

Memonitor jaringan dengan Basic Analysis and Security Engine.

Dadhi Wijayanto

dadhee@gmail.com

http://dadhee.blogspot.com/

Lisensi Dokumen:

Copyright © 2003-2006 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.

Salam opensource...!!

Sebelumnya mohon maaf buat para senior, gw cuma seorang newbie. Bukan bermaksud menggurui hanya sekedar sharing informasi. Aplikasi ini nyaris berguna buat sysAdmin buat mengontrol traffic di jaringannya. Semacam perintah iptraf atau ipstats. Tapi gw kira ini lebih kompleks lagi.

Pendahuluan

Aplikasi yang dibutuhkan adalah Snort, Apache, SSL, PHP, MySQL, dan BASE. Disini gw pake CentOS 4 yang sudah diinstall sebagai web server dan database server.

Langkah pertama setelah CentOS 4 udah diinstal:

Donlot snort dan PCRE

Ente-ente donlot pake paan kek, yang penting bisa donlot. Klo gw lebih seneng pake wget.

wget <http://www.snort.org/dl/old/snort-2.3.3.tar.gz>

disini gw sengaja tidak menggunakan snort versi 2.6.11 dikarenakan versi ini lebih friendly. (padahal belum pernah nyoba. Hehehe).

Buat donlot PCRE.

wget <http://easynews.dl.sourceforge.net/sourceforge/pcpre/pcpre-5.0.tar.gz>

Install PCRE

tar -xvzf pcre-5.0.tar.gz

cd pcre-5.0

./configure

make

make install

Install dan konfigurasi snort

tar -xvzf snort-2.3.3.tar.gz

cd snort-2.3.3

```
# ./configure --with-mysql
# make
# make install
# groupadd snort
```

Buat group dengan nama snort

```
# useradd -g snort snort -->> membuat user dengan nama snort dan menggabungkan ke group snort
# mkdir /etc/snort -->> buat direktori (bla...bla...bla)
# mkdir /etc/snort/rules
# mkdir /var/log/snortInstall rule dan file conf (dari direktori install snort)
# cd rules
# cp * /etc/snort/rules
# cd ../etc
# cp * /etc/snort
```

Buat konfigurasi pada file snort.conf dan ubah beberapa baris

var HOME_NET 10.2.2.0/24

-->>(internal network, gunakan aturan dari CIDR. Kalo gak tau CIDR buka link <http://www.oav.net/mirrors/cidr.html>)

var EXTERNAL_NET !\$HOME_NET

-->>(berarti semua dianggap bukan home net/ diluar jaringan)

change "var RULE_PATH ../rules" to "var RULE_PATH /etc/snort/rules"

-->>menentukan path dari rule buat snort

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

-->>pemberitahuan buat snort kalo sistem ini ada mysqlnya. :D
Memulai snort pada saat sistem restart

tambahkan baris dibawah ini pada file /etc/rc.local:

```
/usr/local/bin/snort -c /etc/snort/snort.conf -i eth0 -g snort -DSetting database MySQL
```

```
# mysql
```

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

```
>Query OK, 0 rows affected (0.25 sec)
```

```
mysql> create database snort;
```

```
>Query OK, 1 row affected (0.01 sec)
```

```
mysql> grant INSERT,SELECT on root.* to snort@localhost;
```

```
>Query OK, 0 rows affected (0.02 sec)
```

```
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('password_from_snort.conf');
```

```
>Query OK, 0 rows affected (0.25 sec)
```

```
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhost;
```

```
>Query OK, 0 rows affected (0.02 sec)
```

```
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
```

```
>Query OK, 0 rows affected (0.02 sec)
```

```
mysql> exit
```

```
>Bye
```

Buat table unt database snort

```
# mysql -u root -p Enter password:
```

```
mysql> SHOW DATABASES;
```

(You should see the following)

```
+-----+
```

```
| Database
```

```
+-----+
```

```
| mysql
```

```
| Snort
```

```
| test
```

```
+-----+
```

```
3 rows in set (0.00 sec)
```

```
mysql> use snort
```

```
>Database changed
```

```
mysql> SHOW TABLES;
```

```
+-----+
```

```
| Tables_in_snort
```

```
+-----+
```

```
| data
```

```
| detail
```

```
| encoding
```

```
| event
```

```
| icmphdr
```

```
| iphdr
```

```
| opt
```

```
| reference
```

```
| reference_system
```

```
| schema
```

```
| sensor
```

```
| sig_class
```

```
| sig_reference
```

```
| signature
```

```
| tcphdr
```

```
| udphdr
```

```
+-----+
```

```
16 rows in set (0.00 sec)
```

```
exit;
```

Kalo udah muncul table2 diatas berarti settingan dan konfigurasi yang udah dilakukan diatas berhasil. Ntar gw mo siapin kopi dulu...

```
... ..
```

```
... ..
```

OK... Kembali ke laaapp...toooooopp....!!

Sekarang donlot dan install BASE

Sebelumnya kita juga perlu mendonlot ADODB buat sesajen (serius amat bacanya. Hehehe...).

Ini buat konek dengan aplikasi database. Seperti biasa kita menggunakan wget.

```
# wget http://easynews.dl.sourceforge.net/sourceforge/adodb/adodb462.tgz
```

Donlot BASE dan kroco-kroconya

Buka browser dan buka link ini:

http://sourceforge.net/project/showfiles.php?group_id=103348

Saya gak mau nerangin lagi cara donlotnya... terserah mo pake apa.

Install ADODB

Kembali ke direktori tempat nyimpen hasil donlot tadi. Ketikin nih perintah.

```
# cp adodb462.tgz /var/www/ -->>Kopiin master adodb ke /var/www/  
# cd /var/www/  
# tar -xvzf adodb462.tgz -->>Ekstrak
```

Install dan konfigurasi BASE

Masih di direktori tempat nyimpen hasil donlot. Ketikin lagi.

```
# cp base-1.1.2.tar.gz /var/www/html/ -->>Kopiin master base-1.1.2 ke /var/www/  
# cd /var/www/html  
# tar -xvzf base-1.1.2.tar.gz -->>Ekstrak  
# mv base-1.1.2 base -->>Rename (biar gampang maksudnya)  
# cd /var/www/html/base/  
# cp base_conf.php.dist base_conf.php -->>Buat file base_conf.php dengan isi dari  
base_conf.php.dist
```

Edit file "base_conf.php" dan tambahkan parameter ini

```
$BASE_urlpath = "/base";  
$DBlib_path = "/var/www/adodb/ ";  
$DBtype = "mysql";  
$alert_dbname = "snort";  
$alert_host = "localhost";  
$alert_port = "";  
$alert_user = "snort";  
$alert_password = "password_from_snort_conf";
```

Penutup

Sampai sejauh ini berarti sudah berhasil. Terus aktifkan daemon apache, mysql, php. Nyalakan browser Mozilla atau Conqueror atau apapun itu selagi berbentuk internet browser.

Ketikan: <http://localhost/base>

Lalu ikuti perintah untuk menginstallnya, (biasanya sih diawali dengan mengklik 'SETUP').

Kalo kali ini berhasil berarti sang admin bisa memonitor aktivitas jaringannya lewat web browser.

Akhir kata... selamat mencoba...