ภาคผนวก

ภาคผนวก ก
การติดตั้งระบบ

ก.1 โปรแกรมที่ต้องการ

1.) ระบบปฏิบัติการลีนุกซ์ Fedora เวอร์ชัน 3 (http://fedora.redhat.com/download)

2.) ระบบปฏิบัติการฟรีบีเอสดี (FreeBSD) เวอร์ชัน 5.2.1

3.) โปรแกรม Snort เวอร์ชัน 2.2.0 (http://www.snort.org/dl/)

4.) โปรแกรม C Compiler เวอร์ชัน 3.4.3-22 (ftp://ftp.gnu.org/gnu/gcc/)

5.) ไลบารี LibPcap เวอร์ชัน 0.8.3-7 (http://rpmfind.net) หรือ (http://www.tcpdump.org/release/libpcap-0.8.3-7.tar.gz)

6.) โปรแกรม MySql เวอร์ชัน 4.1.12 (http://rpmfind.net) หรือ (http://mysql.secsup.org/Downloads/MySQL-4.0/mysql-standard-4.1.12-pc-linux-gnu-i686.tar.gz)

7.) โปรแกรม Apache เวอร์ชัน 2.0.53(http://rpmfind.net) หรือ (http://www.apache.org/dist/httpd/httpd-2.0.53.tar.gz)

8.) โปรแกรม Thai Acid เวอร์ชัน 0.1 beta (http://security.ricr.ac.th)

9.) โปรแกรม PHP เวอร์ชัน 4.3.10(http://rpmfind.net) หรือ (http://www.php.net/distributions/php-4.3.10.tar.gz)

10.) ไลบารี Adodb เวอร์ชัน 4.63 (http://heanet.dl.sourceforge.net/sourceforge/adodb/adodb463.tgz)

11.) ไลบารี PHPlot เวอร์ชัน 5.0RC2 (http://www.phplot.com)

12.) ไลบารี Gd เวอร์ชัน 2.0.33 (http://www.boutell.com/gd/)

13.) ไลบารี JPGraph เวอร์ชัน 1.17 (http://www.aditus.nu/jpgraph/)

14.) โปรแกรม Snortsam เวอร์ชัน 2.2 (http://www.snortsam.net/download.html)

15.) ปลั๊กอิน Snortsam บนโปรแกรม Snort (http://www.snortsam.net/download.html)

16.) โปรแกรม Perl Compatible Regular Expressions เวอร์ชัน 5.0 (http://www.pcre.org)

ก.2 การติดตั้งโปรแกรม

1.) ไลบารี LibPcap

```
# rpm -ivh  libpcap-0.8.3-7.i386.rpm
```

2.) โปรแกรม MySql

```
#  groupadd mysql
# useradd -g mysql mysql
# cd /usr/local
# gunzip < /PATH/TO/MYSQL-VERSION-OS.tar.gz | tar xvf -
# ln -s FULL-PATH-TO-MYSQL-VERSION-OS mysql
# cd mysql
#  scripts/mysql_install_db --user=mysql
#  chown -R root  .
#  chown -R mysql data
#  chgrp -R mysql .
#  bin/mysqld_safe --user=mysql &
```

3.) โปรแกรม Apache และ PHP

ทำการแตกไฟล์ httpd-2.0.53.tar.gz โดยใช้คำสั่ง tar xvfz httpd-2.0.53.tar.gz

3.2 ./configure –prefix=/usr/local/apache \

```
--enable-so     \
--enable-cgi    \
--enable-info   \
--enable-rewrite        \
--enable-speling        \
--enable-usertrack      \
--enable-deflate \
--enable-ssl    \
--enable-mime-magic
```

3.3 make

3.4 make install

2.3.1 แตกไฟล์ PHP โดยใช้คำสั่ง tar xvfz php-4.3.10.tar.gz

2.3.2 ./configure \

--with-apxs2=/usr/local/apache/bin/apxs \

--with-mysql \

--prefix=/usr/local/apache/php \

--with-config-file-path=/usr/local/apache/php \

--enable-force-cgi-redirect \

--disable-cgi \

--with-zlib \

--with-gettext \

--with-gd

2.3.3 make

2.3.4 make install

2.3.5 cp -p php.ini-recommended /usr/local/apache/php/php.ini

2.3.6 เพิ่มบรรทัดนี้ในไฟล์ httpd.conf

LoadModule php4_module modules/libphp4.so

2.3.7 เพิ่ม index.php ในท้ายบรรทัดดังนี้

DirectoryIndex index.html index.php

2.3.8 ลบเครื่องหมาย # ในไฟล์httpd.conf บรรทัดดังนี้

AddHandler php5-script php

AddType text/html php

AddType application/x-httpd-php-source phps

<Files *.php>

SetOutputFilter PHP

SetInputFilter PHP

</Files>

2.3.9 /usr/local/apache/bin/apachectl start

4.) โปรแกรม pcre

2.4.1 tar –xvzf pcre-5.0.tar.gz

2.4.2 cd pcre-5.0

2.4.3 ./configure

2.4.4 make

2.4.5 make install

5.) โปรแกรม Snort

2.5.1 # mkdir /etc/snort

2.5.2 # mkdir /var/log/snort

2.5.3 # tar -xvzf snort-2.2.0.tar.gz

2.5.4 # cd snort-2.2.0

2.5.5 # ./configure --with- mysql

2.5.6 # make

2.5.7 # make install

2.5.8 การติดตั้งกฎและไฟล์คอนฟิกุเรชัน

2.5.9 # cd /home/temp/snort-2.2.0 (ไดเรกทอรีที่เก็บซอสโปรแกรม Snort)

2.5.10 # cd rules

2.5.11 # cp * /etc/snort

2.5.12 # cd ../etc

2.5.13 # cp snort.conf /etc/snort

2.5.14 # cp *.config /etc/snort

6.) ไลบารี ADODB

2.6.1 # cp adodb463.tgz /var/www/html/

2.6.2 # cd /var/www/html/

2.6.3 # tar -xvzf adodb463.tgz

2.6.4 # rm –rf adodb463.tgz

2.6.5 # mv adobd-ภุ- adobd

7.) ไลบารี PHPLOT

2.7.1 # cp phplot-5.0RC2.tar.gz /var/www/html/

2.7.2 # cd /var/www/html/

2.7.3 # tar -zxvf phplot-5.0RC2.tar.gz

2.7.4 # rm -rf phplot-5.0RC2.tar.gz

2.7.5 # mv phplot-5.0RC2.tar.gz phplot

8.) ไลบารี GD

2.8.1 # cp gd-2.0.33.tar.gz /var/www/html/

2.8.2 # cd /var/www/html/

2.8.3 # tar -zxvf gd-2.0.33.tar.gz

2.8.4 # rm -rf gd-2.0.33.tar.gz

2.8.5 # mv gd-2.0.33 gd

9.) ไลบารี JPGraph

2.9.1 # cp jpgraph-1.17.tar.gz /var/www/html/

2.9.2 # cd /var/www/html/

2.9.3 # tar –xvzf jpgraph-1.17.tar.gz

2.9.4 # rm –rf jpgraph-1.17.tar.gz

2.9.5 # cd jpgraph-1.17

2.9.6 # rm -rf README

2.9.7 # rm -rf QPL.txt

2.9.8 # mv jpgraph-1.17 jpgraph

10.) โปรแกรม thai-Acid

2.10.1 # cp thai-acid-0.1.tar.gz /var/www/html/

2.10.2 # cd /var/www/html/

2.10.3 # tar –xvzf thai-acid-0.1.tar.gz

2.10.4 # rm -rf acid-0.1.tar.gz

2.10.5 # mv acid-0.1.tar.gz acid

11.) โปรแกรม Snortsam

2.11.1 # tar -zxvf snortsam-2.22.tar.gz

2.11.2 # cd snortsam-2.22

2.11.3 # chmod +x makesnortsam.sh

2.11.4 # ./makesnortsam.sh

12.) ปลั๊กอิน Snortsam บนโปรแกรม Snort

2.12.1 # tar -zxvf snortsam-patch.tar.gz

2.12.2 # chmod +x patchsnort.sh

2.12.3 # ./patchsnort.sh /usr/local/src/snort

2.12.4 จากนั้นคอมไพล์โปรแกรม Snort ใหม่

2.12.5 # ./snortsam /etc/snortsam.conf

ก.3 การแก้ไขไฟล์คอนฟิกุเรชันโปรแกรม Snort

ไฟล์คอนฟิกุเรชันชองโปรแกรม Snort อยู่ที่ /etc/snort/snort.conf

ระบุตำแหน่งไดเรกทอรีที่เก็บกฎ

```
var  RULE_PATH /etc/snort/
```

ระบุเอาต์พุตของระบบ (เช่นกรณีนี้ให้บันทึกลงฐานข้อมูล MySql)

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

ก.4 การติดตั้งฐานข้อมูลใน MySql

```
# mysql -u root
mysql> set password for 'root'@'localhost'=password('mypassword');
mysql> create database snort;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@localhost;
mysql> connect mysql;
mysql>set password for 'snort'@'localhost'='password('mypassword');
mysql>set password for 'snort'@'%'='password('mypassword');
mysql> flush privileges;
mysql> exit
```


ก.5 การแก้ไขไฟล์คอนฟิกุเรชันโปรแกรม Thai ACID

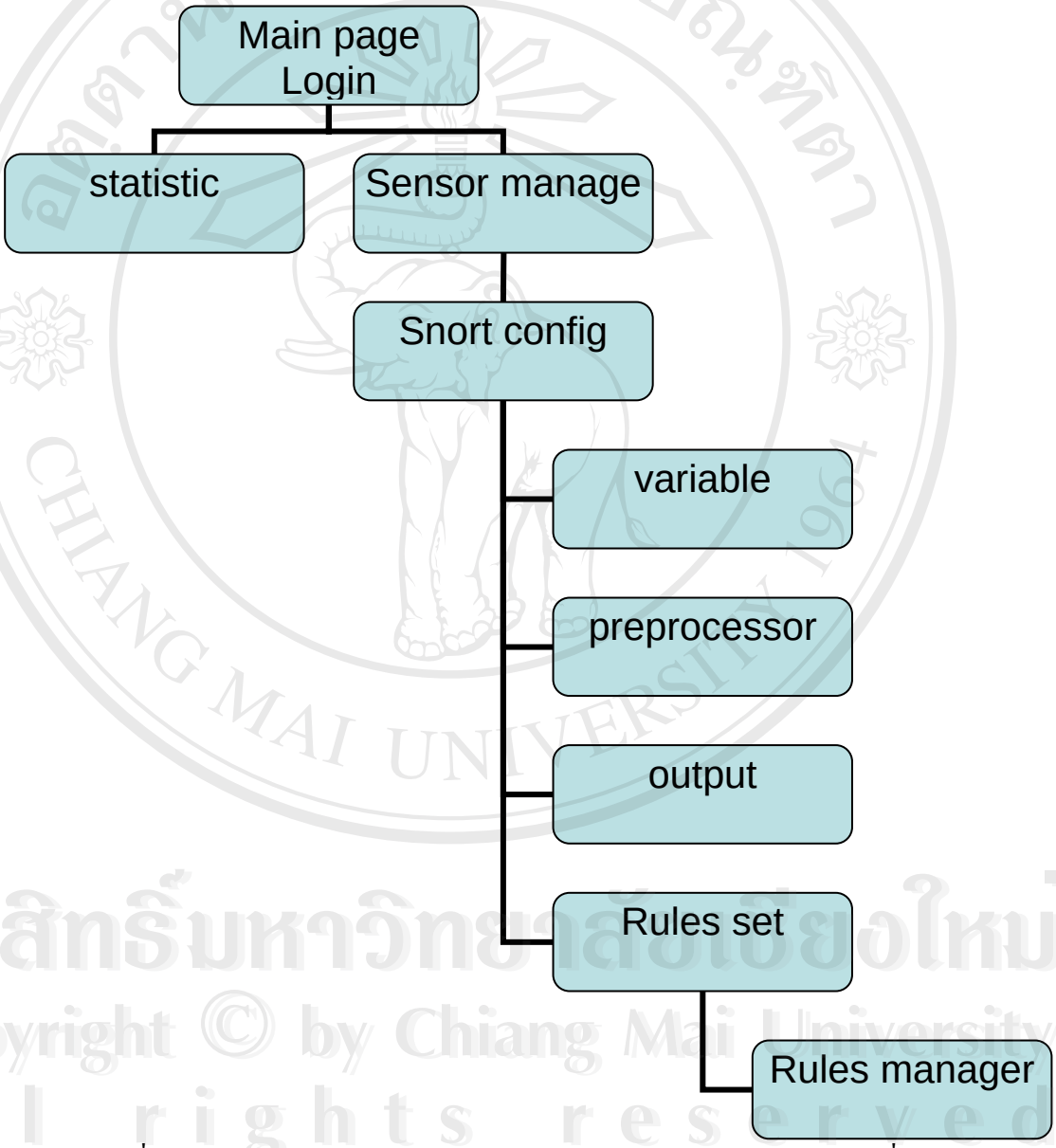
```
# vi /var/www/html/acid/acid_conf.php
$Dblib_path="../adodb";
$DBtype = "mysql";
$alert_dbname="snort";
```

```
$alert_user="snort";
$alert_password="xxx";
$Chartlib_path="../phplot";
```

