

Tutorial Membangun Snort Sebagai Intrusion Detection System

Integrasi terhadap BASE dan MySQL

Tom Gregory

t0m@stibanas.ac.id

<http://tom149c.blogspot.com>

Lisensi Dokumen:

Copyright © 2003 IlmuKomputer.Com

Seluruh dokumen di **IlmuKomputer.Com** dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari **IlmuKomputer.Com**.

Serangan terhadap system di internet semakin merajalela, tentunya sebagai network administrator, bukanlah pekerjaan yang mudah untuk memonitor beratus-ratus IP yang masuk dan keluar dari klien. Memasang honeypot untuk mengelabui *hacker* juga bukanlah satu-satunya cara untuk lebih mengamankan daerah internal dan DMZ. Kita membutuhkan bantuan sebuah program yang dapat memonitor jalannya paket data dan mencatatnya serta menyediakan informasi tersebut untuk selanjutnya bisa dianalisa lebih lanjut.

Adalah SNORT sebuah program yang bekerja sebagai **IDS (Intrusion Detection System)** yang dapat melakukan pencatatan paket-paket data dan koneksi yang sedang berjalan untuk kemudian di tampilkan untuk kita. Penulis sengaja mengintegrasikan SNORT dengan program BASE dan MySQL agar tampilan yang dihasilkan berupa tampilan web dan semua pencatatan yang dilakukan disimpan dalam database.

Sedikit cerita, beberapa bulan yang lalu, penulis sempat meng-install Denyhosts, sebuah program di sistem Linux yang dapat melakukan penolakan terhadap host-host yang dianggap melakukan intrusi ke sebuah sistem. Denyhosts khusus memonitor service SSH, dan mencatatnya dalam sebuah file *hosts.deny* apabila diketahui ada host dari luar yang gagal melakukan login pada service SSH.

Setelah berjalan sampai sekarang, sudah ada sekitar 10-15 host yang masuk dalam daftar host yang di tolak (*hosts.deny*). Penulis berpikir, bahwa memang banyak intrusi dari luar ke dalam sistem, namun apakah hanya ke service SSH? Teringat akan IDS (Intrusion Detection System) yang sangat terkenal, Snort, penulis iseng-iseng menginstallnya beberapa hari yang lalu, dan baru sempat penulis dokumentasikan sekarang ☺

SNORT yang akan penulis install sudah terintegrasi secara *web based* karena penulis juga mengikutsertakan program BASE (*Basic Analysis and Security Engine*) dan ADOdb sebagai tambahan. Dengan adanya BASE, maka akan ada tambahan dalam mengkonfigurasi web server. Diasumsikan dokumen root untuk web server yaitu: */var/www/html/* dan IP server adalah **192.168.10.1** menggunakan interface *eth0*.

Baiklah, sudah bisa dimulai...

Pertama-tama, buat direktori sementara kita untuk mendownload dan kompilasi:

```
# mkdir /root/snorttemp  
# cd /root/snorttemp
```

Kedua, download file-file yang dibutuhkan:

DOWNLOAD FILE-FILE YANG DIBUTUHKAN

Snort Program + Snort Rules

Download **Snort** versi terbaru (*saat artikel ini ditulis versi 2.6.1.1*)

```
# wget http://www.snort.org/dl/current/snort-  
2.6.1.1.tar.gz
```

Kita juga butuh rules untuk **Snort**!

Silakan pergi ke <http://www.snort.org/pub-bin/downloads.cgi>. Lalu perhatikan "**Sourcefire VRT Certified Rules - The Official Snort Ruleset (unregistered user release)**" (kalo Anda sudah register, silakan download yang "**Sourcefire VRT Certified Rules - The Official Snort Ruleset (registered user release)**")

Penulis sudah register, jadi harus login dulu kemudian baru bisa download...

```
# wget http://www.snort.org/pub-  
bin/downloads.cgi/Download/vrt_os/snortrules-snapshot-  
CURRENT.tar.gz
```

PCRE - Perl Compatible Regular Expressions.

