INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES &SEGURIDAD

12

SEGURIDAD FÍSICA DE LA RED

En este fascículo analizaremos la importancia de la seguridad en una red, conoceremos aplicaciones útiles y recomendaremos prácticas seguras para los usuarios.

- BIOMETRÍA
- AMBIENTES SEGUROS
- PORT SCANNING
- SNIFFING
- INGENIERÍA SOCIAL
- IPSEC

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Curso visual y práctico **Técnico en redes y seguridad** es una publicación de Fox Andina en coedición con Dálaga S.A. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Copyright © Fox Andina S.A. I, MMXIII.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Opciones básicas y operaciones avanzadas que son necesarias para obtener un aumento en el nivel de seguridad física y lógica que encontramos en una red de datos.

En la clase anterior vimos en detalle la configuración y administración de recursos compartidos tanto en sistemas Windows como en GNU/Linux. Aprendimos a compartir recursos y conocimos cómo realizar networking entre dispositivos tales como SmartTV, Smartphones y consolas de videojuegos. Revisamos las características de las tecnologías SAN y NAS, y también profundizamos sobre los permisos y la seguridad de los recursos compartidos.

Para terminar, conocimos los alcances de la auditoría, y revisamos la regla del mínimo privilegio y la toma de posesión.

En esta oportunidad, conoceremos en detalle los alcances y el uso de las tecnologías biométricas, veremos aplicaciones que nos servirán para elevar el nivel de seguridad en nuestra red y revisaremos las opciones de port scanning y sniffing.

Para continuar, conoceremos la ingeniería social y recomendaremos algunas prácticas orientadas a los usuarios de una red de datos; terminaremos analizando en detalle qué es IPsec y para qué sirve.

12

2
Tecnologías biométricas

12
Port scanning

18
Ingeniería social

22
IPsec

Tecnologías biométricas

La biometría es aplicada en diversos equipos para brindar acceso a determinados sistemas o equipos, incluso utilizando varios métodos simultáneamente.

Hoy en día se conocen diversos métodos de reconocimiento de patrones únicos, que se utilizan para poder distinguirnos los unos de los otros.

En las **redes informáticas**, necesitamos poder **identificar diversos usuarios** que poseen características diferenciadas para el uso de la red y definir cómo deben pasar determinadas pruebas de reconocimiento para ser identificados y autorizados en los sistemas.

La tecnología actual nos ofrece diversos métodos de reconocimiento de usuario, mediante los cuales se han adoptado reglas para mejorar la experiencia usuario/terminal o, en otras palabras, para aumentar la seguridad y reducir la complejidad en la identificación del usuario. Al momento de iniciar sesión en nuestros equipos, lo que realizamos es el ingreso de una clave que nos identifica como usuarios autorizados; esta clave puede constar de distintos códigos o patrones e, incluso, puede ser ingresada por diversos medios físicos. La **seguridad informática** se mide por la imposibilidad de suplantar usuarios o por el control exhaustivo del ingreso y la confiabilidad en cuanto al manejo de la información dentro del sistema; por ello, se han desarrollado procesos denominados **biométricos**.

Los escaneos de la superficie son comparados con la base de datos existente y de esta forma permiten el ingreso a los sistemas.

Biometría

La **biometría** es el estudio del reconocimiento de determinados patrones físicos basados en rasgos particulares principalmente de los seres humanos. La característica principal es la identificación de patrones únicos, que son irrepetibles e intransferibles y solo se presentan en un único individuo. En nuestras tecnologías biométricas, se realizan procedimientos y cálculos matemáticos y estadísticos, que generan los patrones únicos que son comparados con el individuo. La biometría se basa en especial en categorías según las siguientes características:

- **Características físicas**: estáticas; esto se refiere a las líneas de las huellas digitales, la retina, el iris del ojo, patrones faciales, expresiones, morfología facial, geometría de las extremidades, postura, y todo aquello que pueda ser representado físicamente.
- **Características del comportamiento**: dinámicas; como la firma, el paso, la forma de caminar, una expresión, un movimiento determinado, incluso la frecuencia y la velocidad del tecleo.
- **Mezcla entre ambos**: físicas y de comportamiento; incluyen la voz, el tono, la forma de la voz y el timbre, entre otros.

Métodos

Si bien todos los métodos existentes se aplican en sistemas en los que se requieren una seguridad elevada y un nivel de complejidad intenso, no todos los sistemas son perfectos (pero sí difícilmente franqueables), por lo que se requieren tecnologías precisas, algoritmos de funcionamiento variables y algo maleables que permitan corregir pequeñas distorsiones y admitan una tolerancia (se da principalmente en el reconocimiento de las huellas digitales, a veces una parte puede ser borrada por un accidente, y aun así deben ser identificables).

En todos los sistemas de detección biométricos, cuando el usuario ingresa al sistema, un programa realiza procedimientos de chequeo y comparación con la base de datos, para verificar si estos parámetros calculados estadísticamente concuerdan con el nivel de tolerancia del

Tabla comparativa de sistemas biométricos

	Retina	Huellas dactilares	Vascular dedo/mano	Geometría de la mano	Escritura y firma	Voz	Cara 2D	Cara 3D
Fiabilidad	Muy alta	Muy alta	Muy alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Baja	Alta	Muy alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataque	Muy alta	Alta	Muy alta	Alta	Media	Media	Media	Alta
Adaptación	Baja	Alta	Alta	Alta	Muy alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media	Alta

programa (los programas comerciales varían mucho, desde un 60% hasta precisiones del 99,9%). Los encargados de obtener la lectura son dispositivos preparados para cada uso que, por lo general, están basados en láseres que detectan líneas, surcos o tonalidad mediante principios físicos, y expresan estas señales a través de números que se traducen en una clave determinada.

EL INICIO DE SESIÓN SE REALIZA CUANDO LOS PATRONES ANALIZADOS COINCIDEN CON LOS ALMACENADOS EN LA BASE DE DATOS.

En sistemas poco precisos, estas claves pueden diferenciarse de la de la base de datos, y se estima si es correcta. En sistemas de alta precisión, cuando se aproxima al resultado, estos valores deben ser idénticos, por lo que el hardware de lectura utiliza métodos más avanzados.

Precisión

La medida de la precisión se basa en rendimientos denominados tasa de falso positivo (*False Acceptance Rate*, **FAR**), tasa de falso negativo (*False Non-Match Rate*, **FNMR** o *False Rejection Rate*, **FRR**) y tasa de fallo de aislamiento (*Failure to enroll Rate*, **FTR** o **FER**). Tanto la **FAR** como la **FRR** pueden ser convertidas unas en otras modificando ciertos parámetros. Para estudiar la diferencia entre los dos parámetros, se utiliza la tasa de error similar (*Equal Error Rate*, **EER**), también conocida como tasa de error por crossover (*Crossover Error Rate* o **CER**). Este parámetro, que mide la diferencia entre los falsos, asegura que el método de lectura sea más preciso cuando el **EER** o **CER** se aproxime a **0**.

Parámetros

Los parámetros analizados hoy en día se diferencian mediante la: fiabilidad, facilidad de uso, prevención de ataques, aceptación y estabilidad. Utilizando estas características, se analizan los diferentes objetos por verificar que suelen corresponder a: iris del ojo, retina, huellas digitales, el patrón vascular del dedo y de la mano, la geometría de la mano, escritura, firma, voz, reconocimiento 2D y, en la actualidad, también perfiles en 3D. A continuación, vemos los principales procesos, como identificaciones corporales, para la autenticación de usuarios:

- **Huellas dactilares:** basado en los patrones únicos de cada persona. Se analizan los bordes y los valles de las huellas, y se comparan con las bases de datos. Se dificulta la lectura si las líneas son alteradas por lastimaduras, suciedad, etc.
- **Geografía de la mano:** realiza un escaneo de toda la mano solucionando los errores de lectura de las huellas dactilares, ya que se analiza toda la superficie. Una alternativa económica.
- **Escaneo de retina:** se realiza el análisis de la disposición de los vasos sanguíneos de la retina del ojo en la que se mapean más de 260 zonas únicas.
- **Reconocimiento de voz:** se efectúa el análisis de los patrones y la frecuencia con los que la persona repite una frase, ya que estos son únicos.

Es necesario tener en cuenta que distintos métodos brindan los mismos resultados de reconocimiento, aunque más o menos precisos. ■

Discusiones

Al igual que sucede con los objetos personales (por ejemplo, una llave de nuestro domicilio), existen metodologías por las cuales se puede suplantar a una persona o duplicar las cualidades con el fin de engañar al sistema; de esta manera, los intrusos pueden ingresar al sistema como si fueran los propietarios con todos los beneficios. Por ello, generalmente se aplica más de un método biométrico para comparar e impedir la suplantación del verdadero propietario.

Ambientes seguros

En esta ocasión, revisaremos en detalle las medidas de seguridad para proteger la información de nuestra computadora, ya sea en ambientes hogareños o corporativos.

Existen variados métodos de asegurar los equipos informáticos con los que trabajamos diariamente. Tanto en notebooks como en computadoras de escritorio, servidores o smartphones las formas varían, pero el objetivo se mantiene: **evitar el robo ya sea de los equipos**, físicamente hablando, o de su contenido.

A continuación, vamos a conocer las maneras de protegernos. En primera instancia, separaremos los tipos de hardware para sectorizar las medidas; y vamos a comenzar por los smartphones.

Smartphone

En las tiendas especializadas, encontraremos aplicaciones antirrobo, que protegerán nuestros datos en equipos con **Android**, **Symbian**, **Windows Phone**, **iOS** o **BBOS**, en caso de que hayamos sido víctimas de un asalto.

Se trata de aplicaciones de borrado automático que se activan mediante un simple SMS enviado desde el proveedor de la aplicación de seguridad, lo que ejecuta un **reset** a valores predeterminados de fábrica del dispositivo y todas las unidades de almacenamiento, incluida la tarjeta SD. Un ejemplo de este tipo de aplicaciones es **Lookout** para las plataformas Android e iOS (es posible descargar la versión gratuita con limitaciones desde la tienda específica de cada sistema operativo).

Este tipo de soluciones también se aplican a las tablets. Cabe destacar que estas aplicaciones, además, tienen la capacidad de activar el GPS del equipo para realizar un rastreo de su ubicación.

Existen diversas aplicaciones que nos ayudarán a proteger los equipos smarthphones o tablets.

Equipos portátiles

Pasemos ahora a las portátiles; en este caso, **notebooks**, **netbooks** y **ultrabooks**. Si bien es cierto que la comodidad de poder llevarnos la oficina a cualquier lugar que viajemos es importante, el tamaño de estos equipos los hace muy susceptibles de ser arrebatados.

Pero la tecnología en cuestiones de seguridad siempre está a la vanguardia para proteger nuestros equipos. Todas las portátiles tienen una medida de seguridad física: el puerto Kensington, en el cual se inserta un candado homónimo para amarrar el equipo portátil a algún objeto fijo o pesado para evitar su sustracción. Un ejemplo de esto es el candado de seguridad para equipos portátiles.

Equipos de escritorio

En cuanto a los equipos de escritorio, también podemos mencionar algunas medidas de seguridad físicas tales como los gabinetes con cerradura. Si bien son bastante más costosos que los gabinetes comunes, existen algunos modelos que, en vez de tener los clásicos tornillos para su apertura, poseen una pequeña cerradura en su lateral otorgándole la seguridad extra necesaria para evitar el accionar de dedos curiosos en su interior. Asimismo, podemos mencionar métodos menos profesionales (o caseros si se prefiere) como fijar el gabinete al escritorio mediante tornillos ubicados dentro del gabinete; o como se solía ver en los cibercafés, el uso de un sistema de fijación mediante perfiles de hierro fijados a la pared, con una bisagra y apertura mediante candado.

También sería posible la utilización de alarmas magnéticas, las que se activan al alejar el receptor (ubicado estratégicamente dentro del gabinete) de su emisor (escondido en el escritorio). Un sistema similar existe para los smartphones, pero aprovechando sus sensores

(acelerómetro, giroscopio, etc.). Mediante una simple app, el teléfono hace sonar la alarma si este cambia de posición o es movido.

Servidores

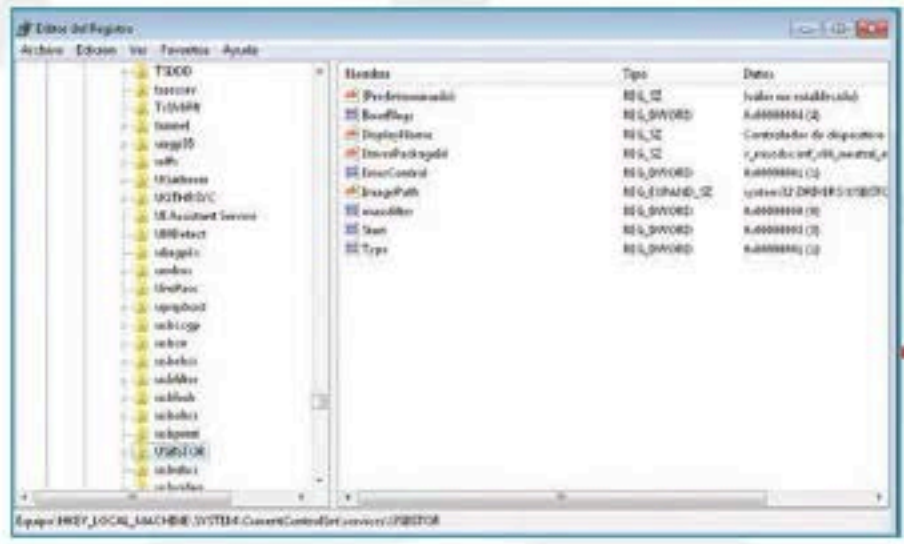
Pasemos ahora a los servidores y hagamos una diferencia imprescindible: los servidores de pequeñas empresas que funcionan en una configuración de hardware similar a una desktop (gabinete, monitor, teclado, mouse, etc.) por un lado. Por el otro, tenemos los servidores de grandes compañías, centros de cómputos, datacenters y proveedores de servicios cloud, que funcionan rackeados. Es decir, en un gabinete de grandes dimensiones en conjunto con otros servidores. Aquí se instalan, en los racks, solamente los motherboards, placas, discos y memoria, sin gabinetes ni monitores u otros periféricos, ya que las tareas se controlan en forma completamente remota.
En el caso del primer grupo, las medidas de seguridad físicas son similares a las que podemos encontrar en las desktop, ya que sus gabinetes también son similares.

LAS TARJETAS MAGNÉTICAS SON EL COMPLEMENTO IDEAL PARA LOS SISTEMAS DE SEGURIDAD BIOMÉTRICOS DE BAJO COSTO, COMO EL DE RECONOCIMIENTO DE VOZ.

Si hablamos de grandes centros de cómputos o similares, encontraremos racks montados sobre rieles, para poder moverlos; en dichos rieles, pueden colocarse candados especiales que evitarán cualquier movimiento de los racks. Pasando a los racks en sí, encontramos dos medidas de seguridad independientes una de otra: en los paneles laterales que nos dan acceso al cableado, existen cerraduras que los aseguran de la forma en que mencionamos anteriormente.
Además, en el panel frontal, podemos encontrar desde cierres con tarjetas magnéticas hasta cerraduras biométricas que funcionan por escaneo de huellas dactilares o reconocimiento de palma, dependiendo de cuán valiosa sea la información almacenada o de qué nivel de paranoia tenga el encargado de asegurarla. El escáner de palma de mano reconoce la morfología de la mano del usuario y no las vetas de la piel. En un ambiente ideal, se utilizaría en combinación con una tarjeta magnética o con un lector de huellas dactilares.

