ระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์บนฟรีบีเอสดี

NETWORK INTRUSION PREVENTION SYSTEM USING FREEBSD

โดย

กมล ขุทรานนท์

KAMON KHUTTARANON

อาจารย์ที่ปรึกษา

ผศ. อัครินทร์ คุณกิตติ

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ภาคเรียนที่ 1 ปีการศึกษา 2551

NETWORK INTRUSION PREVENTION SYSTEM USING FREEBSD

KAMON KHUTTARANON

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/ 2008

ใบรับรองโครงการพัฒนาระบบงาน (SYSTEM DEVELOPMENT PROJECT)

เรื่อง

ระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์บนฟรีบีเอสดี

NETWORK INTRUSION PREVENTION SYSTEM USING FREEBSD

นายกมล ขุทรานนท์

รหัสประจำตัว 49066403

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ

การศึกษาวิชาโครงการพัฒนาระบบงาน หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)

ภาคเรียนที่ 1 ปีการศึกษา 2551

.....อาจารย์ที่ปรึกษา

(ผศ. อัครินทร์ คุณกิตติ)

.....กรรมการสอบ

(รศ.ดร. นพพร โชติกกำธร)

.....กรรมการสอบ

(ผศ.ดร. จันทร์บูรณ์ สถิตวิริยวงศ์)

หัวข้อ	ระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์บนฟรีบีเอสดี
นักศึกษา	นายกมล ขุทรานนท์
รหัสนักศึกษา	49066403
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2551
อาจารย์ที่ปรึกษา	ผศ. อัครินทร์ คุณกิตติ

บทคัดย่อ

เนื่องจากระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญ และได้พัฒนาไม่หยุดยั้ง ทำให้ส่งผลต่อการบุกรุกต่อเครือข่าย ดังนั้นจึงมีแนวคิดที่จะพัฒนาระบบที่สามารถตรวจสอบและป้องกันการบุกรุกเครือข่ายบนระบบปฏิบัติการฟรีบีเอสดี การทำงานอยู่ในรูปคำสั่งแบบตัวอักษร (Command Line) จัดการได้ยาก จึงได้พัฒนาให้สามารถจัดการได้ง่ายผ่านทางเว็บเบสยูสเซอร์อินเทอร์เฟส โดยอาศัยเทคโนโลยีการตรวจจับการบุกรุกของสนอร์ท และการป้องกันการบุกรุกของไฟร์วอลล์ จากนั้นศึกษาการทำงานของสนอร์ทกับไฟร์วอลล์บนฟรีบีเอสดี ออกแบบให้สามารถใช้ข้อมูลการดักจับแพ็กเก็ตของสนอร์ทจัดเก็บลงฐานข้อมูล พัฒนาให้สามารถจัดการกฎไฟร์วอลล์ได้ผ่านทางเว็บเบสยูสเซอร์อินเทอร์เฟส ใช้ภาษา PHP ในการพัฒนา และเชื่อมต่อกับฐานข้อมูลของสนอร์ท โดยใช้โปรแกรม MySQL เป็นระบบฐานข้อมูล และใช้ Apache เป็นเว็บเซิร์ฟเวอร์ที่สามารถเรียกใช้ได้ผ่านเว็บเบสยูสเซอร์อินเทอร์เฟส ในการวิเคราะห์แบบจำลองเชิงแนวคิดของระบบได้อาศัยการวิเคราะห์ และออกแบบเชิงโครงสร้าง (Structured Analysis and Design) แบ่งออกเป็น 3 ส่วน คือ แผนภาพกระแสข้อมูล (Data flow diagrams) นำมาใช้ในการอธิบายกระแสข้อมูล แผนภาพกิจกรรม (Activity diagram) นำมาใช้ในการแสดงกิจกรรมการทำงานของระบบ และแผนภาพความสัมพันธ์ของเอ็นติตี้ (Entity-relationship diagram) ใช้เป็นแผนผังแสดงความสัมพันธ์ระหว่างเอ็นติตี้ หรือกลุ่มของข้อมูล

การพัฒนาระบบได้สร้างส่วนของการติดต่อผู้ใช้งานแบบเว็บให้สามารถแสดงการวิเคราะห์การเตือนง่ายขึ้นด้วยการแบ่งรายละเอียดการเตือน การค้นหาข้อมูลการเตือน การกำหนดกฎออกแบบให้สามารถสร้างกฎให้กับไฟร์วอลล์ และสร้างกฎสำหรับตรวจสอบของสนอร์ทเบื้องต้น นอกจากนี้ยังสามารถเรียกดูกฎที่เคยสร้าง สำรอง และกู้คืนกฎ ในการพัฒนาโครงการนี้ได้ทดสอบการทำงานแล้วสามารถทำงานได้จริง ยังขาดส่วนย้อนกลับของสนอร์ทที่ส่งถึงไฟร์วอลล์ สามารถเรียกดูการเตือนเพื่อใช้วิเคราะห์ระบบ แล้วกำหนดกฎป้องกันการบุกรุกของไฟร์วอลล์ผ่านเว็บเบสยูสเซอร์อินเทอร์เฟส เพื่อควบคุมการป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

Title	NETWORK INTRUSION PREVENTION SYSTEM USING FREEBSD
Student	Mr. Kamon Khuttaranon
Student ID.	49066403
Degree	Master of Science
Programme	Information Science
Academic Year	2008
Advisor	Asst. Prof. Akharin Khunkitti

ABSTRACT

Since Computer network and Internet is used to basic of network and it is developed continuously, thus it maybe impact to network because of intrusion. So we have come up with the idea to develop system that is based-component of intrusion detection system and intrusion prevention system and it is on FreeBSD. System management is used by command line that it is not easy to use. So Simplify Network Intrusion Prevention System to manage and analyze packets with configuration on web site and to learning process of Snort (Intrusion detection System) and IPFIREWALL (IPFW or Intrusion Prevention System) using FreeBSD. System is designed to capture packet to Snort database that it will be used to analyze packet before control firewall by using Web-based user interface. The graphic user interface is based on web-based development by PHP, Database is MySQL database and Web server is Apache server. In analysis model concept of tool, we use the Structured Analysis and Design to explain development of our tool by splitting into 3 parts. First, Data flow diagrams are used to explain overall flow of data. Second, Activity diagrams are used to analyze activity of tool. Third, Entity-relationship diagrams are used to analyzes entity of tool

This system development is designed with web user interface that's easy to analyze alerts by splitting detail of alerts. Our can search information of alerts and create basic rules of firewall and snort. By the way, our can see old rules, backup rules and recovery rules. The Project can work with successfully but it hasn't feedbacked of snort to control firewall. This Project can use to analyze alerts, control rules and create rules of firewall that it can use in the real world and it is based on control efficiency.

กิตติกรรมประกาศ

โครงงานพัฒนาระบบงานนี้เกิดขึ้นและสำเร็จลุล่วงไปได้ด้วยดี ผู้จัดทำโครงงานขอกราบขอบพระคุณ ผู้ช่วยศาสตราจารย์ อัครินทร์ คุณกิตติ ซึ่งเป็นอาจารย์ที่ปรึกษาโครงงานที่ได้กรุณาเสียสละเวลาอันมีค่าในการให้คำแนะนำและแนวคิดในการจัดทำโครงงาน และให้คำปรึกษาด้านวิชาการที่เป็นประโยชน์ในการทำโครงงานและให้ความช่วยเหลือด้านอื่นๆ ด้วยการดูแลเอาใจใส่ตลอดการทำโครงงานเสมอมา ผู้จัดทำมีความซาบซึ้งในความกรุณาเป็นอย่างยิ่ง จึงขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้

ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ ที่ให้กำเนิด ให้การศึกษา ให้กำลังใจและเป็นแรงผลักดันให้ผู้จัดทำมีกำลังใจที่จะมุ่งมั่นในการศึกษาครั้งนี้จนเป็นผลสำเร็จลุล่วงด้วยดี

และขอบคุณเพื่อนๆที่ให้คำแนะนำต่างๆ

นายกมล ขุทรานนท์

ตุลาคม 2551

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

รูปที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาของโครงการ

ระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญ และได้พัฒนาไม่หยุดยั้ง ส่งผลให้เกิดการบุกรุกในรูปแบบต่างๆ ดังนั้นการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ (Network Security) เป็นเรื่องที่ต้องมาควบคู่กันกับการจัดการระบบเครือข่ายคอมพิวเตอร์ โดยการกำหนดนโยบายการรักษาความปลอดภัยการให้บริการต่างๆ ของระบบเครือข่ายฯ เพื่อป้องกันการเข้าใช้งานที่อาจเกิดการบุกรุกต่อระบบเครือข่ายคอมพิวเตอร์ จำเป็นอย่างยิ่งที่จะต้องมีระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ (Network IPS-Network Intrusion Prevention System) ในการช่วยตรวจสอบและป้องกันการบุกรุกในรูปแบบต่างๆ เช่น การใช้งานระบบเครือข่ายฯ ที่ไม่ปกติ และการพยายามโจมตีระบบเครือข่ายคอมพิวเตอร์เพื่อให้ไม่สามารถใช้งานได้ตามปกติ เป็นต้น การทำงานของระบบป้องกันการบุกรุกเครือข่ายบนระบบปฏิบัติการ ฟรีบีเอสดี มักอยู่ในรูปแบบ command line ทำให้การจัดการไม่สะดวก

ด้วยเหตุผลดังกล่าวข้างต้น ได้ตระหนักถึงความสำคัญของการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เป็นอย่างยิ่ง ทำให้ต้องมีการเตรียมการรับมือกับการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ ด้วยการจัดหาระบบป้องกันการบุกรุกระบบเครือข่าย (Network IPS – Network Intrusion Prevention System) ที่มีประสิทธิภาพเพื่อป้องกันระบบเครือข่ายภายใน ให้มีความปลอดภัยและปลอดจากการบุกรุกต่างๆ เพื่อสร้างเครื่องข่ายที่มีความปลอดภัยและมีประสิทธิภาพสูงสุด โดยอาศัยเทคโนโลยีการรักษาความปลอดภัยของ สนอร์ท กับไฟร์วอลล์ พัฒนาบนระบบปฏิบัติการ ฟรีบีเอสดี และเพื่อที่จะสามารจัดการระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ ได้มีประสิทธิภาพและง่ายในการติดตั้งเพื่อใช้งาน จึงได้มีแนวคิดที่จะพัฒนาส่วนติดต่อผู้ใช้แบบเว็บสำหรับช่วยในการควบคุมการทำงานและการสร้างกฎของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ บน ระบบปฏิบัติการ ฟรีบีเอสดี ให้ใช้งานง่าย อีกทั้งสามารถทำการสำรองข้อมูลกฎก่อนที่จะมีการเปลี่ยนแปลงแก้ไขและสามารถเรียกกฎที่ได้มีการติดตั้งไว้ใช้งานอยู่เดิมก่อนมีการแก้ไขกลับขึ้นมาใช้งานใหม่ได้

1.2 เป้าหมายในการพัฒนาระบบ

เนื่องจากการใช้งานจัดการกับระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ บนระบบปฏิบัติการ ฟรีบีเอสดี ที่มีอยู่เดิมเป็นการทำงานโดยการใช้การป้อนคำสั่งในลักษณะ Command line และConfiguration file จึงทำให้เกิดความยุ่งยากต่อการเรียกใช้งาน ดังนั้นระบบที่จะมีการพัฒนาขึ้นมาใหม่จะเป็นระบบที่มีการรองรับการใช้งานโดยที่ผู้ใช้สามารถที่จะเรียกใช้ระบบการติดตั้งกฎผ่านเว็บและทำการติดตั้งคำสั่งโดยการป้อนเพียงข้อมูลที่จำเป็นต่อระบบทำให้จัดการได้ง่าย สะดวกต่อการเรียกใช้หรือการติดตั้งกฎ สามารถเรียกดูกฎทั้งหมดที่ได้ทำการติดตั้งไว้แล้วได้ รวมทั้งยังสามารถทำการสำรองข้อมูลกฎก่อนที่จะมีการเปลี่ยนแปลงแก้ไข สามารถเรียกกฎที่ได้มีการติดตั้งไว้ใช้งานอยู่เดิมก่อนมีการแก้ไขกลับขึ้นมาใช้งานใหม่ และเรียกดูล็อกการเตือนได้

1.3 ขอบเขตในการพัฒนาระบบ

พัฒนาโปรแกรมให้สามารถกำหนดกฎของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์บนฟรีบีเอสดี โดยมีขอบเขตพัฒนาดังนี้

- ออกแบบส่วนติดต่อกับสนอร์ทและไฟร์วอลล์บนฟรีบีเอสดี โดยออกแบบให้สนอร์ทมีการเก็บการเตือนและล็อกการใช้งานไว้ในฐานข้อมูล และไฟร์วอลล์ สามารถควบคุมการเข้าใช้งานเครือข่าย และการออกใช้งานนอกเครือข่าย
- พัฒนา Web User Interface เป็นส่วนติดต่อกับผู้ใช้ที่ใช้งานง่ายผ่านทางเว็บที่พัฒนาโดยภาษา PHP บนเว็บ เชื่อมต่อกับฐานข้อมูล และไฟร์วอลล์บนฟรีบีเอสดี เพื่อให้ผู้ใช้ได้ทำการจัดการติดตั้งและควบคุมแก้ไข และเรียกดูรายละเอียดต่างๆได้อย่างสะดวกและใช้งานได้ง่าย

1.4 องค์ประกอบของระบบงาน

ระบบงานประกอบด้วยองค์ประกอบต่างๆ ดังต่อไปนี้

1.4.1 เครื่องคอมพิวเตอร์เซิร์ฟเวอร์

ระบบปฏิบัติการ ฟรีบีเอสดี 7.0 ทำหน้าที่เป็นระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ซึ่งต้องเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ ฟรีบีเอสดี เวอร์ชัน 7.0 เพื่อรองรับการตรวจสอบข้อมูลที่ผ่านเข้าออก
- ติดตั้งซอฟต์แวร์ ป้องกันและแปลงหมายเลขเครือข่าย โดยเลือกใช้ โปรแกรมไฟร์วอลล์ หรือ IPFW
- ติดตั้งซอฟต์แวร์ตรวจจับแพ็กเก็ต โดยเลือกใช้โปรแกรมสนอร์ท
- ติดตั้งส่วนให้บริการเว็บเซิร์ฟเวอร์สำหรับเป็นส่วนติดต่อกับผู้ใช้เพื่อใช้ในการควบคุมระบบ โดยเลือกใช้โปรแกรม Apache
- ติดตั้งซอฟต์แวร์ภาษา โดยเลือกใช้โปรแกรม PHP เวอร์ชัน 5
- ติดตั้งซอฟต์แวร์เก็บล็อกสำหรับการเตือน โดยเลือกใช้โปรแกรม Mysql
- ติดตั้งโปรแกรมระบบป้องกันภัยเครือข่ายคอมพิวเตอร์

1.4.2 เครื่องคอมพิวเตอร์ไคลเอ็นท์ ที่ใช้ควบคุมระบบการกำหนดกฎ ของ ระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ที่อยู่บนฟรีบีเอสดี โดยผ่านทางเว็บ ซึ่งได้รับการเตรียมความพร้อมดังนี้

- ติดตั้งระบบปฏิบัติการ วินโดว์เอ็กพี
- ติดตั้งโปรแกรมเว็บบราวเซอร์ สำหรับติดต่อกับเว็บเซิร์ฟเวอร์ เพื่อควบคุมโปรแกรมการกำหนดกฎของระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์

1.5 ขั้นตอนในการพัฒนาระบบ

ประกอบไปด้วยขั้นตอนต่างๆ ดังนี้

1.51. ศึกษาความเป็นไปได้ในการพัฒนาระบบ

เพื่อกำหนดขอบเขตของปัญหาและวางแผนวิธีการพัฒนาโปรแกรม รวมถึงกำหนดเป้าหมายในการพัฒนาโครงการ โดยศึกษา ดังนี้

- ศึกษาวิธีการติดตั้งและการใช้งานซอฟต์แวร์ต่างๆ ที่ใช้สำหรับการสร้างระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ และระบบเว็บเซิร์ฟเวอร์ เพื่อรองรับการติดต่อจากภายนอก ได้แก่ ฟรีบีเอสดี, ไฟร์วอลล์, สนอร์ท, Apache เว็บเซิร์ฟเวอร์, PHP และ Mysql
- ศึกษาเทคโนโลยีการรักษาความปลอดภัยของ สนอร์ท และไฟร์วอลล์บนระบบปฏิบัติการ ฟรีบีเอสดี

- ศึกษาวิธีการสร้างกฎสำหรับการกรองและ การแปลงหมายเลขเครือข่าย ให้มีประสิทธิภาพ
- ศึกษารูปแบบการใช้งานระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ เพื่อนำไปใช้เป็นแบบตัวช่วยสร้างกฎ ให้มีการใช้งานที่ง่าย
- ศึกษาเทคโนโลยีการรักษาความปลอดภัยเครือข่ายโดยใช้โปรแกรมไฟร์วอลล์ IPFW
- ศึกษาเทคโนโลยีการเตือนของสนอร์ทเพื่อใช้ในการวิเคราะห์และการจัดการระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์บนระบบปฏิบัติการ ฟรีบีเอสดี

1.5.2 การวิเคราะห์และออกแบบ

ทำการวิเคราะห์และออกแบบรวมถึงกำหนดความต้องการของโครงการพัฒนาระบบ โดยได้ทำการออกแบบให้ระบบสามารถเพิ่มหรือลบกฎที่ทำการสร้างและป้อนข้อมูลที่จำเป็นสำหรับการสร้างกฎ และการตรวจสอบการแจ้งเตือนของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ โดยสามารถระบุ ไอพีแอดเดรส ของเครื่องภายในองค์กร ไอพีแอดเดรส ที่เชื่อมต่อกับอินเตอร์เน็ต, โปรโตคอล เป็นต้น นอกจากนี้ สามารถสำรองข้อมูลกฎและเรียกกฎที่มีการใช้งานอยู่เดิมก่อนที่จะทำการแก้ไขเปลี่ยนแปลงขึ้นมาทำงานได้ และแสดงผลการตรวจสอบการทำงานของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์

1.5.3 การพัฒนาและทดสอบ

- ทำการติดตั้งระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์และทดสอบการทำงานของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์
- ทำการพัฒนาโปรแกรมและทดสอบการทำงานของโปรแกรมในฟังก์ชันต่างๆ
- ทดสอบกฎของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ ที่โปรแกรมได้สร้างขึ้น

1.5.4 การทดลองใช้งานและปรับปรุงแก้ไข

นำโปรแกรมมาทดลองใช้งานและปรับปรุงแก้ไขเพื่อให้สามารถใช้งานได้ถูกต้องและง่ายยิ่งขึ้น

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้พัฒนาความรู้ความเข้าใจในเรื่องการทำงานของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์
2. ได้พัฒนาความรู้ความเข้าใจเรื่องการทำงานของ การกรองแพ็กเก็ตและการแปลงหมายเลขเครือข่าย โดยใช้ไฟร์วอลล์
3. ได้พัฒนาความรู้ความเข้าใจเรื่องการทำงานตรวจจับแพ็กเก็ตของสนอร์ท
4. ได้พัฒนาความรู้ความสามารถในการวิเคราะห์ ออกแบบและพัฒนาระบบงานและสามารถนำไปใช้ประโยชน์ต่อการทำงานในอนาคตได้
5. ได้โปรแกรมประยุกต์ที่ผู้ดูแลระบบหรือผู้ใช้งานทั่วไป สามารถเรียกใช้งานและทำการแก้ไขการทำงานกฎต่างๆของระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ โดยสะดวก รวดเร็ว และ ง่ายต่อการใช้งานยิ่งขึ้นในลักษณะการทำงานแบบเว็บ
6. เป็นอีกทางเลือกหนึ่งในการเลือกใช้โปรแกรมประยุกต์ที่ช่วยในด้านการรักษาความปลอดภัยทางด้านเครือข่าย บนระบบปฏิบัติการ ฟรีบีเอสดี เป็นเรื่องง่าย

บทที่ 2
ระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์

ระบบเครือข่ายคอมพิวเตอร์และระบบอินเทอร์เน็ตเป็นโครงสร้างพื้นฐานที่สำคัญและได้พัฒนาไม่หยุดยั้ง ส่งผลให้เกิดการบุกรุกในรูปแบบต่างๆ ดังนั้นการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์เป็นเรื่องที่ต้องมาควบคู่กันกับการจัดการระบบเครือข่ายคอมพิวเตอร์เพื่อป้องกันต่อการบุกรุก จึงจำเป็นอย่างยิ่งที่จะต้องมีระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ในการช่วยตรวจสอบและป้องกันการบุกรุกในรูปแบบต่างๆ เช่น การใช้งานเครือข่ายที่ไม่ปกติ และการพยายามโจมตีเครือข่ายให้ใช้งานไม่ได้ตามปกติ เป็นต้น การทำงานของระบบป้องกันการบุกรุกระบบเครือข่ายคอมพิวเตอร์ที่มีแนวคิดในการนำมาพัฒนาต้องอาศัยเทคโนโลยีการทำงานของสนอร์ทกับไฟร์วอลล์ซึ่งเป็นฟรีแวร์ เหมาะสมกับเครือข่ายที่ต้องการความปลอดภัยในการติดต่อระหว่างเครือข่ายภายในกับภายนอกเครือข่าย โดยลักษณะการทำงานของระบบป้องกันการบุกรุกระบบเครือข่ายเครือข่ายคอมพิวเตอร์จะทำตรวจสอบ และทำการวิเคราะห์แพ็กเก็ตคอนเท็น และจะตรวจจับแพ็กเก็ตที่ตรงกับซิกเนเชอร์และเตือน (Alert) แล้วค่อยไปกำหนดกฎเพื่อใช้ป้องกันการบุกรุก

2.1 องค์ประกอบของระบบป้องกันการบุกรุกระบบเครือข่าย

ระบบป้องกันการบุกรุกเครือข่ายช่วยให้เกิดความปลอดภัยต่อเครือข่ายโดยการตรวจสอบและป้องกันภัยที่จะมาบุกรุกครือข่าย แบ่งออกเป็นสองส่วนการทำงาน คือ

- ส่วนที่แรกคือส่วนที่ตรวจจับการบุกรุกเครือข่าย (Intrusion Detection) อาศัยการทำงานของโปรแกรมสนอร์ทในการตรวจจับแพ็กเก็ต และเตือนการบุกรุกเครือข่าย

- ส่วนสองคือส่วนที่ป้องกันการบุกรุกเครือข่าย (Intrusion Prevention) บนระบบปฏิบัติการฟรีบีเอสดี มีไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ตเข้า-ออก เครือข่าย

2.2 สนอร์ท

สนอร์ทเป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกเครือข่าย (Network intrusion detection) พัฒนาเริ่มแรกโดย Martin Roesch การทำงานของสนอร์ทจะใช้ไลบรารี (Library) พื้นฐานที่ชื่อ libpcab ซึ่งใช้กันโดยทั่วไปในพวก Network sniffer และ Network analyzer สำหรับสนอร์ทนั้นสามารถทำ Protocol anaysis, Content searching/matching, ตรวจจับการบุกรุก และprobe เช่น

buffer overflow, stealth port scan, CGI attack, SMB probe, OS Fingerprint และอื่นๆ นอกจากนี้ยังมีคุณสมบัติในการทำ real-time alerting

2.2.1 โหมดการทำงานของสนอร์ท

- Sniffer Mode คือโหมดที่สนอร์ทใช้อ่านแพ็กเก็ตบนเครือข่ายอย่างต่อเนื่อง

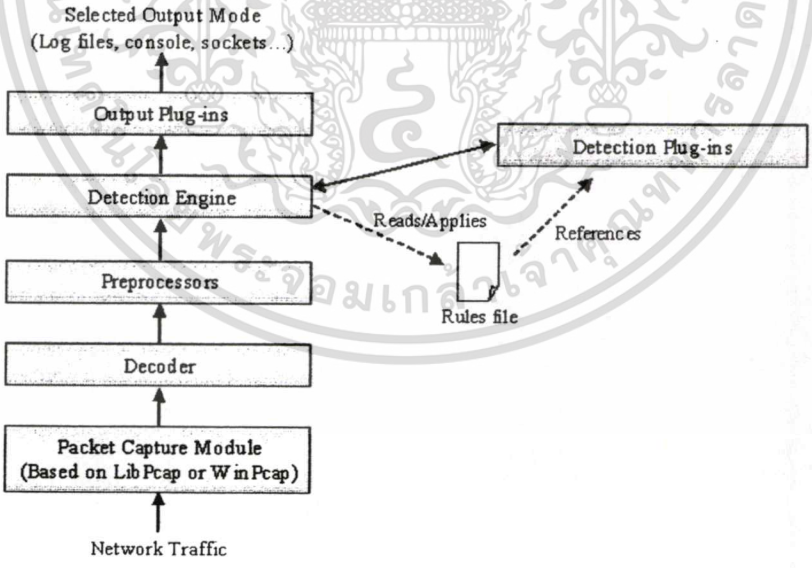
- Packet Logger Mode คือโหมดที่จัดการเรื่อง log การทำงานของแพ็กเก็ตลงบนดิสก์ หรือลงในฐานข้อมูล

- Network Intrusion Detection System (NIDS) Mode คือโหมดที่ทำการตรวจสอบวิเคราะห์แพ็กเก็ตกับกฎ (Rules) ซึ่งเก็บอยู่ใน snort.conf แล้วทำการเตือน (Alert) เมื่อพบแพ็กเก็ตที่ต้องสงสัย

- Inline Mode เป็นโหมดระบบป้องกันการบุกรุก (Intrusion Prevention System (IPS)) ทำการตรวจสอบกับกฎ (Rules) ถึงการ drop หรือ ให้ผ่านแพ็กเก็ต โดยใช้ IPFW

2.2.2 สนอร์ทบร็อกไดอะแกรม

สนอร์ทบร็อกไดอะแกรมมีองค์ประกอบการทำงานดังนี้



รูปที่ 2.1 แสดงการทำงานของสนอร์ทไดอะแกรม

จากรูปที่ 2.1 แสดงการทำงานของสนอร์ทไดอะแกรม ซึ่งสามารถอธิบายการทำงานได้ดังนี้

Decoder เมื่อมีการดักจับแพ็กเก็ตดูโครงสร้างข้อมูลและระบุโปรโตคอลที่เชื่อมต่อแล้ว จากนั้นก็ทำการ Decode ในส่วนของ IP ว่าเป็น TCP หรือ UDP เช่น วิเคราะห์พอร์ต และAddress โดยสนอร์ทจะทำการเตือน หรือ Alert เมื่อพบว่าในส่วนของ Header ผิดปกติ

Preprocessors เป็นตัวกรอง ที่ระบุสิ่งที่จะส่งต่อไปยังส่วนถัดไป (ในส่วนของ โมดูล (Modules) เช่น Detection Engine) ตัวอย่างเช่น กรณีของการพยายามเพื่อให้ได้ TCP/UDP ports หรือ ส่งแพ็กเก็ต UDP ออกมาในปริมาณมากๆ ในช่วงเวลาสั้นๆ นั้นคือการทำ Portscan โดยในส่วนของ Preprocessors function จะรับแพ็กเก็ตที่เป็นอันตรายแล้วส่งให้ Detect engine ตรวจสอบต่อไป

Rules Files คือ Plane text files ที่บรรจุรายการของ Rule ด้วย Syntax ซึ่ง Syntax ประกอบด้วย โปรโตคอล, Address, Output plug-ins ที่เกี่ยวข้อง เป็นต้น

Detection Plug-ins เป็นโมดูลที่ใช้อ้างอิงเพื่อระบุ Rules files และใช้จัดการเพื่อแยก pattern ออกมา

Detection Engine ทำงานร่วมกับส่วนของ Detection plug-ins เพื่อจับคู่ หรือ Match แพ็กเก็ตที่ตรงกับ Rules เป็นเสมือนหน่วยความจำของสนอร์ท

Output Plug-ins: เป็นโมดูลที่แจ้ง (Alert, logs) ให้ผู้ใช้รู้การเข้าใช้งานระบบ เช่น Alert_syslog, Alert_fast, database เป็นต้น

2.2.3 องค์ประกอบของกฎของสนอร์ท (Snort Rule)

Rules Header เป็นส่วนที่ต้องการระบุต้นทาง ปลายทาง และทิศทางของแพ็กเก็ตที่ผ่านมายัง Sensor โดยมีตัวแปร ดังนี้

- Action เป็นส่วนที่บอกว่าต้องการให้ทำ Action อะไร เมื่อมีการตรวจจับแพ็กเก็ตที่ต้องการได้
    - Alert คือ แจ้งเตือน ปกติรันใน Daemon mode ข้อมูลนั้นก็จะถูกเก็บไว้ที่ "/var/log/snort/alert"
    - Log คือ ข้อมูลจะถูกเก็บลงล็อกไฟล์ โดยถ้าไม่มีการระบุที่เก็บไฟล์จะแก็บไว้ที่ "/var/log/snort"
    - Pass คือ แพ็กเก็ตนั้นจะถูกดร็อปทิ้งไป ถูกใช้โดยไฟร์วอลล์
    - Activate คือ แจ้งเตือนและทำ Dynamic rules
    - Dynamic คือ ใช้โดย Activate rule แล้วทำ act
- Layer4 เป็นส่วนที่กำหนดว่าจะให้ Rules นั้น ๆ ตรวจจับแพ็กเก็ตใน Layer 4 ใด ที่เป็น TCP,UDP,ICMP และ IP

