Capítulo 3.
Evaluación de características de seguridad en soluciones antispam comerciales

3.1 Introducción

En la actualidad, el correo electrónico se ha convertido en una parte fundamental de nuestra forma de comunicación con el mundo exterior, permite comunicarnos con gente de todo el mundo de manera prácticamente instantánea. Un mismo correo puede ser enviado a varias personas a la vez, además de permitir enviar archivos de todo tipo. dicho escenario era casi imposible de imaginarlo unos años atrás cuando el correo era solo por vía física cuando el cartero llevaba las cartas a cada domicilio, sin embargo, en medio de tanta información, resulta interesante saber cuáles de los correos que recibimos son en realidad confiables y de nuestro interés.

Además de los correos personales y de cuestiones de trabajo, existen otros, los cuales desconocemos su origen y el modo en que el remitente obtuvo nuestra dirección de correo electrónico. La vía más utilizada de envío de spam es la basada en el correo electrónico, pero también puede presentarse por programas de mensajería instantánea o por teléfono celular.

El spam es utilizado, por lo general, para el envío de publicidad, aunque también se usa en la propagación de códigos maliciosos. Además de los riesgos que representa el spam por el envío de contenidos dañinos, y por la molestia que causa al usuario recibir publicidad no deseada; también existen efectos colaterales de su existencia, tales como son la pérdida de productividad que genera en el personal la lectura de correo, y el consumo de recursos (ancho de banda, procesamiento, etc.) que generan este tipo de correos.

El gran crecimiento de los buscadores de Internet ha dado lugar al nacimiento de los llamados Spamdexing, que consiste en la modificación deliberada y deshonesta de páginas html para incrementar la posibilidad de aparecer primeras como resultado de una búsqueda.

3.2 Software Antispam

Resulta útil encontrar alguna medida que proteja a los usuarios del envío masivo y malintencionado de correo electrónico. Se conoce con el nombre de “herramientas antispam” a todo aquel software o dispositivo que se encarga de detectar y eliminar los correos no deseados. El objetivo principal de una herramienta antispam es filtrar el tráfico de correo electrónico, eliminando el correo no deseado a la vez que detecta aquellos mensajes que son de nuestro interés permitiéndoles el paso a nuestra bandeja de entrada.

Las herramientas antispam utilizan diversos mecanismos para filtrar el correo no deseado. Algunas técnicas hacen uso de diccionarios, los cuales son consultados por la herramienta antispam en nuestro propio sistema y tienen como función el detectar palabras o patrones específicos que suelen aparecer en el correo spam. Este diccionario puede ser configurado de manera manual, con palabras y frases que el propio usuario relaciona con correos malintencionados, o puede ser producto de alguna aplicación diseñada para tal fin. Otra técnica es el uso de listas de confianza.

De acuerdo con esta clasificación, los tipos más utilizados de listas son negras y blancas. Se definen como listas blancas a todas aquellas direcciones de correo que se consideran de confianza y de las cuales el usuario siempre desea recibir correos. En el otro extremo están las listas negras, dentro de las cuales están identificados remitentes de correo spam. De este modo, el antispam se encarga de bloquear el paso de los correos cuya dirección está contenida en alguna lista negra y de permitir el de las direcciones contenidas en las listas blancas.

También existen las llamadas listas grises propuestas por Evan Harris para intentar limitar la recepción de mensajes que se considera que podrían ser spam.

Se refiere al proceso por medio del cual el servidor de correo (a nivel del protocolo SMTP) rechaza el mensaje enviado y pide que éste sea reenviado. Esta técnica trata de aprovechar la existencia de "errores temporales" en el estándar SMTP. Un MTA que funcione conforme a dicho estándar reintentará el envío. Los MTA

utilizados por los spammers no suelen cumplir con los estándares y generalmente envían mensajes en masa sin preocuparse si han llegado correctamente.

El filtrado por medio de las listas grises generalmente es utilizado por SpamAssassin, una herramienta de filtrado de correo electrónico para servidores. SpamAssassin realiza este tipo de filtrado basado en sus bases de datos internas cuando sospecha que alguna fuente de correo (servidor) está enviando mensajes de correo electrónico de tipo spam.

