicaciones web aplican la arquitectura cliente-servidor; por tanto, adolecen de los mismos problemas que los protocolos de red. En especial, el ataque MITM que vimos al principio de esta misma unidad.

La herramienta WebGoat permite ilustrar estos problemas. Al descargarla tenemos un entorno de aplicaciones web (Tomcat) configurado con unas lecciones para enseñar qué peligros corremos.

Caso práctico 4

Validación JavaScript

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

Objetivo. Utilizaremos un ataque MITM para anular la validación de datos en el navegador.

Material. Ordenador Windows con conexión a Internet.

1. Nos conectamos a Internet para descargar el software desde la página oficial. Vamos a la pestaña *Downloads* y elegimos el fichero .zip, que trae todo: el entorno y las lecciones (Fig. 8.27). Hay un fichero .war solo con las lecciones.



Fig. 8.27. *Descargamos la herramienta.*

2. Al descomprimir el fichero .zip aparece una carpeta con varias subcarpetas y unos scripts (Fig. 8.28). Lanzamos el webgoat.bat que arranca el servidor web en el puerto 80. Si acaso en nuestra máquina ya hay otra aplicación en este puerto, hay un segundo .bat para el puerto 8080.



Fig. 8.28. *Carpeta de arranque.*

3. Como era de esperar, una aplicación que intenta crear un nuevo puerto de escucha es detenida por el firewall (Fig. 8.29). Pulsamos *Desbloquear*.

Por cierto, el aviso dice que el programa que lo pide es Java: en efecto, el motor de servlets Tomcat está escrito en Java.



Fig. 8.29. *Desbloqueamos.*

4. Aparece la ventana de ejecución de Tomcat. No debemos cerrarla, porque esto detiene la aplicación.

5. Abrimos el navegador Firefox para empezar las lecciones. La URL será: localhost/WebGoat/attack. Nos solicitará usuario y contraseña: utilizamos guest/guest (Fig. 8.30).

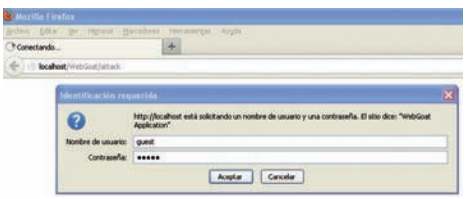


Fig. 8.30. *Autenticación.*

6. La pantalla principal es una introducción a la herramienta. En el lazo izquierdo hay un menú que nos permite elegir la lección que queremos aprender.

7. Antes de empezar con las lecciones, vamos a instalar la herramienta que nos permitirá realizar el ataque MITM. En este caso es un simple plugin del navegador. Vamos al administrador de complementos y buscamos Tamper Data.

8. Una vez instalado, podemos empezar la primera lección. En el menú de WebGoat vamos a *Parameter Tampering* y elegimos *Bypass Client Side JavaScript Validation*. El objetivo de esta lección es demostrar que, aunque hagamos validaciones de entrada de datos en la interfaz de usuario, también hay que hacerlas en el servidor, porque los datos que ha validado el navegador pueden ser alterados en el camino.

(Continúa)

Caso práctico 4

(Continuación)

9. El ejercicio consiste en siete entradas de datos que están validadas desde JavaScript (Fig. 8.31).

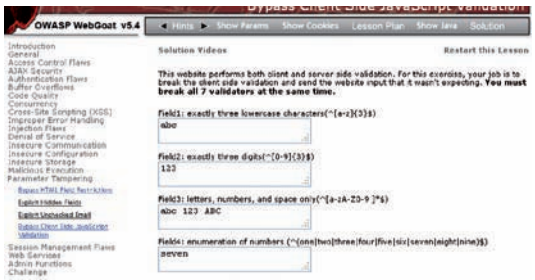


Fig. 8.31. *Enunciado del ejercicio.*

10. Podemos comprobar que es cierto: la segunda entrada solo admite tres números. Si ponemos otra cosa, aparece una ventana de error.

11. Rellenamos todos los campos con valores correctos y, antes de pulsar *Submit*, vamos al menú de Firefox llamado *Herramientas* para activar el plugin del ataque (Fig. 8.32).

