El Día a Día del Administrador de Sistemas (y de su profesor): Listas negras antispam Hágalo usted mismo

INCINERADOR DE BASURA

En la Universidad de Niederrhein, los futuros administradores de sistemas implementan mecanismos de defensa contra el spam llamando la atención de la Mafia de la Viagra. Los resultados son listas negras y conocimiento experto de métodos para combatir la amenaza. **POR JÜRGEN QUADE Y CHARLY KÜHNAST**

En la Universidad de Niederrhein [1], Krefeld, Alemania, un proyecto prepara a los estudiantes para su futuro laboral, el trabajo en equipo y la locura diaria, de la que forma parte el emergente spam. Contra éste puede lucharse utilizando varios métodos, siendo las listas negras de spam (SBL) uno de ellos. Actualmente, los estudiantes de la universidad están trabajando en la implementación y el mantenimiento de una SBL.

Siguiendo la idea de "Luchar contra el Spam con Spam", configuramos deliberadamente cuentas de correo IMAP y POP3 que no estaban protegidas contra el spam, las cuales actuaban como señuelo para atrapar correo spam. Para atraer a los spammers, los estudiantes desplegaron direcciones de correo señuelos tan ampliamente como pudieron, y para hacerlo ignoraron todas las reglas concernientes a la responsabilidad de uso de las direcciones de correo y las publicaron en páginas web de redes sociales; también las publicaron en grupos de noticias de pruebas como *de.test* y visitaron los rincones más oscuros de la web que pudieron encontrar.

No tardaron mucho tiempo en obtener resultados satisfactorios: Las cuentas se llenaron con montones de spam. La misión de los estudiantes era configurar un sistema para determinar el origen de los mensajes entrantes tan rápido como fuera posible (identificando la dirección IP del servidor emisor) y añadir el spam a la lista negra por un período de tiempo definido.

Listado 1: Configuración de Policyd-weight

```
01 ## DNSBL settings
02 @dnsbl_score = (
03 #HOST,                    BAD SCORE, GOOD SCORE, LOG NAME
04 'list.dsbl.org'           3.5,       0,          'DSBL_ORG',
05 'ix.dnsbl.manitu.net'     3.5,       0,          'IX_MANITU',
06 'sbl.hsnr.de',            3.5,       0,          'HSNR_DE',
07 );
```

El objetivo que se pretendía conseguir era permitir al servidor de correo comparar las direcciones IP de los servidores de entrega de correo con la lista negra cuando se comprueban las cuentas. Si el servidor de correo nota que un servidor de entrega de correo ha estado involucrado en una lista de distribución

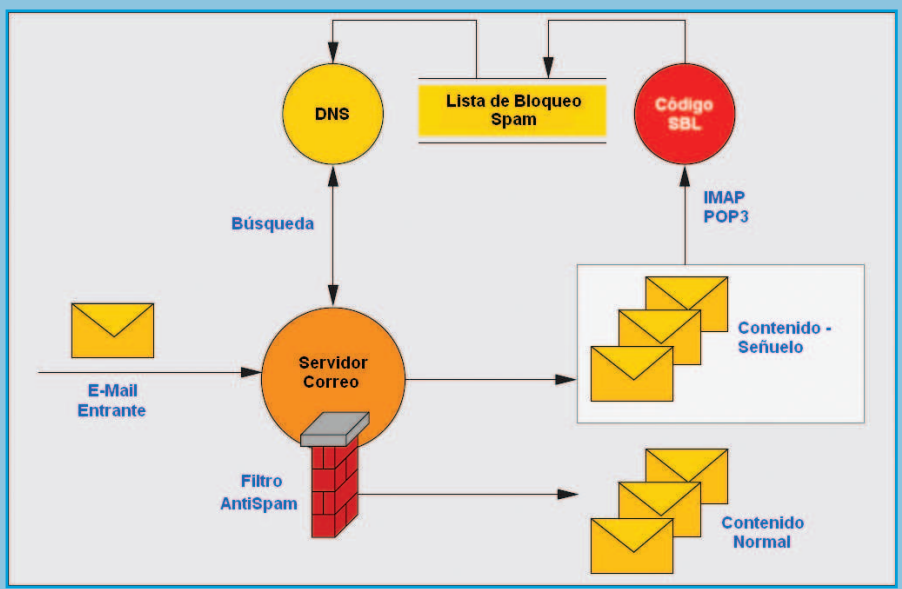

Figura 1: Tras la batalla contra el servidor web, Siege muestra los resultados.

SYSADMIN

Esta solución de red basada en servidor nos permite iniciar sesión con un smartcard.

recientemente, se le rechaza el correo (ver Figura 1).