Software

Ahora, vamos a dar un paso al costado, dejando un poco el aspecto físico de la seguridad en equipos informáticos. Nos enfocaremos en lo que el software tiene para ofrecernos ya que, en gran medida, nuestros datos están al alcance de cualquiera que pueda ingresar a nuestro equipo desde Internet.



Aquí vemos la ubicación de la entrada del registro que debemos modificar para desactivar los puertos USB.

El primer paso en la seguridad a nivel software de una computadora, sea de escritorio, portátil o servidores, reside ni más ni menos que en el BIOS. En el BIOS es posible configurar la contraseña de usuario y la contraseña de supervisor. La diferencia entre ambas radica en que la contraseña de usuario solo servirá para acceder al BIOS y modificarla como también para iniciar el equipo en caso de configurar el arranque protegido por contraseña. En cambio, la contraseña de supervisor sirve, además de para iniciar el equipo, para acceder al BIOS y modificar las configuraciones de este a nuestro antojo.

En esta imagen, podemos observar el panel frontal de un sistema de servidores rackeados.

Los candados Kensington son ideales para proteger un equipo portátil, ya que podemos atarlo al escritorio.

Inhabilitar USB

Como todos sabemos, los dispositivos de almacenamiento masivo externos son cada vez más comunes en el uso diario. Estamos hablando de discos duros externos, pendrives, tarjetas de memoria, entre otros.

Dado que los puertos USB están incorporados en el motherboard, es muy fácil encontrarlos sea cual sea el equipo que estamos utilizando. De todos modos, tenemos la posibilidad, mediante un método combinado de hardware y de software, de inhabilitarlos para evitar que usuarios no autorizados conecten tales dispositivos al equipo.

SI OLVIDAMOS LA CONTRASEÑA DE SUPERVISOR DEL BIOS, NO HABRÁ MÁS ALTERNATIVA QUE REALIZAR UN CLEAR CMOS PARA PODER ACCEDER NUEVAMENTE.

En esta imagen, podemos apreciar un lector de palma de mano **HandPunch 4000**, uno de los más completos (y costosos) del mercado.

Tomando como base el sistema operativo Windows, veamos cómo realizar este procedimiento.

Primero, debemos ingresar al editor del registro, para lo cual presionamos la combinación de teclas **WINDOWS+R**, y escribimos **regedit**, seguido de un clic en el botón **Aceptar**. Tras confirmar el alerta del UAC de Windows, se abrirá el editor.

Ya dentro del editor del registro, nos desplazamos hasta la posición **HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/UsbStor**, en el árbol de claves del panel derecho.

Luego hacemos doble clic en el panel derecho sobre la clave **Inicio**; en el cuadro emergente, verificamos que esté seleccionada la base hexadecimal y cambiamos la información del valor (casi siempre estará configurada en 3) por el valor 4.

Finalmente, aceptamos los cambios, cerramos el editor y reiniciamos el equipo. Si no hubo inconvenientes, al volver a iniciar, veremos que no nos será factible conectar ningún dispositivo a los puertos USB.

Vale aclarar que, una vez realizado el cambio y reiniciado el equipo, tampoco podremos conectar un teclado o un mouse a los puertos USB, por lo que, si se trata de una portátil, no habría mayores inconveniente; pero de tratarse de un equipo de escritorio, solo podremos controlarlo en forma remota, por eso, antes de inhabilitar los puertos, debemos asegurarnos de que el manejo remoto está activado y bien configurado.

Otras opciones

En el caso de versiones server de Windows, podemos modificar el bloqueo de cualquier unidad, incluidas las ópticas (CD-ROM, DVD, Blu-ray), desde las políticas de grupo, utilizando los filtros y las configuraciones correspondientes. También del lado del software podemos limitar, bloquear o permitir el flujo de información en ambos sentidos, mediante aplicaciones específicas. La primera que evaluaremos es el ya conocido firewall.

Este tipo de aplicaciones trabaja directamente sobre la capa 7 del modelo OSI (para más detalles ver recuadro **El modelo OSI**). En esta capa, podemos encontrar los protocolos DHCP (protocolo de configuración dinámica de host), DNS (sistema de nombres de dominio), SNMTP y POP3 (protocolos de envío y recepción de correo electrónico, respectivamente), FTP (protocolo de transferencia de archivos), HTTP y TELNET. A nivel profesional, un firewall nos permitirá restringir el paso de información en uno u otro sentido, dependiendo de las reglas que tenga configuradas. Por ejemplo, podemos definir que un dominio, rango de IPs o usuarios puntuales puedan enviar correo electrónico, pero otros no. Dependiendo del sector de la red que intentemos proteger, puede funcionar en solitario o en compañía de un servidor proxy.

Los servidores proxy, a diferencia de los firewalls que funcionan como filtros directos, actúan como completos intermediarios entre las conexiones de dos equipos de una red; por lo tanto, ninguno de los dos extremos de la conexión sabe con exactitud qué equipo generó la petición o la respuesta, ya que su cara visible es el servidor proxy.

Entre las desventajas de un servidor proxy, podemos encontrar el anonimato, ya que ninguno de los extremos conoce la identidad del otro; el abuso, ya que debe recibir y procesar peticiones de y hacia muchos usuarios, por lo que deberá comprobar quiénes tienen derechos de conexión y quiénes no, tarea para nada sencilla; irregularidad, dado que en algunos casos, cuando es imprescindible la conexión uno a uno entre emisor y receptor (como por ejemplo en TC/IP), puede resultar problemático ya que el proxy media entre varios usuarios.

Por lo anteriormente expuesto, debemos hacer un balance entre los problemas que podemos enfrentar al utilizar un servidor proxy y los beneficios que podríamos obtener de él. ■

Todas las computadoras portátiles incluyen el conector Kensington que vemos al lado del conector de auriculares.

En la actualidad, las portátiles pueden incluir lector de huellas dactilares; si no, podemos agregarlo por poco dinero.

Sistemas biométricos

Los sistemas de seguridad biométricos no son, hoy en día, ninguna novedad. En diferentes tipos de compañías, podremos encontrar desde lectores de huellas dactilares, de palma de mano, reconocimiento facial, reconocimiento de retina, de voz y sistemas mixtos que combinen dos o más de los anteriores. Incluso, desde hace unos años, algunas notebooks incorporan un lector de huellas dactilares en su configuración de fábrica. Solo debemos definir qué tanto necesitamos asegurar la información y cuánto dinero estamos dispuestos a invertir.

Software útil aplicado a la seguridad de la red

Existen muchas soluciones de software que nos ayudarán a proteger nuestra red; en estas páginas analizaremos algunas de ellas.

A esta altura, ya todos conocemos las buenas costumbres en lo que se refiere al uso de contraseñas. Se recomiendan que tengan al menos ocho caracteres, con letras, números, caracteres especiales, y no utilizar la misma para distintos sitios. El problema es que nuestra vida online es tan amplia que nos sería imposible memorizarlas a todas si respetamos estos criterios. La solución es un gestor de contraseñas, conozcamos algunas opciones.

El inventario generado por **KeePass** incluye diversos dispositivos de hardware, como los servidores de red.

Contraseñas

Existen muchas aplicaciones que pueden ayudarnos con las contraseñas, entre ellas se destaca **KeePass** (**http://keepass.info**) por sus múltiples ventajas:

- **Libre y gratuito:** open source (Certificado OSI) y en español. Solo será necesario que descarguemos el paquete de idioma adicional.
- **Generador de contraseñas:** con solo un clic, ya tenemos la contraseña que cumpla con las reglas propuestas, o generadas según un patrón pre-establecido, o, si queremos algo aún más robusto, generado según alguno de los tantos plugins disponibles.
- **Multiplataforma:** Windows, Mac, Linux y los SO de celulares (**Android**, **iPhone**, **BlackBerry**, hasta **J2ME** y **Palm OS**). Y sumando movilidad, por supuesto cuenta con una versión portable. No importa dónde nos encontremos, siempre contaremos con nuestras contraseñas a la mano.
- **Base de datos:** su base de datos se puede sincronizar con los múltiples servicios de file server en la nube (Google Drive, SkyDrive, Dropbox, Box, etc.); y si hacemos algún cambio sobre una

Fing

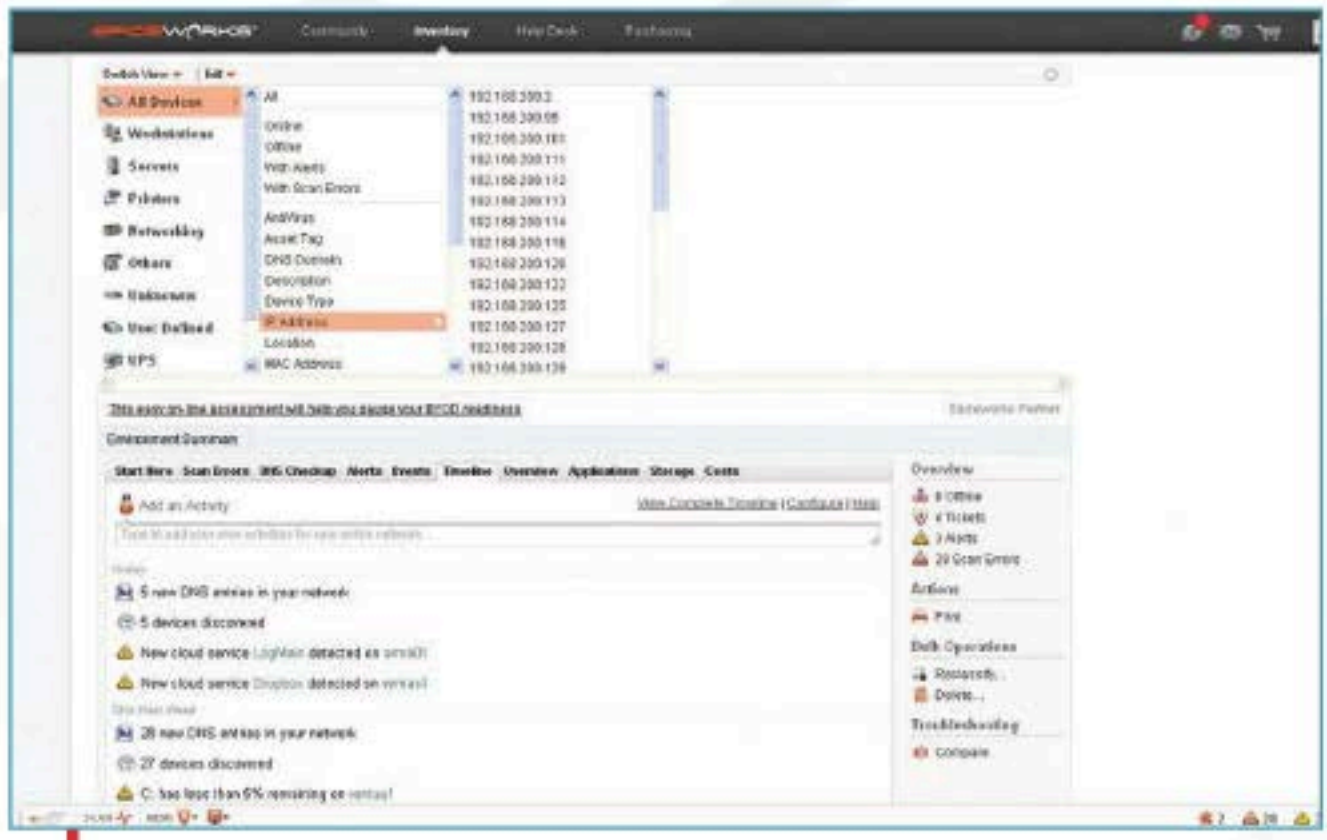
Nuestro smartphone puede ser una herramienta muy poderosa a la hora de detectar problemas en la red. **Fing** es una aplicación para iPhone, iPad y Android que escanea la red mostrándonos un listado de los dispositivos conectados, **dirección IP**, **MAC Address**, **información de NetBios** (nombre, dominio, rol), **trace router.** Con un segundo escaneo, podemos ver los servicios y puertos abiertos en cada PC. También contamos con versiones para Windows, Mac OSX y GNU/Linux. Fing es una aplicación gratuita.

contraseña, por ejemplo en nuestra PC, veremos la información actualizada en nuestro teléfono celular. Dicha base de datos cuenta con un método de criptografía simétrica llamado **Twofish**, con cifrado por bloques con un tamaño de bloque de 128 bits; el tamaño de clave puede llegar hasta 256 bits.

Una alternativa interesante es **LastPass**. Posee varias ventajas y desventajas en comparación con KeePass; su uso dependerá de las necesidades particulares de los usuarios.
También es OpenSource y multiplataforma, pero la versión gratuita tiene limitaciones; si queremos tener todas las funciones, tendremos que comprar una licencia anual. Casi no requiere configuración, solo la carga inicial de los datos de usuario y contraseña. Es importante señalar que **Store Secure Notes** es una función extra que permite almacenar otros tipos de datos de forma segura. No solo nombres de usuario y contraseñas, cualquier dato de texto confidencial puede ser encriptado. Por otra parte, su uso es bastante intuitivo, pero, para un usuario neófito, es recomendable la versión Premium ya que no requiere de ningún plugin adicional. Su sitio web oficial es **https://lastpass.com**.

