

GUÍA

**SNORT+MYSQL+ACID+PHP
+
APACHE**

EN SLACKWARE 10.1

Por Daniel Medianero Garcia
meleslack@gmail.com
www.meleagro.es.kz
2005 ESPAÑA

INTRODUCCIÓN

Esta guía pretende ayudaros a configurar Snort de manera que los avisos de seguridad se guarden en una base de datos realizada con MySQL puedan consultarse facilmente a través de ACID en formato PHP, alojando dicha página en un servidor local APACHE.

Los contenidos de esta guía han sido probados con éxito por mí y no son la única manera de hacerlo, simplemente os proporciono un material que os oriente, y quizá consiga, en la tarea de realizar las cosas de un modo más facil en el mundo GNU/Linux.

Este documento ha sido escrito con la ayuda de la herramienta OpenOffice (<http://www.openoffice.org>), y la máquina donde se han realizado las pruebas tenia un Sistema Operativo Slackware Linux 10.1 (<http://www.slackware.com>). No me responsabilizo de la mala utilización de los contenidos de este documento, ni de los daños que pudiera provocar en vuestras máquinas (cada uno es responsable de lo que teclea).

Los paquetes que utilicé fueron los siguientes:

snort-2.3.3	(http://www.snort.org)
acid-0.9.6b23	(http://acidlab.sourceforge.net/)
adodb-4.62-for-php	(http://adodb.sourceforge.net/)
jpgraph-1.17	(http://www.aditus.nu/jpgraph/)
mysql-4.1.10	(http://www.mysql.com)
apache-1.3.33	(http://www.apache.org)
php-4.3.11	(http://www.php.net)

Todos son Código abierto y libre.

Supongo que si utilizáis snort, mysql y demás sobre linux es porque estáis en fase de aprender en linux, pero que no sois ya unos recién llegados, por ello se supone que tenéis ciertos conocimientos de manejo de directorios, crear usuarios y grupos, y algo de dominio sobre algún editor de texto, yo he elegido vi.

Paso Número 1: Instalación de Snort

Descomprimos el snort en /usr/src usando "tar zxvf snort-2.3.3.tar.gz"
Entramos al directorio correspondiente "cd /usr/src/snort-2.3.3"
Lo configuramos para que se compile preparado para trabajar con mysql:
"./configure --sysconfdir=/etc --prefix=/usr --with-mysql=/usr && nice -19 make"
Lo compilamos usando "make install"
Creamos el directorio donde se guardarán los logs "mkdir /var/log/snort"
Ya tenemos snort preparado.

Paso Número 2: Configuración MYSQL

Yo instalé el mysql utilizando un paquete precompilado para slackware (un tgz) desde linuxpackages (<http://www.linuxpackages.net>) y lo instalé con installpkg. Hay que tener en cuenta que para utilizar mysql hay que tener el servidor mysql levantado, esto se hace con una simple orden "/usr/bin/mysqld_safe &", hay varias órdenes para realizar lo mismo y mysql puede dar algunos fallos hasta conseguir ponerlo a punto pero tales problemas quedan fuera del propósito de esta guía.

Suponemos por tanto que mysql se encuentra instalado y funcionando. Entramos en el tecleando "mysql". Podemos entrar con el usuario root y es recomendable tener contraseña para él, con lo cual la orden de entrada quedaría así:
"mysql -u root -p".

Creamos una base de datos para snort, tecleando "CREATE DATABASE snort;", recuerdo que se supone que estamos ya en mysql, no en línea de comandos. Le ponemos una contraseña a la base de datos "grant all on snort.* to root@localhost identified by "tu_contraseña";".

El siguiente paso a mi me dió problemas desde dentro de mysql asique salía línea de comandos con "exit;" y le puse "mysql -u root -ptu_contraseña < /usr/src/snort-2.3.3/schemas/create_mysql snort", con esto snort crea una base de datos sirviendose de mysql, que es la que usaremos para gestionar las alertas. Ahora para comprobar que todo salió bien entramos de nuevo en mysql y tecleamos "use snort" para elegir la base de datos que queremos y "show tables;", al realizar este comando deberíamos ver varias tablas en mysql, si no hay ninguna es que algo no os salió bien. La salida que me dió a mí fue la siguiente:

```
+-----+
| Tables_in_snort |
+-----+
| data              |
| detail           |
| encoding         |
| event            |
| icmp_hdr         |
| ip_hdr           |
| opt              |
| reference         |
| reference_system |
| schema           |
| sensor           |
| sig_class        |
| sig_reference    |
| signature        |
| tcp_hdr         |
| udp_hdr         |
+-----+
16 rows in set (0.00 sec)
```

Paso Número 3: Configuración de Snort

Ya que snort va a tener muchos archivos de configuración lo ideal es que creemos un directorio para él en /etc y que metamos la configuración que vamos a usar, que básicamente es el archivo general de configuración y las reglas, con los siguientes comandos:

```
"mkdir /etc/snort"  
"mkdir /etc/snort/rules"  
"cd /usr/src/snort-2.3.3/"  
"cp etc/* /etc/snort"  
"cd rules"  
"cp * /etc/snort/rules"
```

Bien, ya tenemos los ficheros donde queremos ahora necesitamos personalizar nuestro archivo principal de configuración para decirle 2 cosas, primero la ruta en la cual debe buscar las reglas que acabamos de copiar y segundo decirle que nos introduzca las alertas que se vayan produciendo en la base de datos que hemos creado.

