Administración de la seguridad

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190213

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Como veremos seguidamente, el concepto de seguridad informática es difuso y prácticamente inalcanzable, por lo que será preferible centrarnos en lo que podríamos llamar fiabilidad, entendida como garantía de calidad de servicio de un sistema informático. En este módulo veremos los elementos que pueden comprometer esta fiabilidad, y también las herramientas que un administrador tiene a su disposición a la hora de evitar y detectar las carencias de seguridad de un sistema informático. Finalmente, en los últimos apartados de este módulo introducimos el concepto del mal llamado delito informático, las responsabilidades derivadas de este tipo de acciones, así como las bases de una disciplina de reciente creación, la informática forense, la cual nos puede ayudar a determinar, una vez ha sucedido un incidente, qué ha pasado y quién ha sido su autor.

Objetivos

En los materiales didácticos asociados a este módulo, el estudiante encontrará las herramientas y los contenidos necesarios para alcanzar los objetivos siguientes:

1. Conocer los problemas básicos que comporta la administración de seguridad de un sistema informático.

2. Conocer cuáles son las responsabilidades que tiene un administrador en cuanto a los equipos y los datos que se encuentran contenidos en un sistema informático, y las responsabilidades en las que pueden incurrir las personas que vulneran su seguridad, así como qué hay que hacer una vez ha sucedido un incidente de seguridad para poder determinar qué ha pasado y quién ha sido su presunto autor.

3. Saber establecer planes de recuperación del sistema en caso de ataque o pérdida de información.

1. Seguridad informática

Aunque sea de una manera intuitiva, todos entendemos que un sistema informático se considerará seguro si se encuentra libre de todo riesgo o daño. Aunque no resulta muy sencillo formalizar el concepto de seguridad informática, entenderemos como tal el conjunto constituido por diversas metodologías, documentos, software y hardware que determinan que los accesos a los recursos de un sistema informático sean llevados a cabo exclusivamente por los elementos autorizados a hacerlo.

Efecto de desastres naturales

Aunque no se tendrán en consideración las medidas que hay que aplicar para prevenir o reducir el efecto de los desastres naturales u otros tipos de accidentes (incendios, inundaciones, etc.), en un estudio real pueden ser de importancia vital.

Dado que es del todo imposible garantizar la seguridad o inviolabilidad absoluta de un sistema informático, en lugar del inalcanzable concepto de seguridad será preferible utilizar el término **fiabilidad**. Por lo tanto, no se podrá entender la seguridad informática como un concepto cerrado, consecuencia de la aplicación mecánica de una serie de métodos, sino como un proceso que se puede ver comprometido en cualquier momento de la manera más insospechada posible.

En general, pues, diremos que un sistema informático es fiable cuando se satisfacen las tres propiedades siguientes:

- **Confidencialidad**: sólo pueden acceder a los recursos que integran el sistema los elementos autorizados a hacerlo. Por recursos del sistema no sólo se entiende la información, sino cualquier recurso en general: impresoras, procesador, etc.

- **Integridad**: los recursos del sistema sólo pueden ser modificados o ser alterados por los elementos autorizados a hacerlo. La modificación incluye diversas operaciones, como el borrado y la creación, además de todas las posibles alteraciones que se puedan hacer sobre un objeto.

- **Disponibilidad**: los recursos del sistema tienen que permanecer accesibles a los elementos autorizados.

Como podemos imaginar, es muy difícil encontrar un sistema informático que maximice las tres propiedades. Normalmente, y según la orientación del sistema, se priorizará alguna de las tres vertientes.

Ejemplo de priorización de la confidencialidad de la información

En un sistema que almacene datos de carácter policial, el elemento que hay que priorizar es la confidencialidad de la información, aunque también hay que tener muy en cuenta la preservación (en la medida en que se pueda) de la integridad y la disponibilidad. Observamos que no sirve de nada garantizar la confidencialidad mediante algún método criptográfico si permitimos que un intruso pueda borrar fácilmente la información almacenada en el disco duro del servidor (ataque contra la integridad). Por otra parte, es absolutamente necesario que los datos puedan estar disponibles en el transcurso de una actuación policial, por lo que tampoco podemos olvidar la propiedad de disponibilidad en un sistema de estas características.

1.1. Tipo de ataques

La protección de un sistema informático no sólo se tiene que dirigir al hardware y al software, sino también a los datos, tanto si se encuentran circulando por una red como si están almacenados en un disco duro o en otros soportes.

Pensemos que, si bien casi siempre es posible sustituir el hardware o el software, los datos, objetivo primordial de todo sistema informático, no tienen sustituto en caso de que se pierdan definitivamente.

Los ataques que pueden sufrir el hardware, el software y, de una manera muy especial, los datos, se clasifican en cuatro grandes grupos:

1) Interrupción: ataque contra la disponibilidad en el cual se destruye o queda no disponible un recurso del sistema.

Ejemplo de ataque de interrupción

Un ejemplo de ataque de interrupción es cortar una línea de comunicación o deshabilitar el sistema de ficheros del servidor. Otro son los ataques de denegación de servicio.

2) Intercepción: ataque contra la confidencialidad, en el cual un elemento no autorizado consigue el acceso a un recurso. En este tipo de ataque no nos referimos únicamente a posibles usuarios que actúen como espías en la comunicación entre emisor y receptor.

Ejemplo de ataque de interceptación

Un proceso que se ejecuta subrepticiamente en un ordenador y que almacena en un fichero las teclas que pulsa el usuario que utiliza el terminal, constituiría un ataque de intercepción.

El software o hardware que registra la actividad de un teclado de una estación de trabajo recibe el nombre genérico de *keylogger*.

Ved también

Sobre los ataques de denegación de servicio, ved el subapartado 3.6 de este mismo módulo.

3) Modificación: ataque contra la integridad en el cual, además de conseguir el acceso no autorizado a un recurso, también se consigue modificarlo, borrarlo o alterarlo de cualquier manera.

Ejemplos de ataque de modificación

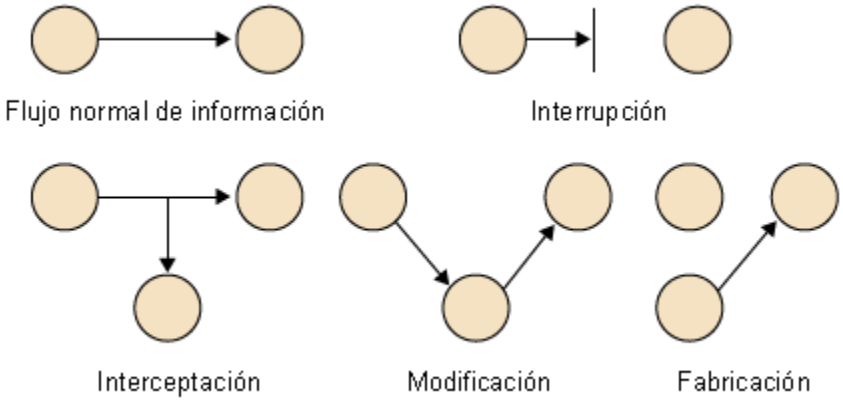
Los ataques hechos por los intrusos (borrado de bases de datos, alteración de páginas web, etc.) son ejemplos típicos de esta modalidad de ataque.

4) Fabricación: ataque contra la integridad en el cual un elemento consigue crear o insertar objetos falsificados en el sistema.

Ejemplos de ataque de fabricación

Un ejemplo de ataque de fabricación es añadir, de una manera no autorizada, un nuevo usuario –y la contraseña correspondiente– en el fichero de contraseñas.

Representación de los diferentes tipos de ataques que puede sufrir la comunicación entre emisor y receptor



1.2. Ataques provenientes de personas

La mayor parte de los ataques que puede sufrir un sistema informático se producen en manos de personas que, con diversos objetivos, intentan acceder a información confidencial, destruirla o simplemente conseguir el control absoluto del sistema atacado. Conocer los objetivos de los atacantes y sus motivaciones resulta, pues, esencial para prevenir y detectar las acciones.

Ved también

Las amenazas lógicas (virus, troyanos, etc.) se considerarán en el apartado 3 de este módulo, dedicado a la seguridad del sistema.

Así pues, los ataques provenientes de personas se pueden clasificar en dos grandes grupos:

1) Ataques pasivos. El atacante no modifica ni destruye ningún recurso del sistema informático, simplemente lo observa, normalmente con la finalidad de obtener alguna información confidencial. A menudo este ataque se produce sobre la información que circula por una red. El atacante no altera la comunicación, sino que sencillamente la escucha y obtiene la información que se transmite entre el emisor y el receptor. Como la información que se transmite no resulta alterada, la detección de este tipo de ataque no es una tarea sencilla, porque la escucha no tiene ningún efecto sobre la información circulante. Una solución muy eficaz que permite resolver este tipo de problema consiste en el uso de técnicas criptográficas para hacer que la información no se transmita en claro y no pueda ser comprensible para los espías.

Ved también

Una herramienta criptográfica que se utiliza mucho es el PGP (*pretty good privacy*). Sobre esta herramienta, podéis ver el apartado 2 de este mismo módulo.

2) Ataques activos. En una acción de este tipo, el atacante altera o destruye algún recurso del sistema. Por ejemplo, en el caso de un espía que monitoriza una red, se podrían dar problemas muy serios, como los que exponemos a continuación:

- **Suplantación de identidad**: el espía puede suplantar la identidad de una persona y enviar mensajes en su nombre.

- **Reactuación**: uno o diversos mensajes legítimos son interceptados y reenviados diversas veces para producir un efecto no deseado (por ejemplo, intentar repetir diversas veces un ingreso en una cuenta bancaria).

- **Degradación fraudulenta del servicio**: el espía evita el funcionamiento normal de los recursos del sistema informático. Por ejemplo, podría interceptar y eliminar todos los mensajes que se dirigen a un usuario determinado.

- **Modificación de mensajes**: se modifica una parte del mensaje interceptado y se reenvía a la persona a quien iba dirigido originalmente.

Como ya se ha indicado previamente, conocer las motivaciones que pueden tener las personas para atacar los sistemas informáticos puede ser vital a la hora de prevenir todo tipo de intrusiones. Veamos, pues, el perfil de los posibles atacantes de un sistema informático:

- **Personal de la misma organización**: aunque por defecto el personal interno disfruta de la confianza de la organización, hay que tener en cuenta que algunos ataques se pueden producir desde dentro mismo de la institución. A menudo no hace falta que estos ataques sean intencionados (aunque, cuando lo son, son los más devastadores que se pueden producir); pueden ser accidentes provocados por el desconocimiento del personal (por ejemplo, el formateo accidental de un disco duro).

Desinformación

Una política de seguridad adecuada puede evitar los problemas provocados por la desinformación o falta de conocimiento.

- **Antiguos trabajadores**: una parte muy importante de los ataques a sistemas informáticos son los realizados por antiguos trabajadores que, antes de dejar la organización, instalan todo tipo de software destructivo como, por ejemplo, virus o bombas lógicas que se activan en ausencia del trabajador que, despedido o descontento por las condiciones de trabajo, ha decidido cambiar de empleo. La presencia de este tipo de software no siempre es fácil de detectar, pero al menos sí que se pueden evitar los ataques que el antiguo trabajador pueda llevar a cabo desde fuera con el nombre de usuario y la contraseña de que disponía cuando todavía trabajaba en la organización. Por lo tanto, como norma general, hay que dar de baja todas las cuentas del ex trabajador y cambiar las contraseñas de acceso al sistema, cuanto más rápido mejor.

Nombre de los usuarios

Los nombres de los usuarios se pueden deducir fácilmente dentro de una organización porque a menudo se encuentran normalizados bajo algún criterio (por ejemplo, el usuario Pedro Juan podría tener el nombre de usuario *pjuan*).

- ***Hackers*** (**intrusos informáticos**): estas personas llevarán a cabo normalmente ataques pasivos orientados a obtener información confidencial (por ejemplo, un examen de un curso universitario), o simplemente con la finalidad de ponerse a prueba para obtener el control del sistema atacado. Además, si el atacante es lo bastante hábil, incluso podría borrar las huellas de sus acciones en los ficheros que las registran (llamados genéricamente ficheros log). Como este tipo de acciones no producen ningún efecto

Ved también

En el apartado 3, describiremos algunas de las técnicas que pueden utilizar los intrusos para llevar a cabo sus acciones.

"visible", no son fácilmente detectables. Los intrusos suelen aprovechar la vulnerabilidad conocida de sistemas operativos y software para conseguir el control de todo el sistema informático. Para llevar a cabo este tipo de acciones basta con ejecutar diversos software que se pueden obtener en Internet y que automatizan los ataques a los sistemas informáticos sin que el intruso necesite disponer de muchos conocimientos técnicos.

Además de las herramientas que hemos mencionado, los intrusos disponen de otras técnicas más sencillas (al menos desde el punto de vista informático), pero igual de efectivas. Por ejemplo, puede resultar muy productivo hacer una sencilla búsqueda de contraseñas escritas en papeles entre la basura contenida en una papelera (*trashing*), o de una manera más ingeniosa el intruso podría suplantar la identidad de otra persona para averiguar la contraseña (*mascarada*). Asimismo, un intruso que quisiera obtener una contraseña en un sistema determinado, podría llamar por teléfono al administrador, hacerse pasar por otra persona y pedir la contraseña con la excusa de que la ha olvidado o perdido. En un exceso de buena fe, el administrador podría cambiar la contraseña y entregar la nueva al intruso en la misma comunicación telefónica. Las variantes de este tipo de ataques son múltiples y muchas se incluyen dentro de lo que se denomina *ingeniería social*, es decir, la manipulación de las personas a fin de que hagan determinadas acciones que en realidad no quieren hacer.

Otras finalidades ilícitas

Otras finalidades ilícitas que hay que considerar: utilización del sistema atacado como servidor de copias no autorizadas de software o como trampolín para atacar otras máquinas.

Delito de daños

Las acciones de los intrusos (*hackers*) pueden ser constitutivas de delito de daños –entre otros– y pueden implicar responsabilidades civiles y penales.

- **Intrusos remunerados**: a pesar de no ser un tipo de ataque muy frecuente, también vale la pena tenerlo en cuenta. En este caso, los intrusos se encuentran perfectamente organizados (incluso pueden estar en diferentes localizaciones geográficas) y atacan de una manera conjunta el sistema de una organización determinada. Disponen de muchos medios técnicos y reciben remuneraciones muy elevadas de la organización rival que dirige el ataque, a menudo con el ánimo de acceder a información confidencial (un nuevo diseño, un nuevo software, etc.) o bien con la intención de provocar un daño importante en la imagen de la organización atacada.

1.3. Mecanismos de seguridad

La seguridad global de un sistema informático depende, en gran medida, del diseño esmerado de las siguientes medidas:

- **Medidas de prevención**: aumentan la seguridad del sistema durante su funcionamiento.
- **Medidas de detección**: se utilizan para detectar violaciones de la seguridad de un sistema.
- **Medidas de recuperación**: permiten la recuperación del funcionamiento correcto del sistema una vez se ha producido el ataque.

Ejemplos de medidas de prevención, detección y recuperación

Algunos ejemplos de medidas de seguridad son:

1) Medidas de prevención: el uso de cortafuegos para evitar a los intrusos.
2) Medidas de detección: uso de la herramienta de seguridad e integridad de datos *Tripwire*.
3) Medidas de recuperación: además de los mecanismos de copia de seguridad, también entra dentro de esta categoría el software de análisis forense (como la herramienta *Encase*, por ejemplo), los cuales permiten averiguar cuál ha sido la puerta de entrada al sistema y también las actividades que ha llevado a cabo el intruso.

Dado que el desarrollo en profundidad de estos tres puntos no es posible por motivos obvios de espacio, en este módulo nos limitaremos a exponer los problemas básicos que comporta la administración de un sistema con respecto a la prevención y detección de violaciones de la seguridad.

Ved también

Ved los planes de contingencia y de análisis de riesgos en el módulo "El sistema informático dentro de la organización".