Untuk program BASE, kita butuh PCRE silakan download di <http://www.pcre.org/> (*yang terbaru saat tulisan ini ditulis adalah versi 6.7*)

```
# wget  
ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-  
6.7.tar.gz
```

LIBPCAP

Silakan download LIBPCAP di <http://www.tcpdump.org/>
(yang terbaru saat tulisan ini ditulis adalah versi 0.9.5)

```
# wget http://www.tcpdump.org/release/libpcap-0.9.5.tar.gz
```

BASE (Basic Analysis and Security Engine)

Download BASE di <http://secureideas.sourceforge.net/>
(versi terbaru saat tulisan ini ditulis adalah versi 1.2.7)

```
# wget  
http://surfnet.dl.sourceforge.net/sourceforge/secureideas/  
base-1.2.7.tar.gz
```

ADODB (ADODB Database Abstraction Library for PHP (and Python))

Download ADODB di <http://adodb.sourceforge.net/>
(versi terbaru saat tulisan ini ditulis adalah adodb-493a-for-php)

```
# wget  
http://surfnet.dl.sourceforge.net/sourceforge/adodb/adodb4  
93a.tgz
```

Kalo sudah di download semua, silakan di ekstrak semuanya:

```
# tar xzvf snort-2.6.1.1.tar.gz  
# tar xzvf snortrules-snapshot-CURRENT.tar.gz  
# tar xzvf pcre-6.7.tar.gz  
# tar xzvf libpcap-0.9.5.tar.gz  
# tar xzvf base-1.2.7.tar.gz  
# tar xzvf adodb493a.tgz
```

Kemudian delete file arsipnya:

```
# rm -rf *.gz
```

Seharusnya isi dari pada direktori **snorttemp** adalah sebagai berikut:

```
sh-3.00# ls  
adodb base-1.2.7 doc libpcap-0.9.5 pcre-6.7 rules snort-2.6.1.1 so_rules  
sh-3.00#
```

Sekarang tinggal kompilasi, dimulai dari **LIBPCAP**...

KOMPILASI PROGRAM LIBPCAP

```
# cd /root/snorttemp/libpcap-0.9.5
# ./configure
# make && make install
```

PCRE - Perl Compatible Regular Expressions.

```
# cd /root/snorttemp/pcre-6.7
# ./configure
# make && make install
```

SNORT

```
# cd /root/snorttemp/snort-2.6.1.1
# ./configure --enable-dynamicplugin --with-mysql
# make && make install
```

Untuk **Snort**, kita perlu membuat direktori map untuk log dan rulesnya:

```
# mkdir -p /etc/snort/rules
# mkdir /var/log/snort
```

Selanjutnya, bagian terpenting. Copy seluruh isi ekstrak **snortrules** ke direktori map **snort**:

```
# cp rules/* /etc/snort/rules/
# cp -rvf so_rules /etc/snort/
# cp -rvf doc /etc/snort/
```

Yang sangat penting lainnya:

```
# cd snort-2.6.1.1/etc
# cp * /etc/snort/
```

Edit *snort.conf* sesuai dengan kebutuhan:

```
# nano /etc/snort.conf
```

Lakukan perubahan pada baris-baris berikut:

ganti "var HOME_NET any" jadi "var HOME_NET 192.168.10.0/24"
ganti "var EXTERNAL_NET any" jadi "var EXTERNAL_NET !\$HOME_NET"
ganti "var RULE_PATH ../rules" jadi "var RULE_PATH /etc/snort/rules"

Berhubung tadi kita sudah meng-kompilasi **Snort** dengan opsi *--with-mysql* dan

memang integrasi dengan database dibutuhkan untuk program **BASE**, maka sekarang kita akan membuat database untuk **Snort** agar bisa berinteraksi lewat **BASE**. Temukan baris:

```
# output database: log, mysql, user=root password=[password ] dbname=snort  
host=local$
```

dan hilangkan tanda "#"

```
output database: log, mysql, user=root password=[password] dbname=snort  
host=local$
```

Sesuaikan juga username, password dan database yang akan digunakan. **BASE** akan melakukan koneksi database menggunakan username, password dan database tersebut. Pastikan Anda memasukkannya dengan benar. Silakan simpan konfigurasi Anda.

