

Seguridad y Alta Disponibilidad



Seguridad y Alta Disponibilidad

JESÚS COSTAS SANTOS





La ley prohíbe
fotocopiar este libro

SEGURIDAD Y ALTA DISPONIBILIDAD

© Jesús Costas Santos
© De la edición: Ra-Ma 2011

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos (hardware, software, sistemas operativos, etc.) suelen ser marcas registradas. RA-MA ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y solo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

RA-MA es marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, RA-MA Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

Reservados todos los derechos de publicación en cualquier idioma.

Según lo dispuesto en el Código Penal vigente ninguna parte de este libro puede ser reproducida, grabada en sistema de almacenamiento o transmitida en forma alguna ni por cualquier procedimiento, ya sea electrónico, mecánico, reprográfico, magnético o cualquier otro sin autorización previa y por escrito de RA-MA; su contenido está protegido por la Ley vigente que establece penas de prisión y/o multas a quienes, intencionadamente, reprodujeren o plagiaren, en todo o en parte, una obra literaria, artística o científica.

Editado por:

RA-MA Editorial

Calle Jarama, 3A, Polígono Industrial Igarsa
28860 PARACUELLOS DE JARAMA, Madrid

Teléfono: 91 658 42 80

Fax: 91 662 81 39

Correo electrónico: editorial@ra-ma.com

Internet: www.ra-ma.es y www.ra-ma.com

ISBN: 978-84-9964-089-1

Depósito Legal: M-24.265-2011

Maquetación: Antonio García Tomé

Diseño de Portada: Antonio García Tomé

Filmarción e Impresión: Closas-Orcoyen, S.L.

Impreso en España

Índice

INTRODUCCIÓN	7
CAPÍTULO 1. PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD	9
1.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA.....	10
1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	11
1.2.1 Alta disponibilidad	21
1.3 ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS.....	22
1.4 AMENAZAS.....	24
1.4.1 Amenazas provocadas por personas	24
1.4.2 Amenazas físicas y lógicas.....	24
1.4.3 Técnicas de ataque.....	25
1.5 PROTECCIÓN	26
1.5.1 Auditoría de seguridad de sistemas de información	27
1.5.2 Medidas de seguridad.....	28
1.6 REFERENCIAS WEB	29
RESUMEN DEL CAPÍTULO	29
EJERCICIOS PROPUESTOS	30
TEST DE CONOCIMIENTOS	32
CAPÍTULO 2. SEGURIDAD PASIVA	33
2.1 PRINCIPIOS DE LA SEGURIDAD PASIVA	34
2.2 COPIAS DE SEGURIDAD	35
2.2.1 Modelos de almacén de datos	36
2.2.2 Recomendación sobre el tipo de copia a efectuar	37
2.2.3 Recuperación de datos	44
2.3 SEGURIDAD FÍSICA Y AMBIENTAL	47
2.3.1 Centros de Procesado de Datos (CPD)	47
2.3.2 Ubicación y acondicionamiento físico	48
2.3.3 Control de acceso físico	49
2.3.4 Sistemas biométricos	50
2.3.5 Circuito Cerrado de Televisión (CCTV)	51
2.4 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI).....	52
2.4.1 Tipos de SAI	53
2.4.2 Potencia necesaria	53
2.5 REFERENCIAS WEB	60
RESUMEN DEL CAPÍTULO	61
EJERCICIOS PROPUESTOS	62
TEST DE CONOCIMIENTOS	64

CAPÍTULO 3. SEGURIDAD LÓGICA	65
3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA.....	66
3.2 CONTROL DE ACCESO LÓGICO.....	67
3.2.1 Política de contraseñas	67
3.2.2 Control de acceso en la BIOS y gestor de arranque.....	73
3.2.3 Control de acceso en el sistema operativo.....	77
3.3 POLÍTICA DE USUARIOS Y GRUPOS.....	82
3.4 REFERENCIAS WEB	84
RESUMEN DEL CAPÍTULO	85
EJERCICIOS PROPUESTOS.....	86
TEST DE CONOCIMIENTOS	87
CAPÍTULO 4. SOFTWARE ANTIMALWARE.....	89
4.1 SOFTWARE MALICIOSO	90
4.2 CLASIFICACIÓN DEL MALWARE	91
4.2.1 Métodos de infección.....	92
4.3 PROTECCIÓN Y DESINFECCIÓN	94
4.3.1 Clasificación del software antimalware	94
4.3.2 La mejor herramienta antimalware	100
4.4 REFERENCIAS WEB	102
RESUMEN DEL CAPÍTULO	102
EJERCICIOS PROPUESTOS.....	103
TEST DE CONOCIMIENTOS	104
CAPÍTULO 5. CRIPTOGRAFÍA.....	107
5.1 PRINCIPIOS DE CRIPTOGRAFÍA	108
5.2 TIPOS DE ALGORITMOS DE CIFRADO	109
5.2.1 Criptografía simétrica	111
5.2.2 Criptografía de clave asimétrica	115
5.2.3 Criptografía híbrida	117
5.2.4 Firma digital	120
5.3 CERTIFICADOS DIGITALES	122
5.3.1 Terceras partes de confianza	125
5.3.2 Documento Nacional de Identidad electrónico (DNIe)	125
5.4 REFERENCIAS WEB	126
RESUMEN DEL CAPÍTULO	127
EJERCICIOS PROPUESTOS.....	128
TEST DE CONOCIMIENTOS	129
CAPÍTULO 6. SEGURIDAD EN REDES CORPORATIVAS	131
6.1 AMENAZAS Y ATAQUES	132
6.1.1 Amenazas externas e internas	136
6.2 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS).....	137
6.3 RIESGOS POTENCIALES EN LOS SERVICIOS DE RED	139
6.4 COMUNICACIONES SEGURAS	140
6.4.1 VPN	145

6.5 REDES INALÁMBRICAS	148
6.5.1 Sistemas de seguridad en WLAN	149
6.5.2 Recomendaciones de seguridad en WLAN	155
6.6 REFERENCIAS WEB	158
RESUMEN DEL CAPÍTULO	158
EJERCICIOS PROPUESTOS	159
TEST DE CONOCIMIENTOS	160
CAPÍTULO 7. SEGURIDAD PERIMETRAL.....	161
7.1 CORTAFUEGOS	162
7.1.1 Tipos de cortafuegos	168
7.1.2 DMZ	173
7.2 PROXY	174
7.2.1 Tipos, características y funciones principales	174
7.3 REFERENCIAS WEB	181
RESUMEN DEL CAPÍTULO	182
EJERCICIOS PROPUESTOS	182
TEST DE CONOCIMIENTOS	183
CAPÍTULO 8. CONFIGURACIONES DE ALTA DISPONIBILIDAD	185
8.1 SOLUCIONES DE ALTA DISPONIBILIDAD	186
8.2 RAID	187
8.3 BALANCEO DE CARGA	194
8.4 VIRTUALIZACIÓN	199
8.4.1 Virtualización de servidores	205
8.5 REFERENCIAS WEB	210
RESUMEN DEL CAPÍTULO	211
EJERCICIOS PROPUESTOS	212
TEST DE CONOCIMIENTOS	213
CAPÍTULO 9. NORMATIVA LEGAL EN MATERIA DE SEGURIDAD INFORMÁTICA.....	215
9.1 LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD)	216
9.1.1 Ámbito de aplicación de la LOPD	216
9.1.2 Agencia Española de Protección de Datos	217
9.1.3 Tratamiento de los datos	218
9.1.4 Niveles de seguridad	219
9.2 LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSICE)	221
9.2.1 Entornos Web	222
9.2.2 Comunicaciones comerciales	222
9.3 REFERENCIAS WEB	224
RESUMEN DEL CAPÍTULO	224
EJERCICIOS PROPUESTOS	225
TEST DE CONOCIMIENTOS	226
MATERIAL ADICIONAL	227
ÍNDICE ALFABÉTICO	229

1960. 1961. 1962. 1963.
1964. 1965. 1966. 1967.
1968. 1969. 1970. 1971.
1972. 1973. 1974. 1975.
1976. 1977. 1978. 1979.
1980. 1981. 1982. 1983.
1984. 1985. 1986. 1987.
1988. 1989. 1990. 1991.
1992. 1993. 1994. 1995.
1996. 1997. 1998. 1999.
2000. 2001. 2002. 2003.
2004. 2005. 2006. 2007.
2008. 2009. 2010. 2011.
2012. 2013. 2014. 2015.

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 contienen 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 dia al resto de usuarios mediante noticias y post en blogs y webs especializadas. Sirvase 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:** calidad 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:** calidad 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 interesarán 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

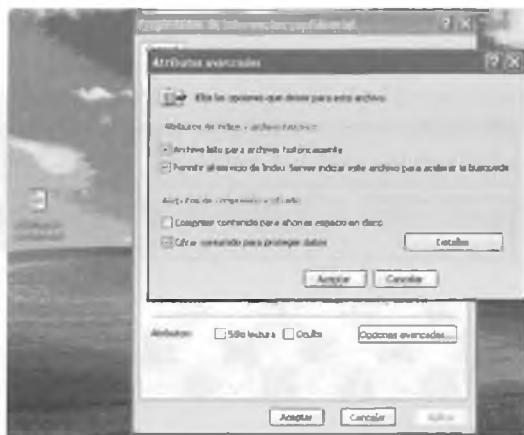
Como veremos en capítulos posteriores, en un sistema personal es posible obtener el acceso al sistema de ficheros si podemos arrancar desde una distribución USB o CD/DVD Live, o incluso acceder al sistema local como administrador, realizando una escalada de privilegios, teniendo de este modo permisos 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.

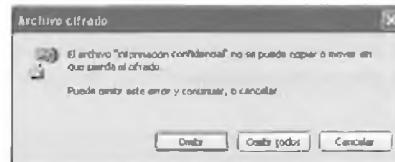


Verificaciones

- 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, si es posible borrarlo.

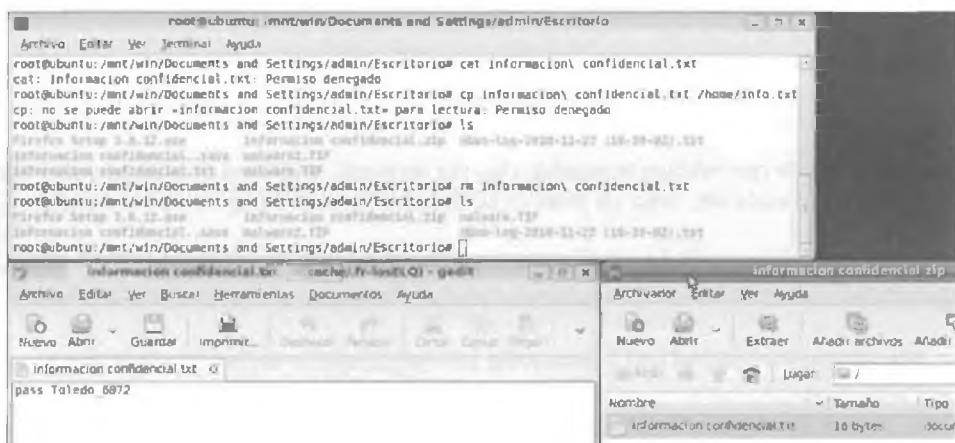


- El archivo cifrado no es portable o copiable a una unidad externa ya que el sistema operativo pierde el control sobre su cifrado. En caso de intentar enviarlo a unidad USB nos indicará lo siguiente.



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

- 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, si podremos acceder a su contenido confidencial.



PRÁCTICA 1.2

INTEGRIDAD

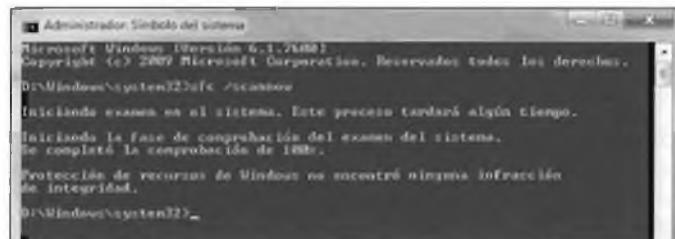
Amenaza o vulnerabilidad

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 ninguna 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
```

```

Archivo Editar Ver Terminal Ayuda
root@ubuntu:/home/almos# rkhunter --checkall
[ Rootkit Hunter version 1.3.2 ]

Checking system commands...
Performing 'strings' command checks
  Checking 'strings' command [ OK ]
Performing 'shared libraries' checks
  Checking for preloading variables
  Checking for preload file
  Checking LD_LIBRARY_PATH variable [ Not Found ]
[ Not Found ]
[ Not Found ]
[ Not Found ]

Performing file properties checks
  Checking for prerequisites
    /bin/bash [ OK ]
    /bin/cat [ OK ]
    /bin/chmod [ OK ]
    /bin/chown [ OK ]
    /bin/cp [ OK ]
    /bin/date [ OK ]
    /bin/df [ OK ]
    /bin/dmesg [ OK ]
    /bin/echo [ OK ]

```

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

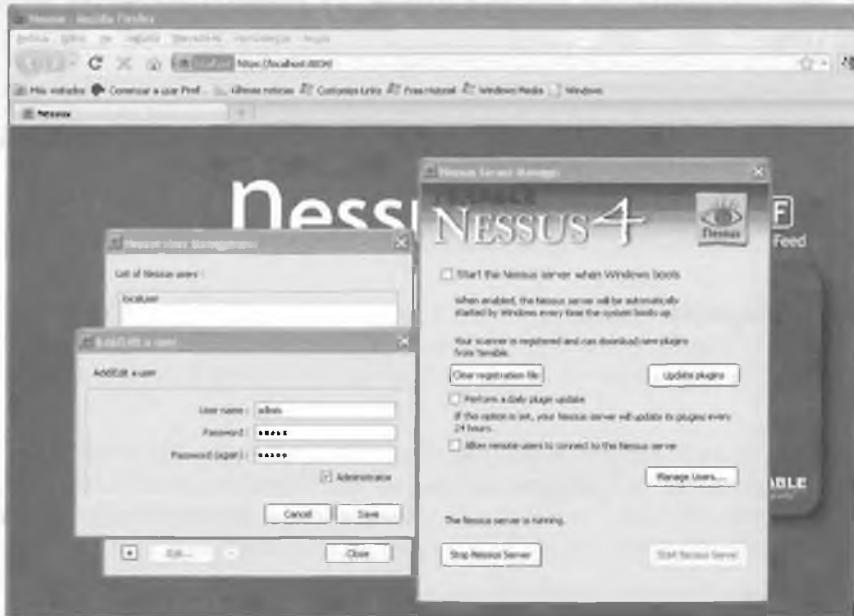
Para las versiones de software de servidores y de los sistemas operativos es posible **buscar posibles vulnerabilidades existentes**:

- 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.



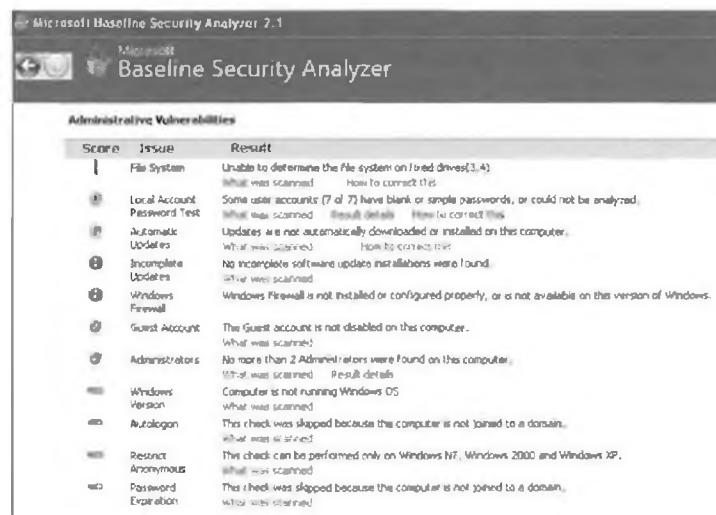
Ejemplo de búsqueda de vulnerabilidades por fabricante, en este caso Microsoft.

- 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 faltan. 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
```

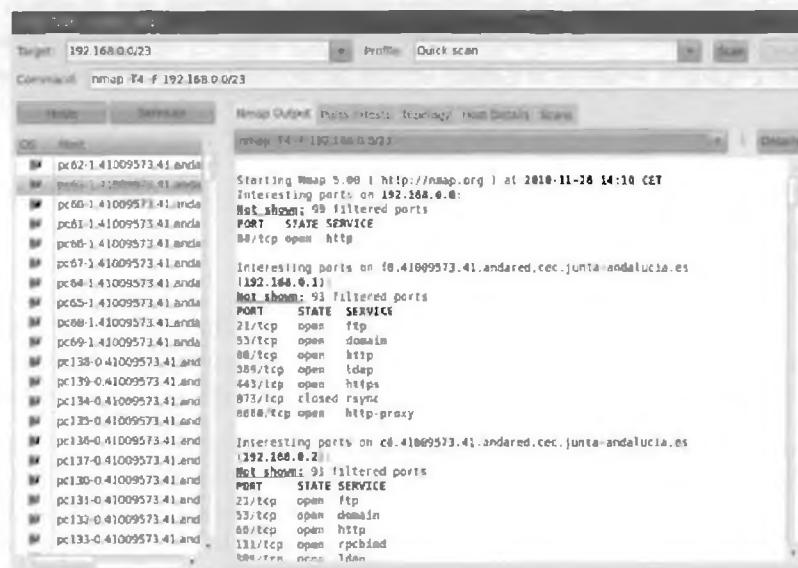
Podemos ver después de este escaneo modo comando las versiones de los sistemas operativos de dichas máquinas, direcciones MAC e IP, puertos abiertos (22 SSH, 80 HTTP, 53 DNS, 135 MSRPC, etc.) o cerrados y versiones de las aplicaciones (OpenSSH 3.91, Apache httpd 2.0.52, etc.).

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 jueves: 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 fisigonean 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, ciberdelinciente 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 analizado 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 <i>spam</i> , 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 <i>mail</i> engañosas pueden ser <i>scam</i> si hay pérdida monetaria y <i>hoax</i> (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 <i>scam</i> , <i>phishing</i> , <i>hoax</i> , <i>malware</i> , 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 <i>mail Spoofing</i> .
Pharming	Redirigir un nombre de dominio (<i>domain name</i>) 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 <i>sniffing</i> , observando directamente la introducción de credenciales (<i>shoulder surfing</i>), 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 <i>bots</i> , que se ejecutan de manera autónoma y automática, en multitud de <i>host</i> , 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 <i>botnet</i> , 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 operatividad 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 cuánto 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 analiza-

dos, 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.

2

Seguridad pasiva

OBJETIVOS DEL CAPÍTULO

- ✓ Profundizar en aspectos de seguridad pasiva, como son las copias de seguridad y medidas específicas de seguridad física y ambiental.
- ✓ Valorar la importancia de realizar periódicamente copias de seguridad de la información sensible de nuestros sistemas.
- ✓ Analizar los distintos aspectos que influyen en la ubicación física de los sistemas.
- ✓ Valorar la importancia para la empresa de un centro de procesamiento de datos (CPD) y analizar qué medidas específicas requiere.
- ✓ Analizar los distintos dispositivos hardware que permiten mejorar la seguridad física, como sistemas de alimentación ininterrumpida (SAI), sistemas de refrigeración, armarios de seguridad, circuitos cerrados de televisión, etc.
- ✓ Investigar sobre nuevos métodos de seguridad física y de control de acceso a los sistemas mediante biometría.

2.1 PRINCIPIOS DE LA SEGURIDAD PASIVA

La **seguridad pasiva** intenta minimizar el impacto y los efectos causados por accidentes, es decir, se consideran **medidas o acciones posteriores** a un ataque o incidente. A continuación se presenta una tabla que relaciona los posibles problemas con soluciones propuestas:

Tabla 2.1

Amenazas	Medidas paliativas
Suministro eléctrico: cortes, variaciones del nivel medio de tensión (subidas y bajadas), distorsión y ruido añadido.	<ul style="list-style-type: none"> - Sistema de alimentación ininterrumpida (SAI o UPS). - Generadores eléctricos autónomos. - Fuentes de alimentación redundantes.
Robos o sabotajes: acceso físico no autorizado al hardware, software y copias de seguridad	<ul style="list-style-type: none"> - Control de acceso físico: armarios, llaves, blindaje, biometría. - Vigilancia mediante personal y circuitos cerrados de televisión (CCTV).
Condiciones atmosféricas y naturales adversas: temperaturas extremas, humedad excesiva, incendios, inundaciones, terremotos.	<ul style="list-style-type: none"> - Elegir la correcta ubicación de sistemas, teniendo en cuenta en la construcción la probabilidad de catástrofes naturales y ambientales. - Centro de respaldo en ubicación diferente al centro de producción. - Proporcionar mecanismos de control y regulación de temperatura, humedad, etc.

Las consecuencias o efectos producidos por las distintas amenazas previstas son:

- ✓ Pérdida y/o mal funcionamiento del hardware.
- ✓ Falta de disponibilidad de servicios.
- ✓ Pérdida de información.

Como hemos visto en el capítulo anterior la pérdida de información es el aspecto fundamental en torno a la que gira gran parte de la seguridad informática, por lo que, como medida transversal y siempre recomendada en primer lugar abordaremos la planificación y realización de **copias de seguridad**, que permitan recuperar los datos.



NOTICIA DE ACTUALIDAD

A continuación se propone leer una noticia de actualidad relacionada con la seguridad pasiva y comentar en clase determinadas preguntas de análisis de la misma, en concreto la podemos encontrar en la URL <http://www.weblogssl.com/2008/09/23/caida-general-de-x-horas-durante-la-madrugada-del-23-de-septiembre-de-2008>, también descargándose el material adicional del libro.

- ¿A qué se dedica la empresa? ¿Qué ha ocurrido y qué consecuencias ha tenido? ¿Por qué ha existido corte en el servicio de la empresa? ¿Crees que se encontraban bien dimensionados los generadores de gasoil para la carga que tenían que soportar?
- ¿Qué equipos se apagaron primero al intentar reiniciar con el segundo grupo de emergencia? ¿A qué temperatura deben de permanecer las salas de estos equipos? ¿Qué peligros se corrían?
- ¿Qué tipos de medidas ha tomado la empresa *a posteriori*? ¿Las ves acertadas?
- ¿Qué tipo de medidas y recomendaciones crees que podrías aportar personalmente para evitar este tipo de incidentes en el futuro?

2.2 COPIAS DE SEGURIDAD

Por acción de algún tipo de *malware*, acceso no autorizado a nuestro sistema, por fallos en el hardware o, simplemente, por accidente o descuido, la información contenida en nuestro equipo puede resultar dañada o incluso desaparecer. Las copias de seguridad o *backup*, son réplicas de datos que nos permiten recuperar la información original en caso de ser necesario, es un archivo digital, un conjunto de archivos o la totalidad de los datos considerados lo suficientemente importantes para ser conservados.



Uno de los principios de seguridad: "Ordenar de mayor a menor prioridad qué archivos, datos y configuraciones son difíciles de volver a realizar o recuperar, y mantener de forma segura copias de seguridad de los mismos, distribuidas en espacio y tiempo".

Corresponde a cada usuario determinar los datos, que por su importancia, serán almacenados en la copia de seguridad. Estas copias, se pueden almacenar en soportes extraíbles (CD/DVD, pendrive, cintas de *backup*, etc.), en otros directorios o particiones de datos de nuestra propia máquina, en unidades compartidas de otros equipos o en discos de red, en servidores remotos, etc. Es aconsejable que dichas copias de seguridad se encuentren cifradas y comprimidas en un solo archivo facilitando su confidencialidad, mantenimiento y distribución.

Teniendo en cuenta los **modelos de almacenamiento** masivo de los sistemas hoy en día encontramos:

- **Direct Attached Storage (DAS)**: es el método tradicional de almacenamiento y el más sencillo. El dispositivo de almacenamiento se encuentra directamente conectado físicamente al sistema que hace uso de él. Es el caso convencional disponer un disco duro conectado directamente al sistema informático. Los discos duros extraíbles, y las particiones de datos, son una solución sencilla y económica para realizar copias de seguridad locales.
- **Network-Attached Storage (NAS)**: almacenamiento conectado en red. Las aplicaciones hacen las peticiones de datos a los sistemas de ficheros de manera remota mediante protocolos de red, como NFS, FTP, CIFS o SMB. Las carpetas compartidas en red y servidores específicos NAS son una buena solución para una LAN de tamaño pequeño o medio.
- **Storage Area Network (SAN)**: red de área de almacenamiento. Los dispositivos de almacenamiento se encuentran conectados a una red de alta velocidad directamente y resuelven las peticiones que se le realizan. La infraestructura necesaria hace que solo sea posible en grandes organizaciones.

A modo de ejemplo veremos cómo implementar un servidor NAS como servidor de archivos para distintos usuarios en una red corporativa en el capítulo 8.

2.2.1 MODELOS DE ALMACÉN DE DATOS

Los datos de la copia deben ser almacenados de alguna manera y probablemente deban ser organizados con algún criterio. Para ello se puede usar desde una hoja de papel con una lista de las cintas de la copia de seguridad y las fechas en que fueron hechas, hasta un sofisticado programa con una base de datos.

Un almacén **desestructurado** o conjunto de disquetes, CD/DVD, memorias USB, discos duros externos o cintas de *backup*, con una mínima información sobre qué ha sido copiado y cuándo. Ésta es la forma más fácil de implementar pero ofrece pocas garantías de recuperación de datos. Lo habitual es trabajar con almacenes estructurados, en función de la cantidad de archivos que se salvaguardan a la hora de realizar la copia de seguridad, podemos distinguir tres tipos de copia:

- **Completa, total o íntegra**: es una copia de seguridad total de todos los archivos y directorios seleccionados.
- **Incremental**: se hace una copia de seguridad solo de los archivos que han cambiado desde la última copia de seguridad realizada, sea del tipo que sea. Tiene en cuenta los bits de archivo modificado.
- **Diferencial**: es similar a la incremental pero realiza una copia de todos los archivos que han cambiado desde la última copia de seguridad total que hayamos hecho.

Si hacemos una copia de seguridad total el día 1 de cada mes y copia de seguridad incremental el resto de los días, cada copia incremental solo guardará los archivos que se hayan modificado ese día, por tanto el volumen de información de cada *backup* incremental será menor que el de la total. Si tenemos que realizar la restauración de archivos ante un desastre, debemos disponer de la copia total y de todas las copias incrementales que hayamos realizado desde la copia total.

Si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad diferencial el resto de los días, cada copia diferencial guardará los archivos que se hayan modificado desde el día 1. La ventaja es que se requiere menos espacio que la copia total y que en el proceso de restauración únicamente necesitaremos la última copia total y la última copia diferencial. Una copia diferencial anula a la copia diferencial anterior. Por el contrario, se consume más tiempo en realizar la copia y también más espacio que en el caso de copia incremental.

2.2.2 RECOMENDACIÓN SOBRE EL TIPO DE COPIA A EFECTUAR

Si el volumen de datos de nuestra copia de seguridad no es muy elevado (menos de 4 GB), lo más práctico es realizar **siempre copias totales** ya que en caso de desastre, tan solo debemos recuperar la última copia.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) pero el volumen de datos que se modifican no es elevado (sobre 4 GB), lo más práctico es realizar una primera copia total y, posteriormente, realizar **siempre copias diferenciales**. Así, en caso de desastre, tan solo debemos recuperar la copia total y la última diferencial. Periódicamente debemos realizar una copia total y así empezar de nuevo.

Si el volumen de datos de nuestra copia de seguridad es muy elevado (mayor de 50 GB) y el volumen de datos que se modifican también lo es, las copias diferenciales ocuparán mucho espacio, por lo tanto en este caso lo más práctico será realizar una primera copia total y posteriormente realizar **siempre copias incrementales**, ya que son las que menos espacio ocupan. El problema es que en caso de desastre debemos recuperar la última copia total y todas las incrementales realizadas desde que se hizo la última copia total. En estos casos, conviene hacer copias totales más a menudo para no tener que mantener un número muy elevado de copias incrementales.

Tabla 2.2

Método de copia	Espacio de almacenamiento	Velocidad de copia	Restauración	Copia recomendada
Completo	Máximo	Muy lento	Muy simple	Pocos datos a copiar
Completo + Incremental	Mínimo	Rápido	Compleja	Muchos datos que cambian frecuentemente
Completo + Diferencial	Intermedio	Lento	Sencilla	Datos cuya velocidad de cambio es moderada

En grandes compañías donde la realización de copias de seguridad está perfectamente **planificada**, se suelen utilizar **sistemas mixtos**. Por ejemplo en un caso típico se realizarían las siguientes tareas:

- ✓ Todos los días 1 de cada mes, a las 23:00 horas: copia de seguridad total.
- ✓ Todos los viernes a las 23:00 horas: copia de seguridad diferencial desde la copia de día 1.
- ✓ Todos los días (excepto los viernes y el día 1) a las 23:00 horas: copia de seguridad incremental desde la copia del día anterior.

Con esta planificación nos aseguramos disponer de copia de seguridad diaria. En caso de desastre deberíamos recuperar la copia total, la última diferencial y todas las incrementales desde la última diferencial.

Para garantizar la disponibilidad de los datos, en caso de desastre en la ubicación principal, es recomendable distribuir en distintas ubicaciones las copias de seguridad. Para ello se puede utilizar una empresa especializada que **transporte y custodie** duplicados de las copias, así como emplear **alojamiento remoto**, o **backup online** o **en la nube**.

PRÁCTICA 2.1



COPIAS DE SEGURIDAD CON HERRAMIENTAS DEL SISTEMA

Como hemos analizado, las copias de seguridad son parte fundamental de los sistemas, existen multitud de herramientas, algunas preinstaladas en los propios sistemas operativos, otras como aplicaciones específicas. Algunas de las opciones que se deben de analizar son:

- **Compresión:** es el mejor método para disminuir el espacio de almacenaje necesario y de ese modo reducir el coste.
- **Duplicación:** copias de seguridad duplicadas en un segundo soporte de almacenamiento. Esto puede hacerse para cambiar de lugar las copias, para optimizar velocidades de restauración, o incluso para disponer de una segunda copia a salvo en lugar o soportes diferentes. Se suele realizar en un soporte portable, económico y de alta capacidad como: CD/DVD, discos duros o unidades de cinta externas/extraíbles, o en memorias de estado sólido.
- **Cifrado:** la alta capacidad de los soportes de almacenamiento desmontables implica un riesgo de perderse o ser robados. Si se cifra la información de estos soportes se puede reducir el problema, aunque esto presenta nuevos inconvenientes. Primero, cifrar es un proceso que consume mucho tiempo de CPU y puede bajar la velocidad de copiado. En segundo lugar, una vez cifrados los datos, la compresión es menos eficaz. Aunque para información confidencial es recomendable emplear esta opción.
- **Nombre del archivo:** suele incluir el tipo de copia y la fecha (en el caso de copias totales) o fechas (en el caso de copias diferenciales e incrementales) de los datos. En ocasiones se indican las carpetas que contiene.

Ejemplos: copia de seguridad total el 1 de enero de 2011: copiatotal_01ene11.tar.bz2

Copia diferencial el 8 de enero de 2011: copiadiferencial_01ene11-08ene11.tar.bz2

GNU/Linux

Bajo los sistemas GNU/Linux las operaciones de administración son habituales realizarlas mediante comandos del sistema, en este caso se propone un modelo de gestión de copias de seguridad con 2 herramientas en modo comando, **tar** para el empaquetado de archivos y **cron** para la automatización de tareas. Alternativamente se podría emplear para la compresión y cifrado de las copias de seguridad otras herramientas como gzip, zip, bzip2, rar, etc., y cfs o herramientas más sofisticadas de cifrado de particiones como **Truecrypt**, la cual veremos en el Capítulo 5.

Centrándonos en las 2 primeras propuestas tar y cron, veamos en primer lugar sus opciones:

TAR

- Empaquetando con tar, opciones más comunes:
 - tar -vcf nombre_archivo.tar nombre_carpetas_a_empaquetar.
 - v: (*verbose*) permite obtener una descripción de los archivos empaquetados/desempaquetados.
 - c: (*create/crear*) crea un archivo tar.
 - f: (*file/archivo*) indica que se dará un nombre al archivo tar.
 - --newer=fecha: realiza un empaquetado incremental teniendo en cuenta que archivos han sido modificados desde la fecha que se le indique.
- Desempaquetando con tar, opciones más comunes:
 - tar -tvxf mi_archivo.tar.
 - t: ver el contenido (*sin extraer*).
 - x: (*extract/extraer*) extrae los archivos en la carpeta que contiene el tar.

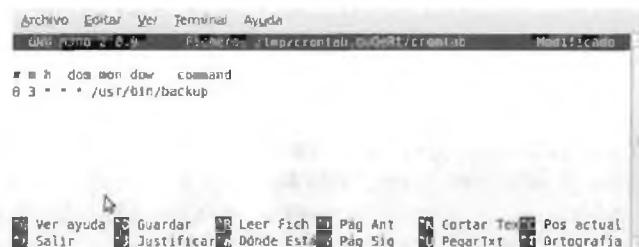
CRONTAB

La sintaxis crontab es la siguiente: crontab [-e | -l | -r] [usuario].

El parámetro -e indica la edición del cron, -l ver las tareas programadas en el archivo cron y -r borrar un archivo cron. Si no se especifica el usuario, el comando se ejecutará para el usuario en sesión. Editaremos el archivo crontab con la instrucción:

```
crontab -e
```

Con este comando nos mostrará un listado de editores de texto para editar la tabla cron de tareas programadas. Una vez seleccionado el editor deseado, por ejemplo nano, seleccionado por su facilidad de uso, podremos definir líneas de configuración con la frecuencia con que queremos que se ejecute un determinado proceso, script o programa.



Cada línea de crontab tiene el siguiente formato:

```
* * * * * comando_o_programa_a_ejecutar
| | | | |
| | | | | -----Día de la semana (0 - 6) (0 Domingo)
| | | | | -----Mes (1 - 12)
| | | | | -----Día del mes (1 - 31)
| | | | | -----Hora(0 - 23)
| | | | | -----Minuto (0 - 59)
```

La tarea se ejecutará de acuerdo a estos parámetros, por ejemplo, si quisieras ejecutar el programa */usr/bin/backup*, todos los días viernes a las 3 de la mañana la sintaxis sería la siguiente:

```
0 3 * * 5 /usr/bin/backup
```

Para especificar más de un valor en un registro se puede utilizar la coma (,) para separar los valores; en el ejemplo anterior puedes definir que la tarea se repita los lunes y los viernes a las 3 de la mañana de la siguiente manera:

```
0 3 * * 1,5 /usr/bin/backup
```

A modo de ejemplo se mostrará un script para realizar un *backup* completo o total del sistema cada 1 de mes (nomenclatura CTM_fecha), otro *backup* completo semanal cada Domingo (CTS_fecha) y *backups* diarios incrementales (ID_fecha) (solo de los cambios realizados desde el último *backup* completo).

Lo primero que tenemos que hacer es **tener claro dónde guardaremos nuestras copias de seguridad y qué directorios queremos resguardar**, ya que deberemos modificar un par de líneas del *script*, también debemos indicarle dónde se almacenará la fecha del último *backup* completo, para que se tenga en cuenta en la copia incremental.

Las copias de seguridad se realizarán sobre la carpeta que indiquemos en BACKUPDIR en nuestro caso /home/Backups. Lo recomendable es realizar la copia de seguridad sobre un dispositivo extraíble, por ejemplo, un disco duro externo USB, indicando una carpeta donde esté montado el dispositivo.

Una mejora añadida sería la creación de la copia en una carpeta remota. Al igual que se automatiza la creación de la copia, se podría ejecutar automáticamente un comando que, vía NFS, SMB, FTP o SSH, vuelque los archivos en un servidor remoto para mayor seguridad. También existen herramientas para realizar directamente copias de seguridad remotas como **rsync**.

```
#!/bin/bash
# script de copia completa e incremental
# modificar directorios a respaldar y destino del Backup
DIRECTORIOS="/bin /boot /etc /initrd /home /lib /opt /root /sbin /srv /usr /var"
# Directorio donde se guarda el backup
BACKUPDIR=/home/Backups
# Directorio que guarda la fecha del último backup completo
FECHADIR=/home/Backups
DSEM=`date +%-a` # Dia de la semana (por ej. mié)
DMES=`date +%-d` # Dia del mes (por ej. 06)
DYM=`date +%-d%b` # Dia y mes (por ej. 06jun)
# "NUEVO" coge la fecha del backup completo de cada domingo # Backup mensual
completo - sobrescribe el del mes anterior
if [ $DMES = "01" ]; then
tar -cf $BACKUPDIR/CTM_$DYM.tar $DIRECTORIOS
fi

# Backup semanal completo
# Actualiza fecha del backup completo
if [ $DSEM = "dom" ]; then
AHORA=`date +%-d-%b`
echo $AHORA > $FECHADIR/fecha-backup-completo
tar -cf $BACKUPDIR/CTS_$DSEM.tar $DIRECTORIOS

# Backup incremental diario - sobrescribe semana anterior
# Obtiene fecha del último backup completo, opción newer.
else
NUEVO="--newer=`cat $FECHADIR/fecha-backup-completo`"
tar $NUEVO -cf $BACKUPDIR/ID_$DSEM.tar $DIRECTORIOS
fi
```

Cuando tengamos el *script* retocado a nuestro gusto le damos permisos de ejecución y lo copiamos a la carpeta /usr/bin, por ejemplo:

```
chmod u+x backup-script
cp backup-script /usr/bin/
```

Después bastará con hacer que el *script* se ejecute cada día mediante cron, por ejemplo a las 3 de la mañana, para que no nos moleste mientras trabajamos con el PC.

```
crontab -e
escribiremos en la tabla:
0 3 * * * /usr/bin/backup-script
```

Para determinar la fecha del último *backup* completo y poder hacer así el *backup* incremental, se utiliza un fichero de texto con la fecha en cuestión, denominado *fecha-backup-completo*, que se actualiza cada domingo. La primera vez que se ejecute el *script* se creará un *backup* completo en vez de incremental diario, sea el día que sea, ya que ese archivo todavía no existe. Lo que debemos hacer es ejecutar el *script*, invocando el *script* (sin esperar a la ejecución automática con cron) la primera vez para realizar el *backup* completo y después crear este fichero con la fecha actual. Podemos crear dicho fichero fácilmente así:

```
echo `date +%-d-%b` > /home/Backups/fecha-backup-completo  
Sustituyendo /home/Backups/ por la ruta pertinente.
```

Si queremos restaurar el sistema lo único que debemos hacer es entrar a un terminal, loguearnos como root y, situados en el directorio raíz o punto donde queramos, restaurar el *backup* e introducir estos comando:

```
cd /  
tar -xf ruta_del_backup_que_queremos_resutarar.tar
```

WINDOWS

En Windows existen varias utilidades del sistema para realizar copias de seguridad. Los archivos del sistema se almacenan en la carpeta Windows por defecto en la instalación. De las recomendaciones más habituales a la hora de poder realizar copias de seguridad para restaurar el sistema operativo son:

- Realizar una instalación del sistema operativo diferenciando 2 particiones una con suficiente tamaño para el sistema operativo y aplicaciones a instalar, y otra dedicada a datos de usuarios. Una posible restauración o sobreinstalación del sistema operativo no afectará a la partición independiente de datos de usuario.
- No guardes información relevante en las carpetas facilitadas por el propio sistema operativo como Mis Documentos, Escritorio, etc., ya que son carpetas que, en caso de tomar la decisión de sobre instalar el sistema operativo, no te asegura su continuidad tal y como estaban, ya que vuelve a configurarlas.
- Realizar una vez instalado y configurado el sistema, controladores, sus aplicaciones fundamentales estables, y configurado, puntos de restauración, que permitan en un momento determinado de inestabilidad volver a dicha configuración anterior conocida y estable.

Windows posee 2 herramientas interesantes para realizar copias de seguridad y puntos de restauración, en **Inicio/Todos los programas/Accesorios/Herramientas del sistema**.

Por un lado, **Copia de seguridad** para generar *backups* de los archivos origen deseados, con un formato específico .bkf, en un soporte como dispositivos de almacenamiento externos. Estos archivos de *backup* se pueden restaurar a partir de la propia herramienta. El asistente proporcionado facilita la tarea para crear tus copias de seguridad.

Por otro, **Restaurar Sistema** permite crear puntos de restauración así como restaurar anteriores, con la finalidad de **guardar o restablecer la configuración de nuestro equipo en un momento determinado**. En caso de tener un problema de configuración por causa de un programa o cambios inesperados o indeseados producidos por *malware*, podremos volver a una la configuración en la que nuestro equipo funcionaba correctamente, y por precaución creamos un punto de restauración, configuración en la que nuestro equipo funcionaba correctamente. El propio sistema crea sus propios puntos de restauración, pero es recomendable crear unos cuando vamos a realizar un cambio importante de software o hardware en nuestro equipo.

PRÁCTICA 2.2



COPIAS DE SEGURIDAD CON APLICACIONES ESPECÍFICAS

Las herramientas propias del sistema poseen funcionalidades óptimas y suficientes en la mayoría de los casos, pero vamos a analizar varias herramientas que pueden resultar de interés para usos específicos como disponer de opciones como **distintos algoritmos de cifrado, contraseñas, compresión, gestionar copias remotas, etc.**

Windows

En el caso de Windows existen muchas aplicaciones de gestión de copias de seguridad pero las opciones que permite las analizaremos con la herramienta **Cobian Backup**.

Cobian Backup es un programa gratuito, multitarea, capaz de crear copias de seguridad en un equipo, unidad extraíble, red local (carpetas compartidas o ubicación de servidor) o incluso en/desde un servidor FTP. Soporta conexiones seguras mediante SSL. Se ejecuta sobre Windows y uno de sus grandes fuertes es que consume muy pocos recursos y puede estar funcionando en segundo plano.

Cada tarea de respaldo que le asignemos puede ejecutarse en el momento, diaria, semanal, mensual o anualmente, o en un tiempo especificado. Hace copias completas, incrementales y diferenciales.

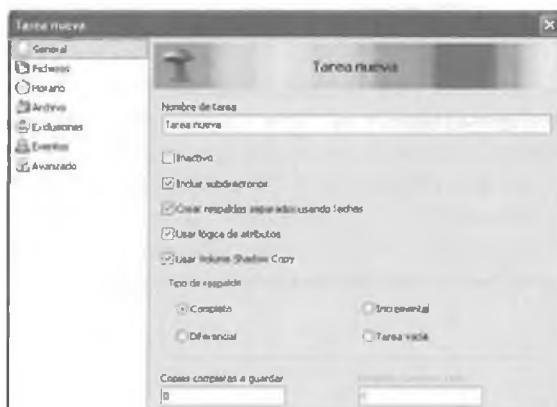
Soporta compresión ZIP, Zip64 o SQX. Además ofrece la opción de proteger todas las funciones del programa por contraseña.

Existe la opción de cifrar sus ficheros usando 4 métodos diferentes de cifrado fuerte: RSA-Rijndael (1024-256-bits), Blowfish (128-bits), Rijndael (128-bits) o DES (64-bits). Estos y otros algoritmos se clasificarán en el capítulo 5 de criptografía.

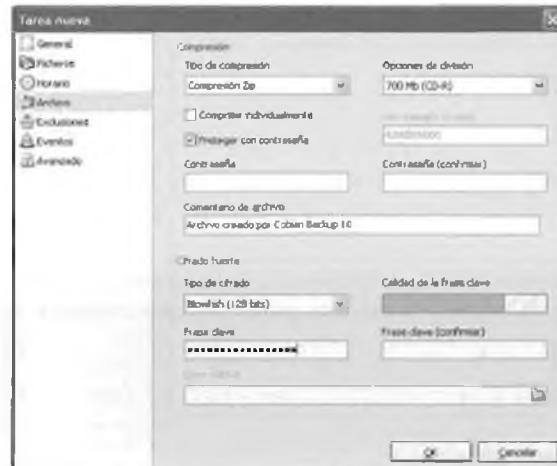
También pueden definir eventos disparados antes o después de la copia, como por ejemplo provocar el cierre de un determinado programa que utilice un fichero que se va a copiar y hacer que, una vez finalizada la copia, se vuelva a iniciar.

La aplicación permite generar distintas **tareas** de ejecución programadas en tiempo, en cada una de las cuales podremos indicar principalmente una serie de características, tras pulsar el botón de Tarea nueva (reloj), podremos configurarle paso por paso:

- **General:** Nombre nombre y tipo de copia completa, incremental o diferencial.



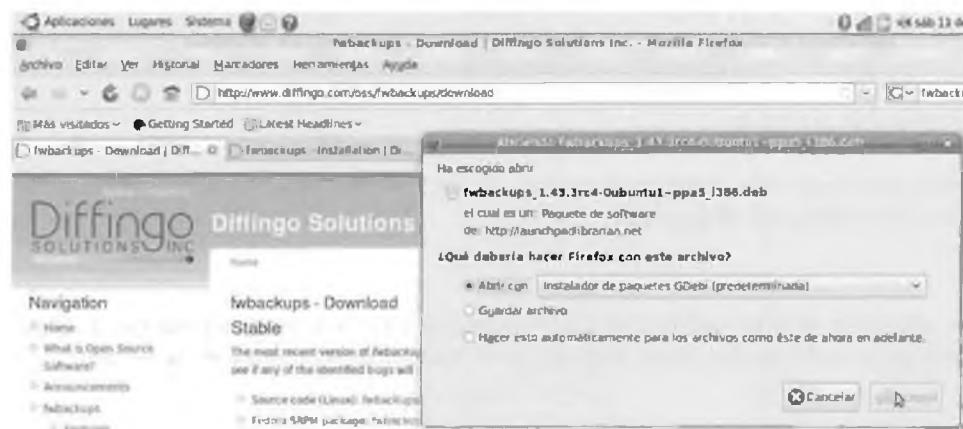
- **Ficheros:** Ubicación ubicación de ficheros/carpetas a copiar y ubicación destino que puede ser un sitio FTP, para realizar copias remotas.
- **Horario:** Indicando indicando que periodicidad y en qué momento fecha y hora queremos que se ejecute.
- **Archivo:** Opciones opciones de compresión y protección mediante algoritmo de cifrado con contraseña, del *backup*.



GNU/Linux

En el caso de GNU/Linux nos encontramos en la misma situación, existen gran cantidad de herramientas de automatización de *backups* en los repositorios disponibles. En concreto comentamos la herramienta **fwbackups** por su intuitiva interfaz gráfica.

Es multiplataforma y puede hacer *backups* individuales o recurrir a *backups* programados, en local o remoto, así como completos, incrementales, o diferenciales. También te permite hacer *backups* en formato tar, tar.gz, tar.bz2 o rsync. Desde la web www.diffingo.com/oss/fwbackups/download podemos descargar la última versión e instalarlo con el instalador de paquetes GDebi, por ejemplo bajo Ubuntu.





La configuración de archivos/carpetas origen (pestaña *path*), destino (*destination*), tipo de copia, compresión y temporización es sencilla e intuitiva, pudiendo realizar *backups* programados o en el momento.

2.2.3 RECUPERACIÓN DE DATOS

¿Podemos recuperar archivos borrados definitivamente de nuestro sistema? En el caso de haber sido víctima de un ataque o haber sufrido un accidente como corte de suministro eléctrico o fallo de hardware, la recuperación de archivos en disco lo intenta. Cuanto menor tiempo y modificaciones de disco transcurran entre el borrado o accidente y nuestro intento de recuperación, mejor será nuestro resultado. Por ejemplo, cuando en un sistema de ficheros de un sistema operativo se borra un fichero de un medio de almacenamiento (disco duro, pendrive USB, cinta, etc.), marca aquellas posiciones que ocupaba dicho fichero en el dispositivo como libres, para poder almacenar nueva información, pero no las borra. Los datos permanecerán en esas posiciones hasta que se sobreesciban con nueva información. Por lo que es posible recuperarlo mediante alguna herramienta software.

PRÁCTICA 2.3



RECUPERACIÓN DE DATOS

Existen diferentes soluciones que realizan el rastreo de información marcada como borrada en un medio de almacenamiento y que puede ser recuperable.

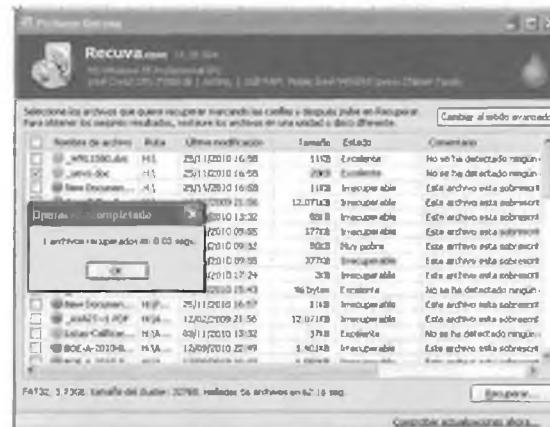
Windows

Recuva es una aplicación de archivos borrados para sistemas Windows, permite seleccionar el tipo de archivo y en qué unidades buscar archivos que están borrados o no visibles directamente en la unidad.



Es importante saber que no siempre es posible recuperar el 100% de los datos, en ocasiones se puede recuperar parcialmente parte de texto, imágenes, etc.

En muchas ocasiones los nombres de los archivos recuperados no coinciden con el original, en nuestro caso el archivo nuevo.doc que creamos y borramos definitivamente en una memoria USB (sin pasar por la papelera de reciclaje), nos lo recuperó con el nombre _uevo.doc.



El método que poseen estos programas para la búsqueda de datos en clúster de un dispositivo está basado en comparar los datos contenidos en ellos con las estructuras de datos de los formatos de archivos más comunes: texto (odt, doc, txt), gráficos (bmp, jpg, gif, png, tiff), videos (avi, mpg, mov), sonido (mp3, wav, wma), otros como html, pdf, rar, etc.

GNU/Linux

Existen diversas herramientas de recuperación de datos incluso algunas de ellas se encuentran disponibles en USB o CD/DVD Live para poder recuperar archivos incluso en caso de no poder arrancar el sistema operativo. Algunas de las más conocidas y disponibles en los repositorios de descargas son:

- **TestDisk**: incluye TestDisk que puede recuperar particiones perdidas y sectores de arranque, y **PhotoRec**, que es una herramienta sencilla de usar para la recuperación de archivos.
- **Foremost**: recupera archivos basándose en una serie de estructuras internas además de otros datos. Fue desarrollado por la fuerza aérea de los Estados Unidos y trabaja sobre todo con discos duros.
- **Scalpel**: realiza las mismas funciones que Foremost, pero se centra en un mejor rendimiento y un menor consumo del sistema, de tal manera que trabaja mejor con equipos viejos o con poca RAM.

En el caso de **Foremost**, es un programa de línea de comandos pero sin interfaz interactiva, como PhotoRec. Para instalarlo podemos ejecutar: `sudo aptitude install foremost`.

Para ver la ayuda podemos ejecutar: `foremost -h`.

En nuestro caso usaremos las siguientes opciones:

- ✓ `-t`: con una lista de extensiones de archivo, separadas por comas.
- ✓ `-v`: que es el modo detallado, para saber qué está haciendo foremost de una manera más completa.
- ✓ `-o`: indicará la carpeta dónde van a ir los archivos recuperados.
- ✓ `-i`: donde indicaremos el sitio en el que están los archivos a recuperar.

Ejemplo: `sudo foremost -t jpeg,png,gif -o foremost -v -i /dev/sda1`

`/dev/sda1` es la partición donde queremos buscar los archivos borrados o perdidos. En ocasiones es necesario realizar una copia exacta del dispositivo o partición mediante el comando dd (*duplicate disk*): `dd if=/dev/sda1 of=/home/usuario/imagen.dd`, pudiendo posteriormente emplear como ubicación de entrada (-i) a foremost dicho archivo con extensión .dd.

Foremost encuentra y guarda en carpetas por cada formato, tanto los disponibles como legibles en el disco duro, como los recuperados. Los nombres de los archivos pueden no corresponder con los originales por lo que habrá que realizar un análisis posterior de los mismos hasta encontrar los recuperados. En caso de querer conocer las particiones disponibles podemos ejecutar previamente `sudo fdisk -l`.

```

Archivo Editar Ver Terminal Ayuda
Foremost started at Wed Dec 8 11:27:39 2010
Invocation: foremost -v -t png -i /dev/sda5 -o recuperado
Output directory: /home/usuario/recuperado
Configuration file: /etc/foremost.conf
Processing: /dev/sda5
[...]
File: /dev/sda5
Start: Wed Dec 8 11:27:39 2010
Length: 37 GB 140172235204 bytes

Num Name (bs=512) Size File offset Comment
0: 00525298.png 1 KB 268952814 [32 x 32]
1: 00525383.png 2 KB 268999568 [48 x 48]
2: 00525474.png 1 KB 269042883 [32 x 32]
3: 00525552.png 1 KB 269082731 [32 x 32]
4: 00525620.png 2 KB 269120529 [48 x 48]
5: 00525708.png 1 KB 269162862 [32 x 32]
6: 00525883.png 1 KB 269252069 [32 x 32]
7: 00526154.png 2 KB 269391109 [48 x 48]
8: 00526231.png 2 KB 269431557 [48 x 48]
9: 00526478.png 1 KB 269553016 [32 x 32]
10: 00652748.png 1 KB 336501403 [32 x 32]
[...]

```

2.3 SEGURIDAD FÍSICA Y AMBIENTAL

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, *hackers*, virus, etc., la seguridad de la misma será nula si no se ha previsto cómo combatir un robo o un incendio.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa, que intenta a acceder físicamente a una sala de operaciones de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr acceder y robar una cinta o DVD de *backup*, que intentar acceder de forma remota o lógica a los datos que contienen los sistemas.

Así, la seguridad física consiste en la **aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial**.

Se refiere a los **controles y mecanismos de seguridad**, dentro y alrededor de la ubicación física de los sistemas informáticos, así como los medios de acceso al mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

En este tema se abarcarán medidas aplicables tanto a equipos de hogar y pequeñas oficinas como a servidores y centros de procesamiento de datos (CPD), que por su gran valor en la empresa requieren de medidas de seguridad específicas.

2.3.1 CENTROS DE PROCESADO DE DATOS (CPD)

Seddenomina procesamiento de datos o CPD a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como **centro de cómputo** (Iberoamérica) o **centro de cálculo** (España), o centro de datos por su equivalente en inglés **data center**. Dichos recursos consisten esencialmente en unas dependencias debidamente acondicionadas, servidores y redes de comunicaciones.

Un CPD, por tanto, es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento informático y en general electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Por ejemplo, un banco puede tener un *data center* con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías que son medianas o grandes tienen algún tipo de CPD, mientras que las más grandes llegan a tener varios interconectados, en distintas ubicaciones geográficas, con distintos **centros de respaldo**.

Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia o fallo. Debe elegirse una localización totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal.

El equipamiento hardware no tiene por qué ser igual al del CPD, aunque el software y los datos sí, por lo que es necesario contar con una **réplica de los mismos datos** con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo, por lo que existen políticas de gestión de copias síncronas o asíncronas de datos.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el **garantizar la continuidad y alta disponibilidad** del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica. Requisitos generales:

- **Disponibilidad y monitorización “24x 7x 365”:** proporcionará disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.
- **Fiabilidad infalible (5 nubes):** un 99,999% de disponibilidad, lo que se traduce en una única hora de no disponibilidad al año.
- **Seguridad, redundancia y diversificación:** almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y servicios de telecomunicaciones con balanceo de carga, SAI o sistemas de alimentación ininterrumpida, control de acceso físico, etc.
- **Control ambiental/prevención de incendios:** el control del ambiente trata de la calidad del aire, temperatura, humedad, inundación, electricidad, control de fuego, etc.

Generalmente, en un CPD todos los grandes servidores se suelen concentrar en una sala denominada sala fría, **nevera o pecera**. Esta sala requiere un sistema específico de refrigeración para mantener una temperatura baja (entre 21 y 23 grados centígrados), necesaria para evitar averías a causa del sobrecalentamiento. Según las normas internacionales, la temperatura exacta debe ser **22,3 grados centígrados**, recomendada entre 15º y 23º, y humedad relativa entre 40% y 60%.

La pecera suele contar con medidas estrictas de seguridad en el acceso físico, así como medidas de extinción de incendios adecuadas al material eléctrico, tales como extinción por agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno.

Un CPD y sus centros de respaldo por sí solo no bastan para hacer frente a una contingencia grave. Es necesario disponer de un **Plan de Contingencias** corporativo, con las **actuaciones en caso de incidente**.

Veremos algunas de las configuraciones avanzadas empleadas en alta disponibilidad en CPD y centros de respaldo en el Capítulo 8.

2.3.2 UBICACIÓN Y ACONDICIONAMIENTO FÍSICO

Aunque son difíciles de predecir con exactitud, las condiciones atmosféricas adversas severas se localizan espacial y temporalmente en ciertas partes del mundo y la **probabilidad de que ocurran está documentada**.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la ubicación y posterior construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de condiciones atmosféricas adversas, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, construcciones antisísmicas, la provisión de calor, iluminación o combustible para la emergencia. Algunos de los aspectos a tener en cuenta son:

- **Incendios:** son causados por el uso inadecuado de combustibles, fallo de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. Algunas precauciones: ubicación en área no combustible o inflamable, tener extintores manuales (portátiles) y/o automáticos (rociadores).
- **Sistema de aire acondicionado:** control de temperatura y humedad relativa según recomendaciones, entre 15º - 23º C, y 40 - 60 %, respectivamente.

- **Inundaciones:** ubicación estanca de agua, con especial precaución en puertas y ventanas.
- **Terremotos:** los fenómenos sísmicos pueden ser tan intensos que causen la destrucción de edificios. Es recomendable conocer la actividad sísmica de la localización de nuestro centro de datos para disponer de las técnicas de seguridad constructivas requeridas.
- **Rayos e interferencias electromagnéticas:** para evitar posibles desastres provocados por derivaciones de carga por rayos, y minimizar el efecto no deseado de interferencias en las comunicaciones, las salas de sistemas se protegen mediante jaula de Faraday, convirtiéndose en un búnker con respecto a radiaciones externas.

2.3.3 CONTROL DE ACCESO FÍSICO

Los ordenadores, servidores, así como las copias de seguridad con datos importantes y el software, son elementos valiosos para las empresas y están expuestas a posibles robos y actos delictivos como sabotajes o destrozos, por parte de personal ajeno o propio de la empresa. El software es una propiedad muy fácilmente sustraible y las unidades de almacenamiento como memorias USB, cintas y discos son fácilmente copiados sin dejar ningún rastro.

El uso de **credenciales de identificaciones** uno de los puntos más importantes del sistema de seguridad físico, a fin de poder efectuar un control eficaz del ingreso y salida del personal a los distintos sectores de la empresa. El control de acceso físico no solo requiere la capacidad de identificación, sino también **asociarla a la apertura o cerramiento de puertas**, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución. A las personas se les puede identificar por:

- **Algo que se posee**, por ejemplo una llave, una tarjeta de identificación o tarjeta inteligente (*SmartCard*).
- **Algo que se sabe**, por ejemplo un número de identificación único (PIN - *Personal Identification Number*) o una *password*, que se solicitará a su ingreso.
- **Algo que se es** (señas de identidad: manos, ojos, huellas digitales y voz) o **sabe hacer** (firma escrita) es un principio que emplea la **biometría**. Es el método más seguro, ya que es muy difícil de falsificar.

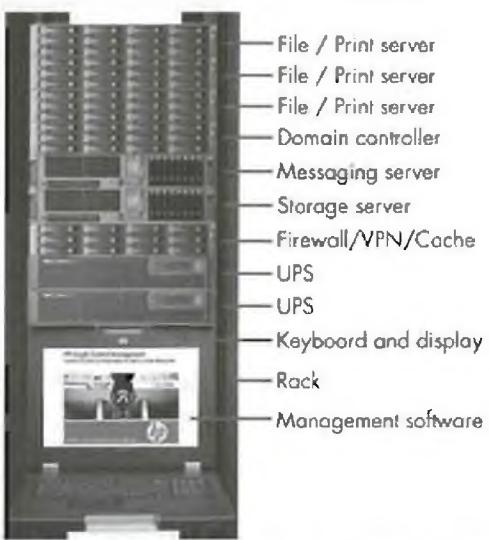
Cada una de estos identificadores asociados a cada persona o usuario se almacenan en una base de datos que debe controlar un **servicio de vigilancia** para su posterior seguimiento, si fuera necesario. La principal precaución con el personal de vigilancia es que éste puede llegar a ser sobornado. Las tarjetas pueden ser copiadas, robadas, etc., y los números secretos pueden llegar a usuarios no autorizados, permitiendo entrar a cualquier persona que la posea. La biometría ayuda a mejorar el nivel de seguridad.