Desde cierto punto de vista, mientras las listas negras se refieran estrictamente hablando a las listas de servidores o cuentas de correo desde las cuales está prohibido recibir correo y listas blancas se refiera a las que son inmediatamente autorizadas (verificadas), las listas grises se refieren a aquellas de las que no se tiene conocimiento aún (no son fuentes confiables de envío de correo, pero tampoco son fuentes confirmadas como emisores de spam) o bien, dependiendo de las políticas internas del servidor en el cual se implementa el filtro, se refiere a las sospechosas de estar difundiendo spam.

Las técnicas remotas, a diferencia de las locales, utilizan herramientas que se conectan a servidores remotos, los cuales se encargan de determinar si un correo es spam o no. Estos servidores utilizan grandes bases de datos que contienen direcciones de correo electrónico, palabras, frases, entre otros patrones para identificar el correo electrónico no deseado. Existe una gran diversidad de productos que pueden ayudarnos a resolver el problema del spam, tanto versiones gratuitas como comerciales.

Las técnicas antispam se aplican mediante distintos programas que se encuentran a disposición de los usuarios en Internet o en negocios especializados en informática. Es necesario seleccionar aquella opción más adecuada para nuestros intereses, ya que por ejemplo no es lo mismo un antispam para un usuario común que para la red completa de una empresa. También reviste vital importancia el tipo de navegación que realicemos habitualmente y si nuestra actividad o intereses insumen la necesidad de descargar muchos contenidos y archivos desde internet. En los últimos tiempos se han desarrollado diferentes técnicas para filtrar el correo

no deseado o spam. En algunos casos, estos programas actúan en los encabezados de los mensajes, otros se especializan en el cuerpo de los mismos, un tercer grupo se enfoca en las direcciones de los remitentes y otros trabajan con el mensaje completo.

Las técnicas y alternativas disponibles.

Los programas antispam más efectivos son los que combinan varias técnicas de las mencionadas anteriormente. De entre todas las posibilidades, las técnicas que encaran el mensaje completo parecen tener más opciones para lograr una mayor efectividad antispam. Vamos a ver el funcionamiento y las características básicas de las técnicas indicadas anteriormente:

- Filtros que actúan en la dirección del remitente: estos filtros antispam desarrollan su tarea sobre el campo del mensaje, es decir, donde puede determinarse la dirección o el dominio del remitente. A su vez, también detectan algunas palabras que figuren en el asunto o en el texto del correo para determinar si el mensaje es o no un spam. Esta clase de técnicas ha perdido efectividad debido a que los spammers las burlan fácilmente (véase figura 3.1).

X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MjtTQ0w9Ng==X-Message-Status: n:0

X-SID-PRA: Jess <tpaesefjks@4y813k4W35r.com>

X-Message-Info:
P3NBY493gE4b+MtahrAQLz+y/tMPHXWiXobcK5lbB4F9O3wSIhadbVu9hRPGZfwqyt+yfNU1+wKHNbJjfcgt1s2VjHTzzJEu

Received: from .com ([83.111.107.18]) by SNT0-MC1-F47.Snt0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);

Date: Fri, 19 Jan 2001 05:22:07 -0500

From: Jess <tpaesefjks@4y813k4W35r.com>

Subject: Hows your weekend?

Figura 3.1 Filtros en la dirección del remitente

- Filtros sobre el cuerpo del mensaje: en este caso, el análisis se centraliza en el texto principal del correo electrónico. Aunque puede ser efectivo al

detectar determinados términos que caracterizan al spam, tienen la desventaja de no tener en cuenta el campo o los encabezados (véase figura 3.2).