ภาคผนวก ข

คู่มือการใช้งานโปรแกรม

ข.1 โครงสร้างของระบบ



รูปที่ ข.1 แสดงโครงสร้างหลักของระบบแสดงผลทางสถิติและการจัดการเรื่องกฎ

ข.2 วิธีการใช้งานระบบแสดงผลทางสถิติและการจัดการเรื่องกฎการตรวจสอบการบุกรุก

เมื่อเริ่มใช้ระบบจะปรากฏหน้าจอเพื่อให้ผู้ดูแลระบบป้อนบัญชีรายชื่อและ

รหัสผ่านเพื่อเข้าสู่ระบบ ดังรูป ข.2

รูป ข.2 แสดงหน้าจอล๊อคอินเพื่อเข้าสู่ระบบ

จากรูป ข.2 ขั้นตอนการล็อคอินคือ

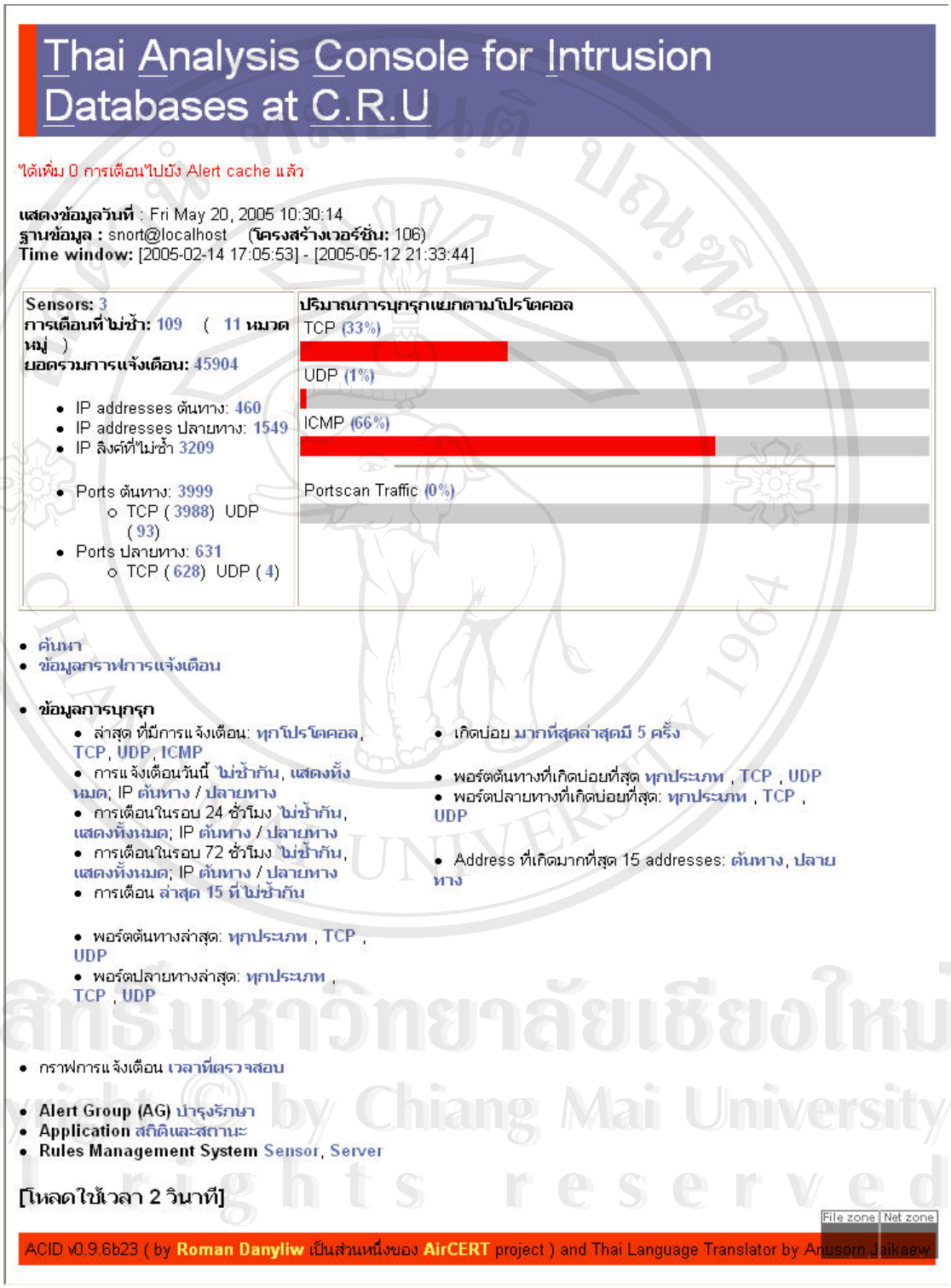
1. ป้อนบัญชีรายชื่อผู้ใช้งานระบบในช่อง User name
2. ป้อนรหัสผ่านในช่อง Password
3. กดปุ่ม OK เพื่อเริ่มเข้าสู่ระบบ

รูป ข.3 แสดงหน้าจอหลักของระบบการติดต่อผู้ใช้

จากรูป ข.3 สามารถใช้งานได้ดังนี้

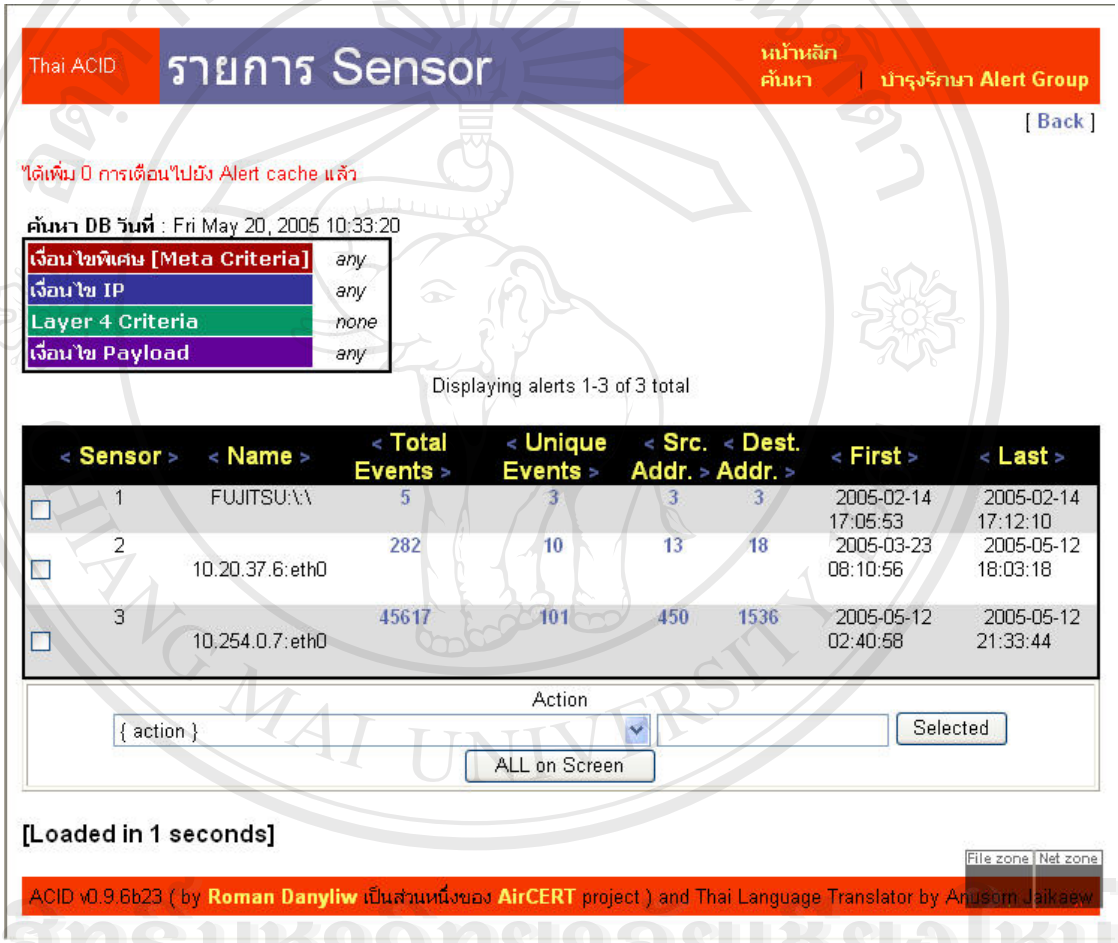
1. เลือกที่ Statistic Monitoring เพื่อเลือกแสดงข้อมูลการบุกรุกเครือข่าย
2. เลือกที่ Sensor Management เพื่อจัดการเกี่ยวกับกฎของเครื่องเซ็นเซอร์ (Sensor)

ข.3 วิธีการใช้งานระบบแสดงผลทางสถิติ



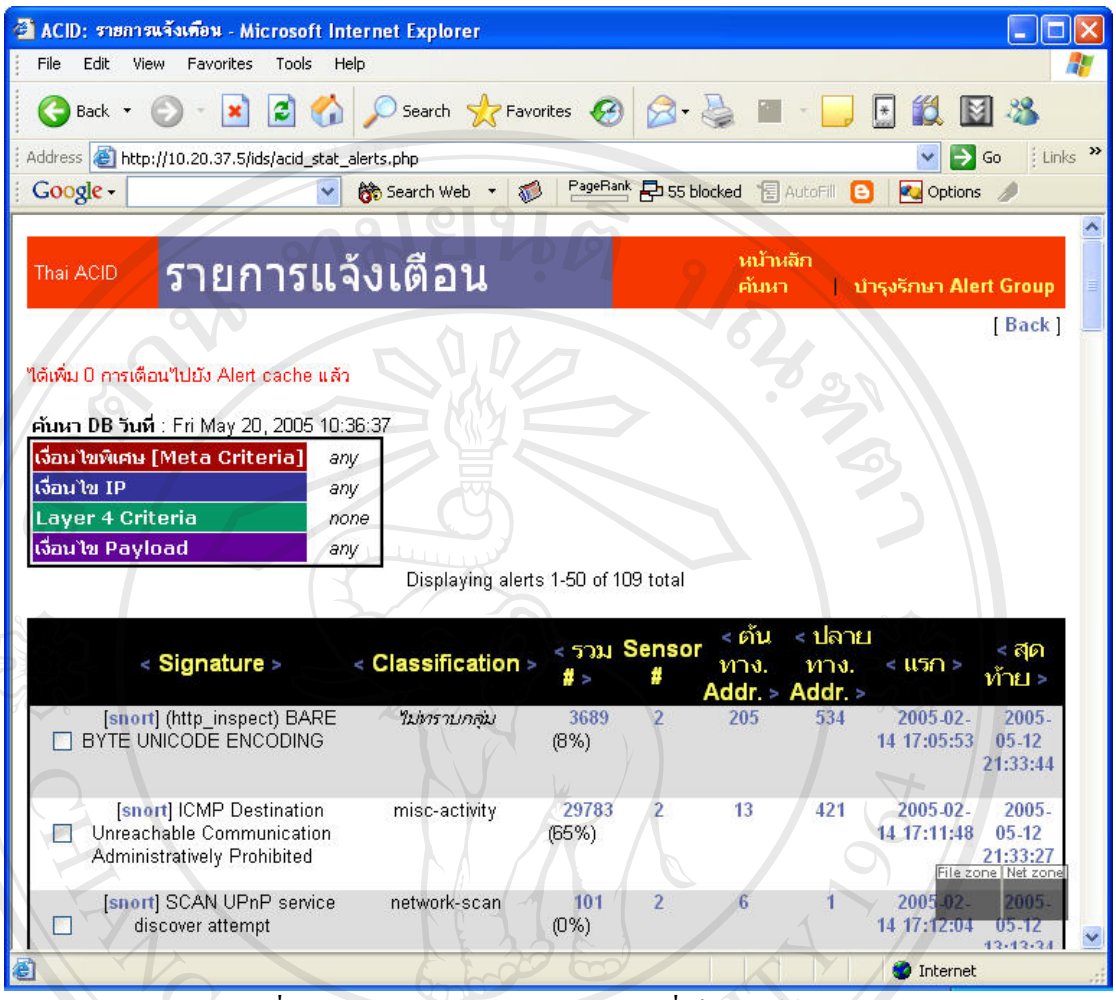
รูปที่ ข.4 แสดงหน้าจอหลักของการรายงานผลการบุกรุกเครือข่าย

