

Construir un IDS con Snort + MySQL + BASE + PHP5 + Apache2



Daniel Medianero García (M3134GR0)

dmedianero@gmail.com

ftp://meleagro.homeunix.org

http://meleagro.esp.cc



Introducción

Los IDS son una parte muy importante en la prevención de ataques, constituyen una primera barrera que nos puede ayudar a corregir fallos de seguridad o a recopilar información acerca de un posible futuro atacante. Este documento está orientado fundamentalmente a la construcción de un Detector de intrusos casero utilizando Snort, es por ello que no se utiliza ninguna herramienta propietaria, con lo cual además de salirnos gratis tendremos un IDS libre.

Esta guía es una ampliación y actualización sobre el documento "Guía Snort + MySQL + "ACID + PHP en Slackware 10.1" que realicé hace algo más de un año. Las razones por las cuales me he decidido a actualizar dicho trabajo son varias: la actualización del software utilizado para construir el IDS (Detector de Intrusos) por ejemplo el salto a PHP5 y Apache2, e incluso la modificación del mismo (en esta ocasión cambiamos el gestor ACID por BASE), la puesta al día de manera más general, ya que en la anterior estaba muy marcado su uso para la distribución de Linux Slackware en una versión concreta. En esta ocasión utilizo Slackware como distribución y aunque uso algún paquete hecho especialmente por mí para este propósito (snort o pcre) los pasos son más generales y cualquier usuario de Linux podrá montarse un IDS gracias a esta guía en su propia distribución de Linux, si bien se exigen unos conocimientos previos.

Creo que debería comentar el cambio más drástico que incluye este documento respecto del anterior, se trata del uso de BASE en lugar de ACID. La decisión ha sido fácil, por un lado ahora trabajo en seguridad informática, cosa que no hacía en el momento de escribir la primera guía y he podido ver que BASE es utilizado en mayor medida que ACID (esa es mi experiencia), por otro lado ya lo había conseguido usando ACID y la propuesta de hacer algo diferente también ha tenido su peso en la elección. A esto hay que sumar que BASE está basado en ACID y que la diferencia tampoco es tanta como para desconcertarse. Por si fuera poco ACID no se actualiza desde Agosto del 2003, con lo cual está todo dicho.

Pocas cosas me quedan ya por decir, que todas las acciones se realizan con privilegios de root y comentar que cuando hable de líneas el número puede variar en vuestros archivos, pero es una orientación muy aproximada. Si encontráis alguna errata podéis notificármelo a mi correo electrónico (dmedianero@gmail.com), cualquier mejora u observación es bien recibida y espero que este documento os sea de provecho ya que hay muy poca documentación en castellano al respecto.

Instalar y configurar Snort

Snort es la parte fundamental de esta guía. no obstante es el detector de intrusos en sí, y el resto del software de esta guía está encaminada a la mejor y mas comprensible lectura de las alertas que Snort proporciona.

Snort puede descargarse gratuitamente desde la web oficial (<http://snort.org>) aunque probablemente para cualquier distribución de Linux haya binarios disponibles en formato rpm, deb e incluso pra Slackware tenemos en Linuxpackages.net binarios en tgz.

Sin embargo no he utilizado el tgz de Linuxpackages.net, ya que no está compilado con la opción del soporte para MySQL, que es especialmente importante, ya que el propósito de esta guía es que Snort vuelque sus alertas en una base de datos MySQL de la cual se leen los datos en una interfaz web construida en PHP (BASE) a través de ADODB, de manera que sea muy facil hacer graficos de las alertas, verlas por destino, por puerto, eliminarlas, archivarlas,etc.

Bajamos el tgz de mi Ftp personal, está especialmente compilado para este fin, la orden quedaría así:

```
#wget ftp://meleagro.homeunix.org/slackware/snort-2.6.0.1-i686-2dmg.tgz
```

Ahora procedemos a la instalación del mismo:

```
# installpkg snort-2.6.0.1-i686-2dmg.tgz
```

Creamos el grupo snort, con el cual será ejecutado el programa:

```
# groupadd snort
```

A continuación deberíamos tener las reglas de snort en el directorio /etc/rules y el directorio de logs creado en /var/log/snort. Si has utilizado mi paquete no debes preocuparte pues está todo colocado por defecto en su sitio, en caso contrario coloca cada directorio en su lugar antes de continuar.

Después editamos el archivo de configuración de Snort /etc/snort/snort.conf, dejandolo así:

```
linea 111: "var RULE_PATH /etc/snort/rules"
```

```
linea 684: "output database:log,mysql, user=snort password=tu_contraseña_BBDD dbname=snort" host=localhost
```

Con esto le estamos indicando el lugar de donde usar las reglas de detección y que debe volcar las alertas en una base de datos MySQL llamada snort con una determinada contraseña (a elegir por nosotros). He utilizado las reglas publicas oficiales VRT en la compilación del paquete, estas pueden obtenerse gratuitamente y sin subscripción en la web oficial de Snort. Ya tenemos el Snort configurado, ahora para que se ejecute al iniciar la computadora metemos las siguientes lineas en el fichero /etc/rc.d/rc.local:

```
echo 'Iniciando IDS...'
```

```
snort -c /etc/snort/snort.conf -i eth0 -g snort -D
```

Esto es válido para distribuciones con inicio de tipo BSD, para otras distribuciones con inicio SysV (Debian, Ubuntu, Mandriva, SUSE, etc) estos scripts suelen estar en /etc/init.d

Configurar MySQL

Suponemos que hay un servidor MySQL ejecutándose en el sistema, sino lo instalamos con los binarios correspondientes y lanzamos el servidor, en el caso de Slackware con el comando:

```
# /etc/rc.d/rc.mysql start
```

Para los usuarios de Slackware que tengan problemas con la iniciación del servidor MySQL, que muchas veces da problemas, les recomiendo una web:

<http://mysql.conclase.net/curso/index.php?cap=instalara>

en ella se explica con detalle como poner el servidor y hay guías sobre MySQL muy interesantes. Aunque no utilizéis Slackware esta web os puede ser de mucha utilidad si tenéis dudas respecto de MySQL.

Entramos en la consola de MySQL con el comando:

```
# mysql
```

Esto suponiendo que la BBDD no tenga contraseña, sino lo haríamos con el comando:

```
# mysql -u usuario -p
```

y se nos pedirá una contraseña para ingresar, usualmente el usuario será root. Una vez dentro creamos una BBDD que será la que utilizará Snort:

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

y le asignamos una contraseña para entrar al servidor MySQL si no tenía una antes, lo que es especialmente recomendable:

```
mysql> SET PASSWORD FOR root@localhost=PASSWORD('tu_contraseña_BBDD');
```

aquí suponemos que el usuario de la BBDD es root. Salimos de la consola MySQL:

```
mysql> exit;
```

Ahora vamos a crear el esquema de la BBDD de Snort, que serán las tablas que se utilizarán para volcar sus alertas. Para ejecutar este paso es muy importante tener Snort compilado con soporte de MySQL, si habéis utilizado mis paquete snort el comando queda así:

```
# mysql -u root -p < /usr/lib/snort-2.6.0.1/schemas/create_mysql snort
```

se nos pedirá la contraseña que metimos anteriormente a la BBDD.

Ya deberíamos tener la BBDD preparada, no obstante vamos a comprobarlo, para ello entramos en la consola MySQL y tecleamos las siguientes ordenes:

```
mysql> use snort;
```

```
mysql> show tables;
```

La salida a la segunda orden debe ser la siguiente para comprobar que llevamos todo bien hecho hasta este paso:

```
+-----+
| 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 |
+-----+
```

Instalación y configuración de BASE

Base es la interfaz en PHP que con la cual nos relacionaremos para ver las alertas, eliminarlas, clasificarlas, etc. La descarga e instalación es muy sencilla e independiente de la distribución de Linux que usemos, apenas unos comandos que colocarán BASE en un lugar en el cual Apache2 pueda servirnoslo posteriormente:

```
# cd /var/www/htdocs

# wget http://belnet.dl.sourceforge.net/sourceforge/secureideas/base-1.2.6.tar.gz

# tar zxvf base-1.2.6.tar.gz

# mv base-1.2.6 base

# rm base-1.2.6.tar.gz
```

Una vez descargado pasamos a la configuración, esta se centrará en el fichero `base_conf.php` que debemos copiar de la plantilla que se nos proporciona:

```
# cp /var/www/htdocs/base/base_conf.php.dist /var/www/htdocs/base/base_conf.php
```

Procedemos a la configuración del fichero `base_conf.php`, yo utilizo el editor `vi`, pero podéis utilizar `emacs`, `gvim` o `KWrite`, mientras lo uséis con privilegios de `root`.

Hay que dejar las líneas que os marco tal y como se puede ver a continuación (las líneas no tienen porqué coincidir exactamente, es una orientación relativa):

```
línea 44: $BASE_urlpath= '/base';

línea 66: $DBlib_path = '/var/www/htdocs/base/adodb/';

línea 87: $alert_dbname = 'snort';

línea 90: $alert_user = 'root';

línea 91: $alert_password = 'tu_contraseña_BBDD';
```

guardamos el fichero y salimos. El siguiente paso a realizar es copiar las firmas del Snort al directorio de BASE, estas firmas son ficheros en texto plano con detalles sobre las alertas de Snort, que nos servirán como información para leer cuando salten dichas alertas, las copiamos a su destino adecuado con los siguientes comandos:

```
# mkdir /var/www/htdocs/base/signatures

# cp /usr/lib/snort-2.6.0.1/signatures /var/www/htdocs/base/signatures
```

Ya tenemos BASE configurado, ahora tenemos que poner un método de autenticación, para que el acceso a BASE esté restringido a un usuario con contraseña. No hace falta explicar lo peligroso que resulta no realizar este paso. Para ello creamos el fichero `/var/www/htdocs/base/.htaccess` y le ponemos este contenido:

AuthName ?Base Access?

AuthType Basic

AuthUserFile /var/www/htdocs/base/htpasswd.users

require valid-user

Instalación de ADODB

ADODB será un intermediario entre BASE y MySQL, su instalación es muy sencilla e independiente de la distribución de Linux que utilicemos, basta con escribir los siguientes comandos:

```
cd /var/www/htdocs/base
```

```
wget http://ovh.dl.sourceforge.net/sourceforge/adodb/adodb491.tgz
```

```
tar zxvf adodb491.tgz
```

```
rm adodb491.tgz
```

Instalación de los módulos PEAR

PEAR es un FrameWork de PHP el cual se nos instala junto con PHP5, a través de él vamos a instalar unos módulos de los que se servirá BASE para crear los gráficos de las alertas.

El proceso es muy sencillo e independiente de la distribución de Linux que utilicemos, siempre y cuando nuestro PHP5 esté instalado correctamente e incluya PEAR, en Slackware así es. Los comandos son los siguientes:

```
# cd /var/www/htdocs/base

# wget http://pear.php.net/get/Image_Color-1.0.2.tgz

# tar zxvf Image_Color-1.0.2.tgz

# rm Image_Color-1.0.2.tgz

# pear install Image_Color-1.0.2.tgz

# wget http://pear.php.net/get/Image_Canvas-0.3.0.tgz

# tar zxvf Image_Canvas-0.3.0.tgz

# rm Image_Canvas-0.3.0.tgz

# pear install Image_Canvas-0.3.0.tgz

# wget http://pear.php.net/get/Image_Graph-0.7.tgz

# tar zxvf Image_Graph-0.7.2.tgz

# rm Image_Graph-0.7.2.tgz

# pear install Image_Graph-0.7.2.tgz
```

Configuración de Apache2

Suponemos que hay un servidor http ejecutándose en el sistema, sino lo instalamos con los binarios correspondientes. Para configurarlo paramos el servidor, en el caso de Slackware con el comando:

```
# /etc/rc.d/rc.httpd stop
```

Lo primero que vamos a hacer es terminar de configurar el acceso al portal de BASE, es decir configurar el acceso mediante contraseña, para ello ejecutamos los comandos:

```
# mkdir /var/www/passwords
```

```
# /usr/bin/httpasswd -c /var/www/passwords/passwords tu_usuario_portal_BASE
```

con el segundo comando le estamos diciendo el usuario que tendrá acceso al portal, y tras ejecutarlo nos pedirá la contraseña para dicho usuario.

Es recomendable que el servidor Apache2 no se ejecute como root, por ello deberíamos crear un usuario y un grupo específico para él, en algunas distribuciones la instalación de Apache crea un usuario y un grupo "apache", yo he utilizado el usuario y grupo "web":

```
# groupadd web
```

```
# useradd -g web web
```

Procedemos a la configuración del servidor, todo se hace a través del fichero de configuración /etc/apache2/httpd.conf, añadiendo al fichero:

```
Include /etc/apache2/mod_php.conf
```

con ello habilitamos el soporte para PHP. Modificamos las líneas indicadas (las líneas no tienen que coincidir exactamente, es una orientación relativa):

```
línea 309: User web
```

```
línea 310: Group web
```

con esto haremos que el servidor sea lanzado con los usuarios que creamos anteriormente, lo que constituye una medida de seguridad. Al final del fichero añadimos lo siguiente:

```
<Directory "/var/www/htdocs/base/">  
  
AuthType Basic  
  
AuthName "Detector de Intrusos"  
  
AuthUserFile /var/www/passwords/passwords  
  
Require user tu_usuario_portal_BASE  
  
</Directory>
```

esto ya termina de configurar la autenticación y deja nuestro Apache2 listo para ser lanzado. Ejecutamos el servidor http:

```
# /etc/rc.d/rc.httpd start
```

Configuración web de BASE

Ahora terminaremos de configurar via web el BASE, para ello ejecutamos nuestro navegador favorito y en la dirección le metemos la siguiente:

http://localhost/base/base_main.php

nos aparecera una imagen como la siguiente:

Basic Analysis and Security Engine (BASE)

The underlying database snort@localhost appears to be incomplete/invalid

The database version is valid, but the BASE DB structure (table: acid_ag) is not present. Use the [Setup page](#) to configure and optimize the DB.

hacemos click sobre el enlace "Setup page" y en la siguiente pantalla sobre el botón AG.

Si todo va bien debería salirnos una pantalla similar a la siguiente:

The screenshot shows the BASE web interface with a blue header and navigation menu. The main content area displays a list of successfully created database tables and a table of operations. The operations table has columns for Operation, Description, and Status. The status for both 'BASE tables' and 'Search indexes' is 'DONE'. Below the table, there is a message about the underlying Alert DB configuration and a section for additional DB permissions. At the bottom, there is a footer with navigation links and version information.

Home | Search | Alert Group Maintenance [Back]

Successfully created 'acid_ag'
Successfully created 'acid_ag_alert'
Successfully created 'acid_ip_cache'
Successfully created 'acid_event'
Successfully created 'base_iden'
Successfully created 'base_users'

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	DONE
Search indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

The underlying Alert DB is configured for usage with BASE.

Additional DB permissions
In order to support Alert purging (the selective ability to permanently delete alerts from the database) and DNS/whois lookup caching, the DB user 'snort' must have the DELETE and UPDATE privilege on the database 'snort@localhost'.

Go to the [Main page](#) to use the application.

[Loaded in 0 seconds]

Alert Group Maintenance | Cache & Status | Administration

BASE 1.0.1 (mitchelle) by Kevin Johnson and the BASE Project Team
Built on ACID by Roman Danyliw

Lo cual indica que se ha terminado de definir la BBDD que utilizará Snort para volver sus alertas. Ya tenemos listo el IDS, para acceder a él desde el propio PC se utiliza la dirección proporcionada antes, desde el exterior se utiliza la dirección del PC seguida de

/base/base_main.php, se nos pedirá usuario y contraseña y ya tendremos la interfaz web BASE para interactuar con ella.

Notas

La utilización de BASE queda fuera del propósito de este manual. Es bastante sencillo lo que no lo es tanto es entender las alertas, aunque tenemos buena documentación en los enlaces que BASE nos proporciona y las firmas de Snort.

Levantar los servidores Apache2 y MySQL no ha sido el propósito de esta guía pero no debería ser excesivamente complicado, se supone que alguien que quiera montar un IDS debe tener ciertos conocimientos y hay abundante información sobre ello en la red.

Repito que cualquier errata que encontréis podéis comunicármela y así haremos de esta guía algo mejor para todos. Cualquier duda que tengáis al respecto os remito a mi Blog (<http://meleagro.esp.cc>) y a mi dirección de correo electrónico (dmedianero@gmail.com).

Software necesario

Snort 2.6.0.1 (<http://snort.org/>)

PHP 5.1.4 (<http://www.php.net/>)

MySQL 5.0.24 (<http://www.mysql.com/>)

BASE 1.2.5 (<http://secureideas.sourceforge.net/>)

Apache 2.0.58 (<http://www.apache.org/>)

ADODB 491 (<http://adodb.sourceforge.net/>)

PEAR (<http://pear.php.net/>)

PCRE 6.7 (<http://www.pcre.org/>)

Sobre el autor

Daniel Medianero García (M3134GR0) está terminando Ingeniería Técnica en Informática de Gestión en la Universidad Complutense de Madrid y trabaja en la empresa de seguridad informática S21sec (<http://www.s21sec.com>).

Es un adicto al Slackware y en la guerra de escritorios se decanta por KDE. Podéis encontrarle en los foros de EspacioLinux (<http://espaciolinux.com>) y en IRC en el canal #slackware-es del servidor FreeNode. Podéis encontrar este documento junto con otros en su Ftp personal (<ftp://meleagro.homeunix.org>), además de algunos scripts y paquetes para Slackware creados y mantenidos por él.

Licencia del documento

Derechos de Autor © 2006 por Daniel Medianero García.
Este documento esta liberado bajo la licencia creative commons.