Google peligroso – búsqueda de datos confidenciales

Michał Piotrowski

CABERNET SERVER

Google peligroso – búsqueda de datos confidenciales

Michał Piotrowski

Las informaciones que deben ser protegidas, a veces se hacen públicas. Las revelan inconscientemente los usuarios mismos, a causa de su negligencia o ignorancia. Como resultado, en Internet, al alcance de todos, podemos encontrar datos de carácter confidencial. Basta usar Google.

Google responde a cerca del 80% de todas las búsquedas en la Red, y con este resultado es el navegador usado con más frecuencia. Lo debe a su extremadamente eficaz mecanismo de generación de resultados y a opciones avanzadas de búsqueda. Sin embargo, tenemos que recordar que Internet es un medio muy dinámico, y por eso los resultados visualizados por Google no siempre son actuales. A veces algunas páginas encontradas son muy viejas, mientras que Googlebot, script automático que explora e indexa recursos WWW, no ha visitado muchas páginas similares.

En la Tabla 1 se hallan los operadores más importantes y más útiles que precisan la búsqueda, junto con descripción y con resultado que producen, en cambio la Figura 1 representa los sitios en documentos a los que se refieren los operadores durante la búsqueda en recursos de Internet (el ejemplo es la página web de la revista *hakin9*). Son sólo unos ejemplos – si haces preguntas acertadas en Google, podrás conseguir muchas informaciones interesantes.

Buscamos la víctima

Con Google podemos visualizar no sólo los recursos de Internet accesibles para todos,

En este artículo aprenderás...

- cómo, con el uso de Google encontrar bases de datos y otros datos de carácter confidencial,
- cómo encontrar informaciones sobre sistemas y servicios en la red expuestos a los ataques,
- cómo encontrar en Google hardware de red accesibles al público.

Lo que deberías saber ...

- usar el navegador en Internet,
- tener un conocimiento básico del protocolo HTTP.

Sobre el autor

Michał Piotrowski es licenciado en informática. Tiene muchos años de experiencia en el puesto de administrador de redes y sistemas. Lleva más de tres años trabajando como inspector de seguridad. En la actualidad es especialista en seguridad de redes teleinformáticas en una de las instituciones financieras más grandes en Polonia. En su tiempo libre programa y se dedica a la criptografía, es aficionado al Software Libre.

Tabla 1. *Operadores de consulta en Google*

Operador	Finalidad	Ejemplo de uso
`site`	limita los resultados a las páginas que se hallan en un dominio determinado	`site:google.com fox` encuentra todas las páginas que contienen la palabra *fox* en el texto, que se hallan en el dominio **.google.com*
`intitle`	limita los resultados a los documentos con la frase indicada en el título	`intitle:fox fire` encuentra páginas que contienen la palabra *fox* en el título y *fire* en el texto
`allintitle`	limita los resultados a los documentos que contienen frases indicadas en el título	`allintitle:fox fire` encontrará todas las páginas en cuyo el título hay palabras *fox* y *fire*; funciona como `intitle:fox intitle:fire`
`inurl`	limita los resultados a las páginas con la frase indicada en la dirección URL	`inurl:fox fire` encontrará las páginas que contienen en el texto la palabra *fire* y *fox* en la dirección URL
`allinurl`	limita los resultados a las páginas con todas las freses indicadas en la dirección URL	`allinurl:fox fire` encontrará las páginas con palabras *fox* y *fire* en la dirección URL; funciona de modo parecido a `inurl:fox inurl:fire`
`filetype, ext`	limita los resultados a los documentos de tipo indicado	`filetype:pdf fire` devuelve los documentos PDF con la frase *fire*, y `filetype:xls fox` devuelve los las hojas de Excel que contienen *fox*
`numrange`	limita los resultados a los documentos que en cuyo contenido aparece el número del rango indicado	`numrange:1-100 fire` devuelve las páginas con los números del rango de 1 a 100 y la palabra *fire*. Lo mismo se obtiene con la consulta: `1..100 fire`
`link`	limita los resultados a las páginas con vínculos a la localización indicada	`link:www.google.es` devuelve documentos en cuyo contenido por lo menos hay un vínculo a la página *www.google.es*
`inanchor`	limita los resultados a las páginas con vínculos que contienen la frase indicada en la descripción	`inanchor:fire` devuelve documentos con vínculos que contienen la palabra *fire* en la descripción (no en la dirección URL que indican, sino en la parte subrayada del texto)
`allintext`	limita los resultados a los documentos en cuyo texto hay la frase indicada, y que al mismo tiempo no la contienen en título, vínculos y ni direcciones URL	`allintext:"fire fox"` devuelve documentos con la frase *fire fox* sólo en el texto.
`+`	con su uso la frase indicada aparecerá con mucha frecuencia en los resultados	`+fire` clasifica los resultados en relación a mucha frecuencia de aparición de la palabra *fire*.
`-`	con so uso la frase indicada no aparecerá en los resultados	`-fire` devuelve los documentos en cuyo contenido no hay palabra *fire*.
`""`	permite buscar las frases enteras, no sólo las palabras	`"fire fox"` devuelve los documentos en cuyo contenido hay frase *fire fox*
`.`	se sustituye con un signo particular	`fire.fox` devuelve documentos en cuyo contenido hay frases *fire fox*, *fireAfox*, *fire1fox*, *fire-fox* etc.
`*`	se sustituye con la palabra particular	`fire * fox` devuelve documentos con la frase *fire the fox*, *fire in fox*, *fire or fox* etc.
`|`	OR lógico	`"fire fox" | firefox` devuelve documentos con la frase *fire fox* o con la palabra *firefox*

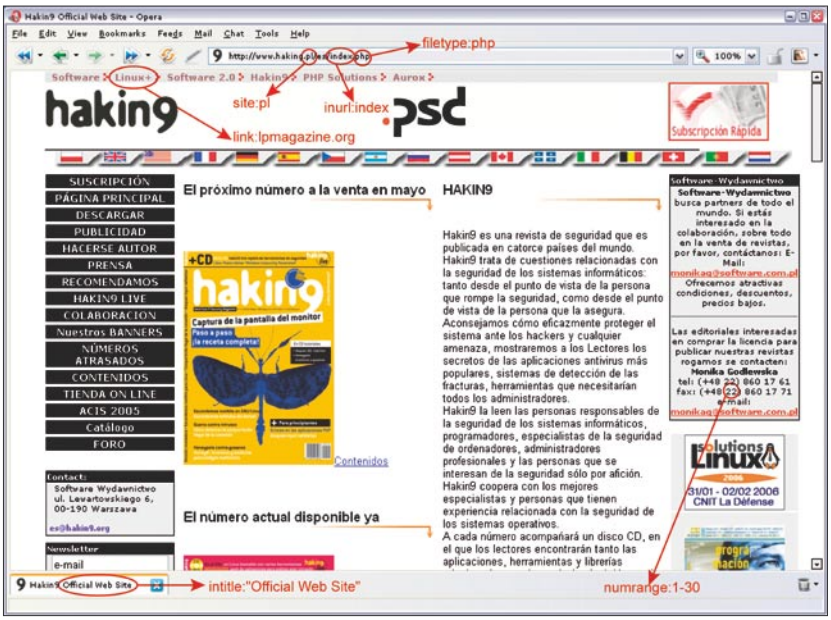

Figura 1. *Uso de operadores en la consulta, en el ejemplo de las páginas web de la revista hakin9*