- HOME_NET เป็นต้นทาง โดยที่ค่า HOME_NET ได้ระบุไว้แล้วใน Snort.conf ซึ่งผู้ใช้สามารถเปลี่ยนแปลงค่าดังกล่าวได้ โดยปกติจะเป็น IP Address ของเครื่องนั้น ๆ หรือเป็น NetID ก็ได้ ในส่วนนี้มีค่า Default เป็น $HOME_NET
- PORT เป็นการระบุพอร์ตในส่วนของ HOME_NET
- Direction เป็นทิศทางที่แสดงถึงการเดินทางของแพ็กเก็ตมี 2 แบบคือ -> และ <>
- External_NET เป็นปลายทาง ค่าของ External_NET ได้ถูกระบุแล้วใน Snort.conf เช่นกัน โดยปกติจะเป็นค่า !$HOME_NET แต่ในส่วนนี้มีค่า Default เป็น $EXTERNAL_NET
- PORT เป็นการระบุพอร์ตในส่วนของ EXTERNAL_NET

Rules Option เป็นส่วนของการระบุแพ็กเก็ตที่ต้องการจะตรวจจับที่มีรายละเอียดมากขึ้น นั่นคือ ถ้ามีรายละเอียดมากเท่าไหร่ก็จะทำให้ ได้แพ็กเก็ตที่ตรงกับความต้องการมากขึ้นเท่านั้น

Meta-Data Rules Option เป็น Option ที่ใช้แสดงออกมาให้ผู้ใช้เห็นเมื่อมีการ Alert

- MSG เป็นส่วนที่บอกชื่อของ Pattern นั้น ๆ โดยที่เมื่อสนอร์ทดักจับแพ็กเก็ตได้แล้วชื่อในส่วนนี้จะถูกแสดงออกมาในส่วนที่เรียกว่า Signature
- Sid เป็นส่วนที่บอกถึง Signature ID เพื่อใช้ในการอ้างอิงกับ Snort.org ว่ามีการระบุ ID ให้กับ Pattern นั้น ๆ แล้วหรือยัง โดยที่ปกติแล้ว ถ้าเป็น Rules ที่สร้างขึ้นเองจะต้องมี Sid ที่มาก 1,000,000 เป็นต้นไป เพราะค่าที่ต่ำกว่า 1,000,000 Snort.org ขอสงวนไว้ใช้กำหนด Rules มาตรฐาน และค่าที่ <100 ถูกจองไว้ใช้ในอนาคต
- Rev เพื่อป้องการซ้ำของ Sid โดยที่แต่ละ Rules อาจจะมี Sid เหมือนกันและมีค่า Rev ที่ต่างกันก็ได้
- Classtype เป็นการแยกหมวดหมู่ของ Rules ที่สร้างขึ้น โดยที่แต่ละหมวดหมู่ก็จะมี Priority ที่ต่างกัน
- Priority เป็นกำหนด Priority ให้กับ Rules นั้น ๆ เมื่อไม่ต้องการใช้ Priority Default ที่อยู่ใน Classtype

Payload Detection Rules Option เป็นออฟชัน (Option) ที่บอกลักษณะของ Payload ที่อยู่ในแพ็กเก็ต ที่ต้องการจะให้สนอร์ทดักจับมีดังนี้

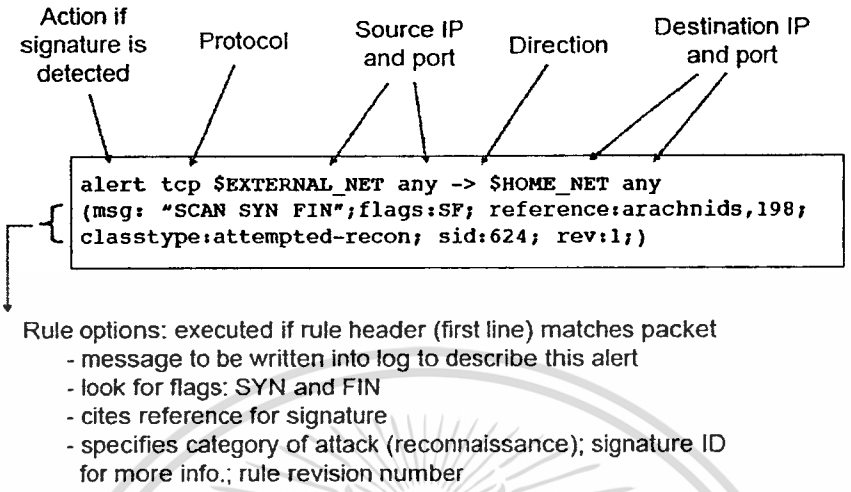
- Content เป็นเนื้อหาของ Payload ที่สามารถระบุได้ทั้ง รหัส ASCII code หรือ เป็นข้อความเลยก็ได้

- Nocase เป็นส่วนที่กำหนดให้ข้อความที่อยู่ใน Content ให้เป็น Non Case sensitive
- Rawbytes เป็นส่วนที่ให้นำ Content ไป Matching กับ RAW Traffic
- Depth ถ้ากำหนดให้เท่ากับ 5 สนอร์ทก็จะนำค่าของ Content ไป Matching กับ 5 ไบต์แรกที่อยู่ใน Payload
- Offset ถ้ากำหนดให้เท่ากับ 5 Snort จะนำค่าของ Content ไป Matching กับ Payload หลังจาก 5 ไบต์แรก
- Distance เป็นส่วนที่กำหนดให้ไม่ต้องสนใจค่าที่อยู่ใน Payload ตามจำนวนไบต์ที่กำหนด เช่น 10 ไบต์แรก , 20 ไบต์แรก
- Within ใช้ในการกำหนด จำนวน N ไบต์ ในการเปรียบเทียบข้อมูล Content payload

Non-Payload Detection Rules Option เป็น Option ที่บอกลักษณะต่าง ๆ ของ IP Header

- ttl คือค่า IP time-to-live ของ IP Package โดยสามารถกำหนดแบบไม่เจาะจงก็ได้ เช่น <3 [น้อยกว่า 3],5-10[ระหว่าง 5 ถึง 10] เป็นต้น
- tos คือค่า TOS ของ IP Package
- id คือค่า id field ของ IP Package
- ipopts คือค่าของ IP Option
- dsize คือการระบุขนาดของ Package Payload Size โดยสามารถกำหนดแบบไม่เจาะจงก็ได้ เช่น 300<>400 [ระหว่าง 300 ถึง 400] เป็นต้น
- flow คือ Keyword ที่ระบุถึงทิศทางการไหลของ TCP stream reassembly ใน Traffic
- ack คือการระบุค่าของ Acknowledgement ใน IP Package
- seq คือการระบุค่าของ Sequence ใน IP Package
- window เป็นการระบุค่าของ Window size ใน IP Package
- itype คือ ICMP Type ของ ICMP Package
- icode คือ ICMP Code ของ ICMP Package
- icmp_id คือ ICMP ID ของ ICMP Package
- icmp_seq คือ ICMP Sequence ของ ICMP Package
- sameip ให้ Alert เมื่อมี IP Source และ IP Destination ที่เหมือนกัน

ตัวอย่าง Snort rule



รูปที่ 2.2 แสดงรายละเอียดของ Snort rule

จากรูปที่ 2.2 แสดงรายละเอียดของ Snort rule เป็นตัวอย่างของ Snort Rules ที่กำหนดให้มีการ Alert โปรโตคอลที่ Alert คือ TCP จาก EXTERNAL_NET ทุกพอร์ต ที่ไปยัง HOME_NET ให้ตรวจสอบทุกพอร์ตเช่นกัน โดยกำหนดให้มี Rule option ดังที่ระบุในวงเล็บ ตัวอย่างเช่น Msg คือ ให้แสดงข้อความ SCAN SYN FIN แสดงตอนเกิด Alert อ้างอิง Signature คือ Arachnids ประเภทของ Signature คือ Attempted-recon ด้วย Sid หมายเลข 624 เวอร์ชัน 1

2.2.4 การอิมพลีเมนต์สนอร์ท

การอิมพลีเมนต์สนอร์ทเพื่อใช้สนอร์ทในการตรวจจับการบุกรุกเครือข่ายทำได้โดยติดตั้งโปรแกรมสนอร์ท จากนั้นทำการเพิ่มข้อมูลลงในไฟล์ "/etc/rc.conf" ดังนี้

Snort_enable="YES"

คือ การกำหนดให้โปรแกรมสนอร์ทสามารถใช้งานได้

2.3 ไฟร์วอลล์

ไฟร์วอลล์ทำหน้าที่กรองแพ็กเก็ต เพื่อป้องกันการบุกรุกเครือข่าย ใช้ Rule ในการกำหนดนโยบายการเข้ามาใช้งานภายในเครือข่าย และการติดต่อกับนอกเครือข่าย สนับสนุนการแปลงหมายเลขเครือข่าย หรือ Network address translation (NAT) และตรวจสอบการเชื่อมต่อที่อนุญาติให้ผ่าน หรือไม่ก็บล็อกการเชื่อมต่อ ในการทำงานของ NAT และการกรองแพ็กเก็ตใช้คอมพิวเตอร์

ทำหน้าที่กรองแพ็กเก็ตและแปลงหมายเลขเครือข่ายโดยใช้ระบบปฏิบัติการ หรือ ซอฟแวร์ เป็นตัวจัดการ ซึ่งการพัฒนาระบบได้ใช้ไฟร์วอลล์ในฟรีบีเอสดี หรือ IPFW หรือ IPFIREWALL

2.3.1 คุณสมบัติของไฟร์วอลล์

- ป้องกัน (Protect) เป็นเครื่องมือที่ทำงานในเชิงป้องกัน สามารถควบคุมแพ็กเก็ตให้ผ่านเข้า-ออกได้เฉพาะแพ็กเก็ตที่เห็นว่าปลอดภัย ซึ่งตรวจสอบได้จากกฎพื้นฐานที่แอดมินได้กำหนดไว้

- ควบคุมการเข้าใช้งานเครือข่าย (Access Control) โดยควบคุมให้เป็นไปตามกฎพื้นฐานที่แอดมินได้กำหนดไว้

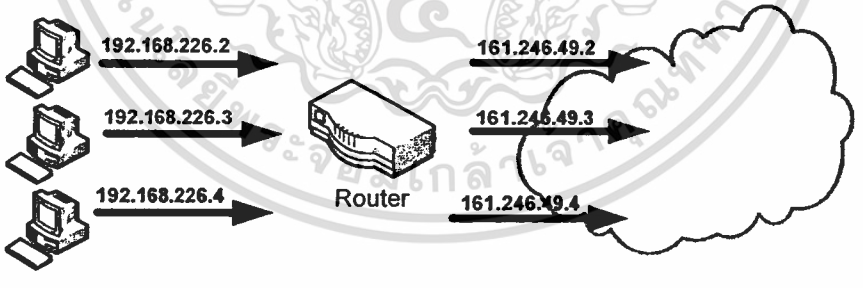
-กฎพื้นฐาน (Rule Base) คือ อาศัยกฎในการเปรียบเทียบกับแพ็กเก็ต เพื่อตรวจสอบสิทธิในการผ่านเข้า-ออกเครือข่ายว่าให้ผ่าน หรือไม่ให้ผ่าน โดยแอดมินสามารถเข้าไปกำหนดได้ ตัวอย่างนโยบายพื้นฐานเช่น

ipfw add pass all from any to any

จากตัวอย่างคือการอนุญาติให้ทุกทราฟิกบนอินเตอร์เฟสผ่านเข้าระบบได้

2.3.2 ลักษณะการทำงานของการแปลงหมายเลขเครือข่าย

การแปลงหมายเลขเครือข่ายช่วยให้เครื่องที่มีหมายเลขไอพีแอดเดรสที่ไม่ได้จดทะเบียนอย่างถูกต้อง (Private IP) สามารถติดต่อกับเครือข่ายอื่นๆได้



รูปที่ 2.3 แสดงการทำงานของ NAT

จากรูปที่ 2.3 แสดงการทำงานของ NAT เพื่อให้เครือข่ายภายในสามารถใช้งานอินเทอร์เน็ตได้

โดย command ที่ใช้ทำ NAT ตัวอย่างดังนี้

/sbin/ipfw add divert natd all from any to any via le1

จากคำสั่งที่แสดงเป็นการทำการ Divert packet ผ่านพอร์ต NAT โดยอนุญาตทุกโปรโตคอลผ่านไปมาได้ทุกที่ผ่าน Interface le1

2.3.3 การอิมพลีเมนต์ด้วยไฟร์วอลล์

การอิมพลีเมนต์ด้วยไฟร์วอลล์บนระบบปฏิบัติการฟรีบีเอสดี ทำให้ผู้ดูแลระบบสามารถกำหนดนโยบายให้กับไฟร์วอลล์ไปควบคุมการเข้าและออกของแพ็กเก็ตแต่ละอินเตอร์เฟส ซึ่ง IPFW ถูกรวมเข้ามาในการติดตั้ง FreeBSD ตั้งแต่ต้น ในลักษณะโมดูล (Module) ดังนั้น หากเราระบุ ไว้ในไฟล์ /etc/rc.conf ระบบจะโหลดโมดูลของไฟร์วอลล์ เข้ามาให้โดยอัตโนมัติทันที โดยเพิ่มข้อความลงในไฟล์ /etc/rc.conf ดังนี้

Firewall_enable="YES"

คือ การเปิดการใช้งานแพ็กเก็ตฟิลเตอร์

firewall_script="/etc/ipfw.conf.sh"

คือ กำหนดไฟล์ script ที่ตั้งกฎไว้

firewall_logging="YES"

คือ เปิดการทำงานของการ log ข้อมูล

คำเตือน ต้องกำหนดค่า net.inet.ip.fw.verbose ในไฟล์ sysctl ให้มีค่าเท่ากับ 1 และในไฟล์ /etc/rc.conf ไม่มีการกำหนด การจำกัดการ log ข้อมูล ให้ไปตั้งค่าที่ตัวแปรของ syscl แทน โดยแก้ไขที่ไฟล์ /etc/sysctl.conf

net.inet.ip.fw.verbose_limit=5

IPFW Command

คำสั่ง IPFW เป็นการสั่งด้วยมือ เพื่อเพิ่มหรือลด กฎการทำงานของ ไฟร์วอลล์ ในขณะที่กำลังใช้งานอยู่ ซึ่ง ปัญหาของการใช้วิธีนี้คือ เมื่อปิดเครื่องลง กฎทั้งหมดที่เราสร้างขึ้น หรือเปลี่ยนแปลง จะหายไปหมด แนะนำให้เขียน กฎที่ต้องการเก็บไว้ในไฟล์ และโหลดไฟล์ เหล่านั้นเมื่อตอน boot เครื่องแทน แต่คำสั่ง IPFW ในลักษณะนี้ ยังมีประโยชน์ เพื่อแสดงให้เห็นกฎไฟร์วอลล์ ที่กำลังทำงานอยู่ผ่านทาง Console การคำนวณของ IPFW จะแสดงค่าจำนวนนับของแพ็กเก็ต (Packet) ที่ตรงกับกฎแต่ละกฎ ในระหว่างการทดสอบกฎนั้น เมื่อเราดูที่ จำนวนนับเหล่านี้ เป็นการยืนยันว่า กฎที่ตั้งไว้ทำงานได้จริง คำสั่งสำหรับดูกฎทั้งหมดที่ตั้งไว้ ตามลำดับ

ipfw list

คำสั่งสำหรับดูกฎทั้งหมด พร้อมเวลาล่าสุดที่กฎนั้นทำงาน

ipfw -t list

คำสั่งดูช้อมูลของกฎทั้งหมด แถวแรกคือ หมายเลขประจำกฎ ตามด้วยจำนวนแพ็กเก็ตขาออกที่ตรงกับกฎ ตามด้วยจำนวนแพ็กเก็ตขาเข้าที่ตรงกับกฎ และ ต่อมาเป็นตัวกฎ ที่เราตั้งไว้

ipfw -a list

คำสั่งดูกฎที่ dynamic

ipfw -d list

คำสั่งดูกฎ dynamic ที่หมดอายุ

ipfw -d -e list

คำสั่งกำหนดให้ จำนวนนับเป็น 0 เพื่อเริ่มนับใหม่

ipfw zero

คำสั่งกำหนดให้ จำนวนนับเป็น 0 เพื่อเริ่มนับใหม่ เฉพาะกฎข้อใดข้อหนึ่ง (NUM)

ipfw zero NUM

ถ้าเราไม่ได้ต้องการทำ NAT ก็ไม่จำเป็นต้องคอมไพล์เคอร์เนล (Compile kernel) ของ FreeBSD ด้วยออฟชัน (Options) ต่อไปนี้

options IPFIREWALL

options นี้เปิดการทำงานของ IPFW ให้เป็นส่วนหนึ่งของ kernel

options IPFIREWALL_VERBOSE

options นี้ เปิดการทำงาน เพื่อเก็บข้อมูลแพ็กเก็ตที่วิ่งผ่าน IPFW โดยต้องระบุคำว่า 'log' ลงไปใน rule set

options IPFIREWALL_VERBOSE_LIMIT=5

options นี้ จำกัดจำนวนข้อความ การเก็บข้อมูลที่วิ่งผ่าน syslogd ควรใช้ออฟชันนี้ เพื่อป้องกันการมุ่งร้าย ที่มีต่อ การทำงานของไฟร์วอลล์ ซึ่งจะหยุดการโจมตีแบบ denial of service ที่ทำผ่าน syslog flooding

options IPFIREWALL_DEFAULT_TO_ACCEPT

options นี้จะอนุญาต ให้ทุกสิ่งทุกอย่าง ผ่านทะลุไฟร์วอลล์ไปได้ ซึ่งจะเป็นไอเดียที่ดี เมื่อเราติดตั้งไฟร์วอลล์เป็นครั้งแรก

options IPDIVERT

options นี้ใช้เพื่อเปิดการใช้งาน NAT

หมายเหตุ: ถ้าเราไม่ได้ระบุ IPFIREWALL_DEFAULT_TO_ACCEPT เข้าไปด้วย หรือ เราไม่ได้ตั้งกฎ เพื่ออนุญาตให้แพ็กเก็ตผ่านเข้ามาได้ ไว้ก่อน จะกลายเป็นว่า เราจะกั้นแพ็กเก็ตทั้งหมด ไม่ให้เข้า ไม่ให้ออก จากเครื่องของเรา

IPFW Rule Sets

rule set คือกลุ่มของกฎ IPFW ที่เขียนขึ้นมาเพื่ออนุญาต หรือ ปฏิเสธแพ็กเก็ต (Packet) ตามค่าที่อยู่ในแพ็กเก็ตนั้นๆ การแลกเปลี่ยนทั้ง 2 ทางคือไป-กลับ ระหว่างการสื่อสารของคอมพิวเตอร์ โดยปกติ rule set ของไฟร์วอลล์จะตรวจสอบแพ็กเก็ต 2 รอบเสมอ ครั้งแรกตอนมาจากเครื่องบนอินเทอร์เน็ต (Internet) ที่ติดต่อมา และตอนกลับออกไปยังอินเทอร์เน็ตไปยังเครื่องที่เรียกมา การบริการต่างๆ (เช่น telnet, www , mail และอื่นๆ) ถูกกำหนดโดยโปรโตคอลประจำตัว และ เลขประจำ port สิ่งเหล่านี้เป็นขอบเขตการเลือกขั้นต้น ที่ใช้สร้างกฎ สำหรับการอนุญาต หรือ ปฏิเสธงานบริการเหล่านั้น เมื่อแพ็กเก็ตเข้ามายังไฟร์วอลล์ มันจะถูกเปรียบเทียบกับกฎข้อที่ 1 ใน rule set และจะดำเนินตามกฎแต่ละข้อ ตั้งแต่บนจนถึง กฎล่างสุด ตามลำดับหมายเลขประจำกฎ และเมื่อแพ็กเก็ตตรงกับกฎข้อใด กฎจะทำงานทันทีกับแพ็กเก็ตนั้น ด้วยวิธีการนี้ถูกเรียกว่า การค้นหาแบบ "the first match wins" และถ้าแพ็กเก็ตนั้นไม่ตรงกับกฎข้อใดๆ เลย มันจะถูกดักจับด้วยกฎข้อหลักของ IPFW คือกฎหมายเลข 65535 ซึ่งจะปฏิเสธทุกๆ แพ็กเก็ต โดยไม่มีการแจ้งข้อมูลกลับไปยังต้นทางแต่อย่างใด

ขั้นตอนเหล่านี้ เป็นพื้นฐานของการใช้กฎ ที่มีลักษณะแบบ "keep state","limit","in"/"out" เป็น Rule set ของ ไฟร์วอลล์ ประเภท Inclusive

ไฟร์วอลล์ ประเภท Inclusive จะอนุญาตให้ข้อมูลที่ตรงกับ กฎที่ตั้งขึ้นผ่านได้เท่านั้น ด้วยวิธีนี้ เราสามารถควบคุมได้ว่างานบริการใดบ้างที่จะอยู่หลังไฟร์วอลล์ ที่มีจุดหมายปลายทางไปยังอินเทอร์เน็ต และยังควบคุมงานบริการ ซึ่ง สามารถมาจากอินเทอร์เน็ตที่จะเข้ามาถึงยังเครือข่ายของเรา ด้วยการออกแบบให้ปฏิเสธทุกอย่างเป็นอันดับแรก จึงทำให้ไฟร์วอลล์ ประเภท Inclusive มีความปลอดภัยเป็นอันมาก มากกว่าไฟร์วอลล์ ประเภท Exclusive และเป็นประเภทเดียวที่เราพูดถึงกัน

Rule Syntax

รูปแบบการเขียนกฎ ที่นำเสนอต่อไปนี้ เป็นแบบธรรมดา เพื่อให้เข้าใจการสร้าง Rule set ของไฟร์วอลล์ แบบ Inclusive สำหรับรูปบบการเขียนกฎ ที่สมบูรณ์นั้น ให้ดูจาก man IPFW

กฎ ประกอบด้วย Keywords โดยที่ Keywords เหล่านี้ต้องเขียนตามลำดับ จากซ้ายไปขวา ในแต่ละบรรทัด Keywords แสดงให้เห็นด้วยตัวพิมพ์ใหญ่ บาง Keyword มีคำสั่งย่อย ซึ่งอาจจะมี Keyword สำหรับ ตัวมันเอง และ อาจจะมีคำสั่งย่อยด้วยก็ได้ เครื่องหมาย "#" ใช้เป็นตัวเริ่มต้นประโยคหมายเหตุ และ อาจจะระบุไว้ตอนท้ายบรรทัดของกฎ ขณะที่ บรรทัดว่างจะไม่ถูกตีความ

CMD RULE NUMBER ACTION LOGGING SELECTION STATEFUL

CMD

กฎใหม่แต่ละกฎ ต้องมีคำนำหน้าด้วยคำว่า "add" เพื่อสั่งเพิ่มกฎเข้าไปในตารางเก็บข้อมูลภายใน

RULE_NUMBER

กฎแต่ละกฎ ต้องมีหมายเลขประจำกฎ ไว้สำหรับทำงานตามหมายเลขนั้น

ACTION

กฎจะทำงานร่วมกับคำสั่งต่อไปนี้ ซึ่งจะทำงานทันทีที่แพ็กเก็ตตรงกับข้อกำหนดของกฎ

allow | accept | pass | permit

คำสั่งทั้งหมดนี้มีความหมายเหมือนกัน คือ อนุญาตให้แพ็กเก็ตที่ตรงกับกฎ ผ่านออกจากตรวจสอบของไฟร์วอลล์ได้ และการตรวจสอบจะสิ้นสุดลง ที่กฎตัวนี้

check-state

เป็นการสั่งให้ตรวจสอบแพ็กเก็ตกับ ตารางกฎแบบไดนามิก (Dynamic) คือถ้าตรวจสอบว่าตรงกัน ให้ดำเนินการตามคำสั่งที่เกี่ยวข้องกับกฎ ซึ่งทำงานร่วมกับกฎแบบไดนามิกข้อนั้น แต่ถ้าไม่ตรงกับกฎ ให้ผ่านไปยังกฎข้อต่อไป กฎแบบ check-state จะไม่มีขอบเขตสำหรับการตรวจสอบ และถ้าไม่มีการใช้กฎแบบ check-state ใน Rule set ตารางกฎแบบไดนามิกจะถูกตรวจสอบตั้งแต่กฎที่ระบุเป็น keep-state ตัวที่หนึ่ง

deny | drop

ทั้งสองคำมีความหมายเดียวกัน คือ ปฏิเสธแพ็กเก็ตที่ตรงกับกฎ การตรวจสอบยุติทันที

Logging

log หรือ logamount

เมื่อ packet ใดตรงกับกฎ และมีการใช้ log จะมีการบันทึกข้อความไปที่ syslogd ด้วยข้อความว่า SECURITY การบันทึก log จะทำงานต่อเมื่อ จำนวนแพ็กเก็ตที่ถูกบันทึก ไม่เกินจำนวนที่ระบุไว้ใน logamount แต่ถ้าไม่มีการระบุ logamount ไว้ การบันทึก log จะตรวจสอบข้อจำกัดของการบันทึก จากค่าที่ให้ไว้ในตัวแปร net.inet.ip.fw.verbose_limit และในทั้งสองกรณีนั้น หากมีค่าเป็น 0 จะเป็นการยกเลิก ข้อจำกัดในการบันทึก log ในกรณีที่การบันทึก log เต็มตามข้อจำกัดที่กำหนดไว้ เราสามารถกำหนดค่าในการจำกัด การบันทึก log ได้ ทั้งนี้ให้ดูคำสั่ง reset log ของ IPFW เพิ่มเติม

หมายเหตุ: การบันทึก log จะทำงานหลังจากที่แพ็กเก็ตถูกตรวจสอบว่าตรงกับกฎ และจะทำงานก่อนคำสั่งสุดท้าย (accept, deny) แต่ทั้งนี้ขึ้นอยู่กับว่าเราจะตัดสินใจให้ กฎข้อไหนที่เราต้องการบันทึกบ้าง

Selection

คำต่อไปนี้ ใช้เพื่อเป็นการบอกถึงรายละเอียดของแพ็กเก็ต เพื่อใช้ในการตรวจสอบว่าแพ็กเก็ตนั้นตรงกับกฎหรือไม่ และต้องเรียงลำดับตามนี้

udp | tcp | icmp

ทั้งนี้ยังสามารถใช้ ชื่อโปรโตคอล (Protocol) ที่อยู่ใน /etc/protocols

from src to dst

คำว่า from ใช้เพื่อเป็นการตรวจสอบกับ IP address การตั้งกฎต้องระบุทั้งต้นทางและปลายทาง สำหรับคำว่า "any" ใช้ระบุเพื่อให้ตรงกับทุกๆ IP address ส่วนคำว่า "me" กำหนดเพื่อให้ตรงกับ IP address ที่ใช้ใน FreeBSD ในเครื่องของเราที่มีไฟร์วอลล์กำลังทำงานอยู่ ตัวอย่างเช่น "from me to any" หรือ "from any to me" หรือ "from 0.0.0.0/0 to any" หรือ "from any to 0.0.0.0/0" หรือ "from 0.0.0.0 to any" หรือ "from any to 0.0.0.0" หรือ "from me to 0.0.0.0" โดย IP address ถูกระบุตัวเลข IP address และ จุด ตามด้วย /mask-length หรือ สามารถใช้แบบ IP address และจุด เท่านั้นก็ได้

port number

สำหรับโปรโตคอลที่รองรับหมายเลขพอร์ต (Ports) (เช่น TCP และ UDP) มันเป็นข้อบังคับที่เราต้องระบุ หมายเลขพอร์ตสำหรับ ข้อมูลที่เราต้องการ ตรวจสอบให้ถูกต้อง ทั้งนี้ชื่อบริการต่างๆ ที่อยู่ใน /etc/services อาจนำมาใช้แทนค่าของหมายเลขพอร์ตได้

in | out

ใช้แทนแพ็กเก็ตที่ตรงกับ ด้านขาเข้า หรือ ด้านขาออก คำว่า in และ out เป็นข้อบังคับที่เราต้องระบุไว้ในกฎ

via IF

แพ็กเก็ตที่เข้ามาทาง lan card ที่ระบุ จะถูกตรวจสอบเสมอ

setup

เป็นคำที่เป็นข้อบังคับว่า session start ตามการเรียกร้องของแพ็กเก็ตแบบ TCP

keep-state

เป็นคำบังคับ ขึ้นอยู่กับการตรวจสอบความถูกต้องของไฟร์วอลล์ ซึ่งจะสร้างกฎไดนามิก (Dynamic) ขึ้นมา ตรวจสอบกฎทั้ง 2 ทาง ระหว่าง ต้นทางและปลายทาง IP/port ใช้โปรโตคอลเดียวกัน

limit {src-addr | src-port | dst-addr | dst-port}

ไฟร์วอลล์จะอนุญาตให้เชื่อมต่อได้จำนวนหนึ่งเท่านั้น ที่ใช้กฎเดียวกัน โดยจำนวนของต้นทางและปลายทางต้องระบุให้ครบ คำว่า "limit" และ "keep-state" ไม่สามารถใช้ร่วมกันในกฎเดียวกัน โดย limit จะมี keep-state เตรียมให้อยู่แล้ว

บทที่ 3
การวิเคราะห์และออกแบบโครงงานพัฒนาระบบ

3.1 ความต้องการของระบบ

3.1.1 Functional Requirements

1. สามารถให้ผู้ใช้งานผ่านทาง Web page
2. สามารถสร้างกฎป้องกันและตรวจสอบการบุกรุกด้วยไฟร์วอลล์ และ snort ได้
3. สามารถเพิ่ม ลบ แก้ไข ค่ากฎ
4. สามารถเรียกค่าและแก้ไข configuration มาใช้ได้
5. สามารถแสดงล็อกไฟล์และเตือนการใช้งานได้
6. สามารถสำรองข้อมูลกฎและเรียกกฎที่มีการใช้งานอยู่เดิมก่อนที่จะทำการแก้ไขเปลี่ยนแปลงขึ้นมาทำงานได้

