Introducción

Este libro surge con el propósito de acercar al lector a los aspectos más importantes que encierra la seguridad informática y los relativos a garantizar alta disponibilidad en los sistemas críticos, ante las crecientes amenazas sobre los sistemas informáticos, donde cada vez contenemos más valiosa información. Con la reforma curricular de formación profesional, enmarcada en la Ley Orgánica de Educación (LOE), los ciclos formativos de la familia profesional de Informática y Comunicaciones poseen como contenido transversal la materia de seguridad informática, debido a la creciente demanda de personal cualificado para su administración. Con tal propósito, puede servir de apoyo también para estudiantes del las Ingenierías Técnicas.

Hoy en día, existen muchos usuarios y profesionales de la Informática que discuten las ventajas e inconvenientes de la utilización de un determinado sistema operativo, antivirus o cortafuegos como solución única a los problemas de la seguridad informática, no entendiendo que en esta materia ha de trabajarse en todos los frentes posibles. Aquí no hay preferencia por ningún sistema en particular, ni se intenta compararlos para descubrir cuál es el mejor de todos, sino enriquecer los contenidos al exponer sus principales características, manejo y métodos para conseguir la máxima fiabilidad de los sistemas.

A lo largo del libro se analiza la seguridad informática y la alta disponibilidad desde distintas perspectivas, con un total de **51 prácticas**, para completar una visión global de la materia y no dejar ningún aspecto vulnerable:

- **Principios básicos** y problemática de la Seguridad y Alta disponibilidad. Capítulo 1.
- **Seguridad pasiva**, analizando soluciones de copia de seguridad y seguridad física y ambiental en los sistemas informáticos. Capítulo 2.
- **Seguridad lógica**. Gestión de usuarios, privilegios, contraseñas y actualizaciones de sistemas y software. Capítulo 3.
- **Software de seguridad** *antimalware*. Capítulo 4.
- **Criptografía** en comunicaciones y protección de la información. Capítulo 5.
- **Seguridad en redes corporativas**, atendiendo a las amenazas internas y estudiando los fundamentos de comunicaciones seguras, con especial atención a inalámbricas. Capítulo 6.
- **Seguridad perimetral** mediante configuración de cortafuegos y proxy. Capítulo 7.
- **Configuraciones avanzadas de alta disponibilidad**, como redundancia en el almacenamiento mediante RAID, balanceo de carga, virtualización de servidores. Capítulo 8.
- **Normativa legal** en materia de seguridad informática. LOPD y LSSICE. Capítulo 9.

Uno de los objetivos de este libro es darnos a conocer las innovaciones en ataques y vulnerabilidades más actuales en materia informática, haciéndonos más prevenidos y aprendiendo a realizar acciones totalmente seguras. Para ello se presentan en cada capítulo **noticias de actualidad** relacionadas con la temática del mismo, que permitan la reflexión y el conocimiento de nuevos avances.

Para todo aquel que use este libro en el entorno de la enseñanza (Ciclos Formativos o Universidad), se ofrecen varias posibilidades: utilizar los conocimientos aquí expuestos para inculcar aspectos genéricos de la seguridad informática y alta disponibilidad o simplemente centrarse en preparar a fondo alguno de ellos.

Ra-Ma pone a disposición de los profesores una guía didáctica para el desarrollo del tema que incluye las soluciones a los ejercicios expuestos en el texto. Puede solicitarla a *editorial@ra-ma.com*, acreditándose como docente y siempre que el libro sea utilizado como texto base para impartir las clases.

1 Principios de seguridad y alta disponibilidad

OBJETIVOS DEL CAPÍTULO

- ✓ Analizar la problemática general de la seguridad informática.
- ✓ Conocer los principios sobre los que se sustenta.
- ✓ Conocer el significado de alta disponibilidad.
- ✓ Identificar las principales vulnerabilidades, ataques y medidas de seguridad a adoptar sobre los sistemas.
- ✓ Diferenciar la seguridad física y lógica, y la pasiva de la activa.

Con la proliferación de la informática en todos los ámbitos de la vida, el número de usuarios y profesionales de informática ha crecido exponencialmente en los últimos años, del mismo modo que las necesidades de comunicación y compartición de recursos en red.

Las dos nuevas problemáticas que subyacen de esta nueva realidad son, por un lado asegurar los sistemas y la información que disponemos, y por otro poder tener acceso a los servicios el mayor tiempo posible, sin interrupciones y con un cierto nivel de calidad, siendo la base para el estudio de la seguridad informática y la alta disponibilidad respectivamente.

1.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

Las tecnologías de la información y la comunicación (TIC), y concretamente la informática, se ha instalado en todos los ámbitos de la sociedad: sanidad, educación, finanzas, prensa, etc., siendo cada vez más útil e imprescindible para el desarrollo de sus actividades cotidianas. Del mismo modo que se extiende el uso de la informática, la seguridad informática debe tener una importancia cada vez mayor, teniendo en cuenta que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros.

La seguridad informática consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Los **principales objetivos** de la seguridad informática por tanto son:

- ✓ Detectar los posibles problemas y amenazas a la seguridad, minimizando y gestionando los riesgos.
- ✓ Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
- ✓ Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- ✓ Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

Durante el desarrollo del libro, veremos que el conjunto de vulnerabilidades, amenazas, ataques y medidas de seguridad han ido aumentando y modificándose con el tiempo, **siendo necesario estar al día en esta materia**. Para ello haremos uso de diversas noticias de actualidad y reflexiones sobre las mismas.

La comunidad de usuarios y profesionales en materia de seguridad informática mantienen al día al resto de usuarios mediante noticias y post en blogs y webs especializadas. Sírvase como ejemplo el blog y repositorio de blogs de seguridad informática disponible en la web del Instituto Nacional de Tecnologías de la comunicación S.A. (en adelante INTECO), sociedad anónima estatal adscrita a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información:

http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad

NOTICIA DE ACTUALIDAD

La seguridad informática lleva asociada un conjunto de palabras, en muchos casos nuevos términos en inglés. A lo largo del libro y en los artículos de actualidad se irán repitiendo, por lo que es recomendable ir construyendo nuestro glosario de términos con palabras como *pharming*, *tabnabbing*, *malware*, *sniffing*, *spoofing*, *phishing*, *scam*, *spam*, *botnet*, *spyware*, *keylogger*, etc.

Te proponemos que leas un artículo de actualidad, que podrás encontrar descargando el material adicional y en la web *www.securitybydefault.com/2010/01/origen-y-evolucion-del-efraude.html*, en el cual deberás identificar palabras relacionadas con conceptos de seguridad informática que no conozcas y realizar un glosario de términos con sus definiciones. Comenta en grupo las siguientes cuestiones:

- **¿Has recibido alguna vez un intento de *phishing* mediante correo electrónico de tipo *spam*? ¿Podrías indicar algún ejemplo?**
- **Realizar un debate en el que se analicen las más conocidas amenazas existentes en la actualidad y qué tipo de medidas de prevención preliminares se podrían tomar.**

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independientemente de las medidas que tomemos, por lo que debemos hablar de niveles de seguridad. **La seguridad absoluta no es posible** y en adelante entenderemos que la seguridad informática es un conjunto de **técnicas** encaminadas a obtener **altos niveles de seguridad** en los sistemas informáticos.

Podemos entender como seguridad una característica de cualquier sistema que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas informáticos, sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de **fiabilidad**, probabilidad de que un sistema se comporte tal y como se espera de él. Por tanto, se habla de tener sistemas fiables en lugar de sistemas seguros.

> El experto Eugene H. Spafford cita en su frase célebre: "el único sistema que es totalmente seguro es aquel que se encuentra apagado y desconectado, guardado en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armados. Aún así, no apostaría mi vida en ello".

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: confidencialidad, integridad y disponibilidad.

- **Confidencialidad**: cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado. Comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene.
- **Integridad**: cualidad de mensaje, comunicación o datos, que permite comprobar que no se ha producido manipulación alguna en el original, es decir, que no ha sido alterado.
- **Disponibilidad**: capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento que se necesite, evitando su pérdida o bloqueo.

Hay que tener en cuenta que, tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad. Generalmente **tienen que existir los tres aspectos descritos para que haya seguridad**.

Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad. Por ejemplo, en un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad. En cambio, en un servidor de archivos en red, se priorizará la disponibilidad frente a la confidencialidad. En un entorno bancario, la faceta que más ha de preocupar a los responsables del sistema es la integridad de los datos, frente a su disponibilidad o su confidencialidad: es menos grave que un usuario consiga leer el saldo de otro que el hecho de que ese usuario pueda modificarlo.

Junto a estos tres conceptos fundamentales se suelen estudiar conjuntamente la **autenticación** y el **no repudio**.

- **Autenticación**: verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario en informática, cuando el usuario puede aportar algún modo que permita verificar que es quien dice ser, se suele realizar mediante un usuario o *login* y una contraseña o *password*.
- **No repudio** o **irrenunciabilidad**: estrechamente relacionado con la autenticación y permite probar la participación de las partes en una comunicación. Existen dos posibilidades:
  - **No repudio en origen**: el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el destinatario.
  - **No repudio en destino**: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Si la autenticidad prueba quién es el autor o el propietario de un documento y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

Al grupo de estas características y objetivos de la seguridad se les conoce como **CIDAN**, nombre sacado de la inicial de cada característica. La relación de los mismos se presenta en la figura siguiente.

En la imagen superior se ilustra cómo se relacionan los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de nivel interior, no puede aplicarse el exterior. De esta manera, la **disponibilidad** se convierte en el **primer requisito de seguridad**, cuando existe ésta, se puede disponer de **confidencialidad**, que es imprescindible para conseguir **integridad**, imprescindible para poder obtener **autenticación** y, por último, el **no repudio**, que solo se obtiene si se produce previamente la autenticación.

A continuación veremos tres casos prácticos a modo de ejemplo sobre confidencialidad, integridad y disponibilidad.

PRÁCTICA 1.1

CONFIDENCIALIDAD

En esta práctica guiada estudiaremos cómo se puede asegurar la confidencialidad de los datos en sistema Windows, mediante la encriptación de archivos y carpetas.

La confidencialidad o privacidad de datos es uno de los aspectos críticos de la seguridad, por esto Microsoft incluyó a partir de su sistema Windows 2000, y posteriores, el método de archivos encriptados conocido como **EFS** (*Encrypted File System*) que cumple este propósito.

Encrypting File System (EFS) es un sistema de archivos que, trabajando sobre NTFS, permite cifrado de archivos a nivel de sistema. Permite a los **archivos administrados por el sistema operativo** ser cifrados en las particiones NTFS en donde esté habilitado, para proteger datos confidenciales. EFS es incompatible con la compresión de carpetas.

El usuario que realice la encriptación de archivos será el único que dispondrá de acceso a su contenido, y al único que se le permitirá modificar, copiar o borrar el archivo, **controlado todo ello por el sistema operativo**.

Amenaza o vulnerabilidad

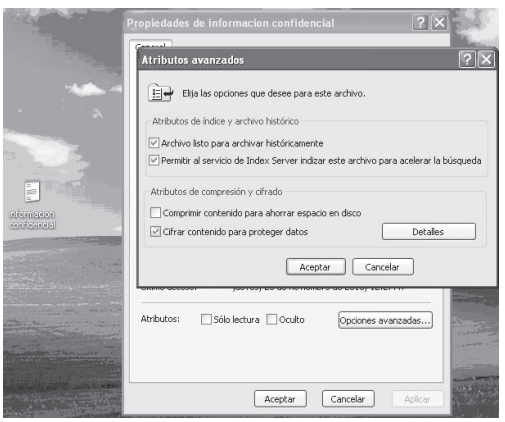
Como veremos en capítulos posteriores, en un sistema personal es posible obtener el acceso al sistema de ficheros si podemos arrancar desde una distribución USB o CD/DVD Live, o incluso acceder al sistema local como administrador, realizando una escalada de privilegios, teniendo de este modo permisos para acceder al sistema de ficheros por completo y por tanto incluso a carpetas restringidas por el sistema operativo. Para evitar la

apertura, lectura o modificación de información privada bajo sistemas Windows podemos utilizar las opciones de encriptación EFS.

Proceso de encriptación

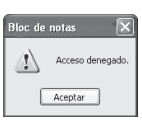
Para probarlo podemos crear un archivo de texto plano (no cifrado) con una información confidencial en su interior. En primer lugar seleccionaremos el archivo (o carpeta) a encriptar y con el botón derecho accederemos a la ventana de **Propiedades**. En su pestaña **General** pulsaremos sobre **Opciones Avanzadas** y en **Atributos de compresión y cifrado** marcaremos la opción de **Cifrar contenido para proteger datos**.

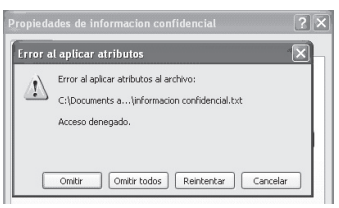
Nota: En caso de no tener habilitada dicha opción deberá ejecutar *gpedit.msc* (editor de directivas de grupo) y habilitar la directiva local, *Directiva de equipo local\Configuración de Windows\Configuración de seguridad\Directivas de clave pública\Sistema de cifrado de archivos*. Gpedit no se encuentra preinstalado en las versiones *Home* de los sistemas operativos Windows.



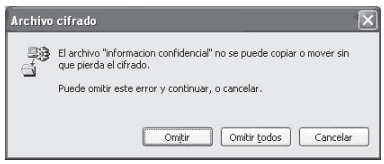
Verificaciones

1. Si accedemos con otro usuario al sistema que tenga permisos para acceder a todo el sistema de archivos, por ejemplo desde una cuenta de tipo administrador (distinta a la que ha cifrado el archivo), podemos ver que el nombre del archivo nos aparecerá en color verde y, al intentar acceder a él, nos indicará acceso denegado. Igualmente si intentamos modificar el archivo para que deje de estar cifrado y aplicamos los cambios nos indicará error al aplicar los atributos. Aunque no es posible leer ni modificar su contenido, sí es posible borrarlo.



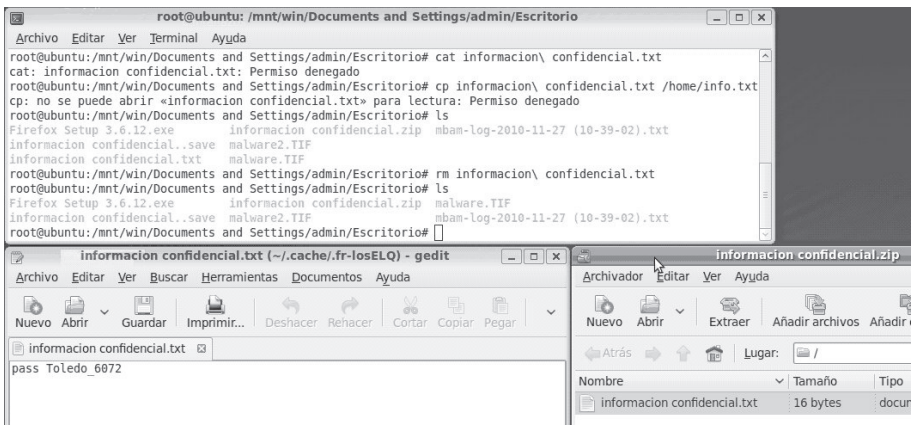


2. El archivo cifrado no es portable o copiable a una unidad externa ya que el sistema operativo pierde el control sobre su cifrado. En caso de intentar enviarlo a unidad USB nos indicará lo siguiente.



Una recomendación más, no comprimir los archivos cifrados ya que dejan de estarlo.

3. En caso de tener acceso al sistema de archivos con un arranque desde una distribución modo Live (en nuestro ejemplo Ubuntu), montando la partición correspondiente (en este caso el punto de montaje */mnt/win*) podremos borrar el archivo, pero no se nos permitirá ni copiarlo ni leer la información contenida. Si hemos comprimido el archivo en zip desde Windows, sí podremos acceder a su contenido confidencial.