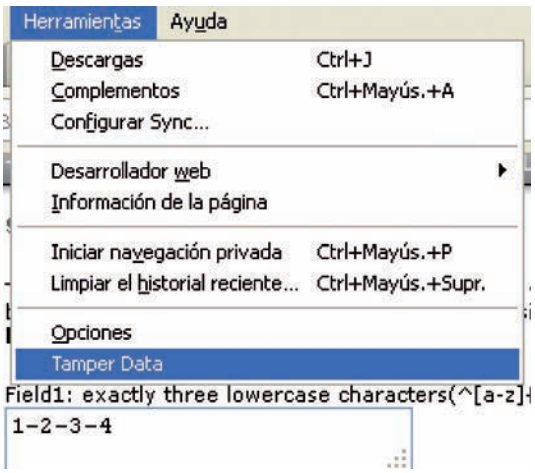


Fig. 8.32. *Activamos el ataque.*

12. Aparece una ventana donde interceptaremos todas las peticiones HTTP de nuestro navegador para que podamos verlas y, si queremos, modificarlas (Fig. 8.33). Pulsamos en *Comenzar modificación*.



Fig. 8.33. *Ventana de Tamper Data.*

13. Ya podemos pulsar el botón que envía el ejercicio para ser corregido. Como hemos puesto valores correctos en todos los campos, la validación JavaScript es satisfactoria y se genera la petición al servidor. En este punto, nuestro plugin actúa deteniendo la comunicación. Su ventana nos muestra la petición y nos pregunta si lo dejamos pasar, la interrumpimos aquí o la modificamos (Fig. 8.34).

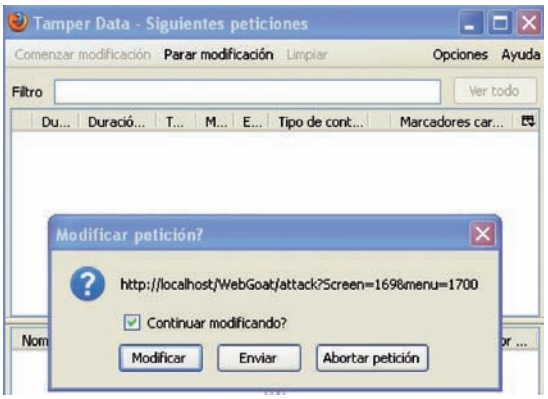


Fig. 8.34. *Petición interceptada.*

14. Pulsamos en *Modificar* y aparece una ventana con toda la información: a la izquierda los detalles de la petición y a la derecha los campos con nuestros valores legales que hemos introducido (Fig. 8.35).

Nombre de parámetro post	Valor de parámetro post
field1	abc
field2	123
field3	abc+123+ABC
field4	seven
field5	90210
field6	90210-1111
field7	301-604-4882

Fig. 8.35. *Valores legales.*

15. Para cumplir el ejercicio, debemos cambiar todos los valores por otros que no sean válidos (Fig. 8.36).

Nombre de parámetro post	Valor de parámetro post
field1	123456
field2	aabbcc
field3	*-)
field4	diez
field5	codigo postal
field6	codigo postal local
field7	neo

Fig. 8.36. *Valores incorrectos.*

16. Ahora podemos dejar que la petición modificada llegue al servidor. Si lo hemos hecho bien, la respuesta del servidor será que la lección está completada.

Caso práctico 5

Alteración de datos

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

Objetivo. Utilizaremos un ataque MITM para modificar un precio en una tienda web.

Material. Ordenador Windows con conexión a Internet.

1. Continuamos el caso práctico anterior con una nueva lección. Esta vez elegimos *Exploit Hidden Fields*. Aparece un formulario donde podemos elegir las unidades que vamos comprar de un determinado artículo (Fig. 8.37).



Fig. 8.37. *Carro de la compra.*

2. Introduciendo una cantidad y pulsando en *UpdateCart*, actualizamos el precio total. Por ejemplo, dos televisores cuestan 5 999,98 dólares.

3. Vamos a intentar que nos salga más barato. Activamos la herramienta Tamper Data y elegimos comprar diez unidades. Al pulsar el botón, nuestro atacante intercepta la petición y podemos ver todos los datos (Fig. 8.38).

Nombre de parámetro post	Valor de parámetro post
QTY	100
SUBMIT	UpdateCart
Price	2999.99

Fig. 8.38. *Datos de la compra.*

4. Como podemos ver, el diseñador de esta tienda web ha cometido un grave error: el precio de cada televisor viene como un dato más. Ahora es fácil modificarlo: lo dejamos en 99 centavos (Fig. 8.39).

Nombre de parámetro post	Valor de parámetro post
QTY	100
SUBMIT	UpdateCart
Price	0.99

Fig. 8.39. *Rebajamos el precio.*

5. Aplicamos los cambios y dejamos que la petición llegue hasta el servidor. Si lo hemos hecho bien, el servidor genera una página de felicitación porque hemos conseguido comprar diez televisores de 3 000 dólares por menos de 100 dólares en total.

3.1. Contramedidas

En este punto quienes deben tomar medidas son los programadores de aplicaciones, más que los técnicos de sistemas. Los ejemplos que hemos visto son suficientemente claros para que los responsables del software que corre en el servidor nunca confíen en que los datos de una petición son válidos solo porque han superado los controles que se han puesto en el navegador.