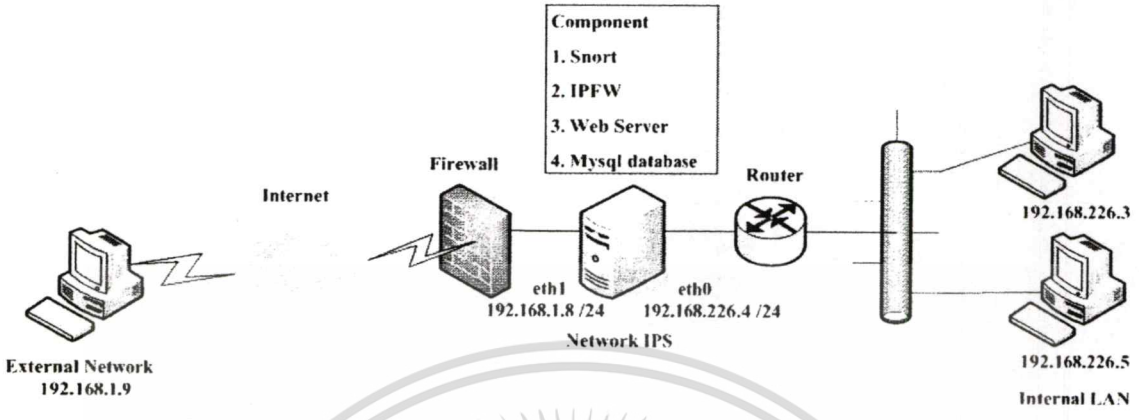
3.1.2 Non-functional Requirements

1 เมื่อเครื่องให้บริการการระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์เสียหาย หรือไม่สามารถใช้งานได้เมื่อมีการนำเอาเครื่องสำรองมาใช้งานแทน ระบบสามารถนำค่า Configuration และกฎ ที่สำรองไว้ มาใช้งานแทนได้

2 เมื่อเครื่องให้บริการระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ เดิมได้ทำการซ่อมแซมแก้ไขจนสามารถใช้งานได้ตามปกติแล้ว ระบบต้องสามารถนำค่า Configuration และกฎ ต่างๆ ที่เคยกำหนดไว้มาใช้งานได้

3. มีการกำหนดสิทธิในการเข้าใช้งานระบบ โดย ที่จะสามารถใช้งานระบบได้นั้นจะต้องเป็นผู้ดูแลระบบเท่านั้น
4. สามารถเรียกดูจำนวน Alert ที่แสดง

3.2 ภาพรวมของระบบป้องการบุกรุกเครือข่ายคอมพิวเตอร์



รูปที่ 3.1 แสดงภาพรวมของระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์

จากรูปที่ 3.1 ระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ติดตั้งบนระบบปฏิบัติการฟรีบีเอสดีทำงานตรวจสอบ และป้องกัน ซึ่งพัฒนาโดยใช้ภาษา PHP ในการควบคุมการทำงานของระบบ ผู้ใช้งานจะทำการกำหนดค่า configuration และกฎ ต่างๆสำหรับจัดการระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์เพื่อให้บริการกับเครื่องคอมที่อยู่ภายในเครือข่ายที่ต้องการเชื่อมต่อออกสู่ภายนอกเครือข่ายและสร้างความปลอดภัยต่อเครือข่ายคอมพิวเตอร์ โดยผู้ดูแลระบบสามารถจัดการควบคุมผ่านทางเว็บเบสยูสเซอร์อินเทอร์เฟส เพื่อกำหนดค่า configuration และเก็บค่าดังกล่าวไว้ใน configuration file ของระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์

ระบบสามารถจัดการ และเก็บค่า Configuration ของระบบโดยสามารถทำผ่านเว็บเบสยูสเซอร์อินเทอร์เฟส

เครื่อง Network IPS เตรียมความพร้อมดังต่อไปนี้

- ติดตั้ง Web Server เพื่อให้ผู้ใช้เข้ามา Configure ระบบ
- ติดตั้ง PHP เพื่อเป็นคำสั่งในการConfigure จัดการในส่วนวิเคราะห์ระบบ
- ติดตั้ง Mysql เพื่อเก็บล็อคที่ได้จากการตรวจจับแพ็กเก็ตของสนอร์ท และเก็บกฎ
- ติดตั้ง สนอร์ท อินไลน เพื่อทำหน้าที่ตรวจจับแพ็กเก็ต
- ติดตั้ง IPFW และ NAT โดยใช้ IPFW ทำหน้าที่ divert แพ็กเก็ตผ่านพอร์ต
- ติดตั้งโปรแกรมส่วนติดต่อกับผู้ใช้แบบเว็บสำหรับการจัดการระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์บนระบบปฏิบัติการ ฟรีบีเอสดี

เมื่อติดตั้งระบบดังกล่าวแล้ว ผู้ดูแลระบบสามารถใช้เครื่องคอมพิวเตอร์ เรียกใช้เว็บเบสยูสเซอร์อินเทอร์เฟส เพื่อเข้าไปตั้งค่าระบบการจัดการระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์บนระบบปฏิบัติการ ฟรีบีเอสดี และใช้วิเคราะห์การทำงานของระบบ โดยมีขั้นตอนดังนี้

- ผู้ดูแลระบบเรียกใช้ เว็บเบสยูสเซอร์อินเทอร์เฟส เพื่อทำการล็อกอินเข้าไปใช้งาน
- ผู้ดูแลระบบสามารถตั้งค่าข้อมูลที่จำเป็นต่างๆ เช่น ค่า configuration ต่างๆ
- ผู้ดูแลระบบทำการยืนยันการตั้งค่าต่างๆที่ได้ตั้งไว้ จากนั้นโปรแกรมจะจัดการ configuration file และทำงานตามที่ได้ตั้งไว้
- ผู้ดูแลระบบสามารถสร้าง และแก้ไขการตั้งค่าต่างๆได้ สามารถสำรองค่าที่ตั้งไว้และเรียกค่าที่สำรองมาใช้ได้
- ผู้ดูแลระบบสามารถดูการทำงานของระบบได้

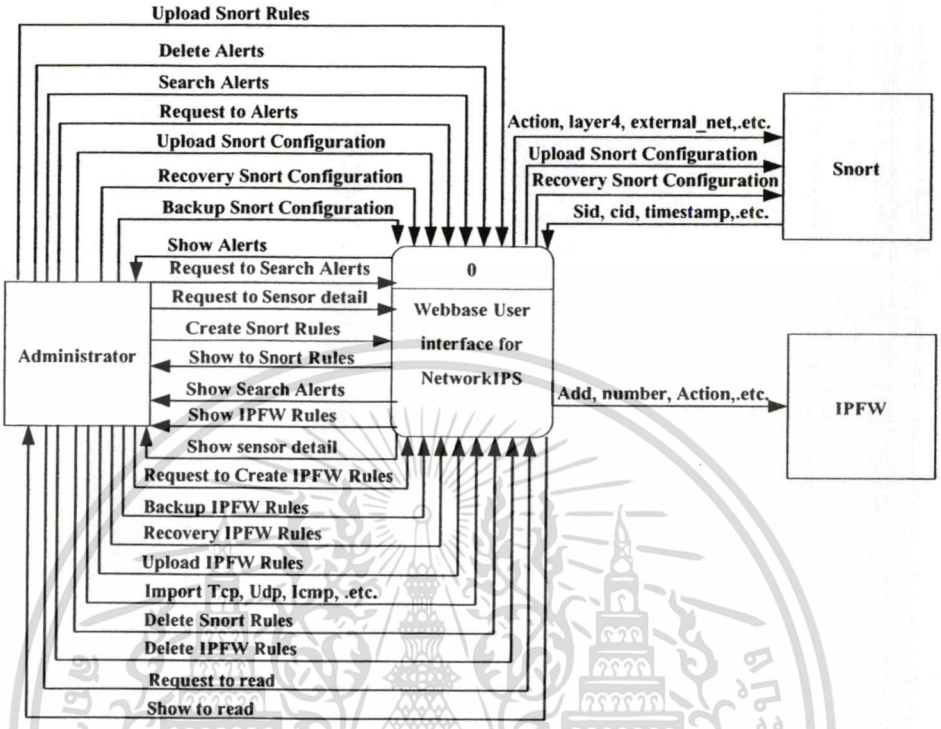
3.3 การวิเคราะห์และการออกแบบระบบ

การออกแบบระบบในโครงงานนี้ใช้การออกแบบเชิงโครงสร้าง คือ Context Diagram, Dataflow Diagram level 0 และ Dataflow Diagram level 1 และ activity diagram ซึ่งสัญลักษณ์ที่ใช้ในการวิเคราะห์ระบบ มีรายละเอียดดังนี้

ตารางที่ 3.1 ตารางสัญลักษณ์

สัญลักษณ์	คำอธิบาย
 Entity	คือ หน่วยภายนอก (External Entity)
 Process	คือ กระบวนการหรือขั้นตอนการทำงาน
 Data store	คือ ข้อมูลที่จัดเก็บ
 Flow of Data	คือ การไหลของข้อมูล

3.3.1 Context diagram

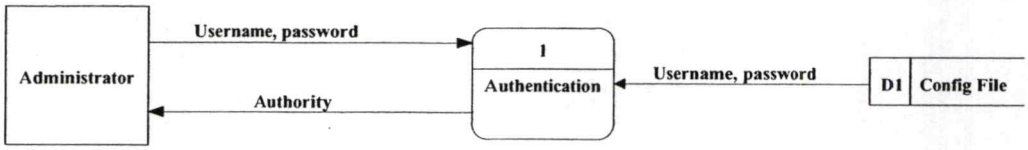


รูปที่ 3.2 แสดง Context diagram ของระบบป้องกันการบุกรุกเครือข่าย

จากรูปที่ 3.2 แสดงการทำงานในส่วนของ Context diagram เพื่อแสดงภาพรวมของระบบ โดยผู้ที่สามารถใช้ระบบได้คือ administrator สามารถจัดการผ่านเว็บเบสยูสเซอร์อินเทอร์เฟส โดยจะไปเรียกค่า หรือข้อมูลของระบบเพื่อนำมาวิเคราะห์ผ่านเว็บเบสยูสเซอร์อินเทอร์เฟสเชื่อมโยงกับฐานข้อมูลของ Snort หาแนวทางป้องกัน แล้วกำหนดกฎให้กับ IPFW เพื่อให้เกิดความปลอดภัยต่อระบบเครือข่ายภายใน นอกจากนี้เว็บเบสยูสเซอร์อินเทอร์เฟสสามารถรองรับการจัดการสำรองกฎ กู้คืนกฎ และอัพโหลดกฎ ผ่านทางเว็บเบสยูสเซอร์อินเทอร์เฟส

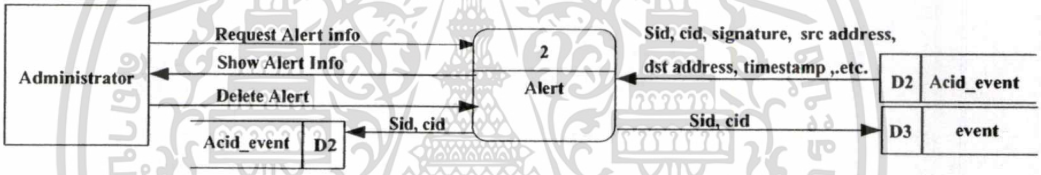
3.3.2 Dataflow diagram

แผนภาพการไหลของข้อมูล (Dataflow diagram) มีรายละเอียด ดังนี้



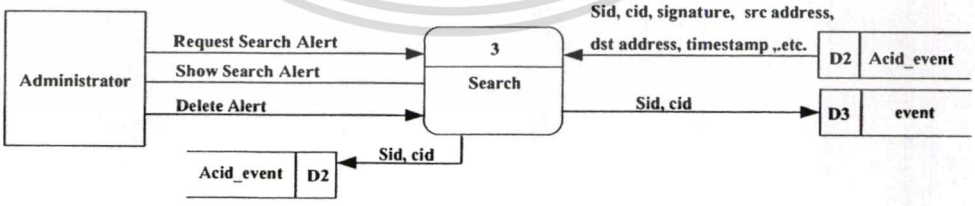
รูปที่ 3.3 แสดง Dataflow diagram level 1 ของ Authentication

จากรูที่ 3.3 แสดง Dataflow diagram level 1 ของ Authentication โดยจะตรวจสอบ ชื่อและรหัสของผู้ใช้ ก่อนที่จะอนุญาตให้เข้าใช้งานในระบบ



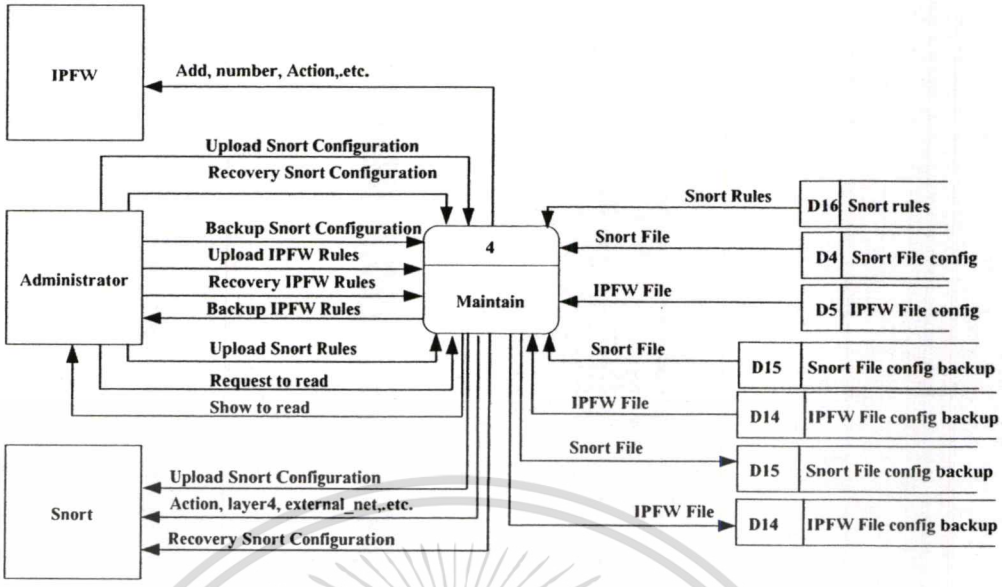
รูปที่ 3.4 แสดง Dataflow diagram level 1 ของ Alert

จากรูที่ 3.4 แสดง Dataflow diagram level 1 ของ Alert เพื่อใช้เรียกดู Alerts และสามารถลบ Alerts



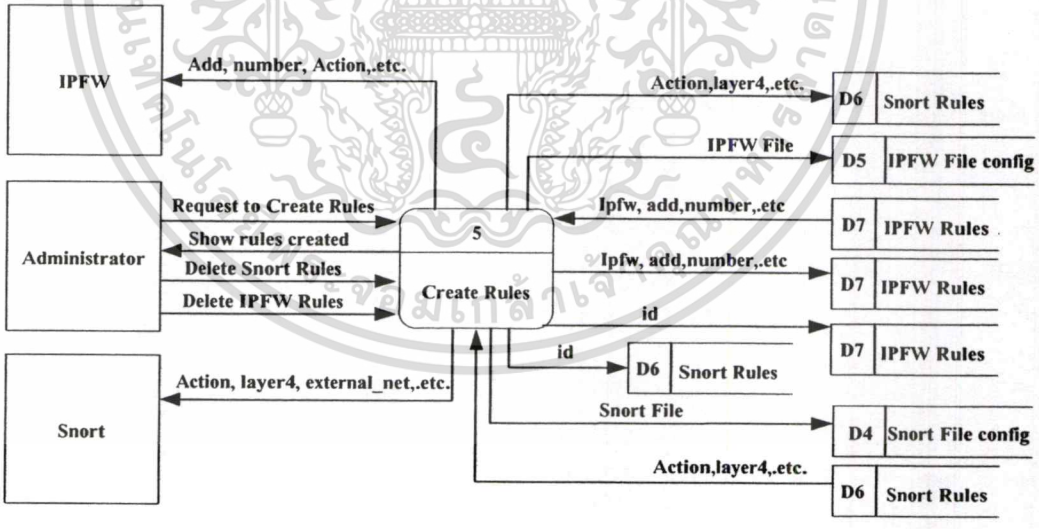
รูปที่ 3.5 แสดง Dataflow diagram level 1 ของ Search

จากรูที่ 3.5 แสดง Dataflow diagram level 1 ของ Search เพื่อใช้เรียกดู Alerts โดยวิธีการค้นหา



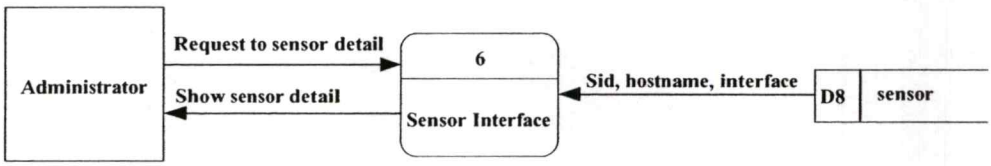
รูปที่ 3.6 แสดง Dataflow diagram level 1 ของ Maintain

จากรูที่ 3.6 แสดง Dataflow diagram level 1 ของ Maintain เพื่อใช้จัดการในส่วนของ File Configuration และ Rules ในเรื่องของการสำรองกฎ, กู้คืนกฎ และ อัพโหลดกฎ เข้าสู่ระบบ



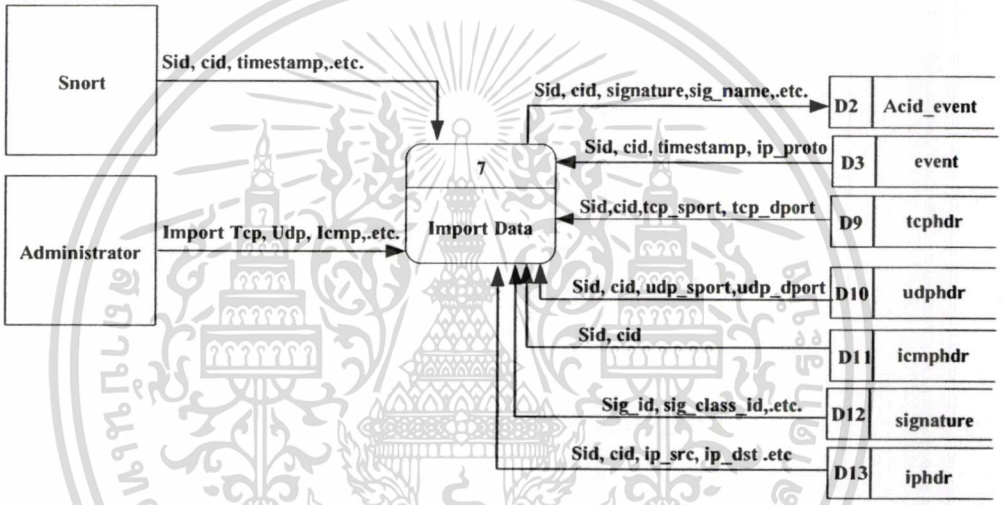
รูปที่ 3.7 แสดง Dataflow diagram level 1 ของ Create Rules

จากรูที่ 3.7 แสดง Dataflow diagram level 1 ของ Create Rules เพื่อใช้ในการสร้างกฎและลบกฎ ของสนอร์ท และไฟร์วอลล์



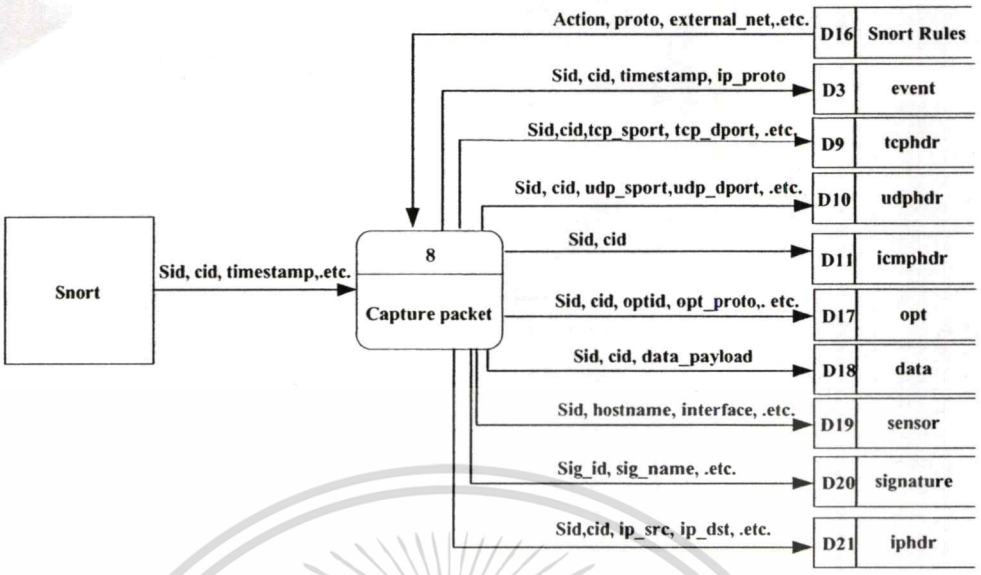
รูปที่ 3.8 แสดง Dataflow diagram level 1 ของ Sensor Interface

จากรูที่ 3.8 แสดง Dataflow diagram level 1 ของ Sensor Interface เพื่อใช้เรียกดูรายละเอียดของ Sensor ที่ใช้งาน



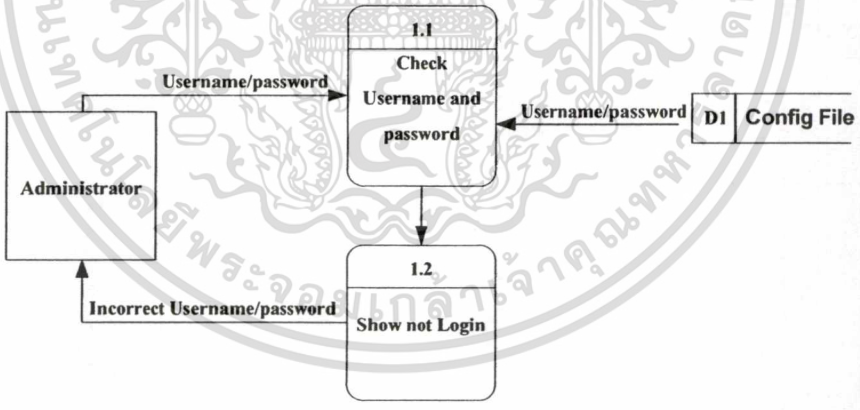
รูปที่ 3.9 แสดง Dataflow diagram level 1 ของ Import data

จากรูที่ 3.9 แสดง Dataflow diagram level 1 ของ Import data เพื่อนำข้อมูลเข้าสู่ตาราง Acid_event และนำไปวิเคราะห์รายละเอียดของ Alerts ในฟังก์ชัน Alerts และฟังก์ชัน Search



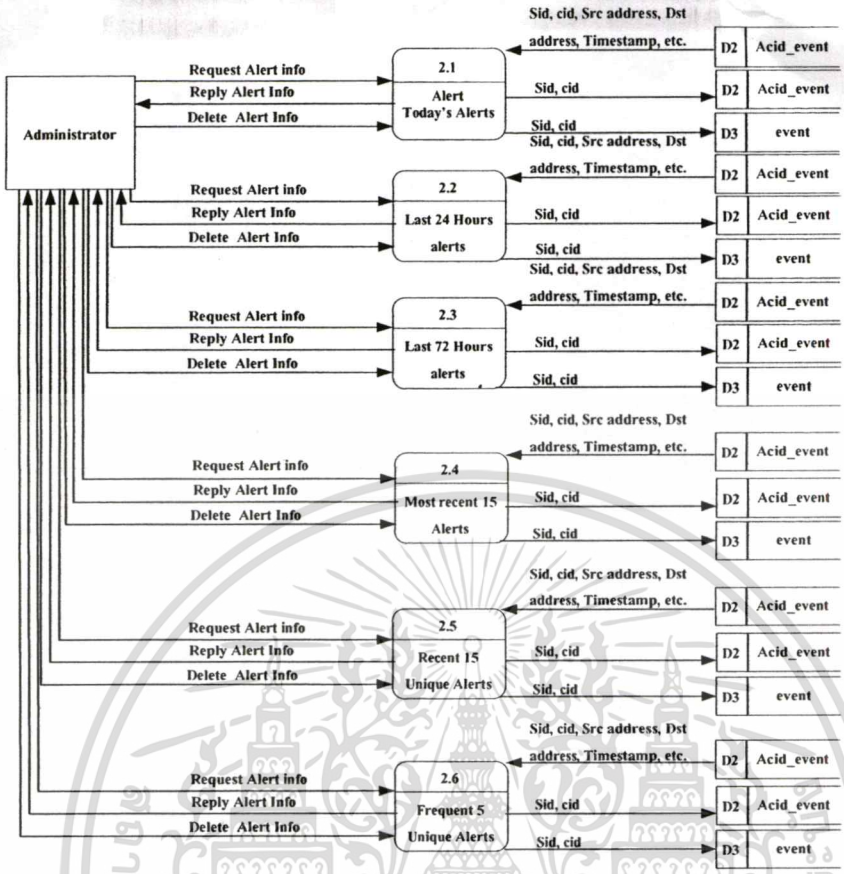
รูปที่ 3.10 แสดง Dataflow diagram level 1 ของ Capture packet

จากรูที่ 3.10 แสดง Dataflow diagram level 1 ของ Capture packet ใช้นำเข้าข้อมูลที่ดักจับได้เก็บลงฐานข้อมูลสนอร์ท



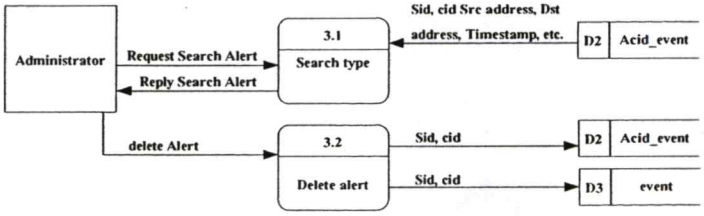
รูปที่ 3.11 แสดง Dataflow diagram level 2 ของ Authentication

จากรูปที่ 3.11 เป็นการแสดงการไหลของข้อมูลของ Dataflow diagram level 2 ในส่วนของการพิสูจน์สิทธิการเข้าใช้งานผ่านเว็บเบสยูสเซอร์อินเทอร์เฟส ถ้าข้อมูลที่ป้อนไม่ถูกต้องระบบจะให้กลับไปป้อนข้อมูลใหม่ เพื่อจะได้เข้าใช้งานเว็บเบสยูสเซอร์อินเทอร์เฟสได้



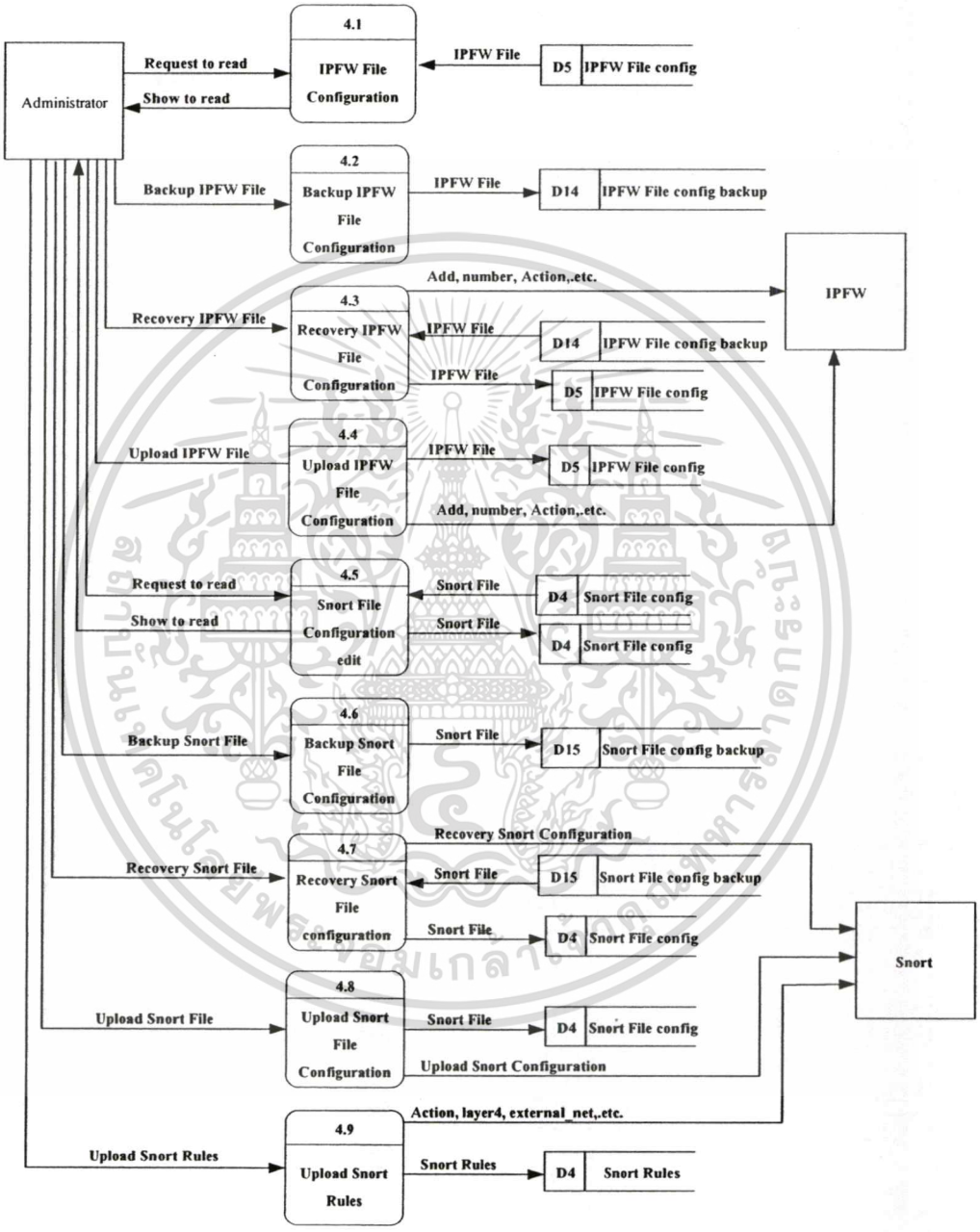
รูปที่ 3.12 แสดง Dataflow diagram level 2 ของ Alert

