INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

TECNOLÓGICO DE MONTERREY

BASE-LINE DEL COMPORTAMIENTO DE SERVICIOS PARA DETERMINAR EL FINE-TUNNING DE MECANISMOS TECNOLOGICOS DE INFORMACION

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA
OBTENER EL GRADO ACADEMICO DE:
MAESTRO EN ADMINISTRACION
DE TELECOMUNICACIONES

POR
FLAVIO RAFAEL CARRANZA GONZALEZ

MONTERREY, N. L. JUNIO DE 2008

INSTITUTO TECNOLOGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

CAMPUS MONTERREY

TECNOLÓGICO DE MONTERREY

BASE-LINE DEL COMPORTAMIENTO DE SERVICIOS PARA DETERMINAR EL FINE-TUNNING DE MECANISMOS TECNOLOGICOS DE INFORMACION

TESIS

PRESENTADA COMO REQUISITO PARCIAL PARA
OBTENER EL GRADO ACADEMICO DE:
MAESTRO EN ADMINISTRACION
DE TELECOMUNICACIONES

POR
FLAVIO RAFAEL CARRANZA GONZALEZ

MONTERREY, N. L. JUNIO DE 2008

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

M.C. Ricardo Morales González

ALUMNO: CARRANZA GONZALEZ FLAVIO RAFAEL
MATRICULA : 770753

TESIS

Base-LINE del comportamiento de servicios para determinar el fine-tunning de mecanismos tecnologicos de información

COASESOR: Dr. Juan A. Nolazco

Objetivo: Seleccionar una aplicación genérica y un mecanismo tecnológico de seguridad de Información para establecer un modelo que permita determinar el comportamiento normal del servicio. (Web, **Emails**, Routers, etc)

Capitulo 1

1.1 SITUACION PROBLEMATICA

"La cosa maravillosa acerca del Internet es que estas conectado con quien sea en donde quiera que se encuentre. La terrible acerca del Internet, es que estas conectado con cualquiera..." Vint Cerf, citado en el bootcamp de Cisco (2003).

Con la expansión progresiva de Internet en servicios (correo electrónico, comercio electrónico, VoIP, servicios de almacenamiento, Video en demanda, etc.) y el uso de sistemas cada vez más desarrollados y automatizados, la penetración y aceptación de este medio de comunicación es mayor, así como su por su capacidad de generar conocimiento y de cierta medida, riqueza.

Por ejemplo Hoy por hoy, tenemos en México, aproximadamente 12 millones de usuarios de Internet, reportados por la AMIPCI (Asociación Mexicana de Internet), además de que las nuevas tecnologías tales como redes inalámbricas, Dispositivos Móviles, etc, permiten más penetración y la cantidad de usuarios es más basta dada la facilidad de conexión que estas herramientas permiten, lo que nos lleva a pensar que este crecimiento y este contacto con el resto de los usuarios globales, entre todos los dispositivos conectados a la red, es cada vez más desmedido y con mayores dificultades de controlar, esto debido a las amenazas ya sea de problemas en el servicio o Virus o cualquier agente nocivo de la red, además de las innumerables fallas por desconocimiento e imprudencia de la configuración de estos dispositivos, con todo lo cual se pudiera exponer información confidencial a ser destruida o manipulada. CISSP (2001).

Los servidores conectados a Internet simultáneamente por país, de entre los cuales pueden estar albergados muchos de los servicios mencionados previamente, así como información confidencial, el INEGI presenta la siguiente información, de entre la que hallamos a países como Estados Unidos, Alemania y Japón entre los países con mayor participación en equipos con servicios conectados a Internet y países como China y Malaria con muy pocos portales:

País	1997	1998	1999	2000	2001	2002
Total mundial	**30 116 706**	**43 545 197**	**72 004 971**	**106 708 678**	**141 382 198**	**144 978 564**
Alemania	1 132 174	1 449 915	1 635 067	2 040 437	2 426 202	2 594 323
Argentina	19 982	66 454	142 470	270 275	465 359	465 359
Australia	665 403	792 351	1 090 468	1 615 939	2 288 584	2 564 339
Brasil	117 200	215 086	446 444	876 596	1 644 575	1 644 575
Canadá	839 141	1 119 172	1 669 664	2 364 014	2 890 273	2 890 273
China	16 322	17 255	71 769	70 391	89 357	89 357
España	196 403	306 559	469 587	455 487	538 655	589 979
Estados Unidos de América	20 623 995	30 489 463	53 175 956	80 566 947	106 193 339	106 193 339
Francia	355 031	511 193	1 233 071	1 122 407	788 897	1 388 681
Italia	254 296	386 632	301 528	1 019 711	680 461	672 638
Japón	1 168 956	1 687 534	2 636 541	4 640 863	7 118 333	7 118 333
Corea	121 932	202 510	460 974	397 809	439 859	694 206
Malasia	32 269	47 852	59 012	68 248	74 007	74 007
México	**41 659**	**112 620**	**404 873**	**559 165**	**918 288**	**918 288**

Tabla I Servidores conectados a Internet por país (2002)

Como podemos ver de la tabla anterior, existe un numero creciente conexiones simultaneas desde cualquier parte del mundo, en las cuales residen utilerías públicas, sistemas de defensa militar, de instituciones financieras, equipo de medición, medico, etc. En México potencialmente el uso de los servicios de Internet que los usuarios invierten en tiempo cuando están conectados a la red se divide entre las áreas proyectadas a continuación, en la siguiente tabla siendo la actividad más común la lectura de correo.

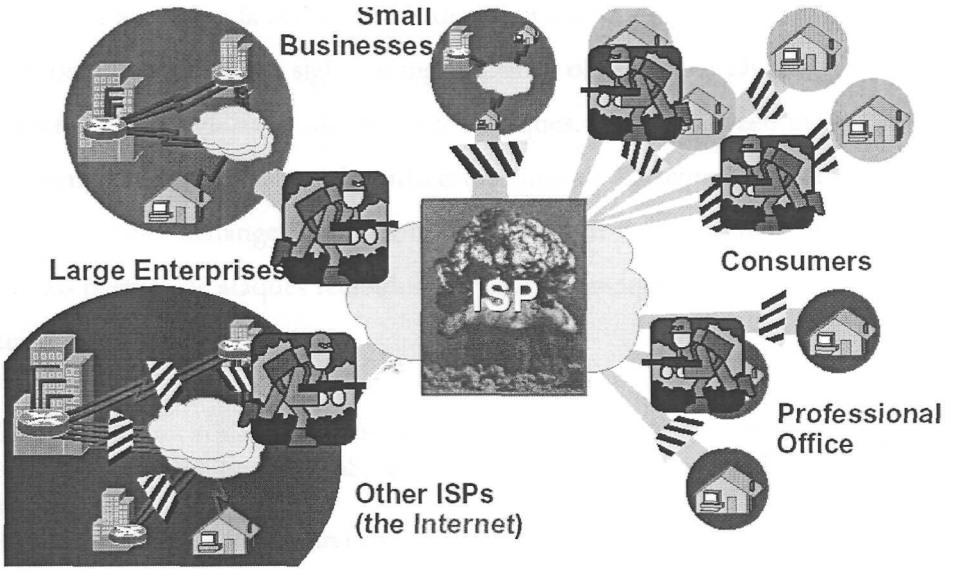
Concepto	Absolutos	Relativos
Correo Electrónico	4 226 298	25.9
Consulta o Investigación en Línea	4 173 144	25.5
Chat	2 844 475	17.4
Educación	2 304 668	14.1
Entretenimiento	2 069 771	12.7
Software	308 829	1.9
Video Conferencias	245 036	1.5
Otros	97 889	0.6
No sabe	68 585	0.4

Tabla II Uso de los servicios de Internet en México (2002)

Con todo lo anterior, no nos queda mas que experimentar cierto sentido de pánico ante este crecimiento exponencial de dispositivos conectados a Internet debido a las inminentes ataques informáticos por virus, gusanos de red, caballos de Troya, y toda aquellas amenazas potenciales alojadas en cualquiera de los **144 978 564** Servidores de Internet, INEGI (2003)

Todo lo anterior sin contar los cambios debido a este uso diversificado de la red ; Raveendran (2003) comentó en el ultimo Bootcamp de CISCO, que el uso de herramientas mas fáciles para los ciberpunks amateurs para hacer daño, han creado mas amenazas, así como la motivación que el manejo de valores monetarios a través del comercio electrónico a través de Internet crea en sus usuarios, todo esto, según Raveendran, ha llevado a ataques directos a la infraestructura de INTERNET, considera sagrada en antaño, Hoy día es muy común que los proveedores de servicios o ISP's (de sus siglas en Ingles Internet Service Provider) reciban de sus clientes llamadas de solicitud de ayuda debido a que están recibiendo ataques en sus servicios.

La gráfica siguiente nos puede dar una radiografía más inteligible del área de batalla que actualmente se vive en los servicios de Internet, bootcamp Cisco (2003).



Grafica 1- ISP's , sus abonados en el campo de batalla

Como sabemos los individuos que se conectan a Internet lo hacen mayormente para intercambiar correos, Sriagesh (1995), en su análisis del costo de estructuras e Interconexión y sus acuerdos, establece además, que las ganancias por parte de los ISP's por sus servicios andan del orden de entre los $5 Millones y los $118 Millones de dólares, pero que no existe un punto central de control y no

están regulados como los servicios telefónicos. Por lo que a través de los enlaces, hoy por hoy, viajen infinidad de datos entre los diferentes puntos interconectados, que igual pudiera ser información confidencial clasificada o un ataque para derribar alguno de los servicios de alguna empresa.

1.2 Hechos Reales

51% de los usuarios de correo electrónico en el trabajo revisan su correo al menos cada hora, incluyendo aquellos, 32%, que dicen que lo verifican constantemente. GALLUP ORGANIZATION (2000).

Como observamos, el correo se convierte en pieza fundamental para llegar a cada individuo en la red y de alguna suerte llevar a cabo ataques a las vulnerabilidades presentes en programas, equipos y configuraciones para acceder a la información, debido a ello hoy día podemos contabilizar entre 20 a 40 ataques de Dos/DDoS (de sus siglas en inglés Denial of service or Distribuited DoS) en la red en cualquier momento, por detallar el alcance estos ataques, según Raveendran (2003), Hoy día los atacantes han cambiado sus objetivos a las infraestructuras de la víctima, los ISP's y los IXP's (de sus siglas en inglés, Internet Exchange Point), con el fin de llegar a sus objetivos finales, así por ejemplo, expone que de los perfiles de ataques recibidos por los proveedores de servicios en EU todos los días, se obtienes tendencias como

- 90% de los ataques son de los denominados scripts infantiles o Script Kiddy
- 9% son de los del tipo DDoS, estos ataques la mayoría de las veces provocan daños colaterales.
- 1% atacan la infraestructura directamente.

Estos ataques vienen acompañados de sobrecargas de los recursos como los discos duros, el ancho de banda, los buffers, las bombas a los puertos más vulnerables. Muestra del caso podemos hallar los ataques de aquellos proveedores como Yahoo!, CNN (Febrero 2000)

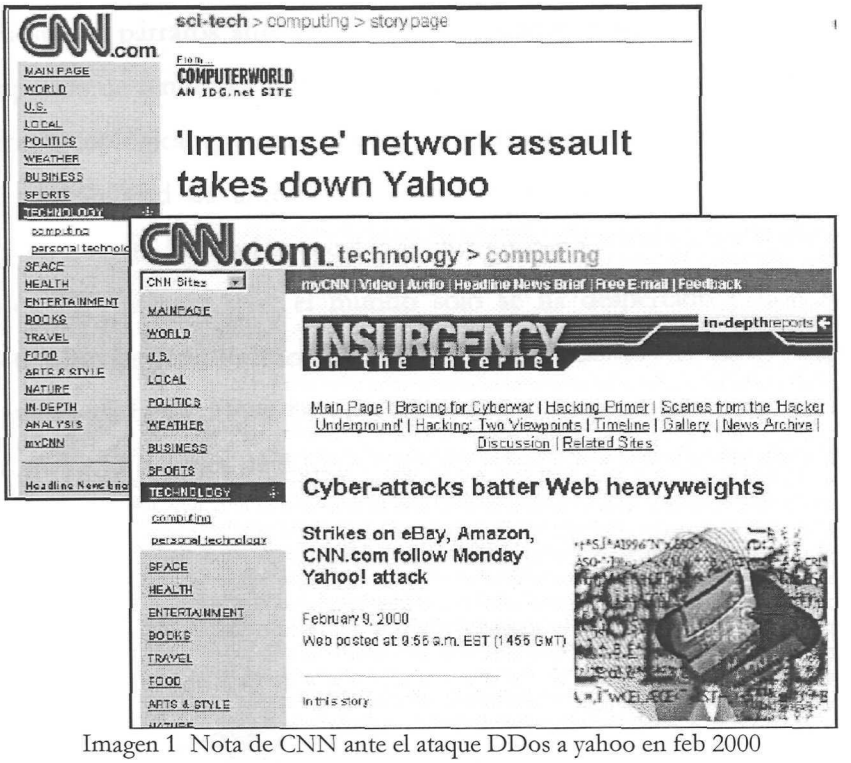


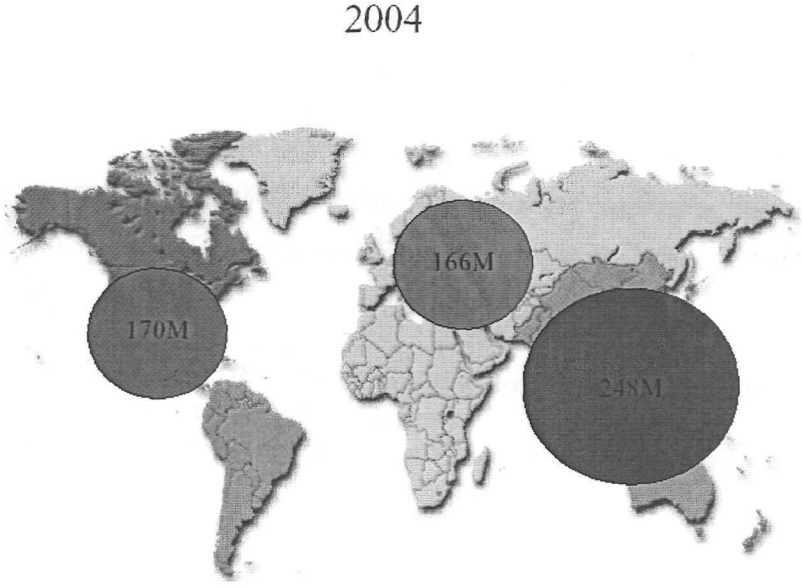
Imagen 1 Nota de CNN ante el ataque DDos a yahoo en feb 2000

La mayoría de estos ataques pasan a través del tráfico propio de los proveedores de servicio de Internet, pues a través de ellos es como se llega a las localidades remotas a través de los enlaces entre proveedores y a su vez entre ellos y sus clientes, además de que por otro lado, permiten un ancho de banda de indudable capacidad para llevar a cabo ataques masivos y por si fuera poco, un sinnúmero de localidades desde donde llevar a cabo ataques.

Dado que los ISP's son redes "transitorias", la forma en que se atiende a estos incidentes sucede de forma diferente a las otras redes, por lo que existe una gran necesidad de detallar y eliminar todas estas fallas y ataques.

1.3 Transiciones Geopolíticas

Como se ha expuesto en párrafos anteriores, si bien la mayor parte de los ataques son o han sido sobre aquellas empresas de renombre o de gran capital, las cuales se hallan localizadas en países con mayor participación tecnológica, que como ya hemos visto, tienen mayor presencia en Internet, esto no disminuye la probabilidad de amenazas a la integridad de la información en otras regiones geográficas, como en nuestro país, así lo menciona Ravendran (2003), quien dice, que el Internet no es exclusivo de los EU, asegura que, el mundo solo se ha despertado y notado este hecho, el crecimiento más notorio es Asia-Pacífico. Además de las acciones del 11 de septiembre de 2001 demuestran una guerra-asimétrica. Para la cual el Presidente George Bush formó Homeland Security, con una inversión de $2.12 billones de dólares tan solo para la tecnología y la caber-seguridad. (ISAC, 2002).



Gráfica 2 Millones de usuarios de Internet por región

En el pasado las guerras requerían de soldados que encararan a los enemigos. Hoy día es mas difícil de hallar, Asegura Harris (CISSP, 2003) a los enemigos, algunos ataques son mas difíciles de rastrear, y los objetivos del atacante son algunas veces mas nebulosos. Los soldados actuales, no solo requieren conocer como se operan los nuevos sistemas de armamento manejados por tecnología, sino también

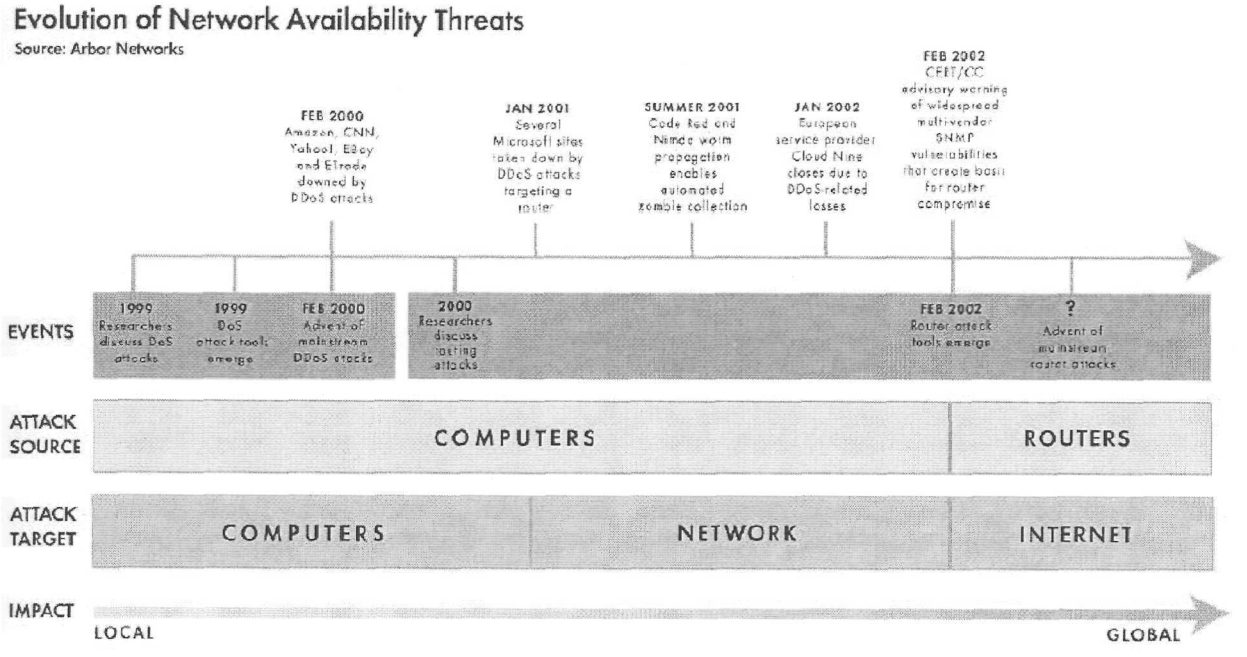
como defender estos sistemas de ataques y saber como atacar los sistemas de defensa del enemigo, de lo que podemos desprender que en el futuro las guerras y las batallas por el poder serán llevadas a cabo sobre las líneas de computadoras en lugar de los tradicionales campos de batalla.

Aunado a todas estas tendencias de Internet, existen organismos que se encargan de verificar el uso correcto de los servicios de Internet, como el instituto de ética computacional el IAB (de sus siglas en inglés, Internet Architecture Board) o los principios de seguridad de sistemas aceptados generalmente (de sus siglas de inglés, Generally Accepted System Security Principle GASSP) los cuales promueven un uso mesurado de los recursos así como establecen dentro de lo posible, las reglas del uso y convivencia dentro de Internet, mas existe aún mucha tarea por hacer en cuanto a la regulación de su uso en muchos de los ámbitos legales por el uso de este recurso.

Asimismo, existen varios organismos que pretenden brindar apoyo de primera mano, para la notificación de cualquier eventualidad con algún sistema en cuanto a sus vulnerabilidades detectadas o posibles fallas, como es el caso de la Carnegie Mellon (CERT de sus siglas en ingles Computer Emergency Respond Team, ,1994-2001) quienes apuntan a los siguientes causas de las cuales se derivan aquellas fallas o Vulnerabilidades por configuración de los servicios de red:

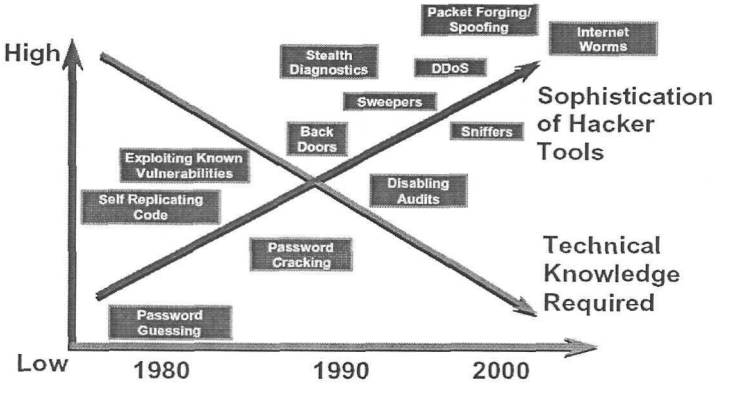
- Implementación: Las fallas de implementación conducen a expandir las intrusiones sin importar los avances en la tecnología de seguridad.
- Configuración.- Los errores serán la mayor fuente de vulnerabilidades las mas fáciles de remediar.
- Diseño: Requerimientos de seguridad inadecuados sin importar los errores pasados.
- Los cambios en la tecnología, pueden minimizar algunas vulnerabilidades, pero estas siempre traen nuevas vulnerabilidades e impactan las contramedidas.
- La carrera del ejército por técnicas de amenaza y sus contramedidas.
- Explotar las vulnerabilidades conocidas por siempre: una vez descubiertas, las técnicas de ataque persisten y se convierten mas automatizadas y fáciles de implementar : Gusanos, Troyanos, Spoofing, Sniffing, DoS, etc.

Muestra de lo anterior lo podemos ver en la grafica siguiente, el cual se gráfica contra el tiempo, como es que las vulnerabilidades se han ido explotando y las tendencias del crecimiento de las mismas en los diferentes niveles de las capas de la red.