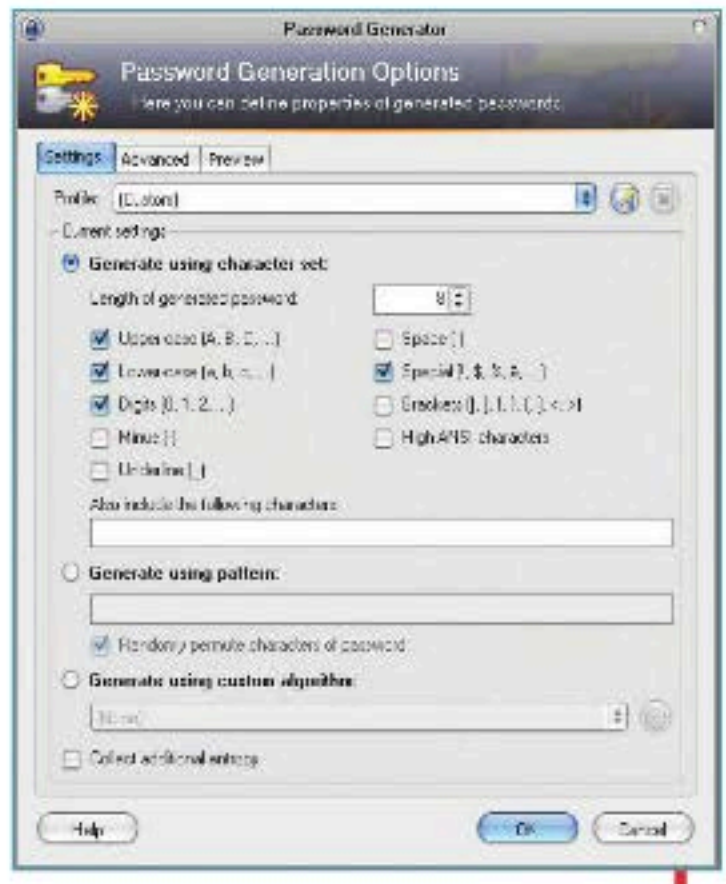
Monitores de actividad

Spiceworks (www.spiceworks.com/free-pc-network-inventory-software) tiene una doble funcionalidad. Primero, nos ayudará a hacer un inventario del numeroso equipamiento, y luego podemos configurar alertas de monitorizaciones.
Como escáner de inventario, descubriremos que podemos encontrar en nuestra red numerosos dispositivos: computadoras, servidores, impresoras, NAS, cámaras IP, DVRs, teléfonos IP, relojes, switches administrables, router, fotocopiadora, UPS, etc., son solo algunos de los dispositivos que es posible descubrir en una LAN corporativa.
Una vez realizado el inventario, contaremos con un listado muy completo separado por familias (todos los equipos, computadoras, servidores, impresoras, networking, otros, desconocidos, terminales de usuarios, UPS y controladores de dominio), al que podremos acceder vía web desde cualquier terminal y con el cual podremos interactuar según nuestra necesidad. Por ejemplo, las direcciones IP fijas, seguramente las tenemos anotadas en un archivo de texto.
Cuando elegimos un dispositivo, el software reconoce si se trata de una terminal, un servidor, un dispositivo, o un terminal de usuario (celular). Este último dato puede ser muy útil en empresas donde se cuida la seguridad de los terminales conectados a la red y que no están autorizados.
El software no es ciento por ciento preciso, hay equipos que serán reconocidos, pero permite editar el inventario para una mejor comprensión posterior.
El inventario es muy útil, pero no lo consultaremos con frecuencia; por otra parte, si consultamos el dashboard del programa en forma periódica, encontraremos mucha información que nos será útil para el mantenimiento preventivo.
Entre otros datos, veremos información sobre los buzones de Exchange, con un ranking de cuáles son los más llenos y, así, poder advertir a los usuarios que limpien su bandeja. A continuación, listamos algunas de las opciones adicionales que nos ofrece:

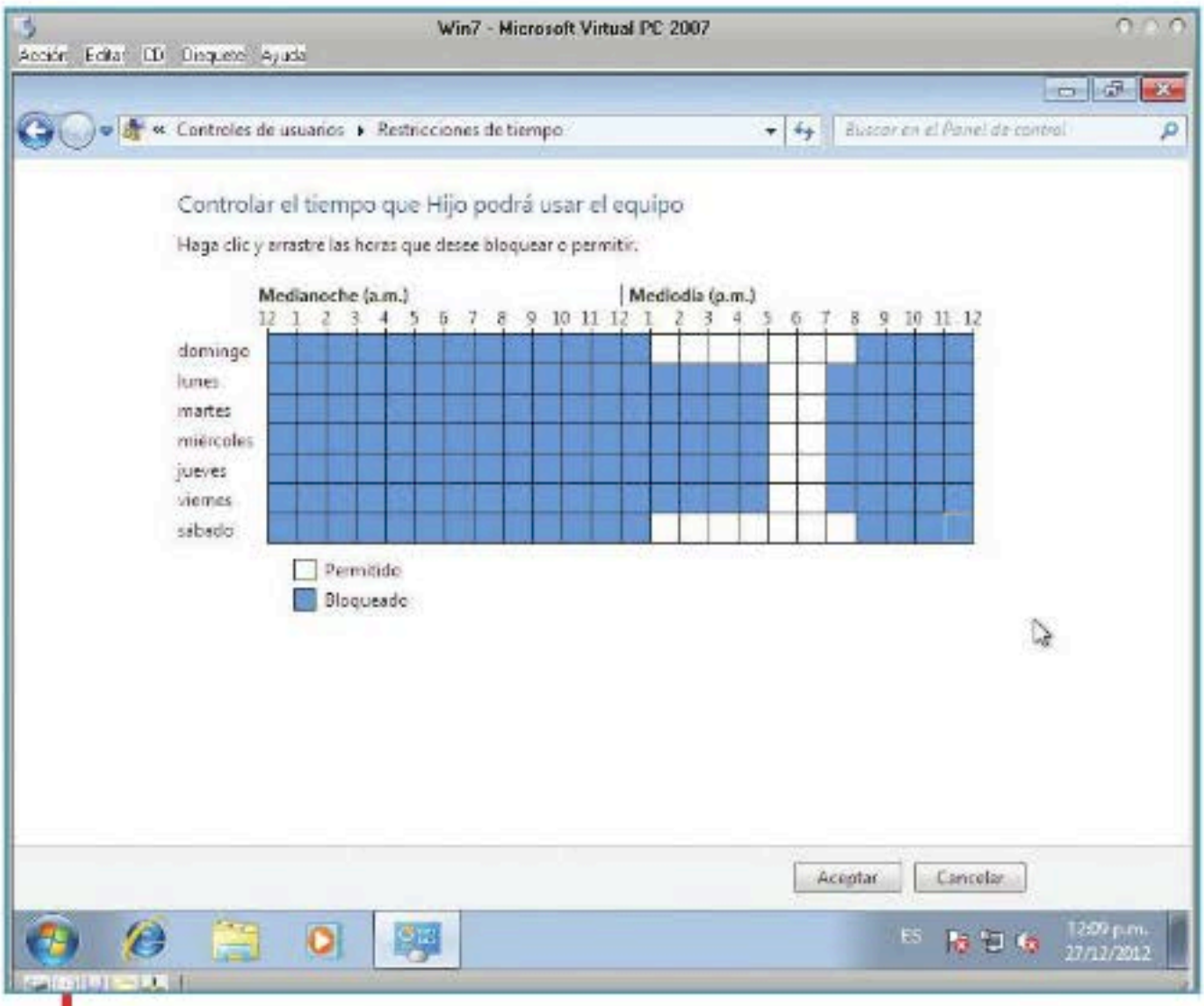


El inventario generado por **Spiceworks** se puede ordenar y filtrar según nuestra conveniencia para acceder a los datos en forma rápida.

- Un entorno gráfico con los últimos eventos (errores o alertas del servidor).
- Estadísticas de seguridad en las que veremos qué máquinas funcionan con la aplicación antivirus sin actualizar.



Es posible generar claves según los parámetros que configuramos en forma previa.



Windows Live Protección infantil, incluido dentro del paquete **Windows Live Essentials**, protege la conexión de Internet para los menores.

- Un detalle del software sin actualizar en determinadas PCs.
- La configuración de las alertas es bastante flexible.
- El software es gratuito y se apoya mucho en una comunidad activa.
- El registro inicial puede ser algo molesto si solo queremos probarlo, pero sin dudas es un software que ayudará mucho a los profesionales IT de cualquier empresa.

Pandora FMS (**http://pandorafms.com**) es un proyecto Open Source de monitorización de propósito general que recoge datos de cualquier sistema. Se encarga de generar alarmas, mostrar gráficos, informes, mapas y cuadros de mando en un entorno web sencillo.
Es capaz de monitorizar cualquier sistema operativo: Windows, FreeBSD, OpenBSD, NetBSD, MacOs. Hasta escenarios de virtualización en Vmware. Algunas de las aplicaciones que pueden ser supervisadas son las siguientes: **SAP**, **Tomcat**, **Weblogic**, **IIS**, **JBoss**, **Exchange**, **WebSphere**, **Oracle** y **ERP**.
Otra de las opciones de monitorización es **Nagios** (**www.nagios.org**), un sistema de monitorización Open Source que vigila el hardware y los servicios de red (SMTP, POP3, HTTP y SNMP, entre otros).
Lo más interesante de este tipo de programas es la posibilidad de alertarnos por correo electrónico o mensajes SMS cuando los márgenes que definimos han sido alcanzados.

Control parental

El cuidado de nuestros hijos enfrente de la computadora es tan personal que sería imposible encontrar una única solución. Las dos mayores necesidades que se les plantean a los padres por primera vez son: restringir horarios, para que por ejemplo, no lleguen de la escuela y lo primero que hagan sea encender la computadora. Y la otra preocupación es la de ayudarlos a mantenerlos seguros cuando están en Internet. Por supuesto, la mejor solución es la educación, pero, aunque los acompañemos cuando están usando la PC, hay momentos del día en que pueden estar solos y hacer uso libre de ella. Con un software **Parental Control**, podemos ayudarlos a estar más seguros mientras están conectados, sin necesidad de vigilarlos constantemente.
Enfoquémonos en los más pequeños. La herramienta que todos tenemos a mano es el **Control Parental** incluido en los sistemas **Windows**. Ella nos permitirá limitar el tiempo que los chicos pasan frente al monitor, controlar los programas que pueden utilizar, los juegos que pueden usar, y el tiempo que podrán utilizar la computadora.
Para activar el Control Parental de Windows, debemos hacer clic en **Inicio/Panel de control/Cuentas de usuario y protección infantil/Control parental**. Lo primero será crear un usuario a nuestro hijo en la PC por monitorear, y, como es de suponer, usuarios para los padres. Si nuestro hijo aún no cuenta con su propio usuario, el mismo programa nos invitará a crearlo.
Una vez activado el **Control Parental**, las configuraciones que nos ofrece son las siguientes:

- **Límite de tiempo:** aquí podremos configurar en qué franja horaria y qué días de la semana podrán hacer uso de la PC. No queremos que, si el chico se despierta a medianoche, pueda encender la computadora
- **Juegos:** el acceso a los juegos se puede manejar gracias a diversas clasificaciones. Por ejemplo, a un niño de tres años, le permitiremos jugar con los clasificados como **Edad Temprana**.
- **Permitir o bloquear programas específicos:** quizás en un ambiente hogareño no requiere configuración, pero aquellos que trabajan desde su casa, podrán proteger su fuente de trabajo, evitando accidentes indeseables como la eliminación de información.

Cuando nos preocupa la experiencia que nuestros hijos tendrán en Internet, pensamos en limitar las búsquedas, bloquear o permitir determinados sitios web, y saber con quién podrá comunicarse por chat. Para ayudamos en esta tarea, tenemos a **Windows Live Protección infantil**.

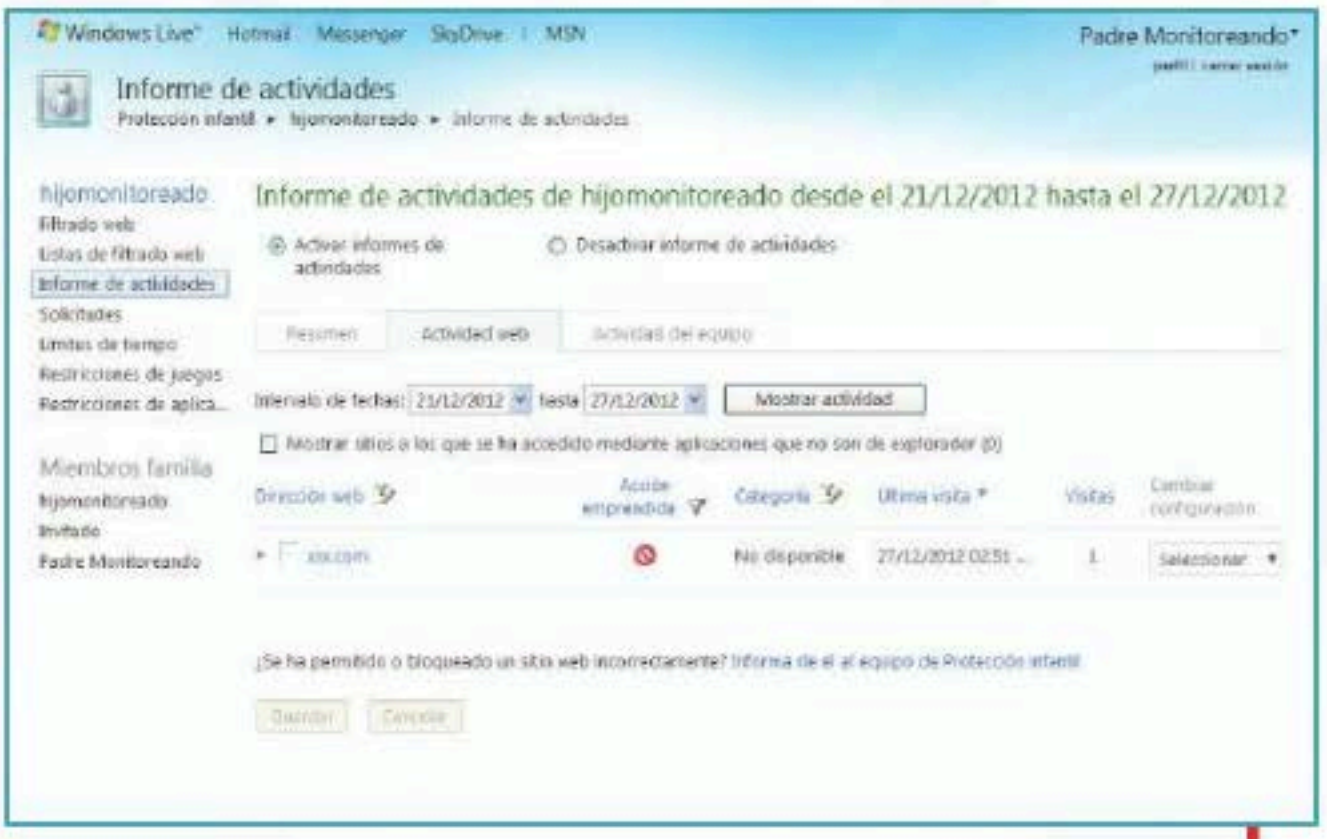
Con este programa gratuito, incluido en **Windows Live Essentials**, no solo podremos administrar estos requerimientos, también contaremos con informes útiles y fáciles de leer acerca de sus actividades en Internet. Lo encontramos en Inicio/Panel de control/ Tareas iniciales.

Una vez instalado el software, y los usuarios padre e hijo están asociados, el control se realiza desde el sitio **http://familysafety.live.com**.

Las opciones que nos ofrece son las siguientes:

- **Web Filtering:** filtrar la navegación web en todos los navegadores, no solo en IE. Podemos permitir solo los sitios en los que confiamos, permitir sitios que el filtro determina como amigables para los niños, sitios de interés general, y se bloquearán las redes sociales, web mail, web chat, y los sitios para adultos, o permitir todo, excepto los sitios para adultos.
- **Reporte de actividad:** podremos obtener una lista de los sitios web visitados por el niño. A los padres más "restrictivos", les podría llegar a interesar esta función, pero la verdad es que el listado se tornaria interminable en solo un par de dias.
- **Gestión de Contactos:** seremos capaces de evitar el contacto con desconocidos. Solo podrá chatear con los contactos autorizados.

Una alternativa a este software, es el **K9 Web Protection**, con similares prestaciones. Su mayor ventaja es que este software gratuito es multiplataforma. Podemos instalarlo en Windows, Mac OSX y en nuestros terminales iPhone, iPad, Android, y así protegeremos todo acceso a la web.