PRÁCTICA 1.2

INTEGRIDAD

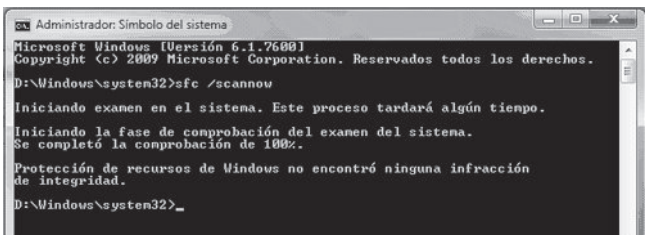
Amenaza o vulnerabilidad

En caso de que algún tipo de *malware* reemplace o falsifique archivos del sistema operativo, ocultándose para realizar tareas no autorizadas, la búsqueda y detección del mismo se complica ya que los análisis *antimalware* y de los procesos sospechosos por parte de administradores de sistemas, no dudarán de la veracidad de dichos archivos y procesos. A este tipo de *malware* se le denomina **rootkit**, programa que sustituye los ejecutables binarios del sistema para ocultarse mejor, pudiendo servir de puertas trasera o *backdoor* para la ejecución *malware* remota.

System File Checker (**SFC**) es una utilidad de los sistemas Windows que comprueba la integridad de los archivos de sistema. **Rootkit hunter** es una herramienta más completa bajo GNU/Linux que entre otras tareas, como examinar los permisos de los ejecutables del sistema, buscar *rootkits* conocidos rastreando ficheros ocultos, realiza la comprobación de integridad de los archivos de sistema, es decir, verifica que no han sido modificados.

Verificación Windows

SFC examina la integridad de todos los archivos de sistema protegidos de Windows y reemplaza los que están corruptos o dañados por versiones correctas, si es posible.



En este proceso, si el sistema detecta que tiene algún problema, puede ser que nos solicite el disco de instalación de Windows en el caso de que necesite reparar algún fichero dañado. Si el proceso determina que no hay errores, al final nos mostrará un texto como el de la ventana de arriba, "Protección de recursos de Windows no encontró alguna infracción de integridad".

Si recibes un mensaje diciendo que no puede reparar algunos archivos, podemos averiguar qué archivos son y qué pasa con ellos. Cuando se ejecuta sfc, crea un archivo LOG que podemos consultar en la carpeta *C: \ WINDOWS \LOGS\CBS\CBS.log*.

Sintaxis de sfc

sfc[/scannow] [/scanonce] [/scanboot] [/revert] [/purgecache] [/cachesize=x]

Los parámetros más usados son:

- ✓ */scannow*: explora de inmediato todos los archivos del sistema protegidos.
- ✓ */scanboot*: explora todos los archivos del sistema protegidos cada vez que se reinicia el equipo.
- ✓ */?*: muestra la Ayuda en el símbolo del sistema.

Si sfc descubre que un archivo protegido se ha sobrescrito, recupera la versión correcta del archivo de la carpeta *raízDelSistema\system32\dllcache* y luego reemplaza el archivo incorrecto.

Si la carpeta *raízDelSistema\system32\dllcache* está dañada o es inservible, se puede utilizar sfc */scannow* o sfc */scanboot* para reparar el contenido del directorio Dllcache.

Verificación GNU/Linux

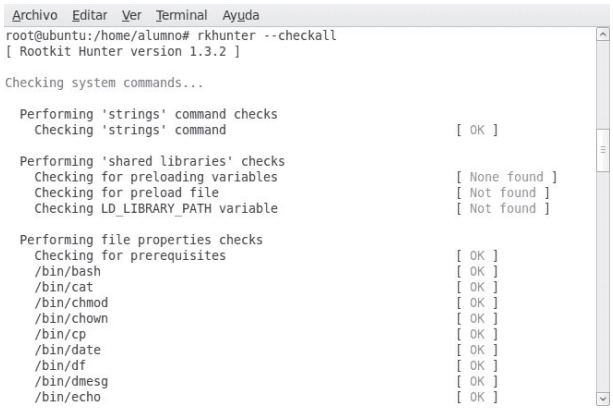
1. *Rootkit Hunter* se puede instalar mediante el comando:

   sudo aptitude install rkhunter

   Se recomienda antes de ejecutarlo, como todo software de seguridad actualizará a la versión más actual: sudo rkhunter - -update

2. Para la ejecución sobre el sistema, verificando todas sus opciones:

   sudo rkhunter - -checkall



Comprueba, entre otros aspectos, las cadenas y atributos de los comandos o ejecutables del sistema, la existencia de archivos *rootkits*, etc.

Una vez finalizado nos dará un informe completo con las advertencias y posibles archivos sospechosos encontrados.

PRÁCTICA 1.3

DISPONIBILIDAD

Identificar y analizar la **disponibilidad** de servicios o servidores, puertos abiertos y versiones de sistemas operativos que los soportan, supone la información base para el estudio de las innumerables **vulnerabilidades de los sistemas en red**. De este modo se podrán tomar medidas frente a estos puntos débiles de nuestros sistemas.

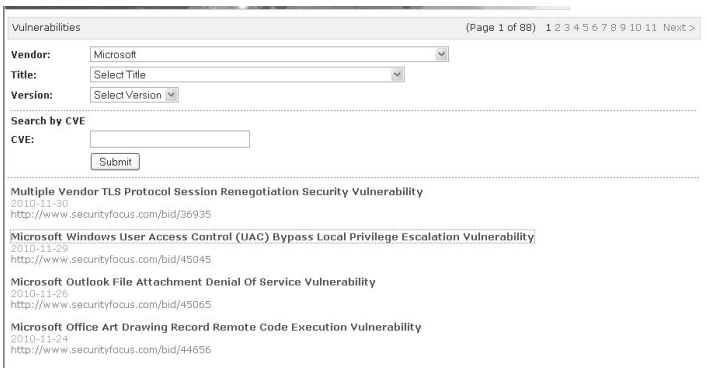
Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Utiliza paquetes IP para determinar qué **equipos** se encuentran disponibles en una red, qué **servicios** ofrecen y mediante qué **aplicaciones** (nombre y versión de la aplicación), qué **sistemas operativos** (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando, así como otras características.

Aunque generalmente se utiliza Nmap en **auditorías de seguridad**, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

Amenaza o vulnerabilidad

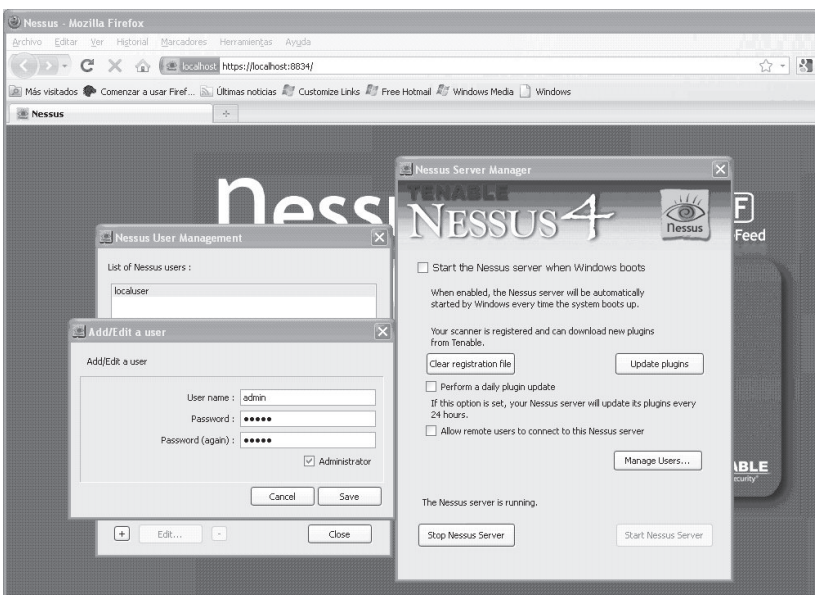
Para las versiones de software de servidores y de los sistemas operativos es posible **buscar posibles vulnerabilidades existentes**:

- *www.securityfocus.com*. Informes sobre vulnerabilidades en aplicaciones y sistemas operativos, se puede buscar información sobre las versiones de los productos de distintos fabricantes e incluso descargar *exploits* de verificación.

