UNIVERSIDAD DEL AZUAY

Facultad de Ciencias de la Administración
Escuela de Ingeniería de Sistemas

"Control de los Spam mediante el software libre SpamAssassin"

Trabajo de graduación previo a la obtención del título de "Ingeniero de Sistemas"

Autores: Luis Alfredo Chérrez Avila.

Director: Ing. Fabian Carvajal Vargas.

Cuenca, Ecuador
2006

Dedicatoria

Este trabajo lo dedico a mi tía que ha estado a mi lado siempre a mis padres, hermano, mi novia, y amigos que, con su dedicación y apoyo incondicional, me han ayudado cada día para sobresalir y poder concluir con una meta más de mi vida, obtener un titulo profesional.

AGRADECIMIENTO

Ante todo quiero dar gracias a Dios, por darme vida y salud para haber podido llegar a este punto de mi vida gracias por haberme brindándome cada día fuerza, sabiduría, seguridad y firmeza terminar una etapa más de mi vida profesional.

Agradezco a mi director de monografía el Ing. Fabián Carvajal, ya que gracias a su asesoramiento pude realizar el presente trabajo .El fue una gran ayuda y apoyo para la realización de la misma.

Mi más sincero agradecimiento a la “Universidad del Azuay” y a mis profesores de la misma que, por su enseñanza y colaboración, han contribuido en mi formación académica y personal.

INDICE DE CONTENIDOS

INDICE DE ILUSTRACIONES Y CUADROS

.

INDICE DE ANEXOS

RESUMEN

Hoy en día es común recibir muchas propagandas en nuestros correos de diferentes fuentes. Esta propaganda que es enviada usualmente sin previa autorización se le conoce como "SPAM."

Ésta es la razón de nuestro estudio, encontrar varios métodos para eliminar la información no deseada en nuestro correo electrónico. Las Empresas que quieren evitar el SPAM, debe instalar un software de ANTISPAM para ahorrar tiempo y dinero.

Como se menciona anteriormente este estudio esta basado en la correcta configuración y entrenamiento de la herramienta llamada SPAMASSASSIN que no tiene costo.

Al final de este estudio podremos observar una mejora en la reducción del SPAM.

ABSTRACT

It is common today to receive in our e-mail lots of propaganda from different sources. This propaganda, which is usually sent with no previous authorization, is called “SPAM”.

This is the reason of our research, to find a variety of methods to eliminate unwanted information in our electronic mail. Companies which want to avoid SPAMS, should install an ANTISPAM software to save time and money.

As mentioned above, this research was based on the configuration of the software, which is free, and on the training of users of this software, known as SPAMASSASSIN.

At the end of this research, we will observe an improvement in the reduccion of SPAM.

INTRODUCCION

La descarga del correo es, cada día con más fuerza, una actividad de alto riesgo, ya que el grado de contaminación del mismo es creciente en número y peligrosidad.

De hecho, disponer de filtrado de correo perimetral y en la estación debería entenderse como una obligación, pero la realidad es que no siempre se cumplen estas condiciones de contorno.

Una vez descargado el correo, toca revisarlo. Revisar tantos mensajes requiere cierto tiempo, y aunque un repaso de las cabeceras suele bastar para distinguir el spam de lo que no es correo basura, siempre hay que echar un ojo a la carpeta de correo no deseado, por si el antispam local del cliente ha clasificado como basura un correo legítimo. No podemos correr el riesgo de perder información valiosa, seamos usuarios domésticos o usuarios corporativos.

Uno de los objetivos que tenemos en este trabajo es dar el conocimiento de lo que es el spam para de esta manera poder luchar en contra de él.

Con la ayuda de una buen filtro antispam en nuestro caso el Spamassassin y con el entrenamiento necesario que se le de a esté no correremos más el riesgo de llenarnos de correos no deseados o de perder un correo importante que haya sido tomado como spam.

Mediante la investigación y una buena configuración de la herramienta se ha podido llevar a cabo los objetivos planteados para nuestro proyecto.

CAPITULO 1. INTRODUCCION A LOS SPAM

Introducción

En la actualidad se denomina spam o correo basura a todo tipo de comunicación no solicitada, realizada por vía electrónica.

De este modo se entiende por Spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. En este capitulo conoceremos todo lo que se refiere al spam, de donde provino este término.

1.1 Conocimientos del Spam.

El Spam también conocido como *junk-mail* son mensajes no solicitados que inundan la Internet con muchas copias e incluso millones, que por lo general son de aspecto publicitario de productos dudosos, métodos para hacerse rico o servicios en la frontera de la legalidad; en un intento por alcanzar la atención de la gente. Las personas o empresas que envían los spam no se dan cuenta que están perjudicando a mucha gente ya que ha pasado de ser algo molesto a llegar a ser un verdadero problema por la gran cantidad de correo basura que circula por la red y que nos hace perder tiempo y dinero para eliminarlo ya que en nuestro país la mayoría de la gente tiene que pagar por la conexión a Internet.

"En España el spam está terminantemente prohibido por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), publicada en el BOE del 12 de julio de 2002."[1] Aparte, a los poseedores de bases de datos de correos electrónicos se les podría aplicar la Ley Orgánica de Protección de Datos (LOPD) por tratarse de datos de carácter personal.

Aunque hay algunos spammers que envían solamente un mensaje, también hay muchos que llenan los buzones todas las semanas, con mensajes y archivos adjuntos de temas que a nadie interesa como el tema de filtrar el agua de la ducha con un análisis de varias páginas, que nadie lee.

---

1. http://www.masadelante.com/faq-que-es-spam.htm

1.2 Historia del termino spam

El origen de la palabra spam tiene raíces estadounidenses con unas curiosas derivaciones socio-culturales:

La empresa estadounidense Hormel Foods lanzó en 1937 una carne en lata originalmente llamada Hormel's Spiced Ham. El gran éxito del invento lo convirtió con el tiempo en una marca genérica, tan conocida que hasta el mismo fabricante le recortó el nombre, dejándolo con solo cuatro letras: Spam. El Spam alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial, y desde 1957 fue comercializado en todo el mundo. En los años 60 se hizo aun más popular gracias a su innovadora anilla de apertura automática, que ahorraba al consumidor el uso del abrelatas.

Fue entonces cuando los Monty Python empezaron a hacer burla de la carne en lata. Su divertidísima costumbre de gritar la palabra *spam* en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado, que perturba la comunicación normal en Internet.

“En un famoso sketch de 1969 los comediantes británicos representaban a un grupo de hambrientos vikingos atendidos por camareras que les ofrecían "huevo y panceta; huevo, salchichas y panceta; huevo y spam; huevo, panceta, salchichas y spam; spam, panceta, salchichas y spam; spam, huevo, spam, spam, panceta y spam; salchichas, spam, spam, panceta, spam, tomate y spam, ...". La escena acababa con los vikingos cantando a coro "Spam, spam, spam, spam. ¡Rico spam! ¡Maravilloso spam! Spam, spa-a-a-a-a-am, spa-a-a-a-a-a-am, spam. ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico spam! Spam, spam, spam, spam".”[2]

Como la canción, el spam es una repetición sin fin de texto de muy poco valor o ninguno, que aplicado a los mensajes electrónicos, se refiere a los mensajes enviados de forma masiva y dirigidos a personas que, en principio, no desean recibirlos.

Más del 40% de los mensajes proceden de Estados Unidos a pesar de que allí está prohibido, seguido por Corea del Sur con el 15% y China con el 12%.

---

2. http://www.brujula.com.ar/wiki/Spam.html#Historia_del_t.C3.A9rmino

1.3. Spam en diferentes medios

Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico, el spam también puede tener como objetivo los teléfonos móviles a través de mensajes de texto y los sistemas de mensajería instantánea comunicaciones mediante VoIP y a veces mediante vía fax. A continuación detallamos brevemente algunos medios por los cuales se propaga el spam.

1.4 Medios de Propagación del Spam

1.4.1 El spam por mensajería instantánea

Utiliza los sistemas de mensajería instantánea, tales como MSN Messenger. Muchos sistemas de mensajería ofrecen un directorio de usuarios, incluyendo información demográfica tal como edad y sexo. Los publicistas pueden reunir esta información, conectarse al sistema, y enviar mensajes no solicitados. Para enviar mensajes instantáneos a millones de usuarios de la mayoría de los servicios de mensajería instantánea sólo se requiere software de scripting y los nombres de usuario de los receptores y los bombardean con mensajes publicitarios.

1.4.2 El spam por telefonía móvil

Esto se da a través del servicio de Servicio de mensajes cortos (SMS) de un teléfono móvil. Esto puede resultar especialmente irritante para los consumidores no sólo por la molestia sino también porque muchas veces deben pagar para recibir el mensaje de texto.

1.4.3 El spam en las comunicaciones de Voz sobre IP

Se ha predicho que las comunicaciones de Voz sobre IP (VoIP) serán vulnerables a ser spammeadas por mensajes pregrabados. A pesar de que se han reportado muy pocos incidentes, muchas compañías ya han comenzado a intentar vender defensas contra ello.

1.4.4 El spam en mensajería de juegos en línea

Muchos juegos en línea permiten a los jugadores contactarse entre ellos vía mensajería peer-to-peer o salas de chat. Estos servicios de mensajería también están siendo utilizados por jugadores inescrupulosos para promover ciertos sitios web y tiendas en línea, sin preocuparse por violar

directamente el acuerdo de usuario final del juego, el cual prohíbe utilizar las comunicaciones dentro del juego para tales propósitos.

1.4.5 Spam por ventanas emergentes (Pop ups)

Se trata de enviar un mensaje no solicitado que emerge cuando nos conectamos a Internet. Aparece en forma de una ventana de diálogo y advertencia del sistema Windows titulado "servicio de visualización de los mensajes". Su contenido es variable, pero generalmente se trata de un mensaje de carácter publicitario.

Para ello se utiliza una funcionalidad del sistema de explotación Windows, disponible sobre las versiones Windows NT4, 2000, y XP y que permite a un administrador de redes enviar mensajes a otros puestos de la red.

La solución más sencilla para evitar estas ventanas emergentes consiste en desactivar este servicio de Windows. Otro método consiste en utilizar un cortafuegos destinado a filtrar los puertos TCP y UDP (135, 137,138, 139 y 445) de su ordenador, pero con esta medida es posible que deje de funcionar la red.

1.4.6 El Phising

No es exactamente una modalidad de Spam, más bien una técnica de ingeniería social para recolectar datos de forma fraudulenta.

El Phising es la duplicación de una página web para hacer creer al visitante que se encuentra en la página original en lugar de en la ilícita. Se suele utilizar con fines delictivos duplicando páginas web de bancos y enviando indiscriminadamente correos mediante Spam para que se acceda a esta página con el fin de actualizar los datos de acceso al banco, como contraseñas, fechas de caducidad, etc.

1.4.7 El Hoax

Es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena.

Algunos hoax informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de la suerte.

Los objetivos que persigue quien inicia un hoax son normalmente captar direcciones de correo o saturar la red o los servidores de correo.

1.4.8 El Scam

No tiene carácter de comunicación comercial. Este tipo de comunicación no deseada implica un fraude por medios telemáticos, bien vía teléfono móvil o por correo electrónico.