จากรูปที่ 3.12 เป็นการแสดงการไหลของข้อมูลของ Dataflow diagram level 2 ในส่วนของ Alert โดยในส่วนนี้สามารถเรียกดูการ Alert ได้โดยมีรายละเอียดดังนี้ คือ เรียกดูการเตือนรายวัน หรือ Alert Today's day, เรียกดูการเตือนล่าสุดใน 24 ชั่วโมง หรือ Last 24 Hours alerts, เรียกดูข้อมูลการเตือนล่าสุดภายใน 72 ชั่วโมง หรือ Last 72 Hours alerts, เรียกดูการเตือน 15 การเตือนมากสุดล่าสุด หรือ Most recent 15 alerts, เรียกดูการเตือน 15 การเตือนล่าสุด หรือ Recent 15 unique alerts, เรียกดูการเตือนที่บ่อยๆ 5 alert หรือ Frequent 5 Unique Alerts โดยทั้งหมดออกแบบให้สามารถลบการเตือนทิ้งได้



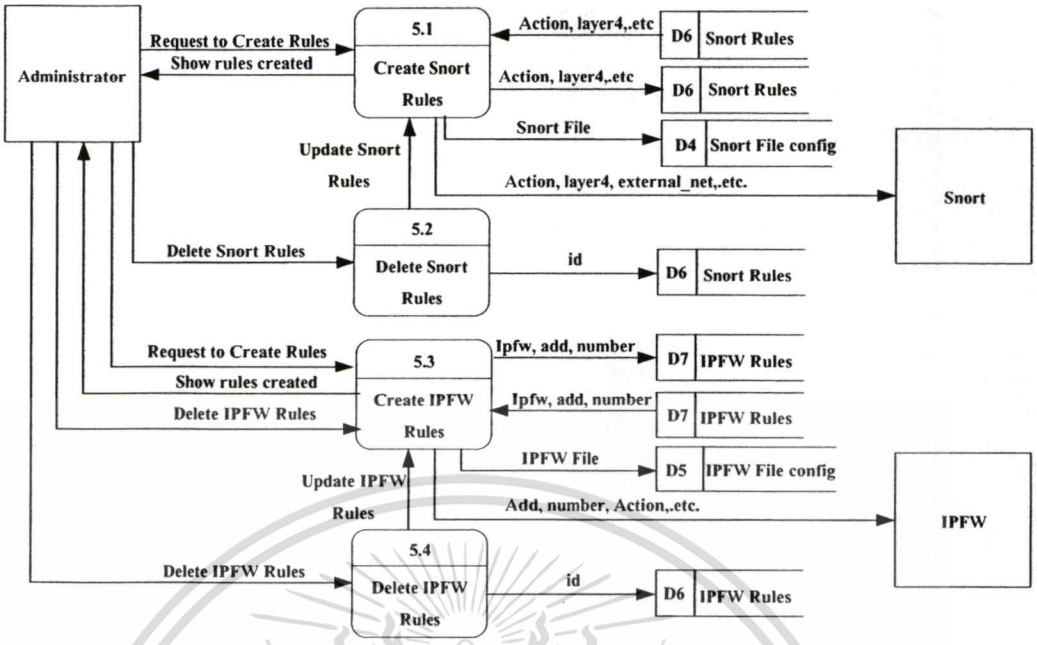
รูปที่ 3.13 แสดง Dataflow diagram level 2 ของ Search

จากรูปที่ 3.13 เป็นการแสดงการไหลของข้อมูลของ Dataflow diagram level 2 ในส่วนของ Search การทำงานคือต้องใส่ค่าที่ต้องการค้นหาจากนั้นระบบจะแสดงรายการที่ต้องการค้น และสามารถจัดการกับ Alert โดยการลบทิ้งได้



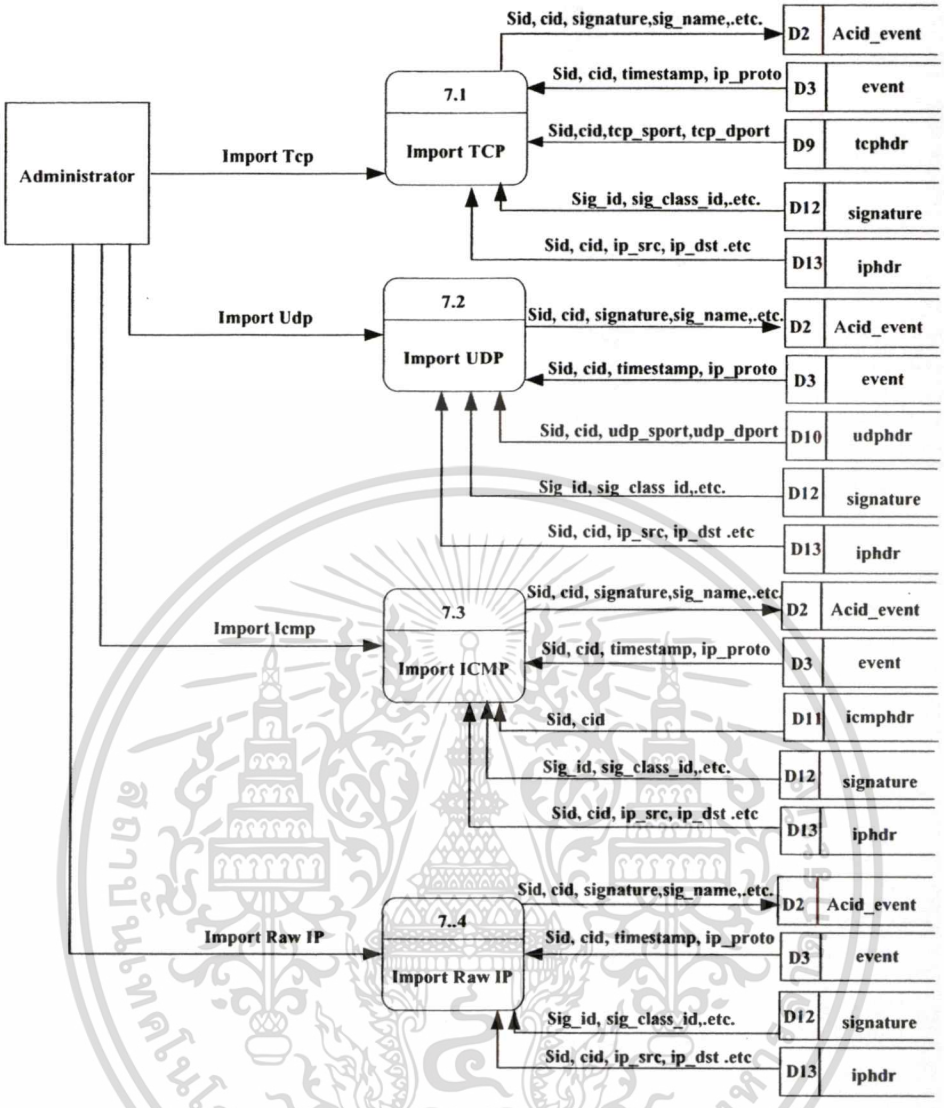
รูปที่ 3.14 แสดง Dataflow diagram level 2 ของ Maintain

จากรูปที่ 3.14 เป็นการแสดงการไหลของข้อมูลของ Dataflow diagram level 2 ในส่วนของ Maintain โดยส่วนนี้สามารถเรียกดู File Configuration และ Rules ที่ใช้งาน นอกจากนี้ยังสามารถสำรองกฎ กู้คืนกฎ และอัพโหลดกฎ แบ่งเป็น 2 ส่วนคือ ส่วนสนอร์ท กับส่วนไฟร์วอลล์ (IPFW)



รูปที่ 3.15 แสดง Dataflow diagram level 2 ของ Create Rules

จากรูปที่ 3.15 เป็นการแสดงการไหลของข้อมูลของ Dataflow diagram level 2 ในส่วนของ Create Rules ช่วยในการจัดการ rules สามารถสร้าง Rules และลบ Rules ของสนอร์ท และไฟร์วอลล์ (IPFW)

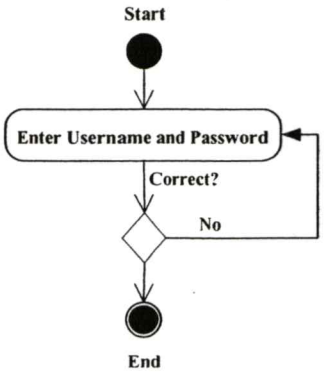


รูปที่ 3.16 แสดง Dataflow diagram level 2 ของ Import data

จากรูปที่ 3.16 เป็นการแสดงการไหลของข้อมูลของ Dataflow diagram level 2 ในส่วนของ Import data ใช้นำข้อมูลเข้าสู่ตาราง Acid_event เพื่อนำข้อมูลไปวิเคราะห์ในส่วนของฟังก์ชัน Alerts และฟังก์ชัน Search

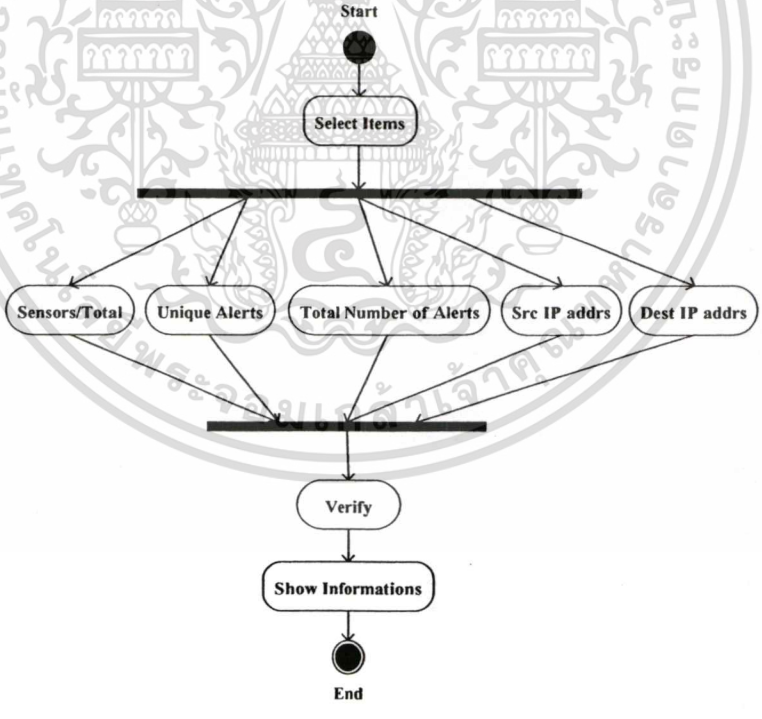
3.3.3 ฟังก์ชันการทำงาน

ระบบป้องกันการบุกรุกเครือข่ายเครือข่ายสามารถแสดงรายการ จำนวน และเปอร์เซนของการเตือน แสดงให้เห็นว่าโปรโตคอลไหนมีการใช้งานเป็นอย่างไร และมีฟังก์ชันการทำงานหลัก 7 ส่วน คือ ส่วนของ Alert , การ Login , การ Search, การทำ Maintain, การ Create Rules, การแสดง Sensor Interface และ การ Import data โดยมีรายละเอียดดังต่อไปนี้



รูปที่ 3.17 แสดง Activity ของ Autentication Login

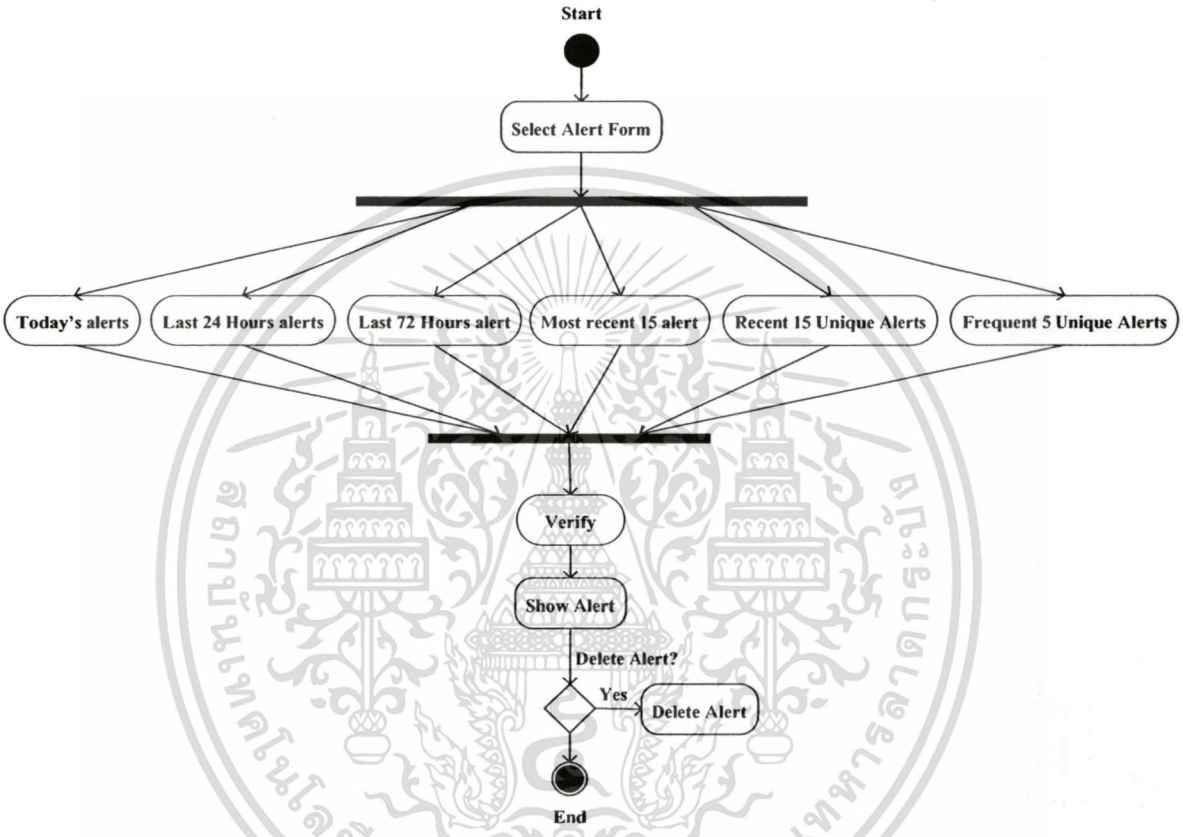
จากรูปที่ 3.17 แสดง Activity ของ Autentication Login เมื่อผู้ใช้กรอกข้อมูล Username และ password ระบบจะพิสูจน์สิทธิการเข้าใช้งานระบบ ว่าสามารถ Login เข้าสู่ระบบได้หรือไม่ แล้วจึงแสดงสถานะ Login ออกมา



รูปที่ 3.18 แสดง Activity ของ Main

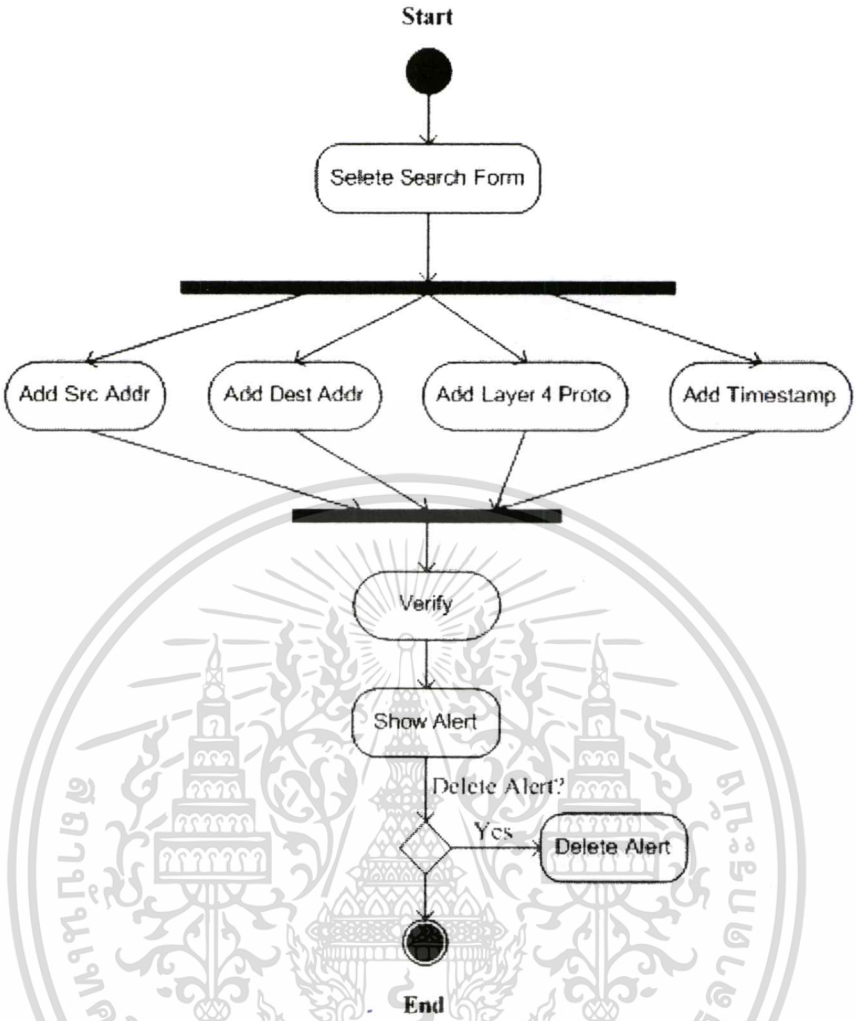
จากรูปที่ 3.18 แสดง Activity ของ Main ในการทำงานนี้สามารถเรียกดูรายละเอียดของ Sensor Interface, สามารถเรียกดู Unique Alerts, Total Number of Alerts, Src IP addrs และ Dest IP

addrs เพื่อนำมาวิเคราะห์และหาแนวทางป้องกัน โดย Src IP addrs ช่วยให้สามารถวิเคราะห์ Source IP address ที่มีการ Alerts ออกมาเป็นจำนวนเปอร์เซ็นและช่วงเวลาที่ตรวจสอบการใช้งาน และในส่วนของ Dest IP addrs แสดง Alerts ออกมาเป็นจำนวนเปอร์เซ็นและช่วงเวลาที่ตรวจสอบการใช้งานของ Destination IP address



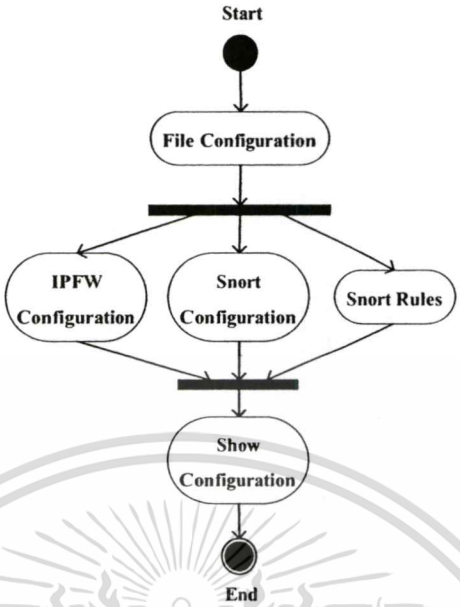
รูปที่ 3.19 แสดง Activity ของ Alert

จากรูปที่ 3.19 แสดง Activity ของ Alert เป็นลำดับการทำงานโดยเริ่มจากคลิก เลือกรูปแบบของ alert จากนั้นก็จะแสดงรายละเอียดการ alert โดยสามารถทำการลบ Alert ที่ต้องการได้



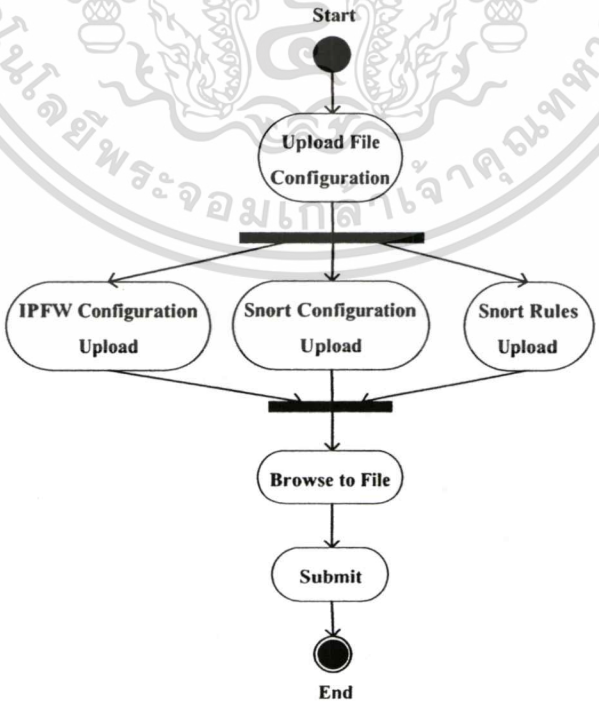
รูปที่ 3.20 แสดง Activity ของการ Search

จากรูปที่ 3.20 แสดง Activity ของ Search สามารถใส่ค่าที่ต้องการ เพื่อค้นหารายละเอียดที่ต้องการ และลบค่าการเตือนที่ต้องการได้



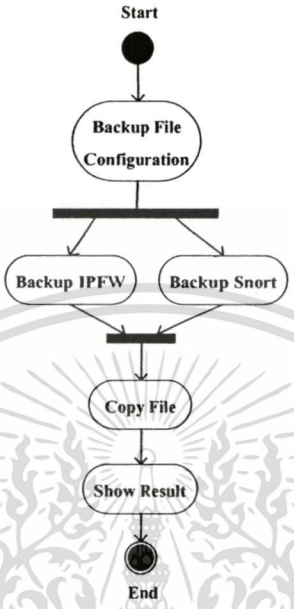
รูปที่ 3.21 แสดง Activity ของ File Configuration

จากรูปที่ 3.21 แสดง Activity ของ File Configuration ซึ่งใช้ในการสำรวจ File Configuration ที่ได้สร้างไว้ รวมถึง Rules ด้วย



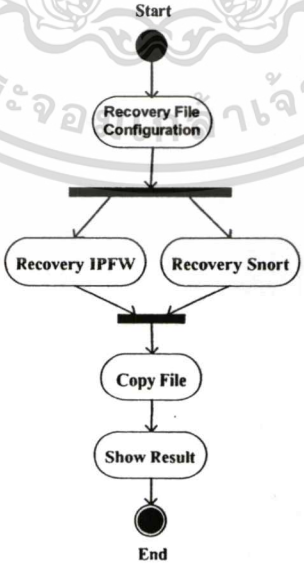
รูปที่ 3.22 แสดง Activity ของ Upload File Configuration

จากรูปที่ 3.22 แสดง Activity ของ Upload File Configuration ซึ่งใช้ในการ Upload File Configuration สามารถทำการ Upload File Configuration ที่ได้สร้างไว้ได้



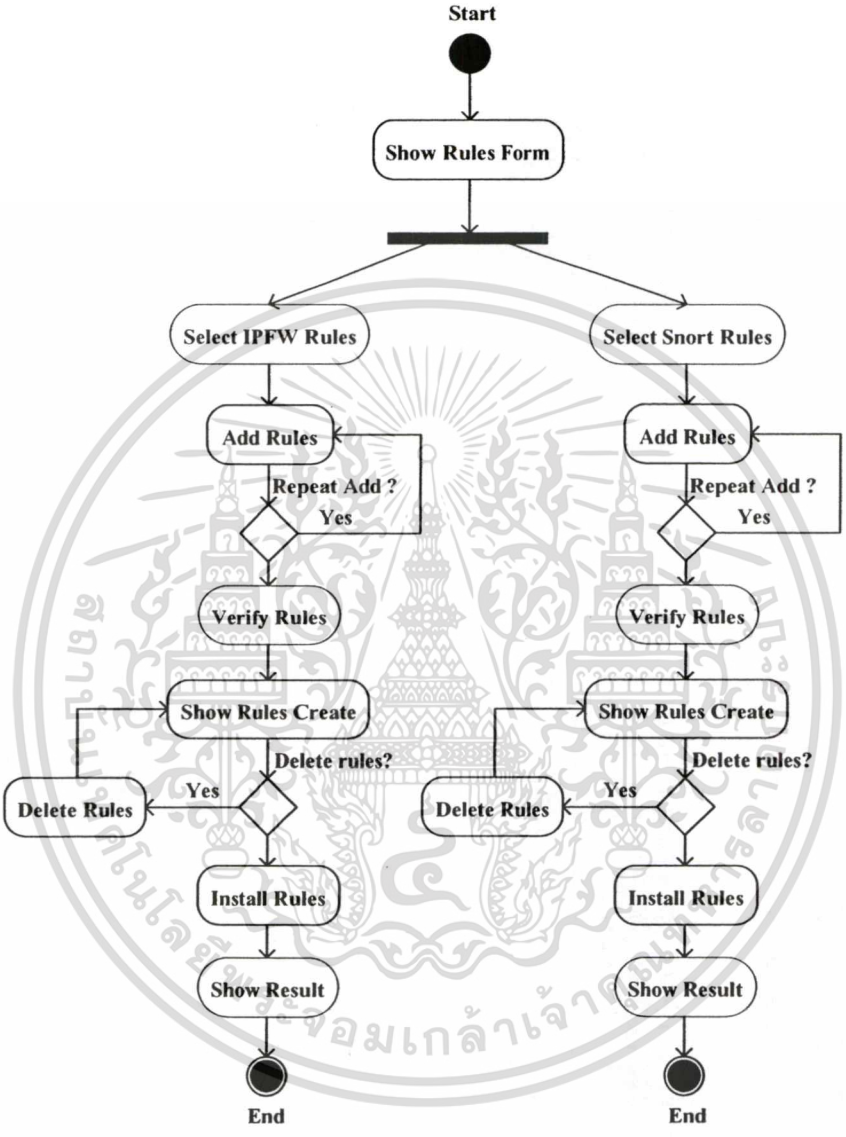
รูปที่ 3.23 แสดง Activity ของ Backup File Configuration

จากรูปที่ 3.23 แสดง Activity ของ Backup File Configuration เพื่อใช้ในการสำรองไฟล์



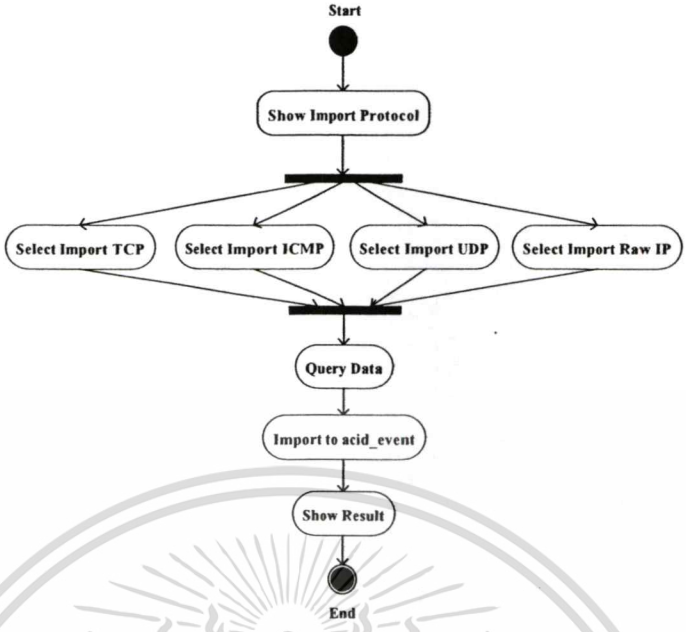
รูปที่ 3.24 แสดง Activity ของ Recovery File Configuration

จากรูปที่ 3.24 แสดง Activity ของ Recovery File Configuration เพื่อนำค่าที่เคยติดตั้งนำมาใช้งาน



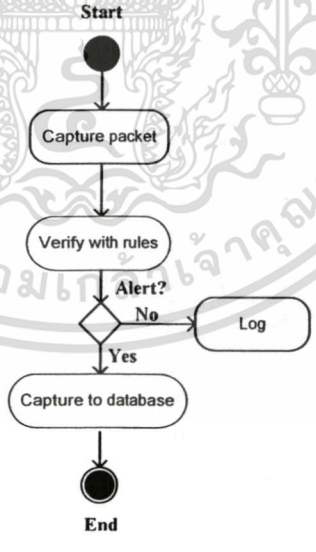
รูปที่ 3.25 แสดง Activity ของ Create Rules

จากรูปที่ 3.25 แสดง Activity ของ Create Rules โดยสามารถเข้าไปกำหนดกฎ หรือลบกฎที่สร้างขึ้นเองของสนอร์ท และของ IPFW Rules โดยสามารถเลือกการติดตั้ง และขั้นตอนการทำงาน



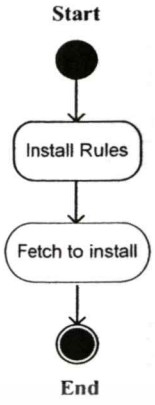
รูปที่ 3.26 แสดง Activity ของ Import data

จากรูปที่ 3.26 แสดง Activity ของ Import data เพื่อนำข้อมูลที่เก็บไว้มาแสดงผล ได้เร็วขึ้น



รูปที่ 3.27 แสดง Activity ของ Capture packet

จากรูปที่ 3.27 แสดง Activity ของ Capture packet ของ Snort โดยจะทำการดักจับแพ็กเก็ต แล้วทำการเปรียบเทียบกับ Rules ในกรณีที่ตรงกับ Snort Rules ที่เป็น Alert ก็จะทำการจัดเก็บลงฐานข้อมูลของ Snort แต่ถ้าเป็น log จะเก็บลง log file