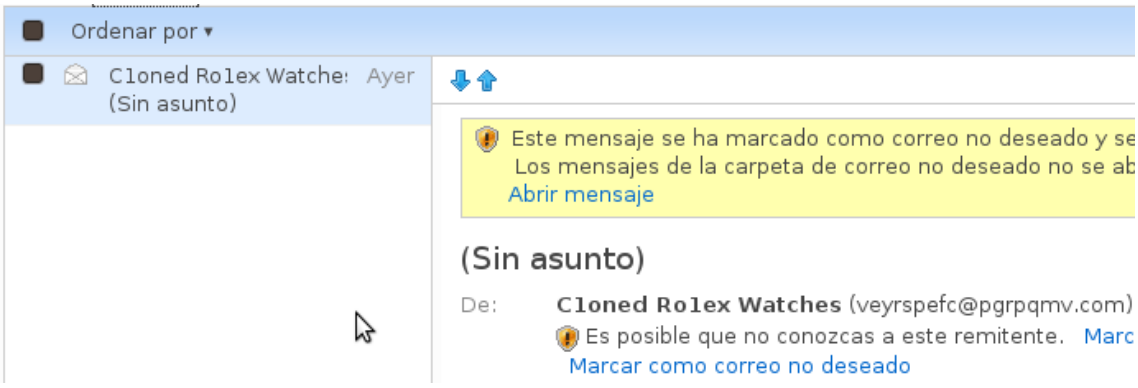

Figura 3.2 Filtros sobre el cuerpo del mensaje

- Filtros centrados en el contenido integral: suelen ser los más efectivos, ya que tienen en cuenta todos los aspectos del mensaje. Estudian las fórmulas básicas que manejan los encabezados, textos y campos de los correos no deseados, para así detectarlos más rápidamente y con mayor eficacia.

Otra de las técnicas que completa el análisis de los mensajes que llegan a la bandeja de entrada de cada cuenta de correo electrónico es el filtrado Bayesiano, que trabaja concretamente con los contenidos de los mensajes, identificando patrones de texto que se reiteran en los mensajes con spam para poder así detectarlos.

Al igual que sucede con los antivirus, los antispam se actualizan continuamente y van adquiriendo nuevas funciones para incrementar su potencial de protección.

3.3 Herramientas Antispam para correo electrónico

Dentro de las herramientas antispam, existen unas que son gratuitas o de libre distribución y que no implican ningún costo para utilizarlas.

Dentro de todo servidor de correo es indispensable contar con alguna herramienta antispam que nos ayude a realizar el filtrado de los correos que pasen por nuestro servidor antes de ser enviados a su destino final.

Estas herramientas, por lo general, son fáciles de conseguir, de instalar, de configurar, usar, etc. Una de las herramientas más importantes y usadas actualmente en spamassassin, que es un programa distribuido bajo la licencia Apache 2.0 y se usa principalmente para el filtrado de correo electrónico en busca de mensajes con spam mediante el uso de reglas.

Utiliza una gran variedad de técnicas de detección de spam, que incluyen algunas basadas en DNS y sumas de comprobación, contiene programas externos de filtrado bayesiano, listas negras y bases de datos en línea para realizar su trabajo.

Spamassassin puede ser integrado con el servidor de correo para filtrar automáticamente todos los mensajes que pasen por el servidor. También puede ser ejecutado de forma individual por el usuario dentro de su propio buzón de correo, es altamente configurable, si se utiliza como filtro de todo el sistema todavía puede ser configurado para soportar por las preferencias del usuario.

3.4 Características y funcionamiento

Es una aplicación basada en Perl. Puede ejecutarse como una aplicación independiente o como un subprograma de otra aplicación (como MailScanner) o como un cliente (spamc) que se comunica con un proceso en específico (spamd). El último modo de operación da beneficios en cuanto a rendimiento, pero en determinadas circunstancias, puede introducir riesgos de seguridad adicionales.

Spamassassin utiliza más de 100 reglas para identificar los mensajes de correo. Si el mensaje llega al puntaje requerido viene marcado en la línea de asunto del mismo mensaje como spam a través de un tag. Cada vez que el puntaje sea más alto, el correo tiene más probabilidad de ser spam. A puntaje bajo, corresponde casi siempre un mensaje de correo que no es spam.

Todo este proceso es añadido al mismo mensaje, en modo que el usuario pueda darse cuenta del porqué un determinado mensaje ha sido identificado como spam. Normalmente marca el mensaje con la cadena ** spam ** o [spam] en el asunto y explicando en el cuerpo por qué el correo recibido tiene aspecto de spam.

El usuario tiene que decidir qué hacer con esos correos. Por ejemplo, borrarlos directamente a nivel de servidor sin enterarse de su existencia.

Spamassassin toma el mensaje de correo (cabeceras y cuerpo) y busca determinados patrones. Por cada patrón que encuentra suma una determinada cantidad de puntos. Cuando los puntos superan un puntaje fijado por el usuario (por defecto es 5) el correo se marca como spam.

El puntaje y el valor de cada patrón son configurables por cada usuario, que además puede añadir nuevos patrones a buscar. Los patrones existentes, que son muchos, van desde ver si el remitente tiene una dirección que empieza por un número hasta buscar frases en el cuerpo como "viagra" por ejemplo.

