Antivirus para armar…

o más bien, hágalo usted mismo

M.Sc. Alberto García Fumero

FLISOL 2014 Ciudad de La Habana

ClamAV (Clam antivirus)

El proyecto ClamAV Antivirus fue fundado en el año 2001 por Tomasz Kojm. Nació como un proyecto *opensource* que pretende identificar y bloquear virus en el sistema.

Pero...¿y por qué? ¿qué sentido tiene?

¿Acaso hay virus en Linux o UNIX?

(Porque todo el mundo me dice que a Linux no le entran los virus, y yo he visto que las máquinas Windows se infectan y esas no...)

- Una de las vulnerabilidades de GNU/Linux (en realidad, vulnerabilidad de sus usuarios) es que multitud de usuarios piensan que Linux no es vulnerable a los virus. Los virus y ataques malintencionados presentan una **amenaza real** a los sistemas Linux. Si un binario infectado contiene uno de esos virus, al ser ejecutado el binario, el sistema se infectaría.
- **el nivel de infección dependerá de los privilegios del usuario que ejecutó el programa**. Por eso se recomienda tanto no trabajar con nivel de root a no ser que resulte imprescindible.
- Normalmente uno no trabaja (no debería trabajar) con la cuenta root. Para eso existen **sudo** y las tantísimas cuentas que crean las aplicaciones que necesitan permisos especiales.
- Si el virus entra por la cuenta de superusuario podría llegar a infectar el sistema entero. En caso de un usuario normal, el sistema operativo estaría seguro aunque los datos del usuario no. El virus podría borrar e incluso enviar esos datos a otro equipo remoto.
- Por otro lado, las vulnerabilidades de escalada de privilegios pueden permitir que malware ejecutándose bajo una cuenta de acceso limitado también se propague por todo el sistema.

Además existen virus multiplataforma...

Un virus no tiene por qué ser para Window$$ o UNIX/Linux exclusivamente.

El primer virus multiplataforma (Windows, Linux, Mac, fue creado por el grupo de fabricantes de virus 29A (29A en hexadecimal es 666 en decimal) hace ya muchos años.

De todas formas, repito: **solo tendría acceso a lo que el usuario infectado tuviera acceso**.

Pero bueno, ¿y si pongo un antivirus y me borra adjuntos por error? Los antivirus se equivocan, hay falsos positivos... mis usuarios me van a matar!

Ciertamente siempre hay errores...

- **Microsoft Anti-Virus para Windows (MWAV): en su momento identificó a Windows 95 como un virus**
- **Kaspersky antivirus detectaba al antivirus de Segurmática como un virus**
- **Segurmática detectaba una versión de WinRAR (craqueada!) como virus, y lo borraba.**

Pero el riesgo es cada vez menor, ya que se puede controlar qué se manda borrar y qué no se borra, y el análisis del código sospechoso es cada vez más cuidadoso.

¿Y puedo acaso ser un portador asintomático?

- Que los virus no prosperen en Linux no significa que me sienta en libertad de olvidarme de que existen... ¿qué tal si por descuido comparto un documento infectado que copié en una máquina Windows?
- ¿Conocen la historia de María Tifoidea? **María Tifoidea** o **María la Tifosa** (*Typhoid Mary*, en inglés), fue la primera persona en los Estados Unidos a la que se identificó como un portador sano de los patógenos asociados con la fiebre tifoidea. Se presume que infectó a 53 personas, tres de los cuales murieron, en el transcurso de su carrera como cocinera. Fue puesta en cuarentena en dos ocasiones por las autoridades de salud pública, y murió después de casi tres décadas en cuarentena total.

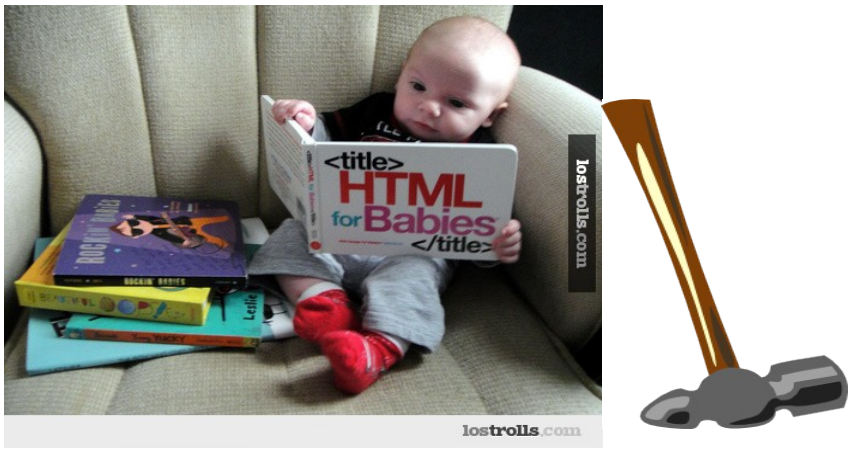
Está bien, está bien, buscaré un antivirus... ¿cuáles tengo?