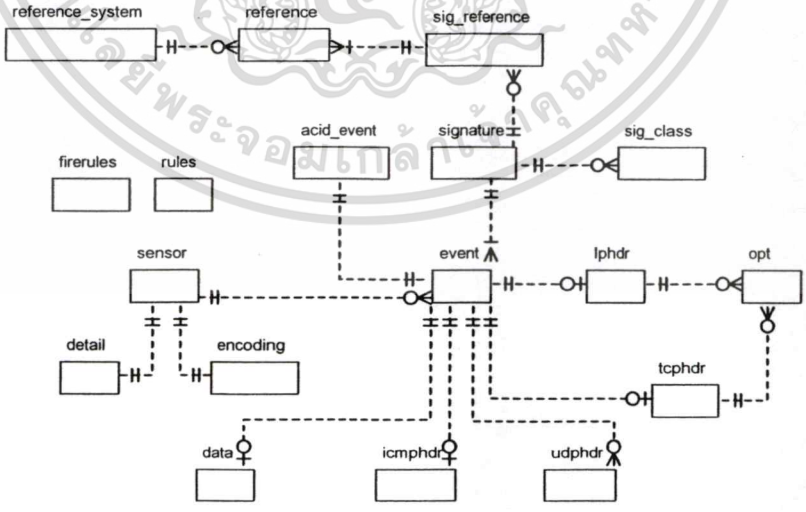
รูปที่ 3.28 แสดง Activity ของ IPFW

จากรูปที่ 3.28 แสดง Activity ของ IPFW เมื่อมีการติดตั้ง IPFW Rules ก็จะทำการดึง (Fetch) กฎมาทำการติดตั้ง

3.4 โครงสร้างฐานข้อมูล

3.4.1 โครงสร้างฐานข้อมูล Snort

โครงสร้างของฐานข้อมูล Snort มีรายละเอียดดังต่อไปนี้



รูปที่ 3.29 แสดง Entity Relationship diagram

จากรูปที่ 3.29 แสดง Entity Relationship diagram เพื่อแสดงความสัมพันธ์ของตารางในฐานข้อมูล Snort โดยรายละเอียดการจัดเก็บแสดงดังในตารางข้างล่าง

ตารางที่ 3.2 แสดงรายละเอียดของตาราง

ชื่อตาราง	**คำอธิบาย**
ตาราง Data	แสดงเนื้อหาของแพ็กเก็ตเพล์โหลด
ตาราง Detail	แสดงรายละเอียดที่เซ็นเซอร์เก็บล็อค
ตาราง encoding	แสดงประเภทการเข้ารหัสสำหรับแพ็กเก็ตเพล์โหลด
ตาราง Event	แสดง Meta-data ที่ตรวจพบ
ตาราง Icmphdr	แสดง ข้อมูลที่เก็บรายละเอียดของ ICMP protocol
ตาราง Iphdr	แสดงข้อมูลที่เก็บเก็บรายละเอียดของ IP protocol
ตาราง Opt	แสดงข้อมูลที่เก็บไอพี และทีซีพีอ๊อฟชั่น
ตาราง Reference	แสดงข้อมูลที่เก็บReference IDs สำหรับซิกเนอร์เซอร์
ตาราง Rules	แสดงการเก็บ rules ที่สร้างของ Snort
ตาราง Reference_system	แสดงข้อมูลที่เก็บรายการของ Reference system
ตาราง Sensor	แสดงข้อมูลที่เก็บชื่อเซ็นเซอร์
ตาราง Signature	แสดงรายการที่ใช้จัดระเบียบการ Alert ตาม signature names, priorities และ revision IDs
ตาราง Sig_class	แสดงการจัดการรายการของ alert กับ signature classifications
ตาราง Sig_reference	แสดงการเก็บข้อมูลอ้างอิงสำหรับซิกเนอร์เซอร์
ตาราง Tcphdr	แสดงการเก็บรายละเอียด TCP protocol
ตาราง Udphdr	แสดงการ เก็บรายละเอียด UDP protocol
ตาราง Acid_event	แสดงการเก็บข้อมูลเหตุการณ์ที่จะใช้แสดงผล
ตาราง firerules	แสดงการเก็บค่าในการสร้างกฎของ IPFW Rules

3.4.2 โครงสร้างตารางฐานข้อมูล Snort

ตารางที่ 3.3 แสดงฟิลด์ข้อมูลของตาราง Data

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
ข้อมูลเพล์โหลด	data_payload	text	คือ Packet payload ที่ถูกเข้ารหัสสอดคล้องกับ sensor.encoding

ตาราง Data คือ แสดงเนื้อหาของแพ็กเก็ตเพล์โหลด

ตารางที่ 3.4 แสดงฟิลด์ข้อมูลของตาราง Detail

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
ชนิดล็อค	detail_type	tinyint(3) unsigned	ประเภทล็อค คือ 0,1
รายละเอียดล็อค	detail_text	text	รายละเอียดการจัดเก็บล็อค คือ fast, full

ตาราง Detail คือ รายละเอียดที่เซ็นเซอร์เก็บล็อค

ตารางที่ 3.5 แสดงฟิลด์ข้อมูลของตาราง encoding

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
ประเภทการเข้ารหัส	encoding_type	Tinyint(3) unsigned	ประเภทการเข้ารหัส คือ 0,1,2
รูปแบบการเข้ารหัส	encoding_text	text	รูปแบบการเข้ารหัส คือ hex, base64, ascii

ตาราง Encoding คือ ประเภทการเข้ารหัสสำหรับแพ็กเก็ตเพล์โหลด

ตารางที่ 3.6 แสดงฟิลด์ข้อมูลของตาราง Event

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
หมายเลขซิกเนเชอร์	signature	int(10) unsigned	คือ Signature ID
ไทม์แสตมป์	timestamp	datetime	เก็บเวลาที่ทำการเก็บล็อค

ตาราง Event คือ Meta-data ที่ตรวจพบ

ตารางที่ 3.7 แสดงฟิลด์ข้อมูลของตาราง Icmphdr

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
ชนิดไอซีเอ็มพี	icmp_type	tinyint(3) unsigned	คือ ICMP type
โค๊ดไอซีเอ็มพี	icmp_code	tinyint(3) unsigned	คือ ICMP code
เช็คซัมไอซีเอ็มพี	icmp_csum	smallint(5) unsigned	คือ ICMP checksum
หมายเลขไอซีเอ็มพี	icmp_id	smallint(5) unsigned	คือ ICMP ID
ลำดับหมายเลขไอซีเอ็มพี	icmp_seq	smallint(5) unsigned	คือ ICMP sequence number

ตาราง Icmphdr คือ เก็บรายละเอียดICMP protocol

ตารางที่ 3.8 แสดงฟิลด์ข้อมูลของตาราง Iphdr

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
หมายเลขไอพีแอดเดสต้นทาง	ip_src	int(10) unsigned	คือ Source IP address (32-bit unsigned int)
หมายเลขไอพีแอดเดสปลายทาง	ip_dst	int(10) unsigned	คือ Destination IP address (32-bit unsigned int)

ตารางที่ 3.8 (ต่อ)

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
เวอร์ชั่นของไอพี	ip_ver	tinyint(3) unsigned	คือ IP version
ความยาวไอพีเฮดเดอร์	ip_hlen	tinyint(3) unsigned	คือ IP Header length
ไอพีไทป์อ๊อฟเซอร์วิส	ip_tos	tinyint(3) unsigned	คือ IP type-of-service
ความยาวดาต้าแกรมไอพี	ip_len	smallint(5) unsigned	คือ IP datagram length
หมายเลขไอดีไอพี	ip_id	smallint(5) unsigned	คือ IP ID
แฟก์ไอพี	ip_flags	tinyint(3) unsigned	คือ IP flags
หมายเลขอ๊อฟเซ็ตของไอพี	ip_off	smallint(5) unsigned	คือ IP fragment offset
ไทม์อ๊อฟไลท์ของไอพี	ip_ttl	tinyint(3) unsigned	คือ IP time-to-live
โปรโตคอลไอพี	ip_proto	tinyint(3) unsigned	คือ IP protocol
เช็คซัมไอพี	ip_csum	smallint(5) unsigned	คือ IP checksum

ตาราง Iphdr คือ เก็บรายละเอียด IP protocol

ตารางที่ 3.9 แสดงฟิลด์ข้อมูลของตาราง Opt

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
หมายเลขอ๊อฟชั่น	optid	int(10) unsigned	คือ Option ID (multiple options per alert)

ตารางที่ 3.9 (ต่อ)

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขอ๊อฟชั่นโฟโต้	opt_proto	tinyint(3) unsigned	คือ Option protocol (IP, TCP)
หมายเลขอ๊อฟชั่นโค๊ด	opt_code	tinyint(3) unsigned	คือ Option code
ขนาดของอ๊อฟชั่น	opt_len	smallint(6)	คือ Option length
ข้อมูลอ๊อฟชั่น	opt_data	text	คือ Option data

ตาราง Opt คือ เก็บไอพี และทีซีพีอ๊อฟชัน

ตารางที่ 3.10 แสดงฟิลด์ข้อมูลของตาราง Reference

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขรีเฟอร์เรนต์	ref_id	int(10) unsigned	คือ Reference ID
หมายเลขซิทเท็มรีเฟอร์เรนต์	ref_system_id	int(10) unsigned	คือ Reference system ID
หมายเลขเท็ก	ref_tag	text	คือ Reference tag (e.g. CVE-CAN-2001-01)

ตาราง Reference คือ เก็บ Reference IDs สำหรับซิกเนอร์เซอร์

ตารางที่ 3.11 แสดงฟิลด์ข้อมูลของตาราง Reference_system

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขซิทเท็มรีเฟอร์เรนต์	ref_system_id	int(10) unsigned	คือ Reference system ID
ชื่อหมายเลขซิทเท็ม	ref_system_name	varchar(20)	คือ Reference system name (e.g. CVE)

ตาราง Reference_system คือ เก็บรายการของ Reference system

ตารางที่ 3.12 แสดงฟิลด์ข้อมูลของตาราง Rules

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขลำดับ	id	int(10) unsigned Auto increment	คือจำนวนนับ
ชนิดแอ็คชั่น	action	varchar(10)	คือ Action (Alert,Log,Pass)
ชนิดโปรโตคอล	layer4	varchar(10)	คือ Layer4 Protocol
หมายเลขไอพีแอดเดสภายนอกเครือข่าย	exter_net	varchar(10)	คือ External IP address
หมายเลขพอร์ตภายนอกเครือข่าย	exter_port	varchar(5)	คือ External Port
ทิศทาง	direction	varchar(255)	คือ Direction
หมายเลขไอพีแอดเดสภายในเครือข่าย	home_net	varchar(10)	คือ Internal IP address
หมายเลขพอร์ตภายในเครือข่าย	home_port	varchar(5)	คือ Internal port
ข้อความ	msg	varchar(255)	คือ Message
เนื้อหา	content	varchar(255)	คือ Content
ชนิดคลาส	classtype	varchar(10)	Classtype(Attempted Admin)
หมายเลขไพร์ออริตี้	priority	int(10) unsigned	คือ priority
หมายเลขเซนเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขรีวิสชั่น	rev	int(10) unsigned	คือ Revision number

ตาราง Rules คือ ตารางเก็บ rules ที่สร้าง

ตารางที่ 3.13 แสดงฟิลด์ข้อมูลของตาราง Sensor

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซนเซอร์	sid	int(10) unsigned	คือ Sensor ID
ชื่อโฮส์ของเซ็นเซอร์	hostname	text	คือ โฮสต์ ของเซ็นเซอร์
อินเทอร์เฟส	interface	text	คือ Network interface

ตารางที่ 3.13 (ต่อ)

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
			(e.g. eth0)
ฟิวเตอร์	filter	text	คือ BPF filter
รายละเอียด	detail	tinyint(4)	คือ รายละเอียดการล็อค
การเอ็นโค๊ด	encoding	tinyint(4)	คือรูปแบบการเข้ารหัสของเพล์โหลด
อีเวนท์สุดท้าย	last_cid	int(10) unsigned	คือ Last Event ID

ตาราง Sensor คือ เก็บชื่อเซ็นเซอร์

ตารางที่ 3.14 แสดงฟิลด์ข้อมูลของตาราง Signature

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขซิกเนอร์เชอร์	sig_id	int(10) unsigned	Signature ID
ชื่อซิกเนอร์เชอร์	sig_name	varchar(255)	Signature Name
หมายเลยคลาสซิฟีเคชั่น	sig_class_id	int(10) unsigned	Classification ID
หมายเลขไฟร์ออริตี้	sig_priority	int(10) unsigned	Priority
หมายเลขรีวิสชั่น	sig_rev	int(10) unsigned	Revision number
หมายเลขซิกเนอร์เชอร์ภายใน	sig_sid	int(10) unsigned	Internal signature ID

ตาราง Signature คือ รายการที่ใช้จัดระเบียบการ Alert ตาม signature names, priorities และ revision IDs

ตารางที่ 3.15 แสดงฟิลด์ข้อมูลของตาราง Sig_class

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขคลาสซิฟีเคชั่น	sig_class_id	int(10) unsigned	คือ Classification ID
ชื่อคลาสซิฟีเคชั่น	sig_class_name	varchar(60)	คือ Classification name

ตาราง Sig_class คือ การจัดการรายการของ alert กับ signature classifications

ตารางที่ 3.16 แสดงฟิลด์ข้อมูลของตาราง Sig_reference

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขซิกเนอร์เชอร์	sig_id	int(10) unsigned	คือ Signature ID
หมายเลขลำดับรีเฟอร์เรนท์	ref_seq	int(10) unsigned	คือ Reference sequence number (multiple references)
หมายเลขรีเฟอร์เรนท์	ref_id	int(10) unsigned	คือ Reference ID

ตาราง Sig_reference คือ เก็บข้อมูลอ้างอิงสำหรับซิกเนอร์เชอร์

ตารางที่ 3.17 แสดงฟิลด์ข้อมูลของตาราง Tcphdr

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซนเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
หมายเลขพอร์ตทีซีพีต้นทาง	tcp_sport	smallint(5) unsigned	คือ TCP source port
หมายเลขพอร์ตทีซีพีปลายทาง	tcp_dport	smallint(5) unsigned	คือ TCP destination port
หมายเลขลำดับทีซีพี	tcp_seq	int(10) unsigned	คือ TCP sequence number
หมายเลขแอ็คทีซีพี	tcp_ack	int(10) unsigned	คือ TCP ACK number
อ๊อฟเซตทีซีพี	tcp_off	tinyint(3) unsigned	คือ TCP offset
ทีซีพีรีเซอร์ฟ	tcp_res	tinyint(3) unsigned	คือ TCP reserved
แฟ็กทีซีพี	tcp_flags	tinyint(3) unsigned	คือ TCP flags
ทีซีพีวินโดว์	tcp_win	smallint(5) unsigned	คือ TCP window
ทีซีพีเช็คซัม	tcp_csum	smallint(5) unsigned	คือ TCP checksum

ตารางที่ 3.17 (ต่อ)

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
พ็อยเตอร์ยูอาพีทีซีพี	tcp_urp	smallint(5) unsigned	คือ TCP urgent pointer

ตาราง Tcphdr คือ เก็บรายละเอียด TCP protocol

ตารางที่ 3.18 แสดงฟิลด์ข้อมูลของตาราง Udphdr

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
พอร์ตยูดีพีต้นทาง	udp_sport	smallint(5) unsigned	คือ UDP soure port
พอร์ตยูดีพีปลายทาง	udp_dport	smallint(5) unsigned	คือ UDP destination port
ขนาดยูดีพี	udp_len	smallint(5) unsigned	คือ UDP length
เช็คซัม	udp_csum	smallint(5) unsigned	คือ UDP checksum

ตาราง Udphdr คือ เก็บรายละเอียด UDP protocol

ตารางที่ 3.19 แสดงฟิลด์ข้อมูลของตาราง firerules

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขไอดี	id	int(10) unsigned auto_increment	เก็บหมายเลขไอดี
ไอพีไฟร์วอลล์	ipfw	VARCHAR(5)	เก็บไอพีไฟร์วอลล์
เพิ่ม	add1	VARCHAR(5)	เก็บเครื่องหมายเพิ่ม
หมายเลขกฎ	num	int(10) unsigned	เก็บหมายเลขกฎ
ปฏิเสธ	deny	VARCHAR(5)	เก็บการปฏิเสธ
โปรโตคอล	proto	VARCHAR(5)	เก็บโปรโตคอล
จาก	from1	VARCHAR(5)	เก็บตัวแปรจาก
หมายเลขเครือข่ายภายใน	in1	VARCHAR(15)	เก็บหมายเลขเครือข่ายภายใน
ถึง	to1	VARCHAR(4)	เก็บตัวแปรถึง
หมายเลขเครือข่าย	out	VARCHAR(15)	เก็บหมายเลขเครือข่าย

ตารางที่ 3.19 (ต่อ)

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
ภายนอก			ภายนอก
พอร์ต	sport	int(10)	เก็บหมายเลขพอร์ต

ตาราง firerules คือ ตารางที่ไว้เก็บค่าในการสร้างกฎของ IPFW Rules

ตารางที่ 3.20 แสดงฟิลด์ข้อมูลของตาราง Acid_event

ชื่อข้อมูล	ชื่อเขตข้อมูล	ชนิดของข้อมูล	คำอธิบาย
หมายเลขเซ็นเซอร์	sid	int(10) unsigned	คือ Sensor ID
หมายเลขอีเวนท์	cid	int(10) unsigned	คือ Event ID
หมายเลขซิกเนเชอร์	signature	int(10) unsigned	คือ Signature ID
ชื่อซิกเนอร์เชอร์	sig_name	varchar(255)	คือ sig_id
หมายเลขคลาสซิฟีเคชั่น	sig_class_id	int(10) unsigned	คือ Classification ID
หมายเลขไพร์ออริตี้	sig_priority	int(10) unsigned	Priority
ไทม์แสตมป์	timestamp	datetime	เก็บเวลาที่ทำการเก็บล็อค
หมายเลขไอพีแอดเดสต้นทาง	ip_src	int(10) unsigned	คือ Source IP address (32-bit unsigned int)
หมายเลขไอพีแอดเดสปลายทาง	ip_dst	int(10) unsigned	คือ Destination IP address (32-bit unsigned int)
โปรโตคอลไอพี	ip_proto	tinyint(3) unsigned	คือ IP protocol
หมายเลขเลเยอร์4 พอร์ตต้นทาง	layer4_sport	smallint(5) unsigned	คือ พอร์ตต้นทาง
หมายเลขเลเยอร์4 พอร์ตปลายทาง	layer4_dport	smallint(5) unsigned	คือ พอร์ตปลายทาง

3.5 โครงสร้างของ Configuration File

ระบบส่วนติดต่อกับผู้ใช้แบบเว็บสำหรับการจัดการระบบป้องกันการบุกรุกเครือข่ายมี Configuration files ดังนี้

3.5.1 System Configuration file

ประกอบไปด้วยไฟล์คอนฟิกต่างๆดังนี้

/etc/rc.conf เป็นไฟล์ที่เก็บข้อมูล ไอพีแอดเดรส ชื่อเครื่อง เกตเวย์ เป็นต้น

/usr/local/etc/apache22/httpd.conf เป็นไฟล์ไว้เก็บการกำหนดค่าการทำงานของเว็บเซิร์ฟเวอร์

3.5.2 IPFW Configuration file

/etc/IPFW.conf.sh เป็นไฟล์ที่ใช้สร้าง และกำหนดกฎของไฟร์วอลล์

เช่น กำหนดในไฟล์ดังนี้

```
/sbin/ipfw -f flush
/sbin/ipfw add 1500 divert natd ip from any to any via le1
```

3.5.3 Snort Configuration file

/usr/local/etc/snort_inline.conf เป็นไฟล์ที่ใช้ไว้ตั้งค่าของโปรแกรมสนอร์ท เช่นปรับให้ข้อมูลเข้าเก็บในฐานข้อมูล โดยมีโครงสร้างดังนี้

output database: [log | alert], [type of database], [parameter list]

<u>หมายเหตุ</u>

[log | alert] คือ ระบุว่าจะเก็บข้อมูลในส่วนของ alert หรือ log โดยปกติแล้วจะใช้ log

[type of database] เช่น mysql หรือ postgresql หรือ unixodbc

[parameter list] กำหนดให้ key=value คั่นแต่ละ key ด้วยช่องว่าง โดย key คือ

- Dbname คือชื่อฐานข้อมูลที่เชื่อมต่อ
- Host คือ ชื่อโฮส์ของ RDBMS ที่ใช้
- Port คือ ชื่อพอร์ตของ RDBMS ที่ใช้
- Password คือ รหัสผ่านการเข้าฐานข้อมูล
- Sensor_name คือ ชื่อ sensor ของสนอร์ท ถ้าไม่ระบุจะสร้างให้เอง

- Encoding คือ การเข้ารหัสข้อมูล มีสามชนิดคือ hex, base64 และ ascii

- Detail คือ รายละเอียดการเก็บข้อมูล มี full และ fast (default)

ตัวอย่างเช่น

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

การรัน Snort (daemon)

Snort_inline –D –c /etc/snort_inline/snort_inline.conf –i eth1 –u snort –N –l /var/log/snort_inline/YYYYMMDD

หมายเหตุ

-D คือ รันในโหมด daemon mode

-c คือ Load configuration file

-i คือ อินเทอร์เฟส

-u คือ รันโดย UID user

-N คือ ไม่เก็บ log โดยให้ Alert ปกติ

-l คือ กำหนดตำแหน่งที่เก็บ log

บทที่ 4
การพัฒนาและผลการทดสอบระบบ

ในการพัฒนาระบบงานของระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ โดยใช้สนอร์ท และ IPFW พร้อมการเชื่อมต่อกับผู้ใช้ผ่านทางเว็บเบสยูสเซอร์อินเตอร์เฟส ขั้นตอนการพัฒนาระบบงานมีดังนี้

4.1 การวางแผนการปฏิบัติงาน

การวางแผนการปฏิบัติงาน ได้เลือกใช้ระบบปฏิบัติการ ฮาร์ดแวร์ และซอฟต์แวร์ เพื่อพัฒนาระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ และโปรแกรมเว็บเบสสำหรับการควบคุมสั่งงานดังต่อไปนี้

4.1.1. ระบบปฏิบัติการ เลือกใช้ระบบปฏิบัติการ FreeBSD 7.0

เป็นระบบปฏิบัติการแบบยูนิกซ์ที่ได้รับความนิยมอย่างแพร่หลาย และไม่ต้องเสียค่าใช้จ่าย โดยระบบปฏิบัติการฟรีบีเอสดี นั้นเป็นระบบปฏิบัติการที่มีเสถียรภาพและมีความปลอดภัยสูงกว่าระบบปฏิบัติการ Linux สามารถ download ได้จาก ftp://ftp.freebsd.org/pub/FreeBSD/releases/

4.1.2. ซอฟต์แวร์ช่วยตรวจสอบแพ็กเก็ต เลือกใช้ Snort_inline เวอร์ชัน 2.4.5 เป็นโปรแกรมสำหรับตรวจจับแพ็กเก็ต สนอร์ทอินไลนเป็นระบบตรวจจับการบุกรุกที่ดัดแปลงมาจากระบบตรวจจับการบุกรุกของสนอร์ท ซึ่งเป็นเครื่องมือที่ใช้ตรวจจับและป้องกันการบุกรุกเครือข่าย โดยสามารถดาวน์โหลดได้จากเว็บไซต์ http://snort_inline.sourceforge.net/download.html

4.1.3. ภาษาที่ใช้ในการพัฒนาซอฟต์แวร์ เลือกใช้ PHP เวอร์ชัน 5.2.5

ภาษา PHP จัดเป็นภาษา script ที่สามารถทำงานร่วมกับ HTML โดยสามารถเขียน script แทรกเข้าไปใน tag ภาษา HTML ได้ หรือสามารถเขียนเป็นไฟล์ PHP ก็ได้ โดย PHP เป็น open source ที่สามารถใช้งานได้กับหลายๆ ระบบปฏิบัติการ เช่น Windows, Linux , Unix เป็นต้น และยังสามารถรองรับการติดต่อกับฐานข้อมูลหลายๆ ชนิดด้วย สามารถดาวน์โหลดได้จากเว็บไซต์ www.php.net

4.1.4. เว็บเซิร์ฟเวอร์ เลือกใช้ Apache เวอร์ชั่น 2.2.6

เป็นเว็บเซิร์ฟเวอร์ที่สามารถจัดการได้อย่างมีประสิทธิภาพสูง และสามารถทำงานตอบสนองต่อระบบงานได้ ดาวน์โหลดได้จากเว็บไซต์ http://www.apache.net/

4.1.5. ระบบฐานข้อมูล เลือกใช้โปรแกรม MySQL Server เวอร์ชั่น 5.0.45

โปรแกรม MySQL เป็นฐานข้อมูล ช่วยในการเก็บข้อมูลให้เป็นระเบียบ รองรับคำสั่ง SQL (Structured Query Language) เป็นซอฟต์แวร์โอเพนซอร์ส สามารถดาวน์โหลดได้ที่ www.sql.com

4.2 การพัฒนาระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์

การพัฒนาระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์ โดยมีลำดับการพัฒนาดังต่อไปนี้

4.2.1 ติดตั้งโปรแกรม IPFW และตั้งค่าระบบแปลงไอพีแอดเดรส หรือ NAT

เพื่อทำหน้าที่ในการแปลงไอพีแอดเดรสส่วนบุคคลไปเป็นไอพีแอดเดรสสาธารณะให้ผู้ใช้งานภายในเครือข่ายสามารถออกสู่อินเตอร์เน็ต โดยคอมไฟล์ Kernel บนระบบปฏิบัติการฟรีบีเอสดี หลังจากนั้นก็ไปตั้งค่าใน /etc/rc.conf

สร้างไฟล์ ipfw.conf.sh เพื่อใช้กำหนด Rules และสร้าง NAT ดังนี้

```
/sbin/ipfw -f flush
/sbin/ipfw add 1500 divert natd all from any to any via le1
/sbin/ipfw add 6500 pass all from any to any
```

แล้วค่อยสร้างกฎมาควบคุมในภายหลัง

4.2.2 ติดตั้งฐานข้อมูล คือ Mysql

ใช้เก็บข้อมูล เพื่อความเป็นระเบียบของข้อมูล และสะดวกต่อการเรียกใช้งานข้อมูลได้รวดเร็ว

4.2.3 ติดตั้งโปรแกรมเว็บเซิร์ฟเวอร์ คือ Apache

เพื่อทำเป็นเว็บเซิร์ฟเวอร์ ในการ Remote เข้ามาจัดการข้อมูล

4.2.4 ติดตั้งโปรแกรม PHP

เพื่อใช้จัดการการทำงานบนเว็บ

4.2.5 ติดตั้งโปรแกรม Snort_inline

เพื่อใช้ตรวจจับแพ็กเก็ต

4.2.6 จัดการแก้ไขไฟล์ Snort_inline.conf

เพื่อกำหนดรูปแบบการจัดเก็บไฟล์ ซึ่ง มีดังนี้

output alert_full: snort_inline-full.log เป็นการจัดเก็บแบบ Full log

output alert_fast: snort_inline-fast.log เป็นการจัดเก็บแบบ Fast log

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

เป็นการจัดเก็บลงฐานข้อมูล

4.2.7 จัดการ Path ที่เก็บไฟล์ Rules

เพื่อกำหนด Path ที่ใช้เก็บ Rules โดย Rules สามารถไปดาวน์โหลดได้ที่ www.snort.org

RULE_PATH /www/rules

4.2.8 จัดการเกี่ยวกับ log

เพื่อจัดการ log ให้จัดเก็บตามที่กำหนด โดยสามารถกำหนดรายละเอียดการจัดเก็บ log ได้ที่ /usr/local/etc/snort_inline/logrotate.d ดังนี้

```
/var/log/snort/alert /var/log/snort/*log{
   Daily
   rotate 7
   size 100k
   missingok
   compress
   sharedscripts
   postrotate
        /etc/init.d/snortd restart 1>/dev/null || true
   endscript
}
```

หมายเหตุ โดยอธิบายส่วนที่สำคัญในการปรับปรุงระบบ อันแรกเป็น Daily คือการจัดเก็บ log รายวัน ซึ่งถ้าเยอะไปสามารถกำหนดให้จัดเก็บเป็นรายเดือน คือ monthly ต่อมาเป็น size 100k กำหนดขนาดไฟล์ที่จัดเก็บ ในที่นี้คือ 100k และ compress คือให้ขัดเก็บแบบบีบอัด สามารถแก้เป็น nocompress ได้