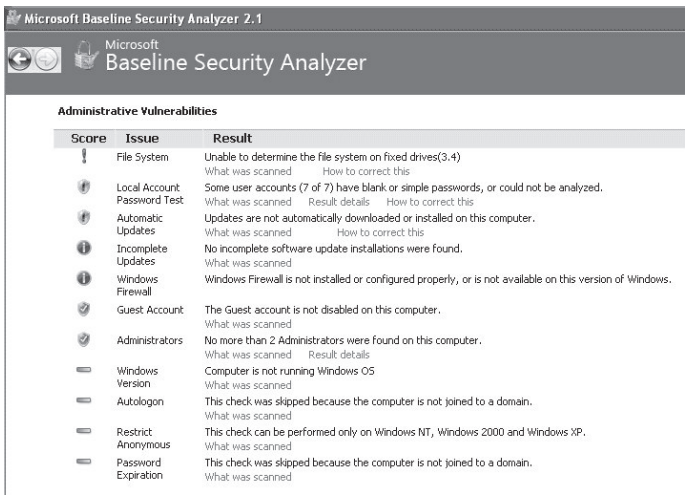


Ejemplo de búsqueda de vulnerabilidades por fabricante, en este caso Microsoft.

- *www.nessus.org*. Aplicación que detecta vulnerabilidades, tanto para sistemas y aplicaciones de Windows como GNU/Linux. En su última versión Nessus4 funciona como servidor web.

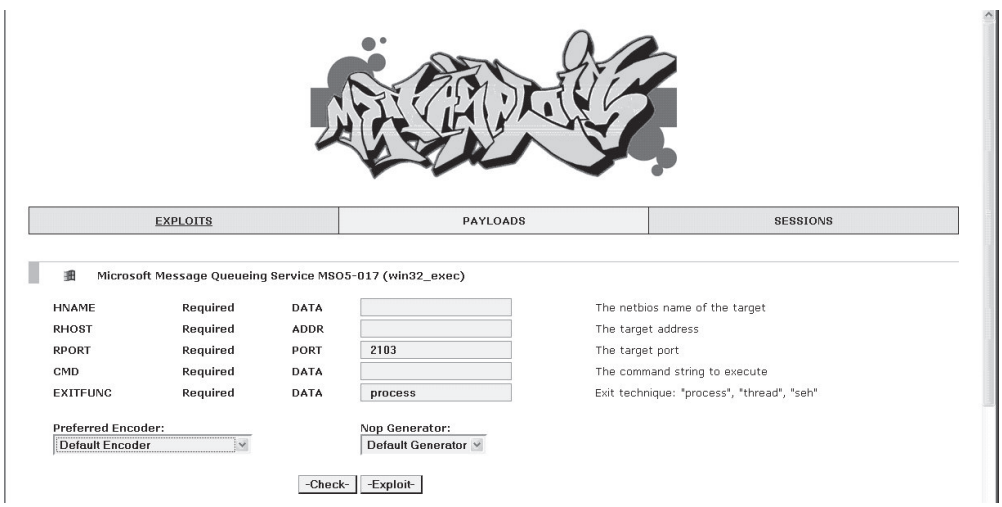


- *Microsoft Baseline Security Analyzer* (MBSA) es una herramienta diseñada para analizar el estado de seguridad según las recomendaciones de seguridad de Microsoft y ofrece orientación de soluciones específicas. Sirve para detectar los **errores más comunes de configuración de seguridad y actualizaciones de seguridad** que falten. En la siguiente imagen, a modo de ejemplo, vemos el resultado de un análisis en el cual se analizan aspectos como:
  - Sistema de ficheros. Recomendado NTFS por su mayor nivel de seguridad.
  - Cuentas de usuario. Analiza si poseen contraseñas y son seguras.
  - Actualizaciones. Analiza si el sistema posee las últimas actualizaciones que previenen de vulnerabilidades actuales.
  - Cortafuegos activo y configurado.
  - Número de cuentas de administrador.



Del análisis y estudio de estas vulnerabilidades se aprovechan los desarrolladores de *exploits* (del inglés *to exploit*, explotar o aprovechar), software, un fragmento de datos o una secuencia de comandos que pretende aprovecharse de un error, fallo o vulnerabilidad de una aplicación o sistema operativo. El fin del *exploit* puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros. Como ejemplo de posible consecuencia de la ejecución de un *exploit*, la toma de control de un sistema, mediante su consola de comandos.

Para explorar las vulnerabilidades más comunes existen aplicaciones como **metasploits**, herramienta con interfaz modo comando y web, que posee un conjunto de *exploits* para aprovechar las vulnerabilidades más conocidas de puertos, sistemas y aplicaciones.



Metasploits en su formato web, a través del puerto 55555. Tras buscar y seleccionar la vulnerabilidad a explorar (dispone de filtros de búsqueda por fabricante, puerto o aplicación), indicaremos la máquina (IP destino) en la cual queremos rastrear la vulnerabilidad y, a continuación, ejecutaremos el escaneo.

Recomendación

Por todo esto es de vital importancia **actualizar los sistemas**, tanto el sistema operativo como el resto de aplicaciones, tan pronto como sea posible.

Para facilitar esta tarea, la mayoría de **aplicaciones** tienen la opción de que las **actualizaciones se realicen automáticamente**, lo que permite tener los programas actualizados sin la necesidad de comprobar manual y periódicamente si la versión utilizada es la última disponible, y por tanto la más segura.

Recomendamos **activar la notificación de actualizaciones automáticas**, sobre todo de las aplicaciones más utilizadas y más expuestas a un posible ataque, sistema operativo, navegadores web, programas de ofimática, reproductores multimedia, etc., y **controlar la veracidad** de las actualizaciones **antes de instalarlas**.

Actualmente existe software malicioso (*malware*) que **sobrescribe las actualizaciones de aplicaciones conocidas**, como es el caso de algunos de los productos de Adobe y Java. A modo de ejemplo, existe una **variante del** *malware* **que imita Adobe Reader 9** y sobrescribe AdobeUpdater.exe encargado de comprobar si está disponible una nueva versión del software. De esta forma si hemos sido infectados y se ha sobrescrito dicha aplicación, al notificarnos que una nueva versión está disponible, si la instalamos, en realidad estaremos instalando aplicaciones *malware*.

Verificación

Nmap es una aplicación que puede utilizarse en modo comando o mediante una interfaz gráfica denominada znmap o zenmap. Se puede obtener la versión más reciente de Nmap en *http://www.insecure.org/nmap/*.

A continuación se puede ver un resumen de un análisis típico en modo comando con Nmap. Los únicos parámetros de Nmap que se utilizan en este ejemplo son la opción –A, que habilita la detección de sistema operativo y versión, y la opción -T4 que acelera el proceso, y después el nombre de los dos objetivos.

```
# nmap -A -T4 scanme.nmap.org saladejuegos
Starting nmap ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11


Interesting ports on saladejuegos.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
```

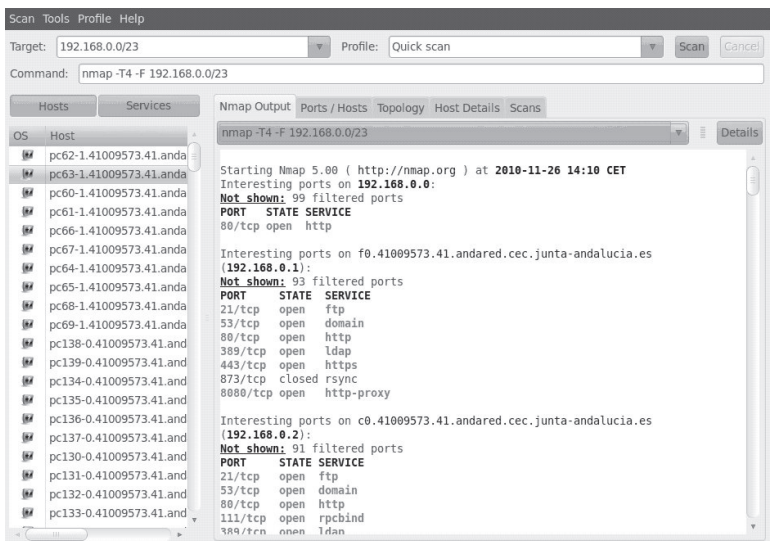
Podemos ver después de este escaneo modo comando las versiones de los sistemas operativos de dichas máquinas, direcciones MAC e IP, puertos abiertos (22 SSH, 80 HTTP, 53 DNS, 135 MSRPC, etc.) o cerrados y versiones de las aplicaciones (OpenSSH 3.91, Apache httpd 2.0.52, etc.).