Grafica 3 Arbor Evolucion de amenazas en la red

De la misma suerte CISCO, expone que la tendencia de vulnerabilidades explotadas en la siguiente gráfica



Gráfica 4 CISCO- análisis de vulnerabilidades

Capitulo 2

2.1 Problema

La cantidad de correos que actualmente se reciben diariamente en el buzón de correo de cualquier individuo con acceso a Internet resulta asombrosa, debido al creciente uso de spamming.

Como podemos ver el correo es hoy día casi parte de cualquier historia terrible de seguridad electrónica, como lo percibe la empresa New York Life Investment Management,, la cual comenzó a suscribir a sus clientes a través del correo electrónico, en 1996 y que hoy día cuenta con casi 2 millones de abonados a los cuales se les notifica semanalmente de sus estados de cuenta, balances, etc. Información confidencial que solo puede ser vista por el emisor y el receptor mediante los mecanismos apropiados de seguridad. Tetzalff (Marzo,2004) dice que la seguridad del correo electrónico es algo más de pensarse que en el pasado, simplemente por que no cruzaba por la mente de muchas personas. Hace años los usuarios no se preocupaban por el hecho de que estaba enviando información privada a través del Internet. Tetzalff menciona que es importante ser capaz de proveer un alto nivel de protección para toda esta información sin que el usuario sea puesto en una logística extra para que acceda a un área segura.

German (Noviembre, 2001) Vicepresidente de servicios de aplicaciones en el departamento de TI de AFLAC, considera que el mayor reto de seguridad en un corporativo actualmente es abrir el correo electrónico a Internet, AFLAC quien genera en promedio 15000 a 2000 correos electrónicos diarios, de los cuales 10000 son enviados externamente, con este tráfico hacia y desde Internet, AFLAC en un solo mes recibió 450 ataques de Internet y mas de 20 virus. Los programas de escaneo de virus en las compuertas a Internet, entre las estaciones de trabajo y los servidores ofrecen alguna protección, pero aquellos usuarios quienes descargan correo electrónico personal infectado, pueden poner en riesgo a las compañías. La encriptación puede no ser la respuesta, debido a que con estándares de encriptación competentes, los usuarios de diferentes organizaciones no pueden compartir fácilmente

material encriptado. " Hasta que la seguridad no sea transparente como teclear una dirección, los usuarios no van a hacerlo.." Afirma Mitchell (noviembre, 2001) de Hewitt Associates.

De todo lo anterior, podemos notar que las empresas tienen una creciente necesidad de asegurar a sus usuarios y a uno de sus principales medios de transacciones que es el correo, Problema que nos lleva a investigar las principales formas de aseguramiento de este servicio y las principales causas de que puedan hacer fluctuar su operación o comprometer sus recursos y que sobretodo estos modelos sean fáciles de implementar. Por ejemplo el Spamming, que es un ataque usado para sobresaturar a los servidores y a los clientes con correos no solicitados (CISSP,2002) es una creciente muestra del mal empleo del uso del correo por parte de los intrusos o atacantes de estos servicios.

La prohibición del spamming es una tarea imposible y se requieren de grandes esfuerzos, según Wagner (2003), se debe de poner énfasis en los desarrollos de mecanismos para controlar el correo electrónico indeseable y hacer que los emisores de los correos paguen por los costos de la infraestructura de distribución. La propuesta menciona que en primera instancia, los proveedores de Internet, deberán aliarse para establecer el límite superior de correos indeseables o basuras, además, hacer saber que esta abierta la puerta para este manejo de servicios. Y el paso final, usa los ingresos generados para reinvertir en publicidad y además para reforzar a fin de identificar los emisores de estos correos indeseables y que usen el tráfico sin pagar. Esta iniciativa, aún esta lejos de poder implementarse, pero en el plano legal se ha adelantado en ello, al menos en EU.

Hoy día además del spamming, tenemos una gran variedad de códigos ejecutables que posibilitan la entrada a los sistemas si autorización, tales variante incluyen: Klez, Nimbda, Code Red, Melissa, etc. y sus formas mas comunes de distribución es : el correo electrónico, ftp, el compartir archivos en red, etc. y su costo resulta muy levado como la perdida de grabaciones, archivos de sistema, y distribución de información y contraseñas, como lo menciona Tadjer (2001), así como el tiempo sin operación debidas a estos virus, lo que trae perdidas monetarias a las empresas, así como desprestigios y la perdida potencial de clientes y mercado, así como solvencia económica, factores por demás alarmantes para la continuidad de una empresa; Hoy día las mejores practicas no han podido aún

minimizar la cantidad de problemas y tráfico por virus en la red. Tales Mejores prácticas, se pueden enumerar como:

- Escaneo periódico de los sistemas
- Verificar que los servicios abiertos no sean puertos vulnerables.
- Determinar si los sistemas puedan estar comprometidos en su seguridad, si nuevos puertos son hallados
- Asegurarse que la aplicación de parches al sistema no deshabiliten previos parches de seguridad.

La Universidad de Carnegie Mellon (CERT, 2000) asegura que el 99% de las intrusiones, son resultado de la explotación de las vulnerabilidades conocidas o errores de configuración, a los cuales, las contramedidas están disponibles. Investigaciones han demostrado que cerca del 30% de los ataques explota las vulnerabilidades que pueden ser prevenidas con parches y otro 65% a través de sistemas mal configurados.

Harris (2002), además asegura que las vulnerabilidades residen:

- En las configuraciones incorrectas de los firewalls
- En los servidores que no están correctamente asegurados
- Servidores de 2 nivel que no proveen la combinación correcta y detallada de seguridad necesaria para acceder a bases de datos internas de manera controlada.
- Las bases de datos internas aceptan solicitudes desde cualquier punto
- Los ruteadores están configurados para permitir pasar los paquetes solamente, en lugar de rutear los paquetes correctamente

Como hemos visto, además de todas las formas de ataques, también tenemos problemas por parte de las implementaciones y configuraciones de los diferentes niveles de seguridad, por lo que habrá que establecer modelos de aseguramiento a fin de moldear y estructurar los niveles de seguridad. Los problemas reales de seguridad que las empresas están atravesando tienen que ver con los productos que compran e instalan y de la arquitectura de los mismos. De entre las opciones que hallamos en el mercado de escaneo podemos contar con algunas como las que describe Spanbauer (2003)

NMAP Esta utilería ayuda a explorar o auditar grandes redes, que puertos están abiertos o que servicios, las versiones de SO, y los paquetes de los firewalls en uso. Este es un software libre de código abierto.

Nessus Esta herramienta es un pulg-in, actualización de la base de datos de vulnerabilidades en línea diariamente, reconocimiento de servicios y puertos no estándares, No destructivo.

SysUpdate Selecciona y personaliza y remotamente aplica estándares como NSA, SANS, NIST, ISO 17799 y otras políticas.

Ecora: Análisis de Lineamientos Básicos: Windows, Novell, Unix, Cisco, etc.

De entre los software de Firewalls tenemos, entre muchos otros:

- CISCO PIX
- CheckPoint
- WatchGuard
- Winroute
- Symantec Gateway 5400

Dependiendo de la técnica o tecnología para la seguridad, esta no proveerá una cobertura adecuada, dado que los factores humanos, una buena planeación y la continua evaluación son necesarios. Los principios de seguridad son el mayor factor que influye en los diseños de las redes. Esto es un proceso interactivo de revisiones, comparaciones e implementaciones.

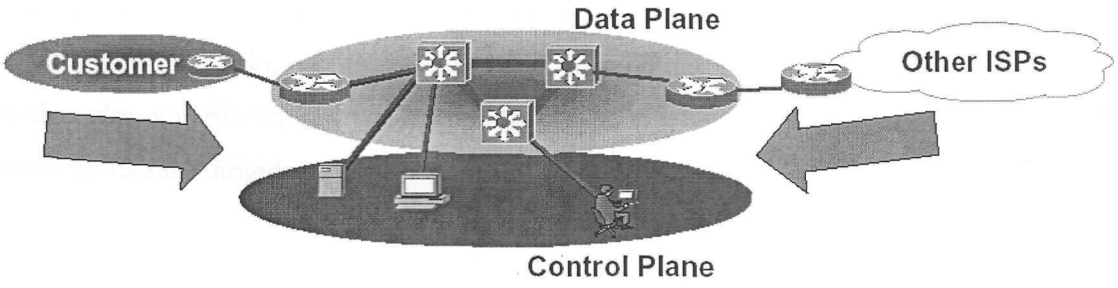
Harris (2002) expone que las diferentes capas de seguridad varían desde el código de programación, los protocolos utilizados, los sistemas operativos, y las configuraciones de las aplicaciones hasta las actividades del usuario y los programas de seguridad que gobiernan todas estos asuntos. En el punto de vista arquitectónico de la red, se deben de poner atención en los datos que fluyen de entrada y salida de un determinado ambiente, así como el saber que datos están siendo autorizados y

monitoreados en diferentes puntos, y como todas las soluciones de seguridad hablan a las demás ante diferentes situaciones.

Como podemos ver la mayoría de estos verificadores de puertos, Firewalls o segmentadores y detectores de intrusos basan sus políticas y configuraciones en el análisis de eventos ya sufridos en las redes o tráficos de patrones establecidos por virus o vulnerabilidades ya conocidas o experimentadas, no establecen algunas prácticas de pronósticos y/o medición de patrones para determinar posibles amenazas dentro de la red. Por otro lado, los ingenieros de sistemas de información requieren usar y analizar los datos de ataques para aprender de las experiencias pasadas, según el planteamiento de Moore, Ellison y Linger (2001), con su teoría de los árboles de ataques a las redes de información.

Estos problemas pueden ser evitados si los administradores configuran las computadoras y mantienen estas configuraciones actualizadas conforme los problemas y debilidades sean identificados, según Derek Simmel (CERT, 2001), así mismo, debido al rol de servicio del equipo, es común que un servidor almacene muchas de los documentos mas valuables y confidenciales. Normalmente estos equipos, son configurados para proveer una capacidad centralizada para una organización, tal como para comunicaciones (correo-electrónico) o sirven de autentificadotes para el acceso a al red.

A nivel ISP, actualmente los datos de correo, Video en demanda, transacciones, mensajes, P2P, IP phone, viajan a través de un mismo canal, el INTERNET. Y por ende la exposición de la información esta latente ante la vista de todos los usuarios de Internet en cualquier momento.



Grafica 5 Servicios de los ISP's

En la gráfica anterior podemos verificar los planos de los datos a través de su tráfico por Internet, desde el consumidor, los ISP's (de sus siglas de ingles Internet Service Provider), y podemos ver, existe un plano de control, el cual verifica el uso del tráfico, El rol de los ISP's el cual tiene como fin, asegurar el servicio en contra de ataques, fallas y errores al cliente, ayudar a asegurar a otros proveedores, proteger a los usuarios de que provengan de la infraestructura de otros clientes. Los ISP's además necesitan protegerse de otros ISP's, Ayudar a sus clientes a protegerse de Internet, proteger al Internet mismo del uso que sus clientes le den, ya que actualmente en cualquier momento existen entre 20 a 40 ataques de DOS/DDoS en la red.

Los puntos de acción de seguridad los ISP's han caído en las siguientes tareas:

- Proteger a los ruteadores de los ataques de DoS
- Proteger el protocolo de ruteo de ataques directos o inserción de rutas
- Proteger la Red de ataques directos o redireccionamiento
- Verificar de donde provinieron los ataques.
- Coleccionar datos de los ataques para reforzar las leyes.

Muchos mecanismos automatizados de Seguridad de Información necesitan adecuarse para que se activen acciones en base a comportamientos no normales para determinado servicio (Ricardo Morales, enero 2004).

La mayoría de las configuraciones de tecnologías clave, herramientas y tecnologías usadas para construir y escalar el Internet no están documentadas, según expone Raveendran (Cisco Bootcamp, Enero 2003), por otro lado, existen variedad de lugares desde los cuales descargar mecanismos de escaneo de redes, y verificación de vulnerabilidades conocidas y que pueden ser usadas por intrusos para perpetrar ataques dirigidos a empresas o como simple diversión.

En resumen, nuestro problema radica, en que no existe un modelo de seguridad que prevalezca o que asegure la funcionalidad y la seguridad de la información en Internet, ni a nivel de ISP's ni a nivel de usuario final. Todos o la mayoría de los mecanismos usados se basan en estándares desarrollados con el conocimiento adquirido de ataques previamente perpetuados. Es decir, no es necesario pagar una gran cantidad por la herramienta más nueva del mercado si no asegurarse de contar con todas las bases necesarias para mantener la seguridad. Asimismo, de los mecanismos de seguridad actuales en el mercado, para el vendedor normalmente no existen base-lines ó lineamientos básicos para la seguridad, solo para la implementación del producto, por lo tanto, no existe los pasos mínimos necesarios para mantener un ambiente seguro previo necesario para la instalación de la solución, que nos permita tener información necesaria para determinar el tipo de evento que pueda estarse sucediendo en la red ante un eventual ataque a la integridad del servicio, una preparación tanto física, como a través de los diferentes niveles de seguridad: programación, aplicaciones, ruteo, etc. , una clasificación de los eventos y el rastreo de los mismos, la forma de reacción y las actividades post-ataques. Por otro lado, y en base a los paso anteriores, establecer la configuración mas adecuada para los mismos: ruteadores, proxy's, Firewall's, IDS's, e incluso los servidores de correo.

Ante la constante proliferación de virus y las posibilidades de vulnerabilidades en los sistemas de protección o en las aplicaciones, es necesario examinar y determinar correctamente el tráfico generado por estos sistemas a fin de determinar el flujo normal de los sistemas tecnológicos y cuando se pueda estar presentando los síntomas de alguna amenaza de ataque computacional en las redes.

Capitulo 3

3.1 Objetivo

* Establecer un modelo de monitoreo de Seguridad de Información con las variables mencionadas que genere indicadores de la Seguridad de Información bajo un esquema corporativo.

Establecer los mínimos niveles de seguridad a través de toda la organización, a fin de establecer una arquitectura de seguridad desarrollada debidamente Así como establecer los mecanismos mínimos necesarios ante la seguridad evaluada o requerida por una organización.

*Seleccionar una aplicación genérica y un mecanismo tecnológico de seguridad de Información para establecer un modelo que permita determinar el comportamiento normal del servicio. (Web, E-mails, Routeadores, etc)

Principalmente, estudiar los diversos mecanismos tecnológicos implementados para la seguridad del correo-electrónico, tales como los ruteadores, proxy's, firewalls, IDS's, antivirus y sus interacciones, a fin de lograr su configuración adecuada y lograr que esta sea lo más fácil de implementar.

Dentro de los objetivos no están el desarrollar Herramientas que brinden este tipo de servicios, pero si lograr conjuntar los elementos necesarios para que las diversas herramientas puedan cumplir con su acometido y lograr la mitigación de los correos no deseados, así como evitar al máximo este tipo de tráfico que puede trastornar el flujo operativo normal de cualquier empresa.

Por otro lado, se planea establecer en base a los comportamientos de las incidencias de correos de entrada o salida, el flujo y el comportamiento real para evitar cualquier posible ataque de correos no deseados.

Lineamientos Básicos:

Basados en Warren (1997), las ventajas del uso de los lineamientos son:

- Fácill de usar
- Simple
- Que los entrenamientos sean mínimos para el uso del método;
- Rápido de implementar

Dentro de las desventajas, Warren (1997) menciona:

- Que la naturaleza de estos métodos de seguridad no resuelven todas los necesidades
- Normalmente, estos lineamientos están diseñados, para el uso dentro de un ambiente general.

Capitulo 4

4.1 Marco Teórico

4.1.1Seguridad de la Información

La mayoría de las personas creen el tema de seguridad y la criptografía es solo usada por los militares durante la guerra para la comunicación sin que los enemigos capten sus secretos. Así, por ejemplo, durante la 2ª Guerra Mundial los Alemanes usaron sus maquinas "Enigma" para enviar mensajes. Ellos pensaron que los mensajes eran infranqueables ya que Enigma aplicaba diferentes códigos para cada letra del mensaje. Sin embargo alto IQ británico se la ingeniaron para descifrar los códigos de enigma con las computadoras mas avanzadas entonces, y se las ingeniaron también para ver los correos de Hitler, los cual ayudó a los aliados en Europa y África. Julio cesar, 2000 años antes estaba enviando mensajes usando un sistema de criptografía en sus mensajes a sus tropas. El usaba rotar cada letra del mensaje por un numero de letras, por ejemplo ataque se convertiría en cvcswf (rotando 2 letras hacia delante en el alfabeto).

Cuando el primer sistema de correo electrónico fue creado en la Arpanet, la seguridad no era realmente un problema. Solo los investigadores y algunos trabajadores de gobiernos tenían acceso. Rubestein (Noviembre, 2001) Presidente de EMA (de las siglas en inglés Electronic Messaging Association), comenta que anteriormente con la excepción de Lotus Notes, el cual era usado en conexiones punto a punto entre las organizaciones y siempre tenía alguna clase de encriptación, no había control acerca de lo que los empleados enviaban fuera, a donde lo enviaban o que recibían.; Ya sea si es un virus o una propiedad intelectual, las compañías siempre luchan por controlar que llega y que sale de sus redes.

Haney (marzo, 2004), analista de Celent, comenta que la atención a la seguridad del correo electrónico tiene sus orígenes en las porciones de las leyes de desregulaciones financieras de años pasados. Los reguladores tienen la autoridad de mandar altos niveles de protección para la seguridad del

consumidor, así como reforzar las provisiones de salvaguarda de los datos: se espera que comiencen a existir instituciones financieras que tengan mayor cuidado de la información confidencial para sus clientes.

Aunado a todos estos problemas de inseguridad en los correos, también existen actualmente el *espionaje industrial*, como Hill y Michael (1995) denominan como un intento de gobiernos extranjeros o industrias de adquirir información no pública o clasificada. Aunque resulta difícil concienciar de ello, Hoy es una realidad, aunque tiene sus dificultades de medición como la economía subterránea, pues nadie sabe a ciencia cierta cual es su costo. En los estados unidos el costo estimado de este espionaje puede ser de aproximadamente $100 billones de dólares anuales en perdidas en ventas. Wright y Roy (1999) consideran que existen varios puntos a ser expuestos para establecer un programa para estar alerta contra esta clase de amenaza. Tales puntos consisten en detallar que información necesita protección, quien pudiera estar buscando robársela y como detenerlos. Estos métodos pueden incluir videos, correos informativos, sesiones, publicaciones internas con historias reales de los daños causados por los intrusos de las computadoras, virus; historias de éxito puede citar organizaciones en las cuales la inteligencia competitiva ha sido bien administrada. Y principalmente enfocarse en el uso de las maquina de fotocopiado y fax, teléfonos celulares, correos electrónicos y las redes computacionales. El mayor problema de esta implementación resulta ser la rutina o la presión del tiempo pueden conducir al personal a desatender las políticas de seguridad.

En general, en nuestro país según el estudio de Peñalva (2001) IDC en México, el mercado de software de seguridad aun no posee una clara percepción del ROI (de las siglas de inglés Return of invest) generado por las aplicaciones de seguridad. Los beneficios de estas soluciones son percibidos solos como intangibles y se los vincula fuertemente con los altos costos de mantenimientos y altas inversiones en infraestructura.

Otra gran amenaza a la estructura del correo, consiste en los errores de desarrollo de los software de aplicación como el caso de la empresa Sendmail, el software de correo desarrollado en 1981 y que actualmente aún se halla en el mercado, se ha descubierto que presenta una vulnerabilidad de su

seguridad y su operación, error en su diseño que deja la posibilidad de que cualquier intruso pueda leer y borrar correo o derribar redes de computadoras. Sendmail es usado para almacenar y enviar mensajes en sistemas tales como Sun Microsystems Inc. Hewlett-Packard Co. E IBM.. El investigador de Internet Security Systems, Inc. Ingevaldson, (marzo, 2004) Descubrió esta vulnerabilidad. Evidenciando que cualquier proceso que el administrador pueda hacer, un intruso también las pudiera realizar si tuviera control de la vulnerabilidad encontrada. Los hackers computacionales normalmente escriben software para afectar a los programas mas usados, como el virus "Slammer", el cual explotó un mecanismo similar de los servidores de Microsoft.

4.1.2 Tendencias de seguridad

Las redes se han convertido en sistemas indispensables para los negocios en áreas de gobierno, comerciales, y organizaciones académicas. Los sistemas conectados por red, permiten acceder a la información necesitada rápidamente, mejorar las comunicaciones y al mismo tiempo reducen los costos y permiten la colaboración, y proveen de mejores servicios para el consumidor y finalmente están conduciendo a un comercio electrónico. CERT

Muchas Organizaciones se han movido a arquitecturas de cliente-servidor distribuidas, donde los servidores y las estaciones de trabajo se comunican a través de la red. Al mismo tiempo, esta conexión también permite el acceso a la Internet para sostener una presencia visible en Internet con los clientes, asociados y proveedores. Mientras las redes de computadoras han revolucionado la forma en que las compañías realizan negocios, los riesgos que ellos introducen pueden ser devastadores. Ataques en las redes pueden estar dirigidos a la perdida monetaria, tiempo, productos, reputación, información sensitiva, e incluso vidas.

El instituto de Seguridad de computación 2000 y el Departamento de Crímenes y seguridad en computación del FBI (CSI, 00) indican que el que el numero de crímenes computacionales y otras ramas de seguridad de información están en crecimiento y que el costo también esta elevándose. Por ejemplo, 70% de 585 reportaron crímenes computacionales en los últimos 12 meses. Las perdidas

financieras de 273 Organizaciones que fueron capaces de cuantificar totalizaron $265,586,240 mas del doble que en el año anterior.

Ingeniería para el diseño de fácil uso no esta siendo empatada con la ingeniería para la facilidad de una administración segura. Los productos de Software de Hoy, las estaciones de trabajo, y las computadoras personales dan el poder computacional a una cantidad creciente de personas quienes usan esa capacidad para realizar su trabajo mas eficientemente. Los productos son muy fáciles de usar, que hasta la gente con pequeñas habilidades tecnológicas o conocimientos puede instalar y operarlos en sus computadores de escritorio. Desafortunadamente, es difícil de configurar y operar muchos de estos productos seguramente. La espacio entre el conocimiento necesitado para operar el sistema y aquel necesario para mantenerlo seguro es el resultado del incremento de numero de sistemas vulnerables.