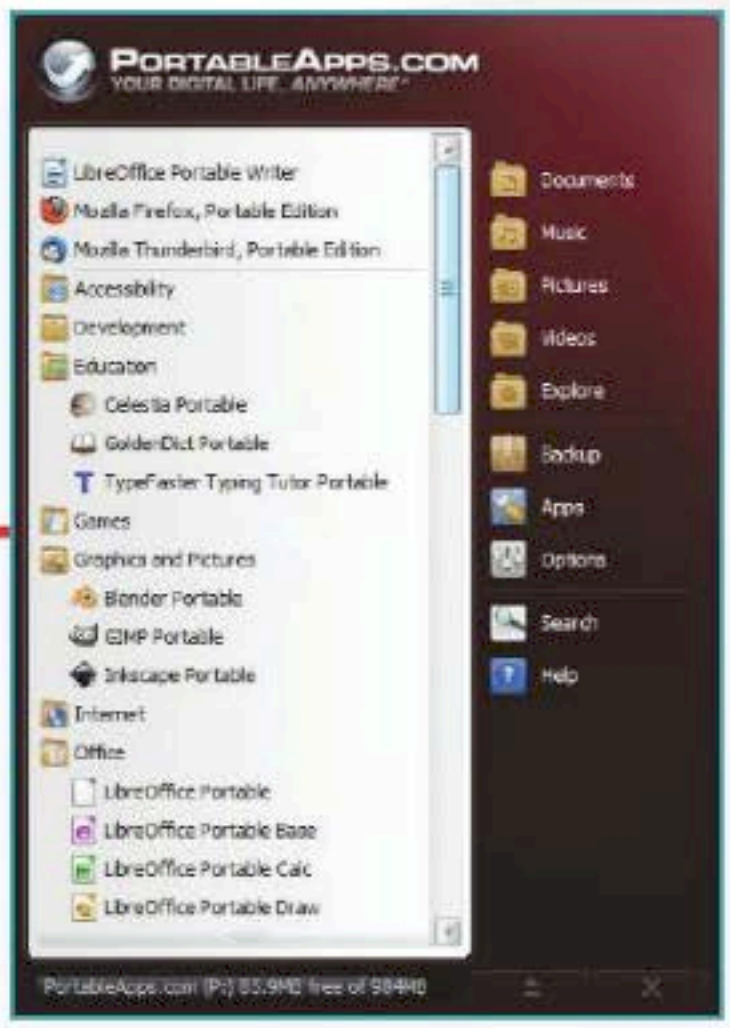
Un informe online estará disponible para que los padres puedan consultar la actividad de sus hijos.

Otras recomendaciones

Tener una carpeta en el servidor con aplicaciones portables siempre nos sacará de un apuro. Seguramente, cada uno de nosotros tendremos nuestras propias preferencias sobre qué herramientas usamos a diario, pero las versiones portables recomendadas son las siguientes:

- **ClamWin Portable:** uno de los antivirus portables más confiable.
- **Spybot - Search & Destroy:** aplicación para eliminar spyware.
- **7-Zip:** para comprimir y descomprimir cualquier archivo, soporta las extensiones de archivos comprimidos más populares.
- **XnView:** podremos ver casi cualquier imagen sin importar su extensión.
- **FileZilla:** cliente FTP que rara vez está instalada en una terminal de un usuario común.
- **Skype:** uno de los clientes de chat más populares.
- **OpenOffice:** suite ofimática compatible con los archivos generados por Word, Excel y PowerPoint.
- **Mozilla Thunderbird:** cliente de e-mail compatible con Exchange.
- **WinDirStat:** se encarga de analizar el disco duro en busca de archivos que ocupan mucho espacio.

Según el ámbito donde nos desempeñemos, encontraremos aplicaciones más específicas que nos serán útiles; cada una de ellas está disponible en la dirección **http://portableapps.com**.■



En PortableApps, encontraremos una gran variedad de aplicaciones portables, todas ellas gratuitas y libres.

Port scanning

El port scanning nos permite conocer el estado de todos nuestros puertos de comunicaciones y tomar medidas preventivas para el control de accesos.

Cuando hablamos de **port scanning**, nos estamos refiriendo a las técnicas que explorarán los puertos de comunicación de nuestra PC o servidor que se encuentra conectada a una red. Este conjunto de técnicas las emplearemos para conocer qué puertos están abiertos, cerrados o protegidos y qué tipo de servicio está brindando una PC o servidor.

El rastreo se realiza sobre los protocolos **TCP**, **UDP**, **HRSP**, entre otros. Los más utilizados son el TCP y UDP. Deberemos comprender que nuestra PC o servidor posee un total de 65536 puertos para realizar el intercambio de información con otros equipos dentro de una red. Estos puertos van del 0 al 65535.

Estándar

Existe un estándar establecido por la Agencia de Asignación de Número de Internet (IANA), que indica que los puertos del 0 al 1023 son reservados; en este rango entran las aplicaciones que utilizan: **HTTP**, **FTP**, **IRC**, **POP3**, **FTP** y **SMTP**, entre otros.

El rango que va del 1024 al 49151 se denomina **registrado** y es usado por cualquier tipo de aplicación. Y el último rango del 49152 al 65535 es dinámico y, por lo general, lo utiliza el sistema operativo para una aplicación que necesita conectarse a un servidor.

El escaneo de puertos nos ayudará a detectar vulnerabilidades en nuestro equipo y a analizar los posibles problemas que esto ocasionaría en el sistema.

Vulnerabilidades

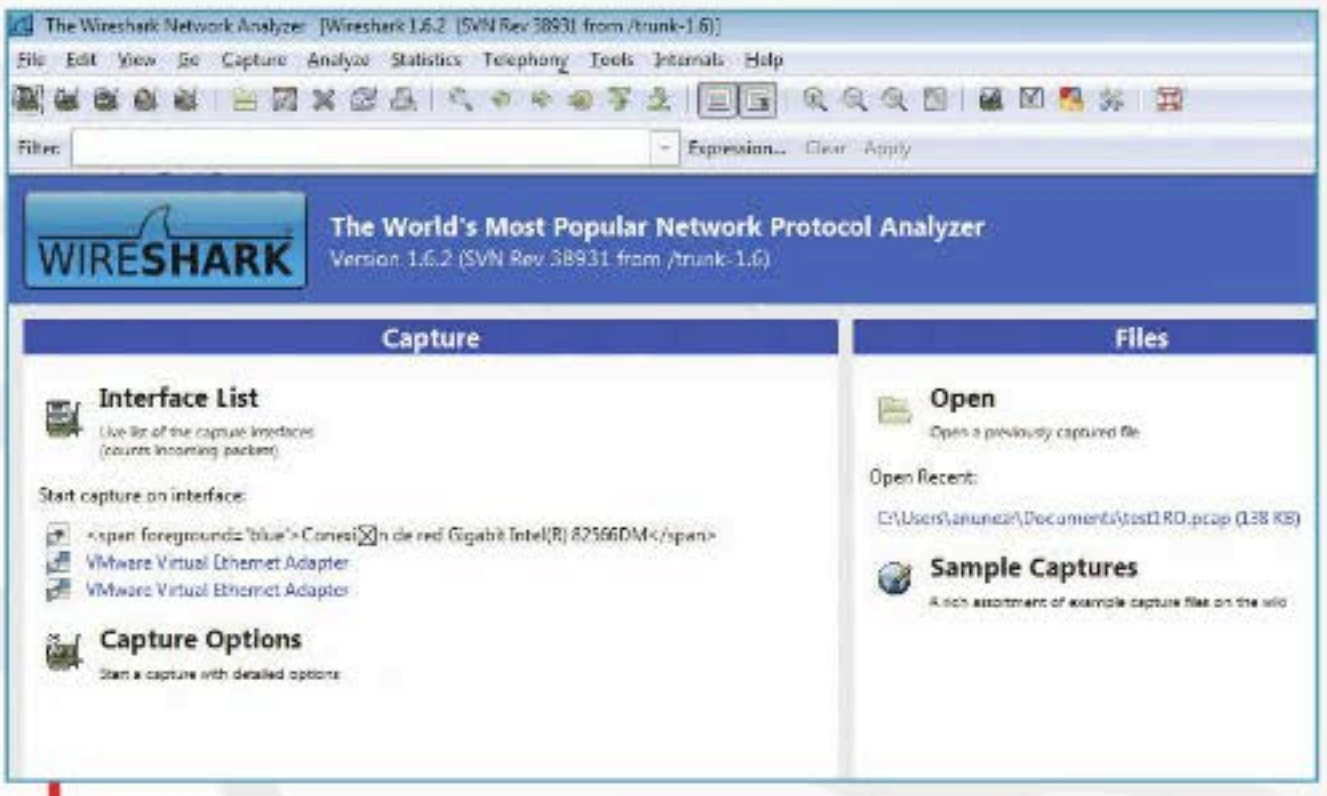
Detectaremos vulnerabilidad en nuestro sistema dependiendo de los puertos que estén abiertos, ya que cada uno de ellos es utilizado por distintos programas y servicios de la PC. Los problemas pueden aparecer debido a que el escaneo puede ser realizado por personas malintencionadas, quienes, una vez dentro de la red, la explorarán en forma completa, tratando de encontrar equipos con puertos abiertos e intentando obtener privilegios administrativos sobre el sistema, para ocasionar problemas o tener acceso a información confidencial.

Además de encontrar puertos abiertos, pueden utilizar programas infectados con código malicioso conocidos como **exploits**, los cuales aprovecharán o explotarán dichos puertos abiertos para tener control sobre el sistema, causar daño en él o corromper la información.

Aplicaciones

En los sistemas operativos, vamos a contar con programas (firewalls) que se encargan de monitorear las conexiones tanto entrantes como salientes. Su función es controlar que todo el tráfico de cada uno de los puertos no sea realizado por algún programa en forma inadecuada, y proteger nuestro sistema.

Para que podamos realizar el escaneo de puertos, los sistemas Windows cuentan con un comando que permite ver el estado de los puertos, denominado **NETSTAT**, que carece de interfaz gráfica. Pero también podremos realizar el escaneo por medio de programas que se dedican a este fin, entre los que recomendamos y destacamos **Nmap**, **SuperScan**, **Wireshark** y **Cports**.



Con **Wireshark**, vamos a poder realizar capturas del tráfico de la red en forma pasiva, lo que nos permitirá detectar vulnerabilidades en nuestra red.

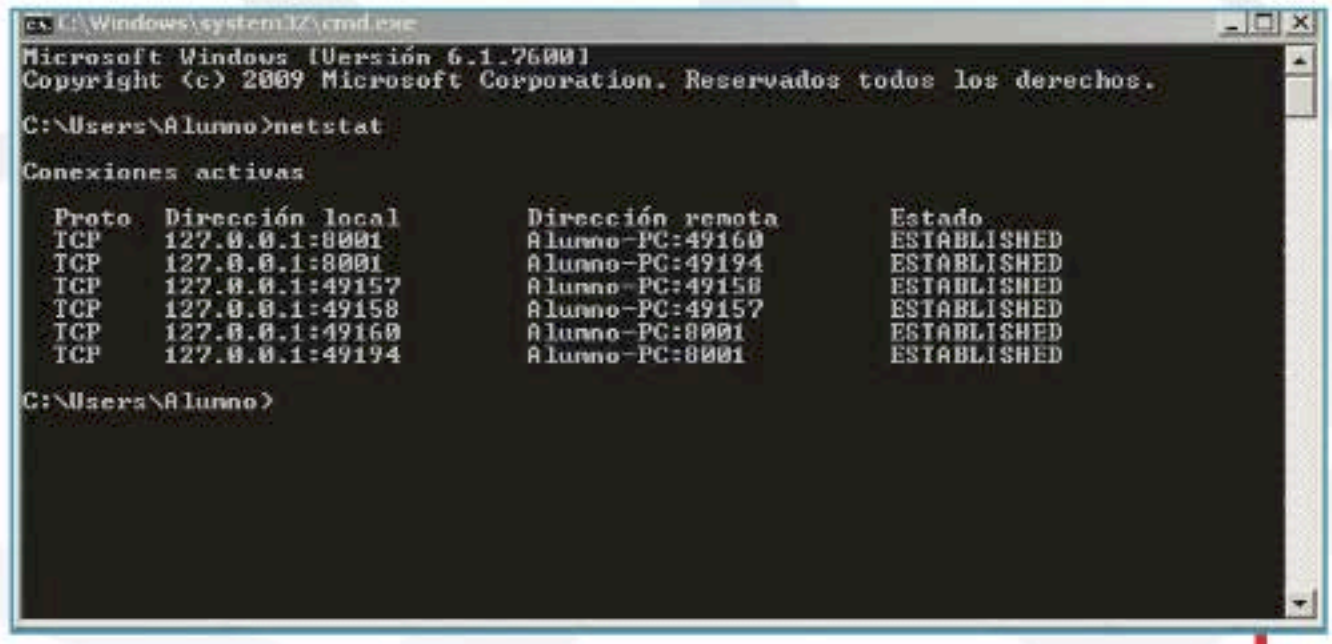
- **Nmap**: este software de exploración de puertos nos permite analizar de distintas formas nuestro equipo; es una herramienta muy completa ya que, por

medio de la barra de comandos, podremos configurar según nuestras necesidades los argumentos del comando nmap.
Debemos tener en cuenta que necesitaremos conocer de antemano los argumentos para tener distintos resultados en pantalla, por ejemplo, si queremos ver el sistema operativo instalado el equipo, tendremos que incluir el argumento –O; si queremos realizar el escaneo sobre IPv6, tendremos que agregar el argumento -6 y, si quisiéramos especificar solo un puerto o varios, lo que tendremos que agregar es el argumento –p <RANGO>.
Un ejemplo de un comando para Nmap sería el que vemos a continuación:

```
Nmap –O XXX.XXX.XXX.XXX
Nmap –p 1-1024 –O XXX.XXX.XXX.XXX
```

También disponemos dentro del Nmap de una solapa llamada Ports/hosts, en la que encontraremos los puertos abiertos del equipo analizado, el tipo de protocolo que utilizan, el servicio al que pertenecen y una descripción de estos.
En caso de colocar un rango de IP para escanear, dispondremos de una solapa, llamada Topology, donde se armará la topología de red en la que se encuentra conectado nuestro equipo.

- **SuperScan:** es un simple y eficiente software para explorar nuestra red en busca de puertos abiertos. Para que podamos utilizar este software, solo tendremos que colocar una IP de comienzo y una IP de fin del rango que queramos explorar y, una vez colocados los datos, tendremos que iniciar la exploración; dependiendo de la cantidad de equipos que hayamos definido en el rango, nos indicará por pantalla las IP de los equipos, los tipo de protocolos analizados, los números de puertos abiertos y la cantidad total de equipos descubiertos.
Tenemos la posibilidad de visualizar los resultados en formato HTML. Este tipo de vista nos indicará más datos, como el nombre del equipo en la red, el dominio, si es que pertenece a alguno, y una descripción más profunda del puerto y protocolo analizado, por ejemplo: 123 – Network Time Protocol; 137 – NetbiosNameService.



Gracias al comando NETSTAT, vamos a poder conocer en qué estado se encuentran nuestros puertos; aunque carece de interfaz gráfica, es efectivo.

También, podremos aplicar distintas opciones, como decidir qué tipo de protocolo queremos escanear TCP, UDP o ambos, los tiempos de respuestas, la velocidad del escaneo y, además, contamos con herramientas de red como el Ping, para testear la conectividad de los equipos, y traceroute para conocer cuántos saltos hay hasta el equipo y búsqueda por nombre o IP. Actualmente se encuentra disponible la versión 4.