Cada norma tiene un valor en puntos que se asigna a un mensaje si coincide con los criterios de la prueba. Las calificaciones pueden ser positivas o negativas, con valores positivos que indican "spam" y negativos los mensajes que no son spam. Un mensaje se compara con todas las pruebas y SpamAssassin combina los resultados en una puntuación global que se asigna al mensaje. Cuanto mayor sea la puntuación, mayor es la probabilidad de que el mensaje sea spam.

3.5 Alternativas

Además de spamassassin, existe una gran variedad de herramientas antispam gratuitas o libres, no necesariamente para servidores de correo, sino como clientes dentro del equipo de cómputo de los usuarios, entre las cuales están las siguientes:

K9 Antispam.

K9 es un programa anti-spam realizado por Robin Keir. La principal diferencia de K9 con casi todos los demás programas anti-spam (incluso aquellos de pago) existentes es su forma de analizar y clasificar los mensajes. K9 no se basa en palabras fijas, patrones fijos o reconocimiento de mensajes conocidos. K9 aplica a la identificación de mensajes un filtro bayesiano, una estadística de todas las palabras y estructuras del mensaje, cuya media lo marcará como bueno o como spam. Este método, combinado con el aprendizaje de lo que el propio usuario considera y no considera spam, hace que alcance una precisión superior al 99%.

Funciona con cuentas POP3, a través de outlook y outlook express, detectándolas automáticamente en algunos casos o insertando la configuración manualmente tú mismo. Puedes configurar una 'lista negra' para considerarlos spam automáticamente, y una 'lista blanca' para realizar exactamente lo contrario; evitar que sean considerados como tal.

SpamAware

SpamAware actúa como un filtro para el cliente microsoft outlook controlando qué correos son seguros y cuáles pueden ser eliminados sin tener que preocuparse.

El programa actúa mediante el motor Spamassassin que hace la selección de correos perjudiciales seleccionándolos como tales. En caso de confusión, SpamAware permite establecer una lista negra para determinar que destinatarios queremos que el programa bloquee, y una lista blanca para que los mensajes enviados por los destinatarios seleccionados en esa lista puedan ser abiertos sin problema.

Spamihilator

Spamihilator, una eficaz arma en la lucha contra el spam. Se trata de un filtro que actúa entre cliente y servidor de correo electrónico, examinando a conciencia cada uno de los mensajes y dejando pasar sólo aquellos que cumplan ciertas normas.

Todo el proceso se realiza en segundo plano, sin que se tenga que hacer nada; lo único que se pide es modificar algunos parámetros de la cuenta de correo electrónico (usuario y servidor POP3) para adaptarla al filtro de Spamihilator, haciéndolo compatible con prácticamente cualquier cliente: outlook express, microsoft outlook, eudora, pegasus, opera, mozilla, netscape, becky, etc.

El programa usa un sistema de filtrado basado en los estudios matemáticos de Thomas Bayes, que calcula un tanto por ciento de probabilidad de un mensaje de ser spam, además de usar otros filtros más comunes como la existencia de ciertas palabras en el mensaje y el uso de una "lista negra" de remitentes bloqueados y otra "lista blanca" de remitentes admitidos.

La interfaz de configuración es muy sencilla y ofrece múltiples opciones, entre ellas la de cambiarla de idioma, pero no se recomienda ponerla en español porque sinceramente, se entiende mejor en inglés.

Spampal

SpamPal es un programa que se coloca entre el programa cliente de correo electrónico (eudora, outlook, etc.) y el servidor de correo electrónico. Spampal analiza el correo entrante del servidor de correo y aquel mensaje que considere spam (correo no deseado) le asigna una etiqueta especial y lo envía al programa cliente de correo. En el programa cliente de correo se definen filtros que se encargaran de enviar los mensajes recibidos con la etiqueta especial a una carpeta o buzón, desapareciendo de la bandeja de entrada de nuestro programa de correo habitual, de esta forma separamos nuestro correo del catalogado como spam.

Al comienzo del uso del programa SpamPal conviene revisar la carpeta o buzón donde se almacena el correo spam, pues puede ocurrir que se etiquete como spam correo que realmente no lo es, y para evitar que vuelva a ocurrir se añadirá la dirección de correo a las Listas Blancas ("WhiteList").