Para ello editamos el archivo con "vi /etc/snort/snort.conf", localizamos la línea donde se encuentre var RULE_PATH y la sustituimos por esto : var RULE_PATH /etc/snort/rules

La siguiente modificación la encontramos aproximadamente en la línea 530, donde ponga output database lo cambiamos por:

```
output database: log, mysql, user=root password=tu_contraseña dbname=snort host=localhost
```

Guardamos y salimos, ya tenemos configurado el snort.

Paso Número 4: Instalación y configuración de ACID

Descomprimos el Acid con "tar zxvf acid-0.9.6b23.tar.gz" y lo llevamos a donde nos interesa con "mv ./acid /var/www/htdocs/", hacemos lo mismo con jppgraph y adodb.

```
"tar zxvf jppgraph-1.17.tar.gz"  
"mv ./jppgraph-1.17 /var/www/htdocs/acid/jppgraph"  
"tar zxvf adodb462.tgz"  
"mv ./adodb /var/www/htdocs/acid/adodb"
```

Ahora debemos editar el fichero de configuración de Acid. Tecleamos

```
"vi /var/www/htdocs/acid/acid_conf.php"
```

En la línea donde esté \$Dblib_path, aproximadamente la 13 le metemos esto:

```
$Dblib_path = "/var/www/htdocs/acid/adodb";
```

Y en la configuración de las alertas, aproximadamente la línea 33 dejamos las variables así:

```
$alert_dbname = "snort";  
$alert_host = "localhost";  
$alert_port = "";  
$alert_user = "root";  
$alert_password = "tu_contraseña";  
$ChartLib_path = "/var/www/htdocs/acid/jppgraph/src";
```

Ahora en donde tenemos puesto el Acid editamos un fichero que se dedicará a la autenticación para la consulta de la base de datos de alertas, lo hacemos con "vi /var/www/htdocs/acid/.htaccess" Y a ese archivo, que es creado por nosotros y está en blanco le metemos lo siguiente:

```
AuthName ?Acid Access?  
AuthType Basic  
AuthUserFile /var/www/htdocs/acid/htpasswd.users  
require valid-user
```

Guardamos el fichero y salimos y ya tenemos configurado el Acid.

Paso Número 5: APACHE

Yo instalé Apache usando el paquete precompilado oficial de slackwarees un tgz y se instala con installpkg. Bien, una vez instalado tenemos que editar el archivo de acceso para que pida nombre de usuario y contraseña. Para ello tecleamos "vi /etc/apache/access.conf", y le añadimos las siguientes líneas:

```
<Directory /var/www/htdocs/acid/>  
  
AllowOverride AuthConfig  
order allow,deny  
allow from all  
Options ExecCGI  
</Directory>
```

Ahora editamos el archivo de configuración general de apache con el editor vi, tecleando "vi /etc/apache/httpd.conf", buscamos donde ponga User y Group y las cambiamos por estas:

```
User web
```

```
Group web
```

También debemos descomentar la línea Include /etc/apache/mod_php.conf

Una vez hemos hecho esto debemos asegurarnos de que tengamos en nuestra máquina al usuario web y al grupo web, si no existen los crearemos.

Para que Apache funcione hay dos comandos básicos, para levantar el servidor usaremos "/usr/sbin/apachectl start", y para pararlo "/usr/sbin/apachectl stop". Si vamos a querer que se levante el servidor Apache cuando nuestra máquina arranque podemos incluir la orden de arranque en /etc/rc.d/rc.local. Ya tenemos configurado apache, para comprobarlo teclear en la dirección del navegador "localhost", y debe salir la pantalla de bienvenida de Apache.

Paso Número 6 - Activando Snort

Ahora debemos levantar snort con "snort -devyq -c /etc/snort/snort.conf -l /var/log/snort/ -D" y hacer que snort arranque con nuestra máquina con "echo "snort -devyq -c /etc/snort/snort.conf -l /var/log/snort/ -D" >> /etc/rc.d/rc.local". Con esto ya tenemos snort corriendo en nuestro sistema.

Paso Número 7 - Visualizando Nuestro ACID

Por último ya solo queda visualizar en el navegador nuestra base de datos de las alertas del snort, es muy simple, basta con ponerle esta dirección al navegador "<http://localhost/acid>".

Notas

Podría pasar que os pidiera autentificaos dos veces, no pasa nada simplemente meterle el usuario y contraseña y ya está. Espero que os haya funcionado, quizá debáis cambiar algunos pasos, yo para ponerlo me guí de varios manuales. Si tenéis alguna duda o queréis contactar conmigo podéis hacerlo por correo electrónico a meleslack@gmail.com, en mi página web <http://www.meleagro.es.kz> o en los foros de <http://www.starlinux.net>, allí soy Meleagro.

Madrid, España 2005, Daniel Medianero García es estudiante de Ingeniería Técnica en Informática de Gestión y un curioso de GNU/Linux, en especial de la distribución Slackware y todo lo relacionado con la seguridad informática.