Los usuarios consideran que sus equipos estarán siempre que se les necesite y asumen, que sus departamentos de TI están operando todos los sistemas seguramente. Pero este no es el caso. Los administradores de sistemas y las Redes normalmente tienen tiempo insuficiente, conocimientos y habilidades para hacer frente a la amplia rama de demandas requerida para mantener los sistemas complejos y redes en operación y funcionales. Adicionalmente, los métodos de ataque desarrollados y las continuas vulnerabilidades del software emergente introducen nuevos tratos para la tecnología instalada en la organización Así, aún las organizaciones con vigilancia y concisa-seguridad descubrieron que la seguridad comienza a degradar casi inmediatamente después de que algunos ajustes, o trabajos acerca de la configuración o nuevas tecnologías son instaladas. La seguridad inadecuada en las infraestructuras de TI puede negativamente afectar la integridad. Confidencialidad y disponibilidad de los sistemas y los datos,

Ya sea que lo conozca o no, la red de su organización y sus sistemas son vulnerables a ataques internos y externos. Las organizaciones no pueden construir productos y realizar negocios sin una infraestructura de TI robusta. Y una infraestructura vulnerable de TI a un intruso no puede ser robusta. Además, los usuarios tienen una organización, ética y con frecuencia responsabilidades

legales para proteger la competitividad e información sensitiva. Esta debe también preservar la imagen y reputación de las organizaciones y los negocios con los socios Todos estos deben de estar comprometidos por los accesos de intrusos.

En los 80's los intrusos eran Expertos en sistemas con un alto grado de experiencia quienes personalmente creaban los métodos para acceder dentro de los sistemas. El uso de herramientas automatizadas y scripts para explotar eran una excepción en lugar de una regla. Para el año 2000, debido a la expansión y fácil disponibilidad de las herramientas de intrusión y scripts de explotación que podían fácilmente duplicar métodos conocidos de ataque, absolutamente cualquiera podía atacar una red. Mientras que los usuarios expertos se están haciendo mas listos, como se ha demostrado por los tipos cada vez mas sofisticados de ataques, los intrusos novatos requieren de conocimientos menos sofisticados para copiar o lanzar métodos conocidos de ataques. Muestra de ello lo podemos constatar con los taques de DDoS y las variantes del gusano LoveLetter, en los cuales la severidad y alcance de los métodos de ataque se han incrementado.

En la primera mitad de 1980, los intrusos manualmente ingresaban comandos en una computadora personal y podían acceder decenas a centenas de Sistemas; 20 años mas tarde ellos pueden usar métodos automatizados para acceder desde miles a decenas de miles de sistemas. En los años 80's era relativamente simple determinar si un intruso había penetrado su sistema y que había hecho. Para el año 2000, sin embargo, intrusos podían totalmente cancelar su presencia, por ejemplo, deshabilitando los servicios comunes usados y reinstalando sus propias versiones, borrando sus ataques en los archivos de registro. En los 80's y principios de los 90's, los ataques de Denegación de Servicio (DoS , de sus siglas en inglés) era poco probables y no considerados como serios. Hoy día, un ataque DoS exitoso en un proveedor de Internet que conduce sus operaciones electrónicamente puede poner al proveedor fuera del negocio. Desafortunadamente, estos tipos de ataques ocurren más frecuentemente cada año.

Debido a la explosión del uso de Internet, la demanda de administradores de sistemas competentes con la experiencia necesaria excede por mucho a la suministrada a los individuos recién graduados o

aquella lograda mediante la práctica. Como resultado, la gente que no esta propiamente calificada están siendo contratados o promovidos dentro de un trabajo. Esta tendencia es exacerbada por el hecho que algunos administradores de sistemas experimentados y habilidosos cambien de trabajo frecuentemente para incrementar sus salarios o dejar el mercado laboral debido a fastidio.

Las auditorias actuales y los nuevos productos típicamente se enfocan en las tecnologías de sistemas esenciales y redes sin considerar lo concerniente a la organización (por ejemplo, políticas y procedimientos) y aspectos humanos (por ejemplo administración, cultura, conocimiento y habilidades, incentivos) que pueden dramáticamente afectar la seguridad de la infraestructura de TI. Como resultado, las compañías con frecuencia implementan soluciones incompletas o las acortan con la idea de que solucionaran el problema.

4.1.3Amenazas de la Información

La seguridad de igual forma e importancia que la calidad no es un camino ni un destino, si no una forma de trabajo y modo de vida [Allen, Julia, 2001]. Debemos visualizar la seguridad no como un estado Operativo, sino como un proceso continuo de evaluación y acción y más aún como un método pro-activo encausado a disminuir los riesgos que puedan aquejar la integridad y aumentar la seguridad y evitar al máximo el peligro o daño. En la medida que podamos llevar a cabo estos procesos es que la seguridad podrá ser prolongada, y conseguir un estado de confiabilidad. Ya que hoy día nos hallamos en un ambiente cuya constante mas evidente es el cambio y el dinamismo; donde las amenazas, ataques e intrusiones no solo existen en el plano físico sea este de integridad física de una persona hasta la infraestructura de energía una nación, sino también el plano electrónico hacia aquellas objetivos como los sistemas de información.

Nuestra generación esta viviendo la denominada "era de la información" y hoy día la información tiene un valor financiero, por lo que un manejo inapropiado del mismo, o su destrucción, el daño a la integridad o la restricción al acceso por negligencia o no disponer de la misma en tiempo y en forma, representa costos financieros cuantificables y un potencial daño en perdidas de oportunidades de

negocio y perdida de imagen los cuales resultan difíciles de medir pero de gran magnitud e importancia.

La necesidad de integrar a los usuarios, tanto internos como externos, en un ambiente que les permita con mayor rapidez y eficiencia, colaborar entre ellos conlleva riesgos en nuestro actual manejo de información a través de la globalización de las comunicaciones y la unificación de la misma a través de una sola red: Internet. Dichos riesgos pueden ser directos sobre latente factor humano o indirectos en forma de amenazas externas como lo son: virus, caballos de Troya, hackers, delincuentes informáticos y hasta terroristas informáticos (muy clásicos ya en estas fechas de ataques masivos). No hay forma absoluta de eliminar por completo estos riesgos siendo que requeriremos integrarnos a trabajar y conectarnos por este medio a una audiencia muy adversa en intereses y necesidades, para fines informativos, de investigación, de colaboración, desarrollo de oportunidades y toda clase de los nuevos negocios electrónicos; pero en cada caso podremos encontrar la forma de mitigar la exposición a los riesgos presentes y establecer mecanismos para reducir la potencialidad de incidentes futuros..

De igual forma que en la calidad, el problema no es realizar una proeza técnica sino un cambio de cultura organizacional, en la forma de trabajar de los individuos y en la óptica mediante la cual prestamos nuestros servicios o damos acceso libre y transparente a la información que cada individuo según sea el caso requiera. Crear la conciencia del valor de la información y hacer presente los riesgos potenciales es una tarea importante. Así podemos establecer normas de seguridad acerca de los equipos conectados a la red a fin de establecer los mecanismos para evitar que puedan ser abordados fácilmente y permitir el acceso a la red de una empresa por un intruso desde los mismos; los datos que requieren máxima seguridad y que no deban de estar expuestos deberán ser franqueados y con acceso seguro y para la seguridad de red deberá de mantener aquellos puertos que no estén usando deshabilitados.

De todo lo que hasta ahora hemos comentado podemos notar que existen varias amenazas en cuestiones de seguridad las cuales podemos asociar como:

- DAÑO .- Fallas de Software o Hardware
- DESASTRE.- Inundaciones, Incendios
- INTRUSO.- Hacker, Espía
- FUGA.- Empleado Deshonesto
- MODIFICACION.- Error Fraude

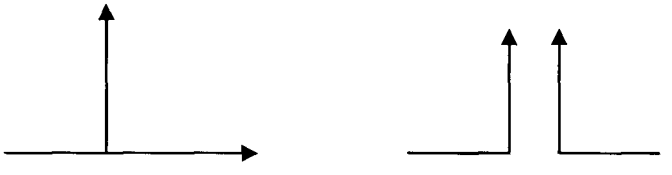
De entre las amenazas más comunes de los sistemas de información podemos enumerar también por mencionar algunas, las siguientes de las cuales el número de incidencias se ha incrementado notablemente en los últimos años:

- Revelación/Fuga de Información
- Violación de Integridad
- Enmascaramiento/Personificación
- DDoS/DoS-Negación del Servicio
- Enmascaramiento/Personificación
- Uso Ilegítimo

Amenazas genéricas: backdoors, caballos de Troya, ataques internos (La mayoría de los problemas de seguridad en Internet son de control de acceso o de autentificación)

De entre los ataques mas conocidos tenemos los

Ataques Pasivos Ataques activos



Los ataques pasivos solo pueden observar la comunicación de los datos.

Los ataques activos pueden modificarlos los datos algunas veces difíciles de realizar, pero potencialmente muy dañinos

- Personificación/Modificación de Correo
- Personificación/Robo de Sesión de TCP/IP

Durante el desarrollo de esta era de la información nos hemos topado con cada vez un peligro mas que fundado, reales y cada vez mas dañinos, respecto a las amenazas de posibles ataques hacia de la información de las empresas, así como para los usuarios finales. Muestra de ellos son las siguientes tablas estadísticas tomadas de la universidad de Corniege Mellon Software Ingineering Institute CERT, el cual fue creado en 1998 y como podemos ver la gama de reportes desde su creación han ido de la mano con el crecimiento del uso de Internet así como de la factibilidad de contar con elementos de computo desde el hogar y lugares remotos.

Numero de Incidentes Reportados

1988-1989

Año	1988	1989
Incidentes	6	132

1990-1999

Año	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidentes	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Año	2000	2001	2002	2003
Incidentes	21,756	52,658	82,094	137,529

Total de Incidentes reportados (1988-2003): **319,992**

Otro de los servicios altamente atacados como hemos mencionados son los servicios de correo, los cuales han sufrido de ataques como falsificación de identidad, relay ó libre transporte de correo a través de servidores que proporcionan el servicio, spamming por mencionar algunos de los problemas de seguridad mas frecuentes.

Mesajes de Correo Manejados
1988-1989

Año	1988	1989
Correo	539	2,869

1990-1999

Año	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
Correo	4,448	9,629	14,463	21,267	29,580	32,084	31,268	39,626	41,871	34,612

2000-2003

Año	2000	2001	2002	2003
Correo	56,365	118,907	204,841	542,754

Total de mensajes de correo manejados (1988-2003): **1,185,123**

Por otro lado según los datos del departamento de justicia de EUA, durante el año de 1998 se tuvieron las siguientes estadísticas en cuento a casos de ataques a los sistemas de información que fueron notificados :

	Casos	%
Total de casos	419	
Fueron a Juicio	83	20%
Convictos	47	11%
En prisión	20	5%

Tabla III Porcentajes de Juicios vs ataques informáticos

En México, el acceso ilícito a sistemas y equipos de informática esta tipificado en el Diario Oficial del 17 de mayo de 1999:

Revelación de secretos y acceso ilícito a sistemas y equipos de Informática
CAPITULO I
Revelacion de secretos
CAPITULO II
Art. 211bis1 .- al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de 6 meses a 2 años de prisión y de 100 a 300 días de multa.

Muchos de estos atentados hacia la Seguridad de la Información han sido hasta esos momentos con fines de diversión o como mero reto para poder probar el nivel de poder franquear la excelencia informática públicamente, pero con el crecimiento de las empresas y desde el punto de vista que el conocimiento es símbolo de poder, estos ataques informáticos podemos percibirlos cada vez mas asentados y dirigidos a objetivos específicos, podemos hallar actualmente grupos adversarios que emplearán técnicas de guerrillas por Internet; por otro lado, la recolección de información de inteligencia no estará orientada solamente a los objetivos de tecnología.

4.1.4 Operaciones de Seguridad

Las Operaciones de seguridad conciernen a todo aquello que tenga lugar para mantener la red, los sistemas computacionales y el ambiente en línea y trabajando de una manera segura y protegida Las Operaciones toman lugar después de que la red es desarrollada e implementada. Esto incluye el continuo mantenimiento de un ambiente y las actividades que deben de tomar lugar en el día a día o semana a semana.

4.2 Seguridad del Correo Electrónico

El Internet fue desarrollado primero principalmente por las agencias de gobierno y las universidades para comunicar y compartir información, pero los negocios de hoy dependen de la productividad y su rentabilidad.

El correo electrónico se ha convertido en una parte importante e integrada en la vida de las personas. Es usada para comunicar con la familia, amigos, negocios, asociados de negocios y clientes, compañeros de trabajo y gerencia, etc. Generalmente, la seguridad, autentificación y la integridad de un e-mail no esta considerada en el uso del Día a día. Los usuarios están mas preocupados por los documentos agregados que puedan contener virus que por el hecho que un correo electrónico pueda ser fácilmente falsificado y sus contenidos puedan ser cambiados mientras están en transmisión.

Es muy fácil falsificar los mensajes de correo electrónico, es decir, alterar el nombre en el campo "De:" Todos los usuarios necesitan hacer esto para modificar la información dentro de la sección de preferencias de su cliente de mail y reinicializar la aplicación. Un atacante puede enviar un mensaje a la secretaria del Gerente General diciéndole que el departamento de TI esta teniendo problemas con algunos servidores, y pidiéndole que cambie su contraseña a "password" para iniciar su sesión en la red. Si ella recibe esta correo electrónico y en el campo "De:" aparece el nombre del administrador de la red en el, ella probablemente completara este requerimiento sin pensarlo 2 veces.

Este tipo de actividad es rara hoy día, pero probablemente se haga mas usada como una táctica de ingeniería social. La solución requiere autentificación apropiada para asegurar que un mensaje realmente viene de una fuente indicada. Las compañías que toman en serio los niveles de seguridad, implementaran una aplicación de correo electrónico para su protección como PGP (del las siglas en inglés Pretty Good Privacy) o el uso de una llave o código publico (del ingles: Public Key infraestructura, PKI y firmas digitales. Estas compañías pueden también considerar el uso de un protocolo de encriptación para apoyar a la lucha contra los buscadores de datos en la red y la intercepción no autorizada de mensajes.

Un correo electrónico que viaja desde el TEC (ITESM) tiene muchos saltos entre la fuente y el destino. Existen varios puntos de intercepción potenciales que pueden permitir al atacante interceptar, ver, modificar o borrar los mensajes durante su travesía.

Si un usuario va a usar un esquema de seguridad para proteger su mensaje de que pueda ser visto, modificado, falsificado o borrado, él y el destinatario deben de usar el mismo sistema de encriptación. Si la clave de criptografía pública va a ser usada, ambos usuarios deben de tener una forma de intercambiar las llaves de encriptación. Este tipo de protección ocurre en las capas de aplicación y presentación del sistema de interconexión (Modelo OSI, de sus siglas de inglés Open System Interconnect) Si un administrador, o profesional de seguridad, desea asegurar que todos los mensajes sean encuitados entre los 2 puntos y no quisieran tener que depender de los usuarios para que encripten sus mensajes, el puede implementar la capa de Conexiones Seguras (SSL, de las siglas de Ingles Secure Socket layer)

4.2.1 Como Trabaja El correo Electrónico

Un usuario tiene un cliente de mail que puede ser usado para modificar, crear, direccional, enviar y reenviar mensajes. Este cliente puede proveer otra funcionalidad como usar una libreta personal de direcciones, agregar archivos, establecer banderas, retraer mensajes y almacenar mensajes en diferentes carpetas.

Bien, el usuario crea un mensaje pero el mensaje no es servible hasta que sea enviado a alguien más. Es aquí donde el Protocolo Simple de Transferencia de Correo SMTP (de sus siglas de inglés Simple Mail Transfer Protocol) aparece. SMTP trabaja como un agente de transferencia de mensajes y mueve los mensajes de los usuarios de una computadora a el servidor de correo cuando el usuario presiona el botón de enviar. SMTP es un estándar de intercambio de mensajes y la mayoría de la gente lo ha visto mediante el esquema: alguien@dominio.com

Muchas veces un mensaje necesitará navegar a través del Internet y a través de diferentes servidores de correos antes de arribar a su servidor de correo destino. El protocolo de SMTP es quien transportará el mensaje y trabaja sobre el protocolo de control de transmisión, TCP (de sus siglas en ingles Transport Control Protocol). TCP es usado como el transporte debido a su confiable protocolo y proveerá de una secuencia y reconocimiento para asegurar que el mensaje del correo electrónico llegue a su destino exitosamente.

El cliente del usuario de correo Electrónico debe ser compatible con SMTP para ser propiamente configurados a usar este protocolo. El cliente provee una interfase al usuario, de tal forma que el usuario pueda crear y modificar mensajes como lo desee, y luego el cliente pasa el mensaje a SMTP. Si una analogía de oficina de correos fuese usada, el cliente de correo electrónico pudiera ser una maquina de escribir que se usa para escribir un mensaje, SMTP pudiera ser el cartero que lleva el mensaje y lo entrega en la oficina de correos, la ofician de correos puede ser el servidor de correos. El servidor de correos tiene la responsabilidad de entender donde el mensaje debera ser entregado y rutear el mensaje para que llegue a su destino.

El software más común de SMTP dentro del mundo de UNIX es SendMail, que es realmente una aplicación para servidores de correo. Esto significa que Unix usa sendmail para almacenar, mantener y rutear los mensajes de e-mail. Dentro del mundo de Microsoft, Microsoft Exchange es mayormente usado, y en Novell, Groupwise es el servidor común de SMTP. SMTP trabaja de cerca con 2 protocolos POP e IMAP, los cuales se explican en las siguientes secciones.

POP Post Office Protocol (POP) es un protocolo de servidor de correo de Internet que soporta mensajes de entrada y salida, El servidor de correo usando POP almacena y re-direcciona mensajes de correo electrónico y trabaja con SMTP para mover mensajes entre servidores de correo.

Una compañía puede tener un servidor de POP que mantenga los buzones de correo, y las compañías más grandes servidores de POP para cada departamento. Existen también servidores de Internet POP que posibilitan a las personas en cualquier parte del mundo a intercambiar mensajes.

Este sistema es muy usual debido a los mensajes son mantenidos en el Server hasta que los usuarios están listos para descargar sus mensajes en lugar de intentar empujar el mensaje derecho a la computadora de un usuario, la cual puede estar apagada o mal funcionando. El servidor de correo electrónico puede implementar esquemas de autentificación diferentes para asegurar que un individuo esta autorizado para acceder un particular buzón, y es usualmente manipulado a través de usuarios y contraseñas.

IMAP Internet Message Access Protocol (IMAP) es también un protocolo de internet que posibilita al usuario para acceder al correo en un servidor de correo. IMAP provee los mismos tipos de funcionalidad que POP, pero tiene más capacidades y funcionalidades. Si un usuario esta usando POP, cuando se accede al servidor de correo para ver su ha recibido mensajes, todos los mensajes serán automáticamente descargados a su computadora. Una vez que el mensaje es descargado del servidor de POP, estos son eliminados del servidor. POP puede provocar frustración para aquellos usuarios móviles debido a que los mensajes son automáticamente descargados a su computadora o dispositivo y ellos pueden no tener el espacio necesario para mantener todos sus mensajes.

Si un usuario usa IMAP, este puede descargar todos sus mensajes o dejarlos en el servidor de correo dentro de la carpeta remota del Server, llamada buzón. El usuario puede manipular los mensajes dentro de este buzón para colocarlos en el Server o en su maquina local. La persona puede borrar o crear mensajes, buscar mensajes específicos y colocar y borrar banderas de seguimiento. Esto

posibilita al usuario de mayor libertad y mantener los mensajes en un repositorio central hasta que el usuario escoja descargar los mensajes.

Email Relaying (Transferencia de correo-electrónico) Actualmente existen diversos tipos de sistemas de correos que corren sobre diferentes sistemas operativos. La mayoría de las empresas tienen sus correos públicos en las zonas DMZ (desmilitarizadas) y pueden tener uno o mas servidores de correo en sus LAN (de las siglas de inglés, Local Area Network). Aquellos en la DMZ, deben de estar asegurados y sus mecanismos de transferencias de correos (relaying) correctamente configurados para evitar que sean usados como actividades no deseadas como spamming.

4.3 Mejores Prácticas

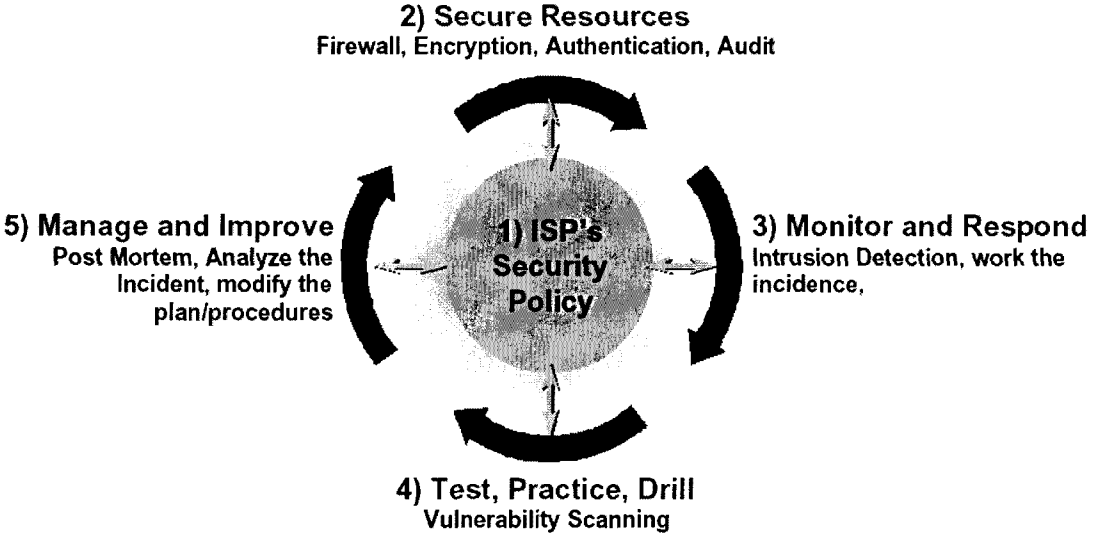
De entre las practicas comunes para fijar los elementos básicos de seguridad de los mecanismos de correo, se hallan la habilitación solo de aquellos puertos necesarios para que el cliente de correo pueda conectarse con el servidor, y aquellos puertos para la navegación del Server con Internet, como lo son los puertos 25 (SMTP) , 110 (POP) , 53 (DNS), 443 (SSL), etc, mas las configuraciones de 2 o 3 Nivel de aseguramiento, son actualmente esenciales a fin de lograr diferentes niveles de seguridad y acceso, la verificación del flujo de la información en las diferentes capas es otra mas de las mejores prácticas: a nivel físico, a nivel datos, a nivel de red, y aplicación, así como las pruebas de penetración deben ser parte importante del modelo y agenda del operador.