Otra solución muy empleada para la seguridad de los sistemas informáticos en las salas de equipamiento informático, es disponer los mismos en un **armario** o **rack bajo llave**.

Un **rack** es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están **normalizadas** para que sea compatible con equipamiento de cualquier fabricante. Constan de un armazón metálico con un ancho normalizado de **19 pulgadas**, con 2 guías verticales que poseen agujeros a intervalos regulares llamados unidades de **Rack** (U) agrupados de tres en tres. Verticalmente, los **racks** se dividen en regiones de **1,75 pulgadas de altura = 1 U**, con tres agujeros en cada guía.

El alto (4 - 46U) y la profundidad del bastidor (600, 800, 1000 mm) no está normalizada, ya que así se otorga cierta flexibilidad al equipamiento.

El armazón suele contar con bandejas horizontales donde puede apoyarse el equipamiento no normalizado como un monitor, PC de sobremesa y un teclado o un ratón.



Los dispositivos que se suelen alojar son: servidores, paneles de parcheo (que centralizan todo el cableado del armario) sistemas de audio y vídeo, sistemas de alimentación ininterrumpida (UPS o SAI), *switches*, *routers*, cortafuegos, periféricos que permitan configuración como monitores, ratón, teclado, etc.

2.3.4 SISTEMAS BIOMÉTRICOS

Definimos la biometría como la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. Es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos, de esta forma permitirá el control de acceso físico, incluso es aplicable como método de identificación y acceso a sistemas operativos y aplicaciones. Las características biométricas de una persona son **intransferibles** a otra, por lo que hace a estos sistemas **muy seguros**.

Veamos a continuación algunas de las formas de identificación biométricas más comunes:

- **Huella digital:** se basa en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados **minucias**) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Está aceptado que cada persona posee más de 30 minucias, y que dos personas no tienen más de ocho minucias iguales, lo que hace al método sumamente confiable, y uno de los más empleados por su baja relación calidad/precio.
- **Verificación de voz:** la dicción de una (o más) frase es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.), este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc., por lo que no es un mecanismo muy adoptado.
- **Verificación de patrones oculares:** basado en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0). La principal desventaja es que es un método intrusivo. Las personas son reacias a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

■ **Verificación Automática de Firmas (VAF)**: es extremadamente difícil reproducir las dinámicas del trazo de realización de las firmas, aunque el efecto visual final parezca similar. La VAF, usa emisiones acústicas, toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es **único en cada individuo**.

Existen algunas otras soluciones a la biometría más complejas y menos usadas en acceso a organizaciones o a un sistema informático concreto, como son la geometría de la mano, el reconocimiento facial o patrones térmicos.

Lo que sigue a continuación es una tabla en la que se recogen las diferentes características de los sistemas biométricos:

Tabla 2.3

	Ojo (Iris)	Huellas dactilares	Escritura y firma	Voz
Fiabilidad	Muy alta	Muy alta	Media	Alta
Facilidad de uso	Media	Alta	Alta	Alta
Prevención de ataques	Muy alta	Alta	Media	Media
Aceptación	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Baja	Media

2.3.5 CIRCUITO CERRADO DE TELEVISIÓN (CCTV)

Se llama **protección electrónica** a la detección de robo, intrusión, asalto e incendios mediante la utilización de **sensores conectados a centrales de alarmas**. Estas centrales tienen conectados los elementos de señalización, que son los encargados de hacer saber al personal de una situación de emergencia. Uno de los métodos más empleados en las empresas son los circuitos con cámaras de grabación de vídeo o **circuitos cerrados de televisión (CCTV)**.

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizadas como medida disuasiva, incluso en ocasiones se instalan falsificaciones o cámaras que no graban) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

En la actualidad unas de las cámaras más empleadas, por bajo coste y buenas prestaciones son las **cámaras IP**. Son dispositivos autónomos que cuentan con un servidor web de vídeo incorporado, lo que les permite transmitir su imagen a través de redes IP como redes **LAN, WAN**, o incluso **WLAN** o **inalámbrica**. Las cámaras IP permiten al usuario tener la cámara en una localización y ver el vídeo en tiempo real desde otro lugar a través de Internet o una red local.

2.4 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI)

Un **SAI** (Sistema de Alimentación Ininterrumpida), también conocido por sus siglas en inglés **UPS** (*Uninterruptible Power Supply*, suministro de energía ininterrumpible), es un dispositivo que gracias a sus **baterías** puede proporcionar energía eléctrica tras un corte de suministro eléctrico a todos los dispositivos que tenga conectados, durante un tiempo limitado, permitiendo de este modo poder apagar los equipos sin que sufran cortes sus fuentes de alimentación.

Los distintos dispositivos hardware no irán enchufados a las tomas de corriente directamente, se enchufarán a la SAI que será la que estará conectada a las tomas de corriente, haciendo de este modo de intermediario entre la red eléctrica y los dispositivos hardware.



Existen distintos modelos de SAI ajustándose a las necesidades energéticas de los equipos conectados a las mismas.

Otra de las funciones de los SAI es la de **mejorar la calidad de la energía eléctrica** que llega a los aparatos, **filtrando subidas y bajadas de tensión y eliminando armónicos de la red eléctrica**. Los SAI dan energía eléctrica a equipos llamados **cargas o equipos críticos**, como pueden ser aparatos médicos, industriales o informáticos que, como se ha dicho antes, requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Tabla 2.4

Característica	Descripción
Tipo y número de conectores	Los conectores de alimentación de la carga se diferencian entre tipo IEC y Schucko. Existen tomas que solo filtran variaciones de la señal eléctrica de entrada (impresora, fax, escáner), de aquellas que filtran y tienen alimentación de la batería en caso de corte de suministro (equipos, monitores, dispositivos de comunicaciones) denominadas de <i>backup</i> .
Otras conexiones	Conectores para la protección de Líneas de Datos RJ11-RJ45 para dispositivos de Teléfono/Fax/DSL/Internet/MODEM. Conexiones seriales COM o USB para monitorización y consulta de estado remoto, mediante software específico.
Tiempo de funcionamiento solo con batería	Según el modelo y la carga conectada, la batería suele estar diseñada para suministrar alimentación desde varios minutos hasta varias de horas y, de esa forma, apagar los sistemas conectados correctamente.
Regulador de voltaje	Integrado para evitar picos (subidas y bajadas) de tensión que se producen en la línea de suministro de entrada y que si no se filtran pueden afectar a las fuentes de alimentación de los equipos.

2.4.1 TIPOS DE SAI

Habitualmente, los fabricantes de SAJ clasifican los equipos en función de la tecnología y calidad de la señal eléctrica generada a su salida:

- **SAI OFFLINE**: los más económicos, recomendados para equipos en el hogar. No estabilizan la corriente y solo generan la tensión de salida cuando se produce un corte de suministro eléctrico.
- **SAI INLINE o LINE INTERACTIVE**: equipos de gama media-alta que estabilizan la corriente incorporando un estabilizador de salida (AVR). Solo general la tensión de salida cuando se produce un corte de suministro eléctrico. Son adecuados para ordenadores, centralitas telefónicas y equipos servidores de pequeñas y medianas empresas (Pymes).
- **SAI ONLINE o de DOBLE CONVERSION**: equipos de gama alta, pensados para proteger sistemas críticos. Estos equipos generan siempre la tensión de salida nueva, independientemente de la entrada.

2.4.2 POTENCIA NECESARIA

Para ajustar las dimensiones y capacidad eléctrica de la batería de la SAI a la que enchufar nuestros equipos, también denominados carga, es necesario realizar un cálculo de la potencia que consumimos y por tanto que necesitamos suministrar por las conexiones de batería de la SAI.

La **potencia eléctrica** se define como la cantidad de energía eléctrica o trabajo que se transporta o que se consume en una determinada unidad de tiempo.

Cuando se trata de corriente continua (CC) la potencia eléctrica (P) desarrollada en un cierto instante por un dispositivo de dos terminales, es el producto de la diferencia de potencial entre dichos terminales (V) y la intensidad

de corriente (I) que pasa a través del dispositivo. Esto es, $P = V \times I$. Si I se expresa en amperios y V en voltios, P estará expresada en vatios.

En circuitos eléctricos de corriente alterna (CA), como son las tomas de corriente (enchufes), se emplean medidas de potencia eficaz o aparente y potencia real. La unidad de potencia que suministran comercialmente los SAI es el **voltiamperio (VA)**, que es **potencia aparente**, también denominada potencia efectiva o eficaz, consumida por el sistema.

Si tenemos la potencia en vatios (W) **potencia real**, de forma aproximada se multiplica por 1,4 para tener en cuenta el pico máximo de potencia que puede alcanzar su equipo y de esta forma obtener la potencia aparente en VA.

Por ejemplo: $200 \text{ W} \times 1,4 = 280 \text{ VA}$. En ocasiones el factor 1,4, puede ser 1,33 ó 1,6 o factor divisor 0,7 ó 0,75, depende de la eficiencia energética del dispositivo electrónico.

Algunos métodos para calcular el consumo en W de nuestros equipos y de esta forma estimar.

- Mediante un medidor de potencia o mediante una pinza ampermétrica (ver la siguiente figura) que mida la corriente suministrada para los equipos conectados, de esta forma multiplicando por la tensión nominal (en España 230 V), podremos obtener el consumo medio aproximado.



- Conociendo el consumo medio (W) suministrado en las características del fabricante.
- Mediante un modelo aproximado de estimación de consumos, tomando como referencia estimaciones previas. Por ejemplo podemos ver estimaciones de consumos en la web de etiquetado de eficiencia energética Energy Star. Veremos un ejemplo a continuación.

La carga total enchufada a la batería de la SAI, se recomienda que **no sobrepase el 70%** del total de la potencia suministrada por la misma.

Por ejemplo: en caso de querer enchufar a 4 tomas de una SAI, 2 PC y 2 monitores que consumen en total 200 W, nuestra SAI deberá de suministrar $200 \times 1,4 = 280 \text{ VA}$. Por tanto, nuestra SAI deberá de tener al menos una potencia máxima suministrada de $280 \times 100/70 = 400 \text{ VA}$.

Tabla 2.5

Dispositivo	Consumo (W)	Dispositivo	Consumo (W)
PC Económico Core2 Duo (2,8 GHz) o Athlon II X2 / 2 GB RAM / 500 GB	41	Monitor 15" CRT	45
Escríptorio multimedia, Phenom II o Core i7 / 2,7 GHz / 4 GB RAM / 500 GB y gráficos más potentes	67	Monitor 17" CRT	55
PC de escritorio a medida para CAD, gráficos o investigación científica: Xeon / 2,7 GHz / 8 GB RAM / 500 GB / 64 bit OS	190	Monitor 17" LCD	19
Netbook: Atom o Via Nano, 10" LCD-TFT.	5,9	Monitor 19" LCD	21
Portátil económico: Core2 Duo or Turion 64 X2, 15-17" LCD-TFT.	12	Monitor 30" LCD	110
Impresora láser	600	Módem externo	9
Multifunción láser	250	Impresora inyección de tinta	40
Multifunción inyección	50	Escáner	10

PRÁCTICA 2.4

MONITORIZACIÓN DE SAI

A modo de ejemplo se presenta a continuación la parte posterior de una SAI de la compañía **Emerson, Liebert PowerSure™ PSP 650VA**:

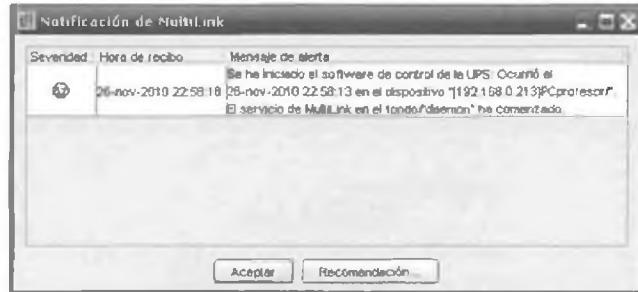


Recomendación de conexión del fabricante, en tomas de *backup* y filtrado: monitores, equipos de sobremesa y de comunicaciones (*switch, router, etc.*), en tomas de protección contra picos de corriente: impresoras, escáner, fax.



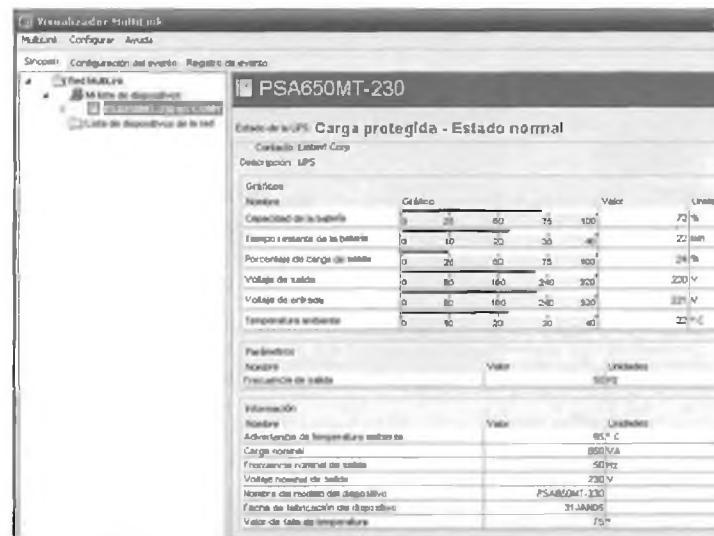
Las SAI disponen entre otras funciones de conexión para monitorización y consulta de estado remoto, mediante puerto serial COM o USB normalmente, a través de un software específico suministrado por la compañía fabricante. A continuación se muestran las características y funcionamiento del software multiplataforma (Windows, GNU/Linux, etc.) **Multilink** que facilita el fabricante Emerson con sus SAI:

Posee un sistema de alertas que indican el estado y posibles incidencias y medidas a tomar sobre los sistemas conectados a la SAI:



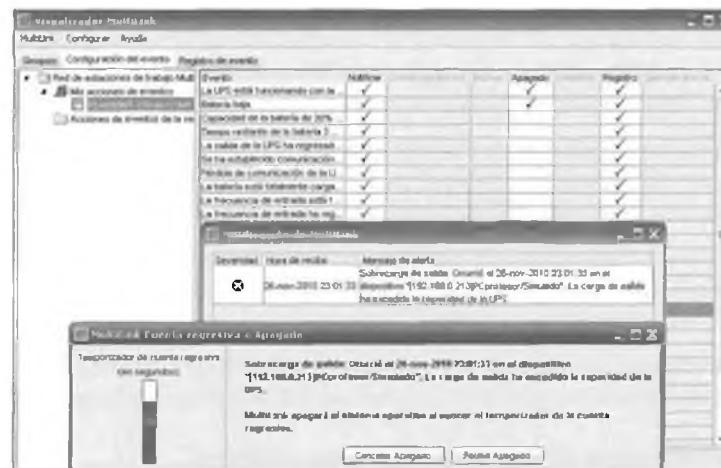
La pantalla de monitorización de estado permite visualizar en una primera pestaña una **sinopsis** de los principales parámetros:

Capacidad de la batería, tiempo restante en caso de falta de suministro de entrada, porcentaje de carga conectado a la salida de la SAI, es recomendable que se encuentre siempre por debajo del 60 - 80%, voltajes de salida y entrada y sensor de temperatura.



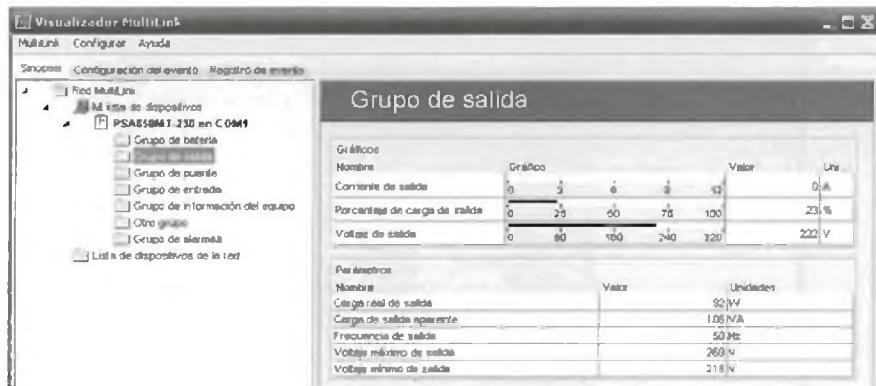
Existen otras 2 pestañas de configuración y registro de eventos:

Es posible efectuar eventos sobre la SAI y ver qué tipo de recomendaciones y efectos produciría sobre nuestro sistema. En el ejemplo se ha producido artificialmente una sobrecarga de salida, más consumo energético del que puede suministrar la batería de la SAI, y como medida de seguridad en un tiempo límite de 1 minuto el software apagará el sistema operativo como medida de seguridad.



A su vez, la pestaña de registro de eventos, facilita un histórico de eventos en la SAI.

Es posible ver con más profundidad aspectos del grupo de salida, entrada, etc., para analizar por ejemplo el consumo en W y VA de los equipos conectados, por ejemplo en el caso de tener conectados un PC Pentium 4 a 2 Ghz con 2 GB de memoria RAM y un monitor LCD de 17" el consumo conjunto es de 92 W y 106 VA. Como podemos ver el factor multiplicativo entre la potencia real (W) y la aparente (VA) es de $106/92=1,15$. Podemos concluir, de este modo, que el factor multiplicativo 1,4 es aproximado y nos servirá para realizar cálculos teóricos.



PRÁCTICA 2.5

CÁLCULO ENÉRGETICO DE SAI



ENERGY STAR es un programa voluntario de etiquetado para la eficiencia energética iniciado por la Agencia de protección del medio ambiente estadounidense (EPA) en 1992. La Comunidad Europea, a través de un acuerdo celebrado con el gobierno de los Estados Unidos, participa en el programa ENERGY STAR para los equipos ofimáticos (*European Council Decision*).

El etiquetado ENERGY STAR representa los requisitos de eficacia energética que cualquier fabricante respetuoso con el medio ambiente debe cumplir. Con esta etiqueta podemos elegir los modelos de los equipos ofimáticos con mayor eficiencia energética y que mejor se adapten a nuestros criterios de rendimiento.

En la web www.eu-energystar.org podemos encontrar información y consejos sobre las ventajas que supone la compra del equipo ofimático más eficiente desde el punto de vista energético, qué configuración de ahorro de energía resulta más ventajosa y cómo sacarle el máximo rendimiento.

Posee también una interesante aplicación de **cálculo estimado de consumo energético para usuarios particulares y empresas**. A continuación se muestra una tabla resumen de consumos medios aproximados de dispositivos ofimáticos en modo encendido o activo:

Podemos concluir que los sistemas con pantalla integrada y multifunción consumen aproximadamente menos del 50% que sus equivalentes con pantalla separada o componentes (escáner, impresora, etc.) separados.

A modo de ejemplo plantearemos el siguiente supuesto práctico:

La empresa Scripting S.L. nos contrata para dimensionar tanto sus armarios de servidores y comunicaciones, como sus SAIs en un entorno de oficina:

En la entrevista con el responsable de IT nos indica: "Disponemos de 2 PCs de escritorio con sus monitores, 2 portátiles, 1 impresora láser, 1 escáner, 1 servidor para *backup* con un monitor para su configuración, 1 panel de parcheo y 1 dispositivo multifunción *router* inalámbrico. Estamos interesados en poder poner los equipos principales de nuestra empresa en un armario de 19"" que tenemos de unos 100 cm de alto. Nuestras instalaciones no sufren demasiadas subidas, bajadas ni cortes de electricidad, pero queremos prevenir posibles eventualidades".

Tabla 2.6

Dimensiones Ancho x alto (cm)	Dispositivo	Consumo
20 x 40	PC escritorio	75 W
30x 35	Portátil	32 W
40 x 30	Impresora láser	180 W
20 x 10	Router inalámbrico	0,1 A lectura de pinza amperimétrica
32x 35	Monitor	30 W
48,26 x 8,88	Servidor	Fuentes de alimentación 600 W, consumo medio 30%
48,26 x 4,44	Panel de parcheo	
32 x 10	Escáner	2,3 A lectura de pinza amperimétrica

Datos 1 U = 1,75 ", 1" = 2,54 cm. SAI ofertada por el proveedor APC 800 VA con 6 tomas de *backup* y filtrado y 2 tomas con filtros de bajadas y picos de tensión, disponibles en modelos *offline*, *inline* u *online*, tanto versión *rack*, de ocupación 1 U, como para sobremesa.

Contestaremos a las siguientes cuestiones:

Tipo de SAI seleccionada (*on-line*, *in-line* u *off-line*). Justifica la respuesta.

La mejor opción en relación calidad precio suele ser la SAI *inline*, en caso de tener muchas alteraciones en el suministro eléctrico, y necesitar una disponibilidad mayor de los sistemas por las características de la empresa, optariamos por la opción *online*. Tan solo para usuarios domésticos se recomienda la opción *offline*.

Diferenciar dispositivos según ubicación:

- Oficina: 2 PCs y 2 monitores, 2 portátiles, 1 impresora, 1 escáner.

Consumo de equipos conectados a SAI (W): Optaremos por una SAI de sobremesa *inline*. A la SAI conectados a batería para *backup* solo serán necesarios los 2 PCs y 2 monitores. Por tanto el consumo será de $(75 + 30) \times 2 = 210 \text{ W} \rightarrow 210 \times 1,4 = 294 \text{ VA}$ aproximadamente. Si se recomienda que la SAI debe estar al 60% de carga $294 \times 100/60 = 490 \text{ VA}$, por lo que las SAI ofertada por APC (800 VA) será suficiente.

Los 2 portátiles llevan su propia batería no es necesario tenerlos conectados a la SAI. La impresora y el escáner se conectarán a las 2 conexiones de filtrado disponibles.

- Armario o *rack*: 1 servidor, 1 monitor, 1 router, 1 panel de parcheo.

Para el armario disponible: ¿Es posible ubicar los equipos más críticos en el armario disponible por la empresa?

1 U = $1,75 \times 2,54 = 4,44 \text{ cm}$ de altura. Recordamos el ancho normalizado son $19" = 19 \times 2,54 = 48,26 \text{ cm}$.

El armario en total dispone de $100 \text{ cm} / 4,44 \text{ cm/U} = 22,52 \text{ U}$ por tanto tan solo dará cabida a 22 U.

- Armario o *rack*: De ancho normalizado y por tanto atornillables directamente: 1 servidor ($8,8/4,4 = 2 \text{ U}$), 1 panel de parcheo ($4,4/4,4 = 1 \text{ U}$), en bandejas independientes separadas: 1 monitor ($35/4,4 = 7,95$ por tanto 8 U) y 1 router ($10/4,4 = 2,27$ por tanto 3 U).

En total serán necesarios 2 bandejas de ocupación 1 U cada una, más 1U para la SAI, más 14 U para el resto de equipos = 17 U.

Consumo de equipos conectados a SAI (W): Optaremos por una SAI de rack *in-line*. A la SAI conectados a batería para *backup* solo serán necesarios el servidor, *router* y 1 monitor. Por tanto, el consumo respectivamente será de $(0,3 \times 600\text{ W} + 0,1\text{ A} \times 230\text{ V} + 30\text{ W}) = 233\text{ W} \rightarrow 233 \times 1,4 = 326,2\text{ VA}$ aproximadamente. Si se recomienda que la SAI debe estar al 60% de carga $326,2 \times 100/60 = 543,66\text{ VA}$, por lo que las SAI ofertada por APC (800 VA) será suficiente.

El panel de parcheo es un elemento pasivo no conectado a red eléctrica.

2.5 REFERENCIAS WEB

- Soluciones de almacenamiento para empresas HP:
<http://welcome.hp.com/country/es/es/smb/storage.html>
- Soluciones de almacenamiento y copia de seguridad Dell:
<http://www.dell.es/>
- Empresa dedicada a copias de seguridad remotas:
<http://www.copiadeseguridad.com/>
- Blog de seguridad informática. Copias de seguridad:
<http://www.bloginformatico.com/etiqueta/copias-de-seguridad>
- Almacenamiento de datos en Internet Idrive:
<http://www.idrive.com>
- Seguridad física. Red - Iris:
<http://www.rediris.es/cert/doc/unixsec/node7.html>
- Sitio web sobre SAI:
<http://www.newsai.es/>
- Catálogo, manuales y documentación de SAI:
<http://www.apc.com/es/>
- Noticias y medidas de seguridad para CPD:
<http://www.seguridadcpd.com/>
- Soluciones técnicas para el control de acceso físico:
<http://www.accesor.com/>
- Soluciones técnicas de biometría:
<http://www.biometriaaplicada.com/>



RESUMEN DEL CAPÍTULO

En este capítulo hemos analizado los principios de la **seguridad pasiva** para intentar minimizar el impacto y los efectos causados por accidentes.

Por un lado, después de ver en el Capítulo 1 que el elemento fundamental a proteger en un sistema son los datos, hemos analizado:

- Modelos de almacenamiento según el volumen de información y tamaño de la organización: DAS, NAS y SAN.
- La importancia, como recomendación transversal en seguridad informática, de una adecuada política de gestión de copias de seguridad de los datos críticos de una organización, analizando tipos (completa, incremental y diferencial), temporización, cifrado y comprensión, así como redundancia y distribución geográfica de las mismas.
- Las posibilidades de recuperar datos perdidos o borrados, mediante software específico.

En cuanto a las medidas relativas a la seguridad física se han estudiado:

- Ubicación y acondicionamiento de centros de procesamiento de datos (CPD) y de respaldo, atendiendo a aspectos como:
 - Refrigeración y protección frente a incendios e inundaciones.
 - Control de acceso físico, con medidas como la biometría, armarios de seguridad y circuitos cerrados de televisión (CCTV) para controlar robos y sabotajes.
 - SAI - UPS o generadores autónomos, dimensionados para proporcionar energía eléctrica estable en caso de fallos o alteraciones de suministro.



EJERCICIOS PROPUESTOS



- 1. Realiza una tabla comparativa en la que compares el tamaño en Gigabytes (GB), precio del dispositivo, y divide el precio/capacidad o tamaño en GB para obtener el precio por cada GB de distintas memorias comerciales: memoria RAM, disco duro a 5400 y 7200 rpm, CD, DVD, cinta de *backup*, memorias y discos duros USB.
- ¿Cuál es la memoria más barata? ¿Cuál es la más rápida? ¿Crees que las memorias de estado sólido o *flash* sustituirán a los discos magnéticos como el disco duro? Busca y comenta algunos sistemas informáticos que hayan sustituido el disco duro por memorias de estado sólido.
- 2. Busca información comercial en HP o Dell sobre sistemas de almacenamiento en cinta.
- ¿Crees que hoy en día se siguen utilizando? ¿Cuáles suelen ser sus aplicaciones? ¿Por qué crees que se siguen empleando? ¿Cuál es el coste por MB? Busca una unidad lectora/grabadora de cinta y una cinta e indica su coste.
- 3. Busca una empresa que se dedique a recuperar los datos de fallos físicos de discos e indica sus precios y servicios ofertados. ¿Te parecen caros los servicios de recuperación de datos? ¿Cuáles son los principales fallos, recomendaciones y precauciones que se deben tener con los discos duros?
- 4. Para realizar copias de seguridad en Internet hemos visto que existen sitios FTP gratuitos como Dropbox, Idrive o Mozy, existen otras empresas especializadas en *backup* remoto de pago. Analiza qué servicios ofrecen y a qué precios, las empresas www.copiadaseguridad.com y www.perfectbackup.es.
- 5. Para garantizar un espacio seguro de nuestras copias de seguridad podemos optar por contratar los servicios de empresas que realicen la recogida y custodia de copias de seguridad ¿Qué servicios y precios ofrecen empresas como www.esabe.com y www.copiassegura.com? ¿Qué normativa deben cumplir con respecto a seguridad informática?
- 6. Realiza una comparativa de distintas aplicaciones de software de copia de seguridad analizando las opciones que permiten respecto a: tipo (completa/incremental/diferencial) y temporización de copias, origen y destino de copias (opciones de alojamiento remoto), compresión, algoritmos de cifrado y contraseñas. Ejemplos para Windows: Cobian, Uranium Backup, Backup4all, Fiabee, FBackup, etc., y para GNU/Linux: Fwbackups, Rsync, Bacula, Amanda, Simple Backup, Duplicity, Backup PC, Suite Simple Backup, Back in time, etc.
- 7. Dentro de las herramientas de copia de seguridad encontramos herramientas específicas de realización de copia exacta, clonado o imágenes de disco, que permiten la restauración exacta de una determinada partición de disco. Indica algunos ejemplos de software de clonado de discos ¿Cómo se guardará la copia de seguridad por ejemplo para una partición que ocupe 40 GB? ¿Se realiza en un único soporte?
- 8. En ocasiones para poder restaurar la configuración de un equipo es interesante tener una copia de seguridad de nuestros controladores. Realiza una copia de seguridad de los controladores o *drivers* de tu equipo mediante alguna aplicación específica como **DriverMax** o similar. Valora ventajas e inconvenientes de este tipo de software en función de las opciones que permite realizar. ¿Qué utilidad puede tener una copia de seguridad de tus *drivers*? ¿Es posible siempre recuperarlos, incluso teniendo el listado de dispositivos? ¿Y en caso de no tener dicho listado?
- 9. Análisis de mejoras de un CPD en una solución real. Lee y analiza el siguiente caso real “Solución integral de CPD altamente seguro para Supermercados Condis”, en la fuente web: http://www.abast.es/cs_condis_cpd.shtml.
 - ¿Qué se considera un “traslado en caliente”? ¿Cuáles eran los riesgos que corrían y que podrían poner en peligro su anterior CPD? ¿Qué es una auditoría? ¿Quién tomó la decisión de cambio?
 - ¿Cómo se podrían resumir las soluciones adoptadas por la empresa en los distintos ámbitos? ¿Las SAIs y el resto de sistemas se encuentran en la misma sala? ¿Por qué?

- 10. Busca información referente al lector de huella dactilar y el software asociado Fingerprint Logon Manager, que HP integra en sus portátiles y contesta las siguientes preguntas como entrada en tu blog:
 - ¿Cuáles son las ventajas de usar el lector de huellas digitales para iniciar sesión en un equipo? ¿Cómo es el proceso de configuración software del lector de huellas digitales?
 - ¿Qué precauciones o recomendaciones de uso se recomiendan a la hora de emplear el lector de huella? ¿Se puede iniciar la sesión en Windows con el lector de huellas digitales? ¿Es compatible con otro tipo de sistemas operativos?
 - ¿Se puede usar un dedo diferente para iniciar sesión en el PC? ¿Es posible que varios usuarios inicien sesión con el lector de huellas digitales en el mismo PC?
- 11. Para evitar robos en espacios públicos, o aulas, existen una serie de soluciones de seguridad física como: armarios de seguridad con llave, carritos móviles para equipos informáticos, cables de seguridad para portátiles y llaves y candados para equipos y periféricos.
 - Encuentra un armario y sus características en dimensiones para que dé cabida a un *switch*, panel de parcheo, PC (sobremesa con funciones de servidor) con monitor, teclado, ratón y SAI. En primer lugar, deberás elaborar una lista con las dimensiones de cada componente para poder hacer una estimación del espacio necesario en el armario.
 - ¿Qué precio y en qué distribuidor has encontrado dicho armario? ¿Qué características tiene la puerta y la llave de dicho armario, crees que sería totalmente seguro? Explica tus razones.
- 12. A través del distribuidor www.senor.com podrás encontrar un conjunto de soluciones de seguridad para aulas de ordenadores. Diseña una solución con presupuesto, que permita dar seguridad a un aula como la que dispones, en la que se quiera tener también 15 ordenadores portátiles.
- 13. Busca en la web de alguna empresa que facilite soluciones de control de accesos a CPD, como por ejemplo www.zksoftware.es, encuentra y explica las diferencias existentes, entre los terminales de presencia (con tarjeta identificadora), terminales de huella dactilar, y terminales con código y *password*. Analiza y explica cómo funciona el software de control de accesos, para una empresa con cientos de empleados.
- 14. Si tu equipo no dispone de lector de huella, existen diversos periféricos que permiten el control del PC únicamente mediante la utilización de la huella registrada de usuario. Investiga acerca de los precios y características de periféricos como teclado, ratón, disco duro o memoria USB o incluso lector de huella USB independiente, así como las opciones de software que existen, como eNDeSS. ¿Qué niveles de acceso controla dicho software? Realiza una tabla resumen con precios y características.
- 15. Analiza las características y el funcionamiento del sistema BioCloser de reconocimiento de voz. Explica su principio de funcionamiento y para qué se puede emplear.
- 16. Busca información acerca del control de acceso *Biopassword* y descubre su principio de funcionamiento probándolo a través de su demo. ¿Cuál es el principio de funcionamiento? ¿Qué parámetros mide? ¿Crees que podría ser útil este sistema como control de acceso biométrico?
- 17. Diseña una infraestructura de cámaras de vigilancia IP inalámbricas, con 4 cámaras que permita controlar la planta de un edificio. Indica los equipos necesarios aparte de las cámaras, espacio de almacenamiento necesario y períodos de realización de copias de seguridad.
 - Crea una tabla con el coste de la instalación desglosado con cada uno de sus componentes así como la mano de obra de instalación y configuración.
 - ¿Qué leyes se aplican sobre la filmación de vídeo en espacios públicos y en privados? A modo de resumen, ¿qué precauciones y recomendaciones se deben tomar a la hora de realizar grabaciones de seguridad? Busca alguna noticia sobre la implantación de cámaras de seguridad en las vías públicas de las ciudades y qué tipo de controversias ha originado.
- 18. Encuentra una SAI para todos los sistemas de tu aula, sirviéndote y ajustando los consumos de los equipos en base a las estimaciones de Energy Star, y teniendo como máximo una carga del 70% de la potencia máxima suministrada por la batería. Justifica tu respuesta e indica tipo, número y tipos de tomas, potencia suministrada en VA, etc. En caso de no encontrar una SAI con suficiente capacidad, realiza una división de la carga entre distintas SAIs.
 - Es necesario disponer una SAI para un portátil o un notebook? ¿Por qué? ¿Qué función realiza el transformador de corriente del portátil? ¿Y las celdas de baterías?



TEST DE CONOCIMIENTOS

1 Las medidas de seguridad biométricas:

- a) Permiten el acceso a un sistema mediante contraseña asimétrica.
- b) Emplean la biología para medir parámetros de seguridad.
- c) Emplean características biológicas para identificar usuarios.
- d) Son el fundamento de la identificación mediante certificado digital.

2 Las SAIs:

- a) Permiten conectarse ininterrumpidamente a la red eléctrica.
- b) Suministran corriente eléctrica frente a cortes de luz.
- c) Son dispositivos de almacenamiento de alta disponibilidad.
- d) Son programas que permiten mantener confidencialidad.

3 Los armarios o bastidores para albergar sistemas no poseen:

- a) Profundidad variable.
- b) Ancho fijo.
- c) Altura múltiplo de 1 U.
- d) Profundidad fija.

4 El sistema biométrico másiable y seguro es:

- a) Reconocimiento de voz.
- b) Huella dactilar.
- c) Iris.
- d) Escritura y firma.

5 La pinza ampermétrica sirve para realizar medidas de:

- a) Voltaje (V).
- b) Potencia aparente (VA).
- c) Corriente eléctrica (A).
- d) Potencia real (W).

6 En caso de tener una instalación CPD crítico con un suministro eléctrico muy fluctuante, el tipo de SAI a utilizar es:

- a) Online o doble conversión.
- b) Offline.
- c) Inline.
- d) Línea interactiva.

7 Si el espacio que disponemos para realizar copias de seguridad es limitado éstas deben ser:

- a) Completas.
- b) Incrementales.
- c) Diferenciales.
- d) Completas + Diferenciales.

8 El sistema biométrico mas empleado por su relación fiabilidad/coste es:

- a) Reconocimiento de voz.
- b) Huella dactilar.
- c) Iris.
- d) Escritura y firma.

9 En los sistemas GNU/Linux para realizar copias de seguridad automatizadas no se emplea el comando:

- a) Bkp.
- b) Crontab.
- c) Tar.
- d) Gzip.

3

Seguridad lógica

OBJETIVOS DEL CAPÍTULO

- ✓ Profundizar en aspectos de seguridad lógica.
- ✓ Valorar la importancia del uso de contraseñas seguras.
- ✓ Restringir el acceso autorizado en el arranque, sistemas operativos, ficheros, carpetas y aplicaciones.
- ✓ Analizar las ventajas de disponer el sistema y aplicaciones actualizadas.
- ✓ Garantizar el acceso restingido de los usuarios a datos y aplicaciones, mediante políticas de seguridad.

3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA

El activo más importante que se poseen las organizaciones es la **información**, y por lo tanto deben existir técnicas más allá de la seguridad física que la aseguren, estas técnicas las brinda la seguridad lógica.

La **seguridad lógica** consiste en la *aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo*. A lo largo de los capítulos 3 (seguridad en el acceso lógico a sistemas), 4 (software antimalware), y 5 (criptografía), veremos algunos de los métodos fundamentales.

Algunas de las principales amenazas que tendrán que combatir los administradores de sistemas son el **acceso y modificaciones no autorizadas a datos y aplicaciones**.

La seguridad lógica se basa, en gran medida, en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en identificación, autenticación y autorización de accesos.



Como principio básico de seguridad lógica en la configuración de sistemas: todo lo que no está permitido debe estar prohibido.



NOTICIA DE ACTUALIDAD

A lo largo de este capítulo vamos a comprobar la importancia de emplear contraseñas fuertes y la responsabilidad que tienen sobre el control de las mismas los desarrolladores de software y administradores de sistemas.

Para ello se propone la lectura del artículo “Utilizando mapas como contraseñas de acceso, una nueva idea de seguridad informática”, fuente: http://noticias.lainformacion.com/ciencia-y-tecnologia/tecnologia-general/utilizando-mapas-como-contraseñas-de-acceso-una-nueva-idea-de-seguridad-informatica_Kt8uDQyuXZu27JJbyXmVr4/.

Se propone comentar en grupo las siguientes cuestiones:

- ¿Qué longitud de contraseña presenta este nuevo método? ¿Qué código de caracteres utiliza?
- ¿Qué mecanismos y herramientas malware elude? ¿Qué metodología se podría emplear para obtener la contraseña?
- ¿Qué precauciones deberíamos de tomar a la hora de registrar nuestras contraseñas? ¿Y especialmente en redes sociales?

3.2 CONTROL DE ACCESO LÓGICO

El control de acceso lógico es la principal línea de defensa para la mayoría de los sistemas, permitiendo prevenir el ingreso de personas no autorizadas a la información de los mismos.

Para realizar la tarea de controlar el acceso se emplean 2 procesos normalmente: identificación y autenticación. Se denomina **identificación** al momento en que el usuario se da a conocer en el sistema; y **autenticación** a la verificación que realiza el sistema sobre esta identificación.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de ahí a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina *single login* o sincronización de *passwords*.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un **servidor de autenticaciones** sobre el cual los usuarios se identifican y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas. Es el caso de servidores LDAP en GNU/Linux y Active Directory sobre Windows Server.

Los sistemas de control de acceso protegidos con contraseña, suelen ser un punto crítico de la seguridad y por ello suelen recibir distintos tipos de ataques, los más comunes son:

- **Ataque de fuerza bruta:** se intenta recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Cuanto más corta, más sencilla de obtener probando combinaciones.
- **Ataque de diccionario:** intentar averiguar una clave probando todas las palabras de un diccionario o conjunto de palabras comunes. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta, ya que muchos usuarios suelen utilizar una palabra existente en su lengua como contraseña para que la clave sea fácil de recordar, lo cual no es una práctica recomendable.

Una forma sencilla de proteger un sistema contra los ataques de fuerza bruta o los ataques de diccionario es establecer un **número máximo de tentativas**, de esta forma se bloquea el sistema automáticamente después de un número de intentos infructuosos predeterminado. Un ejemplo de este tipo de sistema de protección es el mecanismo empleado en las tarjetas SIM que se bloquean automáticamente tras tres intentos fallidos al introducir el código PIN.

A continuación veremos criterios para establecer políticas seguras de contraseñas.

3.2.1 POLÍTICA DE CONTRASEÑAS

Las contraseñas son las claves que se utilizan para obtener acceso a información personal que se ha almacenado en el equipo y aplicaciones, como en los entornos web (*mail*, banca *online*, redes sociales, etc.). Para que una contraseña sea segura se recomienda:

- **Longitud mínima:** cada carácter en una contraseña aumenta exponencialmente el grado de protección que ésta ofrece. Las contraseñas a ser posible deben contener un mínimo de 8 caracteres, lo ideal es que tenga 14 caracteres o más.

- **Combinación de caracteres** (letras minúsculas y mayúsculas, números y símbolos especiales): cuanto más diversos sean los tipos de caracteres de la contraseña más difícil será adivinarla.

Para un ataque de **fuerza bruta** que intenta encontrar contraseñas generando todas las combinaciones posibles, si empleamos una contraseña de 5 caracteres en minúscula para el idioma español que posee 27 caracteres diferentes, tendría que probar $27^5 = 14\,348\,907$ combinaciones a probar.

En caso de emplear mayúsculas y minúsculas el número de combinaciones se multiplicaría siendo $(27 \times 2)^5 = 52^5 = 380\,204\,032$ combinaciones a probar.

Algunos métodos que suelen emplearse para crear contraseñas resultan fáciles de adivinar, a fin de evitar contraseñas poco seguras, se recomienda:

- ✓ **No incluir secuencias ni caracteres repetidos.** Como "12345678", "222222", "abcdefg".
- ✓ **No utilizar el nombre de inicio de sesión.**
- ✓ **No utilizar palabras de diccionario de ningún idioma.**
- ✓ **Utilizar varias contraseñas para distintos entornos.**
- ✓ **Evitar la opción de contraseña en blanco.**
- ✓ **No revelar la contraseña a nadie y no escribirla en equipos que no controlas.**
- ✓ **Cambiar las contraseñas con regularidad.**

PRÁCTICA 3.1



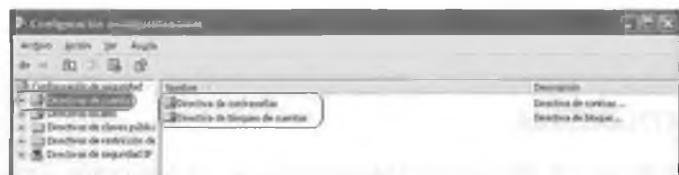
CONFIGURACIÓN DE CONTRASEÑAS SEGURAS

Todas las recomendaciones anteriormente citadas están muy bien cuando se conocen y se llevan a cabo, pero, ¿no sería mejor opción evitar que los usuarios tengan contraseñas **inseguras o débiles** y que no se cambien nunca? Veamos qué opciones de configuración sobre el control de contraseñas poseen los sistemas operativos.

Windows

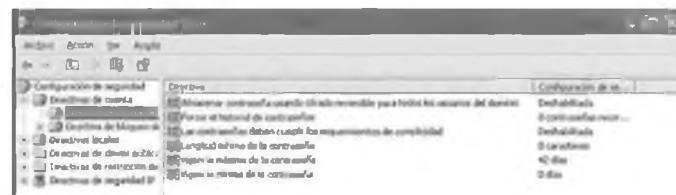
Las **directivas de cuentas** nos permiten configurar el comportamiento que van a tener éstas ante una serie de sucesos. La importancia de una correcta configuración de estas directivas radica en que desde ellas vamos a poder controlar de una forma más eficiente la forma de acceder a nuestro ordenador.

En primer lugar, accedemos a la ventana de **Directivas de seguridad de cuentas**, mediante la ejecución del comando `gpedit.msc` o desde el *Panel de control / Herramientas administrativas / Directivas de seguridad local*.



Una vez en la ventana de las **Directivas de seguridad local** nos encontramos a la izquierda con varias directivas. Trataremos la **Directivas de cuentas**. Como podemos ver, en este grupo de directivas tenemos dos subgrupos, **Directiva de contraseñas** y **Directiva de bloqueo de cuentas**. Vamos a ver qué podemos hacer en cada uno de ellos:

✓ Directiva de contraseñas:



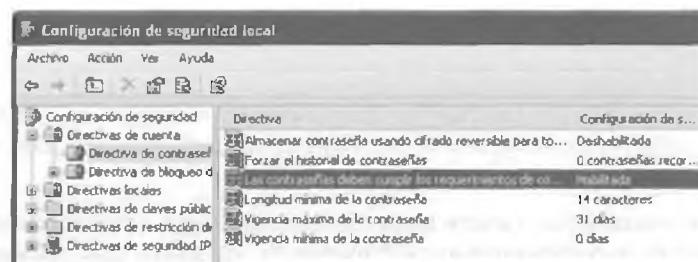
Dentro de las directivas de contraseña nos encontramos con una serie de directivas como:

- **Almacenar contraseña usando cifrado reversible para todos los usuarios del dominio.**
- **Forzar el historial de contraseñas:** Establece establece el número de contraseñas a recordar, los usuarios no pueden utilizar la misma contraseña cuando ésta caduca.. Se recomienda un valor mínimo de 1.
- **Las contraseñas deben cumplir los requerimientos de complejidad:** Se recomienda habilitar esta opción, la cual obliga para nuevas contraseñas:
 - 6 caracteres como mínimo.
 - Contener caracteres de al menos tres de las cinco clases siguientes: Mayúsculas, minúsculas, dígitos en base 10, caracteres no alfanuméricos (por ejemplo: !, \$, # o %), otros caracteres Unicode.
 - No contener tres o más caracteres del nombre de cuenta del usuario.
- **Longitud mínima de la contraseña.**
- **Vigencia máxima de la contraseña:** Establece establece el número de días máximo que una contraseña va a estar activa.
- **Vigencia mínima de la contraseña:** Establece establece el número de días mínimos que una contraseña va a estar activa. Si es mayor que 0, los usuarios no pueden cambiar repetidamente las contraseñas para eludir la configuración de directiva Forzar el historial de contraseñas con el fin de utilizar su contraseña original.

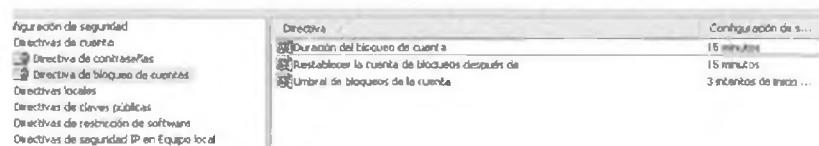
✓ Directiva de bloqueo de cuentas:

- **Duración del bloqueo de cuentas:** Establece establece, en minutos, el tiempo que una cuenta debe permanecer bloqueada.
- **Restablecer la cuenta de bloques después de:** Establece establece, en minutos, el tiempo que ha de pasar para restablecer la cuenta de bloques.
- **Umbral de bloques de la cuenta:** Establece establece el número de intentos fallidos para bloquear el acceso a una cuenta.

✓ Recomendaciones:



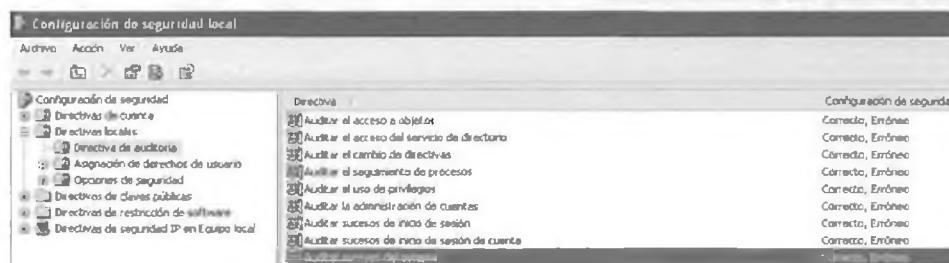
Se recomienda configurar la política de contraseñas para que la longitud mínima sea de 14 caracteres, tenga las características de complejidad requeridas y haya que modificarlas cada mes. En caso de más de 3 intentos fallidos bloquear la cuenta 15 minutos, para evitar ataques de fuerza bruta.



Se debe comprobar la nueva política de contraseñas creada y renovar las contraseñas creadas con anterioridad. En caso de no cumplir con los requisitos impuestos, a los usuarios se les mostrará el siguiente mensaje.



Para controlar por parte del administrador los accesos al sistema podemos habilitar en *Directivas locales* / *Directiva de auditoría* / *Auditar sucesos de inicio de sesión*, tanto correctos como erróneos. El **visor de sucesos** en panel *Panel de control / herramientas administrativas* nos permitirá analizarlos.



GNU/Linux

El control sobre complejidad y cifrado en contraseñas se realiza en GNU/Linux mediante el servicio **PAM** (*Pluggable Authentication Module*). Mediante PAM podemos comunicar a nuestras aplicaciones con los métodos de autenticación que deseemos de una forma transparente, lo que permite integrar las utilidades de un sistema Unix clásico (*login*, *ftpFTP*, *telnet*...) con esquemas diferentes del habitual *password*: claves de un solo uso, biométricos, tarjetas inteligentes...

El módulo **pam_cracklib** está hecho específicamente para determinar si es suficientemente fuerte una contraseña que se va a crear o modificar con el comando *passwd*.

Para instalarlo ejecutaremos: `sudo apt-get install libpam-cracklib`.

Uno de los comandos de asignación de contraseñas a usuarios en el acceso a sistemas GNU/Linux suele ser *passwd*, y su archivo de configuración asociado es */etc/pam.d/passwd*. A su vez éste suele referenciar a */etc/pam.d/common-password*.

En dicho archivo podremos indicarle las características de los módulos a emplear, en el ejemplo *pam_cracklib.so* (instalado para el control de la complejidad en contraseñas de usuario) y *pam_unix.so* (preinstalado y el más empleado por defecto). Mostramos a modo de ejemplo 2 líneas de configuración convencionales:

```
password required pam_cracklib.so dcredit=-1 ucredit=-1 lcredit=-1 minlen=8  
password required pam_unix.so use_authtok nullok md5
```

- La primera linea incluye el módulo de verificación cracklib, e indica que la longitud mínima sea 8 (minlen), y que debe contener digitos (dcredit), mayúsculas (ucredit) y minúsculas (lcredit).
- En la segunda indicamos que los archivos que contienen las contraseñas posean encriptación MD5. En versiones actuales de distribuciones GNU/Linux se incluyen algoritmos de cifrado más seguros como SHA.

Cuando empleemos de nuevo el comando *passwd* para renovación de contraseñas de un usuario, dicho comando verificará que se cumplen las reglas descritas en el archivo de configuración *common-password*.

Para visualizar los accesos al sistema y otros sucesos del sistema o **logs**, estos se guardan en archivos ubicados en el directorio */var/log*, aunque muchos programas manejan sus propios logs y los guardan en */var/log/<programa>*. Con respecto al acceso e identificación de usuarios encontramos:

- **/var/log/auth.log**: se registran los *login* en el sistema. Los intentos fallidos se registran en líneas con información del tipo *invalid password* o *authentication failure*.

A continuación realizaremos un análisis en profundidad a distintos niveles, de los mecanismos de control de acceso a los sistemas mediante contraseña:

- ✓ **1º nivel**: control con contraseña del arranque y de su propia configuración proporcionado por la BIOS.
- ✓ **2º nivel**: control mediante contraseña del arranque y de la edición de las opciones proporcionadas por los gestores de arranque.
- ✓ **3º nivel**: control mediante usuario y contraseña por parte de los sistemas operativos. El sistema operativo permite el control de acceso a datos y aplicaciones mediante la configuración de privilegios a los distintos perfiles de usuario o individualmente a estos.
- ✓ **4º nivel**: contraseña y cifrado de acceso a datos y aplicaciones, entre otros los archivos ofimáticos, comprimidos, sitios web (*mail*, banca *online*), etc.

PRÁCTICA 3.2

PELIGROS DE DISTRIBUCIONES LIVE!

Son innumerables los sistemas operativos arrancables desde unidades extraíbles USB, CD o DVD en modo Live sin necesidad de formatear e instalarlos en disco duro. Incluyen gran cantidad de aplicaciones de recuperación de datos y contraseñas de usuario.

Desde las opciones de SETUP o configuración de la BIOS, podemos hacer que arranque en primer lugar desde cualquiera de las mencionadas unidades.

Vulnerabilidades

A modo de ejemplo mencionaremos algunas distribuciones arrancables en modo Live:

- **Ultimate Boot CD (UBCD)**: posee en un entorno simulado Windows aplicaciones como antivirus, recuperación de datos, aplicaciones de recuperación y borrado de contraseñas de la BIOS (cmos_pwd), borrado y restitución de nuevas contraseñas de usuarios de sistemas Windows instalados en disco, incluso creación de nuevas cuentas de usuario administrador.
- **Backtrack**: distribución específica con un conjunto de herramientas de auditorías de seguridad, entre otras algunas que permiten escalada de privilegios en sistemas Windows (ophcrack) y GNU/Linux (John the ripper).
- **Ophcrack**: distribución específica que contiene la aplicación de mismo nombre con capacidad de extraer contraseñas de usuarios en sistemas Windows. Veremos más adelante un ejemplo de aplicación.
- **Slax**: distribución basada en *Slackware*, muy ligera y arrancable desde USB. Permite el montaje y acceso a los sistemas de ficheros instalados en disco.
- **Wifiway** y **Wifislax**: distribuciones orientadas a realizar auditorias *wireless*, como recuperación de contraseñas.

En la mayoría de las ocasiones desde estas distribuciones es posible acceder a las particiones y sistemas de ficheros de forma transparente, es decir, sin restricciones del sistema operativo, por lo que puede comprometer la seguridad de los datos y ficheros.

Comprobación

A modo de ejemplo podemos comprobar después de arrancar con un DVD Live de **Backtrack** el listado de particiones disponibles en el disco duro mediante el comando ejecutado como *root*: `fdisk -l`.

Tras analizar las particiones disponibles, montaremos por ejemplo en una carpeta creada por ejemplo `/mnt/win`, la partición de formato NTFS de Windows `/dev/sda2`, con el comando: `mount -t ntfs /dev/sda2 /mnt/win`.

La opción `-t` nos permite indicar el formato de la partición. De esta forma podemos acceder a través de la carpeta `/mnt/win` a todos los ficheros de dicha partición.

```

root@bt: /mnt - Shell - Konsole
Session Edit View Bookmarks Settings Help
Unable to open /l
root@bt: ~# fdisk -l

Disk /dev/sda: 58.5 GB, 58508410640 bytes
255 heads, 63 sectors/track, 7113 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xcfce28d

Device Boot Start End Blocks Id System
/dev/sda1 1 10 80253+ de Dell Utility
/dev/sda2 * 11 5002 40588190 7 HFS/NTFS
/dev/sda3 5004 7112 16458592+ f W3 Ext'd (LBA)
/dev/sda5 5004 7112 16458581 7 HFS/NTFS

root@bt: ~# ls
install.sh
root@bt: ~# cd ...
root@bt: ~# perl
root@bt: ~# cd ext/
root@bt: ~# ls
root@bt: ~# mkdir nn
root@bt: ~# mount -t ntfs /dev/sda2 /mnt/win
root@bt: ~#

```

Recomendación

Configurar el arranque para que siempre se realice en primer lugar desde el disco duro donde estén instalados los sistemas operativos y configurar con contraseña el *setup* de la BIOS para evitar modificaciones no autorizadas en la secuencia de arranque.

3.2.2 CONTROL DE ACCESO EN LA BIOS Y GESTOR DE ARRANQUE

BIOS (Basic Input/Output System): es el nivel más bajo de software que configura o manipula el hardware de un ordenador de manera que cada vez que iniciamos el ordenador este se encarga de reconocer todo el hardware que contiene el ordenador y controlar el estado de los mismos.

En la BIOS podemos configurar cualquier parámetro referente al hardware, de qué dispositivo arrancará en primer lugar o parámetros más comprometidos como el voltaje que se le suministra al núcleo del microprocesador.

Por este motivo tendremos que proteger nuestra BIOS de manera que solo un Administrador o un usuario responsable puedan cambiar los valores de la configuración.

Según la versión y la marca de la BIOS podemos configurar la seguridad del mismo de distintas formas. Estableceremos una clasificación sobre los niveles de seguridad que suele tener:

- **Seguridad del sistema (system)**: en cada arranque de la máquina nos pedirá que introduzcamos una contraseña que previamente se ha configurado en el BIOS. En caso de no introducirla o introducirla incorrectamente, el sistema no arrancará.
- **Seguridad de configuración de la BIOS (setup)**: en este apartado se suelen distinguir dos roles aplicables: Usuario (solo lectura) y Administrador (lectura/modificaciones).

PRÁCTICA 3.3



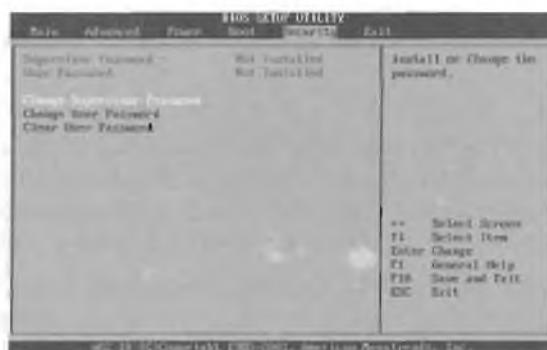
CONFIGURANDO CONTRASEÑA EN LA BIOS

En toda la explicación de esta actividad nos basaremos en una BIOS concreta del fabricante AMI, por lo que es recomendable reconocer qué tipo de BIOS estamos manejando (Award, Phoenix, etc.) y consultar la web del fabricante de la placa base para obtener el manual que contiene los pasos detallados para la configuración de la seguridad.

Proceso de asignación de contraseñas

Entraremos en el *setup* de nuestra BIOS (normalmente pulsando en el principio del arranque, tras pulsar el botón de encendido la tecla Supr o F12) y nos dirigiremos a la sección "security" para poder configurar las contraseñas. En esta sección nos encontraremos con una serie de opciones para cambiar o borrar las contraseñas. Estas son:

- ✓ *Change supervisor password*: crear, cambia o elimina la contraseña del Administrador.
- ✓ *Change user password*: crear o cambiar la contraseña del usuario.
- ✓ *Clear user password*: elimina la contraseña del usuario.



Seleccionaremos "change supervisor password" para crear la nueva contraseña del Administrador, introduciremos la contraseña dos veces y pulsaremos en "OK". Tras definir la contraseña del administrador, la vista de la sección "security" cambia. Ahora nos encontraremos con más opciones que las que se mostraban por defecto en esta sección, como:

- **User access level:** define el nivel de acceso que tendrá el usuario. Estos niveles pueden variar entre:
 - *No access* (sin acceso), *View only* (solo lectura), *Limited* (modificar con limitaciones) y *Full Access* (todos los permisos).
- **Password Check:** este parámetro permite configurar cuando queremos que la BIOS pida la contraseña tanto al Administrador como al usuario normal. La opciones son:
 - *Setup*: la contraseña se pedirá en el inicio del asistente de configuración de la BIOS.
 - *Always*: la petición de la contraseña se realizará en cada arranque de la máquina.

Ahora cambiaremos las opciones del usuario normal ya que por defecto tiene pleno acceso a la BIOS. En nuestro caso los configuraremos para que solo pueda visualizar la BIOS. Para ello, seleccionaremos "User Access Level" y marcaremos la opción "View Only". Por último, configuraremos para que siempre que se inicie la máquina nos pida la contraseña, mediante la opción "Password Check" lo podremos configurar seleccionando el parámetro "always":



Con esto ya tenemos configurada la seguridad de nuestra BIOS para evitar accesos no deseados a la BIOS y al arranque del sistema. Una vez configurada la seguridad de los usuarios, podemos reiniciar nuestra máquina para verificar que nos pedirá la contraseña en el arranque de la BIOS:

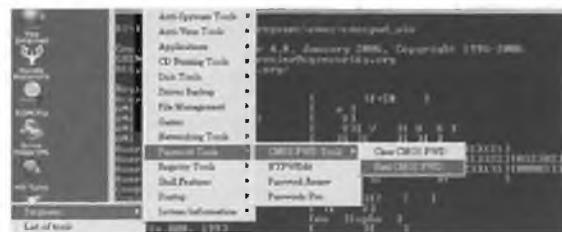


Introduciremos la contraseña y podremos inicializar nuestra máquina sin problemas.