Existen varios antivirus con versiones que funcionan sobre Linux (Avast!, AVG, Avira, BitDefender, F-Prot, Nod32, Kaspersky, SavUNIX), pero prácticamente todas, menos uno (ClamAV), son propietarios, aunque algunos resultan gratis para uso personal. Si se van a usar en una empresa hay que pagar.

O sea, en la realidad tengo prácticamente un solo candidato.

Dele a un niño de tres años un martillo...

… y todo lo que vea le parecerá un clavo!



- Disponiendo en la práctica de un solo antivirus, lo utilizamos para todo.
- Se ha ido desarrollando una “cultura ClamAV” que incluye paquetes de compatibilización con ClamAv para las cosas más disímiles: **clamassassin, proftpd-mod-clamav, clamfs**, **nautilus-clamscan, clamsmtp, pyclamd, squidclamav...**
- **ClamAV** lo mismo analizará un flujo (streaming), que descontaminará ficheros, que chequeará directorios. Es notablemente flexible. Aquí se pone de manifiesto una de las cosas buenas del **modelo del bazar**: siempre se deja la puerta abierta.

¿Y cómo es ClamAV comparado con Kaspersky, Nod32, etc?

Muy raras veces, si alguna, aparece ClamAV en una tabla comparativa.

Ciertamente aún ClamAV carece de algunas de las comodidades y posibilidades de que disponen los mejores antivirus para Windows. Por ejemplo, viene “de caja” como aplicación de línea de comandos, sin interfaz gráfica (ah, pero puedo instalarme después una interfaz; le conozco al menos tres distintas!) y por el momento solo funciona a demanda (esto puede flexibilizarse). No está preparado para escanear automáticamente, en tiempo real, un dispositivo (por ejemplo, una flash) recién insertado, y aún no chequea memoria.

¿Y por qué ClamAV no trae esas cosas ya incorporadas? ¿No sería mejor para el usuario final?

Es una buena pregunta. Ciertamente sería mucho mejor para el usuario final.

Pero recordemos que nuestro modelo es el del bazar, no el de la catedral. Los programadores trabajan en lo que pueden o quieren, sin obligación.

Hasta ahora nadie ha considerado el problema tan crítico como para desarrollar una solución libre completa. Sucede que...

Todo buen trabajo de software comienza a partir de las necesidades personales del programador (todo buen trabajo empieza cuando uno tiene que rascarse su propia comezón). (La Catedral y el bazar)

¿Tal vez usted sea el elegido?

Esta carencias pueden suplirse en muchos casos haciéndolo trabajar en combinación con otros paquetes.

Toda herramienta es útil empleándose de la forma prevista, pero una *gran* herramienta es la que se presta a ser utilizada de la manera menos esperada (La Catedral y el bazar)

Los programadores y gurúes de Linux suelen concentrarse en áreas muy específicas de trabajo, dejando sin embargo la posibilidad de compatibilizar su resultado con otras soluciones de otras áreas. Por ejemplo, es usual que los programas funcionen en modo de texto, dejando abierta la posibilidad de variar la interfaz gráfica en dependencia del entorno de trabajo que tenga la distribución o los gustos del usuario.

Para gustos están los colores, y para escoger... **Linux!**

Ya lo instalé, pero no le veo interfaz gráfica... ¿no la tiene?

Pues... no. Está hecho en modo de comando.

