INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

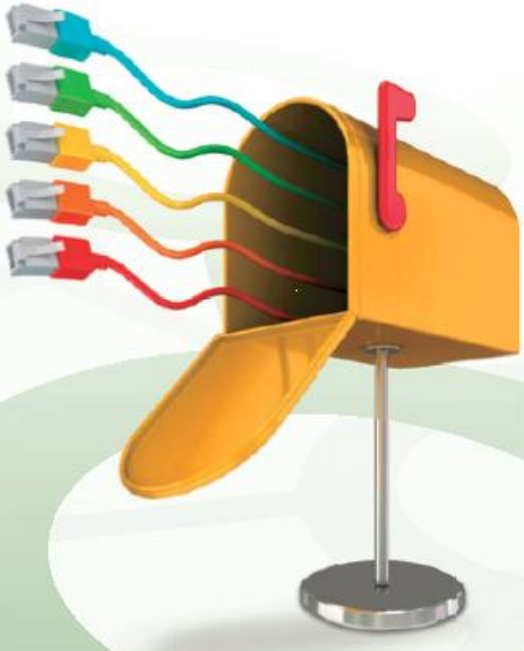
Argentina $ 22.- // México $ 49.-

19

Técnico en REDES & SEGURIDAD

SERVIDORES DE MAIL

En esta clase veremos las características de los servidores de correo tanto en sistemas Windows como en GNU/Linux. Analizaremos también las opciones de seguridad y las mejores aplicaciones.



- SERVIDOR DE CORREO
- CORREO EN LINUX Y WINDOWS
- OTROS USOS DEL E-MAIL
- E-MAILS TEMPORALES
- ANÁLISIS DE HEADERS

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

Impreso en Sevagraf S.A. Impreso en Argentina.

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...

Características y opciones de los servidores de correo electrónico tanto en plataformas Windows como en GNU/Linux; además, las opciones de seguridad relacionadas.

En la clase anterior, vimos las características de los servidores web y FTP, conocimos qué son y qué ventajas nos entregan. Aprendimos a instalar estos servidores y revisamos las consideraciones que debemos tener en cuenta para administrarlos. Luego, vimos conceptos importantes sobre la seguridad en los servidores web y FTP; finalmente, analizamos las diferencias entre los protocolos HTTP y HTTPS.

En este fascículo, analizaremos qué es un servidor de correo electrónico, y aprenderemos a instalarlo y a configurarlo en sistemas operativos Windows y GNU/Linux. Para continuar, conoceremos los peligros del spam y de qué forma se filtra en el servidor, deshabilitaremos el Open Relay y conoceremos algunos servicios para obtener cuentas de e-mail temporales. Para terminar, realizaremos el análisis de los headers de e-mails.

19

4
Servidor de correo en Windows Server

8
Servidor de correo en Linux

12
Spam

22
Análisis de headers de e-mails

Qué es un servidor de correo

En esta sección, conoceremos a uno de los protagonistas de las infraestructuras de comunicaciones: el servidor de correo.

Luego de tantos años de utilizar el correo electrónico (**e-mail**), el intento de dar una definición de él puede resultar un poco obvio, pero su funcionamiento no es tan evidente como podría parecer. Lo cierto es que su uso data del año 1982, por lo que merece una mención especial por la subsistencia a través del tiempo, y la manera en que se ha ido adaptando para cubrir las necesidades de los usuarios y las empresas.

Servidor de correo

En líneas generales, decimos que un servidor de correo electrónico hace las veces de una casilla de **correo postal**, a la que una persona nos puede enviar algo físico, ya sea una carta o una encomienda, y que hasta que no nos acercamos a retirarla seguirá ahí guardada. En caso de que el envío sea más grande que el espacio disponible en la casilla (que es literalmente una especie de casillero, semejante a un **locker** de seguridad de un supermercado), la puerta no cerrará y no se podrán guardar más elementos. En el correo electrónico ocurre algo similar. En este caso, existe un servidor que provee el espacio virtual en términos de una determinada cantidad de **gigabytes**, que será utilizado para recibir mensajes y sus archivos adjuntos. En caso de que se llene, no podremos continuar recibiendo más envíos de correos.

AUNQUE SUELEN UTILIZARSE LOS PROTOCOLOS DE CORREO EN TEXTO PLANO, ES POSIBLE AGREGAR SEGURIDAD AL HACER USO DE SUS VERSIONES SEGURAS.

El servidor de correo electrónico, entonces, presta en principio el **espacio de almacenamiento**, pero esto no es suficiente, ya que resulta necesario, además, establecer un mecanismo por el cual un usuario logre recibir los mensajes y otro para que pueda enviarlos. En términos físicos, ese trabajo lo hará la propia **empresa de correo**, que se encargará de proveer el espacio físico, las oficinas, los empleados, etc.

Outlook.com es el servicio de Microsoft, que reemplazó a Hotmail, el más popular de los webmails.

En términos técnicos, ese trabajo es organizado por las empresas proveedoras del servicio, para ello se deben utilizar los **protocolos de comunicación**.

Protocolo

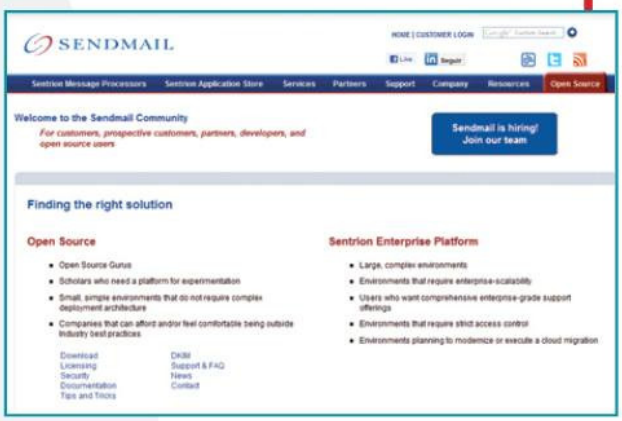
En el caso del correo electrónico, el protocolo que se utiliza para realizar el envío de los mensajes es el llamado **SMTP** (**Simple Mail Transfer Protocol**) o protocolo de transferencia simple de correo, que está definido en el **RFC 2821** y trabaja en el puerto **25/TCP**. Esta comunicación se basa en el **modelo cliente-servidor** para realizar el envío y recepción de mensajes, y supone la existencia de una aplicación cliente que se encargue de realizar la tarea de conexión en forma activa.

Para realizar la recepción del correo, es necesario contar con otro protocolo de comunicaciones, de las opciones disponibles el más importante es el llamado **POP** (**Post Office Protocol**) o protocolo de oficina de correo, el cual se encuentra definido como estándar en el **RFC 1939**, y que suele utilizarse en la versión 3, por lo que también se lo refiere como **POP3**. Otro protocolo muy utilizado para la recepción de mensajes de correo es el llamado **IMAP** (**Internet Message Access Protocol**) o protocolo de acceso a mensajes de Internet, que utiliza principalmente el puerto **143/TCP**; su versión actual es la 4 y se encuentra definido en el estándar **RFC3501**.

La nube

Si bien los servidores de e-mail son fundamentales en toda infraestructura tecnológica que implique la comunicación entre usuarios, con la masificación de Internet se dio un fenómeno particular que implicó que el e-mail se transformara naturalmente en el primer servicio **en la nube** por medio del uso de los **webmails**, o servidores de correo que pueden ser accedidos directamente desde una página web a través de Internet. Estos no requieren el uso de un cliente de software instalado localmente en un sistema. Esta característica promovió el uso del correo electrónico desde **cualquier ubicación**, e independizó al servicio de toda plataforma operativa. Los webmails son, entonces, servidores que incluyen además el propio cliente, de modo que el usuario solo debe acceder con usuario y contraseña, o con algún otro sistema de acceso más seguro, para visualizar la interfaz.
Un aspecto por el que siempre se ha tenido especial cuidado con el correo electrónico es su **seguridad**, ya que tanto el SMTP como el POP y el IMAP son protocolos que funcionan normalmente sobre la base de la comunicación en **texto plano**, es decir, no cifran los datos que transfieren, y pueden ser objeto de ataques, como falsificación de remitente, escucha de protocolo (**sniffing**) y otros. Por tal motivo, también existen versiones seguras, que, en el caso del POP corresponde al uso del puerto **995/TCP**, en el caso de IMAP es el puerto **993/TCP**, y en el caso de SMTP es el **465/TCP**.
En cuanto a la **intercompatibilidad**, es importante tener en cuenta que las diferentes implementaciones de software suelen presentar algunas diferencias en el uso de los estándares existentes, por lo que muchas veces se recomienda que el par cliente-servidor se base en sistemas ofrecidos por el mismo fabricante, como por ejemplo, el cliente **Microsoft Outlook** y el servidor **Microsoft Exchange Server,** o el cliente **Lotus Notes** (**IBM**) y el servidor **Lotus Domino**. Esto suele darse cuando los fabricantes agregan funcionalidades o características especiales a sus sistemas, que implican la modificación de los protocolos, en detrimento de la compatibilidad con otros sistemas no propios.

Sendmail es uno de los servidores de correo electrónico más difundido del mundo.



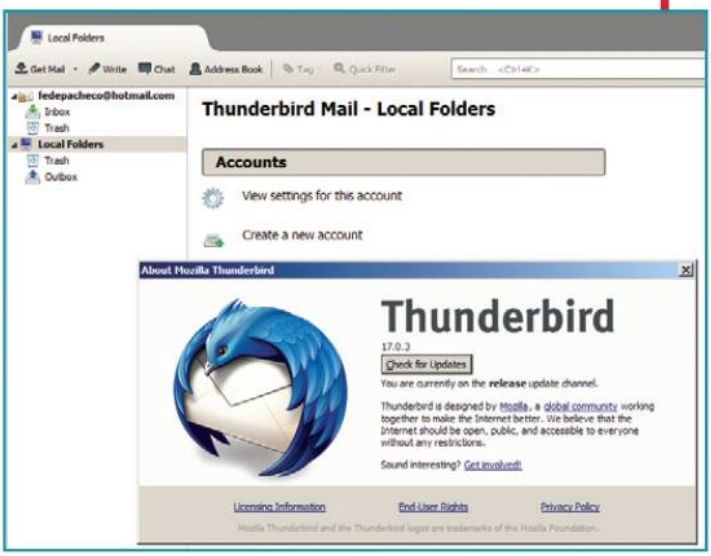
DNS y correo electrónico

El sistema **DNS** (*Domain Name System*) también suele ser utilizado para enviar y recibir correo electrónico, ya que lo que se provee generalmente no es una dirección IP, sino su nombre, como por ejemplo, smtp.servidor.com o pop3.servidor.com. De esta forma, se resuelve primero el nombre y, luego, se realiza la conexión. El sistema DNS incluye, de hecho, un registro especial para identificar los servidores de correo electrónico, que es el denominado **MX**.

Plataformas

Si bien existen servidores de correo para cada una de las distintas plataformas y sistemas operativos modernos, históricamente han sido **GNU/Linux** y los derivados de **Unix** los preferidos de las grandes infraestructuras. Este hecho se basa, quizás, en su alta estabilidad en años en los que no había muchas opciones extras. Las ventajas incorporadas por Microsoft a su sistema de correo, por ejemplo, no han tenido especial relación con la eficiencia, sino más bien con las funcionalidades, ya que proveyeron interfaces de administraciones muy poderosas e intuitivas para los administradores, y mayor comodidad para los usuarios.
En suma, como centro de gran parte de las comunicaciones mundiales, los servidores de correo electrónico deben ser considerados en todo su espectro cuando de redes se trata. ■

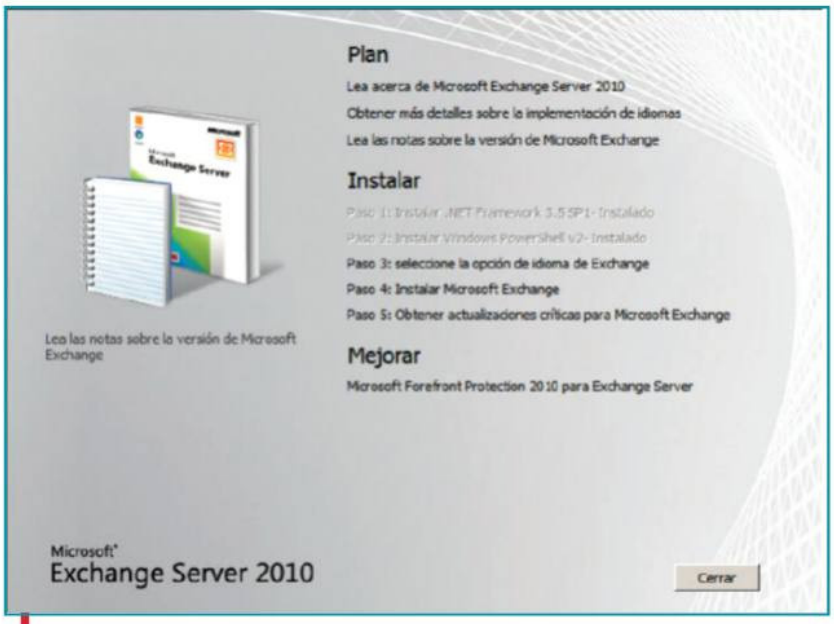
Thunderbird es uno de los clientes de correo más utilizados, y se distribuye como software libre.



Servidor de correo en Windows Server

Los correos electrónicos han reemplazado en un gran porcentaje al correo postal. Por este motivo, los servidores de e-mail son ampliamente utilizados; aquí conoceremos sus detalles.