Recomendaciones

Cabe destacar que la seguridad de la BIOS es muy vulnerable ya que existen varias formas para resetear la BIOS, y volver a sus valores de fábrica y por tanto que las contraseñas desaparezcan. Una de ellas es quitando la pila de la placa base, o a través de la conexión del *jumper CLR_CMOS* que suelen traer junto a la pila. A veces con un simple candado que asegure la apertura de la torre y no permita el acceso a la placa base es suficiente.

Otra forma para resetearla es con una distribución Live como Ultimate Boot CD for Windows, o con el PC arrancado bajo Windows, ejecutar una aplicación como *cmos_pwd*, que encuentran y borran las contraseñas.



Es importante cuidar la fortaleza de la contraseña de la BIOS a ser posible que sea de la mayor longitud posible (suele ser dependiendo del modelo entre 6 y 10 caracteres), y que contenga mayúsculas, minúsculas y números para hacer más difícil la obtención de la contraseña por personas no deseadas.

Del mismo modo es recomendable que el administrador no publique, ni escriba de forma visible su contraseña y la renueve periódicamente.

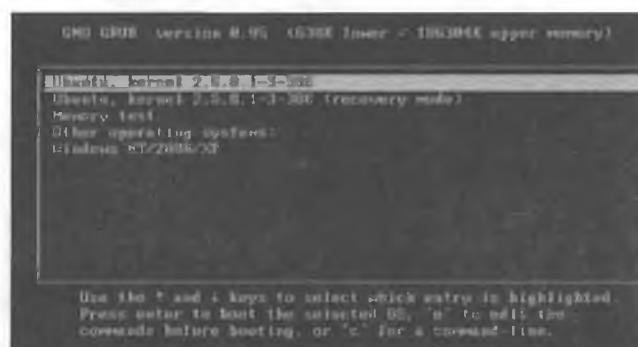
PRÁCTICA 3.4

CONTRASEÑA EN EL GESTOR DE ARRANQUE

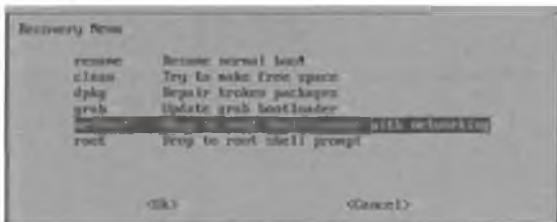
Cuando tenemos instalado varios sistemas operativos en disco duro, para seleccionar con qué sistema arrancaremos se emplea un gestor de arranque. Unos de los más populares y empleados con sistemas operativos GNU/Linux es GRUB.

Amenaza o vulnerabilidad

Después de realizar la BIOS las comprobaciones de hardware y dar paso al arranque de los dispositivos configurados (Boot Sequence), es posible visualizar el menú de arranque de GRUB pulsando la tecla ESC, siempre que lo tengamos instalado (por defecto en distribuciones como Ubuntu) y no se muestre.



La opción de recovery mode bajo sistemas GNU/Linux tiene un propósito de recuperación en caso de fallo del sistema, pero puede ser utilizada entre otras acciones para recuperar y modificar contraseñas de administrador (*root*) o incluso acceder a información del disco duro.



Vemos dentro del menú de recuperación como es posible acceder a una consola con privilegios de *root*. Permitiría ejecutar comandos de cambios de contraseña sin conocer la anterior como: *passwd root*.

Otra opción si tuviéramos restringida la opción de recuperación, sería editando alguna de las entradas del menú, pulsando la tecla *e*, y en la línea kernel modificar el final de la misma sustituir el texto desde "ro" incluido, por *init=/bin/bash*. Si arrancamos después de la edición, desde esta opción este cambio ejecutará en el arranque una shell con permisos de *root*, teniendo control total sobre el sistema.

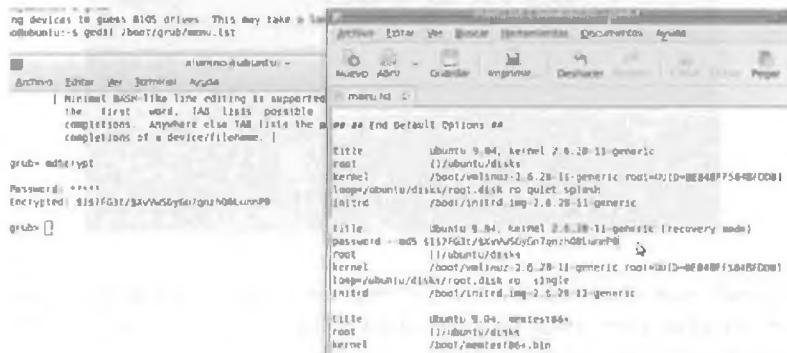
Proceso de asignación de contraseña a GRUB

Como recomendación se propone:

- Añadir contraseña encriptada al menú de edición es decir imposibilitar la edición por cualquier usuario no autorizado.



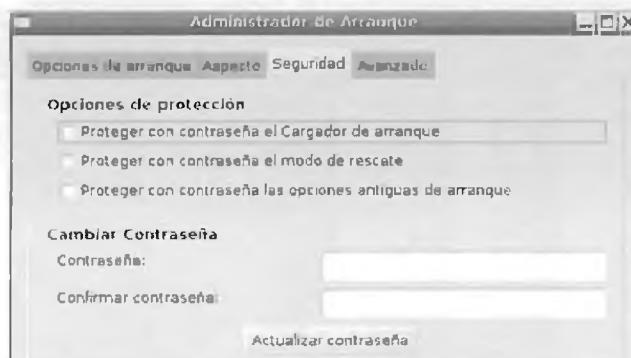
- Añadir encriptada contraseña en modo de recuperación.



- 1º Mediante el comando `grub`, nos abrirá una consola que nos permitirá encriptar en codificación MD5 cualquier texto que deseemos como contraseña, mediante el comando `md5crypt`. Copiamos el texto de salida en MD5, comenzará por \$1\$.
- 2º Editamos el archivo `menu.lst` de `grub`, habitualmente localizado en `/boot/grub/`. Tras la línea comentada `password - -md5 1`, escribiremos una línea con nuestra contraseña encriptada. Esto no permitirá la edición de ninguna de las entradas del menú, si no conocemos la contraseña.
- 3º En el archivo `menu.lst` buscaremos las líneas que hagan mención a (recovery mode) y después de la línea `title` añadiremos una línea de `password`. Esto no permitirá arrancar en modo recuperación a menos que conoczamos la contraseña. Podriamos añadirle contraseña a las opciones que queramos de este modo.

Es también posible realizar dichas modificaciones mediante la aplicación gráfica **Start Up Manager**. Su instalación: `sudo aptitude install startupmanager`.

Una vez instalado, podemos acceder a la aplicación en Sistema -> Administración -> Administrador de Arranque o con el comando `startupmanager` con permisos de `root`.



3.2.3 CONTROL DE ACCESO EN EL SISTEMA OPERATIVO

Existen métodos de acceso al sistema operativo muy seguros como por ejemplo mediante huella dactilar, pero el más utilizado sigue siendo a través de una contraseña asociada a una cuenta de usuario.

Como hemos visto anteriormente existen métodos para poder acceder a los sistemas operativos sin control de contraseña, en el caso de GNU/Linux mediante el modo de recuperación. En el caso de Windows para versiones como XP mediante el modo prueba de fallos o pulsando 2 veces en la ventana de inicio de usuarios `Ctrl + Alt + Supr` e intentando acceder a la cuenta del usuario Administrador sin contraseña, ya que en la instalación no se le asigna ninguna, por tanto por defecto suele estar vacía.

Pero existen otros métodos, normalmente asociados a poder arrancar con una distribución Live para poder recuperar o conocer las contraseñas de cualquier usuario, así como borrarlas o modificarlas.

Como recomendación, estas herramientas empleadas nos servirán para auditar nuestros sistemas de credenciales de acceso a sistemas operativos y ver el nivel de fortaleza de las mismas, ya que dependiendo del nivel de nuestras contraseñas no siempre será posible recuperarlas.

PRÁCTICA 3.5



RECUPERACIÓN DE CONTRASEÑAS

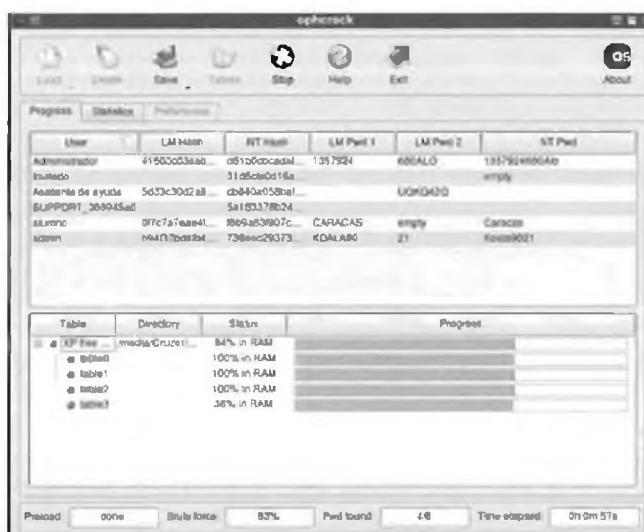
Windows

Ophcrack es una aplicación que permite recuperar contraseñas de Windows. También se encuentra disponible en distribuciones como Backtrack, o incluso posee su propia distribución Live. Se basa en el conocimiento de cómo almacena Windows sus contraseñas de usuario (normalmente en *windows/system32/config/SAM* sólo solo accesible sin arrancar el sistema operativo, por ejemplo desde una distribución Live), y emplea una comprobación mediante fuerza bruta y diccionarios que habrá que cargar dependiendo de la versión y el idioma deseado.



Como vemos en la figura debemos indicarle en primer lugar la ruta del directorio donde se almacenan las contraseñas, normalmente *Windows/system32/config*. Previamente habremos montado la partición correspondiente.

Por otro lado, mediante el botón **Tables**, indicaremos la ruta donde podrá encontrar la tabla de diccionario con el qué queremos probar, en este caso, hemos cargado *XP_free_fast*. Una vez cargadas las tablas de diccionario, ejecutaremos el comienzo de pruebas, y como vemos para los usuarios de la partición de Windows seleccionada ha encontrado para los usuarios: Administrador – 1357924680Alo, alumno – Caracas, y para admin. – Koala9021. Vemos que incluso para contraseñas de cierta longitud y con caracteres numéricos, mayúsculas y minúsculas ha sido capaz de recuperar las contraseñas (columna NT Pwd).



Recomendación: Ophcrack encuentra grandes dificultades con contraseñas creadas con palabras separadas por espacios y caracteres especiales, por lo que se recomienda su uso.

GNU/Linux

En los sistemas GNU/Linux el archivo que controla usuarios y sus contraseñas encriptadas es `/etc/shadow` visible tan solo por el usuario `root`, aunque en caso de poder acceder a una partición GNU/Linux y a su sistema de ficheros, tenemos el fichero visible.

La estructura del mismo es un listado con una línea por cada usuario en la que la segunda columna separada por `:` es la contraseña encriptada según algún algoritmo de cifrado, habitualmente MD5 si comienza por `1`, o SHA si comienza por `6`, opción más segura e incluida por defecto en las versiones de distribuciones actuales.

```
chipcard:**:14657:0:99999:7::1
saned:**:14657:0:99999:7::1
pulse:**:14657:0:99999:7::1
messagebus:**:14657:0:99999:7::1
polkituser:**:14657:0:99999:7::1
avahi:**:14657:0:99999:7::1
haldaemon:**:14657:0:99999:7::1
usuario:$6$ZBxMuuzDG50/83$L5zDTWxRSXZhpk9KvNeX4FrZV9othJyCEpzLR7FLArZYgntJAdY2byBSkGHcd2o
XJacukdzH317P2VCArv1:14938:0:99999:7::1
ejabberd:**:14882:0:99999:7::1
root:**:
```

Arrancando desde una distribución Backtrack accedemos al contenido del archivo `/etc/shadow` de una partición GNU/Linux instalada en disco duro y previamente montada. Vemos que el usuario de `login` posee su contraseña encriptada con SHA.

Mediante la aplicación John the Ripper, podemos efectuar distintos tipos de ataques contra este archivo (deberemos indicarle la ruta del `archivo_shadow`) para descubrir contraseñas encriptadas, por ejemplo:

```
john - -single archivo_shadow
```

Permite realizar una búsqueda con combinaciones simples, mediante palabras habituales, incluido el nombre de usuario.

```
john - - wordlist=password.lst archivo_shadow
```

Realiza una búsqueda empleando como diccionario el archivo:

```
john - - incremental=all archivo_shadow
```

Realiza un ataque de fuerza bruta probando con combinaciones de números, caracteres en mayúsculas, minúsculas, etc.



En la figura se muestra la obtención de la contraseña del usuario "usuario" y contraseña "usuario".

PRÁCTICA 3.6



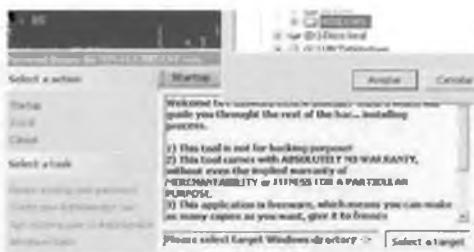
MODIFICACIÓN DE CONTRASEÑAS

En caso de olvidar la contraseña o querer modificarla sin conocerla, podemos recurrir a herramientas en modo Live que permiten resetearlas o cambiarlas sin autorización de administrador.

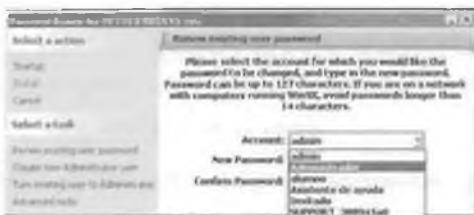
Windows

Existen diferentes opciones sólo nos centraremos en algunas de las más sencillas, todas ellas requieren de la posibilidad de arranque desde una distribución Live:

1. Mediante la distribución UBCD podemos ejecutar la aplicación *Password Renew*. Le indicaremos en qué directorio se encuentra la carpeta de sistema:



A continuación nos mostrará el listado de usuarios disponibles, pudiendo realizar acciones como renovar una contraseña (sin conocer la anterior), crear un usuario administrador, o modificar el tipo de cuenta de un usuario, por ejemplo, limitado a administrador.



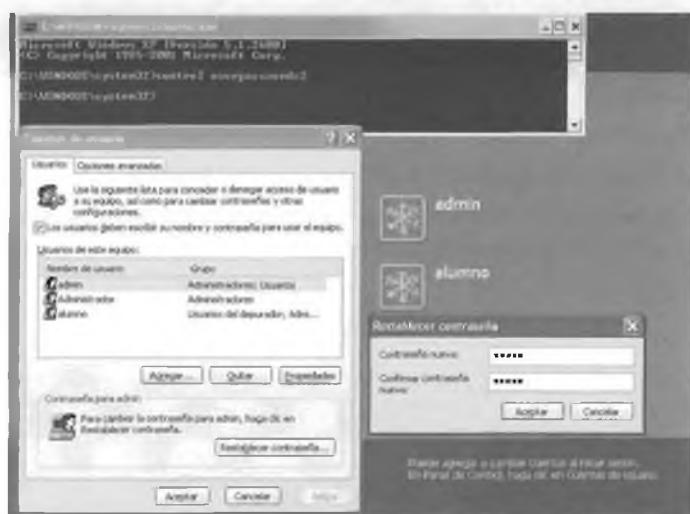
2. Otra vulnerabilidad que presentan los sistemas Windows es a través de herramientas que pueden verse modificadas o sustituidas por una consola de comandos (*cmd.exe* con privilegios de administrador). Por ejemplo la utilidad **StickyKeys** software de ayuda y accesibilidad, que se activa pulsando la tecla SHIFT 5 veces seguidas.

El fichero que ejecuta es *sethc.exe* ubicado en *C:\WINDOWS\SYSTEM32*. La vulnerabilidad consiste en sustituir *sethc.exe* por *cmd.exe* (consola de comandos) y así cuando pulsemos la tecla SHIFT 5 veces seguidas se nos abrirá la shell de comandos, desde la cual podemos hacer ejecutar los comandos que queramos sobre el equipo.

Vemos los comandos para sustituir el ejecutable *sethc.exe* por *cmd.exe*, desde una distribución Live con la partición de Windows montada.

```
a!utmo@ubuntu:/mnt/win/Windows/system32$ ls -l cmd.exe
a!utmo@ubuntu:~$ root 482944 2804-08-19 15:42 cmd.exe
a!utmo@ubuntu:/mnt/win/Windows/system32$ ls -l sethc.exe
a!utmo@ubuntu:~$ root 3258 2804-08-19 15:43 sethc.exe
a!utmo@ubuntu:/mnt/win/Windows/system32$ cp sethc.exe sethc.old.exe
a!utmo@ubuntu:/mnt/win/Windows/system32$ cp cmd.exe sethc.exe
a!utmo@ubuntu:/mnt/win/Windows/system32$
```

En la página de inicio de sesión pulsamos 5 veces la tecla shift y nos ejecutará la consola de comando. Podremos ejecutar todo tipo de comandos, como por ejemplo **control userpasswords2** que nos abrirá la utilidad de configuración de contraseñas de usuarios, pudiendo renovarlas sin conocerlas previamente.



GNU/Linux

En el caso de GNU/Linux, si podemos acceder al sistema de ficheros y modificamos en */etc/shadow* para cualquier usuario, su contraseña actual por una contraseña encriptada que conoczamos, podremos acceder con la nueva contraseña. Debemos de tener en cuenta 2 consideraciones:

- ✓ Analizar qué sistema de encriptación emplea el sistema de verificación de GNU/Linux, podemos analizar el archivo **/etc/pam.d/common-password**, y la línea correspondiente al módulo *pam_unix.so*, al final de la misma suele indicar el algoritmo de cifrado empleado en */etc/shadow*. Por ejemplo: *password required pam_unix.so use_authtok nullok sha-512*
- ✓ Tener un conjunto de contraseñas cifradas conocidas, o emplear una herramienta de cifrado MD5 o SHA de texto plano para obtener el texto cifrado correspondiente. Por ejemplo en la web <http://www.hashgenerator.de/> podremos cifrar texto plano mediante diferentes algoritmos.

3.3 POLÍTICA DE USUARIOS Y GRUPOS

La definición de cuentas de usuario y su asignación a perfiles determinados, grupos o roles, así como la asignación de privilegios sobre los objetos del sistema es uno de los aspectos fundamentales de la seguridad, y una de las tareas fundamentales del administrador de sistemas. Este proceso lleva generalmente cuatro pasos:

- **Definición de puestos:** separación de funciones posibles y el otorgamiento de los mínimos permisos de acceso requeridos por cada puesto para la ejecución de las tareas asignadas.
- **Determinación de la sensibilidad del puesto:** determinar si una función requiere permisos críticos que le permitan alterar procesos, visualizar información confidencial, etc.
- **Elección de la persona para cada puesto:** requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto.
- **Formación inicial y continua de los usuarios:** deben conocer las pautas organizacionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él. Debe estar orientada a incrementar la **conciencia** de la necesidad de proteger los recursos informáticos.

La **definición de los permisos de acceso** requiere determinar cuál será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible **clasificar la información**, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados. Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación es conveniente comenzar definiendo las medidas de seguridad sobre la **información más sensible o las aplicaciones más críticas**, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones. Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

PRÁCTICA 3.7



CONTROL DE ACCESO A DATOS Y APLICACIONES

Tanto en sistemas personales como en sistemas en red controlados por servicios de directorio como LDAP o Active Directory bajo Windows Server, el control sobre la seguridad de los objetos del sistema (archivos, carpetas, procesos, recursos de red, recursos hardware, etc.) se realiza mediante el control y asignación de permisos.

Sobre el sistema de archivos es posible establecer listas de control de acceso (**ACL**) que de forma individual permite asignar permisos a un usuario, sin tener en cuenta el grupo al que pertenece.

Windows

En la siguiente actividad vamos a configurar algunos aspectos de seguridad y asignación de permisos a usuarios locales, en sistemas Windows. Para modificar la configuración de seguridad local iremos a *Panel de control / Herramientas administrativas / Directiva de seguridad local*. Podremos modificar **Directiva de auditoría**, **Asignación de derechos de usuario** u **Opciones de seguridad**, en el árbol de la consola haz clic en **Directivas locales**, estas directivas se aplican a un equipo y contienen tres subconjuntos:

- **Directiva de auditoría:** Determina si los sucesos de seguridad se registran en el registro de seguridad del equipo. El registro de seguridad forma parte del Visor de sucesos.
- **Asignación de derechos de usuario:** Determina qué usuarios o grupos tienen derechos de inicio de sesión o privilegios en el equipo, entre otros:
 - Ajustar cuotas de memoria para un proceso, permitir el inicio de sesión local, hacer copias de seguridad y restaurar archivos y directorios, generar auditorías de seguridad, o tomar posesión de archivos y otros objetos.
- **Opciones de seguridad:** Habilita o deshabilita la configuración de seguridad del equipo, como la firma digital de datos, nombres de las cuentas Administrador e Invitado, acceso a CD-ROM y unidades de disco, instalación de controladores y solicitudes de inicio de sesión.

Pero para tener un mayor control sobre la configuración del nivel de acceso por parte de cada usuario a cada recurso del sistema, como por ejemplo una carpeta, es necesario realizar la configuración de ACL. En Windows es posible realizarla mediante el comando **cacls**.

Como sabemos en un sistema local las carpetas de usuario no son accesibles por otros usuarios del sistema. En caso de querer un usuario1 dar acceso de lectura, solo a un usuario2 a su carpeta *MisDocumentos/Musica*, podemos ejecutar con el usuario1 en la consola de comandos:

```
cacls "Mis Documentos\Musica" /t /e /g Usuario2:R
```

Las opciones principales son:

- ✓ /t: modifica las ACL de los archivos especificados en el directorio actual y subdirectorios.
- ✓ /e: modifica en vez de reemplazar la ACL.
- ✓ /g usuario: permisos R(lectura), E(escritura), C(cambiar), F(control total). Permite asignarlos (grant).
- ✓ /p: permite reemplazar los existentes o quitárselo todos con :N.

GNU/Linux

Para brindar privacidad y protección, cada archivo o directorio tiene asociados permisos diferentes para el dueño, para el grupo y para los demás usuarios. En el caso de archivos, los permisos que pueden darse o quitarse son: (r) lectura, (w) escritura y (x) ejecución. En el caso de directorios, los permisos son: (r) para listar los archivos, (w) para escribir, crear o borrar archivos y (x) para acceder a archivos del directorio.

Los permisos de un archivo pueden ser modificados por el dueño, propietario o por el administrador del sistema con el comando **chmod** que espera dos parámetros: cambio por realizar al permiso y nombre del archivo por cambiar. Los permisos se pueden especificar en octal o con una o más letras para identificar al usuario (u para el usuario, g para el grupo, o el resto de usuarios y a para todos), un +, un - o un = y después letras para identificar los permisos (r, w o x). Por ejemplo:

```
chmod og+x sube.sh
```

Añade (+) al resto de usuarios (o) y al grupo al que pertenece el archivo (g), permiso de ejecución del archivo (x) *sube.sh*, que debe estar en el directorio desde el cual se da el comando.

El dueño de un archivo puede ser modificado solo por el administrador del sistema con el programa **chown**. Un usuario que pertenezca a varios grupos puede cambiar el grupo de uno de sus archivos a alguno de los grupos a los que pertenezca con el programa o comando **chgrp**, por ejemplo:

```
chgrp estudiantes tarea1.txt
```

Cambiará el grupo del archivo tarea1.txt a estudiantes. Los grupos a los cuales un usuario pertenece son mostrados por el comando groups.

En caso de querer emplear listas de control de acceso y poder permitir o denegar permisos a usuarios concretos, emplearemos los comandos:

- **getfacl**: permite ver la información de permisos sobre un archivo.
- **setfacl**: permite asignar permisos sobre un archivo.

En primer lugar observaremos si la partición del sistema de archivos posee entre sus opciones la de control mediante ACL, leyendo el archivo /etc/fstab, y viendo la línea correspondiente, si posee entre las características u opciones de montaje la opción acl. Por ejemplo:

```
/dev/sda2  /mnt/Linux auto  rw,user,auto,exec,acl  0  0
```

En caso de no disponer de dicha opción podemos montarla de nuevo con la opción:

```
mount -o remount,acl /dev/sda2.
```

Por ejemplo para añadir el permiso de que un usuario2 pueda leer y escribir(rw) sobre un archivo, y verificar que se han asignado los permisos, podremos ejecutar la sentencia:

```
setfacl -m user:usuario2:rw- archivo  
getfacl archivo
```

3.4 REFERENCIAS WEB

- Sitio web sobre seguridad informática de Microsoft:
<http://www.microsoft.com/spain/protect/>
- Manual de administración segura de GNU/Linux:
<http://es.tldp.org/Manuales-LuCAS/GSAL/gsal-19991128.pdf>
- Seguridad en GNU/Linux:
<http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGLIN00.html>
- Administración de aspectos de seguridad en GNU/Linux y Windows:
<http://www.adminso.es/wiki/index.php/>
- Cómo de fuerte es tu contraseña:
<http://howsecureismypassword.net/>
- Comprobador de contraseñas de Microsoft:
<http://www.microsoft.com/latam/protect/yourself/password/checker.mspx>
- Administración de usuarios en GNU/Linux:
http://www.linuxtotal.com.mx/index.php?cont=info_admon_008



RESUMEN DEL CAPÍTULO

La **seguridad lógica** consiste en la *aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo*.

Para ello se emplean técnicas como el control de acceso lógico mediante contraseña a distintos niveles:

- En el arranque y configuración de la BIOS, y gestores de arranque.
- En el sistema operativo, datos y aplicaciones.

Una contraseña segura debe parecerle a un atacante una cadena aleatoria de caracteres, para ello se recomienda que sea lo más **larga y compleja** (combinación de letras mayúsculas y minúsculas, números y símbolos).

Los administradores de sistemas deben auditárlas comprobando la fortaleza de las mismas, y configurar las opciones para asegurar que los usuarios tengan **contraseñas fuertes y se cambien regularmente**.

Los sistemas operativos son capaces de gestionar usuarios y sus privilegios o procedimientos autorizados, sobre las aplicaciones y archivos. El principio de la política de privilegios debe ser *todo lo que no está permitido debe estar prohibido*.

Para asegurar este principio se recomienda que el uso habitual de sistema se realice con cuentas de usuario con privilegios limitados y tan solo en los momentos en los que sea necesario, como por ejemplo en una instalación de una aplicación o *driver*, se adoptarán privilegios de administrador.



EJERCICIOS PROPUESTOS

■ 1. Lee el artículo sobre “Recomendaciones para la creación y uso de contraseñas seguras” de Inteco, disponible en la siguiente página web http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/recomendaciones_creacion_uso_contrasenias y contesta a las siguientes cuestiones:

■ ¿Qué porcentaje de usuarios emplea contraseñas para el acceso a sus sistemas de archivos? ¿Qué porcentaje de usuarios en EEUU apunta su contraseña en papel o archivo electrónico en el PC? ¿Qué porcentaje de usuarios emplea la misma contraseña en distintos servicios?

■ 2. En caso de tener acceso al archivo `/etc/shadow` de un equipo local, y conteniendo éste las siguientes líneas:

```
alumno1:$1$zmDCo$pP/
Rrln2jTy3OeTvjL8Mg0:14544:0:99999:7:::
```

```
root:$1$bM36INXG$nlckzvSVJy.z42A-
tf5p6n.:11585:0:99999:7:::
```

■ ¿Qué contraseña poseen los usuarios: `root` y `alumno1`? ¿En qué tiempo has sido capaz de descifrar las contraseñas? ¿Qué algoritmo de cifrado poseen sus contraseñas? ¿Qué significado poseen cada uno de los campos que componen cada línea del archivo?

■ 3. Lee el siguiente artículo sobre el uso de cuentas limitadas y administrador en sistemas Windows:

http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/cuenta_administrador_vs_limitada

■ ¿Qué perfiles tipo y limitaciones de uso existen en las cuentas de usuario en sistemas Windows? ¿Con qué tipo de cuenta utilizarías normalmente el sistema? ¿Qué tipo de limitaciones tendrías? ¿Para qué sirve el comando `runas`?

■ 4. Desde un usuario con rol administrador, agregar la posibilidad a la cuenta limitada creada anterior-

mente de cambiar la fecha/hora e instalar controladores de dispositivo y revocarle el privilegio de acceso al CD-ROM., Activar el archivo de sucesos o log de sucesos asociados a esos privilegios.

■ Acceder como usuario rol-limitado y verificar privilegios y limitaciones. Acceder como usuario rol-administrador y verificar el archivo de suceso o log.

■ ¿Los usuarios con cuenta limitada pueden acceder a la configuración de directivas locales? ¿Es lógico?

■ 5. Investiga sobre la finalidad y opciones uso de la aplicación **Windows SteadyState**. ¿Qué opciones de configuración segura facilita?

■ 6. Investiga sobre las opciones de configuración de contraseña y cifrado de acceso a archivos ofimáticos (doc, xls, odt, pdf, ppt, odp...), comprimidos (zip, rar,...), etc. ¿Es posible en caso de olvidar la contraseña recuperarlas? ¿En qué casos de los anteriormente descritos?

■ 7. Investiga sobre la finalidad y opciones de uso de la aplicación **Keepass Password Safe**. ¿Qué opciones de configuración segura facilita? ¿Es posible recordar las contraseñas de sitios web y acceder sin teclearlas?

■ 8. Explica las diferencias existentes en sistemas GNU/Linux entre el uso del comando `chmod` y `setacl`.

■ 9. A partir de qué versión del sistema operativo Windows se solicita para realizar tareas de administración como cambios en la configuración de red, instalación de drivers o aplicaciones, la contraseña de un usuario administrador ¿Por qué crees que es interesante dicha opción? ¿Se realiza dicha petición en sistemas GNU/Linux?

■ 10. ¿Qué utilidad tienen las aplicaciones “congelador” del sistema operativo como **DeepFreeze**? Busca alguna otra aplicación disponible para Windows y otra para GNU/Linux: ¿Es posible instalar aplicaciones y guardar datos teniendo activa este tipo de aplicación? ¿Qué protección ofrecen?



TEST DE CONOCIMIENTOS



1 ¿Qué tipo de cuenta se recomienda para un uso cotidiano en sistemas Windows?

- a) Administrador.
- b) Invitado.
- c) Limitada.
- d) Mínimos privilegios.

2 Una contraseña segura no debe tener:

- a) Más de 10 caracteres.
- b) El propio nombre de usuario contenido.
- c) Caracteres mayúsculas, minúsculas y símbolos.
- d) Frases fáciles de recordar por ti.

3 ¿Qué es la identificación?

- a) Momento en que el usuario se da a conocer en el sistema.
- b) Verificación que realiza el sistema sobre el intento de *login*.
- c) Un número de intentos de *login*.
- d) Un proceso de creación de contraseñas.

4 Para un usuario experimentado como tú, las actualizaciones deben ser:

- a) Automáticas, descargar e instalar actualizaciones automáticamente.
- b) Descargar actualizaciones y notificar si deseas instalarlas.
- c) Notificar, pero no descargar ni instalar.
- d) Desactivar actualizaciones automáticas.

5 Las contraseñas de sistemas GNU/Linux se encuentran encriptadas en el archivo:

- a) /etc/groups.
- b) /etc/passwd.
- c) /etc/shadow.
- d) /etc/sha-pass.

6 En caso de tener configurada con contraseña el SETUP de la BIOS, y querer prohibir el arranque en modo Live, el primer dispositivo de arranque debe ser:

- a) LAN.
- b) HD.
- c) USB.
- d) CD.

7 El comando john --wordlist=password.lst passwords, realiza un ataque:

- a) Diccionario.
- b) Fuerza bruta.
- c) Simple.
- d) PWstealer.

8 Activando la directiva local de seguridad en sistemas Windows “las contraseñas deben cumplir los requisitos de complejidad”, las contraseñas nuevas o renovadas no pueden tener:

- a) 5 caracteres.
- b) Números.
- c) Mayúsculas.
- d) Minúsculas.
- e) Caracteres especiales.

9 Una de las vulnerabilidades en la instalación de Windows XP es:

- a) Crea un conjunto de usuarios administrador.
- b) Crea un usuario Administrador con una contraseña débil.
- c) Crea un usuario Administrador sin contraseña.
- d) Crear 2 usuarios al menos sin contraseña.

10 Desde la utilidad de usuarios y password de Windows de Ultimate Boot Recovery no podemos:

- a) Resetear contraseñas.
- b) Recuperar contraseñas.
- c) Modificar contraseñas seguras.
- d) Dejar contraseñas en blanco.



4

Software antimalware

OBJETIVOS DEL CAPÍTULO

- ✓ Comprender qué es el software malicioso (*malware*) y sus posibles fuentes.
- ✓ Crear conciencia de análisis de riesgo y toma de precauciones en las operaciones informáticas.
- ✓ Identificar las nuevas posibilidades y riesgos que poseen Internet y las redes sociales.
- ✓ Analizar las distintas herramientas de seguridad software *antimalware* existentes.

4.1 SOFTWARE MALICIOSO

Gracias al desarrollo de las comunicaciones y al creciente uso de la informática en la mayoría de los ámbitos de la sociedad, los sistemas de información se han convertido en objetivo de todo tipo de ataques y son sin duda el principal **foco de amenazas**. Por esta razón es fundamental identificar qué recursos y elementos necesitan protección así como conocer los mecanismos o herramientas que podemos emplear para procurar su protección.

Con el nombre de **software malicioso** o **malware** agrupamos clásicamente a los virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para acceder a ordenadores **sin autorización**, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto.

En sus comienzos, la motivación principal para los creadores de virus era la del **reconocimiento público**. Cuanta más relevancia tuviera el virus, más reconocimiento obtenía su creador. Por este motivo, las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes, modificar los caracteres de escritura, formatear el disco duro, etc.

Sin embargo, la evolución de las tecnologías de la comunicación y su penetración en casi todos los aspectos de la vida diaria ha sido vista por los **ciberdelincuentes como un negocio muy lucrativo**. Los creadores de virus han pasado a tener una **motivación económica**, por lo que actualmente son grupos mucho más organizados que desarrollan los códigos maliciosos con la intención de que pasen lo más desapercibidos posible, y dispongan de más tiempo para desarrollar sus actividades maliciosas.

Hay varias formas en las que el creador del programa malicioso puede **obtener un beneficio económico**, las más comunes son:

- **Robar información sensible** del ordenador infectado, como datos personales, contraseñas, credenciales de acceso a diferentes entidades, *mail*, *banca online*, etc.
- Crear **una red de ordenadores infectados**, generalmente llamada *red zombi* o *botnet*, para que el atacante pueda manipularlos todos simultáneamente y vender estos servicios a entidades que puedan realizar acciones poco legítimas como el envío de *spam*, de mensajes de *phishing*, acceder a cuentas bancarias, realizar ataques de denegación de servicio, etc.
- Vender **falsas soluciones de seguridad** (*rogueware*) que no realizan las acciones que afirman hacer, por ejemplo, falsos antivirus que muestran mensajes con publicidad informando de que el ordenador está infectado cuando en realidad no es así, la infección que tiene el usuario es el falso antivirus.
- Cifrar el contenido de los ficheros del ordenador y solicitar un **rescate económico** al usuario del equipo para recuperar la información, como hacen los criptovirus.



NOTICIA DE ACTUALIDAD

Descubre alguno de los nuevos peligros de la red, como son las redes *botnet* leyendo y analizando la siguiente noticia:

<http://prensa.pandasecurity.com/2010/07/panda-security-y-defence-intelligence-ayudan-al-fbi-a-arrestar-a-cibercriminales-%E2%80%93-hacker-detenido-en-eslovenia/>

Comentar en el grupo de clase:

- ¿Cuál era la finalidad del ataque descrito?
- ¿Cuáles son los nuevos peligros derivados del uso de Internet, como las denominadas redes zombi? ¿Qué tipo de precauciones y revisiones realizarías en tu equipo para evitar formar parte de estas redes?
- ¿Crees qué Internet es una red segura? ¿Por qué?

4.2 CLASIFICACIÓN DEL MALWARE

Los distintos códigos maliciosos que existen pueden clasificarse en función de diferentes criterios, los más comunes son:

- **Virus:** de su analogía con los virus reales ya que infectan otros archivos, es decir, solo pueden existir en un equipo dentro de otro fichero, generalmente son ejecutables: .exe, .src, o en versiones antiguas .com, .bat. También pueden infectar otros archivos, por ejemplo un virus de macro infectará programas que utilicen macros, como los productos Office. Los virus infectan a un sistema cuando se ejecuta el fichero infectado.
- **Gusano:** característica principal es realizar el máximo número de copias posibles de sí mismos para facilitar su propagación. Se suelen propagar por los siguientes métodos: correo electrónico, archivos falsos descargados de redes de compartición de ficheros (P2P), mensajería instantánea, etc.
- **Troyano:** código malicioso con capacidad de crear una puerta trasera o *backdoor*, que permita la administración remota a un usuario no autorizado. Pueden llegar al sistema de diferentes formas, las más comunes son: descargado por otro programa malicioso, al visitar una página web maliciosa, dentro de otro programa que simula ser inofensivo, etc.

Debido a la gran cantidad y diversidad de códigos maliciosos que existen, que muchos de ellos realizan varias acciones y se pueden agrupar en varios apartados a la vez, existen varias **clasificaciones genéricas** que engloban varios tipos de códigos maliciosos son las siguientes:

- **Ladrones de información (infostealers)**: Agrupa todos los tipos de códigos maliciosos que roban información del equipo infectado, son los capturadores de pulsaciones de teclado (*keyloggers*), espías de hábitos de uso e información de usuario (*spyware*), y más específicos, los ladrones de contraseñas (*PWstealer*).
- **Código delictivo (crimeware)**: Hace referencia a todos los programas que realizan una acción delictiva en el equipo, básicamente con fines lucrativos. Engloba a los ladrones de información de contraseñas bancarias (*phishing*) que mediante mensajes de correo electrónico no deseado o *spam* con *clickers* redireccionan al usuario a falsas páginas bancarias. Dentro de este ámbito encontramos otro tipo de estafas electrónicas (*scam*) como la venta de falsas herramientas de seguridad (*rogueware*).
- **Greyware** (o *grayware*): Engloba todas las aplicaciones que realizan alguna acción que no es, al menos de forma directa, dañina, tan solo molesta o no deseable. Agrupa software de visualización de publicidad no deseada (*adware*), espías () que solo roban información de costumbres del usuario para realizar campañas publicitarias (páginas por las que navegan, tiempo que navegan por Internet...), bromas (*joke*) y bulos (*hoax*).

4.2.1 MÉTODOS DE INFECCIÓN

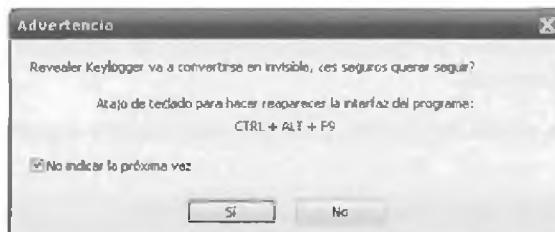
Pero, ¿cómo llega al ordenador el *malware* y cómo prevenirlos? Existen gran variedad de formas por las que todo tipo de *malware* puede llegar a un ordenador; en la mayoría de los casos prevenir la infección resulta relativamente fácil **conociéndolas**:

- **Explotando una vulnerabilidad**: cualquier sistema operativo o programa de un sistema puede tener una vulnerabilidad que puede ser aprovechada para tomar el control, ejecutar comandos no deseados o introducir programas maliciosos en el ordenador.
- **Ingeniería social**: apoyado en técnicas de abuso de confianza para apremiar al usuario a que realice determinada acción, que en realidad es fraudulenta o busca un beneficio económico.
- **Por un archivo malicioso**: esta es la forma que tienen gran cantidad de *malware* de llegar al equipo: archivos adjuntos a través de correo no deseado o *spam*, ejecución de aplicaciones web, archivos de descargas P2P, generadores de claves y *cracks* de software pirata, etc.
- **Dispositivos extraíbles**: muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que, mediante la ejecución automática que se realiza en la mayoría de los sistemas cuando el dispositivo se conecta a un ordenador, pueda ejecutarse e infectar el nuevo equipo, y a su vez, nuevos dispositivos que se conecten.
- **Cookies maliciosas**: las *cookies* son pequeños ficheros de texto que se crean en carpetas temporales del navegador al visitar páginas web; almacenan diversa información que, por lo general, facilitan la navegación del usuario. Las denominadas *cookies maliciosas* monitorizan y registran las actividades del usuario en Internet con fines maliciosos, por ejemplo capturar los datos de usuario y contraseña de acceso a determinadas páginas web o vender los hábitos de navegación a empresas de publicidad.

PRÁCTICA 4.1

KEYLOGGER

En la práctica que realizaremos a continuación instalaremos un software de recuperación de pulsaciones de teclado denominado **Revealer Keylogger** que se ejecuta al inicio y se encuentra oculto, pudiendo enviar remotamente por **FTP** o **mail**, el archivo que registra, en el que se encontrarán tras un período de tiempo credenciales de usuario por ejemplo de sitios web como correo, banca electrónica, o redes sociales.



En el equipo local que lo tenemos instalado si pulsamos **CTRL + Alt + F9** podemos ver el estado de registro, observando en qué momentos ha entrado en determinadas páginas web y qué ha tecleado.



En la secuencia vemos como después de teclear la URL www.yahoo.es ha escrito el texto: informatica (+Intro) y a continuación koala (+Intro), posibles nombre de usuario y contraseña respectivamente, de uno de los servicios de yahoo, como el correo electrónico.

Recomendación

La manera de prevenir estos ataques es realizar escaneos periódicos *antimalware* con una o varias herramientas fiables y actualizadas, controlar los accesos físicos y limitar los privilegios de las cuentas de usuario para evitar instalaciones no deseadas.

4.3 PROTECCIÓN Y DESINFECCIÓN

Aunque, como se ha visto, existen gran cantidad de códigos maliciosos, es muy fácil prevenir el quedarse infectado por la mayoría de ellos y así poder utilizar el ordenador de forma segura, basta con seguir las **recomendaciones de seguridad**:

- ✓ Mantente informado sobre las novedades y alertas de seguridad.
- ✓ Mantén actualizado tu equipo, tanto el sistema operativo como cualquier aplicación que tengas instalada, sobre todo las herramientas *antimalware* ya que su base de datos de *malware* se actualiza en función del nuevo *malware* que se conoce diariamente.
- ✓ Haz copias de seguridad con cierta frecuencia, guárdalas en lugar y soporte seguro para evitar la pérdida de datos importantes.
- ✓ Utiliza software legal que suele ofrecer mayor garantía y soporte.
- ✓ Utiliza contraseñas fuertes en todos los servicios, para dificultar la suplantación de tu usuario (evita nombres, fechas, datos conocidos o deducibles, etc.).
- ✓ Crea diferentes usuarios en tu sistema, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas. Utilizar la mayor parte del tiempo usuarios limitados que no puedan modificar la configuración del sistema operativo ni instalar aplicaciones.
- ✓ Utiliza herramientas de seguridad que te ayudan a proteger y reparar tu equipo frente a las amenazas de la red. Actualizar la base de datos de *malware* de nuestra herramienta antes de realizar cualquier análisis, ya que el *malware* muta y se transforma constantemente.
- ✓ Analizar nuestro sistema de ficheros con varias herramientas, ya que el hecho de que una herramienta no encuentre *malware* no significa que no nos encontremos infectados. Es bueno el contraste entre herramientas *antimalware*.
- ✓ Realizar periódicamente escaneo de puertos, test de velocidad y de las conexiones de red para analizar si las aplicaciones que las emplean son autorizadas. Veremos estos aspectos con más profundidad en el capítulo 6, relativo a redes.
- ✓ No debes fiarte de todas las herramientas *antimalware* que puedes descargar de Internet de forma gratuita o las que te alertan que tu sistema está infectado, ya que algunas de ellas pueden contener código malicioso, publicidad engañosa, no ofrecer la protección prometida e incluso dar como resultado falsos positivos (*FakeAV*). Es el denominado *rogueware*.

4.3.1 CLASIFICACIÓN DEL SOFTWARE ANTIMALWARE

En cuanto a las herramientas disponibles para realizar una correcta prevención y corrección son muy diversas según el frente que se desee atajar. Es importante resaltar que las herramientas *antimalware* se encuentran más desarrolladas para entornos más utilizados por usuarios no experimentados y por tanto más vulnerables, usualmente entornos Windows, aunque la realidad es cambiante y cada vez son mayor el número de infecciones en archivos alojados en servidores de archivos y de correo electrónico bajo GNU/Linux, y aplicaciones cada vez más usadas como Mozilla Firefox.

Antivirus: programa informático específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos. Es una herramienta clásica que pretende ser un escudo de defensa en tiempo real para evitar ejecuciones de archivos o accesos a web maliciosas. Existen versiones de pago y gratuitas, los fabricantes suelen tener distintas versiones para que se puedan probar sus productos de forma gratuita, y en ocasiones para poder desinfectar el *malware* encontrado será necesario comprar sus licencias.

Algunas de las variantes actuales que podemos encontrar son:

- **Antivirus de escritorio:** instalado como una aplicación, permite el control antivirus en tiempo real o del sistema de archivos.
- **Antivirus en línea:** cada vez se están desarrollando más aplicaciones web que permiten, mediante la instalación de *plugins* en el navegador, analizar nuestro sistema de archivos completo.
- **Análisis de ficheros en línea:** servicio gratuito para análisis de ficheros sospechosos mediante el uso de múltiples motores antivirus, como complemento a tu herramienta antivirus. De esta manera podrás comprobar si algún fichero sospechoso contiene o no algún tipo de código malicioso.
- **Antivirus portable:** no requieren instalación en nuestro sistema y consumen una pequeña cantidad de recursos.
- **Antivirus Live:** arrancable y ejecutable desde una unidad extraíble USB, CD o DVD. Permite analizar nuestro disco duro en caso de no poder arrancar nuestro sistema operativo tras haber quedado inutilizable por algún efecto de *malware* o no querer que arranque el sistema operativo por estar ya infectado y no poder desinfectarlo desde el mismo.

Entre otras herramientas específicas destacamos:

- **Antispyware:** el *spyware*, o programas espía, son aplicaciones que se dedican a recopilar información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet, generalmente a alguna empresa de publicidad. Existen herramientas de escritorio y en línea, que analizan nuestras conexiones de red y aplicaciones que las emplean, en busca de conexiones no autorizadas.
- **Herramientas de bloqueo web:** nos informan de la peligrosidad de los sitios web que visitamos, en algunos casos, nos informan de forma detallada, qué enlaces de esas páginas se consideran peligrosos y cuál es el motivo. Existen varios tipos de analizadores en función de cómo se accede al servicio: los que realizan un análisis en línea, los que se descargan como una extensión/*plugin* de la barra del navegador y los que se instalan como una herramienta de escritorio.

A continuación vamos a realizar varias prácticas que permitan ver el espectro de herramientas fundamentales de escaneo *antimalware*.

PRÁCTICA 4.2



ANTIMALWARE

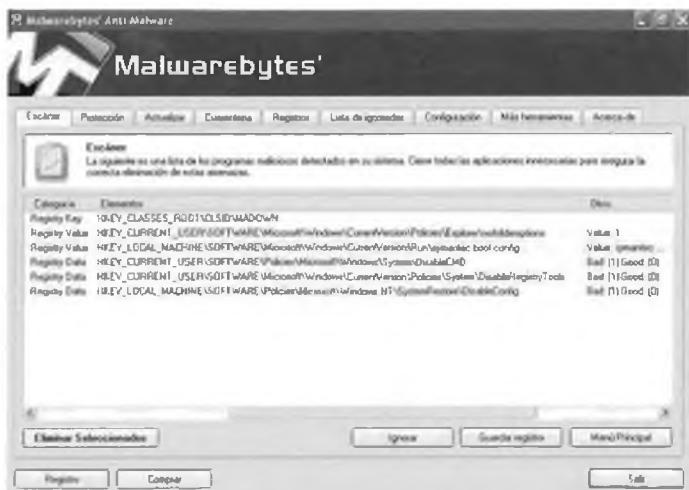
Una de las herramientas más utilizadas por su grado de actualización de base de datos de malware y su eficacia es el software **Malwarebytes** para Windows. Su descarga e instalación es sencilla. Podremos obtener una versión gratuita en <http://www.malwarebytes.org/>.

1. En primer lugar realizaremos una actualización de la aplicación, mediante su pestaña **Actualizar**. A continuación podemos realizar un análisis completo del sistema desde su pestaña **Escáner**.

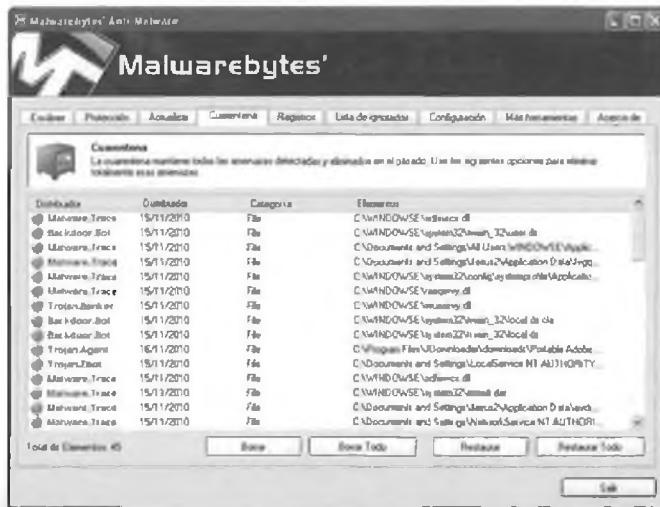


Tras realizar el escáner podremos analizar cada una de las entradas y eliminar las que deseemos.

Esta herramienta es muy útil frente a *rootkits* que hayan modificado el registro de Windows y no permita su edición o la ejecución de comandos mediante la consola.



Las 3 últimas entradas restituyen valores correctos del registro.



De un análisis concreto podemos ver como ha sido capaz de detectar: código *malware* (*malware.trace*), puertas trasera (*backdoor*), troyanos (*trojan*), etc.

PRACTICA 4.3

Los tiempos en los que los antivirus para GNU/Linux eran poco efectivos, casi ni existían o estaban en un segundo plano, poco a poco se van quedando atrás. Debido a que como hemos comentado anteriormente, el mayor número de archivos alojados en servidores de red se encuentra en sistemas GNU/Linux, debemos de conocer herramientas que permitan realizar un análisis exhaustivo y de calidad bajo esta plataforma.

La herramienta que presentaremos es el antivirus **ClamAV**, y su versión gráfica **Clamtk**. Es posible instalarlas mediante los comandos:

- ✓ `sudo aptitude install clamav`
- ✓ `sudo aptitude install clamtk`

Como siempre el primer paso será actualizar la herramienta de forma *online*, mediante el comando: `sudo freshclam`.

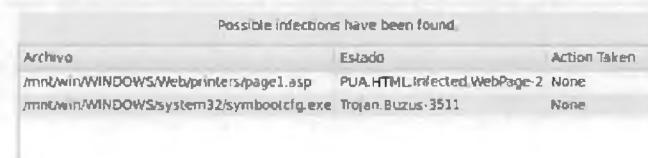
Una vez realizada la actualización de la base de datos de virus, podemos escanear el directorio deseado (/home en este caso) de forma recursiva (opción -r) y que tan sólo solo nos muestre los archivos infectados (-i), por ejemplo:

```
sudo clamscan -r -i /home
```

En el caso de ejecutar la versión gráfica mediante: `sudo clamtk`



En este caso se ha empleado la herramienta para un caso anteriormente comentado: escanear un sistema de archivos Windows sin arrancar el sistema operativo propio. Se ha arrancado en modo Live el sistema desde el CD de instalación de Ubuntu, configurado los parámetros de red para tener conexión con el repositorio de aplicaciones, instalado clamAv y clamTK, y montando la partición deseada (en este caso en `/mnt/win`).



Vemos como ha sido capaz de detectar 2 archivos *malware*, que desde el propio sistema operativo Windows y con la aplicación *Malwarebytes* no había sido capaz de detectar.

PRÁCTICA 4.4

ANÁLISIS ANTIMALWARE LIVE!

A modo de ejemplo de herramienta específica que podemos emplear para rescatar archivos y analizar el *malware* de un sistema, presentaremos **AVG Rescue CD**. Es un conjunto independiente de herramientas que se puede iniciar desde un CD o un disco *flash* USB. Puede utilizarse para recuperar equipos que no permitan el reinicio o que estén infectados y no puedan funcionar con normalidad. Tanto el CD como la unidad *flash* USB constituyen un **sistema autónomo** con el sistema operativo **GNU/Linux** y AVG preinstalados.

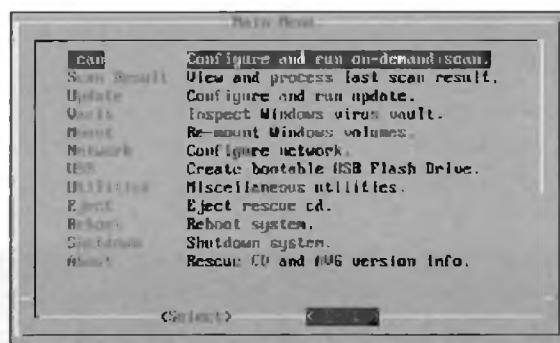
Realizaremos el ejemplo con una memoria USB. En primer lugar descargaremos el archivo RAR desde la web del fabricante y se extraerá en la raíz de un dispositivo USB (unidad *flash*). Para hacer que nuestro USB sea arrancable, seleccionándolo desde la BIOS, ejecutaremos desde Windows el archivo **makeboot.bat** extraído, al ejecutarse, el archivo sobrescribirá el registro de arranque. En la ventana de línea de comandos de Windows abierta, presiona cualquier tecla para preparar la unidad *flash* USB.

Una vez dispuestos los archivos en la memoria podremos arrancar nuestro equipo seleccionando como primer dispositivo de arranque la unidad USB. Una vez arrancado AVG Rescue mostrará en primer lugar una pantalla de bienvenida, seleccionaremos por defecto la primera opción AVG Rescue CD.

Durante el arranque real, AVG Rescue CD montará automáticamente todos los discos duros del equipo. De este modo, los discos duros podrán analizarse y editarse. Así mismo, la conexión de red se configurará automáticamente, si es necesario se indicarán los parámetros de red.

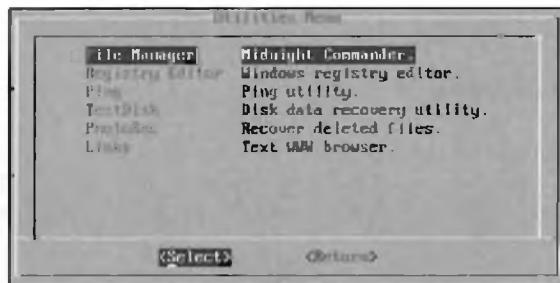
En el siguiente paso, se pregunta si deseamos ejecutar una actualización de AVG, será recomendable realizarla, teniendo en cuenta que debemos disponer de una conexión a Internet activa.

Una vez finalizado el procedimiento de arranque, se abrirá una sencilla interfaz de usuario, como la que se muestra a continuación.



Desde este menú, se puede obtener acceso a todas las funciones esenciales de AVG Rescue CD que son entre otras:

- **Analizar:** para iniciar un análisis *malware*.
- **Resultados del análisis:** visualizar informes de análisis finalizados.
- **Actualizar:** iniciar una actualización de AVG.
- **Montar:** iniciar el montaje de los dispositivos de almacenamiento.
- **Red:** para configurar la conexión de red.
- **Utilidades:** conjunto de herramientas útiles como se presenta en el siguiente menú. Por ejemplo para editar el registro de Windows en caso de que haya sido acaparado y no modificable por algún *rootkit*. Otras opciones: recuperar archivos borrados con Testdisk y Photorec, un explorador de archivos, etc.



4.3.2 LA MEJOR HERRAMIENTA ANIMALWARE

Conocer qué herramienta se ajusta mejor a mis necesidades en cuanto a consumo de recursos, opciones de escaneo, y cantidad de *malware* encontrado en test de prueba, no es fácil.

Muchas de las empresas desarrolladoras de software *antimalware*, muestran estudios en sus propias web demostrando que son mejor que la competencia, pero estos estudios pierden validez al ser conducidos por la propia empresa. También pierden validez los estudios conducidos por los propios usuarios (a pesar de que estos tengan buenos conocimientos de seguridad informática) debido a que generalmente la muestra de virus es muy pequeña o se pueden malinterpretar los resultados, por ejemplo contando la detección de un falso positivo como verdadera cuando no lo es y debería contarse como falsa.

También tenemos que tener en cuenta que la tasa de detección puede variar de mes a mes, debido al gran número de *malware* que se crea, y aunque la tasa de variaciones suele ser pequeña lo mejor es comparar un estudio con otro un poco más antiguo (meses, no años). Hay que recordar que ningún antivirus es perfecto (no existe el 100% de detección), y además, puede que un antivirus detecte un virus que otro antivirus no detectaría y viceversa.

Los estudios con más validez son los que son hechos por empresas o **laboratorios independientes**, entre las empresas más importantes y más precisas que realizan los estudios tenemos:

- ✓ AV Comparatives (<http://www.av-comparatives.org>).
- ✓ AV-Test.org (<http://www.av-test.org>).
- ✓ ICSA Labs (<http://www.icsalabs.com>).
- ✓ Virus Bulletin (<http://www.virusbtn.com>).
- ✓ West Coast Labs (<http://westcoastlabs.org>).

En ocasiones las herramientas *antimalware* no suponen una solución a una infección, ya que detectan posibles amenazas pero no corrigen el problema. En estos casos es más efectivo un **control a fondo** de los procesos de arranque, los que se encuentran en ejecución y otros archivos del sistema que hagan uso por ejemplo de las conexiones de red establecidas.

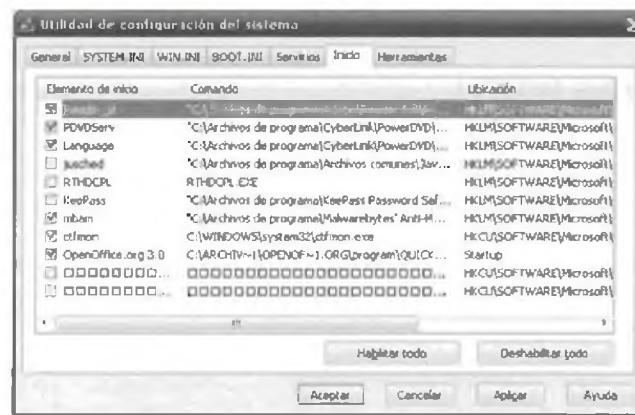
PRÁCTICA 4.5



ANÁLISIS ANIMALWARE A FONDO

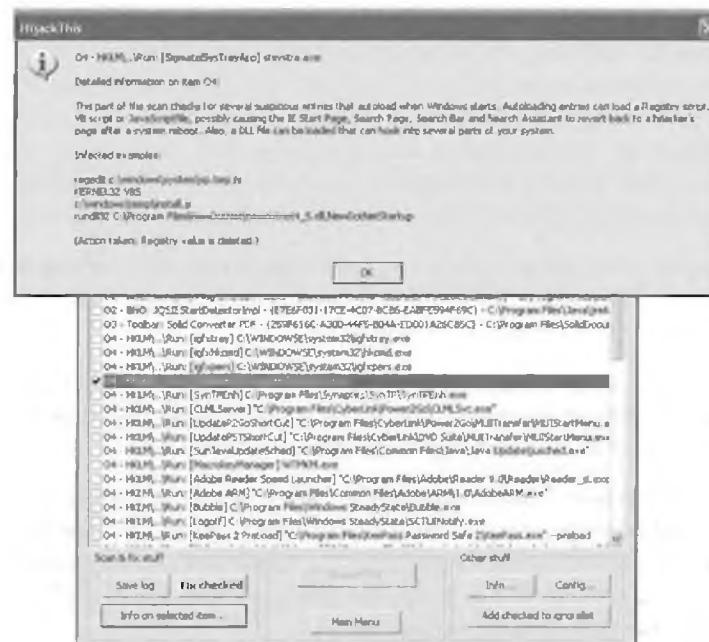
En los sistemas operativos es necesario realizar tareas de monitorización y control exhaustivas para detectar anomalías y modificaciones no deseadas. A continuación veremos que para sistemas Windows existen diversas herramientas que nos permiten controlar y detectar modificaciones si las inspeccionamos periódicamente y analizamos las variaciones que se produzcan:

- Los procesos de arranque en el sistema, mediante la ejecución de la herramienta `msconfig`.



