การลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต

FALSE POSITIVE ALERT DECREMENT OF SNORT INTRUSION DETECTION

ศิวกาญ เพียงงาม

SIWAKARN THIANGNGAM

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมฐานความรู้

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2552

การลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต

FALSE POSITIVE ALERT DECREMENT OF SNORT INTRUSION DETECTION

ศิวนาถ เทียนงาม

SIWANART THIAN-NGAM

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2552

KMITL-2009-EN-M-230-166

FALSE POSITIVE ALERT DECREMENT OF SNORT INTRUSION DETECTION

SIWANART THIAN-NGAM

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2009

KMITL-2009-EN-M-203-166

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต

Thesis Title False Positive Alert Decrement of Snort Intrusion Detection

นักศึกษา นายศิวนาถ เทียนงาม

รหัสประจำตัว 47061168

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมสารสนเทศ

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.มยุรี เลิศเวชกุล

หมายเลขวิทยานิพนธ์ KMITL-2009-EN-M-230-166

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.พิทักษ์	ธรรมวาริน	
ผศ.พิชญ	สุพรรณกูล	
ดร.สัญญา	คูณขาว	
รศ.ดร.ชวลิต	เบญจางคประเสริฐ	
ผศ.มยุรี	เลิศเวชกุล	

วัน / เดือน/ ปี ที่สอบ วันจันทร์ที่ 19 ตุลาคม พ.ศ. 2552 เวลา 09.00-11.00 น.

สถานที่สอบ ณ อาคาร A ชั้น 2 ห้องประชุม 6

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร.กอบชัย เดชหาญ)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 19 ตุลาคม พ.ศ. 2552

หัวข้อวิทยานิพนธ์	การลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต
นักศึกษา	นาย ศิวนาถ เทียนงาม
รหัสนักศึกษา	47061168
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
พ.ศ.	2552
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผศ. มยุรี เลิศเวชกุล

บทคัดย่อ

ในการใช้งานโปรแกรมตรวจจับการบุกรุกระบบเครือข่าย (Network Intrusion Detection System : NIDS) มักจะประสบปัญหาจากการสร้างการแจ้งเตือนที่ผิดพลาด (False Positive) จำนวนมาก ผู้วิจัยจึงเสนอแนวทางในการแก้ปัญหาโดยการพัฒนาระบบประเมินคุณภาพการแจ้งเตือนสำหรับโปรแกรมสนอร์ต (Snort) ซึ่งเป็นโปรแกรมตรวจจับการบุกรุกระบบเครือข่ายประเภทฟรีแวร์ โดยระบบที่นำเสนอได้ประยุกต์ใช้ระบบเครือข่ายใยประสาท (Neural Network) ที่ผ่านการฝึกด้วยพารามิเตอร์ เพื่อสร้างระดับค่าบ่งชี้ประเภทการบุกรุก ซึ่งสามารถนำไปประเมินเพื่อกำหนดระดับคุณภาพของการแจ้งเตือนเพื่อใช้คัดกรองการแจ้งเตือนที่ผิดพลาดต่อไป ในงานวิจัยนี้ได้ทดสอบระบบประเมินคุณภาพการแจ้งเตือนสำหรับโปรแกรมสนอร์ตที่พัฒนาขึ้นกับข้อมูลการแจ้งเตือนจากโปรแกรมสนอร์ตที่ติดตั้งในระบบเครือข่ายของบริษัทแห่งหนึ่ง ซึ่งมีการเชื่อมโยงการใช้งานสำหรับเครือข่ายภายในและการเชื่อมโยงกับเครือข่ายภายนอก (Internet) เป็นจำนวน 4239 รายการ และผลลัพธ์ที่ได้จากการทดสอบพบว่าโปรแกรมสนอร์ตสามารถช่วยคัดกรองและลดการแจ้งเตือนที่ผิดพลาดได้ร้อยละ 83.19

Thesis Title	False Positive Alert Decrement of Snort Intrusion Detection
Student	Mr. Siwanart Thian-ngam
Student ID.	47061168
Degree	Master of Engineering
Program	Information Engineering
Year	2009
Thesis Advisor	Asst. Prof.Mayuree Lertwatechakul

ABSTRACT

Network Intrusion Detection (NIDS) generate a lot of false positive alerts that always annoy and make trouble to network administrators. As to solve the mentioned problem, this research has developed an alert quality assessment system to reduce false positive alert of Snort, a famous freeware NIDS. The proposed system is consisted of Neural Network that was trained by a well-form dataset the neural network maps input parameters of an attack in an attacking type, an index value and hence the alert's quality. The alert quality is useful in filtering false alert. The developed alert quality assessment system was tested with 4239 records of Snort alert log from a real networking system which composed of Intranet and Internet access subsystems. The result showed that the proposed system could filtering and reduce false alert at approximately 83.19 percent

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้อย่างดี ด้วยคำแนะนำ และคำปรึกษาจาก ผศ. มยุรี เลิศเวชกุล ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ข้าพเจ้ารู้สึกทราบซึ้งในความอนุเคราะห์จากท่านอาจารย์ และขอขอบพระคุณเป็นอย่างสูง

ขอกราบพระคุณคณาจารย์ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุก ๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอกราบพระคุณคณาจารย์ภาควิชาวิศวกรรมเคมี คณะวิศวกรรมศาสตร์ มหาวิทยาลัยบูรพา ที่ได้สนับสนุนข้อมูล หนังสือต่าง ๆ และที่พักที่ใช้ในการทำวิจัย

ขอขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ ในภาควิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยี พระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกคนที่ให้คำแนะนำต่าง ๆ และคอยให้กำลังใจเสมอมา

ขอขอบคุณบัณฑิตศึกษาและบัณฑิตวิทยาลัย คณะวิศวกรรมศาสตร์ที่ให้ความช่วยเหลือในเรื่องต่าง ๆ

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา และครอบครัวของข้าพเจ้าที่เป็นกำลังใจและให้การสนับสนุนในทุกเรื่อง ๆ ทำให้ข้าพเจ้าสามารถทำวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี

คุณค่าและประโยชน์อันพึงมาจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

ศิวนาถ เทียนงาม

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญตาราง(ต่อ)

สารบัญตาราง(ต่อ)