จากรูปที่ ข.4 จะแสดงข้อมูลในภาพรวมการบุกรุกโดยแบ่งตามปริมาณการถูกบุกรุกตามโปรโตคอล 3 โปรโตคอลหลักได้แก่ TCP, UDP และ ICMP และทำการสรุปยอดการแจ้งเตือนทั้งหมดแยกเป็นการแจ้งเตือนที่ไม่ซ้ำกัน นอกจากนั้นยังแยกรายงานไอพีแอดเดรส ต้นทางที่บุกรุกไปยังไอพีเป้าหมายหรือปลายทาง รวมถึงเรื่องของพอร์ตที่ใช้เชื่อมต่อด้วย



รูปที่ ข.5 แสดงข้อมูลการตรวจจับจากเครื่องเซ็นเซอร์ที่กำหนดไว้

จากรูปที่ ข.5 จะแสดงข้อมูลสรุปจำนวนเหตุการณ์ละเมิดกฎที่เซ็นเซอร์แต่ละตัวทำการตรวจสอบโดยแสดงจำนวนที่เซ็นเซอร์แต่ละตัวทำการตรวจจับได้



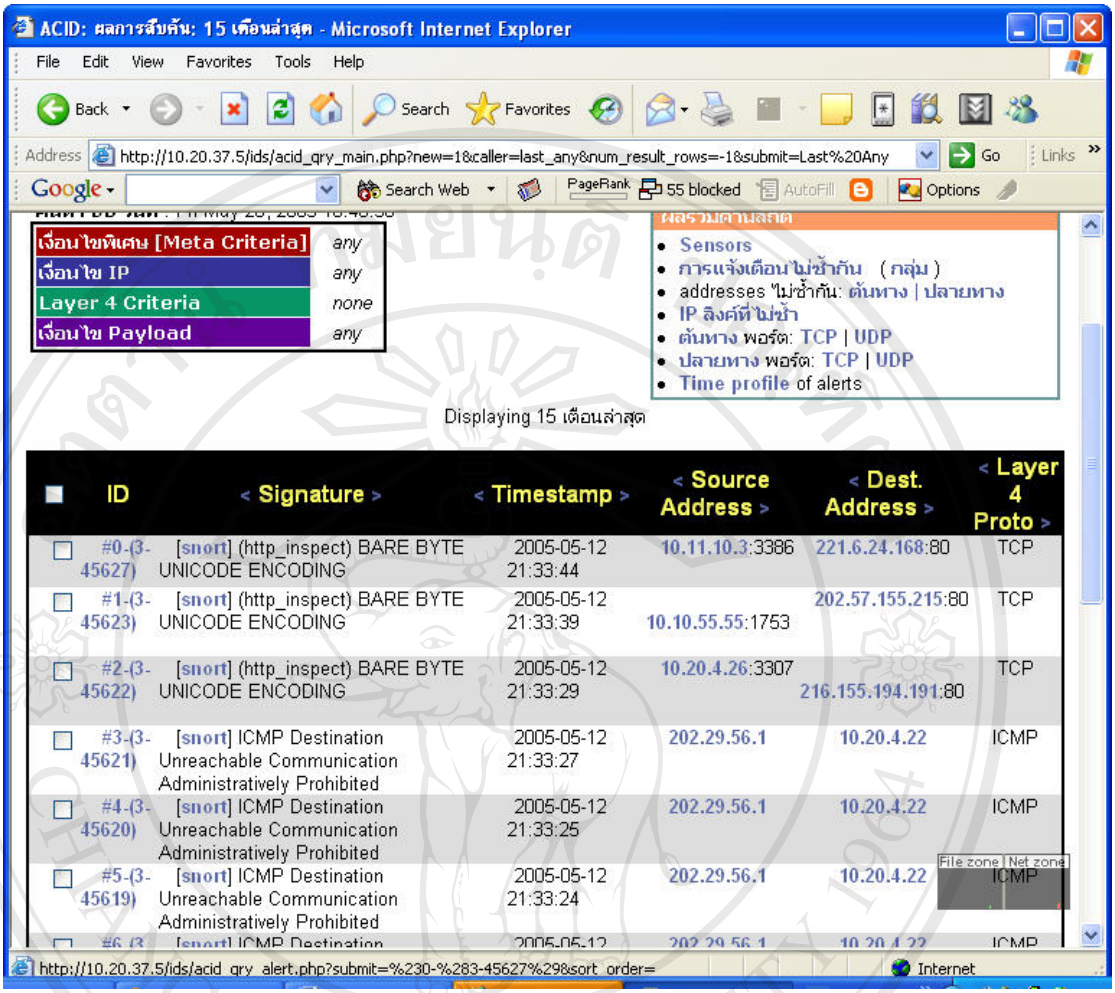
รูปที่ ข.6 แสดงข้อมูลรายการแจ้งเตือนที่เซ็นเซอร์ตรวจพบ

จากรูปที่ ข.6 เป็นการแสดงข้อมูลการบุกรุกที่เซ็นเซอร์ตรวจพบโดยแต่ละส่วนมีความหมายดังนี้

1. Signature เป็นรูปแบบของการบุกรุกที่ตรวจพบ
2. Classification เป็นประเภทของการบุกรุก
3. รวม# เป็นจำนวนรวมที่ตรวจพบ
4. Sensor# เป็นจำนวนเซ็นเซอร์ที่ตรวจพบ
5. ต้นทาง Addr เป็นจำนวนหมายเลขไอพีแอดเดรสที่พบว่ามีการทำผิดกฎ
6. ปลายทาง Addr เป็นจำนวนหมายเลขไอพีแอดเดรสเป้าหมายที่มีการติดต่อจากไอพีแอดเดรสต้นทาง

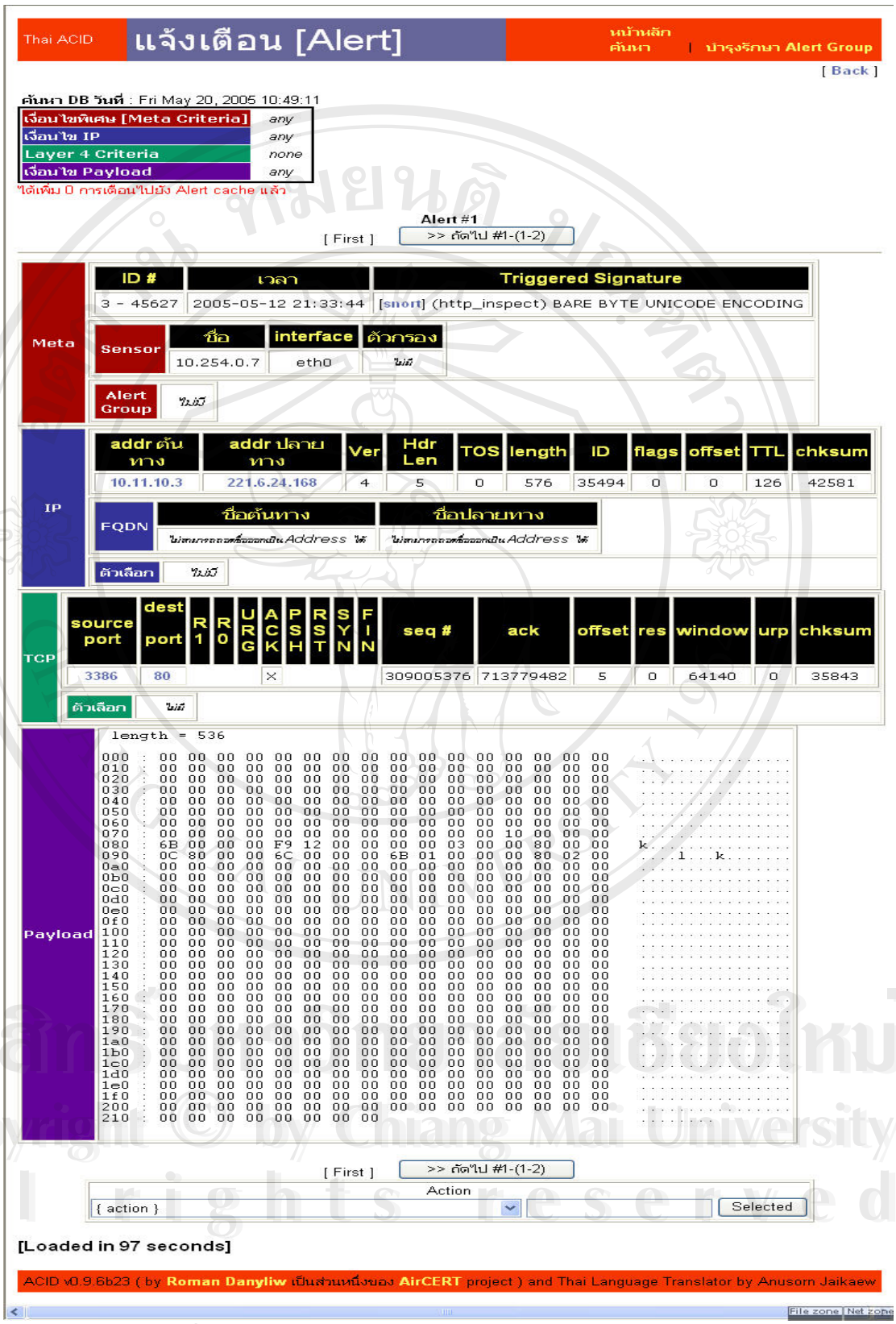
7 แรก เป็นเวลาเริ่มต้นของการตรวจพบ

8 สุดท้าย เป็นเวลาที่ตรวจพบครั้งสุดท้าย



รูปที่ ข.7 แสดงรายผลการแจ้งเตือนล่าสุด 15 รายการ

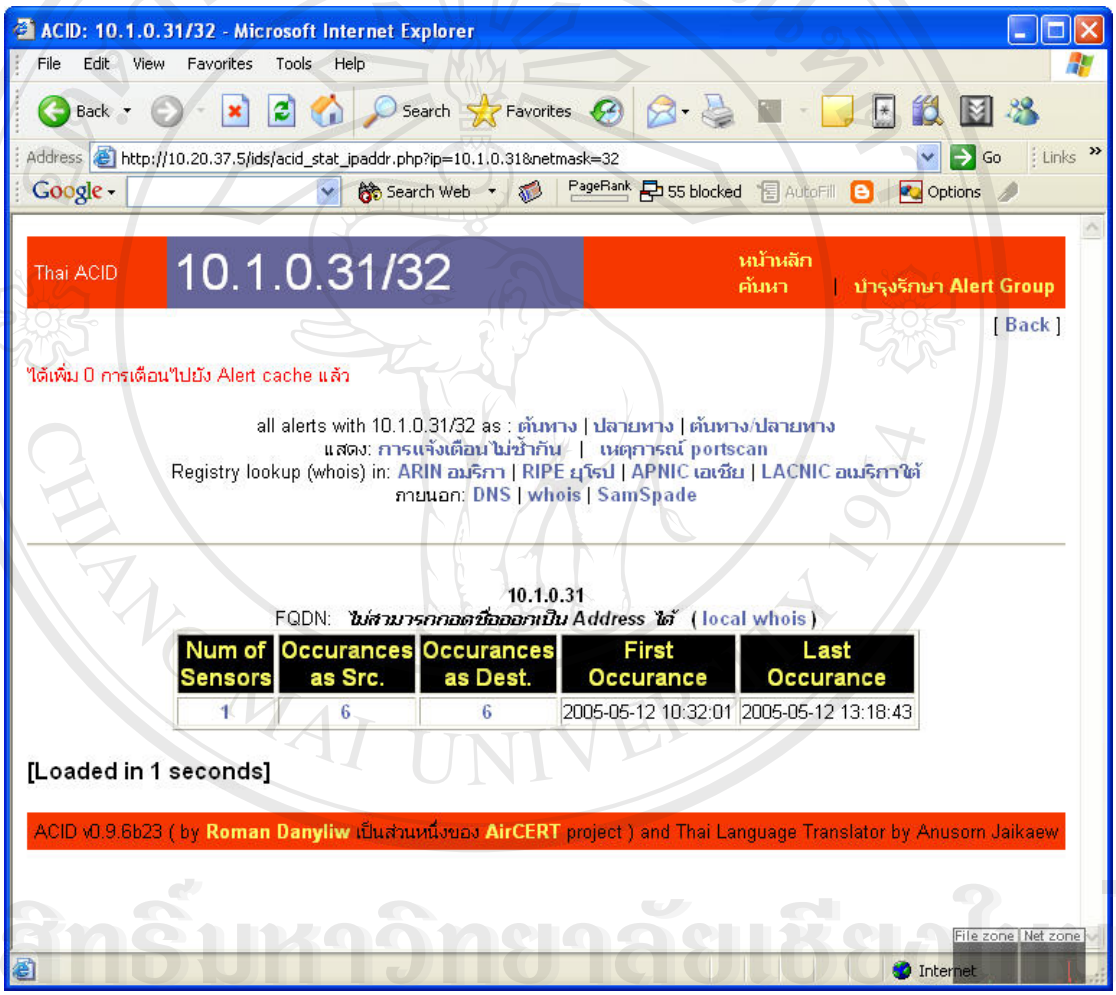
จากรูปที่ ข.7 จะมีข้อมูลการบุกรุกล่าสุด 15 รายการ โดยทำการแสดงรายละเอียดรูปแบบการบุกรุก เวลาที่ตรวจพบไอพีแอดเดรสที่มีแนวโน้มการละเมิดกฎ (Source Address) และไอพีแอดเดรสเป้าหมาย (Dest. Address) ที่อาจถูกละเมิดและประเภทของโปรโตคอล (Layer4 proto)