Un **servidor de correo electrónico** es una aplicación que se aloja en una computadora servidor (con un sistema operativo servidor en la mayoría de los casos), por lo general dentro de Internet (podemos montar un servidor de correos dentro de una red tipo LAN, MAN, etc.). El objetivo de dicha aplicación es simular el correo postal tradicional, pero de manera electrónica sobre una red de transmisión de datos. Se intercambian correos electrónicos en lugar de cartas y paquetes físicos. Los correos electrónicos permiten el envío no solo de mensajes, sino también de archivos adjuntos, como documentos de Microsoft Word e imágenes.



La aplicación de servidor de correos electrónicos **Microsoft Exchange** es una de las más utilizadas en el ambiente empresarial.

Instalación

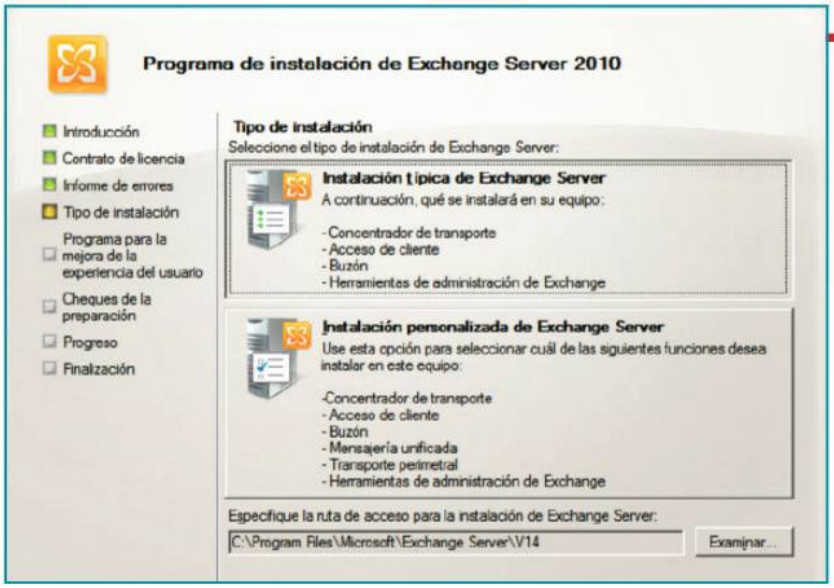
Vamos a ilustrar cómo instalar y configurar Microsoft Exchange 2010 Server (la instalación se suele realizar sobre Windows 2003 Server o Windows 2008 Server en sus diferentes versiones), pero existen otras aplicaciones servidores de correo en el mercado.

UN SERVIDOR DE CORREO SIMULA EL CORREO POSTAL TRADICIONAL, PERO DE MANERA ELECTRÓNICA.

Para instalar **Microsoft Exchange 2010 Server**, debemos ejecutar el archivo setup.exe, que se encuentra dentro de la carpeta del instalador. A continuación, el instalador nos muestra una serie de pasos por seguir para poder hacer efectiva la instalación de la aplicación:

- **Paso 1**: instalar .NET Framework 3.5 SP1.
- **Paso 2**: instalar Windows PowerShell v2.
- **Paso 3**: seleccionar la opción de idioma que deseamos para Exchange.
- **Paso 4**: seguir las instrucciones para instalar Microsoft Exchange.
- **Paso 5**: obtener actualizaciones críticas para Microsoft Exchange.

Se recomienda no instalar el servidor de correo sobre un controlador de dominio por razones de seguridad. Para iniciar el proceso de instalación, debemos hacer un clic sobre el primer paso que se encuentra activo. En ocasiones, no es necesario ejecutar los pasos 1, 2 o 3 porque los componentes ya se encuentran instalados; en esos casos, el instalador desactiva estos pasos (aparecen en gris y finalizan con el mensaje Instalado). Desde el paso 4 comienza la instalación de Exchange.



A continuación, el instalador nos va a mostrar una introducción; en este punto presionamos el botón **Siguiente**. Luego, nos ofrecerá el contrato de licencia, y lo aceptamos. Debemos optar entre realizar una instalación típica o una instalación personalizada, y especificar la ruta de instalación en el sistema. Las diferencias principales entre ambas opciones de instalación son las siguientes:

▶ **Instalación típica de Exchange Server**: implica la instalación de los componentes Concentrador de transporte, Acceso de cliente, Buzón y Herramientas de administración de Exchange, entre otras opciones importantes.

▶ **Instalación personalizada de Exchange Server**: además de comprender los componentes mencionados en el tipo de instalación anterior, se anexan Mensajería unificada y Transporte perimetral.

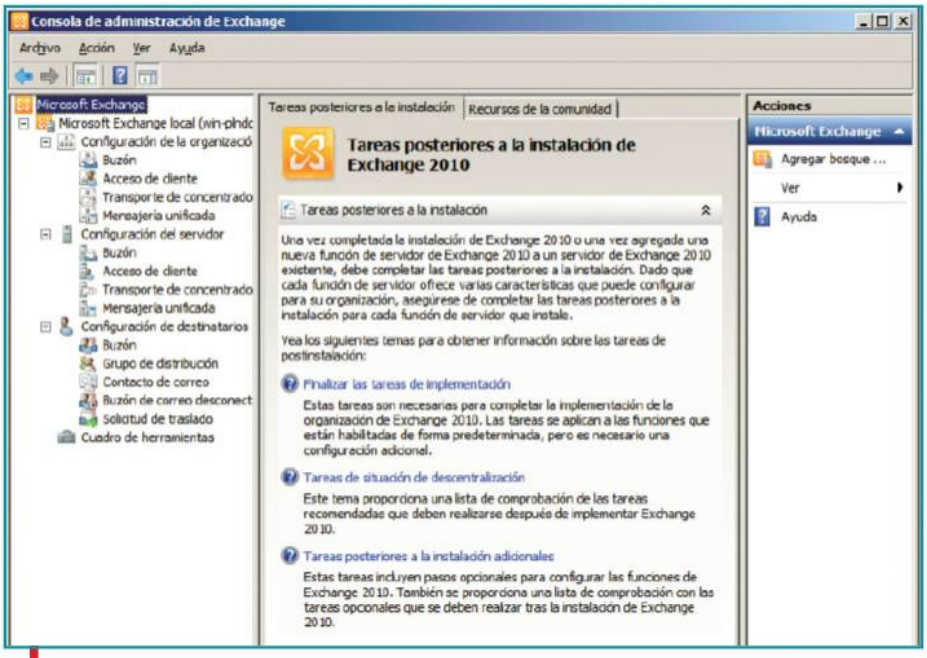
Una vez seleccionado el tipo de instalación, debemos introducir el nombre de la organización e indicar si existen clientes con clientes de correo anteriores. Siguiendo con la instalación, el instalador realiza las comprobaciones necesarias. Al finalizar estas, se muestran los mensajes de error de configuración y de no aptitud de la computadora huésped en caso de que existan. Si no se produce ningún mensaje de error, nos encontramos en condiciones de comenzar la instalación. Para ello, presionamos el botón **Instalar**. Una vez finalizada la instalación, presionamos el botón **Finalizar**. Por último, se va a iniciar la **Consola de administración Exchange**. Se recomienda reiniciar el servidor, de ser posible, para terminar con la instalación. Para configurar nuestro servidor de correo, vamos a utilizar la **Consola de administración de Exchange** para realizar configuraciones generales y **Active Directory** para configuraciones puntuales sobre usuarios (modificar las propiedades de una cuenta de correo por ejemplo).

La instalación de Microsoft Exchange Server dispone de un completo asistente, que nos permitirá realizar una instalación típica o personalizada.

Consola de administración de Exchange

Para comenzar a configurar Microsoft Exchange, debemos tener en cuenta la estructura de la organización en donde va a funcionar el servidor de correos, en lo que respecta a usuarios o servidores externos con los que debe interactuar, caso contrario Exchange no va a realizar el intercambio de información con ellos. Como mencionamos en apartados anteriores, es necesario asignarle un nombre a la organización durante el proceso de instalación de la presente aplicación. La consola de administración nos permite configurar los aspectos que mencionamos a continuación:

Al finalizar la instalación de Microsoft Exchange Server, veremos un resumen con información sobre el resultado de cada parte del proceso.



Exchange está fuertemente integrada con Active Directory. La primera permite la configuración de los servicios, y la segunda, la de los usuarios.

▶ **Configuración de la organización**: nos permite configurar opciones globales de la organización de Exchange, como por ejemplo, funciones de acceso administrativo para usuarios y grupos. Esta configuración está compuesta por las siguientes secciones:

▶ **Buzón**: engloba la configuración de las funciones de servidor de buzón, como listas de direcciones, carpetas personalizadas administradas, directivas de buzón de administración de registros de mensajería (MRM) y libretas de direcciones sin conexión.

▶ **Acceso de cliente**: nos permite crear y administrar directivas de buzón de Exchange y aplicar un conjunto común de directivas o configuraciones de seguridad a un grupo de usuarios.

▶ **Transporte de concentradores**: esta función es implementada por Active Directory dentro de la organización. Permite administrar todo el flujo de correo interno, aplica las directivas de enrutamiento de mensajes de la organización y es la responsable de la entrega de mensajes a un buzón de un destinatario particular. Aquí se define cómo y cuándo se envían los mensajes.

▶ **Mensajería unificada**: alcanza a toda la organización; permite la administración de los planes de marcado, IP de puertas de enlace y operadores automáticos de mensajería unificada.

▶ **Configuración de servidores**: Nos permite configurar los servidores Exchange y los componentes de los que disponen (bases de datos, protocolos y administración de registro de mensajería, por ejemplo). Dentro de esta opción de menú, podemos definir los servicios activos (POP3, SMTP, etc.) y los grupos de almacenamiento de los servidores. Un grupo de almacenamiento es un contenedor para buzones y carpetas públicas. Por ejemplo, para modificar los parámetros de un servidor, debemos seleccionar el servidor, seleccionar las propiedades y establecer los parámetros de configuración que consideremos apropiados. Para un servidor de correo saliente (SMTP), podemos configurar parámetros como la forma de autenticación, el límite de los mensajes, etc.

▶ **Buzón**: administra las bases de datos de los buzones de los servidores.

▶ **Acceso de cliente**: gestiona las libretas de direcciones sin conexión, la función Microsoft Outlook Web Access y el acceso desde dispositivos móviles con Active Sync.

▶ **Transporte de concentradores**: permite listar todos los servidores con esta función y configurar los conectores de recepción SMTP de Exchange que no son la puerta de enlace por la cual reciben los mensajes.

▶ **Mensajería unificada**: nos permite configurar aspectos relacionados con mensajes de voz, de fax, correos electrónicos, etc., a los que tienen acceso los usuarios.

▶ **Configuración de destinatarios**: en esta sección, debemos definir y gestionar los destinatarios de correos electrónicos dentro de la organización.

Spam

La palabra spam**, o correo basura, se utiliza para englobar aquellos correos electrónicos no solicitados, no deseados o que proceden de remitentes desconocidos o anónimos. Por lo general, estos correos son del tipo publicitario enviados en grandes cantidades, de forma masiva. El spam incrementa los costos de mantenimiento de una red y el tráfico en ella, perjudicando su rendimiento y estabilidad. Para evitar correos no deseados, los servicios de correo ponen a disposición del usuario filtros de contenido que automatizan el proceso de acumulación y eliminación de estos.**

Un destinario es un objeto o entidad que puede recibir un correo electrónico desde Exchange. Incluye usuarios, contactos, grupos y otros elementos. Desde aquí, podemos administrar grupos de distribución de Exchange, por ejemplo. Esta opción de menú posee las siguientes secciones:

- **Buzón**: permite administrar los usuarios de los buzones y los buzones de los recursos (salas y equipos). Dentro de esta sección, podemos habilitar la mensajería unificada y los dispositivos móviles.
- **Grupo de distribución**: gestiona los grupos de distribución de correos.
- **Contacto de correo**: nos permite gestionar todo lo relacionado con contactos de correo.
- **Buzón desconectado**: desde este punto, podemos ver y habilitar buzones.

Cuadro de herramientas

Además, Exchange cuenta con un conjunto extra de herramientas para optimizar su funcionamiento.
Para comenzar a utilizar Exchange, es necesario recopilar información acerca de la organización huésped. Primero, debemos seleccionar la opción de menú Microsoft Exchange Local, presionamos el botón derecho del mouse y, luego, seleccionamos la opción Recopilar datos de mantenimiento, de la organización del menú que se despliega. A continuación, presionamos el botón Siguiente y, por último, el botón Recopilar. De ahora en adelante, en el menú principal de administración de Exchange se debería reconocer correctamente el servidor junto con sus bases de datos.

Active Directory

Cuando instalamos Exchange, este se integra totalmente con Active Directory. Luego de la instalación, cuando creamos un usuario nuevo, su cuenta de correo electrónico se crea en forma automática. Desde la pestaña Configuración de destinatarios, si seleccionamos la opción Propiedades, podemos acceder a los siguientes ítems de configuración:

- **Direcciones de correo electrónico**: nos permite consultar las direcciones electrónicas del usuario, agregar nuevas direcciones o modificar las existentes.
- **Configuración del buzón**: realiza la administración de los registros de mensajería y las cuotas de almacenamiento de un usuario.
- **Características del buzón**: podremos habilitar o deshabilitar servicios y características del buzón de un usuario, como por ejemplo, protocolos que utiliza, Outlook Web Access, Exchange ActiveSync, POP3, etc.; y consultar sus propiedades.
- **Configuración de ujo de correo**: nos permite configurar opciones relacionadas con la entrega de mensajes (permisos delegados y dirección de reenvíos), restricciones de tamaño de mensajes y restricciones de entrega.
- **General**: permite asociar nombres simples a cuentas de correo, ocultar usuarios de listas de distribución, y consultar y editar permisos de acceso de buzón, entre otras cosas.

