Written by Mr. Sontaya Photibut
Saturday, 02 May 2009 15:37

การติดตั้ง Intrusion Detection ด้วย Snort และ BASE

Snort เป็น Open Source IDS (intrusion detection system) เครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่ายและทำงานแบบ real-time alerting และ Snort สามารถเก็บล็อกไฟล์ที่เราต้องการลง database ได้ เช่น MySQL, PosgrestSQL เป็นต้น

Requirements

- เครื่องของคุณต้องทำเป็น web server แล้ว (apache2, MySQL5, PHP5)
- install(YaST)
  - Snort
  - PCRE (Perl Compatible Regular Expressions)
  - LIBPCAP

Install BASE (Basic Analysis and Security Engine)

Base เป็น plug-ins สำหรับดึงข้อมูลมาตรวจสอบจาก database ทำให้สะดวกในการ monitoring

```
# mkdir /usr/src/snort
# cd /usr/src/snort
# wget http://nchc.dl.sourceforge.net/sourceforge/secureideas/base-1.3.9.tar.gz
# tar -zxvf base-1.3.9.tar.gz -C /srv/www/htdocs/
# mv /srv/www/htdocs/base-1.3.9 base
# chmod 757 /srv/www/htdocs/base/
```

Install ADOdb: (ADOdb Database Abstraction Library for PHP

```
# cd /usr/src/snort
# wget http://nchc.dl.sourceforge.net/sourceforge/adodb/adodb504.tgz
# tar -zxf adodb504.tgz
# tar -zxvf adodb504.tar.gz -C /srv/www/htdocs/
# mv /srv/www/htdocs/adodb504 adodb
```

Configure Snort

```
# vi /etc/snort/snort.conf
```

เปลี่ยน "var HOME_NET any" ไปเป็น "var HOME_NET 192.168.0.0/24"
(เครือข่ายที่ต้องการ monitor)
เปลี่ยน "var EXTERNAL_NET any" ไปเป็น "var EXTERNAL_NET !$HOME_NET"
เปลี่ยน "var RULE_PATH ../rules" to "var RULE_PATH /etc/snort/rules"

Create Database for Snort

□□□□□□□□□□□□ /usr/share/doc/packages/snort/schemas
create_mysql

□□□□□□□□□□□□ DB □□□□ snort (□□□□□ command □□□□ phpMyAdmin □□□□□□□□□□□□□□□□)
□□□□ import □□□□ create_mysql □□□□□□□ DB snort □□□□
mysql -u root -p
(root password)
mysql> create database snort;
mysql> exit
mysql -D snort -u root -p </usr/share/doc/packages/snort/schemas/create_mysql
(root password)

vi /etc/snort/snort.conf
output database: log, mysql, user=root password=password dbname=snort host=localhost

□□□□□ **snort**□□□□□□□□□□□□□□□□□□□ error □□□□□□□□
snort -c /etc/snort/snort.conf
□□□□□□□□□□□□□□□□□□□□□□□□ (□□□□□□□□□ error □□□□□□□□□□□ ok)

Rule application order: ->activation->dynamic->drop->alert->pass->log
Log directory = /var/log/snort

--== Initialization Complete ==--

,,_ -*> Snort! <*-
o")~ Version 2.4.4 (Build 28) x86_64
"" By Martin Roesch & The Snort Team: http://www.snort.org/team.html
(C) Copyright 1998-2005 Sourcefire Inc., et al.
NOTE: Snort's default output has changed in version 2.4.1!
The default logging mode is now PCAP, use "-K ascii" to activate
the old default logging mode.

□□ Ctrl+C □□□□□□□□□□□□□□□□

BASE web page setup
□□□□ web browser (firefox) http://yoursite.com/base/

Step 1
□□□□ Continue

Step 2
Language : english
Path to ADODB : /srv/www/htdocs/adodb
□□□□ Submit Query

Step 3
Database type : MySQL
Database Name : snort
Database Host : localhost
Database User Name : root
Database Password : ******
□□□□ Submit Query

Step 4
Admin User Name: root
Password : *******
Full Name : SYSBASD

Step 5
□□□□□□□□ Create BASE AG
□□□□□□□□ Now continure to stop5...

Install Image_Color, Image_Canvas and Image_Graph
□□□□□□□□ php5-gd □□□ YaST

```
# pear5 channel-update "pear.php.net"
# pear5 install Image_Color
# pear5 install Image_Canvas-alpha
# pear5 install Image_Graph-alpha
```

□□□□

```
# cd /srv/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
# pear5 install Image_Color-1.0.2.tgz

# wget http://pear.php.net/get/Image_Canvas-0.3.1.tgz
# tar zxvf Image_Canvas-0.3.1.tgz
# rm Image_Canvas-0.3.1.tgz
# pear5 install Image_Canvas-0.3.1.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
# pear5 install Image_Graph-0.7.2.tgz
```

Starting Snort

```
# chmod 775 /srv/www/htdocs/base/
# snort -c /etc/snort/snort.conf -i eth0 -g root -D
```

Web base runing

http://www.yoursite.com/base/