

Configuración de Snort con interface ACID

Iván Belmonte <ttyp0@inet2u.com>

02-04-2002

Configuración de un sistema de detección de intrusiones

INDICE DE CONTENIDOS

- 1) Introducción
- 2) Qué es Snort y qué es ACID
- 3) Pre-requisitos
- 4) Compilar Snort
- 5) Configuración de la MySQL
- 6) Configurar Snort
- 7) Configuración de ACID
- 8) Autenticación para acceder a ACID
- 9) Have Fun!

1. Introducción

Este documento trata de describir los pasos a realizar para la instalación y configuración de un sistema de detección de intrusiones. Durante la escritura del documento daré algunos pasos por sabidos o ya realizados, para cualquier duda recomiendo consultar la documentación oficial de las aplicaciones a configurar.

La obtención del código fuente de las aplicaciones que vamos a configurar se puede llevar a cabo en los websites oficiales, son los siguientes:

Apache -> <http://www.apache.org>

MySQL -> <http://www.mysql.org>

Php -> <http://www.php.net>

Snort -> <http://www.snort.org>

ACID -> <http://acidlab.sourceforge.net>

En esos mismos websites está la documentación oficial. Recomiendo mucho su lectura, utilizando este documento solo como guía de referencia.

También podeis dirigiros a <http://www.linuxdoc.org> y consultar los HOWTO's oficiales sobre cada aplicación.

2. Qué es Snort y qué es ACID?

Snort es lo que se llama un IDS (Intrusion Detection System). Su funcionamiento es similar al de un *sniffer*, poniendo en *modo promiscuo* la tarjeta de red de la máquina en la que corre. De esta manera, esa tarjeta de red *sniffa* todos los paquetes que circulan por un mismo switch, es decir, los capta y lee aun sin ser suyos.

En muchas ocasiones se puede oír hablar de *sniffers* con intenciones de intrusión en sistemas ajenos... la verdad es que puede ser un arma de doble filo, y su objetivo principal es el de proteger, no el de atacar.

Un IDS bien configurado y mantenido nos alertará de los intentos de intrusión y ataques varios que nuestra red pueda sufrir... un IDS mal mantenido nos llenará un disco duro de porquería y nos colapsará el tráfico de la red.

ACID (Analysis Console for Intrusion Databases) es una interface web desarrollada en lenguaje PHP, que nos muestra los registros guardados por Snort. Snort puede guardarlos en una base de datos o en simples ficheros de texto (por ejemplo syslog)... si queremos usar ACID para visualizar sus efectos, deberemos usar MySQL como almacén parqa los logs recogidos por Snort.

Atención: es importante saber que, según configuremos Snort, este recogerá mayor o menos cantidad de logs. Configurar Snort para que recoja todo tipo de alertas es un suicidio (podemos llegar a captar mas de 100 Mb de logs diarios)... por tanto debemos descartar muchas de las opciones que vienen por defecto, tratando de minimizar su uso y dedicarlo a aquellos ataques que realmente sean peligrosos para nuestra red.

3. Pre-requisitos

ACID es una interface web, por lo que partimos de la base de que el sistema operativo

sobre el que esta funcionando tiene instalado un servidor web, en mi caso particular (y para las explicaciones de este documento) es un APACHE (www.apache.org)

Snort debe dejar los logs en una base de datos si queremos poderlos visualizar con ACID, por lo que previamente necesitamos una base de datos, como por ejemplo MySQL. Aunque también podemos hacerlo con PostgreSQL, Oracle y alguna otra más... yo lo he hecho con MySQL, así que este documento supondrá un caso similar al mío.