Deshabilitaremos las 2 entradas últimas, potencialmente maliciosas ya que poseen nombres no identificables.

- Los procesos en ejecución podemos analizarlos mediante la herramienta **Autoruns** y **Process Explorer**, que se incluyen en la suite de herramientas **Sysinternals**. Con Autoruns podremos identificar el fabricante y la ruta de ejecución del proceso. Existen otras pestañas como: listado de DLL conocidas, servicios, procesos de inicio de sesión, localización de drivers registrados, etc. Process Explorer muestra los vínculos entre cada proceso y los archivos y DLLs que emplea, socket que abre, usuario que lanza el proceso, hilos de ejecución, etc.
- Herramientas avanzadas de análisis del sistema como la proporcionada por Trend Micro **HijackThis**: permite la búsqueda exhaustiva de elementos no deseados en el arranque, el registro de Windows o los directorios de sistema. Para cada una de las entradas, podemos buscar información acerca de si es potencialmente malicioso o no. A partir de la información suministrada en web de seguridad podremos hacer una desinfección del sistema en caso de infección.



4.4 REFERENCIAS WEB

- Historia del *malware*:
<http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/>
- Útiles gratuitos de seguridad informática del CERT - INTECO – Centro de Respuesta a Incidentes de Seguridad. Instituto Nacional de Tecnologías de la Comunicación:
http://cert.inteco.es/software/Proteccion/utiles_gratuitos/
- Foro de análisis *malware*: <http://www.forospyware.es/>
- Web sobre software *antimalware*: <http://www.antivirusgratis.com.ar/>
- Sección de software gratuito *antimalware* en Softonic: <http://www.softonic.com/s/malware>



RESUMEN DEL CAPÍTULO



Atrás quedaron los años en los que se entendía como virus un código que se ejecutaba en un ordenador con la finalidad de dejarlo inoperativo, concepto muy genérico que se ha visto desarrollado en el término **malware** o software malicioso, orientado actualmente a la obtención de beneficios económicos.

Entre los nuevos tipos de *malware* encontramos a parte de los clásicos virus, gusanos y troyanos, el *greyware* inofensivo generalmente como *Adware*, Broma (*Joke*), Bulo (*Hoax*), los ladrones de información o *infostealers* como *spyware*, *keyloggers* y *PWstealer* o ladrones de contraseñas, así como software dedicado a fines delictivos o *crimeware* que mediante falsificaciones web, *rogueware*, mensajes de *spam* que redireccionan a web falsas para intentar hacer *phishing*, ingeniería social y aprovechando puertas traseras (*backdoor*) y *exploits* para manejar redes zombi o *botnets*, son capaces de lucrarse económicaamente.

Como vemos el *malware* se encuentra cada vez más **especializado y diversificado**, por lo que las empresas desarrolladoras de **herramientas** de prevención, detección y desinfección se encuentran siempre corriendo a tapar las nuevas vulnerabilidades y amenazas.

A la hora de seleccionar la **mejor herramienta** debemos buscar cuáles se ajustan mejor a nuestras necesidades, utilizando siempre el contraste de varias y analizando los informes independientes que realizan los laboratorios de test de herramientas *antimalware* conocidas.

Para mantenerse sin “infecciones”, las **recomendaciones** son: tomar precauciones de uso compartido de dispositivos, así como en la navegación y descarga en Internet. Mantener siempre actualizadas nuestras aplicaciones y sistemas operativos, así como nuestras herramientas *antimalware*, controlar los procesos en ejecución y realizar chequeos periódicos, y mantenerse muy informado de las últimas tendencias en software *malware*, para evitar situaciones comprometidas.



EJERCICIOS PROPUESTOS

- 1. Lee el siguiente artículo sobre la historia de los virus: http://www.nod32-la.com/tutorials/cronologia_de_los_virus_informaticos.pdf y contesta a las siguientes cuestiones:
 - ¿Cómo ha cambiado la finalidad del software *malware* desde sus orígenes hasta hoy? ¿Existen virus para MacOS? ¿A medida que pasan los años la aparición del *malware* es más rápido o lento? ¿Qué dispositivos son el objetivo de los nuevos creadores de *malware*? ¿Por qué?
- 2. Lee el siguiente artículo de comparativa de distintos antivirus, disponible en: <http://www.diarioti.com/gate/n.php?id=25518> y contesta a las siguientes cuestiones:
 - ¿Qué antivirus funcionó mejor ante el test propuesto en 2009? ¿Y en segundo y tercer lugar? ¿Y en el 2008? ¿Qué porcentaje de CPU consume en la máxima carga de trabajo el antivirus más eficiente? ¿Cuál es el único gratuito que superó todas las pruebas?
- 3. Analiza la siguiente noticia “Madrid, capital del spam” <http://www.csospain.es/Madrid,-capital-del-spam-/seccion-alertas/noticia-91980> y contesta:
 - ¿Cómo se denomina al correo basura y por qué? ¿Cuál es el país con mayor emisión de correo basura? ¿En qué posición se encuentra España? Comenta algún caso en el que hayas recibido correo basura con intento de *phishing* y cómo lo detectaste.
- 4. Investiga acerca de secuestradores del navegador web (*browser hijacker*) y de la consola de comandos (*shell hijacker*). ¿Qué efectos no deseados tiene sobre el sistema?
- 5. Busca información sobre el archivo autorun.inf que poseen los dispositivos de almacenamiento y cómo se camufla y opera *malware* a través de este archivo. Dentro de la clasificación de *malware* que hemos visto, ¿qué tipo de *malware* suele ser autorun.inf? ¿Cómo se propaga? ¿Qué efecto tiene? ¿Parece inofensivo? ¿A qué tipo de sistemas operativos afecta? ¿Qué medidas de seguridad puedes tomar? ¿Qué es la desactivación de la ejecución automática? ¿Cómo se puede realizar? ¿Para qué sirve USB Vaccine?
- 6. Visualiza este videotutorial y descubre otra forma de eliminar el *malware*. ¿Con qué programa se realiza la desinfección?

www.cristalab.com/tips/como-eliminar-virus-autorun.inf-de-un-dispositivo-usb-c764361/
- 7. Repartir entre los alumnos de la clase las diferentes herramientas *antimalware* en su versión gratuita, trial o de evaluación, de escritorio y en línea de Ad-aware, Avast, AVG, Avira, Bitdefender, ClamAv, eScan, ESET, F-Secure, G DATA, Kaspersky, Kingsoft, Malwarebyte's, McAfee, Microsoft Security Essentials, Norman, Panda, Sophos, Symantec Norton, TrendMicro o TrustFort. Realiza un escaneo de tu equipo con al menos 2 de ellas y compara el resultado analizando distintas características como:
 - Tiempo y tamaño de la actualización de la aplicación, número de archivos analizados, ocupación en disco de los archivos analizados, % de CPU ocupada en escaneo y en espera, opciones de escaneo, tiempo total de escaneo, *malware* encontrado y desinfectado, recomendaciones de seguridad propuestas.
- 8. Si deseas utilizar alguna herramienta *antimalware* de la que desconoces la reputación del fabricante, te

recomendamos, antes de instalarla, comprobar la confiabilidad de la aplicación en la lista actualizada de <http://www.forospyware.com/t5.html>. Indica al menos cinco programas *Rogueware* o *FakeAVs*.

- 9. Realiza una lista de los programas instalados y los procesos en ejecución en tu sistema. Busca en esta lista realizada si se encuentra algún *FakeAVs* dentro de la lista de Forospyware. Puedes ayudarte del artículo sobre procesos legítimos del sistema operativo en sistemas Windows de ESET:

<http://blogs.eset-la.com/laboratorio/2009/05/07/procesos-legitimos-nativos-sistema-operativo-i/>

■ 10. Entra en la web www.siteadvisor.com (McAfee) y verifica distintas URL de las que tengas dudas sobre su nivel de seguridad. Haz un listado con el informe de al menos tres URL.

■ 11. Investiga sobre la inyección de código SQL (SQL Inyection) con la finalidad de obtener las tablas de usuarios y contraseñas de base de datos de sitios web. ¿Cómo es posible realizarlo? Prueba mediante la distribución Backtrack un intento de inyección SQL en un sitio web en el que sea necesario registrarse. ¿Qué tipo de precauciones tendrías como administrador web para evitar inyección SQL?



TEST DE CONOCIMIENTOS



1 *Malware* que toma el control remoto del usuario administrador:

- a) *Hoax*.
- b) *Joke*.
- c) *Rootkit*.
- d) *Gusano*.

2 *Malware* que envía mensajes electrónicos con noticias falsas o bulos:

- a) *Hoax*.
- b) *Joke*.
- c) *Rootkit*.
- d) *Gusano*.

3 *Malware* que permite capturar lo que se pulsa por teclado para capturar posibles usuarios y contraseñas:

- a) *Clicker*.
- b) *Spyware*.
- c) *Exploit*.
- d) *Keylogger*.

4 Diferencia entre el *scam* y el *spam*:

- a) Fraude bancario y correo basura.
- b) Fraude electrónico y correo basura.
- c) Correo basura y fraude *malware*.
- d) Troyano y gusano.

5 La finalidad actual de crear *malware* es:

- a) Lucrarse.
- b) Hacer el mal.
- c) Divertirse.
- d) Buscar errores en las aplicaciones.
- e) Crear parches de seguridad posteriores.

Distribuidor	Categoría	Elementos
<input checked="" type="checkbox"/> Extension.Mismatch	File	c:\documents and settings\networkservice\configuración local\archivos temporales
<input checked="" type="checkbox"/> Extension.Mismatch	File	c:\documents and settings\networkservice\configuración local\archivos temporales
<input checked="" type="checkbox"/> Extension.Mismatch	File	c:\documents and settings\networkservice\configuración local\archivos temporales
<input checked="" type="checkbox"/> Worm.Conficker	File	c:\WINDOWS\system32\lggygon.dll
<input checked="" type="checkbox"/> Worm.Conficker	File	e:\RECYCLER\z-5-3-42-2819952290-8240756988-879315005-3665\wgkvsg.vmx
<input checked="" type="checkbox"/> Dont.Steal.Our.Software.A	File	e:\Año 2010-2011\SI\malwarebytes 1.45\patrick.exe
<input checked="" type="checkbox"/> Worm.Palevo	Registry Value	HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Wi
<input checked="" type="checkbox"/> Worm.Palevo	Registry Value	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Wi
<input checked="" type="checkbox"/> Hijack.Shell	Registry Data	HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Explor
<input checked="" type="checkbox"/> PUM.Hijack.StartMenu	Registry Data	

Para la figura mostrada, contesta a las preguntas 6, 7 y 8.

6 Despues de realizar un análisis *antimalware*, ¿qué tipo de *malware* es la 4^a entrada?

- a) Gusano.
- b) Troyano.
- c) Virus.
- d) PWstealer.

7 ¿Qué ha modificado la 7^a entrada?

- a) Consola de comandos.
- b) Administrador de tareas.
- c) Registro.
- d) Archivo ejecutable.

8 ¿Qué inhabilita la 9^a entrada?

- a) Consola de comandos.
- b) Administrador de tareas.
- c) Registro.
- d) Archivo ejecutable.

9 ¿Bajo qué término se engloban acciones maliciosas no demasiado perjudiciales?

- a) Hoax.
- b) Greyware.
- c) Joke.
- d) Infostealer.

5

Criptografía

OBJETIVOS DEL CAPÍTULO

- ✓ Profundizar en aspectos de criptografía asociada a la confidencialidad de la información y de las comunicaciones.
- ✓ Garantizar la confidencialidad de la información.
- ✓ Garantizar la privacidad de las comunicaciones.
- ✓ Diferenciar ventajas e inconvenientes de la criptografía simétrica y asimétrica.
- ✓ Analizar nuevos procesos de identificación digital seguros mediante firma digital, certificado digital y dni electrónico.

5.1 PRINCIPIOS DE CRIPTOGRAFÍA

La **criptografía** (del griego “oculto” y “escribir”, literalmente “escritura oculta”) es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos. Otra aplicación frecuente es la de cifrar información contenida en soportes de almacenamiento para garantizar la privacidad y confidencialidad de la misma.

Con más precisión, cuando se habla de esta área de conocimiento como ciencia, se debería hablar de **criptología**, que a su vez engloba tanto las técnicas de cifrado, es decir, la **criptografía** propiamente dicha, como sus técnicas complementarias, entre las cuales se incluye el **criptoanálisis**, que estudia métodos empleados para romper textos cifrados con objeto de recuperar la información original en ausencia de las claves.



La criptografía se considera una rama de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas matemáticas con el objeto principal de *cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves*.

En la terminología de criptografía, encontramos los siguientes aspectos:

- La **información original** que debe protegerse se denomina **texto en claro** o **texto plano**.
- El **cifrado** es el proceso de convertir el *texto plano* en un **texto ilegible**, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* se basa en la existencia de una **clave** o información secreta que adapta el *algoritmo de cifrado* para cada uso distinto.
- Los algoritmos de cifrado se clasifican en dos grandes tipos:
 - **De cifrado en bloque**: dividen el texto origen en bloques de bits de un tamaño fijo y los cifran de manera independiente.
 - **De cifrado de flujo**: el cifrado se realiza bit a bit, byte a byte o carácter a carácter.
- Las **dos técnicas más sencillas** de *cifrado*, en la criptografía clásica, son:
 - **La sustitución**: supone el cambio de significado de los elementos básicos del mensaje, las letras, los dígitos o los símbolos.
 - **La transposición**: supone una reordenación de los mismos, pero los elementos básicos no se modifican en sí mismos.
- El **descifrado** es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la **clave**.



NOTICIA DE ACTUALIDAD

Lee el siguiente artículo sobre la competición existente para condecorar al algoritmo de cifrado más seguro, tras detectar debilidades en el algoritmo "estándar de oro" SHA.

Artículo "Se busca el algoritmo más seguro del mundo", fuente <http://www.laflecha.net/canales/blackhats/noticias/se-busca-el-algoritmo-mas-seguro-del-mundo>.

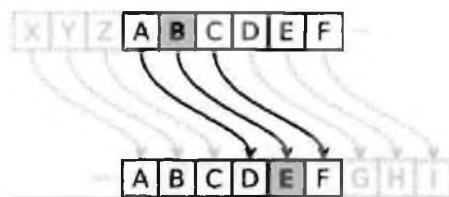
Comenta con el resto de compañeros en clase:

- ¿Qué es el NIST y para qué sirve? ¿Cuántas versiones de SHA existen?
- ¿En qué año se prevé la finalización del concurso? ¿Con qué algoritmo se realizó previamente este proceso?

5.2 TIPOS DE ALGORITMOS DE CIFRADO

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares, de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo empleó en sus campañas, uno de los más conocidos en la literatura.

César utilizó un esquema criptográfico simple pero efectivo para comunicarse con sus generales. El método de cifrado introducido por Julio César introduce el concepto de **clave criptográfica**. El desplazamiento de 3 letras es la clave que se utiliza por César para cifrar el mensaje, necesitándose la misma clave para descifrarlo. El ejemplo de César muestra un criptosistema de clave simétrica en el que se utiliza la misma clave para cifrar y descifrar el mensaje.



Existen dos grandes grupos de *algoritmos de cifrado*:

- **Simétricos o de clave simétrica o privada:** los algoritmos que usan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*.
- **Asimétricos o de clave asimétrica o pública:** los que emplean una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Estos forman el núcleo de las técnicas de cifrado modernas.

Según el principio de Kerchoff la fortaleza de un sistema o algoritmo de cifrado debe recaer en la clave y no en el algoritmo, cuyos principios de funcionamiento son conocidos normalmente, en caso de no conocer la clave no podremos descifrar el mensaje.

PRÁCTICA 5.1



SCRIPTS DE CIFRADO

1. A modo de ejemplo de algoritmo de sustitución, podemos ejecutar el siguiente comando para cifrar mediante codificación César un archivo de texto plano (en el ejemplo denominado documento):

```
Archivo Editar Ver Terminal Ayuda
root@alumno-laptop:/home/alumno/Documentos/Confidencial# cat documento
Este archivo contiene informacion relevante y datos de ingresos periodicos
Pass1: jokoala
Pass2:
Ingresos
etc
root@alumno-laptop:/home/alumno/Documentos/Confidencial# cat documento | tr [a-z] [d-zabc] | tr [A-Z] [D-ZABC] >
documento_cesar
root@alumno-laptop:/home/alumno/Documentos/Confidencial# cat documento_cesar
Hvh dufklyr frqwlhqb lqirupdflrq uhhohydqwh b gdwrv gh lajuuhvrv shulrglfrv
Sdvl1: mmrdod
Sdvv2:
Lajuhvrv
hwf
root@alumno-laptop:/home/alumno/Documentos/Confidencial#
```

Como vemos el comando `tr` permite realizar una sustitución carácter a carácter. Mediante tuberías o *pipes* se han incorporado mayúsculas y casos límite como son los caracteres 'x', 'y' y 'z'.

2. Otro ejemplo donde se sustituyen las vocales por caracteres especiales de puntuación, a→b→etc.

```
Archivo Editar Ver Terminal Ayuda
root@ubuntu:/home/alumno/Documentos/Confidencial# cat documento | tr [aeiou] [;,_-] | tr
[AEIOU] [;,_-] > documento_sustitucion
root@ubuntu:/home/alumno/Documentos/Confidencial# cat documento_sustitucion
st :rch,v. cnt,_n_l: .nf,rm:c,n r_l v:nt
Pass1: jokoala
Pass2:
Ingresos
etc
root@ubuntu:/home/alumno/Documentos/Confidencial#
```

3. Por otro lado, como ejemplo de algoritmo de transposición, pasaremos a un *script* denominado *transposición*. Se un documento en texto plano, y palabra a palabra y carácter a carácter, irá dándole la vuelta, colocando de esta forma cada carácter en una posición diferente pero sin modificarlo.

```

root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: document
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: documento_transposition
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: el documento_transposition
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: es un ataque
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: 256B
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: se origina
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: de
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: transposition.sh
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: 
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: #!/bin/bash
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: if [ ! -f $1 ]
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: then
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: echo "No existe archivo original '$1'"
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: else
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: test -f $1_transposition && touch $1_transposition
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: while read linea
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: do
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:     for palabra in ${linea}
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:     do
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:         longitud=$(echo $palabra | wc -c)
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:         longitud=$((longitud+1))
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:         for i in $(seq $longitud+1 1)
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:             do
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:                 reemplazamiento=$(echo $palabra | cut -c${i})
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:                 echo -n "$reemplazamiento "
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:             done
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:         echo -n " "
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:     done
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh:     done
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: done
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: fi
root@ubuntu:/home/alumno/Documentos/Confidencial/bash_transposition.sh: done < $1

```

5.2.1 CRIPTOGRAFÍA SIMÉTRICA

La **criptografía simétrica** es un método criptográfico en el cual se usa una **misma clave para cifrar y descifrar mensajes**. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario y éste lo descifra con la misma.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Esto lo posibilita la **longitud y el conjunto de caracteres que emplee**. Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. Algunos ejemplos de algoritmos de cifrado simétrico son:

- El **algoritmo de cifrado DES** usa una clave de 56 bits, lo que significa que hay $2^{56} = 72.057.594.037.927.936$ claves posibles. Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días.
- Algoritmos de cifrado como **3DES**, **Blowfish** e **IDEA** usan claves de **128 bits**, lo que significa que existen 2^{128} claves posibles. La mayoría de las tarjetas de crédito y otros medios de pago electrónicos tienen como estándar el algoritmo 3DES.
- Otros algoritmos de cifrado muy usados son **RC5** y **AES**, Advanced Encryption Standard, también conocido como **Rijndael**, estándar de cifrado por el gobierno de los Estados Unidos.

Los **principales problemas** de los sistemas de cifrado simétrico no son su seguridad sino:

- **El intercambio de claves:** una vez que el remitente y el destinatario hayan intercambiado las claves pueden usarlas para comunicarse con seguridad, pero, ¿qué **canal de comunicación seguro** han usado para transmitirse las claves? Sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

- **El número de claves que se necesitan:** si tenemos un número n de personas que necesitan comunicarse entre sí, se necesitan $n/2$ claves diferentes para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Para solucionar estos problemas se mejora la seguridad de los sistemas, mediante la criptografía asimétrica y la criptografía híbrida.

PRÁCTICA 5.2



CIFRADO SIMÉTRICO

PGP (*Pretty Good Privacy*) es el programa más popular de encriptación y de creación de llaves públicas y privadas para seguridad en aplicaciones informáticas, por lo que se considera híbrido. PGP se ha convertido en el estándar de seguridad para las plataformas en que se ha lanzado y permite añadir seguridad a documentos, aplicaciones, etc.

GPG o GNU Privacy Guard es una herramienta para cifrado y firmas digitales, que viene a ser un reemplazo del PGP (*Pretty Good Privacy*) pero con la principal diferencia que es software libre licenciado bajo la GPL. No usa algoritmos de software que están restringidos por patentes, entre estos se encuentra el algoritmo de cifrado IDEA que está presente en PGP casi desde sus inicios. En su lugar usa una serie de **algoritmos no patentados** como ElGamal, CAST5, Triple DES (3DES), AES y Blowfish. Es una aplicación que viene preinstalada en las distribuciones GNU/Linux, aunque existen versiones gratuitas para Windows.

El comando gpg con la opción -c puede ser empleado para realizar cifrado simétrico, pidiéndonos una frase contraseña o clave privada que será empleada tanto para el cifrado como el descifrado.

```
gpg -c archivoorigen
```

La aplicación gpg genera un archivo en el mismo directorio donde se ubique el archivo de origen a cifrar, añadiendo por defecto la extensión gpg. El archivo de salida es binario, para que se componga de caracteres ASCII, añadiremos la opción -a, siendo el formato de salida asc.

En caso de querer descifrar el archivo de salida ejecutamos: gpg -d archivo.asc, en caso de que el archivo haya sido cifrado con caracteres de salida ASCII.

```
Archivo Editar Ver Terminal Ayuda
root@ubuntu:/home/alumno/Dокументos/Confidencial# gpg -c -a documento
gpg: el agente gpg no está disponible en esta sesión
root@ubuntu:/home/alumno/Dокументos/Confidencial# ls
documento documento.asc documento cesar documento.gpg
root@ubuntu:/home/alumno/Dокументos/Confidencial# cat documento.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.9 (GNU/Linux)

jA8EAwMC9xq94xBsIIlgwyWtrP0C6S93wIm)rlXpd3/K3fd0IxjhUVc50+SMbfJT
X05b9/6mv0V3cwNlpvYi30z+7GdQbcb+I4oC181rfpmIv+e4Ns1GGtjUxhcqvQAM
wsmR8qDNc1GA15MoHuyLvaalcvmayV7x5Y5dfQ=
=ITj2
-----END PGP MESSAGE-----
```

Vemos que un fichero creado en texto plano se ha convertido en un archivo no interpretable (documento.asc).

PRÁCTICA 5.3

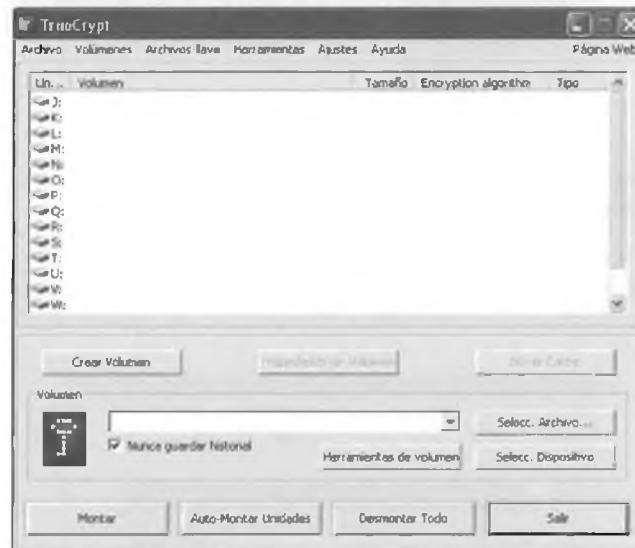
CIFRADO DE DATOS Y PARTICIONES

La confidencialidad de los datos almacenados en una unidad es fundamental, para ello vimos en el primer capítulo a modo de ejemplo como Windows integraba un sistema de encriptación denominado EFS, que aportaba seguridad en el acceso sólo permitiéndoselo al usuario que realizaba la operación.

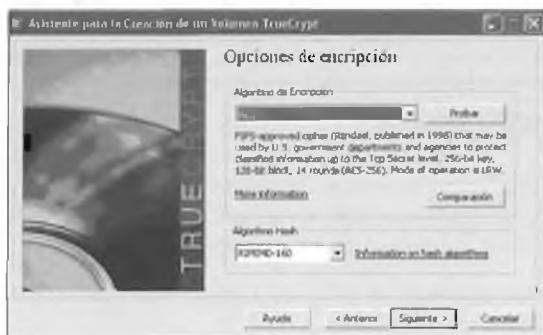
En este caso iremos un paso más adelante y veremos una aplicación para cifrar y ocultar en el ordenador datos que el usuario considere reservados o confidenciales.

TrueCrypt ofrece la posibilidad de crear discos virtuales o aprovechar una partición ya existente para guardar ficheros cifrados, pudiendo escoger entre varios algoritmos de cifrado, como AES, Serpent o Twofish, y determinar de qué capacidad será la unidad virtual. Allí podremos guardar cualquier documento de forma segura y cómoda. Se integra con el explorador de archivos que usemos, es fácil de usar, permitiendo crear hasta 32 unidades diferentes. Existen versiones para sistemas operativos Windows, Mac OS X, y GNU/Linux.

1. Descargaremos la aplicación y la instalaremos. En primer lugar podemos disponer de la herramienta traducida al español pulsando *Settings / Language / Download Language Pack*, descargamos un archivo zip y lo descomprimimos en la misma carpeta donde instalamos. Tras reiniciar la aplicación podremos seleccionar *Settings / Language / Español*.



2. A continuación podremos crear un volumen normal (botón “Crear Volumen”), seleccionamos la opción en un archivo, que se creará en la ubicación que seleccionemos (indicaremos un nombre por ejemplo *volumen_cifrado*). Entre las opciones de encriptación podremos seleccionar entre diferentes algoritmos pudiendo ver una tabla comparativa con rendimientos en procesos de encriptación y desencriptación.



Una vez seleccionado, elegimos el tamaño de tu volumen cifrado y añadiremos una contraseña lo más segura posible.

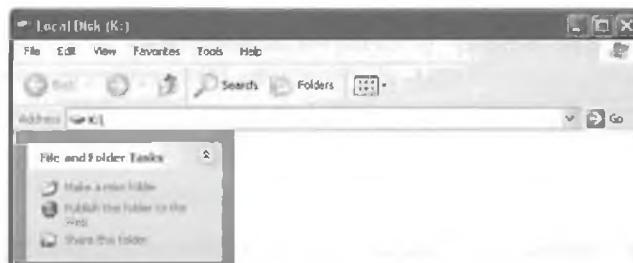


Seleccionamos el sistema de ficheros (por ejemplo: NTFS por defecto) y nos indicará a continuación que el volumen ha sido creado.

- Para utilizarlo debemos montar una unidad con el archivo creado. Seleccionamos una unidad disponible, por ejemplo K, y pulsaremos el botón **Seleccionar archivo**, donde navegaremos hasta la ruta del archivo creado para el volumen encriptado. Pulsaremos **Montar** y se nos pedirá nuestra contraseña:



Haciendo doble clic sobre la unidad accederemos a nuestro volumen cifrado.



Cualquier fichero que arrastremos hacia la unidad se guardará cifrado de forma transparente, y **sin necesidad de que teclees de nuevo la contraseña** (solo se te pide cuando montas la unidad). Puedes utilizar tu volumen cifrado TrueCrypt como **otra unidad más de disco**. Por último no olvidemos desmontar el volumen, pulsaremos el botón *Desmontar*.

Es recomendable realizar copia de seguridad del archivo ya que en caso de borrarlo perderemos la información contenida en él.

5.2.2 CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA

En este caso, cada usuario del sistema criptográfico ha de poseer una pareja de claves:

- **Clave privada:** será custodiada por su propietario y no se dará a conocer a ningún otro.
- **Clave pública:** será conocida por todos los usuarios.

Esta pareja de claves es complementaria: **lo que cifra una solo lo puede descifrar la otra y viceversa**. Estas claves se obtienen mediante algoritmos y funciones matemáticas complejas de forma que por razones de tiempo de cálculo, es imposible conocer una clave a partir de la otra.

Los sistemas de cifrado de clave pública se basan en **funciones resumen o funciones hash de un solo sentido** que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil.

Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función resumen o *hash* de un sentido es algo parecido, pero tiene una simplificación o atajo, si se conoce alguna parte de la información, sería fácil computar el inverso. Por ejemplo, si tenemos un número compuesto por dos factores primos y conocemos uno de los factores, es fácil computar el segundo.

Algunos de los algoritmos empleados como funciones resumen o hash son MD5 y SHA.

PRÁCTICA 5.4



FUNCIONES RESUMEN (HASH)

En la siguiente práctica vamos a analizar la **integridad de un archivo** descargado mediante la comprobación de su valor resumen calculado. En muchas ocasiones las web de los fabricantes originales muestran junto a su archivo de instalación el valor resumen calculado, con el que podremos verificar tras descargar el archivo de instalación su integridad o que no ha sido modificado o es una falsificación.

En el caso de GNU/Linux podemos emplear el comando `md5sum nombreArchivo` y nos calculará el valor resumen MD5, pudiendo contrastarlo con el valor del fabricante. Para Windows existe la posibilidad de descargar una pequeña aplicación `md5sum.exe`.

Si ejecutamos: `md5sum Documento.txt`.

A la salida nos mostrará: `86372149c86767b4ef3209612e1a272e *Documento.txt`

En caso de querer verificar el resultado automáticamente crearemos un archivo `.md5`: `md5sum Documento.txt > NombredelHASH.md5`

Para verificar la integridad del archivo: `md5sum -c NombredelHASH.md5`

- ✓ Si el archivo no ha sido modificado mostrará: `Documento.txt: OK`
- ✓ Si el archivo ha sido modificado: `Documento.txt: FAILED md5sum: WARNING: 1 of 1 computed checksum did NOT match`

El tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño de la clave del cifrado simétrico con el del cifrado de clave pública para medir la seguridad.

En un ataque de fuerza bruta sobre un **cifrado simétrico** con una clave del tamaño de 80 bits, el atacante debe probar hasta 2^{80} claves para encontrar la clave correcta.

En un ataque de fuerza bruta sobre un **cifrado de clave pública** con una clave del tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits. La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el **uso de claves públicas de 1024 bits** para la mayoría de los casos.

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes **desventajas**:

- Para una misma longitud de clave y mensaje se necesita **mayor tiempo de proceso**.
- Las **claves deben ser de mayor tamaño** que las simétricas.
- El **mensaje cifrado ocupa más espacio** que el original.

Herramientas software como PGP o en comunicaciones TCP/IP, protocolos como SSH o la capa de seguridad TLS/SSL, utilizan un **cifrado híbrido** formado por la **criptografía asimétrica** para **intercambiar claves de criptografía simétrica** y la **criptografía simétrica** para la transmisión de la información.

- Algunos **algoritmos** de técnicas de clave asimétrica son:
 - Diffie-Hellman, RSA, DSA, ElGamal, criptografía de curva elíptica.
- Algunos **protocolos** y software que usan los algoritmos antes citados son:
 - DSS (*Digital Signature Standard*) con el algoritmo DSA (*Digital Signature Algorithm*).
 - PGP y GPG, una implementación de OpenPGP.
 - SSH, SSL y TLS.

5.2.3 CRIPTOGRAFÍA HÍBRIDA

El uso de claves asimétricas ralentiza el proceso de cifrado. Para solventar dicho inconveniente, el procedimiento que suele seguirse para realizar el cifrado de un mensaje es **utilizar un algoritmo de clave pública**, más seguro, tan solo empleado para el cifrado en el envío de una pequeña cantidad de información: por ejemplo una clave simétrica, **junto a uno de clave simétrica**, para el cifrado del mensaje, reduciendo de esta forma el coste computacional.

A modo de ejemplo describiremos un proceso de comunicación seguro:

Ana y Bernardo tienen sus pares de claves respectivas.

- Ana escribe un **mensaje** a Bernardo. Lo cifra con el sistema de criptografía de **clave simétrica**.
- La clave que utiliza se llama **clave de sesión** y se genera aleatoriamente. Para **enviar la clave de sesión de forma segura**, ésta se cifra con la clave pública de Bernardo, utilizando por lo tanto criptografía de **clave asimétrica**.
- Bernardo recibe el mensaje cifrado con la clave de sesión y ésta misma cifrada con su clave pública. Para realizar el proceso inverso, en primer lugar utiliza su clave privada para **descifrar la clave de sesión**.
- Una vez ha obtenida la clave de sesión, ya puede **descifrar el mensaje**.

Con este sistema conseguimos:

- **Confidencialidad**: solo podrá leer el mensaje el destinatario del mismo.
- **Integridad**: el mensaje no podrá ser modificado.

Pero todavía quedan sin resolver los problemas de **autenticación y de no repudio**.

PRÁCTICA 5.5



CIFRADO ASIMÉTRICO

1. Emplearemos gpg para la generación de un par de claves para cifrado asimétrico mediante: gpg --gen-key

Durante el proceso de generación se nos irán haciendo diversas preguntas, como el tipo de cifrado que queremos utilizar, la intensidad de cifrado, la fecha de expiración de la clave en cuestión y nuestro nombre y apellidos así como una dirección de correo, que es lo que va a constituir el USERID.

Nos va a bastar con aceptar las opciones que ya vienen por defecto, ya que en la mayoría de los casos éstas son apropiadas:

- ✓ Tipo de claves, la primera opción (DSA and ElGamal) que nos permite encriptar y firmar.
- ✓ Tamaño de las claves que se puede elegir entre 1024 y 4096 bits. Por defecto se recomienda 2048, a mayor tamaño más segura es la clave y mayor el tiempo de cómputo al encriptar y desencriptar.
- ✓ Tiempo de validez queremos que tenga la clave. Por defecto viene la opción 0 que es que no caduque nunca. En el caso de poner que caduque al cabo de cierto tiempo habrá que volver a generar las claves y volver a mandar la nueva clave pública a aquellos que usaban la que ha caducado.
- ✓ Último paso, generar la clave, se nos va a preguntar por una **frase de paso** o **passphrase**, es decir, una contraseña. Esta contraseña nos va a asegurar que nadie más que nosotros mismos va a poder usar esta clave GPG, por lo que es importante elegir una contraseña fuerte y difícil de adivinar, pero que sea lo suficientemente clara para nosotros como para no olvidarla, puesto que si esto sucede no podremos volver a utilizar más la clave gpg relacionada.

Cuando se produce el proceso de generación de las claves es buena idea reproducir mp3, mover el ratón... , para que se generen números aleatorios y se creen antes las claves.

Si es la primera vez que se ejecuta nos crea un directorio en el que guardará el fichero de configuración así como los archivos **secring.gpg** y **pubring.gpg**. En el primero se almacenaran las claves privadas y en el segundo las claves públicas.

Para ver las claves públicas que tenemos disponibles hay que hacerlo con el comando gpg --list-keys o gpg -k. Esto lo que hace es listar las claves que hay disponibles dentro del fichero pubring.gpg. En el ejemplo podemos ver 1 clave pública disponible, el **identificador de cada clave** (ClaveID) es el número que aparece después de 1024D al hacer gpg --list-keys, en nuestro caso 5D10BEF4.

```

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

gpg: /root/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 5D10BEF4 marcada como de confianza absoluta
claves públicas y secretas creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 llave(s) necesaria(s), 1 completa(s) necesaria(s),
      modelo de confianza PGP
gpg: nivel: 0 validez: 1 firmada: 0 confianza: 0=Q, Bn, Bm, Bf, lu
pub 1024D/5D10BEF4 2018-12-15
      Huella de clave = 6058 B3B2 AA00 2742 C157 BB0C 2A82 C4E5 5D10 BEF4
uid          Jesus Costas Santos (Generación de claves para cifrado asimétrico) <jesus@msn.com>
sub 2048G/620B8237 2018-12-15

root@ubuntu:/home/alumno/Documentos/Confidencial# gpg -k
root@ubuntu:/home/alumno/Documentos/Confidencial# gpg -k
pub 1024D/5D10BEF4 2018-12-15
uid          Jesus Costas Santos (Generación de claves para cifrado asimétrico) <jesus@msn.com>
sub 2048G/620B8237 2018-12-15

```

Para ver las claves privadas que tenemos disponibles hay que hacerlo con el comando gpg --list-secret-keys. Esto lo que haces listar las claves que hay disponibles dentro del fichero secring.gpg.

Se llaman anillos a los archivos en los que se guardan las claves públicas y las privadas. Si se quiere borrar alguna clave primero hay que borrar la clave privada y después la pública. Para borrar claves privadas se hace con el comando gpg --delete-secret-key ClaveID. Para las claves públicas se hace con el comando gpg --delete-key ClaveID

Copia y distribución de claves

Una vez generadas las claves, para que el resto de personas y entidades puedan comprobar nuestros mensajes firmados, tenemos que darles nuestra clave pública. Esto se puede hacer de varias maneras:

1. Subiéndola a un **servidor de claves públicas**. Los servidores de claves suelen estar interconectados, es decir, que subiendo la clave a un servidor, el resto ya tiene conocimiento de la existencia de nuestra nueva clave. El servidor pgp de rediris puede ser usado para este propósito. La orden a teclear para remitir nuestra clave es:

```
gpg --send-keys --keyserver pgp.rediris.es ClaveID.
```

Para hacer una búsqueda de claves públicas, de entidades o usuarios con los que queremos comunicarnos o verificar un mensaje recibido de éstos: gpg --keyserver NombreDelServidor --search-keys ClaveID.

Para bajarnos dicha clave pública: gpg --keyserver NombreDelServidor --recv-keys ClaveID

2. Enviándola por correo o dándola en un soporte portable (USB, CD/DVD, etc.), mediante un fichero. Si tan sólo solo queremos que no sea de dominio tan público sino que sólo solo unos pocos tengan conocimiento de nuestra clave pública, para ello deberemos volcar esta clave a un fichero de texto. El comando para ello podría realizarse de 2 formas:

```
gpg - -armor - - output ficheroclave - - export ClaveID
```

Es importante tener una copia aparte de nuestra clave privada, para que en caso de desastre informático o pérdida de datos podamos recuperarla. Para exportar la clave privada a un fichero y poder tener una copia de seguridad: gpg --armor --output fichoedoclave --export-secret-key ClaveID

Después de emplear el método de distribución deseado, el comando a ejecutar en la máquina destinataria para importar una clave volcada en un fichero, es: gpg - - import ficheroclave

Eliminar claves distribuidas en servidores

Si se ha olvidado la contraseña o hemos perdido la clave privada, o consideramos que se encuentra en estado comprometida, podemos generar un **certificado de revocación** y subirlo a un servidor de claves. Se recomienda crear este certificado al crear las claves ya que al final del proceso de generación se pide la contraseña. Esta clave ha de guardarse en un lugar seguro ya que si alguien la obtuviese podría revocar nuestras claves y dejarlas inutilizadas. La orden para generar este certificado es: gpg -o revocation.asc --gen-revoke ClaveID

Si queremos revocar una clave hay que importar el fichero que tiene el certificado de revocación, una vez revocada la clave ya no podemos cifrar mensajes aunque si se pueden desencriptar.

Para importar a nuestra relación de claves: gpg --import revacion.asc

```

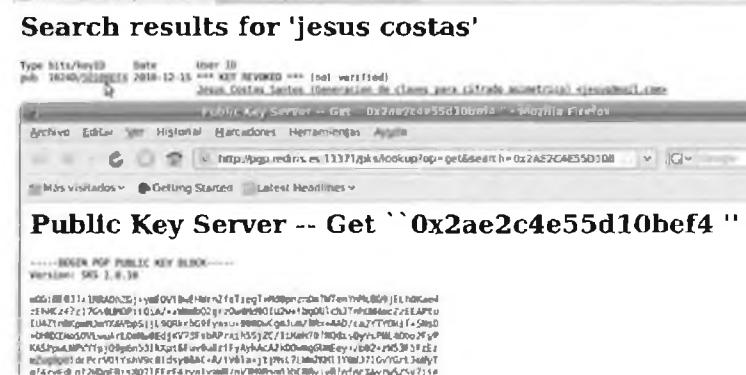
Archivo Editar Ver Terminal Ayuda
Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Jesus Costas Santos (Generación de claves para cifrado asimétrico) <jesus@mail.com>
clave RSA de 1024 bits, ID 5D1B8EFA, creada el 2010-12-15
se fuerza salida con armadura ASCII.
Certificado de revocación creado.

Por favor consérvelo en un medio que pueda esconder; si alguien consigue
acceso a este certificado puede usarlo para inutilizar su clave.
Es inteligente imprimir este certificado y guardarlo en otro lugar, por
si acaso su medio resulta imposible de leer. Pero precaución: el sistema
de impresión de su máquina podría almacenar los datos y hacerlos accesibles
a otras personas!
root@ubuntu:/home/alumno/Documentos/Confidencial# gpg --import revocation.asc
gpg: clave 5D1B8EFA: "Jesus Costas Santos (Generación de claves para cifrado asimétrico)
<jesus@mail.com>" certificado de revocación importado
gpg: Cantidad total procesada: 1
gpg:   nuevas revocaciones de claves: 1
gpg: 3 deducida(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 8 validad: 1 firmada: 8 confianza: 0-, 0q, 0n, 0m, 0f, lu
root@ubuntu:/home/alumno/Documentos/Confidencial# cat revocation.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (Ubuntu/Linaro)
Comment: A revocation certificate should follow

-----BEGIN PGP PUBLIC KEY BLOCK -----
root@ubuntu:/home/alumno/Documentos/Confidencial# gpg -k
/root/.gnupg/pubring.gpg
-----[REDACTED]-----
pub 1024R/5D1B8EFA 2010-12-15 [revocada: 2010-12-15]
uid          Jesus Costas Santos (Generación de claves para cifrado asimétrico)
<jesus@mail.com>
```

Como vemos en la figura anterior al listar el listado de claves, muestra la fecha de revocación.

El último paso es comunicar a los servidores de claves que nuestra clave ya no es válida, con la orden: `gpg --keyserver NombreDelServidor --send-keys ClaveID`. Tras realizar dicha operación podemos buscar y ver el estado del certificado en el servidor público de certificados.



5.2.4 FIRMA DIGITAL

Una de las principales ventajas de la criptografía de clave pública es que ofrece un método para el desarrollo de **firmas digitales**. La firma digital permite al receptor de un mensaje **verificar la autenticidad del origen de la información** así como verificar que dicha información **no ha sido modificada** desde su generación. De este modo, la firma digital ofrece el soporte para la **autenticación e integridad** de los datos así como para el **no repudio en origen**, ya que la persona que origina un mensaje firmado digitalmente no puede argumentar que no lo hizo.

Una firma digital está destinada al mismo propósito que una manuscrita. Sin embargo, una firma manuscrita es sencilla de falsificar mientras que la digital es imposible mientras no se descubra la clave privada del firmante.

La firma digital es un **cifrado del mensaje** que se está firmando pero utilizando la **clave privada** en lugar de la pública.

Sin embargo, ya se ha comentado el principal inconveniente de los algoritmos de clave pública: su lentitud que, además, crece con el tamaño del mensaje a cifrar. Para evitar este problema, la **firma digital** es el resultado de **cifrar con clave privada el resumen de los datos a firmar**, haciendo uso de **funciones resumen o hash**.

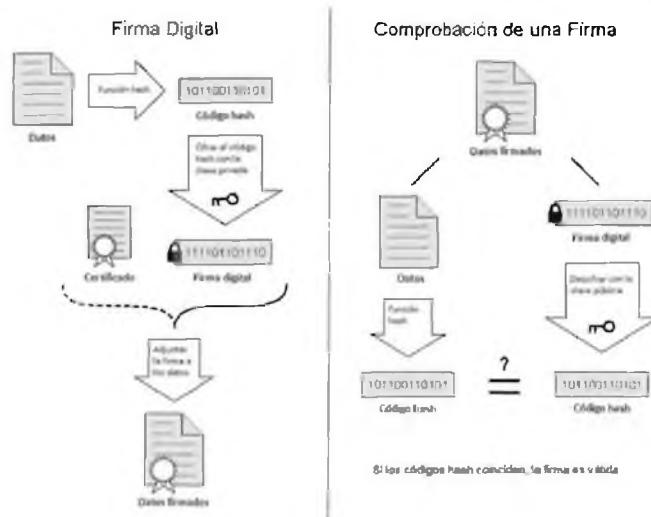
A modo de ejemplo: Ana y Bernardo tienen sus pares de claves respectivas.

Ana escribe un mensaje a Bernardo. Es necesario que Bernardo pueda verificar que realmente es Ana quien ha enviado el mensaje, por lo tanto, Ana debe enviarlo firmado:

1. Ana resume el mensaje o datos mediante una función *hash*.
2. Cifra el resultado de la función hash con su clave privada. De esta forma obtiene su **firma digital**.
3. Envía a Bernardo el mensaje original junto con la firma.

Bernardo recibe el mensaje junto a la firma digital. Deberá comprobar la validez de ésta para dar por bueno el mensaje y reconocer al autor del mismo (integridad y autenticación).

4. Descifra el resumen del mensaje mediante la clave pública de Ana.
5. Aplica al mensaje la función *hash* para obtener el resumen.
6. Compara el resumen recibido descifrado, con el obtenido a partir de la función *hash*. Si son iguales, Bernardo puede estar seguro de que quien ha enviado el mensaje es Ana y que éste no ha sido modificado.



Mecánica de la generación y comprobación de una firma digital.

Con este sistema conseguimos:

- **Autenticación:** la firma digital es equivalente a la firma física de un documento.
- **Integridad:** el mensaje no podrá ser modificado.
- **No repudio en origen:** el emisor no puede negar haber enviado el mensaje.

PRÁCTICA 5.6



FIRMA DIGITAL DE UN DOCUMENTO

La firma digital de un documento se compone del cifrado con nuestra clave privada del valor resumen calculado con una función hash de un mensaje o archivo. Existen diversos modos de envío de documentos firmados, documento + firma en un solo archivo cifrado, o documento y firma en archivos separados. Los parámetros de gpg para obtener la firma digital de documentos son los siguientes:

- ✓ *clearsign*: se une la firma digital al contenido del archivo, el cual no se cifra.
- ✓ *s*: se une la firma digital al contenido del archivo, el cual se cifra con la clave privada, como resultado tenemos un archivo binario. Se emplea para firmar archivos binarios, comprimidos, ejecutables, etc.
- ✓ *b*: firma y mensaje están contenidos en archivos separados.

A modo de ejemplo podemos realizar: `gpg -- clearsign documento`, tendremos a la salida un archivo `documento.asc`, donde el contenido no está cifrado y se encuentra firmado digitalmente al final, entre *begin pgp signature* y *end pgp signature*.

Para verificar la validez de las firmas digitales emplearemos la opción `--verify`, teniendo en cuenta que la entidad o usuario que quiera realizar la comprobación de nuestra firma deberá tener nuestra clave pública disponible, es decir importada previamente.

En la figura vemos después de ejecutar: `gpg -b -a documento`, generando de este modo una firma separada del documento, denominada `documento.asc`, una verificación de dicha firma.

```
root@ubuntu:/home/almirno/Documentos/Confidencial# cat documento.asc
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.9 (GNU/Linux)

IEYEAABCACAYFAK8JM/MACcok0tyJMaRjS82VHQACDB+NAx7YNb81vAgnuzkopB7E
KRUAn31ZikLFqdqNqC8rlH0Sbvw4kv
=9U4r
-----END PGP SIGNATURE-----
root@ubuntu:/home/almirno/Documentos/Confidencial# gpg --verify documento.asc
gpg: Firmado el mié 15 dic 2010 22:32:35 CET usando clave DSA ID 10F9F368
gpg: Firma correcta de "Jesus Costas 2 (Generación de claves 2) <jcostas@mail.com>"
```

5.3 CERTIFICADOS DIGITALES

Según puede interpretarse de los apartados anteriores, la eficacia de las operaciones de cifrado y firma digital basadas en criptografía de clave pública solo está garantizada si se tiene la certeza de que la clave privada de los usuarios solo es conocida por dichos usuarios y que la pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios.

Para garantizar la **unicidad de las claves privadas** se suele recurrir a **soportes físicos** tales como tarjetas inteligentes (*SmartCards*) que garantizan la imposibilidad de la duplicación de las claves. Además, las tarjetas criptográficas suelen estar protegidas por un número personal o PIN solo conocido por su propietario que garantiza que, aunque se extravie la tarjeta, nadie que no conozca dicho número podrá hacer uso de ella. Como caso particular encontramos el **DNI electrónico o DNIE**.

Por otra parte, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales o documento electrónico que asocia una clave pública con la identidad de su propietario.

En general un certificado digital es un archivo que puede emplear un software para firmar digitalmente archivos y mensajes por ejemplo de correo electrónico, en los cuales puede verificarse la identidad del firmante.

Como ejemplo encontramos los certificados digitales que identifican a personas u organizaciones, y que contienen información sobre una persona o entidad, nombre, dirección, mail, el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc., así como una clave pública y una firma digital de una autoridad certificadora u organismo de confianza, en España La Casa de la Moneda y Timbre. En el apartado siguiente veremos la importancia de las autoridades certificadoras.

El formato estándar de certificados digitales es X.509 y su distribución es posible realizarla:

- Con clave privada (suele tener extensión *.pfx o *.p12) más seguro y destinado a un uso privado de exportación e importación posterior como método de copia de seguridad.
- Solo con clave pública (suele ser de extensión *.cer o *.crt), destinado a la distribución no segura, para que otras entidades o usuarios tan solo puedan verificar la identidad, en los archivos o mensajes firmados.



Entre las aplicaciones de los certificados digitales y el DNIe encontramos, realizar compras y comunicaciones seguras, como trámites con la banca online, con la administración pública (hacienda, seguridad social, etc.) a través de Internet, etc.

PRÁCTICA 5.7

UTILIDADES DE CERTIFICADOS

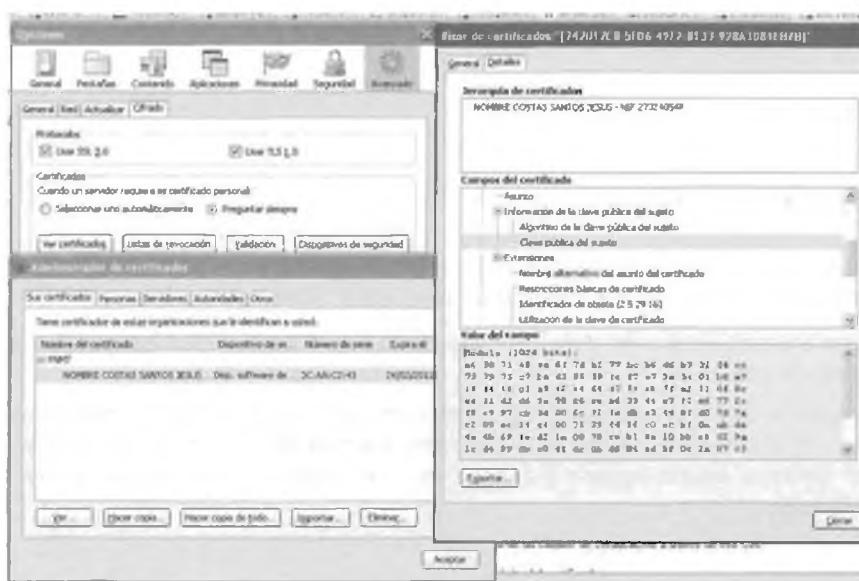
Los certificados digitales son de gran utilidad hoy en día y nos sirven principalmente para garantizar la autenticidad y generar confianza de mensajes, información y sitios web, entre otras aplicaciones.

- 1) En primer lugar analizaremos como una visualización del certificado digital nos puede servir para atestiguar la veracidad de un sitio web:

En los navegadores web, cuando visitamos sitios web seguros (<https://>) que poseen formulario de envío de credenciales o de datos privados que deben ser enviados de forma segura, se muestra un candado en la parte inferior derecha del navegador. Pulsando sobre él podremos ver su certificado digital, así como la entidad certificadora.



- 2) Los certificados personales o de entidad pueden ser instalados en el sistema operativo, en aplicaciones como navegadores web o clientes de correo electrónico, para posibilitar accesos a páginas web seguras y cifrar mensajes, eliminando el uso de credenciales escritas por teclado. A continuación vemos las opciones de Mozilla Firefox; en su pestaña Avanzado podemos visualizar los certificados instalados y realizar acciones de exportaciones o ver sus atributos.



5.3.1 TERCERAS PARTES DE CONFIANZA

Una vez definido el concepto de certificado digital se plantea una duda: ¿cómo confiar si un determinado certificado es válido o si está falsificado? La validez de un certificado es la confianza en que la clave pública contenida en el certificado pertenece al usuario indicado en el certificado.

La manera en que se puede confiar en el certificado de un usuario con el que nunca hemos tenido ninguna relación previa es mediante la **confianza en terceras partes**.

La idea consiste en que **dos usuarios puedan confiar directamente entre sí, si ambos tienen relación con una tercera parte y que ésta puede dar fe de la fiabilidad de los dos**.

La necesidad de una Tercera Parte Confiable (TPC o TTP, *Trusted Third Party*) es fundamental en cualquier entorno de clave pública de tamaño considerable debido a que es impensable que los usuarios hayan tenido relaciones previas antes de intercambiar información cifrada o firmada. Además, la mejor forma de permitir la **distribución de las claves públicas (o certificados digitales)** de los distintos usuarios es que algún **agente**, en quien todos los usuarios confíen, se encargue de su publicación en algún repositorio al que todos los usuarios tengan acceso.

En conclusión, se podrá tener confianza en el certificado digital de un usuario al que previamente no conocemos si dicho certificado está avalado por una tercera parte en la que sí confiamos. **La forma en que esa tercera parte avalará que el certificado es de fiar es mediante su firma digital sobre el certificado.**

Por tanto, podremos confiar en cualquier certificado digital firmado por una tercera parte en la que confiamos. La TPC que se encarga de la firma digital de los certificados de los usuarios de un entorno de clave pública se conoce con el nombre de **Autoridad de Certificación** (AC).

El modelo de confianza basado en Terceras Partes Confiables es la base de la definición de las **Infraestructuras de Clave Pública** (ICP o PKI, *Public Key Infrastructures*), formado por:

- Autoridad de certificación (CA): emite y elimina los certificados digitales.
- Autoridad de registro (RA): controla la generación de los certificados, procesa las peticiones y comprueba la identidad de los usuarios, mediante el requerimiento de documentación de identificación personal oportuna.
- Autoridades de repositorio: almacenan los certificados emitidos y eliminados.
- Software para el empleo de certificados.
- Política de seguridad en las comunicaciones relacionadas con gestiones de certificados.

5.3.2 DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO (DNIe)

El Documento Nacional de Identidad (DNI), emitido por la **Dirección General de la Policía** (Ministerio del Interior), es el documento que acredita, desde hace más de 50 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que, esencialmente, son:

- Acreditar electrónicamente y sin posibilidad de duda, la identidad de la persona.
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.

Para responder a estas nuevas necesidades nace el **Documento Nacional de Identidad electrónico (DNIe)**, similar al tradicional y cuya principal novedad es que **incorpora un pequeño circuito integrado (chip)**, capaz de guardar de forma segura, mediante medidas específicas de seguridad para impedir su falsificación, información en formato digital como:

- Un certificado electrónico para autenticar la personalidad del ciudadano.
- Un certificado electrónico para firmar electrónicamente, con la misma validez jurídica que la firma manuscrita.
- Certificado de la Autoridad de Certificación emisora.
- Claves para su utilización.
- La plantilla biométrica de la impresión dactilar.

Para la utilización del DNI electrónico es necesario contar con determinados elementos:

- ✓ Hardware específico: lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados por ejemplo vía USB).
- ✓ Software específico: mediante controladores o módulos criptográficos que permitan el acceso al chip de la tarjeta y, por tanto la utilización de los certificados contenidos en él. En Windows es el servicio *Cryptographic Service Provider* (CSP), y en los entornos GNU/Linux o MAC el módulo criptográfico se denomina PKCS#11.

5.4 REFERENCIAS WEB

- Web especializada en aplicaciones de seguridad y criptografía:
<http://www.kriptopolis.org/>
- Taller de criptografía:
<http://www.cripto.es/>
- Libro electrónico sobre criptografía avanzada:
http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- Web de la Fábrica Nacional de Moneda y Timbre, Autoridad de Certificación y expedición de certificados digitales:
<http://www.cert.fnmt.es/>
- Camerfirma. Web de las cámaras de comercio con información sobre certificados digitales:
<http://www.camerfirma.com/>
- Web del DNI electrónico. Ministerio del interior:
<http://www.dnielectronico.es/>
- Información práctica sobre el DNI electrónico:
<http://www.dnielectronico.eu/>



RESUMEN DEL CAPÍTULO

Desde los orígenes de la humanidad los mensajes que se transmitían se han intentado realizar de tal modo que no se pudieran entender por cualquier persona que lo interceptara. La **criptografía**, arte o ciencia de cifrar y descifrar información mediante técnicas especiales, se emplea frecuentemente para permitir un intercambio de mensajes que solo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

El cifrado es el proceso de convertir un texto plano en uno ilegible, denominado **texto cifrado**. Existen dos métodos criptográficos, principalmente:

- **Criptografía simétrica:** con una misma clave para cifrar y descifrar mensajes. Implementada en algoritmos como DES, 3DES, Blowfish e IDEA, RC5 y AES.
- **Criptografía asimétrica:** cada usuario posee una pareja de claves, una clave privada que no se dará a conocer, y una clave pública que será conocida por el resto de los usuarios con los que quiera comunicarse. Implementada en algoritmos como Diffie-Hellman, RSA, DSA, ElGamal.

Alguna de las **aplicaciones actuales** de la criptografía simétrica, por su menor coste computacional, es el envío y recepción de mensajes largos o el cifrado de sistemas de ficheros.

Herramientas software como PGP o en comunicaciones TCP/IP, protocolos como SSH o la capa de seguridad TLS/SSL, utilizan un **cifrado híbrido** formado por la criptografía asimétrica para intercambiar claves de criptografía simétrica y la criptografía simétrica para la transmisión de la información.

Una de las principales ventajas de la criptografía de clave pública o asimétrica es que ofrece un método para el desarrollo de la **firma digital** o resultado de cifrar con clave privada el resumen de los datos a firmar, haciendo uso de funciones resumen o *hash*, y garantizando la autenticación y el no repudio en el origen de los datos.

Otra de las aplicaciones del cifrado asimétrico es la creación y uso de **certificados digitales** o documentos electrónicos (archivos) que asocian una clave pública con la identidad de su propietario.

Una de sus aplicaciones más destacadas a nivel mundial es el **DNI electrónico (DNIe)** similar al tradicional y cuya principal novedad es que **incorpora** un pequeño circuito integrado (chip), capaz de guardar de forma segura información como el certificado digital del propietario.

Para el uso de certificados digitales confiables es necesario crear un modelo de confianza basado en Terceras Partes Confiables e implantar **Infraestructuras de Clave Pública** (ICP o PKI, *Public Key Infrastructures*), que incorporen autoridades de certificación y registro como intermediarios en el uso de certificados digitales.