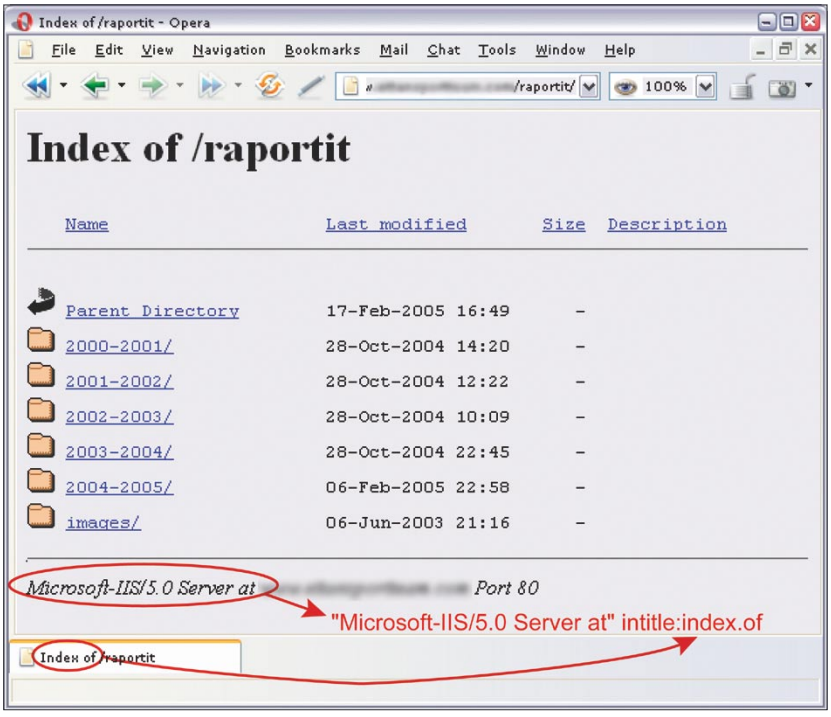

Figura 2. *La detección del servidor IIS 5.0 con el uso del operador intitle*

sino también los que nunca se deben revelar. Si realizamos una consulta apropriada, a menudo se nos visualizan unos resultados verdaderamente sorprendentes. Empecemos con algo fácil.

Imaginémonos que se ha encontrado un hueco de seguridad en un programa usado por todos. Supongamos que tiene relación con el servidor *Microsoft IIS* en la versión 5.0 y que un asaltante hipotético quiere encontrar algunas máquinas con este software para atacarlas. Desde luego, para hacerlo podría usar un escáner, pero prefiere usar Google. Por eso, escribe la frase: `"Microsoft-IIS/5.0 Server at" intitle:index.of` y en el resultado se le visualizan los vínculos a los servidores buscados, y en concreto a listados con contenidos de archivos que se hallan en estos servidores. Es así porque en la configuración estándar, el software *IIS* (y muchos otros) agrega a algunas páginas generadas de modo dinámico los anuncios con su nombre y su versión (véase Figura 2).

Es el ejemplo de información que en si misma no es peligrosa; por esta causa muchas veces no se hace caso a ella y se la deja en la configuración estándar. Por desgracia, esta información en circunstancias determinadas puede tener un significado esencial para el atacante. La Tabla 2 representa más ejemplos de búsquedas de otros tipos de servidores en Google.

Otro modo de encontrar versiones específicas de los servidores WWW consiste en buscar las páginas estándar, que se suministran con ellos; accesibles después de una instalación correcta. Aunque suene raro, en la red hay un montón de servidores cuyo valor predeterminado no se modificó después de la instalación. Muy a menudo son unas máquinas mal protegidas, olvidadas: objetivos fáciles de conquistar para los atacantes. Podemos encontrarlas usando las consultas de ejemplo presentadas en la Tabla 3.

Este método es muy fácil y muy útil a la vez. De este modo podemos ganar el acceso a gran cantidad de servicios en la red o a sistemas operativos que usan aplicaciones en las que se detectaron errores no eliminados por los administradores perezosos o ignorantes de peligro. Como ejemplo podemos citar dos programas bastante populares: *WebJeff Filemanager* y *Advanced Guestbook*.

El primero es un manager de ficheros en web, con el que se envian los ficheros al servidor y crea, visualiza, elimina y modifica los ficheros presentes en el servidor. Por desgracia, *WebJeff Filemanager* en la versión 1.6 tiene un error que facilita la lectura del contenido de cualquier fichero

Tabla 2. *Google: búsqueda de varios tipos de servidores WWW*

Consulta	Servidor
`"Apache/1.3.28 Server at" intitle:index.of`	*Apache* 1.3.28
`"Apache/2.0 Server at" intitle:index.of`	*Apache* 2.0
`"Apache/* Server at" intitle:index.of`	cualquier versión de *Apache*
`"Microsoft-IIS/4.0 Server at" intitle:index.of`	*Microsoft Internet Information Services* 4.0
`"Microsoft-IIS/5.0 Server at" intitle:index.of`	*Microsoft Internet Information Services* 5.0
`"Microsoft-IIS/6.0 Server at" intitle:index.of`	*Microsoft Internet Information Services* 6.0
`"Microsoft-IIS/* Server at" intitle:index.of`	cualquier versión de *Microsoft Internet Information Services*
`"Oracle HTTP Server/* Server at" intitle:index.of`	cualquier versión del servidor *Oracle*
`"IBM _ HTTP _ Server/* * Server at" intitle:index.of`	cualquier versión del servidor IBM
`"Netscape/* Server at" intitle:index.of`	cualquier versión del servidor *Netscape*
`"Red Hat Secure/*" intitle:index.of`	cualquier versión del servidor *Red Hat Secure*
`"HP Apache-based Web Server/*" intitle:index.of`	cualquier versión del servidor HP

Tabla 3. *Búsqueda de páginas WWW estándar de instalación*

Consulta	Servidor
`intitle:"Test Page for Apache Installation" "You are free"`	*Apache* 1.2.6
`intitle:"Test Page for Apache Installation" "It worked!" "this Web site!"`	*Apache* 1.3.0 – 1.3.9
`intitle:"Test Page for Apache Installation" "Seeing this instead"`	*Apache* 1.3.11 – 1.3.33, 2.0
`intitle:"Test Page for the SSL/TLS-aware Apache Installation" "Hey, it worked!"`	*Apache* SSL/TLS
`intitle:"Test Page for the Apache Web Server on Red Hat Linux"`	*Apache* en el sistema Red Hat
`intitle:"Test Page for the Apache Http Server on Fedora Core"`	*Apache* en el sistema Fedora
`intitle:"Welcome to Your New Home Page!" Debian`	*Apache* en el sistema Debian
`intitle:"Welcome to IIS 4.0!"`	*IIS* 4.0
`intitle:"Welcome to Windows 2000 Internet Services"`	*IIS* 5.0
`intitle:"Welcome to Windows XP Server Internet Services"`	*IIS* 6.0

presente en el servidor. Lo puede leer un usuario que activa el demonio WWW. Por eso, basta que el intruso escriba en un sistema indicado la dirección */index.php3?action=telecharger&fichier=/etc/passwd* y se le visualizará el contenido del fichero */etc/passwd* (veáse Figura 3). Desde luego, para encontrar los servidores adecuados, el usuario empleará Google, escribiendo en el campo de consulta: `"WebJeff-Filemanager 1.6" Login`.