En caso de caída del sistema nos puede ser útil tener en consideración el protocolo de actuación siguiente:

1) Desconexión del equipo atacado de la red. Con esta acción, evitamos que el intruso cause más daños y que pueda eliminar (si todavía no lo ha hecho) las huellas de sus acciones.

2) Hacer una copia de seguridad a bajo nivel que se utilizará posteriormente para analizar el ataque.

3) Analizar y compilar toda la información posible sobre el ataque: log, software instalado por el atacante (troyanos, por ejemplo), puerta de entrada que ha utilizado, etc.

4) Restaurar el sistema y aplicar las actualizaciones del software instalado (o *patch*) para solucionar la vulnerabilidad de la que se ha servido el atacante para introducirse en el sistema. Además, hay que notificar el ataque a los usuarios con la finalidad de que cambien las contraseñas de las cuentas lo antes posible.

Dirección recomendada

Hay muchas listas de correo de seguridad que aportan información de vulnerabilidad y actualizaciones diariamente. Por ejemplo, http://www.hispasec.com.

5) Si se detecta que la máquina ha sido utilizada como trampolín para atacar otras máquinas, hay que avisar a los responsables de estos sistemas. También hay que notificar el ataque al jefe de la organización del sistema atacado y, en caso de que se considere necesario, denunciarlo a la policía (todos los cuerpos policíacos del Estado disponen de unidades especializadas en este tipo de delito) y notificarlo al Computer Emergency Response Team (CERT). Finalmente, también es posible solicitar informes periciales a los colegios de ingenieros informáticos y a empresas especializadas del sector.

El CERT es un equipo de respuesta a los incidentes de seguridad de los sistemas informáticos. Cada país dispone de su propio CERT, el cual ofrece servicios de asistencia técnica, análisis y documentación sobre los incidentes de seguridad que se producen.

Dirección recomendada

Podéis acceder al IRIS-CERT en la dirección http://www.rediris.es/cert.

2. Seguridad del entorno

En este apartado, veremos algunas medidas de protección física que se pueden utilizar para evitar los accesos no autorizados a los sistemas informáticos. Una organización puede invertir mucho dinero en software que evite y detecte los accesos ilícitos a sus sistemas, pero toda esta inversión no servirá de nada si los recursos físicos del sistema se encuentran al alcance de todo el mundo.

El hardware suele ser el elemento más caro de un sistema informático y, por lo tanto, hay que tener especial cuidado con las personas que tienen acceso material a él. Una persona no autorizada que accediera al sistema podría causar enormes pérdidas: robo de ordenadores, introducción de software malicioso en el servidor (por ejemplo, un troyano o un *keylogger*), destrucción de datos, etc.

Para evitar este problema, hay diversas medidas de prevención como, por ejemplo, las siguientes:

- Mantener los servidores y todos los elementos centrales del sistema en una zona de acceso físico restringido.
- Mantener los dispositivos de almacenamiento en un lugar diferente del resto del hardware.
- Llevar a cabo inventarios o registros de todos los elementos del sistema informático (útil en casos de robo).
- Proteger y aislar el cableado de la red (tanto para protegerlo de daños físicos como del espionaje).
- Instalación de cámaras de videovigilancia.
- Utilización de contraseñas en los protectores de pantalla.
- Utilización de contraseñas de BIOS.
- Desactivar las opciones de autocompletar y recordar contraseñas de los navegadores de Internet.
- Escoger una topología de red adecuada a nuestras necesidades de seguridad.
- Garantizar la seguridad del hardware de red (encaminadores, conectores, concentradores y módems).
- Mecanismos de autenticación de los usuarios que quieren acceder al sistema.

Ved también

Ved las políticas de copias de seguridad en el módulo "Administración de servidores".

Ved también

Sobre la topología de red segura y sobre la seguridad del hardware de red, ved el módulo "Administración de la red".

Se llamada **autenticación** al proceso de verificación de la identidad de una persona o de un proceso que quiere acceder a los recursos de un sistema informático.

Mecanismos de autenticación hay de muchos tipos diferentes, desde los más baratos y sencillos (por ejemplo, un nombre de usuario y una contraseña) hasta los más caros y complejos (por ejemplo, un analizador de retina). Como siempre, según los objetivos y el presupuesto de la organización, hay que escoger el que más se ajuste a nuestras necesidades. También hay que tener en cuenta que muchos de estos mecanismos son complementarios y se pueden utilizar al mismo tiempo.

Situación de un mecanismo de autenticación

Hay diversos niveles en los cuales situar un mecanismo de autenticación:

- Instalado en la BIOS.
- Instalado en el sector de arranque del equipo.
- Solicitado por el sistema operativo.
- Solicitado por un software.

2.1. Mecanismos de autenticación de usuarios

Hay diversos mecanismos de autenticación de usuarios. Los podemos clasificar de la siguiente manera:

1) Sistemas basados en elementos conocidos por el usuario

El principal mecanismo dentro de estos tipos de autenticación son los sistemas basados en **contraseñas**. Es uno de los métodos que se utilizan más a menudo para autenticar un usuario que quiere acceder a un sistema. Obviamente es el método más barato, pero también es el más vulnerable, ya que aunque la palabra de paso o contraseña tendría que ser personal e intransferible, a menudo acaba en poder de personas no autorizadas. Por otra parte, aunque las contraseñas se almacenen cifradas en un fichero, es posible descifrarlas con múltiples técnicas (por ejemplo, un ataque de diccionario).

Aunque la asignación de las contraseñas a los usuarios se basa en el sentido común, cabe recordar los aspectos siguientes:

- Memorizarla y no llevarla escrita.
- Cambiarla periódicamente (con carácter mensual, por ejemplo).
- No repetir la misma contraseña en cuentas diferentes.
- Evitar introducirla en presencia de otras personas.
- No tirar documentos con contraseñas a la papelera.
- Evitar utilizar palabras de diccionario.
- Evitar utilizar datos que pueden ser conocidos por otras personas (por ejemplo, nombre y apellido del usuario, *login*, DNI, número de teléfono móvil, etc.).
- Utilizar contraseñas de un mínimo de ocho caracteres.
- Evitar la reutilización de contraseñas antiguas.
- No utilizar contraseñas exclusivamente numéricas.
- Favorecer la aparición de caracteres especiales (¡, *, ¿, etc.).
- No utilizar secuencias de teclado del tipo “qwerty”.
- Utilizar mnemotécnicos para recordar la contraseña.

Ved también

Sobre el uso de diccionarios en los ataques a contraseña, ved el subapartado 3.2 de este módulo.

Aunque como usuarios de un sistema informático pensamos que no es necesario tomar precauciones con nuestra contraseña porque no almacenamos ninguna información importante en el sistema, vale la pena detenerse a pensar que una persona lo bastante hábil podría obtener el control de todo el sistema a partir de la obtención de una cuenta sin ningún privilegio especial.

A modo de ejemplo, según Eugene H. Spafford en su artículo "Observing Reusable Password Choices", publicado a principios de los años noventa, el 30% de las cuentas de los sistemas Unix de la muestra analizada tenían contraseñas que se podían descifrar en sólo unos minutos de tiempo de CPU[1]. Teniendo en cuenta que los ordenadores actuales son mucho más rápidos, si la política de asignación de contraseñas (y la educación de los usuarios en su uso) no ha variado, el problema se habrá agravado todavía más.

(1)CPU es la sigla de la expresión inglesa correspondiente a *unidad de control de proceso*.

Lectura complementaria

Eugene H. Spafford. "Observing Reusable Password Choices". En: *Usenix Security III Proceedings* (págs. 299-312).

2) Sistemas basados en elementos que posee el usuario

A diferencia de los métodos anteriores, estos sistemas no se basan en lo que conoce el usuario, sino en lo que posee. Podemos distinguir:

a) Sistemas basados en tarjetas inteligentes y *tokens* de seguridad

Una tarjeta inteligente[2] es similar a una tarjeta de crédito, pero a diferencia de ésta las tarjetas inteligentes alojan un microprocesador (y memoria) que las dota de las características siguientes:

(2)En inglés, *smartcard*.

- Capacidad para hacer cálculos criptográficos sobre la información que almacenan (algoritmos DES, Triple DES, DSS, RSA, etc.).
- Almacenaje cifrado de la información.
- Protección física y lógica (clave de acceso) a la información almacenada.
- Capacidad para almacenar claves de firma y cifrado.

Ved también

Los algoritmos DES, Triple DES, DSS, RSA se describen en el subapartado 2.2 de este módulo.

Ved también

Sobre las claves de firma y cifrado, ved el subapartado 2.2 de este mismo módulo.

Es un método de autenticación que cada vez utilizan más las organizaciones, a pesar del coste de adaptación de la infraestructura a los dispositivos que permiten la lectura de las tarjetas.

Además, las tarjetas pueden ser de contacto (es decir, tienen que ser insertadas en la ranura de un lector para que puedan ser leídas), o sin contacto. Por ejemplo, este segundo tipo se ha empezado a utilizar con éxito en diversos países como sistema de pago en el transporte público.

Otra solución para resolver el problema de la autenticación, bastante popular en el sector empresarial, consiste en el llamado *token* de seguridad. Suelen ser dispositivos físicos de tamaño reducido (algunos incluyen un teclado para in-

troducir un PIN), similares a un llavero, que calculan contraseñas de un único uso (cambian con cada *login* o cada cierto tiempo). Pueden almacenar claves criptográficas, como por ejemplo, la firma digital o medidas biométricas.

b) Sistemas biométricos

Los sistemas biométricos se basan en las características físicas del usuario que se tiene que autenticar (o en patrones característicos que puedan ser reconocidos como, por ejemplo, la firma). Como principal ventaja, el usuario no tiene que recordar ninguna contraseña ni hace falta que lleve ninguna tarjeta encima. Suelen ser mucho más caros que los métodos anteriores, motivo por el cual todavía no se utilizan mucho, aunque algunos de estos métodos ofrecen un alto nivel de seguridad (por ejemplo, el reconocimiento dactilar). Entre las diferentes características que se pueden utilizar para reconocer a un usuario mediante medidas biométricas, destacamos los siguientes:

Seguridad de los sistemas biométricos

Aunque aparentemente estos sistemas son muy difíciles de falsificar, hay que ver los trabajos realizados por el Netherlands Forensics Institute, sobre la seguridad real que presentan los sistemas biométricos.

- Voz.
- Olor corporal.
- Escritura.
- Huellas dactilares (probablemente es el método más utilizado y de menos coste).
- Patrones de la retina o del iris.
- Geometría de la mano.
- Trazado de las venas.
- Estructura facial.

Ved también

Ved, en el apartado 4 de este módulo, cómo se tiene que hacer el almacenamiento de los datos personales.

2.2. Protección de los datos

Para evitar los ataques contra la confidencialidad y las técnicas de espionaje se pueden utilizar diversos métodos criptográficos. A continuación definiremos los criptosistemas de clave privada y clave pública, las funciones resumen y la firma digital, y estudiaremos las implicaciones que pueden tener estos elementos en la seguridad global del sistema informático.

Ved también

Sobre técnicas de espionaje, ved el subapartado 1.2 de este módulo.

Una *cifra* o *criptosistema* es un método secreto de escritura, mediante el cual un texto en claro se transforma en un texto cifrado o **criptograma**. El proceso de transformar un texto en claro en texto cifrado se nombra **cifrado**, y el proceso inverso, es decir, la transformación del texto cifrado en texto en claro, se llama **descifrado**. Tanto el cifrado como el descifrado son controlados por una o más **claves criptográficas**.

Se llama **criptografía**[3] a la ciencia y estudio de la escritura secreta. Junto con el **criptoanálisis** (técnica que tiene como objetivo averiguar la clave de un criptograma a partir del texto en claro y del texto cifrado), forman lo que se conoce con el nombre de **criptología**.

(3)La palabra *criptografía* proviene de las palabras griegas *krypto* (oculto) y *graphia* (escritura).

Para proteger la confidencialidad de los datos (almacenados o circulando por la red), pueden usarse criptosistemas de clave privada (simétricos) o de clave pública (asimétricos).

2.2.1. Criptosistemas de clave privada

Los **criptosistemas de clave compartida** son criptosistemas en los cuales el emisor y el receptor comparten una única clave. Es decir, el receptor podrá descifrar el mensaje recibido sólo si conoce la clave con la cual el emisor ha cifrado el mensaje.

El algoritmo más representativo de los criptosistemas de clave privada es el *Data Encryption Standard* (DES), de 1977. Este algoritmo cifra la información en bloques de 64 bits de longitud utilizando claves de 56 bits. Actualmente se encuentra en desuso, ya que no es seguro. En lugar del DES se utiliza una variante llamada Triple DES, u otros algoritmos como, por ejemplo, IDEA, CAST, Blowfish, etc. No obstante, el actual estándar (desde el año 2002), adoptado como tal por el Gobierno estadounidense, es el llamado *Advanced Encryption Standard* (AES), representado por el algoritmo *Rijndael*. Las especificaciones del AES (que no coinciden exactamente con su representante, el algoritmo *Rijndael*), determinan un tamaño de bloque fijo de 128 bits y medidas de clave de 128, 192 o 256 bits. A continuación veremos un criptosistema verdaderamente ingenioso y conceptualmente muy elegante.

2.2.2. Criptosistemas de clave pública

La criptografía de clave pública fue introducida por Diffie y Hellman en 1976.

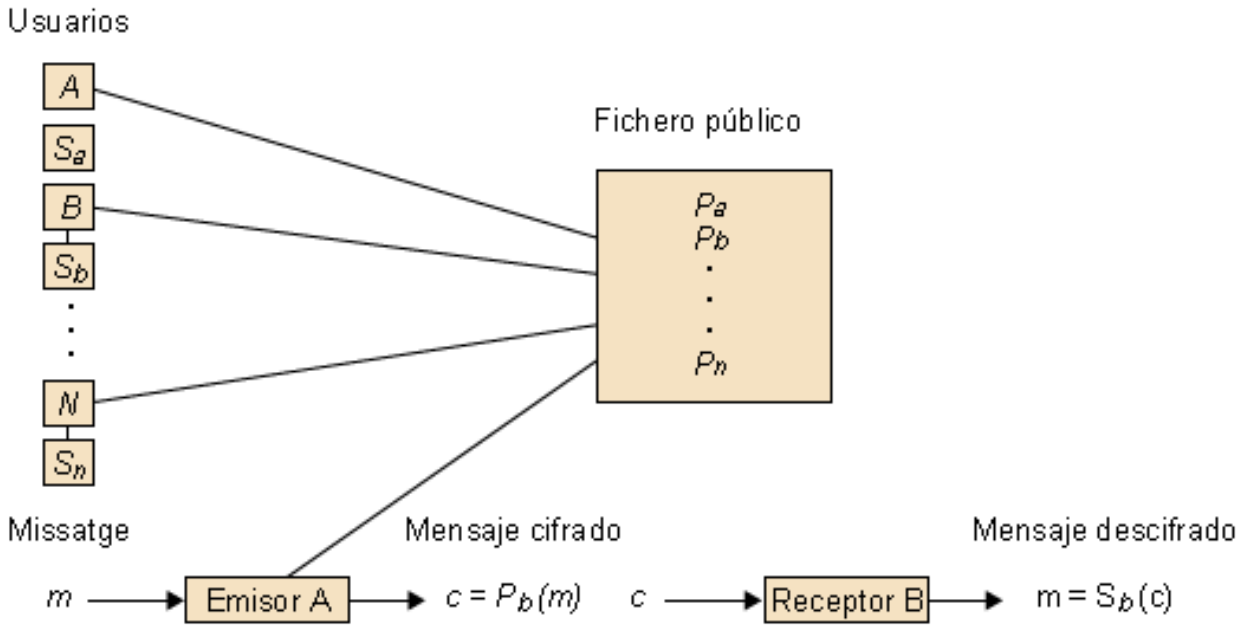
Los **criptosistemas de clave pública** son un tipo de criptosistemas donde cada usuario u tiene asociada una pareja de claves $<P_u, S_u>$. La clave pública, P_u, es accesible para todos los usuarios de la red y aparece en un directorio público, mientras que la clave privada, S_u, tan sólo es conocida por el usuario u.