Así por ejemplo se pueden establecer perímetros de acceso, mediante la implementación de las siguientes normas (CISSP, 2002):

- Aseguramiento del viaje de la información estableciendo conexiones vía IPSEC, para la capa de red, en las sesiones de VPN
- Establecimiento de llaves públicas PKI para la entrega de correos.
- Habilitar solo aquellos puertos que sean estrictamente necesarios
- Instalación de antivirus, así como detectores de intrusos
- Uso de SSL (de las siglas de inglés Secure Socket Layer) en la capa de transporte del sistema OSI, cuando sea necesario acceder a información confidencial.
- Escaneo de puertos para determinar la seguridad del perímetro del ambiente de operación de los servicios de correo.

Por parte de CISCO, existen una seria de pasos a fin de lograr un equipo SWAT para este nivel se seguridad y continuidad del servicio, el cual plantea los siguientes pasos:

- Preparación
- Identificación
- Clasificación
- Rastreo del ataque
- Reacción
- Tareas pos-ataque



Grafica 6_6 Pasos de seguridad, CISCO&Arbor

Microsoft y check-list, es considerado para este estudio como parte integral a fin de establecer un base-line o comportamiento básico que permite los objetivos planteados:

Tareas constantes

- Limitar los derechos de los usuarios solo a los necesarios
- Limitar las vulnerabilidades cuando se instalen equipos nuevos en la red
- Eliminar los acceso vía Terminal Server al menos número de cuentas posibles
- Correo una estructura de 2 nivel de DNS para proteger la identidad de los servicios internos

Tareas Diarias

- Escaneo de los puertos y direcciones asignadas

Tareas semanales

- Examinar firewalls desde dentro y desde fuera con escaneadotes de puertos y herramientas apropiadas

Capitulo 5

5.1 Metodología

5.1.1 Tipo de Investigación

Esta es una investigación del tipo Correlacional en la cual investigaremos las variables de tráfico en la red en función de la cantidad de la proliferación de correos procedentes del dominio emisor en la red en un determinado momento, así como los posibles ataques o pruebas potenciales que se puedan dar en la red. Y por otro lado, en caso de contar con el tiempo necesario, verificar la acción de la displicencia humana ante la configuración de los dispositivos tecnológicos de seguridad.

Los pasos para el presente estudio conllevan los siguientes pasos

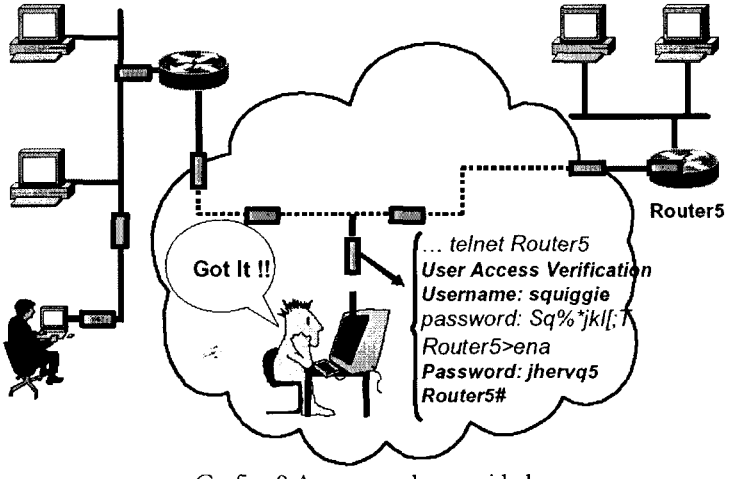
1. Necesidad de la Información ante el problema presente
2. Delimitación y alcances del estudio.
3. Procedimiento de recolección de datos y análisis

1.- Generar conciencia de las fallas de los servicios de correo, y los lineamientos básicos de las configuraciones de equipos tecnológicos para el correcto aseguramiento para evitar este tipo de tráfico y la necesidad de aseguramiento de la información y establecimiento de mecanismos de defensa y respuesta a eventos ataques de la información, buscar las variables mayormente indiquen patrones de comportamiento en las redes y sus interacciones, así mismo adentrarse en las mecánicas de operación y codificación de los servicios de correo, redes a nivel aplicación, Red, etc., métrica de asociación a los estándares de seguridad.

2.- El alcance de la presente esta enfocado al dominio de los servicios de correo, aunque se estudiaran de cerca algunos otros protocolos como los de web por su estreches con algunos servicios de correo. De igual forma, el estudio comprende algunos sistemas tecnológicos como Firewalls, Proxy's, e

IDS's y IPS'sa fin de establecer correctamente la configuración base y la adecuada para el correcto funcionamiento de los servicios de correo-electrónico.

3.-Investigación en Bases de Datos calificadas, así como con los organismos certificados en el tema como CISSP, CISA, ISC2, GIAC,etc. a través de las fuentes de productos del ramo actualmente en el mercado: CISCO, SYMANTEC, Arbor, IntruVert, etc. mediante pruebas de laboratorio del análisis de diferentes configuraciones e implementaciones, así como estudios de campo y comunicación con los administradores de TI de diferentes organizaciones para contemplar los diferentes escenarios. Dado que el presente estudio será Correlacional cualitativo basando la deducción de productos desarrollados para el diseño de un Modelo que permita en nuestro entorno tecnológico desarrollar las bases necesarias de la seguridad de redes, esta no será del todo necesario.



Grafica 9 Amenazas de seguridad

5.2 Modelo

Lineamientos Básicos de Dispositivos tecnológicos de seguridad y ajustes necesarios para el correcto servicio (Correo y tráfico no deseado)

Actualmente existen muchas formas de tratar de detener la emisión de correo no deseado tanto por la parte tecnológica como por medio de la parte legal, tal es el caso de la ley federal aprobada el 1° de Enero de 2004 en EU, "can-Spam" para denunciar a vendedores en Internet por el envío masivo de correos no solicitados; otras formas son las listas negras universales o la instauración de sellos informáticos para limitar la recepción de correos no deseados, con la idea de obligar a quien envía correo basura a pagar un precio específico por cada correo electrónico enviado (Nava)

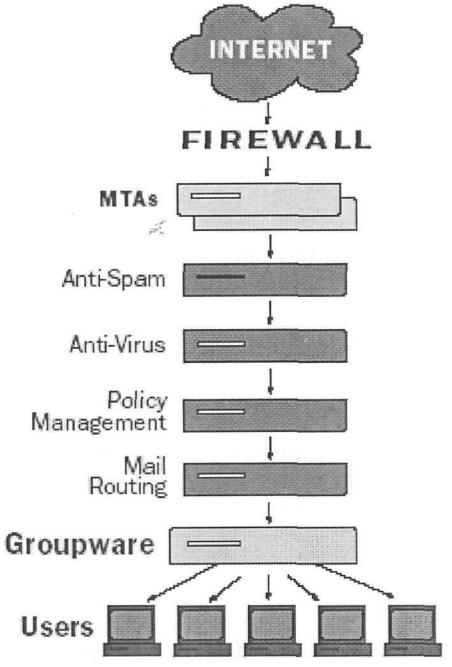
Varios son los niveles en los cuales se presentan los problemas de tráfico de correo no deseado, como por ejemplo, el usuario final con la descarga de cientos de correos que alteran su tiempo de trabajo, el tráfico que el dominio receptor recibe de todos los correos no deseados, en el proveedor de servicio al procesar todo el tráfico de diferentes puntos de la red de Internet con ataques o tráficos de correos masivos o correos no deseados en varias direcciones, el servicio de correo usado como relay dado el caso de un ataque de hackers, etc.

Actualmente existen varios sistemas de atención ante correos no deseados y los cuales están basados en técnicas de estadísticas de arribos entre las más conocidas esta la del algoritmo Adaboost, Naive Bayesian y Aproximaciones basadas en Memoria (Androutsolpoulos, Paliouras, Karkaletsis, Sakkis, Spyropulos, Stamatopoulos) los cuales por la dirección del presente estudio no serán estudiadas a fondo, pero si los dispositivos tecnológicos basados en estos modelos.

Todos estos modelos permiten la identificación de las amenazas y correos no deseados que intenten generar tráfico no esperado en cualquier punto de Internet; más sus procedimientos para evitar correos publicitarios no deseados, tienen que trabajar en conjunto con otros modelos de determinación de servicios maliciosos y ataques como virus. Hoy día, las mejores prácticas en la

solución de estas amenazas encausan a que las mejores soluciones todos estos modelos se integren en mayor o menor grado en dispositivos diseñados por varios fabricantes, esto con el fin de mitigar todas las amenazas que a través del Internet podemos recibir, tales como virus, gusanos, troyanos , todos ellos viajando a través de los servicios de correo.

Como vemos en la siguiente gráfica, son varias las capas que hay que validar antes de enviar o recibir un correo de forma segura según se muestra y a fin de evitar tráfico no deseado hacia Internet. Y los filtros que se presentan son aquellas configuraciones básicas para lograrlo. En esencia el servicio SMTP es frágil y puede ser mal usado por su infinidad de opciones que en su momento fueron grandes capacidades de este servicio según los su RFC 821 que fue desarrollado en 1982 (http://www.faqs.org/rfcs/rfc821.html). Pero desgraciadamente estas mismas ahora son utilizadas como ventajas para quienes explotan estas vulnerabilidades para enviar correos publicitarios no deseados.



Políticas para evitar correos no deseados

Las capas conformadas por el servicio de transferencia de correos hacia/desde Internet actualmente están conformadas por los siguientes niveles:

Primeramente el punto de conexión con el tráfico global o el punto más externo de la red empresarial, esta separada mediante un FireWall el cual se encarga de limitar los accesos a los puertos no deseados así como verificar aquellos paquetes de tráfico que puedan contener algún índice de ataque.

Y los servicios de transferencia de correo desde los dominios y las transacciones de estas conexiones con servicios remotos en donde se validan, los servicios básicos de SMTP según el protocolo y servicios de DNS, de acuerdo a las reglas básicas.

A continuación las reglas de filtraje y validación de correos no deseados, los servicios de verificación de los archivos agregados y cuerpo del correo contra virus, troyanos o gusanos.

Las políticas administrativas, para el manejo de flujo de correos dependiendo de las unidades de negocio hacia donde o desde donde vallan dirigidos.

El ruteo de correos internos, a fin de establecer las configuraciones necesarias de servicios de ruteo, accesos de usuarios, etc;

Todos los puntos anteriores los pudiéramos agrupar por etapas dependiendo del trato que se le intente dar el flujo del correo o colocar todos en conjunto como los lineamientos básicos que cada servicio de correo debe manejar para asegurar el control correcto de la manipulación de tráfico no deseado.

De la anterior serie de capas, podemos ver actualmente las soluciones como el MS-Exchange 2003, por ejemplo, del que podemos notar que la nueva generación de Servidores de correo de Microsoft ,

cuenta con un esquema de verificación de tráfico y detección de correos del tipo "spam" o correo no deseado., mediante el uso del servicio Exchange Intelligent Message Filter Service, el cual basados en las tecnologías de Microsoft, verifica todo el tráfico de correo de acuerdo a ciertas guías de servicio como (Microsoft Technet):

Verifica en la conexión de SMTP entrante de cada correo entrante si es parte de una lista de aceptación

Verifica si la conexión de SMTP del correo entrante es parte de una lista de bloqueo

Verifica contra una lista de bloqueo de tiempo real configurada en algún servidor referenciado en Internet (como el caso de www.spamhaus.org).

Si los filtros anteriores no contrarrestan el flujo del mensaje, se procederá a verificar la dirección del emisor, contra la lista de filtros de emisores configurados manualmente.

Si ninguno de los pasos anteriores evita el flujo normal del correo hacia el buzón destino, filtro de mensajes inteligente de MS-Exchange 2003 asigna un nivel de confidencia al mensaje spam o correo no deseado SCL el cual es mayor , igual o menor que el máximo establecido para el servidor, y con estos valores automáticamente este filtro tomará acción eliminando o entregando finalmente el correo.

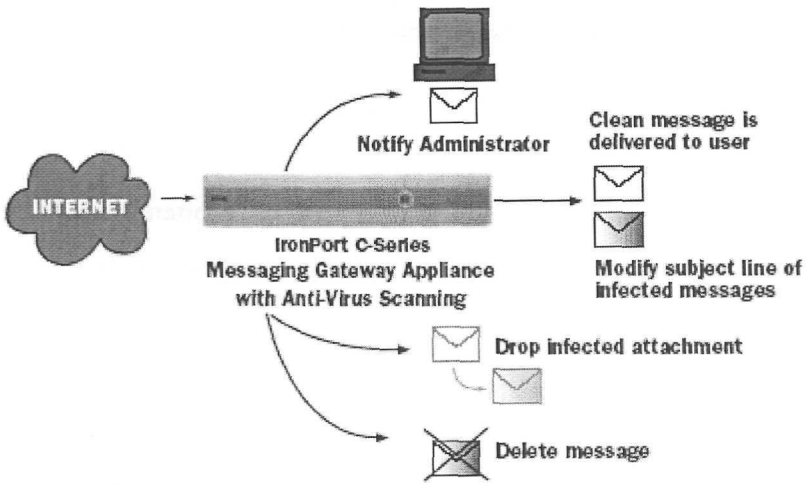
Como se observa, en esta plataforma, existe una tendencia a fusionar varias de las capas de servicio para el filtraje de correos no deseados, como el caso de servicios de MTA (trasferencia de correo), los servicios de ruteo y el servicio de filtraje de correo no deseado (anti-spam). Estas acciones aunque resuelven parte del filtraje del correo no resuelven de fondo el problema dado que aquellos dominios hallados como de emisores de correos no deseados, y localizados en las listas negras, pueden ser también reconocidos por los emisores de estos correos, buscando agregar nuevas direcciones o dominios que no estén registrados para continuar con su operación.

Esta bien puede ser la forma básica de aseguramiento del tráfico de correos confiables hacia cualquier dominio en cualquier empresa, pero actualmente este proceso conlleva a una gran capacidad de procesamiento debido a la alta taza de correos comerciales no solicitados (spam) que atacan a cualquier Dominio o mejor dicho a cualquier registro MX de DNS, el cual es la referencia inequívoca de la actividad de SMTP en esta IP (referencia a través del servicio de DNS según BIND)

Asimismo, en los siguientes niveles de procesamiento de flujo de correo electrónico, tales como los grandes corporativos y los proveedores de servicio, otras tecnologías como Brigthmail (Symantec) o Postini, y actualmente Mail Hosted (Symantec), están ofreciendo servicios de administración de tráfico de correo, otorgando toda la capacidad tecnológica para soportar un gran nivel de correos de acceso y entrega, filtrando todos aquellos que muestren señales de amenaza a los dominios de correo administrados, así mismo también ofrecen servicios de antivirus, filtrado de contenido que pareciera ser hoy en día un acopio de esfuerzos de las diferentes tecnologías para mantener el tráfico de Internet libre de correos con elementos maliciosos o tráfico no deseado (DoS, DDoS, etc).

En estos servicios ofrecidos además de las técnicas ofrecidas por los servicios de antiSpam tradicionales como los mostrados previamente, se establecen servicios como Prevención de amenazas y filtros de Repudiación, basados en servicios como los ofrecidos por las organizaciones internacionales de monitoreo de tráfico como es el caso de los reportes del tráfico de Internet localizados en el portal http://www.internettrafficreport.com/main.htm en el cual aparecen los tiempos de respuesta en los diferentes puntos de interconexión entre las redes de todo el mundo a fin de determinar posibles problemas de tráfico por fallas técnicas o ataques dirigidos (DoS, etc); Logrando así detectar en que punto de la red global aparece alguna lentitud y sus causantes. De este forma, para los casos comerciales, como IronPort, este genera una red de servicios de apoyo entre diferentes Universidades y grandes corporativos que actualizan de información a los diferentes equipos de manejo de correo no deseado, manteniendo una red con datos en línea de cualquier anomalía en tráfico de correo en Internet. Por otro, lado con el apoyo de otra serie de sitios de

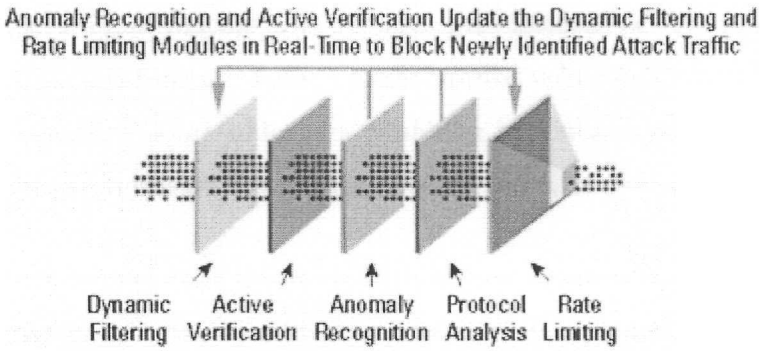
Internet capaces de monitorear en diferentes latitudes de la red el flujo de correos publicitarios no deseados para indicar cualquier cambio o incremento del flujo de algún mensaje en especial para reportarlo a los diferentes equipos como el ya mencionado Spamhaus, este tipo de servicio permite lograr una lista universal de usuarios y dominios permitidos o censurados



Políticas Ironport

De lo anterior podemos desprender que como lineamiento para el correcto seguimiento del tráfico de los equipos, estos deberán estar referenciados a organizaciones internacionales o contar con algún elemento de medición actualizado del estado del tráfico en todo momento, así como las incidencias de correos no deseados viajando en la red en todo momento.

Otras formas, como en el caso de CISCO, basados en un esquema de multi-verificación de procesos (MVP), que integra una variedad de verificaciones, análisis y técnicas de robustecimiento para identificar y separar tráfico malicioso del tráfico legítimo. Como se ve en la siguiente gráfica.



CISCO MVP

Filtraje- se realizan filtrajes estáticos y dinámicos de DDoS. El filtraje dinámico es posible por la integración de varios módulos de esta tecnología, y verifica el comportamiento del tráfico y su análisis, para la verificación de flujos sospechosos y el bloqueo de fuentes y flujos verificados como maliciosos.

Verificación Activa.- Determina si en el tráfico recibido no halla sido comprometido mediante spoofing.

Reconocimiento de anomalías.- monitorea el tráfico que no ha sido detenido por los filtros previos y compara este contra el lineamiento de tráfico básico inteligentemente obtenido en el tiempo por parte del dispositivo, buscando por desviaciones que puedan identificar la fuente del ataque malicioso.

Análisis de protocolos- procesa los flujos que la parte de reconocimiento de anomalías reconoce a forma de determinar ataques de aplicaciones específicas.

Limitación de ancho de banda- se penaliza a aquellas fuentes de tráfico que consuman demasiados recursos (tanto de ancho de banda como conexiones).

Como se ha visto hasta ahora muchas son las fases provenientes de diferentes fabricantes, pero nuestro estudio aplica hacia la forma de hallar y medir aquellas vulnerabilidades en las configuraciones anteriormente mencionadas y sobre todo para establecer los lineamientos básicos de operación y buscar conjuntar de entre todos ellos la forma más clara y optima de operación.

Asimismo, nuevos estándares se están desarrollando a fin de contrarrestar aquellas vulnerabilidades de SMTP, como es el caso de Microsoft y ePrivacy, quien el 30 de abril del 2003, introdujeron TEOS (Estándar abierto de correo electrónico confiable Trusted Email Open Standard), cual esta basado en 3 principios:

Mejores prácticas
Habilitación y uso de tecnología
Supervisión

Mejores Prácticas

A	Estándares de Responsabilidad	Identidad del emisor
		Aseveración del tipo de mensaje
B	Certificación de Correo Electrónico Emisor confiable	Aseveraciones requeridas: Tipo de mensaje Relación/permiso
C	Orientado al consumidor Programas de certificación	Aseveraciones requeridas (además de las anteriores) : Aseveraciones visibles Sello de seguridad (verificación de un clic) Enlace de política de privacidad

En vista de las pros y contras de cada una de las tecnologías disponibles en el mercado, los lineamientos básicos que con las tecnologías hoy podemos tener para minimizar la posibilidad de trafico no deseado, nos basaremos en las siguientes salvaguardas deberán ser implementadas siempre que se configure algún filtro de correo no deseado.

Evitar el uso de las respuestas ante direcciones no localizadas dentro del dominio de correo en cuestión a fin de evitar correos involuntarios no deseados o ante ataques de diccionario para la determinación de cuentas posibles en el dominio.

Los servidores de correo o equipos segmentadores de red (Firewalls) deberán ser equipados con programas de filtrado de correos no deseados (spam) que permitan solo el acceso de/hacia dominios confiables o especificados por los usuarios y que filtren los correos no deseados en base a los encabezados o frases en el cuerpo del mensaje.