4.2.9 รันโปรแกรม snort_inline

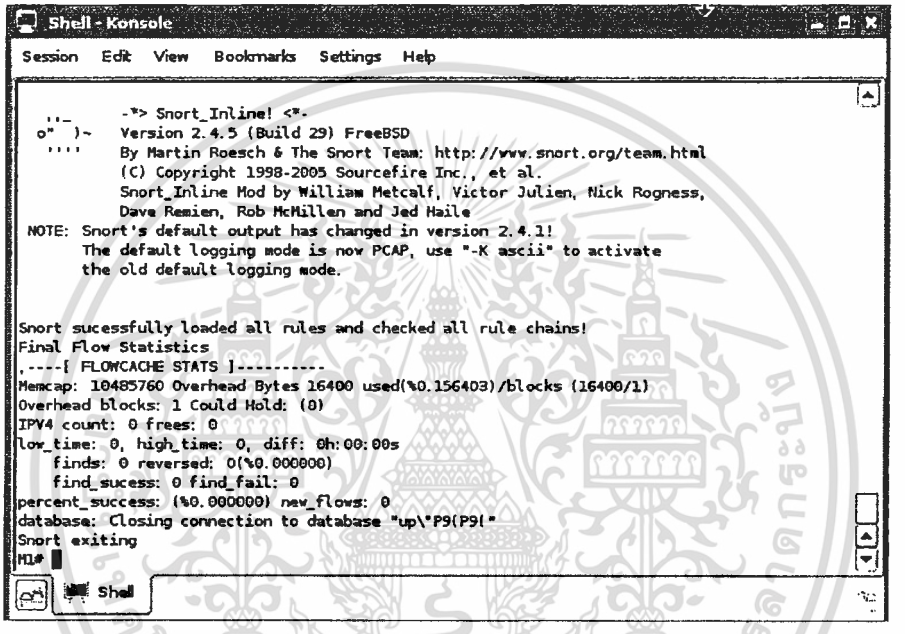
จากนั้นทำการรันให้สนอร์ททำงานดังนี้

snort_inline –D –c /usr/local/etc/snort_imline.conf

การทดสอบ Rules ของสนอร์ท ใช้คำสั่งดังนี้

snort_inline –T –c /usr/local/etc/snort_inline.conf

ถ้า Rules ไม่มีข้อผิดพลาดจะปรากฏข้อความดังนี้

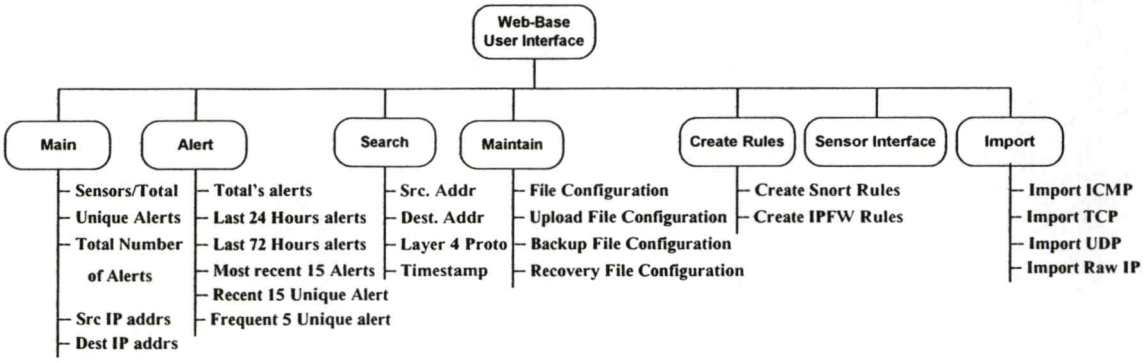


รูปที่ 4.1 แสดงผลการทดสอบ Rules ของสนอร์ท

จากรูปที่ 4.1 แสดงผลการทดสอบ Rules ของสนอร์ท ถ้า Rules ถูกต้อง จะไม่มีข้อผิดพลาด (Error) เกิดขึ้น

4.3 โครงสร้างเว็บเบสยูสเซอร์อินเตอร์เฟส

โครงสร้างของเว็บเบสยูสเซอร์อินเทอร์เฟสสามารถแสดงได้ดังนี้

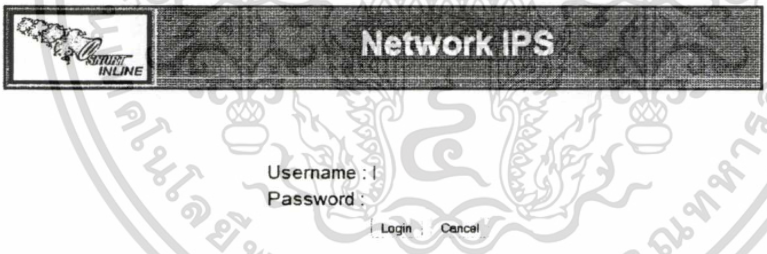


รูปที่ 4.2 แสดงโครงสร้างการทำงานของเว็บเบสยูสเซอร์อินเทอร์เฟส

จากรูปที่ 4.2 แสดงโครงสร้างการทำงานของเว็บเบสยูสเซอร์อินเทอร์เฟส เป็นภาพรวมของระบบเว็บเบสยูสเซอร์อินเทอร์เฟส เพื่อใช้วิเคราะห์ และสร้างกฎในการป้องกันระบบผ่านเว็บ

4.3.1 เว็บเบสยูสเซอร์อินเทอร์เฟส Login

เว็บเบสยูสเซอร์อินเทอร์เฟส Login เป็นส่วนที่ป้องกันการเข้าใช้เว็บเบสยูสเซอร์อินเทอร์เฟสโดยที่ไม่ได้รับการอนุญาต

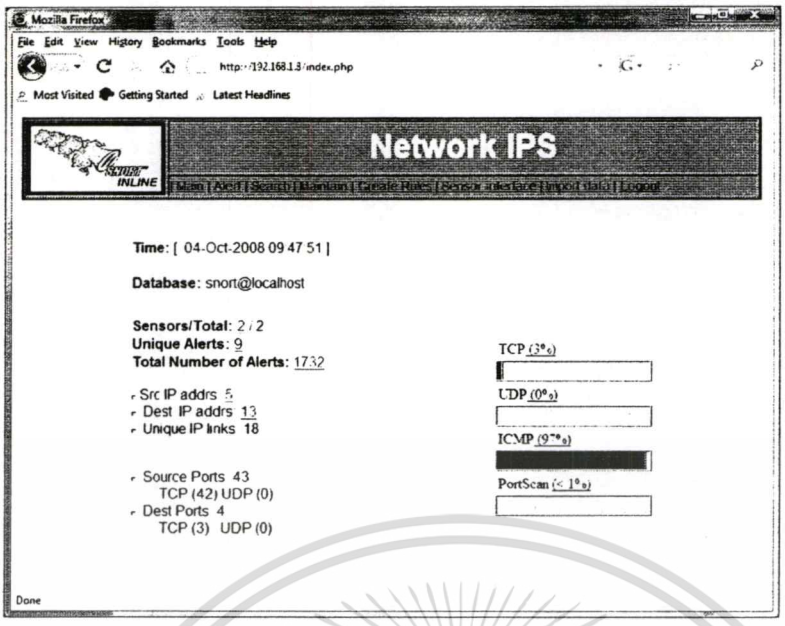


รูปที่ 4.3 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟส Login

จากรูปที่ 4.3 เป็นการแสดงหน้า Login ของเว็บเบสยูสเซอร์อินเทอร์เฟส

4.3.2 เว็บเบสยูสเซอร์อินเทอร์เฟส Main

เว็บเบสยูสเซอร์อินเทอร์เฟส Main แสดงรายละเอียดการเตือน เพื่อใช้ในการวิเคราะห์ระบบ ดังรูปที่ 4.4

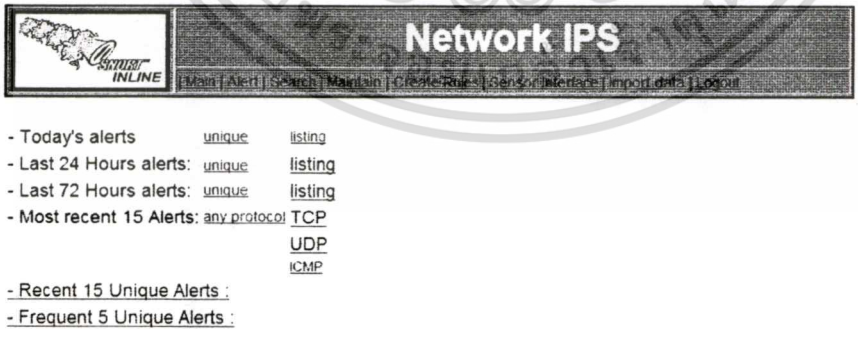


รูปที่ 4.4 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า main

จากรูปที่ 4.4 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า main สามารถวิเคราะห์ทราฟิกที่มีการ Alert โดยสามารถดูเปอร์เซ็นของการใช้งานของ Src IP addrs และ Dest IP addrs และจำนวน Alerts ทั้งหมดได้

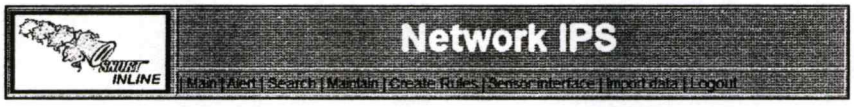
4.3.3 เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Alert

เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Alert แสดงการเตือน โดยแสดง ดังรูปที่ 4.5



รูปที่ 4.5 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Alert

จากรูปที่ 4.5 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Alert โดยหน้านี้สามารถเรียกดู Alerts โดยสามารถเรียกดูได้เช่น Today's alerts , Last 24 Hours alerts, Last 72 Hours alerts, Most recent 15 Alerts, Recent 15 Unique alerts และ Frequent 5 Unique Alerts



Listing Alerts ALL : Last 15 Alerts

Delete Alert

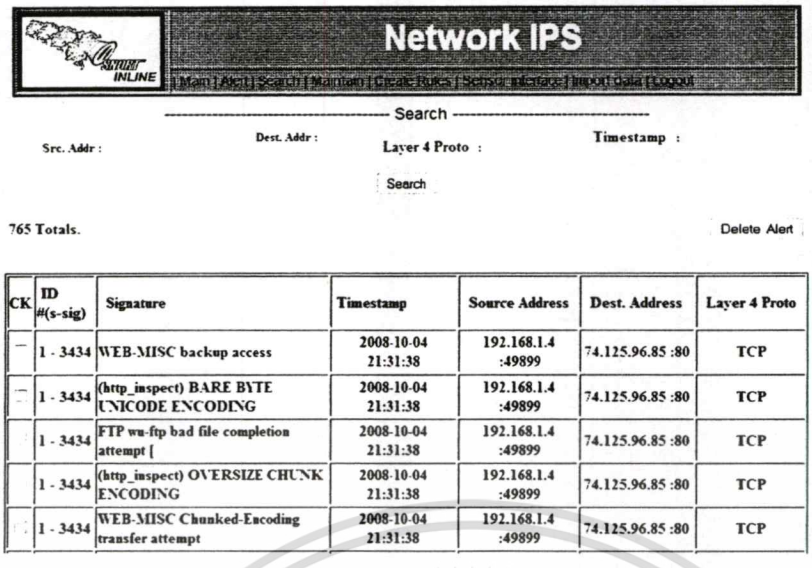
CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 108	(http_inspect) BARE BYTE UNICODE ENCODING	2008-10-03 10:28:42	192.168.226.3 : 2199	203.150.224.132 : 80	TCP
	1 - 121	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:50	192.168.226.3 : 2199	203.150.224.132 : 80	TCP
	1 - 137	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:21	192.168.226.3 : 2192	203.151.233.16 : 80	TCP
	1 - 159	(http_inspect) BARE BYTE UNICODE ENCODING	2008-10-03 10:29:32	192.168.1.4 : 49398	192.168.1.8 : 80	TCP
	1 - 164	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:32	192.168.226.3 : 2233	203.151.233.16 : 80	TCP
	1 - 166	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:33	192.168.226.3 : 2237	203.151.233.16 : 80	TCP
	1 - 168	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:49	192.168.1.4 : 49390	192.168.1.8 : 80	TCP
	1 - 189	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:51	192.168.226.3 : 2199	203.150.224.132 : 80	TCP

รูปที่ 4.6 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Most Recent 15 Alerts: TCP

จากรูปที่ 4.6 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Alert in last 15 Alerts ซึ่งแสดงรายละเอียดผลการทดลอง

4.3.4 เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Search

เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Search สามารถใส่ค่าเพื่อค้นหาได้คือ Src.Addr, Dest.Addr, Layer 4 Proto และ Timestamp ดังรูปที่ 4.7

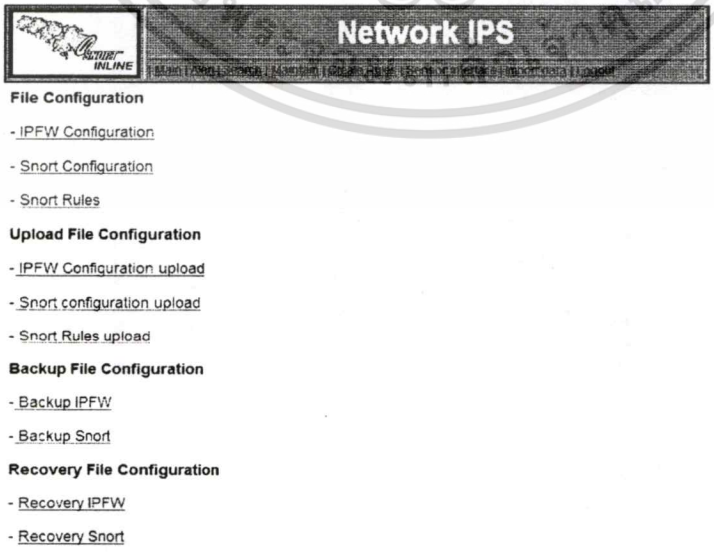


รูปที่ 4.7 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Search โดยค้นหาโปรโตคอล TCP

จากรูปที่ 4.7 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Search โดยค้นหาโปรโตคอล TCP หน้าเว็บ Search สามารถใช้ค้นหาข้อมูลที่ต้องการโดยอาศัยคำที่ต้องการค้น สามารถค้นหาเพื่อดู Src addr หรือ Dest addr หรือ Layer 4 Proto หรือ Timestamp

4.3.5 เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Maintain

เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า File configuration ใช้จัดการกับ Configuration file ต่างๆ คือ IPFW Configuration, Snort Configuration และสามารถเรียกค่า Configuration file เก่ามาใช้งาน



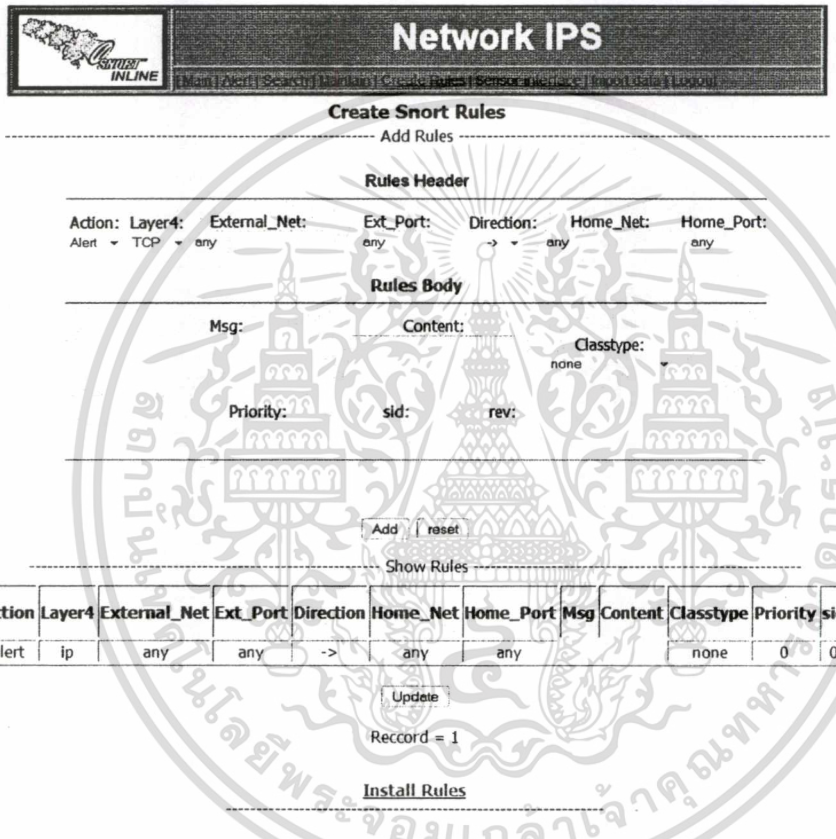
รูปที่ 4.8 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Maintain

จากรูปที่ 4.8 แสดงหน้าเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Maintain ซึ่งรายละเอียดจะกล่าวในภาคผนวก

4.3.6 เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Create Rules

เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Create Rules แบ่งเป็น 2 ส่วนคือ

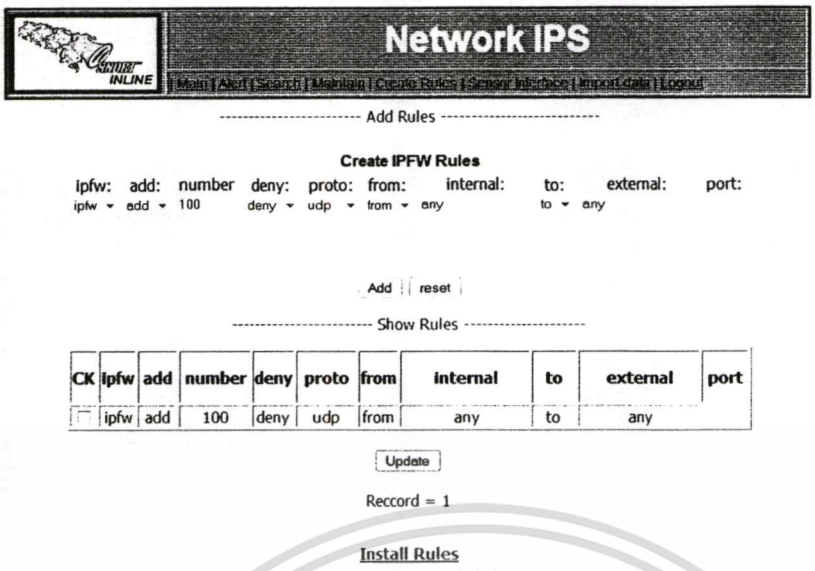
- เพื่อใช้จัดการ Rules ของสนอร์ท สามารถเพิ่มกฎ และลบกฎ



รูปที่ 4.9 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Create Rules

หมายเหตุ ค่า Rules ที่ทำการเพิ่มเข้าไปจำต้องมีหมายเลข sid ที่มากกว่า 1,000,000 ในกรณีที่ต้องการกำหนดเอง หรือใช้ค่า sid ที่มีอยู่ก็ได้ หรือ ไม่ต้องกำหนดในส่วน Rules body ก็ใช้ได้แล้ว การทำงานในการกำหนด Rules เองอาจจะไม่รัดกุมพอ ดังนั้นควรไป update Rules เสมอ โดยการไปดาวน์โหลด Rules ได้ที่เว็บของสนอร์ท

- เพื่อใช้ในการสร้าง IPFW Rules โดยสามารถจัดการได้ ดังรูปที่ 4.10

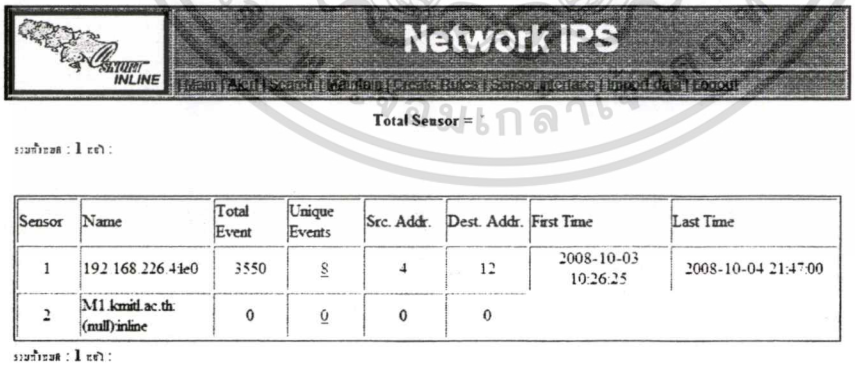


รูปที่ 4.10 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า IPFW Rules

จากรูปที่ 4.10 แสดงหน้าเว็บการสร้าง IPFW Rules โดยสามารถสร้างกฎ และทำการลบกฎที่สร้างขึ้นได้

4.3.7 เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Sensor Interface

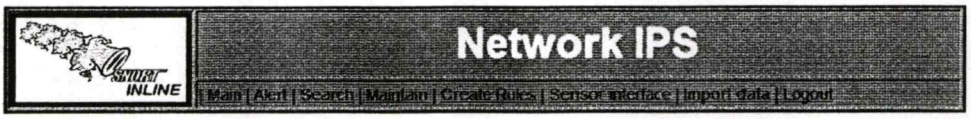
แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Sensor Interface แสดงจำนวน Sensor Interface ที่ตรวจจับและจำนวนเหตุการที่ตรวจจับ รายละเอียดอื่นๆ ดังรูปที่ 4.11



รูปที่ 4.11 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Sensor Interface

จากรูปที่ 4.11 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Sensor Interface แสดงชื่อของ Sensor Interface

4.3.8 เว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Import data

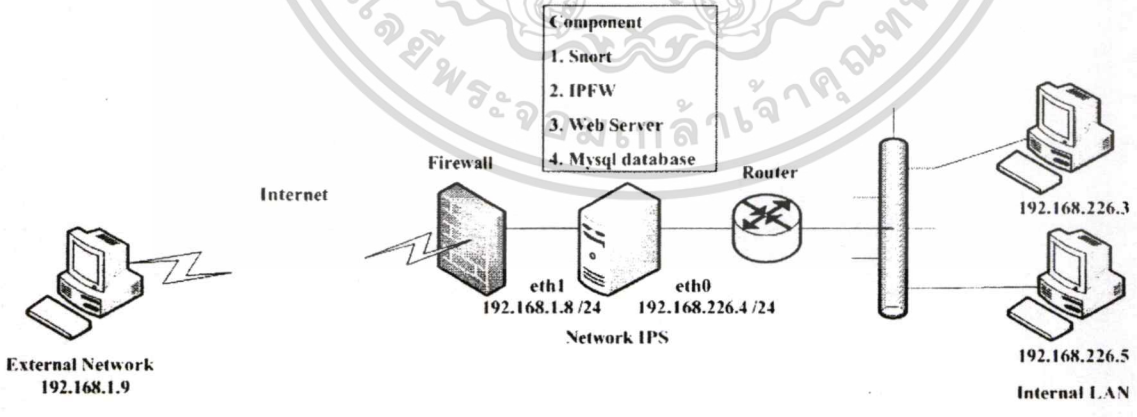


รูปที่ 4.12 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Import data เข้าสู่ตาราง acid_event

จากรูปที่ 4.12 แสดงการ Import data เข้าสู่ตาราง acid_event โดยออกแบบมาเบื้อต้นเพื่อใช้นำเข้าข้อมูลเพื่อการวิเคราะห์

4.4 การทดสอบระบบโดยใช้ PortScan

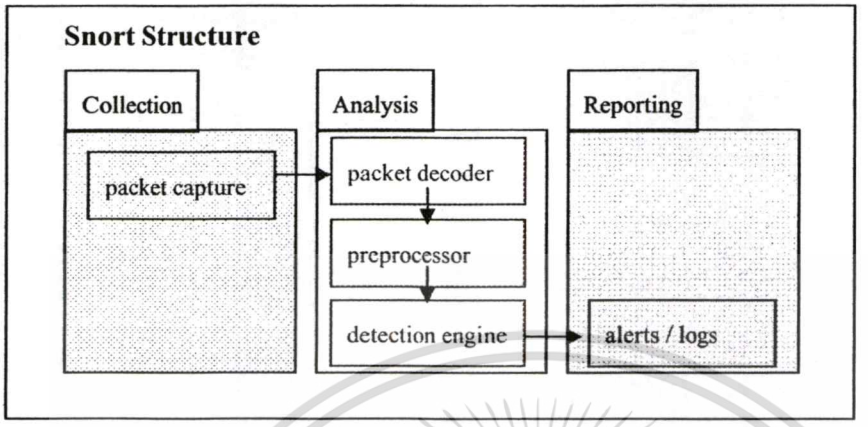
การทดสอบโดยการใช้ โปรแกรม PortScan ทำการ Scan เพื่อตรวจสอบการตรวจจับการบุกรุก โดยมีไดอะแกรมการทดสอบ ดังรูปที่ 4.13



รูปที่ 4.13 แสดงไดอะแกรมการทำงานของระบบป้องกันการบุกรุกเครือข่าย

จากรูปที่ 4.13 แสดงไดอะแกรมการทำงานของระบบป้องกันการบุกรุกเครือข่ายโดยอนุญาตให้เครือข่ายภายในสมารถติดต่อไปยัง Internet ได้ และป้องกันไม่ให้ External network เข้า

มาใช้งานภายในเครือข่าย และมีการตรวจจับแพ็กเก็ตแสดง Alerts เพื่อใช้ในการวิเคราะห์ป้องกันระบบเครือข่าย สามารถแสดงโครงสร้างการตรวจจับแพ็กเก็ตได้ ดังรูปที่ 4.14

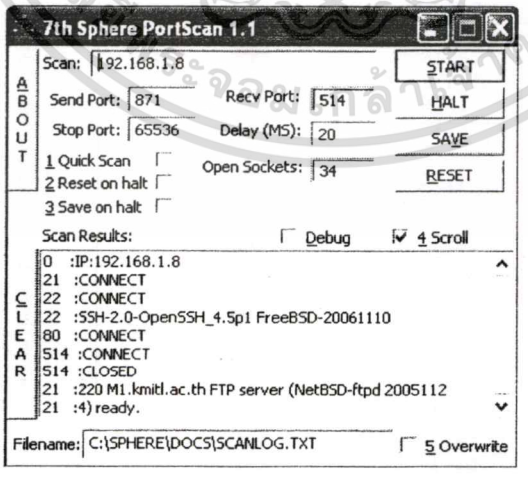


รูปที่ 4.14 แสดงไดอะแกรมการทำงานของ Snort

จากรูปที่ 4.14 แสดงถึงลำดับการทำงานของโปรแกรมสนอร์ท โดยสนอร์ทจะรับแพ็กเก็ตแล้วทำการตรวจจับทำการวิเคราะห์และทำการเตือนเมื่อแพ็กเก็ตนั้นต้องสงสัย หรือ มีรายละเอียดตรงกับ Rules ที่กำหนดไว้ จากนั้นก็นำไปสร้างกฎเพื่อควบคุมการใช้งานเครือข่าย

4.4.1 รันโปรแกรม PortScan

การรันโปรแกรม PortScan สามารถแสดงได้ ดังรูปที่ 4.15

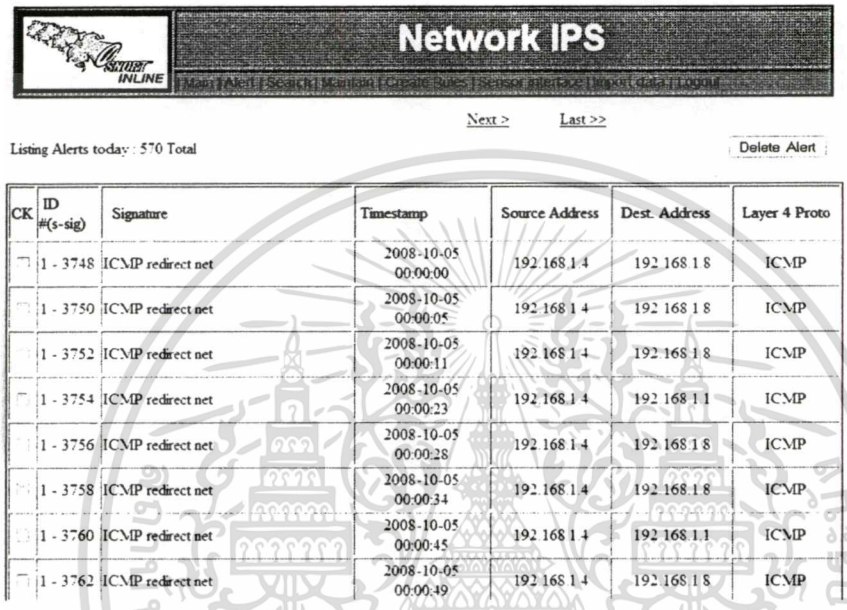


รูปที่ 4.15 แสดงโปรแกรม Portscan

จากรูปที่ 4.15 แสดงการรันโปรแกรม Portscan เพื่อใช้ทดสอบการตรวจจับการบุกรุก โดยสังเกตจากพฤติกรรมการเข้าถึงของแพ็กเก็ต

4.4.2 ผลการทดลองที่มีการ Alert

ผลการทดสอบสามารถแสดงได้ ดังรูปที่ 4.16



CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
☐	1 - 3748	ICMP redirect net	2008-10-05 00:00:00	192.168.1.4	192.168.1.8	ICMP
☐	1 - 3750	ICMP redirect net	2008-10-05 00:00:05	192.168.1.4	192.168.1.8	ICMP
☐	1 - 3752	ICMP redirect net	2008-10-05 00:00:11	192.168.1.4	192.168.1.8	ICMP
☐	1 - 3754	ICMP redirect net	2008-10-05 00:00:23	192.168.1.4	192.168.1.1	ICMP
☐	1 - 3756	ICMP redirect net	2008-10-05 00:00:28	192.168.1.4	192.168.1.8	ICMP
☐	1 - 3758	ICMP redirect net	2008-10-05 00:00:34	192.168.1.4	192.168.1.8	ICMP
☐	1 - 3760	ICMP redirect net	2008-10-05 00:00:45	192.168.1.4	192.168.1.1	ICMP
☐	1 - 3762	ICMP redirect net	2008-10-05 00:00:49	192.168.1.4	192.168.1.8	ICMP

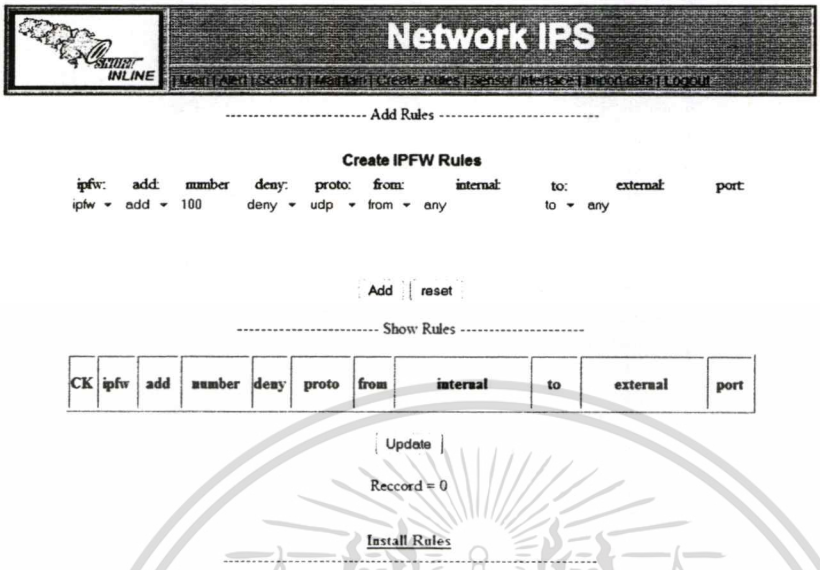
รูปที่ 4.16 แสดงหน้าเว็บเบสยูสเซอร์อินเทอร์ของการเตือนวันนี้