Si no tenemos MySQL instalada y funcionando, podemos instalarla con un instalador (sistema de paquetes propio del sistema operativo rpm, tgz, deb....) o compilandola a mano. Si queremos compilarla, los pasos a seguir son los siguientes:

```
# tar zxvfp mysql.tar.gz
# cd mysql/
# ./configure --prefix=/usr
# make
# make install
# mysql_install_db
# chown -R mysql:mysql /var/lib/mysql
# chown -R mysql:mysql /var/run/mysql
# chmod -R 777 /var/lib/mysql
# chmod -R 777 /var/run/mysql
```

Ahora ya tenemos instalada la MySQL.... solo tenemos que arrancarla:

```
# safe_mysql &
```

La MySQL tiene que arrancar y quedarse en Background... si vemos el mensaje "mysql ended" quiere decir que algo estamos haciendo mal.... entonces debemos ir a /var/lib/mysql y leer el archivo *nombre_de_la_maquina.err*, donde encontraremos el error que produce la MySQL al arrancar. Normalmente suele ser cosa de permisos, por lo que si habeis seguido los pasos indicados anteriormente no deberíais tener ningún problema.

Una vez arrancada la MySQL, si queremos poder usar ACID como interface web para visualizar los logs de Snort, debemos dar soporte para PHP en nuestro servidor web.

Primero deberemos compilar PHP, despues deberemos cargar los módulos de PHP en la configuración de Apache.

Aunque podeis instalar PHP directamente con el sistema de paquetes, vamos a explicar como compilarlo:

```
# tar zxvfp php.tar.gz
```

```
# cd php/

# ./configure --prefix=/usr --with-apxs=/usr/sbin/apxs --with-mod_charset --enable-force-cgi-redirect
--enable-discard-path --with-config-file-path=/etc/apache --enable-safe-mode --with-openssl
--enable-bcmath --with-bz2 --enable-calendar --enable-ctype --with-gdbm --with-db2 --with-db3
--enable-dbase --enable-ftp --enable-gd-imgstrtf --with-gd=/tmp/gd-1.8.2 --with-jpeg-dir=/tmp/gd-1.8.2
--with-gmp --with-mysql=/usr --with-xml=shared --with-readline=/usr --with-mm=/usr --enable-trans-sid
--enable-shmop --enable-sockets --with-regex=php --enable-sysvsem --enable-sysvshm --enable-yp
--enable-memory-limit --with-tsrml-pthreads --enable-shared --disable-debug --with-zlib=/usr

# make

# make install
```

Con esto tendremos PHP compilado.

Nota: esta instalación está basada en un sistema Slackware 8.0 , si compilas en un sistema con otra arquitectura diferente lee el manual oficial de PHP para su compilación. También es interesante leer el `./configure --help` antes de compilar, para saber a que cosas dar soporte dependiendo de las necesidades de cada uno.

Ahora vamos a dar soporte a Apache para SSL y PHP. Debemos editar el archivo `httpd.conf` , en Slackware se encuentra en `/etc/apache` , y añadirle las siguientes líneas para cargar los módulos de PHP y SSL:

```
Include /etc/apache/mod_php.conf

Include /etc/apache/mod_ssl.conf
```

Tal como menciona Apache en los comentarios de su archivo de configuración, `mod_php` necesita las siguientes dependencias:

osslibs

mysql

gmp

apache

Y `mod_ssl` necesita:

Apache

OpenSSL

Si no las teneis instaladas, debeis hacerlo para que el soporte PHP y SSL funcionen correctamente en vuestro servidor Apache.

4. Compilar Snort

Aconsejo leer los archivos *README* e *INSTALL* que vienen con el paquete, en ellos se explica detalladamente cualquier tipo de detalle para la compilación y utilización del programa. Leed también el archivo *README.database*, pues en él se explica paso a paso lo que debéis hacer para configurar Snort contra cualquier base de datos (pgSQL, Oracle, MySQL, etc...).

Aconsejo leer el `./configure --help`, en mi caso la compilación ha sido simple. Solamente para especificar la ubicación de la aplicación y dar soporte a la MySQL:

```
# tar zxvfp snort.tar.gz
# cd snort
# ./configure --prefix=/usr --with-mysql
# make
# make install
```

En este punto, si leéis la documentación oficial de Snort, vereis que dice que (si queremos soporte para MySQL) tenemos que especificar el path hacia donde se encuentran sus librerías... (`./configure --with-mysql=/path/to/libs`) pero si lo haceis así no creo que os funcione. Probadlo sin especificar ningún path y seguramente compilareis con éxito.