Observación

Dada cualquier clave del par $<P_u, S_u>$, no es posible averiguar una a partir de la otra.

Cuando un usuario *A* quiere enviar un mensaje a un usuario *B*, cifra el mensaje utilizando la clave pública como *B* (recordemos que esta clave es accesible por todo el mundo). Cuando el receptor reciba el mensaje, únicamente lo podrá descifrar utilizando su clave privada (la cual se encuentra exclusivamente en su poder).

Cifraje de un mensaje en un criptosistema de clave pública



El criptosistema de clave pública más conocido es el llamado RSA[4], pero hay otros como, por ejemplo, el criptosistema *Digital Signature Algorithm* (DSA). Estos tipos de criptosistemas se basan en funciones matemáticas unidireccionales (no utilizan sustituciones o transposiciones) y son lentos si se comparan con los de clave privada, motivo por el cual se suelen utilizar para intercambiar claves simétricas en los protocolos de comunicación, pero no para cifrar información.

Una ventaja muy importante de este tipo de criptosistema es que permite la incorporación de **firma digital**. Cada usuario podrá firmar digitalmente su mensaje con su clave privada, y esta firma podrá ser verificada más tarde de manera que el usuario que lo ha originado no pueda negar que se ha producido (propiedad de *no repudio*).

Para poder explicar el mecanismo de firma digital habrá que definir previamente el concepto de función *hash*.

[4]El criptosistema RSA fue ideado en 1978 por Rivest, Shamir y Adleman.

DSS

El *Digital Signature Standard* (DSS) es un sistema de firma digital adoptado como estándar por el NIST. Utiliza la función resumen SHA y el algoritmo DSA.

Ved también

Como veremos en el subapartado 4.2.3, la firma digital tiene jurídicamente la misma validez que la convencional.

Una función ***hash*** (o **función resumen**) es una función matemática que hace corresponder una representación de medida fija a un mensaje *m* de medida variable. Esta representación tiene de 128 a 160 bits (los nuevos algoritmos pueden llegar a los 256, 384 y 512 bits) y se llama *valor resumen del mensaje*.

Por ejemplo, lo que se puede ver a continuación es el resultado de aplicar una función resumen a un fichero llamado MD5.TXT:

```
MD5.txt 89736DF30DC47A7D5AC22662DC3B5E9C
```

Las funciones resumen tienen que ser unidireccionales.

Una función resumen o función *hash* (*H*) es **unidireccional** si para cualquier mensaje *m*' del recorrido de H es "difícil" (desde el punto de vista computacional) encontrar a *m* tal que *m*' = *H* (*m*).

Papel de las funciones resumen

Las funciones resumen o funciones *hash* tienen un papel muy importante en la verificación de la integridad del sistema (detección de troyanos, virus, etc.).

El software P2P, por ejemplo, usa funciones *hash* a efectos de identificación de los archivos compartidos entre los diferentes usuarios de la red.

Los algoritmos **MD5**[5] y **SHA-1**[6] son los que se más utilizan para implementar las funciones resumen. Además de los algoritmos SHA-0 (el precursor) y SHA-1, hay diversas variantes (SHA-224, SHA-256, SHA-384 y SHA-512), todos ellos identificados como SHA-2. En la actualidad, todavía no se ha podido encontrar ningún ataque efectivo sobre el algoritmo SHA-1, aunque se han publicado resultados comprometidos sobre funciones similares a SHA-1.

(5)MD5 es la sigla de *message digest*.

(6)SHA-1 es la sigla de *secure hash algorithm*.

Origen de los algoritmos MD5 y SHA-1

El algoritmo MD5 fue desarrollado por Ron Rivest y con resúmenes de 128 bits. Está cuestionado desde el año 2004.

El algoritmo SHA-1 fue desarrollado por la Agencia de Seguridad Norteamericana y con resúmenes de 160 bits.

A continuación, describiremos el funcionamiento del protocolo de firma digital con funciones resumen. Supongamos que el usuario *A* quiere firmar el mensaje *m* y enviarlo al usuario *B*.

1) El usuario *A* calcula el resumen de *m*.

2) A continuación, el usuario *A* firma el resumen, *m*, con su clave privada y obtiene *s*. El usuario *B* recibirá el mensaje *m* y el resumen firmado *s*. Cuando el usuario *B* quisiera verificar el origen del mensaje recibido, haría las acciones siguientes.

3) El usuario *B* calcula el resumen de *m*.

4) A continuación, el usuario *B* descifra el resumen firmado, *s*, utilizando la clave pública del usuario *A*. Si este valor coincide con el calculado en el paso 3, entonces *s* es una firma digital válida para el valor resumen de *m*.

Certificado digital

A la hora de utilizar la clave pública de un usuario, ¿cómo podemos saber que es auténtica? Para resolver este problema, se requiere la participación de una tercera parte (llamada

autoridad de certificación) que confirme la autenticidad de la clave pública de un usuario con la expedición de un certificado digital.

La herramienta criptográfica PGP

El software *Pretty Good Privacy* (PGP) fue desarrollado por Phil Zimmermann en 1991 y, en la actualidad, todavía es una de las herramientas que más se utilizan mundialmente para preservar la confidencialidad de la información y firmar las comunicaciones que se han hecho por correo electrónico, a pesar de las sospechas que han originado sus presuntas *backdoors*.

Backdoors

Las *backdoors* son puertas de entrada a sistemas operativos y software, insertadas por los propios diseñadores o programadores, que les permiten acceder a la aplicación evitando todos los mecanismos de autenticación.

PGP[7] es un software híbrido que utiliza tanto técnicas de criptografía de clave privada como de clave pública. Además de gestionar las claves y permitir diversos algoritmos de cifrado, también permite el borrado seguro de ficheros.

(7)PGP son las siglas que identifican el tipo de software *pretty good privacy*.

Un rasgo esencial que convirtió el PGP en una herramienta muy atractiva para todo el mundo es que su código fuente era de libre distribución (hasta la versión 6.5.8), motivo por el cual Zimmermann sufrió serios problemas con los servicios secretos norteamericanos, ya que en Estados Unidos la exportación de herramientas criptográficas era considerada una práctica similar al contrabando de armas. La venta del PGP a una empresa norteamericana, y la dificultad para acceder a su código fuente, han provocado que sus usuarios sospecharan de la existencia de puertas traseras o *backdoors* (aunque Zimmerman afirma que la versión 7.0.3 se desarrolló bajo su supervisión y no tiene puertas traseras). Por este motivo, el año 1999 apareció un nuevo software, *Gnu Privacy Guard* (GnuPG), obra del alemán Werner Koch y que, como su nombre indica, es un programa libre bajo licencia GNU, el cual desarrolla los estándares de implementación del OpenPGP.

Observación

Un usuario puede firmar digitalmente los ficheros que contiene su propio disco duro para evitar que sean modificados sin su consentimiento.

Direcciones recomendadas

Podéis obtener el software PGP y GnuPGP en las web respectivas de estas organizaciones.

Esteganografía

Se llama *esteganografía*[8] el conjunto de técnicas que permiten ocultar o esconder cualquier tipo de datos. A diferencia de la criptografía, la esteganografía esconde los datos entre otros datos, aunque no los modifica de manera que no sean legibles.

(8)Esteganografía proviene de la palabra griega *stegos* (cubierta), y literalmente significa 'escritura oculta'.

A modo de ejemplo, mediante el uso de técnicas esteganográficas, un fichero de una imagen digitalizada podría ocultar en su interior un fichero de texto con todas las contraseñas de los usuarios de un sistema informático. Desde el punto de vista del usuario que examina la imagen, no se podría apreciar ninguna diferencia entre la imagen original y la imagen que oculta los datos confidenciales; los dos ficheros tendrían el mismo tamaño incluso.

En general, cualquier fichero, tanto si es una imagen como un documento o incluso un fichero de sonido, es susceptible de esconder algún tipo de información. Aunque las diferencias entre el fichero original y el fichero *esteganografiado* sean prácticamente inapreciables, obviamente existen. Una de las técnicas que se pueden utilizar para ocultar información en un fichero consiste en alterar los bits menos significativos del fichero original, de manera que en estas alteraciones se almacene precisamente la información que se quiere ocultar. El tamaño del fichero *esteganografiado* será exactamente el mismo que el del fichero original, aunque el contenido será ligeramente e inapreciablemente *diferente*.

S-TOOLS

Podéis buscar en Internet el software S-TOOLS para hacer pruebas esteganográficas.

No hay ningún tipo de duda de que si la criptografía puede tener usos delictivos, de la esteganografía se puede hacer un uso aún más ilegítimo. Si se localiza un fichero cifrado, se puede creer que se esconde alguna cosa confidencial (aunque descifrarlo sea muy complejo o casi imposible), pero en el caso de la esteganografía, el análisis superficial de los datos ni siquiera puede llegar a crear sospechas de que algún fichero contenga información relevante. Una técnica que se puede utilizar para localizar ficheros que contengan información oculta consiste en la comparación de los valores resumen de los ficheros sospechosos con los valores resumen de los ficheros originales. Por ejemplo, en el caso de que los ficheros sospechosos sean ficheros de sistema operativo, es relativamente sencillo obtener los valores resumen de los ficheros originales del sistema, los cuales se compararán posteriormente con los valores resumen de los ficheros sospechosos para determinar si han sido tratados con técnicas esteganográficas.

Observación

La esteganografía es una técnica de detección similar a la que se utiliza para detectar los problemas de integridad de los ficheros de un sistema informático.

3. Seguridad del sistema

El objetivo de este módulo se centrará en el estudio de las intrusiones y ataques de los que puede ser objeto un sistema informático. Algunas de las técnicas descritas pueden parecer obsoletas, pero a nuestro parecer son didácticamente interesantes y pueden servir de fundamento para comprender procesos más complejos. Asimismo, muchos de los sistemas actuales todavía funcionan con sistemas operativos antiguos, o con sistemas no actualizados que, muy probablemente, son susceptibles de sufrir muchos de los problemas que se describirán acto seguido.

Las fases o etapas de las que suele constar una intrusión son las siguientes:

1) Etapa previa al ataque: recogida de información.
2) Ataque inicial.
3) Acceso completo al sistema.
4) Instalación de *backdoors*, *key loggers*, troyanos, etc. para obtener información y facilitar futuros accesos del atacante.
5) Eliminación de huellas.

Hay muchísimos sistemas informáticos que una vez instalados ya no se actualizan más, muchas veces por miedo a que dejen de funcionar correctamente o simplemente por desconocimiento. Es muy importante hacer las actualizaciones del sistema. En los casos con sistemas complejos donde se pueden tener problemas de compatibilidades con otros equipos, o con software ya instalado, es conveniente disponer de un equipo de reserva idéntico al de producción donde poder hacer las actualizaciones a modo de prueba.

Los procedimientos y herramientas que se estudiarán en este módulo se pueden utilizar para prevenir y detectar las intrusiones en un sistema informático, si bien también pueden ser utilizadas maliciosamente para producir el efecto contrario.

3.1. Seguridad en el sistema de ficheros

En este subapartado consideraremos que la administración de usuarios, grupos y sus privilegios, y también la de ficheros y directorios, se ha hecho correctamente. Aunque tampoco hablaremos a fondo, también hay que tener

[9]ACL son las siglas de *access control lists*.

en cuenta las listas de control de acceso (ACL[9]). Mediante las ACL es posible la asignación de permisos a usuarios o grupos concretos. Esto puede ser útil en caso de que dos usuarios que pertenecen a grupos diferentes necesiten los mismos permisos a la hora de acceder a unos determinados directorios.

Ved también

Ved los módulos "Administración de servidores" y "Administración de usuarios".

Ejemplo de listas de control de acceso

En un proyecto interdisciplinario entre profesores del departamento de informática y el de filosofía (los dos grupos de usuarios con perfiles perfectamente definidos dentro de cada departamento), se podría requerir que los componentes del proyecto tuvieran que acceder a los mismos directorios, necesidad que se podría satisfacer con la creación del ACL correspondiente.

3.2. Ataques a contraseña

A pesar de la existencia de muchos mecanismos de autenticación, lo cierto es que hoy en día la vía de entrada más común para acceder a un sistema informático es el uso del nombre de usuario acompañado de la correspondiente contraseña. En consecuencia, la política de gestión y mantenimiento de contraseñas es vital para garantizar la seguridad del sistema.

En este subapartado, estudiaremos con cierto detalle el fichero de contraseñas de sistemas Unix/Linux. A pesar de su especificidad, muchos de los conceptos que aparecen en este subapartado son fácilmente extrapolables a otros sistemas operativos y útiles para comprender cómo funcionan los ataques a contraseña.

3.2.1. El fichero */etc/passwd* en Unix/Linux

La finalidad de este tipo de ataque consiste en averiguar o descifrar, borrar, modificar o insertar contraseñas en el fichero que las almacena. En los sistemas Unix, cada nombre de usuario (*login name*) tiene una entrada, junto con la contraseña cifrada respectiva, en el fichero */etc/passwd*. Para el buen funcionamiento del sistema, este fichero tiene que tener permisos de lectura para todos los usuarios.

Observación

El fichero */etc/passwd* también contiene cuentas de usuarios *no reales*, relativas a diversos servicios del sistema. Hay que eliminar las que no se tienen que utilizar.

Las entradas del fichero */etc/passwd* tienen el formato que se puede ver en el ejemplo siguiente (el símbolo ":" actúa de elemento separador entre los diferentes campos):

```
Pedro:HGY89fgf801we:UID:GID:información de usuario:directorio de trabajo del usuario:shell por
defecto del usuario
```

Los campos que nos interesan son, básicamente, el primer campo (nombre de *login* del usuario), y el segundo, la contraseña cifrada del usuario. Los campos UID y GID representan, respectivamente, el identificador (único) del usuario y el identificador del grupo del usuario.

Cuando un usuario entra en el sistema, la contraseña del fichero */etc/passwd* no se descifra (ya que el algoritmo de cifrado es unidireccional), sino que se cifra la contraseña introducida por el usuario utilizando el mismo algoritmo de cifrado simétrico y se compara con la contraseña cifrada del fichero */etc/passwd*. En caso de que coincidan, el usuario estará autorizado a entrar. Visto el carácter unidireccional del algoritmo de cifrado, la manera más evidente de romper las contraseñas del fichero */etc/passwd* será el uso de técnicas de fuerza bruta (explorando todo el árbol de posibilidades y, por lo tanto, en general muy lento). Además, sin embargo, también se pueden utilizar los llamados **ataques de diccionario**.

Ataques de fuerza bruta

Las contraseñas de longitud corta pueden ser descifradas rápidamente con ataques de fuerza bruta.

Como ya se ha mencionado anteriormente, el fichero */etc/passwd* tiene que permanecer con permisos de lectura para todos los usuarios, de manera que resulta relativamente sencillo visualizar u obtener el contenido del fichero */etc/passwd*, localmente o remotamente. Una vez se dispone de este fichero, se podrá averiguar las contraseñas, simplemente cifrando todas las palabras contenidas en un fichero de diccionario (se llaman de esta manera los ficheros ASCII que contienen muchas palabras de un idioma determinado o de un tema concreto: deportes, música, etc.) y comparando el resultado con las contraseñas cifradas del fichero */etc/passwd*. Si alguna de las contraseñas cifradas coincide con el resultado de cifrar una palabra del diccionario, habremos obtenido una clave de acceso al sistema de una manera no autorizada.

En realidad, el proceso de cifrar todas las palabras de un diccionario es más complejo de lo que se ha explicado, ya que no hay un único cifrado para cada palabra. A la hora de cifrar una palabra (es decir, en el momento en que se creó o bien se cambió la contraseña), hace falta tener en cuenta 12 bits (llamados *salt* en inglés) que proporcionan 4.096 codificaciones diferentes para cada palabra (el valor del rango de 0 a 4.095 se escoge según la hora del sistema).