En el caso de distribuciones GNU/Linux es posible descargarse de la web del desarrollador el paquete de instalación, descomprimirlo y compilarlo, mediante los siguientes comandos (versión del ejemplo nmap 5.35):

```
bzip2 -cd nmap-5.35DC1.tar.bz2 | tar xvf -
cd nmap-5.35DC1
./configure
make
su root
make install
```

La versión gráfica ZNMAP o ZENMAP para Linux puede obtenerse mediante el comando: *sudo apt-get install zenmap*.

A continuación se muestra un escaneo rápido (*Quick scan*) sobre la red 192.168.0.0/23 equivalente al comando nmap –T4 –F 192.168.0.0/23. Por cada máquina encontrada en la red informa sobre IP, nombre dentro del dominio, puertos abiertos, etc.



Una vez finalizado podremos buscar para los puertos o servicios más vulnerables e inseguros, como por ejemplo telnet (puerto 23), qué equipos se encuentran con dicho puerto abierto. En el capítulo 6, sobre seguridad en redes corporativas volveremos a hacer uso de esta aplicación.

1.2.1 ALTA DISPONIBILIDAD

La alta disponibilidad (*High Availability*) se refiere a la **capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones, debido principalmente a su carácter crítico**. El objetivo de la misma es mantener nuestros sistemas funcionando las 24 horas del día, 7 días a la semana, 365 días al año, manteniéndolos a salvo de interrupciones, teniendo en cuenta que se diferencian dos **tipos de interrupciones**:

- Las **interrupciones previstas**, que se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software.
- Las **interrupciones imprevistas**, que suceden por acontecimientos imprevistos (como un apagón, un error del hardware o del software, problemas de seguridad, un desastre natural, virus, accidentes, caídas involuntarias del sistema).

Las **métricas** comúnmente utilizadas para medir la disponibilidad y fiabilidad de un sistema son el tiempo medio entre fallos o **MTTF** (*Mean Time To Failure*) que mide el tiempo medio transcurrido hasta que un dispositivo falla, y el tiempo medio de recuperación o **MTTR** (*Mean Time To Recover*) mide el tiempo medio tomado en restablecerse la situación normal una vez que se ha producido el fallo. El tiempo en el que un sistema está fuera de servicio se mide a menudo como el cociente MTTR/MTTF. Lógicamente, nuestro principal objetivo es aumentar el MTTF y reducir el MTTR de forma que minimicemos el tiempo de no disponibilidad del servicio.

Existen distintos **niveles de disponibilidad** del sistema, según el tiempo aproximado de tiempo en inactividad por año se determina el porcentaje de disponibilidad. El mayor nivel de exigencia de alta disponibilidad acepta 5 minutos de inactividad al año, con lo que se obtiene una disponibilidad de 5 nueves: 99,999%.

Como **ejemplos de sistemas y servicios de alta disponibilidad** podemos mencionar sistemas sanitarios, control aéreo, de comercio electrónico, bancarios, transporte marítimo, militares, etc., donde la pérdida o interrupción de conectividad pueden suponer graves consecuencias personales y económicas. En el Capítulo 8 profundizaremos en algunas de las técnicas que permiten mejorar la disponibilidad de los sistemas y servicios ofrecidos por estos.

1.3 ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS

La seguridad **es un problema integral**: los problemas de seguridad informática no pueden ser tratados aisladamente ya que la seguridad de todo el sistema es igual a la de su punto más débil. Al asegurar nuestra casa no sirve de nada ponerle una puerta blindada con sofisticada cerradura si dejamos las ventanas sin protección.

La educación de los usuarios es fundamental para que la tecnología de seguridad pueda funcionar. Es evidente que por mucha tecnología de seguridad que se implante en una **organización**, si no existe una clara disposición por parte de los directivos de la empresa y una cultura a nivel de usuarios, no se conseguirán los objetivos perseguidos con la implantación de un sistema de seguridad. Por tanto, la seguridad informática precisa de **un nivel organizativo**, que posibilite unas normas y pautas comunes por parte de los usuarios de sistemas dentro de una empresa, por lo que diremos que:

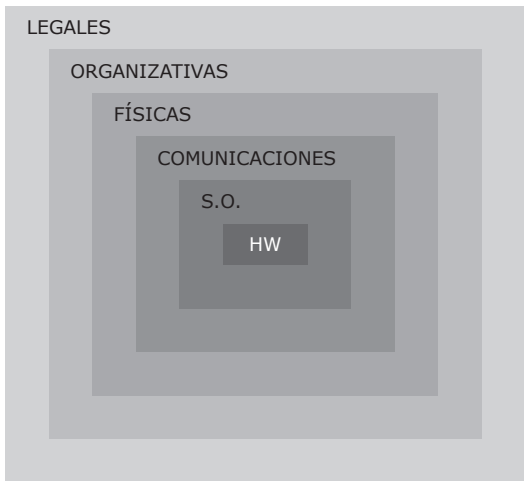
Sistema de Seguridad = TECNOLOGÍA + ORGANIZACIÓN

Los tres elementos principales a proteger en cualquier sistema informático son el *software,* el *hardware* y los datos. En las auditorías de seguridad se habla de un cuarto elemento a proteger, de menor importancia desde el punto de vista de la seguridad informática, los fungibles (elementos que se gastan o desgastan con el uso continuo, como papel de impresora, tóner,...).

Habitualmente **los datos constituyen el principal elemento** de los tres **a proteger**, ya que es el más amenazado y seguramente **el más difícil de recuperar**: con toda seguridad un servidor estará ubicado en un lugar

de acceso físico restringido, o al menos controlado, y además en caso de pérdida de una aplicación (o un programa de sistema, o el propio núcleo del sistema operativo) este *software* se puede restaurar sin problemas desde su medio original (por ejemplo, el CD o DVD con el sistema operativo que se utilizó para su instalación). Sin embargo, en caso de pérdida de una base de datos o de un proyecto de un usuario, no tenemos un medio "original" desde el que restaurar, hemos de pasar obligatoriamente por un sistema de copias de seguridad, y a menos que la **política de copias** sea muy estricta, es difícil devolver los datos al estado en que se encontraban antes de la pérdida.

También debemos ser conscientes de que las medidas de seguridad que deberán establecerse se deben contemplar a diferentes niveles, desde aspectos más **locales**, **personales** o **individuales** hasta los **globales** que afectan a una **organización**, o incluso la ciudadanía y empresas en su conjunto, como son las **leyes**. Por tanto la seguridad informática comprenden el hardware y el sistema operativo, las comunicaciones (por ejemplo, protocolos y medios de transmisión seguros), medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad de usuarios, niveles de acceso, contraseñas, normas, procedimientos, etc.) y legales (por ejemplo, la Ley Orgánica de Protección de Datos, LOPD).



Distintos niveles de profundidad relativos a la seguridad informática

Este esquema sirve de base para el desarrollo del libro analizando la seguridad informática desde distintas perspectivas, completando una visión global de la materia:

- **Seguridad pasiva**: Seguridad física y ambiental y copias de seguridad en los sistemas informáticos. Capítulo 2.
- **Seguridad lógica**: control de acceso a los sistemas, gestión de sistemas operativos: usuarios, privilegios, contraseñas en el Capítulo 3, software de seguridad *antimalware* en el Capítulo 4 y cifrado en la información y comunicaciones mediante el estudio de la criptografía en el Capítulo 5.
- **Seguridad en redes corporativas**: estudiando protocolos y aplicaciones seguras como SSH, TLS/SSL y VPN, configuraciones seguras en inalámbricas en el Capítulo 6 y protegiendo especialmente la seguridad perimetral mediante cortafuegos y proxy en el Capítulo 7.
- **Configuraciones de alta disponibilidad**: mediante redundancia en el almacenamiento RAID, balanceo de carga, virtualización de servidores. Capítulo 8.
- **Normativa legal en materia de seguridad informática**: LOPD y LSSICE. Capítulo 9.