รูปที่ ข.8 แสดงรายละเอียดของข้อมูลของการบุกรุกแต่ละรายการ

จากรูปที่ ข.8 จะแสดงรายอะเอียดของข้อมูล โดยแยกเป็นสามส่วนคือ

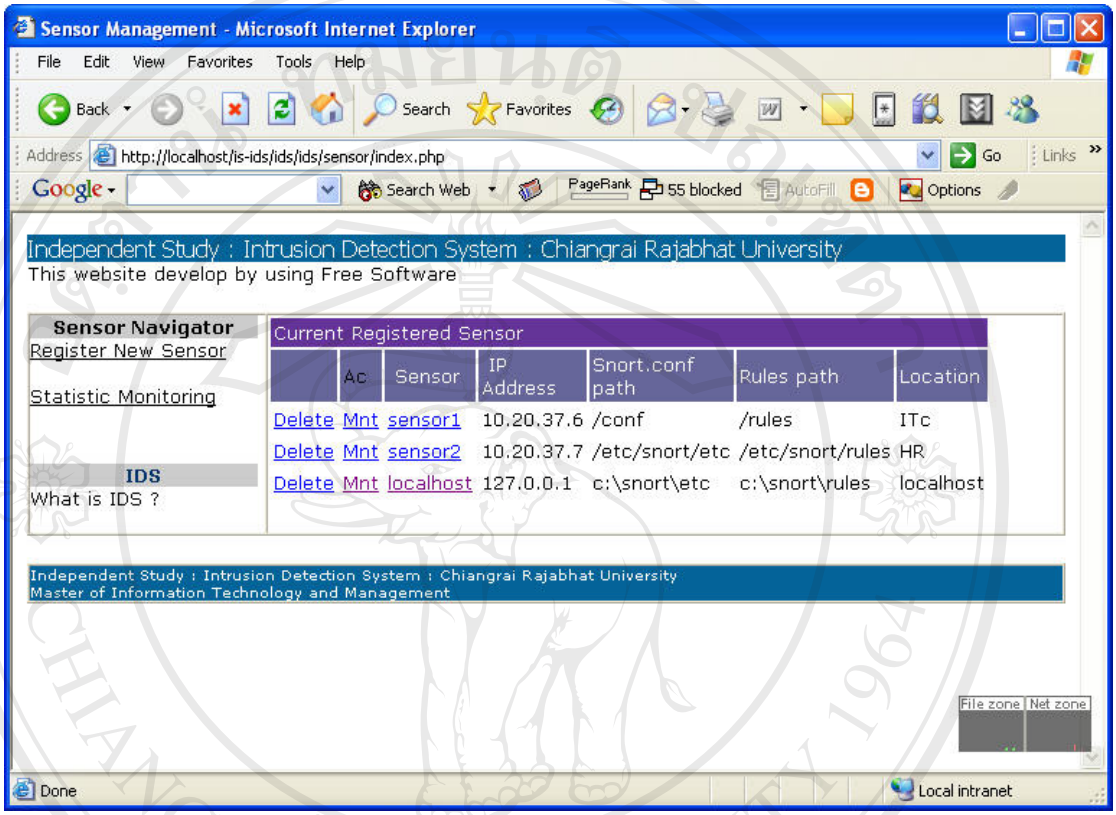
1. Meta เป็นส่วนของข้อมูลทั่วไปเช่น เซ็นเซอร์ที่ตรวจจับได้
2. IP เป็นข้อมูลในส่วนของ IP โปรโตคอล
3. TCP เป็นข้อมูลในส่วนของ TCP โปรโตคอล
4. Payload เป็นข้อมูลที่ใช้ในการส่งไปยังเครื่องปลายทาง



รูปที่ ข.9 แสดงข้อมูลสรุปของเครื่องคอมพิวเตอร์ที่ทำผิดกฎในการตรวจสอบ

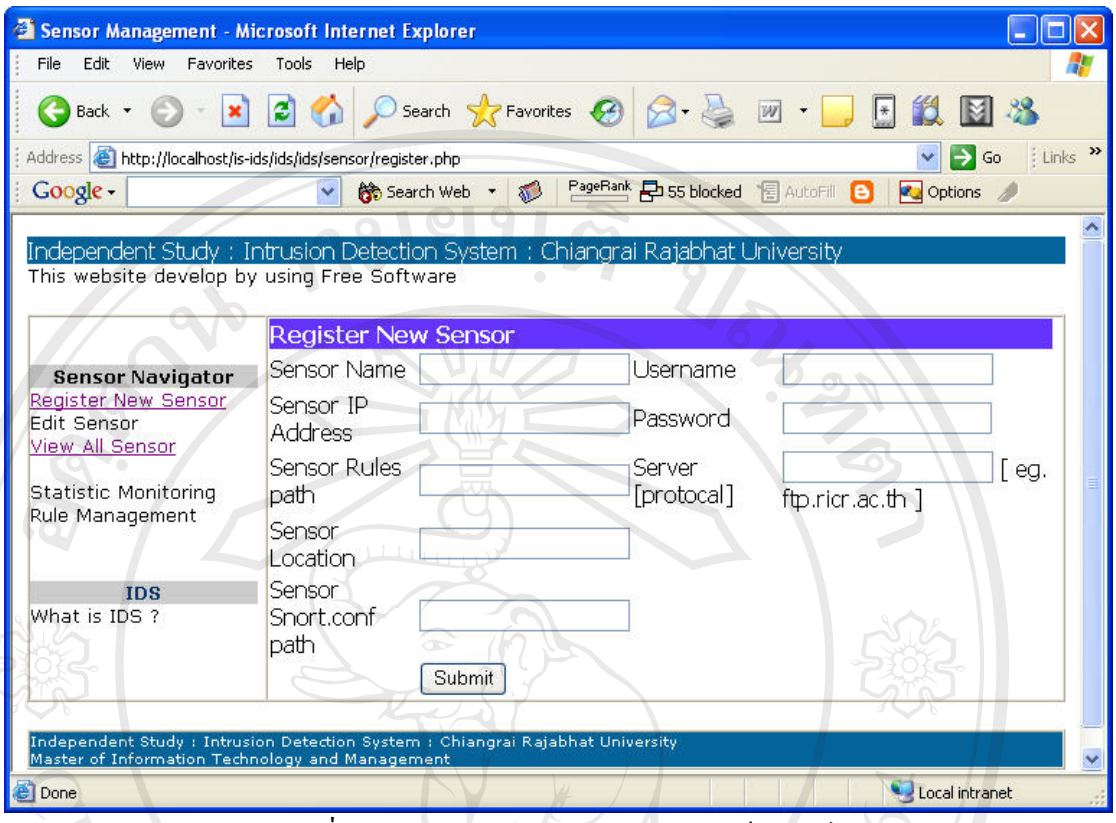
จากรูปที่ ข.9 จะทำการแสดงข้อมูลสรุปของเครื่องคอมพิวเตอร์ที่ทำผิดกฎที่ตั้งไว้ในการตรวจสอบของเซ็นเซอร์ โดยสามารถตรวจสอบได้ว่าเป็นไอพีแอดเดรสที่มาจากที่ใดในโลก แยกตามทวีปคือ อเมริกา ยุโรป เอเชีย และ อเมริกาใต้

ข.4 วิธีการใช้งานระบบจัดการเรื่องกฎการตรวจสอบการบุกรุก



รูปที่ ข.10 แสดงหน้าจอหลักในการจัดการเซ็นเซอร์

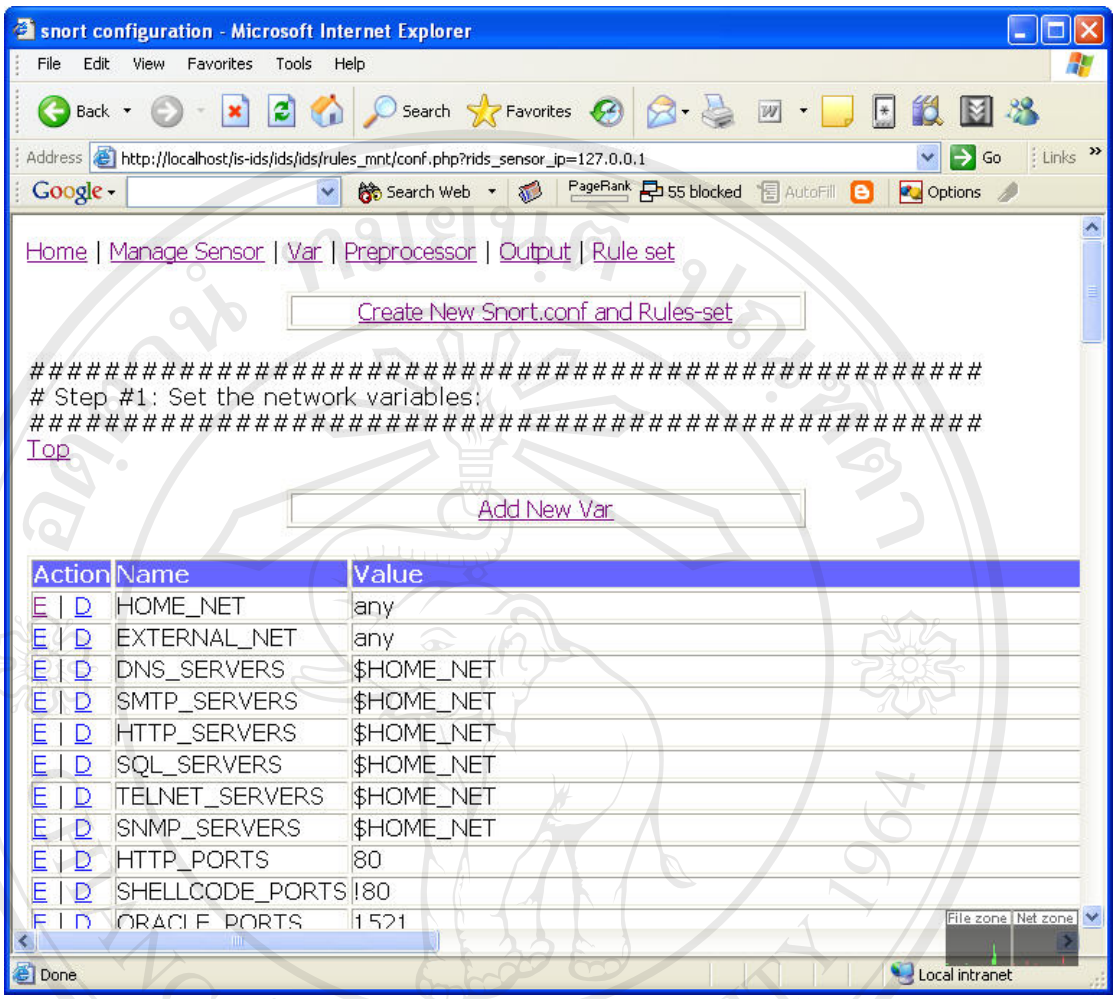
จากรูปที่ ข.10 ได้แสดงข้อมูลเกี่ยวกับเครื่องเซ็นเซอร์ที่ได้ลงทะเบียนไว้ในระบบ เพื่อทำการตรวจจับการบุกรุกเครือข่าย โดยเมื่อต้องการจัดการเกี่ยวกับกฎของเซ็นเซอร์ใดก็ตามต้องทำการลงทะเบียนเซ็นเซอร์นั้นก่อน โดยคลิกที่ Register New Sensor จะปรากฏดังรูปที่ ข.10