Segunda aplicación: *Advanced Guestbook*, es un programa escrito en el lenguaje PHP que emplea la base de datos SQL, que ayuda implementar los libros de visitas en las páginas WWW. En abril de 2004 se publicó una información sobre un error en la versión 2.2 de este programa, que posibilita (gracias a la implementación del código SQL: véase Artículo *AtaquesSQL Injection contra PHP/MySQL* en *hakin9* 3/2005) el acceso al panel de administración. Basta encontrar la página en que de entrada al panel (véase Figura 4) y entrar en el sistema, dejando el campo *username* en hueco, y en el campo *password* escribir `') OR ('a' = 'a`, o al revés: dejar vacío el campo *password* y en el campo *username* escribir `? or 1=1 --`. Nuestro atacante ejemplar, para encontrar los sitios adecuados en la red, puede escribir en el campo de bùsqueda en Google una de las siguintes consultas:

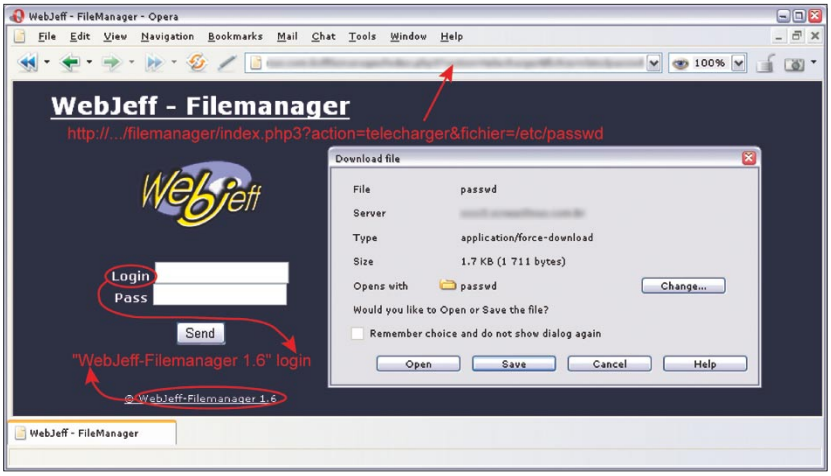

Figura 3. *Versión del programa WebJeff Filemanager adecuada*

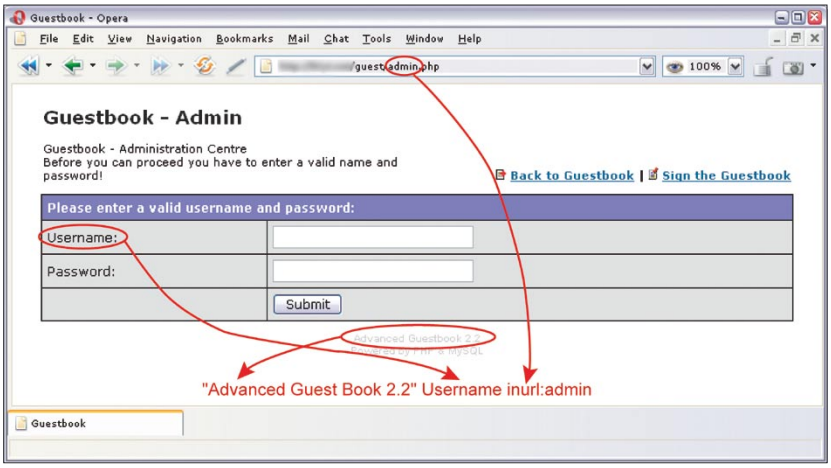

Figura 4. *Advanced Guestbook: página en que se entra en el sistema*

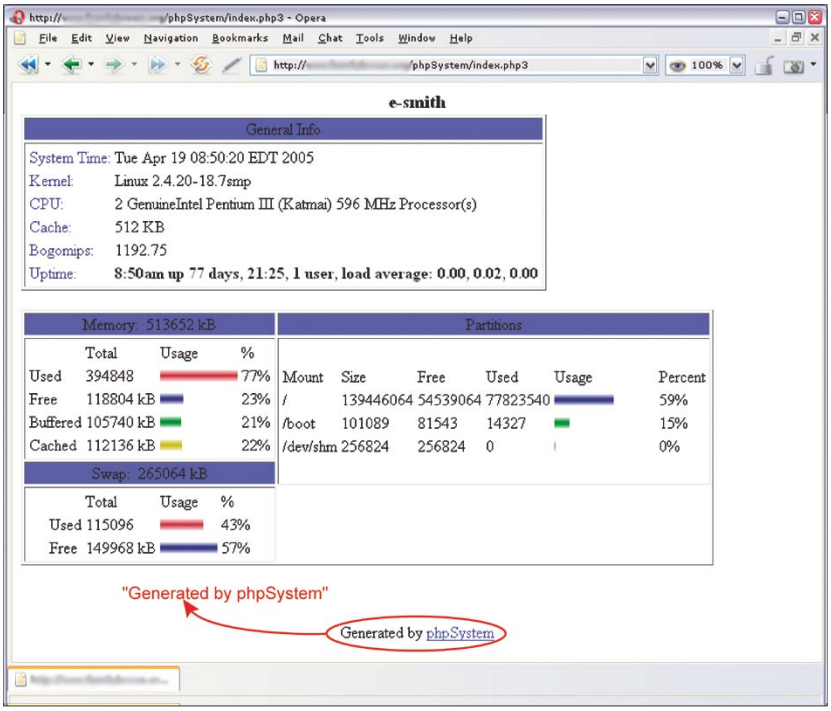

Figura 5. *Estadísticas de phpSystem*

`intitle:Guestbook "Advanced Guestbook 2.2 Powered"` o `"Advanced Guestbook 2.2" Username inurl:admin`.

Para impedir la salida de datos descrita, el administrador tiene que seguir al corriente las informaciones sobre todos los programas que emplea en sus sitios WWW y actualizarlos si se produce un error en cada uno de ellos. Además, vale la pena eliminar de cada página o de cada fichero en que aparecen: anuncios, nombres y números de versiones de programas.