1.4 AMENAZAS

Las amenazas a un sistema informático pueden provenir desde un *hacker* remoto que entra en nuestro sistema con un troyano, pasando por un programa descargado gratuito que nos ayuda a gestionar nuestras fotos, pero que supone una puerta trasera a nuestro sistema permitiendo la entrada a espías, hasta la entrada no deseada al sistema mediante una contraseña de bajo nivel de seguridad. Las amenazas pueden ser **provocadas por**: personas, condiciones físicas-ambientales y software, o lógicas.

1.4.1 AMENAZAS PROVOCADAS POR PERSONAS

La mayoría de ataques a nuestro sistema provienen de personas que, intencionadamente o no, pueden causarnos enormes pérdidas. Generalmente se tratará de piratas informáticos, ciberdelincuentes, *hackers* o *crackers*, que intentan conseguir el máximo nivel de privilegio posible aprovechando algunas vulnerabilidades del software. Se dividen en dos grandes grupos: los atacantes pasivos que fisgonean el sistema pero no lo modifican o destruyen, y los activos que dañan el objetivo atacado o lo modifican en su favor.

Dentro de una organización: El propio personal puede producir un ataque intencionado, nadie mejor conoce los sistemas y sus debilidades, o un accidente causados por un error o por desconocimiento de las normas básicas de seguridad. Por otro lado ex empleados o personas descontentas con la organización pueden aprovechar debilidades que conocen o incluso realizar chantajes.

Hacker: Experto o gurú en aspectos técnicos relacionados con la informática. Personas que les apasionan el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Suele distinguirse entre aquellos cuyas acciones son de carácter constructivo, informativo o solo intrusivo, o que además lo son de tipo destructivo, catalogados respectivamente de *hackers* y *crackers*, o **white hat** y **black hat**. Recientemente ha aparecido el término, más neutro, *grey hat* (sombrero gris), que ocasionalmente traspasan los límites entre ambas categorías. Otros términos y categorías son:

- **Newbie**: *Hacker* novato.
- **Wannaber**: Les interesa el tema de *hacking* pero que por estar empezando no son reconocidos por la élite.
- **Lammer** o **Script-Kiddies**: Pretenden hacer *hacking* sin tener conocimientos de informática. Solo se dedican a buscar y descargar programas de *hacking* para luego ejecutarlos.
- **Luser** (**looser** + **user**): Es un término utilizado por *hackers* para referirse a los usuarios comunes, de manera despectiva y como burla.

Pirata informático, **ciberdelincuente** o **delincuente informático**: Personas dedicadas a realizar actos delictivos y perseguidos legalmente: como la copia y distribución de software, música o películas de forma ilegal, fraudes bancarios o estafas económicas.

1.4.2 AMENAZAS FÍSICAS Y LÓGICAS

Las **amenazas físicas y ambientales** afectan a las instalaciones y/o el hardware contenido en ellas y suponen el primer nivel de seguridad a proteger para garantizar la disponibilidad de los sistemas. En el capítulo 2 veremos con más profundidad los aspectos asociados a:

- ✓ Robos, sabotajes, destrucción de sistemas.
- ✓ Cortes, subidas y bajadas bruscas de suministro eléctrico.
- ✓ Condiciones atmosféricas adversas. Humedad relativa excesiva o temperaturas extremas.
- ✓ Catástrofes (naturales o artificiales) terremotos, inundaciones, incendios, humo o atentados de baja magnitud, etc.
- ✓ Interferencias electromagnéticas que afecten al normal comportamiento de circuitos y comunicaciones.

Una **amenaza lógica** es software o código que de una forma u otra pueden afectar o dañar a nuestro sistema, creados de forma intencionada para ello (el software malicioso, también conocido como *malware,* se analizará a fondo en el Capítulo 4) o simplemente por error (*bugs* o agujeros). Entre otros encontramos:

- **Herramientas de seguridad**: Existen herramientas para detectar y solucionar fallos en los sistemas, pero se pueden utilizar para detectar esos mismos fallos y aprovecharlos para atacarlos.
- *Rogueware* o **falsos programas de seguridad**: También denominados *Rogue*, *FakeAVs*, *Badware*, *Scareware*, son falsos antivirus o antiespías.
- **Puertas traseras** o *backdoors*: Los programadores insertan "atajos" de acceso o administración, en ocasiones con poco nivel de seguridad.
- **Virus**: Secuencia de código que se inserta en un fichero ejecutable (denominado *huésped*), de forma que cuando el archivo se ejecuta, el virus también lo hace. Detrás de la palabra virus existe todo un conjunto de términos que analizaremos con más detalle en el Capítulo 4, dentro de lo que se conoce como *malware*.
- **Gusano** o *Worm*: Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, normalmente mediante correo electrónico basura o *spam*.
- **Troyanos** o **Caballos de Troya**: Aplicaciones con instrucciones escondidas de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.
- **Programas conejo** o **bacterias**: Programas que no hacen nada útil, simplemente se dedican a reproducirse hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco...), produciendo una negación de servicio.
- **Canales cubiertos**: Canales de comunicación que permiten a un proceso transferir información de forma que viole la política de seguridad del sistema; un proceso transmite información a otros que no están autorizados a leer dicha información.

1.4.3 TÉCNICAS DE ATAQUE

Del mismo modo que hemos analizados las amenazas de los sistemas informáticos desde un punto de vista de quién o qué la genera, los tipos de amenazas pueden clasificarse en función de la **técnica que se emplean para realizar el ataque**. Las técnicas más usuales son las que se indican en la Tabla 1.1.

Tabla 1.1

Malware	Programas malintencionados (virus, espías, gusanos, troyanos, etc.) que afectan a los sistemas con pretensiones como: controlarlo o realizar acciones remotas, dejarlo inutilizable, reenvío de *spam*, etc.
Ingeniería social	Obtener información confidencial como credenciales (usuario-contraseña), a través de la manipulación y la confianza de usuarios legítimos. El uso de dichas credenciales o información confidencial servirá para la obtención de beneficios económicos mediante robo de cuentas bancarias, reventa de información o chantaje.
Scam	Estafa electrónica por medio del engaño como donaciones, transferencias, compra de productos fraudulentos, etc. Las cadenas de *mail* engañosas pueden ser *scam* si hay pérdida monetaria y *hoax* (bulo) cuando solo hay engaño.
Spam	Correo o mensaje basura, no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. Suele ser una de las técnicas de ingeniería social basada en la confianza depositada en el remitente, empleadas para la difusión de *scam*, *phishing*, *hoax*, *malware*, etc.
Sniffing	Rastrear monitorizando el tráfico de una red para hacerse con información confidencial.
Spoofing	Suplantación de identidad o falsificación, por ejemplo encontramos IP, MAC, tabla ARP, web o *mail Spoofing*.
Pharming	Redirigir un nombre de dominio (*domain name*) a otra máquina distinta falsificada y fraudulenta.
Phishing	Estafa basada en la suplantación de identidad y la ingeniería social para adquirir acceso a cuentas bancarias o comercio electrónico ilícito.
Password cracking	Descifrar contraseñas de sistemas y comunicaciones. Los métodos más comunes son mediante *sniffing*, observando directamente la introducción de credenciales (*shoulder surfing*), ataques de fuerza bruta, probando todas las combinaciones posibles, y de diccionario, con un conjunto de palabras comúnmente empleadas en contraseñas.
Botnet	Conjunto de robots informáticos o *bots*, que se ejecutan de manera autónoma y automática, en multitud de *host*, normalmente infectados, permite controlar todos los ordenadores/servidores infectados de forma remota. Sus fines normalmente son rastrear información confidencial o incluso cometer actos delictivos.
Denegación de servicio o Denial of Service (DoS)	Causar que un servicio o recurso sea inaccesible a los usuarios legítimos. Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS, a través de una *botnet*, siendo esta técnica el ciberataque más usual y eficaz.

1.5 PROTECCIÓN

Hasta ahora hemos hablado de los aspectos que engloba la seguridad informática, de los elementos a proteger, de los tipos de amenazas que contra ellos se presentan y del origen de tales amenazas; parece claro que, para completar nuestra visión de la seguridad, hemos de hablar de las **formas de protección de nuestros sistemas**.