รูปที่ ข. 11 แสดงหน้าจอการลงทะเบียนเซ็นเซอร์

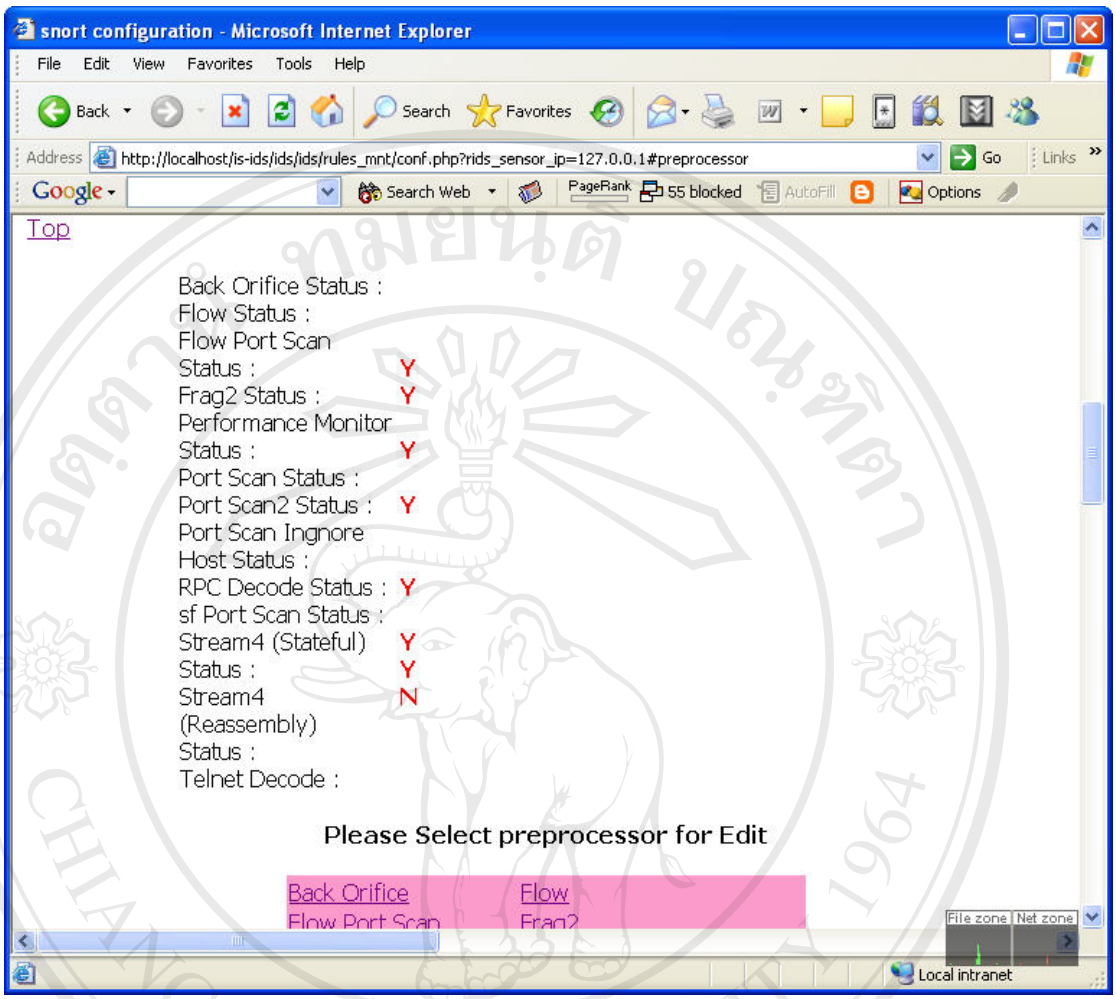
จากรูปที่ ข.11 แสดงหน้าจอการลงทะเบียนมีรายละเอียดดังนี้

1. Sensor Name คือการกำหนดชื่อเรียกของ เซ็นเซอร์
2. Sensor IP Address คือหมายเลขไอพีแอดเดรสของเครื่องเซ็นเซอร์
3. Sensor Rules path คือตำแหน่งของไฟล์ *.rules ในเครื่องเซ็นเซอร์
4. Sensor Location คือตำแหน่งที่ตั้งของ เซ็นเซอร์
5. Sensor Snort.conf path คือตำแหน่งที่ไฟล์ snort.conf ในเครื่องเซ็นเซอร์
6. Username คือชื่อผู้มีสิทธิในการเข้าถึงไฟล์ *.rules และ snort.conf
7. Password คือรหัสสำหรับผู้มีสิทธิในการเข้าถึงไฟล์ *.rules และ snort.conf
8. Server Protocal คือวิธีการเข้าถึงเครื่องเซ็นต์เซอร์ปลายทาง



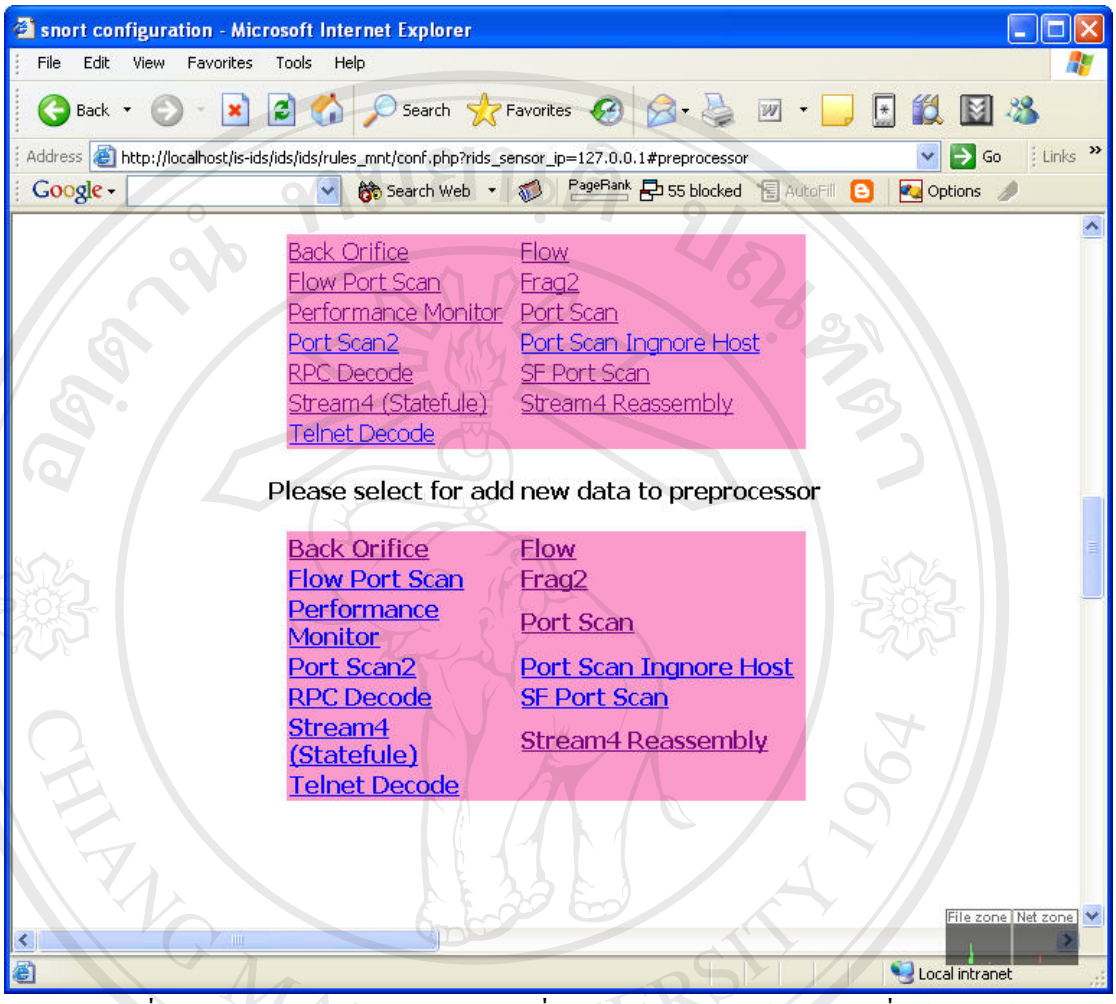
รูปที่ ข.12 แสดงข้อมูลตัวแปรไฟล์ snort.conf ของเซ็นเซอร์

จากรูปที่ ข.12 แสดงข้อมูลตัวแปรจากไฟล์ snort.conf ที่ทำการดึงจากเครื่องเซ็นเซอร์เพื่อนำมาปรับแก้ไข เมื่อคลิกที่ E คือการแก้ไขข้อมูล และ D สำหรับการ ลบข้อมูล



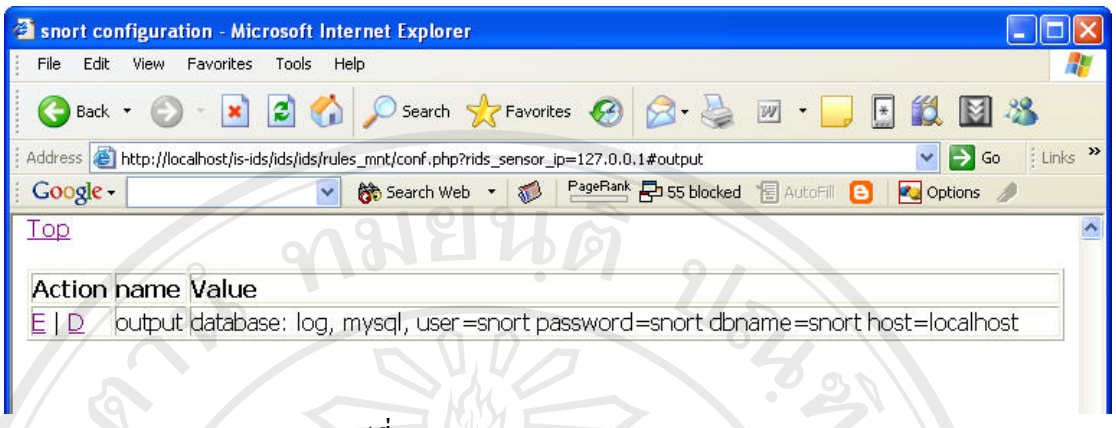
รูปที่ ข.13 แสดงสถานะของ preprocessor

จากรูปที่ ข.13 แสดงสถานะของ preprocessor โดย Y แสดงถึงมีการใช้งาน preprocessor และ N หมายถึงไม่มีการใช้งาน ส่วน preprocessor ที่ไม่มีสถานะ หมายถึงยังไม่ได้มีการกำหนดค่าใดๆ ในการใช้งาน



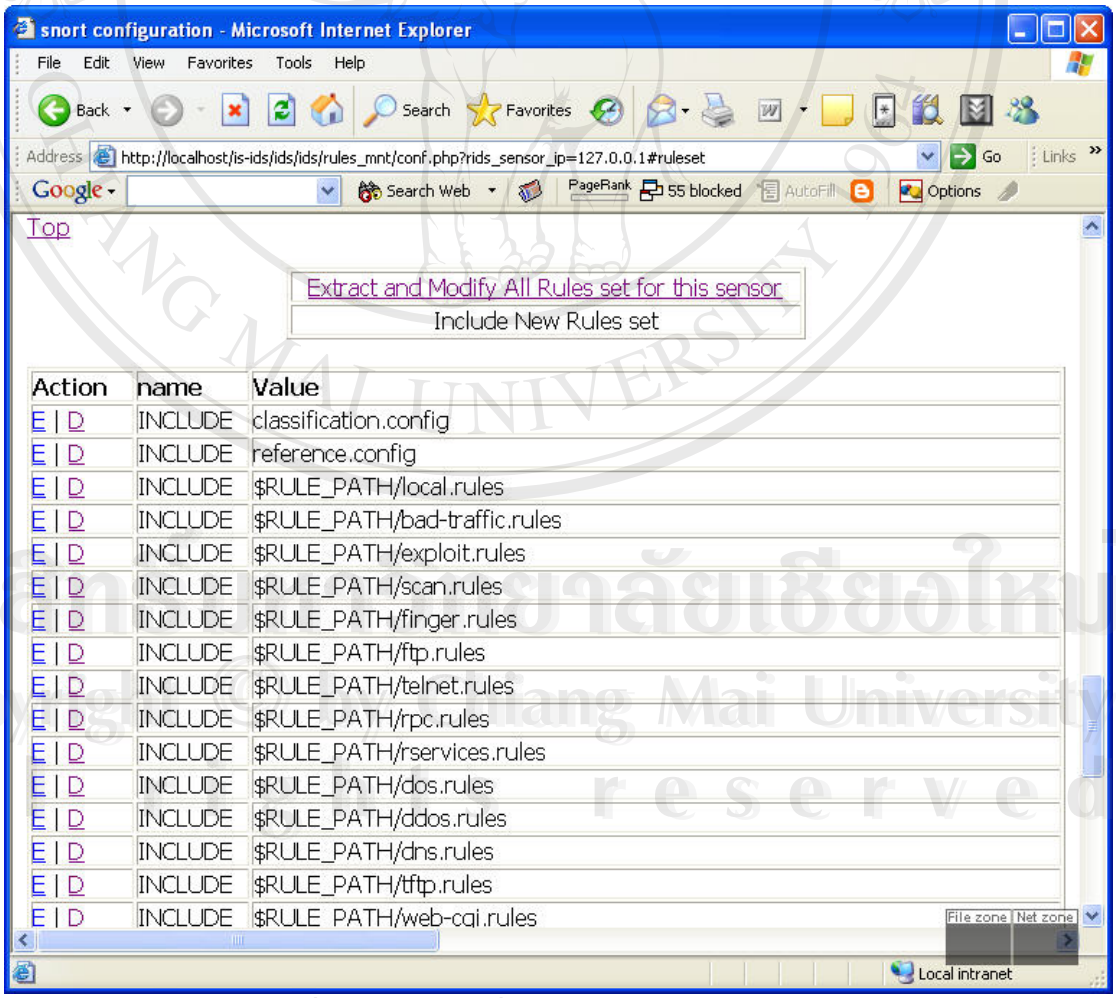
รูปที่ ข.14 แสดงรายการ preprocessor ที่มีอยู่โดยสามารถแก้ไข หรือ เพิ่มข้อมูลได้