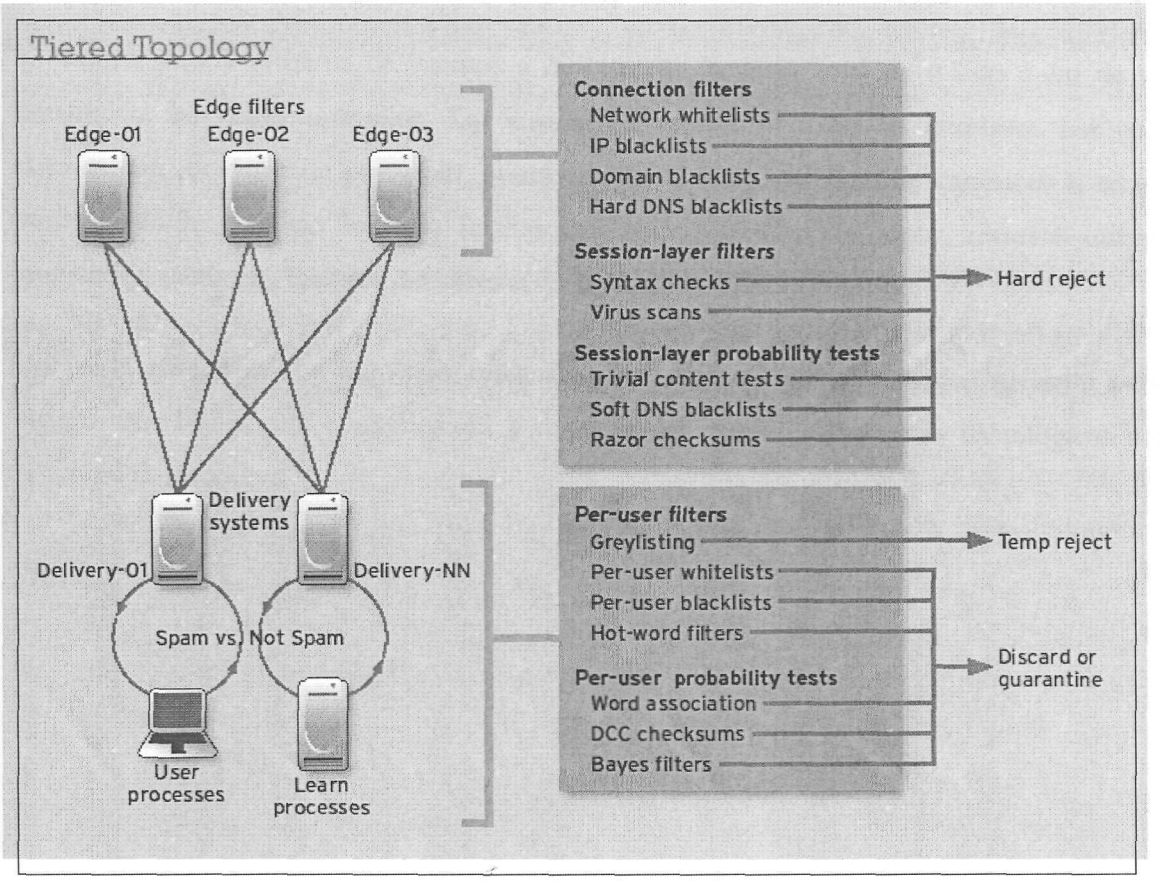
Debe colocarse una lista blanca de acceso para evitar en la medida de lo posible el filtraje de correos deseados

No deben de configurarse auto-respuestas para las confirmaciones de baja de correos no deseados o cualquier medida que pueda crear tráfico no deseado.

Se considerara como correos no deseados aquellas incidencias de tráfico por correos de algún dominio en especial mayores a 20 correos por hora.

Se deberá emplear algún programa automatizado a fin de tomar muestras fehacientes del tráfico en estado estable a fin de determinar dinámicamente el lineamiento base para el funcionamiento normal del servicio de correo.

Lo cual en teoría debe de darnos un esquema como el siguiente propuesto :



Dentro de la parte de configuración de ruteadores y Segmentadotes (Firewalls), podremos seguir los siguientes lineamientos para irlos acotando y alineando a un esquema de seguridad básica: (CERT):

1.- los tiempos de desconexión (tiempos después de los cuales una conexión inactiva es liberada) deben ser colocados al mínimo aceptable. Este procedimiento solo mitiga el efecto de las conexiones en exceso, no los ataques.

2.-verificar si se cuenta con la capacidad de desarrollar reglas de spoofing, para ello deberá contar con la distinción entre el tráfico de arribo y el tráfico de salida, en cada interfase.

3.- dentro de los archivos de eventos a monitorear: la carga total de tráfico a fin de definir el lineamiento básico de operación. Las cuentas de errores en todas las interfases. Las conexiones exitosas con los datos de protocolo, puerto, destino, tiempo; el flujo de conexión: la secuencia de paquetes desde el inicio hasta la finalización. Puertos Socket's abiertos, recursos utilizados del procesador, memoria; cambios del sistema, incluyendo apagado y reinicio.

Los pasos anteriores son esquemas básicos, mas la idea es conjuntar para el presente estudio, los lineamientos básicos de configuración y operación de varios dispositivos tecnológicos a taque a tráfico no deseado.

5.3 Modelos estadísticos que describen el comportamiento del correo no deseado.

Los datos del correo electrónico es información disponible que incluye los datos personales del usuario de Internet (Groebel, Metze-Mangold, van der Peet, Ward) . El correo electrónico puede ser obtenido de varias formas: Proveedor del cliente de correo, el cual es comprado u obtenido libremente y puede solicitar al usuario registrarse.

Desde el programa del cliente, en el cual un código permite transmitir el correo-electrónico al proveedor del programa sin consentimiento o conocimiento. Algunos navegadores, los cuales pueden ser configurados para enviar las direcciones de correo como contraseña anónima en las sesiones de conexión FTP.

Los sitios de Web pueden directamente solicitar las direcciones de los correos de sus visitantes, por ejemplo en el caso de una compra. De la intercepción durante la transmisión de un mensaje De algunos navegadores. Han existido reportes de seguridad que permiten al sitio web conocer el correo de los visitantes. Esto puede ser posible via, por ejemplo javascript.

De las formas mencionadas, existen un sinfín de formas y maneras de conseguir cuentas de correo que eventualmente se transmiten en forma de obtener correo no deseado.

A fin de establecer las formas es que estos correos son recibidos y como es que cambian los patrones de comportamiento de las tramas de correo por persona, por equipo, por servidor, por dominio y aún por proveedor de servicio de Internet, muchas escuelas se han evocado a la determinación de Modelos que puedan proveer de las bases necesarias para determinar cuando un ataque de este tipo de correos se suceda en la red y apoyar a detenerlo y a esclarecer como es que las direcciones y el flujo de correo es que se produjeron.

MET/EMT es una de estas propuestas, que a diferencia de los sistemas detectores de Intrusos provee de las métricas necesarias para ir descubriendo tanto fuera de línea (realizando las pruebas directamente sobre el archivo de correo almacenado localmente en el disco duro)

La detección masiva a gran escala, este rango de actividades de vigilancia con alta precisión, presenta una seria de retos técnicos. Por ejemplo el seguimiento en tiempo real de los escaneadores en prospectiva dentro de ancho de banda grandes presentan retos con respecto a la memoria y la velocidad, dados los análisis temporales necesarios para detectar los escaseaos furtivos. Mas aún, ciertos puntos de unión de redes sufren algún tipo de perdida de información, tal como debidos a rutas asimétricas.

Otra de las soluciones de Monitoreo y determinación del comportamiento básico (Base Line) es SysD una solución de Monitoreo, que emplea un filtro en cascada que coordina una serie de pruebas heurísticas especializadas a través de registros de conexiones extrapoladas, pruebas individuales, escaneos y grupos de escaneo coordinados. Este diseño provee escalabilidad vía la reducción de datos a través de filtros agregados y detectores de escaneo y pruebas en ambientes de anchos de banda elevados con alta cobertura y bajas tazas falsos-positivos (FP) 2 variaciones se especializan en ambientes clase: monitoreo de detección de enclaves (ESD) y detección de puntos de contacto (PSD). Durante el desarrollo del presente estudio, muchas de las herramientas básicas y de código abierto fueron utilizadas a fin de tener una referencia rápida y fácil de usar para la respuesta con el usuario.

Todos los sistemas de detección de intrusos comerciales y de código abierto, contienen técnicas para la detección de puertos abiertos y otras formas de monitoreo. Lo más típico es buscas por X eventos de interés en una ventana de tiempo Y en segundos.

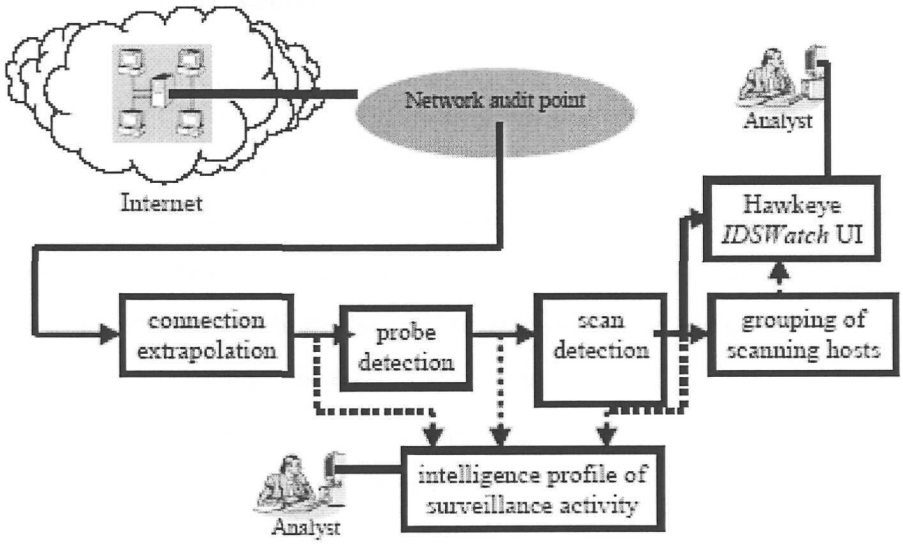
Por lo que para los muestreos descritos posteriormente se pretende de los registros de eventos de los diferentes MTA's para poder ir analizando las tendencias de incidencias de correos de arribos y usarlos posteriormente para compararlos en tiempo real.

ESD y PSD no usan estadísticas de anomalía para detectar pruebas individuales. La razón primaria para esto es que, la vigilancia es pre-valente a las pruebas individuales. ESD Y PSD difieren de SPEDE/SPICE que en lugar de aglutinar para agregar pruebas dentro de los escaneos simplemente realiza pruebas de toda la red.

Otro sistema es el scanlogd, el cual es una detección basada en un equipo huésped, aunque también puede ser configurado para detectar escaneos de puertos de una forma promiscua a través de un husmeador de red (Network Sniffer) , estos servicios aunque utilizados para determinar el tráfico de la red, no nos llevaron a tener un panorama adecuado para contra-restar el flujo de correos no deseados, pues aunque podíamos contar con información del aumento de solicitudes de DNS (UDP-53) y tráfico de correo SMTP (TCP-25) , por lo que nos ayudaron a plasmar las características de la red, y a validar las posibilidades de SPOOFING.

Dentro de los retos de los diferentes sistemas de monitoreo, se halla los métodos de prueba y escaneo, los cuales son variado, irregulares e impredecibles, siguiendo con agendas impredecibles de los atacantes y heurísticas. En segundo plano, completar sesiones reensamblando el código de TCP/IP original es impractico, dado que requeriría conocimiento preciso y completo de todas las idiosincrasias y pilas de implementaciones. Y cuales paquetes tengan errores de red que no les permitan llegar a sus destinos. Mas Aún, en una habilitación en línea de modo promiscuo, el punto de encuentro con la red, es difícil de mantener a las sesiones de tiempo real debido a las diversas conexiones entre muchos equipos.

ESP y PSD, sobre pasan los retos anteriores, con 3 procesos de filtros en cascada, como se muestra en la siguiente figura



Primero sesiones aproximadas entre parejas de IP fuente/destino son extrapoladas con un modelo que es largamente una simplificación del descrito por Lee. Segundo, cada sesión de extrapolación que representa un intento de conexión fallado o un paquete interesante a ser probado. En el caso de ESD, estas son conexiones grandes que muestran solo movimiento en una dirección, de la fuente al destino, sin respuesta. Tercero, cada IP que es probada se le da un valor basado en el número de destino de IP/puerto único que es probado. L IP es un considerada un escaneador su valor es mayor que los básicos determinados empíricamente: las IP's que pasan tal nivel básico son considerados escaneadores (a menos que sean falsos-positivos) dado que una muestra considerable de direcciones menciona que hay conexiones fallidas.

Los efectos de seleccionar los niveles básicos empíricos, estas alertas controlan los números de sistemas de monitoreo y vigilancia producidas; solo una fuente de IP que ejecuta las suficientes pruebas para cruzar los niveles básicos. La selección de los niveles básicos es crítico para la optimización de los sistemas dado que niveles de señalización elevados pueden resultar en un gran número de alertas.

Estas pruebas realizadas indican que al menos aquellas IP's que generan escaneos lo hacen en repetidas ocasiones. El retardo entre-pruebas esta definido como el tiempo promedio entre las pruebas durante la duración del monitoreo, del tiempo de escaneo de la primer IP hasta la ultima. La distancia de grupo es la máxima distancia entre 2 direcciones IP y puede estar distante de cualquier otro (numéricamente, tratando una IP como un numero literal de 4 Bytes) de tal forma que pueden ser consideradas bajo el mismo sistema de monitoreo.

De lo anterior podemos concretar que se pueden hallar Ilustrativas muestras de detección de los rendimientos sobre varios parámetros.

Habilitando los canales para seleccionar los parámetros de los valores apropiados al comportamientos especifico y los parámetros concernientes a los enclaves de seguridad.

Mediante al agrupación de escaneadores se pueden reducir las alertas, pero deben de limitarse en rango para que puedan ser efectivos.

Otros tipos de Detectores de intrusos son NSOM, que usan sistemas de redes artificiales neurálgicas (de las siglas en ingles ANN), en los cuales los patrones de tráfico normal son alimentados a un ANN, el cual subsecuentemente aprende el patrón de comportamiento del tráfico normal.

Otros sistemas utilizan estadísticas descriptivas desde ciertos parámetros dentro de un perfil, y construyen un vector de distancia para el tráfico observado y el perfil. Si la distancia es suficientemente grande el sistema aumenta la alarma. Ejemplos NIDES, EMERALF y Haystack

La gráfica de continuación muestra un diagrama de bloques de NSOM (Network Self-Organizing Maps), en el cual se muestras los diferentes pasos que el sistema ejecuta para alcanzar en tiempo real las clasificaciones del tráfico en la red.

La información seleccionada para ser clasificada es aquella que contenga la siguiente información:
De cada paquete recibido, se extrae la dirección IP de destino: se usan solos los 2 números menos significativos para la clasificación.
Se extraen las direcciones IP del origen: se usan los 2 números menos significativos.
Se extrae el tipo de protocolo

Un vector característico representando al paquete consiste de 5 características representando el destino parcial y la dirección de origen y el tipo de protocolo.

$$nv[i] = \frac{v[i]}{\sqrt{\sum_k v[k]^2}}$$

Donde nv[i] es el valor normalizado de las característica (i), v[i] es la característica de valor de i, y k es el número de características de un vector.

Aún y cuando los tiempos de arribo y salida de los paquetes fueron explícitamente disponibles, antes de los datos fueran procesados, se decidió no usar explícitamente estos.

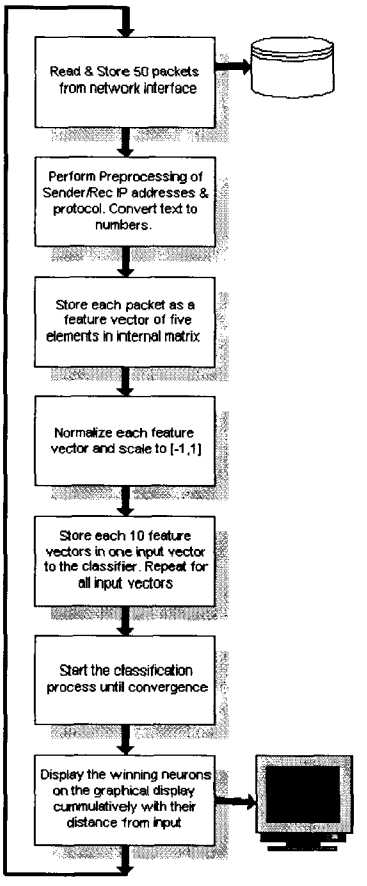
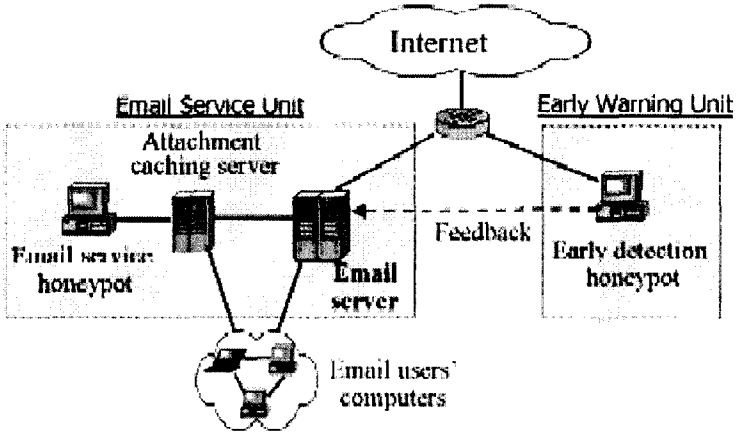


Diagrama NSON

Resientes revisiones, de IDS's dividen éstos sistemas en una gran rama de aproximaciones que incluyen sistemas expertos, patrones relacionales, análisis de transición de estados, redes neuronales y estadísticas.

Así por ejemplo existe el análisis de redes de eventos de tráfico anómalo (de las siglas en ingles Network analysis of Anomalous Traffic Events), en este sistema, el administrador no necesita conocer los parámetros del sistema en estado normal para configurarlo. NATE busca minimizar la cantidad de datos necesarios para la detección de ataques midiendo pequeños número de atributos.

NATE se basa en el análisis de cluster, el cual tiene como propósito agrupar datos, dados que los objetos dentro del cluster sean similares a cada otro y disimilares de los que se hallan fuera. Esto con el fin de detectar el tráfico normal. El muestreo es un análisis estadístico para obtener un subconjunto que representa la población. El muestreo por TCP requiere que cada tráfico mayor sea representado en la muestra.



Gráfica NATE

5.3.1 Estableciendo los lineamientos Básicos de Operación

A nivel estación de trabajo mediante algunas herramientas como el EMT el cual corre un análisis en cada archivo anexo para calcular un número de métricas. Estas incluyen, razón de generación, periodo de vida, razón de incidencia, prevalencia, amenaza, capacidad de esparcimiento (Salvatore,Shlomo, wang, Nimeskern,ChiaweiHau, 2005).

Las reglas especificadas pueden ser ejecutadas sobre archivos de correo electrónico almacenados (EMT) o en tiempo de ejecución (MET). Así por ejemplo algunas de sus reglas básicas se pueden verifican con la siguiente lógica:
Si su razón de nacimiento mayor que un umbral específico T Y enviado desde al menos un número X de usuarios...Mas la idea es correr precisamente esta clase de reglas, pero adecuadas a el tráfico de smtp y servicios de los DNS y RBL, a fin de tener las tendencias de operación de los servicios de MTA's, todo lo anterior aprovechando los registros de eventos, para en base a estos históricos generar los comportamientos que puedan determinar las intendencias que no se comparen con el estado estable y puedan contener una alta probabilidad de correo publicitario no deseado.

Histogramas son usados para modelar el comportamiento de las cuentas de correo.

Este tipo de detecciones por comportamiento, no es nueva. Los fraudes de tarjetas de crédito es el mejor ejemplo de estos sistemas de seguridad basados en el comportamiento. En base a estos comportamientos se han desarrollado Modelos matemáticos que pueden ser usados para capturar la frecuencia del uso del correo (Stolfo,Chia-Wei Hu, Wei-Jen Li, Shlomo Hershkop, Ke wang, Olivier Nimeskern).

5.4 Modelos de Comunicación: "Cliques" o Grupos

Para identificar los grupos de afinidad relacionados a las cuentas de correo que participan con otras en las comunicaciones de correo-electrónico, se requiere captar esta información. Y obtener su comportamiento básico (Base-Line) para así poder identificar el comportamiento que viole estas líneas bases.
Un Ejemplo de comportamiento de un usuario pudiera ser semejante al siguiente:
Los siguientes grupos a los cuales envía correo: {A,B,C}, [A,B,C},{A,B} y {A,B,D}, por lo que los grupos a los cuales el pertenece son {A,B,C} y {A,B,D}. Los grupos repetidos son retirados.

De este modelo, para el presente estudio, se tomó el comportamiento de arribos de correo al dominio a fin de establecer estadísticamente las probabilidades de arribos de Correos No deseados, basados estos en otras indicadores, además del comportamiento base de los Dominios desde donde se envían o se reciben los correos. (Estos fueron tomados de los registros de eventos de SMTP en cada MTA de los servidores analizados para determinar las incidencias y las tendencias de correos)

Así por ejemplo se hallaron en espacios semanales tendencias interesantes, como las siguientes muestras, en las cuales notamos un ataque de Correo Comercial no deseado a la lista interna de correos del Dominio de MIGESA:

12/03/2006	1:7:40 GMT	222.91.8.215	200.57.81.39	-	3jeasca@migesa.com.mx	1019	22916	1	2006-3-12 1:7:16 GMT	re[11]	xxqzvgvryevrr@hotmail.com	-
12/03/2006	1:7:40 GMT	222.91.8.215	200.57.81.39	-	3jeasca@migesa.com.mx	1025	22916	1	2006-3-12 1:7:16 GMT	re[11]	xxqzvgvryevrr@hotmail.com	-
12/03/2006	1:7:40 GMT	222.91.8.215	200.57.81.39	-	3jeasca@migesa.com.mx	1024	22916	1	2006-3-12 1:7:16 GMT	re[11]	xxqzvgvryevrr@hotmail.com	-

En esta podemos observar el número de sesión, la Ip de procedencia y el usuario destino, el cual no existe en el dominio, esta práctica es muy común entre los atacantes actuales al enviar cuentas de correos a dominios existentes con un nombre de usuario al azar, para por medio de diccionarios, - como en caso del plagio de contraseñas, ir eliminando las posibilidades de nombres que no estén dados de alta en el dominio e ir generando la lista de destinatarios validos, ya que algunos dominios, cuando no tienen un usuario válido normalmente notifican al emisor que el destinatario de su mensaje no fue hallado, y mediante esta táctica el atacante puede ir creando la lista de usuarios válidos del Dominio.

Para este caso en especial, la IP del emisor nos ayuda para ir determinando los grupos o cliques, dado que aunque a simple vista podemos darnos cuenta en base al nombre del emisor del correo que es una cuenta falsa, nuestras herramientas no lo pueden determinar tan fácilmente a simple vista.

El presente estudio, considera la posibilidad de asociar basados en el comportamiento, por lo que usando muchos de los eventos, se pretende el reconocimiento de los patrones de conducto tanto de arribos como de envios para un Dominio dado.

A fin de lograr la obtención de el comportamiento y las frecuencias se tomaron ciertas consideraciones, de acuerdo a los histogramas obtenidos en base a los registros de eventos.

Con ellos, la idea es obtener, es modelar el comportamiento en función de horarios (2 zonas de 12 horas diarias, es decir dividido el día en 2).

5.4.1 Funciones de Histogramas de Distancia

De forma general, un histograma es un mapeo simple para contra el número de observaciones que caen en varios categorías discontinuas. Así, denominamos N al número total de observaciones y n el número total de discontinuidades,

$$N = \sum_{k=1}^{n} h_k$$

Donde K, es el índice de las discontinuidades.