Informaciones sobre redes y sistemas

Antes de casi cada ataque al sistema informático se examina el objetivo. Por lo común, la examinación consiste en escanear los ordenadores: con la intención de definir servicios, tipo de sistema operativo y versión del software de servicios presentes. Para hacerlo más rápido se usan los escáners tipo *Nmap* o *amap*, pero existe también otra opción. Muchos administradores instalan las aplicaciones WWW, que al día generan estadísticas de trabajo del sistema, informan sobre el espacio ocupado en los discos duros, contienen listados de procesos activados e incluso logs del sistema.

Son unas informaciones de gran valor para el atacante. Basta que en Google realice consulta para buscar estadísticas del programa *phpSystem*: `"Generated by phpSystem"`; y se le mostrarán las páginas, como la presentada en Figura 5. Asimismo, puede preguntar por las páginas generadas por el script *Sysinfo*: `intitle:"Sysinfo * " intext:"Generated by Sysinfo * written by The Gamblers."`; que contienen muchas más informaciones sobre el sistema (Figura 6).

Hay muchas posibilidades (en la Tabla 4 se presentan ejemplos de búsquedas de estadísticas e informaciones creadas por los programas más populares). Si el intruso encuentra este tipo de informaciones, puede animarse a realizar el ataque contra el sistema encon-

trado. Además, estas informaciones pueden ayudarle a elegir las herramientas adecuadas o exploits. Por eso, si usamos los programas que posibilitan la monitorización de recursos de nuestros ordenadores, tenemos que hacer todo lo posible para proteger el acceso a estos recursos y para que el sistema requiera la contraseña.

Buscamos los errores

Los comunicados sobre errores HTTP pueden tener mucho valor para el atacante, porque precisamente con estas informaciones se pueden obtener varios datos sobre el sistema, configuraciones y construcción de bases de datos. Por ejemplo, para encontrar los errores generados por la base *Informix* basta con escribir la siguiente consulta en el campo de la búsqueda: `"A syntax error has occurred" filetype:ihtml`. En efecto, el atacante encuentra los comunicados que contienen las informaciones sobre configuración de base de datos, disposición de ficheros en el sistema y a veces también sobre contraseña (véase Figura 7). Para restringir los resultados sólo

Tabla 4. *Programas que elaboran estadísticas de funcionamiento de sistema*

Consulta	Tipo de informaciones
`"Generated by phpSystem"`	Tipo y versión de sistema operativo, configuración de equipo, usuarios registrados en el sistema, enlaces abiertas, espacio ocupado en memoria y en discos duros, puntos de montaje
`"This summary was generated by wwwstat"`	estadísticas de trabajo del servidor WWW, disposición de ficheros en el sistema
`"These statistics were produced by getstats"`	estadísticas de trabajo del servidor WWW, disposición de ficheros en el sistema
`"This report was generated by WebLog"`	estadísticas de trabajo del servidor WWW, disposición de ficheros en el sistema
`intext:"Tobias Oetiker" "traffic analysis"`	estadísticas de trabajo del sistema en forma de diagramas MRTG, configuración de la red
`intitle:"Apache::Status" (inurl:server-status | inurl:status.html | inurl:apache.html)`	versión del servidor, tipo de sistema operativo, listado con procesos hijos y conexiones actuales
`intitle:"ASP Stats Generator *.*" "ASP Stats Generator" "2003-2004 weppos"`	actividad del servidor WWW, muchas informaciones sobre los visitantes
`intitle:"Multimon UPS status page"`	estadísticas de trabajo de equipos UPS
`intitle:"statistics of" "advanced web statistics"`	estadísticas de trabajo de servidor WWW, informaciones sobre los visitantes
`intitle:"System Statistics" +"System and Network Information Center"`	estadísticas de trabajo de sistema en forma de diagramas MRTG, configuración del equipo, servicios accesibles
`intitle:"Usage Statistics for" "Generated by Webalizer"`	estadísticas de trabajo de servidor WWW, informaciones sobre visitantes, disposición de ficheros en el sistema
`intitle:"Web Server Statistics for ****"`	estadísticas del trabajo del servidor WWW, informaciones sobre los visitantes
`inurl:"/axs/ax-admin.pl" -script`	estadísticas de trabajo de servidor WWW, informaciones sobre los visitantes
`inurl:"/cricket/grapher.cgi"`	diagramas MRTG con trabajo de interfaces de la red
`inurl:server-info "Apache Server Information"`	versión y configuración del servidor WWW, tipo de sistema operativo, disposición de ficheros en el sistema
`"Output produced by SysWatch *"`	tipo y versión del sistema operativo, usuarios presentes en el sistema, espacio ocupado en memoria y en discos duros, puntos de montaje, procesos activados, logs del sistema