1.5 El Spam en el correo electrónico.

El spam mediante el servicio de correo electrónico nació el 5 de marzo de 1994. Este día una firma de abogados de *Canter and Siegel*, publica en Usenet un mensaje de anuncio de su firma legal, el cual en el primer día después de la publicación, facturó cerca de 10.000 dólares por casos de sus amigos y lectores de la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

El correo electrónico es, con diferencia, el medio más común de *spamming* en internet. Involucra enviar mensajes idénticos o casi idénticos a un gran numero de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el spam generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de spam. Lo único necesario para esto es la lista de direcciones objetivo que por lo general son robadas, compradas, recolectadas en la web o tomadas de cadenas de mail y vendidas a precios muy accesibles.

Algunas personas que envían spam utilizan una supuesta ley en la cual el mensaje que están enviando no puede ser considerado spam si tiene una forma de ser removido.
El mensaje es el siguiente:

"Bajo el decreto S.1618 titulo 3ro. Aprobado por el 105 congreso base de las normativas internacionales sobre SPAM, un mail no podrá ser considerado SPAM mientras incluya una forma de ser removido. Si desea ser borrado de nuestras Bases o no recibir nuestros Mails, reenvié este mail con el subject ELIMINAR y la dirección del mail donde lo recibió". [3]
Esto es mentira, ya que esa ley no existe. Por lo que no se debería nunca contestar esos mensajes ya que si lo hacen confirmarían la existencia de su correo.

---

3. http://www.rompecadenas.com.ar/spam.htm

Es conveniente no responder nunca a un mensaje no solicitado. Lo mejor es aplicar filtros o reglas de mensaje para evitar recibir mensajes de esas direcciones.

El spam está teniendo un efecto corrosivo sobre Internet en su conjunto. En estudios recientes hechos en Estados Unidos por la fundación *Pew*, se muestra que hay un número de usuarios de Internet que empiezan a perder seriamente la confianza en el correo electrónico debido al spam.

La economía de la industria del spam se basa en el envío de millones de mensajes con un costo prácticamente nulo, no requiere conocimientos profundos de cómputo, se puede hacer en el tiempo libre, en muchos países no genera un riesgo de represión o detenciones, y basta con tan solo un grupo pequeño de personas receptoras que hagan las compras o caigan en los engaños para volverlo sumamente lucrativo.

Son más los problemas derivados del empleo del "SPAM" que los posibles beneficios que puedan llegar a derivarse de su empleo.

Desde mi punto de vista no solo el uso de esta práctica va en contravía de las normas de etiqueta de la Red, sino que los resultados que se pueden obtener mediante esta práctica pueden crear mas problemas que beneficios.

Cada día es mayor el consenso por parte de los ciudadanos de Internet en condenar dichas prácticas y lo único que logran las personas o empresas que se dedican a dicha práctica es dar una mala imagen de sí mismos y de los productos o servicios que intentan representar. Esta mala imagen que se crea va en detrimento de la credibilidad que queremos proyectar y más que lograr capturar clientes potenciales lo único que logran hacer es generar rechazo.

1.6 Conclusiones

Desde mi punto de vista el uso de spam no es algo provechoso para ninguna empresa ya que es muy fácil de detectar y es fastidioso para mucha gente que lo recibe lo cual podría provocar una queja directa al proveedor de Internet y la cancelación de la cuenta de quienes envían los spams.

Además que se podría tachar como fraudulentos a las empresas que utilizan estos medios para publicar cualquier anuncio ya que se han dado casos de estafas mediante estos anuncios.

Para evitar todo esto deberíamos fomentar al gobierno para que decrete una ley en contra del spam.

Como nos podemos dar cuenta existen muchos medios por los cuales se propaga el spam pero entre los mas comunes esta el correo electrónico, en el cual centraremos nuestro estudio para filtrar dichos correos basura.

CAPITULO 2. TECNICAS DEL SPAM

Introducción

Las tecnologías y metodologías avanzan constantemente y lo hacen tanto para quienes se dedican a mantener la seguridad en los medios informáticos como para quienes se deciden sacar provecho a costa de ellos en este caso para el uso indiscriminado del spam.

Los spammers para evitar que los potentes filtros antispam actuales frustren toda su labor de lanzar correos no deseados de manera indiscriminada han lanzado una nueva técnica dando un giro efectivo y nuevamente apareciendo en escena. Para lograr esto, los responsables de esta insaciable actividad incluyen en dichos mensajes imágenes en formato gif o jpeg, de este modo, las soluciones actuales no encuentran palabras clave ni texto para analizar, dejando llegar el correo sin obstrucciones.

En estas imágenes se encuentra grabado el texto que normalmente se envía como spam y arriban como correos electrónicos de HTML, por lo que las herramientas no pueden identificarlo. En tan solo un año, esta tendencia creció un doce por ciento ya que ha encontrado la manera de sobrepasar los filtros de seguridad, por lo que se esperan más casos.

Las técnicas del spam que describiremos en este capitulo son cinco de las tantas que existen hoy en día en nuestro medio.

2.1 Obtención de direcciones de correo

Los individuos o empresas que envían spam utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam son:

- Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes.
- Los grupos de noticias de usenet, cuyos mensajes suelen incluir la dirección del remitente.

- Listas de correo: les basta con apuntarse e ir anotando las direcciones de sus usuarios.
- Correos electrónicos con chistes, cadenas, etc. que los usuarios de internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje, pudiendo ser capturadas por un troyano o, mas raramente, por un usuario malicioso.
- Páginas en las que se solicita tu dirección de correo (o la de "tus amigos" para enviarles la pagina en un correo) para acceder a un determinado servicio o descarga.
- Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).
- Entrada ilegal en servidores.
- Por ensayo y error se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales.

2.2 Envío de mensajes

Una vez que tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor y en general a internet, por consumirse gran parte del ancho de banda en mensajes basura.

2.3 Verificación de la recepción

Además, es frecuente que el spammers controle qué direcciones funcionan y cuáles no por medio de pequeñas imágenes contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del spammer, que registra automáticamente el hecho. Otro sistema es el de prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído. Si recibe un correo no solicitado debe borrarlo sin leerlo.

2.4 Troyanos y ordenadores zombis

Recientemente, han empezado a utilizar una técnica mucho más maliciosa, la creación de virus troyanos que se expanden masivamente por ordenadores no protegidos. Así, los ordenadores infectados son utilizados por el spammer como "ordenadores zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros o correos nuevos en busca de más direcciones. Esto puede causar perjuicios al usuario ya que lo hacen pasar por spammer y como el ignora haber sido infectado ya que no se nota nada extraño y al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios.

Actualmente, el 40% de los mensajes de spam se envían de esta forma.

2.5 Servidores de correo mal configurados

Los servidores de correo mal configurados son aprovechados también por los spammer. En concreto los que están configurados como Open Relay. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos. Existen diferentes bases de datos públicas que almacenan los ordenadores que conectados directamente a Internet permiten su utilización por los spammers. El más conocido es la Open Relay DataBase.

2.6 Conclusiones

Conociendo una de las pocas técnicas que utilizan los spammers para saturarnos de spam podemos tener un ligero conocimiento de cómo evitar que nos suceda esto ya que nosotros podemos ser spammer sin darnos cuenta solo por falta de conocimiento de este tema que hoy en día es muy común en nuestro ambiente.

CAPITULO 3. PRECAUCIONES PARA EVITAR EL CORREO BASURA

Introducción

La dirección de correo electrónico es el medio más utilizado para registrar la identidad de una persona en Internet y suele servir de base para la acumulación de información en torno a la misma. En muchas ocasiones contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país de residencia. Esta dirección puede utilizarse en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento.

3.1 Formas de Evitar obtención de su correo

Un buen consejo es elegir una dirección de correo poco identificable.

Los spammers obtienen las direcciones de correo electrónico de formas muy diferentes. Así navegando por la red, en salas de chat e IRC, o incluso en directorios de contactos o usando la ingeniería social. A veces compran incluso listas de correo electrónico en sitios web que venden los datos de sus clientes. Y, cuando todo esto falla, simplemente conjeturan.

Las direcciones de correo electrónico que se refieren a una persona como tal, suelen contener algún elemento que les identifique y son fáciles de recordar.

Esta forma de crear el correo permite a los spammers intuir las direcciones de correo electrónico. Por ejemplo, si su nombre es Jesús Fernández, el spammer probará con las siguientes opciones: jesusfernandez@...., j.fernandez@...., jfdez@....., jesus.fdez@...., etc.

Los spammers incluso cuentan con programas que generan automáticamente posibles direcciones de correo. Pueden crear cientos de direcciones en un minuto, ya que trabajan utilizando diccionarios, es decir, una lista de palabras que se suelen usar en las direcciones de correo. Estos diccionarios suelen contener campos como los siguientes:

• Alias

• Apellidos

• Iniciales

• Apodos

• Nombres de mascotas

• Marcas

• Signos del zodiaco

• Meses del año

• Días de la semana

• Nombres de lugares

• Modelos de coches

• Términos deportivos

• Etc.

Estos programas simplemente introducen datos en cada uno de estos campos e intentan varias combinaciones con todos ellos. Además añaden letras y números en las combinaciones, ya que se suelen introducir fechas de cumpleaños, edades, etc.

Para crear una dirección de correo electrónico y reducir el envío de Spam, sería conveniente no introducir campos que sean potencialmente intuíbles por el spammer.

Otro punto muy importante seria sensibilizar a los niños sobre la utilización del correo y la mensajería instantánea

Los niños son objetivos ideales para promocionar información sobre la composición y las prácticas de consumo del hogar. Por eso es importante recordarles algunos consejos prácticos que ayudarán a evitar que el niño aporte datos personales.

Además, mediante la dirección de correo electrónico no se puede saber quien es el destinatario de correos que pueden tener contenidos no aptos para los niños.

3.2 Métodos para evitar el spam

Para evitar el spam no existe un método eficaz ya que antes de abrir el e-mail es difícil saber si un correo es spam o no. No obstante, si hay algunas cosas que podemos hacer como usuarios para evitar el Spam**.**

3.2.1 Si tienes que poner tu dirección en tu web para que contacten contigo.

En vez de poner la dirección como texto, muéstrala en una imagen con la dirección de correo. Actualmente no se pueden rastrear automáticamente.

En vez de poner el enlace a tu cuenta, usa una redirección (puede ser temporal o por un número de usos), y bórrala cuando recibas excesivo spam.

3.2.2 Modificar la dirección para evitar el rastreo automático.

Por ejemplo, cambiar "nombre@dominio.com" por "nombre (ARROBA) dominio (PUNTO) com", "nombre@dominioNOSPAM.com, quita NOSPAM" o "n0mbre@d0mini0.c0m (sustituir los ceros por “o”)". Ayuda pero no es 100% efectivo.

3.2.3 Una combinación de las anteriores.

Algunos servicios de correo gratuito como Mailinator ofrecen cuentas temporales sin tener que usar contraseñas. Los mensajes se borran automáticamente al cabo de unas horas. Puede ser útil si sólo quieres que contacten contigo una vez, por ejemplo para confirmar un pedido.

3.2.4 En los grupos de noticias y listas de correo.

No poner el remitente verdadero en los post enviados.

Si el archivo de mensajes a la lista es visible desde web, cambiar las direcciones de remite por una imagen, ocultarlas, o escribirlas de forma que sea difícil reconocerla como tal para un programa.

3.2.5 Para evitar spam en una lista.

El foro puede estar moderado, para evitar mensajes inadecuados.