A fin de detallar el comportamiento básico, de la información obtenida por diversos medios (tcpdump, Registros de eventos de los servicios de correo: MS Exchange, maillog: Sendmail, etc. se realiza la obtención de los patrones históricos de comportamiento, por medio de Histogramas de Distancia. Para obtener las tendencias del comportamiento en las 2 zonas horarias establecidas, mencionadas previamente, las cuales estan acotadas a un máximo de 12 hrs. Una vez logrados los histogramas, loas cuales se obtienen en base a las incidencias de las IP's hacia el dominio en cuestión, se obtienen tambien otros parámetros como la distribución de la máxima incidencia de correos, la

información del tiempo de vida, ya sea comparado contra el perido previo anterior (12 hrs) comparado contra el día anterior, 2 días antes o 1 semana antes a fin de poder tazar la incidencia de la IP que esta enviando correo hacia el dominio donde se encuentra realizando la prueba.

Una función de distancia es usada para medir la disimilitud de los histogramas. Para cada par de histogramas h1,h2, existe una distancia correspondiente D(h1,h2), llamada distancia entre h1 y h2. La función de distancia es no-negativa, simétrica y 0 para histogramas idénticos. La disimilitud es proporcional a la distancia. Algunas de las ecuaciones de distancia adecuadas a estos histogramas son:
Intersección de histogramas simplificados (forma L1)
Distancia de euclides (forma L2)
Distancia cuadrática
Distancia de Mahalanobis

Estas medidas estándares fueron modificadas para ser mejormente usadas en el análisis del comportamiento de los correos.

Forma L1 $$D_1(h_1,h_2)=\sum_{i=0}^{n-1}|h_1[i]-h_2[i]|$$

Forma L2 $$D_2(h_1,h_2)=\sum_{i=0}^{n-1}(h_1[i]-h_2[i])^2$$

Cuadrática $$D_3(h_1,h_2)=(h_1-h_2)^T A(h_1-h_2)$$

En donde n es el número de recipientes del histograma. En la función cuadrática A es la matriz donde, aij denota la similiridad entre recipientes i y j. La distancia de Mahalanobis es un caso especial de distancia cuadrática, donde A esta dada por la inversa de la matriz de covarianza obtenida de un conjunto de histogramas de entrenamiento. Estos modelos usados para la determinación de correos, cuyo contenido tenga un alto grado de información no deseada o no solicitada.

Para el Modelo propuesto, nosotros asociamos estas distancias para la frecuencia de distribución de correos entre las IP's de un Dominio previamente verificado de acuerdo a la frecuencia de arribos de correos al dominio.

5.4.2 Comportamiento de usuarios

Este tipo de histogramas son aplicados en las cuentas de usuarios. El máximo tiempo es utilizado como el periodo de entrenamiento del comportamiento básico, por ejemplo, un mes. Asumimos que los recipientes en los histogramas son aleatorios variables que son estadísticamente independientes. Así, se obtiene la siguiente formula:

$$D_4(h_1, h) = (h_1 - h)^T A(h_1 - h)$$

$$A = B^{-1},\ b_{ii} = Cov(h[i], h[i]) = Var(h[i]) = \sigma_i^2 \quad B = \begin{pmatrix} \sigma_0^2 & 0 & \mathrm{K} & 0 \\ 0 & \sigma_1^2 & \mathrm{K} & 0 \\ \mathrm{M} & \mathrm{M} & \mathrm{O} & \\ 0 & \mathrm{K} & 0 & \sigma_{n-1}^2 \end{pmatrix}$$

De aquí

$$D_4(h_1, h) = \sum_{i=0}^{n-1} ((h_1[i] - h[i])^2 / \sigma_i^2)$$

El vector h representa el histograma del periodo examinado (por ejemplo un mes), donde h1 representa el periodo reciente (por ejemplo una semana). σ i describe la dispersión usando el comportamiento del uso alrededor de la media aritmética.

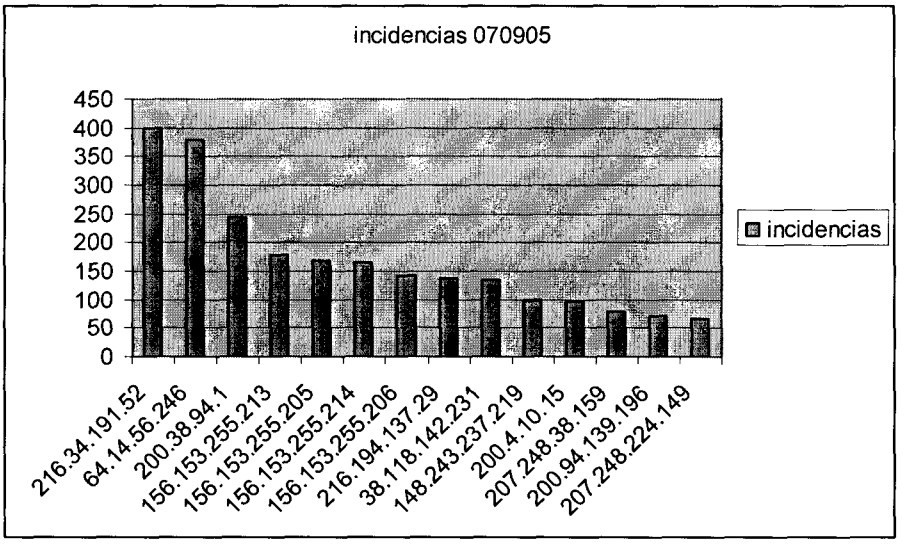
Los histogramas hasta ahora descritos son en su mayoría modelos estáticos, representan las estadísticas de una ventana de tiempo.

5.4.3 Histogramas en operación

A continuación mostramos una ventana de tiempo del registro de eventos del que pudiera ser cualquier servidor de correos al momento de recibir un ataque de correo no deseado.

12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	egonzalg@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	emancerd@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	emenchacag@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	enrique_chapa@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	erick_mancera@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	euflores@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	fsainz@migesa.com.mx	1019	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	egonzalg@migesa.com.mx	1025	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	emancerd@migesa.com.mx	1025	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com
12/03/2006	11:25:22 GMT	222.69.105.114	200.57.81.39	-	emenchacag@migesa.com.mx	1025	523	7	Best Pharmacy BTqe	CKQSYJDTO@msn.com

Algunos de estos modelos no estacionarios tienen que ver con las condiciones de funcionamiento de alguna cuenta de correo en particular sobre subsecuentes transmisiones de correo. La mayoría de las cuentas de correo siguen ciertas tendencias, las cuales son modeladas por algún tipo de distribución. Así por ejemplo de las pruebas muestreadas en el dominio de MIGESA.com.mx durante las fechas de septiembre de 2005.

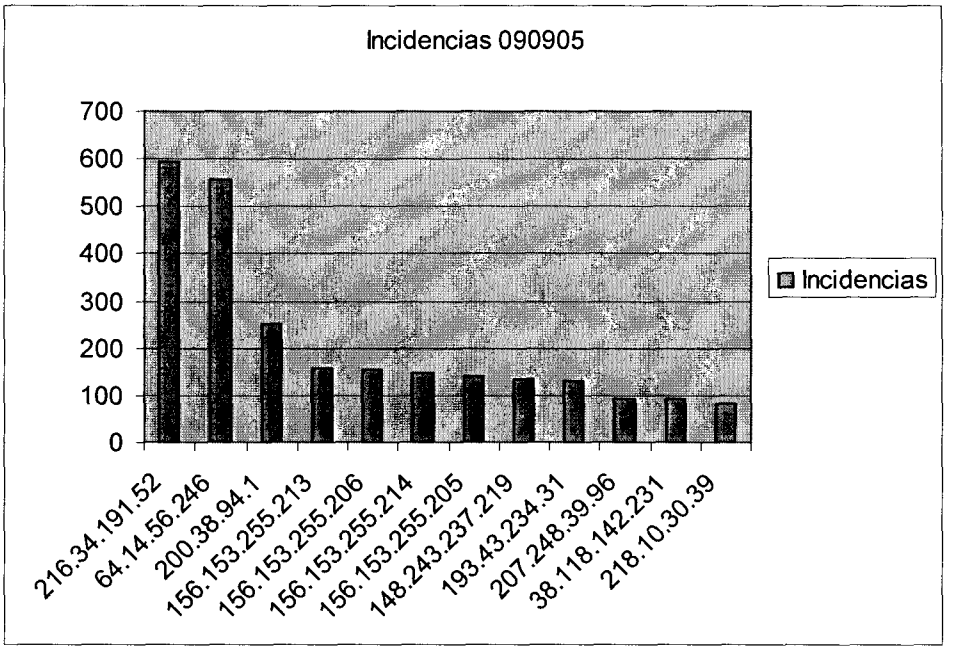


Grafica 070905

De la cantidad de correos recibidos por IP, de las direcciones mencionadas, podemos determinar estadísticamente la taza de arribos, e ir modelado de acuerdo con las herramientas previamente descritos los histogramas y compararlos para obtener y tazar cada dirección IP como probable ataque de servicio o incidencias de correo no deseado.

En la gráfica siguiente se muestra la trama de correos, 2 días después de donde podemos detallar las diferencias entre cada uno de los días e ir asignando probabilidades especificadas dadas las sumas de las características que presenta en base a la cantidad de correos, su procedencia.

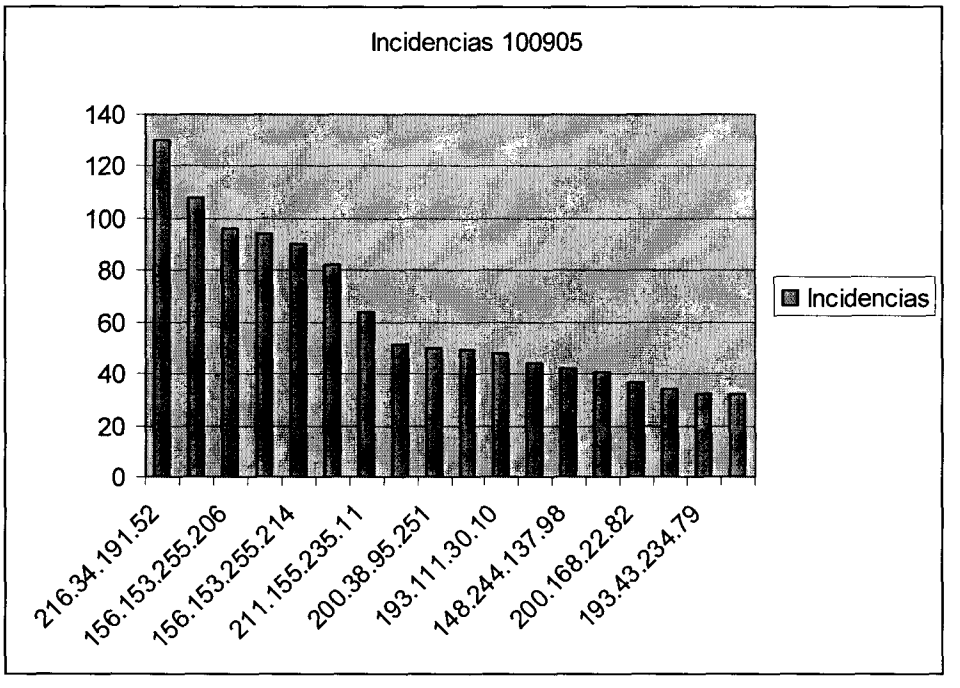
La idea en este servicio, es validar quienes tengan mayor número de transacciones, como se comportan los arribos, zonza 1 o zona 2 (primeras 12 hrs o 12 hrs restantes del día)



Gráfica 090905

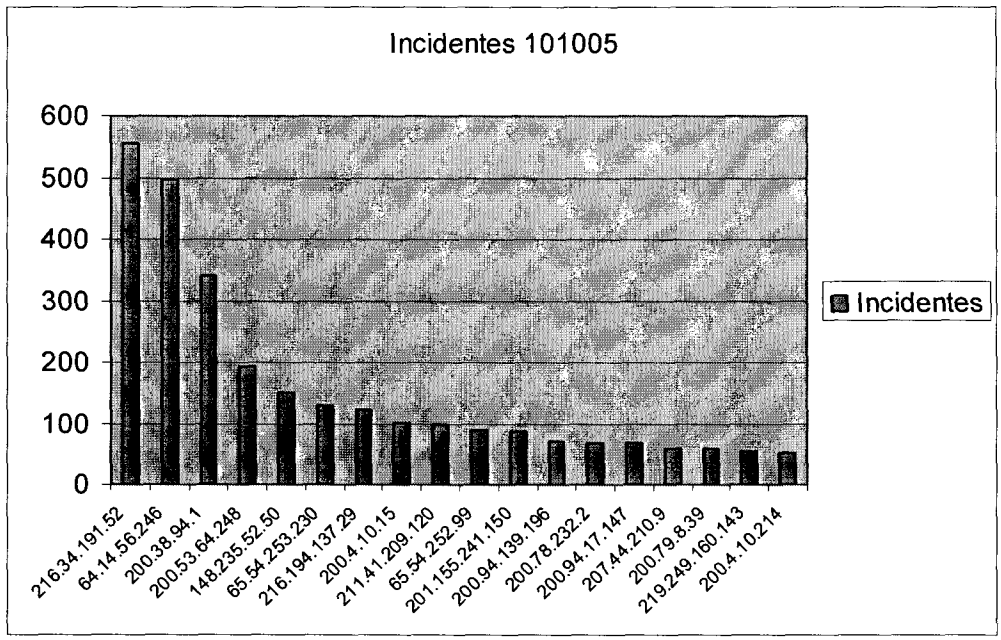
De estos análisis de los registros de eventos, se obtiene cuales serían las IP's con arribos variables, cuales caerían dentro de un rango considerable y cuales se pueden registrar como altamente aleatorias.

La gráfica del día 10 de sep. De 2005, muestra una incidencia menor dado que es un día en fin de semana, pero aún así representa un indicador interesante que refleja el comportamiento de los grupos de trabajo, "cliques" o camaradas según se mostrará en puntos posteriores.



Gráfica 100905

En la siguiente gráfica podemos ver las incidencias de un mes posterior, lo cual, nos demuestra perfectamente los grupos de camaradas con los cuales el dominio de MIGESA tiene un contacto estrecho y existe un intercambio de comunicación (GE, HP, TELCEL, etc) y así mismo incidencias que no aparecían en fechas anteriores. De estas mismas gráficas se determinan los comportamientos o las frecuencias de correos de acuerdo a los días de la semana. (Los días mostrados 7,9,10 y 13 corresponden a los días Miércoles, Viernes, Sábado y Martes respectivament)e, los cuales como se verá más delante, también juegan un papel preponderante para asentar los comportamientos del servicio corporativo del correo.



Gráfica 101005

5.5 Modelos de comunicación: Camaradas

EMT para conformar el comportamiento básico en el intercambio de correos, busca hallar todos aquellos grupos de camaradas en los envios de correos muestreados.

Se busca identificar asociaciones o grupos de cuentas de correos electrónicos relacionados que frecuentemente se comunican entre sí. Y posteriormente se usa esta información para identificar comportamientos de correos inusuales que violen el comportamiento del grupo.

EMT provee un algoritmo para hallar estos grupos de camaradas. Se usa cada correo como un nodo, y se establece un límite entre los 2 nodos si el número de correos intercambiados entre ellos es más grande que el umbral definido para un usuario. Para cada grupo de camaradas hallado en el patrón de envíos de mensajes EMT calcula las palabras más frecuentes que aparecen en estos correos.

Lo anterior es traspolado en nuestro análisis como lo hemos descrito previamente a el uso de MTA's en lugar de un usuario en especial, y sus grupos o claques, las IP's de los dominios con quienes tiene transacciones regularmente, para este caso se establecen los umbrales de las frecuencias halladas de los arribos, las cuales como observamos andan en el orden de 60 correos por Ip y las desviaciones en las extremos del histograma que pueden llegar hasta 660 o el polo opuesto de al menos 1 incidencia por IP emisora de correo.

MET/EMT deben estudiar el número de transacciones en aras de la seguridad y la privacidad de los usuarios, y el valor y el costo del mecanismo de protección que el sistema pueda proveer.

El sistema MET puede ser configurado para extraer características de los contenidos de los correos sin revelar información privilegiada. Como en este caso en el cual lo encausamos a través de los DNS's.

Debido a la practicidad del presente estudio, los análisis de acuerdo a las distancias entre los histogramas, se realizaron mediante el apoyo de funciones obtenidas de otras soluciones a fin de obtener de varias herramientas las cuales se detallaran más delante, las mejores prácticas de los modelos actuales.

5.6 FILTROS analizados

Algunos de los filtros mencionados, son altamente dependientes en constantes desconocidas (como aquellos correos no deseados que no sean listados en los blacklist). Por lo que algunos correos no llegan finalmente a sus destinos, tales causas pueden ser provocadas debido:

Buzones llenos

Servidores sobrecargados

Filtros de SPAM (Falsos Positivos)

Los problemas de falsos positivos, es cuando los correos legítimos son falsamente identificados como spam o correos chatarra debido a su contenido, volumen o inclusión en balcklist. Los siguientes filtros detienen efectivamente el correo comercial no deseado pero eventualmente también filtran correos legítimos

Filtros Basados en Contenido- los mensajes de correo bloqueados por estos filtros son aquellos debido a las palabras o símbolos y otros indicadores que identifiquen los correos con un potencial de comercial no deseado.

Filtros Basados en Volumen- Muchos ISP usan esta clase para contar demandas de alto volumen desde fuentes de correo basura. Si la cantidad de correos excede cierto volumen (ancho de banda, mensajes por segundo, o número de conexiones simultaneas desde un servidor determinado) los mensajes serán bloqueados o re-direccionados a una carpeta de elementos basura.
Apoyados en las mediciones obtenidas en los histogramas y soportados con las comparaciones de los diferentes histogramas, estos pueden apoyar ágilemente a determinar la aparición de un correo con estas características, es decir ante un desborde de incidencias de correo de una IP nueva o una IP previamente en algún grupo, el cual ya ha sido tazada con un numero finito de correos promedio enviados o recibidos.

BlackList[lista negra]- son listas de IP's que están asociadas con emisores de correos no deseados conocidos.

De los Filtros basados en contenido, estos podemos sumarizarlos como DCC (distribuited Checksum Clearinghouse), Algoritmos Genéticos basado en filtros de spam (SpamAssasin) y Filtros Nayve Bayessian (BogoFilter, Spamprove).

Estos Filtros los hallamos con el soporte una Herramienta conocida como PROCMAIL en la cual, incluye dentro de sus servicios muchas de estas modelaciones a fin de lograr la cuantización de eventos necesarios para determinar la posibilidad de un correo dentro de estas listas negras. Dentro de las principales modelaciones se encuentran las de mayor capacidad actualmente: Nayves-Bayessian.

Capitulo 6

6.1 PRUEBAS Y ANALISIS

El análisis del tipo de correo no deseado, puede ser clasificado dentro de las técnicas basadas en contenido, y técnicas de flujo basadas en estadísticas. Existen productos comerciales que usan firmas basados en el análisis del contenido. Los del tipo colaborativo para el filtraje han sido también desarrollados analizando el contenido, los basados en clasificación que usan métodos heurísticos o reglas tales como SPAMASSASIN resultan comunes. Otra más de las opciones resulta ser MSN8 el cual utiliza las aproximaciones basadas en el método Bayessian para la clasificación de contenido de los correos.

Los comportamientos, basados en técnicas como el EMT usa los perfiles de los usuarios, grupos y analiza los archivos anexos de los correos para las estadísticas de la detección de gusanos de correo o virus. Sin embargo, en esas pruebas son estas técnicas para determinar la detección de correos no deseados, por cantidad de arribos, por el comportamiento y por su procedencia, además tales técnicas también requieren obtener datos de al menos a nivel servidor y tener un medio de privacidad para los intrusos.

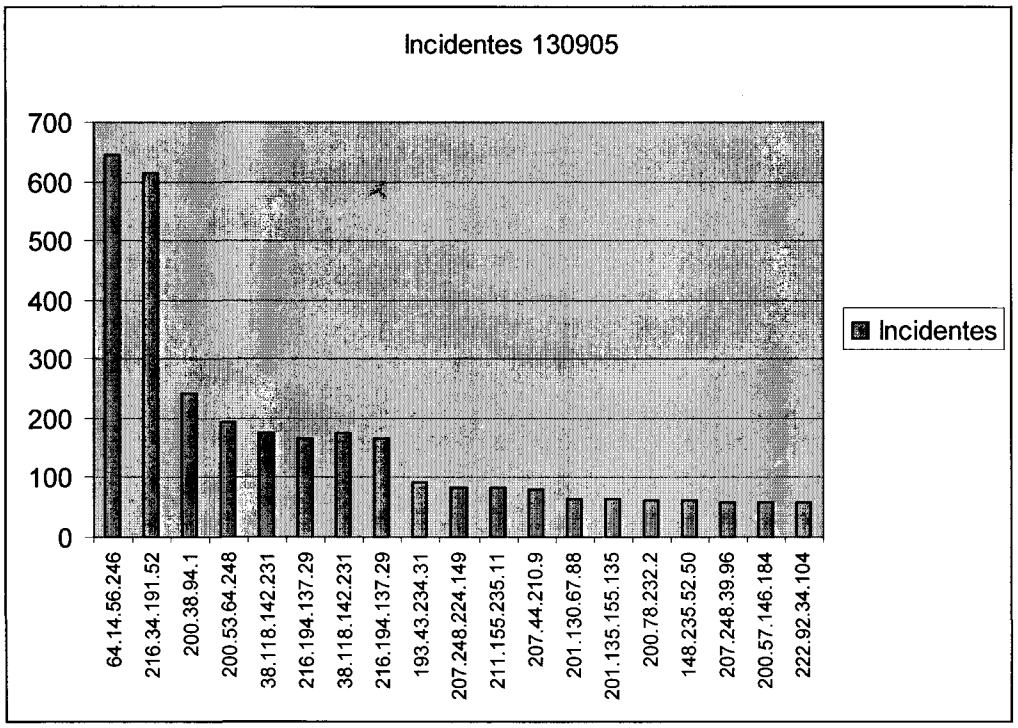
6.1 Parámetros evaluados

Analizando los registros de eventos previamente detallados en base a los registros de eventos para obtener los patrones de comportamiento, encontramos que es necesario en base a las mejores prácticas y apegados a los Modelos observados de EMT, obtener el comportamiento de un Dominio y su recepcion de correos para a partir de ello lograr en tiempo real comparar los comportamiento anómalos.