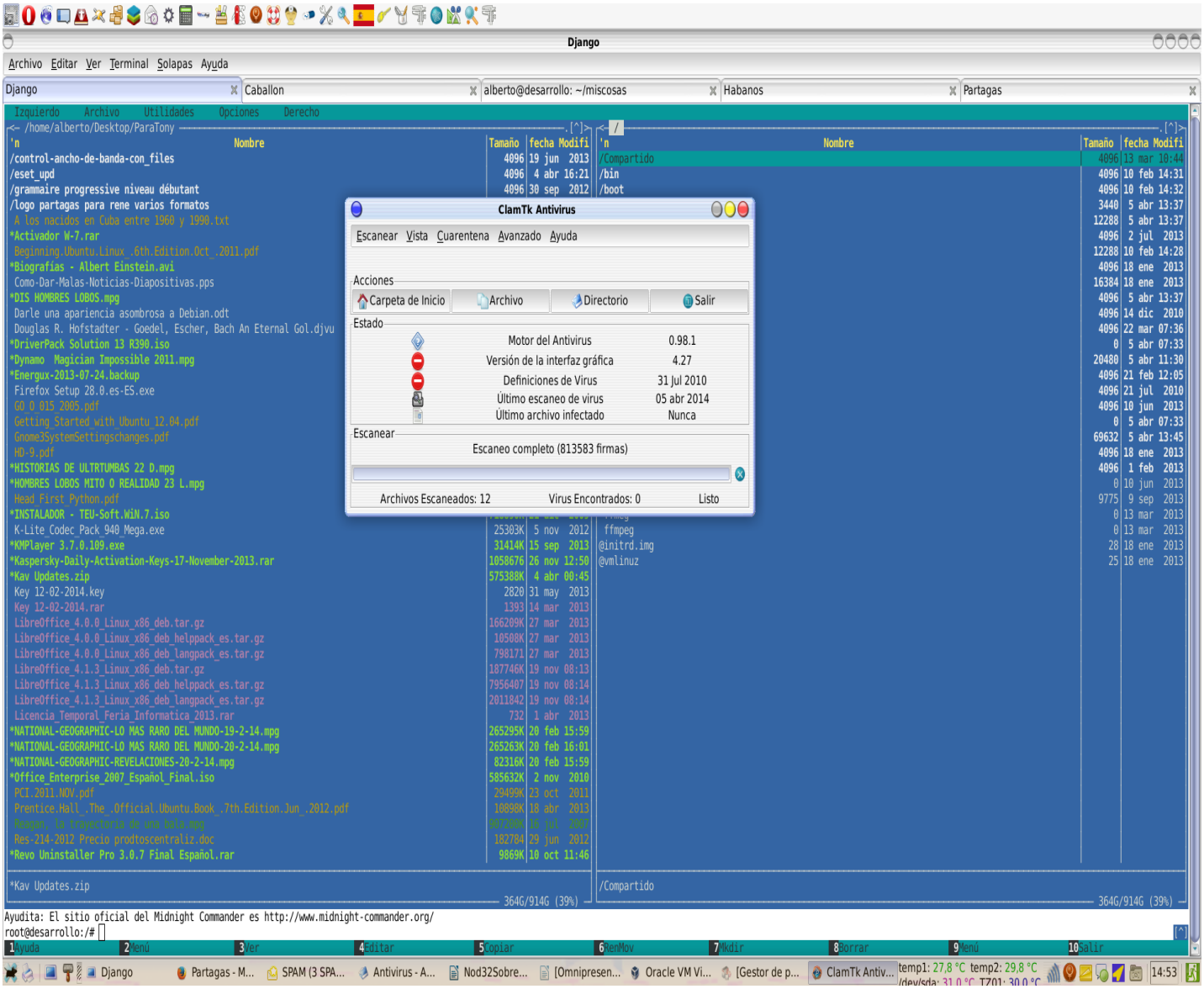
La buena noticia (aparte del gran número de parámetros que se puede usar y su flexibilidad) es que a alguien le molestó el asunto lo suficiente para ponerse a crearla.

Nuevamente acudimos al bazar, esta vez a buscar una interfaz gráfica. Le conozco al menos 3:

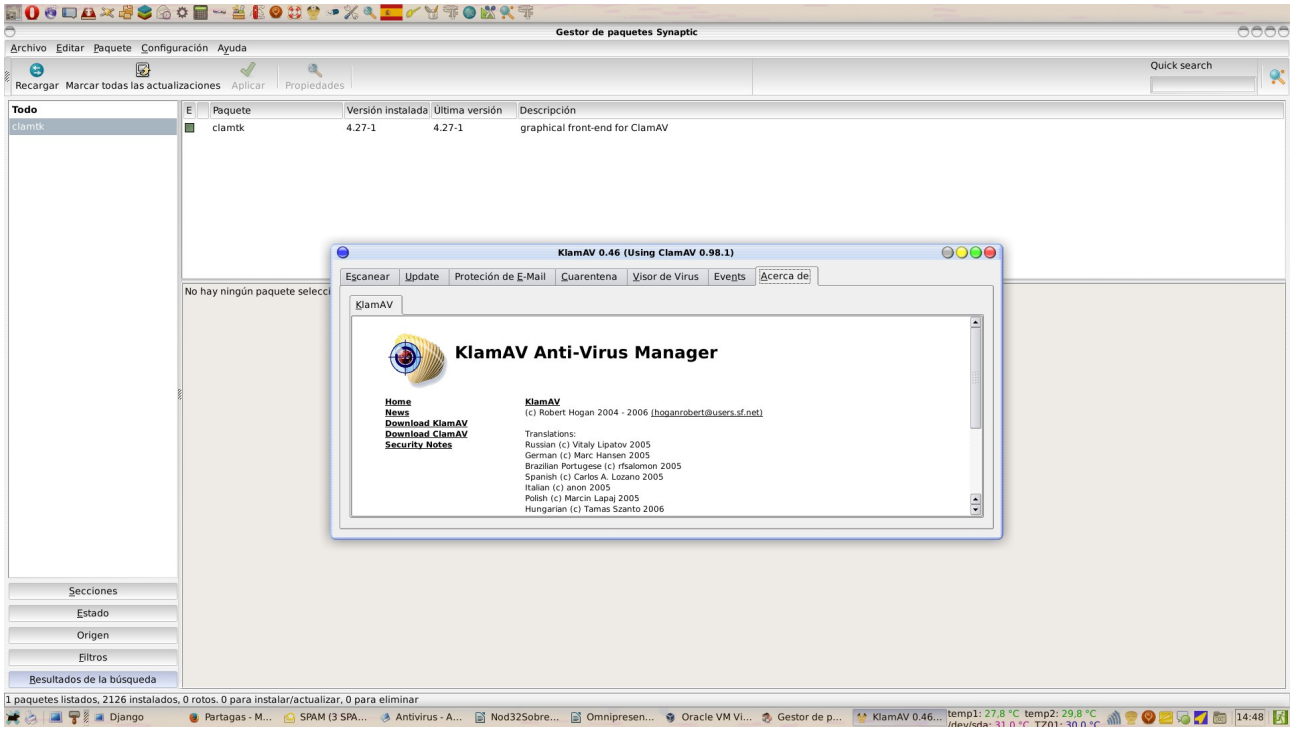
Interfaces gráficas de ClamAV

Antiviral

ClamTK


Django
Archivo Editar Ver Terminal Solapas Ayuda
Django
Caballon
alberto@desarrollo: ~/miscosas
Habanos
Partagas
ClamTk Antivirus
Escanear Vista Cuarentena Avanzado Ayuda
Acciones
Carpeta de Inicio
Archivo
Directorio
Salir
Estado
Motor del Antivirus 0.98.1
Versión de la interfaz gráfica 4.27
Definiciones de Virus 31 Jul 2010
Último escaneo de virus 05 abr 2014
Último archivo infectado Nunca
Escanear
Escaneo completo (813583 firmas)
Archivos Escaneados: 12
Virus Encontrados: 0
Listo
Ayudita: El sitio oficial del Midnight Commander es http://www.midnight-commander.org/
root@desarrollo:/#

KlamAV


Gestor de paquetes Synaptic
Archivo Editar Paquete Configuración Ayuda
Recargar
Marcar todas las actualizaciones
Aplicar
Propiedades
Quick search
Todo
clamtk
E
Paquete
Versión instalada
Última versión
Descripción
clamtk
4.27-1
4.27-1
graphical front-end for ClamAV
KlamAV 0.46 (Using ClamAV 0.98.1)
Escanear
Update
Proteción de E-Mail
Cuarentena
Visor de Virus
Events
Acerca de
KlamAV
KlamAV Anti-Virus Manager
Home
News
Download KlamAV
Download ClamAV
Security Notes
KlamAV
(c) Robert Hogan 2004 - 2006 (hoganrobert@users.sf.net)
Translations:
Russian (c) Vitaly Lipatov 2005
German (c) Marc Hansen 2005
Brazilian Portugese (c) rfsalomon 2005
Spanish (c) Carlos A. Lozano 2005
Italian (c) anon 2005
Polish (c) Marcin Lapaj 2005
Hungarian (c) Tamas Szanto 2006
Secciones
Estado
Origen
Filtros
Resultados de la búsqueda
1 paquetes listados, 2126 instalados, 0 rotos. 0 para instalar/actualizar, 0 para eliminar
Django
Partagas - M...
SPAM (3 SPA...
Antivirus - A...
Nod32Sobre...
Omnipresen...
Oracle VM Vi...
Gestor de p...
KlamAV 0.46...
temp1: 27,8 °C
temp2: 29,8 °C
14:48

En esto de las interfaces gráficas, cada cual tiene sus criterios...

Nada prohíbe que usted intente hacer una también, que le de las facilidades que busca y no encontró en otras. Claro, si es que nos... pica lo suficiente. Y si tenemos algún conocimiento del tema, por supuesto.

No olvide que...

Usted es un usuario de software libre. NO SE MENOSPRECIE!

Puede modificar y reciclar programas y scripts, y adaptarlos a sus necesidades. En el software libre modificar y reciclar no es una opción, es la norma.

Use el lenguaje de programación que conozca, y láncese a la aventura.

O use algún paquete que le permita crear ventanas y “rellene los espacios en blanco” de cada módulo de acciones (según el lenguaje que sea), mandando a ejecutar el binario del ClamAV (el clamscan) con los parámetros deseados.

Por ejemplo:

Una propuesta sencilla (que yo también soy un niño de 3 años en algunas cosas, desde que descubrí ese paquete) es usar **WXPython** para generar la interfaz gráfica y mandar a ejecutar el clamscan mediante algo como:

retcode = call("clamscan" + " -r --remove=yes "+directorio+' &', shell=True)

Una vez que tenga cómo lanzar el binario, puedo pensar en formas de capturar la salida del comando, y obrar en consecuencia: ejecutar un sonido o poner una ventana o avisarme por correo o por el chat si encontró virus, por ejemplo...