SUPERSCAN ES UN SIMPLE Y EFICIENTE SOFTWARE PARA EXPLORAR NUESTRA RED EN BUSCA DE PUERTOS ABIERTOS

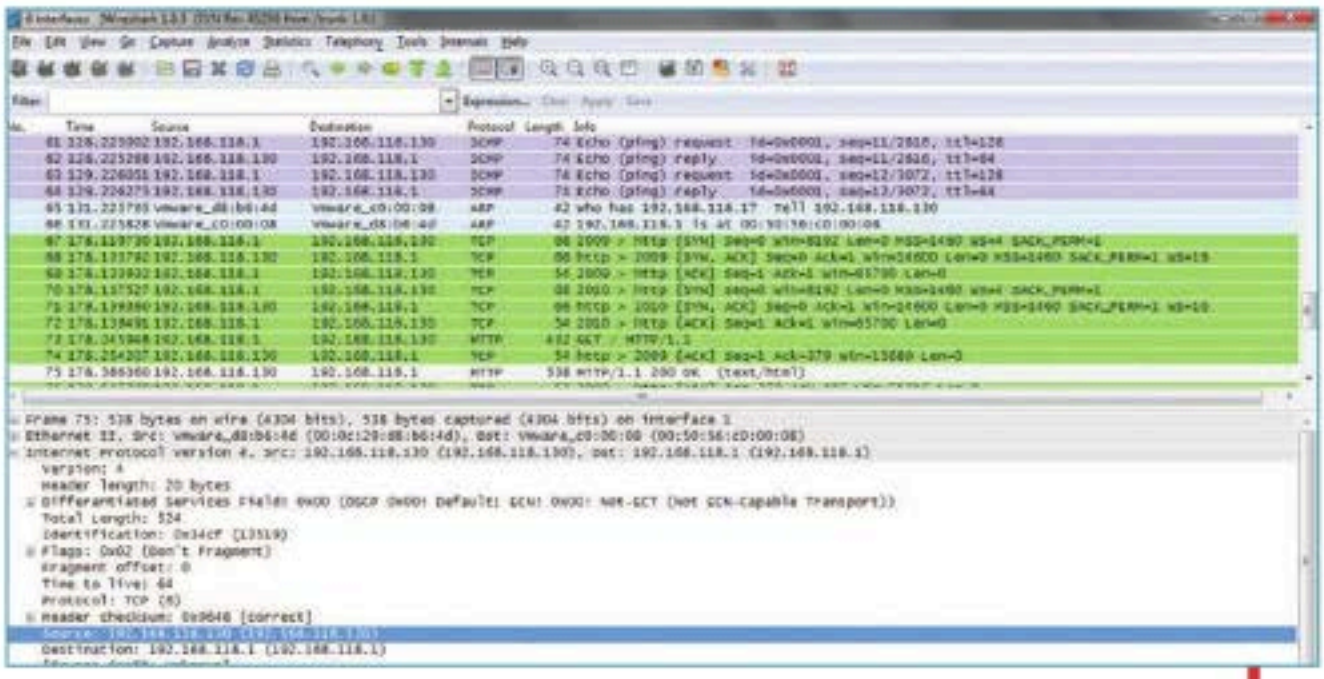
- **Wireshark:** recomendable software para que realicemos escaneo de puertos. Este software trabaja en modo pasivo, es decir, que no generará tráfico en nuestra red.
La forma de trabajo es simple: en la PC que se ejecute, entra en un estado pasivo, y lo que realiza es escuchar todo el tráfico que viaja por nuestra red. Para empezar a usarlo, lo que tendremos que hacer, luego de instalarlo, es seleccionar nuestra placa de red y, si queremos, configurar algunas opciones de captura, filtros, captura de múltiples placas de red.

Cuando realicemos el escaneo, veremos cómo las capturas aparecerán en pantalla y variarán de color según el protocolo capturado. Se pueden aplicar filtros para ver solo ciertos puertos, ciertos protocolos e incluso es posible aplicar filtros por IP, en el caso de que queramos capturar el tráfico de alguna/s PCs. Wireshark nos permite guardar las capturas que realicemos; esto nos brinda la posibilidad de estudiarlas con más tiempo y con un análisis exhaustivo en otro momento.

- **Cports:** aplicación que nos muestra en forma gráfica y constante todo el flujo de tráfico que pasa por los puertos y los protocolos del sistema; realiza un monitoreo en tiempo real de la PC en forma local; en la pantalla vamos a poder apreciar el nombre del proceso, el usuario que lo creó y el tiempo de creación.
También nos permite cerrar las conexiones no deseadas y no creadas por nosotros, permitiéndonos guardar la información de los puertos en un archivo HTML, XML, o delimitado por tabuladores. Si Cports interpreta que algunas conexiones son creadas por aplicaciones en forma sospechosa, las marcará con color rosa.
Es una herramienta freeware y pesa solamente 46 KB.

Consideraciones

Debemos tener en cuenta que podemos realizar el escaneo de los puertos dentro de nuestra red, con las aplicaciones



Por medio de las distintas marcas en que **Wireshark** visualiza los puertos, podemos identificar si la actividad de estos no es la normal.

mencionadas, pero existen páginas web que nos permiten realizar dicha tarea. Es decir, que realizaremos el escaneo desde afuera de nuestra red. Este tipo de escaneo se realiza sobre la IP pública de nuestra PC. Esta IP es la que nos brinda nuestro proveedor de Internet cuando nos conectamos a Internet; estas páginas nos servirán para corroborar si nuestros puertos en Internet se encuentran protegidos o no.

Algunos de los sitios que brindan este tipo de servicio desde Internet son los siguientes: **Puertos abiertos**, **Adsl ayuda** y **Nmap online**. A continuación revisaremos sus características.

Puertos abiertos

El sitio **www.puertosabiertos.com** se dedica al port scanning, donde una vez que ingresemos nos encontraremos con una página que indica nuestra IP Pública y la IP de nuestra LAN interna, además de algunos datos de nuestros proveedor de Internet, como son el nombre, el proxy y la localización de nuestro equipo.

También tendremos información sobre el navegador con el cual estamos navegando, la versión, el idioma, el sistema operativo, y una variedad de componentes web que indicarán su estado (On u Off).

La página cuenta con un menú en la parte izquierda donde podremos encontrar varias opciones desde Escanear puertos on-line, Conoce tu IP, Información de puertos, Listado de puertos, Geolocalizador IP, Archivos peligrosos e-mail, nosotros accederemos a Escanear puertos on-line. Aquí podremos seleccionar un conjunto de puertos por escanear o algún puerto específico que nosotros indiquemos.

El grupo de puertos se divide en susceptibles, servidores y troyanos desde el I hasta el VII. Una vez que seleccionamos el o los puertos, presionamos el Escanear, la página procesará los puertos; una vez terminado, nos mostrará por pantalla el resultado, indicando el estado del puerto más una explicación detallada de cada uno.

Adsl Ayuda

El sitio **www.adslayuda.com** es sencilla, ya que no contiene imágenes ni un formato al que estamos acostumbrados a ver en la mayoría de las páginas web, es decir, un menú de navegación y fondo de color; simplemente es una página en blanco que nos provee un script para testear los puertos, tenemos un campo para que escribamos el número de puerto que queremos escanear, colocamos el número de puerto, hacemos clic en Comprobar y esperamos el resultado.

Debajo del campo que tenemos que llenar, aparece nuestra IP pública y la IP de la red Internet, la página la llamará VERDADERA IP.

Nmap online

El sitio **http:// http://nmap.online-domain-tools.com** está realizada igual que **Nmap**. En ella, podremos escanear la PC en forma rápida, en forma completa o anteponiendo en los campos correspondientes el número del puerto de inicio y el puerto de fin, de los cuales queremos explorar. También tendremos una opción personalizada para colocar el comando con los argumentos que nos sean necesarios. Cuando seleccionemos la forma en que queremos realizar el escaneo, hacemos clic en Scannow y, en unos minutos, tendremos el resultado en pantalla, aunque bien podríamos pedirle al escaneo que nos lo envíe por e-mail.

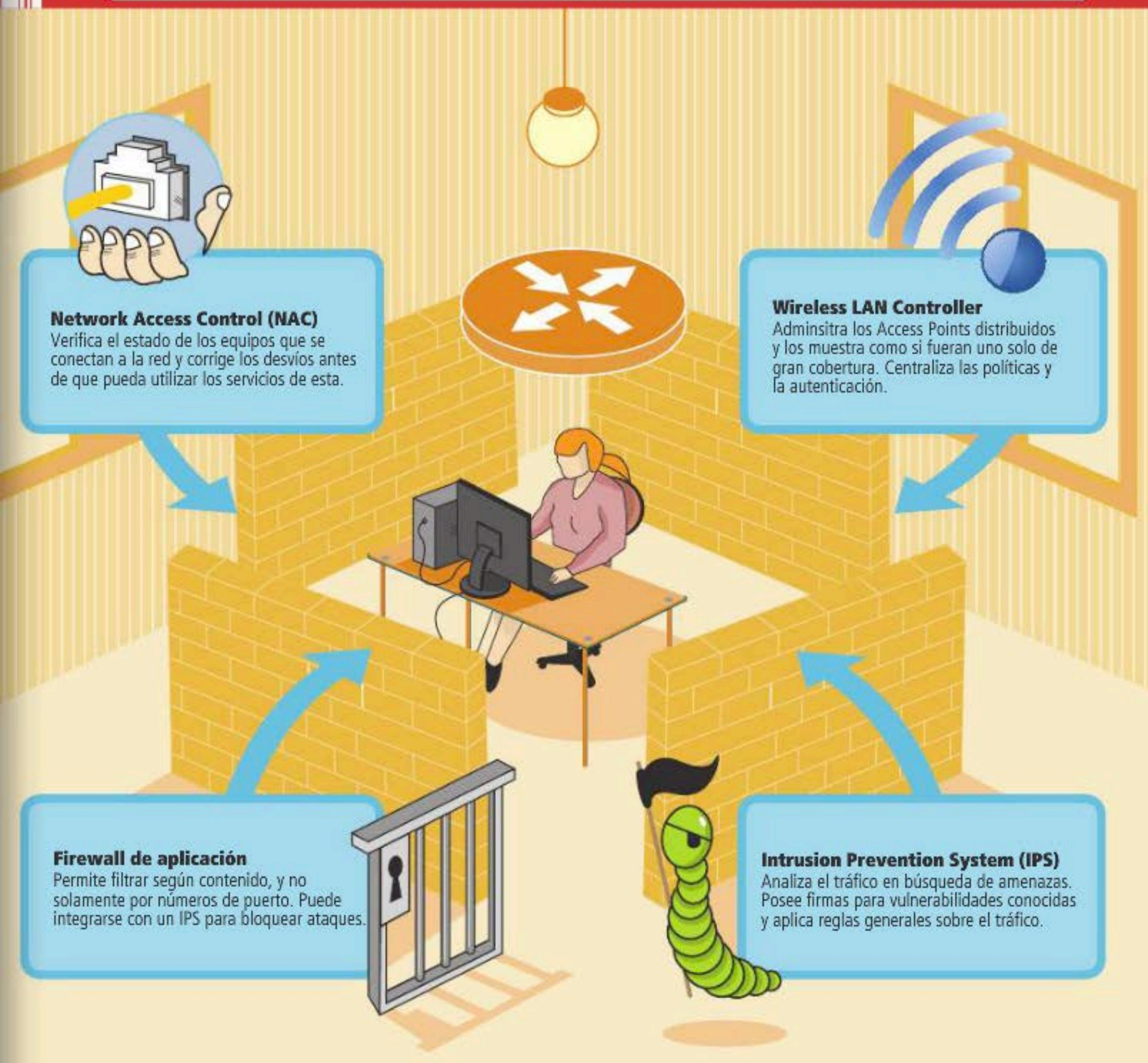
La página cuenta con la lista de todos los argumentos y su correspondiente explicación para que podamos colocar el argumento personalizado según nuestras necesidades; además, contamos con una explicación detallada de los tres tipos de escaneo que nos brinda el sitio. ■

NETSTAT

Es un comando de Windows, que funciona por medio de la consola de comandos (CMD). Lo que realiza netstat es mostrar de forma exacta los puertos que están abiertos y escuchando, o abiertos y transmitiendo información. Para utilizarlo, debemos abrir una ventana de CMD y ejecutar el comando NETSTAT.

Es una herramienta útil que, si bien no tiene interfaz gráfica como otros software, nos brinda información útil de nuestros puertos.

Soluciones de seguridad



Network Access Control (NAC)
Verifica el estado de los equipos que se conectan a la red y corrige los desvíos antes de que pueda utilizar los servicios de esta.

Wireless LAN Controller
Adminsitra los Access Points distribuidos y los muestra como si fueran uno solo de gran cobertura. Centraliza las políticas y la autenticación.

Firewall de aplicación
Permite filtrar según contenido, y no solamente por números de puerto. Puede integrarse con un IPS para bloquear ataques.

Intrusion Prevention System (IPS)
Analiza el tráfico en búsqueda de amenazas. Posee firmas para vulnerabilidades conocidas y aplica reglas generales sobre el tráfico.

Endpoint Protection (adicional a estos cuatro elementos básicos)
Debemos considerar un sistema Endpoint Protection que permita controlar los dispositivos que se conectan a las terminales. Los dispositivos removibles pueden introducir amenazas a la red, software no autorizado o pirateado, conexiones hacia redes externas no autorizadas (wireless, 3G, etc.) y también permiten a los usuarios llevarse información confidencial.

Sniffing y análisis de protocolos y de tráfico

Con el uso de herramientas MARS (Monitoring, Analysis and Response System), podremos analizar, detectar y prevenir problemas en nuestra red.

Un **sniffer** es un programa que monitorea toda la actividad de la red, capaz de escuchar todo el tráfico de nuestra LAN, y la captura de datos para su posterior análisis. Antiguamente, era una herramienta utilizada por hackers para obtener cualquier tipo de información confidencial, como los datos y las contraseñas de home banking, números de tarjetas de crédito, etc.

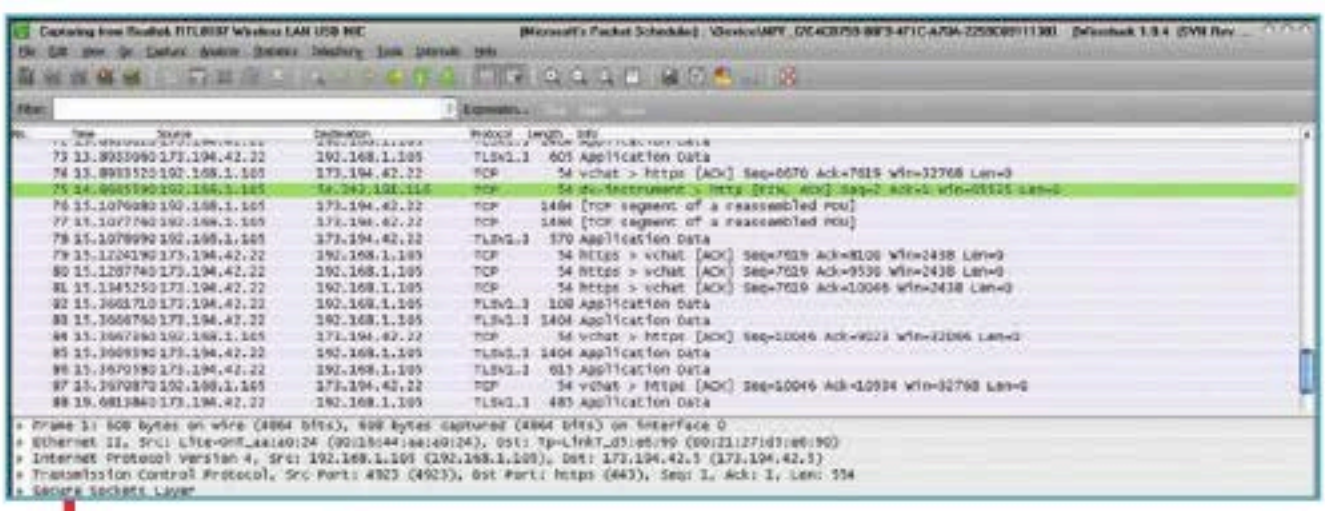
Switch con **portmirror**; la mejor manera de monitorear con WireShark.