EJERCICIOS PROPUESTOS

- 1. Investiga acerca de los distintos métodos de cifrado que se emplearon en la 2^a Guerra Mundial y concretamente sobre Enigma. ¿Cuál era su palabra clave?
- 2. Realiza un *script* para GNU/Linux que permita mediante un menú de opciones seleccionar entre los diferentes comandos (gpg simétrico, asimétrico, firma digital, revocación, publicación de claves públicas, etc.) y *scripts* (sustitución y transposición) que hemos visto a lo largo de las prácticas del capítulo.
- 3. Busca información acerca de qué es y para qué sirve la **esteganografía**. Introduce un mensaje de texto o una fotografía dentro de un archivo de música, imagen o vídeo, mediante algún software específico bajo Windows como PicCrypt, Xiao Steganography o SteganG o bajo GNU/Linux como OpenStego. Comprueba que es posible recuperar el mensaje o archivo oculto.
- 4. Revisa en la web www.camerfirma.com, uno de los usos que tiene el certificado digital para la firma y el envío de correos electrónicos con certificado digital, describe el proceso. ¿Qué garantiza? ¿Qué es S-MIME? Explica una posible utilidad que tendría el uso de certificado digital para minimizar el *spam*.
- 5. Busca qué Autoridades Certificadoras Admitidas de certificados digitales existen en España. Describe el proceso para la obtención del certificado digital, para ello visita la web www.fnmt.es. ¿Es válido para todos los navegadores web? ¿Puede emplearse para firmar otro tipo de archivos? ¿Es posible exportarlo o solamente se puede emplear en un solo equipo? ¿Qué precauciones podemos tener con el certificado digital en cuanto a protección mediante contraseñas en la exportación?
- 6. Realiza los trámites para la obtención de tu certificado digital.
 - ¿Dónde lo tienes que descargar? ¿Dónde tienes que ir a recogerlo? ¿Qué caducidad posee? Instálalo en Internet Explorer y Mozilla Firefox. Realiza una copia de seguridad con contraseña privada, y elimínalo de un PC inseguro al que puedan acceder otros usuarios. Una persona que acceda a nuestro equipo en el que tenemos instalado un certificado digital, ¿puede acceder a distintos sitios web de información personal de tipo legal?
- 7. Realiza una búsqueda de los servicios de empresas como bancos, y de la administración pública (seguridad social, hacienda, etc.) a los que se puede acceder de forma segura, mediante certificado digital y mediante DNIe.
 - En caso de disponer de certificado digital y/o DNI electrónico intenta acceder de forma segura a alguno de los servicios comentados e indica el proceso de acceso y las posibilidades que te ofrece el servicio. ¿Consideras estos servicios útiles para el ciudadano? ¿Para qué colectivos especialmente pueden ser útiles estas aplicaciones?
- 8. Qué diferencias existen entre la instalación de un certificado en un servidor web y un servidor de certificados. Busca cómo se instala y qué opciones ofrece el servidor de certificados integrado en el servidor IIS de Microsoft. Realiza una petición por parte de un cliente de un certificado digital.
- 9. Investiga acerca de la aplicación OpenSSL. ¿Qué tipo de algoritmos emplea? ¿Para qué sistemas operativos se encuentra disponible? ¿Qué utilidades posibilita?



TEST DE CONOCIMIENTOS

1

Indica qué sentencia es falsa con respecto al DNIe:

- a) Posee la misma utilidad en Internet que el DNI anterior.
- b) Posee mucho más nivel de seguridad que el anterior.
- c) Lo poseen actualmente muchas menos personas que el anterior.
- d) Exige un hardware bastante económico para emplearlo.

2

Con el certificado digital y el DNIe todavía no puedo realizar trámites como:

- a) Acceder a la declaración de la renta.
- b) Realizar devoluciones *online* de un producto.
- c) Averiguar mis datos de la Seguridad Social.
- d) Pedir una cita para el médico.

3

En un sistema criptográfico el aspecto más importante es:

- a) Longitud de la clave.
- b) La asimetría.
- c) La clave.
- d) Tiempo de cifrado.

4

¿Cuál de estos tipos de mecanismos de identificación no poseen validez alguna todavía?

- a) DNIe.
- b) Firma digitalizada.
- c) Firma digital.
- d) Certificado digital.

5

La codificación RSA-3, es un método:

- a) Asimétrico.
- b) Simétrico.
- c) Hash.
- d) Híbrido.

6

¿Qué tipo de cifrado se emplea en este comando gpg -c?

- a) Asimétrico.
- b) Simétrico.
- c) Hash.
- d) Firma digital.
- e) Híbrido.

7

¿Para qué se emplea este comando gpg -b?

- a) Cifrado Asimétrico.
- b) Cifrado Simétrico.
- c) Publicación de clave pública.
- d) Firma digital.
- e) Cifrado Híbrido.

8

¿Para qué se emplea este comando gpg --send-keys?

- a) Cifrado Asimétrico.
- b) Cifrado Simétrico.
- c) Publicación de clave pública.
- d) Firma digital.
- e) Híbrido.

the first time in the history of the world, the
whole of the human race has been gathered
together in one place.

It is a

place where
the whole
world is
represented.

It is a

place where
the whole
world is
represented.

It is a

place where
the whole
world is
represented.

It is a



6

Seguridad en redes corporativas

OBJETIVOS DEL CAPÍTULO

- ✓ Valorar los nuevos peligros derivados de la conexión a redes.
- ✓ Adoptar medidas de seguridad en redes corporativas o privadas tanto cableadas como inalámbricas.
- ✓ Analizar las principales vulnerabilidades de las redes inalámbricas.
- ✓ Comprender la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros.
- ✓ Conocer y emplear protocolos y aplicaciones seguras en comunicaciones.

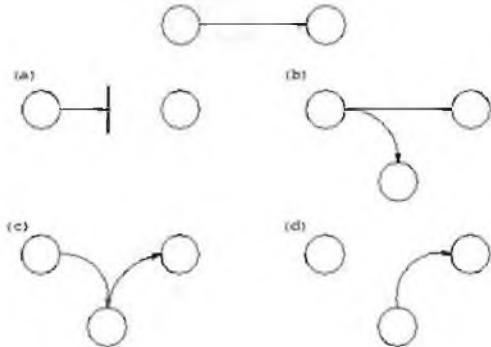
6.1 AMENAZAS Y ATAQUES

Sin importar si están conectadas por cable o de manera inalámbrica, las redes de ordenadores cada vez son más esenciales para las actividades diarias. Los ataques e intrusiones de personas no autorizadas a través de las redes públicas y privadas cada vez son más frecuentes, y pueden causar interrupciones costosas de servicios críticos y pérdidas de trabajo, información y dinero.

De forma genérica las **amenazas** en comunicaciones podemos dividirlas en cuatro grandes grupos:

- **Interrupción:** un objeto, servicio del sistema o datos en una comunicación se pierden, quedan inutilizables o no disponibles.
- **Interceptación:** un elemento no autorizado consigue un acceso a un determinado objeto.
- **Modificación:** además de conseguir el acceso consigue modificar el objeto, es posible incluso la **destrucción** una modificación que inutiliza al objeto afectado.
- **Fabricación:** modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el “fabricado”.

En la figura se muestran estos tipos de ataque de una forma gráfica:



Flujo normal de información entre emisor y receptor y posibles amenazas: (a) interrupción, (b) interceptación, (c) modificación y (d) fabricación

Como ejemplos prácticas de dichas amenazas, encontramos diversas **técnicas de ataques informáticos en redes**. Algunos son:

- **Ataque de denegación de servicio:** también llamado *ataque DoS (Deny of Service)*, es un caso específico de **interrupción** de servicio. Causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Mediante *botnet* o *redes zombi* se pueden llegar a controlar cientos o miles de máquinas para realizar ataques distribuidos de saturación de servidores o DDoS.
- **Sniffing,** es una técnica de **interceptación**: consiste en rastrear monitorizando el tráfico de una red.

- **Man in the middle:** a veces abreviado MitM, es un caso específico de **interceptación y modificación de identidad**. Un atacante supervisa una comunicación entre dos partes, falsificando las identidades de los extremos, y por tanto recibiendo el tráfico en los dos sentidos.
- **Spoofing:** es una técnica de **fabricación**, suplantando la identidad o realizando una copia o falsificación, por ejemplo encontramos falsificaciones de IP, MAC, web o mail.
- **Pharming:** es una técnica de **modificación**. Mediante la explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los propios usuarios, permite modificar las tablas DNS redirigiendo un nombre de dominio (domain name) conocido, a otra máquina (IP) distinta, falsificada y probablemente fraudulenta.



NOTICIA DE ACTUALIDAD

Analiza la noticia “*Tabnabbing; phishing a través de las pestañas del navegador*”, encontrada en <http://www.hispasec.com/unaaldia/4231>, e indica:

- ¿Qué tipo de amenaza de las anteriormente vistas supone el *Tabnabbing*? ¿Cómo funciona?
- ¿Qué tipo de medidas de precaución podemos tomar ante este tipo de amenaza?

A continuación veremos una serie de prácticas en las que se emplean dichas técnicas.

PRÁCTICA 6.1



Sniffing – MitM – ARP Spoofing - Pharming

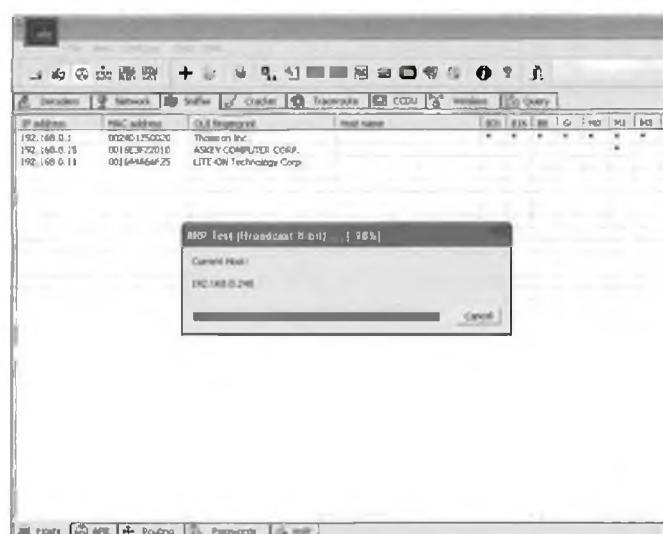
La monitorización del tráfico de red es un aspecto fundamental para analizar qué está sucediendo en la misma, y poder tomar precauciones y medidas de seguridad en la misma.

Herramientas como **Wireshark**, **NMAP** o **Cain & Abel** permiten realizar una monitorización de qué equipos se encuentran conectados en una red y qué puertos y aplicaciones utilizan.

En nuestro caso vamos a realizar una serie de prácticas que permiten ver las vulnerabilidades de protocolos como ARP y DNS, y de este modo tomar ciertas precauciones.

Emplearemos una herramienta para sistemas Windows denominada **Cain & Abel**, aunque para GNU/Linux podemos emplear Ettercap que posee similares prestaciones.

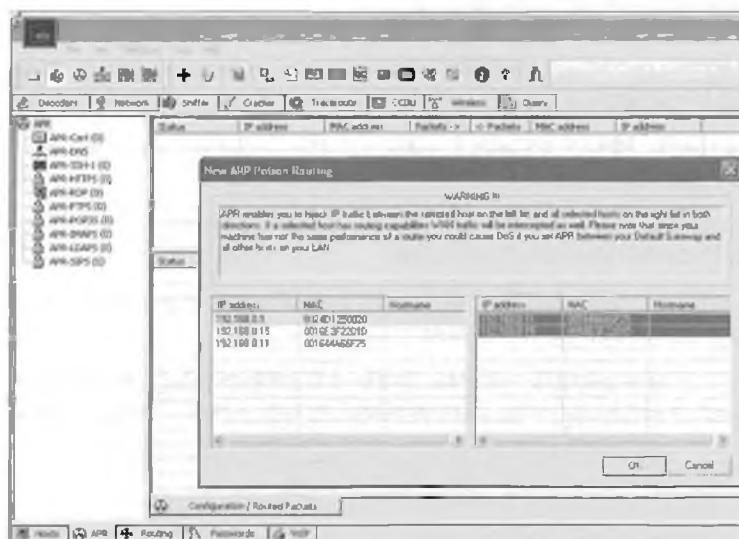
En primer lugar seleccionaremos la pestaña superior **Sniffer** y la inferior **Hosts**. Pulsaremos sobre el botón superior de **sniffing**, escaneará nuestra red local y nos dará información (IP y MAC) de qué equipos se encuentran en red con nuestro equipo.



ARP POISONING

El ARP *Spoofing*, también conocido como ARP Poisoning o ARP Poison Routing, es una técnica usada para infiltrarse en una red Ethernet commutada (basada en *switch* y no en *hubs*), que puede permitir al atacante monitorizar paquetes de datos en la LAN (red de área local), incluso modificar el tráfico.

El principio del ARP *Spoofing* es enviar mensajes ARP falsos (falsificados, o *spoofed*) a los equipos de la LAN. Normalmente la finalidad es **asociar la dirección MAC del atacante con la dirección IP de otro equipo**, como por ejemplo la puerta de enlace predeterminada (gateway). De esta forma cualquier tráfico dirigido a la dirección IP de ese equipo suplantado (por ejemplo el gateway), será enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a el equipo real (ataque pasivo o escucha, empleado en MitM) o modificar los datos antes de reenviarlos (ataque activo).



Para realizar un ataque ARP Poisoning o de envenenamiento ARP, seleccionamos la pestaña inferior APR, y pulsaremos el botón superior +. Seleccionaremos de los equipos de nuestra LAN, por qué equipo queremos hacernos pasar (columna izquierda) y en qué equipos queremos infectar su tabla ARP (columna derecha) con una entrada de nuestra MAC asociada a la IP del equipo a suplantar. En este caso el equipo por el que nos haremos pasar será la puerta de enlace (192.168.0.1), ya que la mayoría del tráfico irá dirigido a este equipo.

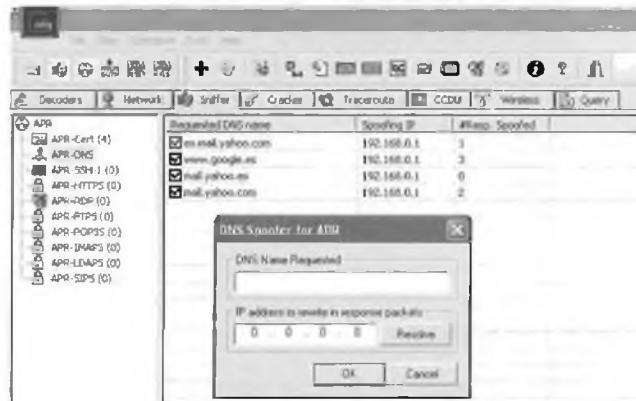


Podemos ver el antes y después de dicho envenenamiento en uno de los equipos infectados: 192.168.0.11. En primer lugar la MAC de la puerta de enlace o *router* era 00-24-d1-25-00-20, a continuación después de realizar el envenenamiento disponemos de 2 entradas con la misma MAC, del equipo que va a recibir todo el tráfico que vaya dirigido a la puerta de enlace.

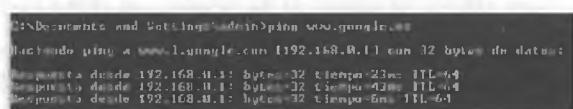
Mediante esta técnica es posible monitorizar el tráfico que va dirigido al *router* y rastrear protocolos no seguros como FTP, HTTP, POP, SMTP, Telnet o FTP, y de esta forma obtener credenciales.

PHARMING

Es posible realizar una inserción en las tablas locales de nombres de dominio, posibilitando un redireccionamiento a una IP con una web falsa. Seleccionando la pestaña inferior APR, y la opción APR-DNS podemos crear entradas de nombres de dominio con IP falsas.



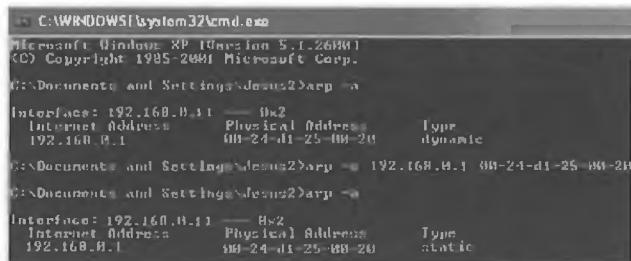
Vemos como después de realizar DNS *spoofing*, en unos de los equipos afectados, al hacer *ping* a google nos envía a una dirección IP falsa.



Las falsificaciones de sitios web donde se hacen uso de credenciales mediante formularios, ponen en peligro nuestras contraseñas y por tanto la privacidad e integridad de nuestros datos. En el ejemplo se han realizado falsificado webs de acceso a correo electrónico de yahoo.

Recomendaciones

Para evitar este tipo de ataques se recomienda entre otras acciones, el uso de **tablas ARP estáticas**, o al menos, entradas estáticas como la que da acceso a la puerta de enlace, ya que la mayoría del tráfico pasa a través de esta IP. Se puede realizar mediante el comando: arp -s IP MAC.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP Version 5.1.2600
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jesus2>arp -s
Interface: 192.168.0.1 --- Rx2
Internet Address Physical Address Type
192.168.0.1 00-24-d1-25-00-20 dynamic

C:\Documents and Settings\Jesus2>arp -s 192.168.0.1 00-24-d1-25-00-20
C:\Documents and Settings\Jesus2>
```

En redes grandes con gran cantidad de administración no es una buena solución, realizar esta configuración a mano. Para esos casos lo mejor es monitorizar los intentos de modificación de tablas ARP, por ejemplo mediante software específico de detección de intrusos (IDS) como **SNORT**, o específicos de intentos de duplicados ARP: bajo GNU/Linux **Arpwatch** o en Windows **DecaffeinatID** o realizar una monitorización específica mediante **Wireshark** que es capaz de detectar intentos de duplicados ARP.



En el caso de **DNS spoofing**, debemos tener especial precaución con las falsificaciones de sitios web, comprobando en los sitios web que enviamos credenciales (*mail*, redes sociales, banca, comercio *online*, etc.) que emplean protocolos seguros, como **HTTPS**, certificado digital que permite ver su autenticidad, y otros aspectos como la veracidad de su URL, o que nunca nos pedirán por otras vías de comunicación (*teléfono* o *mail*) el envío de dichas credenciales.

6.1.1 AMENAZAS EXTERNAS E INTERNAS

Las amenazas de seguridad causadas por intrusos en redes corporativas o privadas de una organización, pueden originarse tanto de forma interna como externa.

- **Amenaza externa o de acceso remoto:** los atacantes son externos a la red privada o interna de una organización, y logran introducirse desde redes públicas. Los objetivos de ataques son servidores y *routers* accesibles desde el exterior, y que sirven de pasarela de acceso a la redes corporativa.
- **Amenaza interna o corporativa:** los atacantes acceden sin autorización o pertenecen a la red privada de la organización. De esta forma pueden comprometer la seguridad y sobre todo la información y servicios de la organización.

Con estos 2 frentes abiertos, veremos por un lado como defender la **seguridad en la red corporativa** de forma interna (capítulo 6), y por otro como disponer de medidas de **protección perimetral** (capítulo 7), en los equipos y servicios que están expuestos a redes públicas.

Para protegernos de las posibles **amenazas internas** algunas propuestas son:

- ✓ Realizar un buen diseño de direccionamiento, parcelación y servicios de subredes dentro de nuestra red corporativa. Para ello se emplean técnicas como, subnetting, redes locales virtuales o VLAN y creación de zonas desmilitarizadas o DMZ, aislando y evitando que los usuarios puedan acceder directamente en red local con los sistemas críticos.
- ✓ Políticas de administración de direccionamiento estático para servidores y *routers*.
- ✓ Monitorización del tráfico de red y de las asignaciones de direccionamiento dinámico y de sus tablas ARP.
- ✓ Modificación de configuraciones de seguridad y, en especial contraseñas por defecto de la administración de servicios.
- ✓ En redes inalámbricas emplear máximo nivel de seguridad.

6.2 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Un sistema de detección de intrusos o IDS es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o *host*, aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, pero aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

Los tipos de IDS que encontramos son:

- **HIDS (Host IDS):** protegen un único servidor, PC o *host*. Monitorizan gran cantidad de eventos, analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción. Recaban información del sistema como ficheros, logs, recursos, etc., para su posterior análisis en busca de posibles incidencias.
- **NIDS (Net IDS):** protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son *sniffers* del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan en tiempo real todos los paquetes que circulan por un segmento de red aunque estos no vayan dirigidos a ese determinado dispositivo).

La arquitectura de un IDS, a grandes rasgos, está formada por:

- La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en *host*, el propio sistema.
- Reglas y filtros sobre los datos y patrones para detectar anomalías de seguridad en el sistema.
- Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía *mail*, o SMS.

Con respecto a la ubicación del IDS se recomienda disponer uno delante y otro detrás del cortafuegos perimetral de nuestra red, para obtener información exacta de los tipos de ataques que recibe nuestra red ya que si el cortafuegos está bien configurado puede parar o filtrar muchos ataques.

PRÁCTICA 6.2



IDS - SNORT

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc., conocidos. Todo esto en tiempo real.

Snort (<http://www.snort.org/>) está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y GNU/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Puede funcionar como *sniffer* (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis *offline*) o como un IDS normal (en este caso NIDS).

1. En primer lugar **instalaremos** la aplicación bajo GNU/Linux mediante: aptitude install snort.

2. Snort en modo *Sniffer* y registro de paquetes: snort -dev -l ./log -h 192.168.1.0/24.

En este modo (dev) visualizaremos las cabeceras de los paquetes TCP/IP, es decir, en modo *snifferSniffer*: modo verbose (v) mostrará las cabeceras IP, TCP, UDP y ICMP, visualizará los campos de datos que pasan por la interface de red (d), y las cabeceras a nivel de enlace (e).

Las opciones siguientes -l sirve para indicar el directorio de logs y -h para almacenar registros de tráfico de la red o *host* que se le indique.

3. **Filtros:** Para monitorizar tan sólo solo el tráfico descodado de un **determinado puerto**, se puede indicar por ejemplo: snort -vd host 192.168.1.5 and dst port 8080. En el cual solo se mostrará el tráfico del *host* 192.168.1.5 con puerto de destino 8080.

4. **IDS:** El modo detección de intrusos de red se activa añadiendo a la línea de comandos de snort la opción -c snort.conf. En este archivo, snort.conf, se guarda toda la configuración de las reglas, preprocesadores y otras configuraciones necesarias para el funcionamiento en modo NIDS. Por tanto podemos ejecutar: snort -dev -l ./log -h 192.168.1.0/24 -c ../etc/snort.conf.

5. **Modos de alerta:** Hay varias maneras de configurar la salida de las alertas, el modo en que se almacenarán éstas en el archivo alert.ids. Snort dispone de siete modos de alertas en la línea de órdenes: *completo*, *rápido*, *socket*, *syslog*, *smb* (WinPopup), *consola* y *ninguno*.

Como ejemplo, en modo de alerta completa (-A Full) nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen/destino e información completa de las cabeceras de los paquetes registrados.

```
snort -A full -dev -l ./log -h 192.168.1.0/24 -c ../etc/snort.conf
```

6.3

RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

TCP/IP es la arquitectura de protocolos que usan los ordenadores para comunicarse en Internet y, actualmente, casi en cualquier otra red. Emplean **puertos de comunicaciones o numeración lógica que se asigna para identificar cada una de las conexiones de red, tanto en el origen como en el destino**. No tiene ninguna significación física.

Los servicios de red más habituales tienen asignados los llamados *puertos bien conocidos*, por ejemplo el 80 para HTTP o web, el 21 para transferencia de ficheros FTP, el 23 para TELNET, etc.

Tabla 6.1

Rango	Puertos	Servicios sobre puertos bien conocidos
0-1023	Servicios bien conocidos	20 y 21: FTP 22: SSH comunicación cifrada 23: Telnet no cifrado 24: SMTP y 110: POP3 53: DNS
1024- 49151	Registrados	80: HTTP y 443 HTTPS cifrado
49152-65535	Dinámicos y/o privados	137,138,139: NetBIOS compartir archivos e impresora y 445: SMB

Los distintos sistemas y sus aplicaciones de red, ofrecen y reciben servicios a través de dichos puertos de comunicaciones. Solo a través de un conocimiento y análisis exhaustivo de los puertos y las aplicaciones y equipos que los soportan podemos asegurar nuestras redes. El análisis y control de los puertos se pueden realizar desde distintos frentes:

- En una **máquina local** observando qué conexiones y puertos se encuentran abiertos y qué aplicaciones los controlan.
 - El comando **netstat** permite ver el estado en tiempo real de nuestras conexiones.
 - Los **cortafuegos o firewall personales** son una medida de protección frente a ataques externos.
- En la **administración de red** para ver qué puertos y en qué estado se encuentran los de un conjunto de equipos.
 - La aplicación **nmap** permite un escaneo de puertos, aplicaciones y sistemas operativos, en un rango de direcciones.
 - Los **cortafuegos y proxys perimetrales** ofrecen protección mediante un filtrado de puertos y conexiones hacia y desde el exterior de una red privada.

Tras realizar un análisis exhaustivo a nivel de puertos, debemos proteger nuestras conexiones, haciéndolas seguras, por ejemplo cuando enviamos información confidencial.

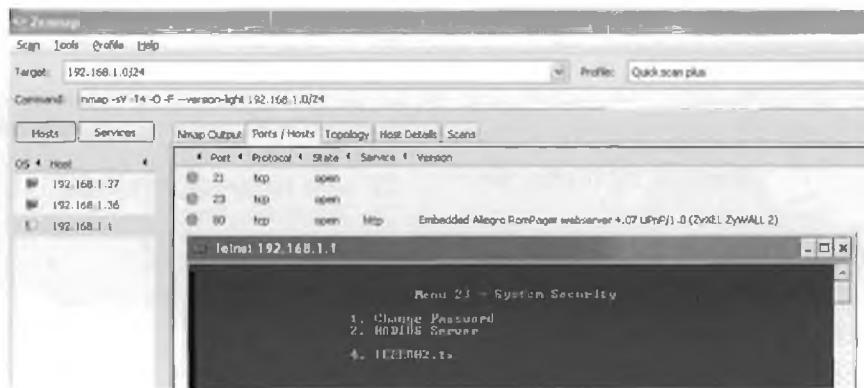
PRÁCTICA 6.3



ANÁLISIS DE PUERTOS

Mediante el comando **netstat** tanto en sistemas GNU/Linux como Windows podremos analizar el estado de nuestras conexiones y puertos. A modo de ejemplo bajo Windows netsat -anob, nos mostrará un listado completo mostrando número de puerto, estado (a la escucha, establecidas, o cerrados a la espera) y proceso responsable de dicho estado. En GNU/Linux las opciones más comunes del comando son netsat -atup.

Como vimos en el capítulo 1 **nmap** es una aplicación de gran utilidad en el análisis de puertos. Entre otras aplicaciones servirá para la administración de protocolos seguros en redes locales.



Tras realizar un análisis de nuestra red vemos como nmap nos muestra para la puerta de enlace 192.168.1.1, el modelo de fabricante de nuestro *router*, y los puertos y servicios que ofrece, ftp FTP (21), telnet/Telnet (23) y http (80). En numerosas páginas web y en las propias del fabricante a través de su manual de configuración, podemos encontrar listados con las contraseñas por defecto de usuarios de administración telnet y web.

Recomendación

Controlar el estado de conexiones, evitar protocolos inseguros como Telnet, y configuraciones y contraseñas por defecto, ya que en caso de que un atacante interno o externo pueda acceder a nuestra red o al control de un sistema importante, podrá efectuar una configuración no autorizada, o incluso una denegación de servicio.

6.4 COMUNICACIONES SEGURAS

La mayoría de las comunicaciones que empleamos en la red como HTTP, FTP o SMTP/POP, no emplean cifrado en las comunicaciones. Aunque existen protocolos que emplean comunicaciones cifradas como SSH a través del puerto 22, SSH, soportando incluso el envío seguro de archivos mediante SFTP.

Otras alternativas para establecer comunicaciones seguras entre 2 sistemas cifrando las comunicaciones a distintos niveles son:

SSL y TLS: *Secure Sockets Layer* -Protocolo de Capa de Conexión Segura- (**SSL**) y *Transport Layer Security* -Seguridad de la Capa de Transporte- (**TLS**), su sucesor. Se ejecutan en una capa entre los protocolos de aplicación y sobre el protocolo de transporte TCP. Entre otros se emplea a través de puertos específicos con: HTTPS , FTPS, SMTP, POP3, etc.

IPSEC o *Internet Protocol security*, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. Actúan en la capa 3 lo que hace que sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP. Una ventaja importante frente a otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio.

PRACTICA 6.4

SSH

SSH es un protocolo que permite acceder a máquinas remotas y ejecutar comandos a través de una red, mediante una comunicación segura cifrada a través del puerto 22. Permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves mediante certificados para no escribir contraseñas al conectar a los dispositivos y transferencia de datos de aplicaciones por un canal seguro tunelizado de forma sencilla.

En este caso práctico instalaremos un servidor de SSH al cual accederemos desde un intérprete de comandos desde GNU/Linux y desde Windows.

1. Para la instalación del servidor SSH en GNU/Linux abriremos la consola y escribiremos lo siguiente: `aptitude search ssh`

Con este comando estamos buscando algún paquete que coincida con nuestra búsqueda. Tras ejecutar dicha orden nos saldrán todos los posibles paquetes que tengan relación con el nombre del paquete que hemos introducido anteriormente. En la lista de paquetes encontrados, buscaremos el paquete “`openssh-server`” que será el que tengamos que instalar en la máquina que hará de servidor, una vez localizado el nombre exacto del paquete, escribiremos en la consola la siguiente orden: `aptitude install openssh-server`.

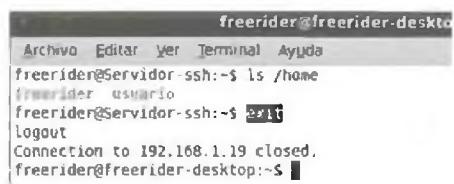
Una vez instalado el servidor, ya podemos acceder desde cualquier máquina de la LAN o de fuera de ella.

2. Para conectarnos al servidor de ssh que hemos instalado anteriormente, cogeremos una máquina cliente GNU/Linux distinta a la máquina en la que está corriendo el servidor de ssh, pero en red con ella. Realizaremos dicha operación mediante el siguiente comando: `ssh direccion_ip` (si está dentro de la misma red del servidor) o `ssh nombre_de_dominio` (si está en una red diferente a la del servidor).

Al iniciar la conexión nos pedirá la contraseña de un usuario válido en el servidor remoto.

Si la autenticación de la contraseña es correcta, ya podemos realizar cualquier acción en la máquina remota a través de la consola. Podemos apreciar que el nombre de la máquina cliente que aparece en el prompt ha cambiado por el nombre de la máquina servidora remota:

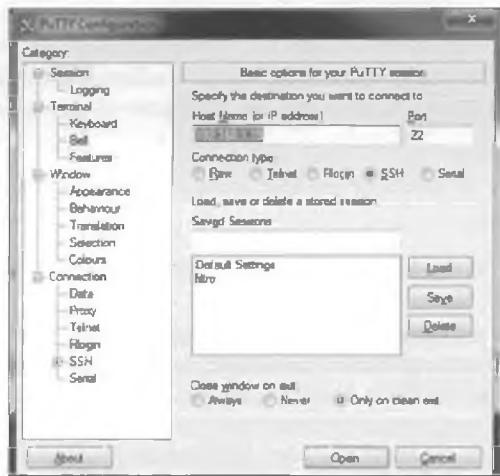
Una vez conectados, podremos ejecutar comandos como por ejemplo: listar los archivos que hay dentro del directorio “`home`” de la máquina remota:



Una vez finalizadas las acciones tendremos que desconectarnos del servidor ssh mediante la siguiente orden: exit. Al ejecutar dicha orden veremos como nos da una confirmación en la que nos dice que la conexión con la ip remota ha sido cerrada:

3. Si queremos realizar la conexión mediante un cliente bajo sistema operativo Windows, emplearemos el software específico **Putty**. Es un cliente SSH y telnet, de código abierto, podremos interactuar con la consola de Linux sin necesidad de estar en una máquina cliente con Linux.

Una vez instalado la configuración de la aplicación es sencilla. En la parte superior de la misma tenemos el campo "host name (or ip address)" en el que tenemos que introducir el nombre de la máquina remota o bien su dirección IP. Tras introducirlo pulsaremos en "Open":



Acto seguido, nos aparecerá una nueva ventana simulando una ventana de una consola de comandos. Introduciremos el usuario de la máquina remota y su contraseña respectiva. Tras introducir los datos de usuario nos aparecerá una confirmación de la conexión al servidor ssh, pudiendo de este modo ejecutar comandos remotamente.

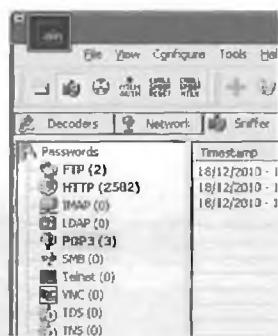


PRÁCTICA 6.5

TLS/SSL. PROTOCOLOS SEGUROS

Amenaza o vulnerabilidades

El software Cain & Abel para sistemas Windows permite en caso de realizar un ataque MitM, poder analizar el tráfico de una red local, identificar los mensajes y extraer credenciales de los protocolos que envían sus mensajes en texto plano, por ejemplo entre los más conocidos y empleados: FTP, POP3, SMTP, Telnet y HTTP.

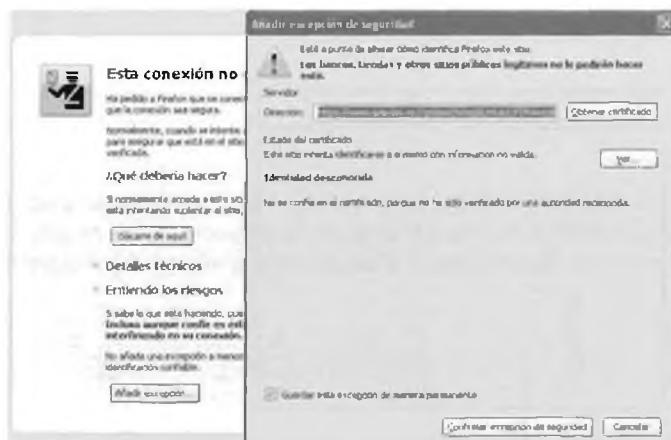


Recomendaciones

En esta práctica veremos distintos ejemplos de aplicación de protocolos seguros:

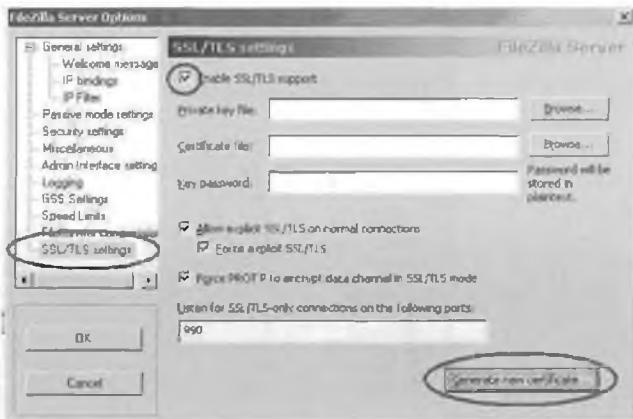
- ✓ **HTTPS:** siempre que visitemos una web en la que enviamos credenciales, verificar que se emplea el protocolo https. Para verificar la autenticidad y confiar en la web, los navegadores web obtienen un certificado SSL del sitio web. En caso de querer administrar una web segura deberemos obtener un certificado SSL para nuestra web, suministrado por una autoridad certificadora externa de confianza como lo son Verisign, Thawte, beTRUSTed o ValiCert.

En ocasiones los navegadores web dudan de la veracidad de los certificados SSL, en ese caso debemos añadir una excepción de seguridad en caso de confiar en el sitio web. De ese modo el navegador web añadirá dicha excepción y confiará en el sitio para próximas visitas.



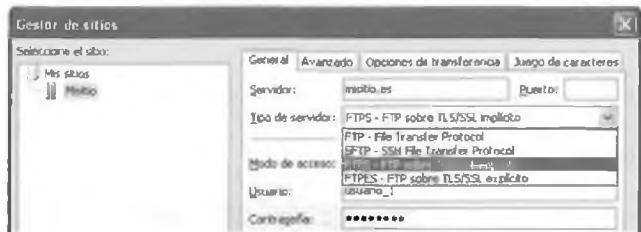
- ✓ **FTP seguro:** la mayoría de los servidores y clientes FTP soportan conexiones seguras, cifradas sobre SSH y TLS/SSL. Veamos como podemos configurar en un servidor FTP administrado las opciones de seguridad SSL. La configuración se realizará sobre el servidor FTP gratuito **Filezilla Server**.

1. En primer lugar configuraremos SSL en Options - SSL/TLS settings. Marcaremos todas las opciones y generar certificado con Generate new certificate. Seleccionamos la opción de longitud de clave, y rellenamos los campos para la creación del certificado y se especificará la ruta al certificado. Una vez generado asignaremos puerto de escucha alternativo para las conexiones seguras en Listen for SSL/TLS-only connections... (pe. el 990).



A continuación para los usuarios que se deseen conectar mediante soporte SSL/TLS, debemos de marcar la casilla Force SSL for user login en sus opciones de contraseña.

2. En la mayoría de **clientes FTP**, las opciones de configuración de cuentas de usuario FTP, permiten conexiones seguras mediante SSH y SSL/TLS.



Al intentar conectarnos mediante TLS/SSL nos mostrará una pantalla para aceptar el certificado del servidor, si confiamos lo aceptaremos, haciendo que dicha conexión vía FTP sea cifradas y no viajarán datos en texto plano.

3. En caso de no poder configurar las opciones en el servidor TLS/SSL por disponer de un alojamiento con opciones reducidas, es posible al menos emplear en la mayoría de los casos, como opción segura SFTP a través de SSH. En la mayoría de los casos usuario y contraseña se corresponden con los de FTP.



- Correo electrónico: en las cuentas de correo es recomendable revisar la configuración y sus opciones para que siempre empleen https.

Para la configuración de cuentas de *mail* a través de clientes de escritorio algunos servidores como gmail comienzan a requerir el uso de puertos y protocolos de transferencia seguros mediante SSL:

Cuenta de Correo: *usuario@gmail.com*.

Datos POP: Servidor: *pop.gmail.com*. Usar SSL: Sí. Puerto: 995.

Datos SMTP: Servidor: *smtp.gmail.com*. Usar TLS / SSL: Sí. Puerto: 465 ó 587.

Recomendación

Siempre que tengamos que configurar servicios tanto clientes como servidores, que requieran el uso y envío de contraseñas, es recomendable el uso de configuraciones y puertos que transmitan sus mensajes cifrados.

6.4.1 VPN

Una red privada virtual o VPN (*Virtual Private Network*), es una tecnología de red que permite una **extensión de una red local** de forma segura sobre una red pública, como Internet.

Algunas aplicaciones de dicha tecnología son la posibilidad de conectar utilizando la infraestructura de Internet, dos o más sucursales de una empresa, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de trabajo, etc. Para hacerlo posible de **manera segura** es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

- **Autenticación y autorización:** se controlan los usuarios y/o equipos y qué nivel de acceso debe tener.
- **Integridad:** los datos enviados no han sido alterados, se utilizan funciones resumen o hash, como MD5 y SHA.
- **Confidencialidad:** que la información que viaja a través de la red pública solo puede ser interpretada por los destinatarios de la misma. Para ello se hace uso de algoritmos de cifrado como DES, 3DES y AES.
- **No repudio:** los mensajes tienen que ir firmados.

Básicamente existen tres arquitecturas de conexión VPN:

- **VPN de acceso remoto:** el modelo más usado, usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas públicas compartidas, domicilios, hoteles, etc.) utilizando Internet como vínculo de acceso.

- **VPN punto a punto:** conecta ubicaciones remotas como oficinas, con una sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Mediante la técnica de **tunneling** se encapsulará un protocolo de red sobre otro creando un túnel dentro de una red.
- **VPN over LAN:** es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Emplea la misma red de área local (LAN) de la empresa, aislando zonas y servicios de la red interna, a los que se les puede añadir cifrado y autenticación adicional mediante VPN. Permite también mejorar las prestaciones de seguridad de las redes inalámbricas, haciendo uso de túneles cifrados IPSEC o SSL que agregan credenciales de seguridad del propio túnel VPN.

El protocolo estándar que utiliza VPN es IPSEC, pero también trabaja con PPTP, L2TP, SSL/TLS, SSH, etc. Dos de las tecnologías más utilizadas para crear VPN's, en realidad son diferentes protocolos o conjuntos de protocolos, PPTP y L2TP:

- **PPTP o Point to Point Tunneling Protocol:** es un protocolo desarrollado por Microsoft y disponible en todas las plataformas Windows. Es sencillo y fácil de implementar pero ofrece menor seguridad que L2TP.
- **L2TP o Layer Two Tunneling Protocol:** Se trata de un estándar abierto y disponible en la mayoría de plataformas Windows, Linux, Mac, etc. Se implementa sobre IPSEC y proporciona altos niveles de seguridad. Se pueden usar certificados de seguridad de clave pública para cifrar los datos y garantizar la identidad de los usuarios de la VPN.

PRÁCTICA 6.6

CONEXIÓN REMOTA CON VPN

En este caso práctico instalaremos un **servidor de VPN** en los sistemas operativos Windows y GNU/Linux mediante el programa **Logmein Hamachi** que permite la comunicación entre 2 máquinas remotas mediante VPN de manera fácil y sencilla.

A cada cliente Hamachi se le asigna una dirección de la red 5.0.0.0 Esta dirección es asignada cuando el cliente se autentifica en el sistema la primera vez, y es en adelante asociada con la clave de cifrado pública del cliente. Mientras el cliente retenga esta clave, puede autenticarse en el sistema y utilizar esa dirección IP 5.X.X.X. La red 5.0.0.0/8 es utilizada para evitar colisiones con redes IP privadas que podrían estar utilizándose en la parte cliente. El bloque de direcciones 5.0.0.0 está reservado por la IANA y no está actualmente en uso en el dominio de encaminamiento de Internet, pero no está garantizado que esto continúe así en el futuro.

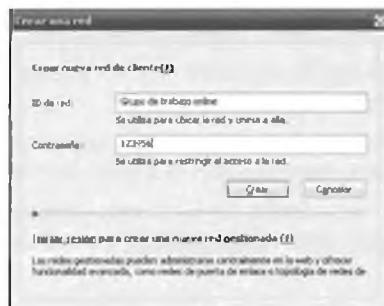
1. Antes de empezar la instalación es necesario **registrarse en la página** web de Logmein para tener acceso al instalador del programa y poder usar dicha aplicación más adelante.

<https://secure.logmein.com/ES/products/hamachi2/download.aspx>

La aplicación se ofrece de dos modos, con gestión o sin gestión. En nuestro caso elegiremos la opción "con gestión" para disfrutar de todas las utilidades de esta aplicación. Acto seguido crearemos la cuenta de usuario pulsando el botón "Crear cuenta". Crearemos la cuenta de usuario con los datos de formulario requeridos, y con la cuenta activa, volveremos a entrar en la web, accederemos a nuestra cuenta e iremos a la sección "products" / "logmein Hamachi". Una vez dentro de la página de la aplicación, pulsaremos en "get started" para obtener el instalador. Tras esto pulsaremos en "download now" para obtener el instalador.

2. Realizaremos la **instalación**, y ejecutaremos la aplicación para empezar a crear nuestra red VPN. Para ello ejecutaremos el programa y pulsaremos en la opción “Crear una nueva red”:

Para crear la nueva red tendremos que insertar un nombre para la red y una contraseña para evitar que se añadan usuarios ajenos a nosotros. Tras llenar los campos, pulsaremos en “crear”.



Una vez creada la red veremos como el menú principal de Hamachi muestra directamente la red que acabamos de crear:



Con esto ya disponemos de un servidor VPN a la escucha de peticiones cliente.

3. Para conectarnos desde otro ordenador en una ubicación distinta de nuestra LAN, ejecutaremos la misma aplicación que efectuará el papel de cliente en otro ordenador. Seleccionaremos la opción de menú “Red” y “Unirse a una red existente”:



En la siguiente ventana tendremos que insertar el id de red que hemos creado anteriormente y la contraseña. Tras esto pulsaremos en “unirse”. De esta forma ya estamos agregados a la red virtual:



Una vez conectados de forma segura entre 2 equipos, podemos compartir archivos, ejecutar aplicaciones de forma compartida, entre otras opciones, de la misma forma que lo haríamos en una LAN.

Pulsando con el botón derecho sobre el nombre del equipo que queramos realizar la acción, nos mostrará un menú con las opciones disponibles, por ejemplo Explorar, para buscar archivos y carpetas compartidas.

4. Cliente GNU/Linux Hamachi. Para la instalación descargar el paquete que permitirá instalar la aplicación de la web del fabricante. Tras esto descomprimir el fichero en una carpeta e instalarlo, mediante el comando `make install`, contenido en la carpeta hamachi-version-lnx.

Sin movernos el mismo directorio de la carpeta donde hemos descomprimido todos los ficheros, iremos al directorio tuncfg, para ejecutar el cliente: `./tuncfg`.

A continuación generamos la información de la cuenta: hamachi-init.

Arrancamos el servicio de hamachi con la siguiente orden: `hamachi start`. Tras esto ponemos el servicio en línea con la siguiente orden: `hamachi login`.

Para añadirnos a la red que hemos creado en windows lo haremos de la siguiente manera. En primer lugar definimos nuestro nombre a nuestra máquina con la orden: `hamachi set-nick Linux`.

Posteriormente, entraremos a la red creada en windows: `hamachi join nombre_de_red password`, para nuestro caso nombre de red: Grupo de trabajo *online* y contraseña 123456. A continuación nos indicará `Joining Grupo de trabajo online .. ok`

Para aparecer conectado en la red virtual utilizaremos la siguiente orden: `hamachi go-online nombre_de_red`

Verificamos los usuarios de la red y su status mediante: `hamachi list`.

6.5 REDES INALÁMBRICAS

En los últimos años ha irrumpido con fuerza, en el sector de las redes locales, las **comunicaciones inalámbricas**, también denominadas *wireless*. La tecnología inalámbrica ofrece muchas **ventajas** en comparación con las tradicionales redes conectadas por cable.

- Una de las principales ventajas es la capacidad de brindar **conectividad en cualquier momento y lugar**, es decir mayor disponibilidad y acceso a redes.
- La **instalación** de la tecnología inalámbrica es **simple y económica**. El coste de dispositivos inalámbricos domésticos y comerciales continúa disminuyendo.
- La tecnología inalámbrica permite que las redes se amplíen fácilmente, sin limitaciones de conexiones de cableado, por lo que es fácilmente **escalable**.

A pesar de la flexibilidad y los beneficios de la tecnología inalámbrica, existen algunos **riesgos y limitaciones**.

- Utilizan rangos del espectro de radiofrecuencia (RF) **sin costes de licencia** por su transmisión y uso. Estos rangos al ser de uso público están saturados y las señales de distintos dispositivos suelen interferir entre sí.
- El área problemática de la tecnología inalámbrica es la **seguridad**. Permite a cualquier equipo con tarjeta de red inalámbrica interceptar cualquier comunicación de su entorno.

Para tratar estas cuestiones de seguridad se han desarrollado técnicas para ayudar a proteger las transmisiones inalámbricas, por ejemplo la **encriptación** y la **autenticación**. A pesar de las siguientes técnicas que se presentan a continuación, y de los problemas propios asociados a las comunicaciones cableadas (fibra, cable de pares, coaxial) como las interferencias y deterioros o daños físicos del material, éstas siguen siendo los medios de acceso físico más seguros que existen en la actualidad.

6.5.1 SISTEMAS DE SEGURIDAD EN WLAN

Los sistemas de cifrado empleados para autenticación como encriptación en redes inalámbricas son:

- **Sistema abierto u Open System:** es decir sin autenticación en el control de acceso a la red, normalmente realizado por el punto de acceso, ni cifrado en las comunicaciones.
- **WEP o Wired Equivalent Privacy o Privacidad Equivalente a Cableado:** sistema estándar diseñado en la norma básica de redes inalámbricas 802.11. Emplea para la encriptación de los mensajes claves de 13 (104 bits) o 5 (40 bits) caracteres, también denominadas WEP 128 o WEP 64 respectivamente. Existen también dispositivos que permiten configuraciones de 152 y 256 bits. En cuanto a la autenticación existen 2 métodos:
 - **Sistema abierto u Open system,** el cliente no se tiene que identificar en el Punto de Acceso durante la autenticación. Después de la autenticación y la asociación a la red, el cliente tendrá que tener la clave WEP correcta.
 - **Claves precompartida, Pre-Shared Keys o PSK.** En la autenticación mediante clave precompartida, se envía la misma clave de cifrado WEP para la autenticación, verificando y controlando el acceso de este modo el punto de acceso.

Es aconsejable usar la autenticación de sistema abierto para la autenticación WEP, ya que es posible averiguar la clave WEP interceptando los paquetes de la fase de autenticación.

- **WPA o Wi-Fi Protected Access o Acceso Protegido Wi-Fi:** creado para corregir las deficiencias del sistema previo WEP. Se han realizado 2 publicaciones del estándar WPA como solución intermedia, y el definitivo WPA2 bajo el estándar 802.11i. Se proponen 2 soluciones según el ámbito de aplicación:
 - **WPA Empresarial o WPA-Enterprise** (grandes empresas): la autenticación es mediante el uso de un servidor RADIUS, donde se almacenan las credenciales y contraseñas de los usuarios de la red.
 - **WPA Personal** (pequeñas empresas y hogar): la autenticación se realiza mediante clave precompartida, de un modo similar al WEP.

Una de las mejoras de WPA sobre WEP, es la implementación del protocolo de integridad de clave temporal (**TKIP - Temporal Key Integrity Protocol**), que **cambia claves dinámicamente** a medida que el sistema es utilizado.

Aportando un mayor nivel de seguridad en el cifrado, es posible emplear el algoritmo de cifrado simétrico **AES**, más robusto y complejo que **TKIP**, aunque su implementación requiere de hardware más potente por lo que no se encuentra disponible en todos los dispositivos.

Aunque WPA es indiscutiblemente el sistema más seguro, uno de los grandes problemas que se plantea es la compatibilidad y disponibilidad de las distintas versiones y algoritmos de cifrado del mismo.

PRÁCTICA 6.7

WEP

Actualmente realizar **auditorías wireless** para medir el nivel de seguridad de nuestras redes inalámbricas es una práctica esencial como administrador en las corporaciones. Existen multitud de aplicaciones que permiten monitorizar y recuperar contraseñas de redes inalámbricas (*airodump*, *aircrack*, etc.), así como distribuciones Live (Backtrack, Wifiway, Wifislax, etc.) que las incorporan y disponen de *script* o aplicaciones que automatizan el proceso de desencriptado de contraseñas.

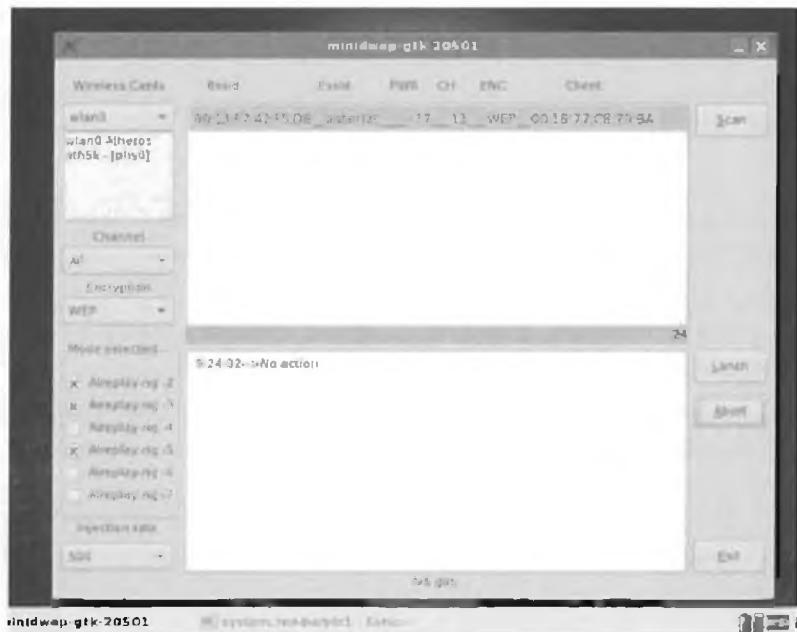
1. En nuestra práctica vamos a comprobar la vulnerabilidad de las claves WEP utilizando la distribución Live Wifiway 2.0 que contiene la aplicación **Minidwep-gtk** que nos ayudará a desencriptar dicha clave. Con el sistema iniciado nos dirigimos al menú principal - wifiway - suite aircrack-ng - minidwep-gtk. Al abrir la aplicación nos aparecerá lo siguiente:

En la columna de la izquierda tenemos una opción: "wireless cards", en la que podemos seleccionar la tarjeta de red que deseemos en caso de tener 2 o más tarjetas instaladas en nuestra máquina.

En la misma columna tenemos las opciones del canal "Channel". Podemos elegir en qué canal queremos hacer el rastreo de redes inalámbricas.

Encryption permite seleccionar el tipo de encriptación de las redes que se mostrarán en la lista de redes.

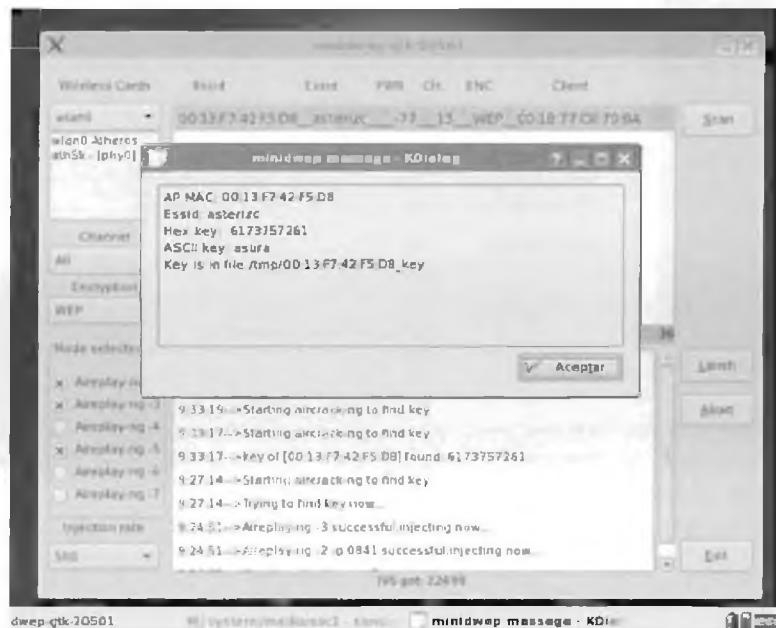
2. A continuación realizaremos el escaneo con el botón "Scan", en la parte superior tendremos la lista de redes inalámbricas que capta nuestra tarjeta de red inalámbrica. En esta lista se especifica la dirección MAC del punto de acceso, su nombre, la potencia con que captamos la señal, el canal que usa para transmitir y el tipo de encriptación.



3. Una vez escaneadas las redes, seleccionaremos la red de la que queremos descifrar su contraseña y pulsaremos el botón "Launch".

Dependiendo de la calidad de la señal, la distancia al punto de acceso, el tráfico en la red inalámbrica por parte de otros equipos conectados y las características de nuestra tarjeta de red inalámbrica, tendremos que esperar más o menos tiempo hasta que la aplicación recoja suficientes paquetes de información, en los que se incluyen vectores de inicialización o IVs, que les permitan descifrar la clave de dicha red.

- La aplicación realizará de forma automática una serie de acciones para la recogida masiva de paquetes, en el caso de que todo vaya bien, nos mostrará una ventana que contiene un resumen de las acciones realizadas así como la clave descifrada en código ASCII:



Recomendación

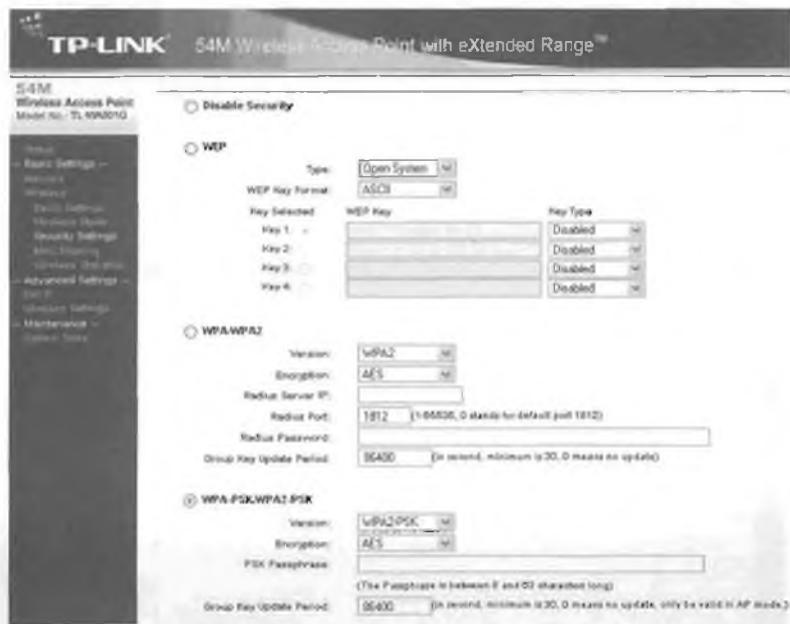
Configurar el nivel de seguridad más alto posible, controlar periódicamente los usuarios autorizados conectados, y renovar periódicamente las contraseñas.

PRÁCTICA 6.8

WPA

Una configuración más segura que WEP, la proporciona WPA. Para familiarizarnos con la configuración de los puntos de acceso inalámbricos emplearemos un simulador de configuración del dispositivo TP-LINK TL-WA501G. Para ello accederemos a la web:

<http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm>, y en su sección Gireles, visualizaremos las opciones de Security Settings:



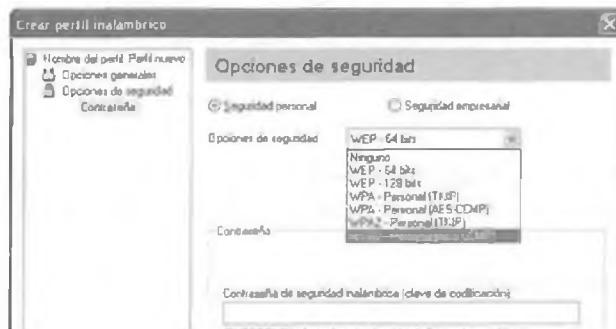
- Vemos en su sección **Security Settings** como es posible deshabilitar la seguridad, o elegir entre WEP, WPA/ WPA2 con servidor Radius, y WPA/WPA2 – PSK es decir con clave precompartida, en las que será posible indicar una clave de cifrado.

Entre las opciones WEP, podemos seleccionar el método de autenticación: Automático, sistema abierto o *shared key*.

En las opciones WPA encontramos tanto para la configuración personal como enterprise, podemos seleccionar la versión WPA o WPA2, y el algoritmo de cifrado TKIP o AES, así como el tiempo de actualización dinámica de la clave (*group key update period*).

Para el caso de WPA con autenticación mediante servidor Radius podemos indicarle la IP de la máquina y el puerto del servicio de autenticación.

- En la configuración de la tarjeta de red de los **clientes inalámbricos**, debemos especificar las opciones de configuración adecuadas. Vemos a continuación las opciones de configuración WPA de una tarjeta de red Intel(R) PRO/Wireless 3945ABG Net.



PRÁCTICA 6.9

SERVIDOR DE AUTENTICACIÓN RADIUS

Una opción más segura que permita controlar la autenticación de usuarios se puede realizar mediante la configuración de un servidor Radius. Radius o Remote Authentication Dial-In User Server, es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza los puertos 1812 y 1813 UDP para establecer sus conexiones.

En esta práctica realizaremos la instalación y configuración de un servidor Radius bajo GNU/Linux llamado **freeradius**, para autenticar conexiones que provienen de un punto de acceso Linksys WRT54GL.

- La instalación del paquete se realiza mediante: `aptitude install freeradius`. Tras la instalación tendremos que **configurar los usuarios** que se autenticarán en radius. Esta autenticación se realiza a través del fichero `/etc/freeradius/users` que contiene, en texto plano, los usuarios que tienen permitida la autenticación. Algunos usuarios se encuentran preconfigurados, podremos añadir las líneas de usuarios que deseemos.

En dicho fichero introduciremos los usuarios que queremos autenticar y sus respectivas contraseñas tal y como muestra la imagen:

```

# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name.
"John Doe"
    Cleartext-Password := "Hello"
    Reply-Message = "Hello, %{User-Name}!"