Este programa funciona de forma diferente a otras utilidades anti-spam, ya que se establece como un potente filtro entre el servidor y el cliente de correo, y no elimina los mensajes que considere como spam sino que los marca de forma especial añadiendo una etiqueta al asunto.

3.6 Equipos Antispam (Appliance)

Existe una variedad de herramientas antispam que no son gratuitas y que la mayoría de las veces tiene un costo muy elevado adquirirlas, pero ese costo también trae la ventaja de tener un soporte personalizado y en cualquier momento se puede consultar y tener contacto con los distribuidores de las diversas herramientas.

Algunos equipos cuentan con una interfaz Web y otros por línea de comandos para realizar la administración y configuración correspondiente. Para el caso de la interfaz web, la herramienta es relativamente sencilla para configurar, sin embargo, la interfaz por línea de comandos trae consigo un sistema operativo linux con el cual se puede realizar la configuracion de todos los parámetros necesarios.

Algunas razones por las que se prefieren Herramientas de Hardware (Appliances) para el filtrado del correo spam son:

- El cliente prefiere comprar Hardware en lugar de Software
- Facilidad de instalación
- Requerimientos de Sistema Operativo
- Independencia del Hardware existente

Realizan labores similares a una herramienta gratuita, pero con la gran diferencia de que este tipo de herramientas integran módulos que se encargan de clasificar a los mensajes que se detectan como posible spam. Uno de ellos es el manejo de cuarentena, que es donde se almacenan los correos sospechosos de ser spam y que se encuentran en revisión

Otro plus que tienen estas herramientas es que filtran también los mensajes que son detectados con virus adjuntos dentro de ellos, esto a su vez sirve para llevar un control sobre los tipos de virus más comúnmente detectados en este tipo de mensajes.

Además, estas herramientas cuentan con una consola de administración, mediante la cual se llevan estadísticas de la actividad de la herramienta, También muestra el monitoreo en tiempo real. Y permite realizar otras configuraciones adicionales en caso que se requieran (cambio de servidor de correo, cambio de ip de la herramienta, segmento de red, etc.).

Hoy en día, aparecen nuevos tipos de spam, en una era donde las amenazas crecen constantemente, las herramientas antispam tradicionales enfrentan retos importantes y no es suficiente tener una herramienta de este tipo actualmente, el uso de la seguridad en la nube será una buena opción para responder a estas amenazas. Hay que mencionar que la nube involucra al "software como servicio" y puede ser aplicado en la arquitectura de nube de seguridad. Una de sus principales caracteristicas es la defensa conjunta global y en línea en tiempo real. Recoger las amenazas globales de spam en todo el mundo utilizando grandes capacidades de cómputo para realizar una evaluacion temprana de amenazas conocidas.

La industria ha visto que una de las mejores opciones para resolver el problema del spam es el uso de los servicios de seguridad en la nube, ejecutar un fuerte análisis de las plataformas de cómputo, revisión en tiempo real de ataques a traves del e-mail, responder en un tiempo muy corto a estas amenazas, permitiendo a los usuarios obtener la mejor protección en tiempo real para reducir las amenazas existentes sobre el correo electrónico

Hace dos años, la industria de la seguridad había creado el concepto de "Seguridad a través de la nube para el e-mail", el desarrollo de nubes para la seguridad de los sistemas de correo electrónico, estableciendo seguridad en la nube por medio de las defensas tradicionales, tales como listas negras y blancas,

clasificación de bases de datos, algoritmos bayesianos, acceso dinámico para los recursos necesarios en servicios automatizados de 7 * 24 horas para el análisis de los sistemas y establecer sistemas de correo basados en patrones de comportamiento.

3.7 Metodología utilizada

La Subdirección de Seguridad de la Información UNAM/CERT realizó una serie de pruebas a algunas soluciones antispam que se encuentran actualmente en el mercado, esto con la finalidad de dar a conocer las fortalezas y debilidades con las que cuenta cada herramienta.

Cada herramienta se sometió a las siguientes pruebas:

- Efectividad en el filtro de spam, calidad y flexibilidad en el manejo de la consola de administración.
- Visualización de reportes y opciones de filtrado de los mismos.
- Efectividad en el filtro antivirus, detección y manejo de cuarentena, actualizaciones antivirus y manejo de consola de administración.
- Pruebas de carga durante envío masivo de correos con spam y virus.