Está bien, ya instalé uno de ellos, pero cansa esto de estar lanzándolo a mano cada vez que quiero revisar algo. ¿Cómo puedo acoplarlo con el resto de mi sistema?

Ciertamente ClamAV es un antivirus "**a demanda**". Pero podemos acoplarlo a algunas cosas...

- Tenemos a **Nautilus-clamscan** como una extensión de Nautilus que añade un item "**Scan for viruses**" al menú que aparece al hacer clic derecho sobre un fichero en Nautilus. El proceso se muestra en una ventana de progreso.
- Pudiera explorar el paquete nautilus-actions.
- Podemos armar una solución similar para Dolphin, usando la experiencia del colega Alex Vergara Gil .

Ya empezaron los problemas! Cuando mando a actualizar el ClamAV me pide Internet! Soy 100% cubano! ¿Qué me hago entonces?

Aunque en la práctica se puede actualizar ClamAV descargando en una máquina las firmas daily.cvd y main.cvd y luego copiándolas a los clientes mediante scp (a mano o mediante un script), sería deseable en ocasiones usar **freshclam**, sobre todo cuando las estaciones de trabajo son Windows y usamos el porte de ClamAV para Windows, Clamwin..

Para ello hubimos de realizar las siguientes modificaciones:

- Crear una entrada en el servidor DNS para clamav.ettpartagas.co.cu
- Comentar la línea Example en /usr/local/etc/freshclam.conf (usamos el ClamAV en código fuente, no el paquete .deb)
- Declarar DatabaseMirror clamav.ettpartagas.co.cu
- Declarar DatabaseCustomURL http://clamav.ettpartagas.co.cu/clamav/main.cvd
- Declarar DatabaseCustomURL http://clamav.ettpartagas.co.cu/clamav/daily.cvd
- Poner en no el ScriptedUpdates
- Normalmente el directorio /usr/share/clamav pertenece a root.staff, con permisos 42755. Le pusimos 4257 para que el freshclam creara un directorio temporal allí (lo necesita).
- Crear el fichero /var/log/freshclam.log (pararse en el directorio /var/log y teclear touch freshclam.log) para que ponga los logs allí.
- Crear en el servidor web el directorio /var/www/clamav, donde depositamos las firmas daily.cvd y main.cvd.

Con esto, al ejecutar **freshclam** en las máquinas clientes se actualizan las firmas (algunos mensajes de advertencias por cuestiones de detalle, pero en la automatización no se ven ;-))

Por ninguna parte el ClamAV me dice que va a revisar mi correo. Yo quiero que ClamAV me revise mi correo como lo hacen los demás!

Bueno, no todos lo hacen. Pero los buenos, sí.

Para revisar la mensajería entrante a un equipo mediante el ClamAV, son posibles dos enfoques:

- Mediante un script, salvar el flujo de correo entrante a un fichero temporal para revisarlo y luego reencauzarlo (esta es la solución para un usuario terminal)
- Acoplar ClamAV al MTA (por ejemplo, al Postfix o al Exim). Esta es la solución para tener chequeado un nodo completo.

Analicemos la solución para el caso del usuario terminal, esto es, una persona con una máquina aislada que se conecta directamente a su proveedor de servicios de Internet.
Si el cliente de correo es KMail, KlamAv puede automáticamente acoplar ClamAV y KMail, protegiendo el equipo. Para el caso de un cliente de correo como Evolution (no lo he probado con Thunderbird, pero supongo que en principio debe funcionar esta misma solución que presento a continuación, y que me encontré hace años, una tarde que pude salir a aguas internacionales) una vía es preparar un "filtro" que haga un "piping" del flujo (stream) de correo entrante (aprovechando que ClamAV es capaz de analizar un flujo mediante clamscan -) hacia un fichero temporal, revisar ese fichero y luego reencauzar el correo, como se dijo anteriormente.

La solución incluye instalar previamente el paquete **zenity**, para mostrar el resultado en una ventana gráfica.

- **aptitude install zenity**

  como primera cosa.

  Veamos el filtro:

  ```
  #! /bin/sh

  FILE=/tmp/$$_outclam.tmp

  clamscan - 1> $FILE

  if [ $? -eq 1 ]; then

  STRING=$(grep "FOUND" $FILE |cut -d: -f2)

  zenity --warning --title="evolution> Virus detected" --text="$STRING" &

  exit 1

  fi

  exit 0
  ```

- Observemos el **“-”** pasado como parámetro a clamscan: se le está indicando analizar un flujo.
- Ubico este script en, digamos, /usr/local/bin. Luego abro **Evolution** y busco el menú Editar/Filtro de Correo. Alli declaro un nuevo filtro (por ejemplo, con el nombre FiltroClamAV) y le indico en "**Buscar elementos que cumplen con estos criterios**" la opción "Si se cumplen todas las condiciones". En "Encauzar al programa" selecciono el camino hacia el script (/usr/local/bin/nombre-del-script) y le indico que el programa devuelve un 1 (clamscan devuelve un 1 cuando encuentra un virus). Finalmente en la opción "Luego" selecciono que mueva ese correo a una carpeta dedicada a los mensajes sospechosos o que sin más lo elimine. Acepto, cierro la ventana y ya está listo. Puedo hacer una prueba sencilla con una firma de virus para pruebas como EICAR para quedarme tranquilo.