จากรูปที่ 4.16 เมื่อทำการ Scan ระบบจะรู้ได้ว่ามีการ Scan Port โดยการตรวจสอบของสนอร์ท ซึ่งจะไปตรงกับ singnature ที่ได้กำหนดไว้ ก็จะทำการAlert แล้วทำการเก็บล็อคไว้

4.5 การทดสอบระบบโดยการสร้าง IPFW rules

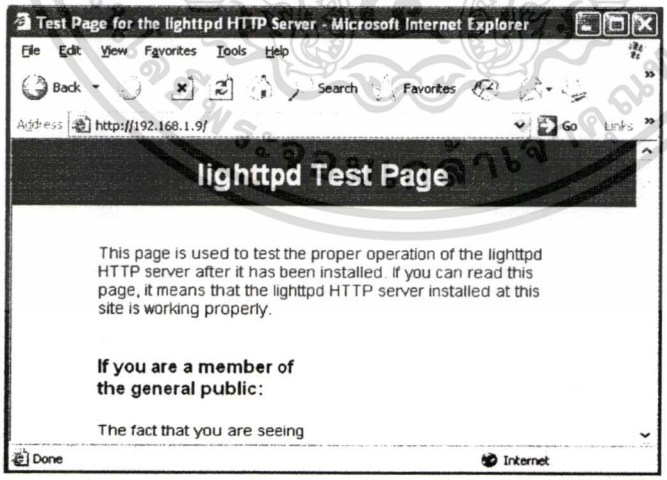
การทดสอบระบบโดยการสร้าง IPFW rules โดยจะแสดงเป็น 2 ส่วน คือ

4.5.1 การทดสอบก่อนการติดตั้ง Rules



รูปที่ 4.17 แสดงฟอร์มของ IPFW Rules

จากรูปที่ 4.17 เป็นการแสดงฟอร์มของ IPFW Rules ใช้ในการกำหนดกฎของ IPFW โดยสามารถใส่กฎเข้าไป แล้วระบบจะแสดงกฎที่สร้างขึ้นให้ตรวจสอบอีกครั้งก่อนติดตั้ง (Install Rules)



รูปที่ 4.18 แสดงการเรียกใช้งาน http://192.168.1.9 พอร์ต 80 ก่อนการติดตั้งกฎ

จากรูปที่ 4.18 แสดงการเรียกใช้งาน http://192.168.1.9 พอร์ต 80 จากเครื่องหมายเลข IP address 192.168.226.3 สามารถเรียกใช้งานได้ก่อนติดตั้ง IPFW Rules

```
C:\Documents and Settings\Administrator>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=10ms TTL=127
Reply from 192.168.1.9: bytes=32 time<1ms TTL=127
Reply from 192.168.1.9: bytes=32 time=2ms TTL=127
Reply from 192.168.1.9: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\Documents and Settings\Administrator>
```

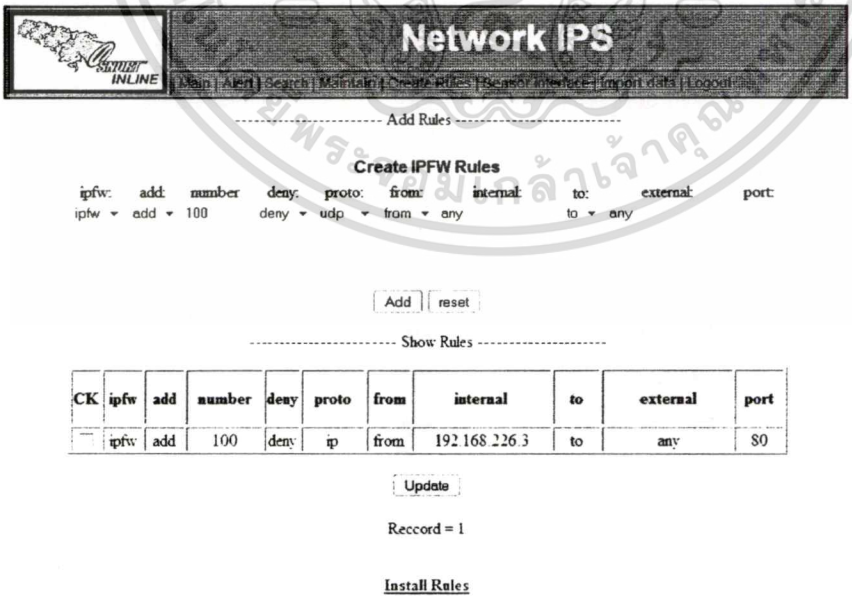
รูปที่ 4.19 แสดงการทดสอบ ping จากหมายเลข IP address 192.168.226.3 ไปยังหมายเลข IP address 192.168.1.9

จากรูปที่ 4.19 แสดงการทดสอบ ping จากหมายเลข IP address 192.168.226.3 ไปยังหมายเลข IP address 192.168.1.9 ซึ่งสามารถ ping ได้

4.5.2 การทดสอบหลังการติดตั้ง Rules

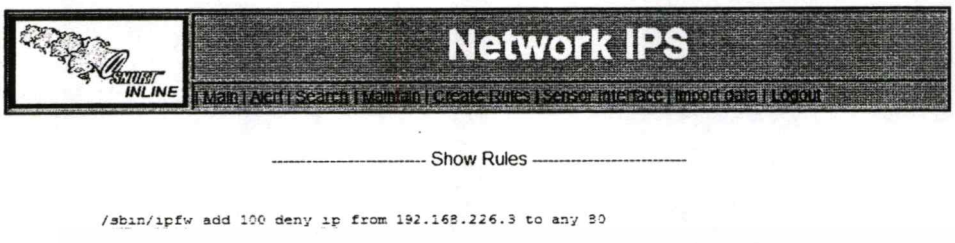
ทำการติดตั้ง Rules ดังนี้

ipfw add 100 deny ip from 192.168.226.3 to any 80



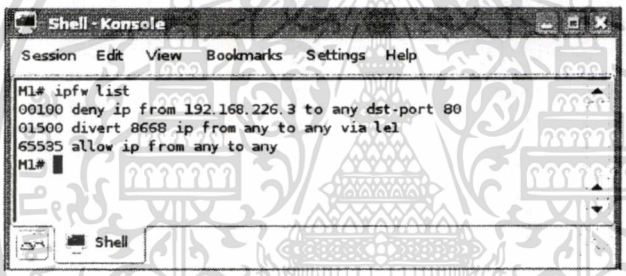
รูปที่ 4.20 แสดงการสร้าง IPFW Rules

จากรูปที่ 4.20 เป็นการแสดงค่า IPFW Rules ที่สร้างขึ้นมาดังที่เห็นในตาราง แล้วทำการ Install Rules



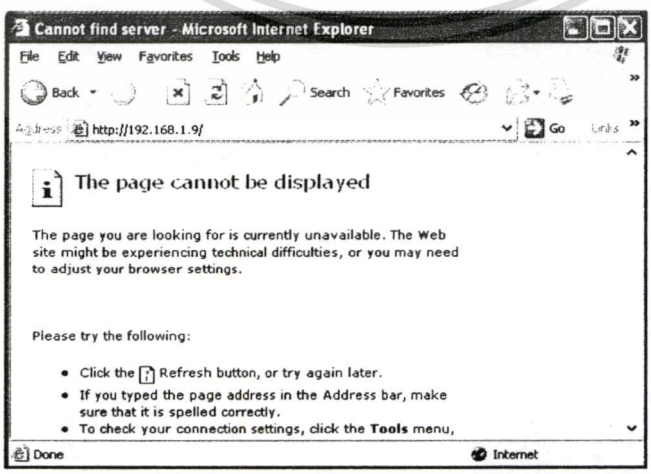
รูปที่ 4.21 แสดง IPFW Rules ที่สร้าง

จากรูปที่ 4.21 แสดง IPFW rules ที่สร้าง และได้ติดตั้งแล้ว



รูปที่ 4.22 แสดง Rules ที่ได้ติดตั้ง

จากรูปที่ 4.22 แสดง Rules ที่ได้ติดตั้งบนฟรีบีเอสดี



รูปที่ 4.23 แสดงการเรียก http://192.168.1.9 พอร์ต 80 หลังติดตั้ง

จากรูปที่ 4.23 แสดงการเรียกใช้งาน http://192.168.1.9 พอร์ต 80 จากเครื่องหมายเลข IP address 192.168.226.3 ไม่สามารถเรียกใช้งานได้หลังติดตั้ง IPFW Rules

```
C:\Documents and Settings\Administrator>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=10ms TTL=127
Reply from 192.168.1.9: bytes=32 time<1ms TTL=127
Reply from 192.168.1.9: bytes=32 time=2ms TTL=127
Reply from 192.168.1.9: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\Documents and Settings\Administrator>
```

รูปที่ 4.24 แสดงการทดสอบโดยการ ping จากหมายเลข IP address 192.168.226.3 ไปยังหมายเลข IP address 192.168.1.9

จากรูปที่ 4.24 แสดงการทดสอบโดยการ ping จากหมายเลข IP address 192.168.226.3 ไปยังหมายเลข IP address 192.168.1.9 พบว่าสามารถ ping ได้

บทที่ 5
บทสรุปและแนวทางพัฒนาในอนาคต

การพัฒนาโครงงานในครั้งนี้อยู่ภายใต้สภาวะแวดล้อมแบบปิดคือได้ทดลองโปรแกรมทั้งหมดบนโปรแกรม Vmware และนำโปรแกรมสนอร์ทอินไลนทำหน้าดักจับแพ็กเก็ต ตรวจสอบแพ็กเก็ต และนำโปแกรมไฟร์วอลล์ ทำการกรองแพ็กเก็ต และป้องกันแพ็กเก็ตที่ผ่านบนระบบปฏิบัติการฟรีบีเอสดี

5.1 สิ่งที่ได้รับจากการพัฒนาระบบ

หลังจากผ่านกระบวนการวิเคราะห์ ออกแบบ พัฒนาและทดสอบระบบ โดยสามารถสรุปการทำงานที่ได้พัฒณาดังนี้

- ได้ระบบที่สามารถทำงานผ่านเว็บ ช่วยให้สะดวกต่อการวิเคราะห์การเตือน และสามารถติดตั้งกฎต่างๆ ผ่านเครื่องมือต่างๆที่ได้พัฒนา
- ได้รับความรู้และพัฒนาความสามารถในการวิเคราะห์ ออกแบบ พัฒนา และทดสอบระบบ
- ได้รับความรู้และเข้าใจการทำงานของสนอร์ทอินไลน และการทำงานของ IPFW บนระบบปฏิบัติการฟรีบีเอสดี
- ได้นำระบบไปใช้งานและอาจจะพัฒนาต่อยอดได้ในอนาคต

5.2 ข้อจำกัดของระบบ

ข้อจำกัดของระบบสามารถสรุปได้ ดังนี้

- เนื่องจากระบบป้องกันการบุกรุกคอมพิวเตอร์ได้พัฒนาบนพื้นฐานการทำงานบนเว็บ ซึ่งช่วยให้สะดวกต่อการวิเคราะห์และการกำหนดกฎ แต่เนื่องจาก ในเร้าติ้งเทเบิลของฟรีบีเอสดี จะมี ไอพีแอดเดรสของเกตเวย์ ดังนั้น เมื่อเครื่องลูกข่ายติดต่อ เข้ามาที่อินเตอร์เฟซภายในของ NAT ระบบจะส่งต่อไปยัง อินเตอร์เฟซ ที่เป็นเครือข่ายเดียวกันกับเกตเวย์ เท่านั้น
- เครื่องในเครือข่ายภายในที่ต้องการเชื่อมต่อออกสู่เครือข่ายภายนอก ต้องตั้งค่าไอพีแอดเดรสให้ตรงกับกฎหรืออินเตอร์เฟซของเครื่องที่ให้บริการจึงสามารถเชื่อมต่อได้

- การป้องกันเครือข่ายขึ้นอยู่กับการกำหนดกฎที่เหมาะสม ซึ่งการตรวจจับอาจจะไม่รัดกุมได้ดังนั้นควรไปดาวน์โหลด Rules ที่มีการ update มาติดตั้งด้วย
- การป้องกันยังไม่ตอบสนองต่อการควบคุมย้อนกลับ (Feedback) ของสนอร์ทที่ส่งถึงไฟร์วอลล์ ทำให้ยังไม่เป็นระบบป้องกันการบุกรุกที่เต็มรูปแบบ

5.3 สรุปแนวทางในการพัฒนาในอนาคต

การป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์นั้น ทางที่จะทำให้ระบบเครือข่ายมีความปลอดภัย คือ การกำหนดกฎให้ครบถ้วนเหมาะสม การออกแบบการตรวจจับที่ดี และเพื่อสะดวกต่อการกำหนดค่าหมายเลขเครือข่ายอาจจะนำระบบอื่นๆ เข้าติดตั้งเพิ่มเพื่อช่วยให้ระบบดีขึ้น เช่น ติดตั้ง และออกแบบการใช้งาน DHCP เพิ่ม เป็นต้น การพัฒนานี้ได้ออกแบบการ configuration เบื้องต้น การดึงข้อมูลมาวิเคราะห์อาจจะพัฒนาให้ดึงมาแสดงแบบต่อเนื่อง และในส่วนของการพัฒนาได้พัฒนาโดยใช้หลักการของสนอร์ท และ หลักการของไฟร์วอล์ ความสามารถของระบบยังไม่เป็นระบบป้องกันการบุกรุกที่เต็มรูปแบบ ยังขาดส่วนย้อนกลับ (Feedback) ในการควบคุมที่สนอร์ทส่งถึงไฟร์วอลล์ ซึ่งระบบป้องกันการบุกรุกที่เต็มรูปแบบนั้นต้องสามารถหยุดการบุกรุกได้เมื่อพบว่ามีการบุกรุก ดังนั้นสามารถนำไปพัฒนาต่อในส่วนย้อนกลับของสนอร์ทควบคุมไฟร์วอลล์เพื่อให้การทำงานมีประสิทธิภาพยิ่งขึ้น

บรรณานุกรม

กิตติ ภักดีวัฒนะกุล และกิตติพงษ์ กลมกล่อม. 2548. **คัมภีร์การวิเคราะห์และออกแบบระบบเชิงวัตถุด้วย UML.** พิมพ์ครั้งที่1. กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์.

บัณฑิต จามรภูมิ. 2549. **คู่มือระบบยูนิกซ์ FreeBSD เล่ม 1.** กรุงเทพฯ : บริษัท บัณฑิตเพลส จำกัด.

ภูวดล ด่านระหาญ. 2544. **การติดตั้ง Snort ร่วมกับ ACID (+MySQL).** ThaiCERT. [Online] Available: http://www.thaicert.org/paper/ids/snort2.php.

สมศักดิ์ โชคชัยชุติกุล. 2550. **insight PHP ฉบับสมบูรณ์.** พิมพ์ครั้งที่ 7. กรุงเทพฯ: โปรวิชั่น จำกัด.

Nick Rogness. **A How-To Guild for running snort_inline on FreeBSD.** [Online] Available: http://freebsd.rogness.net/snort_inline/.

ภาคผนวก ก

การติดตั้งโปรแกรมที่เกี่ยวข้อง

ขั้นตอนการติดตั้งโปรแกรมต่างๆ ที่เกี่ยวข้องกับระบบป้องกันการบุกรุกเครือข่าย และเว็บเบสสำหรับติดต่อกับผู้ใช้ การพัฒนาระบบนี้ใช้โปรแกรมทั้งหมดที่ดาวน์โหลดมาได้โดยไม่เสียค่าใช้จ่ายทั้งสิ้นและมีขั้นตอนการติดตั้งแต่ละโปรแกรมดังนี้

1. การติดตั้งระบบปฏิบัติการ FreeBSD 7.0 เป็นระบบปฏิบัติการของระบบ

1) Boot เครื่องด้วยแผ่น FreeBSD 7.0

2) เลือกประเทศไทย รหัส 212

3) เลือก Keymap

4) เมื่อเข้าเมนู Sysinstall ให้เลือกการติดตั้งแบบ Custom

5) เมื่อเข้าเมนู Option ไม่ต้องเปลี่ยนค่าใดๆ

6) การกำหนด partition ให้เลือก A คือใช้ทั้งหมด

7) เมื่อเข้าสู่การ Install Boot Manager ให้เลือกแบบ Standard

8) กำหนด Label ที่ต้องการสร้างและขนาด เช่น / = 256 MB , swap = 256 MB , /usr = 700 MB และ /data = เนื้อที่ส่วนที่เหลือทั้งหมด

9) ส่วนของ Distribution ให้เลือกการติดตั้งแบบ minimal

10) เลือก Media คือ CD/DVD

11) Commit รอการติดตั้งเสร็จแล้ว Boot เครื่องหนึ่งครั้ง

2. การติดตั้ง NAT

1) การที่จะให้ NAT ทำงานได้นั้นจะต้องมีการ compile kernel ให้รู้จักก่อนดังนี้

```
# cd /sys/i386/conf
# ls -l
# cp GENERIC LOCAL
# ee LOCAL
options     IPFIREWALL                  #firewall
options     IPFIREWALL_VERBOSE     #enable logging to syslogd(8)
```

```
options         IPFIREWALL_FORWARD      #enable transparent proxy support
options         IPFIREWALL_VERBOSE_LIMIT=100    #limit verbosity
options         IPFIREWALL_DEFAULT_TO_ACCEPT    #allow everything by default
options         IPDIVERT                        # allow to divert port
# config LOCAL                                  #จะปรากฏข้อความข้างล่าง
Don't forget to do a ``make depend"
Kernel build directory is ../compile/LOCAL
# cd ../compile/LOCAL                           #จากนั้นทำการ compile
# make depend && make
# make install
```

2) ทำการเพิ่มข้อความต่อไปนี้ลงบนไฟล์ /etc/rc.conf ดังนี้

```
firewall_enable=YES
firewall_script="/etc/ipfw.conf.sh"
firewall_type="OPEN"
firewall_quiet="YES"
firewall_logging="YES"
natd_enable="YES"
natd_interface="le1"
```

3. การติดตั้ง Apache Web server เวอร์ชัน 2.2.6

ทำการติดตั้ง ดังนี้

```
#cd /tmp
#fetch http://www.apache.org/dist/httpd/httpd-2.2.6.tar.gz
#tar zxf httpd-2.2.6.tar.gz
#cd /tmp/httpd-2.2.6
#./configure –with-mysql
#make
#make install
```

4. การติดตั้ง PHP

1) ดาวน์โหลดโปรแกรม php-5.2.5.tar.gz จากเว็บไซต์ http://www.php.net จากนั้นทำการ unzip

2) ติดตั้งด้วยคำสั่ง

#gzip –cd php-5.2.5.tar.gz | tar xvf –

#chmod 777 php-5.2.5

#cd php-5.2.5

#./configure --with-gd --enable-sockets --with-mysql

#make

#make install

3) ปรับแต่งไฟล์ php.ini แล้วบันทึกไว้ที่ /usr/local/lib/php.ini

5. การติดตั้ง Mysql

1) ดาวน์โหลดโปรแกรม mysql-5.0.45.tar.gz จากเว็บไซต์ http://www.mysql.com จากนั้นทำการ unzip

2) ติดตั้งด้วยคำสั่ง

#gzip –cd mysql-5.0.45.tar.gz | tar xvf –

#chmod 777 mysql-5.0.45

#cd mysql-5.0.45

#./configure

#make

#make install

6. การติดตั้ง Snort_inline

1) ก่อนติดตั้ง snort_inline ให้ไปดาวน์โหลดโปรแกรม Libnet-1.0.2a เพื่อใช้จัดการกับแพ็กเก็ต และ ติดตั้ง Libdnet-1.11 ก่อน

2) ดาวน์โหลดโปรแกรม snort_inline-2.4.5.tar.gz จากเว็บไซต์ http://snort-inline.sourceforge.net/download.html จากนั้นทำการ unzip

3) ติดตั้งด้วยคำสั่ง

#gzip –cd snort_inline-2.4.5.tar.gz | tar xvf –

#chmod 777 snort_inline-2.4.5

#./configure --enable-inline --enable-ipfw --enable-divert –with-mysql

#make

make install

7. ตัวอย่างชนิดของ Alert

ตัวอย่าง snort_inline-full

[**] [1:466:4] ICMP [**]

[Classification: Attempted Administrator Privilege Gain] [Priority: 1]

09/15-10:38:53.739071 192.168.226.4:53526 -> 192.168.226.3:1041

TCP TTL:64 TOS:0x8 ID:11202 IpLen:20 DgmLen:1395 DF

***AP**F Seq: 0x3973860 Ack: 0x5626666 Win: 0xFFFF TcpLen: 20

ตัวอย่าง snort_inline-fast

09/15-10:38:53.739071 [**] [1:466:4] ICMP [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.226.4:53526 -> 192.168.226.3:1041

ภาคผนวก ข

คู่มือการใช้งานเว็บเบสยูสเซอร์อินเตอร์เฟส สำหรับระบบป้องกันการบุกรุกเครือข่ายคอมพิวเตอร์

1.เริ่มต้นเข้าใช้งาน

การเริ่มเข้าใช้งานเริ่มจากผู้ใช้พิมพ์ http://192.168.226.4/Login.php ซึ่งเป็นหน้าแรกของเว็บเบส

รูปที่ ข.1 แสดงหน้าจอการ Login

จากรูปที่ ข.1 แสดงหน้าจอการ Login

ให้กรอก Username : root

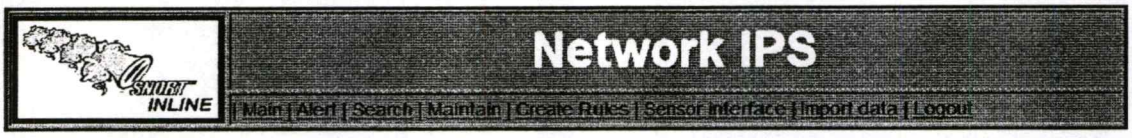
Password : root

รูปที่ ข.2 แสดงหน้าจอการ Login กรณีข้อมูลไม่ถูกต้อง

จากรูปที่ ข.2 แสดงหน้าจอการ Login กรณีข้อมูลไม่ถูกต้อง

2. เมนูการใช้งาน

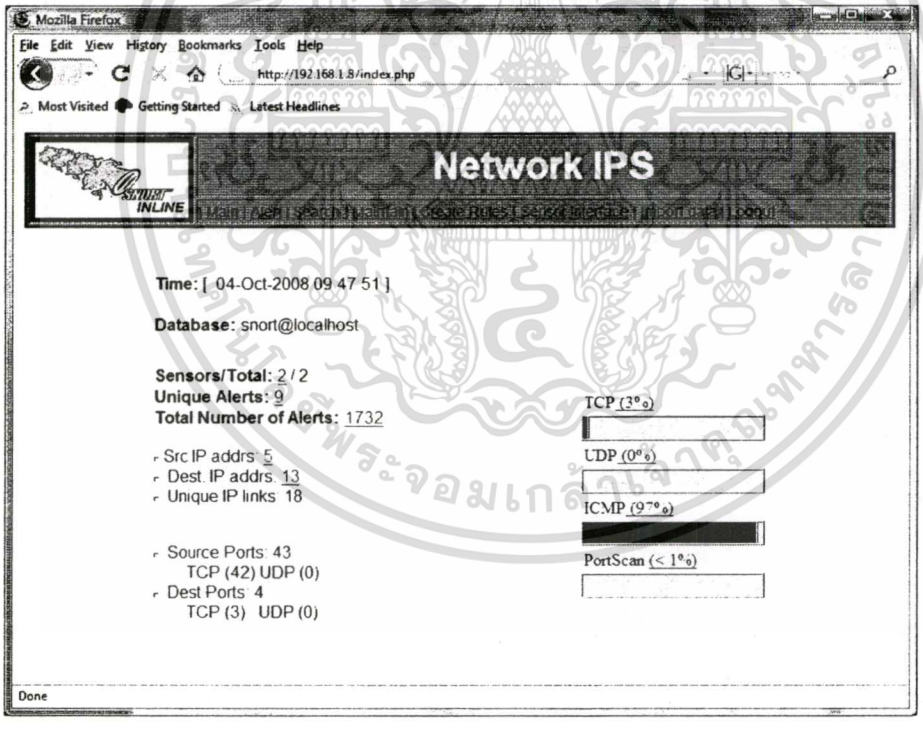
ระบบประกอบด้วยเมนูหลักๆ ดังนี้คือ



รูปที่ ข.3 แสดงเมนูของระบบ

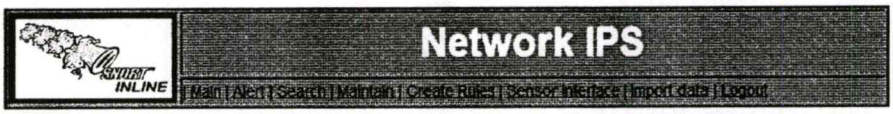
จากรูปที่ ข.3 แสดงเมนูของระบบ ซึ่งมี เมนู Main, Alert, Search, Maintain, Create Rules, Sensor Interface, Import data และ logout

2.1) เมนู main เป็นการแสดงรายละเอียดของ Alert ดังรูปที่ ข.4



รูปที่ ข.4 แสดงหน้าจอเมนู main

จากรูปที่ ข.4 แสดงหน้าจอเมนู main ซึ่งสามารถเรียกดู Sensors/Total, Unique Alerts, Total Number of Alerts, Src IP addrs และ Dest IP addrs



Unique Alerts ALL : 9 Total

Signature	Total	Sensor	Src. Addr.	Dest. Addr.	First Time	Last Time
	1 (0%)	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00
1	1685 (97%)	1	2	3	2008-10-03 10:26:25	2008-10-04 21:47:00
11	2 (0%)	1	1	1	2008-10-04 16:53:25	2008-10-04 19:17:04
16	1 (0%)	1	1	1	2008-10-04 17:46:06	2008-10-04 17:46:06
2	24 (1%)	1	4	7	2008-10-03 10:28:21	2008-10-04 21:19:56
3	13 (0%)	1	2	7	2008-10-03 10:28:42	2008-10-04 21:31:38
6	1 (0%)	1	1	1	2008-10-03 10:37:36	2008-10-03 10:37:36
7	1 (0%)	1	1	1	2008-10-03 10:37:57	2008-10-03 10:37:57
8	4 (0%)	1	1	1	2008-10-03 11:18:21	2008-10-04 16:14:52

รูปที่ ข.5 แสดง Unique Alerts All

จากรูปที่ ข.5 แสดง Unique Alerts All แสดงถึงจำนวนของ signature ที่พบ ณ เวลาช่วงไหน

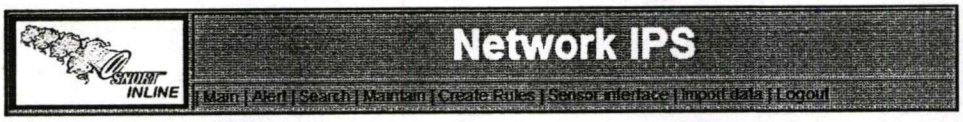
Listing Alerts ALL : 1740 Total

Delete Alert

CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 2	ICMP redirect net	2008-10-03 10:26:25	192.168.1.4	192.168.1.1	ICMP
	1 - 4	ICMP redirect net	2008-10-03 10:26:30	192.168.1.4	192.168.1.8	ICMP
	1 - 6	ICMP redirect net	2008-10-03 10:26:37	192.168.1.4	192.168.1.1	ICMP
	1 - 8	ICMP redirect net	2008-10-03 10:26:40	192.168.1.4	192.168.1.8	ICMP
	1 - 10	ICMP redirect net	2008-10-03 10:26:45	192.168.1.4	192.168.1.8	ICMP
	1 - 12	ICMP redirect net	2008-10-03 10:26:49	192.168.1.4	192.168.1.8	ICMP
	1 - 14	ICMP redirect net	2008-10-03 10:26:52	192.168.1.4	192.168.1.1	ICMP

รูปที่ ข.6 แสดง Total Number of Alerts

จากรูปที่ ข.6 แสดง Total Number of Alerts แสดงชื่อ Signature ที่พบ ณ เวลาต่างๆ



SOURCE IP LISTING :5 ALL :

IP address	Sensor #	Total #	Unique Alerts	Dest. Addr.
0.0.0.0	1	1	1	1
192.168.1.2	1	15	2	3
192.168.1.4	1	1708	7	7
192.168.1.8	1	1	1	1
192.168.226.3	1	7	3	3

รูปที่ ข.7 แสดงรายการSrc IP Addrs

จากรูปที่ ข.7 แสดง Src IP addrs ที่ตรวจพบ และจำนวน Alerts ที่พบ

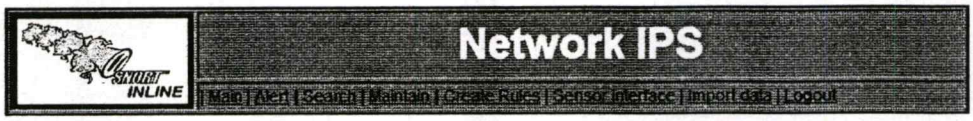
DESTINATION IP LISTING :13 ALL :