Ahora debéis copiar ciertos archivos de configuración que vienen con el paquete, pero que la instalación no copia donde deben ir:

```
# cp snort.conf /etc/
# mkdir /etc/snort-rules
# cp *.rules /etc/snort-rules
```

El archivo *snort.conf* os podeis imaginar para que sirve... y los archivos *loquesea.rules* son archivos con especificaciones de reglas de Snort, según las cuales ha de logear los paquetes que crucen la red, dando un tipo de aviso en cada caso. Quisiera hacer referencia a la documentación relacionada con las reglas, el *Snort Users Manual*.

5. Configuración de la MySQL

Para que Snort deje sus logs en la base de datos, primero que crear una nueva base de datos con sus tablas correspondientes, así como un usuario que SOLO tenga acceso a esa base de datos.

En el punto de los pre-requisitos hemos dejado la MySQL recién instalada y funcionando, ahora hay que añadirle usuarios. El usuario con más permisos es el 'root', aunque **es importante** entender que **los usuarios del sistema no son los mismos usuarios que los de la MySQL**. De modo que desde la cuenta de cualquier usuario del sistema se puede acceder a cualquier cuenta de mysql.

Si tecleamos para empezar el siguiente comando, entraremos directamente en la MySQL con permisos de root (administrador):

```
# mysql -u root
```

Lo primero que debemos hacer es establecer una contraseña para el acceso del administrador:

```
mysql> GRANT ALL PRIVILEGES ON mysql.* TO root@localhost IDENTIFIED BY 'vuestro_password';
```

No es objetivo de este documento explicar la sintaxis y estructura de MySQL, de modo que me remitiré a puntualizar lo necesario para su utilización con Snort y ACID. De este modo, el siguiente paso es crear una base de datos para Snort:

```
mysql> CREATE DATABASE snort;
```

Una vez creada la base de datos de Snort, debemos crear un usuario con todos los permisos sobre esa base de datos, para no tener que utilizar el usuario 'root', ya que esto nos supondría un riesgo innecesario. Crearemos un usuario "snort" y le daremos permisos sobre su base de datos:

```
mysql> GRANT ALL PRIVILEGES ON snort.* TO snort@localhost IDENTIFIED BY 'password';
```

Creada la base de datos y creado el usuario, ya podemos salir de la MySQL y seguir con la configuración. Las tablas de la base de datos que acabamos de crear, serán las tablas que Snort necesite para dejar sus logs según la información contenida en cada tipo de log (más adelante lo configuraremos). Para crearlas debemos simplemente volcar el contenido de un fichero que ya contiene la estructura:

```
# mysql snort -u root -p < ./contrib/create_mysql
```

6. Configuración de Snort

Debemos editar el archivo de configuración que hemos copiado antes en /etc. Cuando editeis el */etc/snort.conf* vereis que está muy comentado, y antes de cada opción hay una explicación de varias líneas.

```
var HOME_NET 192.168.1.0/24
```

```
var HOME_NET $eth0_ADDRESS
```

```
var HOME_NET [192.168.1.0/24,192.168.10.0/24,172.26.0.0/24]
```

Primero definimos el rango de direcciones de nuestra red interna. Tenemos tres maneras de hacerlo... La primera define un rango de ip's, la segunda define el rango de ip's del cual forma parte la ip que tiene la tarjeta de red en el momento de lanzar Snort, y la tercera especifica varios rangos de ip's (si tenemos subredes, por ejemplo).

De este mismo modo definimos ciertas máquinas importantes de nuestra red:

```
var SMTP 192.168.1.10
```

```
var HTTP_SERVERS [192.168.1.10,192.168.1.20]
```

```
var SQL_SERVERS [192.168.1.10,192.168.1.20]
```

```
var LOCAL_HOSTS [192.168.1.1,192.168.1.100,192.168.1.110,192.168.1.254]
```

Y también definimos la red externa (Internet por ejemplo):

```
var EXTERNAL_NET any
```

A partir de aquí, debemos definir los preprocesadores. Esto es, plug-ins o partes del programa que definen una manera de *esnifar* los paquetes y detectar un mal funcionamiento o un tipo de ataque. Los preprocesadores están sobradamente comentados y explicados antes de cada línea de código, por lo que no pienso explicar lo que hace cada uno, solo debéis leer su descripción y activarlo si lo queréis. Simplemente debéis saber que la manera de declarar cada preprocesador es la siguiente:

```
preprocessor nombre: argumento1,argumento2,argumento3,argumento4
```

Cabe destacar un preprocesador especial, SPADE (Statistical Package Anomaly Detection Engine), que estudia el tráfico en las máquinas que nosotros le especifiquemos, y a partir de ese estudio saca conclusiones de lo que es un paquete *anómalo* y lo que no lo es. Es decir, la probabilidad de que un paquete se dirija a la dirección IP 10.10.10.10, al puerto 8080, es de un 10%.... mientras que la probabilidad de que un paquete se dirija a esa misma IP al puerto 8079 es de un 0,1 %. El grado de anomalía de un paquete se mide según la siguiente fórmula:

$$A(X) = -\text{Log}_2(P(X))$$

Por lo que el grado de anomalía de 10.10.10.10:8080 es de 3.32 (casi no es anómalo), mientras que para 10.10.10.10:8079 es de 9.97 (muy anómalo).

Para entender mejor el funcionamiento del SPADE, recomiendo leer el fichero *README.Spade*. La configuración de SPADE se realiza también en el fichero *snort.conf*, con el resto de los preprocesadores.

Por último, deberemos configurar los *Output Plugins*, que definen a donde tienen que ir a parar los logs que Snort genera. Deciden si van a ficheros de texto (logs) o a una base de datos, y decide también en que formato irán escritos (binario, texto plano, xml...). Como nos interesa poder acceder a los datos desde ACID y éste está escrito en PHP, diremos que guarde la salida en la base de datos MySQL:

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

Aparte de eso, si quereis podeis especificar que tambien guarde los logs en otros formatos y/o localizaciones (syslog, por ejemplo). Leed la documentación escrita en el mismo *snort.conf* para decidir el formato y el lugar de almacenamiento de los logs.

Finalmente, podemos ponernos a escribir reglas de *logging* pero para eso os recomiendo que leais **Snort Users Manual**, pues lo explica MUY detenidamente y muy bien. Snort tiene ya diversos archivos con reglas escritas, que para empezar ya estan bien. Las añadireis al final del *snort.conf*, y teneis que especificarle la ruta... es decir, si las teneis en */etc/snort-rules* (por ejemplo) pues debereis especificar esa ruta antes de cada fichero de reglas. Es **MUY** recomendable mirarse los ficheros de reglas antes de incluirlos, puesto que las reglas por defecto son muy restrictivas, y logean TODO (hasta los *echo-request* y *echo-reply* de los *pings*) por lo que si lo dejais tal cual, es posible que en una semana os hayais quedado sin un solo Mb libre en vuestro disco duro. Debeis leer los ficheros de reglas, y comentar aquellas reglas que creais mas restrictivas, o las que menos os preocupen... es decir, si sabeis que vuestro hermano (como ocurrió en mi caso) utiliza *'Msn Messenger'* podeis comentar la regla que lo logea en el archivo *policy.rules*, pues sabeis de sobras que esos paquetes no son raros ni malos para vuestra red. Lo mismo con cada servicio que ofrezcais... simplemente debeis logear aquellos tipos de paquetes que concuerden con ataques, o intentos de intrusion (si mirais los archivos de reglas en seguida vereis a lo que me refiero), por ejemplo buffer overflows en los servicios, intentos de FTP como root, login erroneo por telnet, etc.... Quizá al principio se os escape un poco de las manos, y veais que vuestro Snort tiene muchas reglas y no sabeis diferenciar las que son buenas de las que son malas... no pasa nada. Simplemente dejad que Snort logee, y a medida que vaya pasando el tiempo ireis viendo cuales son las cosas que hacen que vuestra base de datos crezca de un modo exagerado, entonces vais a los archivos de reglas, y comentais la regla que logea eso que no quereis que logee.