¿Y no puedo poner algo de eso también en el servidor de correo?

La solución para proteger todo un nodo mediante **ClamAV** es un poco más complicada, pero por supuesto más completa. Por su complejidad no la veremos acá. Conozco al menos tres variantes: acoplarlo con **amavis-new** y de paso con **spmassassin** (muy bueno), usar **MailScanner** (puedo poner no solamente **ClamAV**, sino otros varios antivirus en línea, pero su modelo de funcionamiento consume muchos recursos) o usar **clamsmtp** (me dicen que es la solución más liviana).

Ya que estoy expandiendo sus usos... ¿Puedo acoplarlo a mi navegación? Sería muy bueno...

Puede acoplarse el Squid con el ClamAV, y de esa manera tener la posibilidad de revisar el tráfico **HTTP.** Esto añade una capa de protección adicional a nuestra red. Ahora bien, solo se podrán chequear las conexiones HTTP **que no sean cifradas**. El tráfico a través de una conexión con (https://) no podrá ser chequeado, precisamente por estar cifrado. En tales casos las soluciones deberán ser otras.

¿Cómo logro que el Squid le pase el flujo HTTP al ClamAV? Para ello se utiliza el **Protocolo de Adaptación de Contenidos de Internet**

El Protocolo de Adaptación de Contenidos de Internet (o ICAP, del inglés Internet Content Adaptation Protocol) es un protocolo de red abierto y público, originado en 1999 para la redirección de contenidos con fines de filtrado y conversión. fue estandarizado en Abril de 2003 como **RFC 3507**. Permite el uso de antivirus, filtrado de contenidos, traducción dinámica de páginas, inserción automática de anuncios, compresión de HTML, etc. Los servicios basados en ICAP tienen dos posibilidades de implantación, dependiendo de si la redirección al servidor de filtrado se realiza inmediatamente después de la solicitud del cliente (modo “request”) o tras la respuesta del servidor de destino (modo “response”). Normalmente se asocia el filtrado de acceso al modo solicitud y el filtrado de contenido al modo respuesta.

El protocolo ICAP se combina con un módulo llamado **squidclamav**, el cual realiza el trabajo de invocar al ClamAV.

La solución que hemos considerado requiere de la instalación de Squid3, c-icap, ClamAV (por supuesto...) y el módulo squidclamav, descargable desde Internet. Puesto que el paquete c-icap no viene en Debian 6, y la versión de preferencia del Squid que trae este Debian es la 2.7, lo mejor es upgradear a Debian 7, que sí trae c-icap y un Squid3 más reciente. Nos aseguramos también de instalar el ClamAV más reciente que podamos (lo tenemos funcionando con 0.98.1).

Configuración del ClamAV

Primero que todo, instalamos ClamAV, de preferencia el más reciente. Necesitaremos que clamd esté activo, así que si instalamos el ClamAV que trae el Debian instalamos también el paquete clamav-daemon. En cualquier caso, asegurarse de que el clamd esté activo.
Hay otros paquetes que será necesario instalar si no los tenemos ya instalados:
aptitude install gcc make curl libcurl4-gnutls-dev c-icap libicapapi-dev

Descomprimimos el squidclamav, nos movemos con cd hacia su directorio y mandamos configurar:

./configure --with-c-icap

Finalizada la configuración, compilamos con make y finalmente instalamos el paquete con make install

Este squidclamav trae una página a la cual se redirigirá al usuario en caso de que lo que se esté accediendo mediante HTTP contenga un virus. Tomamos ese fichero clwarn.cgi y lo copiamos en /usr/lib/cgi-bin (o donde corresponda ir a los ficheros que se ejecuten vía cgi).

Ahora vamos a /etc/squidclamav.conf y allí declaramos la redirección, de esta forma:

redirect http://192.168.0.104/cgi-bin/clwarn.cgi

Nos aseguramos de que esté bien declarado el camino al socket clamd:

clamd_local /var/run/clamav/clamd.ctl

en el caso de que clamd esté trabajando por un socket local, o si es un socket Inet, especificamos el puerto y la IP de escucha.