Setting Database untuk SNORT

Silakan buat database untuk snort, terserah dengan apa, namun penulis sarankan menggunakan **phpmyadmin**, karena lebih mudah dan memiliki tampilan yang menyenangkan. Jangan lupa untuk menyesuaikan dengan keadaan konfigurasi database yang sudah kita edit tadi di **/etc/snort/snort.conf**. Table layout ada di file **create_mysql** di direktori **/root/snorttemp/snort-2.6.1.1/schemas**.

Kalo sudah jadi, silakan test konfigurasi **Snort**:

```
# snort -c /etc/snort/snort.conf
```

Apabila tidak ada error, berarti SUKSES !! Silakan batalkan test dengan menekan **Ctrl+C**.

Memindahkan ADODB dan BASE

ADODB

Kembali ke tempat semula:

```
# cd /root/snorttemp/
```

Pindahkan direktori **ADODB** ke root direktori web server:

```
# mv adodb /var/www/
```

BASE (Basic Analysis and Security Engine)

Pindahkan direktori **base-1.2.7** ke direktori web server yang dapat diakses:

```
# mv base-1.2.7 /var/www/html/
```

lalu kita pindah ke sana:

```
# cd /var/www/html/
```

Agar mudah diakses, ganti namanya menjadi **base**:

```
# mv base-1.2.7 base
```

Ganti permissionnya:

```
# chmod 757 base
```

Sampai disini, kita bisa bernafas lega. Yang udah cape, silakan istirahat dulu, kalo memang udah malam bisa tidur dulu dan lanjutkan besok pagi. Tapi kalo belum, lanjuuutt !!

BASE Web based Setup

Silakan buka web browser Anda, dan arahkan ke
<http://192.168.10.1/base/setup>

Kalo tidak ada masalah, akan tampil halaman seperti dibawah ini:

The screenshot shows the 'Settings' page of the BASE Setup Program. It has a title bar 'Basic Analysis and Security Engine (BASE) Setup Program'. Below the title bar, there is a message: 'The following pages will prompt you for set up information to finish the install of BASE. If any of the options below are red, there will be a description of what you need to do below the chart.' The settings are displayed in a table:

Settings
Config Writeable: Yes
PHP Version: 4.3.10-16
PHP Logging Level: [ERROR][WARNING][PARSE]

At the bottom of the table is a 'Continue' button.

Klik Continue

Step 1 of 5

Masukkan path ADODB (**[/var/www/adodb](#)**):

The screenshot shows 'Step 1 of 5' of the BASE Setup Program. It has a title bar 'Basic Analysis and Security Engine (BASE) Setup Program'. The form contains two input fields: 'Pick a Language:' with a dropdown menu set to 'english' and a help icon [?]; and 'Path to ADODB:' with a text box containing '/var/www/adodb' and a help icon [?]. At the bottom is a 'Submit Query' button.

Klik Submit Query

Step 2 of 5

Masukkan informasi yang ada, dan biarkan pilihan "**Use Archive Database**" apa adanya:

Basic Analysis and Security Engine (BASE) Setup Program

Step 2 of 5

Pick a Database type: MySQL [?]

Database Name: snort

Database Host: localhost

Database Port: Leave blank for default

Database User Name: root

Database Password: HHgGH-AASnt1254

☐ Use Archive Database [?]

Archive Database Name:

Archive Database Host:

Archive Database Port: Leave blank for default

Archive Database User Name:

Archive Database Password:

Submit Query

Klik Submit Query

Step 3 of 5

Jika mau, kita bisa menggunakan pilihan "**Use Authentication System**" agar lebih aman:

Basic Analysis and Security Engine (BASE) Setup Program

Step 3 of 5

☐ Use Authentication System [?]