Uso del sniffer

Hoy podremos utilizar un sniffer con otros propósitos. Alguna vez, nos habrá pasado que tenemos una pérdida del rendimiento sobre la red que gestionamos y necesitamos alguna herramienta que nos ayude a localizar el problema, a saber por qué tenemos microcortes, y sospechamos de un problema de broadcast. Lo que nos limita es la imposibilidad de trabajar en modo promiscuo, o sea, no poder escuchar el tráfico total de nuestra red.

Solo podremos monitorear un segmento de ella. Al monitorear un puerto del switch, solo veremos el tráfico por tránsito de este único puerto. Si monitoreamos el puerto del servidor, tendremos el mayor tráfico, pero no la totalidad.

Por ejemplo, si el problema se origina al momento de imprimir; el tráfico desde la PC al **print server** no pasa por el servidor y está fuera del umbral de audición del sistema de escucha.



Ejemplo de captura con WireShark. Luego de aplicar los filtros correspondientes, la información se reduce para su fácil lectura.

Entonces, antes de empezar con la captura, debemos analizar dónde y cómo instalar nuestra herramienta.

Hoy por hoy, contar con un hub es casi imposible, e instalarlo no es recomendable ya que podremos obtener mejores resultados con análisis sectorizados. Aunque sí, podríamos aprovechar un pequeño hub, si lo ubicamos en cascada sobre el puerto del switch por monitorear.

Alternativas

Una alternativa es el modo bridge, en el cual nuestra PC cuenta con dos placas de red, y podremos intercalarlo por ejemplo con el servidor.

La forma más cómoda de trabajar es sobre un switch administrable que cuente con la posibilidad de configurar un **portmirror** (también llamado **SPAN** en entornos **Cisco**). Como su nombre lo indica, se trata de un puerto en espejo, donde todo el tráfico se replicará en el otro.

Por último, **ARP Spoofing** es una técnica en extremo agresiva, basada en el envío de falsos mensajes de **ARP** (*Address Resolution Protocol*). Entonces, todo el tráfico dirigido a la dirección IP de ese

nodo será erróneamente enviado a nuestra PC y luego redirigido al destinatario real.

Wireshark

Wireshark (**www.wireshark.org**) es el analizador de protocolos Open Source y gratuito más conocido. Disponemos de versiones para Windows y Mac OSX.
Lo utilizaremos para realizar análisis y para capturar todos los paquetes sobre el segmento de red que estemos monitoreando. Podremos aplicar filtros por protocolo para ayudarnos a buscar lo que queremos. Un ejemplo de aplicación podría ser analizar el tráfico de una comunicación VoIP, donde son varios los puertos que deben estar abiertos (usualmente los puertos TCP y UDP 5060 y 5061 para las registraciones, y los puertos UDP del 10000 al 20000 para el audio). Si un puerto está mal configurado, el softphone se registrará, pero no tendremos audio, o quizás el audio sea en un solo sentido (transmite, pero no recibe), etc. Con esta herramienta, podemos encontrar el problema con solo capturar diez segundos de tráfico y aplicar el filtro que nos interesa

WIRESHARK CUENTA CON UNA AMPLIA GAMA DE FILTROS QUE FACILITAN LOS CRITERIOS DE BÚSQUEDA.

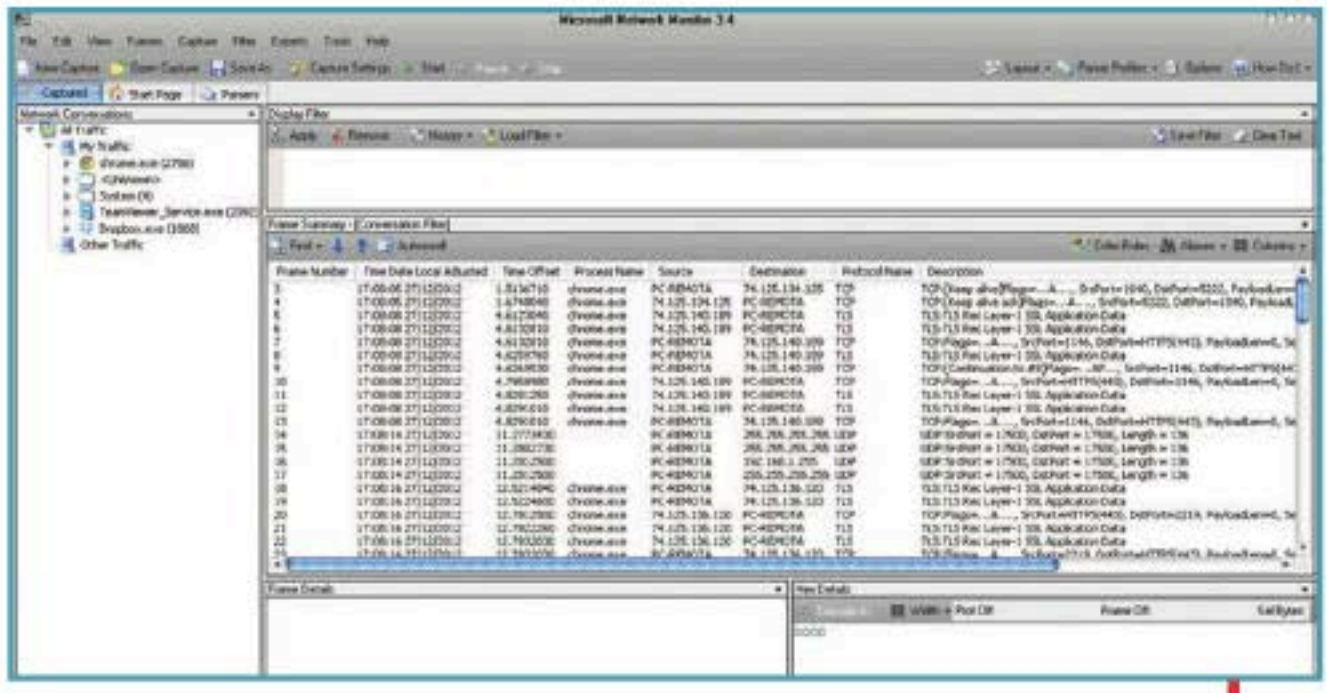
No obstante, si necesitamos auditar, o analizar tráfico en profundidad, Wireshark nos da mucha más flexibilidad como analizador de protocolos.
Otra posible aplicación es la detección de la multitud de tipos de ataques DoS: **direct attacks**, **TTL expiry attacks**, **IP unreachable attacks**, **ICMP transit attacks**, **reflection attacks**, entre otros. Con una pequeña captura del tráfico, salta a la vista el ataque de denegación de servicios (*Denial of Service*).

Microsoft Network Monitor

Microsoft Network Monitor (**www.microsoft.com/en-us/download/details.aspx?id=4865**) es una herramienta de diagnóstico de red que nos ayudará a monitorizar nuestra red y nos mostrará una gráfica de las estadísticas de la red.
Con este software gratuito, podremos realizar tareas de resolución de problemas rutinarias, como la localización de un servicio caído, o un servidor que esté recibiendo un número desproporcionado de peticiones de trabajo.
Por otra parte, recoge estadísticas de todos los frames que detecta en el segmento de red sobre un buffer de captura, en donde podremos analizar los siguientes datos:

- La dirección fuente de la PC que envía el frame a la red.
- La dirección destino de la computadora que recibe el frame.
- Los protocolos usados para enviar el frame.
- Una porción del mensaje que está siendo enviado o transmitido.

Ejecutar el software desde una PC cualquiera no dará mucha ayuda, pero podremos conectarnos al agente de un servidor. El **Network Monitor Agent** está incluido en Windows NT Workstation y Server, y, desde la PC, podremos capturar tráfico de red en una subred distinta mediante el agente remoto.
Una posible utilidad es tomar una captura de tráfico de red entre dos PC que están separados por un router, para observar si hay paquetes de red perdidos o corruptos. Para realizar este trazado, debemos tener en cuenta que los relojes de sistema deben estar sincronizados. Esto se puede lograr por la línea de comandos **Net Time**: `net time \\PC-REMOTA /set /yes`.
El nombre **Network Monitor** puede no ser preciso, ya que se podría interpretar como un analizador de paquetes, comparable con **WireShark**.



Ejemplo de captura con **Microsoft Network Monitor**, similar al de WireShark.

TCPDUMP

Tcpdump es una herramienta en línea de comandos sobre terminales en sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros, con la que podremos analizar el tráfico de nuestra red. Para Windows, contamos con **WinDump**, basado en la misma herramienta. Las múltiples opciones de parámetros y filtros nos dan infinidad de combinaciones. Podremos monitorear el tráfico que ingrese de una IP, un sitio, un host, desde un puerto específico, o cuyo destino sea una dirección MAC determinada.

Ingeniería social

Comprenderemos el significado de la ingeniería social para obtener información de los usuarios, el arte del engaño en su máxima expresión.

La **ingeniería social** es el proceso o acción para obtener información de los usuarios de un sistema y está muy relacionada con la comunicación entre las personas. Es utilizada por los delincuentes informáticos, ya que estas técnicas tienen un alto porcentaje de efectividad.

Como herramienta principal, se utiliza la comunicación (relación entre personas), y se trata de persuadir a los usuarios (víctimas) para que entreguen información valiosa, nombres de usuarios y contraseñas, tanto personales como empresariales, por medio de engaños.

Efectividad

Su nivel de efectividad se debe a que esta serie de engaños y mentiras son aplicadas directamente sobre el usuario, el cual es vulnerable y cae en las trampas o, si se aplican a los sistemas, se necesita la participación del usuario para que se obtenga la información buscada.

Debemos aclarar que los datos empresariales son los más buscados, ya que se puede obtener de ellos un rédito económico. Si bien nuestra herramienta principal es entablar relaciones comunicacionales, los sustentos por los cuales lograremos nuestro cometido serán: Internet y el teléfono, a través de ellos generaremos un vínculo de confianza y luego engañaremos a las personas para poder hacernos con los datos de, por ejemplo, su usuario y contraseña de e-mail, su usuario y contraseña de **home banking**, entre otros datos e información sensible.

Ejemplos

Por lo general, podemos entender a la ingeniería social como el conjunto de las habilidades para obtener información de terceros a partir de engaños y artimañas. Partiremos de un engaño haciéndonos pasar, por citar un ejemplo, por un agente del *call center* del banco donde la víctima posee una cuenta bancaria; por medio de una llamada telefónica, le pediremos datos para corroborar que los que se encuentran en el sistema del banco son los correctos, pero lo que en realidad estamos obteniendo es que la víctima nos brinde sus datos de acceso a su cuenta bancaria sin ningún impedimento. Para frenar este tipo de engaños y artimañas, las entidades bancarias, en sus páginas correspondientes al inicio de sesión de home banking, nos indican que nunca llamarán por teléfono para pedir datos confidenciales a sus usuarios, y advierten además a sus usuarios que nunca revelen sus contraseñas.

El teléfono es uno de los medios más utilizados para realizar ingeniería social.

También podremos citar el siguiente ejemplo, en el que nos haremos pasar por administradores de sistemas de alguna compañía de correo electrónico donde nuestra víctima tiene habilitada una cuenta de correo. Enviamos un e-mail

Phishing

Es uno de los métodos utilizados en la ingeniería social para obtener datos confidenciales de los usuarios de ciertos servicios, como pueden ser correos electrónicos o home banking. Para tener éxito, lo que se realiza son copias fieles de las páginas en las que las víctimas validen sus datos, por ejemplo e-mail o home banking; estas colocan sus datos verdaderos y, al enviarlos, terminan en casillas de correo de delincuentes informáticos.

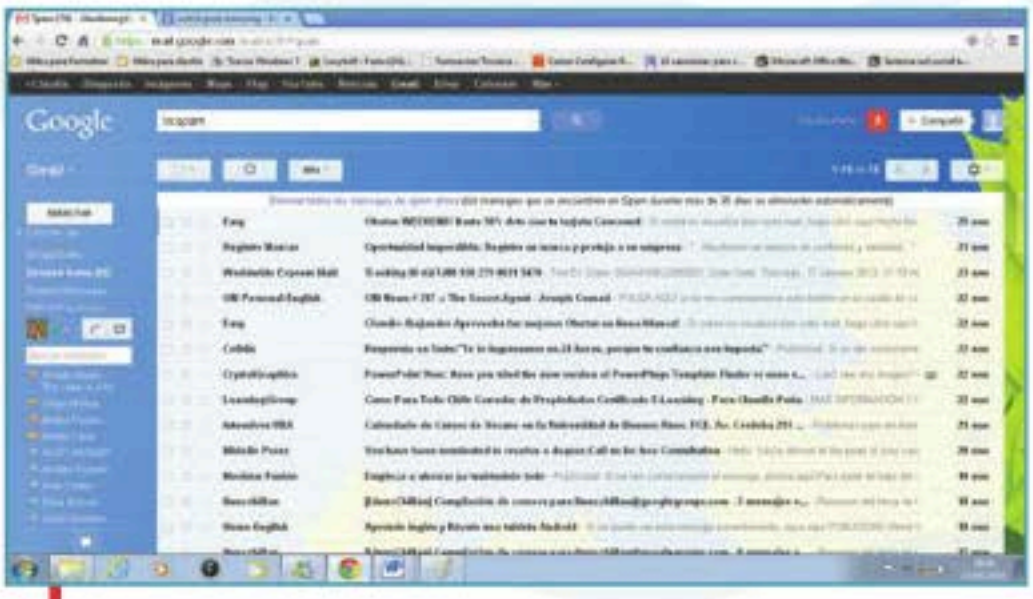
al usuario indicándole que el sitio que le brinda el servicio de correo electrónico, por una reestructuración, está modificando su base de datos y necesita que el usuario valide nuevamente sus credenciales. Lograremos el éxito a partir de un e-mail inventado, el cual se identifica como propio del servicio de sistemas del servicio de e-mail. El usuario inexperto cae en la trampa y entrega, sin darse cuenta, sus datos de acceso al correo. Además, la ingeniería social se basa en habilidades psicológicas e intenta generar en los usuarios (víctimas) una sensación, por ejemplo, de miedo al decir que se necesitan validar sus datos para una reincorporación correcta en el nuevo sistema de mensajería, si no sus cuentas quedarán inutilizables y perderán todos sus contactos. Esto no es cierto, ya que este tipo de ataque se lo conoce como **phishing**, el phishing también se utiliza en las páginas web sobre todo en las páginas de bancos y servicios financieros, donde los usuarios son informados que tienen que validar sus credenciales para una mejora en los sistemas web; una vez que la víctima coloca sus datos y los envía, un e-mail nuevo le indicará que el proceso se realizó con éxito, cuando en realidad sus datos terminaron en alguna dirección de correo del delincuente informático.

UN INGENIERO SOCIAL COMPRENDE MUCHO LA ACTUALIDAD TECNOLÓGICA Y, GRACIAS A ESO, ACUDE A LAS HERRAMIENTAS PRECISAS PARA LA OBTENCIÓN DE INFORMACIÓN SENSIBLE.