Configuración del c-icap

Ahora debemos configurar el icap. Vamos a /etc/default/c-icap y allí nos aseguramos de que se lance al iniciarse el sistema, poniendo:

START=yes

Seguidamente nos movemos a /etc/c-icap/c-icap.conf y cambiamos algunas cosas. Donde dice ServerAdmin, poner la dirección correcta:

ServerAdmin alberto@ettpartagas.co.cu

Ahora cambiamos el ServerName y ponemos el correcto:

ServerName partagas.ettpartagas.co.cu

Buscamos el tag Service y declaramos el objeto compartido:

Service squidclamav squidclamav.so

Hecho esto, lanzamos el servicio icap:

service c-icap start

Configuración del Squid3

Instalamos Squid3 y seguidamente pasamos a configurar el fichero /etc/squid3/squid.conf. Buscamos el tag icap_enable, y lo ponemos en on:

icap_enable on

Buscamos el tag icap_send_client_ip y lo ponemos en on:

Buscamos el tag icap_send_client_username y lo ponemos también a on:

icap_send_client_username on

Buscamos el tag icap_client_username_header y le ponemos X-authenticated-User:

icap_client_username_header X-Authenticated-User

Ahora nos aseguramos de que el Squid3 le pase por el protocolo icap al squidclamav lo que acaba de recibir:

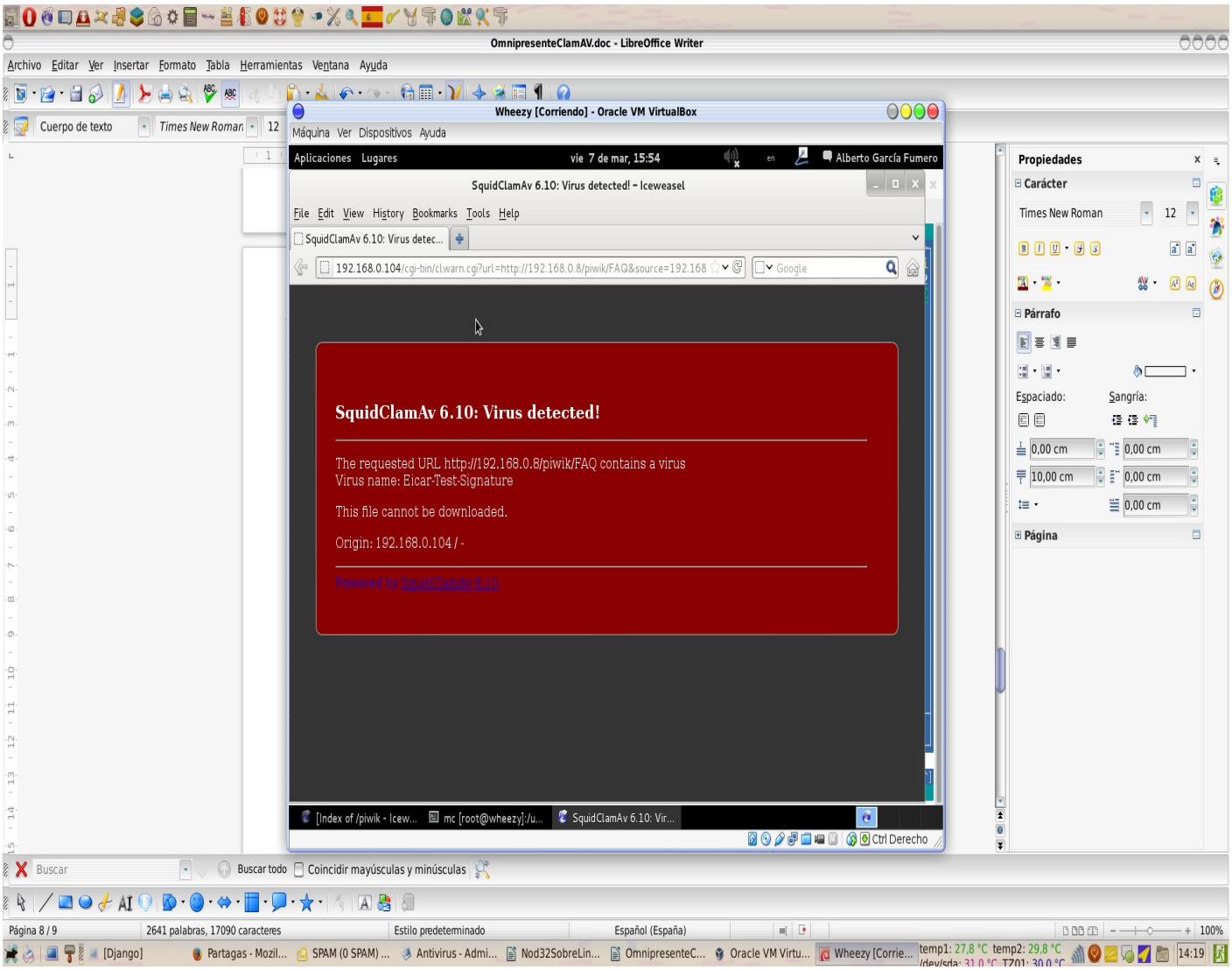
icap_service service_req reqmod_precache bypass=1
icap://127.0.0.1:1344/squidclamav