Para proteger nuestro sistema hemos de realizar un **análisis de las amenazas potenciales** que puede sufrir, las **pérdidas** que podrían generar y la **probabilidad de su ocurrencia**. Este análisis convencionalmente se realizará mediante auditorías de seguridad.

1.5.1 AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el **análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades** que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos **los resultados**, **se detallan**, **archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo**, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad. Los **objetivos** de una auditoría de seguridad de los sistemas de información son:

- ✓ Revisar la seguridad de los entornos y sistemas.
- ✓ Verificar el cumplimiento de la normativa y legislación vigentes
- ✓ Elaborar un informe independiente.

Una auditoría se realiza con base a un patrón o conjunto de directrices o **buenas prácticas sugeridas**. Existen **estándares orientados a servir como base para auditorías de informática**. Uno de ellos es **COBIT** (Objetivos de Control de las Tecnologías de la Información), y adicional a éste podemos encontrar el estándar **ISO 27002**, el cual se conforma como un **código internacional de buenas prácticas de seguridad de la información**, éste puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los **requisitos de auditoría y sistemas de gestión de seguridad**, como lo es el estándar **ISO 27001**.

Los servicios de auditoría constan de las siguientes **fases**:

- ✓ Enumeración de sistemas operativos, servicios, aplicaciones, topologías y protocolos de red.
- ✓ Detección, comprobación y evaluación de vulnerabilidades.
- ✓ Medidas específicas de corrección.
- ✓ Recomendaciones sobre implantación de medidas preventivas.

1.5.1.1 Tipos de auditoría

Los servicios de auditoría pueden ser de distinta índole:

- **Auditoría de seguridad interna**: se contrasta el nivel de seguridad de las redes locales y corporativas de carácter interno.
- **Auditoría de seguridad perimetral**: se estudia el perímetro de la red local o corporativa, conectado a redes públicas.
- **Test de intrusión**: se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada.

- **Análisis forense**: análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, se denomina análisis post mórtem.
- **Auditoría de código de aplicaciones**: análisis del código independientemente del lenguaje empleado, un ejemplo concreto y frecuente se realiza con los sitios web, mediante el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, *Cross Site Scripting* (XSS), etc.

Realizar auditorías con **cierta frecuencia** asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Algunas de las auditorías que trabajaremos a lo largo del libro son empleadas en ocasiones para acceder a sistemas y conexiones remotas no autorizadas, aunque en nuestro caso deben servir para ver el nivel de seguridad que disponemos en nuestros sistemas. Entre las más comunes son las auditorías de contraseñas de acceso a sistemas y de conexiones inalámbricas o *wireless*.

1.5.2 MEDIDAS DE SEGURIDAD

A partir de los análisis realizados mediante auditorías, hemos de **diseñar una política de seguridad** que defina responsabilidades y **reglas a seguir** para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina **mecanismos de seguridad**, son la parte más visible de nuestro sistema de seguridad y se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red. Se distinguirán y estudiarán en los próximos capítulos las medidas de seguridad:

- **Según el recurso a proteger**:
  - **Seguridad física**: trata de proteger el hardware, teniendo en cuenta entre otros aspectos la ubicación y las amenazas de tipo físico: robos, catástrofes naturales o artificiales, etc. Algunas medidas son el estudio de la ubicación correcta, medidas preventivas contra incidentes como incendios o inundaciones o el control de acceso físico.
  - **Seguridad lógica**: protege el software tanto a nivel de sistema operativo como de aplicación, sin perder nunca de vista el elemento fundamental a proteger, la información o datos de usuario. Dentro de sus medidas se encuentran: copias de seguridad, contraseñas, permisos de usuario, cifrado de datos y comunicaciones, software específico *antimalware*, actualizaciones o filtrado de conexiones en aplicaciones de red.
- **Según el momento en el que se ponen en marcha las medidas de seguridad**:
  - **Seguridad activa**: son **preventivas** y evitan grandes daños en los sistemas informáticos, por tanto se consideran acciones **previas** a un ataque. Son de este tipo todas las medidas de seguridad lógica.
  - **Seguridad pasiva**: son **correctivas**, minimizan el impacto y los efectos causados por accidentes, es decir se consideran medidas o acciones **posteriores** a un ataque o incidente. Son de este tipo todas las medidas de seguridad física y las copias de seguridad que permiten minimizar el efecto de un incidente producido.

1.6 REFERENCIAS WEB

- INTECO - Instituto Nacional de Tecnologías de la Comunicación:
  www.inteco.es
- Hispasec Sistemas: Seguridad y Tecnologías de información. Noticias diarias y resúmenes anuales de noticias de actualidad sobre seguridad informática:
  www.hispasec.com
- Guía completa de seguridad informática:
  http://www.rediris.es/cert/doc/unixsec/unixsec.html
- Web de seguridad informática de la empresa de tecnologías de información (IT) IDG:
  www.idg.es
- Blog de seguridad informática de la empresa Trend Micro con noticias actuales:
  http://blog.trendmicro.es
- Portal de ISO 27001 en español:
  www.iso27000.es
- Blog sobre auditoría y seguridad informática ISO 27001:
  http://sgsi-iso27001.blogspot.com

RESUMEN DEL CAPÍTULO

Hablar hoy en día de un sistema informático totalmente seguro es imposible, la conectividad global permite extender el campo de posibles amenazas. Aunque éstas provienen de distintos ámbitos: **personas** (personal de una organización, *hackers* y *crackers* en red), **amenazas lógicas** (*malware* y *exploits* sobre vulnerabilidades de las aplicaciones), así como todo tipo de **amenazas físicas** como robos o catástrofes (naturales o artificiales como incendios).

En este capítulo se han analizado los fundamentos y conceptos para conseguir sistemas y configuraciones fiables, partiendo del principio de garantizar **disponibilidad**.

Hoy en día se realizan un importante y gran número de operaciones a través de las redes de comunicaciones y la disponibilidad de sus servicios ofrecidos se convierten en ocasiones en algo crítico, pasamos a hablar de **alta disponibilidad** cuando son necesarias medidas específicas que garanticen la operatibilidad 24 horas al día, 7 días a la semana, los 365 días al año.

Sobre la disponibilidad de los sistemas se sustentan otros aspectos que se deben perseguir para mejorar la seguridad informática como la **confidencialidad**, **integridad**, **autenticación** y el **no repudio**.

Debemos ser conscientes de que las **medidas de seguridad** comprenden un conjunto de elementos que no pueden ser tratados dejando de lado o desprotegido ninguno de ellos: hardware, sistema operativo, comunicaciones, medidas de seguridad físicas (ubicación de los equipos, suministro eléctrico, etc.), los controles organizativos (políticas de seguridad, normas, procedimientos, etc.) y legales (como la Ley Orgánica de Protección de Datos, LOPD). Dichas medidas se diferencian en función de qué elemento protegen **seguridad física** y **seguridad lógica**, y según sean preventivas (**activas**) o correctivas después de un incidente (**pasivas**).

En los siguientes capítulos analizaremos periódicamente el nivel de seguridad proporcionado por nuestros sistemas mediante **auditorías** y estudiaremos las medidas oportunas para hacer de la seguridad la seña de identidad de nuestros sistemas.

EJERCICIOS PROPUESTOS

A lo largo de los siguientes ejercicios propuestos se presentan una serie de recomendaciones y herramientas genéricas para todo tipo de usuarios sean administradores o no.