Así pues, cada palabra del diccionario tendrá que ser codificada 4.096 veces para asegurar que no nos dejamos ninguna posibilidad por explorar. Cabe decir, sin embargo, que la presencia de los bits de *salt* no dificulta (computacionalmente no representa un coste insalvable) la ruptura de las contraseñas, pero permite que dos usuarios que tengan la misma contraseña aparezcan cifrados de una manera diferente en el fichero */etc/passwd*.

La creación de contraseñas fuertes dificulta en gran manera los ataques basados en el uso de diccionarios. En este sentido, el administrador dispone de diversas herramientas que permiten comprobar la calidad de las contraseñas de los usuarios del sistema. Por ejemplo, las aplicaciones *npasswd* o *passwd+* (entre otras) permiten la llamada *comprobación proactiva de contraseñas*, la cual

Ved también

Recordad que, en el subapartado 2.1, hemos visto algunas recomendaciones para la creación de contraseñas.

permitirá eliminar las contraseñas que, según una serie de criterios, sean consideradas débiles. Así pues, en caso de que un usuario escoja una contraseña que no satisfaga estos criterios, se verá obligado a escoger otra.

Rechazo de contraseñas

Se pueden rechazar, por ejemplo, las contraseñas que:

- No tengan como mínimo un cierto número de caracteres.
- Las que se basen en datos conocidos del usuario o de la organización (tanto si están al derecho como al revés).
- Las que no mezclen minúsculas y mayúsculas.
- Las formadas por palabras de diccionarios, etc.

Además, el administrador también puede ejecutar con una cierta periodicidad (y con la autorización para hacerlo), herramientas como *Crack* o *John the Ripper* para hacer ataques de diccionario sobre el mismo fichero de contraseñas y poder comprobar de esta manera la robustez. Estas herramientas automatizan el procedimiento de ataque basado en diccionarios e incluso permiten llevar a cabo ataques de fuerza bruta, efectivos cuando las contraseñas tienen un número de caracteres muy reducido.

3.2.2. Ocultación de contraseñas en Unix: el fichero */etc/shadow*

Mediante la técnica de ocultación de contraseñas[10], las contraseñas cifradas que antes se podían localizar en el fichero */etc/passwd* (con permiso de lectura para todos los usuarios), ahora pasan a localizarse en el fichero */etc/shadow*, el cual podrá ser leído únicamente por el usuario *root*. Las entradas del fichero de contraseñas */etc/passwd* son idénticas a las que hemos visto anteriormente, con la excepción de que ahora el campo de la contraseña contendrá un símbolo (generalmente una x) que indicará la localización de la contraseña en el fichero */etc/shadow* en los programas que lo requieran:

(10)La técnica de ocultación de contraseñas recibe en inglés el nombre de *shadowing*.

```
Pedro:<b>x</b>:500:100:Pedro Juan:/export/home:/bin/bash
```

Además, cada usuario tendrá una entrada en el fichero */etc/shadow* que contendrá el nombre de usuario, la contraseña cifrada y una serie de campos que sirven para implementar mecanismos de envejecimiento de contraseñas (*agin password*), los cuales no se detallarán, ya que exceden los propósitos de estos materiales:

```
Pedro:<b>HGY89fgf801we</b>:120078:0::7:10::
```

En la actualidad, en muchas distribuciones de Linux la opción de *shadowing* se encuentra activada por defecto y a veces ni siquiera se puede desactivar.

3.3. Código malicioso y amenazas lógicas

Se llama *código malicioso*[11] a cualquier fichero que pueda resultar pernicioso por un sistema informático.

(11)En inglés, *malware*.

Algunas veces, el código malicioso se puede insertar dentro de un programa "autorizado". El código malicioso también puede estar oculto y provocar todo tipo de daños como, por ejemplo, el borrado de datos o el envío de información confidencial del usuario por correo electrónico. En otras ocasiones, el

código malicioso no se inserta dentro de un programa autorizado, sino que aparece como un nuevo software que desarrolla alguna función útil. El usuario lo ejecuta con una finalidad y el programa, en virtud del código malicioso que contiene, lleva a cabo acciones desconocidas por el usuario.

El código malicioso, en todas sus múltiples variantes, se puede encuadrar dentro de lo que se llaman *amenazas lógicas* (de las cuales, los virus y los troyanos son los elementos más representativos):

- **Software incorrecto**. Consiste en el aprovechamiento de vulnerabilidad accidental del software (errores de programación) con finalidades destructivas. Dicho de otra manera, consiste en utilizar el software con un objetivo diferente del objetivo con que fue concebido. Esta vulnerabilidad recibe el nombre genérico de errores[12] y el software que se utiliza para aprovecharlos se llama *exploit*. Para evitar este tipo de problema, es fundamental estar al día de todos los agujeros de seguridad que presenta nuestro software mediante una suscripción a listas o foros de seguridad que publican esta vulnerabilidad y explican dónde se pueden encontrar las actualizaciones del software con que se solucionan.

[12]En inglés, *bug*.

Dirección recomendada

Hay muchas "listas de correo" de seguridad que aportan información de vulnerabilidad y actualizaciones diariamente. Por ejemplo, en Hispasec Sistemas.

- **Herramientas de seguridad mal utilizadas**. Escáneres, detectores[13], software para atacar contraseñas, etc.

[13]Detector en inglés se expresa como *sniffer*.

- **Bombas lógicas**. Son partes de código de un software que se mantiene inerte hasta que no se produce una cierta condición que lo activa (una fecha, una secuencia de teclas, etc.). Algunos programadores maliciosos insertan estas partes de código en su software con la intención de activarlas si son despedidos de la organización en que trabajan.

Ved también

Los escáneres y los detectores se estudian en los subapartados 3.4 y 3.5.

- **Virus**. Habitualmente, los virus son secuencias de código que se insertan en un fichero ejecutable (llamado *huésped*) de manera que, cuando se ejecuta, también lo hace el virus. Su principal cualidad es la autorreplicación, es decir, la capacidad de insertarse en otro software del sistema informático atacado. Pueden tener efectos sumamente destructivos (o simplemente perseguir la replicación): formateo de un disco duro, borrado de ficheros, disminución del rendimiento del sistema, etc. Los virus constituyen uno de los problemas de código malicioso más importantes en sistemas informáticos basados en Windows.

Con respecto al software antivirus, además de los basados en la búsqueda de patrones víricos dentro de los ficheros infectados, también hay diversos productos que, bajo la denominación de antivirus, actúan en realidad como software protector de la integridad del sistema, y permiten tan sólo la instalación de software autorizado (firmado digitalmente por el fabricante).

Tipos de virus

Hay muchos tipos de virus: de sector de inicio, de macro, multiplataforma, multiproceso, de compresión (como forma de ocultación), interpretado, sobrescritos (destruyen el fichero) o añadidos (lo conservan), etc.

- **Gusanos**. Similares al virus, un gusano es un programa que es capaz de autoejecutarse con la finalidad de propagarse por la red y colapsar el ancho de banda de los sistemas atacados o dañar los ordenadores (pueden ir acompañados de virus).

Observación

Uno de los incidentes de seguridad más importantes que han tenido lugar en Internet fue producto de un gusano el año 1988 y provocó la caída de miles de máquinas.

- **Troyanos**. Son partes de código insertadas en el software que habitualmente se utiliza en el sistema. Este código se mantiene oculto y lleva a cabo tareas diversas sin que el usuario o el administrador se den cuenta de ello. Camuflado bajo la apariencia de un software útil o habitual, no suelen ocasionar efectos destructivos. Generalmente, capturan contraseñas y otros datos confidenciales y los envían por correo electrónico a la persona que ha introducido el troyano dentro del sistema atacado. También pueden abrir agujeros de seguridad que posteriormente podrán ser aprovechados por el atacante. Realmente, los efectos de los troyanos pueden llegar a ser muy perniciosos y su uso puede ser fuente de delitos. Por ejemplo, mediante un troyano es posible activar remotamente una webcam y grabar al usuario destino con total desconocimiento por parte de éste.

Ejemplo de troyano

Un ejemplo muy conocido de troyano es el software BackOrifice, una herramienta de administración remota para sistemas Windows 95/98.

- ***Backdoors***. Son puertas de entrada a sistemas operativos y software, insertadas por los propios diseñadores o programadores, que les permiten acceder a la aplicación evitando todos los mecanismos de autenticación.

Ved también

Ved el subapartado 2.2.2 relativo al PGP.

- ***Phising***. Prácticamente todos los usuarios de Internet hemos tenido que sufrir la recepción de correos electrónicos que, haciéndose pasar como "fiables" y procedentes de entidades bancarias reales, nos solicitan información confidencial que una verdadera entidad bancaria nunca solicitaría a través del correo electrónico. Los *links* o vínculos de estos correos nos remiten a sitios web falsos y que no corresponden a la entidad bancaria real.

Pharming

El *pharming,* en el cual se explota una vulnerabilidad en el software de los servidores o de los usuarios, permite que el atacante redirija un nombre de dominio a otra máquina diferente. Es una variante muy técnica de efectos similares al *phising*.

- ***Hoax***. Tan "popular" como el *phising* o el *spam*, un *hoax* no es más que un correo electrónico en el que se avisa de la existencia de virus (naturalmente falso) de efectos devastadores contra los cuales no existe ningún antivirus que los pueda detectar.

- ***Adware***. Es un software que muestra publicidad diversa. Habitualmente, se instala sin el consentimiento del usuario.

- ***Spyware* o software espía**. Es un software que envía datos a empresas sobre nuestros hábitos de Internet. Como de costumbre, suelen instalarse sin el permiso del usuario. Existen múltiples soluciones para "limpiar" nuestros sistemas de este tipo de software.

A continuación estudiaremos las diferentes técnicas que se pueden utilizar para detectar y prevenir la presencia de código malicioso en nuestro sistema informático. Según la configuración del sistema, la detección del código malicioso (normalmente ficheros compilados) será una tarea más o menos complicada. Por ejemplo, si se conoce la última fecha de actualización del sistema y se localiza algún fichero de sistema *posterior* a esta fecha, se puede pensar en la presencia de código malicioso. En este sentido, puede resultar de mucha ayuda la observación de los parámetros siguientes:

- Última fecha de modificación de los ficheros.
- Fecha de creación de los ficheros.
- Tamaño de los ficheros.

Desgraciadamente, las fechas y tamaños de los ficheros se pueden alterar con facilidad y, por lo tanto, no son una fuente de información segura. Una vez más, las funciones resumen nos pueden ser de mucha utilidad para garantizar la integridad de todo el sistema. Estas funciones resumen permiten obtener lo que podríamos llamar una "huella" única de un fichero o conjunto de ficheros. Así, pues, el administrador puede obtener en cualquier momento una instantánea o huella "única" del sistema informático utilizando funciones resumen.

Ved también

Recordad que las funciones resumen se han estudiado en el apartado 2 de este módulo.

Cualquier alteración de un fichero, por mínima que sea, provocará que cuando el administrador vuelva a calcular la función resumen, obtenga un resultado diferente. La herramienta más conocida para llevar a cabo esta función recibe el nombre de *Tripwire* (hay versiones para Linux, UNIX y Windows NT). Es configurable, incluye un lenguaje de macros para poder automatizar tareas y utiliza diversos algoritmos de resumen (entre ellos, el algoritmo MD5[14]). El funcionamiento de *Tripwire* es el siguiente: una vez se ha instalado el sistema, se obtiene un resumen de cada fichero relevante y se almacena en una base de datos.

(14)Recordad que MD5 son las siglas de *message digest*.

Cuando el administrador quiere comprobar la integridad del sistema, ejecuta *Tripwire*, y si se ha producido algún cambio en algún fichero, se generará la señal de aviso correspondiente en el fichero de salida de la aplicación. El funcionamiento correcto de este procedimiento sólo se puede garantizar si la base de datos donde se guardan las salidas resumen no es modificable por ningún usuario. Esto se puede conseguir haciendo que la base de datos tenga atributo de sólo lectura, o mejor todavía, almacenándola en un medio que no admita reescrituras como, por ejemplo, un CD-ROM.

Como hay algunos ficheros del sistema que pueden variar a menudo (por ejemplo, el fichero de contraseñas), *Tripwire* permite actualizar la base de datos sin volver a calcular el resumen entero de todo el sistema. Tened presente que conviene obtener el primer resumen del sistema antes de abrirlo a los usuarios.

3.4. Detectores

Se llaman *detectores*[15] los programas que permiten la captura y la grabación de la información que circula por una red.

(15)Detector en inglés se expresa como *sniffer*.

Su funcionamiento se basa en la activación del modo promiscuo de las interfaces de red de las estaciones de trabajo. Con la activación de este modo, la estación de trabajo podrá monitorizar, además de los paquetes de información que se dirigen a ella de una manera explícita, el tráfico entero de la red. Eso incluye, por ejemplo, la captura de nombres de usuario y contraseñas, o incluso la intercepción de correos electrónicos (o cualquier otro documento confidencial).

Carnivore

El software Carnivore (DCS 1000) es una aplicación parecida a un *sniffer*. Se instala en los proveedores de servicios de Internet y permite la vigilancia e interceptación de las comunicaciones a través de la red.

La actividad de los detectores es difícilmente detectable porque no quedan huellas en ningún sitio. No podemos tener constancia de la información que puede haber sido interceptada por la acción de los detectores (si no es de manera indirecta, por medio de los ataques que puede sufrir el sistema informático).

No obstante, se pueden utilizar medidas de protección de alcance más general. Por ejemplo, si se cifran los documentos que se envían por la red con PGP, aunque puedan ser interceptados, muy difícilmente podrán ser descifrados por el espía. Desgraciadamente, las herramientas criptográficas protegen la información que circula, pero no permiten establecer conexiones seguras.

Wireshark

El detector por excelencia se llama Wireshark (conocido como Ethereal hasta el año 2006) y tiene versiones para Unix y Windows.

Por este motivo es de vital importancia la instalación de otras herramientas como, por ejemplo, un servidor de Secure Shell (SSH) y las respectivas utilidades de los clientes. Secure Shell permite el establecimiento de inicios de sesión seguros y se puede utilizar como sustituto del comando Telnet. Una vez instalado, configurado e iniciado el servidor, el uso de las diferentes utilidades de los clientes se puede ejecutar de una manera muy sencilla y similar al habitual Telnet, motivo por el cual la utilización de Secure Shell no necesita ninguna fase de aprendizaje.

Finalmente, advertimos que los detectores tienen muchas ventajas para el administrador del sistema, no sólo para monitorizar, por ejemplo, el flujo de información que circula por la red, sino para protegerse de muchas amenazas. Por ejemplo, si sospechamos que nuestro sistema ha sido **troyanizado**, podemos monitorizarlo con un detector para averiguar sus efectos.

3.5. Escáneres

Los escáneres son herramientas de seguridad que sirven para detectar la vulnerabilidad de un sistema informático. En general, se pueden dividir en dos categorías: los escáneres de sistema y los escáneres de red.

Los **escáneres de sistema** se utilizan para detectar la vulnerabilidad del sistema informático local: problemas de configuración, permisos erróneos, contraseñas débiles, etc.

Los **escáneres de red** analizan los servicios y puertos disponibles de *huéspedes* remotos en busca de debilidades conocidas que puedan aprovechar los atacantes (en cierta manera, pues, automatizan las tareas que llevaría a cabo un intruso remoto).

Un **puerto** indica un punto por el cual entra o sale la información de un ordenador. Los protocolos relativos a Internet (FTP, Telnet, etc.) utilizan, emisor y receptor, un puerto de salida y recepción común en ambos extremos de la comunicación. El llamado **escaneo de puertos** consiste en averiguar los puertos TCP/UDP[16] que están abiertos en una máquina remota perteneciente a una red determinada. Los puertos abiertos constituyen una información muy interesante para los posibles intrusos, ya que la vulnerabilidad de los servicios que se encuentran abiertos o en funcionamiento puede permitir, al ser aprovechadas o "explotadas", el acceso no autorizado al sistema. La asignación de los puertos no es arbitraria y viene determinada por la Internet Assigned Numbers Authority (IANA).