Admin User Name:

Password:

Full Name:

Submit Query

Klik Submit Query

Step 4 of 5

Klik **Create BASE AG** untuk membuat database:

Basic Analysis and Security Engine (BASE) Setup Program

Successfully created 'acid_ag'
 Successfully created 'acid_ag_alert'
 Successfully created 'acid_ip_cache'
 Successfully created 'acid_event'
 Successfully created 'base_roles'
 Successfully INSERTED Admin role
 Successfully INSERTED Authenticated User role
 Successfully INSERTED Anonymous User role
 Successfully INSERTED Alert Group Editor role
 Successfully created 'base_users'

Step 4 of 5		
Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality	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 "root" must have the DELETE and UPDATE privilege on the database "snort@localhost"

Now continue to [step 5...](#)

Kalo sudah, lanjutkan ke **step 5...**

Basic Analysis and Security Engine (BASE)

- Today's alerts: unique listing Source IP Destination IP
- Last 24 Hours alerts: unique listing Source IP Destination IP
- Last 72 Hours alerts: unique listing Source IP Destination IP
- Most recent 15 Alerts: any protocol TCP UDP ICMP
- Last Source Ports: any protocol TCP UDP
- Last Destination Ports: any protocol TCP UDP
- Most Frequent Source Ports: any protocol TCP UDP
- Most Frequent Destination Ports: any protocol TCP UDP
- Most frequent 15 Addresses: Source Destination
- Most recent 15 Unique Alerts
- Most frequent 5 Unique Alerts

Added 0 alert(s) to the Alert cache

Queried on : Mon June 26, 2006 12:13:56
 Database: snort@localhost (Schema Version: 107)
 Time Window: no alerts detected

Search
 Graph Alert Data
 Graph Alert Detection Time

Sensors/Total: 0 / 1
 Unique Alerts: 0
 Categories: 0
 Total Number of Alerts: 0

- Src IP addrs: 0
- Dest. IP addrs: 0
- Unique IP links 0
- Source Ports: 0
 - TCP (0) UDP (0)
- Dest Ports: 0
 - TCP (0) UDP (0)

Traffic Profile by Protocol

TCP (0%)

UDP (0%)

ICMP (0%)

Portscan Traffic (0%)

Alert Group Maintenance | Cache & Status | Administration

BASE 1.2.5 (sarah) (by Kevin Johnson and the BASE Project Team
 Built on ACID by Roman Danyliw)

[Loaded in 1 second]

Untuk melihat tampilan grafis dari traffic **BASE**, Anda bisa mendownload *Image_Color*, *Image_Canvas* dan *Image_Graph*

```
# pear install Image_Color
# pear install Image_Canvas-alpha
# pear install Image_Graph-alpha
```

Selesai....

Ganti permission direktori base dari 757 ke 775

```
# chmod 775 base
```

Delete juga direktori temporary `/root/snorttemp`:

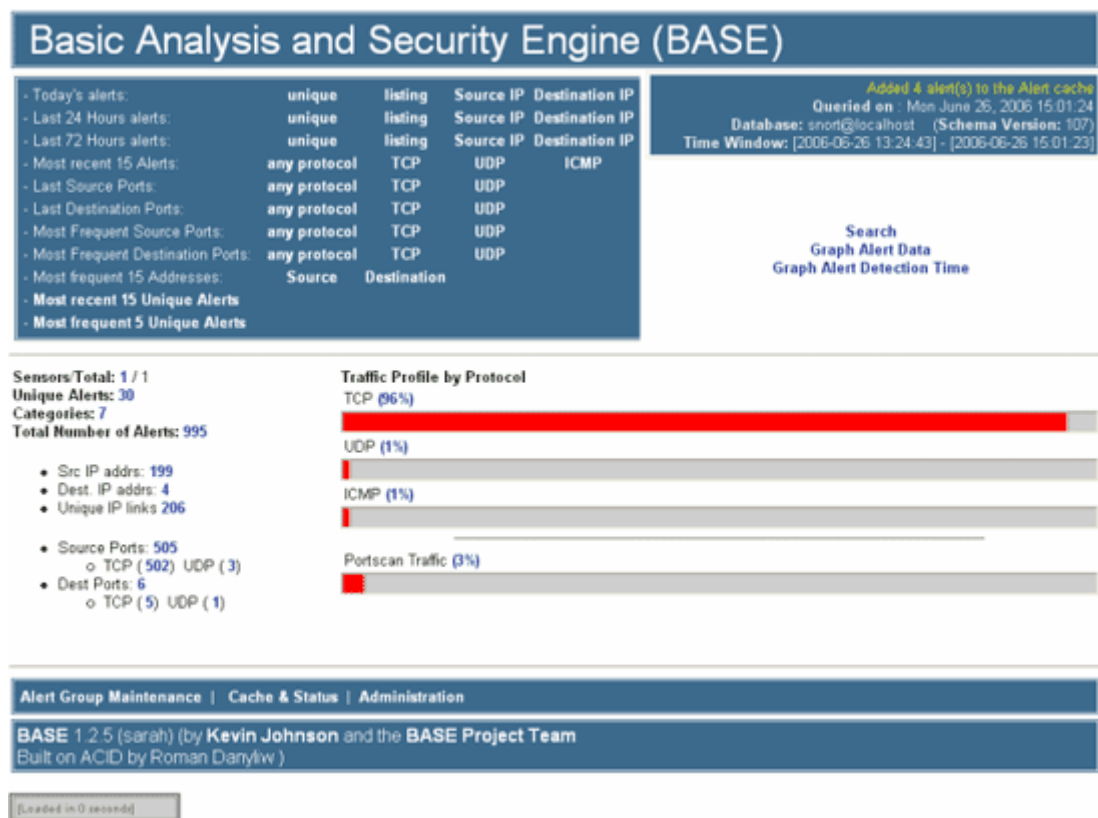
```
# rm -rf /root/snorttemp
```

Menjalankan SNORT

Untuk menjalankan **Snort**, silakan jalankan perintah berikut:

```
# /usr/local/bin/snort -c /etc/snort/snort.conf -i eth0 -g root -D
```

Silakan tunggu beberapa waktu. Apabila tidak ada error, silakan akses ke web server yg pada kasus ini pada alamat <http://192.168.10.1/base/> , lakukan pengujian dengan melakukan port scanning ke server, maka Snort akan mencatat dan menampilkannya dan pada tampilan **BASE** akan seperti ini:



Selesai sudah tutorial ini, semoga menjadi sangat bermanfaat mengingat banyaknya serangan yang datang secara membabi-buta ke segala penjuru dunia belakangan ini ☺

Tutorial ditulis berdasarkan dokumen-dokumen dari:

- <http://www.snort.org/docs/>
- web2.uwindsor.ca/courses/cs/aggarwal/cs60564/projects/BASE.doc

Biografi Penulis



Thomas Gregory Ajawaila. Lahir di Jakarta, 28 Mei 1984. Selesai menamatkan Sekolah Menengah Umum Marsudirini Bekasi tahun 2002. Masih berjuang untuk menyelesaikan kuliah di STIMIK Perbanas Jakarta angkatan 2002. Saat ini sedang mendalami ilmu keamanan komputer dan melakukan riset terhadap perkembangan keamanan komputer melalui jaringan RT/RW Net. Aktif dalam organisasi kampus sebagai pencetus dan pendiri Himpunan Mahasiswa Sistem Informasi STIMIK Perbanas merangkap ketua pada periode 2006/2007. Penulis juga berlaku sebagai Moderator pada mailing list Jasakom-Perjuangan dan sebagai Owner pada mailing list Jasakom-Moderator. Penulis aktif di komunitas Jasakom dan melakukan riset serta penelitian, kecenderungan untuk menulis pun tak bisa dihindari.

Berpengalaman sebagai system administrator pada web server STIMIK Perbanas (<http://stibanas.ac.id>), sebagai hacking trainer pada beberapa instansi / lembaga training seperti Informatics, dan Sokka Data Informatika yang telah melayani klien-klien dari beberapa perusahaan dan instansi pemerintah seperti PT. Wijaya Karya, Pusintek Departemen Keuangan, TNI-AL, dan PT. Sinar Mas.

Informasi lebih lanjut tentang penulis ini bisa didapat melalui:

URL : <http://tom149c.blogspot.com>
Email : t0m@stibanas.ac.id / sick.minded@gmail.com