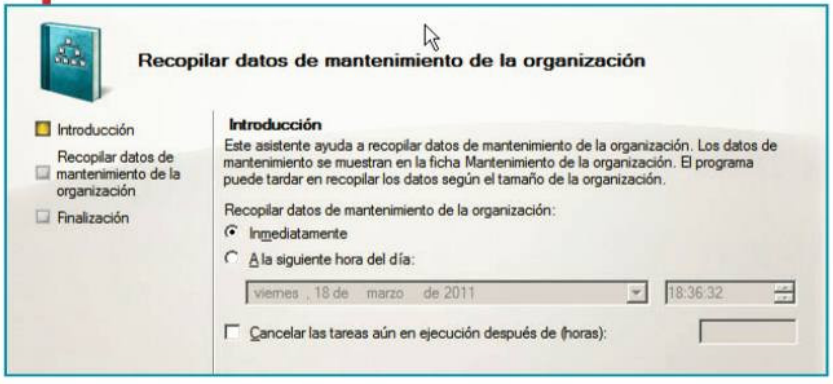
Webmail

Otra opción muy útil de configuración consiste en configurar Exchange para que los usuarios puedan acceder a sus cuentas de correo a través de la Web, utilizando un navegador. Primero, debemos corroborar si el servicio se encuentra activo (si no, debemos activarlo). Dentro de la Consola de administración de Exchange, ingresamos a la Configuración de servidor, seleccionamos la opción de menú Acceso de cliente y luego el servidor que utiliza (se encuentra listado). Solo nos resta consultar la pestaña Outlook Web Access.

Filtrado inteligente de mensajes de Exchange

Para evitar que ingresen mensajes no deseados, por lo general spam, podemos utilizar la herramienta **Content Filter Agent**. Esta nos ayudará a determinar la probabilidad de que los correos entrantes sean o no deseados. Utilizando esta probabilidad, podemos elegir bloquear los correos en la puerta de enlace, en el almacén de correos o en el buzón.
Si no se encuentra instalada, debemos posicionarnos en la opción de menú Inicio/Programas/Exchange y ejecutar la aplicación Exchange Management Shell. Luego, dentro de la aplicación antes mencionada, nos posicionamos en la ruta C:\Archivos de programa\Microsoft\Exchange Server\V14\Scripts y ejecutamos la sentencia install-AntispamAgents.ps1 para instalar una serie de componentes que nos permiten lidiar con el spam. Entre ellos, se encuentra Content Filter Agent. Luego de la instalación del componente, reiniciamos el servicio de transporte. Content Filter Agent está disponible para configurar en la Consola de administración en las secciones Configuración de la organización y Transporte de concentradores. Para acceder al componente, seleccionamos la opción Filtro de correo no deseado. ■

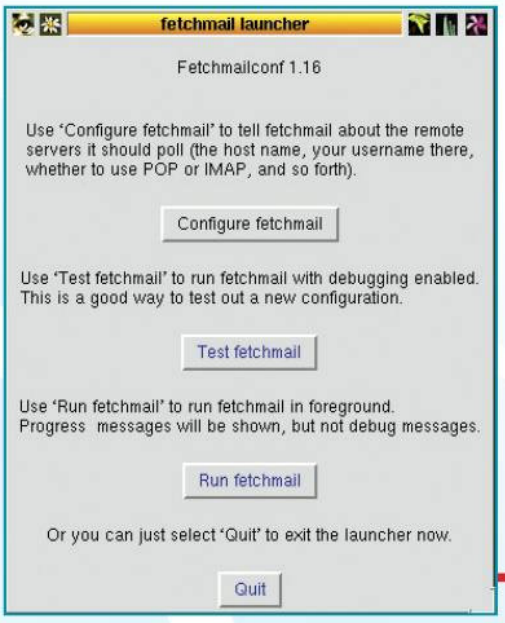
Las listas Robinson o ficheros de exclusión son registros de personas que no desean recibir publicidad por ningún medio, incluidos los e-mails.



Servidor de correo en Linux

El mundo GNU/Linux cuenta con gran cantidad de sistemas de correo. Lograremos un completo servidor integrando todas sus funciones.

Existen numerosas soluciones que integran las distintas funcionalidades requeridas en un servidor de correo moderno. Algunas de estas funcionalidades son: transferencia de e-mails (**MTA**, **Message Transfer Agent**), recupero de e-mails (**MRA**, **Mail Retrieval Agent**), procesamiento de e-mails y listas (**MLM**, **Mail List Manager**), antispam, antivirus, webmail y, por último, interfaz de administración. Todos estos componentes, cuando son comercializados, suelen integrarse como un único producto y mostrados a través de una única interfaz. En el mundo Linux, debemos ser nosotros quienes instalemos e integremos todos estos servicios.
En estas páginas, nos centraremos en las tecnologías disponibles en ambientes Linux; veremos las características de cada producto, su instalación y su configuración.



Interfaz gráfica de **Fetchmail** para configuración y pruebas. Facilita la administración del servicio.

MTA

Los **MTA** más comúnmente utilizados en Linux son **Postfix**, **Qmail** y **Sendmail**. Sendmail (**sendmail.com/sm/open_source**) es un ruteador de e-mails que soporta numerosos protocolos para envío de e-mails, como por ejemplo SMTP. Fue desarrollado por Eric Allman en los años 80. Actualmente, Sendmail cuenta con una versión open source mantenida por la comunidad y una versión propietaria mantenida por Sendmail Inc. Para instalarlo, descargamos el código fuente en un directorio y ejecutamos: `./buildinstall`. Esto deberá crear los binarios en `/usr/sbin` y crear links desde `/usr/bin/newaliases` y `/usr/bin/mailq` a `/usr/sbin/sendmail`. Luego de la instalación, es necesario configurar `/etc/mail/sendmail.cf` y el resto de los archivos requeridos. La configuración de Sendmail es compleja, por lo que será necesario utilizar la guía de instalación.

▶ **Postfix** (**postfix.org**) fue desarrollado originalmente en 1997 por Wietse Venema en los laboratorios de IBM como un reemplazo de Sendmail. Se distribuye bajo licencia IBM Public License. Postfix posee una limitada cantidad de funciones, por lo que deben utilizarse otros productos que completan la funcionalidad del servicio. Posee soporte para los estándares SMTP, LMTP, encriptación STARTTLS, autenticación SASL, encapsulamiento MIME, notificaciones DSN, IPv4 e IPv6. Para la instalación, utiliza GCC como compilador por defecto. Desde el directorio fuente, simplemente ejecutamos `make`. Si este es exitoso, debemos proceder con el resto de la instalación. Si el SO cuenta con una versión de Sendmail instalada, debemos realizar algunas modificaciones para que Postfix sea el servidor por defecto. Creamos el usuario en `/etc/passwd`

```
postfix:*:12345:12345:postfix:/no/where:/no/shell
```

y los grupos en `/etc/group`

```
postfix:*:12345:
postdrop:*:54321:
```

A continuación, ejecutamos `makeinstall` desde root, que, en forma interactiva, nos guiará por la instalación. Por defecto, los archivos de configuración de Postfix se encuentran en `/etc/postfix`. Los archivos más importantes son `main.cf` y `master.cf`; root debe ser dueño de estos archivos.

▶ **Qmail** (**qmail.org**), escrito por Dan Bernstein, es tal vez el segundo MTA más utilizado en Internet. Es considerado un servicio pequeño, rápido y seguro. Para su instalación, debemos ejecutar los siguientes comandos, reemplazando `x.yy` por la versión utilizada:

```
mkdir -p /usr/local/src
```

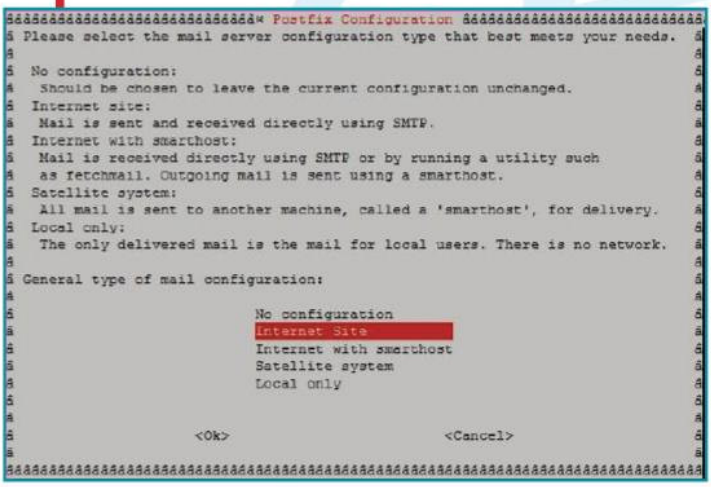
```
mv netqmail-x.yy.tar.gz ucspi-tcp-x.yy.tar.gz /usr/local/src
mkdir -p /package
mv daemontools-x.yy.tar.gz /package
chmod 1755 /package
```

Luego, desempacar y compilar (es necesario un compilador C) ejecutando `makesetupchecky ./config`. Para información detallada de instalación, podemos recurrir a **lifewithqmail.org**.
Los agentes para búsqueda de e-mails en un servidor remoto más populares son fetchmail, getmail y fdm. Originalmente, **fetchmail** (**fetchmail.berlios.de**) fue desarrollado por Eric Raymond en 1996, tomando como base a popclient. Soporta todos los protocolos disponibles: POP2, POP3, RPOP, APOP, KPOP, IMAP, ETRN y ODMR. Incluso, soporta IPv6 e IPSEC.
En cuanto a la autenticación de los clientes, soporta APOP, KPOP, OTP, CompuServe RPA y Microsoft NTLM, entre otros. Se lo puede configurar para soportar encriptación end-to-end vía túneles SSH.
Para instalar fetchmail desde una terminal, ejecutamos desde el usuario root los siguientes comandos:
`apt-getinstallfetchmail` (Debian y Ubuntu)
`yuminstallfetchmail` (CentOS y Fedora)
`pacman -S fetchmail` (Arch Linux)
`emergefetchmail` (Gentoo)
Una vez instalado, es posible configurarlo utilizando el entorno gráfico con el comando `fetchmailconf`.

▶ **Getmail** (**pyropus.ca/software/getmail**), desarrollado por Charles Cazabon en 1998, se presenta como un reemplazo de fetchmail por ser flexible, seguro y confiable, y por su facilidad de uso e instalación. Soporta POP3, POP3-sobre-SSL, IMAP4, IMAP4-sobre-SSL, SDPS (extensión de POP3). Para instalarlo, debemos instalar Python, luego descargar el tarball, desempacarlo en el directorio deseado y ejecutar: `python setup.py install`.
La ruta por defecto de instalación es `/usr/local/` o `/usr/`.
Tengamos en cuenta que no es necesario realizar ninguna configuración sobre nuestro MTA, ya que getmail escribe directamente sobre los archivos maildir, mboxrd o MDA.

▶ **Fdm** (**fdm.sourceforge.net**) entrega e-mails de diversas formas dependiendo de las reglas definidas por el usuario.
El e-mail puede ser recuperado desde el standard input (stdin), IMAP, POP3 o desde maildirs. Puede ser filtrado basado en expresiones regulares, tamaño, fecha, o la salida de un comando de consola. Cada correo puede ser reescrito por un proceso externo, dropeado, dejado en el servidor o entregado a buzones con formato maildir, mbox, a un archivo o tubería (pipe), o a cualquier combinación de estos. Está diseñado para ser liviano y con una configuración compacta. Originalmente, se pensó para usuarios individuales, pero puede ser configurado para un entorno multiusuario. En estos casos, usa segregación de permisos para minimizar la cantidad de código ejecutándose como root.
Para su instalación, descargamos el tarball, lo descompactamos y ejecutamos `make`. Luego, ejecutamos `makeinstall` para que sea instalado en la ubicación por defecto (`/usr/local`).

La interfaz de configuración interactiva de **Postfix**. Permite configurar el servicio rápida y fácilmente.



Para no utilizar root, es recomendable crear un usuario: `useradd -u 999 -s /bin/nologin -d /var/empty -g=uid _fdm`.
Debemos examinar el archivo de configuración que se encuentra en `/etc/fdm.conf` y editarlo según las necesidades.

MLM

Los list managers se encargan de recibir un correo y distribuirlo a un número determinado de receptores. Este tipo de servicios permiten que las personas se suscriban y desuscriban a distintas listas de interés. Los más populares son Ecartis, Mailman, Majordomo, Procmail SmartList.

EL SERVICIO MTA ES EL ENCARGADO DE RECIBIR CORREO, ALMACENARLO EN EL BUZÓN CORRECTO, Y ENVIAR E-MAILS HACIA OTROS DOMINIOS.

▶ **Majordomo** (**greatcircle.com/majordomo**) es tal vez el más popular de todos. Está desarrollado en lenguaje de scripting Perl, lo que lo hace algo ineficiente. Pero Perl es muy poderoso sobre todo para procesamiento de texto.
El hecho de que esté desarrollado utilizando scripting permite que el código sea extendido en cada implementación. Para su instalación, debemos desempacar el tarball, crear el usuario y grupo (reemplazar `x.yy` por la versión descargada):
`majordomo:x:16:16:Majordomo LM:/usr/local/majordomo-x.yy:`
`majordomo:*:10883:0:88888:7:::`
Ejecutamos `makewrapper`, `makeinstall` y `makeinstall-wrapper`.

▶ **Ecartis** (**ecartis.org**) fue desarrollado por Rachel Blackman en 1997, pero antes se conocía como Listar. Posee algunas funcionalidades no encontradas en majordomo.