Otro tipo de engaño que resultó efectivo por mucho tiempo fue el envío de correo electrónico en el que se indica que se tienen fotos privadas de alguna personalidad del mundo del espectáculo y, al querer bajarla o hacer clic en el enlace, daremos permiso a un código malicioso para que realice envíos masivos de e-mails a nuestros contactos, como si fuésemos nosotros los que enviamos dichos correos. Cuando sucede esto, estamos frente un caso de **spam**. También existen hechos de la ingeniería social que se relacionaron con catástrofes naturales como fue el tsunami y el huracán Katrina; u ocasionados por el hombre, como el ataque a las torres gemelas, entre otros acontecimientos, donde los e-mails indicaban que tenían fotos o videos inéditos de esos hechos. La reacción que provocó en este sentido la ingeniería social fue la curiosidad de los usuarios por este tipo de imágenes o videos, los cuales tampoco existían, y los usuarios, por el simple hecho de conocer el contenido que el mensaje les indicaba, eran víctimas de spam o sus datos eran sustraídos.

Metas

Muchos de los usos de la ingeniería social tienen como meta fines económicos, y propagan estos ataques a las personas que pertenecen a alguna compañía, para conseguir los accesos a los sistemas de la organización; así ponen en riesgo información confidencial de la empresa.



Dentro de la carpeta llamada Spam podemos encontrar todos los e-mails que sean de origen dudoso. Esto lo realizan los servidores en forma automática.

De esta manera, con la ingeniería social tendremos muchas formas de incrementar los ataques y obtener los datos de los usuarios. Lo fundamental es preparar a los usuarios contra este tipo de ataques y, en lo que se refiere a la parte de seguridad informática, para no acceder a vínculos extraños o a aquellos de dudoso origen; también para no ser engañados por mensajes de correo electrónico ni por las páginas que sean creadas con la técnica de phishing.
Además, se necesita que la preparación de los usuarios sea continua y constante. Debido a que la ingeniería social es aplicada con la tecnología, a medida que esta evoluciona, las técnicas de ingeniería social se van aplicando a estas tecnologías que se encuentran en constante evolución. ■

Por medio del phishing, las páginas pueden ser imitadas, y los usuarios que intentan ingresar están entregando sus datos privados a terceros.

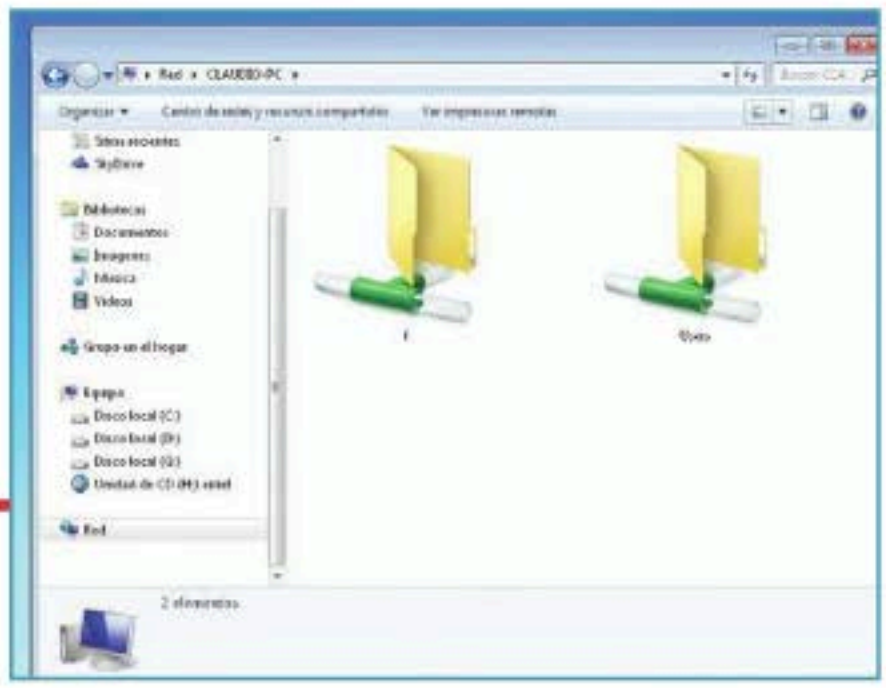
Prácticas recomendadas para los usuarios

Los usuarios de una red, sea corporativa u hogareña, están sujetos a peligros que van más allá de los que habitan en Internet.

Si bien como administradores de red tendremos la capacidad de asegurar los recursos de la red propiamente dicha, siempre es aconsejable educar a los usuarios sobre las medidas de seguridad que deberían tomar para evitar, por negligencia o desconocimiento, problemas que afecten el correcto funcionamiento de la mencionada red. Normalmente, será el administrador quien mantendrá todos los equipos actualizados (el sistema operativo, la suite ofimática, el antivirus, el antispyware y demás software que necesite ser actualizado), ya que la estabilidad del sistema depende en gran parte de ello. De más está decir que tales actualizaciones se realizan desde el servidor central, de manera remota y en simultáneo a todos los equipos que integran la red.

Antivirus

Siempre puede suceder que la empresa antivirus lance una revisión fuera de las fechas estándares por lo que, por unos días (hasta que el script de actualización automático entre en funcionamiento), estaremos con los antivirus desactualizados. Por ello, es una buena medida capacitar a los usuarios para que actualicen (o al menos lo intenten) los antivirus y antispyware. El software en general puede soportar una pequeña demora para su actualización, ya que una falla no necesariamente pondrá en peligro la red.



Utilizar una carpeta compartida en red nos garantiza una copia de los datos en caso de daño en nuestra PC.

Medios extraíbles

Siguiendo con las recomendaciones que deberíamos hacerles a los usuarios de la red, aparece el problema de la utilización de medios extraíbles tales como memorias USB o pendrives, tarjetas SD (o cualquiera de los demás formatos como MMC, CF, MSD, etc.), unidades de disco removibles (se conectan por USB, eSATA, Firewire u otro puerto).

Si bien resultan extremadamente útiles y trasladables debido a su tamaño, si el usuario no toma unas pocas medidas de seguridad, podríamos enfrentar una vasta epidemia de virus informáticos o incluso algún malware en nuestra red. Hoy en día, la gran mayoría de los antivirus tienen la capacidad de realizar un chequeo en el momento de la conexión de dichos dispositivos, e incluso hay antivirus específicos para unidades portables como **MX One** (lo conseguimos en **www.mxone.net**); pero en los casos en los cuales no haya una necesidad manifiesta y justificada, lo ideal sería el bloqueo de los puertos de conexión, para evitar problemas a futuro.

Correo electrónico

Los mensajes de correo electrónico merecen una mención aparte. Es la vía de propagación de **hoaxes** (engaños pensados para infundir pánico o preocupación mediante una aseveración falaz), scripts (porciones de código embebida en el mensaje con el objeto de causar algún daño, tomar control en forma remota de los equipos o incluso abrir un puerto en el equipo para monitorear las comunicaciones de la red), phishing (mensajes que suplantan la identidad del remitente para hacernos ingresar datos sensibles en una página web diseñada como engaño para recolectar esos datos, como por ejemplo, un sitio de home banking), entre otros.

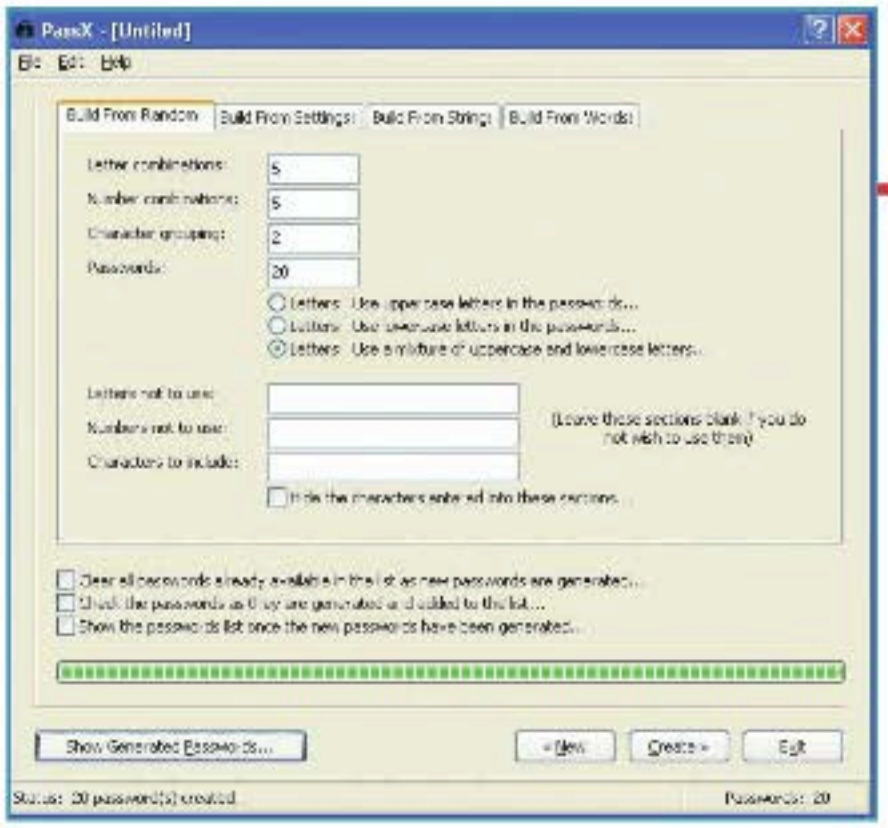
Debemos mantener informados a los usuarios sobre todos estos artilugios para que estén atentos y no caigan en ninguna de estas trampas.

Contraseñas

Finalmente, vamos a remitirnos al apartado en el que más énfasis debemos colocar a la hora de capacitar a los usuarios de la red: las **contraseñas**; y en especial las de los usuarios que, por sus tareas o jerarquía, tengan acceso a Internet desde la red.

Todos los usuarios de computadoras nos hemos visto, como mínimo, tentados a utilizar contraseñas fáciles de recordar, como nuestra fecha de nacimiento, nombre o apodo de algún familiar o mascota e, incluso, de nosotros mismos; y los más osados hasta combinaciones de dos o más de estos datos.

El problema radica en que, a quien realmente quisiera obtener dichos datos, no le sería muy difícil hacerlo. Por eso, siempre sugerimos crear contraseñas que incluyan en lo posible tanto mayúsculas como minúsculas, números, espacios y otros caracteres de los que aparecen en el teclado.



Un generador de claves como PassX nos proveerá de contraseñas prácticamente inquebrantables para nuestros datos.

LOS DISCOS EXTERNOS, PENDRIVES Y TARJETAS DE MEMORIA QUE PASAN DE MANO EN MANO SON UN RIESGO DE CONTAGIO.

También es recomendable que tengan una longitud de no menos de 10 caracteres.

La idea es generar contraseñas lo más complicadas que nos sea posible, para que no puedan ser violadas con facilidad.

El problema radica en nuestra memoria: cada vez hay más servicios que utilizamos: e-mail, Facebook, Twitter, foros, etc. Memorizar una contraseña compleja es una cosa; memorizar más de diez es otra muy distinta.

Pero, como siempre, podemos recurrir al software para echarnos una mano, por ejemplo, **PassX** (**http://es.download.cnet.com/PassX/3000-2653_4-10570802.html**), se trata de un generador de contraseñas que nos permitirá escoger entre varios parámetros para la tarea: podemos definir la longitud, la cantidad de contraseñas por generar (para elegir las que más nos gusten), qué caracteres incluir (mayúsculas, minúsculas, números), e incluso podemos generarlas a partir de una cadena que ha sido predefinida por nosotros.

Pero nos sería imposible recordar más de una contraseña con 15 caracteres aleatorios (o más). Por eso, también podemos recurrir a **KeePass** (**http://keepass.info**), con él podremos almacenar, en una base de datos, la información referida a las contraseñas. Cada registro nos permitirá indicar el nombre de usuario, la contraseña, el nombre del servicio al que podemos acceder con esos datos y su URL. Cabe destacar que todo lo que carguemos en KeePass se almacena de manera encriptada y protegida por una contraseña maestra, la que recomendamos fervientemente que no conste de menos de 20 caracteres como medida de seguridad. Así, solo debemos recordar la contraseña de la base de KeePass, ya que las demás estarán almacenadas en su interior. ■

Las contraseñas

Cuantos más servicios utilizamos, más contraseñas debemos recordar, e invariablemente caemos en la trampa de las contraseñas débiles, como fechas de cumpleaños o el nombre de algún familiar o mascota. Por eso, aconsejamos el uso de generadores de contraseñas como **PassX**. Esta aplicación nos hará la vida más fácil a la hora de conseguir contraseñas seguras.

IPsec

La importancia de la seguridad en Internet llevó a desarrollar protocolos que maximicen y aseguren el intercambio de información en la red.

Cuando hablamos de seguridad en la red (principalmente en Internet), nos referimos a la necesidad de asegurar los millones de paquetes intercambiados por segundo en toda la red. Hoy en día, el acceso a la información se ha convertido en una herramienta de uso diario en todos los aspectos de la vida cotidiana, desde correos electrónicos hasta actividades financieras del más alto nivel.

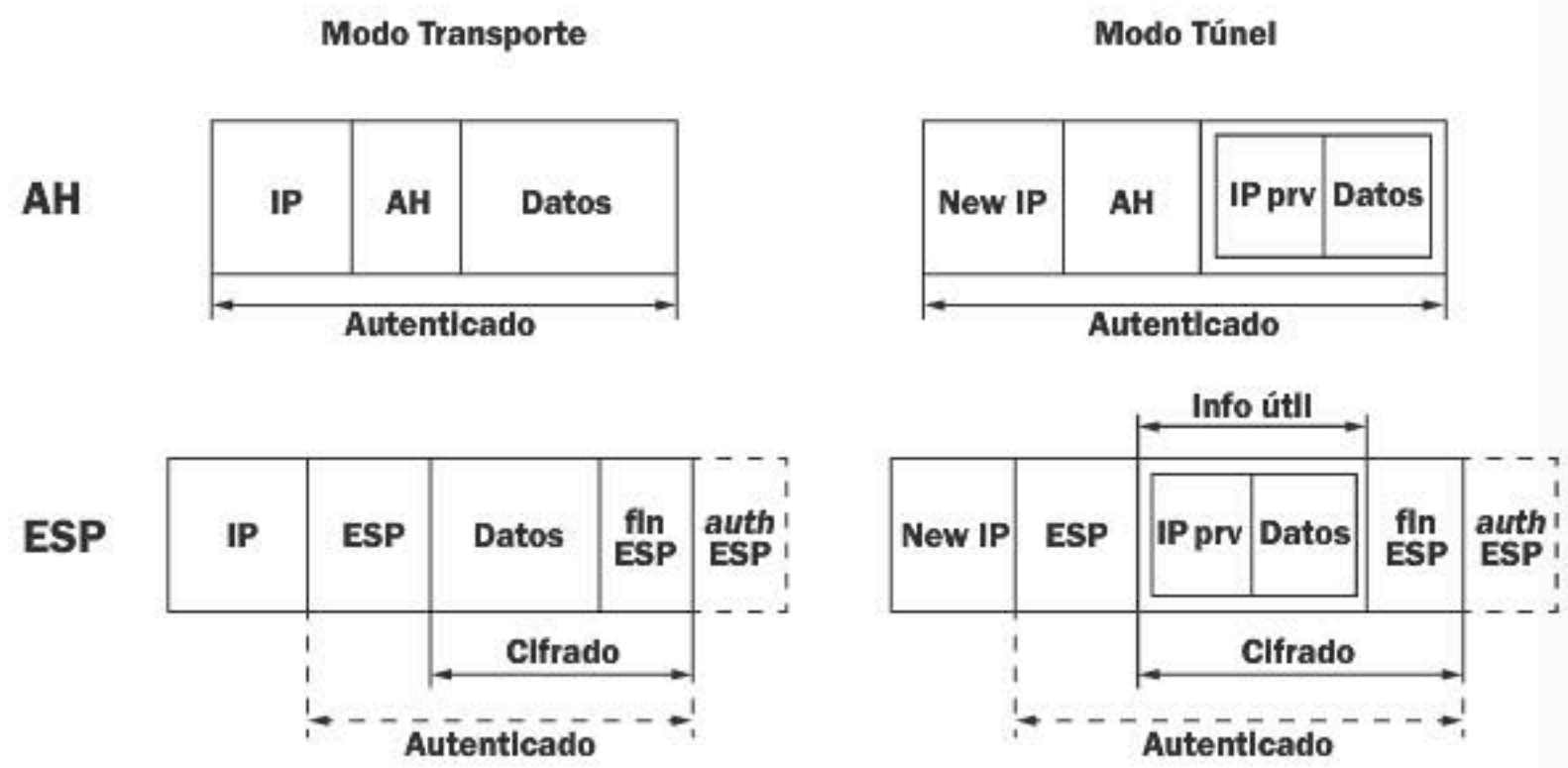
Métodos

Distintos métodos para proteger estas comunicaciones han sido implementados con el paso de los años; con ellos, se han mejorado diversos mecanismos de protección. El **IPsec** (*Internet Protocol Security*, o protocolo de seguridad de Internet) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre **IP** (*Internet Protocol*). Cumple la función de ser una extensión del protocolo IP que proporciona seguridad a este y a capas superiores.

