Configuración de MailScanner y ClamAV con Sendmail.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *jbarrios arroba linuxparatodos punto net*
Sitio de Red: *http://www.linuxparatodos.net/*
Jabber ID: *darkshram@jabber.org*

Introducción

MailScanner, un robusto servicio para filtrado de correo, combinado con ClamAV un funcional anti-virus para GNU/Linux y otros sabores de Unix, resultan una de las soluciones más robustas para la protección contra virus, gusanos y troyanos desde el servidor de correo electrónico.

Procedimientos.

Instalación del software requerido.

- mailscanner
- clamav
- perl-Archive-Zip
- perl-Convert-BinHex
- perl-MailTools
- perl-MIME-tools
- perl-IO-stringy
- perl-TimeDate
- perl-Net-CIDR
- perl-Compress-Zlib
- tnef

Si dispone del disco de extras de curso proporcionado por Linux Para Todos, solo bastará agregar el subdirectorio MailScanner incluido en cualquier depósito yum del sistema, como se describe en el capítulo **"Creando depósitos yum"**. Una vez añadidos los nuevos paquetes al depósito, solo bastará ejecutar:

```
yum -y install mailscanner clamav
```

Lo anterior instalará mailscanner y clamav junto con todas las dependencias que seas necesarias.

También podrá instalar MailScanner descargando la más reciente versión desde http://www.mailscanner.info/ en donde encontrará un paquete *.tar.gz en cuyo interior hay paquetes SRPM que podrá compilar e instalar en el orden indicado siguiendo las instrucciones del README. De igual modo podrá proceder con clamav desde http://clamav.soruceforge.net/

Configuración de MailScanner.

Utilice el editor de texto de su predilección y disponga a editar **/etc/MailScanner/MailScanner.conf** a fin configurar los siguiente parámetros:

Lenguaje de los mensajes de sistema.

Puede configurar MailScanner para que devuelva los mensajes de sistema en español. Localice lo siguiente:

```
%report-dir% = /etc/MailScanner/reports/en
```

Cambie por:

```
%report-dir% = /etc/MailScanner/reports/es
```

Identificación de la organización.

Solo es de carácter informativo y sirve para identificar si un mensaje infectado pertenece a un servidor u otro. Localice lo siguiente:

```
%org-name% = yoursite
```

Cambie por:

```
%org-name% = suempresa
```

Definir anti-virus a utilizar.

Localice lo siguiente:

```
Virus Scanners = none
```

Cambie por:

```
Virus Scanners = clamav
```

Puede utilizar más de un anti-virus si así lo considera conveniente. Solo necesitará instalar las versiónes apropiadas para el sistema operativo que utilice y añadirlos como lista separada por espacios. Ejemplo:

```
Virus Scanners = clamav mcafee sophos trend
```

¿Poner en cuarentena los mensajes infectados o no?

Si decide no poner en cuarentena los elementos adjuntos infectados en los mensajes de correo electrónico y prefiere **eliminar estos adjuntos inmediatamente** después de ser procesados, localice lo siguiente:

```
Quarantine Infections = yes
```

Cambie por:

```
Quarantine Infections = no
```

Codificación de los mensajes de sistema.

De modo predefinido los mensajes de sistema de MailScanner serán enviados con codificación de caracteres US-ASCII, lo cual es poco conveniente para quienes no utilizan solo el inglés. Localice lo siguiente:

```
Attachment Encoding Charset = us-ascii
```

Cambie por:

```
Attachment Encoding Charset = ISO-8859-1
```

Permitir mensajes con etiqueta Iframe

Las etiquetas iframe se utilizan para cargar una página empotrada dentro de un marco. lamentablemente esto representa un riesgo muy alto e innecesario debido a que un mensaje de correo electrónico podría no contener material dañino, pero tal vez el la página que cargue el marco que si lo contenga. Actualmente se considera el enviar correo electrónico utilizando etiquetas Iframe como poco ético por todos los riesgos que conlleva.

Si a pesar de esto quiere permitir utilizar etiquetas iframe en los mensajes de correo electrónico y está consciente de los riesgos y las consecuencias, localice lo siguiente:

```
Allow IFrame Tags = no
```

Cambie por:

```
Allow IFrame Tags = yes
```

Control de Spam.