ตารางที่ **หน้า**

สารบัญรูป

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

รูปที่ **หน้า**

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งหวังเพื่อเพิ่มประสิทธิภาพในการทำงานให้กับโปรแกรมสนอร์ต โดยลดการแจ้งเตือนที่ผิดพลาดที่โปรแกรมสนอร์ตสร้างขึ้นมา การแจ้งเตือนที่ผิดพลาดเป็นปัญหาที่มีความสำคัญเป็นอันดับต้น ๆ ในการรักษาความปลอดภัยบนระบบเครือข่าย การแจ้งเตือนที่ผิดพลาดไม่ได้เกิดขึ้นเฉพาะระบบตรวจจับการบุกรุกเท่านั้น ยังรวมไปถึงไฟร์วอลและอุปกรณ์รักษาความปลอดภัยรูปแบบอื่น ๆ การแจ้งเตือนที่ผิดพลาดหากเกิดขึ้นเป็นจำนวนมากจะทำให้โปรแกรมสนอร์ตทำงานหนักจนไม่สามารถทำงานได้ ดังนั้นในวิทยานิพนธ์ฉบับนี้จึงได้นำเสนอวิธีการลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต โดยประเมินคุณภาพการแจ้งเตือนที่เกิดขึ้นแล้วทำการปรับลดกฎที่เป็นสาเหตุทำให้เกิดแจ้งเตือนที่ผิดพลาด วิธีการดังกล่าวจะสามารถลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตได้อย่างมีประสิทธิภาพ

1.3 สมมุติฐานของการศึกษา

จากที่ได้กล่าวมาข้างต้นว่าโปรแกรมสนอร์ตเป็นฟรีแวร์ที่ผู้ใช้งานสามารถดาวน์โหลดโปรแกรมสนอร์ต และกฎของโปรแกรมสนอร์ตมาใช้งานได้ทันทีโดยโปรแกรมสนอร์ตได้ถูกพัฒนาขึ้นมาจนทำงานได้อย่างมีประสิทธิภาพเป็นที่ยอมรับของคนทั่วโลก จึงได้เกิดสังคมของผู้ใช้งานโปรแกรมสนอร์ตขึ้น โดยกลุ่มดังกล่าวจะทำการเขียนกฎของโปรแกรมสนอร์ตขึ้นมาเพื่อป้องกันรูปแบบการบุกรุกระบบเครือข่ายแบบใหม่ ๆ ที่เกิดขึ้น และเปิดให้ผู้ใช้งานโปรแกรมสนอร์ตดาวน์โหลดกฎไปใช้งาน แต่กฎที่ดาวน์โหลดมาใช้งานนั้นอาจยังไม่ได้รับการตรวจสอบที่ดี หรือกฎที่นำมาใช้งานนั้นอาจไม่เหมาะสมกับกิจกรรมต่าง ๆ ที่เกิดขึ้นภายในระบบเครือข่าย จึงเป็นสาเหตุให้โปรแกรมสนอร์ตสร้างการแจ้งเตือนที่ผิดพลาด

วิธีการแก้ปัญหาข้างต้นนี้ผู้วิจัยได้จัดสร้างระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต โดยการจัดเก็บข้อมูลสภาพแวดล้อมภายในระบบเครือข่ายในขณะที่เกิดการแจ้งเตือน นำข้อมูลมาบันทึกและวิเคราะห์ กับข้อมูลฐานความรู้ (Knowledge Base) ผลที่ได้จะถูกนำมากำหนดค่าให้กับพารามิเตอร์ของระบบ พารามิเตอร์ของระบบจะเป็นข้อมูลขาเข้าของระบบเครือข่ายใยประสาท ระบบเครือข่ายใยประสาทจะทำหน้าที่จำแนกประเภทการบุกระบบเครือข่ายและประเมินระดับค่าบ่งชี้การแจ้งเตือน การแจ้งเตือนที่มีระดับค่าบ่งชี้ต่ำจะถูกนำไปปรับลดกฎที่เป็นสาเหตุทำให้เกิดการแจ้งเตือนที่ผิดพลาด

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการศึกษา

โปรแกรมสนอร์ตตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพจึงได้รับความนิยมในการใช้งาน แต่การแจ้งเตือนผิดพลาดที่เกิดขึ้นจำนวนมากได้กลายเป็นข้อเสียของโปรแกรมสนอร์ต เพื่อลดปัญหาดังกล่าว ทางผู้วิจัยได้เสนอกลไกสำหรับลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต โดยการประเมินระดับค่าบ่งชี้การแจ้งเตือนที่เกิดขึ้น การแจ้งเตือนที่มีระดับค่าบ่งชี้ต่ำจะถูกนำไปปรับลดกฎที่เป็นสาเหตุทำให้เกิดการแจ้งเตือนที่ผิดพลาด

การแจ้งเตือนที่เกิดขึ้นจะถูกจัดเก็บในฐานข้อมูลของระบบ เพื่อนำไปวิเคราะห์และกำหนดค่าให้กับพารามิเตอร์ที่กำหนดเพื่อนำไปใช้ในการประเมินระดับคุณภาพการแจ้งเตือน การประเมินคุณภาพการแจ้งเตือนได้ประยุกต์ใช้ระบบเครือข่ายใยประสาทในการทำงาน ระบบเครือข่ายใยประสาทจะผ่านการฝึกด้วยชุดข้อมูลในกระบวนการเรียนรู้ให้มีความชำนาญ สามารถจำแนกประเภทการบุกรุกระบบเครือข่าย และประเมินระดับค่าบ่งชี้แจ้งเตือนได้อย่างมีประสิทธิภาพ ข้อมูลขาเข้าของระบบเครือข่ายใยประสาทจะเป็นพารามิเตอร์ที่ระบบกำหนดขึ้น ค่าพารามิเตอร์จะถูกกำหนดด้วยข้อมูลสภาพแวดล้อมภายในระบบเครือข่าย และฐานความรู้ของระบบ ผลลัพธ์ที่ได้จากระบบเครือข่ายใยประสาทจะเป็นรูปแบบการบุกรุกระบบเครือข่าย และระดับค่าบ่งชี้การแจ้งเตือน