"Juanma"
    Cleartext-Password := "mama"
    Reply-Message = "Hello, %{User-Name}"
"Macarena"
    Cleartext-Password := "mama"
    Reply-Message = "Hello, %{User-Name}"

```

En nuestro caso introducimos el usuario Juanma y Macarena con sus respectivas contraseñas en texto plano.

- Ahora tendremos que **configurar los clientes**, es decir, los puntos de acceso serán los clientes de nuestro servidor radius.

Para introducir la información sobre los clientes (puntos de acceso que solicitarán la verificación de usuarios inalámbricos finales) en la configuración de Radius modificaremos el archivo `/etc/freeradius/clients.conf` donde introduciremos la información de las IP de los puntos de acceso que quieran emplear el servidor (192.168.1.2 en nuestro caso), así como la contraseña entre punto de acceso y servidor (`secret = futbol`), y el nombre de la red o SSID (`shortname = punxos`) tal como muestra la siguiente imagen:

```

client 192.168.0.97/24 {
    secret = testing123
    shortname = private-network-1
}

client 192.168.0.98/24 {
    secret = testing123-2
    shortname = private-network-2
}

client 192.168.0.99/24 {
    secret = futbol
    shortname = private-network-3
}

```

Reiniciamos el servidor Radius mediante la siguiente orden: `service freeradius restart`.

3. A continuación configuraremos el **punto de acceso** de manera que la autenticación la realice Radius. En nuestro caso accedemos a la sección “wireless security” del punto de acceso para configurar una clave WPA2enterprise y las distintas opciones para Radius:

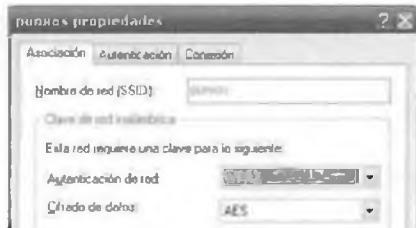


El servidor Radius como vemos se encuentra disponible en la IP 192.168.1.19, la contraseña futbol, el puerto 1812 y los algoritmos de cifrado TKIP + AES.

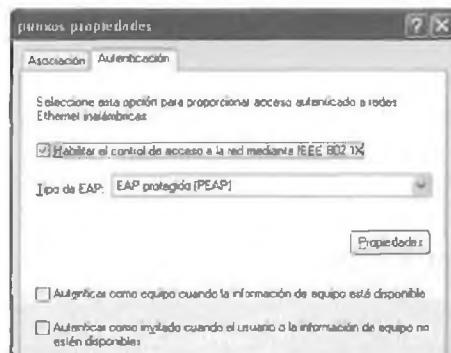
4. Por último, solo queda configurar en **el usuario cliente** final (tarjeta de red inalámbrica) la conexión al punto de acceso de manera que la autenticación pase a Radius. Para la configuración de un cliente windows xp tendremos que buscar la red mediante el asistente de conexión inalámbrica de Windows (en nuestro caso punxos).

Si intentamos realizar una conexión con el punto de acceso, nos bloqueará la conexión ya que detectará que hay un servidor de Radius en la red y el perfil de conexión del cliente no está configurado para autenticación en Radius. Para solucionar este problema entraremos en las propiedades del adaptador wireless y nos dirigimos a la sección “redes inalámbricas”, y configuraremos una nueva configuración o perfil para el SSID concreto (en este caso punxos).

En la configuración de la red, en la sección **Asociación** tenemos que seleccionar una autenticación de red “WPA2” y el cifrado de datos “AES”:



En la pestaña **Autenticación** seleccionaremos las opciones que aparecen en la imagen siguiente.



Pulsamos el botón de *Propiedades* y deseleccionamos la opción que dice “validar un certificado del servidor”. En el caso de querer dicha opción tendriamos que habilitar uno en nuestro servidor en */etc/freeradius/certs*.

Pulsamos el botón “Configurar”, y no activaremos la opción, para que el servidor Radius no acepte automáticamente el usuario y *password* de inicio de sesión en Windows.

Tras esto, guardamos los cambios y nos volvemos a conectar al punto de acceso. Ahora nos pedirá el usuario y contraseña para poder autenticarlo en el servidor Radius.

6.5.2 RECOMENDACIONES DE SEGURIDAD EN WLAN

Dado que el acceso a redes inalámbricas plantea un punto muy débil de seguridad en redes corporativas algunas recomendaciones para mejorar la seguridad son:

- Asegurar la administración del punto de acceso (AP), por ser un punto de control de las comunicaciones de todos los usuarios, y por tanto crítico en la red, cambiando la contraseña por defecto. Actualizar el firmware disponible del dispositivo para mejorar sus prestaciones, sobre todo de seguridad.
- Aumentar la seguridad de los datos transmitidos: usando encriptación WEP o WPA/WPA2 o servidor Radius, y cambiando las claves regularmente.
- Cambia el SSID por defecto y desactiva el broadcasting SSID. Los posibles intrusos tendrán que introducir manualmente el SSID y conocerlo previamente. Aunque la administración de los clientes se complica ya que deberán conocer el nombre exacto del SSID.
- Realizar una administración y monitorización minuciosa:
 - Desactivar el servidor DHCP, y asignar manualmente en los equipos las direcciones IP. Cambiar las direcciones IP del punto de acceso y el rango de la red por defecto.
 - Activar el filtrado de conexiones permitidas mediante direcciones MAC.
 - Establecer un número máximo de dispositivos que pueden conectarse.
 - Analizar periódicamente los usuarios conectados verificando si son autorizados o no.
- Desconexión del AP cuando no se use.
- Actualizar el firmware del dispositivo, para evitar vulnerabilidades o añadir nuevas funciones de seguridad.

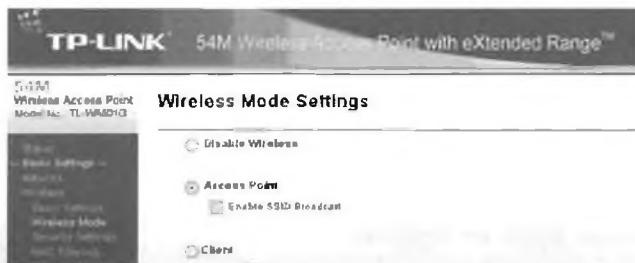
PRÁCTICA 6.10



CONFIGURACIÓN AP SEGURO

Veremos a modo de ejemplo en el simulador de TP-Link <http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm>, como realizar dichas configuraciones:

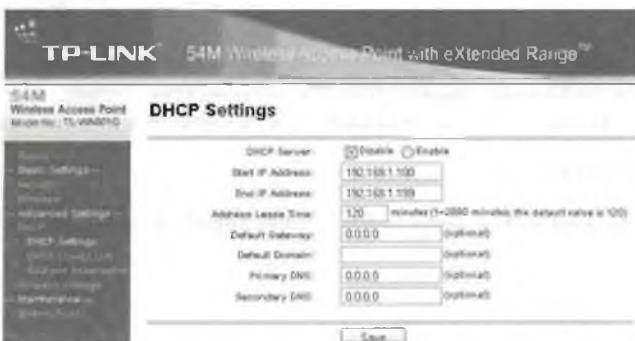
- Deshabilitar el envío del nombre de la red SSID:

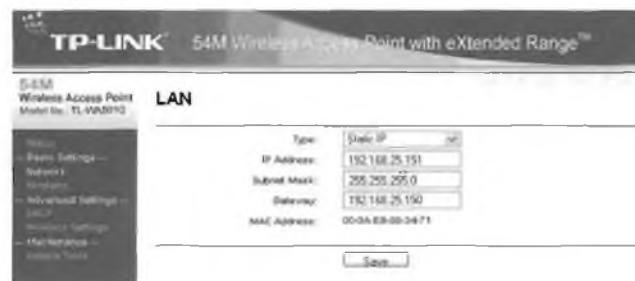


- Modificar el nombre de usuario y su contraseña por defecto de administrador:

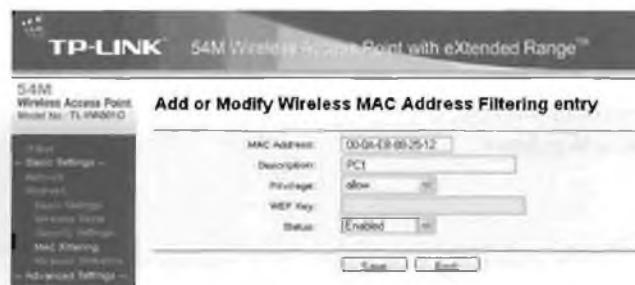


- Deshabilitar el servidor DHCP y reasignación de direcciones IP estáticas en una red diferente a la por defecto (normalmente 192.168.0.0 o 192.168.1.0), estamos suponiendo que el punto de acceso no realiza enruteado por lo que no es la puerta de enlace de nuestra red. IP de configuración del AP 192.168.25.151, la puerta de enlace deberá configurarse de forma independiente.

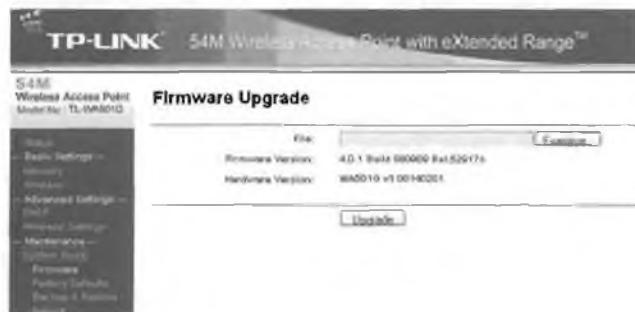




- ✓ Filtrado de MAC: añadiremos las MAC de los dispositivos (previamente inspeccionaremos la MAC en las tarjetas de red inalámbricas) que queremos permitir (privilege = allow) el acceso a la red.



- ✓ Actualización del firmware: es posible descargar de la web del fabricante un archivo, o incluso probar algún software alternativo como **OpenWrt**, **DDWRT** o **Tomato**. Se recomienda siempre realizar previamente una copia de seguridad del firmware actual.



6.6 REFERENCIAS WEB

- Curso abierto con materiales y ejercicios sobre Seguridad Avanzada en Redes:
http://ocw.uoc.edu/informatica-tecnologia-y-multimedia/aspectos-avanzados-de-seguridad-en-redes/Course_listing
- Sitio web sobre seguridad informática en materia de redes:
<http://www.virusprot.com/>
- Noticias sobre seguridad en redes. Asociación de internautas:
<http://seguridad.internautas.org/>
- Conexiones inalámbricas seguras y auditorías wireless en:
<http://www.seguridadwireless.net/>
- Blog especializado en seguridad y redes:
<http://seguridadyredes.nireblog.com/>

RESUMEN DEL CAPÍTULO

A finales del siglo XX y principios del XXI las redes han significado una verdadera revolución tecnológica, a la que millones de usuarios se han unido. Nuevos peligros han surgido como la falsificación (*spoofing*) de identificadores de red y sitios web, ataques de denegación de servicio Dos y DDos y la interceptación del tráfico de red mediante *sniffing* con Man in the Middle.

En este capítulo se han analizado las diferentes técnicas para evitar dichos ataques en redes corporativas, producidos por atacantes internos. Algunas de ellas son, aparte de revisar las configuraciones y contraseñas por defecto de routers y servidores:

- Emplear protocolos seguros cifrados como SSH, los proporcionados por la capa TLS/SSL y VPN para conexiones entre ubicaciones remotas.
- Realizar periódicamente un análisis del tráfico de red mediante *sniffer* y software de detección de intrusos (IDS).
- Evitar accesos no autorizados a la red corporativa, empleando redes cableadas o en todo caso, dado el desarrollo de redes wireless, debido a su facilidad de instalación y bajo coste, emplear mecanismos de seguridad como direccionamiento estático, filtrado MAC y sistemas WEP, WPA y WPA2. En grandes organizaciones se recomienda el uso de servidores de autenticación RADIUS.



EJERCICIOS PROPUESTOS

- 1. Realiza una investigación sobre qué puertos de comunicaciones son más vulnerables, realizando un escaneo de puertos y analizando la información que ofrecen los siguientes enlaces:

<http://www.internautas.org/w-scanonline.php>
<http://www.upseros.com/portscan.php>
<http://www.kuron.com/utils/portscanner/index.php>

- ¿Tienes cerrados los puertos empleados frecuentemente por el *malware*? ¿Qué IP visualiza el escáner de puertos? ¿Es tu conexión a Internet directa, o mediante un *router*? Compara la dirección IP de tu tarjeta de red y la que aparece en el escaneo de puertos.
- ¿Para qué sirven los puertos 23, 135 y 443? ¿Son seguros?

- 2. A continuación se lista una serie de enlaces que permiten realizar un test de la velocidad de acceso a Internet, de modo que un resultado muy inferior al contratado **podría ser un síntoma de tener ocupantes no deseados en nuestra máquina**. **¿Son las velocidades de subida y bajada las esperadas?**

<http://www.adsl4ever.com/test/>
<http://www.testdevelocidad.es/>
<http://www.internautas.org/testvelocidad/>
<http://www.adslayuda.com/test-de-velocidad/>

- Recuerda que el ancho de banda del aula es compartido por todos los PC del mismo. Realiza el test de velocidad de manera individual (sin que nadie en el aula lo realice o esté haciendo uso de Internet).

- 3. Los *packet sniffers* se emplean para monitorizar el tráfico de una red LAN o WLAN y algunos de ellos son Wireshark (anteriormente conocido como Ethereal), Ettercap, TCPDump, WinDump, WinSniffer, Hunt, Darkstat, traffic-vis, KSniffer) y para redes inalámbricas como Kismet o Network Stumbler.

■ Descarga e instala Wireshark en tu equipo, y haz que capture el tráfico que emite y recibe tu tarjeta

de red. Si quieras capturar gran parte del tráfico de la red deberás realizar previamente un ataque MitM a la puerta de enlace o conectarte a una WLAN. Se recomienda siempre que utilices un *sniffer* configurar las opciones de filtrado para monitorizar solo el tráfico deseado. Busca los filtros necesarios para rastrear solo los protocolos FTP, HTTP, POP3, etc.

- ¿Es posible, mediante obtener las contraseñas de protocolos como telnet, HTTP, FTP, SMTP o POP3 de correo electrónico? ¿Cómo? ¿Qué ventajas ofrece https? ¿Te conectarías a una web de un banco mediante http? Intenta acceder a tu correo electrónico vía web (Hotmail, Yahoo, Gmail) ¿es posible descubrir mediante Wireshark la contraseña? ¿Por qué?
- 4. Configura de forma segura un *router* Linksys WRT54GL mediante su web para simulación de configuración *online*:
<http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm>
 - ¿Es posible configurar todos los aspectos analizados en el capítulo?
- 5. Busca información sobre la pintura antiwiñi de EM-SEC Technologies y descubre su principio de funcionamiento. ¿Crees que podría ser útil y seguro? ¿Cómo se implementaría?
 - Puede leer sobre dicha pintura en: <http://www.publico.es/ciencias/273942/una-pintura-protege-a-los-navegantes-de-los-intrusos/version-imprimible>.
- 6. Busca información acerca de AlienVault y de las funciones que ofrece. Descárgalo y realiza pruebas e informes de monitorización del tráfico de red. ¿Puede realizar funciones de IDS? ¿Es software libre?
- 7. Investiga y utiliza el comando scp sobre una conexión SSH para el envío seguro de archivos de un equipo a otro. ¿Es posible abrir y utilizar una sesión SSH empleando cifrado asimétrico con claves RSA? Investiga acerca de cómo hacerlo y realiza la prueba.

- 8. ¿Es posible realizar MAC *spoofing* o falsificación de la dirección MAC de una tarjeta de red? Busca cómo se realiza para sistemas GNU/Linux y Windows y pruébalo.
- 9. Realiza el siguiente test sobre *phishing* de Verisign disponible en <https://www.phish-no-phish.com/> es con consejos útiles para reconocer páginas web falsas y realiza un resumen con recomendaciones útiles. ¿Crees ahora que solo garantizando que la web es https se trata de una web confiable?



TEST DE CONOCIMIENTOS

1 La configuración de clientes de red en WLAN es menos compleja si:

- a) No se habilita DHCP server en el AP.
- b) Se habilita el SSID broadcast.
- c) Se habilita la seguridad WEP.
- d) Se habilita la seguridad WPA.

2 Indique qué sentencia es verdadera:

- a) Las redes inalámbricas son más o menos igual de seguras que las cableadas.
- b) Las redes inalámbricas nunca serán tan seguras como las cableadas.
- c) Las redes cableadas UTP son más seguras que con STP.
- d) Las redes de fibra óptica son menos seguras que las inalámbricas.

3 El mecanismo de seguridad más robusto en redes inalámbricas es:

- a) Open system.
- b) WPA2.
- c) WPA.
- d) WEP.

4 En redes inalámbricas no se recomienda:

- a) Cambiar el SSID de fábrica.
- b) Cambiar el *password* de administrador por defecto.
- c) Habilitar el DHCP.
- d) Tener claves WEP complejas.

5 Con respecto a SSH:

- a) Es un servicio único de GNU/Linux.
- b) En Windows se puede emplear el cliente Putty.
- c) Es un protocolo que emplea el puerto 23.
- d) Ninguna de las anteriores.

6 El puerto que no emplea TLS/SSL es:

- a) 22.
- b) 990.
- c) 995.
- d) 443.

7 Frente a ataques MitM una posible solución es:

- a) Emplear entradas ARP dinámicas.
- b) Emplear direcciones IP dinámicas.
- c) Emplear direcciones IP estáticas.
- d) Emplear entradas ARP estáticas.

8 ¿Cuál de estos programas no funciona como *sniffer*?

- a) Cain & Abel.
- b) Snort.
- c) Wireshark.
- d) LogmeIn.

9 El protocolo estándar para conexiones VPN suele ser:

- a) PPTP.
- b) IPSEC.
- c) L2TP.
- d) SSL/TLS.

7

Seguridad perimetral

OBJETIVOS DEL CAPÍTULO

- ✓ Valorar los peligros externos a las redes corporativas y conocer las medidas de seguridad perimetrales para hacerles frente.
- ✓ Comprender la importancia de los puertos de comunicaciones y su filtrado mediante cortafuegos o *firewall*.
- ✓ Aprender el significado de las listas de control de acceso (ACL) en *routers* y cortafuegos.
- ✓ Comprender la importancia y aprender a configurar servidores y clientes proxy.

Cuando una red corporativa se encuentra interconectada a una red pública, los peligros de ataque a sus servidores, routers y sistemas internos se multiplican.

Las medidas de seguridad perimetral suponen la primera línea de defensa entre las redes públicas y redes corporativas o privadas. Entre otras estudiaremos el uso de **cortafuegos** o *firewall* destinado a bloquear las conexiones no autorizadas, y de **servidores proxy** que hagan de intermediario entre clientes y servidores finales, permitiendo el filtrado y monitorización de servicios.



NOTICIA DE ACTUALIDAD

Analiza la noticia "Chinos aprenden a evitar el *Gran Firewall* de internet", encontrada en:

http://www.bbc.co.uk/mundo/ciencia_tecnologia/2010/03/100320_china_internet_control_censura_firewall_jp.shtml, e indica:

- ¿Qué es el *gran firewall*? ¿Quién controla dicho *firewall*? ¿Para qué?
- ¿Qué tipo de palabras y webs son censuradas? ¿Por qué?
- ¿Qué porcentaje y cómo consiguen eludir el *gran firewall*? ¿Mediante qué aplicaciones?

7.1 CORTAFUEGOS

Un cortafuegos o *firewall*, es una aplicación o dispositivo diseñado para bloquear comunicaciones no autorizadas, permitiendo al mismo tiempo las que si lo están. La configuración para permitir y limitar el tráfico entre diferentes redes o ámbitos de una red, se realiza en base a un conjunto de normas y reglas. Mediante este mecanismo de defensa podemos mantener la seguridad de alto nivel en una red o en una máquina.

La utilización de un cortafuegos es necesaria cuando queremos proteger determinadas zonas de nuestra red o determinados *hosts*, de amenazas que provengan del exterior o, incluso, de amenazas que se provoquen dentro de nuestra propia red ya sean por infecciones o ataques.

Las características fundamentales de los cortafuegos son:

- ✓ Filtrado de paquetes de red en función de la inspección de direcciones de red: MAC, IP o puerto origen y destino, permitiendo con este último criterio proporcionar un filtrado según las aplicaciones asociadas a dicho puerto.
- ✓ Filtrado por aplicación: permite especificar las aplicaciones y reglas específicas para cada una de ellas.
- ✓ Las distintas reglas de filtrado se aplican sobre el tráfico de salida o de entrada en una determinada interfaz de red.
- ✓ Registro o logs de filtrado de paquetes.

PRÁCTICA 7.1

CONFIGURACIÓN DE CORTAFUEGOS

En sistemas GNU/Linux, **Iptables** es una de las herramientas cortafuegos más empleadas, que permite el filtrado de paquetes de red así como realizar funciones de NAT (*Network Address Translation* - Traducción de Dirección de Red). No es necesario instalarlo pues viene incorporado en el núcleo de GNU/linux.

Es una aplicación que contiene una serie de cadenas de reglas de filtrado en 3 tablas. Atender al orden de dichas reglas es muy importante, ya que lee de manera secuencial las cadenas de reglas. Es decir, comienza por la primera y verifica que se cumpla la condición, en caso afirmativo la ejecuta sin verificar las siguientes.

Por consiguiente, si la primera regla en una determinada tabla es rechazar cualquier paquete, las siguientes reglas no serán verificadas.

- La estructura de una orden de iptables sigue el siguiente patrón:

```
iptables -t [tabla] - [tipo_operación] -- [cadena]-- [regla_con_parámetros] - - [acción].
```

Veremos un ejemplo de comando para entender su estructura:

```
iptables -t filter -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 80 -j ACCEPT.
```

Tabla 7.1

tabla	Tipo de operación	Cadena	Regla_con_parámetros	Acción
-t filter	-A	FORWARD	-i eth0 -s 192.168.2.100 -p tcp --dport 80	-j ACCEPT

- El tipo de operación es añadir una regla (A), sobre la tabla filter (tabla por defecto de filtrado), y cadena FORWARD (tráfico enruteado).
- La regla: aceptar (ACCEPT) el tráfico TCP cuyo puerto de destino sea el 80 (HTTP), en el interfaz eth0, con IP origen 192.168.2.100.

- Las opciones más usadas de iptables son: iptables -L

- L: listar las cadenas de reglas de una determinada tabla (por defecto filter).
- F: elimina y reinicia a los valores por defecto todas las cadenas de una determinada tabla.
- A: añadir cadena de regla a una determinada tabla.
- P: añadir regla por defecto, en caso de que no cumpla ninguna de las cadenas de regla definidas.

Para sistemas en los que no se haya definido anteriormente reglas para Iptables el resultado de ejecutar el comando iptables -L tiene que ser similar a permitir todo el tráfico.

- Existen tres tablas incorporadas, cada una de las cuales contiene ciertas cadenas predefinidas:

- Filter table (Tabla de filtros):** Esta tabla es la responsable del filtrado (es decir, de bloquear o permitir que un paquete continúe su camino). Todos los paquetes pasan a través de la tabla de filtros. Contiene las siguientes cadenas predefinidas y cualquier paquete pasará por una de ellas:
 - INPUT chain (Cadena de ENTRADA) — Todos los paquetes destinados a este sistema atraviesan esta cadena (también denominada LOCAL_INPUT o ENTRADA_LOCAL).

- OUTPUT chain (Cadena de SALIDA) — Todos los paquetes creados por este sistema atraviesan esta cadena (también denominada LOCAL_OUTPUT o SALIDA_LOCAL).
- FORWARD chain (Cadena de REDIRECCIÓN) — Todos los paquetes que pasan por este sistema para ser encaminados a su destino recorren esta cadena.
- **Nat table (Tabla de traducción de direcciones de red)** — Esta tabla es la responsable de configurar las reglas de traducción de direcciones o de puertos de los paquetes. Contiene las siguientes cadenas redefinidas:
 - PREROUTING chain (Cadena de PRERUTEO) — Los paquetes entrantes pasan a través de esta cadena antes de que se consulte la tabla de enruteado.
 - POSTROUTING chain (Cadena de POSRUTEO) — Los paquetes salientes pasan por esta cadena después de haberse tomado la decisión de enruteado.
 - OUTPUT chain (Cadena de SALIDA).
- **Mangle table (Tabla de destrozo)** — Esta tabla es la responsable de ajustar las opciones de los paquetes, como por ejemplo la calidad de servicio. Todos los paquetes pasan por esta tabla. Está diseñada para efectos avanzados, y contiene todas las cadenas predefinidas anteriormente.

A la hora de definir una orden de iptables podremos seleccionar la tabla a la que va destinada dicha orden mediante el parámetro `-t`:

```
iptables -t [nat | filter | mangle ]
```

4. Los **modificadores o parámetros** más usuales en las reglas de iptables son los siguientes:

Tabla 7.2

Parámetro	Función
<code>-i</code>	Interfaz de entrada (eth0,eth1,eth2...).
<code>-o</code>	Interfaz de salida (eth0,eth1,eth2...).
<code>--sport</code>	Puerto de origen (puede indicarse el nombre o el número de puerto del protocolo, p.ej: http u 80).
<code>--dport</code>	Puerto destino (puede indicarse el nombre o el número de puerto del protocolo, p.ej: http u 80).
<code>-p</code>	El protocolo del paquete a comprobar, tcp, udp, icmp ó all. Por defecto es all.
<code>-j</code>	Especifica el objetivo de la cadena de reglas, o sea una acción.
<code>--line-numbers</code>	Cuando listamos las reglas, agrega el número que ocupa cada regla dentro de la cadena.

5. Las **acciones** que estarán siempre al final de cada regla (después de `-j`) que determinará qué hacer con los paquetes afectados por la regla pueden ser:

- ACCEPT: Paquete paquete aceptado.
- REJECT: Paquete paquete rechazado. Se envía notificación a través del protocolo ICMP.
- DROP: Paquete paquete rechazado. Sin notificación.
- MASQUERADE: Enmascaramiento enmascaramiento de la dirección IP origen de forma dinámica. Esta acción es solo válida en la tabla NAT en la cadena postrouting.

- DNAT: Enmascaramiento enmascaramiento de la dirección destino, muy conveniente para re-enrutado de paquetes.
- SNAT: Enmascaramiento enmascaramiento de la IP origen de forma similar a masquerade, pero con IP fija.

Ejemplos prácticos

Realizaremos la configuración de un cortafuegos mediante un script que defina:

- Enrutamiento con NAT y registro o log de paquetes FORWARD y PREROUTING. Se crea un registro en /var/log/iptables.log para tener un control de lo que entra y sale de nuestro cortafuegos.
- Reglas que permita el acceso a los protocolos HTTP, DNS y FTP en Internet, pero solo a dos direcciones IP determinadas desde una red local (192.168.2.100 y 192.168.2.114), todos los demás equipos no tendrán acceso.
- Redirección del tráfico web en el puerto 80 por el puerto 3128 (Proxy). Veremos su utilidad en el siguiente apartado.

```
#!/bin/bash
# borrar todas las reglas existentes.
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X
# Aceptar el tráfico desde loopback
iptables -A INPUT -i lo -j ACCEPT
# Habilitar logs de todo lo que entra por FORWARD
iptables -A FORWARD -j LOG --log-prefix 'IPTABLESFORWARD : '
# Permitimos acceso a los puertos 80 (web), 20-21 (ftp/FTP), 53 (dns-tcp y udp)
# a los equipos: 192.168.2.100 y 192.168.2.114
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 20:21 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p tcp --dport 20:21 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.100 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.2.114 -p tcp --dport 53 -j ACCEPT
#Cerramos los puertos bien conocidos (1-1024).
iptables -A FORWARD -i eth0 -p tcp --dport 1:1024 -j DROP
iptables -A FORWARD -i eth0 -p udp --dport 1:1024 -j DROP
#Hacemos log de todo lo entra por el PREROUTING
iptables -t nat -A PREROUTING -j LOG --log-prefix 'IPTABLESPREROUTING: '
#Redirección de puerto 80, hacia el Proxyp proxy, puerto 3128.
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port
3128
#Enmascarar mediante NAT, todo el tráfico (la IP origen de los
#paquetes) de la red interna por la IP de la tarjeta de red externa o pública.
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth1 -j MASQUERADE
# Habilitamos enrutamiento entre tarjetas de red de nuestro equipo.
echo 1 > /proc/sys/net/ipv4/ip_forward
#Fin del script
```

Una vez ejecutado el script podemos ver el resultado de la configuración, mediante el comando: `iptables -nL`.

```

root@usuario-desktop:/home/usuario#
root@usuario-desktop:/home/usuario# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT    all  --  0.0.0.0/0            0.0.0.0/0
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
LOG       all  --  0.0.0.0/0            0.0.0.0/0      LOG flags 0 level 4
prefix   * IPTABLESFORWARD :
ACCEPT   ip  --  192.168.2.100        0.0.0.0/0      tcp dpt:80
ACCEPT   tcp --  192.168.2.114        0.0.0.0/0      TCP dpt:80
ACCEPT   tcp --  192.168.2.100        0.0.0.0/0      TCP dpts:20:21
ACCEPT   tcp --  192.168.2.114        0.0.0.0/0      TCP dpts:20:21
ACCEPT   udp --  192.168.2.100        0.0.0.0/0      UDP dpt:53
ACCEPT   tcp --  192.168.2.100        0.0.0.0/0      TCP dpt:53
ACCEPT   udp --  192.168.2.114        0.0.0.0/0      UDP dpt:53
ACCEPT   tcp --  192.168.2.114        0.0.0.0/0      TCP dpt:53
DROP    tcp --  0.0.0.0/0            0.0.0.0/0      TCP dpts:1:1024
DROP    udp --  0.0.0.0/0            0.0.0.0/0      UDP dpts:1:1024

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@usuario-desktop:/home/usuario# 

```

Por otro lado para ver las reglas PREROUTING y POSTROUTING de la tabla NAT: `iptables -t nat -nL`.

Para ver como se hacen efectivas las reglas de iptables, si intentamos acceder a sitios web desde el equipo configurado con IP 192.168.2.100, veremos como resuelve los nombres de dominio como www.google.es y accede sin problemas. En caso de intentar acceder a una web desde un equipo de la red pero con IP no permitida (ej: 192.168.1.50.), no tendrá acceso a la navegación ya que se bloquea todo el tráfico hacia Internet de cualquier dirección que no sea las aceptada en las reglas.

PRÁCTICA 7.2

ARCHIVOS LOG

La herramienta iptables por si sola no realiza registros de cada una de las conexiones que filtra. Es posible habilitar esta función realizando una serie de configuraciones en distintos archivos de manera que queden registradas todas las entradas y salidas de nuestro cortafuegos.

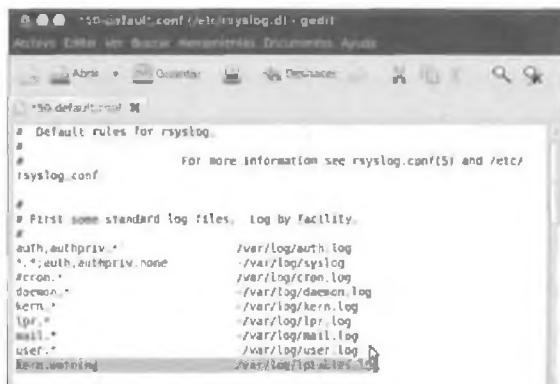
Para ello anteriormente hay que definir la creación del registro a través de la acción `-j log` en las reglas de iptables, pudiendo añadir un prefijo a cada entrada en el log para poder identificar los paquetes de forma más sencilla, mediante `--log-prefix`. Por ejemplo en la práctica anterior hemos configurado:

- ✓ `iptables -A FORWARD -j LOG --log-prefix 'IPTABLESFORWARD :'`
- ✓ `iptables -t nat -A PREROUTING -j LOG --log-prefix 'IPTABLESPREROUTING:'`

Hacemos log de todo lo que filtra FORWARD y PREROUTING.

1. Para habilitar el log en primer lugar vamos al archivo **de configuración del sistema de logs del núcleo** que se encuentra en la ruta `/etc/rsyslog.d/50-default.conf` y añadimos lo siguiente:

`kern.warning /var/log/iptables.log`



En los sistemas GNU/Linux generan mensajes con diferentes niveles de prioridad, de menor a menor son: *debug*, *info*, *notice*, *warning*, *warn*, *err*, *error*, *crit*, *alert*, *emerg* y *panic*. Con la línea anteriormente mencionada, se añade a `iptables.log` cualquier registro del tipo *warning* (nivel 4), asociados normalmente a filtrado de paquetes de red. Una vez introducida la configuración anterior reiniciamos el servicio `rsyslog`, aunque dependiendo de la versión del kernel es posible que sea necesario reiniciar el sistema por completo:

```
/etc/init.d/rsyslog stop
```

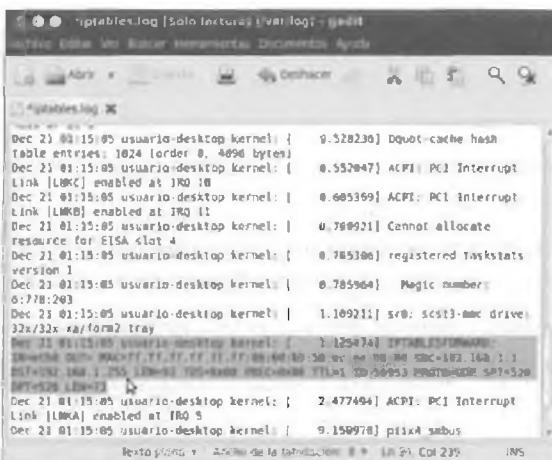
/etc/init.d/rsyslog start

Una vez reiniciado el servicio podemos observar que se ha creado el archivo de log mediante: `cat /var/log/iptables.log`

A medida que se filtren paquetes se irán añadiendo registros a este archivo.

Los logs de iptables es posible también verlos en `/var/log/messages`, el porqué de crear el archivo "iptables.log" es debido a que en este archivo solo se almacenan errores a partir de nivel 4 mientras que en el archivo "messages" se almacena cualquier error, indiferentemente del nivel de error, y por tanto a la hora de buscar un registro de iptables es mucho más costoso.

2. Hasta aquí tenemos la configuración del log de iptables pero ahora vamos a explicar que contiene un registro del mismo. Para ello, introducimos la sentencia anterior "cat /var/log/iptables.log" y vemos que aparece algo similar a lo siguiente:



Análisis de un registro de sucesos del archivo iptables.log

La información se ordena de izquierda a derecha siguiendo al modelo OSI de abajo hacia arriba, primero lo referido a enlace de datos (iface, MAC), luego a red (dirección IP, TOS) y por ultimo de transporte (puerto, ACK, etc.). Se dará un breve detalle de cada campo ya que hay información que podría no estar presente dependiendo de la cadena dentro de la que se realizó el registro de algunos de los protocolos que intervienen en el caso.

- ✓ Dec 21: es el mes y el día del registro. (21 de diciembre).
- ✓ 10:31:41 : es la hora en la que se añadió el registro al archivo de log.
- ✓ Usuario-desktop: es el nombre de la máquina que realiza el log.
- ✓ kernel: [4081.617746]: es el código del log del núcleo.
- ✓ IPTABLESFORWARD: es el prefijo que hemos añadido en la sentencia de iptables para diferenciar los registros que provienen de iptables de cualquier otro registro.
- ✓ IN=eth0 OUT=: interfaces de red por la cual entró la trama y por la cual va a salir.
- ✓ MAC: información que maneja la capa MAC (Media Access Control, junto a LLC conforman la capa de enlace de datos). Se concatenan los 6 bytes de la dirección MAC destino con los 6 de origen y como se trata de un datagrama IPv4 el código es 0800.
- ✓ SRC y DST: IP origen y destino.
- ✓ LEN: longitud total del datagrama, hace referencia al campo LT de la cabecera IP (del bit 17 al 32) y no al campo IHL (longitud de la cabecera, del bit 5 al 8).
- ✓ TOS y PREC: campo tipo de servicio de la cabecera IP, por lo general es 00 y con PREC (precedencia)0x00.
- ✓ TTL y ID: time to live (tiempo de vida) y el campo ID utilizado para rearmar fragmentos.
- ✓ PROTO, SPT y DPT: en este caso, protocolo de transporte y puertos de origen y destino. El valor de PROTO se obtiene del campo protocolo de la cabecera IP. El SPT y DPT son algoritmos de control.

7.1.1 TIPOS DE CORTAFUEGOS

En general, para establecer las diferencias entre los distintos cortafuegos atendemos a la flexibilidad y la facilidad de configuración de los mismos, así como la capacidad de manejo de tráfico. Una clasificación posible es por la ubicación en la que se encuentre el *firewall*:

- **Firewalls basados en servidores:** consta de una aplicación de *firewall* que se instala y ejecuta en un sistema operativo de red (NOS), que normalmente ofrece otra serie de servicios como enrutamiento, proxy, DNS, DHCP, etc.
- **Firewalls dedicados:** son equipos que tienen instalado una aplicación específica de cortafuegos y, por tanto, trabajan de forma autónoma como cortafuegos.
- **Firewalls integrados:** se integran en un dispositivo hardware para ofrecer la funcionalidad de *firewall*. Como ejemplos encontramos *switches* o *routers* que integran funciones de cortafuegos.
- **Firewalls personales:** se instalan en los distintos equipos de la red de forma que los proteja individualmente de amenazas externas. Por ejemplo en un equipo doméstico el cortafuegos preinstalado en sistemas Windows.

Las arquitecturas de cortafuegos más implementadas son:

- **Screening router:** como frontera entre la red privada y la red pública se encuentra un *router* que realiza tareas de filtrado.
- **Dual Homed-Host:** como frontera se dispone un equipo servidor que realizará tareas de filtrado y enrutamiento mediante al menos 2 tarjetas de red, esto permitirá una mayor flexibilidad en la configuración e instalación de aplicaciones de seguridad.
- **Screened Host:** combina un *router* como equipo fronterizo exterior y un servidor proxy que filtrará y permitirá añadir reglas de filtrado en las aplicaciones más empleadas. Veremos el uso y configuración de servidores proxy en un apartado posterior.
- **Screened-subnet:** mediante la creación de una subred intermedia, denominada **DMZ** o **zona desmilitarizada**, entre la red externa y la red privada interna, permitirá tener 2 niveles de seguridad, uno algo menor en el cortafuegos más externo y uno de mayor nivel de seguridad en el cortafuegos de acceso a la red interna.

PRÁCTICA 7.3

CONFIGURACIÓN ROUTER-FIREWALL

La mayoría de los *routers* poseen opciones de configuración de cortafuegos o reglas de filtrado, veremos estos aspectos a 2 niveles dentro los productos de la empresa **Cisco**.

Linksys, es la división para el hogar y pequeñas empresas, entre sus productos encontramos el *router* WRT54GL con una web para simulación de configuración *online*:

<http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm>

Entre otras opciones disponemos de opciones de configuración básica de cortafuegos (opción *Security - Firewall*), así como una configuración más avanzada (opción *Access Restrictions*) donde podemos habilitar 10 políticas de acceso independientes, por ejemplo habilitar el tráfico a determinadas horas, para determinado tipo de tráfico (puertos-protocolos de aplicación), equipos y sitios web.



ACL

Para el caso de los routers CISCO de gama media y alta, es posible configurar listas de control de acceso o ACL, listas de condiciones que se aplican al tráfico que viaja a través de una interfaz del router y se crean según el protocolo, la dirección o el puerto a filtrar. Existen dos tipos de ACL:

- ✓ ACL estándar, donde solo tenemos que especificar una dirección de origen.
- ✓ ACL extendida, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino, ofrecen un mayor control.

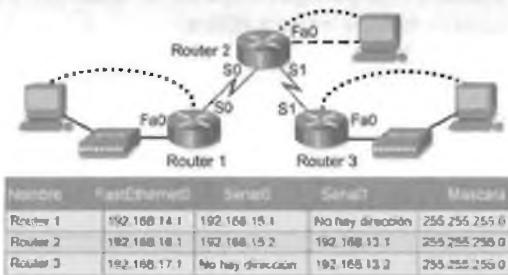
Veamos un ejemplo de ACL estándar:

Una ACL estándar solo filtra la dirección **origen**, donde ésta puede ser una dirección de host, de red o un rango de direcciones. Con la comparación se permite o deniega el acceso. La configuración se hace en modo de configuración global, y luego se hace la asignación de la ACL a la interfaz de red que corresponda, ya sea a la entrada o a la salida del tráfico en dicha interfaz.

La sintaxis completa del comando ACL estándar, para routers CISCO bajo sistema operativo propietario CISCO IOS, es la siguiente:

```
Router(config)# access-list numero_ACL deny|permit dirección_a_filtrar mascara_wildcard
```

Donde: número_ACL es un número que va del 1 al 99 o del 1300-1999, y la máscara de wildcard se obtiene complementando la máscara de subred, es decir si la queremos aplicar sobre una red de clase C, la máscara wildcard será 0.0.0.255 complementaria de 255.255.255.0.



Tomando en cuenta la topología de la imagen, para crear una ACL en Router 1 que solamente permita los paquetes de la red 192.168.16.0:

- ✓ Router1(config)# access-list 1 permit 192.168.16.0 0.0.0.255
- ✓ Router1(config)# interface Serial0
- ✓ Router1(config-if)# ip-access-group 1 in

La explicación de esta ACL es que como es una ACL estándar, se configura lo más cerca del destino (Router1), la dirección a filtrar es una dirección de red de clase C, por lo que la máscara wildcard es 0.0.0.255 ya que verifica la red y no verifica la parte de host.

Las reglas ACL se verifican como en el cortafuegos iptables, hasta que se cumpla una condición, en caso de no ser así, implícitamente hay una línea al final de la ACL que deniega todo lo demás: **Router1(config)# access-list 1 deny any**, la cual no nos afecta en este ejemplo para el funcionamiento que deseamos de la ACL.

Después se asigna en la interfaz de red que corresponda, para eso debe seguir la ruta que seguiría el paquete al tratar de entrar a Router1. La dirección de red a filtrar proviene de Router2, por lo que la trayectoria sería salir de Router2 por su interfaz S0 y entrar a Router1 por la interfaz S0, lo cual la hace la interfaz en la que se debe configurar, justamente a la entrada (in).

PRÁCTICA 7.4



CONFIGURACIÓN DE CORTAFUEGOS CON ENTORNO GRÁFICO

La mayoría de los sistemas operativos personales disponen de cortafuegos preinstalados, como es el caso de los sistemas Windows. Sus funciones han ido aumentando en las últimas versiones como Windows Vista y Windows 7, y en sus versiones de servidor como Windows 2003 y 2008 han proliferado los entornos de gestión de seguridad en redes como **Microsoft Internet Security and Acceleration Server (ISA Server)** y **Microsoft Forefront Threat Management Gateway (Forefront TMG)**.

En nuestro caso, utilizaremos la aplicación **Kerio Winroute Firewall** para gestionar la seguridad del tráfico entrante y saliente de nuestra red.

1. En primer lugar, descargaremos el software desde la siguiente dirección: www.kerio.com. Tras descargar el ejecutable que instalará el *firewall*, ejecutaremos el instalador. Es recomendable desactivar el *firewall* que viene por defecto en Windows para evitar conflictos.

En un momento de la instalación, el programa detectará si hay algún conflicto con el sistema. En caso de ser así, tendremos que deshabilitar dichas opciones que presentan conflictos con el programa seleccionándolos en el mismo cuadro de diálogo.

Tras esto, nos pedirá un nombre de usuario y una contraseña para la administración del *firewall* como **administrador**. Por último, pulsaremos en el botón instalar para empezar la instalación del *firewall* en el sistema operativo. A la hora de instalar el software Kerio Winroute *firewall* se aplica una configuración que bloquea todo el tráfico de Internet por lo que tendremos que realizar más adelante una configuración básica para permitir aquellas conexiones que necesitemos.

2. Terminada la instalación, podemos iniciar el programa de administración "Kerio Administration console" que nos permitirá realizar la configuración de nuestro *firewall*. Como todo programa de administración, este nos pide que nos conectemos a un *host* (podremos configurarlo remotamente o en local=localhost) con el usuario y la contraseña definida en la instalación para poder administrar el software.



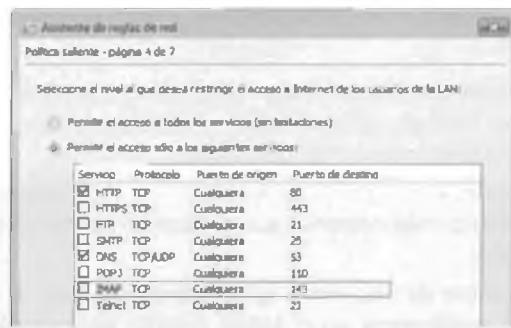
Una vez logueados, el *firewall* nos ejecuta un asistente que nos permite realizar una configuración básica del mismo.

En primer lugar tendremos que indicarle la forma en la que este se conecta a la red seleccionando "Un único enlace de Internet – persistente" ya que es la configuración más sencilla.

Acto seguido, nos pedirá que seleccionemos la interfaz por la que se conecta a la red. Dependiendo de las interfaces que se conectan tendremos que seleccionar una interfaz para la opción que hemos elegido o tantas como haya conectadas para las opciones de "múltiples enlaces a Internet".

El siguiente paso es el que bloqueará o permitirá cierto tráfico a Internet según los protocolos que necesitemos ya sea para la visualización web, transferencia de archivos mediante FTP, etc. Seleccionaremos la segunda opción de la pantalla que dice "permitir el acceso solo a los siguientes servicios" ya que tendremos un control exhaustivo de las aplicaciones que permitimos la conexión.

De la lista que nos aparece seleccionaremos los protocolos cuyo tráfico estará permitido. Realizaremos una configuración sencilla permitiendo solo el protocolo http y DNS para la navegación por Internet. Todos los demás protocolos quedarán bloqueados.



Configurados los servicios que queremos permitir, podemos seleccionar o no la opción para que cree una serie de reglas en el *firewall* que permitan la administración del mismo de manera remota mediante VPN.

3. Realizaremos una prueba básica para ver que el *firewall* funciona correctamente. Para ello nos conectaremos mediante FTP a una máquina remota o de nuestra misma red, si el *firewall* funciona correctamente no nos dejará conectarnos al servidor FTP, pero si nos permitirá la navegación web.
4. Si posteriormente queremos permitir la conexión mediante FTP al servidor local, iremos a la sección "configuración" y pulsamos en el apartado "política de tráfico". En este apartado se muestran las reglas que regulan el *firewall*, añadiremos el servicio FTP a las excepciones pulsando en las filas "Acceso a Internet (NAT)" y "Tráfico del *firewall*", en la casilla de servicios con el botón derecho seleccionamos "editar servicios".

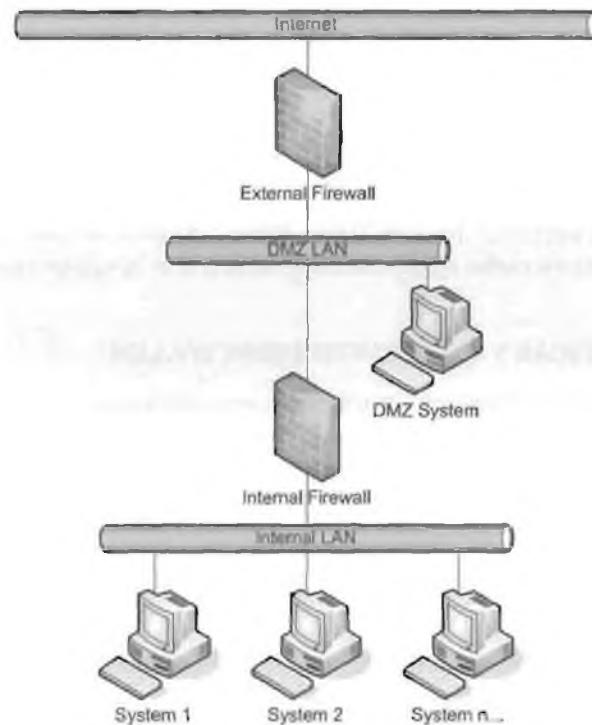


Seleccionamos del desplegable "agregar" el servicio que queremos añadir a las excepciones, en nuestro caso FTP, y pulsamos en aceptar.

7.1.2 DMZ

Cuando se realiza el diseño de una red es importante determinar qué equipos ofrecerán servicios de carácter público y por tanto será accesible desde el exterior de nuestra red corporativa y qué equipos deben ser invisibles desde el exterior para mantener un cierto nivel de seguridad en las comunicaciones internas.

Surge de esta diferenciación el concepto de **zona desmilitarizada** o **DMZ** (*demilitarized zone*) o red perimetral. Se trata de una red local que se ubica entre la **red interna de una organización** y una **red externa**, generalmente Internet, donde se ubican los servidores HTTP, DNS, FTP y otros que sean de carácter público.



Habitualmente, una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (**screened-subnet firewall**).

Por lo general, la **política de seguridad** para la DMZ es la siguiente:

- ✓ El tráfico de la red externa a la DMZ está autorizado y a la red interna está prohibido.
- ✓ El tráfico de la red interna a la DMZ está autorizado y a la red externa está autorizado.

Normalmente el **DMZ host** está separado de Internet a través de un *router* y un cortafuegos, o se encuentran integrados. Es aconsejable que en el cortafuegos se abran al exterior únicamente los **puertos de los servicios** que se pretende ofrecer con los servidores disponibles en la DMZ.

7.2 PROXY

Un servidor proxy o representante es una aplicación o sistema que gestiona las conexiones de red, sirviendo de intermediario entre las peticiones de servicios que requieren los clientes, como http, FTP, irc, telnet, ssh, etc., creando así una memoria caché de dichas peticiones y respuestas por parte de los servidores externos. La finalidad de este tipo de servidores es poder servir más rápidamente a sus usuarios en conexiones siguientes que hayan sido solicitadas y respondidas previamente, sin tener que acceder remotamente de nuevo a los servidores externos.

La mayoría de los servidores proxy también añaden **funciones** de control y autenticación de usuarios, y reglas de filtrado de los contenidos solicitados, así como funciones de registro de logs.

Entre las grandes ventajas de un servidor proxy se encuentra la mejora de velocidad de respuesta a peticiones, ya que si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché, guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

Para evitar contenidos desactualizados, los servidores proxy actuales, se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.

7.2.1 TIPOS, CARACTERÍSTICAS Y FUNCIONES PRINCIPALES

Dependiendo del tipo de tráfico que circulará por una red necesitaremos un proxy que cumpla con las necesidades del tráfico, ya sea para acelerar la descarga de contenidos para no sobrecargar la salida a Internet o para autenticación de usuarios. En función de las características de cada tipo de proxy podemos clasificarlos de la siguiente manera:

- **Proxy caché Web:** se trata de un proxy para una aplicación específica como el acceso a la web. Mantienen copias locales de los archivos más solicitados y los sirven bajo demanda, reduciendo la baja velocidad y coste en la comunicación con Internet. El proxy caché almacena el contenido en la caché de los protocolos HTTP, HTTPS, incluso FTP.
- **Proxy NAT:** integración de los servicios de traducción de direcciones de red y proxy.
- **Proxy transparente:** normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones al puerto 80 típicamente, son redirigidas hacia el puerto del servicio proxy.
- **Proxy anónimo:** permiten aumentar la privacidad y el anonimato de los clientes proxy, mediante una activa eliminación de características identificativas (dirección IP del cliente, cabeceras From y Referer, cookies, identificadores de sesión...).
- **Proxy inverso:** un reverse proxy es un servidor proxy instalado en una red con varios servidores web, sirviendo de intermediario a las peticiones externas, suponiendo una capa de seguridad previa, gestión y distribución de carga de las distintas peticiones externas, gestión de SSL o como caché de contenidos estáticos.
- **Proxy abierto:** acepta peticiones desde cualquier ordenador, esté o no conectado a su red. En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de *spam*, muchos servidores, como los de IRC o correos electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras (*blacklist*).

Tras conocer los distintos tipos de proxy pasaremos a instalar y configurar uno.

PRÁCTICA 7.5

CONFIGURACIÓN DE PROXY. GESTIÓN DE CACHÉ, LOG, CLIENTES Y FILTROS WEB.

En la siguiente práctica, aprenderemos a instalar y configurar los parámetros fundamentales de un servidor Proxypoxy, así como los clientes que hagan uso de él.

1. En sistemas GNU/Linux *Squid* es el servidor Proxy proxy por excelencia, debido a su potencia y estabilidad. Empezaremos por instalar *Squid* mediante el comando: `apt-get install squid3`.

En la instalación de *Squid* nos crea un archivo de configuración del Proxy proxy por defecto en `/etc/squid3/squid.conf`. En este fichero podemos configurar cualquier parámetro del Proxypoxy. No obstante, nosotros crearemos un fichero de configuración propio con los parámetros necesarios para que el Proxy proxy funcione como filtro de contenidos.

Por este motivo, haremos una copia del archivo de configuración que se instala por defecto de tal manera que tengamos una copia de seguridad del archivo en caso de fallo. Ejecutaremos la siguiente sentencia:

```
cp /etc/squid3/squid.conf /etc/squid3/squid.conf.old
```

2. Modificaremos el fichero ejecutando la sentencia "`gedit /etc/squid3/squid.conf`". El contenido del archivo de configuración:

```
# Parámetros generales
#Nombre del proxy
visible_hostname servidor_proxy
puerto de escucha del proxy
http_port 3128

#Dirección de la caché de squid y el tamaño de la misma
cache_dir ufs /var/spool/squid3 2000 16 256
cache_mem 32 MB
maximum_object_size_in_memory 256 MB

#Dirección de los registros de squid
access_log /var/log/squid3/access.log
cache_log /var/log/squid3/cache.log

#Listas de control de acceso
acl acceso_sfc B.0.0.0-0.0.0.0
acl nopermitedas url_regex "/etc/squid3/nopermitidas"
acl noviebs ditdomain "/etc/squid3/noviebs"

#control de acceso
http_access deny nopermitidas
http_access deny noviebs
http_access allow acceso
```

Parámetros generales: almacenamiento caché, nombre y puerto

A continuación vamos a explicar los parámetros que hemos modificado en el fichero de configuración `Squid.conf`:

```
# Parámetros generales
#Nombre del proxy
visible_hostname servidor_proxy
```

Este será el nombre del proxy que mostrará a los clientes proxy cuando *Squid* detecte una página o una palabra no permitida:

```
#puerto de escucha del proxy
http_port 3128
#Direccion de la caché de squid y el tamaño de la misma
cache_dir ufs /var/spool/squid3 2000 16 256
cache_mem 32 MB
maximum_object_size_in_memory 256 MB
```

- **Cache_dir:** determina el tipo de sistema de almacenamiento en caché que utilizará *Squid* (ufs recomendado), así como la dirección de la caché (/var/spool/squid3), tamaño de la caché (2000 MB), número de directorios y subdirectorios de la caché (16 y 256).
- El parámetro **Cache_mem:** determina la cantidad de memoria ram que será utilizada como caché. Un valor entre 8 y 32 megas es lo recomendable, pero dependerá de la cantidad de memoria que tengamos en el sistema.
- **Maximum_object_size_in_memory.** : Se indica que los ficheros descargados con un tamaño mayor del indicado (en kilobytes) no se guardarán en el disco duro. Por defecto 4 megas.

Archivos de log

Continuando con nuestro *script* nos encontramos con los siguientes parámetros:

```
#Dirección de los registros de squid
access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
```

Las rutas anteriores serán las direcciones donde se almacenarán los logs de acceso al proxy y de caché.

Ejemplo de /var/log/squid/access.log:

```
root@usuarioidesktop:~# more access.log
...
1292981643.277 80 192.168.1.16 TCP_MISS/204 310 GET http://clients1.google.es/generate_204 usuario DIRECT/74.125.230.74 text/html
1292981643.435 109 192.168.1.16 TCP_MISS/204 403 GET http://www.google.es/favicon.ico usuario DIRECT/74.125.230.74 text/html
1292981644.376 1 192.168.1.16 TCP_MISS/204 7165 GET http://23.95.13.98/images/usuario.html?image/jpeg
1292981644.376 0 192.168.1.16 TCP_MISS/204 7165 GET http://23.95.13.98/images/usuario.html?image/jpeg
```

El contenido de dicho fichero son todas las webs, ips, fechas, etc., a las que se acceden y cuyas peticiones pasan a través de *squidSquid*. En este fichero también aparecen aquellas peticiones que son denegadas debido a haber sido bloqueadas mediante la configuración del Proxyproxy. Con la captura anterior del registro del archivo *access.log*, pasaremos a analizar detalladamente cada uno de los conceptos que componen un registro:

1292981643.277 80 192.168.1.16 TCP_MISS/204 310 GET http://clients1.google.es/generate_204 usuario DIRECT/74.125.230.74 text/html

- ✓ 1292981643.277 indica la fecha del acceso. La fecha está en formato de epoch (la cantidad de segundos transcurridos desde 00:00:00 UTC 1-1-1970).
- ✓ 80 corresponde con el tiempo de respuesta. Es posible que el tiempo sea 0 puesto que posiblemente sean páginas a las que se les ha denegado el acceso y por tanto no hay una respuesta.
- ✓ 192.168.1.16 corresponde con la dirección ip IP que ha producido esta petición.
- ✓ "TCP_MISS/204" es el protocolo utilizado, en este caso TCP, "MISS/204" es el significado de que el archivo que se intenta descargar no está en la caché y por tanto la petición tiene que salir a Internet para ser descargada.

Otras opciones son "TCP_MEM_HIT": el archivo si se encuentra en la caché de *Squid* o "TCP_DENIED" se ha bloqueado la petición ya que incumple alguna regla del Proxyproxy.

- ✓ 310: el peso del archivo, en bytes.
- ✓ El método de envío del archivo es el significado de "POST" o "GET".
- ✓ El siguiente parámetro es la propia dirección del archivo en cuestión o la web a la que queremos acceder.
- ✓ DIRECT/74.125.230.74 es la dirección del destino a la que le hacemos la petición.
- ✓ Por último, tenemos el tipo de contenido que estamos realizando con la petición, "text/html".

Tras analizar el log, podemos continuar con la explicación de los distintos parámetros que permiten configurar *Squid*.

Autenticación de usuarios

La autenticación de usuarios es otra opción que implementa *Squid*. A través de este servicio, podemos solicitar un usuario y una contraseña para poder tener acceso al Proxyproxy, y por tanto los servicios como navegación web.

De esta manera, podemos acotar qué usuarios tendrán acceso al Proxy y quiénes no y, de aquellos que tengan acceso, podemos tener un control de qué peticiones realiza.

Los siguientes parámetros son los que permiten configurar el sistema de autenticación:

```
#Autenticacion
auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/claves
auth_param basic children 5
auth_param basic realm Squid proxy-caching web Server
auth_param basic credentialsttl 2 hours
acl passwd proxy_auth REQUIRED
```

Explicaremos cada línea detalladamente:

- ✓ La primera línea indicamos el módulo que vamos a usar para la autenticación de los usuarios que se encuentra en "/usr/lib/squid3/ncsa_auth" así como el fichero que contiene las contraseñas de los distintos usuarios que habrá que generar más adelante con la creación de los distintos usuarios /etc/squid3/claves.
- ✓ La segunda línea indica el número de procesos (5) de autenticación que se va a llevar a cabo: *auth_param basic children 5*
- ✓ La tercera linea determina el mensaje que aparecerá en la ventana que solicite el usuario y la contraseña: *auth_param basic realm Squid proxy-caching web Server*
- ✓ La cuarta linea el tiempo que tardará el Proxy en volver a solicitar de nuevo la clave a cada usuario: *auth_param basic credentialsttl 2 hours*
- ✓ Las últimas dos líneas hacen referencia a la creación de una lista de control a través de la cual activamos la solicitud de autenticación de los usuarios: *acl passwd proxy_auth REQUIRED*

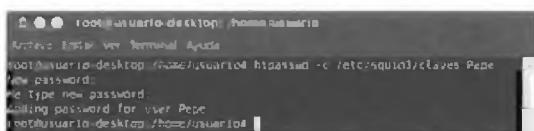
Con estos parámetros hemos terminado de configurar la autenticación en el Proxy pero ahora hay que añadir los distintos usuarios que tendrán acceso al Proxy. Hay que diferenciar los usuarios del sistema con los usuarios del Proxy ya que son totalmente distintos y no tienen ninguna relación. Para añadir los nuevos usuarios lo haremos a través del comando *htpasswd* de la siguiente manera:

```
htpasswd -c /etc/squid3/claves nombre_usuario_nuevo
```

Siguiendo el comando anterior, podemos realizar el siguiente ejemplo:

```
htpasswd -c /etc/squid3/claves pepe
```

Tras ejecutar el comando anterior no pedirá la contraseña del usuario "pepe" que tendremos que introducir en la consola:



Filtros web mediante listas de control de acceso

Las listas de control de acceso nos permiten definir distintos parámetros para conceder o denegar accesos a nuestro Proxy.

Estas listas actúan como un filtro ante las distintas peticiones que pasan por Proxy de manera que podemos acotar que peticiones podrán atravesar nuestro Proxy y cuáles de ellas deberán ser bloqueadas ya que incumplen las expectativas de funcionamiento que realiza nuestro Proxy.

La estructura de una ACL es la siguiente:

```
Acl nombre_de_la_lista tipo_de_filtrado parámetros_del_tipo_de_filtrado
```

A continuación, definimos tres tipos de filtros distintos:

```
# Listas de control de acceso
acl acceso src 0.0.0.0/0.0.0.0
acl nopermitidas url_regex "/etc/squid/nopermitidas"
acl nowebs dstdomain "/etc/squid/nowebs"
```

La primera lista de acceso que hemos definido (acceso) permite escuchar todas las peticiones procedentes de todas las direcciones IP que se comuniquen con el Proxypoxy. Con este parámetro podemos acotar que parte de una red queremos que pase por el Proxy, si fuera necesario. Un ejemplo distinto al anterior sería el permitir solo las peticiones procedentes de la red 172.26.1.0:

```
acl acceso src 172.26.1.0/255.255.0.0
```

La segunda lista de acceso es la que define el filtrado de contenido. Esta lista nos permite añadir al archivo "/etc/squid3/nopermitidas" todas las palabras que queremos que sean filtradas con el fin de bloquear el acceso a las webs que contengan este tipo de palabras:

```
acl nopermitidas url_regex "/etc/squid/nopermitidas"
```

La tercera lista de acceso contiene las webs a las que el Proxy no permitirá el acceso. De igual modo que la lista que filtra el contenido, esta lista también permite añadir al archivo "/etc/squid3/nowebs" todas las URL de las webs que queremos bloquear:

```
acl nowebs dstdomain "/etc/squid/nowebs"
```

Las acl por si mismas no hacen nada, ya que solo definen que lista realizará que tipo de filtrado. Por ello, es necesario permitir o denegar las diferentes ACLs.