Rechazar correos de usuarios no suscritos a la lista.

3.2.6 Para evitar en otros medios.

No reenviar mensajes parte de una cadena de correo electrónico.

No hacer envíos a amigos o colaboradores en los que aparezcan muchas direcciones y, si se hace, usar CCO para que no sean visibles las demás direcciones.

Igualmente, si reenvías un correo electrónico que ya contiene alguna dirección en el mensaje, asegúrate de borrarla.

Al rellenar una inscripción no dar el correo. Si es necesario dar una dirección correcta (envío de contraseñas, confirmación de la suscripción, etc.) utiliza una redirección temporal, o una cuenta gratuita "extra" prescindible de las que se ofrecen en la mayoría de los portales de internet. No se debe hacer caso de las recomendaciones como de este tipo : "preferiblemente cuenta no hotmail".

Leer los correos de remitentes sospechosos como texto, y no como HTML.

No enviar nunca mensajes al spammer, aunque prometan dejar de enviar spam si se les pide. A menudo ofrecen una forma de anular la suscripción a su boletín de mensajes (lo que en inglés llaman "opt-out", u optar por salir) que suele consistir en mandar un mensaje a una dirección de tipo unsubscribe@dominio.com. Si mandas un mensaje a dicha dirección con la esperanza de dejar de recibir correo no solicitado, sólo estás confirmando que tu cuenta existe y está activa, por lo que acabarás recibiendo más spam que antes.

3.3 Formas de bloquear el spam

Se debe tener siempre al día las actualizaciones de seguridad del sistema operativo e instalar un buen cortafuegos (firewall) y un buen antivirus, y tenerlos siempre activados.

Hay formas de bloquear mensajes que tengan ciertas características, por ejemplo, si en el asunto aparece la palabra "porno". Sin embargo, muchos spammers escriben algunas palabras con faltas intencionadas de ortografía o introducen algún espacio o signo de puntuación en la palabra más propensa a ser bloqueada (por ejemplo, escribirían "p0rn0" o "p o r n o"). Por lo que bloquear mensajes no suele ser muy útil.

Utilizar los filtros que proporcionan la mayor parte de los sistemas de correo. Un filtro de correo permite desechar ciertos correos que consideramos spam. Los correos detectados como spam se pueden desviar a una carpeta específica o eliminarse directamente. Se puede filtrar de diversas maneras. Una vez comprobado que un correo es spam se puede definir un filtro para que los siguientes correos que lleguen con el mismo remitente se consideren spam. También se puede crear un filtro que incluya ciertas palabras (sexo, porno, etc) de forma que si en el campo Asunto del correo aparecen esas palabras se considere spam. También hay filtros como el SpamAssassin que analizan el contenido del correo y son capaces de detectar el spam ya que los correos basura suelen tener un lenguaje y una estructura similar.

La otra forma de luchar contra el spam no esta en manos de los usuarios sino que depende de gobiernos**,** entidades diversas y empresas. Se trata de evitar que se envíen los correos basuras. Esto incluye leyes que penalicen a los emisores de spam, listas negras públicas con los emisores de spam, etc.
Por último, hay algunas acciones de prevención que nos pueden ayudar a luchar contra el spam como por ejemplo ser cuidadoso al dejar nuestra dirección de correo, cuantos mas sitios web conozcan nuestra dirección más probabilidades hay de que los emisores de spam conozcan nuestra dirección. Una táctica que puede dar buenos resultados como ya dijimos anteriormente es tener dos cuentas de correo, una para las cosas importantes y otra para cosas menos importantes. La cuenta importante en la que figura nuestro nombre real sólo hay que darlas en sitios de mucha seriedad mientras que con la otra cuenta, con nombre ficticio, podemos ser menos precavidos, aunque desde esa cuenta también es posible saber algunos datos del usuario. Si en la segunda cuenta empezamos a recibir mucho spam podemos darla de baja y crear una nueva.

Informe de Spammers a ISP's, proveedores de correo electrónico. Si usted recibe correo no deseado, fíjese en la dirección del remitente. El nombre del ISP debe estar en el centro (entre el signo de "@" y el sufijo, por ejemplo, ". com"). Reenvíe una copia del correo spam a la dirección de su ISP. La mayoría de los proveedores tomarán las acciones para eliminar spammers de su sistema. Además, envíe una copia de algún correo engañoso o no deseado a la Comisión Federal de Comercio de su país. Ellos usan su base de datos de mensajes no solicitados para aplicar la ley contra los emisores de spam. Vale destacar que en la actualidad en el Ecuador no existe esta comisión.

3.4 Proyectos y servicios en contra del spam

En pocos años, el *spam* se ha convertido en un fenómeno especialmente preocupante. "Se considera que actualmente más del 50 % del tráfico de correo electrónico a nivel mundial está constituido por *spam*. Y aún más inquietante resulta el índice de crecimiento de este fenómeno, puesto que, en 2001, la proporción se situaba en aproximadamente el 7 %."[4]

4.- http://europa.eu/scadplus/leg/es/lvb/l24190a.htm

El *spam* constituye un problema desde muy diversos puntos de vista:

- En la intimidad
- En su naturaleza engañosa y fraudulenta
- En un carácter perturbador de los spam pornográficos
- En la pérdida de tiempo (vaciado de los buzones de correo electrónico) y coste financiero al usuario (adquisición de programas de filtrado)
- En diversos costos financieros considerables para las empresas debido a que sus servicios informáticos deben dedicar cada vez más tiempo y dinero a intentar solucionar el problema. Se ha calculado que, en el 2002, el spam costó a las empresas europeas 2 500 millones de euros solamente en pérdidas de productividad.

Existen algunas disposiciones legislativas que ya existen en muchos países europeos por ejemplo: La Directiva sobre la privacidad y las comunicaciones electrónicas de 2002 prohíbe el envío de mensajes comerciales no solicitados (por correo electrónico, SMS o MMS) salvo que se haya obtenido previamente el consentimiento del abonado a lo cuál lo llaman “régimen de consentimiento previo”. La instauración de este régimen es una primera etapa imprescindible. No obstante, deben añadirse una serie de medidas complementarias destinadas a que la prohibición del spam sea una realidad.

Para ello, la Comunicación propone diferentes tipos de acciones:

- Medidas que deben tomar las autoridades públicas en ámbitos como recursos y sanciones, mecanismos de denuncia, denuncias transfronterizas, cooperación con terceros países y seguimiento,
- Acciones técnicas y de autorregulación referidas a los agentes del mercado,
- Acciones de sensibilización de los consumidores.

Los proyectos que existen, pretende resolver un serio problema de las comunicaciones electrónicas no deseadas, lamentablemente pone en serio peligro los derechos fundamentales de los usuarios de Internet, tales como el derecho a la información, la inviolabilidad de la comunicaciones y el debido proceso legal.

Esta iniciativa legal es precedida de un extenso texto, el cual consigna sus razones, a saber: el procesamiento computacional abusivo y anónimo, con fines de lucro, de los datos personales; y, el perjuicio ocasionado por el spam o correo electrónico masivo, abusivo y no deseado, cuyo tratamiento evidencia la insuficiencia de la autorregulación y las limitaciones de la actual ley sobre protección al consumidor.

Al respecto, esta iniciativa propone:

- Modificar el concepto de dato personal para incluir los relativos a personas jurídicas como: empresas, fundaciones y corporaciones, entre otros.
- Extender el concepto de dato sensible para incluir las direcciones de correo electrónico, nóminas de clientes, y estados financieros y patrimoniales;
- Modificar el concepto de fuente accesible a público, a efectos de evitar ciertas imprecisiones del tenor actual del mismo.
- Reemplazar los casos en que la ley permite el tratamiento de datos sin autorización de la persona a quien se refieren.
- Limitar el tratamiento de datos cuando se recopilan desde Internet.
- Incorporar todo un título nuevo para reglamentar la protección de los datos sensibles en general y las direcciones de correo electrónico en particular.

La preocupación central del proyecto es evitar los envíos de spam, para lo cual se crea un sistema de protección especial para la cuenta de correo electrónico.

Sin embargo, pone en serio peligro los derechos fundamentales de los usuarios de la red, tales como el derecho a la información, la inviolabilidad de las comunicaciones y el debido proceso legal.

En efecto, según la propuesta, la persona titular de la cuenta de correo electrónico podrá requerir al prestador de servicio de Internet que preste servicios de mantención y operación de casilla electrónica, el bloqueo de la dirección del emisor que le envíe un correo no solicitado. Para ello bastará la solicitud, notificación y/o reclamo de cinco usuarios.

Y el que brinda dicho servicio deberá, entre otras obligaciones, elaborar y publicar una lista de todas aquellas direcciones de correo que se ha solicitado bloquear, la cual podrá ser consultada por los sistemas o servidores de correo de otros proveedores.

Así como en muchos países de todo el mundo en el Ecuador también se creo una ley en contra de el envió de daos no solicitados que consta en el articulo 22 del siguiente reglamento creado en gobierno de Gustavo Noboa Bejarano.

REGLAMENTO A LA LEY DE COMERCIO ELECTRONICO.

Decreto Ejecutivo No. 3496. RO/ 735 de 31 de Diciembre del 2002.

Gustavo Noboa Bejarano

PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Considerando: Que mediante Ley No. 67, publicada en el Registro Oficial Suplemento No. 557 de 17 de abril del 2002 se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos;

Que la disposición final de la citada ley dispone que el Presidente de la República debe expedir el correspondiente reglamento; y, En ejercicio de la facultad prevista en el artículo 171 numeral 5 de la Constitución Política de la República Decreta:

Expedir el siguiente REGLAMENTO

GENERAL A LA LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

Art. 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a la que se refiere el artículo 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos y a cuyo contenido se accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos. En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo

requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico. Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

Art. 2.- Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art. 3.- Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a) Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

b) Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo. Las publicaciones que las leyes exijan por

escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito.

Art. 4.- Información original y copias certificadas.- Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberá ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado. Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art. 5.- Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmando que el documento original y el documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original. En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original como el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

Art. 6.- Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Art. 7.- Procedencia e identidad de un mensaje de datos.- La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o sistemas de identificación y autenticación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos.

El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma, su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación, o contratación electrónica. De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.

Art. 8.- Responsabilidad por el contenido de los mensajes de datos.- La prestación de servicios electrónicos de cualquier tipo por parte de terceros, relacionados con envío y recepción de comunicaciones electrónicas, alojamiento de bases de datos, registro electrónico de datos, alojamiento de sitios en medios electrónicos o servicios similares o relacionados, no implica responsabilidad sobre el contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información.

De acuerdo a la ley y por orden de la autoridad competente, el órgano regulador podrá ordenar la suspensión del acceso a cualquier información en redes electrónicas que se declare ilegal y/o que atente contra las leyes o la seguridad nacionales. El proveedor de servicios electrónicos deberá cumplir con la orden de suspender el acceso al contenido en forma inmediata, y en caso de no hacerlo será sancionado con sujeción a la ley por el CONELEC.

Art. 9.- Prestación de servicios de conservación de mensajes de datos.- La conservación, incluido el almacenamiento y custodia de mensajes de datos, podrá realizarse a través de terceros, de acuerdo a lo que establece el Art. 8 de la Ley 67. Los sistemas, políticas y procedimientos que permiten realizar las funciones de conservación de mensajes de datos se denominan Registro Electrónico de Datos. Una vez cumplidos los requisitos establecidos en las leyes, cualquier persona puede prestar servicios de Registro Electrónico de Datos que incluyen:

a. Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades;

b. Preservación de la integridad de la información conservada;

c. Administración del acceso a la información y la reproducción de la misma cuando se requiera;

d. Respaldo y recuperación de información; y,

e. Otros servicios relacionados con la conservación de los mensajes de datos.