3.8 Desarrollo del laboratorio de pruebas

Fue necesaria la implementación de un laboratorio para realizar las pruebas a las herramientas antispam, por lo que la Subdirección de Seguridad de la Información dispuso de dos equipos, los cuales se describen a continuación.

- devsecure.seguridad.unam.mx
- S.O. Debian 2.6.26 – 2 – 686
- Memoria RAM. 4 Gb
- Postfix 2.5.5 – 1.1

- ingecomp.seguridad.unam.mx
- S.O. Debian 2.6.18 – 5 -686
- Memoria RAM. 1 Gb
- Postfix 2.5.5 – 1.

A cada equipo del laboratorio se le configuró un servidor de correo postfix de manera local, esta configuración se realizó dentro del archivo /etc/postfix/main.cf, dentro de esta configuración se agregó lo siguiente:

Nombre del host. (ingecomp y devsecure respectivamente): es el nombre completo que le damos a nuestra máquina al instalar Linux. El valor por defecto es localhost.localdomain, pero es recomendable poner otro para evitar confusiones con algunos usos de localhost que se aplican incluso si se cambia el nombre a la máquina.

Nombre dominio. (seguridad.unam.mx): es el nombre del dominio en que se ubica la máquina; es todo lo que sigue al primer punto en el nombre del host.

La configuración es bastante sencilla. De hecho, es posible que el sistema funcionara sin necesidad de tocar nada. No obstante, es preferible asegurarse modificando los siguientes valores del archivo /etc/postfix/main.cf (es posible que algunos de estos parámetros ya figuren con los valores indicados):

myhostname = ingecomp.seguridad.unam.mx

mydomain = seguridad.unam.mx

myorigin = $myhostname

mail_spool_directory = /var/spool/mail

En la figura 3.3 se muestra de manera general la arquitectura lógica en la que se colocaron los equipos para la realización de las pruebas y por medio de la cual se realizó la comunicación y el envío de correo.

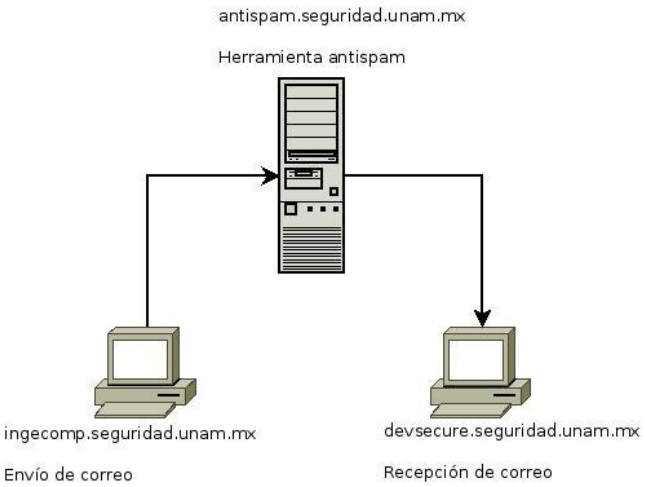

Figura 3.3 Diagrama de la Arquitectura del laboratorio de pruebas

El servidor DNS encargado de hacer la traducción de los nombres de dominio de cada uno de los equipos involucrados fue con el que cuenta el UNAM-CERT.

Un servidor DNS asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres entendibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del equipo ingecomp.seguridad.unam.mx es 192.168.101.118, la mayoría de la gente llega a este equipo especificando ingecomp.seguridad.unam.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

DNS funciona principalmente con base en el protocolo UDP. Los requerimientos se realizan a través del puerto 53.

Los correos electrónicos se enviaron desde diferentes cuentas en el equipo *ingecomp.seguridad.unam.mx*, hacia diferentes cuentas en el equipo *devsecure.seguridad.unam.mx*. La herramienta antispam recolectó todos los correos, los filtró y dejó pasar los que a su consideración, son correos electrónicos normales. Los correos que se clasificaron como spam o virus fueron alojados en la herramienta y no llegaron a su destino final.

El funcionamiento de una herramienta antispam en términos generales se representa por medio de la figura 3.4.