La principal misión de esos controles es ahorrar peticiones fallidas, de manera que los servidores no pierden tiempo y el usuario puede corregir sus erratas inmediatamente.

Es conveniente, además, que el equipo de pruebas de sistemas (responsables de probar una aplicación antes de entregarla al cliente) conozca estas herramientas de interceptación de peticiones, porque pueden ser utilizadas también por cualquier usuario.

También hay que tener en cuenta que los atacantes pueden combinar distintas técnicas para conseguir sus objetivos. Por ejemplo, hay un ataque conocido como SSLStrip donde primero activan un MITM mediante ARP spoofing, como ya hemos visto en el primer apartado de esta unidad, y después procesan las peticiones HTTPS que reciben de las máquinas engañadas. El procesamiento consiste en convertirlas en peticiones HTTP para así no utilizar el cifrado, de manera que los paquetes viajen en texto claro (el objetivo son los paquetes de autenticación: usuario y contraseña).

El ataque es efectivo porque la mayoría de los servidores admiten tanto HTTP como HTTPS. Aunque la página inicial redirige a la versión HTTPS, las demás no. La solución más simple es utilizar servidores que no admitan HTTP.

4. Ataques proxy. Ultrasurf

En la Unidad 7 vimos la utilidad del servidor proxy, tanto para censurar páginas como para mejorar el rendimiento de la conexión a Internet al funcionar como caché.

Sin embargo, algunos usuarios se niegan a que su navegación sea controlada por nadie. Para combatirlo, en Windows instalan algunos programas, como Ultrasurf. Este software se comporta como un proxy en nuestra propia máquina y modifica la configuración de Windows para que todas las conexiones web pasen por él (esto afecta a Internet Explorer y a Chrome, que utiliza la configuración del sistema).

Este proxy interno recibe las conexiones y las encamina fuera de la máquina conectando con otras máquinas en Internet. Estas máquinas utilizan el puerto 443 (el habitual del tráfico SSL). Como en un proxy normal, obtienen las páginas que el usuario pedía y se las mandan al proxy interno, el cual las entrega al navegador. Por tanto, el tráfico del usuario pasa por dos proxy: uno local y otro en Internet.

Caso práctico 6

Evitar el proxy de la empresa

■ **Duración:** 30 minutos ■ **Dificultad:** Media

Objetivo. Saltarse el proxy de la empresa mediante Ultrasurf.

Material. Ordenador Linux con dos tarjetas de red (una de ellas Ethernet), ordenador Windows con tarjeta de red Ethernet, salida a Internet para el ordenador Linux.

1. Conectamos el ordenador Windows al Linux mediante un cable Ethernet. También conectamos el ordenador Linux a Internet (en este ejemplo, será una conexión wifi).
2. Configuramos el ordenador Windows con la dirección 10.0.1.2/8, puerta de enlace 10.0.1.1 (que será la dirección de la interfaz Ethernet del router) y servidor DNS 8.8.8.8 (Fig. 8.40).

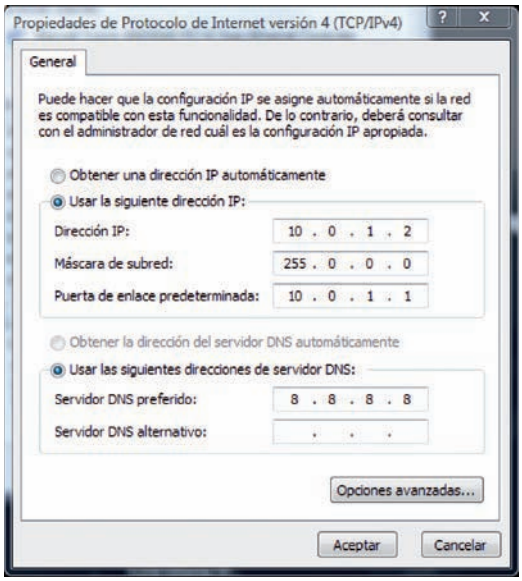


Fig. 8.40. *Configuración del ordenador Windows.*

3. Configuramos el ordenador Linux para que sea router del ordenador Windows (Fig. 8.41):

```
# echo 1 > /proc/sys/net/ipv4/ip _ forward
# iptables -t nat -A POSTROUTING -s 10.0.1.2/32 -o wlan0 -j MASQUERADE
```