La prestación de servicios de Registro Electrónico de Datos se realizará bajo el

régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación. La prestación del servicio de Registro Electrónico de Datos deberá observar todas las normas contempladas en la Ley 67, este reglamento y demás disposiciones legales vigentes. En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento.

Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario.

Art. 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

a) No discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;

b) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente;

c) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);

d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y,

e) Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Art. 11.- Duración del certificado de firma electrónica.- La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en la leyes.

Art. 12.- Listas de revocación.- Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos. Los períodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente.

Art. 13.- Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado. En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado. La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento.

Art. 14.- De la notificación por extinción, suspensión o revocación del

certificado de firma electrónica.- La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al artículo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado.

Art. 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el artículo 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

a) Siempre en la página electrónica determinada por el CONELEC en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,

b) Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica. Opcionalmente, en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública.

Art. 16.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador una vez obtenida la revalidación respectiva emitida por el CONELEC, el deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

Art. 17.- Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONELEC.

Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONELEC, tienen carácter probatorio. Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONELEC, tendrán la calidad de entidades de

certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

Art. 18.- Responsabilidades de las entidades de certificación de información.- Es responsabilidad de la entidad certificadora de información o de la entidad de registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.

El CONATEL podrá requerir en cualquier momento de la entidad de certificación de información, de la entidad de registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

Art. 19.- Obligaciones del titular de la firma electrónica.- A más de las consideradas en la Ley 67 y su reglamento, serán las mismas previstas en las leyes por el empleo de la firma manuscrita.

El órgano que ejerce las funciones de control prevista en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Art. 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales. En el caso de uso de medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario; cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario. Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información

personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades. Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Art. 22.- Envío de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

a. Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción;

b. Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;

c. Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;

d. A solicitud del destinatario se deberá eliminar toda información que de él se tenga

en bases de datos o en cualquier otra fuente de información empleada para el envío de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,

e. Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente. Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino. Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envío periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Art. 23.- Sellado de tiempo.- Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONELEC para prestar este servicio. El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONELEC; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario. Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano.

La prestación de servicios de sellado de tiempo se realizará en régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulan su relación.

Art. Final.- El presente reglamento entrará en vigencia a partir de su publicación en el Registro Oficial.

3.5 Conclusiones

La mayoría de consejos que se dan para evitar el spam o evitar caer en las listas de los spammers son muy buenas y nos podrian ayudar de alguna manera ha evitar que nuestros buzones de entrada estén llenas de propagandas o correos spam. Aunque la mayoría de personas no hacen caso de estos consejos.

Las leyes en contra del spam en nuestro país no son muy buenas por lo que el uso del spam sigue siendo uno de los más comunes en la vía electrónica especialmente el los correos electrónicos.

CAPITULO 4. HERRAMIENTAS PARA EL CONTROL DEL SPAM

Introducción

Existen muchas herramientas para el control del spam sin embargo para nuestro trabajo hemos escogido una herramienta en especial con la cual vamos a trabajar sobre Centos 4.0 y con el servidor Sendmail esta herramienta se le conoce como SpamAssassin 3.1.

A continuación damos un conocimiento básico de la herramienta que nos será de gran ayuda en la realización de nuestro proyecto.

4.1 Introducción al SpamAssassin

SpamAssassin es un filtro de correo que trata de identificar el spam mediante el análisis del texto y el uso en tiempo real de algunas listas negras a través de Internet.

A partir de su base de datos de reglas, utiliza un amplio abanico de pruebas heurísticas en las cabeceras y el cuerpo de los correos para identificar el spam, también conocido como correo electrónico comercial no solicitado. Una vez identificado, el correo puede ser opcionalmente marcado como spam o más tarde filtrado usando el cliente de correo del usuario.

SpamAssassin distingue típicamente con éxito entre el Spam y no-Spam(conocido como Ham) entre el 95% y 100% de casos, dependiendo de qué clase de correo consigues y su entrenamiento de su filtro Bayesian que no es mas que una base de datos en la cual se van almacenando una serie de reglas para ayudar a identificar el spam. Específicamente, SpamAssassin se ha demostrado al producto alrededor de 0.9% negativas falsos (Spam que fue falso) y de alrededor 0.1% positivos falsos (Ham marcado incorrectamente como Spam).

SpamAssassin también incluye plugins para apoyar la divulgación de mensajes del Spam automáticamente o manualmente a las bases de datos de filtración de colaboración tales como Pyzor, DCC, y maquinilla de afeitar de Vipul.

4.2 Descripción del SpamAssassin

SpamAssassin no es un programa para suprimir el spam, dirige el Spam para separarlo del buzón de entrada del correo electrónico o las carpetas de correo para despacharlo cuando recibes el Spam.

SpamAssassin es un filtro o un clasificador del correo. Examinará cada mensaje presentado a él, y asigna una cuenta que indica la probabilidad que el correo es Spam. Un programa externo debe entonces examinar esta cuenta y hacer cualquier encaminamiento que el usuario desee hecho. Hay muchos programas que realizarán fácilmente estas funciones después de examinar la cuenta asignada por SpamAssassin.

SpamAssassin es un filtro del correo que procura identificar el Spam usando una variedad de mecanismos incluyendo análisis del texto, la filtración Bayesian, blocklists del DNS, y bases de datos de filtración de colaboración.

SpamAssassin es un proyecto de la fundación del software de Apache (ASF).

La distribución proporciona “spamassassin”, una línea de comando herramienta para realizar la filtración, junto con el “correo:: Módulo de SpamAssassin el” fijó que permite que SpamAssassin sea utilizado en servidor del SMTP o de POP/IMAP del poder de la Spam-protección, o una variedad de diversos panoramas de Spam-bloqueo.

4.3 Funciones del SpamAssassin

Se realiza una serie de pruebas a los mensajes, para cada prueba que supera, le asigna una puntuación. Cuando la puntuación llega a 5 (valor por defecto) entiende que se trata de un mensaje de spam. Además, desde hace poco SpamAssassin incluye también filtros bayesianos que permiten ajustar delicada y automáticamente la clasificación de un mensaje. Así, en caso de un falso positivo/negativo, podemos adiestrar a SpamAssassin para que tenga en cuenta la característica de éste en el futuro.

Si se desean utilizar los filtros bayesianos del SpamAssassin, y es muy recomendable hacerlo si se quiere tener un alto porcentaje de acierto, será preciso entrenarlo. Según el manual, varios miles de mensajes deben ser proporcionados a SpamAssassin, tanto de spam como de ham. Para ello se usa la herramienta sa-learn (man sa-learn para su

documentación). Con sa-learn --spam <directorio> lo instruimos para que recoja información de correos que sabemos con certeza que son spam, y con sa-learn --ham <directorio> lo instruimos para que recoja información de correos que sabemos con certeza que no son spam. Asimismo, sa-learn tiene una opción que permite pasarle un fichero que contenga una lista de directorios, uno en cada línea, en los cuales buscará el tipo de correo que le especifiquemos.

Este parámetro, --folders=file, es muy útil si queremos recoger una lista de buzones de usuarios que sabemos con seguridad que sólo guardan spam o ham y utilizarlos para continuamente mejorar nuestros filtros desde un job del cron, ya que esta herramienta mantiene una lista de los correos que ya ha analizado y se los salta cada vez, haciendo este proceso bastante eficiente.

Los filtros bayesianos necesitan un gran número de mensajes para aprender, por lo cual deberemos estar una buena temporada enseñándole.
Los filtros bayesianos están activados por defecto, y SpamAssassin adiestra este filtro según su tabla de reglas. Si un mensaje supera las pruebas y es clasificado como spam, añade las reglas de este mensaje a la base de datos bayesiana. Lo mismo si un mensaje no lo clasifica como spam. Así, si las reglas propias funcionan correctamente en vuestro caso esta base de datos se alimentará sin la atención del usuario. Esto sería ideal, pero esto no es así, desgraciadamente, en la realidad. Por lo tanto debemos preparar un sistema que nos facilite este control.

4.4. Configuración e instalación de SpamAssassin

En Centos 4.0 la herramienta SpamAssassin ya viene instalada cosa que nos facilia mucho más nuestro trabajo.

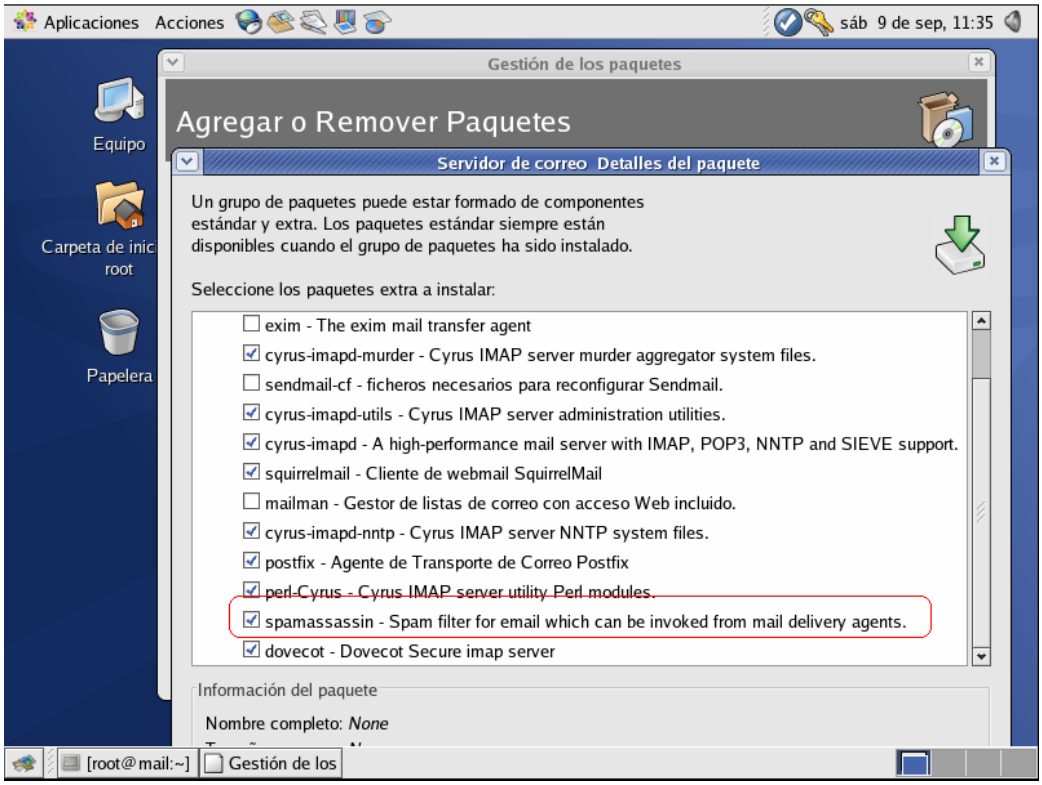

Figura 4.1 Instalación del SpamAssassin en Centos.