Una de sus características sobresalientes es que se carga en el sistema como un módulo. Posee una interfaz web para administración de las listas y los miembros. Para instalarlo, debemos compilarlo utilizando GCC o EGCC; descompactamos el tarball. En el directorio elegido, ingresamos al directorio src y copiamos `Makefile.dist` a `Makefile`. Editamos su contenido para customizar lo necesario y lo salvamos. Luego, ejecutamos el comando `make`, en BSD tal vez sea necesario realizar `gmake`. Una vez instalado, debemos integrarlo con el MTA. Para Sendmail, la forma más sencilla es copiar la salida del script newlist.pl de Eclair en el subdirectorio `/etc/aliases` de Sendmail y, luego, ejecutar el programa newaliases de Sendmail. Para Postfix, también es posible copiar la salida de alias de Eclair en el archivo `default aliases` y luego ejecutar el comando `postaliases`.
En qmail, el método para agregar alias es completamente diferente a los otros dos. Debemos crear un archivo `.qmail-miLista` en el home directory del usuario qmail. Para esto, una vez posicionados en el homedir de qmail, ejecutamos el comando `echo "|/home/ecartis/ecartis -s miLista" > .qmail- miLista`.
No es necesario ejecutar un comando para recrear los aliases de qmail.

▶ **Mailman** (**gnu.org/software/mailman**), desarrollado principalmente en Python por Barry Warsaw, soporta almacenamiento, procesamiento automático, entrega, filtrado de contenido, spam, y más. Para su instalación, se requiere un compilador C (GCC) y el intérprete de Python. Debemos crear el usuario y grupo con los siguientes comandos:

```
groupaddmailman
useradd -c"GNUMailman" -s /no/shell
-d /no/home -g mailmanmailman.
```

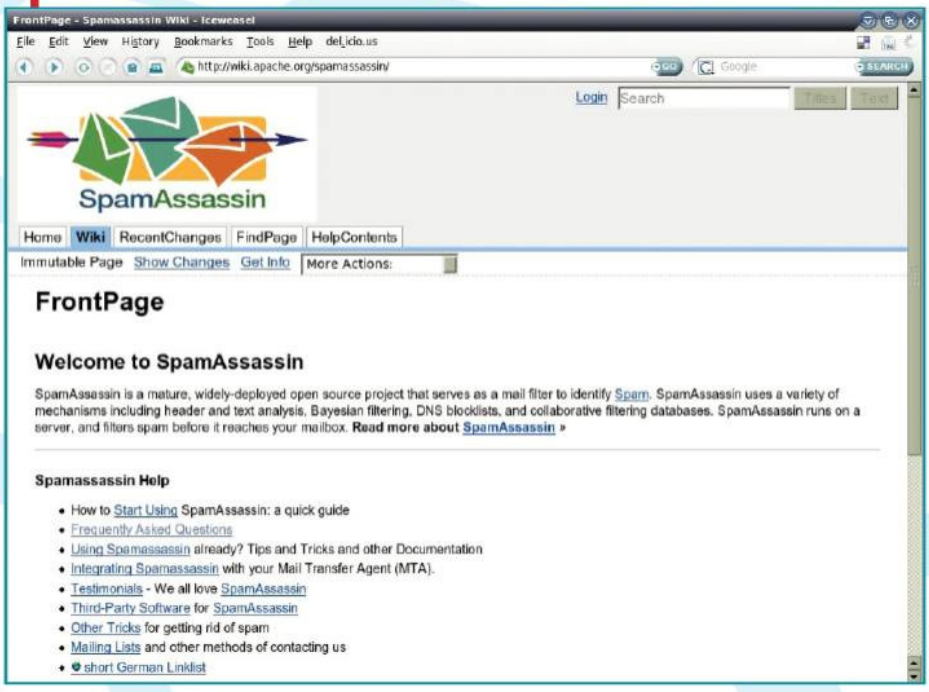
El directorio de instalación por defecto es `/usr/local/mailman`. Una vez descompactado el paquete, ejecutamos:

```
cdmailman-x.yy
./configure
makeinstall
```

Para obtener más detalles o en caso de encontrarnos con errores, podemos consultar la guía de instalación.

▶ **Procmail** y **SmartList** (**procmail.org**) integran una misma suite para administración de listas. Procmail puede ser utilizado para crear servidores de mail, listas, organizar el correo entrante en carpetas/archivos, preprocesar el correo, iniciar programas al recibir nuevos e-mails (por ejemplo para hacer un sonido) o reenviar algunos correos a alguien más en forma automática. SmartList se ejecuta sobre Procmail, y permite la creación y administración de listas, incluyendo la gestión automatizada de las suscripciones, desuscripciones, solicitud de ayuda, autorremoción de direcciones que generan mucho tráfico (spamers), un servidor de archivado (con soporte MIME), y más funcionalidades. Para realizar su instalación, descompactamos y ejecutamos los comandos `make` y `makeinstall`.

SpamAssassin es un proyecto open source maduro que realiza con eficacia el filtrado del correo basura.



Otros componentes

Otro componente fundamental de nuestro servidor es el webmail. Algunos de los más reconocidos son: Roundcube, Zimbra Collaboration Suite, phpGroupWare, Squirrelmail y Atmail.

▶ **Roundcube** (**roundcube.net**) presenta una interfaz muy atractiva similar a la de un cliente de correo de escritorio. Se encuentra disponible en más de 70 lenguajes. Soporta drag & drop, MIME, HTML, texto enriquecido, conexión con LDAP, corrector ortográfico y más. Requiere Apache u otros webservers, PHP y MySQL u otras bases de datos. Para su instalación, debemos extraer el tarball dentro de la estructura del sitio web en Apache. Luego es necesario crear la base de datos en MySQL. El resto de la instalación y configuración se completa accediendo al sitio web con un asistente que nos guía paso por paso.

▶ **Zimbra** (**zimbra.com**) es una suite de colaboración con e-mail, administración de contactos, calendarios de grupo y mucho más. Posee una versión libre y una paga. Zimbra fue adquirido en 2010 por VMWare.

▶ **phpGroupWare** (**hpgroupware.org**) es una suite de colaboración (groupware) multiusuario desarrollada en PHP, que permite administrar contactos, enviar y recibir e-mails, compartir calendarios, administrar y compartir contenido web y documentos, y administrar proyectos.

▶ **Squirrelmail** (**squirrelmail.org**). desarrollado en PHP4, utiliza únicamente HTML (sin JavaScript) para garantizar la compatibilidad entre navegadores. Tiene pocos requerimientos y es fácil de configurar e instalar. Tiene una funcionalidad completa, como por ejemplo soporte MIME, libreta de direcciones y manipulación de carpetas.

▶ **Atmail** (**atmail.com**) es un cliente webmail con soporte para conexión POP3/IMAP con interfaz Ajax, lo que permite una interfaz moderna. Además, incluye múltiples plantillas para cambiar el aspecto según las preferencias del usuario. Puede integrarse con Postfix y Sendmail.

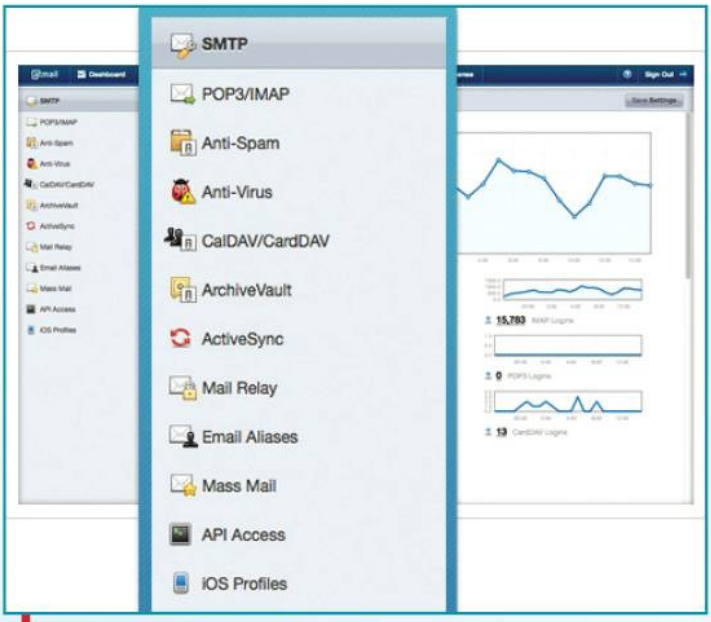
Administración

Para facilitar la tarea del administrador, existen diversas interfaces que nos permiten administrar el servicio de correo. Algunas de las más reconocidas son Korreio, RavenCore Hosting Control Panel, Webmin y Tequila.

▶ **Korreio** (**korreio.sf.net**) se trata de una aplicación que posee una interfaz gráfica para administración de sistemas de e-mails. Posee varios módulos independientes para administrar Postfix, LDAP, Cyrus-IMAP y Cyrus-Sieve.

▶ **RavenCore Hosting Control Panel** (**sourceforge.net/projects/ravencore**) posee interfaz web y utiliza dovecot para descargar correo POP3/IMAP; permite configurar sistemas multiusuario y multidominio con autenticación SASL. También, puede integrarse con aplicaciones como SpamAssassin y ClamAV para escaneo de spam y virus.

▶ **Webmin** (**webmin.com**) posee una interfaz web para administración de servidores Linux. Permite administrar bases de datos, usuarios, DNS, compartir archivos, y mucho más. Posee un módulo de configuración para Postfix.



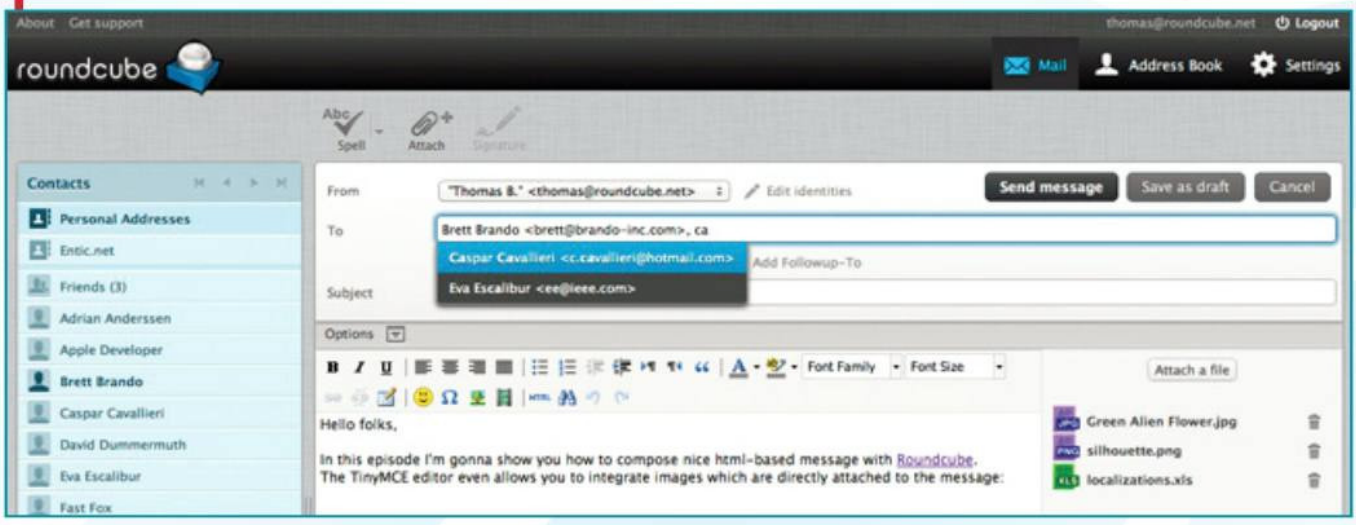
Funcionalidades del webmail **Atmail**. Permite integrar las opciones de antivirus, antispam y dispositivos móviles.

▶ **Tequila** (**loomsday.co.nz/development?id=tequila**) es una interfaz web que permite administrar sistemas Postfix incluyendo reenvío de e-mails y autorrespuesta.

Seguridad

Hoy en día es prácticamente imposible hablar de e-mails sin pensar en la necesidad de establecer una solución para el control de virus y spam. Para esto, podemos utilizar **SpamAssassin**, **Xamime**, **ClamSMTP**, **spampd** y **Vexira** entre otros. SpamAssassin (**spamassassin.apache.org**) es uno de los más famosos antispam en el mundo Linux. Encapsula la lógica en una API abstracta que puede integrarse con variados sistemas de correo, por ejemplo Procmail, Sendmail, Postfix, qmail, y muchos más. ■

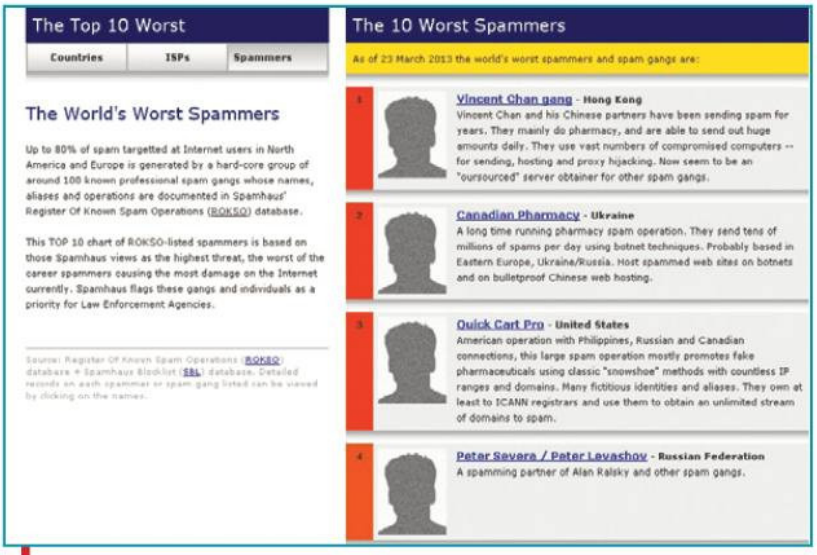
Roundcube presenta una interfaz muy atractiva y amigable. Los controles Ajax facilitan su uso.