El primer paso era preguntar por las cuentas IMAP automáticamente a intervalos regulares. A continuación, las rutinas extraen los detalles del servidor de correo que envía el spam desde las cabeceras del correo. Las cadenas de texto relevantes están localizadas en las líneas *Received*:

```
Received: from bhixhv
(wsip-70-183-106-183➥
.sd.sd.cox.net➥
[70.183.106.183]) by➥
islay.kuehnast.com (Postfix)➥
with ESMTP id B3B1F5D7A3;
Tue,➥
21 Oct 2008 20:17:43ß
+0200 (CEST)
```

La dirección publicada, *islay.kuehnast.com*, decide la dirección del servidor de correo que hace de señuelo. Es bastante obvio que cualquier equipo que le entregue correo será un distribuidor de spam – en muchos casos resulta ser una máquina comprometida que está siendo usada como un emisor constante de spam en una botnet [2]. El nombre que la máquina usa para identificarse a sí misma, *bhixhv* en este caso, es absurdo – esto sucede con casi todos los mensajes de spam.

No es necesaria una búsqueda inversa de la dirección IP, *wsip-70-...*; la IP es correcta. La dirección IP aparece listada en el registro de entrada de Postfix entre corchetes, y de este modo puede extraerse fácilmente con una expresión regular. La misma línea contiene la marca de tiempo del servidor de correo, la cual es importante para detectar de forma automática otras entradas o para eliminar de forma automática una dirección IP de la lista en el caso de que no entregue más spam dentro de un período de tiempo determinado y de este modo habilitarla de nuevo.

Configuración de Zonas DNS

Desde el punto de vista técnico, la SBL es una zona DNS combinada con una consulta DNS para descubrir si un servidor está listado o no en la SBL.

Ahora, la configuración añade la dirección IP que ha descubierto a la zona SBL en el DNS:

```
183.106.183.70.sbl.hsnr.de ➥
IN A 127.0.0.10
IN TXT ➥
"Spam from this IP received:
➥
2008-10-21 20.17h"
```

Como las consultas a la zona SBL implican una búsqueda inversa, hay que introducir los octetos individuales en orden inverso. El DNS resolverá el nombre para la dirección IP *127.0.0.10*; el último octeto *.10* ha sido escogido de forma arbitraria, lo único que hay que tener en cuenta es que ha de ser mayor que *1*. Aquí podrían usarse diferentes números para clasificar los resultados – por ejemplo, para evaluar qué señuelo ha proporcionado la entrada.

La cadena en el registro TXT se almacena en el fichero de registro del correo cuando el servidor de correo rehusa aceptar un correo entrante debido a una consulta SBL. En el más sencillo de todos los casos, se le indicaría al servidor de correo que finalizase el enlace de comunicación con el servidor emisor en el supuesto de que se produzca un acierto SBL. La configuración para Postfix sería algo parecido a lo siguiente:

```
smtpd_recipient_restrictions
= ➥
[Andere_Regeln],➥
reject_rbl_client
sbl.hsnr.de,➥
permit
```

No importa cuánta fe hayamos puesto en la efectividad de las SBL hechas por nosotros mismos, todavía no es una buena idea deshacerse del correo simplemente teniendo en cuenta una entrada de la lista.

Herramientas como Policyd-weight [3] para Postfix ofrecen una solución más exhaustiva aplicando diversos criterios de detección de spam. Por ejemplo, Policyd-weight puede consultar múltiples SBLs y realizar otras comprobaciones (cabecera). El servicio Policy genera un marcador con los resultados y los compara con un umbral configurable para decidir si tiene que aceptar o no el correo.

El Listado 1 muestra una configuración de Policyd-weight con tres SBLs. Si el valor del umbral se establece a, digamos, *8.0*, tiene que aparecer un servidor en las tres listas para que Policy-weight lo clasifique como spammer.

Igualdad de Fuerzas

A propósito, le dimos a los estudiantes la libertad de elegir sus propias armas para implementar la SBL. La variedad de soluciones que propusieron sólo viene a demostrar el viejo dicho "pregúntele a 10 informáticos y obtendrá 11 soluciones". Por ejemplo, las rutinas para extraer los datos relevantes del correo señuelo incluían soluciones tan disparatadas como scripts Batch, PHP, DotNet y C.

Bind 9 ganó la competición de servidores de nombre por su fácil configuración y por su soporte multiplataforma.

Pero de nuevo, algunos participantes quisieron tener el control total del código y programaron un mini servidor de nombres que ofrecía la funcionalidad requerida, pero nada más.

El proyecto del incinerador de basura está aún en marcha. Me pregunto qué soñarán los estudiantes cuando lleguemos al último paso, "¿Monitorización e Informes?" No puedo esperar a verlo. ■

RECURSOS

[1] Universidad de Niederrhein, Departamento de Tecnología Eléctrica y Ciencias de la Computación: *http://www.hs-niederrhein.de/fb03.html* (en alemán)

[2] "Bot Attack: Una insidiosa red de spammers ataca a Charly", por Charly Kühnast, Linux Magazine, edición en castellano, Nº 22: *http://www.linux-magazine.es/issue/22/058-059_BotAttackLM22.crop.pdf*

[3] Policyd-weight: *http://www.policyd-weight.org*

EL AUTOR

Charly Kühnast es Gerente de Sistemas Unix en el centro de datos de Moers, Alemania, cerca del conocido Rhin. Entre sus labores se incluye la seguridad del cortafuegos, la disponibilidad y el cuidado de la DMZ (zona desmilitarizada).