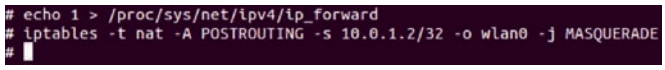


Fig. 8.41. *Damos salida a Internet.*

4. El ordenador Windows tiene acceso total a Internet pasando por el Linux (Fig. 8.42).

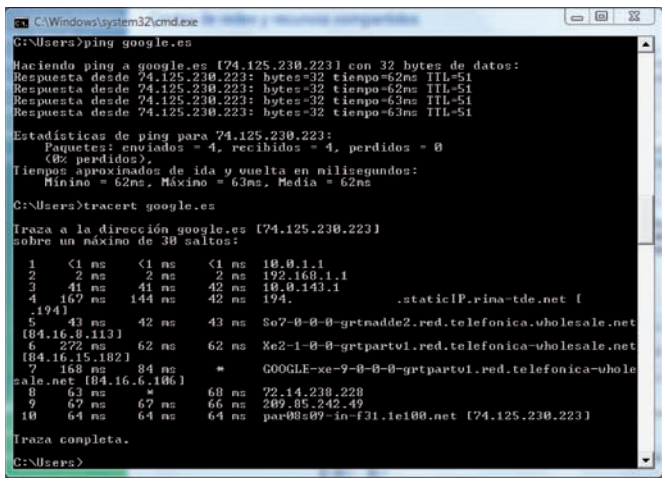


Fig. 8.42. *Conectividad normal.*

5. Ahora instalamos en el Linux un proxy Squid como ya vimos en la Unidad 7. Creamos una regla que impida consultar ninguna página que contenga la palabra google. Para ello creamos un fichero con esa palabra:

```
# echo google > /etc/squid3/prohibido
```

(Continúa)

Caso práctico 6

(Continuación)

Después configuramos el squid.conf (Fig. 8.43):

```
acl prohibido url _ regex –i "/etc/squid3/
prohibido"
http _ access deny prohibido
http _ access allow all
```

```
acl prohibido url_regex -i "/etc/squid3/prohibido"
http_access deny prohibido
http_access allow all
```

Fig. 8.43. *Censuramos.*

6. Reiniciamos el squid para aplicar los cambios. Solo falta introducir una regla en el firewall del Linux para que todo el tráfico web del Windows pase por el proxy (Fig. 8.44).

```
# iptables –t nat –A PREROUTING –i eth0
–p tcp --dport 80 –j DNAT –to-destination
10.0.1.1:3128
```

```
root@alumno-Latitude-D520:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destinat
ion 10.0.1.1:3128
```

Fig. 8.44. *Forzamos pasar por el proxy.*

7. Listo. Desde este momento todas las webs de Google quedan bloqueadas. Lo podemos ver en el log del proxy (Fig. 8.45).

```
1348596704.190      0 10.0.1.2 TCP_DENIED/403 4413 GET http://google.es/ - NONE/- text/html
1348596706.641      0 10.0.1.2 TCP_DENIED/403 4372 GET http://google.es/favicon.ico - NONE/- text/html
```

Fig. 8.45. *Censura efectiva.*

8. El usuario del ordenador Windows también se ha dado cuenta (Fig. 8.46).



Fig. 8.46. *Contenido bloqueado.*

9. De alguna manera, este usuario consigue el software Ultrasurf y lo instala. Al arrancarlo aparece la ventana de la herramienta (Fig. 8.47). Estas herramientas pueden ser utilizadas por cualquier usuario porque no requiere privilegios de administrador: no necesita copiar ficheros en los directorios de Windows (c:\archivos de programa, c:\windows\system, c:\windows\system32, etc.) y para recibir el tráfico abre el puerto 9666 que, como está por encima del 1024, el sistema no aplica ninguna limitación especial. Además, tampoco es extraño que una aplicación hable con otra de la misma máquina.

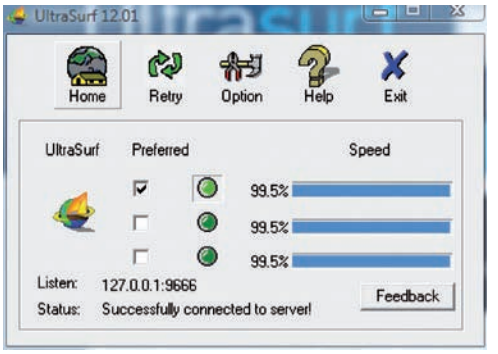


Fig. 8.47. *Ultrasurf.*

10. En la parte inferior muestra la dirección (`127.0.0.1:9666`) donde está escuchando el proxy que incorpora. También informa de que ha conseguido conectar al servidor exterior (el segundo proxy en Internet). Si vemos las conexiones con `netstat -abn`, efectivamente el puerto `9666` está abierto por un programa llamado `u1201.exe` (Fig. 8.48).

```
  TCP    127.0.0.1:9666         0.0.0.0:0              LISTENING
[u1201.exe]
  TCP    127.0.0.1:9666         127.0.0.1:49862        TIME_WAIT
  TCP    127.0.0.1:9666         127.0.0.1:49863        ESTABLISHED
[u1201.exe]
  TCP    127.0.0.1:9666         127.0.0.1:49864        ESTABLISHED
[u1201.exe]
  TCP    127.0.0.1:9999         0.0.0.0:0              LISTENING
[u1201.exe]
  TCP    127.0.0.1:9999         127.0.0.1:49861        ESTABLISHED
[u1201.exe]
```