La configuración de SpamAssassin puede ser llevada acabo de manera global afectando todos los buzones de los usuarios de una instalación o bien, de manera individual donde cada usuario define reglas de filtrado más estrictas o flexibles.

Los parámetros globales de SpamAssassin son definidos en un archivo llamado local.cf ubicado en el sub-directorio de instalación mail/spamassasin, para la presente guía esto correspondería a la ruta absoluta ~/confspama/mail/spamassasin/local.cf, dicho archivo contiene las reglas que serian aplicadas a cualquier buzón que utilice SpamAssassin.

Figura 4.2 Configuración del SpamAssassin

Para aquellos casos en los que un usuario desee definir reglas de filtrado especificas, éstas pueden ser definidas bajo la ubicación del buzón de usuario en un sub-directorio llamado .spamassasin y dentro de un archivo denominado user_prefs, vale mencionar que estas reglas son aplicadas una vez que han sido empleadas todas aquellas definidas a nivel global.

Cada regla en SpamAssassin posee un puntaje, valor que en caso de violarse dicha norma, es asignado al puntaje total del mensaje en la evaluación de ser SPAM, el valor promedio para que un correo electrónico sea considerado chatarra también es configurable como se describirá a continuación, finalmente, vale mencionar que para efectos prácticos, SpamAssassin posee puntajes predefinidos ("default") para todas sus reglas, mismas que pueden ser modificadas.

Aunque la nomenclatura utilizada para definir reglas es intuitiva, SpamAssassin posee un gran número de variantes, por lo que las siguientes normas sólo representan las más básicas para un filtrado elemental. (NOTA: Esta lineas pudieran ser colocadas a nivel global (local.rf), o bien, a nivel usuario (user_prefs) :

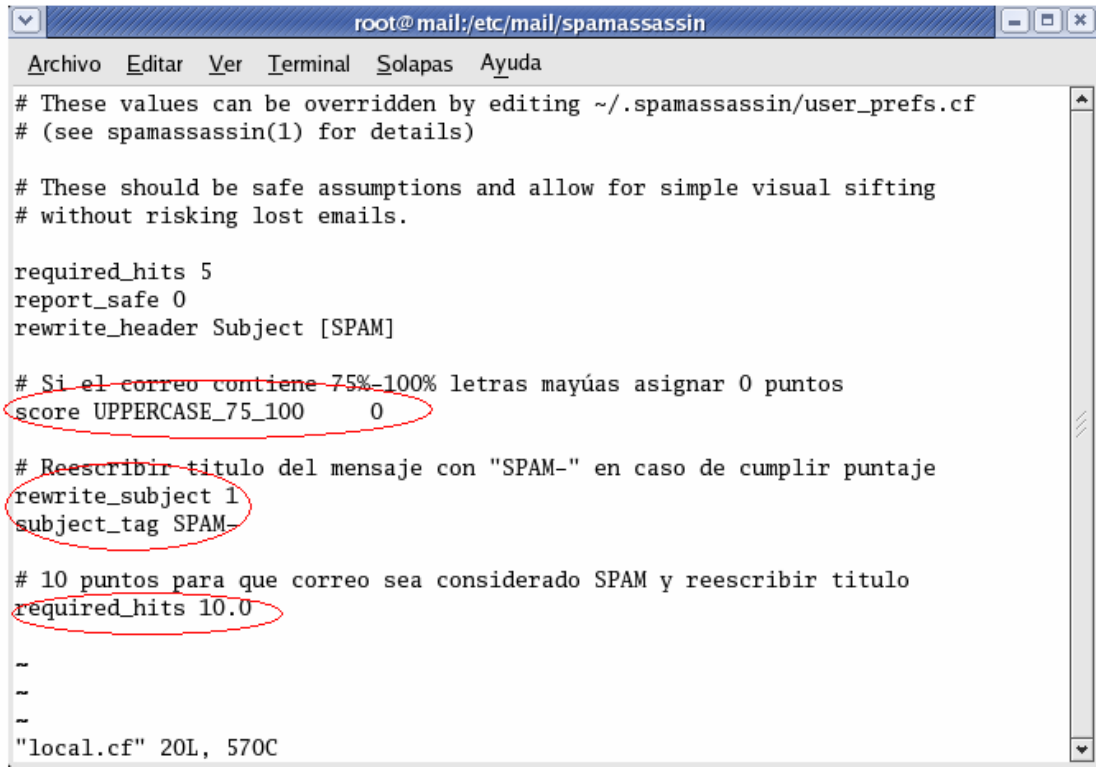

Figura 4.3 Reglas básicas del SpamAssassin para filtrar spam.

La primera declaración -- score UPPER_75_100 -- indica una reasignación de puntaje a cero sobre aquellos correos que contengan entre el 75% y 100% de su cuerpo en letras mayúsculas, esto evita que al ser inspeccionados mensajes de este

tipo su puntaje se eleve considerablemente. La segunda sección indica que el titulo original ("Subject") del mensaje sea modificado agregando el vocablo "SPAM" lo cual facilita su clasificación una vez que el correo sea descargado a una utilería en PC (Outlook, Eudora, Mozilla). Finalmente, la definición required_hits 10.0 indica que aquellos mensajes con un puntaje mayor a 10 les sea agregada la leyenda antes mencionada a su titulo ("Subject").

Aunque en las definiciones anteriores sólo se declaro una regla de SpamAssassin, tome en cuenta que el puntaje de todo mensaje será evaluado en base a los valores pre-definidos ("default"), esto lo obligará a llevar acabo ajustes constantemente sobre el proceso de filtrado, ya sea modificando el umbral de puntaje (required_hits) o cambiando los puntajes de reglas individualmente.

4.5 Entrenamiento del SpamAssassin

Ningún filtro de correo indeseado identifica todo correcto siempre y hay 2 tipos de errores. Los Negativos Falsos son malos, porque significa que un correo no deseado fue omitido y logro escaparse a través de la red. Los Positivos Falsos, son sin embargo peores, porque puedes omitir algo que deberías haber visto, que se ha marcado con la etiqueta de correo indeseado. Ningún filtro del correo indeseado debe ser configurado para ser eliminado automáticamente sin la revisión humana. El correo indeseado se debe enviar siempre a un área de cuarentena, que se debe revisar frecuentemente para asegurarse de que el correo genuino no se pierda.

Los pasos serán:

Mediante el servidor de correo, crearemos dos subcarpetas de la carpeta "Entrada" de la cuenta spam: una llamada Spam y otra llamada Ham

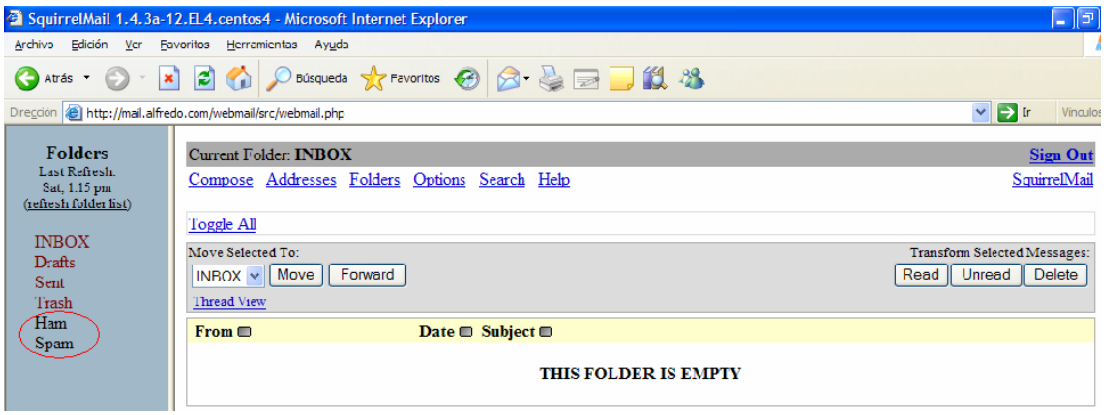

Figura 4.4 Creación de las Subcarpetas Ham y Spam en SquirrelMail

Periódicamente, el servidor de correo recogerá los mensajes del directorio /var/mail/spam/Spam y de /var/mail/spam/Ham y readiestraremos SpamAssassin según la nueva regla.

De esta forma, si recibimos un falso positivo (mensaje legítimo clasificado erróneamente como spam) sólo lo arrastraremos a la subcarpeta "Ham". Y al revés, en caso de falso negativo (mensaje de spam entregado como legítimo), lo arrastramos a la carpeta "Spam". No hará falta borrarlos, puesto que será el mismo servidor el que lo haga. Los falsos positivos, no los moveremos, sino que los copiaremos a la carpeta "Ham". El original, lo guardaremos en una carpeta legítima, a buen recaudo.
Dentro del entrenamiento del Spamassassin tenemos que configurar unos archivos que nos ayuden a determinar los correos buenos y los spam.
Para ello:

Escribimos "cd /etc/mail" sin parámetros para situarnos en el directorio de inicio.

Creamos dos directorios, uno llamado CorreoBasura (para procesar los mensajes de spam) y otro llamado CorreoBueno para procesar los mensajes legítimos.

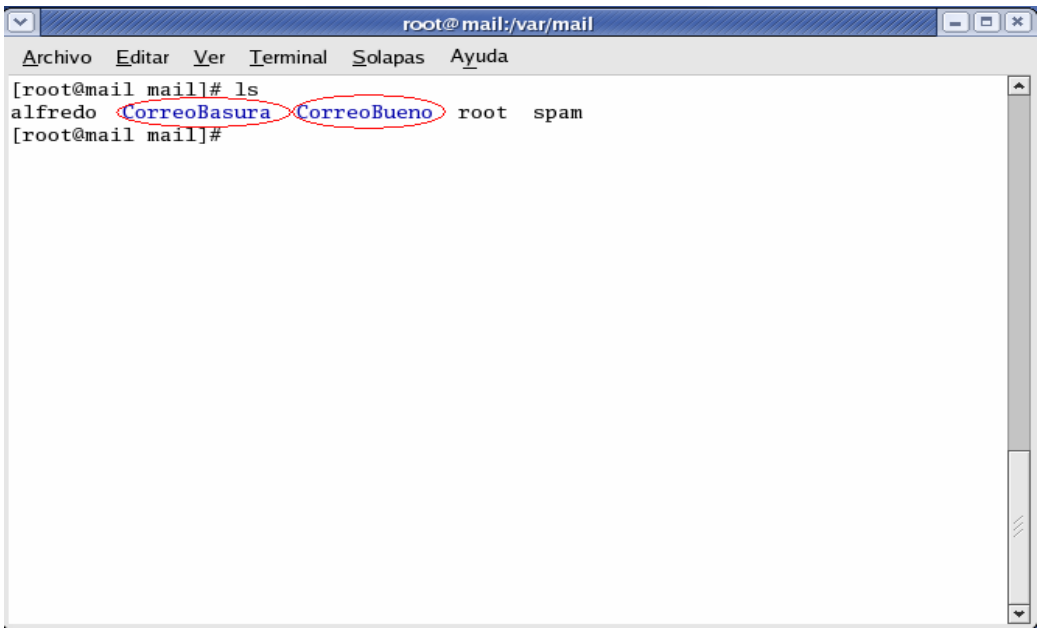

Figura 4.5 Creación de los Subdirectorios CorreoBueno y CorreoBasura para la eliminación del spam

Creamos un archivo llamado EntrenadorSpam dentro de “/etc/init.d” el cual nos va ayudar a procesar los correos.