Spam

El spam, ese enemigo cercano que nos ha mantenido preocupados, parece haber sucumbido ante las técnicas de filtrado modernas.

Pocas palabras hemos visto tantas veces en nuestro buzón de correo electrónico como **spam**. Ya sea en los encabezados de los e-mails, en la carpeta donde se almacenan y se filtran, en las opciones del cliente de correo, el spam, o correo basura, nos acompaña hace más de una década, habiendo pasado por varias etapas. Podemos definir spam específicamente como mensajes de correo electrónico que se han enviado de manera **masiva** y se han recibido además de manera **no solicitada**. Estas dos cualidades simultáneas son las que permiten determinar si un mensaje se trata de spam o no. De hecho, en caso de que la definición permita la duda, se puede contrastar un correo con el hecho de que la identidad personal del receptor y el contexto sean irrelevantes, lo cual determinará definitivamente que se trata de correo basura. Estos mensajes se envían en general a modo de **publicidad** de productos y servicios que, muchas veces, son **ilegales**.



www.spamhaus.org muestra un ranking de los spammers más temidos.

Origen

El origen de la palabra aplicada al mundo de la informática es un tanto incierto, pero de todas las versiones la que pareciera más real es la que cuenta la siguiente historia. Una empresa norteamericana, llamada **Hormel Foods**, tenía un producto denominado **Spiced Ham** (algo así como 'jamón con especias') lanzado al mercado en el año 1937; se trataba básicamente de carne enlatada, que contaba con conservantes y especias, y podía mantenerse por mucho tiempo antes de ser consumido. Durante la Segunda Guerra Mundial, el Spiced Ham se utilizó para alimentar a las tropas soviéticas y británicas, dada su versatilidad y duración. Tal fue su éxito que, desde 1957, comenzó a venderse en latas con sistemas de apertura fácil para evitar el uso de abrelatas tradicionales.

Años más tarde, el grupo cómico inglés **Monty Python** utilizó el nombre en un sketch que realizaba en el programa **Flying Circus**, en el que una pareja en un bar pedía comida y, en el menú, encontraba que todos los platos que había tenían spam, desde huevos con spam, hasta salchichas con spam, jamón con spam, y así todo. De esta forma, el mozo les leía el menú mientras ellos escuchaban repetidamente la palabra *spam*.

Ya en los años 80, se adoptó el término para describir el comportamiento abusivo de algunos usuarios que frecuentaban los primeros **BBSs**, que repetían "spam"

Evolución del spam

Durante los primeros años del siglo XXI, el spam representaba un gran problema debido al enorme consumo de ancho de banda que demandaba su descarga, especialmente cuando las conexiones promedio eran de línea telefónica (Dial-Up). Con el tiempo, las conexiones de banda ancha hicieron que solo fuera una molestia por mezclarse entre los mensajes reales. Hoy en día, con una buena configuración de filtrado, un tiempo de entrenamiento y un buen servicio de e-mail, ya casi podemos considerarlo un problema menos.

una gran cantidad de veces para lograr que el texto de otros usuarios saliera de la pantalla por medio del **scrolling** del texto. De hecho, en los primeros servicios de chat, como **PeopleLink** y **Online America** (posteriormente **America Online**) lo que se repetía eran directamente frases del mencionado sketch de Monty Python. Más allá de la historia, lo cierto es que **no representa una sigla**, y que tuvo diferentes etapas, comenzando por ser un verdadero flagelo, hasta casi estar resuelto en determinados niveles.

Funcionamiento

Una de las primeras preguntas que surgen cuando se habla de spam es cómo los spammers (quienes envían spam) obtienen las direcciones de e-mail para enviarles sus correos basura. Los spammers consiguen armar grandes bases de datos de distintas maneras, a saber: la primera es utilizando algún tipo de **malware** que, al infectar un sistema, se replica **enviándose por e-mail** a los contactos de la **libreta de direcciones** de la persona afectada (ya sea en servicios de webmail como en correo recibido en la PC). Cuando las demás personas están infectadas, repite el proceso y va recopilando direcciones en los sistemas infectados. Otra manera es mediante el **engaño** a los usuarios, utilizando **cadenas de correo** referidas a alguna causa noble, como la lucha contra el cáncer, pedidos de solidaridad, supersticiones varias, onomásticos y demás. En estos correos, se incita al usuario a **reenviar voluntariamente** el e-mail a sus contactos, de modos que entre dichos contactos aparezca quien envía el e-mail originalmente, y este pueda ver todos los reenvíos que se realizan, obteniendo así direcciones de contactos de los contactos. Esto se podría evitar si quienes desean reenviar cadenas de e-mails utilizaran la opción de envío con copia oculta (**BCC** o **Blind Carbon Copy**) para que los receptores no puedan ver a quién más se le está enviando la cadena en cuestión. Otra forma de recopilar direcciones es por medio de la compra de **listas comerciales**, que son **bases de datos** provistas por las empresas y organizaciones que de por sí recaban los datos por otra cuestión, ya sea por motivos de marketing, estudios de mercado, etcétera. Estas bases de datos suelen filtrarse desde dentro de las organizaciones, por medio de empleados que, al tener acceso, las utilizan para comercializar, en tanto que dicho comportamiento por supuesto no está aprobado por la empresa. Una manera bastante más evidente de obtener direcciones de correo electrónico es la simple **búsqueda en Internet**. Tanto en foros como en blogs, redes sociales y otros sitios, la gente coloca sus direcciones de e-mail como parte de la información personal de contacto, sin saber que muchas veces los spammers recolectan esa información con programas robot que recorren la red en su búsqueda. Una forma sencilla de evitar esto es simplemente no dejar nuestra dirección de e mail, pero en caso de que sea necesario, existen escrituras alternativas como **nombre [at] dominio.com** o algo similar para representar la arroba, que es el carácter que normalmente los robots virtuales intentan detectar a la hora de determinar si se ha encontrado una dirección de e-mail. Otros, especialmente en sitios personales, lo evitan colocando el e-mail **en forma de gráfico**. La última de las técnicas clásicas del spammer para obtener direcciones válidas es tomar los dominios más importantes de los correos gratuitos, como **Hotmail** (**Outlook**), **Gmail**, **Yahoo!**, **AOL**, **GMX** y otros, y generar nombres de usuario que se comprobarán contra el servidor de correo solicitando el envío a esa dirección.

Ranking de los 10 ISPs más generadores de spam en el mundo.

EL SPAM ES MASIVO, NO SOLICITADO E INDEPENDIENTE DE LA IDENTIDAD DEL RECEPTOR.

El servidor responderá afirmativamente en caso de que la cuenta exista, y el spammer no le enviará la cuenta, sino que guardará la información en la base de datos como cuenta válida. De esta forma, se explota la posibilidad de que, en dominios muy numerosos, utilizados por millones de usuarios, existan **nombres comunes** y sus combinaciones con números, apellidos, etc. Esta probabilidad es fácil de comprobar al querer sacarnos una nueva cuenta de correo, cuando casi todos los nombres que escribimos ya están previamente registrados y no podemos utilizarlos por tal razón. El spammer aprovechará eso para deducir direcciones válidas y crear más listas de usuarios.

Infraestructura

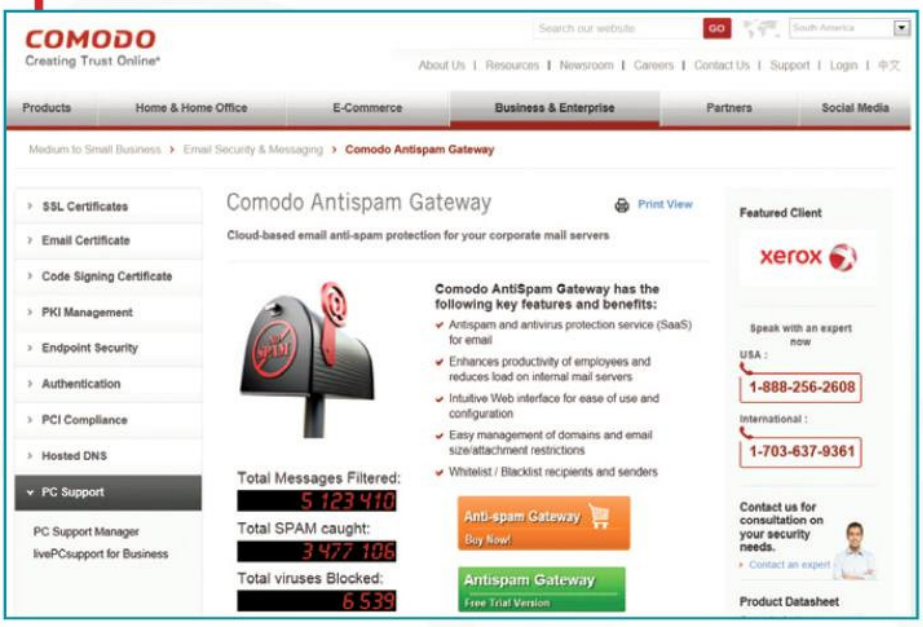
Por otra parte, el spammer requiere de una infraestructura en particular para el envío de miles de millones de mensajes, ya que no puede realizarlo desde una conexión hogareña o comercial, pues el **ISP** la detectaría y la bloquearía justamente por envío de spam. Aquí es donde entran en juego los mecanismos de envío. Uno de los más básicos es **utilizar conexiones hasta saturarlas** y que sean bloqueadas para luego pasar a otra y saturarla, y así de manera sucesiva. Esto puede realizarse en especial desde conexiones **inalámbricas públicas o robadas** en sectores donde se encuentran accesibles físicamente. En forma adicional, se puede utilizar el máximo potencial de las **direcciones IP** y las conexiones de banda ancha sin que se lleguen a bloquear por la saturación en el uso del servicio, pero es una tarea más compleja para el spammer.

Otra técnica consiste en escanear grandes rangos de direcciones IP de Internet en busca de servidores de correo electrónico mal configurados, que permitan realizar lo que se llama **Open Relay**, o envío de correo sin necesidad de autenticación por parte del usuario, es decir, sin que se precise una cuenta en ese dominio o sistema. Si bien este problema en los servidores de correo ha disminuido con el tiempo, muchas veces ocurre que, por algún descuido, queda alguno mal configurado y, por el tiempo que se le permite hasta su bloqueo, será utilizado por el spammer desde el momento inmediato en que lo detecte.

Actualidad

Durante los últimos años, se ha dado una tendencia creciente en el envío de spam de una manera diferente a las tradicionales antes descriptas, y es mediante el uso de **botnets** o redes de **computadoras zombies**. Estas se encuentran infectadas con algún tipo especial de malware que las hace formar parte de la misma red, y permiten ser controladas en forma remota y centralizada por un administrador con fines maliciosos. Uno de los principales servicios que prestan comercialmente (de manera **ilegal**, claro está) las botnets es el del envío de spam, y esto radica en que se aprovechan las conexiones a decenas de miles de sistemas para que sean estos los que realicen el envío, de forma que se haga descentralizadamente y, a cada uno, le corresponda una pequeña porción de la lista de millones de envíos. Esta técnica puede incluir el hecho de forzar el envío del spam a través del sitio del webmail al que el usuario accede, en el caso de que no cuente con un cliente local instalado y configurado.

Comodo Antispam Gateway ofrece una solución antispam por software basada en la nube.



Enfrentar el spam

Existen una serie de contramedidas que se pueden tomar para enfrentar el spam, y todas dependerán del nivel en el que se quieran aplicar. Por ejemplo, una buena idea es contar con una **dirección válida** personal, pero **especial para recibir spam**, la cual sabemos que podemos utilizar para registrarnos en sitios sin preocuparnos de que nos la llenen de publicidad, pero que a la vez podamos acceder en el caso de que nos envíen algún link para registración o similar.

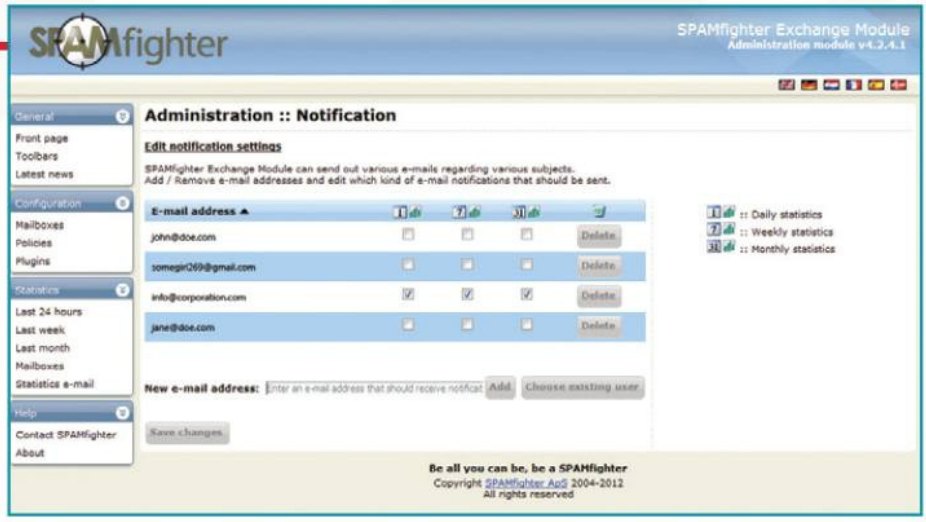
EN LA ACTUALIDAD, EL ENVÍO DE SPAM HA CRECIDO GRACIAS AL USO DE BOTNETS.