1.5 การเปรียบเทียบระหว่างวิธีการที่นำเสนอกับวิธีการแบบอื่น ๆ

ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตเมื่อนำมาเปรียบเทียบกับโปรแกรมสนอร์ตที่ทำงานโดยใช้กฎที่ดาวน์โหลดมาใช้งานทันที โปรแกรมสนอร์ตจะสร้างการแจ้งเตือนขึ้นเป็นจำนวนมากทั้งการแจ้งเตือนเมื่อระบบตกอยู่ในอันตราย และการแจ้งเตือนที่ผิดพลาดอันเนื่องมาจากการกำหนดกฎที่ผิดพลาด หรือกฎไม่เหมาะสมกับสภาพแวดล้อมภายในระบบเครือข่าย ส่งผลให้โปรแกรมสนอร์ตทำงานอย่างไม่มีประสิทธิภาพ ดังนั้นเมื่อเปรียบเทียบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตกับวิธีอื่นแล้ว โปรแกรมสนอร์ตจะสร้างการแจ้งเตือนที่ผิดพลาดน้อยลง

1.6 ขอบเขตการวิจัย

ในวิทยานิพนธ์ฉบับนี้ได้นำเสนอระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต โดยการจัดเก็บข้อมูลสภาพแวดล้อมภายในระบบเครือข่ายในขณะที่โปรแกรมสนอร์ตสร้างการแจ้งเตือน บันทึกและวิเคราะห์ข้อมูลเพื่อกำหนดค่าให้กับพารามิเตอร์ของระบบ การวิเคราะห์ข้อมูลจะเป็นการนำข้อมูลที่จัดเก็บมาตรวจสอบกับข้อมูลฐานความรู้ของระบบ ข้อมูลฐานความรู้ของระบบจะเป็นข้อมูลที่เกี่ยวข้องกับช่องโหว่ต่าง ๆ และข้อมูลเกี่ยวกับซอฟต์แวร์ที่ใช้

งาน ค่าพารามิเตอร์จะนำมาใช้เป็นข้อมูลนำเข้าของระบบเครือข่ายใยประสาท ระบบเครือข่ายใยประสาทจะทำหน้าที่จำแนกรูปแบบการบุกรุกระบบเครือข่าย และประเมินระดับค่าบ่งชี้การแจ้งเตือนที่เกิดขึ้น ผลลัพธ์ที่ได้จะถูกนำเสนอต่อผู้ดูแลระบบเครือข่ายด้วยระบบนำเสนอคุณภาพการแจ้งเตือนที่เกิดขึ้น วิทยานิพนธ์ฉบับนี้จะใช้คอมพิวเตอร์ในการสร้างระบบเครือข่ายใยประสาทด้วยโปรแกรม MATLAB

1.7 เนื้อหาของวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกันคือ

บทที่ 1 กล่าวถึงความเป็นมาของงานวิจัย ความมุ่งหมายและวัตถุประสงค์ สมมติฐาน ทฤษฎีที่ใช้ ขอบเขตของการวิจัย และเนื้อหาของวิทยานิพนธ์

บทที่ 2 กล่าวถึงระบบการตรวจจับการบุกรุกบนระบบเครือข่าย การตรวจจับการบุกรุกระบบเครือข่ายด้วยโปรแกรมสนอร์ต การตั้งค่าโปรแกรมสนอร์ต ระบบเครือข่ายใยประสาท และงานวิจัยที่เกี่ยวข้อง

บทที่ 3 กล่าวถึงสาเหตุการเกิดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต กลไกการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ค่าพารามิเตอร์ และเงื่อนไขการกำหนดค่าพารามิเตอร์ของ Post Processor การจัดเก็บข้อมูลของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต การประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต และการนำเสนอข้อมูลของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

บทที่ 4 กล่าวถึง สภาพแวดล้อมบนระบบเครือข่ายที่ใช้ในการทดสอบระบบประเมินคุณภาพการแจ้งของโปรแกรมสนอร์ต ผลการทดสอบระบบเครือข่ายใยประสาท ผลการทดลองของระบบเมื่อเปรียบเทียบกับวิธีพื้นฐาน และผลการทดลองของระบบเมื่อเทียบกับวิธีการอื่น ๆ

บทที่ 5 เป็นบทสรุปผลการวิจัยและข้อเสนอแนะ

บทที่ 2
ทฤษฎีพื้นฐานที่ใช้ในการวิจัย

บทนี้จะกล่าวถึงทฤษฎีที่เกี่ยวข้องกับงานวิจัย การบุกรุกระบบเครือข่าย รูปแบบการบุกรุกระบบเครือข่าย ระบบการตรวจจับการบุกรุก ประเภทของระบบการตรวจจับการบุกรุก วิธีการตรวจจับการบุกรุก การตรวจจับการบุกรุกด้วยโปรแกรมสนอร์ต การตั้งค่าของโปรแกรมสนอร์ต ระบบเครือข่ายใยประสาท และงานวิจัยที่เกี่ยวข้อง

2.1 ระบบการตรวจจับการบุกรุกบนระบบเครือข่าย

ในปัจจุบันการใช้งานคอมพิวเตอร์ได้เปลี่ยนไปจากในอดีตโดยสิ้นเชิง มีการนำคอมพิวเตอร์เชื่อมต่อเข้าเป็นระบบเครือข่ายเพื่อให้เกิดประโยชน์สูงสุดในการการใช้ข้อมูล และทรัพยากรที่มีอยู่ร่วมกันใน การเชื่อมต่อคอมพิวเตอร์เข้าเป็นระบบเครือข่ายมีทั้งข้อดีและข้อเสียในการใช้งาน หากผู้ใช้งานไม่มีระบบการรักษาความปลอดภัยที่ดีในการป้องกันระบบเครือข่ายก็จะทำให้ระบบเครือข่ายตกอยู่ในอันตรายจากกลุ่มบุคคลที่ไม่ประสงค์ดี กลุ่มบุคคลเหล่านั้นอาจมีแรงจูงใจหลายด้านด้วยกัน เช่น การทดลอง การบุกรุกระบบเครือข่ายเพื่อเข้าถึงข้อมูลที่เป็นความลับ หรือการโจมตีระบบเครือข่ายเพื่อให้เกิดความเสียหาย ดังนั้นในการรักษาความปลอดภัยระบบเครือข่ายจึงมีความจำเป็นอย่างยิ่ง ระบบตรวจจับการบุกรุกบนระบบเครือข่ายเป็นเทคนิคที่เกิดขึ้นมาใหม่และได้นำมาใช้งานเมื่อไม่กี่ปีที่ผ่านมา ระบบตรวจจับการบุกรุกทำหน้าที่ในการเฝ้าระวังหรือตรวจสอบเหตุการณ์ต่างๆที่เกิดขึ้นภายในระบบเครือข่าย เช่น การพยายามที่จะเข้าถึงข้อมูลที่เป็นความลับ การบิดเบือนข้อมูลจากความเป็นจริง และทำให้ข้อมูลเกิดความเสียหาย โดยการบุกรุกระบบเครือข่ายนั้นเกิดได้จากผู้ใช้งานอินเทอร์เน็ต หรือผู้ใช้งานภายในระบบเครือข่ายพยายามทำในสิ่งที่ไม่ได้รับอนุญาต จึงเป็นหน้าที่ของระบบตรวจจับการบุกรุกที่จะทำหน้าที่ตรวจจับสิ่งผิดปรกติที่เกิดขึ้นในระบบเครือข่ายแล้วแจ้งไปยังผู้ดูแลระบบเครือข่าย