(16)TCP es la sigla de *transmission control protocol* y UDP, de *user datagrama protocol*.

Otras funciones de la IANA

La Internet Assigned Numbers Authority también es responsable de la coordinación y mantenimiento del Sistema de Nombres de Dominio (DNS).

Ejemplos de asignación de puertos a servicios de Internet

```
Puerto TCP/UDP 20: FTP (datos)
Puerto TCP/UDP 21: FTP (control)
Puerto TCP/UDP 23: Telnet
Puerto TCP/UDP 25: SMTP
Puerto TCP/UDP 53: DNS
Puerto TCP/UDP 80: HTTP
Puerto TCP/UDP 110: POP3
Puerto TCP/UDP 194: IRC
```

Comando NETSTAT

El comando NETSTAT (válido tanto para sistemas Windows como Unix) puede ofrecer información sobre las conexiones establecidas y los números de puerto que se están utilizando.

Los puertos situados a partir de 1024 hasta el 65535 se llaman **puertos registrados**, no se encuentran bajo el control de la IANA[17] y pueden ser utilizados por determinadas aplicaciones. Por ejemplo, una aplicación cliente de una herramienta de control remoto podría utilizar un puerto de este rango para realizar sus tareas y pasar desapercibido por el usuario local o el administrador del sistema.

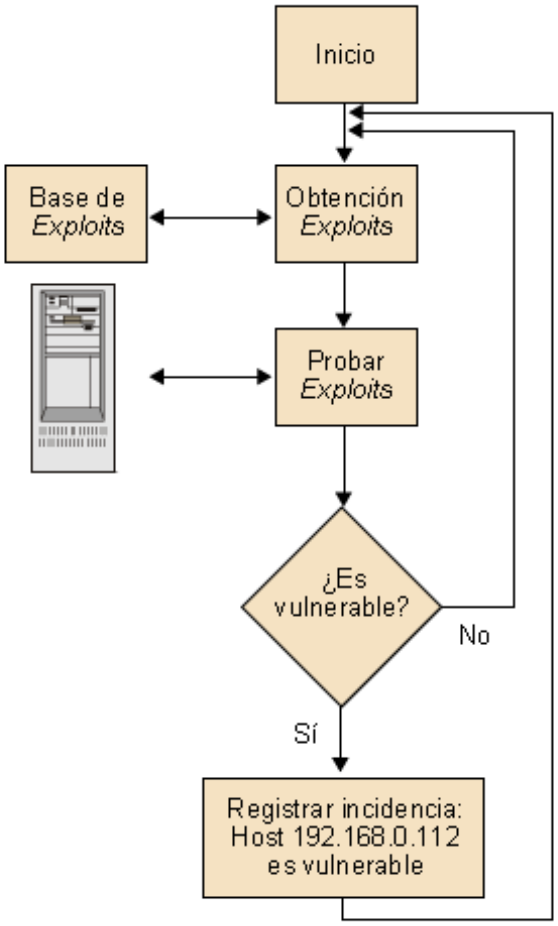
(17)Recordad que IANA son las siglas de la Internet Assigned Numbers Authority.

Todos los escáneres, tanto si son de sistema como de red, comparten, a grandes rasgos, un esquema de funcionamiento similar. Por ejemplo, el diagrama de flujo siguiente representa el algoritmo que seguiría un escáner de red:

Ved también

Ved el aspecto legal del uso de los escáneres en el apartado 4 de este módulo.

Algoritmo de un escáner de red



Aunque los escáneres son herramientas de mucha utilidad para los administradores de los sistemas informáticos, cabe decir que los intrusos también pueden hacer un uso malicioso de ellos. Los escáneres permiten la automatización de centenares de pruebas para localizar la vulnerabilidad de un sistema. Por otra parte, el posible intruso no hace falta que conozca con precisión la vulnerabilidad del sistema; simplemente utiliza la información que le proporciona el escáner, sin necesidad de ser un experto informático.

El análisis de la vulnerabilidad de una red o sistema informático, en definitiva, el estudio de su seguridad, desde el punto de vista de lo que haría un intruso, recibe el nombre de **test de penetración**.

Aunque al principio los escáneres sólo analizaban entornos Unix, en la actualidad existen para todo tipo de plataformas. Por ejemplo, la herramienta Nessus es capaz de evaluar tanto entornos Windows como Unix.

3.6. Ataques de denegación de servicio

Se llaman **ataques de denegación de servicio** (DoS[18], por *denial of service*) toda acción iniciada por una persona o por otras causas, que inutiliza el hardware y/o software, de manera que los recursos del sistema no sean accesibles desde la red.

[18]DoS es acrónimo de la expresión inglesa por ataque de denegación de servicio (*denial of service*).

[19]En inglés, *distributed denial of service*.

Los ataques de denegación de servicio pueden atacar el hardware de la red, el sistema operativo e incluso las aplicaciones del sistema. Los ataques DoS pueden implicar a otros ordenadores intermediarios (incluso miles), con lo cual se consigue un daño todavía mayor. Además, el atacante puede ocultar su dirección IP gracias a los ordenadores puente (llamados **zombies**). Estos tipos de ataques se llaman ataques de denegación de servicio distribuidos[19] (DDoS).

Ejemplos de ataques DoS

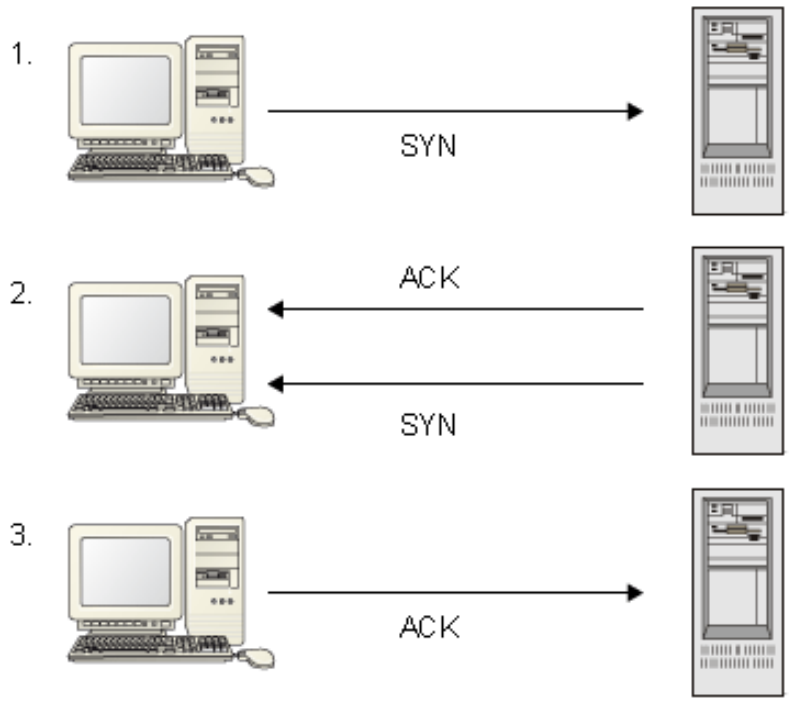
Hay otros tipos de ataques DoS: Smurf, Fraggle, Ping of death, Teardrop, etc.

Ejemplo de ataque DoS: el ataque SYN

Este ataque consiste en el envío, por parte del sistema atacante, de un gran número de solicitudes de conexión por segundo. El sistema atacado responde correctamente las solicitudes de conexión, pero al no obtener respuesta del sistema atacante, se colapsa y no puede atender las solicitudes de conexión legítimas. Este ataque se basa en el *modus operandi* del protocolo de establecimiento de sesión entre cliente y servidor (ved la figura):

1) El ordenador cliente envía una solicitud de sincronización (SYN) al servidor.
2) El servidor responde con un mensaje ACK (*acknowledgement*) y un mensaje de sincronización al cliente.
3) En respuesta a la solicitud de sincronización, el ordenador cliente envía una respuesta ACK al servidor.

Protocolo de establecimiento de sesión en 3 pasos



El servidor mantiene en cola de espera todos los paquetes SYN/ACK que va recibiendo, hasta que son cancelados por el envío del correspondiente ACK por parte del cliente (o bien expira un temporizador que regula el tiempo de espera). El ataque SYN se produce cuando los paquetes enviados por el emisor contienen direcciones IP erróneas y, en

consecuencia, el servidor nunca podrá recibir el paquete ACK que liberaría la cola de recepción. Así, cuando ésta se llena, las nuevas y legítimas solicitudes de conexión no se podrán servir.

3.7. Auditoría y ficheros *log*

Se llama *logging* el procedimiento mediante el cual se registran en un fichero las actividades que suceden en un sistema operativo o en una aplicación. Este fichero, llamado genéricamente log, recoge, por decirlo de alguna manera, las "huellas" de todo lo que ha sucedido en un sistema informático, incluyendo el origen de los posibles ataques de que haya sido objeto.

3.7.1. Los ficheros de log de Unix/Linux

A diferencia de otros sistemas operativos (por ejemplo, Windows), Unix/Linux presenta un gran número de comandos y ficheros relacionados con las tareas de *logging*:

- ***syslog***: fichero de texto que almacena (según un fichero de configuración llamado *syslog.conf*) información diversa relativa a la seguridad del sistema como, por ejemplo, los accesos a determinados servicios, la dirección IP de origen, etc. Es el fichero log más importante del sistema Unix.

Seguridad de los ficheros log

Muchos ficheros log son ficheros de texto y, por lo tanto, pueden ser fácilmente modificados y/o borrados por los intrusos con la finalidad de borrar o cambiar los indicios de su actividad.

- ***lastlog***: este comando informa del último inicio de sesión[20] de los usuarios contenidos en */etc/passwd*. Esta información se encuentra en el fichero */var/log/lastlog*. Los intrusos utilizan software especializado para borrar las huellas en este fichero (es un fichero binario y, por lo tanto, no se puede reescribir fácilmente).

[20]Inicio de sesión en inglés se expresa como *login*.

Localización de los ficheros log

La localización de los ficheros log puede variar sensiblemente según el Unix, o según la distribución de Linux que se utilice. Normalmente, se encuentran en */var/log*.

- ***last***: el comando *last* proporciona información relativa a cada conexión y desconexión al sistema. Esta información se encuentra almacenada en el fichero */var/log/wtmp*. Las mismas observaciones que se han hecho para el comando *lastlog* son aplicables a este caso.

Comando *last*

El comando *last* proporciona la siguiente información: usuarios, terminal o servicio utilizado en el *login*, dirección IP, fecha y hora, duración de la sesión, etc.

- ***utmp***: fichero que almacena los usuarios que se encuentran conectados al sistema informático en un momento determinado. El pedido *who* busca a los usuarios en este fichero. También es un fichero binario.

- ***messages***: fichero que registra actividades diversas del sistema (usuarios conectados, su dirección IP, mensajes de núcleo[21], etc.; es posible configurar la información que se quiere almacenar). Es un fichero de texto y, por

[21]Núcleo en inglés se expresa como *kernel*.

lo tanto, se puede visualizar con el pedido *cat* o modificarlo de una manera muy sencilla con el pedido *grep* o un editor de texto cualquiera.

Una buena estrategia para evitar que los intrusos puedan borrar las huellas en los ficheros log consiste en el uso de herramientas de *logging* diferentes de las proporcionadas por el sistema operativo que mantengan sus propios ficheros de actividad, independientemente de los que pueda utilizar el sistema operativo.

No son los únicos pedidos y ficheros de que dispone Unix para llevar a cabo las tareas de *logging*. Por otra parte, el volumen de información que puede generar la actividad de un sistema informático es tan enorme que son necesarias herramientas especializadas para llevar a cabo tareas de auditoría. Por ejemplo, *logrotate* sirve para establecer sistemas de rotación de log (configurable a partir del fichero */etc/logrotate.conf*), lo cual consiste en comprimir cada cierto tiempo los log objeto de interés y almacenarlos sólo hasta una cierta antigüedad.

3.7.2. Los ficheros log y la investigación de delitos informáticos

De todo lo que se ha visto hasta ahora se desprende fácilmente que la información contenida en los ficheros log (tanto locales en nuestro sistema, como los remotos, alojados, por ejemplo, en los proveedores de servicios de Internet u otros sistemas) es muy importante en la investigación de cualquier incidente de seguridad. Los proveedores de servicios de Internet, según la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE), sólo tienen la obligación de mantener los ficheros log durante un tiempo máximo de doce meses, pero no hay ningún mínimo exigible, motivo por el cual es necesario actuar rápidamente en caso de presunto delito.

De todo esto se desprende que la seguridad es muy importante y se tiene que tener en cuenta ya desde el primer momento en que se diseña la estructura de la red de la empresa, así como en el diseño de la estructura del departamento de informática. Hay empresas en las que el departamento de seguridad está sometido directamente bajo la dirección y en otras está dentro del departamento de informática o en el de sistemas.

La seguridad, en muchos casos, pasará por encima de otros requerimientos, pero en general se tiene que llegar a un convenio entre seguridad y usabilidad.

Desde el punto de vista del director de informática, lo tiene que ver como una parte muy importante, y tiene que tener una partida en el presupuesto directo para temas relacionados con la seguridad.

4. Aspectos legales de la seguridad informática. Marco jurídico penal y extrapenal. El "delito informático"

El "delito informático" no aparece explícitamente definido en el actual Código penal (1995) ni en las reformas posteriores que se han realizado y, por lo tanto, no se podrá hablar de "delito informático" propiamente dicho, sino de delitos hechos con el concurso de la informática o las nuevas tecnologías, en los cuales el ordenador se erige como medio de ejecución del delito, o bien como objetivo de esta actividad (por ejemplo, una intrusión en un sistema informático). El objetivo de este apartado no es aleccionar a los administradores o directores de un sistema informático, sino tan sólo darles a conocer las responsabilidades en que pueden incurrir a causa de su trabajo y, como desafío principal, dotarlos de mecanismos que, en caso de acciones delictivas que tienen por objeto los sistemas que administran o de los que son responsables, les permitan denunciar los delitos de los que han sido víctimas y solicitar las actuaciones legales pertinentes.

Por otra parte, tampoco se pretende hacer una recopilación excesivamente generosa en lenguaje jurídico, ni profundizar en posibles sentencias relacionadas con los delitos que se explicarán en este módulo. La legislación actual todavía presenta vacíos con respecto a los mal llamados "delitos informáticos", de manera que tan sólo se ofrecerán directrices básicas, más bien relacionadas con el sentido común y los artículos del Código penal (entre otras normas), que con la compleja normativa que se va generando en torno a esta nueva problemática.

La vertiente tecnológica o científica de los estudios de ingeniería a menudo deja de lado la vertiente social de la aplicación de los avances que se van produciendo en estas disciplinas. Consiguientemente, el administrador de un sistema puede ser muy competente en el trabajo técnico, pero es posible que tenga muchas dudas a la hora de tratar problemas como los siguientes:

- Si mi jefe me pide que le muestre el contenido del buzón de correo personal de un trabajador, ¿tengo la obligación de hacerlo?

- Se ha producido un acceso no autorizado al servidor y los intrusos han modificado la página web del departamento. ¿Este hecho es denunciable? ¿A quién lo tengo que denunciar?

- El servidor almacena datos de carácter personal. ¿Se tienen que proteger con algunas medidas de seguridad determinadas?

- ¿Es legal la utilización de escáneres (entendidos como herramientas de administración de sistemas)?

- ¿Puedo colgar en Internet una página web con las fotografías y logotipos de mi grupo de música preferido?

- ¿Cómo puedo denunciar el uso de copias no autorizadas de software?

- ¿Puedo utilizar herramientas criptográficas para proteger la información?