```
#control de acceso
http_access allow all
http_access deny nopermitidas
http_access deny nowebs
```

Como vemos, en la primera línea estamos permitiendo todas las peticiones que provienen de cualquier punto de la red a la que se conecta el Proxy.

La segunda línea bloquea la lista llamada "nopermitidas" la cual contenían las palabras no permitidas en una búsqueda.

La tercera línea bloquea la lista llamada "nowebs" que contenían las URL de las webs a las que queremos bloquear el acceso.

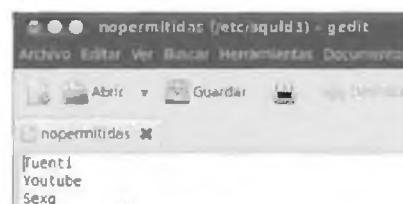
Tras esto, hemos terminado de configurar el fichero de configuración de *Squid* pero aún tenemos que crear un fichero para introducir las webs que no están permitidas. Para ello, ejecutaremos la siguiente sentencia en la consola:

```
gedit /etc/squid3/nowebs
```

El contenido de este fichero serán las direcciones webs de las páginas que vamos a bloquear. El contenido de la siguiente imagen es un ejemplo de cómo podría ser:



Del mismo modo, tendremos que crear el fichero que contenga el contenido que también queremos prohibir. Ejecutamos en la consola la siguiente sentencia: `gedit /etc/squid3/nopermitida`. A continuación, mostramos una imagen de nuestro fichero "nopermitidas":

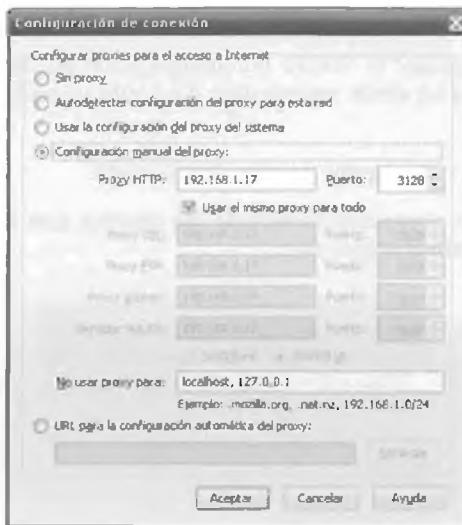


Ya lo tenemos todo configurado y lo último que tenemos que hacer es reiniciar el Proxy para que se efectiva la nueva configuración. Ejecutamos la siguiente sentencia en la consola: `Service squid3 restart`.

Para otras versiones de la distribución Ubuntu, es posible ejecutar la siguiente sentencia: `/etc/init.d/squid3 restart`.

Configuración de cliente proxy

Por último, solo queda configurar los clientes para que las conexiones sean filtradas por el proxy. Para ello en el navegador web del cliente tendremos que introducir la dirección IP y puerto de nuestro Proxy para que navegue a través de él. En caso de tener varios navegadores web disponibles, debemos realizar dicha configuración en todos ellos.



Sin embargo, tenemos otra forma de hacer el **proxy "transparente"** al usuario. Para esto es necesario que el servidor Proxy, además de Proxy, tiene que actuar como un *router*.

A la máquina que aloja el Proxy y hace las funciones de *router* le llegan dos conexiones, una de la LAN y otra que conectará con la puerta de enlace de nuestro servidor.

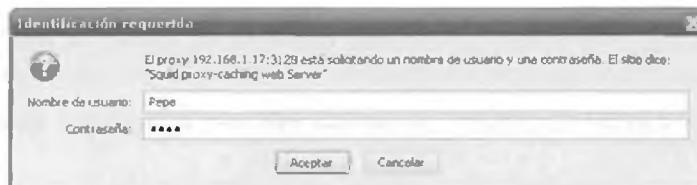
En la configuración IP del cliente tendremos que poner como puerta de enlace la dirección ip IP del Proxy para que el cliente tenga acceso a la red a través del Proxy sin tener que configurar nada en el navegador del cliente. Para ello, añadimos añadiremos en iptables del servidor:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128
```

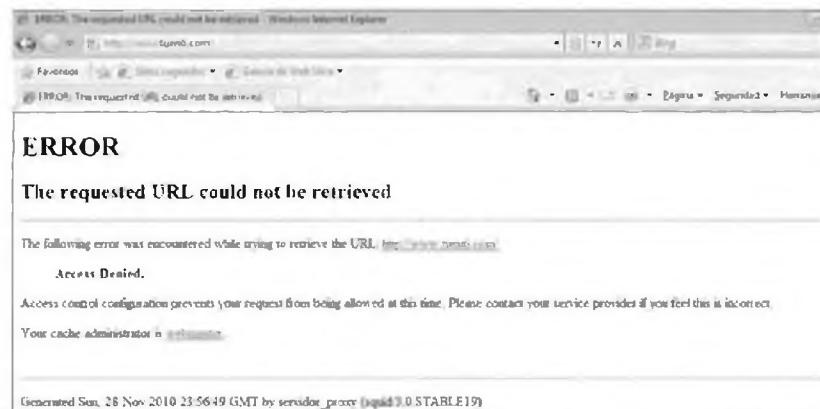
En este caso, eth0 es la interfaz conectado a la red local. Todo lo procedente de esta interfaz con puerto de destino 80 nos lo va a redireccionar al puerto 3128, que es donde tendremos el servidor squid escuchando peticiones.

Autenticación de clientes proxy

Solo nos queda probar el funcionamiento del Proxy. En cualquiera de los 2 casos anteriores, antes de realizar cualquier petición el Proxy nos solicitará nuestro usuario y nuestra contraseña para poder acceder al Proxy:



Una vez autenticados en el Proxy, podemos navegar bajo las restricciones del mismo. Probaremos dichas restricciones intentando entrar en una web no permitida. Para ello intentaremos entrar www.tuenti.com desde el navegador web de algún cliente:



Como vemos en la imagen, el Proxy detecta que la URL introducida no tiene permitido el acceso y bloquea la petición del cliente.

Si la petición es bloqueada por el Proxy el cliente verá en su navegador una pantalla de error y el motivo del error, en el caso anterior se trata de un acceso denegado.

7.3 REFERENCIAS WEB

- Completa información práctica sobre iptables:
<http://www.kriptopolis.org/iptables-0>
- Listado de cortafuegos personales:
<http://www.infospyware.com/cortafuegos/>
- Configuraciones prácticas de cortafuegos:
<http://www.pello.info/filez/firewall/iptables.html>
- Configuraciones de enrutamiento, proxy y cortafuegos para GNU/Linux:
http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_LINUX/frames/frameset_14.html
- Configuraciones de enrutamiento para Windows:
http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_W2000/frames/frameset_enrutamiento.htm
- Configuraciones de funciones de cortafuegos, proxy-caché y servidor VPN para Windows, mediante ISA Server:
http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_W2000/frames/frameset_isa.htm



RESUMEN DEL CAPÍTULO

La conexión a redes públicas por parte de organizaciones potencia las amenazas y ataques a los *routers* de acceso, servidores, incluso a los sistemas internos que poseen información confidencial.

Para evitar este tipo de ataques es necesario disponer de medidas adicionales de seguridad en el perímetro de la organización. Entre otras se han estudiado en este capítulo:

- Enmascaramiento de direcciones IP internas o privadas mediante NAT.
- Filtrado de puertos, aplicaciones asociadas e intentos de acceso a los sistemas mediante **cortafuegos** o *firewalls* tanto en los sistemas perimetrales como en los personales. Dentro de los cortafuegos perimetrales hemos visto las distintas opciones que ofrecen desde *routers* para pequeñas organizaciones, así como configuraciones de servidores con funciones de enrutado y cortafuegos integradas.
- Filtrado de usuarios permitidos, sitios web y búsquedas no autorizadas, mediante servidores proxy. Estos servidores permiten la monitorización y el almacenamiento de accesos a determinados servicios como http, permitiendo mejorar la seguridad y el rendimiento de los mismos. En la mayoría de los casos **se integran** con otros servicios como enrutamiento, NAT y cortafuegos.



EJERCICIOS PROPUESTOS

- 1. Utiliza los siguientes emuladores de *routers* inalámbricos D-Link, y realiza una comparativa entre las opciones de configuración de cortafuegos, proxy y DMZ.

<http://support.dlink.com/emulators/dwl2100ap>
http://support.dlink.com/emulators/di604_reve

(configuración de proxy), para los *routers* anteriores, ¿es posible realizar todas las opciones?

- 2. Realiza la misma configuración de cortafuegos que en la práctica 38 (configuración de cortafuegos), para los *routers* anteriores, ¿es posible realizar todas las opciones?
- 3. Realiza la misma configuración de filtrado proxy de palabras y sitios web que en la práctica 42 (configuración de proxy), para los *routers* anteriores, ¿es posible realizar todas las opciones?
- 4. Investiga sobre la aplicación Webmin como interfaz web para la gestión de servidores bajo GNU/Linux. Descarga e instala la aplicación, y el complemento para la configuración de *Squid*. Realiza la misma configuración que en la práctica 42 (configuración de proxy) mediante la interfaz web de Webmin.
- 5. Para sistemas Windows se encuentra disponible el servidor proxy WinGate. Descarga e instala la aplicación y realiza una configuración similar a la realizada para *Squid*. ¿Cómo podemos ver los logs generados? ¿Qué opciones de filtrado web posee?

■ **6.** La configuración y mantenimiento de listas negras (*blacklist*) de sitios web que queremos restringir en nuestra organización puede llegar a ser una tarea tediosa. Para ello es posible descargar archivos de sitios web poco recomendables o que pertenecen a listas negras de sitios web de confianza y añadirlos a la configuración de nuestro servidor proxy *Squid*. Puedes encontrar archivos con listas negras en sitios web como urlblacklist.com.

■ Descarga el archivo de *blacklist* y anéxalo a la configuración de *Squid*.

■ **7.** Implementa una DMZ con un servidor FTP en el aula e intenta acceder a su contenido desde un equipo ubicado en el exterior del aula. Deberás configurar 2 cortafuegos con diferentes niveles de seguridad y dejando la red DMZ con el servidor FTP en medio.



TEST DE CONOCIMIENTOS

1

Iptables:

- a) Es un conjunto de reglas de *routers*.
- b) Es equivalente a las ACL en Windows.
- c) Emplea características de un *firewall* de Zone Alarm.
- d) Se trata de un cortafuegos basado en reglas de filtrado.

2

En un servidor con cortafuegos iptables que realiza funciones de enrutado únicamente, la opción habitual es:

- a) INPUT.
- b) FORWARD.
- c) OUTPUT.
- d) Ninguna de las anteriores.

3

El archivo donde se almacenan los logs de iptables es:

- a) /var/log/iptables.log.
- b) /etc/init.d/rsyslog.
- c) /var/log/squid/access.log.
- d) /var/log/squid/cache.log.

4

En *Squid* url_regex es una opción:

- a) De control de acceso a determinadas web listadas en un archivo.
- b) De control de acceso a determinadas palabras reservadas listadas en un archivo.
- c) Para registrar sucesos de intento de acceso al proxy.
- d) De control de acceso a los buscadores webs que incluyan palabras reservadas.

5

Los cortafuegos son elementos:

- a) Hardware.
- b) Software.
- c) Pueden ser software y hardware.
- d) Ninguna de las anteriores.

6

Squid como proxy transparente recibe peticiones normalmente en el puerto:

- a) 80.
- b) 53.
- c) 8080.
- d) 3128.

7

Un cliente que utiliza *Squid* como proxy transparente, envía peticiones normalmente al puerto:

- a) 80.
- b) 53.
- c) 8080.
- d) 3128.

8

La integración de un servidor proxy y cortafuegos se denomina:

- a) Screening router.
- b) Dual Homed-Host.
- c) Screened Host.
- d) Screened-subnet.

8

Configuraciones de alta disponibilidad

OBJETIVOS DEL CAPÍTULO

- ✓ Analizar las distintas configuraciones de alta disponibilidad.
- ✓ Valorar la importancia de realizar un buen análisis de riesgos potenciales en sistemas críticos y adoptar medidas para paliar sus posibles consecuencias.
- ✓ Aprender las diferencias, ventajas e inconvenientes entre los sistemas de almacenamiento redundante (RAID) y conocer sus opciones de configuración y prueba.
- ✓ Conocer las opciones de configuración y administración de balanceo de carga entre distintas conexiones de red.
- ✓ Realizar configuraciones de alta disponibilidad de servidores mediante virtualización de sistemas operativos.

8.1 SOLUCIONES DE ALTA DISPONIBILIDAD

Como vimos en el capítulo 1, alta disponibilidad se refiere a la **capacidad de que aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento, debido a su carácter crítico**.

Las empresas con la más alta disponibilidad deben ser más tolerantes a fallos, disponer de sistemas redundantes para los componentes críticos de su negocio y tener una mayor inversión en el personal, procesos y servicios para asegurar que el riesgo de inactividad en las empresas sea mínimo.

En cuanto a las **soluciones** adoptadas en sistemas de **alta disponibilidad**, la **base** de las mismas las estudiamos en el capítulo 2 mediante soluciones de **seguridad pasiva**, aunque para sistemas en los que es necesario un **mayor nivel de seguridad** encontramos:

- **Redundancia en dispositivos hardware**, posibilitando en caso de fallo, la continuidad del servicio. Como ejemplos encontramos duplicados en equipos servidores, fuentes de alimentación (ver la figura siguiente) o dispositivos de red redundantes que no permitan cortes de suministro o caídas de conectividad.



- **Redundancia, distribución y fiabilidad en la gestión de la información.** Se debe procurar que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque, mala operación accidental o situaciones fortuitas o de fuerza mayor. Las técnicas que se estudiarán son:
 - Sistemas RAID de almacenamiento.
 - Centros de procesamiento de datos de respaldo, garantizando copias de seguridad en distintas ubicaciones geográficas.
- **Redundancia en las comunicaciones.** Hoy en día la mayoría de las grandes empresas disponen de una red de oficinas conectadas entre si por red, y los servicios requeridos de las mismas deben estar siempre operativos. Para ello las empresas poseen en ocasiones diferentes conexiones de red independientes, para en caso de fallo de alguna de las líneas, disponer de alternativas. Como caso práctico estudiaremos el **balanceo de carga**.
- **Redundancia y distribución en el procesado.** Los sistemas de clustering o agrupamiento de sistemas servidores permiten escalar la capacidad de procesamiento.
- **Independencia en la administración y configuración de aplicaciones y servicios.** Mediante la **virtualización** hoy en día podemos ofrecer de forma independiente servidores dedicados soportados bajo una misma máquina.

A continuación veremos algunas de las propuestas más empleadas.



NOTICIA DE ACTUALIDAD

Analiza la noticia "Virtualización, cloud y unificación del CPD, principales tendencias tecnológicas para 2011", disponible descargándote el material adicional del libro y cuya fuente es:

<http://www.computing.es/Tendencias/201101030042/INFRAESTRUCTURAS-Virtualizacion-cloud-y-unificacion-del-CPD-principales-tendencias-tecnologicas-para-2011.aspx>. Contesta a las siguientes preguntas:

- ¿Qué es el *cloud computing*? ¿Qué porcentaje y de qué países principalmente están utilizándolo actualmente?
- ¿Qué porcentaje de servidores en producción se estima tener virtualizados en los próximos 3 años, por parte de los responsables de tecnologías de información (IT) en España? ¿Cuáles son las principales barreras y preocupaciones en ese sentido?

8.2 RAID

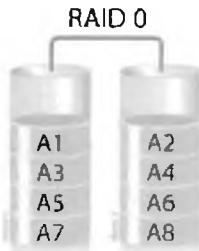
RAID (*Redundant Array of Independent Disks*), o conjunto redundante de discos independientes, originalmente era conocido como *Redundant Array of Inexpensive Disks*, (conjunto redundante de discos baratos) y hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos. La distribución de datos en varios discos puede ser gestionada por:

- **Hardware dedicado:** requiere al menos una **controladora RAID específica**, ya sea como una tarjeta de expansión independiente o integrada en la placa base, que gestione la administración de los discos y efectúe los cálculos de paridad (necesarios para algunos niveles RAID).
- **Software:** el sistema operativo gestiona los discos del conjunto a través de una controladora de disco (IDE/ATA, Serial ATA (SATA), SCSI, SAS o Fibre Channel).
- **Híbridos:** basados en software y hardware específico: mediante controladoras RAID hardware baratas o controladora de disco sin características RAID, pero el sistema incorpora una aplicación de bajo nivel que permite a los usuarios construir RAID controlado por la BIOS.

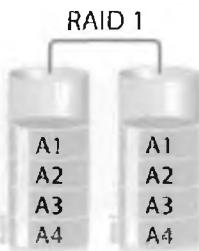
La opción hardware suele ofrecer un **mejor rendimiento** y hace que el soporte por parte del sistema operativo sea más sencillo. Las implementaciones basadas en hardware suelen soportar sustitución en caliente (*hot swapping*), permitiendo que los discos que fallen puedan reemplazarse sin necesidad de detener el sistema.

Las **configuraciones o niveles RAID** estándar y comúnmente usados son:

- **RAID 0 o data striping:** conjunto dividido, distribuye los datos equitativamente entre dos o más discos sin información de paridad que proporcione redundancia, no es redundante. Se usa normalmente para incrementar el rendimiento, aunque también para crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.



- **RAID 1 o data mirroring:** conjunto en espejo. Crea una copia exacta (o **espejo**) de un conjunto de datos en dos o más discos. Un conjunto RAID 1 solo puede ser tan grande como el más pequeño de sus discos. Incrementa exponencialmente la fiabilidad respecto a un solo disco en caso de fallo de uno de los discos. Al escribir, el conjunto se comporta como un único disco, grabando la misma información en todos sus discos constituyentes.



- **RAID 5: conjunto dividido con paridad distribuida:** usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. Al añadir la información de paridad distribuida entre los distintos discos, en caso de fallo de alguno de ellos, será posible recuperar su información a partir de la contenida en el resto de discos. RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, se implementa con soporte hardware para el cálculo de la paridad, aunque es posible realizarlo mediante opciones del sistema operativo.

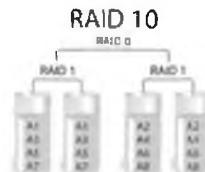
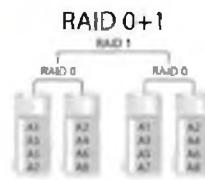


- Otros niveles RAID menos empleados son RAID 2, 3, 4 y 6.

Muchas controladoras permiten **anidar niveles RAID**, es decir, que un RAID pueda usarse como elemento básico de otro en lugar de discos físicos. Los RAID anidados se indican normalmente uniendo en un solo número los correspondientes a los niveles RAID usados, añadiendo a veces un + entre ellos.

Por ejemplo, el RAID 10 (o RAID 1+0) consiste conceptualmente en múltiples conjuntos de nivel 1 almacenados en discos físicos con un nivel 0 encima, agrupando los anteriores niveles 1.

Al anidar niveles RAID, se suele combinar un nivel RAID que proporcione redundancia con un RAID 0 que aumenta el rendimiento. Con estas configuraciones es preferible tener el RAID 0 como nivel más alto y los conjuntos redundantes debajo, porque así será necesario reconstruir menos discos cuando uno falle. Así, el RAID 10 es preferible al RAID 0+1.



PRÁCTICA 8.1

CONFIGURACIÓN DE RAID MEDIANTE SOFTWARE

RAID 1 es utilizado para garantizar la integridad de los datos: en caso de fallo de un disco duro, es posible continuar las operaciones en el otro disco duro sin ningún problema. Para definir este nivel de RAID tendremos que tener al menos dos discos duros de la misma capacidad quedando, de los dos, solamente uno accesible por parte de los usuarios del sistema operativo.

En esta práctica realizaremos un RAID de nivel 1 mediante software en los sistemas operativos Windows XP y Ubuntu 10.04 LTS. Para realizarla será necesario tener al menos 2 discos duros del mismo tamaño, se puede realizar la prueba con máquinas virtuales que posean varios discos duros del mismo tamaño.

RAID en Windows XP

Por defecto en Windows XP Professional no viene activado la opción para hacer RAID por lo que tendremos que activarla siguiendo los siguientes pasos:

Para activar el RAID en Windows XP Profesional tendremos que editar tres archivos del sistema operativo que están en las siguientes direcciones (suponiendo que Windows lo tenéis en la partición C):

```
C:\WINDOWS\SYSTEM32\dmconfig.dll  
C:\WINDOWS\SYSTEM32\dmadmin.exe  
C:\WINDOWS\SYSTEM32\drivers\dmboot.sys
```

- Lo primero que necesitaremos será un editor hexadecimal, por ejemplo podemos utilizar el programa "xvi32". Una vez lo tengamos instalados, copiaremos los ficheros a C:\ (por ejemplo) para editarlos ahí. Lo podemos editar en hexadecimal o modificando la cadena que representan los valores hexadecimales. A continuación mostraremos los cambios que tendremos que hacer:

Editaremos (en formato cadenas de texto) el archivo dmconfig.dll con xvi32:

- Antes: LANMANNT....SERVERNT....WINNT...
- Despues: LANMANNT....WINNT.....SERVERNT

Editaremos el archivo dmadmin.exe con xvi32 y pondremos:

- Antes: servernt....lanmannt....ProductT
- Despues: winnt.....lanmannt....ProductT

Editaremos el archivo dmboot.sys con xvi32:

O en cadena de texto:

- Antes: t.T.y.p.e...WINNT...SERVERNT....
- Después: t.T.y.p.e...SERVERNTWINNT.....

2. Despues tendremos que sustituir los archivos originales por los modificados, pero no lo podemos hacer directamente en el Windows porque este los volvería a sustituir por los originales. Así que tendremos que usar la consola de recuperación arrancando con un cd de instalación de Windows XP o arrancando en modo prueba de fallos y sustituyendo los archivos modificados. Para ello:

Introducimos un cd de instalación de Windows XP y arrancamos desde el mismo, esperamos que se inicie el asistente y elegimos la opción "recuperar una instalación de Windows XP usando la consola de recuperación", presionando la tecla R.

Tras esto, nos aparecerá una lista de las instalaciones de Windows que ha detectado en los discos duros. Le damos al número que deseemos modificar.

Luego nos pedirá la contraseña del administrador de ese Windows. Una vez estamos en la consola, suponiendo que los archivos modificados los dejamos en la raíz del C:\ tendremos que escribir las siguientes ordenes:

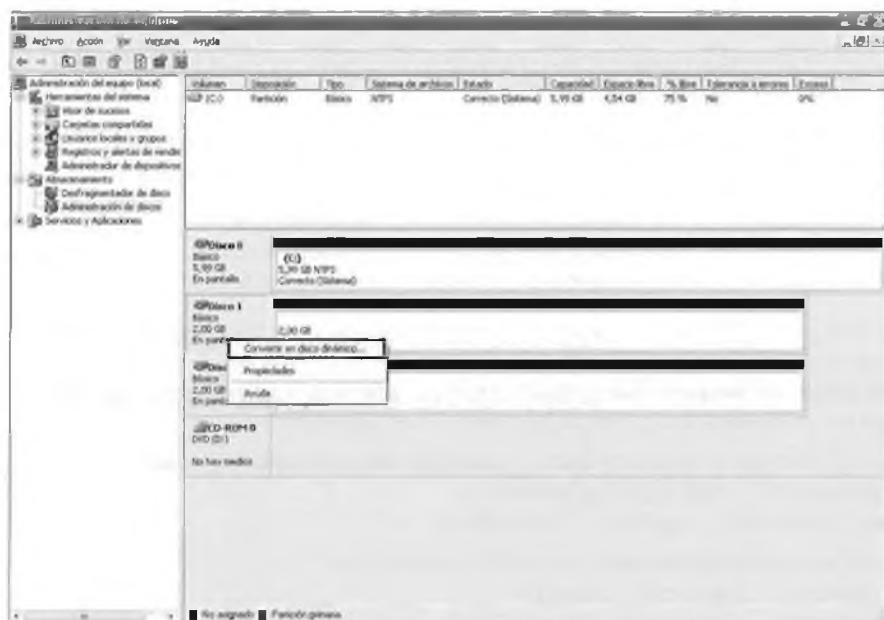
```
>>copy C:\dmconfig.dll C:\WINDOWS\SYSTEM32\  
>>copy C:\dmadmin.exe C:\WINDOWS\SYSTEM32\  
>> copy C:\dmboot.sys C:\WINDOWS\SYSTEM32\DRIVERS\
```

Por último escribimos "exit" y el equipo se reiniciará.

Con esto ya tendremos activadas las opciones para hacer RAID 1 en Windows XP Professional.

3. Ahora vamos a configurar el RAID 1 con los siguientes pasos, una vez reiniciado Windows normalmente:

Presionamos el botón derecho en Mi PC y seleccionamos Administrar, luego vamos a Almacenamiento y dentro de él a **Administración de discos**. Ahora en la lista de los discos duros, en cada fila a la izquierda tendremos un recuadro que pondrá el tipo de disco (Básico, Dinámico) y el tamaño entre otras opciones. Con el botón derecho sobre ese recuadro y pulsamos Convertir en dinámico, en los discos que deseemos crear nuestra unidad RAID 1.



A continuación, presionamos el botón derecho en el espacio no particionado y seleccionamos **Nuevo volumen**. Se iniciara el asistente y le damos al botón *Siguiente*.

Ahora nos aparecerá la lista de los tipos de volúmenes que podemos crear (Simple, Distribuido, Seccionado, Reflejado, Raid-5), a diferencia de antes ya nos aparece el tipo **Reflejado** (que es el que nos interesa). Seleccionamos Reflejado equivalente a RAID 1 y le damos al botón *Siguiente*.

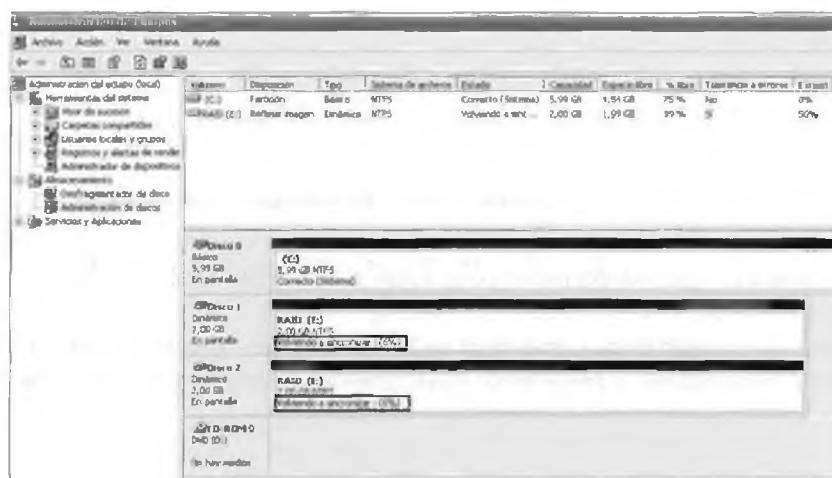
Nos aparecerá una ventana en la que tendremos que **añadir a la zona de Seleccionado los dos discos**. Para añadir alguno, tendremos que seleccionarlo en la zona de Disponible y dárle al botón *Agregar*. Una vez que tengamos los dos añadidos le daremos al botón *Siguiente*.

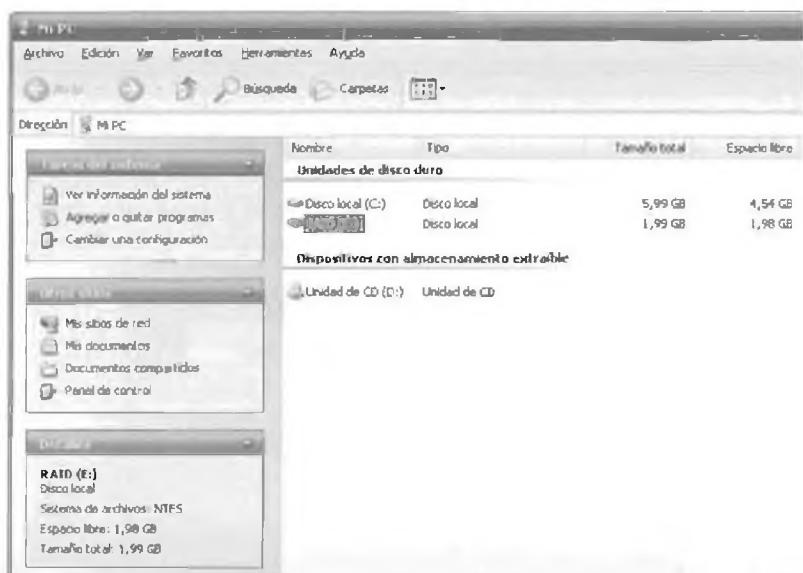


En la siguiente ventana elegiremos la letra que queramos para la partición con RAID 1 y presionaremos el botón *Siguiente*.

Tras esto, elegiremos el formato de la partición, la etiqueta de la partición, marcamos dar formato rápido y le damos al botón *Siguiente*. Por último nos mostrará un resumen de la configuración y le daremos al botón *Finalizar*.

Ahora nos mostrará, en las particiones en RAID, un mensaje que indicará Volviendo a sincronizar con un porcentaje. Esto significa que se están sincronizando los dos discos duros. Tendremos que esperar a que acaben y muestre correcto para poder usar nuestra partición en RAID.





4. Ya está todo hecho, tenemos nuestra partición de datos con RAID 1. Si queremos asegurar que funciona, podemos hacer lo siguiente: apagamos el ordenador y desconectamos uno de los discos duros que tienen una de las dos particiones en el RAID 1. Encendemos el ordenador. Creamos un fichero en la partición del RAID 1 y volvemos a apagar el ordenador.

Conectamos de nuevo el disco duro que habíamos desconectado y volvemos a encender el ordenador. Le damos al botón derecho a *Mi PC* y seleccionamos *Administrar*. Luego vamos a *Almacenamiento* y dentro de él a *Administración de discos*. Veremos que en las dos particiones del RAID aparece el mensaje **Error de redundancia**.

Seleccionamos el disco duro que habíamos desconectado, en el recuadro de la izquierda donde aparecen datos suyos le damos al botón derecho del ratón y seleccionamos **Reactivar disco**.

Ahora aparecerá un mensaje en las dos particiones del RAID 1 que indicará "Regenerando" con un %. Entonces empezará la reconstrucción de los datos. Esperamos a que a finalice y ponga Correcto.

RAID en GNU/Linux

La configuración del RAID en Linux la haremos bajo la distribución Ubuntu. La podremos hacer fácilmente gracias a la aplicación "utilidad de disco" que integra la nueva versión de Ubuntu para particionar y dar formato a los dispositivos de almacenamiento.

1. En primer lugar iremos a Sistema – Administración – Utilidad de Disco.

Para iniciar la configuración del RAID 1 pincharemos en Archivo – Crear – Conjunto RAID...

Se iniciará un asistente que nos permitirá seleccionar el tipo de RAID que deseamos configurar así como las unidades de disco que intervienen en el RAID.

En nuestro caso seleccionaremos como nivel de RAID "Espejo – (RAID 1)", introduciremos un nombre para el conjunto "Raid Espejo" y justamente abajo seleccionaremos los dos discos duros que formarán el RAID:



Si todo está correcto, pulsaremos en "Crear" y nos pedirá que introduzcamos la clave de Administrador tanto para crear las particiones en los discos como para crear el RAID por software.

Una vez creado el conjunto RAID nos aparecerá el conjunto de la siguiente manera:



Tras crear el conjunto el sistema resincroniza ambos discos duros para replicar la información.

2. Una vez terminada la resincronización, tendremos que particionar el volumen del Raid Espejo para crear una partición que sea utilizable por el sistema. Para particionar el volumen pulsamos en "formatear volumen":

Seleccionaremos el tipo de sistema de archivos e introduciremos un nombre para el nuevo volumen. Pulsaremos en "Formato":

3. Al pulsar nos pedirá la confirmación. Tras esto solo nos queda montar la unidad para que sea visible y poder usarla con normalidad. Pulsaremos en "montar volumen".

Montada la unidad, nos aparecerá el icono en el escritorio del sistema del nuevo volumen "Raid 1" que acabamos de configurar.



La manipulación del volumen "Raid 1" es igual que si fuera un disco duro simple por lo que podemos cortar, pegar, mover, renombrar, etc., dentro del mismo.

8.3 BALANCEO DE CARGA

Un balanceador de carga es un dispositivo ya sea hardware o software que se dispone conectado a un conjunto de servidores de manera que **asigna y reparte las peticiones** que provienen de los clientes a los distintos servidores a los que se conecta dicho dispositivo.

Estos dispositivos aplican una serie de algoritmos, como el conocido Round Robin, para repartir la carga de forma equilibrada.

La utilidad de estos dispositivos radica en poder repartir la carga y excluir aquellas conexiones de destino que se encuentren caídas en un momento determinado de manera que un cliente cuya dirección IP de su servidor DNS se encuentre caída, el balanceador de carga detectará que esa dirección IP se encuentra inactiva (el servidor no escucha las peticiones ya sea por fallo en hardware o en software del servidor) y las peticiones cuyo destino se dirigen al servidor caído se redireccionarán a otro servidor DNS que haya conectado al dispositivo encargado del balanceo de la carga.

Este sistema también es muy útil a la hora de **unificar dos o más conexiones** con salida hacia Internet en **una sola**. Al instalar un balanceador de carga al que se conecten varias líneas de Internet, podemos repartir la carga de salida a Internet entre las líneas, pudiendo definir que cantidad de peticiones saldrán por una línea y que cantidad por otra, dependiendo por ejemplo de su velocidad y fiabilidad.

PRÁCTICA 8.2

BALANCEO DE CARGA

En la siguiente práctica estudiaremos como configurar mediante software balanceo de carga mediante **tablas de enrutamiento** en sistemas GNU/Linux y mediante **Kerio Winroute** bajo Windows.

Balanceo de carga mediante tablas de enrutamiento GNU/Linux

Nuestra práctica la realizaremos en la distribución Ubuntu, realizando balanceo de carga entre dos líneas ADSL de diferentes velocidades. La carga de las líneas según la configuraremos en proporción 2-1, es decir, por cada 2 peticiones a la línea rápida de ADSL saldrá 1 petición por la línea lenta de ADSL.

Esta proporción se puede variar según nuestra necesidad ya que si disponemos de dos ADSL de la misma velocidad lo lógico será balancear la cargar al 50%.

En esta práctica necesitaremos una máquina con tres interfaces de red de las cuales: una se conecta a la LAN y las otras dos a las distintas líneas de ADSL. El esquema puede ser el siguiente:

Empezaremos definiendo las direcciones IP de cada una de las tarjetas de red que contiene nuestra máquina que realizará el balanceo de carga:

Ip router ADSL 1 (rápida): 192.168.1.1/24
 Ip router ADSL 2 (lento): 192.168.2.1/24

Servidor con balanceo de carga:

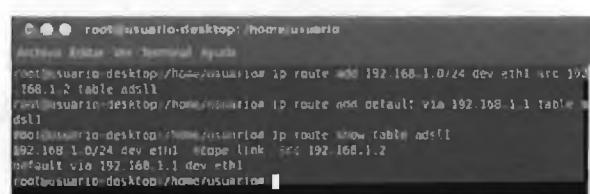
- ✓ eth1 (conectado a router ADSL1): 192.168.1.2/24
- ✓ eth2 (conectado a router ADSL2): 192.168.2.2/24
- ✓ eth0 (será la nueva puerta de enlace de la LAN): 192.168.3.1/24

1. Empezamos a configurar las 3 interfaces del servidor. Para ello nos dirigimos a Sistema - Preferencias - Conexiones de red.
2. Mediante un terminal definiremos dos tablas de enrutamiento distintas que emplearemos para cada una de las líneas de ADSL:

```
# echo 200 adsl1 >> /etc/iproute2/rt_tables
# echo 201 adsl2 >> /etc/iproute2/rt_tables
```

3. Ahora nos centramos en la tabla de enrutamiento del ADSL1. La siguiente configuración define que la red 192.168.1.0/24 es la red conectada a la interfaz eth1 que tiene una dirección IP 192.168.1.2 y que los paquetes con la salida a Internet serán enrutados por la tabla adsl1. Podemos comprobar que la configuración ha sido introducida mediante "ip route show table adsl1":

```
ip route add 192.168.1.0/24 dev eth1 src 192.168.1.2 table adsl1
ip route add default via 192.168.1.1 table adsl1
```



```
root@usuariodesktop:~# ip route add 192.168.1.0/24 dev eth1 src 192.168.1.2 table adsl1
root@usuariodesktop:~# ip route add default via 192.168.1.1 table adsl1
root@usuariodesktop:~# ip route show table adsl1
192.168.1.0/24 dev eth1 scope link src 192.168.1.2
default via 192.168.1.1 dev eth1
root@usuariodesktop:~#
```

4. Del mismo modo introducimos las sentencias pertinentes para la configuración de la tabla de la línea ADSL2:

```
ip route add 192.168.2.0/24 dev eth2 src 192.168.2.2 table adsI2
ip route add default via 192.168.2.1 table adsI2
```

5. Tras definir cada una de las tablas de enrutamiento de los ADSL tendremos que definir la tabla de enrutamiento principal para que los paquetes sean enrutados correctamente.

La configuración individual de las tablas anteriores es para cuando el tráfico está en una de las dos subredes de salida y se necesita saber como enrutarlo. Las sentencias para configurar la tabla principal son las siguientes:

```
ip route add 192.168.1.0/24 dev eth1 src 192.168.1.2
ip route add 192.168.2.0/24 dev eth2 src 192.168.2.2
```

Mediante *ip route show*, veremos el resultado configurado.

6. Tras configurar la tabla principal tendremos que definir las reglas de enruteo. Esto sirve para aplicar las reglas almacenadas en cada una de las tablas cuando se cumple que vienen de las ips correspondientes:

```
ip rule add from 192.168.1.2 table adsI1
ip rule add from 192.168.2.2 table adsI2
```

7. La última sentencia es la más importante de toda la configuración ya que es la que **define el balanceo de carga**.

Con esta sentencia lo que indicamos son las rutas por defecto que tiene que seguir los paquetes cuando su destino no esté dentro de nuestra red con el añadido que en función de la carga saldrá por una puerta de enlace o por otra:

```
ip route add default scope global nexthop via 192.168.1.2 dev eth1 weight 2 nexthop via 192.168.2.2 dev eth2 weight 1
```

Weight 2 y weight 1 son los pesos asignados a cada interfaz de red, son modificables. En el supuesto caso de tener más líneas ADSL conectadas al balanceador de carga habrá que definir el balanceo de carga para cada línea de ADSL adicional que conectemos.

8. Hasta aquí tenemos listo el balanceador de carga pero es importante no olvidar habilitar el enruteo entre las tarjetas de red para que las peticiones que provienen de la LAN sean transferidas a Internet.

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth1 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth2 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

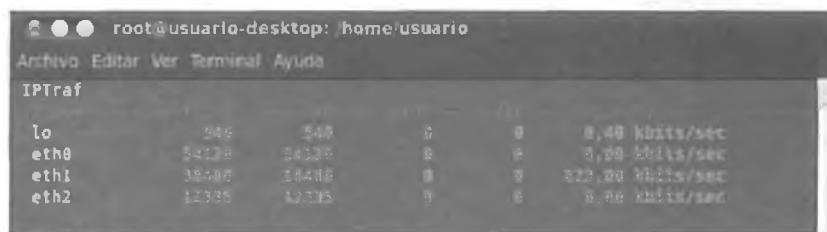
9. Para visualizar que el balanceador realiza su tarea correctamente tenemos a nuestra disposición la herramienta **Iptraf**. Esta herramienta nos permite tener un control de aquellas conexiones que están activas y un contador de paquetes de cada una de las interfaces, entre otras opciones. Para instalarla:

Una vez instalada la ejecutamos *iptraf*. Una vez abierta la herramienta nos dirigimos a la sección "General interface statistics":



En dicha sección tendremos las estadísticas de paquetes que transitan por cada una de las interfaces de red de nuestro balanceador de carga.

Si visualizamos los resultados veremos que del total de los paquetes que provienen de la *LAN* (eth0) gran parte han salido a Internet por la interfaz eth1 que corresponde con el ADSL rápido mientras que una parte más pequeña de los paquetes han salido por la interfaz eth2 que corresponde con el ADSL lento:



Balanceo de carga mediante Kerio Winroute (Windows)

A continuación, realizaremos el balanceador de carga por software en el sistema operativo Windows 7 mediante el programa **Kerio Winroute**. En el capítulo 7 vimos su uso configurando un cortafuegos personal.

Realizaremos la misma configuración de red que para GNU/Linux, en las 3 interfaces de red necesarias.

Podemos iniciar el programa de administración "Kerio Administration console" que nos permitirá realizar la configuración de nuestro balanceador de carga. Como todo programa de administración, nos pedirá que nos conectemos con el usuario y la contraseña definida en la instalación para poder administrar el software. Una vez logueados, el programa ejecuta un asistente que nos permite realizar una **configuración básica** del mismo.

1. En dicha configuración tendremos que seleccionar la opción “Múltiples enlaces de Internet - Balanceo de carga de tráfico”



Tras esto, tendremos que seleccionar que interfaces serán afectadas por el balanceo de carga. Pulsaremos el botón "agregar". En la ventana que nos aparece tendremos que escoger los adaptadores de red que tienen conexión con Internet. Así mismo, podremos configurar el ancho de banda de cada enlace.

La siguiente pantalla del asistente permite realizar la configuración de cortafuegos mediante bloqueo o filtrado de protocolos. A continuación en la configuración de VPN, en la que deseleccionaremos todas las opciones.

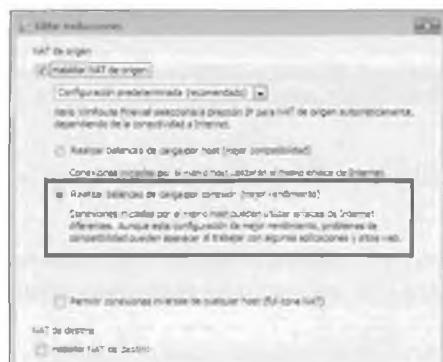
Si tuviéramos algún servidor en la LAN que quisiéramos que fuera visto desde Internet, en la siguiente pantalla tendríamos que introducir la dirección IP y el servicio que estarían activos en dicho servidor. En caso contrario, tendríamos que saltar dicha pantalla. Por último, terminaremos la instalación pulsando el botón "Finalizar" del asistente.

2. Tendremos que configurar un aspecto fundamental para activar el balanceo de carga. Nos dirigimos a la sección “configuración” y entramos en “políticas de tráfico”. En esta pantalla nos mostrará todos los permisos y restricciones que tienen los servicios.

En la regla de "Acceso a Internet (NAT)" tendremos que modificar el tipo de traducción que realiza. Para ello, pulsaremos con el botón derecho sobre el campo "Traducción" de dicha regla y seleccionaremos "Editar traducción".

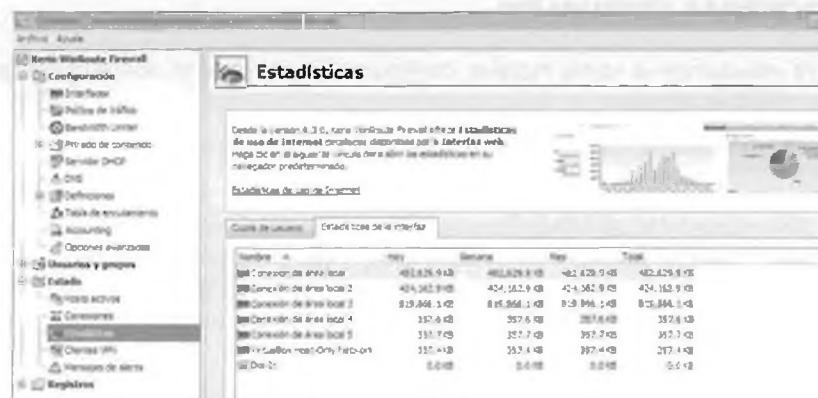


En la ventana de configuración de la traducción tendremos que seleccionar la opción “Realizar balanceo de carga por conexión (mejor rendimiento)”.



3. Si ahora empezamos a realizar peticiones y nos vamos a las estadísticas de la salida a Internet veremos como la carga se balancea entre las dos interfaces.

Para ello nos iremos a la sección "Estado" y pincharemos en "Estadísticas". En dicha pantalla nos iremos a la pestaña "Estadísticas de la interfaz" y veremos como la carga que proviene de la LAN se está balanceando entre las interfaces con salida a Internet.



8.4 VIRTUALIZACIÓN

La virtualización permite la ejecución simultánea de distintos sistemas operativos sobre una aplicación ejecutada y soportada bajo un equipo y un sistema operativo determinado. Permite realizar una abstracción de los recursos de un sistema, creando una capa entre el hardware de la máquina física y el sistema operativo de la máquina virtual.

Esta capa de software maneja, gestiona y arbitra los cuatro recursos principales de un ordenador (CPU, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales que se estén ejecutando en un momento determinado. De modo que nos permite tener varios ordenadores virtuales, con distintos sistemas operativos, ejecutándose sobre el mismo ordenador físico.

El software de gestión de máquinas virtuales se distribuye por empresas como **Microsoft (Virtual PC)**, **VMWare (VMWare)** u **Oracle (Virtual Box)**.

Una vez instalada la aplicación de gestión de máquinas virtuales, el proceso para poder ejecutar distintos sistemas operativos se resume en:

- ✓ Crear y configurar los recursos hardware que darán soporte a la instalación de un determinado sistema operativo.
- ✓ Una vez creada la máquina virtual soporte, instalar mediante una imagen ISO o un CD/DVD de instalación el sistema operativo.
- ✓ Arrancar y utilizar el sistema operativo, pudiendo instalar aplicaciones, guardar datos de forma independiente al sistema operativo que soporta el software gestor de máquinas virtuales.

Sucesivamente podemos ir modificando configuraciones creadas, creando y ejecutando distintas máquinas virtuales independientes dentro del gestor de máquinas virtuales.

PRÁCTICA 8.3



CREACIÓN DE MÁQUINAS VIRTUALES

En la siguiente práctica estudiaremos como instalar, configurar y usar, bajo Windows 7, la aplicación de gestión de máquinas virtuales VMWare Server.

Para la instalación de VMware Server tendremos que descargar, en primer lugar, el paquete instalador de la web oficial de VMware: <http://www.VMware.com/es/>.

Para poder descargar los instaladores de VMware es necesario registrarse en la web. Podemos realizar el registro antes de elegir el producto en la sección "Cuenta" presente en la página principal de la web o de manera instantánea cuando elegimos la descarga de un producto, en nuestro caso VMware Server, rellenando el formulario de registro. Para los usuarios que tengan cuenta en la web, solo tendremos que introducir los datos necesarios para autenticarnos.

Una vez logueados en la web, nos aparecerá una ventana en la que tenemos tanto los seriales de cada uno de los productos de VMware Server como los links de los instaladores.

En nuestro caso copiaremos el serial (Licensing) y descargaremos de forma manual el paquete VMware Server 2 for Windows Operating Systems.

Instalación VMware Server 2.0.2 en Windows 7

1. Una vez descargado el instalador lo ejecutaremos en el sistema operativo y se iniciará el asistente de instalación. En la instalación podemos modificar el directorio donde se almacenarán las máquinas virtuales así como el nombre de la máquina, *Host*, y los puertos a través de los cuales accederemos a la administración web. En un momento de la instalación nos pedirá que introduzcamos el nombre de usuario (necesario para la administración web), el nombre de la compañía y el número de serie:
2. Una vez reiniciado el equipo podemos encontrar todos los componentes de VMware en el menú de inicio. Podemos arrancar el programa desde los accesos directos (VMware Server Home Page) o entrar en un navegador web e introducir las siguientes direcciones para acceder a la administración web:

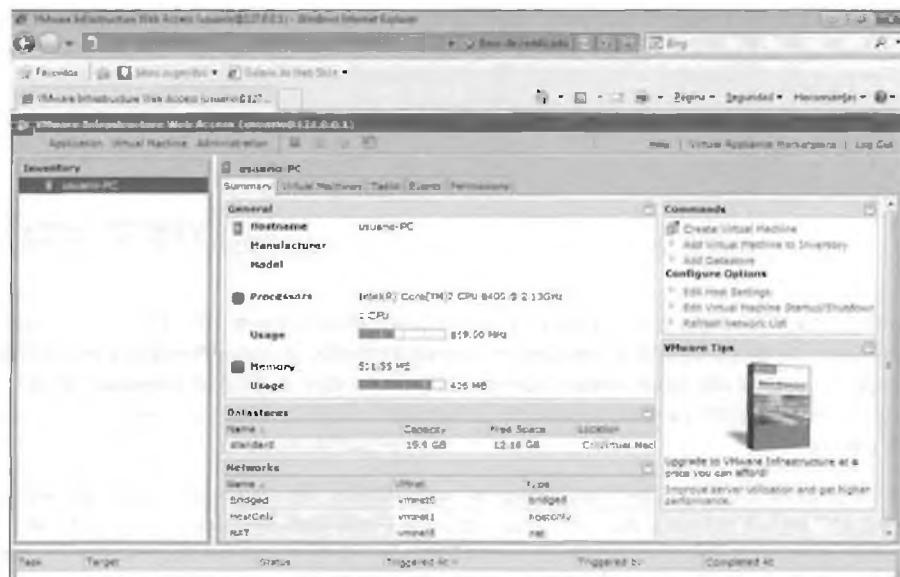
http://<Dirección_ip>:8222
https://<Dirección_ip>:8333



Una vez introducido nombre de usuario y contraseña configurados en la instalación, en la parte derecha de la pantalla tenemos las distintas opciones para crear o añadir máquinas virtuales o Datastores.

En la parte central tenemos un resumen de las características de nuestro Host y de las máquinas virtuales que vayamos creando, cuyo listado aparece en la izquierda, que nos permite tener un control acerca del uso de la CPU, la cantidad de RAM consumida, espacio en disco y conexiones de red.

La parte inferior hace referencia a un registro de actividades en las máquinas virtuales. Se registran cuando se inicia una máquina virtual, cuando se detienen, cuando se modifican, etc.



Creación de una nueva máquina virtual en VMware Server.

3. Para la creación de una máquina virtual nueva nos dirigimos a la opción "Create virtual Machine" en el cuadro de la derecha de la pantalla.

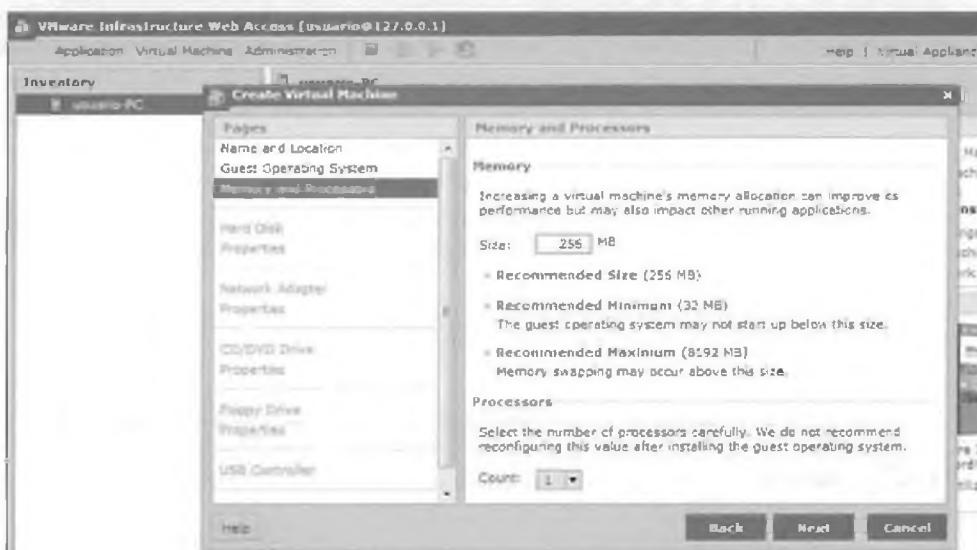
A continuación, nos aparecerá un **asistente** que nos permitirá configurar los aspectos básicos de nuestra máquina virtual.

En primer lugar nos pide que configuremos el nombre de la máquina virtual y la ubicación donde se almacenará.

En nuestro caso, vamos a crear una máquina virtual para instalar el sistema operativo **Freenas** para posteriormente realizar una serie de pruebas como servidor NAS (analizado en el Capítulo 2).

La siguiente pantalla del asistente hace referencia al **tipo de sistema operativo** que vamos a instalar en la máquina virtual y la versión de dicho sistema operativo. Puesto que Freenas es una versión de FreeBSD, seleccionaremos "Other operating systems" y en la versión elegimos "FreeBSD (32-bits)".

A continuación, tendremos que definir la cantidad de **memoria RAM** y el número de procesadores (hilos) que usará nuestra máquina virtual. En nuestro caso, elegimos 256 MB de memoria RAM y una CPU. Debemos tener en cuenta que los recursos hardware que configuremos serán consumidos de la máquina física en la que se ejecute. Por lo que el ajuste de la memoria RAM suele ser un parámetro limitador ya que no es posible ejecutar simultáneamente tantas máquinas virtuales como se desee.



Posteriormente se definirá si la máquina virtual usará un nuevo **disco duro** virtual o uno existente por ejemplo de otra máquina virtual. Ya que nuestra máquina es completamente nueva, elegimos la opción "Create a new virtual disk". Al elegir la opción de disco virtual nuevo tendremos que definir el tamaño del disco y la ubicación del mismo. En esta misma sección también podemos modificar el adaptador de nuestro disco duro y el número del dispositivo que usará.

Tras definir el disco duro, tendremos que configurar el **adaptador de red** que usará la máquina virtual. Para definirlo pulsaremos en "add a network adapter". Las opciones que nos aparecen en cuanto al adaptador de red son bastante sencillas ya que la configuración de los adaptadores de red estará gestionada por la herramienta "Manage Virtual Networks" que veremos con más profundidad en la siguiente práctica.

Podemos elegir tres modos de funcionamiento de nuestro adaptador de red ya sea modo *Bridged*, modo *Host-only* o modo *NAT* (la configuración la realizaremos más adelante). En nuestro caso, seleccionaremos el modo *Bridged*, ya que la máquina virtual se encontrará en red con la máquina física y el resto de equipos de la red de ésta. En este modo debemos asignarle una configuración IP dentro de la máquina virtual a su adaptador de red. Activaremos la opción de “connect at power on”, para que esté activa cuando arrancaremos nuestra máquina virtual.

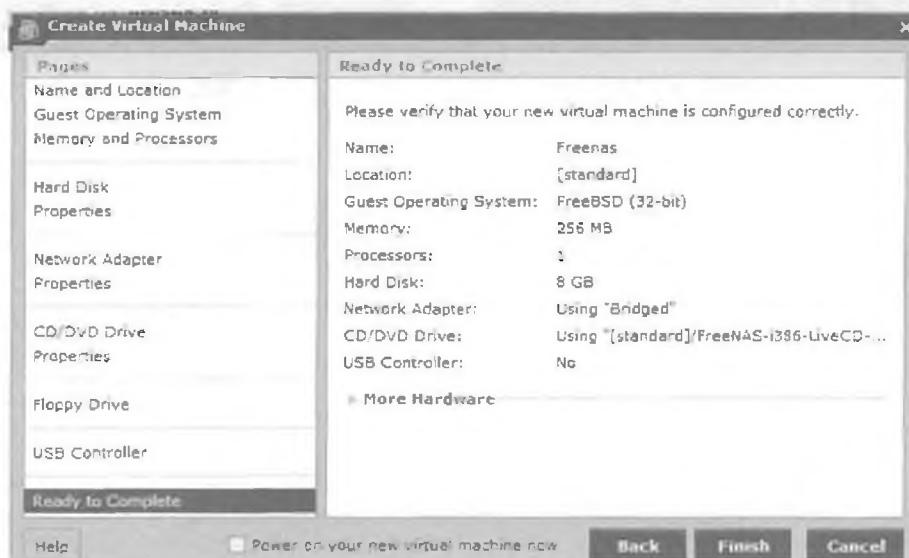
La **instalación de nuestra máquina virtual** es posible realizarla de dos modos, bien sea a través de una imagen .ISO o a través de la unidad de CD/DVD del *Host host* físico.

En nuestro caso añadimos una imagen ISO por lo que pulsamos en “Use an ISO Image”. Al elegir que queremos instalar la máquina virtual a través de una imagen ISO nos aparecerá una pantalla en la que tendremos que seleccionar la ubicación de la imagen ISO dentro del Datastore que tenemos configurado, es decir, la imagen ISO tiene que estar ubicada en la misma carpeta que contiene las máquinas virtuales.

Del mismo modo que la unidad de CD/DVD configurada anteriormente, podemos seleccionar el adaptador y el número de dispositivo que utilizará.

Podemos hacer lo mismo si queremos usar una unidad de Floppy Disk, en nuestro caso, no integraremos esta unidad en nuestra máquina virtual. Del mismo modo podemos utilizar dispositivos USB conectados en la máquina *Host host* para tener acceso desde la máquina virtual. En nuestro caso, tampoco integraremos esta opción.

Por último, el asistente nos da un resumen de la configuración que acabamos de realizar. Si estamos de acuerdo podemos pulsar el botón “finish” para terminar de definir la máquina virtual.



Ya tenemos nuestra máquina virtual creada, ahora solo tenemos que arrancarla e instalar el sistema operativo como si de una máquina normal se tratara. Lo veremos junto con el funcionamiento en la práctica 47 (servidor NAS virtualizado).

