Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Clam Antivirus, un producto GPL (36680 lectures)

Per **Celso González**, ***PerroVerd*** (http://mitago.net)

Creado el 14/05/2002 12:12 modificado el 14/05/2002 12:12

> *Clam es un antivirus para Linux que emplea la base de datos de OpenAntivirus, otro proyecto libre. Clam está desarrollado en C y entre sus caracteristicas se encuentran que es multihebra, soporta Amavis, escanea en archivos comprimidos, se actualiza automáticamente y mucho más.*

Actualmente Clam funciona en Linux, Solaris, FreeBSD y Windows (con cygwin) Podemos descargar Clam desde la página del autor http://www.konarski.edu.pl/~zolw/clam[1] donde también encontraremos un manual en pdf bastante completito.

Instalación

El proceso de instalación es bastante sencillo. Una vez que bajemos el tar.gz correspondiente realizaremos los siguientes pasos como root:

- Añadir un nuevo usuario y grupo al sistema

```
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam Antivirus" clamav
```

- Descomprimir, compilar e instalar

```
# tar zxpvf clam-x.yz.tar.gz
# cd clam-x.yz
# ./configure; make
# make install
```

- Pruebas
  Escanearemos el directorio de las fuentes guardando un log en el archivo scan.txt, esta ejecución nos tiene que detectar 1 fichero infectado con el virus test eicar (no es un virus de verdad, solo se usa para probar los antivirus)

```
$ clamscan -r -l scan.txt clam-x.yz
```

Actualización

El programa encargado de las actualizaciones es el **freshclam**. Este programa podemos ejecutarlo de 3 formas diferentes y básicamente lo que hace es conectarse a 2 servidores diferentes (por motivos de seguridad) para comprobar si ha cambiado la base de datos de virus, y en caso afirmativo descargarla, comprobar su firma e instalarla.

- Modo interactivo
  Siendo root desde una consola ejecutamos freshclam y nos mostrará un resultado parecido a este.

```
# freshclam
Checking for new database - started at Tue May 14 07:36:19 2002
Connecting to www.mat.uni.torun.pl
Connecting to www.konarski.edu.pl
Database is up to date.
```

- Como demonio
  Para ejecutar freshclam como demonio lo único que tenemos que añadir es el parámetro -d seguido del parámetro -c X, siendo X el número de comprobaciones al día que queramos que haga. Evidentemente para que esto funcione bien debería estar en los scripts de inicio.

Opciones

Las opciones más importantes son las que conciernen a la revisión de ficheros comprimidos. Por motivos de copyrights y patentes el programa no lleva ningún tipo de código que se encargue de esto, sin embargo, si permite añadir parámetros para el uso de programas externos que hagan ese trabajo.
Esto se ve claro con un ejemplo, vamos a escanear el directorio /virus revisando los ficheros zip que encontremos

```
# scanclam -r -l scan.txt --unzip=/bin/unzip /virus
```

La palabra clave aquí es --unzip=ruta_al_fichero_encargado_de_descomprimir. Además de los ficheros .zip podemos añadir parametros para los arj, ace, tar, tgz, bzip, etc...

Conclusiones

Un programa muy fácil de usar, bastante eficiente y que al estar realizado en C y no en Java, como los de OpenAntivirus[2], no carga tanto la máquina. La actualización automática nos quita problemas.
Desventajas: no permite desinfectar ficheros, y aunque disponemos de actualización automática la base de datos no está tan al día como la de los antivirus comerciales. Si encuentras uno de estos casos puedes colaborar con la gente de OpenAntivirus enviandoles el virus.

Lista de enlaces de este artículo:

1. http://www.konarski.edu.pl/~zolw/clam.html
2. http://www.openantivirus.org

E-mail del autor: celso _ARROBA_ mitago.net
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1311