- ¿Los administradores de sistemas de rehén[22] son responsables de los contenidos que alojan las páginas web de los clientes?

[22]En inglés, *hosting*.

En este apartado intentaremos orientaros en relación con las dudas que se han expresado, si bien hay que ser consciente de que no hay una línea de actuación única y de que las particularidades de cada caso hacen que haya que ser muy prudente a la hora de enfrentarse con este tipo de problemas. En definitiva, cabe tener muy presente que no todo lo que es técnicamente posible es legal, y que el desconocimiento de las normas no exonera de responsabilidad (penal o no) al trabajador informático.

4.1. Marco jurídico penal de las conductas ilícitas vinculadas a la informática

En este subapartado se estudiarán las sanciones previstas por el Código penal (en muchas ocasiones, penas privativas de libertad). Como se verá, algunas de las acciones planteadas por las dudas del apartado anterior pueden originar responsabilidad penal. Otras, sin embargo, tendrán la consideración de **extrapenales**, entendiendo con este nombre la rama del ordenamiento jurídico que contiene sanciones menos graves que las previstas por el derecho penal (derecho administrativo, derecho civil, derecho laboral, etc.).

4.1.1. Delitos contra la intimidad

El artículo 197.1 del actual Código penal (a partir de ahora, CP) asimila la intercepción del correo electrónico con la violación de la correspondencia.

Derecho a la intimidad

La Constitución española reconoce el derecho a la intimidad en el artículo 18.

Así pues, serán constitutivas de delito las conductas siguientes:

- El apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales.
- La intercepción de las telecomunicaciones.
- La utilización de artificios técnicos de escucha, transmisión, grabación o reproducción de sonido, o de cualquier otra señal de comunicación.

Detección y monitorización

La detección (*sniffing*) es una actividad que se podría enmarcar dentro del artículo 197.

La utilización de herramientas de monitorización de la actividad de un sistema en el terminal de un trabajador (sin su consentimiento) también se podría incluir en el artículo 197.

Para ser constitutivas de delito, estas actividades se tienen que producir sin el consentimiento del afectado (ni autorización judicial motivada) y con la intención de descubrir los secretos o vulnerar la intimidad.

Por lo tanto, abrir el buzón de un correo electrónico que no sea el nuestro propio y leer los mensajes que se almacenan en él podría convertirse en una conducta constitutiva de delito. Hay que ir con mucho cuidado con este tipo de acciones y, como norma general, nunca se tiene que leer ningún correo electrónico que no vaya dirigido a nosotros mismos.

El trasfondo de la intercepción empresarial del correo electrónico es casi siempre el mismo: el derecho de las organizaciones a controlar sus medios de producción. En este sentido, diversas sentencias que se han dictado en los tribunales en relación con el uso de los medios de la empresa con finalidades personales, se han pronunciado a favor de la empresa, ya que se entiende que los medios pertenecen a la empresa y que ésta no es un lugar adecuado para enviar y recibir mensajes de carácter privado (o hacer otras actividades personales, como el uso de los juegos que se incluyen en los sistemas operativos).

Sentencias a favor de la empresa

Hay diversas sentencias que se han dictado a favor de la empresa en relación con el uso de los medios de la empresa con finalidades personales. Por ejemplo, la sentencia del Tribunal Superior de Justicia de Cataluña (TSJC) núm. 9382/2000, de 14 de noviembre, en relación con el despido de un trabajador de una entidad bancaria.

También están los casos de las sentencias de la Sala Social del TSJC, con fecha 29 de enero de 2001, y el caso de la Sala Social del TSJC, con fecha 23 de octubre de 2000.

Una manera útil para hacer saber a los usuarios de una organización cuáles son los usos correctos de los medios de la empresa, y sus limitaciones, consiste en el uso de contratos en los cuales se especifica, por ejemplo, qué obligaciones y responsabilidades tiene un usuario de una cuenta de correo electrónico. Por otra parte, también es importante que los sindicatos tengan conocimiento de ello y que, por lo tanto, los trabajadores sepan que se les puede someter a ciertas medidas de control, las cuales, más que basarse en la apertura de los correos electrónicos, lo tendrían que hacer en el uso de controles menos lesivos, como por ejemplo, el estudio del número de bytes transmitidos, entre otros.

Usurpación y cesión de datos reservados de carácter personal

El resto de apartados del artículo 197 CP[23] (y los artículos 198, 199 y 200 CP) tipifican como conductas delictivas el acceso, utilización, modificación, revelación, difusión o cesión de datos reservados de carácter personal que se encuentren almacenados en ficheros, soportes informáticos, electrónicos o tele-

(23)CP es la abreviatura de Código penal.

máticos, siempre que estas conductas estén hechas por personas no autorizadas (conductas llamadas, genéricamente, abusos informáticos sobre datos personales).

Explícitamente se menciona el agravante de estas conductas cuando los datos objeto del delito son de carácter personal que revelan ideología, religión, creencias, salud, origen racial o vida sexual. Otros agravantes que hay que tener en cuenta se producen cuando la víctima es un menor de edad o un incapacitado, o bien la persona que comete el delito es la responsable de los ficheros que están involucrados. Merece una especial consideración el artículo 199.2, en el cual se castiga la conducta del profesional que, incumpliendo la obligación de reserva, divulga los secretos de otra persona.

4.1.2. Delito de fraude informático

En el artículo 248.2 CP se castiga la conducta de quien, utilizando cualquier manipulación informática, consiga la transferencia no consentida de cualquier activo patrimonial, con ánimo de lucro y perjuicio sobre tercero. La Ley 15/2003, por la cual se aprobó la reforma del Código penal del año 1995, introduce el castigo a las conductas preparatorias para la comisión de delitos de fraude informático. Así pues, también se castiga la fabricación, facilitación o la mera posesión de software específico destinado a la comisión del delito de fraude informático.

Falsificación de tarjetas

El artículo 387 CP considera moneda las tarjetas de crédito, de débito, u otras que se puedan hacer servir como medios de pago. Por lo tanto, la clonación o duplicación de tarjetas de banda magnética se considera un delito de falsificación de moneda.

4.1.3. Delito de uso abusivo de equipamientos

El artículo 256 CP castiga el uso de cualquier equipamiento terminal de telecomunicaciones sin el consentimiento de su titular, siempre que le ocasione un perjuicio superior a 400 euros. Esta cantidad fue establecida por la Ley 15/2003.

Wi-fi

Señalamos que el aprovechamiento no consentido de una conexión *wi-fi* podría tener la tipificación de delito de uso abusivo de equipamientos, siempre y cuando se produjesen los requisitos exigidos por el CP.

4.1.4. Delito de daños

Según el artículo 264.2 CP, el delito de daños consiste en la destrucción, la alteración, la inutilización o cualquier otra modalidad que implique el daño de datos, software o documentos electrónicos almacenados en redes, soportes o sistemas informáticos.

El delito de daños es uno de los delitos "informáticos" más frecuentes y a menudo tiene repercusiones económicas muy importantes en las organizaciones afectadas.

Ejemplos de daños

La alteración de una página web por una persona no autorizada se tipifica como delito de daños.

El envío de virus (con la clara voluntad de causar daños), los ataques DOS, entre otros similares, también podrían tipificarse como delitos de daños.

Tened presente, sin embargo, que la cantidad de 400 euros marca el umbral entre la falta y el delito.

Los daños producidos en un sistema informático se tienen que poder valorar y es esencial adjuntar una valoración de estos daños al denunciar la acción delictiva ante un cuerpo de policía. La valoración de los daños es un proceso

complejo de llevar a término y puede abarcar diferentes aspectos: coste de restauración de una página web, pérdidas en concepto de publicidad no emitida (lucro cesante) o por servicios que no se han podido prestar, etc.

Cabe decir que, si bien la intrusión en un sistema informático de momento no es en sí misma constitutiva de delito (aunque en breve tendrá esta consideración), estos tipos de conductas se suelen encontrar vinculadas a otras conductas que sí que son delictivas, como los delitos contra la intimidad, los daños a un sistema informático o los medios que se hayan hecho servir para llevar a cabo su acceso no autorizado (intercepción de correos electrónicos, detección (*sniffing*) de contraseñas, etc.).

4.1.5. Delitos contra la propiedad intelectual

Según el artículo 270 CP, las conductas relativas a los delitos contra la propiedad intelectual son aquellas en que se reproduce, plagia, distribuye o comunica públicamente, tanto de una manera total como parcial, una obra literaria, artística o científica sin la autorización de los titulares de los derechos de propiedad intelectual de la obra.

Ley de Propiedad Intelectual

Dentro del marco jurídico extrapenal, la Ley de Propiedad Intelectual (RD Legislativo 1/96, de 12 abril, por el cual quedaba el Texto Refundido de la Ley de Propiedad Intelectual), regula la protección de las obras literarias, artísticas o científicas, con independencia del soporte en el que esté plasmada.

Estas condiciones se aplican independientemente del soporte en el que se haya registrado la obra: textos, software, vídeos, sonidos, gráficos o cualquier otro fichero relacionado. Es decir, los delitos relativos a la venta, distribución o fabricación de copias no autorizadas de software son delitos contra la propiedad intelectual.

Permiso de los titulares

No podemos hacer un uso libre de la información que se pueda encontrar en Internet como, por ejemplo, gráficos, animaciones, logotipos, etc., sin el permiso de los titulares de los derechos de propiedad intelectual.

Ejemplos de delitos contra la propiedad intelectual

Veamos algunos ejemplos de delitos contra la propiedad intelectual:

- Reproducción íntegra de software y venta al margen de los derechos de licencia.
- Instalación de copias no autorizadas de software en un ordenador en el momento de su compra.
- Publicación del código fuente de software, software diverso (servidores de *warez*, software pirateado) u otros ficheros (MP3, libros, etc.) en Internet, al margen de los derechos de licencia de estas obras.
- Utilización de una licencia de software sólo para un ordenador para dar servicio a toda la red.
- Ruptura de los mecanismos de protección que permiten el funcionamiento correcto del software (mochilas, contraseñas y otros elementos de seguridad). Estas técnicas reciben el nombre genérico de *cracking* (en castellano, piratería).

El mismo artículo 270 CP prevé penas para quien haga circular o disponga de cualquier medio específicamente diseñado para anular cualquier dispositivo técnico de protección del software.

Con la reforma de la Ley 15/2003, los cuerpos policiales pueden actuar de oficio en la persecución de este tipo de delito. Por otra parte, un particular, dado que normalmente no dispone de los derechos de propiedad intelectual, no puede denunciar directamente estos tipos de delito, aunque es posible hacerlo de manera indirecta a través de organizaciones como la Bussiness Software Alliance (BSA).

Acción de oficio

Actuar de oficio implica que los cuerpos policiales pueden actuar sin necesitar la denuncia de las personas o de sus representantes legales.

Con respecto a la creación de software, también hay algunas consideraciones que hay que tener en cuenta. Según el tipo de contrato al que se encuentre sujeto el trabajador, el software que desarrolle para una organización pertenece a la empresa y, en consecuencia, si el trabajador abandona la organización no se puede llevar el software que ha creado en su antiguo puesto de trabajo. Como en el caso de la utilización del correo electrónico, sería recomendable que el contrato de trabajo especificara esta cuestión.

4.1.6. Delito de revelación de secretos de empresa

Según el artículo 278.1 CP, hace revelación de secretos de empresa quien, con la finalidad de descubrir un secreto de empresa, intercepte cualquier tipo de telecomunicación o utilice artificios técnicos de escucha, transmisión, grabación o grabación del sonido, imagen o de cualquier otra señal de comunicación.

Ejemplo

Hay diversos casos de delito de revelación de secretos de empresa, por ejemplo, el espionaje industrial. Podéis ver el caso Lear (sentencia 53/07 del Juzgado de lo Penal de Lérida, 18 de febrero de 2008).

4.1.7. Delito de defraudación de los intereses económicos de los prestadores de servicios

La defraudación de los intereses económicos de los prestadores de servicios es un nuevo delito, introducido a raíz de la reforma 15/2003 del Código penal. El artículo 286 CP contiene cuatro modalidades de comisión:

1) Se castiga la facilitación del acceso "inteligible" a servicios de radiodifusión sonora o televisiva, prestados a distancia por vía electrónica, mediante la facilitación, importación, distribución, posesión de programas o equipamientos informáticos, destinados a hacer posible el mencionado acceso. Esta modalidad incluye la instalación, mantenimiento o sustitución de estos equipamientos con finalidades comerciales.

2) Se castiga la alteración o duplicación del número de identificación del equipo de telecomunicaciones con ánimo de lucro.

3) Se castiga la facilitación del mencionado acceso a una pluralidad de personas por medio de cualquier publicación pública, aunque sea sin ánimo de lucro.

4) Finalmente, también se castiga la utilización de los equipamientos o software que permite el acceso, así como la utilización de los equipamientos alterados, independientemente de la cuantía de la defraudación.

4.1.8. Otros delitos

Además de los delitos que hemos descrito, es evidente que también se pueden llevar a cabo muchos otros delitos con el concurso de la tecnología:

- amenazas y coacciones (por chat o mediante correo electrónico),
- estafas electrónicas,
- falsedad documental (alteraciones y simulaciones de documentos públicos o privados) o
- difusión de pornografía infantil en Internet.

En relación con este último delito (artículo 189.1 CP), la Ley 15/2003 ha ampliado notablemente el tipo delictivo. Así, la mera posesión (aunque no esté destinada a la venta) de pornografía infantil ya se encuentra castigada (la difusión, creación y venta ya lo estaban). Además, se introducen ciertos agravantes, como por ejemplo, la utilización de menores de 13 años, entre otros. Asimismo, también se castiga la producción, venta, distribución y exhibición de material en el que, aunque no aparezcan directamente menores de edad, se haya modificado la voz o la imagen con la finalidad de que el contenido sea relativo a la pornografía infantil.

Si un sistema informático es víctima de cualquiera de estos delitos, o bien, por ejemplo, se descubre que el sistema que administra es utilizado como plataforma de distribución de copias de software no autorizadas o de pornografía infantil, se tiene que denunciar inmediatamente a la comisaría de policía más próxima, teniendo en cuenta el protocolo de actuación siguiente:

1) Adjunción de los ficheros log (locales) relacionados con el delito cometido.
2) En caso de que se haya producido un delito de daños, hay que adjuntar una valoración de los daños ocasionados.
3) Actuar con rapidez (los proveedores de Internet no almacenan indefinidamente los ficheros log de sus servidores).
4) En caso de que esta acción delictiva se haya producido por correo electrónico, hay que adjuntar las cabeceras completas del correo recibido.
5) Si el administrador lo considera necesario (por ejemplo, descubre pornografía infantil en un servidor de su responsabilidad), puede clonar el disco duro del servidor para preservar la evidencia digital y reinstalar el sistema para evitar que el delito se continúe produciendo.

Condena por compartir pornografía infantil

La primera condena por compartir pornografía infantil en Internet mediante el software *E-mule* se produjo en abril de 2008 en la Audiencia Provincial de Canarias.

4.1.9. Uso de herramientas de seguridad

Hay diversas herramientas de seguridad disponibles:

- **Escáneres de red o de sistema**. A pesar de la posibilidad de utilizar los escáneres con un uso malicioso, sus beneficios son evidentes con respecto a las tareas que tiene que hacer el administrador. La fiabilidad de un sistema informático no se puede basar en la ignorancia de los defectos que presenta y, por lo tanto, los escáneres se convierten en herramientas de gran valor en manos de los administradores. Ahora bien, desde el punto de vista legal, ¿se pueden utilizar? No hay ninguna ley en contra del uso de los escáneres, si bien se ha generado una interesante polémica en torno suyo. Algunas opiniones consideran que el uso de los escáneres es equivalente a ir a un domicilio particular y utilizar la fuerza para abrir la puerta. Otros creen que, por el solo hecho de tener una ubicación en Internet, ya se da el consentimiento implícito para "escanear" la localización.