- **1.** Mantenerse siempre informado y al día es la primera y mejor recomendación. Uno de los peligros más comunes para los usuarios de Internet ya que son actualmente unas de las web más usadas son las denominadas redes sociales. Para ello se propone analizar la siguiente noticia: "Cinco nuevas estafas en Facebook y Twitter", cuya fuente se encuentra descargándose el material adicional del libro y en: *http://www.csospain.es/Cinco-nuevas-estafas-en-Facebook-y-Twitter/seccion-alertas/articulo-196360*, y contestar a las siguientes cuestiones:
  - ¿Qué tipo de ataques son los más comunes que se producen en las redes sociales? ¿Crees qué los ciberdelitos y ciberfraudes proliferarán con el uso de las redes sociales? ¿Qué es una *blacklist*? Indica alguna web con comprobación de direcciones web o URL, IP, direcciones de *mail*, etc., que sean potencialmente maliciosas.
  - Indica qué precauciones tomarías y cómo identificarías un fraude a través de una red social. Busca algún nuevo tipo de estafa que se produzca a través de las redes sociales. ¿Crees que conocer este tipo de noticias te ayudarán a tomar ciertas precauciones? ¿Para qué tipo de usuarios puede ser útil?
- **2.** En la web de Hispasec existen varios recursos muy interesantes, como multitud de noticias y estudios de actualidad, servicio de envío de noticias "Una al día" al que puedes suscribirte tan solo escribiendo tu correo electrónico, o VirusTotal analizador de archivos o URL potencialmente maliciosas. Analiza las noticias de la última semana. ¿Qué vulnerabilidades y amenazas se describen? ¿Qué tipo de precauciones se recomiendan? Realiza un resumen de las mismas y súbelo a tu blog.
- **3.** Emplea contraseñas fuertes y renuévalas periódicamente. Verifica y anota el nivel de fortaleza en tus contraseñas de acceso al sistema operativo, correo electrónico y otras aplicaciones web como redes sociales, banca *online*, etc.:

  http://www.microsoft.com/latam/protect/yourself/password/checker.mspx
  - Según las recomendaciones de Microsoft, una contraseña segura debe parecerle a un atacante una cadena aleatoria de caracteres. Debe tener 14

caracteres o más (como mínimo, ocho caracteres). Debe incluir una combinación de letras mayúsculas y minúsculas, números y símbolos especiales. ¿Tus contraseñas de acceso a sistemas operativos, aplicaciones web como *mail* o redes sociales, son seguras? ¿Cada cuanto tiempo cambias las contraseñas?

- **4.** Mantén actualizado tu sistema operativo y aplicaciones, sobre todo los navegadores web, ya que las vulnerabilidades y amenazas cambian constantemente a través de la red. Comprueba el estado de actualización de tus aplicaciones, especialmente el de navegadores web. Realiza un análisis desde la web de **Secunia** con su inspector *online*:

  http://secunia.com/vulnerability_scanning/online/?lang=es

  - ¿Qué aplicaciones disponían posibles vulnerabilidades al no encontrarse totalmente actualizadas? ¿Cuál es la solución propuesta?

- **5.** Con respecto a tu navegador web, es recomendable tenerlo con una correcta configuración, controlar la aceptación de *cookies* y el bloqueo de ventanas emergentes, así como no recordar contraseñas en caso de compartir el equipo con otros usuarios.

  - Contesta a las siguientes preguntas, explora e identifica: ¿Qué opciones de seguridad o privacidad permiten configurar tus navegadores web? ¿Se aceptan *cookies*? ¿Recuerdan contraseñas? ¿Cuáles? ¿Bloquean ventanas emergentes? ¿Dispones de restricciones de acceso a determinados sitios web?

- **6.** Verifica periódicamente si estás infectado por *malware*. Actualmente la mayoría de las empresas de seguridad informática y creadores de antivirus gratuitos y de pago, ofrecen servicios de escaneo *online* para poder probar sus soluciones. Aunque normalmente no disponen de funcionalidades completas como la desinfección, si sirven para tener conocimiento de qué vulnerabilidades y *malware* tenemos en nuestro sistema. Busca al menos dos antivirus en línea y realiza análisis de tu sistema para tener un contraste en la información obtenida. Entre otras empresas que lo facilitan se encuentran: Panda, Bitdefender, Eset, Kaspersky, Mcafee, TrendMicro, Symantec, etc.

  - Realiza una comparativa entre las soluciones empleadas anotando: número de archivos analizados, ocupación en disco de los archivos analizados, % de ocupación de CPU en ejecución, opciones avanzadas de escaneo, tiempo de escaneo, vulnerabilidades y *malware* encontrado, *malware* desinfectado, soluciones propuestas de desinfección.

- **7.** Realiza copias de seguridad periódicamente de la información fundamental para ti, recuerda que es el elemento fundamental a proteger. Para realizar copias de seguridad hoy en día existen diversas opciones en Internet podemos emplear un sitio FTP gratuito, o servicios más especializados y seguros como **Dropbox**, **Idrive** o **Mozy**, que ofrecen almacenamiento virtual de datos para copias de seguridad remotas. Crea una cuenta y realiza una configuración y prueba de copia de seguridad *online* de archivos de tu equipo.

- **8.** Emplea y conoce a fondo la configuración de todas las herramientas de configuración que te permiten tu sistema operativo y aplicaciones de red. Los sistemas Windows incorporan un **centro de seguridad** donde encontraremos información sobre: *firewall*, actualizaciones automáticas y protección antivirus (solo detecta si tenemos instalado alguno).

  - **Se recomienda** tener activado el *firewall* o cortafuegos para evitar posibles accesos externos, notificar periódicamente y descargar e instalar manualmente actualizaciones, así como disponer de protección antivirus. Si deseamos acceder a Microsoft Update para ver las últimas actualizaciones de nuestro sistema operativo Windows, podremos hacerlo entrando con Internet Explorer 5 o superior a: *http://www.update.microsoft.com*. Contesta a las siguientes cuestiones:

  - ¿Crees que los sistemas GNU/Linux al no disponer de tantas opciones de herramientas antivirus son más seguros que los sistemas Windows? ¿Por qué? ¿Y en caso de tener un servidor FTP bajo Linux, alojando archivos potencialmente maliciosos, sería recomendable tener alguna herramienta que rastree posibles archivos infectados?

  - Configura el *firewall* de Windows para evitar contestar a peticiones de red de eco entrante. ¿Es posible realizar la configuración de cada puerto de red?

  - Configura el *firewall* para evitar que tu navegador web tenga acceso a Internet.

TEST DE CONOCIMIENTOS

1 La primera característica a garantizar en un sistema seguro es:
- a) Confidencialidad.
- b) Integridad.
- c) Disponibilidad.
- d) No repudio.

2 Indica qué sentencia es falsa:
- a) La integridad permite asegurar que los datos no se han falseado.
- b) Confidencialidad es desvelar datos a usuarios no autorizados; que comprende también la privacidad (la protección de datos personales).
- c) Disponibilidad es que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

3 Una de las siguientes medidas no pertenece a la seguridad lógica:
- a) Contraseñas.
- b) SAI.
- c) Copia de seguridad.
- d) SW *antimalware*.

4 ¿Qué elemento de un sistema informático se considera más crítico a la hora de protegerlo?
- a) Comunicaciones.
- b) Software.
- c) Hardware.
- d) Datos.

5 Un *hacker*:
- a) Siempre tiene una finalidad maliciosa.
- b) La mayoría de las veces tiene una finalidad maliciosa.
- c) A veces posee una finalidad maliciosa, entonces se denomina *cracker*.
- d) Es un curioso con una finalidad conocida.

6 El *phishing*:
- a) Es un tipo de fraude bancario.
- b) Es un tipo de *malware* o virus.
- c) Se contrarresta con un *spyware*.
- d) Se propaga mediante correo electrónico siempre.

7 ¿Cuál es el estándar ISO en materia de auditoría de sistemas de información?
- a) ISO 9001.
- b) ISO 27000.
- c) ISO 27002.
- d) ISO 27001.
- e) COBIT.

8 ¿Y el estándar de buenas prácticas en materia de seguridad informática?
- a) ISO 9001.
- b) ISO 27000.
- c) ISO 27002.
- d) ISO 27001.
- e) COBIT.

9 Con respecto a un análisis forense:
- a) Se realiza siempre *a posteriori* de detectar vulnerabilidades.
- b) Se debe realizar semanalmente.
- c) Se realiza tan solo cuando el sistema de información "ha muerto".
- d) Se realiza siempre *a priori* de detectar vulnerabilidades.

10 Una vez se realiza una auditoría:
- a) Si todo se encuentra correcto no es necesario volver a realizar auditorías.
- b) Es recomendable volver a realizarlas periódicamente.
- c) Es poco probable que todo esté perfecto.
- d) Es recomendable volver a realizarlas periódicamente, pero ya no tan exhaustivas.