MailScanner permite también realizar filtrado de correo contra listas negras como SpamCop y Spamhaus.

Edite el fichero **/etc/MailScanner/spam.lists.conf** y defina o confirme las listas negras a utilizar

```
ORDB-RBL                          relays.ordb.org.
#
# spamhaus.org                    sbl.spamhaus.org.
# spamhaus-XBL                    xbl.spamhaus.org.
# combinación de las dos anteriores:
SBL+XBL                           sbl-xbl.spamhaus.org.
#
spamcop.net                       bl.spamcop.net.
NJABL                             dnsbl.njabl.org.
SORBS                             dnsbl.sorbs.net.
```

Localice en el fichero **/etc/MailScanner/MailScanner.conf** lo siguiente:

```
Spam List = ORDB-RBL SBL+XBL # MAPS-RBL+ costs money (except .ac.uk)
```

Cambie por:

```
Spam List = ORDB-RBL SBL+XBL spamcop.net NJABL SORBS
```

Configuración de servicios.

Necesitará inicializar los servicios clamd y freshclam. El segundo, particularmente, se encarga de contactar los servidores que hospedan las bases de datos actualizadas con las más recientes firmas de los más recientes virus, gusanos, troyanos y otros tipos de software maligno.

```
chkconfig clamd on
chkconfig freshclam on
service clamd start
service freshclam start
```

De ser necesario puede actualizar manualmente y de manera inmediata la base de datos de firmas ejecutando simplemente freshclam desde cualquier terminal como root.

Se debe desactivar y detener el servicio de sendmail, el cual será controlado en adelante por el servicio MailScanner:

```
chkconfig sendmail off
chkconfig MailScanner on
service sendmail stop
service MailScanner start
```

Comprobaciones.

Utilice cualquier cliente de correo electrónico y envíe éste como adjunto hacia una cuenta de correo loca el archivo test2.zip incluido en el directorio de MailScanner del disco de extras de curso de Linux Para Todos. El procedimiento deberá entregar el mensaje al destinatario con el título alterado indicando que el mensaje contenía un virus y en el interior un texto que indica que el adjunto fue removido y eliminado.

Si quiere hacer un aprueba rápida, utilice mutt para enviar un mensaje de prueba ejecutando lo siguiente, suponiendo que hay un usuario denominado como «fulano» en el sistema:

```
echo "Prueba Anti-virus" | mutt -a test2.zip -s "Prueba Anti-virus" fulano
```

Lo anterior deberá devolver al destinatario el siguiente mensaje de correo electrónico:

```
Asunto:         {Virus?} Prueba Anti-virus
De:             "Fulano" <fulano@localhost.localdomain >
Fecha:          Mie, 18 de Agosto de 2004, 10:31 pm
```

```
Para:           "Fulano" <fulano@localhost.localdomain >

Atención: Este mensaje contenía uno o más anexos que han sido eliminados
Atención: (test2.zip, clamtest).
Atención: Por favor, lea el(los) anexo(s) "suempresa-Attachment-Warning.txt" para más
información.

Prueba Anti-virus
```

El administrador del servidor de correo recibirá en cambio lo siguiente:

```
Asunto:         Virus Detected
De:             "MailScanner" <postmaster@localhost.localdomain>
Fecha:          Mie, 18 de Agosto de 2004, 10:31 pm
Para:           postmaster@localhost.localdomain

The following e-mails were found to have:Virus Detected
    Sender: root@localhost.localdomain
IP Address: 127.0.0.1
 Recipient: fulano@localhost.localdomain
   Subject: Prueba Anti-virus
 MessageID: i7J3VTXF004487
   Informe: ClamAV: clamtest contains ClamAV-Test-Signature
   Informe: ClamAV: test2.zip contains ClamAV-Test-Signature
            ClamAV: clamtest contains ClamAV-Test-Signature
--
MailScanner
Email Virus Scanner
www.mailscanner.info
```

Si todos los procedimientos de comprobación por algún motivo no funcionan, por favor verifique la sintaxis en todas las líneas modificadas en el fichero **/etc/MailScanner/MailScanner.conf**, como seguramente podrá leer se indica en la bitácora localizada en el fichero **/var/log/maillog**.y que también puede mostrar información de utilidad.

tail -f /var/log/maillog