- **Herramientas criptográficas**. Con respecto a la criptografía, tampoco hay ninguna ley que prohíba su uso en nuestro país. Según el artículo 52 de la Ley General de Telecomunicaciones, España dispone de un régimen de libertad de cifrado para proteger cualquier dato que circule por una red. Por otra parte, este mismo artículo deja la puerta abierta a la definición de mecanismos de control como, por ejemplo, la obligación de notificar al Estado los algoritmos criptográficos que se utilicen.

Se tiene que tener en cuenta, sin embargo, que en algunos países como Estados Unidos la exportación de herramientas criptográficas se asimilaba (hasta finales de 1999) al contrabando de armas. Recordad los problemas que tuvo Zimmermann con la publicación del código del PGP. Como norma general, nunca "se escaneará" un *host* sin autorización.

4.2. Marco jurídico extrapenal

Hay una serie de leyes que delimitan el marco jurídico que es de aplicación en el ámbito de la informática: la Ley Orgánica de Protección de Datos Personales, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico y la legislación que se aplica a la firma digital.

4.2.1. Ley Orgánica de Protección de Datos Personales

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (LOPDP) tiene por objeto la protección de la intimidad de las personas físicas, con respecto al tratamiento de sus datos personales. Por datos personales, se entiende cualquier información relativa a personas físicas identificadas o identificables. Por el tratamiento se entenderá el conjunto de operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación de datos. Además, también hay un reglamento relacionado con esta

Tratamiento de la dirección IP

La dirección IP permite, de manera indirecta, la identificación de un titular telefónico. Es, en consecuencia, un dato personal, y como tal se tiene que someter a las medidas indicadas por la LOPDP.

ley que regula las medidas de seguridad que tienen que satisfacer los ficheros que contengan datos de carácter personal. Estas medidas se disponen en los tres niveles siguientes:

Ficheros con datos personales

Las medidas de seguridad que tienen que satisfacer los ficheros que contengan datos de carácter personal se refieren, de una manera genérica, a todos los ficheros que contengan estos datos personales, no tan sólo aquellos a los cuales se pueda acceder desde Internet.

- **Nivel básico**. Consiste en la implantación de medidas de autenticación y control de acceso para los usuarios que tienen que acceder al fichero con contenido sensible, y también en la elaboración de protocolos de actuación sobre el fichero que permitan la identificación de posibles responsables en las incidencias que se produzcan en la manipulación de los datos. Este nivel es exigible en la gestión de todos los ficheros que almacenan datos de carácter personal.

Lectura recomendada

El Real Decreto 1720/2007, de 21 de diciembre, aprueba el Reglamento de desarrollo de la Ley 15/1999. Los tres niveles de medidas de seguridad para proteger los ficheros con datos personales se desarrollan en este reglamento.

- **Nivel medio**. En este nivel de seguridad, el administrador tiene que elaborar un catálogo sobre las medidas de seguridad genéricas que se tienen que llevar a cabo e implementar mecanismos de autenticación remota seguros. Además, estas medidas se tienen que someter, como mínimo cada dos años, a una auditoría externa que certifique la eficacia de las medidas de seguridad que se han tomado. Son medidas exigibles para todos los ficheros que almacenen datos relativos a la comisión de delitos o infracciones administrativas, Hacienda Pública, servicios financieros y los relativos a la solvencia patrimonial y el crédito.

- **Nivel alto**. Para proteger los ficheros situados en este nivel hace falta el uso de métodos criptográficos para evitar que los datos sensibles sean inteligibles y no puedan ser alterados o capturados mientras circulan por una red. Pertenecen a este nivel los datos relativos a ideología, creencias, origen racial, salud, vida sexual o los obtenidos con finalidades policíacas.

La LOPDP[24] distingue entre el **responsable de los ficheros** y el **responsable de la seguridad de los ficheros**. A la vez, el responsable de los ficheros se desdobla en dos figuras que no tienen por qué ser coincidentes: el **responsable del fichero** o tratamiento (por ejemplo, la empresa X) y el **encargado del tratamiento** (por ejemplo, otra empresa contratada por la empresa X con la finalidad de efectuar el tratamiento de los datos).

(24)LOPDP es la abreviatura de la Ley Orgánica de Protección de Datos Personales.

Secreto profesional

La LOPDP determina el deber de secreto profesional a todos los encargados del tratamiento de datos personales.

Finalmente, el responsable de la seguridad de los ficheros sería cualquier empresa que se responsabilizara de esta seguridad (habitualmente, el encargado del tratamiento y el responsable de seguridad son figuras coincidentes). Para acabar, hay que tener presente que la ley obliga a que todas las empresas que tienen ficheros con datos personales los notifiquen en la Agencia de Protección de Datos.

4.2.2. Ley de servicios de la sociedad de la información y comercio electrónico

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de información y comercio electrónico (LSSICE) representa el desarrollo en nuestro país de la directiva comunitaria sobre comercio electrónico. La LSSICE regula los servicios ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, portales, e incluye, entre otros, el comercio electrónico. Algunas características que la definen son las siguientes:

- Prohibición del correo electrónico no solicitado o no consentido (*spam*). El incumplimiento de esta prohibición puede comportar sanciones de hasta 150.000 euros.

- Regulación de cualquier actividad que genere ingresos o permita la obtención de beneficios económicos (inclusión de "cibertiras" publicitarias [*banners*] en una página web, tiendas virtuales, patrocinios, etc.).

- Sanciones (aplicadas por la Agencia de Protección de Datos) económicas de hasta 600.000 euros para las infracciones consideradas muy graves.

- Obligatoriedad de denunciar hechos ilícitos y suspensión de la transmisión y alojamiento de contenidos ilícitos (mediante solicitud).

- Definición de las responsabilidades de los proveedores de Internet. Por ejemplo, en el caso de hospedaje y *linking* los proveedores no tendrán ninguna responsabilidad sobre la información almacenada, siempre y cuando no tengan conocimiento de que esta información sea ilícita, o bien, si tienen conocimiento de ello, tienen que actuar con la máxima diligencia para imposibilitar el acceso o eliminar el contenido ilícito.

- Obligación de almacenar los ficheros de log, por parte de los proveedores de servicios, como mucho durante un periodo de doce meses (observamos que no se establece ningún periodo mínimo).

4.2.3. Firma electrónica o digital

La firma electrónica es una materia que queda regulada en el Estado español mediante el Real decreto ley 14/1999, de 17 de septiembre, basado en la directiva europea que establece el marco comunitario para la firma electrónica. Este decreto ley determina la eficacia jurídica de la firma digital en el Estado español, y el establecimiento de las condiciones de los servicios de certificación.

Hay dos tipos diferentes de firma:

- **Firma electrónica o digital avanzada**. Permite identificar a la persona que firma y detectar cualquier cambio que se pueda producir de forma posterior a la firma de los datos.

- **Firma electrónica o digital reconocida**. Consiste en la firma electrónica avanzada, basada en un certificado reconocido y generado mediante un dispositivo seguro de creación de firma (los prestadores de servicios de certificación). Es equiparable a la firma manuscrita.

5. Informática forense

Una vez descrito el marco jurídico en el se circunscriben las conductas ilícitas relacionadas con el uso de las tecnologías de la información, se estudiarán brevemente las metodologías de trabajo que se pueden utilizar, una vez ha sucedido el incidente, con la finalidad de averiguar qué ha ocurrido y quién ha sido el autor. Estas técnicas se recogen en una disciplina de reciente creación, situada a caballo entre el marco jurídico y la tecnología, llamada **informática forense**. Las huellas que permiten reconstruir la ejecución de un hecho (el cual no tiene que ser necesariamente constitutivo de delito) se encuentran almacenadas en soportes digitales y se llaman genéricamente **evidencias digitales**.

La evidencia digital presenta, básicamente, las propiedades siguientes:

- Se puede cambiar o eliminar fácilmente.
- Es posible obtener una copia exacta de un archivo sin dejar ninguna huella de esta acción.
- La adquisición de la evidencia puede suponer la alteración de los soportes digitales originales.

El **análisis forense** informático apareció a causa de la necesidad de aportar elementos relevantes en los procesos judiciales en los que las nuevas tecnologías se encontraban presentes, ya sea como objetivos finales (por ejemplo, una intrusión con daños en un sistema informático), o bien como medio (por ejemplo, el envío de amenazas a través del correo electrónico a un personaje público). Su finalidad, en cualquier caso, consiste en responder a la clásica línea argumental policíaca: **qué**, **cuándo**, **dónde**, **quién**, **cómo** y **por qué**.

Precisamente, se podría definir el análisis forense informático como el proceso de aplicar el método científico a los sistemas informáticos con la finalidad de asegurar, identificar, preservar, analizar y presentar la evidencia digital, de forma que sea aceptada en un proceso judicial.

Naturalmente, la informática forense va más allá de los procesos judiciales y, en muchas ocasiones, los informes elaborados por los expertos analistas no tendrán como objetivo final su presentación ante los tribunales, sino la empresa privada.

5.1. Aseguramiento de la escena del acontecimiento

Esta fase únicamente será preceptiva en el transcurso de una actuación policíaca. No obstante, las recomendaciones que se darán pueden ser de mucha utilidad para cualquier perito que tenga que intervenir en el lugar de los hechos. La finalidad de esta etapa consiste en asegurar la escena del acontecimiento, restringiendo su acceso para que nadie pueda alterarla. Los referentes policíacos son evidentes, aunque seguir las recomendaciones que ahora se describirán permitirá preservar, en cualquier caso, su evidencia, así como facilitar su posterior análisis:

Dirección recomendada

Podéis ver un "código de buenas prácticas forenses" en http://cp4df.sourceforge.net.

- Identificar la escena donde se ha producido el hecho a investigar y establecer un perímetro de seguridad.

- Realizar una lista con los sistemas involucrados en el suceso.

- Restringir el acceso de personas y equipamientos informáticos al interior del perímetro.

- Fotografiar y/o registrar en vídeo la escena del suceso. También puede ser muy útil representar esquemáticamente la topografía de la red de ordenadores.

- Mantener el estado de los dispositivos. En algunas ocasiones, puede ser muy importante fotografiar o registrar el contenido de los monitores en funcionamiento, así como la identificación y adquisición de las evidencias volátiles, por ejemplo, la extracción del contenido de la memoria para saber qué procesos se encontraban en ejecución en aquel momento.

- Desconectar las conexiones de red.

- En caso de existir, comprobar y desconectar las conexiones "inalámbricas", ya que pueden permitir conexiones remotas a los equipos objeto de investigación.

- Si hay impresoras en funcionamiento, permitir que acaben la impresión.

- Anotar la fecha y hora del sistema antes de apagarlo. Estos datos también se pueden fotografiar y/o registrar en vídeo.

- Apagar los dispositivos en funcionamiento, o bien sacando el cable de alimentación, o bien mediante el procedimiento de apagado normal. El experto tendrá que evaluar, en cada caso, cuál es el método más adecuado que ofrece más garantías de preservación de la prueba.

- Etiquetar cables y componentes. Además, hay que tener presente que algunos dispositivos requieren cableado muy específico sin el cual no será

posible analizar el aparato en el laboratorio, ya que no se podrá poner en funcionamiento.

En algunas ocasiones, el aseguramiento de la escena se produce en el transcurso de una entrada y perquisición en el sitio de los hechos en presencia de miembros de las Fuerzas y Cuerpos de Seguridad del Estado. En este caso, la entrada contará con la presencia del secretario judicial, con lo cual se puede hacer constar en acta la fecha y hora del sistema, entre otras comprobaciones de las que el secretario judicial podría dar fe y, por lo tanto, podría ahorrar al analista algunos procesos de documentación, fotografías y/o grabaciones de vídeo.

Fecha y hora de un sistema informático

La fecha y hora de un sistema informático no tiene que coincidir con la fecha y hora real. Este desfase puede ser vital a la hora del análisis y hay que hacerlo constar en acta.

5.2. Identificación de la evidencia digital

Se llama así al proceso de identificación y localización de las evidencias que se tienen que recoger para ser analizadas posteriormente. Este proceso no es tan trivial como puede parecer a primera vista ya que, a menudo, el experto se encontrará con configuraciones de sistemas complejos con muchos dispositivos (locutorios, empresas, etc.) o simplemente con usuarios que guardan muchos soportes susceptibles de ser analizados (por ejemplo, un particular adicto a almacenar cualquier software descargado de Internet en miles de CD y DVD). En consecuencia, el analista tendrá que encontrar una solución de compromiso entre la calidad, la validez de la prueba y el tiempo de que dispone para recoger las evidencias.

En primer lugar, el experto tendrá que identificar el sistema informático (un único PC, una red local, un sistema IBM AS/400, un RAID, etc.) con la finalidad de saber dónde se almacenan las evidencias digitales que pueden ser de utilidad para el análisis. Éstas se pueden encontrar en ordenadores locales, en soportes como CD o DVD, en servidores remotos, o incluso en la memoria RAM de los equipamientos en funcionamiento. Este tipo de evidencias, las volátiles (en esencia, las que desaparecen en ausencia de alimentación eléctrica), son las que tendrá que intentar preservar en primera instancia, en los casos en que sea necesario.

También, en este instante, convendrá valorar la posibilidad de realizar un "análisis en caliente" en busca de evidencias que, de otra forma, se perderían al detener el sistema. No obstante, hay que tener presente que este tipo de análisis puede comportar la pérdida de otras evidencias, así como la invalidación de la prueba en un procedimiento judicial, ya que el análisis en caliente implica la manipulación del dispositivo original y, si no se hace con las herramientas forenses adecuadas, se puede alterar su evidencia.

5.3. Preservación de las evidencias digitales

Dada la facilidad con que las evidencias digitales se pueden modificar y/o eliminar, esta fase se convierte en el eslabón más crítico de todo el procedimiento. Es evidente que es del todo imposible obtener una "instantánea" completa de todo un sistema informático en un momento concreto (la naturaleza intrínseca de las evidencias volátiles así lo determina), aunque afortunadamente para el analista, en la gran mayoría de ocasiones, las pruebas determinantes se encuentran almacenadas en el sistema de ficheros, el cual continuará conservando la evidencia a pesar de la falta de alimentación eléctrica.

Localización de evidencias digitales

Podemos localizar evidencias digitales en impresoras, grabadores de tarjetas de banda magnética, discos USB, teléfonos y PDA, tarjetas de memoria, *tokens*, etc.

A diferencia de otras pruebas (por ejemplo, un análisis biológico de ADN), la evidencia digital se puede duplicar o clonar de manera exacta (en los bits), incluyendo los archivos ocultos, eliminados y no sobrescritos, e incluso el llamado *slack file* (al cual nos referiremos posteriormente), posibles particiones ocultas, o el espacio no asignado del disco duro. Así, en virtud de esta característica, y también como garantía de preservación de la prueba, el analista actuante acabará realizando un clon de la evidencia, ya sea en la escena del suceso o en las dependencias del laboratorio.

Apertura de un fichero

La apertura de un fichero implica, si no se utilizan herramientas de análisis forense, la alteración de la última fecha de acceso al archivo. La simple observación de la prueba, en análisis forense, puede implicar su alteración.

A primera vista, resulta tentador aplazar la clonación de los soportes informáticos al momento en que éstos lleguen al laboratorio (ya que es donde se podrá hacer el proceso con todo tipo de garantías y sin prisas), pero eso no siempre será posible. Si, por ejemplo, las evidencias se localizan en el servidor de una empresa, no es posible precintar el equipamiento porque entonces la empresa tendría que detener su actividad. En estos casos, es preferible detener momentáneamente la actividad de la empresa y obtener un clon allí mismo, para reanudar acto seguido la actividad empresarial, o bien realizar un análisis en caliente, con los inconvenientes que ya se han explicado.

Observación

Si nos encontramos un disco duro sumergido en un líquido, hay que conservarlo, siempre que sea posible, en el medio donde se ha encontrado.