จากรูปที่ ข. 14 ได้แยกส่วนของ preprocessor ออกเป็นสองส่วนได้แก่ ส่วนแรกเป็นการแก้ไขข้อมูลของ preprocessor ส่วนที่สองเป็นการเพิ่มข้อมูลเข้าไปใหม่สำหรับ preprocessor



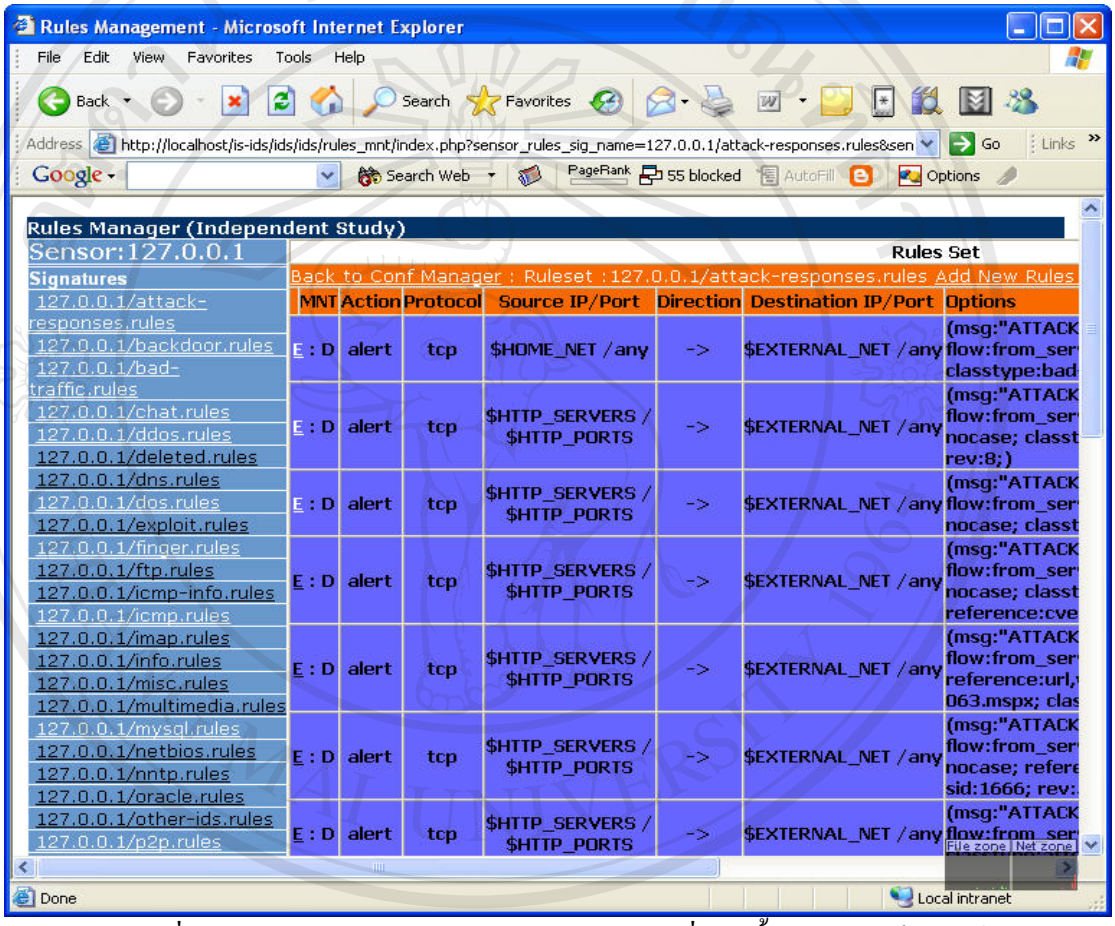
รูปที่ ข.15 แสดงการกำหนด output log

จากรูปที่ ข. 15 แสดงการกำหนด output log เพื่อกำหนดการจัดเก็บข้อมูลไปยังฐานข้อมูลที่กำหนดไว้



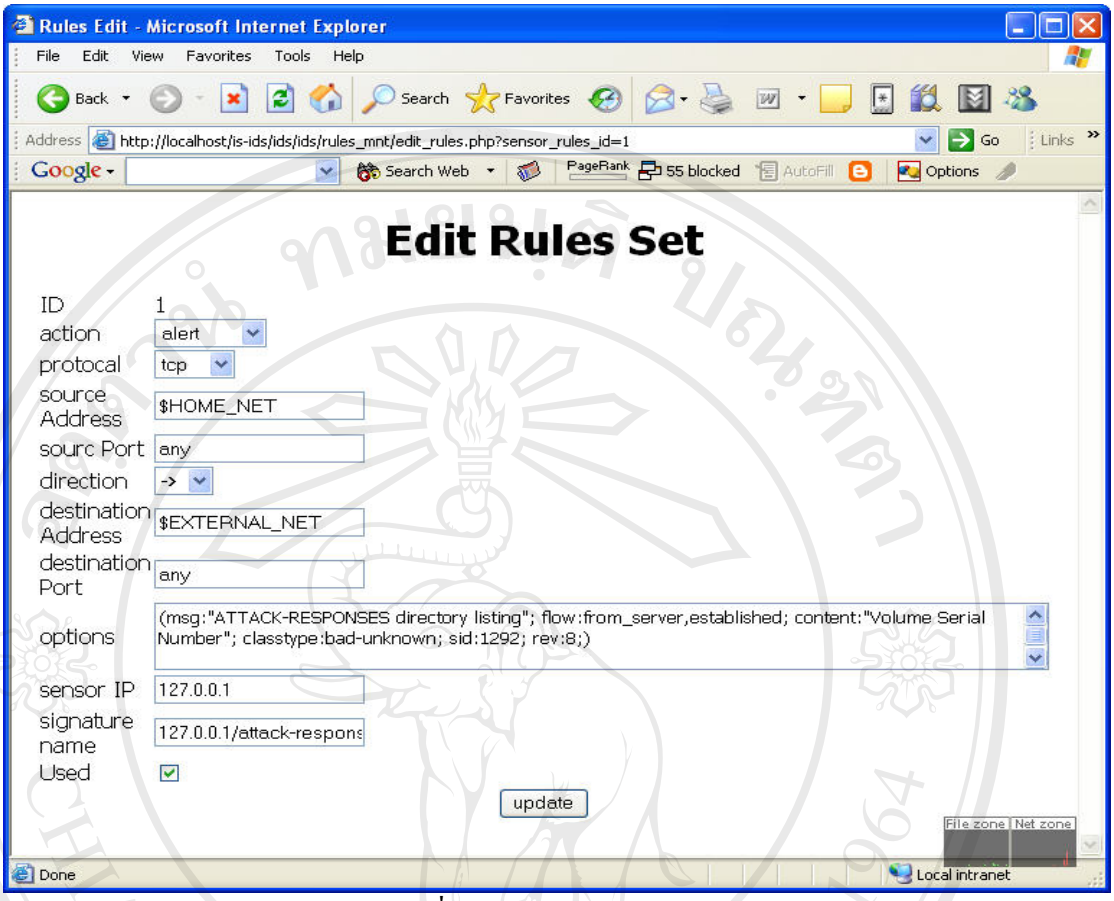
รูปที่ ข.16 แสดงกฎที่มีการเลือกใช้ในการตรวจสอบ

จากรูปที่ ข. 16 แสดงกฎต่างๆ ที่มีการเลือกใช้อยู่ในปัจจุบันในการตรวจสอบเราสามารถเปลี่ยนแปลงแก้ไขหรือลบกฎเหล่านี้ได้โดยคลิกที่ E สำหรับการแก้ไข และ D สำหรับการลบ



รูปที่ ข.17 แสดงหน้าจอรายละเอียดของกฎต่างๆ ที่มีอยู่ทั้งหมดของเซ็นเซอร์

จากรูปที่ ข. 17 แสดงหน้าจอของกฎต่างๆ ที่มีอยู่ทั้งหมดของเซ็นเซอร์โดยด้านซ้ายมือคือชื่อของรูปแบบการบุกรุก (Signature) ด้านขวามือคือรายละเอียดของกฎต่างๆที่ใช้ในรูปแบบการบุกรุก



รูปที่ ข.18 แสดงการแก้ไขกฎ

จากรูปที่ ข.18 แสดงการแก้ไขรูปแบบการของกฎ โดยมีรายละเอียดดังนี้

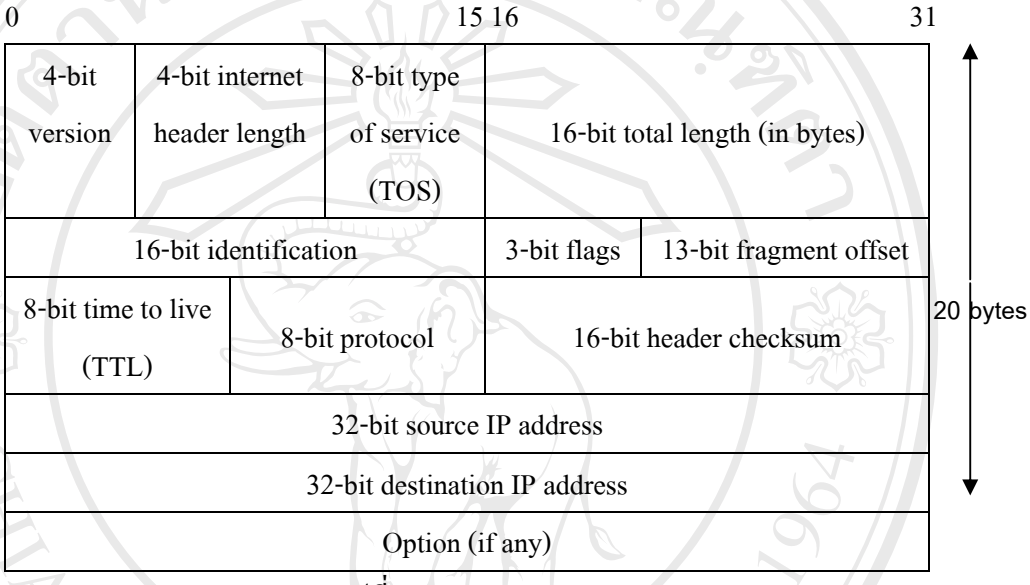
1. action คือรูปแบบของการแจ้งเตือน
2. protocol คือประเภทของโปรโตคอลที่ต้องการตรวจสอบ
3. source address คือไอพีที่ต้องการตรวจสอบซึ่งสามารถใส่ในรูปแบบของตัวแปรที่ได้กำหนดไว้ได้
4. source port คือพอร์ตที่ต้องการพิจารณา
5. direction คือทิศทางที่ต้องการตรวจสอบข้อมูล
6. destination address คือไอพีปลายทางที่ต้องการให้ตรวจสอบ
7. destination port คือพอร์ตปลายทางที่ต้องการตรวจสอบ
8. options คือส่วนอธิบายให้กฎทำงาน
9. sensor ip คือ หมายเลขไอพีของเครื่องเซ็นเซอร์
10. singnature name คือชื่อของกฎที่ใช้ในการตรวจสอบ
11. Used หมายถึงต้องการให้กฎนี้ใช้ในการตรวจสอบด้วยหรือไม่

ภาคผนวก ค

ส่วนประกอบต่างๆในส่วนหัวของแพ็กเก็ต

ค.1 IP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc791.txt



รูปที่ ค.1 IP Packet Header

IP Packet Header Field	Description
Version	The Version field indicates the format of the internet header. This document describes version 4.
IHL	Internet Header Length is the length of the internet header in 32 bit words, and thus points to the beginning of the data. Note that the minimum value for a correct header is 5.
Type of Service	The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic (generally by accepting only traffic above a certain precedence at time of high load). The major choice is

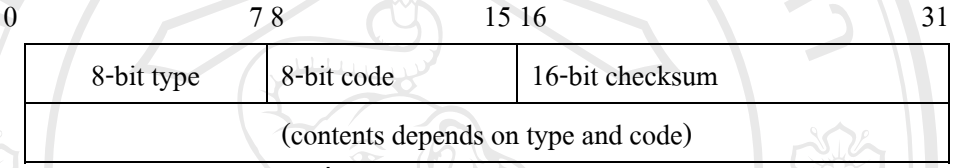
	a three way tradeoff between low-delay, high-reliability, and high-throughput. Bits 0-2: Precedence. Bit 3: 0 = Normal Delay, 1 = Low Delay. Bits 4: 0 = Normal Throughput, 1 = High Throughput. Bits 5: 0 = Normal Relibility, 1 = High Relibility. Bit 6-7: Reserved for Future Use. Precedence 111 - Network Control 110 - Internetwork Control 101 - CRITIC/ECP 100 - Flash Override 011 - Flash 010 - Immediate 001 - Priority 000 - Routine
Total Length	Total Length is the length of the datagram, measured in octets, including internet header and data. This field allows the length of a datagram to be up to 65,535 octets.
Identification	An identifying value assigned by the sender to aid in assembling the fragments of a datagram.
Flags	Various Control Flags. Bit 0: reserved, must be zero. Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment. Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.
Fragment Offset	This field indicates where in the datagram this fragment belongs.
Time to Live	This field indicates the maximum time the datagram is allowed to remain in the internet system. If this field contains the value zero, then the datagram must be destroyed. This field is modified in internet header processing. The time is measured in units of seconds, but since every module that processes a datagram must decrease the TTL by at least one even if it process the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram may exist. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime.
Protocol	This field indicates the next level protocol used in the data portion of the internet datagram.
Header Checksum	A checksum on the header only. Since some header fields change

	(e.g., time to live), this is recomputed and verified at each point that the internet header is processed.
Source Address	The source address.
Destination Address	The destination address.