IPsec

IPsec se desarrolló para el nuevo estándar IPv6 (de uso obligatorio), que posteriormente fue adaptado para IPv4 (se puede aplicar o no). Su funcionamiento y arquitectura se detallan en el RFC2401, y sus principales tareas consisten en autenticar y cifrar cada paquete transmitido por la red; esto implica que toda la información enviada y recibida debe cumplir determinadas características para ser validada.

Uno de los principales motivos para su desarrollo fue que los protocolos IP no proveen ninguna capacidad de seguridad, y se requirió la implementación de un nuevo servicio que fuera capaz de poder asegurar la información. Dos protocolos son empleados en IPsec el **AH** (*Authentication Header*, proporciona integridad, autenticación y aceptación si se eligen los algoritmos criptográficos adecuados) y **ESP** (*Encapsulating Security Payload*, proporciona confidencialidad, y la alternativa de autenticación y protección de integridad) para cifrar el tráfico (únicamente legible por el destinatario autorizado), validación de la integridad (se asegura que la información no sufra errores ni modificaciones durante el transporte), autenticar los extremos (los extremos siempre deben ser de confianza),



En este diagtama vemos el envío de paquetes mediante los protocolos AH y ESP en los distintos modos.

antirrepetición (evita la duplicación en sesiones seguras).

AH: garantiza integridad y autenticidad de los datos de origen del datagrama IP. Calcula un **HMAC** (*Hash Message Authentication Code*, código de autenticación de mensaje hash) a través de un algoritmo hash sobre una clave secreta, del contenido del paquete y las partes inmutables del datagrama. Esta tarea se realiza a través de NAT Transversal (NAT-T). AH protege la carga útil IP y todos los campos útiles del datagrama IP, excepto los campos que serán alterados en el tránsito.

ESP: el protocolo proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. Si bien está permitido, no se aconseja utilizar cifrado sin autenticación. Al contrario que AH, la cabecera IP no está protegida por ESP, pero sí opera directamente sobre IP. El IPsec establece, además, los protocolos para el establecimiento de las claves de cifrado. Según el modelo OSI, IPsec actúa sobre la capa 3, a diferencia de otros protocolos de seguridad como el SSL, TLS y SSH, que operan en las capas 4 y superiores. Esto significa que el protocolo IPsec posee mayor alcance ya que, al trabajar sobre la capa de transporte, puede incluir protocolos como TCP y UDP (los más utilizados), entre otros.

Mediante el modo transporte, se pueden configurar redes VPN en las configuraciones propias del router.

Una de las principales ventajas que presenta IPsec frente a otros protocolos de seguridad reside en que, para que las aplicaciones puedan utilizarlo, no es necesario realizar ningún cambio interno, mientras que para los otros protocolos de seguridad estas deben modificar su código de funcionamiento.

Arquitectura

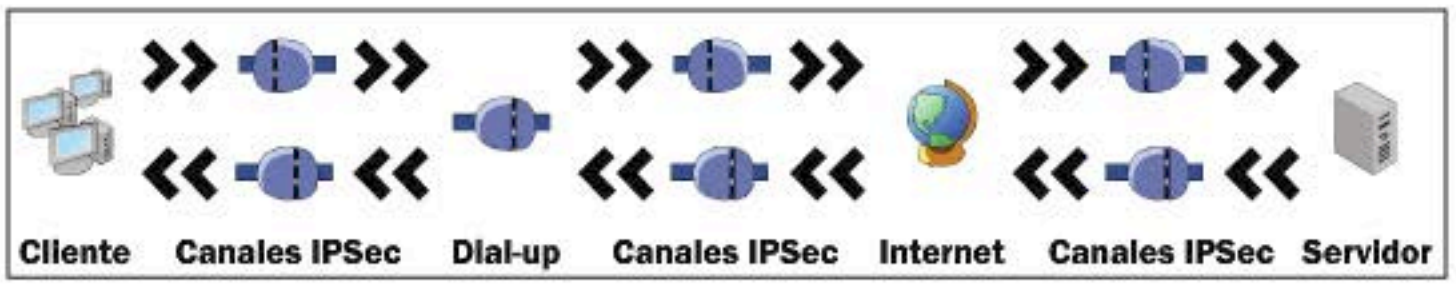
La arquitectura de funcionamiento del protocolo está basada en protocolos criptográficos que aseguran el flujo de paquetes, garantizan la autenticación mutua y establecen los parámetros criptográficos. Utiliza los principios de asociación de seguridad (*Security Association*, **SA**) para realizar funciones de seguridad que, en sí, representan paquetes de algoritmos, y parámetros para cifrar y autenticar el flujo de la información. En la transferencia de información, se implementan asociaciones de seguridad que permiten el flujo bidireccional seguro de la información.

Seguridad

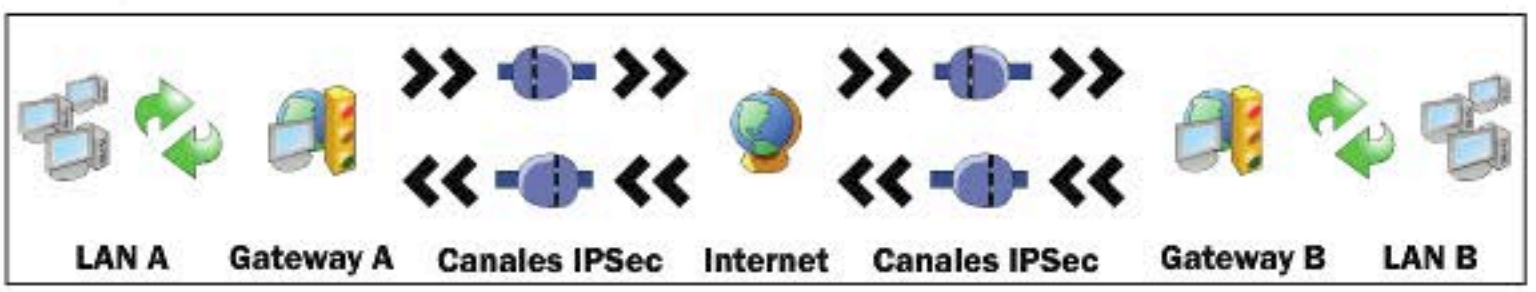
Para determinar qué protección se les asignarán a los paquetes salientes, IPsec utiliza el índice de parámetro de seguridad (*Security Parameter Index*, **SPI**), el índice a la base de datos de asociaciones de seguridad (*Security Association Database*, **SADB**) y la dirección de destino del paquete (según su cabecera); juntos establecen una única asociación de seguridad al paquete.

Para los paquetes entrantes, IPsec asocia los paquetes con las claves de verificación

Modo TRANSPORTE



Modo TUNEL



Aquí se ejemplifica el principio de funcionamiento del modo transporte y también del modo túnel.

La configuración de IPsec puede realizarse a través del administrador web del router.

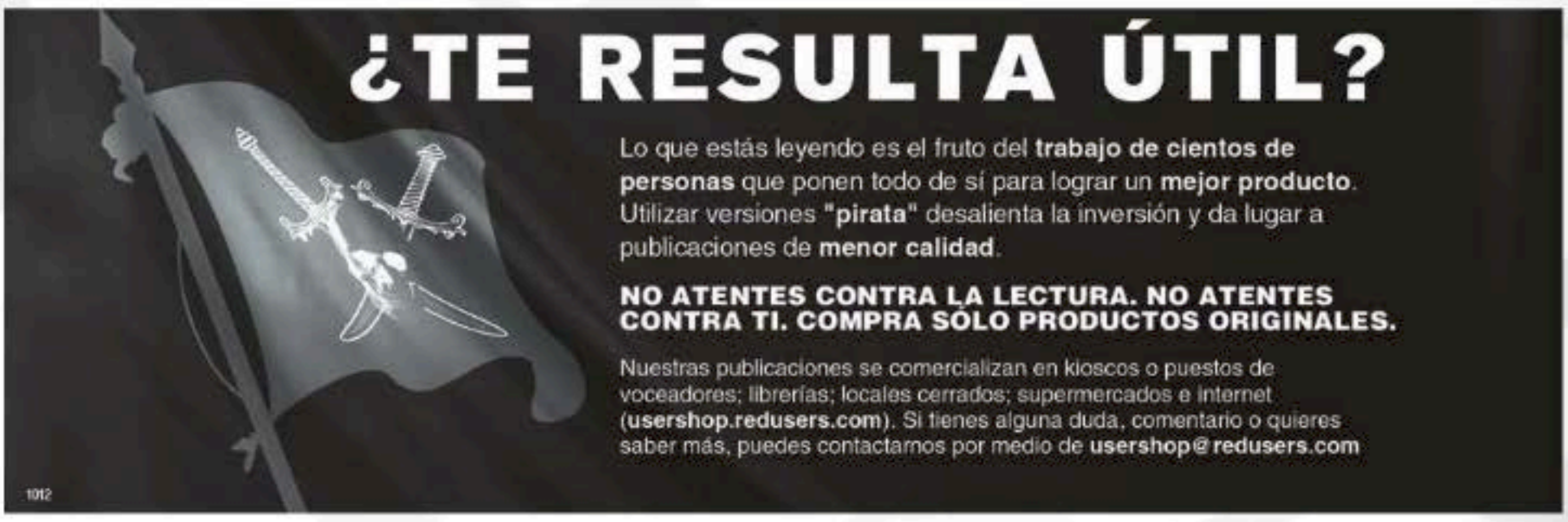
asignadas y utiliza la base de datos de asociaciones de seguridad.
Cada asociación de seguridad define: dirección IP de origen y destino de la cabecera de IPsec resultante, protocolo IPsec (AH o ESP), algoritmo y clave secreta y el SPI (con un número de 32 bits que identifica la asociación de seguridad).
Sin embargo, las asociaciones de seguridad solo especifican cómo se protegerá el tráfico. Para definir qué tráfico proteger, se establece una política de seguridad **SP** (*Security Policy*) que se almacena en la base de datos de políticas de seguridad **SPD** (*Security Policy Database*). Estas políticas definen: direcciones de origen y destino de los paquetes por proteger, protocolos y puertos por proteger, y la asociación de seguridad que se empleará.
Para transmisiones **multicast**, se proporciona una asociación de seguridad al grupo duplicándose para todos los demás receptores del grupo. Utilizando SPI, se les pueden otorgar a diversos grupos más de una asignación de seguridad en distintos niveles y conjuntos de seguridad en un mismo grupo.
IPsec está diseñado para brindar seguridad en modo transporte (extremo a extremo, los ordenadores de los extremos realizan las operaciones de seguridad) y en modo túnel (puerta a puerta, se proporciona el modo de seguridad a múltiples equipos por un único nodo).

En modo transporte

Cuando se realiza la conexión, solo la parte de los paquetes que corresponden a los datos transferidos es cifrada y autenticada. Se maneja la carga del datagrama insertando la cabecera entre la cabecera IP y la del protocolo de las capas superiores, por lo que el enrutamiento permanece intacto.
Pero, cuando se utiliza la cabecera de autenticación, las direcciones IP no pueden ser traducidas (se invalidaría el hash). El modo transporte se utiliza para comunicaciones de equipo a equipo. El mecanismo para encapsular los mensajes IPsec a través de **NAT-T** está especificado en las **RCF**. Se utiliza para establecer conexiones seguras entre las dos terminales por un canal inseguro.

En modo túnel

En este modo se encapsula, cifra y autentica todo el paquete, datos y cabecera. El datagrama IP se encapsula completamente dentro de uno nuevo empleando el protocolo IPsec. El modo es utilizado para entrelazar de red a red creando túneles seguros entre ellas sobre Internet. Se utiliza para realizar conexiones seguras entre dos redes en canales inseguros.
Para proteger la integridad de los datagramas, se emplean códigos de autenticación basados en **HMAC-SHA-1** (códigos de autenticación de mensajes hash que protegen integridad). Estos protocolos emplean algoritmos de resúmenes **MD5** y **SHA** para realizar las operaciones utilizando las claves y los contenidos del datagrama IP.
El receptor de los paquetes comprueba **HMAC** mediante la clave asignada.
Para cifrar la información, se emplean algoritmos estándares de cifrado simétrico. IPsec exige la implementación de **NULL**, **DES**, y otros más actuales y fuertes como **3DES-CBC**, **AES-CBC** y **Blowfish** para confidencialidad. ■



PRÓXIMA ENTREGA

13

IMPRESORAS DE RED

En el próximo número veremos todo lo necesario para imprimir en red. Además, aprenderemos a configurar la impresora de manera adecuada y conoceremos las opciones de software disponible para realizar su correcta administración.

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00012
9 789871 857784

CONTENIDO DE LA OBRA

1 Introducción a las redes informáticas
2 Tipos de redes y topologías
3 Dispositivos de red
4 Instalación de redes cableadas
5 Puesta en marcha de una red cableada
6 Configuración de redes cableadas
7 Instalación de redes inalámbricas
8 Configuración de redes inalámbricas
9 Seguridad en redes cableadas e inalámbricas
10 Configuración avanzada de routers
11 Recursos compartidos y dispositivos multimedia
12 SEGURIDAD FÍSICA DE LA RED
13 Impresoras de red
14 Hardware de servidores
15 Administración de Windows Server
16 Administración de sistemas Linux
17 Administración y asistencia remota
18 Servidores web y FTP
19 Servidores de mail
20 Servidores de archivos e impresión
21 Servidores adicionales
22 VLAN, VPN y trabajo remoto
23 Telefonía IP
24 Cámaras IP