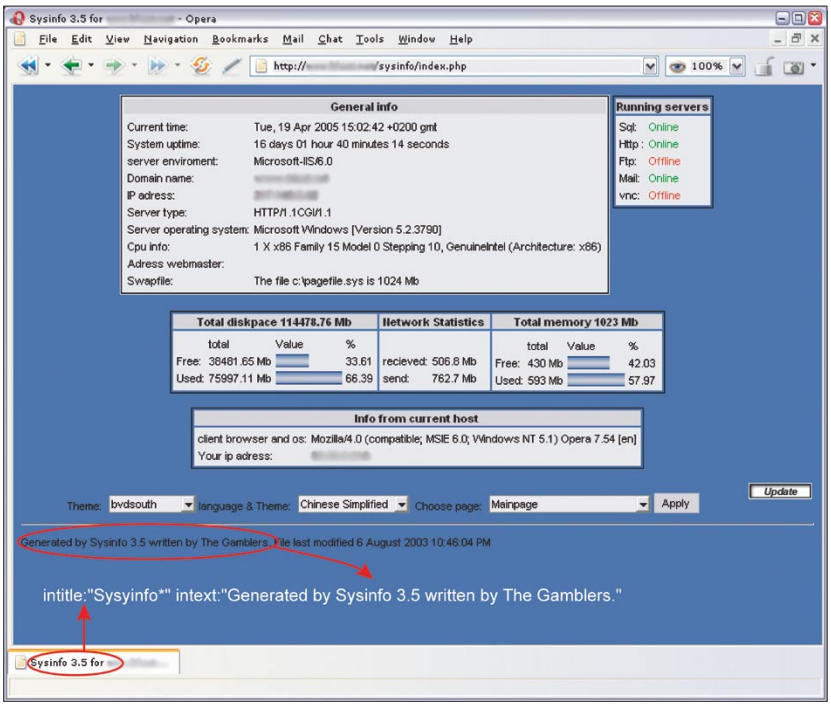

Figura 6. *Estadísticas de Sysinfo*

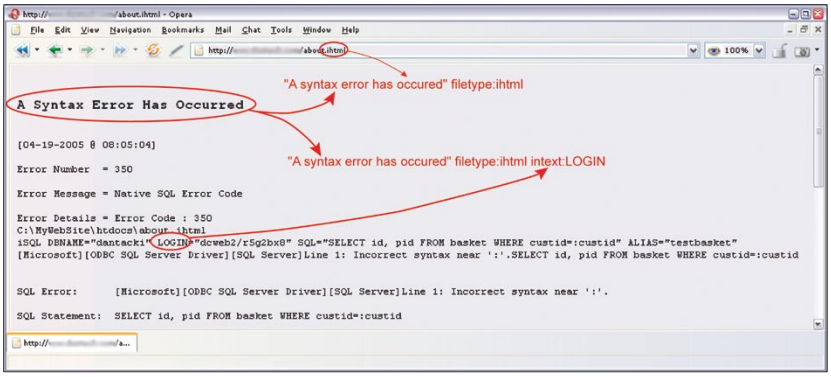

Figura 7. *Modos de aprovecharse de errores en la base de datos Informix*

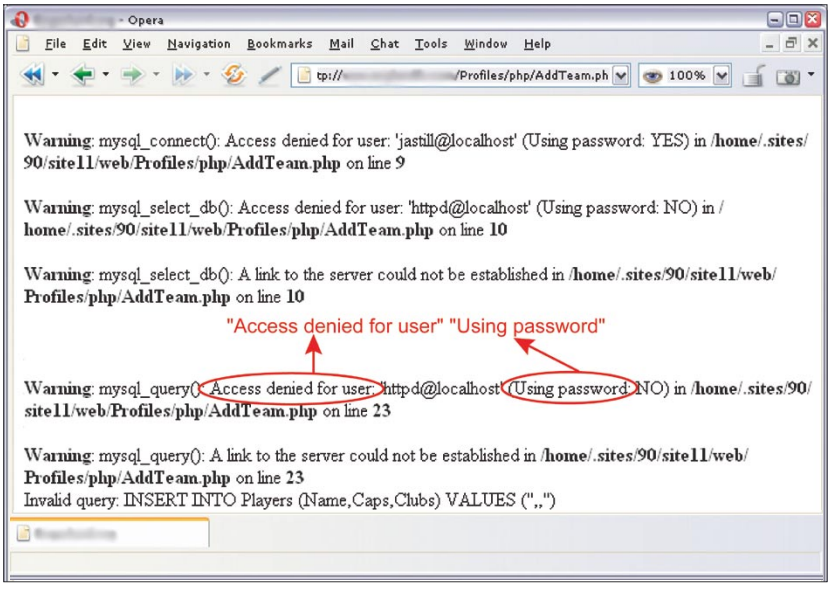

Figura 8. *Error de la base MySQL*

a las páginas con contraseña, podemos modificar un poco la búsqueda: `"A syntax error has occurred" filetype:ihtml intext:LOGIN`.

Asimismo, podemos obtener informaciones interesantes de errores en la base de datos *MySQL*. Lo vemos en el ejemplo de la consulta `"Access denied for user" "Using password"`. Figura 8 representa una de las páginas encontradas de este modo. En la Tabla 5 hay otros ejemplos de consultas que aprovechan este tipo de errores.

El único modo de proteger nuestros sistema contra informaciones sobre errores accesibles en público consiste en eliminarlas rápidemente y, si tenemos esta posibilidad, configurar el software para que almacene informaciones sobre errores en ficheros destinados especialemente a este objetivo y no las envie a las páginas accesibles por los usuarios.

Hay que recordar que incluso si eliminamos rápidamente los errores (y las páginas visualizadas por Google no serán actuales), el intruso puede ver la copia de la página almacenada por *cache* del navegador Google. Basta con indicar el enlace a una copia del sitio WWW en listado de resultados. Por suerte, debido a la cantidad enorme de recursos en Internet las copias se almacenan en *cache* por poco tiempo.

Buscamos las contraseñas

En la red se pueden encontrar varias contraseñas a cualquier tipo de recursos: cuentas de correo electrónico, servidores FTP o incluso a cuentas shell. Es efecto de la ignorancia de los usuarios que ponen las contraseñas en sitios públicos, pero también de la negligencia de fabricantes de software, que no protegen bien a los usuarios, o no les informan sobre la necesidad de modificar la configuración estándar de sus productos.

Pongamos el ejemplo de *WS_FTP*, el cliente FTP, popular y usado por mucha gente que

como la mayoría de software aplicado, recuerda las contraseñas a las cuentas. *WS_FTP* memoriza su configuración e informaciones sobre las cuentas del usuario en el fichero *WS_FTP.ini*. Desafortunadamente, no todos somos conscientes del hecho de que cada uno que gana acceso a la configuración del cliente FTP, a la vez podrá acceder a nuestros recursos. A decir verdad, las contraseñas almacenadas en el fichero *WS_FTP.ini* están encriptadas, pero no es un protección suficiente: si el intruso tiene el fichero de configuración, puede emplear las herramientas para decodificarlos, o simplemente instalar el programa *WS_FTP* y activarlo con nuestra configuración. ¿Cómo el intruso puede encontrar miles de ficheros de configuración del cliente *WS_FTP*? Desde luego, con ayuda de Google. Si realiza consultas `"Index of/" "Parent Directory" "WS_FTP.ini"` o `filetype:ini WS_FTP PWD` se le mostrarán muchos enlaces