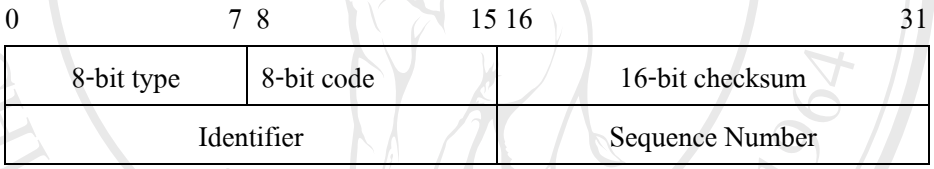
ตารางที่ ค.1 IP Packet Header Fields

ค.2 ICMP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc792.txt



รูปที่ ค.2 Basic ICMP Packet Header



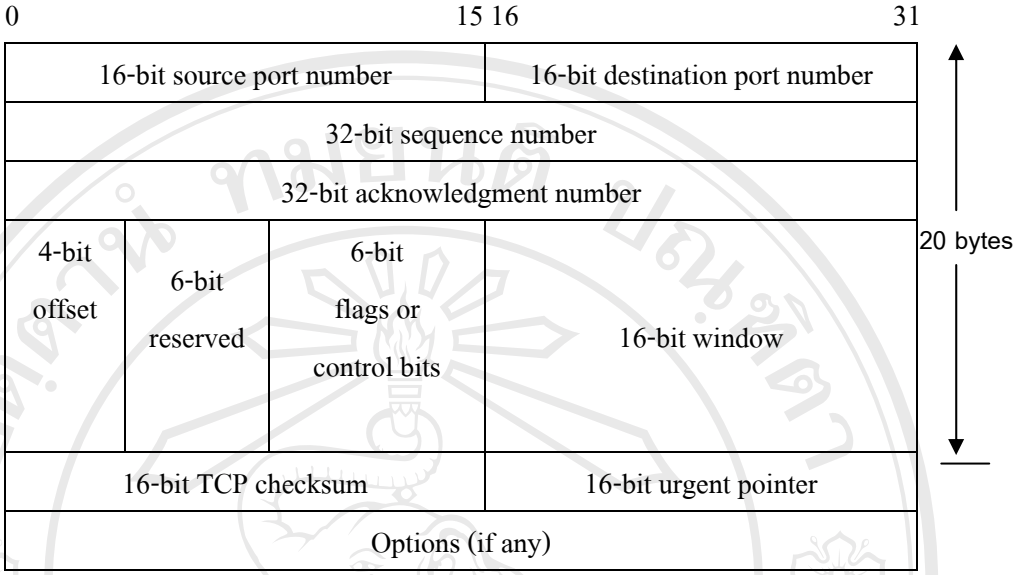
รูปที่ ค.3 ICMP Packet Header used in ping command.

ICMP Packet Header Field	Description
Type	Show type of ICMP packet.
Code	Show the sub-type of code number used for the packets. 0 = net unreachable; 1 = host unreachable; 2 = protocol unreachable; 3 = port unreachable; 4 = fragmentation needed and DF set; 5 = source route failed.
Checksum	Use to detect any errors in the ICMP packet.
Identifier	If code = 0, an identifier to aid in matching echos and replies, may be zero.
Sequence Number	If code = 0, a sequence number to aid in matching echos and replies, may be zero.

ตารางที่ ค.2 ICMP Packet Header Fields

ค.3 TCP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc793.txt



รูปที่ ค.4 TCP Packet Header

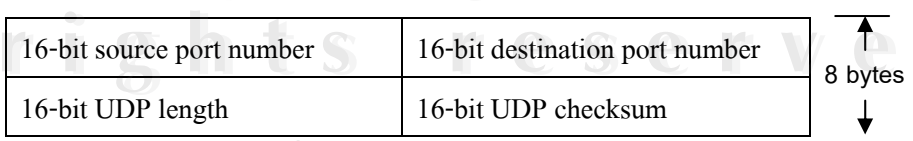
ตารางที่ ค.3 TCP Packet Header Fields

TCP Packet Header Field	Description
Source Port	Source port number.
Destination Port	The destination port number.
Sequence Number	The sequence number of the first data octet in this segment (except when SYN is present). If SYN is present the sequence number is the initial sequence number (ISN) and the first data octet is ISN+1.
Acknowledgment Number	If the ACK control bit is set this field contains the value of the next sequence number the sender of the segment is expecting to receive. Once a connection is established this is always sent.
Data Offset	The number of 32 bit words in the TCP Header. This indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits long.
Reserved	Reserved for future use. Must be zero.
Control Bits	URG: Urgent Pointer field significant ACK: Acknowledgment field significant

	PSH: Push Function RST: Reset the connection SYN: Synchronize sequence numbers FIN: No more data from sender
Window	The number of data octets beginning with the one indicated in the acknowledgment field which the sender of this segment is willing to accept. Tell th other side about the length of TCP window size.
Checksum	A checksum for TCP header and data.
Urgent Pointer	This field communicates the current value of the urgent pointer as a positive offset from the sequence number in this segment. The urgent pointer points to the sequence number of the octet following the urgent data. This field is only be interpreted in segments with the URG control bit set.
Options	Options may occupy space at the end of the TCP header and are a multiple of 8 bits in length. All options are included in the checksum. An option may begin on any octet boundary. There are two cases for the format of an option: Case 1: A single octet of option-kind. Case 2: An octet of option-kind, an octet of option-length, and the actual option-data octets. The option-length counts the two octets of option-kind and option-length as well as the option-data octets.

ค.4 UDP Packet Header

ที่มา : http://www.rfc-editor.org/rfc/rfc768.txt



รูปที่ ค.5 UDP Packet Header

ตารางที่ ค.4 UDP Packet Header Fields

UDP Packet Header Field	Description
Source Port	An optional field, when meaningful, it indicates the port of the sending process, and may be assumed to be the port to which a reply should be addressed in the absence of any other information. If not used, a value of zero is inserted.
Destination Port	Internet destination port address.
Length	Length is the length in octets of this user datagram including this header and the data. (This means the minimum value of the length is eight.)
Checksum	Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort

acid_ag

Field	Type	Null	Default
ag_id	int(10)	No	
ag_name	varchar(40)	Yes	*NULL*
ag_desc	text	Yes	*NULL*
ag_ctime	datetime	Yes	*NULL*
ag_ltime	datetime	Yes	*NULL*

acid_ag_alert

Field	Type	Null	Default
ag_id	int(10)	No	0
ag_sid	int(10)	No	0
ag_cid	int(10)	No	0

acid_event

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
signature	int(10)	No	0

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

sig_name	varchar(255)	Yes	*NULL*
sig_class_id	int(10)	Yes	*NULL*
sig_priority	int(10)	Yes	*NULL*
timestamp	datetime	No	0000-00-00 00:00:00
ip_src	int(10)	Yes	*NULL*
ip_dst	int(10)	Yes	*NULL*
ip_proto	int(11)	Yes	*NULL*
layer4_sport	int(10)	Yes	*NULL*
layer4_dport	int(10)	Yes	*NULL*

acid_ip_cache

Field	Type	Null	Default
ipc_ip	int(10)	No	0
ipc_fqdn	varchar(50)	Yes	*NULL*
ipc_dns_timestamp	datetime	Yes	*NULL*
ipc_whois	text	Yes	*NULL*
ipc_whois_timestamp	datetime	Yes	*NULL*

conf

Field	Type	Null	Default
conf_id	smallint(6)	No	
conf_date	datetime	No	0000-00-00 00:00:00
conf_ip	varchar(15)	No	
conf_name	varchar(50)	No	
conf_value	varchar(200)	No	
conf_type	varchar(15)	No	
conf_detail	varchar(50)	Yes	*NULL*
conf_used	enum('Y', 'N')	No	Y

data

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
data_payload	text	Yes	*NULL*

detail

Field	Type	Null	Default
detail_type	tinyint(3)	No	0
detail_text	text	No	

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

encoding

Field	Type	Null	Default
encoding_type	tinyint(3)	No	0
encoding_text	text	No	

event

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
signature	int(10)	No	0
timestamp	datetime	No	0000-00-00 00:00:00

icmphdr

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
icmp_type	tinyint(3)	No	0
icmp_code	tinyint(3)	No	0
icmp_csum	smallint(5)	Yes	*NULL*
icmp_id	smallint(5)	Yes	*NULL*
icmp_seq	smallint(5)	Yes	*NULL*

iphdr

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
ip_src	int(10)	No	0
ip_dst	int(10)	No	0
ip_ver	tinyint(3)	Yes	*NULL*
ip_hlen	tinyint(3)	Yes	*NULL*
ip_tos	tinyint(3)	Yes	*NULL*
ip_len	smallint(5)	Yes	*NULL*
ip_id	smallint(5)	Yes	*NULL*
ip_flags	tinyint(3)	Yes	*NULL*
ip_off	smallint(5)	Yes	*NULL*
ip_ttl	tinyint(3)	Yes	*NULL*
ip_proto	tinyint(3)	No	0
ip_csum	smallint(5)	Yes	*NULL*

opt

Field	Type	Null	Default

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

sid	int(10)	No	0
cid	int(10)	No	0
optid	int(10)	No	0
opt_proto	tinyint(3)	No	0
opt_code	tinyint(3)	No	0
opt_len	smallint(6)	Yes	*NULL*
opt_data	text	Yes	*NULL*

pre_back_orifice

Field	Type	Null	Default
pre_back_orifice_used	enum('Y', 'N')	No	Y
pre_back_orifice_sensor	varchar(13)	No	

pre_flow

Field	Type	Null	Default
pre_flow_id	tinyint(4)	No	
pre_flow_memcap	varchar(5)	Yes	*NULL*
pre_flow_rows	varchar(5)	Yes	*NULL*
pre_flow_statInterval	varchar(5)	Yes	*NULL*
pre_flow_hash	varchar(5)	Yes	*NULL*
pre_flow_used	enum('Y', 'N')	Yes	*NULL*
pre_flow_sensor	varchar(13)	No	

pre_flow_portscan

Field	Type	Null	Default
pre_flow_portscan_id	tinyint(4)	No	
pre_flow_portscan_scoreBoard_memcapTalker	varchar(15)	Yes	*NULL*
pre_flow_scoreBoard_rowsTalker	varchar(15)	Yes	*NULL*
pre_flow_portscan_scoreBoard_rowsScanner	varchar(30)	Yes	*NULL*
pre_flow_portscan_scoreBoard_memcapScanner	varchar(15)	Yes	*NULL*
pre_flow_portscan_scanner_fixedThreshold	varchar(10)	Yes	*NULL*
pre_flow_portscan_scanner_slidingThreshold	varchar(10)	Yes	*NULL*
pre_flow_portscan_scanner_fixedWindows	varchar(10)	Yes	*NULL*
pre_flow_portscan_scanner_slidingWindows	varchar(10)	Yes	*NULL*
pre_flow_portscan_scanner_slidingScaleFactor	varchar(10)	Yes	*NULL*
pre_flow_portscan_talker_fixedThreshold	varchar(10)	Yes	*NULL*
pre_flow_portscan_talker_slidingThreshold	varchar(10)	Yes	*NULL*
pre_flow_portscan_talker_fixedWindows	varchar(10)	No	
pre_flow_portscan_talker_slidingWindows	varchar(10)	No	
pre_flow_portscan_talker_slidingScaleFactor	varchar(10)	Yes	*NULL*
pre_flow_portscan_server_memCap	varchar(20)	Yes	*NULL*
pre_flow_portscan_server_rows	varchar(10)	Yes	*NULL*