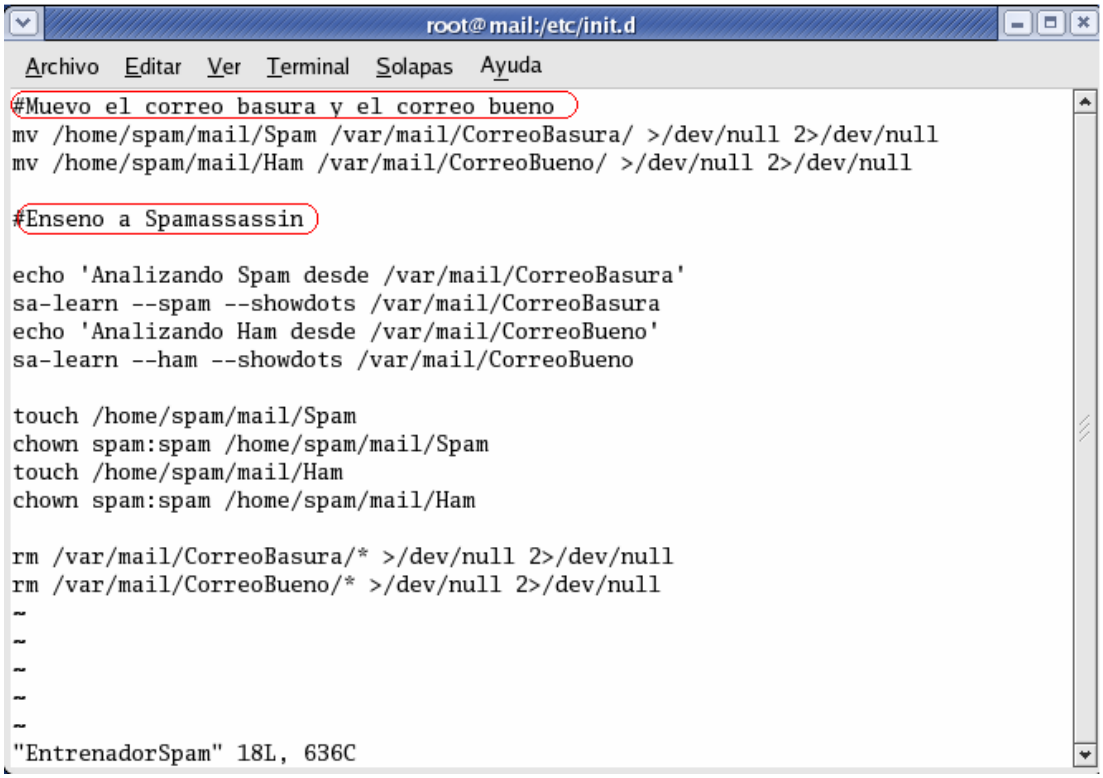

Figura 4.6 Archivo donde están los comandos para entrenar al SpamAssassin.

En las primeras dos instrucciones movemos los mail de las carpetas Spam y Ham a los directorios CorreoBasura y CorreoBueno respectivamente.

Luego enseñamos al spamassassin con las instrucciones sa-learn –spam –showdots para que reconozca los spam analizando el directorio CorreoBasura y lo mismo pero con sa-learn –ham –showdots para reconocer los correos que no son spam.

Entramos al servidor de correo como "root" y editamos su crontab (crontab -e)

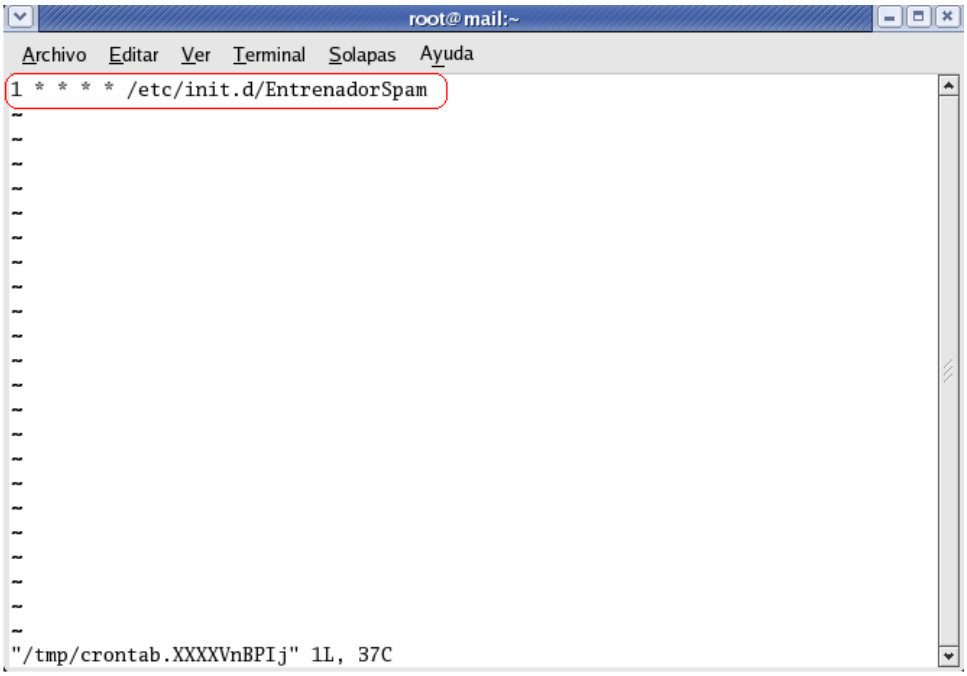

Figura 4.7 Intrucciones del crontab para inicializar el entrenamiento del SpamAssassin

En esta instrucción nos indica que cada hora se ejecutara el archivo EntrenadorSpam el cual es el encargado de procesar el correo.

Una vez terminado, borramos el contenido de los directorios spam y ham y los dejamos preparados para la próxima misión.

Los mensajes que se hayan clasificado correctamente como spam simplemente los borramos.

4.6 Aplicación del SpamAssassin

Configurado SpamAssassin, aun es necesario activarlo para que sea aplicado a todo mensaje electrónico entrante.

A continuación presentaremos un ejemplo de un mensaje que es filtrado por el Spamassssin y colocado una calificación que lo detecta como spam.

Primero enviamos un mensaje mediante el Outlook Express con el asunto spam y un mensaje que encontramos en la página principal del Spamassassin que nos ayuda a entrenar a este filtro reconociendo que correo es spam y que correo es ham (no-spam).

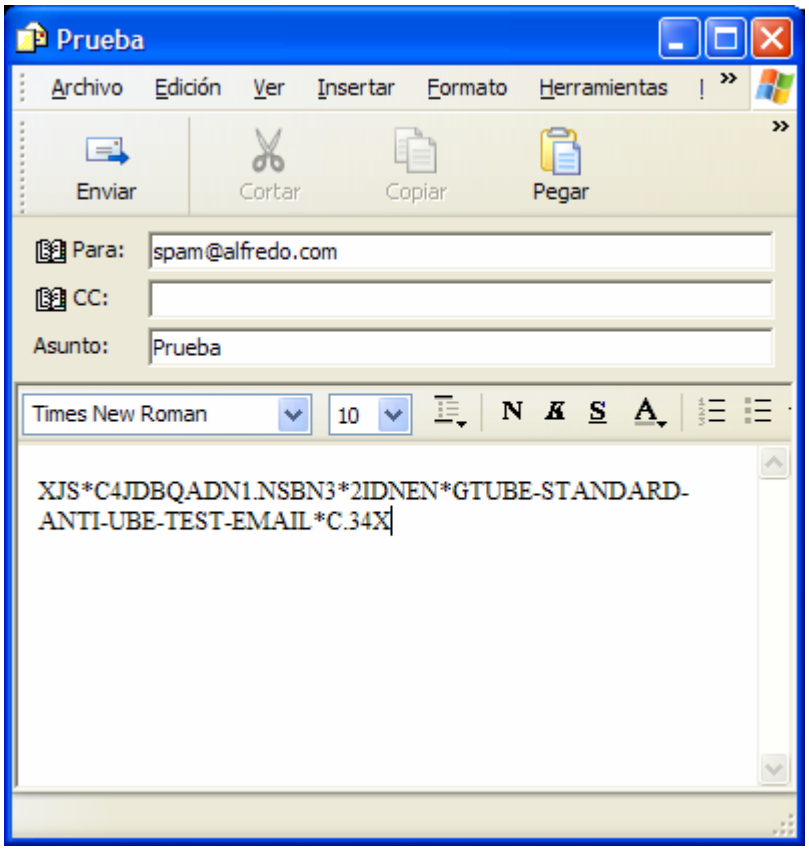

Figura 4.8 Envío de un correo spam

Una vez enviado el correo lo reconocemos en nuestro servidor de correo y entremos en la carpeta donde recibimos el correo y encontramos el siguiente resultado.

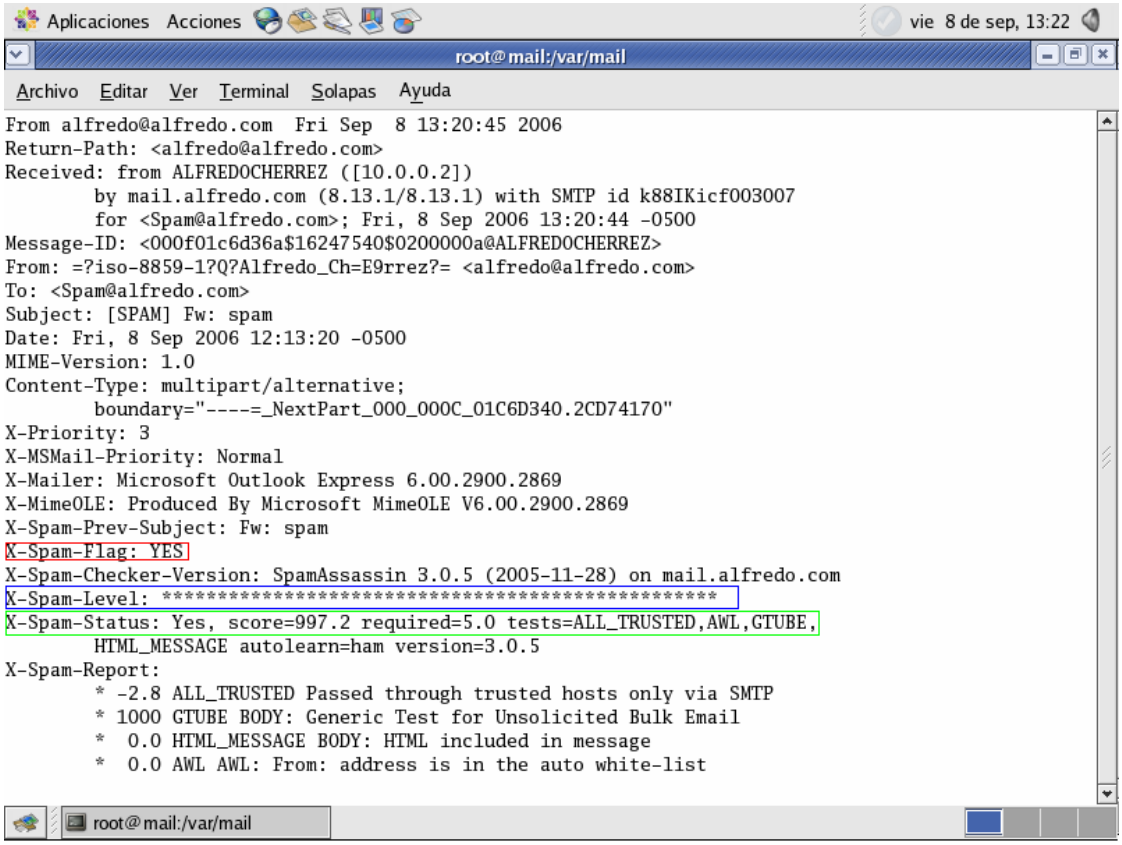

Figura 4.9 Calificación del SpamAssassin a un correo spam.