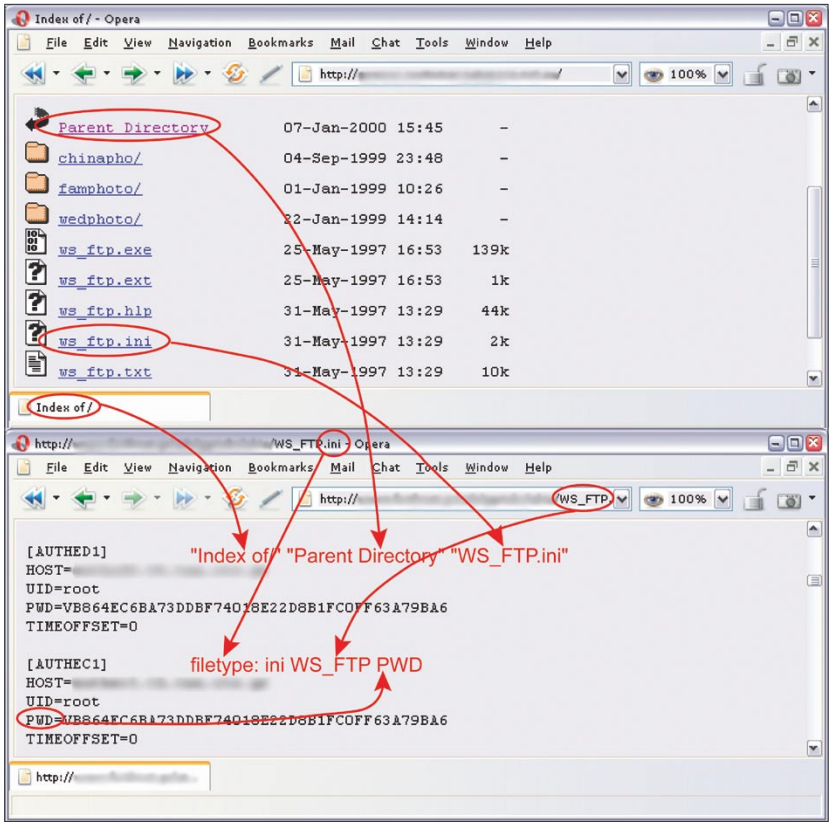

Figura 9. *Fichero de configuración del programa WS_FTP*

Tabla 5. *Comunicados sobre errores*

Consulta	Resultado
`"A syntax error has occurred" filetype:ihtml`	errores de la base *Informix* – pueden contener nombres de funciones, nombres de ficheros, informaciones sobre disposición de ficheros, fragmentos del código SQL y contraseñas
`"Access denied for user" "Using password"`	errores en autorización – pueden contener nombres de usuarios, nombres de funciones, informaciones sobre disposición de ficheros y fragmentos del código SQL
`"The script whose uid is " "is not allowed to access"`	errores PHP relacionados con control del acceso – pueden contener nombres de ficheros, nombres de funciones e informaciones sobre disposición de ficheros
`"ORA-00921: unexpected end of SQL command"`	errores de la base *Oracle* – pueden contener nombres de ficheros, nombres de funciones e informaciones sobre disposición de ficheros
`"error found handling the request" cocoon filetype:xml`	errores del programa *Cocoon* – pueden contener número de versión *Cocoon*, nombres de ficheros, nombres de funciones e informaciones sobre disposición de ficheros
`"Invision Power Board Database Error"`	errores de foro de debate *Invision Power Board* – pueden contener nombres de funciones, nombres de ficheros, informaciones sobre disposición de ficheros en el sistema y fragmentos del código SQL
`"Warning: mysql_query()" "invalid query"`	errores de base de datos *MySQL* – pueden contener nombres de usuarios, nombres de funciones, nombres de ficheros e informaciones sobre disposición de ficheros
`"Error Message : Error loading required libraries."`	Errores en scripts CGI – pueden contener informaciones sobre tipo de sistema operativo y versión de software, nombres de usuarios, nombres de ficheros e informaciones sobre disposición de ficheros en el sistema
`"#mysql dump" filetype:sql`	errores de la base *MySQL* – pueden contener informaciones sobre estructura y sobre contenido de la base de datos

Tabla 6. *Contraseñas: ejemplos de consultas en Google*

Consulta	Resultado
`"http://*:*@www" site`	contraseñas a la página *site*, escritas en forma de *http://username:password@www...*
`filetype:bak inurl:"htaccess|passwd|shadow|htusers"`	copias de seguridad de ficheros, en que se pueden hallar informaciones sobre nombres de usuarios y sobre contraseñas
`filetype:mdb inurl:"account|users|admin|administrators|passwd|password"`	ficheros tipo *mdb*, que pueden contener informaciones sobre contraseñas
`intitle:"Index of" pwd.db`	ficheros *pwd.db* pueden contener nombres de usuarios y contraseñas encriptadas
`inurl:admin inurl:backup intitle:index.of`	directorios que contienen en el nombre las palabras admin y backup
`"Index of/" "Parent Directory" "WS_FTP.ini" filetype:ini WS_FTP PWD`	ficheros de configuración del programa *WS_FTP*, que pueden contener contraseñas a los servidores FTP
`ext:pwd inurl:(service|authors|administrators|users) "# -FrontPage-"`	ficheros que contienen contraseñas del programa *Microsoft FrontPage*
`filetype:sql ("passwd values ****" | "password values ****" | "pass values ****" )`	ficheros que contienen el código SQL y contraseñas agregadas a la base de datos
`intitle:index.of trillian.ini`	ficheros de configuración del mensajero *Trillian*
`eggdrop filetype:user user`	ficheros de configuración del ircbot *Eggdrop*
`filetype:conf slapd.conf`	ficheros de configuración de la aplicación *OpenLDAP*
`inurl:"wvdial.conf" intext:"password"`	ficheros de configuración del programa *WV Dial*
`ext:ini eudora.ini`	ficheros de configuración del programa cliente de correo electrónico *Eudora*
`filetype:mdb inurl:users.mdb`	ficheros *Microsoft Access*, que pueden contener informaciones sobre las cuentas
`intext:"powered by Web Wiz Journal"`	servicios WWW que usan la aplicación *Web Wiz Journal*, que en la configuración estándar posibilita descargar el fichero que contiene la contraseña; en vez de dirección supuesta *http:///<host>/journal/* hay que escribir *http:///<host>/journal/journal.mdb*

`"Powered by DUclassified" -site:duware.com`
`"Powered by DUcalendar" -site:duware.com`
`"Powered by DUdirectory" -site:duware.com`
`"Powered by DUclassmate" -site:duware.com`
`"Powered by DUdownload" -site:duware.com`
`"Powered by DUpaypal" -site:duware.com`
`"Powered by DUforum" -site:duware.com`
`intitle:dupics inurl:(add.asp | default.asp | view.asp | voting.asp) -site:duware.com`
	sitios WWW, que usan aplicaciones *DUclassified*, *DUcalendar*, *DUdirectory*, *DUclassmate*, *DUdownload*, *DUpaypal*, *DUforum* o *DUpics*; que su configuración estándar pueden descargar el fichero con la contraseña, si en vez de la dirección supuesta (para DUclassified) *http:///<host>/duClassified/* se escribe *http:///<host>/duClassified/_private/duclassified.mdb*

`intext:"BiTBOARD v2.0" "BiTSHiFTERS Bulletin Board"`	sitios WWW que usan la aplicación *Bitboard2*, en su configuración estándar se puede descargar el fichero con las contraseñas; en vez de la dirección supuesta *http:///<host>/forum/forum.php* hay que escribir *http:///<host>/forum/admin/data_passwd.dat*

a unos datos que le interesen, que en nuestra ignorancia nosotros mismos le ponemos en sus manos (Figura 9).

Otro ejemplo es la aplicación web que se llama *DUclassified*, con que se agregan y administran anuncios en los sitios WWW. En la configuración estándar de este programa, los nombres de usuarios, las contraseñas y otros datos se guardan en el fichero *duclassified.mdb*, que se halla en el subdirectorio *_private*, no protegido contra lectura. Basta, pues, con encontrar un servicio que emplee *DUclassifield* con la dirección de ejemplo *http:///<host>/duClassified/* y cambiarla en *http://<host>/duClassified/_private/duclassified.mdb*, para obtener el fichero con contraseñas y al mismo tiempo ganar el acceso ilimitado a la aplicación (lo representa Figura 10). En cambio, para encontrar los sitios web que empleen la aplicación descrita, se puede realizar en Google la consulta siguiente: `"Powered by DUclassified" -site:duware.com` (para evitar los resultados relativos al sitio web del fabricante). Es curioso, que el fabricante de *DUclassified,* la empresa DUware, ha elaborado un par de aplicaciones más que también están expuestos a este tipo de ataques.