Fig. 8.48. *Tráfico extraño.*

11. El usuario Windows puede volver a navegar por cualquier web. Como administradores de red revisamos el log del squid y nos extraña que ya no aparezcan conexiones censuradas. Hacemos una captura de tráfico en la interfaz Ethernet con `tcpdump` y encontramos un comportamiento extraño (Fig. 8.49).

```
root@alumno-Latitude-D520:~# tcpdump -i eth0 -l -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
20:32:29.946473 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 509
20:32:30.173615 IP 65.49.2.21.554 > 10.0.1.2.59118: UDP, length 375
20:32:31.007101 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 266
20:32:31.007208 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 266
20:32:31.007260 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 266
20:32:31.007354 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 734
20:32:31.054298 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 266
20:32:31.072412 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 266
20:32:31.074776 IP 10.0.1.2.57668 > 8.8.8.8.53: 50148+ A? www.youtube.com. (33)
20:32:31.086244 IP 10.0.1.2.59118 > 65.49.2.21.554: UDP, length 266
```

Fig. 8.49. *Puertos de escucha.*

12. La máquina Windows (`10.0.1.2`) está intercambiando tráfico continuamente con la máquina `65.49.2.21`. Solo de vez en cuando aparece una conexión a otra máquina (en el ejemplo, una consulta DNS).

13. Hacemos un ping a esa dirección y responde. Abrimos el navegador para entrar en esa dirección aparentemente tan interesante; pero no llega ninguna página (Fig. 8.50).

(Continúa)

Caso práctico 6

(Continuación)

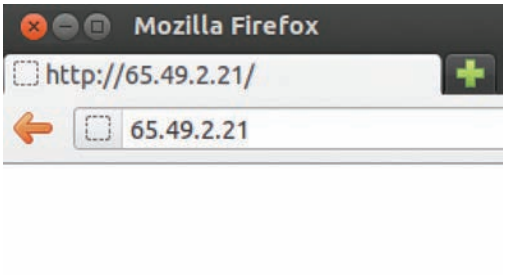


Fig. 8.50. *No es una web.*



Fig. 8.51. *Buscamos su ubicación.*

14. Finalmente, hacemos un `traceroute` para ver dónde está alojada; pero a partir de un punto su rastro se pierde (Fig. 8.51).

15. Con estos datos debemos desconfiar de la máquina `10.0.1.2` y hacerle una revisión por si tiene algún software innecesario.

4.1. Contramedidas

La primera medida es formar a los usuarios para que entiendan que introducir software no controlado es una fuente de problemas:

- No sabemos si ese software amable y gratuito realmente oculta un troyano que puede tomar el control de nuestra máquina. En un ordenador personal podemos hacer lo que queramos, pero no en el ordenador del puesto de trabajo.
- Todo nuestro tráfico web está pasando por máquinas que no conocemos. Pueden utilizarlo para robarnos contraseñas, documentación personal o profesional, realizar ataques MITM, etc.
- Se pone un proxy en una empresa para conseguir unos objetivos y, al evitar utilizarlo, estamos obstaculizando su cumplimiento. Por ejemplo, la optimización del ancho de banda de salida a Internet.

Como aun así algunos lo intentarán, debemos espiar nuestra red, como vimos en la Unidad 7. Primero con medidas estadísticas que evalúen el porcentaje de paquetes que pasan por el proxy comparado con aquellos que utilizan el puerto 443. Si tienden a equilibrarse, tenemos que entrar en detalle. Para ello utilizaremos un NIDS que busque máquinas con alto porcentaje de tráfico 443. Seguramente, la máquina de Internet con la que comunican no es una web ni es posible rastrearla con traceroute ni corresponde a ninguna entrada de DNS.

Por cierto, no podemos directamente bloquear en el firewall el tráfico 443 porque ese puerto es habitual en la navegación segura SSL. Dejaríamos de poder entrar en los correos web, bancos, etc.