La copia o clon se efectuará, normalmente, sobre dispositivos (CD, DVD, discos duros, etc.) aportados por el analista. La elección de uno u otro medio dependerá de la cantidad de información contenida en los soportes originales. Finalmente, el software o hardware utilizado para la obtención del clon calculará un CRC (código de redundancia cíclica) o un valor *hash* que tendrá que ser el mismo, tanto para el disco duro de origen, como para el destino, garantizando de esta manera que el proceso de copia ha funcionado correctamente.

Herramientas para hacer un clon

Existen diversas herramientas para obtener un clon:

- Mediante software: el pedido dd de Linux, Encase, Ilook, etc.
- Mediante hardware: Logicube, etc.

Además de la adquisición de la evidencia, en esta etapa también hay que documentar **quién** preservó la evidencia, **dónde** y **cómo** se hizo y **cuándo**. Acto seguido habrá que empaquetar las evidencias, identificándolas de manera unívoca. Este proceso se lleva a cabo embalando los paquetes con material protector que pueda proteger las evidencias de golpes, lluvia o cualquier otro elemento que pueda estropear los soportes. Esta fase acabará con el transporte de las evidencias a un sitio seguro o a las dependencias del laboratorio donde tengan que ser analizadas. El embalaje y el transporte de las evidencias es el inicio de la denominada **cadena de custodia**, la cual permite garantizar la in-

tegridad de las pruebas, desde su obtención hasta su disposición a la autoridad judicial o al laboratorio donde tengan que ser analizadas. La documentación de la cadena de custodia permite saber, en cualquier momento del proceso, dónde han sido almacenadas las evidencias y quién ha tenido acceso a ellas.

5.4. Análisis de las evidencias digitales

En esta fase, el experto tendrá que responder a las preguntas "policíacas" introducidas al inicio de este apartado 5. Este estudio se fundamentará, sobre todo, en el análisis del contenido de los archivos (datos) y de la información sobre estos ficheros (metadatos).

Ejemplo de metadato

El contenido del campo *autor* que aparece en todos los archivos de Microsoft Word es un buen ejemplo de metadato.

Normalmente, no se realizan análisis exhaustivos de los soportes objeto de interés (sería una tarea inalcanzable), sino que los informes periciales se limitan a responder aquellas cuestiones planteadas en los extremos del análisis.

Los extremos en un caso de intrusión

En un caso de intrusión, los extremos podrían ser: "Averiguar el usuario o usuarios que realizaron los accesos no autorizados en las fechas especificadas".

En general, hay cuatro categorías diferentes de datos que son susceptibles de ser analizados:

- **Datos lógicamente accesibles**. Es decir, los datos contenidos en archivos directamente accesibles. Este análisis, no exento de dificultades, puede no ser muy sencillo a causa de la enorme dificultad que puede existir a la hora de discriminar la información relevante de entre muchos millares de ficheros, la existencia de archivos cifrados, o la presencia de ficheros troyanizados, cuya ejecución podría producir consecuencias inesperadas.

- **Datos localizados en el llamado *ambient data***. Es decir, aquellos datos que aparecen en localizaciones no directamente visibles y que requieren el uso de software específico para ser recuperados. Un buen ejemplo de este tipo de datos es la información residual que se puede encontrar en clústers actualmente no asignados a ningún archivo, o aquella información localizada en el *slack file* (espacio entre el final lógico de un fichero y el final físico del mismo).

- **Datos que han sido borrados o eliminados**, pero que todavía no han sido sobrescritos por otros ficheros y que, por lo tanto, son susceptibles de ser recuperados utilizando las herramientas adecuadas a esta finalidad.

- **Datos ocultos mediante esteganografía**, los cuales son mucho más difíciles de detectar que los archivos cifrados.

Para realizar el análisis de las evidencias se pueden utilizar diversas herramientas, algunas de las cuales ya se han descrito previamente. Posiblemente una de las más conocidas es la herramienta EnCase, de código propietario, la cual abarca, con una interfaz muy amigable, todas las fases del análisis forense, desde la adquisición de los soportes originales y el análisis, hasta la generación automática del informe final. Otras herramientas, también muy conocidas,

son la herramienta Ilook (de momento gratuita para las Fuerzas y Cuerpos de Seguridad del Estado), la distribución de Linux Backtrack o la colección de programas *Coroner's Toolkit* (TCT), desarrollada por Dan Farmer y Wietse Venema.

5.5. Presentación e informe

En el informe elaborado por el experto se presentarán las evidencias relacionadas con el caso, la justificación del procedimiento utilizado y, lo más importante, las conclusiones. En muchas ocasiones el informe será ratificado en presencia del juez, o bien será entregado a empresas y abogados. No obstante, en ningún caso los destinatarios de las pericias tienen que disponer necesariamente de conocimientos informáticos para poder comprender el informe en profundidad. Por lo tanto, en general nunca se tiene que utilizar un lenguaje excesivamente técnico y, cuando haya que hacerlo, habrá que añadir notas aclaratorias a pie de página, o incluso redactar glosarios técnicos, a menudo añadidos al anexo del informe. En los casos en los que los informes tengan que ser defendidos ante el juez, el analista, además del rigor técnico, tiene que ser bastante hábil para comunicar el resultado del análisis de forma concisa y clara.

Resumen

En este módulo hemos estudiado los principios básicos de la administración de seguridad de un sistema informático y los hemos relacionado con las posibles responsabilidades que se pueden derivar de la vulneración de esta seguridad. Hemos dividido el módulo en los cinco apartados siguientes:

- Apartado 1: dedicado a las definiciones básicas relativas a la seguridad informática.

- Apartado 2: en este apartado hemos estudiado las condiciones de seguridad del entorno (control de acceso), y también las herramientas criptográficas que puede utilizar un administrador para proteger la información.

- Apartado 3: el tercer apartado estudia la seguridad del sistema en el sentido más general del término. Se ha escogido el sistema operativo Unix para explicar los conceptos de este apartado porque creemos que las posibilidades y la flexibilidad del Unix hacen que sea sencillo extrapolar los problemas de la seguridad del sistema (y sus soluciones) a cualquier otro sistema operativo y a las redes de ordenadores en general.

- Apartado 4: describe las responsabilidades en que puede incurrir el administrador de un sistema informático (tanto con respecto a la responsabilidad que adquiere sobre el sistema –hardware y software– como por los datos que allí se almacenan. Por otra parte, también enumeramos los posibles delitos de que puede ser víctima en el entorno laboral, y la manera de denunciarlos. La legislación todavía presenta muchos huecos con respecto a esta materia, por lo que somos conscientes de que la lectura del apartado puede generar (y lo tiene que hacer) muchas preguntas que no tienen una respuesta clara. Finalmente, se tiene que entender que la seguridad de un sistema informático no es consecuencia de la aplicación de ninguna fórmula magistral, sino de una serie de medidas que hay que mejorar y adaptar a las nuevas necesidades día a día.

- Apartado 5: describe qué se puede hacer una vez ha sucedido un problema de seguridad (o incluso un delito) para poder averiguar qué ha pasado y quién ha sido el autor. Se define el concepto de informática forense, una nueva disciplina situada a caballo entre la informática y la normativa legal.

Actividades

1. Diseñad un plan de seguridad física para una organización que conozcáis (un centro de cálculo, la organización en que trabajáis, el aula de informática de una facultad, etc.). Para hacerlo os podéis orientar con el esquema siguiente:

- Descripción de los recursos físicos que se quieren proteger.
- Descripción del espacio físico donde se localizan los recursos.
- Descripción del perímetro de seguridad.
- Enumeración de las amenazas que pueden comprometer la seguridad del sistema.
- Posibles medidas de seguridad contra las amenazas anteriores.
- Manera de implementar las medidas anteriores.
- Cálculo del coste estimado de la implementación de las medidas o mejoras que hay que hacer, y también del coste de los datos que hay que proteger y la probabilidad de que se produzca un ataque (accidental o no).

2. Buscad información sobre las asociaciones siguientes, relacionadas con la informática forense:

- International Association of Computer Investigative Specialist (IACIS). Esta asociación ofrece una certificación internacional (CFEC, Computer Forensic External), dirigida a analistas que no formen parte de los cuerpos policiales o judiciales.
- European Network of Forensic Science Institute (ENFSI).
- International Organisation on Computer Evidence (IOCE).
- Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas (es-CERT).

3. La función de un perito judicial consiste en proporcionar al juez la información necesaria para ayudarlo a determinar qué ha sucedido en el caso que se investiga. La figura del perito judicial se introduce en el artículo 456 (y siguientes) de la Ley de Enjuiciamiento Criminal. Buscad los artículos que definen esta figura y razonad las cuestiones siguientes:

a) ¿Creéis que es necesario disponer de la titulación universitaria en Informática para poder ejercer de perito?
b) ¿Cuáles son los derechos y deberes del perito?

Ejercicios de autoevaluación

1. Razonad brevemente cuál de las tres propiedades que tiene que satisfacer todo sistema informático "seguro" es prioritaria en los sistemas siguientes:

- Una organización de defensa nacional.
- Un sistema de transferencia electrónica de dinero.
- Un departamento de la universidad.

2. Relacionad correctamente los conceptos siguientes:

	DES	CAST	DSA	SHA-1	IDEA	RSA	MD5
C. PRIVADO							
C. PÚBLICO							
HASH							

3. La página web del servidor del departamento que administráis ha sido víctima de un ataque y ha sido sustituida por otra página con un contenido completamente diferente. ¿Cuáles son las acciones que tendréis que hacer para denunciar el hecho ante la policía?

4. Determinad si los siguientes enunciados son o no correctos:

a) El envío de correo no solicitado (*spam*) es una conducta que aparece tipificada en el Código penal.

b) La firma electrónica avanzada tiene la misma consideración que la firma manuscrita.
c) La intrusión en un sistema informático, en sí misma, no es una conducta tipificada en el Código penal.
d) La LSSICE obliga a los proveedores de servicios de Internet a mantener los ficheros de log durante un mínimo de tiempo.
e) La figura del responsable del fichero o tratamiento es la misma que la del tratamiento del fichero.

Solucionario

Ejercicios de autoevaluación

1. Confidencialidad, integridad y disponibilidad, respectivamente.

2. Relacionad correctamente los conceptos siguientes:

	DES	CAST	DSA	SHA-1	IDEA	RSA	MD5
C. PRIVADO	*	*			*		
C. PÚBLICO			*			*	
HASH				*			*

3. Acciones que hay que llevar a cabo en el caso de un delito de daños.

- Desconexión de la red.
- Hacer una copia de seguridad a bajo nivel.
- Compilar toda la información posible sobre el ataque (especialmente los ficheros log relativos a la dirección IP desde la cual, de forma presunta, se ha originado el ataque, o por medio de esta dirección).
- Restaurar el sistema y aplicar las actualizaciones de software (por ejemplo, una actualización que resuelva el problema de la vulnerabilidad de las CGI).
- Notificarlo a quien se considere conveniente y según el ataque (a nuestro jefe, al CERT, a otros administradores de otros sistemas implicados, a los usuarios de nuestro sistema, etc.).
- Solicitar una valoración de los daños producidos.
- Denunciar el hecho a la comisaría de policía más próxima y adjuntar a la denuncia toda la información posible sobre el ataque y la valoración de los daños producidos (hecha por la misma organización o bien por un perito externo).

4. a) Incorrecto.
b) Correcto.
c) Correcto.
d) Incorrecto.
e) Incorrecto.

Glosario

autenticación *f* Verificación de la identidad de una persona o proceso a la hora de acceder a un recurso o poder hacer una acción determinada.

análisis forense informático *m* Proceso de aplicación del método científico a los sistemas informáticos con la finalidad de asegurar, identificar, preservar, analizar y presentar la evidencia digital de forma que sea aceptada en un proceso judicial.

certificado digital *m* Documento electrónico firmado por una tercera parte o autoridad de certificación que asocia una clave pública a una persona.

cracking *m* Ved **piratería**.

criptosistemas de clave compartida *m pl* Criptosistemas en los cuales el emisor y el receptor comparten una única clave. Es decir, el receptor podrá descifrar el mensaje recibido únicamente si conoce la clave con la cual ha cifrado el mensaje el emisor.

criptosistemas de clave pública *m pl* Criptosistemas en que cada usuario *u* tiene asociada una pareja de claves <*Pu, Su*>. La clave pública, *Pu*, es accesible para todos los usuarios de la red y aparece en un directorio público, mientras que la clave privada, *Su*, tan sólo es conocida por el usuario *u*.

dato de carácter personal *f* Cualquier información relativa a las personas. En concreto, toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de ser recogida, registrada, tratada o transmitida y que concierne a una persona física identificada o identificable.

fichero automatizado *m* Conjunto organizado de datos que es objeto de tratamiento automatizado.

footprinting *m* Ved **técnica de la huella**.

función *hash* *f* Función matemática que hace corresponder una representación de tamaño fijo a un mensaje m de tamaño variable.
sin. **función resumen**.

National Institute of Standards and Technology *m* Organismo creado en 1901 para proveer a la industria norteamericana de las medidas y la tecnología para mantener la competitividad en los mercados mundiales y el comercio, hoy ofrece servicios que cubren un amplio abanico de actividades tecnológicas y comerciales (normas, transferencia de tecnologías, bases de datos, materiales de referencia, etc.).
Ved **los algoritmos SHA y AES**.
sigla: **NIST**.

NIST *m* Ved **National Institute of Standards and Technology**.

piratería *f* Ataque de fuerza bruta dirigido a romper una clave de acceso a un programa o servicio.
en cracking.

plan de contingencia *m* Protocolo de actuación establecido que se tiene que iniciar cuando se produce una emergencia o desastre.

política de seguridad *f* Conjunto de directrices o estrategias que tienen que seguir los usuarios en relación con la seguridad global del sistema informático.

responsable del fichero *m y f* Persona física o jurídica, pública o privada, y órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento.

seguridad informática *f* Conjunto constituido por diversas metodologías, documentos, software y hardware, que determinan que los accesos a los recursos de un sistema informático sean llevados a cabo exclusivamente por los elementos autorizados a hacerlo.

spoofing *f* Técnica de ataque a un sistema informático en la que el intruso simula una dirección IP de origen, diferente de la dirección IP real del atacante.

técnica de la huella *f* Actividad consistente en la recogida de información sobre el objetivo que se quiere atacar utilizando métodos indirectos: determinación de los dominios y direcciones IP de los sistemas objetivo (busca de información en los servidores *whois* o en las bases de datos *Arin* o *Ripe*, etc.).

en footprinting.

tratamiento de datos *m* Operaciones y procedimientos que permiten la recogida, la grabación, la conservación, la elaboración, la modificación, el bloqueo y la cancelación y las cesiones de datos.

Bibliografía

Bibliografía básica

Anónimo (2000). *Linux máxima seguridad*. Prentice Hall.

Colobran Huguet, M.; Morón Lerma, E. (2004). *Introducción a la seguridad informática*. Planeta UOC.

Dhanjani, N. (2008). *Claves hackers en Linux y UNIX*. McGraw-Hill.

Jimeno García, M. T.; Míguez Pérez, C.; Matas García, A. M.; Pérez Agudín, J. (2008). *Guía práctica hacker*. Ediciones Anaya Multimedia.

Nemeth, E.; Snyder, G.; Hein, T. (2008). *Administración de sistemas Linux, Edición 2008*. Ediciones Anaya Multimedia.

Villalón Huerta, A. (2002). *Seguridad en UNIX y redes. Version 2.1*.

Bibliografía complementaria

Domingo i Ferrer, J. (1999). *Criptografia*. Barcelona: Universitat Oberta de Catalunya.

Guasch Petit, A.; Martínez de Carvajal Hedrich, E.; Peiró Mir, M.; Ríos Boutin, J.; Roca i Marimon, J. (2005). *Auditoria, peritatges i aspectes legals per a informàtics*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

López Sánchez-Montañés, J.; Belles Ramos, S.; Aulí Llinàs, F.; Baig Viñas, R. (2008). *Sistema operatiu GNU/Linux bàsic*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.