IP address	Sensor #	Total #	Unique Alerts	Dest. Addr.
0.0.0.0	1	1	1	1
64.233.189.100	1	3	2	1
64.233.189.101	1	6	3	1
64.233.189.102	1	4	2	1
74.125.96.83	1	1	1	1
74.125.96.85	1	1	1	1
192.168.1.1	1	608	1	2
192.168.1.3	1	1	1	1
192.168.1.8	1	1099	6	2
192.168.1.9	1	1	1	1
192.168.226.4	1	1	1	1
203.150.224.132	1	3	2	1
203.151.233.16	1	3	1	1

รูปที่ ข.8 แสดงรายการ Dest IP Addrs

จากรูปที่ ข.8 แสดง Dest IP Addrs ที่ตรวจพบ และแสดงจำนวน Alerts ที่พบ

2.2) เมนู Alert เป็นเมนูที่แสดงรายละเอียด ดังรูปที่ ข.9 โดยแสดง Alert เป็นรายวัน หรือ 24 ชั่วโมง หรือ 72 ชั่วโมงเป็นต้น



- Today's alerts unique listing
- Last 24 Hours alerts: unique listing
- Last 72 Hours alerts: unique listing
- Most recent 15 Alerts: any protocol TCP
  UDP
  ICMP

- Recent 15 Unique Alerts :
- Frequent 5 Unique Alerts :

รูปที่ ข.9 แสดงรายการที่จะใช้วิเคราะห์ ตรวจดู Alert

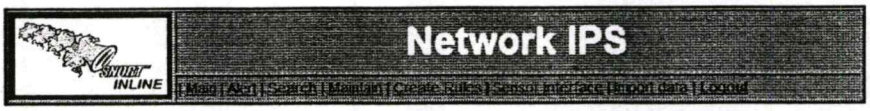
จากรูปที่ ข.9 แสดงหน้าเว็บ Alert ที่จะใช้วิเคราะห์ ตรวจดู Alert ต่างๆตามรายละเอียดที่แสดง

Unique Alerts TO DAY : 6 Total

Signature	Total	Sensor	Src. Addr.	Dest. Addr.	First Time	Last Time
1	199 (11%)	1	2	3	2008-10-04 14:10:10	2008-10-04 21:47:00
11	2 (0%)	1	1	1	2008-10-04 16:53:25	2008-10-04 19:17:04
16	1 (0%)	1	1	1	2008-10-04 17:46:06	2008-10-04 17:46:06
2	3 (0%)	1	2	2	2008-10-04 15:25:27	2008-10-04 21:19:56
3	9 (0%)	1	1	5	2008-10-04 16:21:47	2008-10-04 21:31:38
8	1 (0%)	1	1	1	2008-10-04 16:14:52	2008-10-04 16:14:52

รูปที่ ข.10 แสดงรายการ Today's alerts: unique

จากรูปที่ ข.10 แสดง Today's alerts: unique แสดงจำนวน Signature ที่ Alerts และช่วงเวลาที่พบ



Next > Last >>

Listing Alerts today : 215 Total

Delete Alert

CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 3036	ICMP redirect net	2008-10-04 14:10:10	192.168.1.2	192.168.1.1	ICMP
	1 - 3038	ICMP redirect net	2008-10-04 14:11:11	192.168.1.2	192.168.1.1	ICMP
	1 - 3040	ICMP redirect net	2008-10-04 14:13:11	192.168.1.2	192.168.1.1	ICMP
	1 - 3042	ICMP redirect net	2008-10-04 14:32:01	192.168.1.2	192.168.1.8	ICMP
	1 - 3044	ICMP redirect net	2008-10-04 14:32:50	192.168.1.2	192.168.1.3	ICMP
	1 - 3046	ICMP redirect net	2008-10-04 14:37:01	192.168.1.2	192.168.1.8	ICMP
	1 - 3048	ICMP redirect net	2008-10-04 14:38:00	192.168.1.2	192.168.1.8	ICMP

รูปที่ ข.11 แสดงรายการ Today's alerts: listing

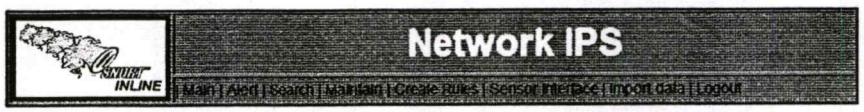
จากรูปที่ ข.11 แสดง Today's alerts: listing ซึ่งแสดงชื่อ signature และเวลาที่ตรวจพบ

Unique Alerts in 24 Hour : 8 Total

Signature	Total	Sensor	Src. Addr.	Dest. Addr.	First Time	Last Time
1	1685 (97%)	1	2	3	2008-10-03 10:26:25	2008-10-04 21:47:00
11	2 (0%)	1	1	1	2008-10-04 16:53:25	2008-10-04 19:17:04
16	1 (0%)	1	1	1	2008-10-04 17:46:06	2008-10-04 17:46:06
2	24 (1%)	1	4	7	2008-10-03 10:28:21	2008-10-04 21:19:56
3	13 (0%)	1	2	7	2008-10-03 10:28:42	2008-10-04 21:31:38
6	1 (0%)	1	1	1	2008-10-03 10:37:36	2008-10-03 10:37:36
7	1 (0%)	1	1	1	2008-10-03 10:37:57	2008-10-03 10:37:57
8	4 (0%)	1	1	1	2008-10-03 11:18:21	2008-10-04 16:14:52

รูปที่ ข.12 แสดงรายการ Last 24 hour Alerts: unique

จากรูปที่ ข.12 แสดง Last 24 hour Alerts: unique แสดงจำนวน Signature ที่ Alerts และช่วงเวลาที่พบ



Next > Last >>

Listing Alerts in last 24 hour : 1731 Total

Delete Alert

CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 2	ICMP redirect net	2008-10-03 10:26:25	192.168.1.4	192.168.1.1	ICMP
	1 - 4	ICMP redirect net	2008-10-03 10:26:30	192.168.1.4	192.168.1.8	ICMP
	1 - 6	ICMP redirect net	2008-10-03 10:26:37	192.168.1.4	192.168.1.1	ICMP
	1 - 8	ICMP redirect net	2008-10-03 10:26:40	192.168.1.4	192.168.1.8	ICMP
	1 - 10	ICMP redirect net	2008-10-03 10:26:45	192.168.1.4	192.168.1.8	ICMP
	1 - 12	ICMP redirect net	2008-10-03 10:26:49	192.168.1.4	192.168.1.8	ICMP
	1 - 14	ICMP redirect net	2008-10-03 10:26:52	192.168.1.4	192.168.1.1	ICMP

รูปที่ ข.13 แสดงรายการ Last 24 hour Alerts: listing

จากรูปที่ ข.13 แสดง Last 24 hour Alerts: listing ซึ่งแสดงชื่อ signature และเวลาที่ตรวจพบ

Listing Alerts ALL : Last 15 Alerts

Delete Alert

CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 108	(http_inspect) BARE BYTE UNICODE ENCODING	2008-10-03 10:28:42	192.168.226.3 : 2199	203.150.224.132 : 80	TCP
	1 - 121	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:50	192.168.226.3 : 2199	203.150.224.132 : 80	TCP
	1 - 137	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:21	192.168.226.3 : 2192	203.151.233.16 : 80	TCP
	1 - 159	(http_inspect) BARE BYTE UNICODE ENCODING	2008-10-03 10:29:32	192.168.1.4 : 49398	192.168.1.8 : 80	TCP
	1 - 164	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:32	192.168.226.3 : 2233	203.151.233.16 : 80	TCP
	1 - 166	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:33	192.168.226.3 : 2237	203.151.233.16 : 80	TCP
	1 - 168	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:49	192.168.1.4 : 49390	192.168.1.8 : 80	TCP
	1 - 189	WEB-MISC Invalid HTTP Version String	2008-10-03 10:28:51	192.168.226.3 : 2199	203.150.224.132 : 80	TCP

รูปที่ ข.14 แสดงรายการ Most Recent 15 Alerts: TCP

จากรูปที่ ข.14 แสดง Most Recent 15 Alerts: TCP ซึ่งแสดงชื่อ signature และเวลาที่ตรวจพบ ชนิดโปรโตคอล TCP

Listing Alerts ALL : Last 15 Alerts

Delete Alert

CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 2	ICMP redirect net	2008-10-03 10:26:25	192.168.1.4	192.168.1.1	ICMP
	1 - 4	ICMP redirect net	2008-10-03 10:26:30	192.168.1.4	192.168.1.8	ICMP
	1 - 6	ICMP redirect net	2008-10-03 10:26:37	192.168.1.4	192.168.1.1	ICMP
	1 - 8	ICMP redirect net	2008-10-03 10:26:40	192.168.1.4	192.168.1.8	ICMP
	1 - 10	ICMP redirect net	2008-10-03 10:26:45	192.168.1.4	192.168.1.8	ICMP
	1 - 12	ICMP redirect net	2008-10-03 10:26:49	192.168.1.4	192.168.1.8	ICMP
	1 - 14	ICMP redirect net	2008-10-03 10:26:52	192.168.1.4	192.168.1.1	ICMP
	1 - 16	ICMP redirect net	2008-10-03 10:26:54	192.168.1.4	192.168.1.8	ICMP

รูปที่ ข.15 แสดงรายการ Most Recent 15 Alerts : ICMP

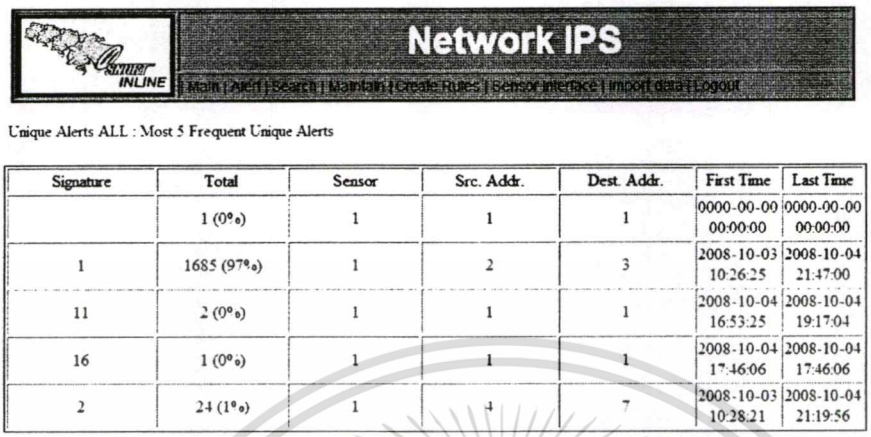
จากรูปที่ ข.15 แสดง Most Recent 15 Alerts : ICMP ซึ่งแสดงชื่อ signature และเวลาที่ตรวจพบ ชนิดโปรโตคอล ICMP

Unique Alerts ALL : Last 15 Unique Alerts

Signature	Total	Sensor	Src. Addr.	Dest. Addr.	First Time	Last Time
	1 (0%)	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00
1	1685 (97%)	1	2	3	2008-10-03 10:26:25	2008-10-04 21:47:00
11	2 (0%)	1	1	1	2008-10-04 16:53:25	2008-10-04 19:17:04
16	1 (0%)	1	1	1	2008-10-04 17:46:06	2008-10-04 17:46:06
2	24 (1%)	1	4	7	2008-10-03 10:28:21	2008-10-04 21:19:56
3	13 (0%)	1	2	7	2008-10-03 10:28:42	2008-10-04 21:31:38
6	1 (0%)	1	1	1	2008-10-03 10:37:36	2008-10-03 10:37:36
7	1 (0%)	1	1	1	2008-10-03 10:37:57	2008-10-03 10:37:57
8	4 (0%)	1	1	1	2008-10-03 11:18:21	2008-10-04 16:14:52

รูปที่ ข.16 แสดงรายการ Recent 15 Unique Alerts

จากรูปที่ ข.16 แสดง Recent 15 Unique Alerts แสดงจำนวน Signature ที่ Alerts และช่วงเวลาที่พบ ล่าสุด 15 Alerts

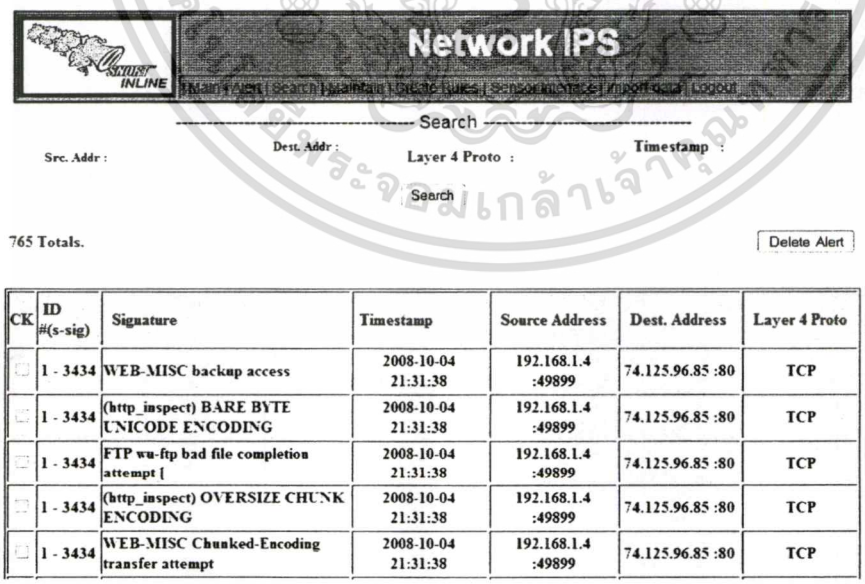


Signature	Total	Sensor	Src. Addr.	Dest. Addr.	First Time	Last Time
	1 (0%)	1	1	1	0000-00-00 00:00:00	0000-00-00 00:00:00
1	1685 (97%)	1	2	3	2008-10-03 10:26:25	2008-10-04 21:47:00
11	2 (0%)	1	1	1	2008-10-04 16:53:25	2008-10-04 19:17:04
16	1 (0%)	1	1	1	2008-10-04 17:46:06	2008-10-04 17:46:06
2	24 (1%)	1	4	7	2008-10-03 10:28:21	2008-10-04 21:19:56

รูปที่ ข.17 แสดงรายการ Frequent 5 Unique Alerts

จากรูปที่ ข.17 แสดง Frequent 5 Unique Alerts แสดงจำนวน Signature ที่ Alerts และช่วงเวลาที่พบบ่อยๆ 5 Alerts

2.3) เมนู Search ไว้ค้นหาข้อมูลที่ต้องการ โดยสามารถป้อนได้ ดังรูปที่ ข.18

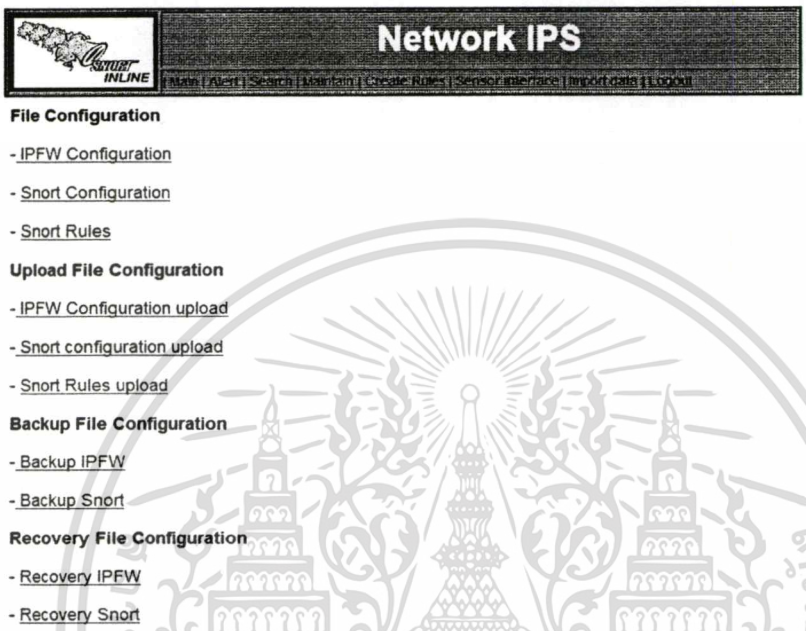


CK	ID #(s-sig)	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
	1 - 3434	WEB-MISC backup access	2008-10-04 21:31:38	192.168.1.4 :49899	74.125.96.85 :80	TCP
	1 - 3434	(http_inspect) BARE BYTE UNICODE ENCODING	2008-10-04 21:31:38	192.168.1.4 :49899	74.125.96.85 :80	TCP
	1 - 3434	FTP wu-ftp bad file completion attempt [	2008-10-04 21:31:38	192.168.1.4 :49899	74.125.96.85 :80	TCP
	1 - 3434	(http_inspect) OVERSIZE CHUNK ENCODING	2008-10-04 21:31:38	192.168.1.4 :49899	74.125.96.85 :80	TCP
	1 - 3434	WEB-MISC Chunked-Encoding transfer attempt	2008-10-04 21:31:38	192.168.1.4 :49899	74.125.96.85 :80	TCP

รูปที่ ข.18 แสดงเมนู Search โดยการค้นหาโปรโตคอล TCP

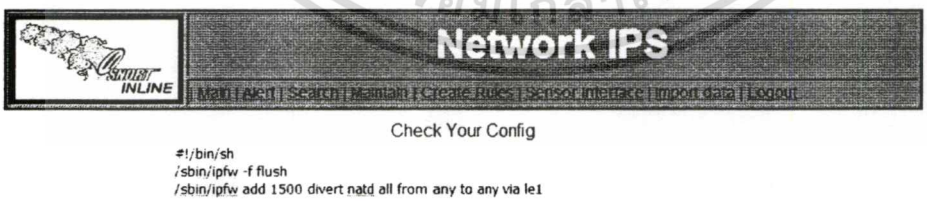
จากรูปที่ ข.18 แสดง เมนู Search โดยการค้นหาโปรโตคอล TCP แล้วแสดงชื่อ signature และเวลาที่ตรวจพบ

2.4) เมนู Maintain เป็นเมนูที่รวบรวมการ configuration บนไฟล์เพื่อทำการแก้ไขไฟล์ configuration ต่างๆ มีรายละเอียด ดังรูปที่ ข.19



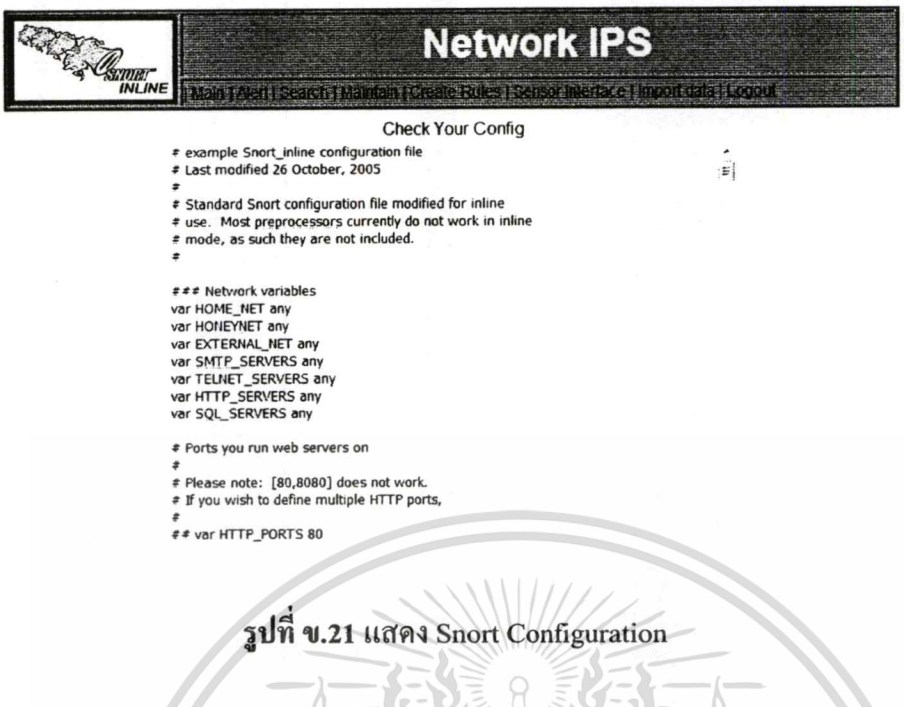
รูปที่ ข.19 แสดงเมนู Maintain

จากรูปที่ ข.19 แสดงเมนู Maintain เพื่อใช้ตรวจดู File Configuration และดูกฎที่เคยตั้ง รวมถึงการสำรองค่า แล้วทำ recovery คืน



รูปที่ ข.20 แสดง IPFW Configuration

จากรูปที่ ข.20 แสดง IPFW Configuration ของ IPFW Rules ที่ได้สร้างไว้



รูปที่ ข.21 แสดง Snort Configuration

จากรูปที่ ข.21 แสดง Snort Configuration เพื่อเปิดไฟล์ configuration ดูรายละเอียด

รูปที่ ข.22 แสดง Snort Rules

จากรูปที่ ข.22 แสดง Snort Rules ที่สร้าง เพื่อทำการตรวจจับ Alerts

รูปที่ ข.23 แสดง Upload IPFW Configuration Rules

จากรูปที่ ข.23 แสดงหน้าเว็บ การ Upload IPFW Configuration Rules

รูปที่ ข.24 แสดง Upload Snort Configuration

จากรูปที่ ข.24 จากรูปแสดงหน้าเว็บ การ Upload Snort Configuration

รูปที่ ข.25 แสดง Upload Snort Rules

จากรูปที่ ข.25 แสดงหน้าเว็บ การ Upload Snort Rules

รูปที่ ข.26 แสดง Backup IPFW Rules

จากรูปที่ ข.26 แสดงหน้าเว็บ การ Backup IPFW Rules

รูปที่ ข.27 แสดง Backup Snort Configuration

จากรูปที่ ข.27 แสดงหน้าเว็บ การ Backup Snort Configuration

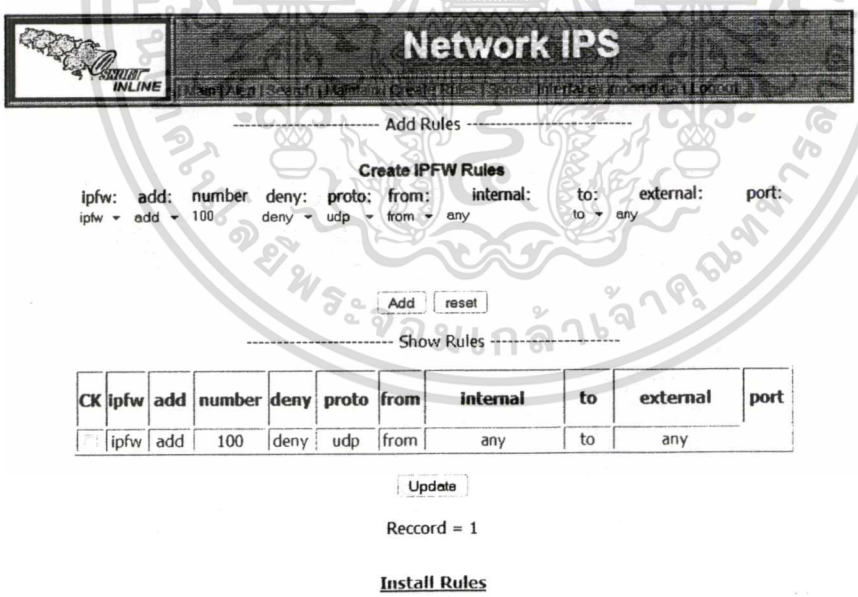
รูปที่ ข.28 แสดง Recovery IPFW Rules

จากรูปที่ ข.28 แสดงหน้าเว็บ การ Recovery IPFW Rules

รูปที่ ข.29 แสดง Recovery Snort Configuration

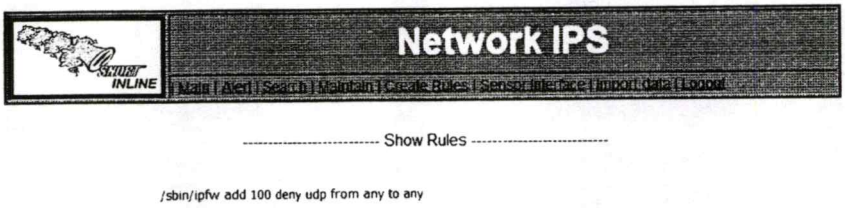
จากรูปที่ ข.29 แสดงหน้าเว็บ การ Recovery Snort Configuration

2.5) เมนู Create Rules เป็นเมนูที่ช่วยในการปรับแต่งแก้ไขกฎของ IPFW ดังรูปที่ ข.30



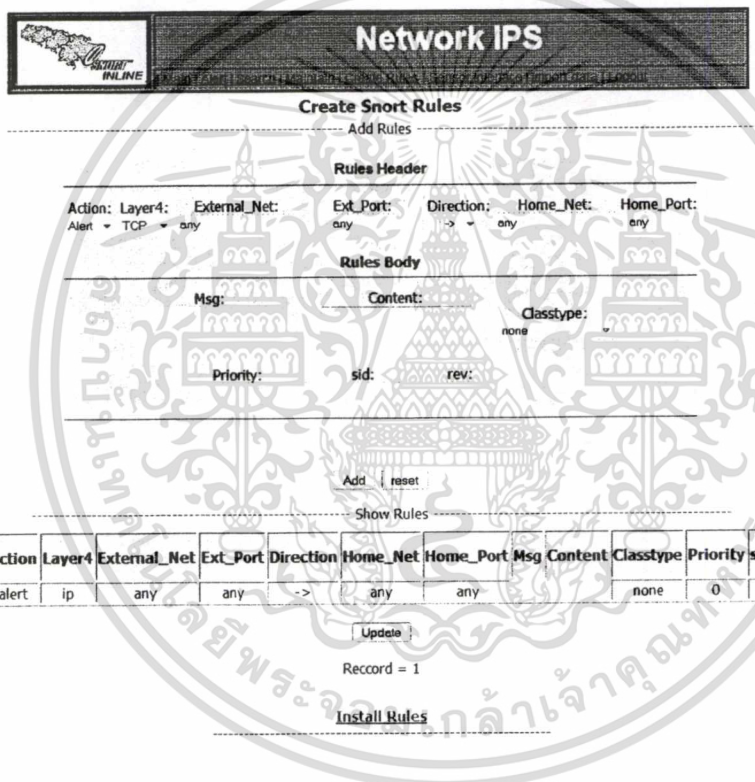
รูปที่ ข.30 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Create IPFW Rules

จากรูปที่ ข.30 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Create IPFW Rules เพื่อใช้สร้างกฎป้องกันการบุกรุก



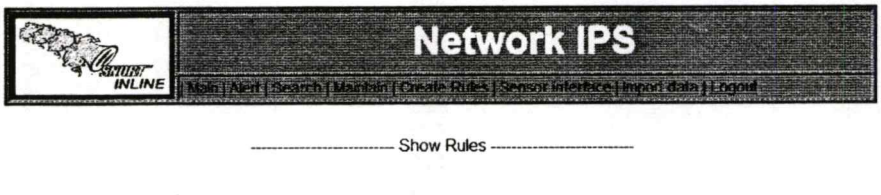
รูปที่ ข.31 แสดงการติดตั้ง IPFW Rules

จากรูปที่ ข.31 แสดง IPFW Rules ที่ได้ติดตั้ง



รูปที่ ข.32 แสดง Create Snort Rules

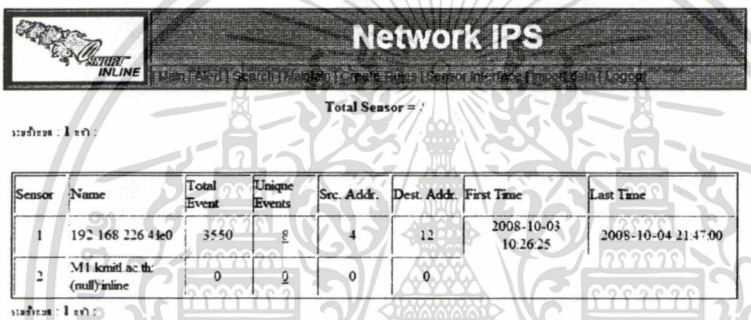
จากรูปที่ ข.32 แสดงการ Create Snort Rules



รูปที่ ข.33 แสดงการติดตั้ง Rules

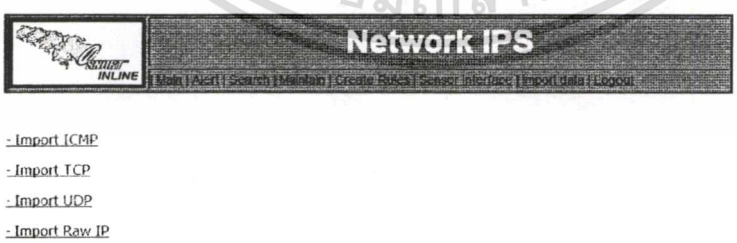
จากรูปที่ ข.33 แสดง Rules ที่ได้ติดตั้งเพื่อทำการตรวจสอบ

2.6) เมนู Sensor Interface เป็นเมนูที่แสดงรายละเอียดของ Sensor Interface ดังรูปที่ ข.34



รูปที่ ข.34 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Sensor Interface

จากรูปที่ ข.34 แสดงเว็บเบสยูสเซอร์อินเทอร์เฟสหน้า Sensor Interface แสดงถึงรายละเอียดของ Sensor Interface



รูปที่ ข.35 แสดงการ Import data เข้าสู่ตาราง acid_event

จากรูปที่ ข.35 แสดงรายการ Import data เข้าสู่ตาราง acid_event เพื่อใช้เตรียมข้อมูลในการวิเคราะห์การบุกรุก

ประวัติผู้เขียน

ชื่อผู้เขียน	นายกมล ขุทรานนท์
วัน เดือน ปีเกิด	4 สิงหาคม 2523
สถานที่เกิด	จังหวัดสงขลา
วุฒิระดับการศึกษา	วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมสารสนเทศ
สถาบันที่สำเร็จการศึกษา	สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีที่สำเร็จการศึกษา	2546