Tampoco tiene mucho sentido utilizar el firewall de red para bloquear todos los paquetes que quieran salir a Internet con destino la IP del proxy externo de Ultrasuft (la 65.49.2.21 de nuestro caso práctico). Este tipo de software es muy listo y suele tener disponibles muchos servidores en distintos puntos de Internet (por tanto, ni siquiera podemos utilizar el bloqueo por subred IP): simplemente prueba esas direcciones una a una hasta que encuentra alguna que todavía no hemos bloqueado.

Aunque circulan muchas listas de estas IP de máquinas proxy (las llamadas listas blacklist), siempre estarán desactualizadas, y mientras tanto nuestro firewall de red está aplicando continuamente múltiples filtros a cada paquete, lo que ralentiza nuestra preciada conexión a la web.

Finalmente, podemos encontrar algunos programas que dicen que son capaces de bloquear Ultrasurf. Debemos desconfiar, porque pueden ser directamente malware, o consumir recursos sin control (suelen ser NIPS especializados), o efectivamente llegar a bloquear Ultrasurf, pero no cualquiera de sus sucesores, como Freegate.

Actividades

3. Investiga cómo podemos combatir a Ultrasurf mediante un traffic shaper.

Síntesis

Los protocolos básicos de TCP/IP son eficaces, pero inseguros. La mayoría es susceptible de sufrir un ataque MITM (Man-In-The-Middle).

- La comunicación entre dos máquinas A y B pasa por una tercera máquina C que puede registrar, incluso alterar **maliciosamente,** los paquetes intercambiados por A y B.
- A y B ignoran qué está ocurriendo porque:
  - C tiene acceso a la conexión física y consigue interponerse.
  - C les ha engañado.

El engaño se puede lograr mediante la técnica de envenenamiento ARP.

- C envía repetidamente mensajes ARP hacia A diciendo que es B.
- C envía repetidamente mensajes ARP hacia B diciendo que es A.

Una vez engañados, al atacante le basta con modificar una sencilla petición DNS para realizar un ataque de fabricación.

Podemos intentar varias contramedidas:

- Tablas **ARP estáticas.** Pero solo tiene sentido en una red muy estable con pocos equipos.
- **Proteger el acceso a la red,** para que sea difícil introducir la máquina C.
- Utilizar seguridad bajo **PKI.**
- Introducir **NIPS** en la red para detectar el tráfico ARP extraño.

Es muy frecuente el ataque a las redes inalámbricas para intentar introducirse en su red (para luego lanzar un MITM, por ejemplo). Los primeros protocolos de seguridad (WEP) se siguen utilizando, aunque son débiles.

- Poniendo la tarjeta en modo monitor capturaremos fácilmente el tráfico en un AP.
- Analizando criptográficamente ese tráfico, en pocos segundos aparece la clave.

Las contramedidas posibles son:

- Utilizar mejores protocolos, como **WPA2.**
- Reducir la **potencia de emisión** del AP para dificultar la captura.
- Elaborar una **lista de MAC** autorizadas en ese AP.

La mayoría de las aplicaciones web utilizan el protocolo HTTP, que transmite la información en texto plano. Los paquetes pueden ser interceptados, incluso en la propia máquina donde ejecuta el navegador, y modificados maliciosamente.

Las contramedidas posibles son:

- En este tipo de aplicaciones la **validación de datos siempre debe hacerse en el servidor** y, opcionalmente, en el cliente.
- Mejorar la **formación** de los programadores y los equipos de pruebas.

Los servicios proxy de Internet a menudo son utilizados por empleados que intentan evitar los controles instalados en la red de la empresa.

- El empleado instala un software que arranca un servidor proxy en su propia máquina.
- Ese software configura el sistema operativo y los navegadores para que todas las consultas HTTP pasen por él.
- Cuando le llega una petición, la encapsula en tráfico HTTPS y la envía a un segundo servidor proxy, esta vez en una máquina de Internet.

Las contramedidas posibles son:

- **Formar a los usuarios** sobre el peligro que supone que sus conexiones pasen por máquinas ajenas. También es potencialmente peligroso instalar software de procedencia desconocida.
- **Analizar estadísticamente** el tráfico de nuestra red: los equipos que tienen un alto porcentaje de conexiones HTTPS son sospechosos, sobre todo si la máquina destino no tiene servidor web, el traceroute se pierde, etc.

Test de repaso

1. Los protocolos TCP/IP son inseguros porque:
- *a)* En su diseño se pensó más en la fiabilidad que en la seguridad.
- *b)* En los años setenta no había hackers.
- *c)* Todos los protocolos son muy seguros: por eso se siguen utilizando.

2. El ataque MITM mediante software:
- *a)* Es un ataque de tipo interrupción.
- *b)* Es un ataque de tipo interceptación.
- *c)* Es un ataque de tipo fabricación.