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

pre_flow_portscan_server_watchnet	varchar(10)	Yes	*NULL*
pre_flow_portscan_server_learningTime	varchar(10)	Yes	*NULL*
pre_flow_portscan_server_IngnoreLimit	varchar(10)	Yes	*NULL*
pre_flow_portscan_server_scannerLimit	varchar(10)	Yes	*NULL*
pre_flow_portscan_misc_uniqueMemCap	varchar(10)	Yes	*NULL*
pre_flow_portscan_misc_uniqueRows	varchar(10)	Yes	*NULL*
pre_flow_portscan_misc_sourceIngnoreNet	varchar(10)	Yes	*NULL*
pre_flow_portscan_misc_dstIngnoreNet	varchar(10)	Yes	*NULL*
pre_flow_portscan_misc_tcppenalties	enum('on', 'off')	Yes	*NULL*
pre_flow_portscan_misc_alertMode	enum('once', 'all')	Yes	*NULL*
pre_flow_portscan_outputMode	enum('msg', 'pktkludge')	Yes	*NULL*
pre_flow_portscan_used	enum('Y', 'N')	Yes	Y
pre_flow_portscan_sensor	varchar(13)	No	

pre_frag2

Field	Type	Null	Default
pre_frag2_id	tinyint(4)	No	
pre_frag2_timeOut	varchar(5)	Yes	*NULL*
pre_frag2_memUsage	varchar(10)	Yes	*NULL*
pre_frag2_ttlLimit	varchar(5)	Yes	*NULL*
pre_frag2_minimumTTL	varchar(5)	Yes	*NULL*
pre_frag2_detectState	enum('Y', 'N')	Yes	*NULL*
pre_frag2_used	enum('Y', 'N')	Yes	*NULL*
pre_frag2_sensor	varchar(13)	No	

pre_performance_monitor

Field	Type	Null	Default
pre_perform_monitor_id	tinyint(4)	No	
pre_perform_monitor_packetCount	varchar(10)	Yes	*NULL*
pre_perform_monitor_file	varchar(30)	Yes	*NULL*
pre_perform_monitor_time	varchar(10)	Yes	*NULL*
pre_perform_monitor_console	enum('Y', 'N')	Yes	*NULL*
pre_perform_monitor_events	enum('Y', 'N')	Yes	*NULL*
pre_perform_monitor_max	enum('Y', 'N')	Yes	*NULL*
pre_perform_monitor_flow	enum('Y', 'N')	Yes	*NULL*
pre_perform_monitor_used	enum('Y', 'N')	Yes	*NULL*
pre_perform_monitor_sensor	varchar(13)	No	

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

pre_portscan

Field	Type	Null	Default
pre_portscan_id	tinyint(4)	No	
pre_portscan_numofport	varchar(5)	No	
pre_portscan_interval	varchar(5)	No	
pre_portscan_localIP	varchar(30)	No	
pre_portscan_logFiles	varchar(30)	No	
pre_portscan_used	enum('Y', 'N')	No	Y
pre_portscan_sensor	varchar(13)	No	

pre_portscan2

Field	Type	Null	Default
pre_portscan2_id	tinyint(4)	No	0
pre_portscan2_scannersMax	char(3)	Yes	*NULL*
pre_portscan2_targetsMax	char(3)	Yes	*NULL*
pre_portscan2_targetLimit	char(3)	Yes	*NULL*
pre_portscan2_portLimit	char(3)	Yes	*NULL*
pre_portscan2_timeOut	char(3)	Yes	*NULL*
pre_portscan2_used	enum('Y', 'N')	Yes	*NULL*
pre_portscan2_sensor	varchar(13)	No	

pre_portscan_ingnorehost

Field	Type	Null	Default
pre_portscan_ingnorehost_id	tinyint(4)	No	
pre_portscan_ingnorehost_host	varchar(25)	No	
pre_portscan_ingnorehost_used	enum('Y', 'N')	No	Y
pre_portscan_ingnorehost_sensor	varchar(13)	No	

pre_rpc_decode

Field	Type	Null	Default
pre_rpc_decode_id	tinyint(4)	No	
pre_rpc_decode_port	varchar(20)	Yes	*NULL*
pre_rpc_decode_alertFragment	enum('Y', 'N')	Yes	*NULL*
pre_rpc_decode_NOmar	enum('Y', 'N')	Yes	*NULL*
pre_rpc_decode_NOarf	enum('Y', 'N')	Yes	*NULL*

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

pre_rpc_decode_NOai	enum('Y', 'N')	Yes	*NULL*
pre_rpc_decode_used	enum('Y', 'N')	Yes	*NULL*
pre_rpc_decode_sensor	varchar(13)	No	

pre_sfportscan

Field	Type	Null	Default
pre_sfportscan_id	tinyint(4)	No	
pre_sfportscan_protocal	varchar(20)	Yes	*NULL*
pre_sfportscan_scanType	varchar(50)	Yes	*NULL*
pre_sfportscan_sensitivity	varchar(10)	Yes	*NULL*
pre_sfportscan_memcap	varchar(15)	Yes	*NULL*
pre_sfportscan_watchIP	varchar(50)	Yes	*NULL*
pre_sfportscan_IgnoreScanner	varchar(50)	Yes	*NULL*
pre_sfportscan_IgnoreScanned	varchar(50)	Yes	*NULL*
pre_sfportscan_LogFiles	varchar(50)	Yes	*NULL*
pre_sfportscan_used	tinyint(4)	Yes	*NULL*
pre_sfportscan_sensor	varchar(13)	No	

pre_stream4_reassembly

Field	Type	Null	Default
pre_stream4_reassembly_id	tinyint(4)	No	
pre_stream4_reassembly_type	enum('clientonly', 'serveronly')	Yes	*NULL*
pre_stream4_reassembly_noalert	enum('Y', 'N')	Yes	*NULL*
pre_stream4_reassembly_port	varchar(6)	Yes	*NULL*
pre_stream4_reassembly_used	enum('Y', 'N')	Yes	*NULL*
pre_stream4_reassembly_sensor	varchar(13)	No	

pre_stream4_stateful

Field	Type	Null	Default
pre_stream4_stateful_id	tinyint(4)	No	
pre_stream4_stateful_disable	enum('Y', 'N')	No	Y
pre_stream4_stateful_detectScan	enum('Y', 'N')	No	Y
pre_stream4_stateful_detectState	enum('Y', 'N')	No	Y
pre_stream4_stateful_disableEvation	enum('Y', 'N')	No	Y

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

pre_stream4_stateful_midStream	enum('Y', 'N')	Yes	*NULL*
pre_stream4_stateful_enforceState	enum('Y', 'N')	Yes	*NULL*
pre_stream4_stateful_keepStat	varchar(50)	Yes	*NULL*
pre_stream4_stateful_timeOut	varchar(5)	Yes	*NULL*
pre_stream4_stateful_memUsage	varchar(5)	Yes	*NULL*
pre_stream4_stateful_ttlLimit	varchar(5)	Yes	*NULL*
pre_stream4_stateful_used	enum('Y', 'N')	Yes	*NULL*
pre_stream4_stateful_sensor	varchar(13)	No	

pre_telnet_decode

Field	Type	Null	Default
pre_telnet_decode_id	tinyint(4)	No	
pre_telnet_decode_port	varchar(5)	Yes	*NULL*
pre_telnet_decode_used	enum('Y', 'N')	Yes	*NULL*
pre_telnet_decode_sensor	varchar(13)	No	

reference

Field	Type	Null	Default
ref_id	int(10)	No	
ref_system_id	int(10)	No	0
ref_tag	text	No	

reference_system

Field	Type	Null	Default
ref_system_id	int(10)	No	
ref_system_name	varchar(20)	Yes	*NULL*

rids_sensor

Field	Type	Null	Default
rids_sensor_id	smallint(6)	No	
rids_sensor_name	varchar(50)	No	
rids_sensor_ip	varchar(50)	No	
rids_sensor_rules_path	varchar(50)	No	
rids_sensor_location	varchar(50)	No	
rids_sensor_snort_conf	varchar(50)	No	
rids_sensor_username	varchar(50)	No	
rids_sensor_password	varchar(50)	No	
rids_sensor_upload	varchar(50)	No	

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

schema

Field	Type	Null	Default
vseq	int(10)	No	0
ctime	datetime	No	0000-00-00 00:00:00

sensor

Field	Type	Null	Default
sid	int(10)	No	
hostname	text	Yes	*NULL*
interface	text	Yes	*NULL*
filter	text	Yes	*NULL*
detail	tinyint(4)	Yes	*NULL*
encoding	tinyint(4)	Yes	*NULL*
last_cid	int(10)	No	0

sensor_rules

Field	Type	Null	Default
sensor_rules_id	int(11)	No	
sensor_rules_action	varchar(15)	No	
sensor_rules_protocal	varchar(4)	No	
sensor_rules_srcAddr	varchar(30)	No	
sensor_rules_srcPort	varchar(11)	No	
sensor_rules_direction	char(2)	No	
sensor_rules_dstAddr	varchar(30)	No	
sensor_rules_dstPort	varchar(11)	No	
sensor_rules_options	varchar(255)	No	
sensor_rules_ip	varchar(13)	No	
sensor_rules_sig_name	varchar(50)	No	
sensor_rules_used	enum('Y', 'N')	Yes	Y

sig_class

Field	Type	Null	Default
sig_class_id	int(10)	No	
sig_class_name	varchar(60)	No	

sig_reference

Field	Type	Null	Default
sig_id	int(10)	No	0
ref_seq	int(10)	No	0

ตารางที่ ค.5 แสดงพจนานุกรมข้อมูลในฐานข้อมูล snort (ต่อ)

ref_id	int(10)	No	0

signature

Field	Type	Null	Default
sig_id	int(10)	No	
sig_name	varchar(255)	No	
sig_class_id	int(10)	No	0
sig_priority	int(10)	Yes	*NULL*
sig_rev	int(10)	Yes	*NULL*
sig_sid	int(10)	Yes	*NULL*

tcphdr

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
tcp_sport	smallint(5)	No	0
tcp_dport	smallint(5)	No	0
tcp_seq	int(10)	Yes	*NULL*
tcp_ack	int(10)	Yes	*NULL*
tcp_off	tinyint(3)	Yes	*NULL*
tcp_res	tinyint(3)	Yes	*NULL*
tcp_flags	tinyint(3)	No	0
tcp_win	smallint(5)	Yes	*NULL*
tcp_csum	smallint(5)	Yes	*NULL*
tcp_urp	smallint(5)	Yes	*NULL*

udphdr

Field	Type	Null	Default
sid	int(10)	No	0
cid	int(10)	No	0
udp_sport	smallint(5)	No	0
udp_dport	smallint(5)	No	0
udp_len	smallint(5)	Yes	*NULL*
udp_csum	smallint(5)	Yes	*NULL*

ค.5 แสดงรายชื่อไฟล์ในโปรแกรม แสดงผล ACID ที่สามารถปรับแต่งการแสดงผลเป็นภาษาไทยได้

acid_ag_common.php	acid_ag_main.php	acid_app_faq.php
acid_common.php	acid_conf.php	acid_db_common.php

acid_db_setup.php	acid_graph_common.php	acid_graph_display.php
acid_graph_form.php	acid_graph_main.php	acid_main.php
acid_maintenance.php	acid_qry_alert.php	acid_qry_common.php
acid_qry_form.php	acid_qry_main.php	acid_qry_sqlcalls.php
acid_stat_alerts.php	acid_stat_class.php	acid_stat_common.php
acid_stat_ipaddr.php	acid_stat_iplink.php	acid_stat_ports.php
acid_stat_sensor.php	acid_stat_time.php	acid_stat_uaddr.php
acid_action.inc	acid_cache.inc	acid_constants.inc
acid_db.inc	acid_include.inc	acid_log_error.inc
acid_log_timing.inc	acid_net.inc	acid_output_html.inc
acid_output_query.inc	acid_signature.inc	acid_state_citems.inc
acid_state_common.inc	acid_state_criteria.inc	acid_state_query.inc

ประวัติผู้เขียน

ชื่อ นายอนุสรณ์ ใจแก้ว

วัน เดือน ปี เกิด 6 มิถุนายน 2519

เบอร์โทรติดต่อ 0-6670-7246

จดหมายอิเล็กทรอนิกส์

anusorn@cru.in.th

ประวัติการศึกษา

วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ สถาบันราชภัฏเชียงราย ปีการศึกษา 2541

ประสบการณ์

พ.ศ. 2542 – ปัจจุบัน นักวิชาการคอมพิวเตอร์ สำนักบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเชียงราย