

**LE SYSTÈME DE DÉTECTION D'INTRUSION SNORT
AVEC CONSOLE DE GESTION**

<http://nassih.com>

© MOHAMED NASSIH.

1. Introduction.

On général les alertes générées par SNORT pourront être consultées directement dans un fichier d'alertes. Une autre façon de faire est d'installer un système d'interface développé en PHP pour visualiser les différentes alertes générées, c'est le système ACID (Analysis Console for Intrusion Detection). ACID pourra visualiser les alertes à partir une base de données mysql.. SNORT doit donc être configuré pour qu'il enregistre ces alertes dans une base de données, qu'il faut créer.

2. Liste de logiciels et bibliothèques.

Évidemment nous avons besoin de SNORT, nous allons configurer SNORT pour qu'il enregistre les logs dans une base de données mysql, nous aurons besoin donc d'installer et configurer le système de gestion de base de données mysql. SNORT utiliser la bibliothèque Libpcap pour capturer les paquets transitant sur le réseau il faut donc s'assurer qu'elle est bien installée.

ACID est une application développée en PHP, nous aurons besoin donc d'installer PHP et le configurer sur un serveur Apache. Nous aurons besoin d'installer aussi la librairie de base de données ADODB. ADODB est une librairie PHP utilisé pour rendre l'accès aux bases de données indépendant du système de gestion des bases de données utilisé.

Les autres bibliothèques à installer sont, Zlib, qui est une bibliothèque utilisée pour la compression/décompression. JPGRAPH, qui est un ensemble de librairies qui sera utilisé par ACID pour générer des graphiques sous forme de courbes ou histogrammes et la bibliothèque PCRE (Perl-Compatible Regular Expressions) qui est un ensemble de fonctions qui implémentent la recherche par expressions rationnelles.

Tableau 2.1 : les liens vers des fichiers d'installations.

Nom	Lien
SNORT	http://www.snort.org/dl/current/snort-2.1.0.tar.gz
MYSQL	http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-4.0.23.tar.gz
APACHE	http://www.apache.org/dist/httpd/httpd-2.0.54.tar.gz
PHP	http://us3.php.net/get/php-4.4.0.tar.gz/from/www.php.net/mirror
ADODB	http://phplens.com/lens/dl/adodb411.tgz
ACID	http://acidlab.sourceforge.net/acid-0.9.6b23.tar.gz
ZLIB	http://www.zlib.net/zlib-1.2.3.tar.gz
JPGGRAPH	http://members.chello.se/jpgraph/jpgdownloads/jpgraph-1.19.tar.gz
LIBPCAP	http://www.tcpdump.org/release/libpcap-0.8.1.tar.gz
PCRE	ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-4.4.tar.gz

3. La mise en place de SNORT.

Étape 1 : installer la bibliothèque PCRE.

Nous allons utiliser dans notre cas la version 4.4 de la bibliothèque PCRE. La figure 3.1 montre comment on pourra installer et configurer cette bibliothèque.

```
# Installer la bibliothèque PCRE
tar -xvzf pcre-4.4.tar.gz
cd pcre-4.4
./configure
make
make install
```

Figure 3.1 : installation de PCRE.

Étape 2 : Installation la bibliothèque ZLIB :

La figure 3.2 montre la compilation et l'installation de la bibliothèque ZLIB.

```
tar -xvzf zlib-1.2.3.tar.gz
cd zlib-1.2.3
./configure
make test
make install
```

Figure 3.2 : installation de ZLIB.

Étape 3 : Installation de MYSQL :

Nous allons créer le groupe mysql et l'utilisateur mysql. Pour créer le groupe, nous utilisons la commande «groupadd mysql». Et nous utilisons la commande «useradd -g mysql mysql -s /dev/null» pour créer l'utilisateur.

```
groupadd mysql
useradd -g mysql mysql -s /dev/null
```

Figure 3.4 : création du groupe et de l'utilisateur mysql.

Pour qu'on puisse utiliser mysql à partir de n'importe quel emplacement dans l'arborescente, nous devons ajouter le chemin /usr/local/mysql/bin au variable PATH. Nous éditons donc le fichier /root/.bash_profile puis nous ajoutons au variable PATH, le chemin suivant :/usr/local/mysql/bin. PATH=\$PATH:\$HOME/bin:/usr/local/mysql/bin.

La figure 3.5 montre l'installation de mysql.

```
tar -xvzf mysql-4.0.17.tar.gz
cd mysql-4.0.17
./configure --prefix=/usr/local/mysql
make
make install
```

Figure 3.5 : installation de mysql.

Nous devons exécuter le script «scripts/mysql_install_db». Le script scripts/mysql_install_db va installer la base de données par défaut, puis initialiser les tables de droits. Nous devons changer le propriétaire des répertoires /usr/local/mysql et /usr/local/mysql/var à mysql et copier le fichier de configuration my-medium.cnf.

```
chown -R root /usr/local/mysql
chown -R mysql /usr/local/mysql/var
chgrp -R mysql /usr/local/mysql
cp support-files/my-medium.cnf /etc/my.cnf
```

Figure 3.6 : les permissions et la copie du fichier de configuration.

La dernière étape est d'ajouter les lignes “/usr/local/mysql/lib/mysql” et “/usr/local/lib” au fichier /etc/ld.so.conf.

Puis nous exécutons la commande “ldconfig -v”, comme root. Ldconfig créer les liens nécessaires, et met en cache les bibliothèques partagées trouvées dans les répertoires dans le fichier /etc/ld.so.conf, et dans les répertoires /lib et /usr/lib.

L'option -v permet d'afficher le numéro de version actuelle, le nom de chaque répertoire traité et les liens qui sont créés.

Pour tester le bon fonctionnement de Mysql, nous allons démarrer le serveur en arrière plan en utilisant la commande /usr/local/mysql/bin/mysqld_safe --user=mysql&. (voir la figure 3.7).

```
[root@localhost mysql-4.0.23]# /usr/local/mysql/bin/mysqld_safe --user=mysql &
[1] 26971
[root@localhost mysql-4.0.23]# Starting mysqld daemon with databases from /usr/local/mysql/var
[root@localhost mysql-4.0.23]#
```

Figure 3.7 : le démarrage du serveur mysql.

Nous exécutons la commande “ps -ef |grep mysql” pour s'assurer que le processus de mysql, mysqld est en exécution.

```
[root@localhost mysql-4.0.23]# ps -ef | grep mysql
root      26971  1864  0 06:11 pts/0    00:00:00 /bin/sh /usr/local/mysql/bin/mysqld_safe --user=mysql
mysql    26994  26971  1 06:11 pts/0    00:00:02 [mysqld]
root      27004  1864  0 06:14 pts/0    00:00:00 grep mysql
[root@localhost mysql-4.0.23]# █
```

Figure 3.8 : vérification du processus mysqld avec la commande ps.

Nous allons configurer Mysql pour qu'il démarre au démarrage du système pour se faire il faut copie le script de démarrage /tmp/mysql-4.0.23/support-files/mysql.server à partir des fichiers sources vers le répertoire /etc/init.d/mysql.

En suite, nous créons les liens symboliques dans le répertoire d'initiation pour les niveaux d'exécution 3 et 5. (Voir la figure 3.8)

```
cd /etc/rc3.d
ln -s /etc/init.d/mysql S85mysql
ln -s /etc/init.d/mysql K85mysql

cd /etc/rc5.d
ln -s /etc/init.d/mysql S85mysql
ln -s /etc/init.d/mysql K85mysql

cd /etc/init.d
chmod 755 mysql
```

Figure 3.9 : créer des liens dans le répertoire d'initiation pour mysql.

libjpeg et libpng sont deux bibliothèques pour gérer les deux formats d'image JPEG et PNG. Nous devons installer les deux RPMs libpng-devel-1.2.2-16.i386.rpm et libjpeg-devel-6b-26.i386.rpm en utilisant les commandes :

```
Rpm -ivh libpng-devel-1.2.2-16.i386.rpm
```

```
Rpm -ivh libjpeg-devel-6b-26.i386
```

Étape 4 : Installation de APACHE, et le configurer avec PHP :

La figure 3.10 montre l'installation d'Apache. "/www" sera le répertoire de base.

```
tar -xvzf httpd-2.0.48.tar.gz
cd httpd_2.0.48
./configure --prefix=/www --enable-so
make
make install
```

Figure 3.10 : l'installation et la configuration de Apache.

La commande «/www/bin/apachectl start» permet de démarrer le serveur. On pourra tester le serveur en essayant d'accéder à la page par défaut d'Apache à partir d'un explorateur. La commande «/www/bin/apachectl stop» permet d'arrêter le serveur Apache. La figure 3.11 montre les commandes pour installer le module PHP.

```
tar -xvzf php-4.3.4.tar.gz
cd php-4.3.4
./configure --prefix=/www/php --with-apxs2=/www/bin/apxs --with-config-file-
path=/
www/php --enable-sockets --with-mysql=/usr/local/mysql --with-zlib-dir=/
usr/local --with-gd (one line)
make
make install
```

Figure 3.11 : l'installation et la configuration de PHP.

Le fichier php.ini-dist est le fichier de configuration de PHP. Nous devons le copier à partir du répertoire qui contient les sources vers /www/php/php.ini en utilisant la commande, cp php.ini-dist /www/php/php.ini. Pour permettre le chargement du module PHP, nous ajoutons les trois lignes de la figure 3.12 au fichier de configuration /www/conf/httpd.conf.

```
LoadModule php4_module modules/libphp4.so AddType application/x-httpd-
php .php
DirectoryIndex index.php index.html index.html.var
```

Figure 3.12 : la configuration de httpd pour PHP.

Pour configurer Apache pour qu'il démarre automatiquement. On doit copier le script de démarrage vers /etc/init.d en utilisant la commande `cp /www/bin/apachectl /etc/init.d/httpd`. La figure 3.14 montre comment on crée les liens pour le 3eme et 5eme niveau.

```
cd /etc/rc3.  
ln -s /etc/init.d/httpd S85httpd  
ln -s /etc/init.d/httpd K85httpd  
cd /etc/rc5.d  
ln -s /etc/init.d/httpd S85httpd  
ln -s /etc/init.d/httpd K85httpd
```

Figure 3.14 : création des liens au niveau 3 et 4.

Étape 5 : Installation de SNORT :

Comme dans le cas de mysql, Nous ajoutons l'utilisateur et le groupe `-snort-` qui seront utilisés par le processus de SNORT.

```
groupadd snort  
useradd -g snort snort -s /dev/null
```

Figure 3.15 : l'ajout de l'utilisateur et du groupe snort.

Nous devons créer le répertoire principal de SNORT, le répertoire des alertes et le répertoire des règles.

```
mkdir /etc/snort  
mkdir /var/log/snort  
mkdir /etc/snort/rules
```

Figure 3.16 : création des répertoires de SNORT.

La figure 3.17 montre l'installation de SNORT.

```
tar -xvzf snort-2.1.0.tar.gz
cd snort-2.1.0
./configure --with-mysql=/usr/local/mysql
make
make install
```

Figure 3.17 : l'installation de SNORT.

SNORT fournit avec les sources un ensemble de règles, ces règles se trouvent dans le répertoire /tmp/snort-2.1.0/rules. Nous devons copier ces règles dans le répertoire /etc/snort/rules en utilisant la commande `cp /tmp/snort-2.1.0/rules/* /etc/snort/rules`.

SNORT fournit aussi les fichiers de configuration, Nous devons les copier dans le répertoire /etc/snort, le fichier principal de configuration est le fichier snort.conf, sera aussi copié. (Figure 3.18).

```
cp /tmp/snort-2.1.0/etc/*.conf /etc/snort
cp /tmp/snort-2.1.0/etc/*.config /etc/snort
cp /tmp/snort-2.1.0/etc/*.map /etc/snort
```

Figure 3.18 : copie des fichiers de configuration.

Le fichier /etc/snort/snort.conf doit être modifié pour qu'il reflète notre configuration. la figure 3.19 montre les lignes à modifier avec les explications requises.

```
# Le réseau à protéger
var HOME_NET 192.168.2.0/24
var EXTERNAL_NET any
# Le chemin du répertoire des règles
var RULE_PATH /etc/snort/rules
# On veut que SNORT log dans la base de données mysql
output database: log, mysql, user=snort password=test dbname=snort
host=localhost
```

Figure 3.19 : modification du fichier snort.conf.

Pour que SNORT démarre automatiquement au démarrage du système, on doit copier le script de démarrage dans le répertoire /etc/init.d, puis créer les liens au niveau 3 et 5. Nous utilisons la commande `cp /tmp/snort-2.3.3/contrib/S99snort /etc/init.d/snort` pour copier le script de démarrage (on a renommé ce fichier à snort). Ce script doit être modifié pour indiquer le chemin du répertoire principal de SNORT, le chemin du fichier de configuration snort.conf et le nom du groupe utilisé par SNORT. (Voir figure 3.20).

```
SNORT_PATH=/usr/local/bin
CONFIG=/etc/snort/snort.conf
SNORT_GID=snort
```

Figure 3.20 : les modification dans le script de démarrage.

Nous créons les liens pour le 3eme niveau et 5eme niveau, et nous donnons à ce fichier le droit d'exécution.

```
chmod 755 /etc/init.d /snort
cd /etc/rc3.d
ln -s /etc/init.d/snort S99snort
ln -s /etc/init.d/snort K99snort
cd /etc/rc5.d
ln -s /etc/init.d/snort S99snort
ln -s /etc/init.d/snort K99snort
cd /etc/init.d
chmod +x snort
```

Figure 3.21 : création des liens et des droits pour le script « snort ».

Étape 6 : La création de la base de donnée snort :

`/usr/local/mysql/bin/mysql` est la commande pour accéder à mysql, Nous aurons le prompt suivant « `mysql>` ». La figure 3.22 montre la création et l'affectation des droits à la base de données snort.

```

# password pour root
mysql> SET PASSWORD FOR root@localhost=PASSWORD('test');
# Créer la base de données snort
mysql> create database snort;
# les droit pour snort
mysql> grant INSERT,SELECT on root.* to snort@localhost;
# password pour snort
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('test');
# les droit pour snort
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort;

```

Figure 3.22 : la création de la base de données snort dans mysql.

La commande exit va permettre de quitter mysql. À partir du répertoire /tmp/snort-2.1.0, on exécute les commandes de la figure 3.23. Ces deux scriptes vont créer les tables nécessaires dans la base de données snort. Il faut fournir le mot de passe, c'est "test" dans notre cas.

```

/usr/local/mysql/bin/mysql -u root -p < ./contrib/create_mysql snort
cd contrib
zcat snortdb-extra.gz | /usr/local/mysql/bin/mysql -p snort

```

Figure 3.23 : scripte pour la création des tables.

On pourra s'assurer que la base de données snort est bien créée avec les tables nécessaires (en utilisant la commande /usr/local/mysql/bin/mysql -p, et visualiser les tables snort créées).

Étape 7 : La mise en place d'ACID.

Les commandes tar -xvzf jpgraph-1.14.tar.gz, tar -xvzf adodb390.tgz et tar -xvzf acid-0.9.6b23.tar.gz permettent de décompresser les fichiers de JPGRAPH, ADODB et ACID dans le répertoire /www/htdocs. Le fichier de configuration d'ACID, /www/htdocs/acid/acid_conf.php doit être modifié, (Voir la figure 3.24).

```

# le chemin vers ADODB
$DBlib_path = "/www/htdocs/adodb";
# il s'agit d'une base de données mysql
$DBtype = "mysql";
# la connexion à la base de données snort pour les
# alertes et les archives
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "test";
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "test";
# le chemin vers la bibliothèque JGRAPH
$ChartLib_path = "/www/htdocs/jpgraph-1.14/src";

```

Figure 3.24 : le fichier de configuration *acid_conf.php*.

Nous démarrons le serveur Apache en utilisant la commande `/etc/rc5.d/S85httpd start` Il nous reste qu'à tester notre implémentation. Nous pourrions accéder à ACID via l'URL `http://adresse/acid/acid_main.php`.

Operation	Description	Status
ACID tables	Adds tables to extend the Snort DB to support the ACID functionality	<input type="button" value="Create ACID AG"/>
Search Indexes	(Optional) Adds indexes to the Snort DB to optimize the speed of the queries	DONE

[Loaded in 0 seconds]

ACID v0.9.6b23 (by Roman Danyliw as part of the AirCERT project)

Figure 3.25 : la page de DBsetup de ACID.

Cette page va nous permettre de créer les tables qui seront utilisées par ACID. Il suffit de cliquer sur le bouton «create ACID AG ». Le système répond :

Successfully created 'acid_ag'
Successfully created 'acid_ag_alert'
Successfully created 'acid_ip_cache'
Successfully created 'acid_event'

En retournant sur la même page http://192.168.2.40/acid/acid_main.php, **ACID** affiche la page principale. (Voir figure 3.26)

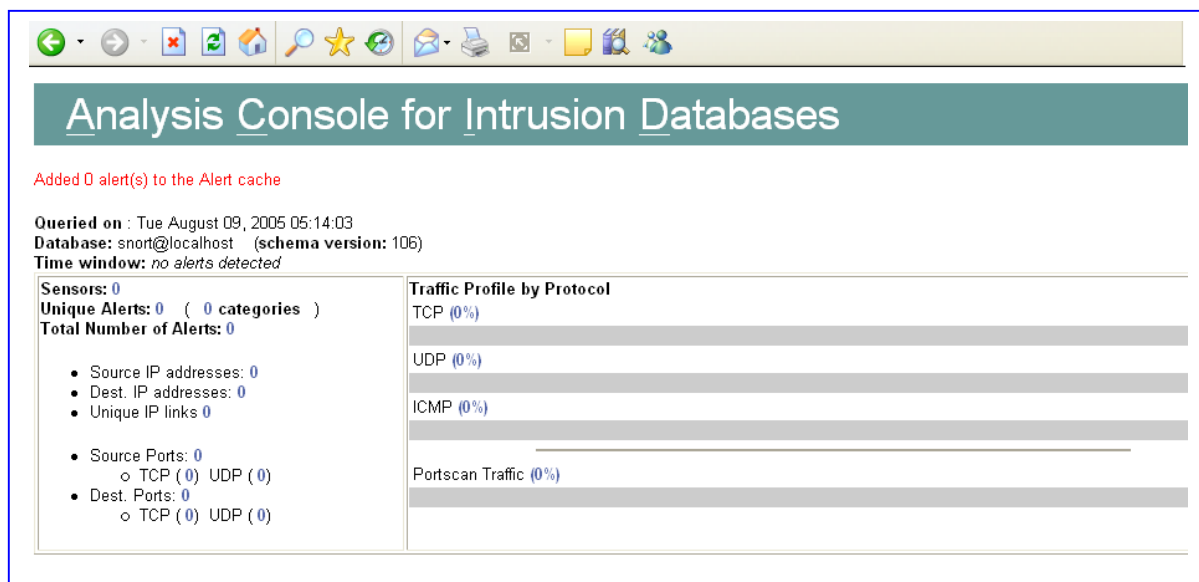


Figure 3.26 : page d'accueil de SNORT.

Nous remarquons qu'il n'y a pas d'alerte, puisque notre SDI est installé seulement dans un réseau de test et il n'y a pas de trafic sur le réseau.