En teoría, todos sabemos que no se debe pegar las contraseñas al monitor o esconderlas debajo del teclado. Mientras tanto, mucha gente escribe sus contraseñas en ficheros y las coloca en sus directorios personales que, contra sus expectativas, se pueden conseguir por Internet. Además, muchos de ellos son administradores de la red, por eso estos ficheros tienen un tamaño considerable. Es difícil definir una norma general para buscar este tipo de datos, pero se obtiene buenos resultados combinando las palabras *account*, *users*, *admin*, *administrators*, *passwd*, *password* etc. y con combinaciones de varios tipos de ficheros *.xls*, *.txt*, *.doc*, *.mdb* y *.pdf*. Merece la pena también fijarnos en directorios en

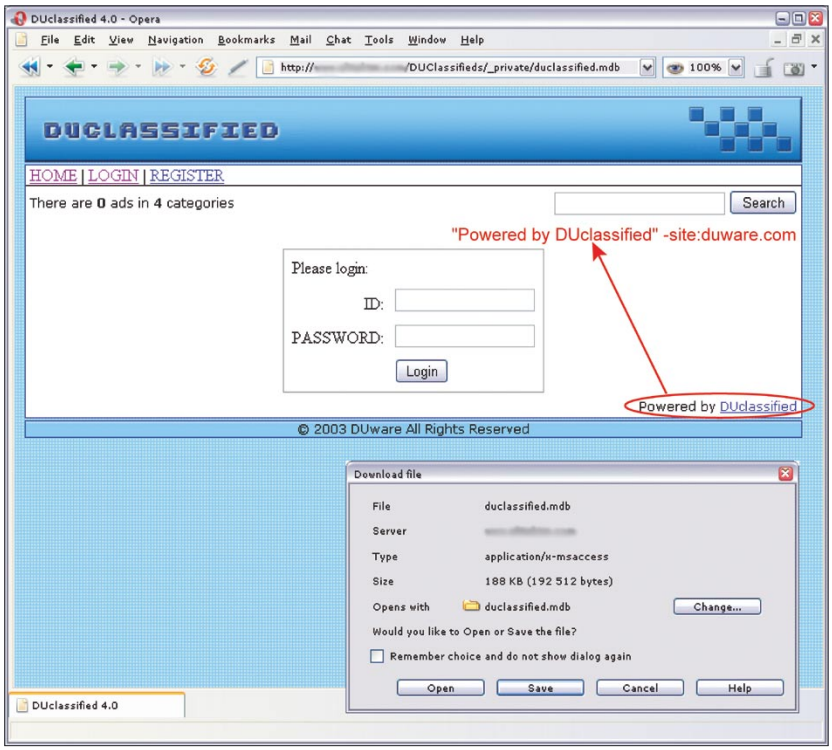

Figura 10. *Programa DUclassified, configurado de modo estándar*

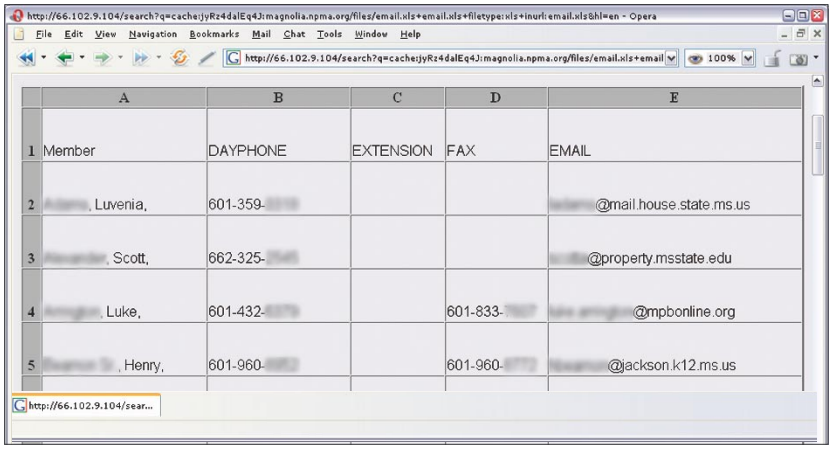

Figura 11. *Listado con direcciones electrónico buscado en Google*

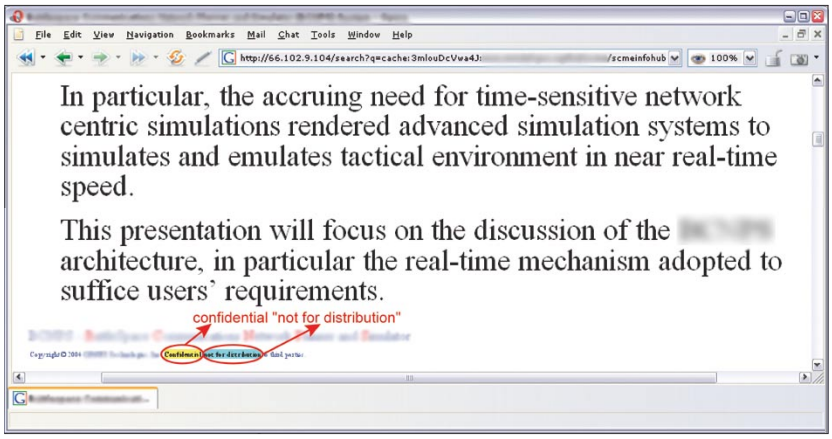

Figura 12. *Documento confidencial encontrado por el navegador*

Tabla 7. *Búsqueda de datos personales y de documentos confidenciales*

Consulta	Resultado
`filetype:xls inurl:"email.xls"`	ficheros *email.xls*, que pueden abarcar datos con direcciones
`"phone * * *" "address *" "e-mail" intitle:"curriculum vitae"`	documentos CV
`"not for distribution" confidential`	documentos con la cláusula confidential
`buddylist.blt`	listados de contacto del mensajero AIM
`intitle:index.of mystuff.xml`	listados de contacto del mensajero *Trillian*
`filetype:ctt "msn"`	listados de contacto del mensajero MSN
`filetype:QDF QDF`	base de datos el programa financiero *Quicken*
`intitle:index.of finances.xls`	ficheros *finances.xls*, que pueden contener informaciones sobre las cuentas bancarias, especificaciones financieras y números de tarjetas de crédito
`intitle:"Index Of" -inurl:maillog maillog size`	ficheros *maillog*, que pueden contener mensajes de correo electrónico
`"Network Vulnerability Assessment Report" "Host Vulnerability Summary Report" filetype:pdf "Assessment Report" "This file was generated by Nessus"`	informes de estudios de seguridad de la red, pruebas de penetración, etc.

cuyo nombre aparecen las palabras *admin*, *backup* o similares: `inurl: admin intitle:index.of`. En Tabla 6 hay ejemplos de consultas para buscar datos relacionados con contraseñas.