La creación de máquinas virtuales permite realizar copias de seguridad y restauración de las mismas de forma muy sencilla. Las distintas máquinas virtuales creadas se encuentran accesibles en la carpeta que hallamos configurado (normalmente C:/ Virtual Machines).

PRÁCTICA 8.4

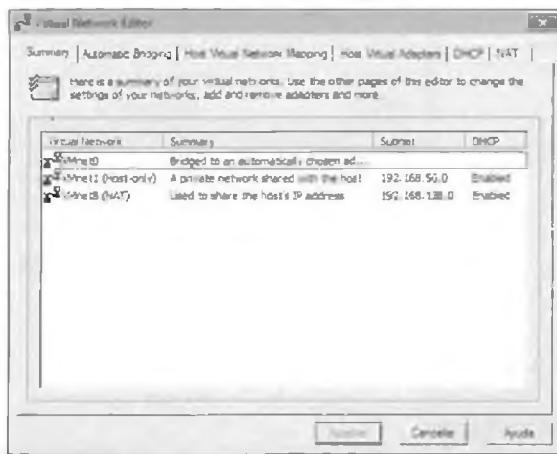
CONFIGURACIÓN DE RED DE MÁQUINAS VIRTUALES

Los **modos de funcionamiento** que podremos asociar a cada tarjeta de red virtual, en cada máquina virtual son:

- **Bridge** o puente permite conectar la máquina virtual a la red que usa el equipo anfitrión. Conecta el adaptador de red de la máquina virtual, con el adaptador "físico" o real del equipo. Es la opción más empleada.
- **Host-only** permite al sistema anfitrión comunicarse con los sistemas invitados de las máquinas virtuales instaladas en el equipo. Las máquinas virtuales sólo pueden comunicarse directamente con el sistema host físico y las máquinas virtuales que también son miembros de la misma red.
- **NAT** permite realizar NAT entre las máquinas virtuales y la red externa a la que pertenece el *host* físico. Permite por tanto la conexión a una red externa en aquellos casos en que únicamente se dispone de una dirección IP, que usa el anfitrión. Por ejemplo se puede conectar una máquina virtual a Internet a través del adaptador de red del equipo anfitrión. Se emplea para aislar la comunicación exterior con las máquinas virtuales.

Como hemos comentado anteriormente, tenemos una herramienta instalada que nos permite configurar ciertos aspectos de las distintas formas de funcionamiento de los adaptadores de red en las máquinas virtuales. Esta herramienta se llama "Manage Virtual Networks" y la podemos encontrar en Inicio - todos los programas - Vmware - Vmware Server - Manage Virtual Networks.

Si abrimos la herramienta nos muestra una pantalla en la que tenemos seis pestañas de configuración:



La primera pestaña "Summary" hace referencia a un resumen de los adaptadores virtuales que están funcionando con VMware así como de la descripción de cada adaptador, subred en la que está trabajando y si tiene activo o no el servicio DHCP que integra la misma herramienta para los modos NAT y Host-only.

La siguiente pestaña "Automatic Bridging" permite controlar y configurar un puente de red entre el adaptador VMnet0 con el adaptador de red física del host.

La tercera pestaña "Host Virtual Network Mapping" permite definir, configurar y desactivar distintos adaptadores de red virtuales que podemos asociar a una máquina virtual y que se comportarán, para las distintas máquinas virtuales configuradas en un mismo modo, como un *switch* virtual interconectando a las distintas máquinas virtuales. Dependiendo del **modo de funcionamiento** que tenga cada uno de ellos podemos observar como podemos configurar distintas opciones.

En el caso de VMnet8, el funcionamiento que tiene por defecto es para realizar NAT, por lo que en dicho adaptador podemos configurar la subred propia en la que trabaja, un servidor DHCP para que asigne las direcciones IP en las máquinas virtuales configuradas con este adaptador y otros aspectos de configuración de NAT como las opciones para la puerta de enlace virtual, así como el port forwarding (en caso de tener acceso a servidores en la máquina virtual desde el exterior), DNS y Netbios.

En la sección “Host Virtual Adapters” muestra una lista de los adaptadores de red que se han creado en el *Host host* físico a través de VMware, por defecto VMNet 1 (*Host-only*) y VMNet8(NAT). Mediante esta sección podemos añadir, habilitar, deshabilitar y eliminar adaptadores según las necesidades.

En la sección “DHCP” tenemos lo referente al funcionamiento del servidor DHCP en cada uno de los adaptadores, de manera que podemos iniciar, parar y reiniciar el servidor o configurar cualquier parámetro del servidor en cada uno de los adaptadores.



Por último, en la sección “NAT” podemos seleccionar que adaptador de red realizará las funciones de NAT así como iniciar, parar y reiniciar el servicio.

Como vemos, VMware tiene una gran cantidad de configuraciones posibles en función de las necesidades que tengamos.

8.4.1 VIRTUALIZACIÓN DE SERVIDORES

Una de las aplicaciones más comunes de la virtualización es poder independizar la administración de servidores bajo una misma máquina física. Las ventajas de disponer de servidores virtualizados frente a servidores físicos son las siguientes:

- ✓ **Ahorro de costes:** podremos adquirir un solo servidor, aunque más potente, y no tener que comprar más servidores sino solamente ir creándolos en el gestor de máquinas virtuales. También permite ahorro en el coste de mantenimiento y en el de personal, además de ahorrar espacio.
- ✓ **Crecimiento más flexible:** instalar un nuevo servidor es mucho más sencillo y rápido frente a hacerlo con un servidor físico.
- ✓ **Administración simplificada:** desde la consola del gestor de máquinas virtuales podemos aumentar o reducir los recursos para una determinada máquina, reiniciarla, instalar parches o simplemente borrarla en caso de problemas.

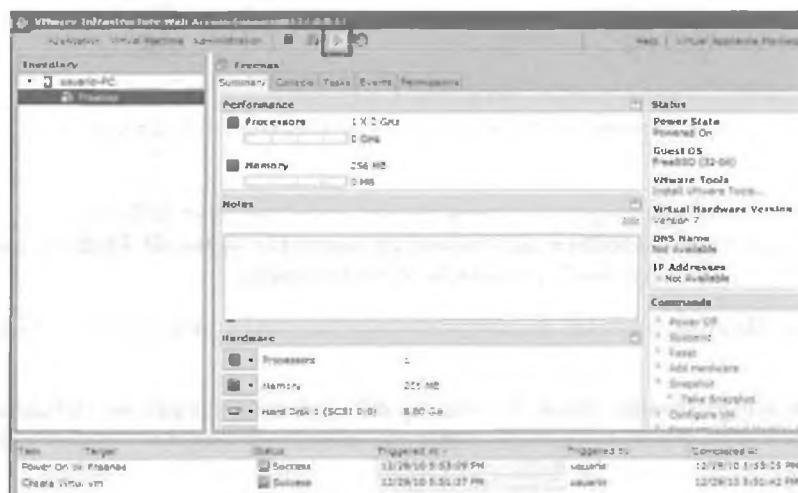
- ✓ **Aprovechamiento de aplicaciones antiguas:** una de las ventajas de la virtualización es la posibilidad de conservar aplicaciones que funcionan en sistemas antiguos y aun así modernizar la infraestructura informática de la empresa. Esa aplicación puede "sobrevivir" en una máquina virtual independiente sin que haga falta conservar el ordenador antiguo.
- ✓ **Centralización de tareas de mantenimiento:** podemos realizar copias de seguridad de un solo golpe de todas las máquinas, programar actualizaciones y otras actividades desde el gestor de máquinas virtuales. También podemos centralizar otras funciones.
- ✓ **Disminuye tiempos de parada:** una ventaja importante, solucionar problemas o realizar copias de seguridad son tareas que se realizan en mucho menos tiempo. Por ejemplo, se puede clonar una máquina y seguir dando servicio mientras se realiza mantenimiento de la máquina virtual de producción como actualizaciones.
- ✓ **Mejor gestión de recursos:** se puede aumentar la memoria o almacenamiento de la máquina huésped para aumentar los recursos de todas las máquinas virtuales a la vez, por lo que se aprovecha mucho mejor las inversiones en hardware.
- ✓ **Balanceo de recursos:** es posible asignar un grupo de servidores físicos para que proporcionen recursos a las máquinas virtuales y asignar una aplicación que haga un balanceo de los mismos, otorgando más memoria, recursos de la CPU, almacenamiento o ancho de banda de la red a la máquina virtual que lo necesite.

PRÁCTICA 8.5

SERVIDOR NAS VIRTUAL

Como vimos en el capítulo 2 existen diversos modelos de almacenamiento **DAS, NAS y SAN**. En esta práctica veremos la instalación de un servidor **NAS (Freenas)** en VMware Server. Usando la configuración anterior de la máquina virtual, vamos a instalar el sistema operativo Freenas en nuestra máquina virtual, con el propósito de tener un servidor FTP disponible en una red local.

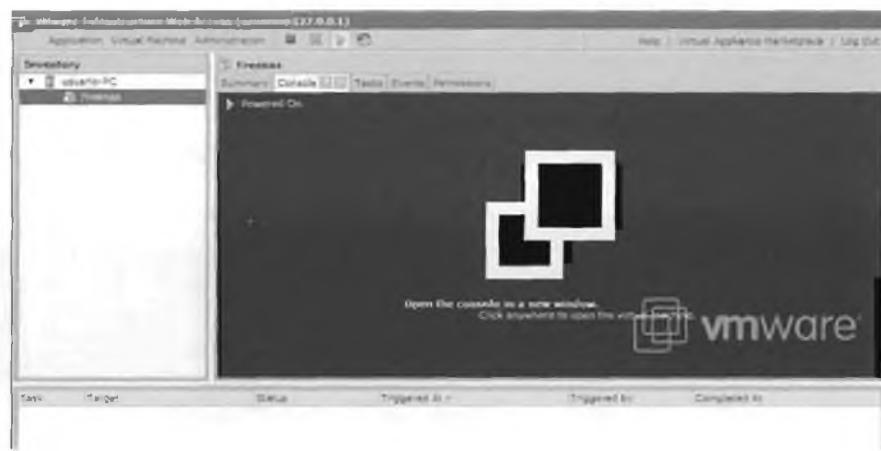
Para ello seleccionaremos la máquina virtual creada previamente y pulsaremos sobre el botón "play" ubicado en la parte superior de la pantalla.



Una vez iniciada la máquina, nos dirigimos a la pestaña "console" para entrar en el modo gráfico de la máquina virtual. Como vemos, VMware nos advierte que es necesario un **plug-in para poder visualizar la máquina virtual**. Pulsaremos en "install Plug-in" para descargar dicho plugin e instalarlo.

Automáticamente, se descargará el *plugin* desde el servidor que ejecuta VMware el cual tendremos que instalar. Tras la instalación del *plugin* será necesario volver a entrar en el navegador web ya que el asistente de instalación lo cerró para aplicar los cambios.

Una vez dentro de la administración web y ubicados en la pestaña "console" de la máquina virtual podemos pulsar el ratón en cualquier lugar para que se abra la ventana que nos permitirá visualizar la máquina virtual.



Acto seguido se abre una ventana nueva en la que podemos visualizar la máquina virtual y esperamos a que cargue completamente Freenas. En las opciones que nos da Freenas para administrar el sistema operativo elegimos la opción 9 "Install/Upgrade to hard drive/flash device, etc." para **instalar el sistema operativo**.



En el asistente elegimos la opción 3 "Install 'full' OS on HDD + DATA + SWAP partition". Tras esto, seleccionamos la unidad de CD/DVD donde se realizará la lectura del sistema operativo para su instalación (VMware Virtual IDE CDROM Drive). Del mismo modo seleccionamos el disco duro en el que queremos realizar la instalación. Introducimos el tamaño de la partición del sistema operativo y de la partición SWAP. Tras la configuración empezará la instalación. Reiniciaremos la máquina una vez terminada la instalación para arrancar el sistema operativo instalado en la máquina virtual.

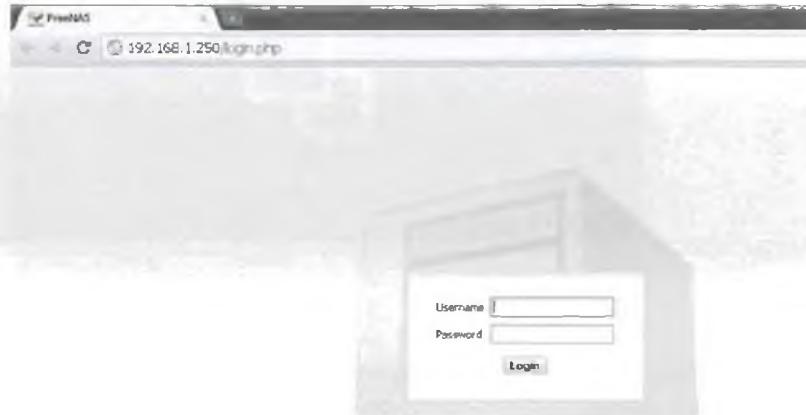
Administración de FreeNAS

FreeNAS es un sistema operativo que se **administra vía web** por lo que podremos realizar su configuración remotamente desde un equipo de la red. En este caso lo haremos desde el propio *host* físico. Una vez arrancado el sistema operativo en la máquina virtual, lo primero será verificar su configuración de red.

En nuestro caso habíamos configurado la tarjeta de red de la máquina virtual en modo *Bbridge*, esto permite configurar manualmente o asignada mediante DHCP una dirección IP en red con la máquina física. Para nuestro ejemplo hemos configurado en la tarjeta de red dentro del sistema operativo FreeNAS con la 192.168.1.250/24, en red con la máquina física 192.168.1.2/24.

Una vez comprobemos que existe conectividad entre máquina física y virtual (por ejemplo realizaremos ping entre las 2 máquinas), abriremos un cliente web en la máquina física e introduciremos en el navegador la siguiente dirección IP, que será la asignada manualmente anteriormente:

http://192.168.1.250



Introducimos el usuario "admin" con la contraseña "freenas" para acceder al administrador web.

System Information	
Hostname	freenas.local
Version	0.7.2 Sabrenta (revision 2543)
Build on	Sat Nov 6 08:54:58 CET 2010
OS Version	FreeBSD 7.3-RELEASE-p3 (revision 199506)
Platform	OpenFiler on Intel(R) Core(TM)2 CPU 6400 @ 2.13GHz
System Time	Wed Dec 29 18:08:49 UTC 2010
Uptime	21 minutes(+) 3 seconds(4)
CPU Temperature	-1.0
CPU Frequency	2132MHz
CPU Usage	0%
Memory Usage	11% of 240MB
Clock Averages	0.08, 0.02, 0.01 [Show process information]
Disk Space Usage	No disk configured

Una vez dentro, instalaremos un servicio FTP, y crearemos un cliente llamado Pepe con contraseña Pepe.

Para iniciar el servicio FTP nos iremos a la sección “Services” y seleccionamos “FTP”. **Habilitamos el servicio** activando la casilla “enable” de la parte superior derecha. Del mismo modo habilitaremos la opción “Only allow authenticated users. Anonymous logins are prohibited.”



Tras habilitar las funciones pulsaremos en el botón “Save and restart” al final de la página. Ahora crearemos el usuario Pepe. Para ello nos dirigimos a la sección “Access” y entramos en “users and groups”. Pulsaremos en el símbolo “+” para **añadir un usuario**. Introduciremos los datos necesarios para el usuario como el nombre, la contraseña, el grupo primario que será FTP y directorio Home.



Tras esto pulsamos en Add. Para aplicar los cambios tendremos que pulsar el botón “apply changes” del menú principal de usuarios y grupos. Ya tenemos todo configurado, ahora solo queda probarlo, accediendo al servidor FTP con la cuenta de usuario Pepe desde una máquina de la red local, con un cliente FTP. En este caso para probarlo lo haremos mediante un navegador web.



Podremos acceder al directorio personal de Pepe para poder almacenar y descargar archivos desde el servidor remoto alojado en una máquina virtual.

8.5 REFERENCIAS WEB

- Descripción de cluster de alta disponibilidad:
<http://www.lintips.com/?q=node/119>
- Información práctica sobre RAID, dispone de un enlace a un emulador del funcionamiento de sistemas RAID de Intel:
http://www.adminso.es/wiki/index.php/2.3.2._Configuraciones_RAID
- Configuración de cluster de alta disponibilidad bajo Windows Server:
<http://www.bujarra.com/?p=2290>
- Configuración de cluster de alta disponibilidad bajo GNU/Linux:
<http://www.alcancelibre.org/staticpages/index.php/como-cluster-heartbeat-centos>
- Software de virtualización VMWare:
www.vmware.com/es/
- Software de virtualización Virtual Box de Oracle:
<http://www.virtualbox.org/>
- Software de virtualización Virtual PC de Microsoft:
<http://www.microsoft.com/windows/virtual-pc/>



RESUMEN DEL CAPÍTULO

En este capítulo hemos analizado y profundizado en distintas configuraciones de alta disponibilidad. Las nuevas necesidades de los usuarios y las empresas exigen alta disponibilidad de los servicios más críticos.

La mejor forma de asegurar la **disponibilidad** de nuestros equipos y los servicios que ellos suministran de manera fiable (99,999%) y sin interrupción las 24 horas del día durante siete días a la semana, es **duplicar** de todos sus componentes críticos y la disposición del software y hardware necesarios para que los elementos redundantes actúen cooperativamente.

Algunas de las soluciones que hemos analizado en este capítulo son:

- **Redundancia y control de errores en el almacenamiento:** mediante sistemas RAID. Los más comúnmente empleados RAID 1 (conjunto en espejo) y RAID 5 (conjunto dividido con paridad distribuida).
- **Balanceo de carga:** gestionando y controlando las peticiones de comunicación a distintos servidores redundantes. Como ejemplo de aplicación hemos visto, en el caso de tener distintas conexiones de red que puedan ser solicitadas como una única.
- **Virtualización:** permite realizar bajo un mismo sistema físico la administración de distintos sistemas operativos. Simplifica e independiza la configuración, instalación, realización de copias de seguridad y restauración de servidores de red.



EJERCICIOS PROPUESTOS



- 1. Busca las distintas soluciones que presenta Dell de fuente de alimentación redundantes. Mediante el análisis de un manual describe su modo de conexión, configuración y funcionamiento. ¿En qué casos consideras que puede ser una buena opción?
- 2. Instala el software de virtualización Virtual Box. Crea una máquina virtual Ubuntu que trabaje en modo NAT. Instala en la máquina virtual un servidor web y configura los aspectos de NAT necesarios para que sea accesible dicho servidor web desde el exterior de la máquina física.
- 3. Para facilitar el manejo de las máquinas virtuales y su interacción con la máquina física en VirtualBox es posible instalar el complemento GuestAdditions. Instálalo y comprueba sus opciones. ¿Qué nuevas funciones permite y mejora? ¿Existe algún equivalente en VMWare Server?
- 4. Realiza mediante virtualización con 4 discos duros bajo GNU/Linux una configuración y prueba de RAID 5. ¿Cómo es posible recuperar la información de uno de los discos en caso de pérdida?
- 5. Configura un servidor mediante una máquina virtual de alta disponibilidad que disponga de los servicios de enruteado, filtrado proxy y cortafuegos adecuado al tráfico de tu clase, permitiendo tan solo el acceso web a los sistemas del aula y permitiendo el acceso únicamente a un servidor web ubicado en la misma.
- 6. Monitoriza el tráfico filtrado por el cortafuegos y el proxy, y realiza un informe en el que indiques:
 - Equipos con conexión, períodos y servicios de acceso.
 - Ranking de los 5 sitios web más visitados.
- 7. Realiza una copia de seguridad de la máquina virtual creada anteriormente y configura otro equipo para que la ejecute con normalidad. ¿En qué tiempo se ha realizado el respaldo de los servicios? ¿Crees que es un método más eficaz que realizar una imagen de disco o partición, con un sistema operativo completamente configurado? Realiza la prueba.
- 8. Descubre e implementa alta disponibilidad y balanceo de carga en un servidor web mediante Apache y Tomcat con la ayuda del siguiente artículo:
http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=apache_tomcat_balanceo.
- 9. Realiza la instalación y configuración de VMware Server sobre una distribución GNU/Linux como Debian.



TEST DE CONOCIMIENTOS

1 ¿Qué sistema RAID controla paridad?

- a) RAID 0.
- b) RAID 1.
- c) RAID 5.
- d) RAID 10.

2 La configuración de red (bajo VMWare) que permite crear una red de máquinas virtuales privada, distinta e independiente de la red a la que pertenece la máquina física es:

- a) Host-only.
- b) Bridge.
- c) NAT.
- d) Ninguna de las anteriores.

3 La administración de los servicios de virtualización (bajo VMWare) se suele realizar mediante:

- a) Aplicación de escritorio.
- b) Correo electrónico.
- c) FTP.
- d) Servicio web.

4 El balanceo de carga no permite realizar:

- a) De 4 conexiones a Internet tener 2 conexiones de igual velocidad.
- b) De 1 conexión a Internet tener 2 conexiones de igual velocidad.
- c) De 2 conexiones a Internet tener 1 sola conexión de velocidades sumadas.
- d) Ninguna de las anteriores.

5 A los sistemas de máximo nivel de alta disponibilidad se les tolera una inactividad anual de:

- a) 5 minutos.
- b) 10 minutos.
- c) 15 minutos.
- d) no se les permite ningún minuto.

6 Bajo sistemas Windows podemos realizar balanceo de carga con la aplicación:

- a) VirtualBox.
- b) Kerio Winroute.
- c) Virtual PC.
- d) WinGate.

7 Bajo sistemas GNU/Linux qué aplicación nos permite monitorizar la actividad de las distintas tarjetas de red:

- a) Iptraf.
- b) Iproute.
- c) Iptables.
- d) Show_ip_route.

— 9 —

— 10 —
— 11 —
— 12 —
— 13 —
— 14 —

9

Normativa legal en materia de seguridad informática

OBJETIVOS DEL CAPÍTULO

- ✓ Conocer la normativa española en materia de seguridad informática.
- ✓ Analizar la normativa y aplicaciones de la LOPD, en materia de seguridad de los datos de carácter personal.
- ✓ Analizar la normativa y aplicaciones de la LSSICE, en materia de comercio electrónico y actividades empresariales vía Internet.
- ✓ Valorar la importancia de la normativa como reguladora de derechos y obligaciones a ciudadanos y empresas.

El último punto que abarca la seguridad informática, cubre el resto de aspectos vistos hasta el momento: seguridad física y lógica, almacenamiento de los datos, comunicaciones y criptografía, es la normativa legal. En este tema veremos la normativa desde dos puntos de vista, la Ley Orgánica de Protección de Datos (LOPD), que pretende proteger el uso de datos de carácter personal por parte de empresas y profesionales, y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), que regula ciertos aspectos de las web que realicen actividades económicas, como publicidad, venta *online*, etc., así como las notificaciones comerciales electrónicas, como SMS o correos electrónicos publicitarios.

9.1 LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD)

La protección de datos de carácter personal es una materia que ha tomado importancia en los últimos años, fundamentalmente a raíz de la aprobación de la **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)**, convirtiéndose en una obligación a cumplir por las empresas si no quieren estar expuestas a sanciones por la **Agencia Española de Protección de Datos (AGPD)**.

La LOPD ha adquirido una gran importancia debido a que equipara y convierte el derecho a la protección de los datos personales en un **derecho fundamental de las personas**.

El derecho fundamental al que hacemos referencia tiene una estrecha relación con el derecho a la intimidad y al honor, encuadrándose todos ellos dentro del art. 18 de la Constitución. Este nuevo derecho fundamental adopta la denominación de libertad informativa o autodeterminación informática, protegiendo el “control que a cada una de las personas le corresponde sobre la información que les concierne personalmente, sea íntima o no, para preservar el libre desarrollo de la personalidad”.

La LOPD establece una serie de **obligaciones** destinadas a la protección de los datos personales contenidos en **ficheros automatizados o informatizados, como en no automatizados o en papel**, que poseen empresas y Administraciones Públicas, y que son tratadas por éstas con diferentes finalidades; gestión de personal, proveedores, clientes, campañas de marketing, etc.



NOTICIA DE ACTUALIDAD

Analiza la noticia “Muchos bancos incumplen la LOPD en materia de videovigilancia”, encontrada en <http://blog.cysia.com/2009/07/la-banca-y-la-lopd/>, e indica:

- ¿Qué requisitos deben cumplir las grabaciones de seguridad en relación al cumplimiento de la LOPD?
- ¿Es necesario pedir el consentimiento de las personas filmadas?

9.1.1 ÁMBITO DE APLICACIÓN DE LA LOPD

Una de las principales dudas que se encuentran los empresarios y profesionales con respecto a la LOPD es la determinación de **qué ficheros o datos de carácter personal** tratados, se encuentran amparados por la normativa.

La LOPD establece su ámbito de aplicación en el artículo 2, al establecer que “la presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”.

Así, para la determinación de qué concretos ficheros o datos de carácter personal entran dentro del ámbito de aplicación de la LOPD debemos tener en cuenta tres conceptos:

- **Dato de carácter personal:** cualquier información concerniente a personas físicas, identificadas o identificables; es decir, toda información numérica, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, tratamiento o transmisión concerniente a una persona física identificada o identifiable.
- **Fichero:** conjunto organizado de datos de carácter personal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Tratamiento:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

9.1.2 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Una vez han sido localizados y determinados los ficheros de datos de carácter personal se procederá a la notificación de los mismos a la Agencia Española de Protección de Datos para su inscripción. Las comunidades autónomas de Madrid, Cataluña y País Vasco, poseen regulaciones y agencias propias.

La Agencia Española de Protección de Datos, a través de su página web www.agpd.es (en el apartado “Canal del Responsable de ficheros – Inscripción de ficheros”), ofrece los **formularios** que deben ser utilizados para la notificación de ficheros, para efectuar la notificación en soporte papel, como para efectuarla por Internet (con certificado digital) o soporte magnético.

El **procedimiento** establecido para la modificación y supresión de ficheros inscritos en la Agencia Española de Protección de Datos, es el mismo que el indicado para la creación de ficheros. Como principal diferencia entre dichos procedimientos, encontramos la necesidad de contar con el **código de inscripción** ya otorgado por la Agencia Española de Protección de Datos en el momento de la inscripción del fichero, para poder efectuar cualquier modificación del fichero inscrito, o bien para la supresión del mismo.

The screenshot shows the 'Notificación de modificación y supresión' (Notification of modification and deletion) form. At the top, there are logos for the Spanish Data Protection Agency and the Royal Decree-Law 15/2007. The main title is 'NOTIFICACIÓN DE MODIFICACIÓN Y SUPRESIÓN'. Below it, there's a section for 'Tipo de solicitud de inscripción' (Type of registration application) with three options: 'Alta' (checkbox checked), 'Modificación' (checkbox), and 'Supresión' (checkbox). There's a note: 'Indicar qué operación se va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de inscripción que se asignó al fichero en el momento de su alta en el RGPD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitarán los datos que se desea modificar y el Nombre o Razón Social del responsable.' Below this is a 'Modelo de divulgación' (Type of disclosure) section with two options: 'Normal' (checkbox checked) and 'Tipo' (radio button). A note states: 'Si la notificación no refiere a un tratamiento de datos sobre miembros de comunidades de propietarios, clientes propietarios, firmas de notarías, oficinas de ferrocarriles, teléfonos móviles, empresas de mensajería, proveedores de servicios, y la finalidad no es la gestión propia de estos establecimientos, puede marcar el cuadro TIPO y seleccionar el modelo que corresponda (se refieren a proveedores, empresas con valores apropiados) o bien seleccionar NORMAL, para parte de un formulario totalmente vacío.' At the bottom, there's a 'Presentación de la documentación' (Presentation of documentation) section with three options: 'Presentación en papel' (checkbox), 'Impresión' (checkbox), and 'Internet firmado con certificado digital' (checkbox checked). At the very bottom are 'Completar' (Complete) and 'Finalizar' (Finish) buttons.

9.1.3 TRATAMIENTO DE LOS DATOS

La LOPD establece una serie de **limitaciones al tratamiento de los datos**; limitaciones fijadas para garantizar un uso adecuado, lícito, no excesivo y con las debidas medidas de seguridad que impidan la alteración, pérdida o tratamiento no autorizado de los datos.

En la mayoría de los supuestos, la **voluntad se manifiesta a través del consentimiento** y, en los casos en los que operan excepciones legales al consentimiento, el afectado manifiesta su voluntad a través de su derecho de oposición al tratamiento de los datos.

La **recogida de los datos** es una operación previa al tratamiento; por ello, la recogida de datos no suele plantear problemas en referencia al consentimiento del afectado puesto que si éste nos proporciona los datos, se entiende que existe un consentimiento implícito (un acto consciente de voluntad). Pero, lo que sí es importante en la recogida es proporcionar al afectado una serie de informaciones o elementos fijados por la ley en el derecho de información (art. 5 de la Ley), para que el afectado pueda suministrar o no sus datos con el **pleno conocimiento del alcance del tratamiento que se va a realizar**. La información que habrá de proporcionarse es:

- ✓ El titular del fichero.
- ✓ Las finalidades del tratamiento.
- ✓ El carácter obligatorio de las respuestas.
- ✓ Los derechos y la posibilidad de ejercerlos.
- ✓ La dirección y las condiciones para ejercitar tales derechos.

El interesado siempre podrá ejercer los derechos que le concede la Ley (impugnación de valoraciones, acceso, rectificación, cancelación y oposición) y **podrá revocar el consentimiento dado** al tratamiento de sus datos o manifestar su oposición parcial a dicho tratamiento.

Además, la Ley establece una serie de principios específicos para el **tratamiento de los datos** por parte del responsable del fichero; principios y **obligaciones impuestas para garantizar su correcto tratamiento, conservación, acceso y destrucción**.

PRÁCTICA 9.1



FORMULARIO LOPD

Un ejemplo de la información a proporcionar al interesado a través de una cláusula LOPD para un formulario de recogida de datos podría ser la siguiente:

"De conformidad con la Ley Orgánica 15/1999 de Protección de Datos Personales y a través de la cumplimentación del presente formulario, Vd. presta su consentimiento para el tratamiento de sus datos personales facilitados, que serán incorporados al fichero "XXXXXXX", titularidad de la EMPRESA XXX, inscrito en el Registro General de la Agencia Española de Protección de Datos, cuya finalidad es la gestión fiscal, contable y administrativa de la relación contractual, así como el envío de información comercial sobre nuestros productos y servicios.

Igualmente le informamos que podrá ejercer los derechos de acceso, rectificación, cancelación y oposición establecidos en dicha Ley a través de carta certificada, adjuntando fotocopia de su DNI/Pasaporte, en la siguiente dirección: EMPRESA XXX. Departamento de Atención al Cliente LOPD. C/XXXXXX nº X. 46000 Localidad.

Los campos señalados con * son obligatorios.

A modo de ejemplo podemos ver los términos legales del registro para acceso a clientes movistar.



Es siempre recomendable al menos revisar que estas cláusulas se incluyen en los términos de los contratos o formularios que rellenemos y aceptemos.

9.1.4 NIVELES DE SEGURIDAD

La LOPD y el Reglamento de Medidas de Seguridad (RD 994/1999), establecen la obligación de establecer una serie de medidas de carácter técnico y organizativo que garanticen la seguridad de los datos de carácter personal, medidas que habrán de adoptarse/implementarse por la empresa o profesional que almacene estos datos. Entre estas medidas se incluye la elaboración de un **Documento de Seguridad** en el que se detallarán los **datos almacenados**, las **medidas de seguridad adoptadas**, así como las **personas que tienen acceso a esos datos**.

La ley identifica tres niveles de **medidas de seguridad**, BÁSICO, MEDIO y ALTO, los cuales deberán ser adoptados en función de los distintos tipos de datos personales (datos de salud, ideología, religión, creencias, infracciones administrativas, de morosidad, etc.). El reglamento ha establecido los niveles de seguridad de forma acumulativa; es decir, que al nivel de seguridad Medio se aplicarán las medidas de seguridad del nivel Básico.

Tabla 8.1

TIPO DE DATOS	MEDIDAS DE SEGURIDAD OBLIGATORIAS
NIVEL BÁSICO	
<ul style="list-style-type: none"> ✓ Nombre ✓ Apellidos ✓ Direcciones de contacto (tanto físicas como electrónicas) ✓ Teléfono (tanto fijo como móvil) ✓ Otros 	<ul style="list-style-type: none"> ✓ Documento de Seguridad ✓ Régimen de funciones y obligaciones del personal ✓ Registro de incidencias ✓ Identificación y autenticación de usuarios ✓ Control de acceso ✓ Gestión de soportes ✓ Copias de respaldo y recuperación
NIVEL MEDIO	
<ul style="list-style-type: none"> ✓ Comisión infracciones penales ✓ Comisión infracciones administrativas ✓ Información de Hacienda Pública ✓ Información de servicios financieros 	<ul style="list-style-type: none"> ✓ Medidas de seguridad de nivel básico ✓ Responsable de Seguridad ✓ Auditoria bianual ✓ Medidas adicionales de Identificación y autenticación de usuarios ✓ Control de acceso físico
NIVEL ALTO	
<ul style="list-style-type: none"> ✓ Ideología ✓ Religión ✓ Creencias ✓ Origen racial ✓ Salud ✓ Vida 	<ul style="list-style-type: none"> ✓ Medidas de seguridad de nivel básico y medio ✓ Seguridad en la distribución de soportes ✓ Registro de accesos ✓ Medidas adicionales de copias de respaldo

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, con carácter general, es la Agencia Española de Protección de Datos (AEPD). Las sanciones tienen una elevada cuantía, siendo España el país de la Unión Europea que tiene las sanciones más altas en materia de protección de datos. Dichas sanciones dependen de la infracción cometida y se dividen en:

- Las **sanciones leves** van desde **601,01 a 60.101,21 €**
- Las **sanciones graves** van desde **60.101,21 a 300.506,05 €**
- Las **sanciones muy graves** van desde **300.506,05 a 601.012,10 €**

Pese al elevado importe de las sanciones, existen muchas empresas en España que todavía no se han adecuado a la misma, o lo han hecho de forma parcial o no revisan de forma periódica su adecuación; por lo que resulta esencial el mantenimiento y revisión de la adecuación realizada.

PRÁCTICA 9.2



NORMAS DE LA ORGANIZACIÓN



En el caso de Windows veremos como al inicio del sistema podemos incluir un mensaje y será necesaria la aceptación del mismo para continuar. Ayudará a recordar las **normas y recomendaciones de seguridad de nuestra organización**, haciendo de este modo que sean conocidas por todos los usuarios.

Ejecutamos gredit.msc para la configuración de directivas de grupo, y en el apartado Configuración de equipo / Configuración de Windows / Directivas locales / Opciones de seguridad, pulsaremos sobre las directiva de **inicio de sesión interactivo: texto de mensaje para los usuarios que intentan iniciar una sesión** así como **inicio de sesión interactivo: título de mensaje para los usuarios que intentan iniciar una sesión**, y añadiremos el texto y título que deseemos.

9.2

LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSICE)

La LSSI, ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) tiene como objeto la regulación del régimen jurídico de los **servicios de la sociedad de la información y de la contratación por vía electrónica**. Entiende por “servicio de la sociedad de la información”, toda actividad que cumple con los siguientes requisitos:

- ✓ Recibe una contraprestación económica.
- ✓ La actividad se realiza a distancia (no presencial).
- ✓ Por medios electrónicos o telemáticos.
- ✓ A petición individual del destinatario del servicio.

Como aplicación práctica de la LSSICE por parte de la Administración, siempre que se pueda percibir un **ingreso económico** (independientemente de la cuantía) a través de un medio telemático, como por ejemplo un sitio web, esta actividad entra en el ámbito de aplicación de esta Ley.

9.2.1 ENTORNOS WEB

Según el **artículo 10.1** de la LSSICE, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente **información**:

1. **Su nombre o denominación social; su residencia o domicilio** o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
2. **Los datos de su inscripción en el Registro Mercantil.**
3. **El número de identificación fiscal** que le corresponda.
4. **Precios del servicio.**

De acuerdo con el artículo 39 de la LSSICE, por la comisión de infracciones se impondrán las siguientes **sanciones**:

- a) Infracciones muy graves, **multa de 150.001 hasta 600.000 euros**. La reiteración en el plazo de tres años de dos o más infracciones muy graves, podrá dar lugar, a la prohibición de operar en España, durante un plazo máximo de dos años.
- b) Infracciones graves, **multa de 30.001 hasta 150.000 euros**.
- c) Infracciones leves, **multa de hasta 30.000 euros**.

PRÁCTICA 9.3



LSSICE WEB

Veamos un ejemplo de cómo cumplir con el artículo 10.1 de la LSSI:

1. Para el caso de un autónomo: se deberá incluir un link a pie de página, de todas las páginas de la web, con el título "Información Legal", "Datos LSSI", o similar, los siguientes datos: Nombre y Apellido, Domicilio: Calle(C.P.) Localidad, DNI/CIF, Email@email, Teléfono.
Sobre la obligación de incluir el **teléfono** se entiende este como "*cualquier otro dato que permita establecer con él una comunicación directa y efectiva*".
2. Para el caso en que se trate de una empresa, se deberá incluir un **aviso legal – LSSI** o similar, con las **Condiciones Generales de Acceso y utilización del sitio web**.

9.2.2 COMUNICACIONES COMERCIALES

Entre otros aspectos, la LSSICE regula, en sus artículos 19 a 22, el envío de **comunicaciones comerciales por vía electrónica**. Es por ello que en este apartado nos centraremos en los supuestos de aplicación de la LSSICE más comunes: el envío de correos electrónicos y SMS-MMS.

En todos estos supuestos, la LSSICE pretende impedir la proliferación del fenómeno conocido como *spam*, para ello se exigen una serie de **requisitos para el envío de comunicaciones comerciales electrónicas y que exista un consentimiento expreso**.

El **artículo 21.1** prohíbe de forma expresa el envío de comunicaciones comerciales electrónicas (por correo electrónico u otro medio equivalente), que no **bubieran sido previamente solicitadas o autorizadas expresamente** por su destinatario (persona física o jurídica). Una vez obtenido el consentimiento previo y expreso para el envío de la comunicación comercial, el **mensaje enviado deberá cumplir con los siguientes requisitos informativos**:

- ✓ Identificar de forma clara el nombre de la persona física o jurídica en nombre de la que envía el mensaje publicitario.
- ✓ Incluir en el comienzo del mensaje la palabra “*Publicidad*” (en los correos electrónicos) o “*Publi*” (especialmente en los SMS).
- ✓ Facilitar al receptor del mensaje la posibilidad de revocar el consentimiento de una forma sencilla y gratuita.

La LSSICE prevé en su apartado segundo, que **no será necesario el consentimiento previo del receptor** del mensaje cuando los **datos hubieran sido obtenidos de forma lícita en el marco de una relación contractual previa**, y que las comunicaciones versen sobre productos o servicios similares a los inicialmente adquiridos o contratados y que sean de la propia empresa, organización o profesional.

La LSSICE establece en su artículo 38 el apartado de infracciones y establece como una infracción leve el envío de comunicaciones comerciales sin el cumplimiento de alguno de los requisitos recientemente analizados (sanción hasta 30.000 €).

En el caso de que se envíen **tres o más comunicaciones** comerciales a un mismo destinatario en el plazo de un año, sin cumplir con los requisitos establecidos, la infracción pasaría a ser considerada como grave (multa de 30.001 a 150.000 €).

PRÁCTICA 9.4

LOPD Y LSSICE EN EL CORREO ELECTRÓNICO

En los correos electrónicos que las empresas envían a sus clientes o usuarios debe de incluirse una cláusula o pie de página con la **Política de privacidad**, a modo de ejemplo:

Política de privacidad. En cumplimiento de la LOPD 15/1999 y de la LSSI-CE 34/2002 se INFORMA que los datos de carácter personal que se facilitan, incluido su correo electrónico, y que resultan necesarios para el envío de la información solicitada, se incorporarán a un fichero automatizado cuya titularidad y responsabilidad viene ostentada XXXX. Al remitir el interesado sus datos de carácter personal y de correo electrónico a XXXX, expresamente se AUTORIZA la utilización de dichos datos a los efectos de las comunicaciones periódicas, incluyendo expresamente las que se realicen vía correo electrónico, así como otras ofertas de servicios, informaciones o productos relacionados con la actividad institucional que se desarrolle.

El interesado podrá ejercitar respecto a sus datos los derechos de acceso, rectificación, cancelación y oposición enviando un correo electrónico a la siguiente dirección electrónica XXXX solicitando, en su caso, (1) Que se le remitan por la misma vía sus datos personales que obran en los ficheros de XXXX a los efectos de su consulta o su posible rectificación o bien (2) Que se cancele y/o revoque la autorización para la recepción de comunicaciones, debiendo notificar a XXXX la efectiva rectificación y/o cancelación de los datos de carácter personal de su fichero.

9.3 REFERENCIAS WEB

- Sitio web de la agencia española de protección de datos:
www.agpd.es
- Web con noticias sobre la LOPD y LSSICE:
www.leydeprotecciondedatos.com
- Noticias sobre denuncias de LOPD:
<http://www.todonoticiaslopd.com/>
- Guía práctica de Microsoft para adaptación a la LOPD:
<http://www.microsoft.com/business/smb/es-es/guias/lopd/home.mspx>
- INTECO – sobre la LSSICE:
http://cert.inteco.es/Formacion/Legislacion/Ley_de_Servicios_de_la_Sociedad_de_la_Information/
- Página web del Ministerio de Industria, Turismo y Consumo sobre la LSSICE:
<http://www.mityc.es/dgdsi/lssi/Paginas/Index.aspx>



RESUMEN DEL CAPÍTULO

En este capítulo hemos analizado la normativa que regula derechos y obligaciones con respecto a dos aspectos fundamentales:

- La Ley Orgánica de Protección de Datos (**LOPD**) pretende proteger el uso de datos de carácter personal de los ciudadanos, en la recogida, tratamiento y eliminación de los mismos mediante ficheros, que realizan empresas y profesionales. El organismo que verifica, controla y sanciona los aspectos de dicha ley es la Agencia Española de Protección de Datos, aunque Madrid, Cataluña y País Vasco poseen sus propias agencias.
- La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (**LSSICE**), regula ciertos aspectos de los servicios electrónicos, como sitios web que realicen actividades económicas, como publicidad, venta *online*, etc., así como las notificaciones comerciales electrónicas, como SMS o correos electrónicos publicitarios.

Estas leyes de reciente creación, 1999 LOPD y 2002 LSSICE, suponen un inicio en la regulación normativa de la informática y sus aspectos de seguridad, garantizando los derechos de las personas y ciudadanos, evitando abusos sobre la privacidad de los datos personales, y ofreciendo un nuevo marco que dé transparencia a las operaciones comerciales a través de las redes de telecomunicaciones, y especialmente a través de Internet.



EJERCICIOS PROPUESTOS

- 1. Explica por qué crees que surge la normativa de protección de datos en España. ¿Crees que los datos personales son empleados en ocasiones con un fin deshonesto? ¿Crees que los medios de comunicación protegen la intimidad de las personas?
- 2. Busca cómo se realiza la notificación de ficheros por Internet o por soporte magnético, y explica el proceso. ¿Cuál es el medio recomendado por la AGPD para la notificación de ficheros?
- 3. Extrae tres noticias de <http://todonoticiaslopd.com/> y explica exactamente qué ha ocurrido, qué tipo de incumplimiento se ha realizado y la sanción propuesta (nivel y cuantía). ¿Qué datos y qué nivel de protección poseen los datos de carácter personal mal empleados?
- 4. En su artículo 19, la LOPD indica con respecto al control de acceso físico (art.19): exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales en donde se encuentren ubicados los sistemas de información con datos de carácter personal.
- ¿Qué tipos de medidas deberíamos de tomar para cumplir con la normativa? Realiza algunas recomendaciones técnicas.
- 5. Busca al menos 2 web españolas, que no cumplan con la LSSI, explica por qué lo has deducido, y otras 2 que sí, indicando cómo has encontrado su aviso legal y qué indica éste con respecto a la LSSI.
- 6. Busca alguna noticia de infracción por incumplimiento de la LSSI, por comunicación comercial, qué sanción se le impuso y cuáles fueron los motivos.
 - ¿Qué tipo de infracción se cometió?
 - ¿Ante qué organismo se interpuso la demanda?
 - ¿Crees que la sanción es proporcionada? Explica tus motivos.
- 7. Analiza las preguntas frecuentes o FAQS de la web del Ministerio de Industria, Turismo y Comercio, en relación a la LSSI:
<http://www.mityc.es/dgdsi/lssi/faqs>
 - ¿Qué acción se puede realizar si nos envían spam? ¿A qué organismo se puede reclamar?
 - Revisa en su web el aviso legal, ¿cumple la Administración con la LSSI? ¿Está obligado a ello?



TEST DE CONOCIMIENTOS

1 ¿En qué año aparece la LOPD?

- a) 1990.
- b) 1995.
- c) 1999.
- d) 2004.

2 Indica cuál de los siguientes datos y archivos no está sujeto a la LOPD:

- a) Archivo con base de datos de música en mi casa.
- b) Ficha de inscripción en papel con datos de un centro polideportivo.
- c) Apuntes en papel sobre un cliente en un restaurante.
- d) Facturas emitidas con datos de clientes de un taller mecánico.

3 La LOPD afecta a ficheros:

- a) Solo en soporte electrónico.
- b) Solo en soporte electrónico pero estructurados.
- c) Tanto en soporte papel como electrónico.
- d) Solo en soporte papel.

4 El organismo que regula y supervisa la protección de datos personales en los ficheros de empresa es:

- a) Asociación Española de Profesionales del Diseño(AEPD).
- b) Agencia Española de Protección Personal (AEPP).
- c) Agencia de Protección de Datos Españoles (APDE).
- d) Agencia Española de Protección de Datos (AGPD).

5 En caso de solicitarme una entidad datos relativos a salud, las medidas de seguridad que deberá adoptar internamente en sus ficheros serán de nivel:

- a) Bajo.
- b) Medio.
- c) Alto.
- d) No los puede registrar si no es un centro sanitario.

6 ¿En qué año aparece la LSSICE?

- a) 1990.
- b) 2002.
- c) 1999.
- d) 2004.

7 La LSSICE no regula aspectos como:

- a) El precio de los SMS.
- b) La información legal sobre los *webmaster*.
- c) La publicidad a través del correo electrónico.
- d) El comercio electrónico.

8 La LSSICE no regula aspectos como:

- a) El precio de los SMS.
- b) La información legal sobre los *webmaster*.
- c) La publicidad a través del correo electrónico.
- d) El comercio electrónico.

Material adicional

El material adicional de este libro puede descargarlo en nuestro portal Web: <http://www.ra-ma.es>.

Debe dirigirse a la ficha correspondiente a esta obra, dentro de la ficha encontrará el enlace para poder realizar la descarga. Dicha descarga consiste en un fichero ZIP con una contraseña de este tipo: XXX-XX-XXXX-XXX-X la cual se corresponde con el ISBN de este libro.

Podrá localizar el número de ISBN en la página 2 (página de créditos). Para su correcta descompresión deberá introducir los dígitos y los guiones.

Cuando descomprima el fichero obtendrá los archivos que complementan al libro para que pueda continuar con su aprendizaje.

INFORMACIÓN ADICIONAL Y GARANTÍA

- RA-MA EDITORIAL garantiza que estos contenidos han sido sometidos a un riguroso control de calidad.
- Los archivos están libres de virus, para comprobarlo se han utilizado las últimas versiones de los antivirus líderes en el mercado.
- RA-MA EDITORIAL no se hace responsable de cualquier pérdida, daño o costes provocados por el uso incorrecto del contenido descargable.
- Este material es gratuito y se distribuye como contenido complementario al libro que ha adquirido, por lo que queda terminantemente prohibida su venta o distribución.

Opinion: *A Discursive Argument*

Opposition to the proposed legislation has been spearheaded by environmentalists who argue that it would undermine the environmental integrity of wetlands and waterways due to the anticipated de-

Índice Alfabético

Símbolos

3DES, 111, 112, 127, 132, 145
802.11i, 149

A

ACL, 82, 83, 84, 162, 170, 178, 181, 183, 186.
 Actualización, 20, 21, 29, 31
Administración, 66, 128, 132, 187, 224, 225
Adware, 92, 102, 108
AEPD, 220
AES, 111, 112, 113, 115, 127, 132, 145, 149, 152, 154,
 155
Agencia Española de Protección de Datos, 216, 217,
 218, 219, 220
AGPD, 224, 225
Alta disponibilidad, 21
Análisis forense, 28
Antimalware, 9, 10, 15, 23, 28, 29, 32, 66, 90, 93, 94, 95,
 100, 102, 103, 105, 108, 224
Antispyware, 95
Antivirus, 29, 31, 90, 95, 100, 103, 108
ARP Poisoning, 134, 136
Ataque de diccionario, 67
Ataque de fuerza bruta, 67, 116
Auditoría de seguridad, 27
Autenticación, 12, 67, 121, 154, 155, 177, 180, 181
AVR, 53

B

Backdoor, 15, 25, 91, 97, 102, 108
Backup, 35, 60, 62
Balanceo de carga, 9, 10, 23, 48, 186, 195, 196, 198, 199,
 212, 213, 216
Bastidor, 49
Biometría, 49, 50 60
BIOS, 71, 73
Blowfish, 42, 44, 111, 112, 127, 132

Botnet, 26, 90, 91, 224
Browser hijacker, 103, 108
Bugs, 25

C

CCTV, 34, 51, 224
Centro de respaldo, 47, 48
Centros de procesamiento de datos, 47, 186
Certificado digital, 60, 64, 108, 123, 125, 127, 128, 129,
 132, 136, 217
César, 109, 110, 111
chgrp, 83, 84
chmod, 83, 84
chown, 83, 84
Cifrado, 38, 41, 69, 108, 109, 111, 115, 116, 117, 122
Cifrado asimétrico, 118, 120, 127, 132, 159, 162
Cifrado híbrido, 117, 127, 132
Cifrado simétrico, 112
Clave, 14, 67, 108, 109, 110, 111, 112, 115, 116, 117,
 118, 119, 120, 121, 122, 123, 125, 127, 128, 129, 132,
 144, 145, 146, 148, 149, 150, 151, 152, 154, 155, 177,
 181, 193, 194
Clave asimétrica, 117
Clave pública, 115, 116, 117, 120, 121, 122, 123, 125
Clave privada, 115, 117, 120, 121, 122
Clave simétrica, 109, 117
Clickers, 92
Cloud computing, 186, 187
Clustering, 186
Confidencialidad, 12, 29, 32, 117, 145
Contraseña, 67, 69, 84, 86, 128, 132, 155, 159, 162
Contraseñas seguras, 84, 86
Control de acceso, 48, 49, 60
Cookies, 92
Copia de seguridad, 29, 31, 35, 60, 128, 132
CPD, 34, 47, 48, 60, 62, 63
Credenciales, 49

Crimeware, 92, 102, 108
 Criptoanálisis, 108
 Criptografía, 108, 109, 112, 116, 117, 120, 122, 126, 216
 Criptografía simétrica, 111, 117
 Cron, 38, 41

D

DAS, 36, 60, 61, 206, 210.
 Data center, 47
 DDoS, 26, 224
 DES, 42, 44, 111, 112, 127, 132, 145
 Diccionario, 26, 224
 Diferencial, 36
 Diffie-Hellman, 117, 127, 132
 Directiva de bloqueo de cuentas, 68
 Directiva, 68
 Directiva de contraseñas, 68
 Disponibilidad, 12, 29, 32, 48
 Distribución Live, 74, 77, 78, 80, 81
 DMZ, 137, 169, 173, 182, 183, 186
 DNIE, 122, 123, 125, 126, 127, 128, 129, 132
 DNS, 139, 224.
 DNS spoofing, 135, 136
 DoS, 26, 132, 224
 DSA, 117, 118, 120, 127, 132
 DSS, 117
 Dual Homed-Host, 169, 183, 186

E

EFS, 18, 14, 15, 113, 115
 ElGamal, 112, 117, 118, 120, 127, 132
 Esteganografía, 128, 132
 Exploits, 19, 21

F

Fabricación, 132
 FakeAV, 94
 Filtrado de direcciones MAC, 155
 Firewall, 29, 31, 139, 162, 168, 171, 172, 173, 181, 183, 186.
 Firma digital, 83, 84, 120, 121, 122, 125
 fnmt, 126, 128, 132

FTP, 29, 31, 42, 43, 44, 93, 135, 136, 139, 140, 141, 142, 143, 144, 145, 165, 166, 172, 173, 174, 183, 186, 206, 208, 209, 210, 213, 216, 224.
 Fuerza bruta, 26, 224

G

Gestor de arranque, 75, 77
 getfacl, 84
 GPG, 112, 117, 118, 120.
 Grayware, 92
 Greyware, 92, 105, 108
 Gusano, 25, 90, 92

H

Hacker, 24, 47
 Hash, 115, 121
 High Availability, 21
 Hoax, 26, 92, 102, 108, 224
 HTTP, 139, 224.
 HTTPS, 123, 125, 136, 139, 141, 143, 145, 146, 148, 159, 160, 162, 174, 200, 203, 224.

I

IDEA, 111, 112, 127, 132
 Identificación, 67
 IDS, 136, 137, 138, 158, 159, 162
 Incremental, 36
 Infostealers, 92, 102, 108
 Ingeniería social, 26, 92, 224
 Integridad, 12, 29, 32, 117, 121, 145
 Interceptación, 132
 Interrupción, 132
 IPSEC, 141, 146, 160, 162
 ISO 27001, 27, 29
 ISO 27002, 27

J

Joke, 92, 102, 108

K

Keyloggers, 92, 102, 108

L

- L2TP, 146, 160, 162
 Lammer, 24
 LDAP, 67
 Log, 71, 166, 168
 Login, 67
 LOPD, 23, 216, 217, 218, 219, 224, 225, 226
 LSSI, 221, 222, 223, 224, 225
 LSSICE, 216, 221, 222, 223, 224

M

- Malware, 10, 11, 15, 17, 20, 21, 25, 26, 29, 31, 32, 35, 41, 66, 90, 92, 94, 95, 96, 97, 98, 99, 100, 102, 103, 104, 105, 108, 159, 162, 224
 Man in the middle, 133
 MBSA, 18, 21
 MD5, 71, 77, 79, 81, 115, 116, 145
 Metasploits, 19, 21
 Minucia, 50
 MitM, 133, 134, 136, 143, 145, 159, 160, 162
 Modificación, 132
 MTTF, 22
 MTTR, 22

N

- NAS, 36, 60, 61, 206, 210
 NAT, 163, 164, 165, 166, 172, 174, 182, 186, 198, 199, 203, 204, 205, 212, 213, 216.
 Nessus, 18, 21
 NetBIOS, 139, 224
 Netstat, 139
 Newbie, 24
 Nmap, 17, 21
 No repudio, 12, 29, 32,, 117, 120, 121, 145

P

- PAM, 70
 Password, 49, 60, 63
 Password cracking, 26, 224
 Pecera, 48
 PGP, 112, 117, 127, 132.
 Pharming, 26, 133, 136, 224
 Phishing, 10, 11, 26, 29, 32, 90, 92, 102, 103, 108, 133, 160, 162, 224

Pinza amperimétrica, 54

- PKI, 125, 127, 132
 POP3, 139, 141, 143, 145, 224.
 Potencia aparente, 54
 Potencia real, 54
 PPTP, 146, 160, 162
 Proxy, 9, 10, 23, 162, 165, 166, 168, 169, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 186, 212, 216
 Proxy abierto, 174
 Proxy anónimo, 174
 Proxy caché Web, 174
 Proxy inverso, 174
 Proxy NAT, 174
 PSK, 149, 152
 pwstealer, 92, 102, 103, 105, 108

R

- Rack, 49
 RADIUS, 149, 153, 158, 162
 RAID, 186, 187, 188
 RC5, 111, 127, 132
 Red zombie, 90, 91
 Restaurar Sistema, 41
 Rijndael, 42, 44, 111
 Rogueware, 25, 90, 92, 94, 102, 108
 Rol, 84, 86
 Rootkit, 15
 Rootkit hunter, 15
 Round Robin, 194
 RSA, 42, 44, 117, 127, 129, 132, 159, 162

S

- SAI, 34, 52, 53, 54, 60, 62, 63, 224
 SAI OFF-LINE, 53
 SAI ON-LINE o de DOBLE CONVERSIÓN, 53
 SAI ON-LINE o LINE INTERACTIVE, 53
 SAN, 36, 60, 61, 206, 210
 Scam, 10, 11, 26, 92, 104, 108, 224
 Screened Host, 169, 183, 186
 Screened-subnet, 169, 183, 186
 Screening router, 169
 Script-Kiddies, 24
 Seguridad activa, 28
 Seguridad física, 28, 47, 66, 216

Seguridad lógica, 28, 66
 Seguridad pasiva, 28
 Serpent, 113, 115
 Servidor de autenticaciones, 67
 setfacl, 84
 SFC, 15
 SHA, 71, 79, 81, 108, 109, 115, 145
 Shell hijacker, 103, 108
 Shoulder surfing, 26, 224
 SmartCard, 49, 122
 SMTP, 135, 136, 139, 140, 141, 143, 145, 224.
 Sniffing, 26, 132, 224
 Spam, 10, 11, 25, 26, 92, 102, 103, 104, 108, 128, 132,
 174, 223, 224, 225.
 Spoofing, 26, 133, 134, 136, 224
 Spyware, 10, 11, 29, 32, 92, 95, 102, 108.
 SQL Inyection, 104, 108
 SSH, 21, 23, 117, 127, 132, 139, 140, 141, 142, 144, 145,
 146, 158, 160, 162, 224.
 SSL, 23, 42, 44, 117, 127, 132, 141, 143, 144, 145, 146,
 158, 160, 162, 174.
 Sustitución, 108, 109, 110, 111, 187

T

Tabnabbing, 133
 Tar, 38, 41
 Telnet, 135, 136, 139, 140, 143, 145, 224
 Texto plano, 14, 81, 108, 110, 111, 112, 127, 132, 143,
 144, 145, 153, 155
 TKIP, 149, 152, 154, 155
 TLS, 23, 117, 127, 132, 141, 144, 145, 146, 158, 160,
 162.

TPC, 125
 Transposición, 108, 110, 111
 Troyano, 25, 90, 91, 92, 103, 108
 Truecrypt, 38, 41
 Twofish, 113, 115

U

UBCD, 72, 75, 80
 UPS, 34, 52, 224

V

VAF, 51
 Vatios, 54
 Virtualización, 9, 10, 23, 186, 199, 205, 206, 210, 212,
 213, 216
 Virus, 25, 47, 90, 91, 100, 103, 108
 VPN, 23, 145, 146, 147, 148, 158, 160, 162, 172, 181,
 198, 199.
 Vulnerabilidad, 27, 29, 31, 91, 92

W

Wannaber, 24
 WEP, 149, 150, 151, 152, 155, 158, 160, 162.
 Wireless, 148, 158
 WLAN, 51, 149, 155, 159, 160, 162
 WPA, 149, 151, 152, 155, 158, 160, 162.
 WPA-Enterprise, 149

X

X.509, 123



La presente obra está dirigida a los estudiantes del Ciclo Formativo de Grado Superior de **Administración de Sistemas Informáticos en Red (ASIR)**, en concreto para el Módulo Profesional **Seguridad y Disponibilidad**.

A lo largo del libro se analiza la seguridad informática y la alta disponibilidad desde distintas perspectivas, completando de este modo una visión global de la materia, para no dejar ningún aspecto vulnerable: *principios y terminología, seguridad pasiva, copias de seguridad, seguridad física y lógica, software antimalware, criptografía de la información y las comunicaciones, seguridad en redes corporativas*, atendiendo especialmente a su seguridad perimetral, *configuraciones avanzadas de alta disponibilidad y normativa en materia de seguridad informática*.

El enfoque del libro es eminentemente práctico, durante el desarrollo de los capítulos se realizan un total de 51 prácticas. En los capítulos se incluyen recomendaciones para desarrollar una completa labor como Administrador de sistemas, además de actividades y ejemplos, con la finalidad de facilitar la asimilación de los conocimientos tratados.

Así mismo, se incorporan test de conocimientos y ejercicios propuestos con la finalidad de comprobar si los objetivos de cada capítulo se han asimilado correctamente.

www.ra-ma.es

En la página web de **Ra-Ma** (www.ra-ma.es) se encuentra disponible material de apoyo y complementario.



ra-ma.e



Ra-Ma®