adaptation_access service_req allow all

icap_service service_resp respmod_precache bypass=1
icap://127.0.0.1:1344/squidclamav

adaptation_access service_resp allow all

Reiniciamos el Squid3 (o mandamos a leer de nuevo al configuración) y si todo está bien puedo hacer una prueba con una firma de virus para pruebas (por ejemplo, EICAR, que la guardo para esas cosas). Copio el fichero EICAR en el /var/www de un servidor web, por ejemplo, y accedo al servidor mediante http://servidor-web. Allí debo ver el fichero del EICAR (o lo que esté usando para pruebas). Si le hago doble clic, squidclamav me presentará la pantalla de advertencia.


OmnipresenteClamAV.doc - LibreOffice Writer
Archivo Editar Ver Insertar Formato Tabla Herramientas Ventana Ayuda
Wheezy [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
Aplicaciones Lugares vie 7 de mar, 15:54 Alberto García Fumero
SquidClamAv 6.10: Virus detected! - Iceweasel
File Edit View History Bookmarks Tools Help
192.168.0.104/cgi-bin/clwarn.cgi?url=http://192.168.0.8/piwik/FAQ&source=192.168
SquidClamAv 6.10: Virus detected!
The requested URL http://192.168.0.8/piwik/FAQ contains a virus
Virus name: Eicar-Test-Signature
This file cannot be downloaded.
Origin: 192.168.0.104 / -
Powered by SquidClamAv 6.10
Propiedades
Carácter
Times New Roman
12
Párrafo
Página
Página 8 / 9
2641 palabras, 17090 caracteres
Estilo predeterminado
Español (España)
100%

Un Centro Antivirus Montado Sobre ClamAV!

Es interesante analizar la posibilidad de escanear equipos remotos desde una estación Linux. Así podría limpiar periódicamente una red.

"De caja" **ClamAV** no puede hacer esto, pues su ámbito está limitado a la estación donde está instalado. Un enfoque prometedor para aproximarse a una solución es compartir directorios (o el disco completo) de la máquina remota, "montar" esos directorios en algún punto de montaje de la máquina local y mandar a ClamAV a escanear ese directorio. Este enfoque resulta práctico para chequear desde la nuestra tanto las estaciones Linux como las Windows.

El paquete **smbnetfs**, incluido en el repositorio de Debian 6, da la posibilidad de tener un punto de montaje con smbfs, compatible por tanto con una red Samba/Windows.

Una vez instalado el paquete mediante aptitude o apt-get, y escogido el usuario que va a interactuar con las máquinas remotas, se crea en su /home/usuario un directorio **.smb** que deberá tener dentro una copia del smb.conf de la máquina local (la nuestra) y una copia del fichero /etc/smbnetfs.conf. Supongamos que tal usuario sea root, y que hayamos creado el directorio e incluido en el sus dos ficheros. Entonces escogeríamos un punto de montaje y ejecutaríamos en consola el comando:

smbnetfs punto-de-montaje

(**smbnetfs -o punto-de-montaje** si hay algún contenido anterior en ese directorio; o sea, si no está vacío)

Dentro de ese directorio tendremos entonces (como subdirectorios) el listado de los grupos de trabajo, y dentro de los tales subdirectorios, el listado de los equipos. No falta entonces más que lanzar desde nuestra amada consola el comando

clamscan -r máquina-que-quiero-escanear

lo cual me dará libre acceso de escaneo a todo lo que esté compartido desde allá. Por supuesto, si se quisiera escanear completamente el equipo, habrá que compartirlo todo.

Mira qué interesante...

De modo que nada impide crear scripts y tener un "Centro Antivirus" en nuestra máquina Linux, el cual revisaría con **ClamAV** tanto el correo entrante, como revisaría directorios locales, como lo haría con equipos remotos!

Podría estudiar más a fondo icap, y tratar de usarlo para chequear también el tráfico FTP...

Faltaría acoplarle la solución para chequear de modo automático un dispositivo que se conecte (por ejemplo, una flash o disco portátil). Esto es más complicado, pero se puede recurrir a clamfs, a monitorear **syslog** para detectar dispositivos recién montados, y mandar a ejecutar clamscan.

El límite lo pone **usted**!

Aprovecho para sugerir la posible estructuración de algún grupo de trabajo de nuestra comunidad de software libre que se dedique a estudiar estas soluciones y conformar, si no un paquete que unifique estas distintas soluciones aisladas (algo bien difícil) , al menos un documento guía para tantos administradores que quisieran pasarse a soluciones de software libre pero tropiezan con las dificultades lógicas que se derivan del pobre acceso a documentación actualizada.

Gracias por su paciencia!