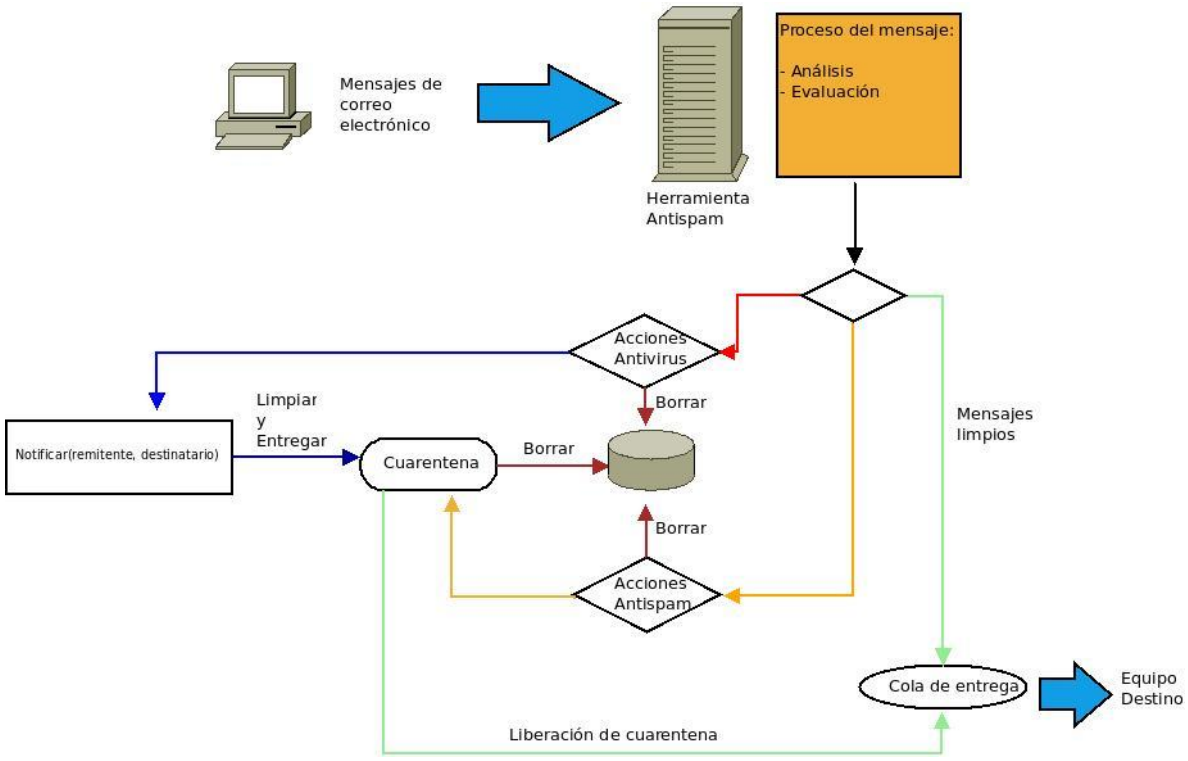

Figura 3.4 Funcionamiento general de una herramienta antispam

El envío de correo se clasificó en 3 rubros (véase tabla 3.1).

Tabla 3.1 Clasificación de correos enviados

CLASIFICACIÓN DE CORREO	Número de correos	Detalles
Spam	33255	Correos clasificados previamente como SPAM
Virus	1516	Correos que contienen archivos adjuntos clasificados como VIRUS
Correo normal	6460	Clasificado como correo válido en un 95%, sin embargo, el otro 5% podemos decir que se encuentra clasificado en SPAM, POSIBLE SPAM o VIRUS

Además, se realizaron pruebas de estrés mandando simultáneamente 52980 correos divididos en 4 cuentas desde el equipo ingecomp.seguridad.unam.mx que enviarán correos válidos, spam y virus a cuatro cuentas en devsecure.seguridad.unam.mx, para verificar la carga del procesador en la herramienta.

Para la realización de las pruebas se utilizaron dos scripts hechos en lenguaje perl, mediante éstos se realizó cada uno de los envíos de correo desde el equipo ingecomp.seguridad.unam.mx hacia el equipo devsecure.seguridad.unam.mx

Cada script tenía una misión diferente, uno se encargaba de hacer el conteo de los correos a enviar y el otro que era el principal encargado de hacer el envío de todos los correos. Se utilizó un tercer script hecho en Shell que se encargó de medir la carga de cpu observada al momento de hacer los envíos de correo masivo, esto con la finalidad de revisar el comportamiento de la herramienta ante un sobre flujo de correos.

En los apéndices se muestran estos scripts como referencia.