También podemos contar con direcciones temporales, pero nos encargaremos de ese tema más adelante.

Una contramedida más técnica y de implementación a gran escala es el uso de **listas negras** de direcciones. Estas listas deben actualizarse con alta frecuencia, dado que las direcciones pueden variar constantemente, y constituyen uno de los mecanismos principales sobre los cuales se basa el filtrado de spam actual a nivel de ISPs y de grandes proveedores de servicios de correo. Esta técnica, sin embargo, no suele ser muy implementada por el usuario final, ya que existen otras más eficientes para ello.

Entre las técnicas que pueden ser implementadas por el usuario en su software cliente, se encuentra el uso de **filtros bayesianos**. Estos filtros implican el uso del **teorema de Bayes**, utilizado ampliamente en estudios de **probabilidad y estadística**, para deducir qué probabilidad hay de que un mensaje sea spam, considerando que posee una cierta cantidad de palabras que aumentan o disminuyen dicha probabilidad. Entonces, existirá una lista

Spamfighter es un potente antispam gratuito para **Mozilla Thunderbird** y **Microsoft Outlook**.



de **palabras prohibidas** o de alto nivel de probabilidad de que representen un spam o se encuentren en él, y se analizará contra ella cada mensaje que arribe. Cuando llegue un nuevo correo, se analiza el contexto y se calcula la probabilidad de que sea spam, teniendo en consideración tanto lo bueno como lo malo. Algunas palabras reducirán mucho la probabilidad, y otras la incrementarán.

Otras técnicas más específicas incluyen la recepción con **autorización explícita**, ya sea mediante el uso de firma digital o algún otro sistema de autenticación, con el problema inherente de que también reduce la funcionalidad del sistema, por quedar fuertemente restringido.

Por último, debemos mencionar que prácticamente todo el software y hardware comercial **antispam** (basado en especial en el análisis bayesiano) suele permitir al usuario tomar decisiones sobre mensajes dudosos, o quitar del filtrado los **mensajes válidos**, de manera que el sistema puede ir aprendiendo a medida que se utiliza, en función de las preferencias particulares de cada usuario. Esto nos lleva a concluir que no existen dos sistemas de filtrado iguales, ya que lo que es spam para una persona, quizás no lo es para otra, y viceversa.

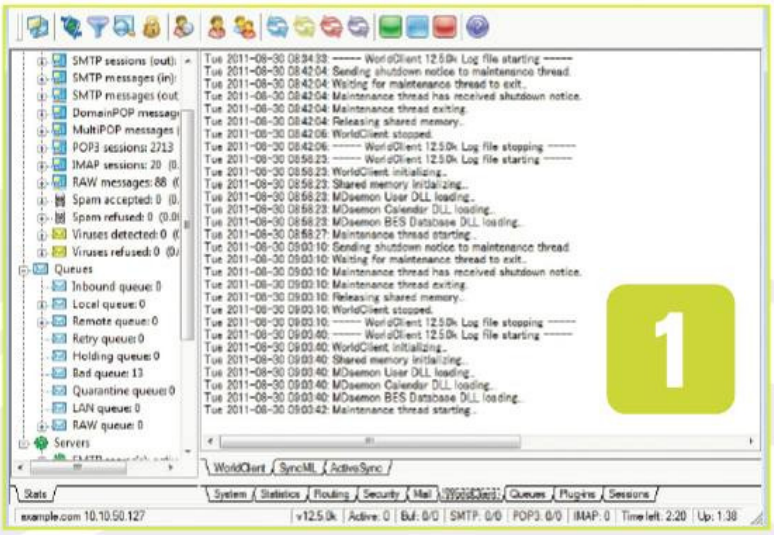
El spammer, por supuesto, contará con una serie de contratécnicas y trucos para evitar que los mecanismos utilizados por los filtros antispam sean efectivos, y estas técnicas son de lo más variadas. Un ejemplo es el uso del **idioma nativo** del receptor, lo cual puede deducirse a veces por el país en el que está alojado el dominio, o colocar datos aleatorios (o específicos quizás) en el campo **From** (de) de manera que pueda ir variando, o contar con un **Subject** (asunto) **amigable** para que tiente al usuario a abrirlo. Además, aprovechando las características comunes de los correos actuales, cuya gran mayoría admite (salvo configuración explícita) el uso del **lenguaje HTML**, se puede manipular dicho lenguaje para que muestre o no muestre ciertas cosas, o que incluya imágenes en vez de palabras para que no puedan ser fácilmente detectadas por el filtro de texto (basado en principio en texto escrito en alguna codificación (**encoding**) como **ASCII**, **UNICODE**, etc. Por supuesto que siempre se intentará codificar también las URLs a las que apunte el mensaje, para que no puedan ser leídas y bloqueadas con facilidad.

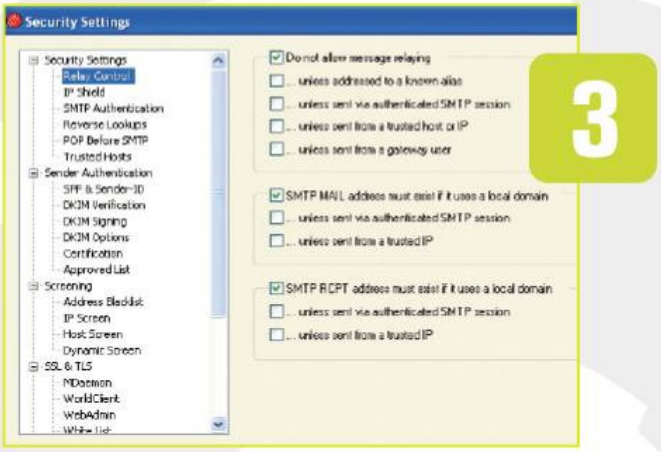
En cuanto a los métodos más alternativos, el spammer utiliza algunos **trucos visuales** o **patrones**, como por ejemplo, la escritura con un espacio entre letras, o con un punto entre letras de una palabra, de modo que para el filtro la palabra **s.e.x.o** no significaría lo mismo que **sexo** y tal vez lo engañaría, pero el usuario que lo lee podría entender de qué se trata sin problemas. La idea en todos los casos es **engañar al filtro**, pero que la información permanezca visible y comprensible para el usuario. Una técnica algo más sofisticada, por no decir de guerrilla, es el agregado en el mensaje de **palabras válidas** para confundir al filtro, que reduzcan la posibilidad de que sea considerado spam al ser analizado, como ser el nombre de la persona, o datos aleatorios que no contengan las palabras clave que suelen ser las que aumentan la probabilidad de que lo sea. ■

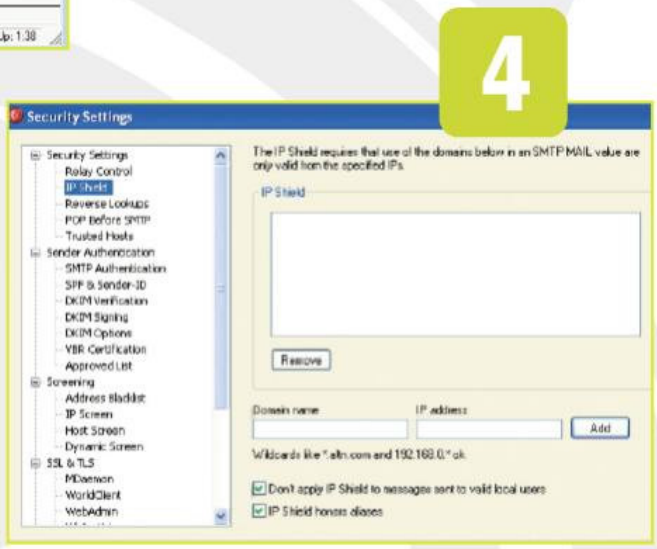
La empresa Barracuda Networks provee **Appliances antispam** para combatir el problema.

Open Relay

Esta función permite que el servidor sea utilizado como server de envío de spam. En estas páginas, aprenderemos a desactivar esta función.





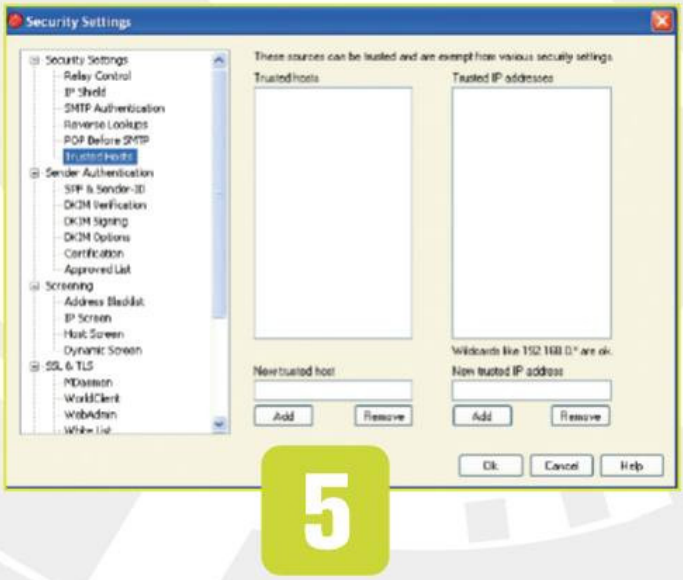


1 Logueados en el servidor donde está instalado el servicio **MDaemon**, abrimos la interfaz administrativa. Allí se presenta la información sobre los e-mails procesados, los entregados, rechazados y los que se encuentran en cuarentena. La versión de referencia posee soporte para dispositivos BlackBerry.

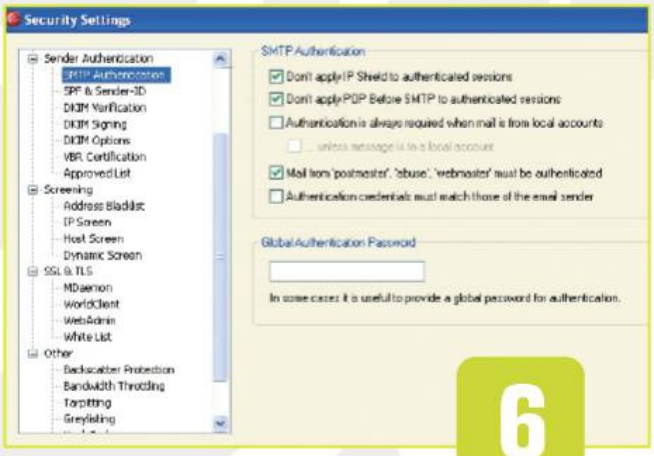
2 Desde la barra superior del menú de opciones, elegimos **Security** y, luego, **Security Settings** o la combinación de teclas **CTRL+S**. Desde esta opción, podremos acceder a todas las configuraciones que hacen a la seguridad del servicio del MDaemon Messaging Server.

3 En **Security Settings**, la primera opción es **Relay Control**. Debemos habilitar la casilla **Do not allow message relaying**, y las casillas **SMTP MAIL address must exist if it uses a local domain** y **SMTP RCPT address must exist if it uses a local domain**.

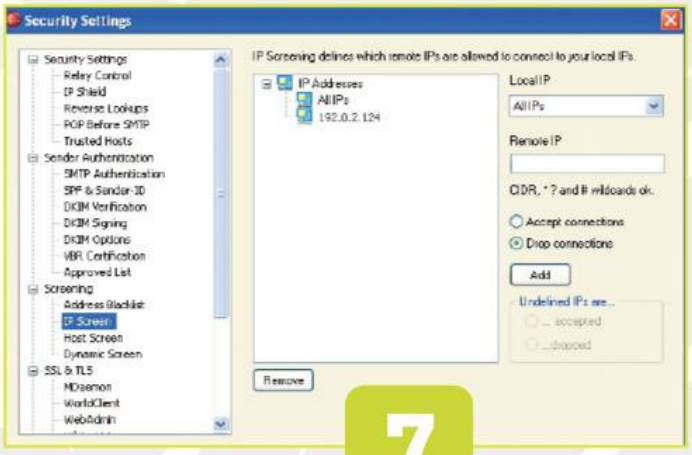
4 Con **IP Shield**, indicamos quién envía e-mails por cada dominio de MDaemon. Ingresamos el nombre del dominio y la IP o rango de red. Se recomienda activar **Don't apply IP Shield to messages sent to valid local users**.



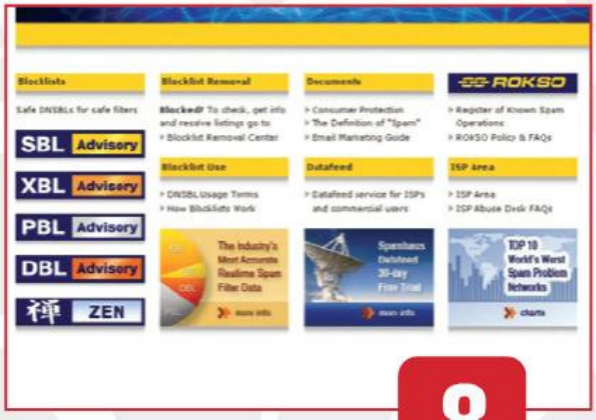
5



6



7



8

5 En la pantalla **Trusted Hosts**, debemos ingresar los hosts o redes confiables. Las redes que ingresemos podrán enviar e-mails sin restricciones. En este sitio, debemos ingresar todas las subredes que posee nuestra red. La opción de ingresar hosts es útil para equipos con IP dinámica.