3. Si el ataque MITM tiene éxito, a continuación:
- *a)* Podemos lanzar ataques de interrupción.
- *b)* Podemos lanzar ataques de interceptación.
- *c)* Las respuestas anteriores son correctas.

4. Si un ataque MITM tiene éxito, a continuación:
- *a)* Podemos lanzar ataques de interrupción.
- *b)* Podemos lanzar ataques de fabricación.
- *c)* Las respuestas anteriores son correctas.

5. El ataque MITM puede realizarse mediante:
- *a)* Hardware: el atacante se interpone en algún tramo de la conexión física entre las máquinas atacadas.
- *b)* Software: el atacante engaña a las máquinas atacadas haciéndose pasar por alguna de ellas.
- *c)* Las respuestas anteriores son correctas.

6. El envenenamiento ARP consiste en:
- *a)* Configurar los equipos para que utilicen tablas ARP estáticas.
- *b)* Desinstalar el protocolo ARP.
- *c)* Enviar respuestas ARP no solicitadas.

7. Para que funcione el ataque por envenenamiento ARP:
- *a)* Basta con enviar una vez los paquetes adulterados, porque las víctimas lo dejan apuntado en su tabla.
- *b)* Hay que repetirlo continuamente, porque las tablas ARP caducan.
- *c)* Debemos introducir un troyano en las víctimas para que desinstale el protocolo ARP.

8. Contra un ataque por envenenamiento ARP:
- *a)* Podríamos bloquear el tráfico ARP en todos los routers de la red.
- *b)* Podríamos utilizar tablas ARP estáticas.
- *c)* Lo ideal es introducir un servidor NIPS que identifique este comportamiento anómalo.

9. Los ataques a las redes inalámbricas intentan:
- *a)* Conseguir la clave del administrador del punto de acceso.
- *b)* Conseguir la clave para conectar al punto de acceso.
- *c)* Las redes inalámbricas son inmunes a cualquier ataque.

10. El ataque a un clave WEP utilizando aircrack-ng:
- *a)* Lo puede lanzar cualquier usuario, porque el software se descarga de Internet.
- *b)* Se puede lanzar desde cualquier punto de Internet, siempre que sea un router wifi.
- *c)* Lo debe lanzar un usuario privilegiado, porque hay que poner la tarjeta en modo monitor.

11. Para evitar un ataque a un AP que utiliza WEP:
- *a)* Mejor sustituir el WEP por WPA.
- *b)* Ocultaremos el nombre de la wifi (SSID).
- *c)* Utilizaremos claves largas.

12. Los ataques a una aplicación web:
- *a)* No suelen ocurrir, porque Internet es una red segura.
- *b)* Pueden ser de tipo MITM, introduciendo el software adecuado en el navegador.
- *c)* Podemos evitarlos si el software del servidor está actualizado.

13. Si una página web realiza la validación de datos de entrada a una aplicación:
- *a)* Es suficiente: debemos fiarnos del programador de esa página.
- *b)* Es insuficiente: una vez validados en la página y enviados al servidor, pueden sufrir modificaciones durante la transmisión.
- *c)* Las páginas web no realizan validación de datos de entrada.

14. Los ataques proxy en una red de empresa:
- *a)* A veces son beneficiosos, porque optimizan la ocupación de la conexión a Internet.
- *b)* Como son inevitables, deberíamos eliminar todas las restricciones de páginas deportivas, juegos, etc.
- *c)* Debemos combatirlos mediante formación a los usuarios y análisis estadístico del tráfico.

15. Cuando un usuario instala un proxy en su máquina:
- *a)* No pasa nada: el firewall de red evitará que salga al exterior.
- *b)* Es una infracción grave, porque ha instalado software no autorizado.
- *c)* Solo puede instalar Ultrasurf, porque es el recomendado por las revistas.

Soluciones: 1 a, 2 c, 3 c, 4 c, 5 c, 6 c, 7 b, 8 c, 9 b, 10 c, 11 a, 12 b, 13 b, 14 c, 15 b.

Comprueba tu aprendizaje

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

1. En el laboratorio del aula, monta una red como aparece en la Figura 8.52. Son cuatro ordenadores y un punto de acceso wifi.

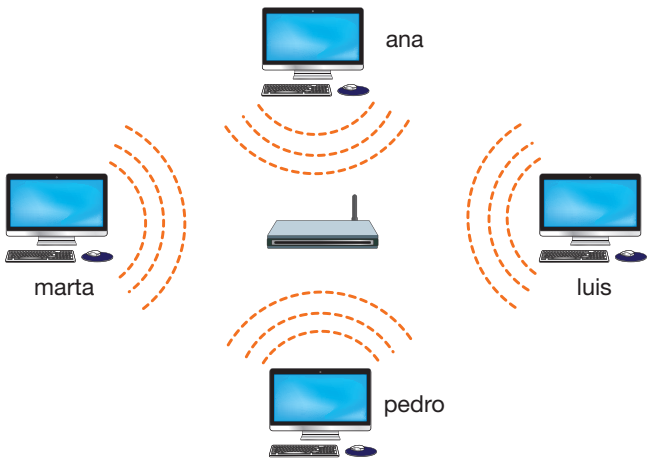


Fig. 8.52. *Red de prueba.*

El trabajo que hay que realizar es el siguiente:

a) El punto de acceso utiliza seguridad WEP y le configuramos una clave de longitud corta: 64 bits.

b) En los ordenadores ana, marta y luis introducimos esa clave para conectarlos entre sí. Podemos utilizar el servidor DHCP del punto de acceso o direccionamiento estático. Documenta los pasos que has ejecutado en cada caso.

c) Desde el ordenador pedro intentaremos obtener la clave atacando con la herramienta aircrack-ng. Documenta el procedimiento y los resultados.

d) Repite el ejercicio, pero ahora con una clave de 128 bits. Compara el número de paquetes capturados necesarios y el tiempo del análisis criptográfico.

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

2. Sobre la misma red del ejercicio 1, el trabajo que hay que realizar es el siguiente:

a) En el ordenador luis instalarás un servidor web cuya página inicial sea la siguiente:

<h1>Hola, soy Luis </h1>

b) Los navegadores web de los ordenadores ana y marta conectan perfectamente con el ordenador luis y permiten mostrar su página inicial.

c) En el ordenador pedro instalamos un servidor web cuya página inicial sea la siguiente:

<h1>Hola, no soy Luis, sino Pedro </h1>

d) En el ordenador pedro realizamos un ataque MITM mediante envenenamiento de ARP. Las víctimas serán ana y luis. El resultado debe ser que, al introducir la IP de luis en el navegador de ana, aparece la página de pedro. Sin embargo, el navegador de marta sigue mostrando la página de luis. Documenta los pasos que has ejecutado.

e) Ampliamos el ataque incluyendo las comunicaciones entre marta y luis. El resultado debe ser que, al introducir la IP de luis en el navegador de marta, aparezca la página de pedro. Documenta los pasos que has ejecutado.

f) Termina el ataque y comprueba que se recupera el funcionamiento normal. Documenta los pasos que has ejecutado.

g) Sustituimos el ordenador luis por una conexión a Internet (si el punto de acceso era además router ADSL, podemos utilizarlo).

h) En el ordenador ana instalamos un proxy Squid como se explica en la Unidad 7. Configuramos marta y pedro para que lo utilicen explícitamente. Comprobamos en el log de ana que las conexiones HTTP pasan por su proxy. Documenta el procedimiento ejecutado.

i) En el ordenador pedro ahora instalamos Ultrasurf y comprobamos en el log de ana que las conexiones HTTP de marta siguen pasando por su proxy, pero ya no hay conexiones de pedro. Documenta el procedimiento ejecutado.

j) Modifica el servidor web de luis para que utilice HTTPS. Comprueba que funciona y después intenta un ataque MITM mediante SSLStrip. Documenta los pasos que has llevado a cabo.

k) Finalmente, modifica el servidor web de luis para que ya no utilice HTTP, sino solo HTTPS. Intenta el ataque SSLStrip y comprueba que ya no es viable. Documenta el procedimiento ejecutado.

https://www.yolibrospdf.com/

Seguridad informática

«La base de tu futuro»

https://www.yolibrospdf.com

El proyecto editorial de McGraw-Hill para la formación profesional ha sido desarrollado según tres principios básicos:

- Una metodología basada en la práctica y en la adecuación de contenidos y procedimientos a la realidad profesional.
- Unos materiales desarrollados para conseguir las destrezas, habilidades y resultados de aprendizaje que necesitarás para conseguir tu título y desenvolverte en el mercado laboral.
- Una presentación de los contenidos clara y atractiva, con variedad de recursos gráficos y multimedia que facilitarán tu aprendizaje.

El proyecto para el módulo profesional *Seguridad informática* ha sido desarrollado considerando las unidades de competencia del **Catálogo Nacional de Cualificaciones Profesionales:**

Unidades de competencia profesional
Mantener y regular el subsistema físico en sistemas informáticos. **(UC0957_2)**
Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación del cliente. **(UC0958_2)**
Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos. **(UC0959_2)**

Confiamos en que esta obra sea una herramienta útil y eficaz, y que contribuya a tu formación como profesional.

https://www.yolibrospdf.com