Como nos podemos dar cuenta en el rectángulo rojo nos dice que el correo es reconocido como spam al darnos YES como resultado.

En el rectángulo azul nos muestra una serie de asteriscos que para nuestro caso cada asterisco representa una puntuación que el Spamassassin esta asignando al mensaje.

Y en rectángulo verde observamos todo lo anterior pero con valores, aquí nos indica que es un spam que obtuvo un valor de 997.2 y que lo requerido para ser considerado un spam es un valor de 5.0.

Por lo tanto spamassassin le coloca una cabecera indicando que el mensaje de correo es spam y dejamos que e usuario decida que hacer con dicho mensaje.

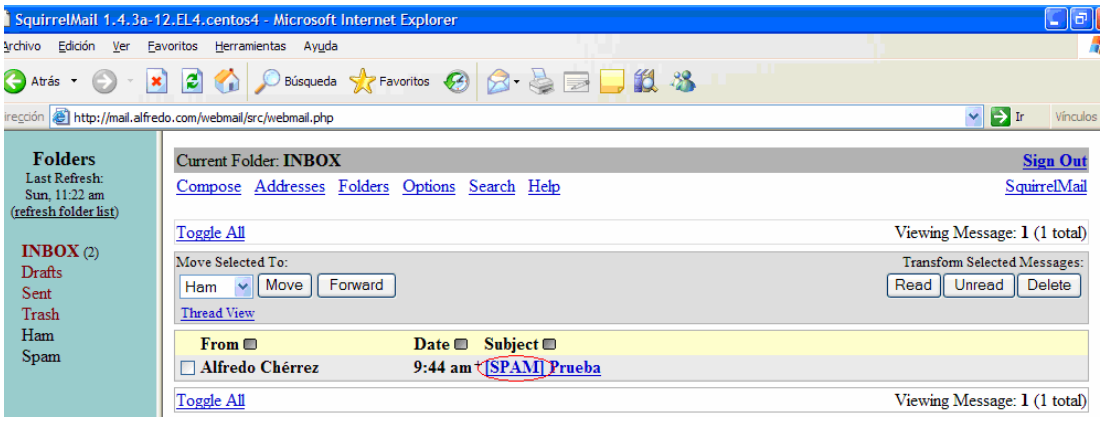

Figura 4.10 Asignación de Spam ala cabecera de un correo

Ahora vamos a enviar un mensaje que no es spam para ver la diferencia de puntaje y comprobar que no coloca una cabecera de spam.

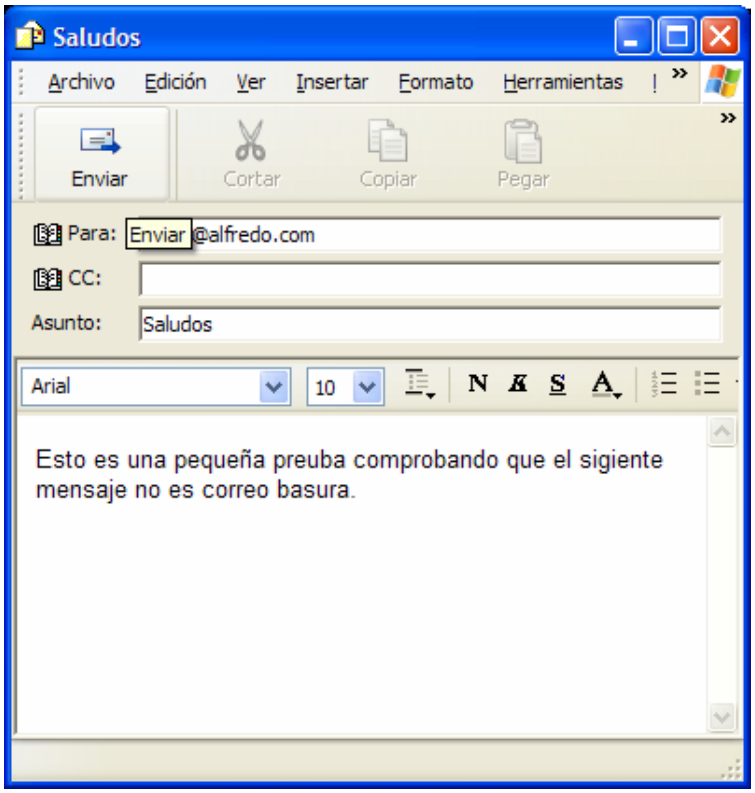

Figura 4.11 Envío de un mensaje de correo normal

Miramos dentro del archivo que se encuentran nuestros correos y obtenemos lo siguiente.

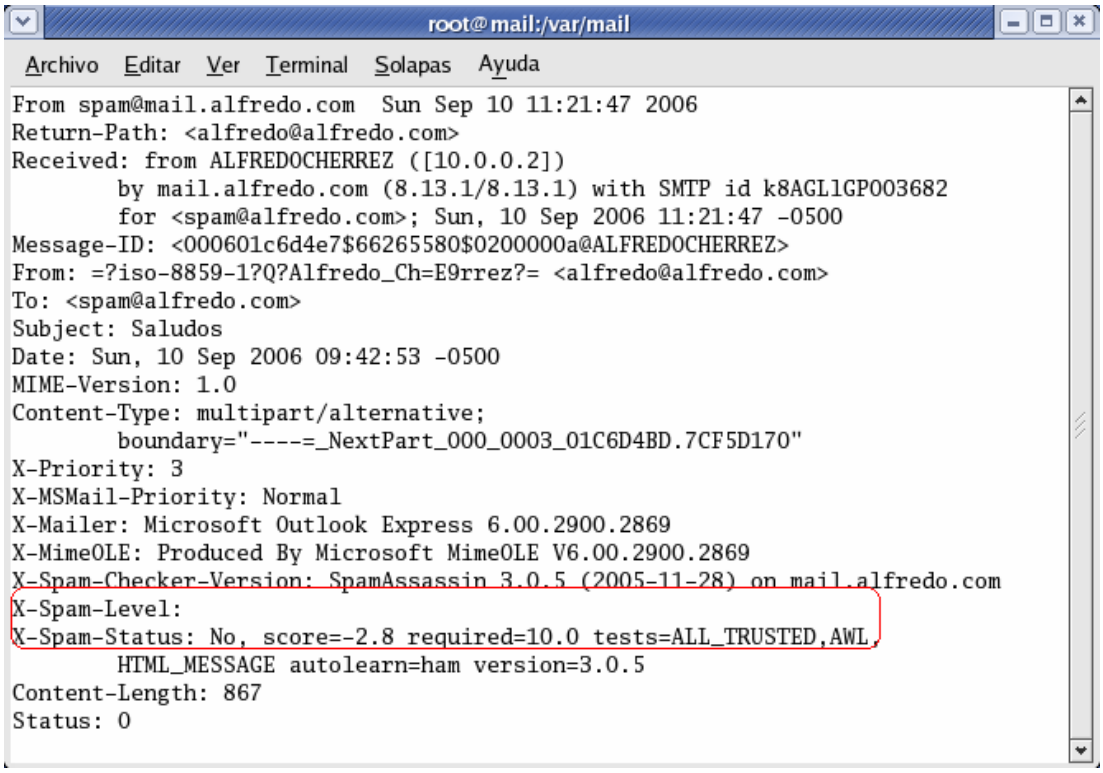

Figura 4.12 Calificación del SpamAssassin a un correo normal

Donde podemos observar que el Spam-Level no contiene ningun asterisco y Status que le proporcionan a este correo es No esto significa que no es un spam y su puntaje es sumamente bajo es de 2.8 por lo que el SpamAssassin no colocara ninguna cabecera en este mensaje.

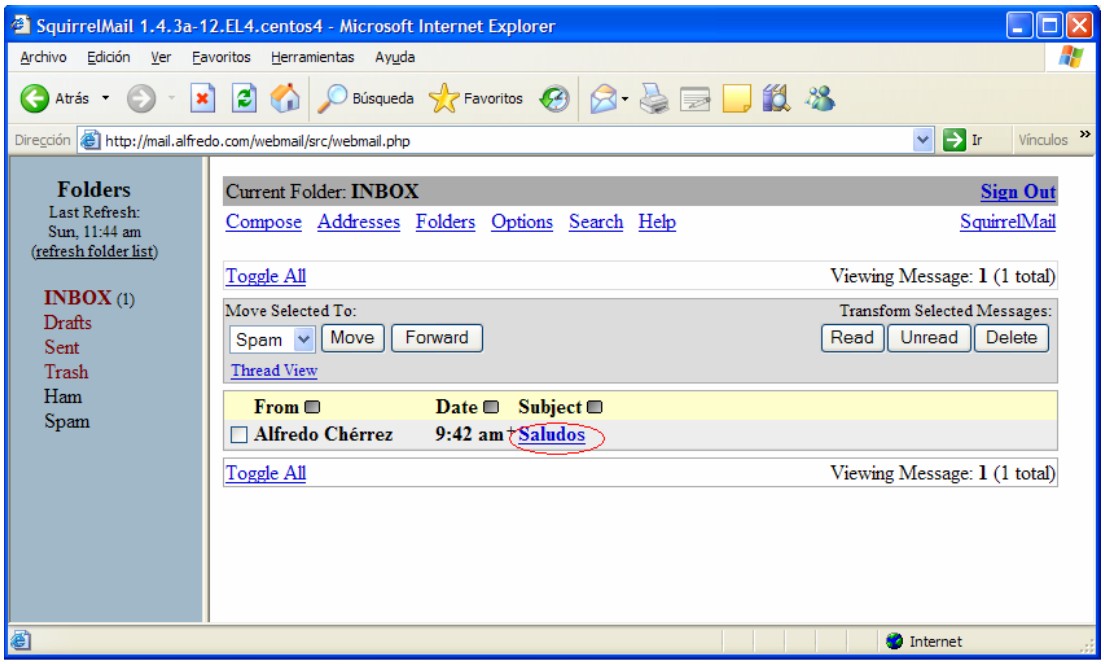

Figura 4.13 Un correo normal en su servidor de Correos

Como podemos observar este correo no contiene ninguna cabecera indicando que es un spam solo contiene el Subject que en este caso es Saludos.

4.7 Conclusiones

La configuración de este software no tubo ningun problema solo se tiene que tener un conocimiento básico de Linux ya que se tubo que configurar los parámetros de red y el DNS para poder configurar un servidor de correo que nos sirvio de gran ayuda en nuestro proyecto.

El entrenamiento del SpamAssassin tubo un poco más de complicación ya que no se pudo contar con una gran cantidad de correos para un mejor entrenamiento.

Además se tubo que crear unos directorios y archivos con una serie de instrucciones.