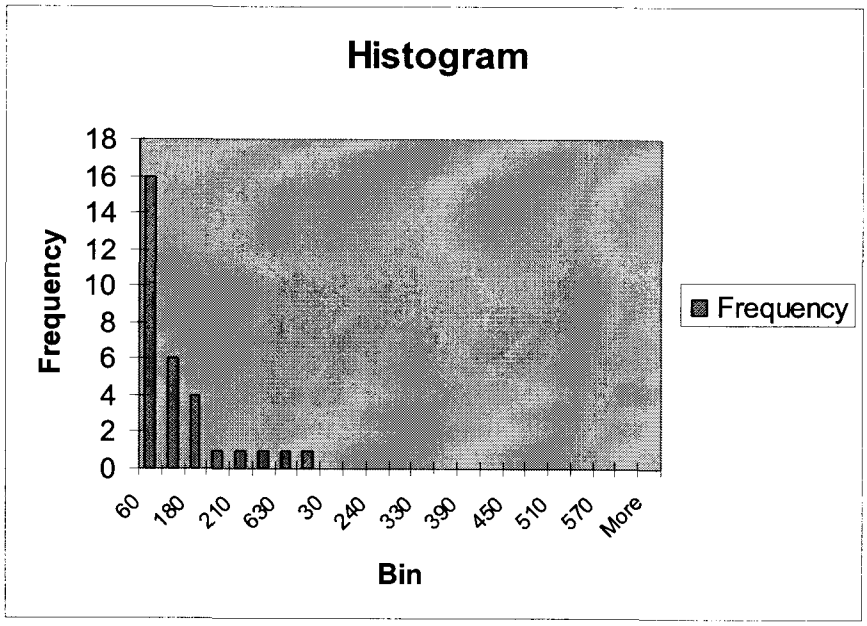
Así por ejemplo de la gráfica siguiente, lograda el 13 de septiembre de 2005, se puede obtener lo siguiente:

- Las tazas de arribos por emisor tienen una frecuencia media de 600 para el máximo número de recepciones.
- La frecuencia total de correos de entrada promedio es de 10000 correos.
- De los histogramas de entrega podemos detectar la taza mayor de entrega distribuido entre el número de correos mas frecuentes: aproximadamente 60 correos
- Los dominios que envíen sus correos en una relación uno a uno, es decir, que entrega correos y cada uno de los buzones del dominio.

A fin de establecer una mejor radiografía de los servicios, se establecen 2 zona de horarios diarios a fin de ir estableciendo en base a los histogramas de los arribos, los cambios de comportamiento en base al día anterior, al medio día anterior, a la semana anterior.



Gráfica 130905



Histograma 130905

Sin embargo, los métodos basados en firmas, fallan en detectar ataques nuevos en las primeras etapas y tales aproximaciones requerirán validar dentro del contenido del mensaje, aumentando los problemas de seguridad de la confidencialidad.

De la gráfica del 13 de sept. De 2005 del tráfico de MIGESA podemos comparar contra la de los días previos 7,9,10 los dominios de grupos con transacciones en tiempo real y determinar con mayor grado de certeza los dominios certificados y las probables cantidad de correos entrantes promedio diarios.

Emisores	Buzones
216.34.191.52	10
64.14.56.246	10
200.38.94.1	8
156.153.255.213	4
156.153.255.205	4
156.153.255.214	4
156.153.255.206	4
216.194.137.29	1
38.118.142.231	20
148.243.237.219	Correo No Deseado- 550
200.4.10.15	2

De esta prueba de igual forma podremos iniciar una semilla de muestra en base a las mediciones, que de una probable frecuencia de unos 10,000 correos entrantes diarios, las variaciones se darán mayormente en las tazas de primer incidencia por lo que se pretenden establecer eventos mutuamente excluyentes, como por ejemplo: que el destinatario sea un buzón no valido dentro del Dominio en cuestión (resultados 550-SMTP) ó que el usuario sea valido pero que repentinamente la taza de arribos se incremente abruptamente.

6.2 Criterios Evaluados

De las sumatorias de probabilidades independientes y a fin de ir conformando la mayor cantidad de enumeración de resultados que nos lleven a conformar la posibilidad máxima =1 , se considera ponderas cada uno de los elementos enumerados a continuación y dentro de cada uno de ellos las probabilidades de asignación:

P [RBL] + P [nuevo emisor IP] + P [sobre pase el comportamiento básico] + P [taza de buzones superior a bases] .

$$P[\frac{A}{B}] = \frac{P[B \mid A]P[A]}{\sum P[B \mid A]P[A]}$$

Algoritmo de escaneo

Supongamos que T es la lista ordenada de correos a muestreas, los cuales son clasificados en función de su incidencia y tiempo de arribo.

La longitud de T = n

Suponemos a C sea las alertas generas por las probabilidades de los grupos o Cliques

Para cada correo T[i], i=1,..n , C[i]=i=1,..n donde a cada correo se le asigna una alerta por la violación por el modelo de grupos o cliques.

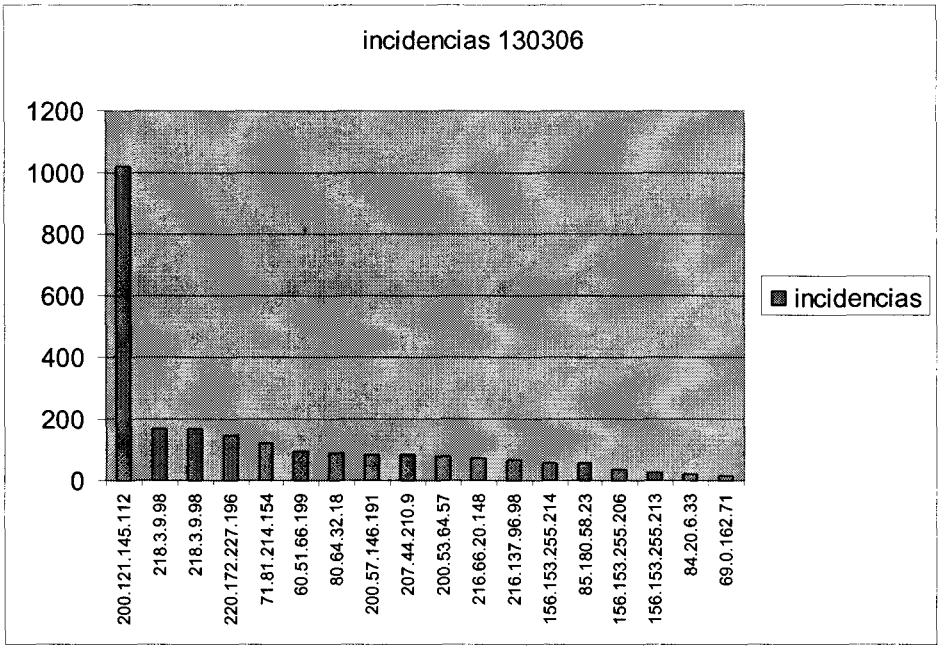
R es el resultado de las alertas

Asumiendo que algunas de las partes son mutuamente excluyentes pero que interaccionan, nos permite usar el teorema de BAYES

6.3 Evaluaciones

Actualmente, además de todas aquellas soluciones comerciales existen aquellas esfuerzo de empresas de talla internacional, que ofrecen los servicios públicos a fin de mitigar el flujo de correos no deseados, como el esfuerzo de empresas como Vodafon, Bell , Sonic.net, etc. a través de un esfuerzo multitudinario, generaron un sistema dinámico en Internet de determinación de dominios con problemas de spam (http://www.spamhaus.org) a fin de que aquellas empresas que desean coordinar sus servicios de SMTP, con esta validación., denominadas RBL (Real time spam Black List) pueden cancelar los correos de Dominios o IP's con fuertes probabilidades de envío de correos comerciales no deseados. Este servicio, que integra redes de varis empresas, se concentran en medir los potenciales de probabilidad ante cualquier correo como un servicio de correo electrónico infomativo comercial no deseado, alrededor del mundo y notifican vía los parámetros RBL los dominios que

vallan coincidiendo con un patrón anómalo de envios de correo, lo cual permite a aquellos servidores de SMTP evitar la recepción o envío de correos a estos dominios.



Gráfica 130306

Muestra de ataque de correo no deseado sufrido en fechas recientes, dadas las métricas de utilización, la información de cantidad de correos superiores al promedio de entrada máximo por emisor = 600, en este caso se disparó una alarma para el administrador del correo indicando la varianza.

La dirección IP de ataque (200.12.145.112), de haber estado configurada la herramienta de RBL con el servicio de SMTP de este dominio, este ataque, bien pudo haber sido minimizado, pero dado que solo se estaba trabajando con los servicios de comportamiento básico, aún no se tenían otros indicadores que permitieran una sinergia para mejorar nuestro Modelo. Motivo por el cual, como ya hemos repasado en el presente estudio, nos llevó a buscar mayor sinergia entre las diversas herramientas, ponderarlas y utilizarlas para establecer una serie de escalaciones antes de poder aceptar como válido un correo de aceptación dentro de un Dominio asegurado.

Las listas de Bloqueo, operan a nivel DNS, es decir por nombre de dominio, y están diseñados para trabajar al momento de la transmisión de SMTP, posibilidad el negar a los correos que sean SPAM o UCE, antes de que ataquen a los servidores o las colas de correo. Debido a que la transmisión de SMTP es terminada antes de que sean trasmitidos los correos, esto habilita la notificación del estatus de entrega al emisor de la negación del servicio y provee de un medio de notificaciones de error seguras.

Si acaso este tipo de filtraje no es empleado a nivel servidor, se puede así mismo utilizar el DNSBL, que incluyen SBL y XBL como parte de los servicios prestados a través del proyecto SPAMHOUS.

Así mismo, existen en Internet muchas asociaciones como la anterior encargadas de recabar datos en línea a fin de limitar los ataques de SPAM, tales como el archivo de tráfico de Internet, el cual es un repositorio moderado para el seguimiento a cualquier desbordamiento masivo de correo a través del tráfico de Internet. Esta información es utilizada para el seguimiento de la dinámica de la red, las características de uso, y los patrones de crecimiento, así como para proveer medios para realizar las pruebas controladas de seguimiento a los patrones citados (http://ita.ee.lbl.gov/).

De entre las pruebas validadas durante el presente ejercicio, con este tipo de filtraje de correo no deseado, se detectaron que usando las configuraciones de los servidores con RBL, existen algunos detalles en cuanto a su funcionalidad, dadas sus características dinámicas, tráfico, debido a las constantes actualizaciones de la lista negra del control de dominios con características de envío de correos no deseados, como para el caso de grandes Instituciones, como universidades, en donde normalmente el flujo de correos tiene patrones de tráfico muy disimilares en el tiempo, como el caso de HITS y resulta muy complejo la modelación y/o establecer los patrones básicos de comportamiento para esos dominios y por ende, provoca una serie de varios falsos-positivos; en este punto, desde el dominio MIGESA.COM.MX, con una infraestructura con MS EXCHANGE 2003

como servicio de correo, se configuraron esquemas de operación con filtraje con RBL aprovechando las características de rastreo y filtraje de correo no deseado del servidor de correo.

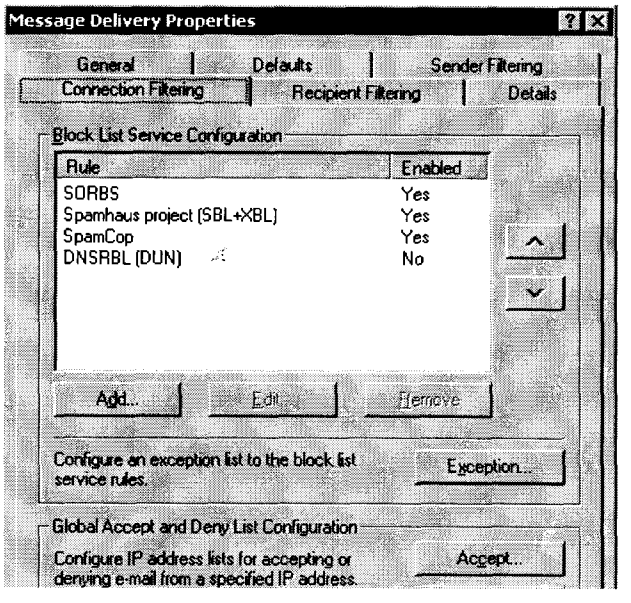
Por otro lado, una mala práctica de los Dominios es la configuración de los servicios de RBL o la falta de conocimiento para llevarlo a cabo, como sucede que en algunos falsos positivos, detectados durante la prueba fueron debidos a que los dominios examinados por SORBS o SPAMHOUS, no contaban con información relacionada con sus información reversa (Reverse Lookup-in arpa) la cual sirve para determinar si el dominio en cuestión proviene de una zona válida con un puntero (PRT) definido en su zona de búsqueda Inversa a fin de permitir la recepción de correos de una fuente confiable y eliminando las posibilidades de pishing. La validación inversa de DNS, para que sea efectiva deberá estar presente en aquellos servidores donde puedan ser consultados a través de Internet.

Durante el desarrollo de estas pruebas, se pudo reducir en un 50 y hasta 60% la recepción de correo comercial no deseado, pero este resultado no fue del todo positivo, pues de entre los problemas hallados, además de los anteriormente mencionados, se encontraron varios problemas para la entrega de correos a dominios como @tec.com desde el dominio @migesa.com.mx pues este tipo de dominios presentaba para los servicios de RBL, un dominio con alto potencial de características de SPAM- Correo no deseado, provocando varios falsos positivos a la hora de envios de correos hacia ese dominio.. Las fuentes utilizadas para el uso de esta prueba fueron los ya mencionados servicios de SPAMHOUS y SORBS (Spam and Open Relay Bloking System); los cuales redujeron en un 75% la cantidad de correo no deseado que el dominio MIGESA.COM.MX recibía, y aún así también una gran cantidad de correos correctos dirigidos hacia o desde este dominio, son desechados, por lo que resulta necesaria, la complementariedad de esta solución con algún otro medio de detección holístico basado en otras corrientes tipo MET.

Aunque efectivos, estos servicios presentan algunas inconsistencias, las cuales son de considerable atención sobre todo para el dominio en cuestión (receptor), pues resulta mas conveniente realizar el

análisis de tráfico, la modelación de las entradas y salidas de correo para tazar las incidencias antes de envitar la entrada de correos, ya que basados en estos sistemas de RBL, estos toman aproximaciones en otras latitudes de la red, que pueden no resultar del todo acertadas para tráfico en observación, pues por ejemplo para el caso de empresas transnacionales, como CEMEX, si acaso hubiera un indicio de correo no deseado en algún punto de su red en Internet, aún cuando emisario estuviara localizado en otro punto, su correo debido a RBL pudiera ser tazado como de alto riesgo de correo no deseado.

En aplicaciones tales como Exchange 2003, estos soportes dinámicos de verificación de las referencias de los dominios de procedencia de los correos, pueden ser configuradas fácilmente, e incluso como ya mencionamos existen en Internet servicios de este tipo gratuitos a fin de ir marginando el envío de los correos comerciales no deseados.



Gráfica Exchange RBL

Como hasta el momento hemos podido determinar, existen varías formas de validar el tráfico de correo no deseado en la red, ya sea apoyados en sitios de soporte por Internet, los cuales realizan la medición y cálculos necesarios y los reflejan a través de las listas dinámicas de bloqueo, existen

también además algunos otros recursos que son a nivel servidor, en los cuales se utilizan formas de seguimientos basados en firmas de ataques previamente descritos o actualmente basados, en comportamientos y/o tendencias de envío entre servidores cercanos (MET), así mismo, existen algunos desarrollos que van mas a niveles mas profundo aprovechando las capacidades físicas de los servidores para muestrear a nivel correo, el uso de palabras con alto contenido de publicidad o enlaces a sitios de este tipo. Los sistemas basados en el monitoreo de la red son generalmente construidos sobre los firewalls empresariales con especial atención a las variaciones en el tráfico y los puertos TCP.

El rastreo de las fuentes de los correos no deseados requiere de que en conjunto todos los sistemas cumplan con determinados estándares y en los encabezados de los correos el seguimiento a la etiqueta de recibido, esto a fin de determinar los equipos por donde los correos atraviesan. De el estudio previo anterior podemos notar que a nivel ISP se debe de asegurar que los entandares su cumplan, y verificar que cada correo que pase por sus sistemas tenga agregada la línea de recibido, por lo que se debe de asegurar que la identidad de la máquina de donde provenga el correo sea debidamente registrada por algún medio. Para ello se debe de poner especial atención a la parte del protocolo donde el comando HELO no pase por alto la solicitud del nombre del dominio, y que este no sea solamente una IP, si no un dominio debidamente registrado. Así, mismo, para dar el correcto seguimiento de los correos a través de los ISP's, estos beberán mantener un sistema de horario estandarizado en todos sus puntos de correo, a fin de rastrear debidamente cualquier posible cambio en el tráfico en condiciones de operación estable.

Muchas de estas características de rastreo, pueden nulificarse debido a las mismas prácticas de las mejores configuraciones de seguridad, donde a fin de evitar los problemas de spoofing, para evitar aquellas técnicas de alteración que permiten tomar las direcciones de fuente o destino por medio de alteraciones aleatorias en las pilas de TCP, y mediante la regla, se bloquean los paquetes de origen a nivel de los ruteadores, a fin de evitar el envío de paquetes ruteados o para el diagnostico con herramientas como en MS Windows TRACERT. Todo con el fin de evitar que el destino pueda

recibir en los datos erróneos de la fuente del paquete TCP o viceversa, debido a que en el camino pueda surgir una alteración de las mencionadas.

Todo lo anterior resulta necesario, así como en el plano legal, cultural y de experiencia para el personal a cargo de los accesos y usos de los correos para limitar tanta derrama de recursos en combatir los correos no deseados. Pero como sucede, existe además las probabilidades del error-humano, por lo que otro nivel de seguimiento a los correos no deseados debe de ser implementado a fin de determinar los estándares de comportamiento sobre las redes en los ISP's.

Motivo por el cual, en nuestro modelaje, se pretende tomar todas las mediciones posibles, tales como el comportamiento básico de arribos diarios, si el dominio asociado con la IP de origen del mensaje existe y si es una entidad certificada en Internet (dominio válido- NIC), los cual revisamos con herramientas como el nslookup (MicroSoft). Hasta aquí tenemos probabilidades que aunque excluyentes, que nos ayudan y nos dan indicios ya de la veracidad de la legitimidad de un correo electrónico y descartar su posibilidad de correo comercial no deseado.

Otrás técnicas actuales que de igual forma dependen de la correcta configuración de las zonas de Dominio y la validación de los mismos a través de los servicios de correo para identificar debidamente la procedencia de un correo, pueden ser:

SPF (Sender Policy Framework), el cual es un mecanismo flexible y efectivo para combatir la falsificación de los nombres de dominio de Internet .

SPF implementa un patrón de seguridad de 3 cuerpos: emisor-receptor-autorizador. El autorizador es consultado para el receptor para verificar que el emisor este autorizado para enviar el correo a su nombre. Esto es idéntico a los 3 cuerpos de seguridad usados por la industria de tarjetas de crédito. En SPF. La dirección de IP del MTA emisor, es el agente de envío. Como la IP del emisor de MTA

es la única requerida para completar la transacción de correo, esta es la que recibe el MTA receptor vía SPF. En este caso, el dueño del nombre del Dominio, sería el autorizador. SPF es un protocolo que le dice al universo en Internet quien puede enviar a nombre del dominio en cuestión.

A continuación se muestra un ejemplo de configuración de una Zona de DNS, con este tipo de validación SF, de esta podremos notar, la configuración en este caso aplica para cada correo que sea tomado por el MTA de este Dominio

```
                2005031383   ; serial number
                10800        ; refresh
                2700         ; retry
                900          ; expire
                86400        ) ; minimum TTL
;
; Zone NS records
;
@               NS                                          dns2.xertix.com.mx.
dns2.xertix.com.mx.   A                                     200.57.88.38
@               NS                                          dns.migesa.com.mx.
;
; Zone records
;
@               MX                                          1
                                                    sendmail01.migesa.com.mx.
@               TXT                                 ( "v=spf1 mx ~all" )
```

CSV (Client SMTP validation). Esta técnica también denominada como certificador de servidor del emisario, requiere de 3 pruebas ligeras y rápidas, a diferencia de algunas otras que requieren mayor demanda de recursos.

El primer paso de este tipo de autentificación utiliza los comandos extendidos de SMTP conocidos como EHLO, lo cual requiere al servidor de correo en cuestión valide la Ip del dominio de procedencia del correo sea correcta. El siguiente nivel de validación consiste en determinar si la computadora desde donde se envía el correo esta autorizada a enviar correos por ese dominio. En la mayoría de las empresas, solo algunos cuantos servidores están capacitados para enviar correo

saliente. Esto se logra mediante la comprobación del registro SRV en el DNS de la zona del Dominio para los servidores con posibilidades de envio, como lo vemos en el siguiente ejemplo

_client._smtp.sendmail01.migesa.com SRV 1 2 0 sendmail01.migesa.com
_client._smtp.www.migesa.com SRV 1 1 0 www.migesa.com

De tal suerte que aquellos con valor 2 tienen la capacidad de envío de correo y los de valor 1, no están capacitados para hacerlo.

El siguiente nivel es la validar la reputación del nombre del Dominio que desea enviar el correo. Esto se logra validando la cantidad de correo con SPAM enviado desde este dominio a través de alguna de las organizaciones como SPAMHOUS.

6.5 Mejores Prácticas Conjuntadas en un servicio de control de correo no deseado.

Todo lo aprendido anteriormente, se pondrá en conjunto por medio del apoyo de una herramienta conocida como PROCMAIL y SPAMASSASSIN, a través de los cuales se modelaran las lecciones aprendidas y se conjuntaran algunas otras para mejorar el nivel de interacción y filtros de correo no deseado para eliminar estas incidencias en los buzones del dominio.

6.5.1 Verificación de Encabezados:

Las Herramientas de correo no deseado usados por las entidades generadoras de estos, tienen ciertas firmas inmersas en sus correos; los identificadores de sus mensajes pueden tener forma determinada, ellos puedan inadvertidamente errar en algunas porciones en los encabezados del Protocolo MIME
Identificación de frases en el cuerpo del mensaje:
Las partes del cuerpo y lo que ud. Pueda hacer con ellas: Bancos africanos y como ud puede obtener el 1/5 por ser familiar de alguien, "esto no es spam", etc.

Por medio de PROCMAIL, se configuraron algunos de estos encabezados, pero a juicio personal, dejamos esta tarea a los protectores de los equipos locales donde residieran los buzones, a los antivirus locales estáticos para realizar esta tarea.