Bien, pero... y eso de que logee??? pues bien, vamos a lanzar nuestro Snort!!! Obviamente lo primero que debeis hacer es lo siguiente:

```
# snort --help
```

Yo lo lanzo del siguiente modo:

```
# snort -dev -l /var/log/snort -h 192.168.1.0/24 -c /etc/snort.conf &
```

El argumento *'-l'* define el directorio donde se deben guardar los logs en formato de texto plano o binario. Para ello tendreis que haber configurado el tipo de salida correspondiente, aparte de la base de datos. Tambien podeis olvidar el archivo de los logs, no definir nada y simplemente logear en la MySQL, eso va segun los gustos de cada uno.

7. Configuración de ACID

ACID, la interface web para la visualización de los logs recogidos por Snort, no necesita instalación alguna, sino simplemente debeis descargarlo, guardarlo en el lugar que mas os plazca (por ejemplo en */var/www* si fuese ahi donde teneis los hostings, no olvideis que a fin de cuentas es una pagina web) y descomprimirlo. A partir de ese momento ya teneis una interface ACID. Para configurarla simplemente debeis editar el archivo

acid_config.php y especificarle los parámetros referentes a la base de datos contra la que va a trabajar (nombre de la base de datos, ip del servidor, login y password, etc...). Una vez apuntado, cread un VirtualHost en vuestro servidor apache (lo se, lo se... leed esto para ver algunos ejemplos: <http://httpd.apache.org/docs/vhosts/examples.html>) apuntando al directorio donde habeis descomprimido ACID, y reiniciad el servidor web. Una vez hecho eso, apuntad con vuestro browser a la direccion del virtualhost:

`http://direccion_de_virtualhost/acid_main.php`

Cuando entreis comprobará el estado de las tablas básicas para iniciar el logging... si no estan creadas correctamente, os pedira permiso para hacerlo, decidle que si y lo hara, ningun problema. Ahora ya debeis tener acceso a la interface ACID y seguramente debeis ver las barritas rojas de las 'gráficas' con el porcentaje de trafico TCP, ICMP y UDP ... pero.... todo el mundo debe tener acceso a ver esta página?? No padre...

8. Autenticación de ACID

Para que ACID os pida autenticación (login y password) al entrar, podeis hacerlo de varios modos, pero yo os recomiendo que lo hagais con la autenticación del propio servidor web.

Para hacerlo con Apache la manera es muy sencilla:

1) *Editad vuestro archivo /etc/apache/access.conf (o donde lo tengais):*

(No importa que esté vacío si lo está, añadidle esto:)

```
<Directory /path/hacia/la/web/de/ACID>
```

```
AllowOverride AuthConfig
```

```
order allow,deny
```

```
allow from all
```

```
Options ExecCGI
```

```
</Directory>
```

2) *Editad un archivo en /path/hacia/la/web/de/ACID qye se llame .htaccess*

```
AuthName "Acid Access"
```

```
AuthType Basic
```

```
AuthUserFile /path/hacia/la/web/de/ACID/usuarios/htpasswd.users
```

```
require valid-user
```

3) *Da de alta los usuarios que t engan que tener acceso a ACID*

```
# htpasswd -c /path/hacia/la/web/de/ACID/usuarios/htpasswd.users admin
```

4) *Seguid añadiendo usuarios, quitando el '-c'*

```
# htpasswd /path/hacia/la/web/de/ACID/usuarios/htpasswd.users admin2
```

```
# htpasswd /path/hacia/la/web/de/ACID/usuarios/htpasswd.users admin3
```

```
# htpasswd /path/hacia/la/web/de/ACID/usuarios/htpasswd.users admin4
```

....

5) *Re-arranad el servidor web*

6) *Apuntad con vuestro browser de nuevo a la pagina principal de ACID.*

9. Have Fun!

Disfrutad del sistema de detección de intrusos. Cualquier duda consultadla en las paginas web oficiales (mencionadas al principio, en la introducción). Si veis algún fallo en las explicaciones de este documento, ruego me las hagais llegar para que yo pueda corregirlas (ttyp0@inet2u.com).