CAPITULO 5. HERRAMIENTAS ADICIONALES

Introducción

Para el control del spam con el filtro Spamassassin se utilizan varias herramientas entre las cuales podemos distinguir el Procmail la cual utilizamos en nuestro proyecto para un mejor funcionamiento del control del spam.

A continuación describimos brevemente esta herramienta y la configuración que se debe realizar para el correcto uso de la misma con el software libre Spamassassin.

5.1 Descripción del Procmail.

Procmail es un software que permite filtrar el correo que nos llega.

Nos permite reenviar guardar el correo en distintas carpetas, reenviar mensajes a otras direcciones de correo o ejecutar programas, sobre ciertos mensajes.

Procmail funciona gracias a un sistema de reglas que él tiene configurado después de determinar si el mensaje que él trató satisface en particular a una regla, ejecuta la acción asociada a la regla.

Cada vez que nos llega un mail, procmail lee la configuración del usuario al que va dirigido. Si ese fichero no existe, procmail deja el mensaje junto al resto de nuestro correo.

Este fichero de configuración se encuentra en nuestro directorio HOME (~), y se llama .procmailrc

5.2 Configuración de Procmail.

Para empezar a usar procmail y filtrar nuestro correo deberemos crear un archivo ~/.procmailrc .

Este fichero consiste en una serie de reglas. Cada regla está formada por una serie de condiciones y una acción.

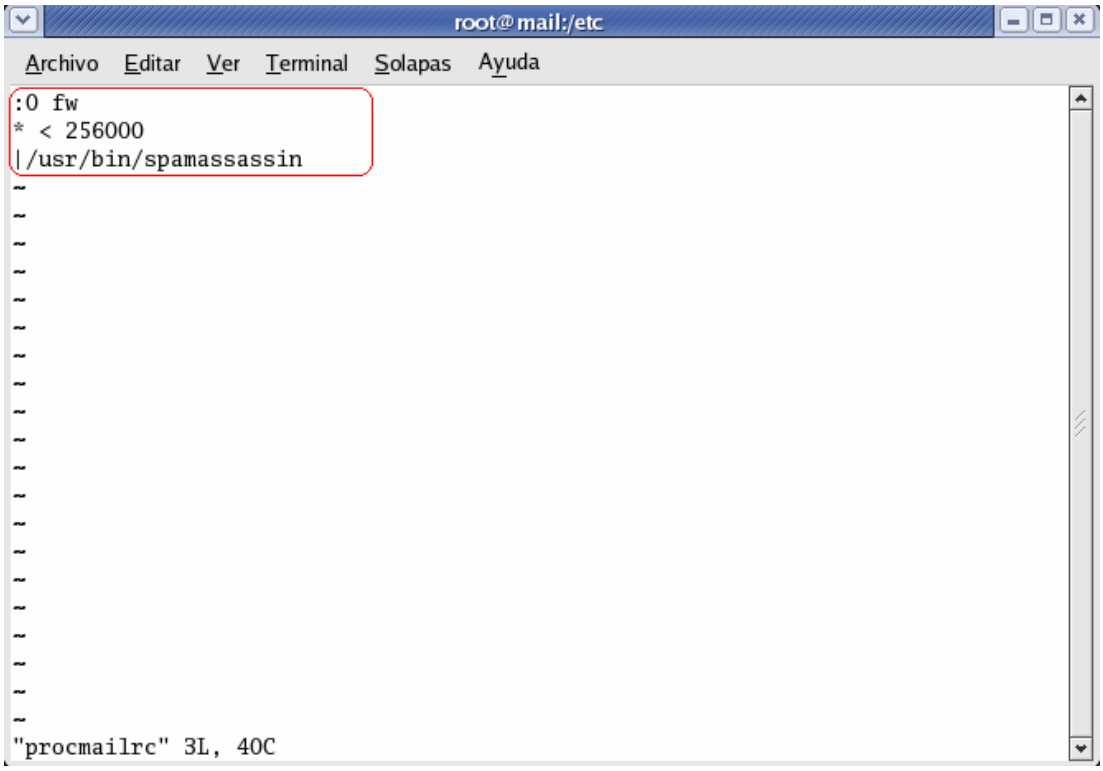

Figura 5.1 Configuración del Procmail para el SpamAssassin

Las siguientes lineas corresponden a las instrucciones de ejecución a ser colocadas dentro de procmail :

Las instrucciones de procmail indican la lectura de todo mensaje (:0) y su redirección hacia el ejecutable de SpamAssassin para ser procesado.

Procmail procesa ciertas reglas de forma secuencial, y si el mail cumple las condiciones de una regla, procmail ejecuta la acción y, si no se especifica lo contrario, no procesa las siguientes reglas.

La sintaxis básica de una regla es:

:0:

* condicion_1

* condicion_2

...

accion

Las condiciones son expresiones regulares que se comparan con las cabeceras del mensaje, o con el valor de alguna variable de procmail.

Comunmente, se trata de comparaciones con los campos Subject, From o To de la cabecera del mensaje.

Por ejemplo:

* ^Subject: AVIS

* ^From:.* lclsi

La primera condición especifica los mensajes cuyo campo Subject empieza por "AVIS". La segunda, aquellos cuyo From contiene "lclsi".

La acción es una de las siguientes:

buzón

Indica a procmail que el mensaje se debe guardar en ese buzón .

! dirección

Indica que se debe reenviar el mensaje a otra dirección de correo electrónico.

| comando

El comando especificado será ejecutado, y el mensaje se pasará como entrada.

Para nuestro estudio de spam hemos aplicado una regla a este fichero pidiendo que elimine los correos con Spam.

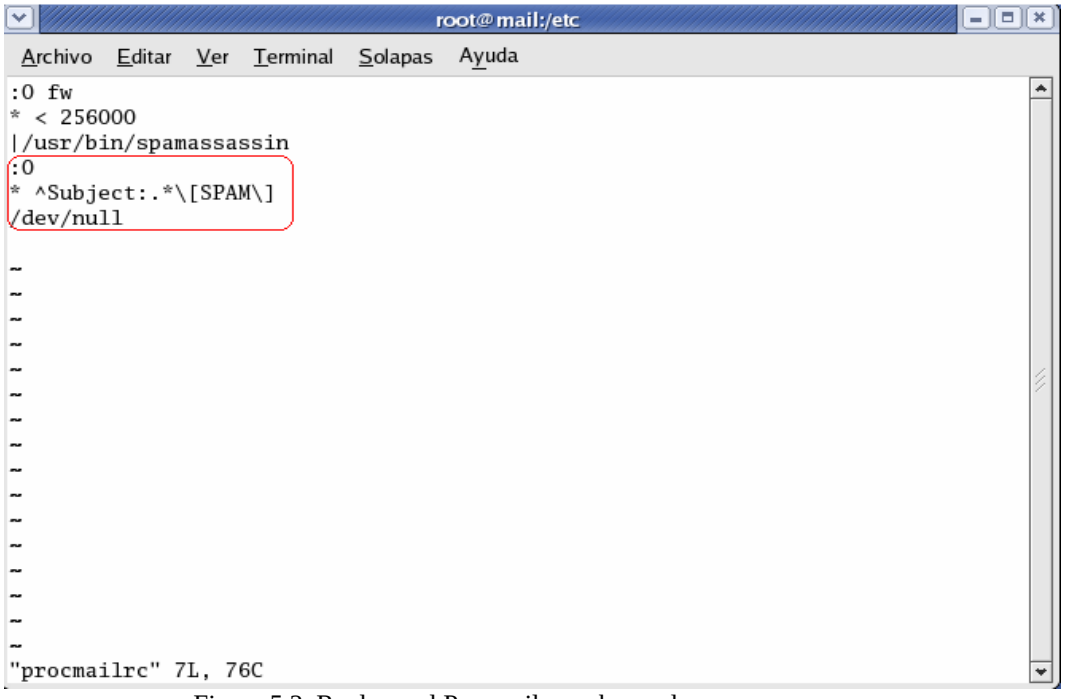

Figura 5.2 Regla en el Procmail para borrar los correos spam.

Esta regla esta eliminando los correos que contengan [SPAM] en su Subject como vimos que SpamAssassin coloca esta cabecera a los mensajes que considera spam.

5.3 Conclusiones

Esta herramienta es muy útil para muchos propósitos en nuestro caso la hemos utilizado para eliminar el spam que es filtrado por el SpamAssassin pero nos podría también ayudar a eliminar virus y a clasificar o reenviar correos.

CONCLUSIONES

El correo electrónico es un medio extremadamente necesario en nuestros tiempos ya que gracias a su ayuda se acortan distancias, se mejora el trabajo y la economía y un sin fin de usos que este servicio presenta para nuestro beneficio.

Sin embargo existen muchas personas o empresas que utilizan este servicio para perjudicar a la gente y así poder obtener un beneficio económico, enviando miles de correos a diferentes personas con el fin de hacer propaganda de algunos productos que en muchos de los casos no son vedad o simplemente no existen. Estos mensajes inundan la red y molestan a muchos usuarios que tienen que mal gastar tiempo y dinero revisando cientos de correos que le llegan a diario sin su autorización.

Como pudimos darnos cuenta estas personas se basan en cientos de métodos para obtener una dirección de correo electrónico valida para su uso y en muchos casos para vendérselos a otras personas que se dedican a lo mismo.

Existen muchos mecanismos de seguridad que se puede tomar para evitar recibir correo indeseado entre estas podemos tomar en cuenta el no exhibir nuestra dirección de correo en cualquier pagina o cadena se envían por Internet ya que la mayoría utiliza estas cadenas para obtener una lista de correos, otra alternativa es tener dos cuentas de correo lo cual no me parece muy adecuado.

El manejo de un antispam es algo necesario en estos días ya que los que envían estos correos van a encontrar la forma de conseguir direcciones verdaderas.

SpamAssassin es una herramienta que si se usa adecuadamente y se lo entrena constantemente es muy poderosa filtrando los correos buenos de los correos indeseados o llamados spam.

Esta herramienta nos permite miles de condiciones y reglas para filtrar los mensajes de correo pero un servidor no puede aplicar todas las reglas o condiciones existentes ya que cada usuarios tiene un criterio diferente de considerar un correo spam o no.

BIBLIOGRAFIA

Artículos de Internet:

SCADPlus Medidas contra las comunicaciones comerciales no solicitadas (spam) http:// europa.eu [Consulta 1 de Agosto 2006]

ANTIVIRUS Que es Spam_ Técnicas, Detección y Prevención de Spam http://www.antivirus.cc/ [Consulta 1 Agosto 2006]

BRUJULA.NET Spam http:// www.brujula.com.ar [Consulta 1 Agosto 2006]

AULACLIC S. Correo no deseado http:// www.aulaclic.es/ [Consulta 1 Agosto 2006]

ENCICLOPEDIA Correo basura http:// enciclopedia.us.es/ [Consulta 1 Agosto 2006]

ÁLVARO MENDOZA MERCADEOGLOBAL.COM Spam http://www.rompecadenas.com.ar/ [Consulta 1 Agosto 2006]

SPAMASSASSIN http://spamassassin.apache.org/ [Consulta 25 de Julio 2006]

EMILIO FLORIDO Luchando contra el Spam www.eldemonio.org- [Consulta 27 julio 2006]

http://lists.badopi.org/pipermail/ [Consulta 5 de Septiembre 2006]

FREEBSD Manual de FreeBSD http://www.freebsd.org/ [Consulta 5 Septiembre 2006]

ANEXOS