6.5.2 Filtraje Bayesian:

No importa que tan bien el encabezado o el cuerpo sean registrados, siempre caerán mensajes de correo no solicitados, por falta de tomar en cuenta algunas características en la forma como se consideran estos correos no deseados, y las consideraciones de los correos legítimos. Los filtros Bayesian toman generan información de correos conocidos como spam y conocidos como legítimos, e identifican las palabras o frases (token) que solo se muestran en correos no deseados y tokens que solo se muestran en los correos legítimos. Cuando un mensaje nuevo es calificado en el futuro, si contiene varios tokens de correo no deseado, su calificación aumenta en la clasificación de correo no deseado. Si contiene mas tokens de correo legítimo, si calificación de correo no deseado decrece. Esto es mucho mejor acercamiento a que solamente se identifiquen estadísticamente las frases como se maneja en el caso donde "Nigeria" puede ser una palabra legítima en un correo en una agencia de viajes, etc.

Por medio de SPAMASSASSIN y PROCMAIL se realizaron pruebas con varios puntos de acercamiento y detalle a fin de lograr establecer, como para el caso de los histogramas de incidencias, aquellos debidos a las palabras que mayormente se repetían en base análisis de incidencias de las palabras por mensaje, y demás, los cuales fueron previamente descritos en el apartado de MET. A fin de encontrar aquellas incidencias fuera de lo normal y registrarla.

6.5.3 Listas Negras y Blancas de Bloqueo automático

Herramientas como Spamassassin mantienen un lista Blanca o AWL (Automatic white List) de los emisores de correo. Cuando un correo nuevo ingresa, se verifica esta Base de datos AWL y se valida la calificación para la dirección IP de donde procede el mensaje, si el número fue alto, se asume que el

nuevo mensaje tendrá un valor semenjante y se incrementa la calificación de correo no deseado para el nuevo mensaje. De lo contrario, si la calificación fue baja, se decrementa con el nuevo mensaje la posibilidad de que sea correo no deseado

6.5.5 RBL-Listas de Bloqueo de Tiempo Real.

Estas se enfocan en las direcciones de IP de los servidores de correo que pasan el mensaje hasta el destinatario. Cuando herramientas como Spamassassin solicita esta lista un servidor en particular de algún dominio donde entregar correo, su respuesta puede derivar a algo parecido a correos no deseados debido a que este servidor es administrado por personal que envía este tipo de correo, o es un correo que permite el transporte de correos libremente que esta mal-configurado, o es un MODEM conectado a Internet.

6.5.6 Conjunto de caracteres y Locales

Este valida cuando los emisores envían correos en caracteres que pueden ser tales como GB2312 o BIG5, con lo cual se filtra todo aquel correo con caracteres que sean chinos, y se asumen Correos no deseados.

Relaying denied:
From 218-160-113-117.dynamic.hinet.net [218.160.113.117] to 8888@800.d2g.com: 1 Times(s)
From 61-229-112-79.dynamic.hinet.net [61.229.112.79] to 8888@800.d2g.com: 2 Times(s)
From [218.17.230.232] to popogigi1986@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871915@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871916@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871917@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871918@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871919@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871920@yahoo.com.tw: 1 Times(s)
From [219.133.174.222] to zczcczcz19871921@yahoo.com.tw: 1 Times(s)

El pasado es una reporte de la herramienta de PROCMAIL, limitando el conjunto de caracteres a solo eng (english) y las denegaciones son los intentos de relar desde las direcciones que aparecen que en realidad son los ataques que tan pronto se dio de alta un dominio, denominado

ADOBELATAM.COM, este fue atacado por las direcciones expuestas en un lapso no mayor de unas 2 hras desde la alta y registro en el DNS.

En los equipos basados en UNIX, es una buena práctica colocar la validación de los servicios que realizan las conexiones a los DEMONIOS de los servidores de SMTP (servicios de transporte: envío y recepción de correo) a través de la validación de que la procedencia desde donde se conecta el emisor cuenta con los tiempos de respuesta, protocolos y servicios necesarios de los DEMONIOS estándares; esto se puede validar con las herramientas como PROCMAIL (los detalles de configuración de esta herramienta están fuera del presente contexto)

```
:0
* !^FROM_DAEMON
* !^FROM_MAILER
* !^X-Loop: soporte@netsinco.com
| $HOME/bin/filter.script
```

A través de esta herramienta se pueden ir conociendo u obteniendo listas de de probables dominios con alto grado de contenido no deseado en correos, los cuales se aprovechan y en base a estos generar o actualizar las listas negras, las cuales restringen a los dominios con las características mencionadas.

En bases a las experiencias previas y conjuntando todas estas prácticas, y en base a las propuestas del presente modelo, se propone como necesario verificar la certeza de la existencia de la cuenta del usuario emisor por medio de la validación a través del protocolo de SMTP agregando al proceso establecido del Modelo de verificación validación de Dominio, de boletinado en alguna lista negra, si existe la configuración de SPF en el Dominio, la idea es hacer una prueba de entrega a el buzón de donde proceda el correo.

De las pruebas realizadas podemos determinar, que la mayor causa de incidencia de correos no deseados, se pueden eliminar en un 30% aproximadamente si se hacen las revisiones necesarias de los

procedimientos previos a nivel red : DNS, verificación en reversa de los datos de dominio (IP), CSV, SPF, usuario válido, etc.

El resto de las opciones de detección y filtraje se logran directamente en las pruebas de los encabezados, cuerpo de mensaje, del seguimiento al comportamiento a los comportamientos de envió desde el dominio, o desde el cliente final, a la determinación de sus grupos sociales, familiares y laborales,

Por medio del PROCMAIL, además de modelar por medio de la técnica de Bayes el Autoaprendizaje de la taza de recepción, también se probaron las listas obtenidas del los registros de eventos, para los comporamientos básicos, así como las listas negras propias de este dominio. Y fueron empleadas a través de las Herramientas mencionadas con los siguientes resultados.

```
# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.
whitelist_from *@diexsa.com
whitelist_from fmmezaa@hotmail.com
whitelist_from *@mexico.com
whitelist_from omartinezf@centel.com.mx
whitelist_fomr icarranzag@hotmail.com
required_hits 8
rewrite_subject 1
subject_tag [SPAM-CND]
report_header 0
use_terse_report 1
skip_rbl_checks 0
```

con la suma de las listas de acceso, las probabilidades empleadas para la modelación de tráfico y para la opción de auto-aprendizaje modelado por la herramienta de SPAMASSASSIN, se pueden lograr buenos resultados de los servicios para erradicar los correos no deseados, ya que se pudieron lograr hasta en un 95% la recepción de esta clase de mensajes en los buzones de los destinatarios.

Capitulo 7

Como se ha mencionado hasta ahora todas las herramientas y probabilidades de ocurrencia fueron basadas y pensadas principalmente en el teorema de Bayes, dadas que muchas de las probabilidades aunque excluyentes (si contienen SPF, Si existe un usuario válido) existen también dependencias con el resto de los eventos, por lo que

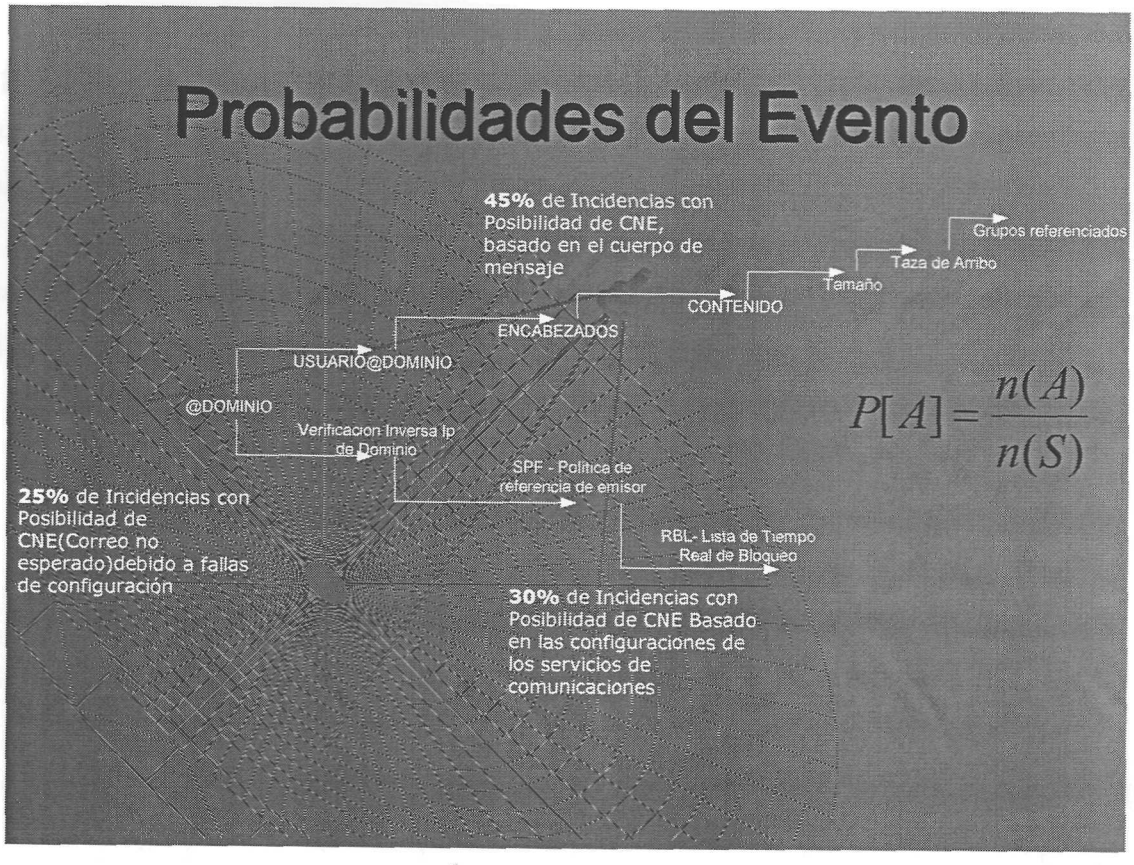
- abc /[abc + (1 - a)(1 - b)(1 - c)]
- En el caso del Filtraje de correo no deseado, lo que se requiere calcular es la probabilidad de que lo sea, y que las piezas de evidencia, a,b,c... son probabilidades asociadas con cada evento.
- Para este caso las evidencias son: Dominio, SPF, RBL, dominio, encabezados de correo

Las incidencias y validaciones de los Eventos, ya en campo nos direron por resultado el siguiente arbol de incidencias, cada punto cabe hacer mencion se subdivide aún en varias opciones obtenidas de las mejores prácticas para cada servicio en particular, como el RFC de SMTP, DNS, SPF, RBL,SVC, etc.

Como resultados hallados que muchos de los problemas por falsos-positivos pueden ser debidos a las fallas de configuración tanto por parte de la configuración de la ZONA donde se encuentra el registro de la referencia MX del IP emisora, como la certificación de sus IP's (a fin de confirmar las redirecciones de correo); estas configuraciones nos llevaron a obtener hasta 20% de correos con probabilidades de correo publicitario no deseado.

Por otro lado, apoyados en las validaciones de los servicios de comunicación, se pueden hallar la certeza de los correos antes de ingresarlos en la cola del MTA, con una probabilidad de aproximadamente 30%.

El restante porcentaje de 50%, puede hallarse en los parámetros propios del cuerpo del mensaje... como en los encabezados, las palabras, el tamaño, etc.



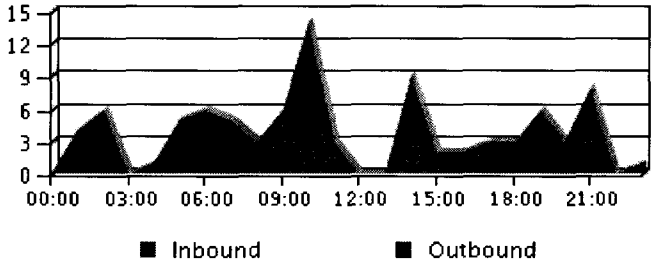
Árbol de Incidencias

7.1 Elementos de Prueba

A través de Herramientas de terceros, como Hosted mail de SYMANTEC se puede obtener histogramas de las tendencias del tráfico, y cotejar contra aquellas de los registros de eventos de los servicios de correo en los dominios locales.

Así por ejemplo por espacio de 2 Meses se mantuvo esta herramienta, conectada al mismo dominio a fin de detallar los comportamientos de correos, y logramos, encontrar mayor información para el detalle del tráfico.

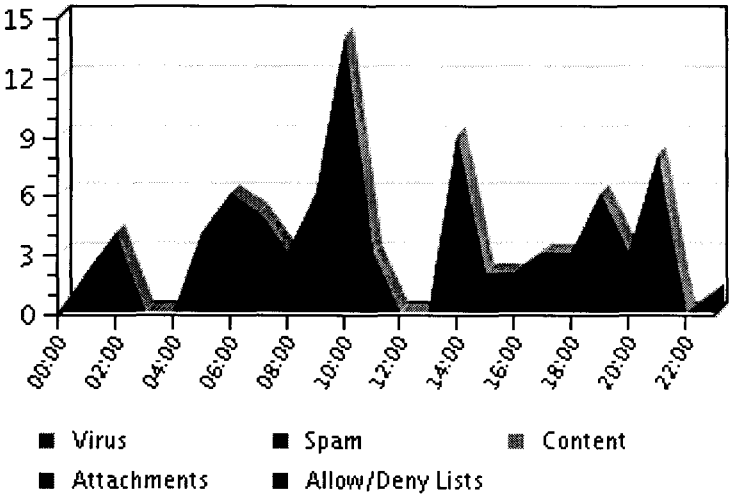
Nosotros, a través de nuestra información tazamos la mayor incidencia de arribos durante las horas 11 a 12:30, y esta herramienta de Symantec muestra un patrón semejante.



Hosted Mail Symantec

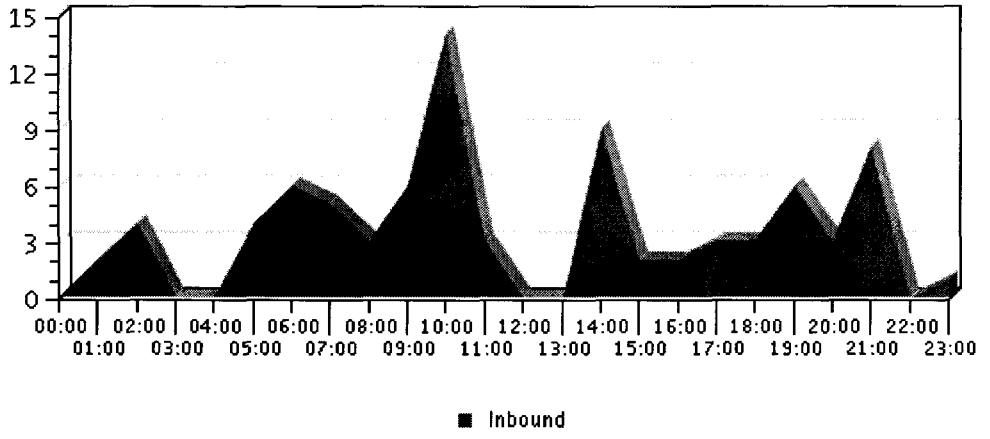
Tráfico promedio de correos de entrada, así como la regencia de aquellos con altas tazas de contenido no deseado, con una frecuencia igual o semejante a las que nosotros habíamos determinado de 16 para las horas de mayor tráfico, nosotros lo habíamos tazado por IP en un lapso de 24 hrs.

En la siguiente gráfica, la herramienta demuestra la cantidad de correo no deseado contra los correos válidados, habla de una diferenciación de hasta 90%, nosotros en nuestro estudio estuvimos hallando 70 a 80% de estos indices de correos no deseados.



HMS Correo no deseado recibido

Esta herramienta, también trae un análisis de tendencias de acuerdo a históricos y presenta gráficas como la siguiente en la cual se corrobora las incidencias de correo no deseado en base a sus incidencias y hallamos nuevamente el índice de 16 incidencias con un alto indice de correo no deseado para las horas indicadas.



En general, las pruebas y obtención de información en base a nuestra experiencia y a las herramientas con que contamos pueden aún dar un servicio de buena calidad y con la capacidad de lograr evitar esta taza de arribos excesiva de correos publicitarios no deseados que como sabemos nos traen un alto grado de improductividad, ni que decir de los costos empresariales y sobre todo, el alentamiento de los servicios de información y comunicaciones.

- Comparativamente es más eficiente usar el comportamiento local que RBL.
- Para servicios de mediana capacidad, dado que se requieren capacidades físicas de calculo y almacenamiento considerables.
- Establecer una cultura pro-activa para la revisión y seguimiento de los registros de eventos.
- No esta basado en el análisis de contenido de los correos al 100%
- Estándares de Responsabilidad: Identidad del emisor, Aseveración del tipo de mensaje, Emisor confiable,Tipo de mensaje: Relación/permiso

BIBLIOGRAFIA

Allen H., Julia; ISBN 0-201-73723-X, 2001; CERT guide to System and Network Security practices; disponible: Texto : ADDISON-WESLEY, SEI Series in software engineering.

Alvarez Marañoz Alvarado y Fábrera Martínez, Pedro pablo, 1999; Comunicaciones seguras[en línea]; disponible: http://www.iec.csic.es/criptonomicon/linux/comseguras.html [febrero 2004]

Andrew P. Moore,Robert J. Ellison, Richard C. Linger; Attack Modeling for Information Security and Survivability ; disponible: http://www.cert.org/archive/pdf/01tn001.pdf [marzo 2004]

ARPANET and the Invention of Mail, disponible http://www.let.leidenuniv.nl/history/ivh/chap3.htm [marzo 2004]

Asociación Mexicana de Internet, disponible: http://www.amipci.org.mx/ [marzo 2004]

Banking Wire, 19/03/2004, L2C103629002804, ELECTRONIC SECURITY: E-MAIL GETS A NEW ENVELOPE [en linea]; disponible: http://0-search.epnet.com.millenium.itesm.mx:80/direct.asp?an=L2C103629002804&db=bwh [marzo,2004]

COFETEL, 2003; Imagenes para el futuro[en línea] , http://www.cofetel.gob.mx/ [marzo 2004]

CISCO, 2004; disponible: http://www.cisco.com/application/x-shockwave-flash/en/us/guest/netsol/ns413/c668/cdccont_0900aecd800d9d38.swf [marzo 2004]

DiSabatino Jennifer, ComputerWorld, 11/12/2001, Vol. 35 Issue 46, p25, 1/3p; The Wild, Wild West disponible: http://0-search.epnet.com.millenium.itesm.mx:80/direct.asp?an=5565800&db=bsh [marzo, 2004]

Eweek, 11/26/2001, Vol. 18 Issue 46, p64, 1/2p, COMDEX TRENDS: WIRELESS, SECURITY, E-MAIL[en línea], disponible: http://0-search.epnet.com.millenium.itesm.mx:80/direct.asp?an=5587169&db=bsh [marzo 2004]

Greene, Barry; 17 Diciembre 2003; Public ISP/NSP/Big Network security Bootcamp Materials [en línea] ; disponible: https://puck.nether.net/pipermail/cisco-nsp/2003-December/007315.html [Febrero 2004]

Harris, Shon; CISSP Certification "All-in-one is All you Need"; disponible: Texto, McGraw Hill, EXAM GUIDE SECOND EDITION

IEEE, 2002; IEEE Communications Society (1952-2002) [en línea]; diponible: http://www.ieee.org/organizations/history_center/comsoc/chapter2.html [febrero 2004]

Peñalva, Ana María; Los presupuestos de TI en la mayoría de las empresas no incluye un rubro de seguridad, informa IDC[en linea] ; disponible: http://www.idclatin.com/mexico/reports15.htm [marzo 2004]

Phillip C. Wright, Géraldine Roy, Volume 11 Number 2 1999 pp. 53-59; Industrial espionage and competitive intelligence: one you do; one you do not [en linea]; disponible: http://0-hermia.emeraldinsight.com.millenium.itesm.mx/vl=4416077/cl=93/nw=1/fm=html/rpsv/cw/mcb/13665626/v11n2/s2/p53 [marzo 2004]

Radcliff, Deborah, Infoworld, 01996649, Marzo 1998; is your ISP secure? [en linea], disponible: http://biblioteca.itesm.mx/cgi-bin/nav/salta?cual=bases:51&recargar=903 [febrero2004]

Selway, William, Bloomerang News, marzo 2003; E-Mail software flaw makes most traffic vulnerable [en línea]; disponible: http://www.detnews.com/2003/technology/0303/04/technology-99333.htm [marzo 2004]

Spanbauer, Scott, PCWORLD, diciembre 2003; Ultimate network security: How to installa a firewall [en línea]; disponible : http://www.pcworld.com/howto/article/0,aid,112920,00.asp [marzo 2004]

Srinagesh, Padmanabhan; Internet Cost Structures and Interconnection Agreements http://www.press.umich.edu/jep/works/SrinCostSt.html [marzo 2004]

Tadjer, rivka, InternetWeek, 10969969, febrero 2001; GET SERIOUS ABOUT SECURITY [en línea]; Dispobible: http://biblioteca.itesm.mx/cgi-bin/nav/salta?cual=bases:51&recargar=903 [marzo 2004]

THE INTERNET & THE WWW:A HISTORY AND INTRODUCTION, disponible: http://www.albany.edu/ltl/using/history.html [marzo 2004]

Vleck, Tom, 29 de octubre 2003; The history of electronic Mail [en línea]; disponible: http://www.multicians.org/thvv/mail-history.html [marzo 2004]

Wagner, Mitch; disponible: http://www.internetweek.com/story/showArticle.jhtml?articleID=6900346 [marzo 2004]

Weil, Nancy; 18 de mayo 2000, CNN; global panel issues Internet security recommendations [en linea]; disponible: http://www.cnn.com/2000/TECH/computing/05/18/global.security.idg/ [marzo 2004]

http://www.alerta-antivirus.es/docs/seguridad_empresas.pdf
http://www.netsa.org.lk/tutorials/slides/sec_issues.pdf

Hoffman, Paul; CISCO; Internet Mail Consortium [En línea]; Disponible: http://www.cisco.com/en/US/about/ac123/ac147/ac174/ac196/about_cisco_ipj_archive_article09186a00800c84ea.html [Octubre 2004]

LeBlanc, Charlene; 20 Junio de 2003;SANS, slippery slope or terra firma? Current and future anti-spam Measures; disponible: http://www.sans.org/rr/whitepapers/email/1153.php [Noviembre de 2004]

TABLAS

GRAFICAS

IMAGEN