6 En la pantalla **SMTP Authentication**, es posible exceptuar las reglas definidas en **IP Shield** para usuarios autenticados; así, evitamos tener que definir todas las redes internas de la organización. Es buena idea forzar la autenticación para cuentas locales.

7 En caso de recibir SPAM frecuentemente de un equipo o tener necesidad de bloquear servidores de e-mail, por ejemplo de competidores, es posible rechazar la conexión SMTP. Para esto, es necesario que definamos la IP del servidor remoto que deseamos bannear, y de esta forma, sus conexiones serán rechazadas.

8 Si nuestro servidor no es configurado apropiadamente para rechazar conexiones del tipo open relay, es probable que sea incluido en una lista negra. Muchos servidores de correo se configuran para rechazar dominios incluidos en listas negras, **spamhaus.org** es un DNSBL reconocido.

Usos alternativos del e-mail

Si bien el e-mail no ha sufrido cambios significativos en su tecnología, en la actualidad integra múltiples aplicaciones.

Si hacemos hincapié en la evolución de las distintas tecnologías de la información y la comunicación, veremos que la gran mayoría ha evolucionado sustancialmente desde su origen. Un ejemplo es la televisión, que, al comienzo era en **blanco y negro**, luego a **colores**, después se han mejorado los tubos de rayos catódicos, hasta que llegó el **plasma**, el cristal líquido (**LCD**) y posteriormente las pantallas de **LEDs**. La radio también sufrió cambios en sus dispositivos receptores, así como lo hicieron prácticamente todos los medios de comunicación, en especial durante los últimos treinta años.

Funcionamiento

El e-mail, sin embargo, pese a sus cumplidas tres décadas de vida, continúa operando exactamente **de la misma forma** en que lo hacía al comienzo, cuando el directorio completo de direcciones en el mundo podía resumirse en un volumen de un tamaño menor que una guía telefónica local. Esto, lejos de ser un estancamiento o síntoma de muerte prematura, denota la **robustez** del sistema, que ha permitido el envío de mensajes digitales a velocidades casi instantáneas por primera vez en la historia.

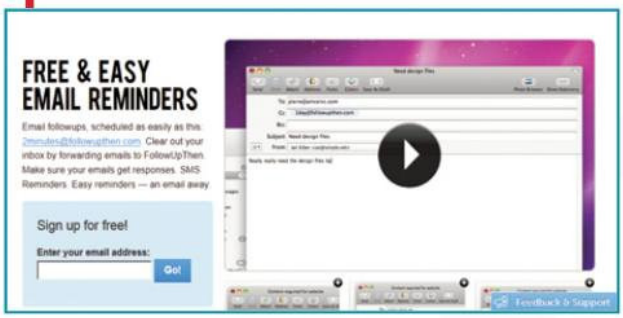
eMailTrackerPro es un servicio que permite realizar seguimiento de mensajes enviados.

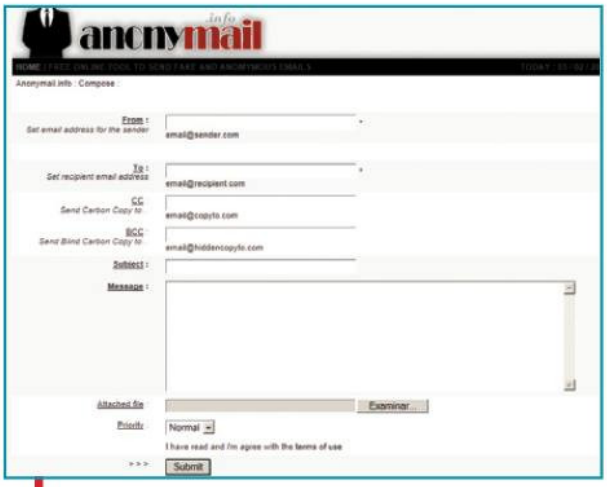
Muchos acusan al e-mail de no haber introducido funcionalidades novedosas o variar su idea principal, lo cual por cierto no ha sido tan así, ya que con el tiempo se han introducido los sistemas de **webmail**, el protocolo **IMAP** para mantener copias en varios lugares a la vez además del servidor, protocolos de seguridad para autenticación de usuarios y algunas otras características.

Usos alternativos

Uno de los **usos alternativos** del correo electrónico en la actualidad ha sido su aprovechamiento como **recordatorio de tareas**. Esta función la han implementado inicialmente los fanáticos de la **productividad personal**, y funciona de una manera muy simple: en el momento en que debemos recordar algo que hemos visto o leído, o algo que nos han dicho, o una serie de enlaces que encontramos navegando, o cualquier cosa que deseemos tener guardado, sacamos el Smartphone y nos lo enviamos por e-mail **a nosotros mismos**. Sí, a nosotros mismos. También se utiliza el envío desde la PC, para el caso que las personas quieran tener algo almacenado que después podrán acceder desde su móvil sin tener que ir nuevamente al sitio web, servicio online o aplicación que lo contiene. Un buen truco es manejar un **asunto característico** para poder filtrarlo luego, o identificarlo a primera vista entre el maremágnum de mensajes. Por lo general, se elige poner algo relacionado con el recordatorio,

FollowUpThen es un servicio que permite utilizar el e-mail como recordatorio programado.





Anonymail es un servicio que permite el envío de mensajes de e-mail anónimos, normalmente utilizado para diversión o con fines didácticos.

o bien una sigla universal, como **FMI** (**For My Information**) en contraste con la sigla utilizada en el lenguaje escrito **FYI** (**For Your Information**). Este uso ha tenido tan buen recibimiento que se han creado servicios online que, de manera automática, nos reenvían un e-mail a nuestra propia casilla un **determinado tiempo** después de recibido, configurable por nosotros, para que lo veamos al otro día o la semana siguiente, también como recordatorio. Incluso, el sistema se ha extendido al punto de que puede enviarse un mensaje también a otro usuario **luego de un tiempo definido**, ya sea para realizar el **seguimiento** de una tarea o como recordatorio.

Seguridad

Otro de los usos que todo especialista de seguridad conoce es la posibilidad de que pueda enviarse un mensaje **de forma anónima**. Esto no debe ser utilizado para fines ilegales ni de dudosa moral, pese a que su origen ha sido el mundo del **hacking**. Para esto, existen servicios online que permiten, sin registrarse, enviar un mensaje a cualquier usuario, el cual lo recibirá como si llegara desde el nombre que escribamos.

La desventaja de este método de anonimato es que **no es posible** en principio **recibir respuestas**, dado que estas, si existieren, llegarían a la dirección original válida realmente. En la actualidad, el uso de estos sistemas es casi siempre **didáctico**, **educativo** o **lúdico**. En efecto, todos los sistemas que ofrecen este servicio online limitan el envío en cantidad mediante el uso de **captchas** (los caracteres que ingresamos manualmente para validar que somos usuarios humanos y no scripts automatizados).
Con el tiempo, el e-mail también se ha convertido en un gran **repositorio** de las comunicaciones, en especial desde la llegada de **Gmail** y el aumento del espacio que nos proporcionaban por usuario los distintos sistemas. De esta manera, comenzó la tendencia de dejar todo en la casilla para **posterior acceso**, o mandar las cosas al e-mail para recuperarlas desde otro lado. Este, de hecho, fue el comienzo conceptual del **almacenamiento en la nube** que muchos utilizan hoy en día. El primer servicio que sin decirlo nos permitió esa funcionalidad fue, sin duda, el e-mail.

SI BIEN EL E-MAIL NO HA VARIADO SU FUNCIONAMIENTO EN TRES DÉCADAS, SÍ SE HA CAMBIADO EL USO QUE SE LE DA.

Seguimiento

Otro de los usos del e-mail ha sido el **seguimiento** de campañas y acciones publicitarias o bien de mensajes que se espera saber si al menos fueron abiertos. Esto se ha realizado desde hace mucho tiempo, colocando **información oculta** en los mensajes, para que se descargue de Internet al abrirse, y así mantener un **registro** de dichas conexiones de forma tal que se pueda determinar si un mensaje se abrió, cuándo se abrió, cuántas veces, desde qué ubicaciones, etcétera. Esto no funciona de la misma forma que los **acuses de recibo**, implementados por el software de correo electrónico, que el usuario suele deshabilitar. No debemos olvidar el uso del e-mail como **canal de envío seguro**, no por medio del uso de protocolos seguros que encripten toda la conexión, sino por medio del envío de **mensajes cifrados**, tanto de mensajes como de archivos adjuntos o también **archivos con cifrado propio**, que se envíen por este medio sin la necesidad de una conexión segura ni el uso de claves en origen y destino. ■

Ayuda a otros servicios

De la misma manera que el e-mail motivó la existencia del almacenamiento en la nube, también ha promovido la introducción del usuario en otros servicios, como hace mucho tiempo en los inicios de la mensajería instantánea. Los primeros usuarios de Hotmail (Microsoft) naturalmente pasaban al MSN Messenger con solo haberse dado de alta en el correo, lo que hizo que muchos usuarios que habrían adoptado la tecnología más tarde, la adoptaran más naturalmente. Lo mismo ocurrió con el paso de Gmail a Gtalk (Google) y Yahoo! a Yahoo! IM (muy pronto caído en desuso, tal como AIM, de AOL).

Servicios de cuentas de e-mail temporales

Un curioso servicio que está creciendo en Internet es el de las cuentas temporales de e-mail. ¿Qué son? ¿Para qué sirven? En estas páginas lo analizamos en profundidad.

El servicio de correo electrónico se ha destacado ampliamente por ser **confiable** y haber cubierto las necesidades de los usuarios durante tres décadas. Si bien se le ha criticado en algunos casos su característica de poco confidencial o inseguro, con el tiempo se han agregado protocolos que cubrieron esta necesidad, haciendo del e-mail un medio de comunicación sumamente **versátil** y **eficiente**. Con la llegada del spam empezó uno de los problemas propios de la arquitectura del e-mail, ya que la sola existencia de las direcciones puede implicar que se reciban mensajes, sean o no requeridos por el usuario. La tecnología apuntaló este inconveniente proveyendo nuevos **dispositivos** y software para **filtrado y análisis** de forma que, durante la última década, el spam pasó de ser un grave problema a ser apenas algo de lo que preocuparse. En la época en que aún el problema todavía lo era, surgieron servicios muy particulares que ofrecían **cuentas** de correo electrónico **sin la necesidad de mantenerlas en el tiempo**.

Airmail es un servicio temporal que ofrece funciones básicas.

Privacidad por sobre todo

Si bien los servicios de cuentas temporales pueden servir para los usos más variados, el principal es la protección de nuestra privacidad, dado que muchos sitios online exigen la creación de perfiles para registrarse, que deben ser validados mediante el envío de un enlace que permitirá determinar si se trata de la misma persona. En general, esta es la única validación que se realiza, y, en caso de poder utilizar cuentas temporales, nuestra identidad podría estar enmascarada y protegeríamos nuestra privacidad.

Cuentas temporales

Uno podría preguntarse de inmediato para qué puede servir una cuenta como la mencionada, y la respuesta en la época de oro del spam era trivial: utilizarla cuando se necesitaba tener una casilla para recibir **mensajes por un tiempo**, como al momento de **registrarse en sitios de dudosa seguridad**.
Esto derivó en la aparición de cuentas de **creación instantánea**, que ni siquiera requieren que el usuario deba ingresar

al sitio para darla de alta, sino que, con el solo hecho de **recibir un mensaje** en esa dirección, la cuenta se crea automáticamente en el sitio que provee el servicio, y nos permite verificarla.
Esto por supuesto tiene la **desventaja** de que, al no existir contraseñas por usuario, **todas las casillas son públicas**, y, si alguien más elige el mismo nombre del alias, ingresará a la cuenta también, sin mayores dificultades.

LAS CUENTAS TEMPORALES OFRECEN UNA DIRECCIÓN REAL PARA UTILIZAR POR UN CORTO TIEMPO.

En definitiva, los servicios de cuentas temporales permiten la creación de cuentas de correo que deben ser chequeadas desde el sitio en cuestión, a modo de **webmail**, y pueden ser **automáticas o configurables**.
Las que son configurables permiten detallar incluso la **duración** que se le pretende dar a la cuenta, que puede ser de unas pocas horas, unos días o unos meses, y además algunas pueden configurarse también para ser accedidas con **usuario y contraseña**, de forma que no tengamos el problema antes mencionado.

Dominios

Por lo general, los sitios que prestan estos servicios cuentan con **varios dominios** para elegir a la hora de crear la cuenta. Esto no era así al principio, pero, con el tiempo, muchos sistemas de registración de usuarios comenzaron a **bloquear** el uso en la creación de nuevos perfiles de **cuentas temporales** detectando justamente el dominio. Esto llevó a que los servicios comenzaran a incluir **alternativas**, que el usuario puede seleccionar llegado el caso. En los sistemas de registración que no validan estos dominios a la hora de crear **nuevos perfiles de usuario** o de registrar a las personas para la descarga autorizada de algo, es posible utilizar las cuentas temporales para, por ejemplo, recibir el e-mail con el **enlace a la descarga**, y no volver a utilizar más la cuenta.
Un gran negocio para nuestra privacidad, si lo pensamos desde ese punto de vista. Incluso, algunos servicios ofrecen directamente la posibilidad de saber en qué **URL** estará accesible nuestra cuenta, de una forma sencilla de recordar. Por ejemplo, podría crearse la cuenta con el alias **AliasTemp** en el dominio **dominiotemporal.com** y que la URL entregada en forma predeterminada sea **aliastemp.dominiotemporal.com**.

Interfaz de una cuenta de **Mailinator**, uno de los pioneros en ofrecer este tipo de servicio.

Servicios

Estos servicios pueden encontrarse en Internet con el nombre de **Disposable Email Address**, o **Temporary Email Address**, y hoy en día son muchos los que lo proveen. Uno de los pioneros en el tema fue el ya bien conocido **Mailinator**, que cuenta con servicio de cuentas temporales automáticamente creadas con la llegada de un e-mail, y permite también el uso de dominios alternativos.
Otros servicios que han ganado popularidad en los últimos años fueron, por ejemplo, **YOPmail** (acrónimo de **Your Own Protection Mail**) que además ofrece la opción de una interfaz completamente en español, una versión del sitio especial para móviles, y cuenta con una extensión para **Firefox**, **Internet Explorer** y **Opera**, para acceder a cuentas de manera más directa. Además, si bien YOPmail no permite el envío de **e-mails anónimos**, sí permite sin embargo enviar un e-mail anónimo hacia otras direcciones de YOPmail.

En este servicio, los mensajes que llegan a una cuenta se mantienen por el término de ocho días, después de los cuales son eliminados. Otro servicio similar a Mailinator y YOPmail es **Airmail**, que ofrece prácticamente los mismos servicios. **GuerrillaMail** por su parte, provee el mismo servicio, pero adicionando la posibilidad de una interfaz de redacción y la creación automática de una **cuenta aleatoria** al visualizar el sitio. Este sistema de creación de cuenta aleatoria al momento de abrir la página también lo provee **10 Minute Mail**, que además, ofrece la cuenta solo por el período de diez minutos, luego de lo cual se autodestruye sin que tengamos que hacer nada, salvo que hayamos seleccionado la opción de que se mantenga por diez minutos más. ■

10 Minute Mail provee cuentas con alias aleatorios por el plazo de 10 minutos.

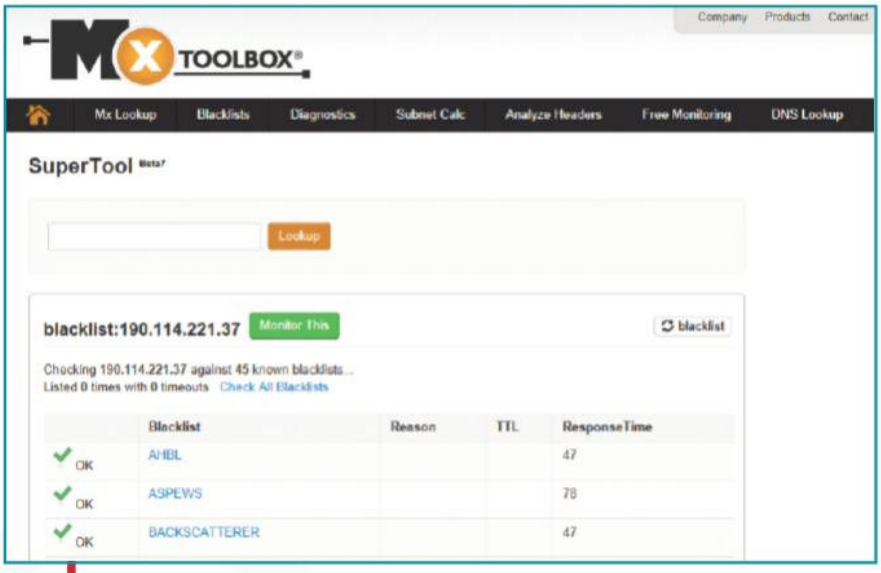
Análisis de headers de e-mails

Analizar el encabezado de un e-mail nos permite conocer algunos datos interesantes a la hora de comprender el sistema y también los parámetros de seguridad asociados.

Los más fanáticos del **networking** y los protocolos con seguridad han tenido el curioso honor de leer documentación técnica correspondiente a los estándares de Internet. De hecho, a los que alguna vez se adentraron en los **RFC** (**Request For Comments**). Para conocer en profundidad los **protocolos**, no hay demasiadas alternativas mas que ir a la documentación, y los protocolos de correo electrónico no son la excepción.

Protocolos

Pero uno se podría preguntar sencillamente para qué adentrarse en el análisis de un protocolo. La respuesta es variada: los especialistas en redes deben conocer la mayor cantidad de aspectos posibles, y en profundidad, en tanto que los especialistas en seguridad, encontrarán allí las bases para crear nuevas **técnicas de ataque** y **construir herramientas**; en cambio, los programadores podrían necesitar comprenderlos o no, dependiendo de qué tan abstracto sea el lenguaje que utilizan y sus utilidades, librerías, etcétera. En cualquier caso, siempre es bueno conocer más.



MXToolbox es una herramienta para análisis de encabezados y provee otras funciones, como el análisis de listas negras.

El tema particular del correo electrónico introduce una **necesidad adicional**, ya que puede requerirse la comprensión

El origen de la comunicación

Dado que muchas comunicaciones electrónicas vía Internet se realizan por medio del correo electrónico, algunas personas tienen tendencia a pensar que es posible determinar siempre la dirección IP de origen de la computadora de la que partió el mensaje. Aunque esto puede ser así, cuando hablamos de sistemas de webmail la información suele quedar naturalmente oculta por el proveedor del servicio, y no nos permite encontrarla.

IP Tracker Online es otro sitio que provee el servicio de análisis de encabezados.

de los encabezados por distintas razones, como ser el **análisis forense informático**, o temas relacionados con la **investigación de las comunicaciones**. Por supuesto que los detalles que permiten interpretarlos se encuentran también en los documentos técnicos RFC, provistos por la organización **IETF**, encargada de estos.

Encabezados

Teniendo en cuenta que todos los programas de correo electrónico generan encabezados para poder enviar los mensajes, sabemos que a priori tenemos disponible cierta información allí. En principio, a esta información se le va agregando información adicional a medida que el mensaje pasa de un servidor a otro, de forma tal que cada uno le pueda **agregar los datos** correspondientes a sí mismo y al tratamiento particular que le haya dado. De la misma manera que cada servidor de e-mail puede modificar dichos **headers** (encabezados), también pueden hacerlo servidores maliciosos, cuyo objetivo sea engañar filtros **antispam** o permitir el ataque a usuarios. Además de esto, algunos **plugins** y extensiones de los programas que se utilizan como clientes de correo en las computadoras de usuario pueden agregar información específica antes de ser procesado por el servidor. En todos los casos, la idea de realizar modificaciones y agregar información, en especial con etiquetas, incluso si solo son conocidas por una sola aplicación, servidor o sistema, tiene como fin que dichos datos puedan ser **identificados** en forma sencilla, para darles un **tratamiento en particular** a algunos, o bien para que cuenten con toda la información suplementaria que corresponde, para que otros servidores puedan tomar decisiones respecto al origen y filtrado.

Campos

Según el **RFC 2076** (**Common Internet Message Headers**) los únicos campos obligatorios que debe contener un mensaje de correo para poder ser procesado y distribuido son **From** (de) y **Date** (fecha), además claro, de **To** (para). Del resto, muchos se utilizan ampliamente, y otros son ignorados o reinterpretados. El RFC en el que están definidos en principio los campos del header de un e-mail es el **RFC 822** (*Standard for ARPA Internet Text Messages*) que fue reemplazado luego por el **RFC 2822** (*Internet Message Format*) en abril de 2001. Algunos campos comunes pero opcionales son: **CC** (*Carbon Copy*), que indica los destinatarios que van en copia, casi siempre por temas informativos o como participantes de una conversación; **BCC** (*Blind Carbon Copy*), que es la versión de CC que no especifica qué otros destinatarios han recibido el mismo mensaje (ideal para mantener la privacidad de los que reciben el correo en caso de ser necesario); **Subject** (asunto), que es el tema o asunto del mensaje, y **Resent-from/to/cc**, que indica si el mensaje ha sido reenviado. Otro campo útil cuya función vale la pena conocer es, por ejemplo, **Reply-To**, que permite detallar una dirección de e-mail de respuesta diferente a la que ha enviado el mensaje. Esto puede ser utilizado por potenciales atacantes que esperan recibir repuesta a sus envíos, pero que han falsificado el campo **From**. Relacionado con esto, el campo **Sender** permite una descripción del nombre que se verá al recibir el mensaje, que puede ser distinto de la dirección del remitente. Este también es usado para **engañar usuarios incautos**, que, al leer el nombre de quien envía, confían en que es quien dice ser, cuando en verdad pueden estar enviando desde una cuenta determinada y tener otro nombre de visualización. Este es el campo en el que se coloca el nombre y apellido de la persona en las cuentas personales.

CONOCER ALGUNAS HERRAMIENTAS ONLINE PUEDE AYUDARNOS A SIMPLIFICAR EL ANÁLISIS.

Algunos otros campos interesantes son **Return-Path**, **Received**, **References** y **Sender**. Uno de los campos que merecen la pena analizarse es el llamado **Message-ID**, que consta de tres partes: la hora de envío en segundos en formato hexadecimal, un valor aleatorio llamado **salt** en formato **#0#0#0#** donde # es un dígito aleatorio, y el nombre de dominio de quien envía el mensaje. Esto quedaría de la siguiente forma: **Message-ID: [hora].[salt]@[nombre-dominio]**. Algunos con funciones específicas son por ejemplo: **MIME-Version**, en el que se incluye información de los contenidos multimedia; **Content-Type**, que detalla el tipo de contenido del mensaje (**text/html**, **text/plain**, **multipart/mixed**, etc.);

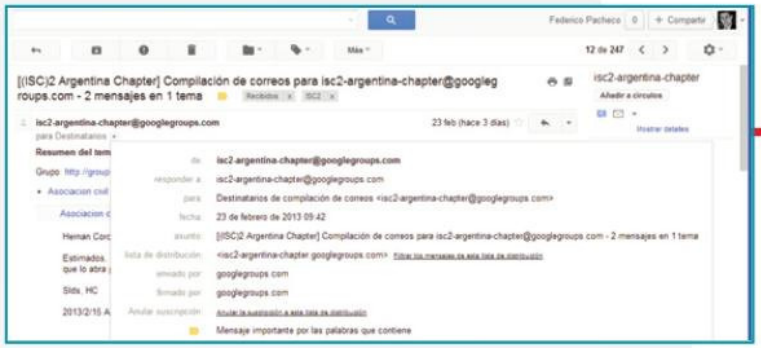
Content-Transfer-Encoding (**Base64**, **7-bit**, **quoted-printable**, entre otras); **Content-Disposition**, que sugiere si debe ser visualizado como **inline** o adjunto, y **Content-Description**, que es una descripción textual del contenido del cuerpo que corresponde al mensaje.

Pautas

Las pautas por seguir para realizar el correcto análisis de los **headers** de un e-mail no tienen demasiados secretos, y pueden resumirse como detallaremos a continuación. Como primera medida, debemos asegurarnos de poder visualizar los **encabezados completos**, lo cual suele ser una opción fácilmente accesible en los programas y servicios de **webmail**, pero que no está por defecto habilitada para evitar que el usuario común reciba demasiada información innecesaria.

SERVICIOS COMO IP TRACKER PERMITEN ANALIZAR ENCABEZADOS.

Una vez visualizado todo, conviene recorrerlo **de abajo hacia arriba**, ya que la información más próxima al usuario está abajo, y es más fácil pensarlo de esta forma, en especial si se desea analizar cuál fue el recorrido que siguió el mensaje antes de llegar al destino final. Por supuesto que no se debería confiar ciento por ciento en lo que se lee en un encabezado de correo electrónico, dado que, como dijimos, podría haber sido modificado por un atacante o usuario malintencionado, o manipulado por la misma persona que lo envió como parte de un ataque. Una **excepción** a esta regla de la desconfianza son los mensajes que están autenticados mediante **protocolos criptográficos**, ya que gracias a eso están técnicamente preparados para garantizar confidencialidad y autenticidad. Si lo único que nos interesa es el recorrido del mensaje, debemos prestar atención al campo que indica la **dirección IP** de cada servidor por el que haya pasado, pero, si lo que nos interesa es estudiar la autenticidad del remitente o algunos temas relacionados con la veracidad del contenido, es necesario apuntar al campo específico y chequear el valor del parámetro respecto lo que buscamos.



Aquí vemos la información extendida de un mensaje de **GMail**, que, si bien no es el encabezado completo, puede brindar detalles importantes.

Servicios online

Es importante señalar que existen **servicios online** que ayudan al análisis de los encabezados, no tanto extrayendo información que nosotros mismos no pudiéramos extraer solos en forma manual, sino ordenándolo todo en un formato más amigable, y realizando una extracción y separación automática de estos. Uno de ellos es **MXToolbox** (que se encuentra en la dirección **http://www.mxtoolbox.com**), una herramienta que solo requiere copiar el encabezado en texto plano y pegarlo en la ventana en cuestión, para que pueda mostrarlo casi al instante de manera prolija y ordenada. También **Google** nos ofrece el servicio de análisis de encabezados mediante la herramienta denominada **Message Header**, de **Google Apps Toolbox**, (en la dirección **http://toolbox.googleapps.com**), y hay otras muy efectivas, como **IP Tracker Online** (que encontramos en la dirección **http://www.iptrackeronline.com**). ■

PRÓXIMA ENTREGA

20

SERVIDORES DE ARCHIVOS E MPRESIÓN

En este fascículo aprenderemos a configurar y administrar un servidor de archivos dentro de un sistema Windows y GNU/Linux. También revisaremos las ventajas de establecer un servidor de impresión.

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 00019
9 789871 857784

CONTENIDO DE LA OBRA