Para impedir que los intrusos tengan acceso a nuestras contraseñas, sobre todo tenemos que pensar dónde y con qué objetivo las escribimos, cómo las almacenamos y qué pasa con ellas. Si nos ocupamos de un sitio web, debemos analizar la configuración de aplicaciones empleadas para buscar los datos mal protegidos o expuestos al ataque y protegerlos de modo apropriado.

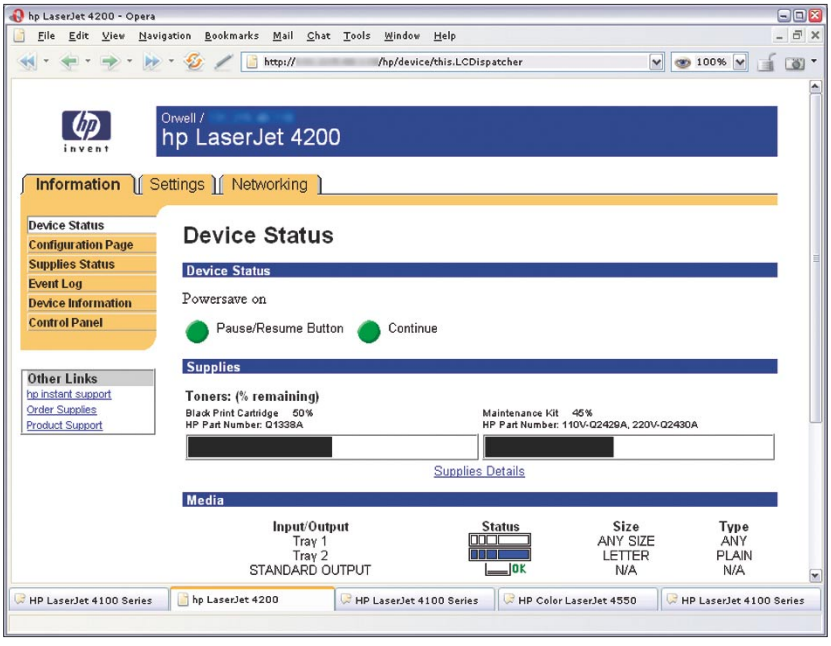

Figura 13. *Página de configuración de la impresora HP encontrada por Google*

Datos personales y documentos confidenciales

Tanto en Polonia, en la Unión Europea, como en los Estados Unidos hay una legislación adecuada cuya finalidad es proteger nuestra privacidad. Deafortunadamente, a veces documentos confidenciales de todo tipo que contienen nuestros datos se colocan en unos sitios accesibles al público o se envian por la red sin protección necesaria. Basta que el instruso gane el acceso al correo electrónico con nuestro Curriculum Vitae enviado cuando buscábamos el trabajo, y conocerá nuestro domicilio, número del teléfono, fecha de nacimiento, desarrollo de educación, conocimientos y experiencia.

En Internet hay muchos documentos de este tipo. Para encontrarlos hay que realizar la siguiente consulta: `intitle:"curriculum vitae" "phone * * *" "address *" "e-mail"`. Asimismo, es fácil encontrar datos personales, en forma de listados con apellidos, números de teléfono y cuentas de correo electrónico (Figura 11). Es así, porque casi todos los usuarios de Internet elaboran varios tipos de libros con direcciones:

Tabla 8. *Series ejemplares para encontrar hardware de red*

Consulta	Equipo
`"Copyright (c) Tektronix, Inc." "printer status"`	impresora PhaserLink
`inurl:"printer/main.html" intext:"settings"`	impresora Brother HL
`intitle:"Dell Laser Printer" ews`	impresoras Della con tecnología EWS
`intext:centreware inurl:status`	impresora Xerox Phaser 4500/6250/8200/8400
`inurl:hp/device/this.LCDispatcher`	impresoras HP
`intitle:liveapplet inurl:LvAppl`	cámaras Canon Webview
`intitle:"EvoCam" inurl:"webcam.html"`	cámaras Evocam
`inurl:"ViewerFrame?Mode="`	cámaras Panasonic Network Camera
`(intext:"MOBOTIX M1" | intext:"MOBOTIX M10") intext: "Open Menu" Shift-Reload`	cámaras Mobotix
`inurl:indexFrame.shtml Axis`	cámaras Axis
`SNC-RZ30 HOME`	cámaras Sony SNC-RZ30
`intitle:"my webcamXP server!" inurl:":8080"`	cámaras accesibles por la aplicación *WebcamXP Server*
`allintitle:Brains, Corp. camera`	cámaras accesibles por la aplicación *mmEye*
`intitle:"active webcam page"`	cámaras con la interfaz USB

sin gran importancia para un intruso común y corriente, pero ya un sociotécnico con experiencia podrá servirse de estos datos, sobre todo si son unos datos de contactos dentro de una empresa. En este caso, buenos resultados se producen también por ejemplo con la consulta: `filetype:xls inurl:"email.xls"`; que busca hojas de cálculo con el nombre *email.xls*.

Lo mismo pasa con mensajeros de la red y listados con datos de contacto almacenados en ellos. Después de encontrar este tipo de especificacon, el intruso podrá hacerse pasar por nuestros amigos. Es curioso cuántos datos personales se puede encontrar en varios documentos oficiales: informes de policía, documentos emitidos por tribunales o incluso documentos con antecedentes médicos.

En la red podemos también encontrar documentos con cláusula de confidencialidad, que contienen informaciones de carácter confidenciales, p. ej. planes de diseño, documentación técnica, varias encuestas, informes, presentaciones y un montón de otro tipo de documentos internos de empresas. Se pueden encontrar, porque a menudo abarcan la palabra *confidential*, la frase *Not for distribution* o similares (véase Figura 12). La Tabla 7 especifica ejemplos de consultas para encontrar documentos que pueden contener datos personales e informaciones confidenciales.

Del mismo modo, como en caso de las contraseñas, para evitar que se descubran nuestras informaciones privadas, sólo podemos ser prudentes y cuidar los datos publicados. Las empresas y las instituciones deben (y en muchos casos tienen que) elaborar e implementar unos reglamentos adecuados, procedimientos y normas que definen circulación interna de informaciones, responabilidad y consecuencias de no cumplir con ellas.

Hardware de red

A muchos administradores no les importa la seguridad de sus equipos, como: impresoras de red o cámaras web. Mientras tanto, una impresora puede ser la primera barrera mal protegida, que al principio conquista el intruso y luego la usa para atacar los demás sistemas en la red o fuera de ella. Las cámaras web por supuesto no son tan peligrosas, pues se puede tratarlas como un entretenimiento, sin embargo no es difícil imaginarse una situación en que estos datos tengan importancia (espionaje industrial, robo). En la Tabla 8 hay consultas para buscar impresoras y cámaras, y en la Figura 13 representa la página de configuración de una impresora encontrada en la red. ■