2.1.1 ประเภทการบุกรุกระบบเครือข่าย [2], [3], [6] และ [14]

- การบุกรุกระบบเครือข่ายจากภายนอก (External Threats)

ปัจจุบันการเชื่อมต่ออินเทอร์เน็ตเป็นสิ่งที่จำเป็นอย่างยิ่งเพื่อใช้ในการค้นหาข้อมูล รับส่งอีเมล์ หรือการใช้งานข้อมูลร่วมกัน แต่การเชื่อมต่อเข้ากับอินเทอร์เน็ตมีทั้งข้อดีและข้อเสีย เนื่องจากผู้ใช้งานอินเทอร์เน็ตมีอยู่ทั่วโลกมีทั้งผู้ที่ใช้งานปรกติและผู้ที่มีพฤติกรรมเป็นอันตรายต่อระบบเครือข่ายที่เรียกว่าแฮกเกอร์ แฮกเกอร์ได้สร้างความเสียหายให้กับองค์กรเป็นอย่างมากไม่ว่าจะเป็นการทำลายชื่อเสียงขององค์กร หรือทำให้องค์กรไม่ได้รับความไว้วางใจจากลูกค้าที่มาใช้บริการ แนวทางในการป้องกันผู้บุกรุกระบบเครือข่ายจากภายนอกนั้นสามารถทำได้หลายวิธีไม่ว่า

จะใช้อุปกรณ์ป้องกันระบบเครือข่าย เช่น ไฟล์วอล IPS หรือ IDS รวมถึงนโยบายในการป้องกันระบบเครือข่าย เครื่องมือและนโยบายที่นำมาใช้งานร่วมกันเปรียบเสมือนเกราะป้องกันที่ทำให้องค์กรมีความเสี่ยงน้อยลง และมีความปลอดภัยจากผู้บุกรุกระบบเครือข่ายเพิ่มมากขึ้น

- การบุกรุกระบบเครือข่ายจากภายใน (Internal Threats)

การบุกรุกระบบเครือข่ายจากภายในเป็นภัยที่เกิดจากบุคคล หรือผู้ใช้งานระบบเครือข่ายภายในองค์กร การบุกรุกภายในองค์กรนั้นเป็นภัยใกล้ตัวที่สร้างความเสียหายให้กับระบบเครือข่ายเป็นอย่างมาก การบุกรุกระบบเครือข่ายจากภายในจะใช้วิธีการบุกรุกระบบเครือข่ายที่ง่ายกว่าแฮกเกอร์ใช้ในการบุกรุกระบบเครือข่ายจากภายนอก โดยผู้บุรุกไม่จำเป็นต้องใช้ประสบการณ์ หรือความรู้มากก็สามารถเข้าถึงข้อมูลที่เป็นความลับขององค์กรได้ ดังนั้นนโยบายด้านความปลอดภัยภายในองค์กรจึงเป็นสิ่งสำคัญอย่างยิ่ง การกำหนดสิทธิ์ในการเข้าใช้งานภายในระบบเครือข่าย และสิทธิ์ในการเข้าถึงข้อมูลหากไม่มีความเหมาะสมหรือเกินกว่างานที่รับผิดชอบของพนักงานก็จะทำให้ข้อมูลที่เป็นความลับตกอยู่ในอันตราย จากการตรวจจับผู้กระทำผิดด้านคอมพิวเตอร์หรืออาชญากรรมคอมพิวเตอร์ ส่วนใหญ่เกิดจากพนักงานภายในองค์กรซึ่งในปัจจุบันสื่อการสอน และหนังสือจำนวนมากที่เปิดเผยวิธีการเข้าบุกรุกระบบเครือข่าย ก็มีผู้คนจำนวนไม่น้อยที่ศึกษา และนำมาลองกับระบบเครือข่ายภายในองค์กรที่ตนเองทำงาน เช่น พนักงานได้นำโปรแกรมแฮกเกอร์ หรือสนิฟเฟอร์มาทดสอบใช้งานเป็นต้น การบุกรุกระบบเครือข่ายจากภายในยังรวมถึงการแอบใช้งานทรัพยากรในบริษัทที่ผิดวัตถุประสงค์ เช่น การใช้เครื่องในบริษัทเล่น P2P (Peer to Peer) ทำให้สิ้นเปลืองแบนด์วิดท์ขององค์กร

2.1.2 รูปแบบการบุกรุกระบบเครือข่าย [3], [6], [7] และ [15]

รูปแบบการบุกรุกระบบเครือข่ายสามารถแบ่งออกเป็น 4 รูปแบบดังนี้

- DoS: Denial of Service

Denial of Service Attacks เป็นลักษณะหนึ่งของการบุกรุกที่กระทำได้ง่ายโดยมุ่งเน้นในการรบกวนขัดขวางการทำงานของคอมพิวเตอร์ อุปกรณ์ต่อพ่วง หรือระบบเครือข่ายคอมพิวเตอร์ให้ทำงานหนักจนไม่สามารถให้บริการได้ตัวอย่างการโจมตีชนิดนี้ได้แก่ Syn flood, PING of Death, Land Attack, Teardrop Attack, ICMP Flood หรือแม้แต่โปรแกรมประเภทไวรัสหรือเวิร์มที่แพร่กระจายอยู่บนอินเทอร์เน็ต

- Unauthorized Access from a Remote Machine

Remote to User Attacks เป็นการโจมตีซึ่งผู้บุกรุกระบบเครือข่ายจะส่งแพ็คเก็จมาที่เครื่องแม่ข่าย (Server) ผ่านระบบเครือข่ายหรืออินเทอร์เน็ต ผู้บุกรุกจะไม่มีชื่อผู้ใช้งาน (Account) อยู่ที่เครื่องแม่ข่าย ผู้บุกรุกจะพยายามทำให้ตัวเองเข้าไปสู่ระบบเครือข่ายด้วยช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากฮาร์ดแวร์ ซอฟท์แวร์ พอร์ตสื่อสาร (Port) หรือระบบปฏิบัติการ ตัวอย่างของการบุกรุกระบบเครือข่ายประเภทนี้ได้แก่ Ftp-write, Fuest, Imap, Named และ Phf sendmail เป็นต้น

- U2R: unauthorized access to local super user (root) privileges

พฤติกรรม U2R (Use to Root) เป็นการบุกรุกระบบเครือข่ายซึ่งผู้บุกรุกระบบเครือข่ายจะเป็นผู้ใช้งานทั่วไปบนระบบเครือข่ายก่อน จากนั้นจะพยายามทำให้ตัวเองให้มีสิทธิ์ในการใช้งานเท่าเทียมกับผู้ดูแลระบบ (Root) เพื่อนำสิทธิ์ที่ได้ไปเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต หรือข้อมูลที่เป็นความลับบนระบบเครือข่าย ตัวอย่างของการโจมตีประเภทนี้ เช่น Eject, Ffbconfig, Fdformat, และ Loadmodule

- Probing: surveillance and other probing

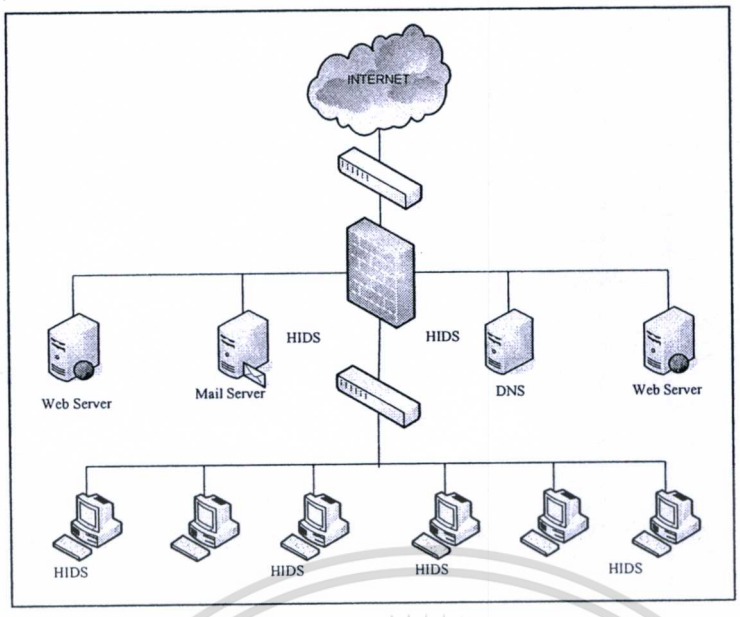
Probing เป็นขั้นตอนแรกที่ผู้บุกรุกระบบเครือข่ายใช้ในการรวบรวมข้อมูลของเหยื่อ ข้อมูลที่เป็นช่องโหว่ เช่น ระบบปฏิบัติการ โปรแกรมที่ใช้งาน พอร์ตที่ใช้งาน หรือข้อมูลที่เกี่ยวข้องกับเหยื่อ เช่น ชื่อของโฮสต์ ที่อยู่ไอพี (IP Address) เซอร์วิส (Service) ปัจจุบันการหาข้อมูลของเหยื่อสามารถทำได้สะดวกและรวดเร็วโดยการใช้ซอฟต์แวร์ทำงาน ผ่านอินเทอร์เน็ต ตัวอย่างซอฟต์แวร์ที่ใช้ในการหาข้อมูลของเหยื่อ ซอฟต์แวร์จำพวก PING Sweep, port scan, account scans และ DNS zone transfer เป็นซอฟต์แวร์ที่มีจำหน่ายอยู่ตามท้องตลาด หรือซอฟต์แวร์ที่เป็นฟรีแวร์เช่น STROBE, NETSCAN, SATAN, NMAP และ NESSUS เป็นต้น

2.1.3 ประเภทของระบบตรวจจับการบุกรุกบนระบบเครือข่าย [2], [3], [7], [20], [22] และ [28]

ปัจจุบันระบบตรวจจับการบุกรุกบนระบบเครือข่ายสามารถจำแนกได้ 2 ประเภท คือ Network–Based IDS และ Host–Based IDS

- Host-based Intrusion Detection System: HIDS

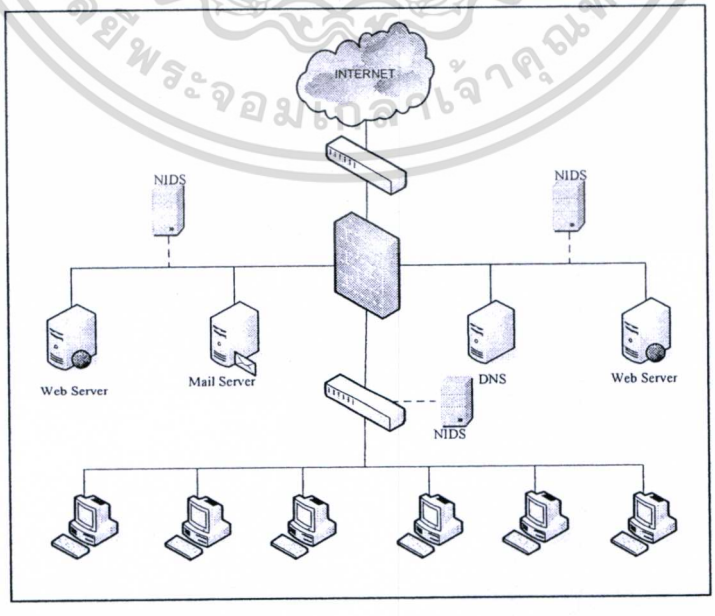
ระบบตรวจจับการบุกรุกบนระบบเครือข่ายบนโฮสต์ (Host-based Intrusion Detection System: HIDS) จะมีการติดตั้งโปรแกรมเอเจนต์ (Agent) ไว้ที่โฮสต์มีระบบเฝ้าติดตาม (monitor) และตรวจจับการใช้งานภายในระบบเครือข่าย ระบบตรวจจับการบุกรุกบนระบบเครือข่ายประเภทนี้ยังใช้ประโยชน์จากไฟล์ประวัติการทำงานงาน (Log File) ในการตรวจจับกิจกรรมที่เป็นอันตรายต่อระบบเครือข่ายอีกช่องทางหนึ่ง การทำงานของ HIDS มีรูปแบบการทำงานที่เป็นรีแอคทีฟ (Reactive) และโปรแอคทีฟ (Proactive) การทำงานที่มีลักษณะเป็นรีแอคทีฟ คือระบบจะสร้างการการแจ้งเตือนก็ต่อเมื่อมีการบุกรุกระบบเครือข่ายจริง หรือมีเหตุการณ์ที่เป็นอันตรายต่อระบบเครือข่ายเกิดขึ้น การทำงานที่มีลักษณะเป็นโปรแอคทีฟคือระบบจะดักจับข้อมูลที่มีลักษณะผิดปรกติ หรือกิจกรรมที่เป็นอันตรายที่เข้ามาในระบบเครือข่ายแล้วนำมาวิเคราะห์เพื่อสร้างการแจ้งเตือนไปยังผู้ดูแลระบบโดยทันที



รูปที่ 2.1 รูปแบบการติดตั้งระบบตรวจจับการบุกรุกบนระบบเครือข่ายบนโฮสต์

- Network-based Intrusion Detection System: NIDS

ระบบการตรวจจับการบุกรุกบนระบบเครือข่าย (Network-based Intrusion Detection System: NIDS) ระบบจะตรวจจับข้อมูลจากทราฟฟิคที่เข้ามาสู่ระบบเครือข่ายไม่ว่าจะมาจากตัวกลางที่มีสาย (Cable) หรือตัวกลางชนิดไร้สาย (Wireless) และนำมาข้อมูลที่ได้มาเปรียบเทียบกับรูปแบบตรวจจับการบุกรุกที่กำหนด (Signature) รูปแบบการตรวจจับการบุกรุกจะถูกกำหนดด้วยกฎ ถ้าข้อมูลที่ตรวจจับได้มีรูปแบบตรงกับรูปแบบในกฎ NIDS ก็จะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบทราบทันที หรือจัดเก็บไว้ในฐานข้อมูลเพื่อนำมาวิเคราะห์ต่อไป



รูปที่ 2.2 รูปแบบการติดตั้งระบบการตรวจจับการบุกรุกบนระบบเครือข่าย

2.1.4 ประเภทการตรวจจับการบุกรุกบนระบบเครือข่าย [15], [19] และ [25]

ประเภทของการตรวจจับการบุกรุกบนระบบเครือข่ายสามารถทำได้ 2 วิธีคือ Knowledge-Based และ Behavior-Based

- Knowledge-Based IDS

จะใช้ฐานความรู้ของระบบในการตรวจจับการบุกรุก ซึ่งประกอบด้วยข้อมูลรูปแบบการบุกรุกระบบเครือข่ายประเภทต่างๆ และข้อมูลช่องโหว่ที่เกิดขึ้นภายในระบบเครือข่าย ดังนั้นประสิทธิภาพการทำงานจะขึ้นอยู่กับความครบถ้วนสมบูรณ์ของข้อมูล และการอัพเดทข้อมูลฐานความรู้ของระบบ

ข้อดี การใช้ฐานความรู้ในการตรวจจับการบุกรุกคือ อัตราการเกิดการแจ้งเตือนที่ผิดพลาดน้อย และข้อมูลที่ได้จากระบบตรวจจับการบุกรุกบนระบบเครือข่ายจะมีความละเอียดสูง สามารถนำไปใช้ประโยชน์ในการรักษาความปลอดภัยบนระบบเครือข่ายต่อได้

ข้อเสีย การใช้ฐานความรู้ในการตรวจจับการบุกรุกระบบเครือข่าย คือความยากในการจัดทำฐานความรู้ให้ครอบคลุม เช่น ข้อมูลการบุกรุกระบบเครือข่ายประเภทต่างๆ ข้อมูลช่องโหว่บนระบบเครือข่าย และการอัพเดทฐานความรู้อย่างสม่ำเสมอ นอกจากนั้นการตรวจจับการบุกรุกรูปแบบดังกล่าวจะไม่สามารถตรวจจับการบุกรุกแบบ U2R ได้

- Behavior-Base IDS

ใช้รูปแบบพฤติกรรมปรกติบนระบบเครือข่ายในการตรวจจับการบุกรุก พฤติกรรมปรกติสามารถกำหนดได้จากพฤติกรรมการใช้งานทั่วไปบนระบบเครือข่ายหรือข้อมูลอ้างอิงจากอินเทอร์เน็ต เช่น ข้อมูลจาก CVE Mitre[4] หรือ CERT[6] ระบบตรวจจับการบุกรุกจะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่ายเมื่อตรวจพบพฤติกรรมที่ไม่ปรกติเกิดขึ้น

ข้อดี การใช้รูปแบบพฤติกรรมปรกติบนระบบเครือข่ายในการตรวจจับการบุกรุกสามารถตรวจจับการบุกรุกรูปแบบใหม่ที่ไม่เคยเกิดขึ้นในระบบเครือข่ายได้ และสามารถตรวจจับการบุกรุกที่ไม่เกี่ยวข้องกับช่องโหว่ที่เกิดขึ้นบนระบบเครือข่าย เช่น การบุกรุกแบบ U2R

ข้อเสีย เทคนิคดังกล่าวจะเกิดการแจ้งเตือนที่ผิดพลาดสูง เนื่องจากพฤติกรรมที่เกิดขึ้นภายในระบบเครือข่ายมักมีการเปลี่ยนแปลงอยู่ตลอดเวลา จึงเป็นการยากที่จะรูปแบบพฤติกรรมปรกติให้กับระบบตรวจจับการบุกรุกระบบเครือข่าย

2.1.5 วิธีการตรวจจับการบุกรุกระบบเครือข่าย [5], [7], [10], [14], [18] และ [28]

- Signature Detection

เป็นการเรียนรู้การบุกรุกระบบเครือข่ายที่เกิดขึ้น และนำข้อมูลที่ได้มาจัดเก็บเพื่อนำมากำหนดเป็นรูปแบบการตรวจจับการบุกรุกระบบเครือข่าย เมื่อเหตุการณ์ที่เกิดขึ้นตรงกับรูปแบบการตรวจจับการบุกรุกจะมีการสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย การตรวจจับการบุกรุกด้วยเทคนิคนี้จะมีความถูกต้องแม่นยำสูง แต่จะมีข้อจำกัดหากระบบตรวจจับการบุกรุกระบบ

เครือข่ายไม่เคยพบกับกิจกรรมหรือเหตุการณ์ที่เกิดขึ้นมา ระบบตรวจจับการบุกรุกระบบเครือข่ายจะมองว่าพฤติกรรมดังกล่าวเป็นการบุกรุกระบบเครือข่าย และจะสร้างการแจ้งเตือนที่ผิดพลาดไปยังผู้ดูแลระบบเครือข่าย ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่ผู้ดูแลระบบเครือข่ายจะต้องปรับปรุงรูปแบบการบุกรุกระบบเครือข่ายอยู่เสมอเพื่อให้สามารถตรวจจับการบุกรุกรูปแบบใหม่ ๆ ที่เกิดขึ้น

- Anomaly Detection

เป็นการตรวจจับสิ่งผิดปรกติจากรูปแบบของข้อมูลที่กำหนดขึ้น โดยระบบตรวจจับการบุกรุกระบบเครือข่ายจะสร้างชุดข้อมูลปรกติและกำหนดให้เป็น “Normal Use” หากเกิดเหตุการณ์หรือพฤติกรรมแตกต่างไปจากชุดข้อมูลปรกติที่กำหนดขึ้น ระบบตรวจจับการบุกรุกระบบเครือข่ายจะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย การตรวจจับการบุกรุกระบบเครือข่ายโดยการกำหนดชุดข้อมูลปรกติจะถูกนำมาใช้การตรวจสอบการละเมิดสิทธิ์ในการเข้างาน หรือการเข้าถึงไฟล์ที่เป็นระบบปฏิบัติการ ขีดจำกัดของการตรวจจับการบุกรุกระบบเครือข่ายชนิดนี้คือหากกำหนดชุดข้อมูลปรกติไม่ครอบคลุม จะทำให้ระบบตรวจจับการบุกรุกระบบเครือข่ายสร้างการแจ้งเตือนที่ผิดพลาด หรือการกำหนดชุดข้อมูลปรกติผิดพลาดก็อาจจะทำให้ระบบตรวจจับการบุกรุกบนระบบเครือข่ายทำงานล้มเหลวได้ เช่น ผู้ใช้งานได้ขโมยข้อมูลของบริษัททุกๆ คืนที่เวลา 3.00 AM ระบบตรวจจับการบุกรุกระบบเครือข่ายอาจเข้าใจว่าเป็นพฤติกรรมปรกติทำให้ไม่ระบบตรวจจับการบุกรุกบนระเครือข่ายไม่ประสบความสำเร็จในการทำงาน

- Integrity Verification

มีรูปแบบการทำงานที่ไม่ซับซ้อนแต่มีประสิทธิภาพในการทำงานสูง จะทำงานโดยการค่าสร้างผลรวม (Checksum) ให้กับทุกๆไฟล์บนระบบเครือข่ายแล้วนำมาเปรียบเทียบกับค่าผลรวมเริ่มต้นที่คำนวณได้ก่อนนำไฟล์ไปใช้งาน เมื่อระบบตรวจจับการบุกรุกบนระบบเครือข่ายเปรียบเทียบค่าผลรวมของไฟล์ก่อนนำมาใช้งานกับที่ใช้งานจริงมีค่าไม่ตรงกัน ก็จะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย

การตรวจจับการบุกรุกด้วยวิธีการนี้จะถูกนำมาใช้ในการตรวจหาความเสียหายของเว็บเพจที่ทำงานอยู่บนเครื่องให้บริการเว็บไซต์ หากเว็บเพจถูกแก้ไขระบบตรวจจับการบุกรุกจะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่ายโดยทันที

2.2 การตรวจจับการบุกรุกบนระบบเครือข่ายด้วยโปรแกรมสนอร์ต [2], [3], [14] [15], [19], [20] และ [22]

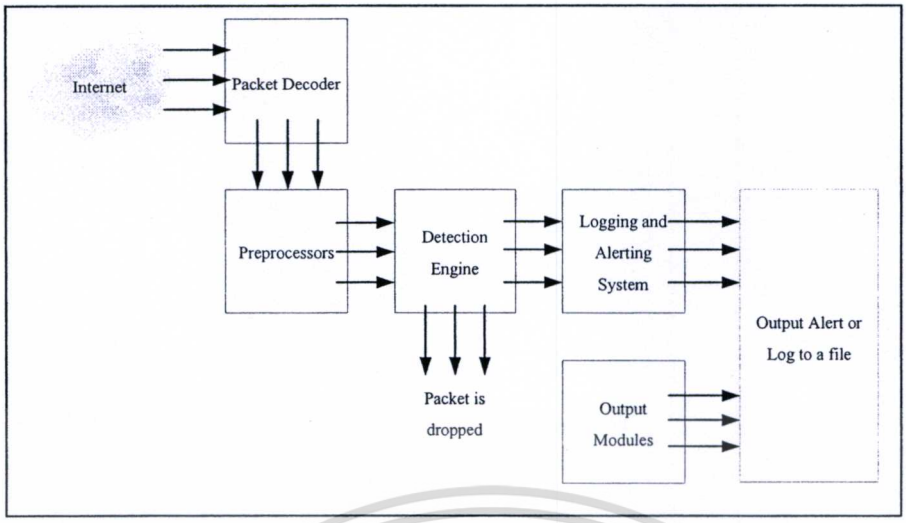
โปรแกรมสนอร์ตได้ถูกพัฒนามาอย่างต่อเนื่อง โดยโปรแกรมสนอร์ตมีจุดเริ่มต้นมาจากเครื่องมือที่ใช้ในการจัดการระบบเครือข่ายที่มีโครงสร้างการทำงานไม่ซับซ้อนจนกลายเป็นระบบตรวจจับการบุกรุกบนระบบเครือข่ายที่ได้รับความนิยมจากผู้ใช้งานทั่วโลก ตั้งแต่โปรแกรม-

สนอร์ตถูกสร้างขึ้นในปี 1998 สนอร์ตเซ็นเซอร์ (Snort Sensor) ได้ถูกติดตั้งทั่วโลกไปแล้วกว่า 500,000 เซ็นเซอร์ โปรแกรมสนอร์ตเป็นระบบตรวจจับการบุกรุกบนระบบเครือข่ายที่ทำงานโดยใช้ระบบเครือข่ายเป็นโครงสร้างพื้นฐาน Marty Roesch เป็นผู้สร้างโปรแกรมสนอร์ตขึ้นมา โดยโปรแกรมสนอร์ตที่ถูกพัฒนาขึ้นมานั้นเป็นเพียงเครื่องมือที่ใช้ในการวิเคราะห์ทราฟฟิคภายในระบบเครือข่ายเท่านั้น เมื่อนำโปรแกรมสนอร์ตมาเปรียบเทียบกับโปรแกรม Tcpdump โปรแกรมสนอร์ตจะแสดงผลลัพธ์ออกมาในรูปของเลขฐาน 2 แต่โปรแกรม Tcpdump จะแสดงผลลัพธ์ออกมาเป็นภาษาที่มนุษย์สามารถเข้าใจได้ จึงทำให้โปรแกรมสนอร์ตไม่ได้รับความนิยมในการใช้งาน ทำให้ Marty ตัดสินใจไม่พัฒนาโปรแกรมสนอร์ตเวอร์ชั่นอื่น ๆ จึงเป็นจุดสิ้นสุดของโปรแกรมสนอร์ตและทำให้โปรแกรมสนอร์ตกลายเป็นเพียงความทรงจำเท่านั้น

โปรแกรมสนอร์ตได้ถูกนำมาพัฒนาขึ้นใหม่อีกครั้ง จากกลุ่มผู้เชี่ยวชาญด้านการรักษาความปลอดภัยบนระบบเครือข่ายโดยพัฒนามาจากโปรแกรมสนอร์ตของ Marty ทำให้ความสามารถของโปรแกรมสนอร์ตเพิ่มมากขึ้น โปรแกรมสนอร์ตสามารถใช้ในการดักจับแพ็คเก็จ เก็บประวัติของแพ็คเก็จ และเป็นระบบการตรวจจับการบุกรุกระบบเครือข่ายที่ทำงานได้อย่างมีประสิทธิภาพ

ระดับที่เหมาะสมในการตรวจจับแพ็คเก็จของโปรแกรมสนอร์ต จะอยู่ที่การสื่อสารบนระบบเครือข่ายมีปริมาณไม่เกิน 100 Mb/s โปรแกรมสนอร์ตจะมีความสามารถในการตรวจจับแพ็คเก็จได้ลดลงเมื่อการสื่อสารบนระบบเครือข่ายที่มีปริมาณเพิ่มขึ้นเป็น 200 – 300 Mb/s และจะไม่สามารถทำงานได้เมื่อการสื่อสารบนระบบเครือข่ายมีปริมาณสูงเกินกว่า 500 Mb/s จากข้อมูลที่กล่าวมาชี้ให้เห็นว่าโปรแกรมสนอร์ตจะทำงานได้อย่างมีประสิทธิภาพจะต้องมีสภาวะแวดล้อมที่เหมาะสมในการทำงาน

โปรแกรมสนอร์ตเป็นฟรีแวร์ที่สามารถนำมาใช้ได้โดยไม่ต้องเสียค่าใช้จ่ายแต่อย่างใด ผู้ที่ต้องการใช้งานสามารถดาวน์โหลดซอฟท์แวร์ได้ที่ www.snort.org หรือเว็บไซต์อื่น ๆ โปรแกรมสนอร์ตได้ถูกแบ่งการทำงานออกเป็นหลายโมดูล แต่ละโมดูลจะทำงานร่วมกันเพื่อตรวจจับการบุกรุกบนระบบเครือข่าย และสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่ายโดยส่วนประกอบของโปรแกรมสนอร์ตได้แสดงในรูปที่ 2.3



รูปที่ 2.3 ส่วนประกอบของโปรแกรมสนอร์ต

2.2.1 Packet Decoder

Packet Decoder จะทำหน้าที่รับแพ็คเก็จจากระบบเครือข่ายภายในหรืออินเทอร์เน็ต และจัดเตรียมแพ็คเก็จ แพ็คเก็จที่มาสู่ Packet Decoder จะมีประเภทของแพ็คเก็จที่แตกต่างกันออกไป เมื่อ Packet Decoder ได้รับแพ็คเก็จก็จะจัดเตรียมแพ็คเก็จจัดส่งไปยังการทำงานส่วนอื่น เช่น Preprocessor หรือ Detection Engine

2.2.2 Preprocessor

Preprocessor เป็นส่วนที่เพิ่มขึ้นมาในโปรแกรมสนอร์ตทำหน้าที่ในการจัดเตรียมแพ็คเก็จก่อนจัดส่งไปยัง Detection Engine Preprocessor บางตัวสามารถทำการตรวจจับการบุกรุกได้โดยการตรวจสอบจากความผิดปรกติในส่วนหัวของแพ็คเก็จ และสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย Preprocessor จะมีความสำคัญอย่างยิ่งสำหรับระบบตรวจจับการบุกรุกที่ใช้ Detection Engine ในการกำหนดกฎในการตรวจจับการบุกรุกระบบเครือข่าย แฮกเกอร์มักจะใช้เทคนิคที่แตกต่างกันออกไปเพื่อไม่ให้ระบบตรวจจับการบุกรุกไม่สามารถตรวจพบ ตัวอย่างเช่น ผู้ใช้งานสร้างกฎในการตรวจจับสตริงของโปรแกรม หรือสคลิปต์ที่เป็นการบุกรุกระบบเครือข่ายประกอบไปด้วย “scripts/iisadmin” ในแพ็คเก็จที่มาจากโปรโตคอล HTTP (Hyper Text Tranfer Protocal) ถ้านำสตริงมาเปรียบเทียบกับแพ็คเก็จที่เข้ามาเป็นที่แน่นอนว่าจะสามารถตรวจจับการบุกรุกได้ แต่ถ้าแฮกเกอร์ได้ทำการปรับแต่งสตริงระบบตรวจจับการบุกรุกก็จะไม่ตรวจพบสตริงดังกล่าว

ตัวอย่างการปรับแต่งชุดสตริงเพื่อหลีกเหลี่ยงการตรวจพบของระบบตรวจจับการบุกรุก

- “scripts/./iisadmin”
- “scripts/examples/../iisadmin”
- “scripts\iisadmin”

- "scripts/.\iisadmin"

แฮกเกอร์สามารถแทรกเลขฐาน 16 หรือ Unicode ลงใน URI (Uniform Resource Identifier) ซึ่งเป็นสิ่งที่สามารถทำได้โดยไม่ผิดกฎการทำงานของ HTTP จึงทำให้เว็บเซิร์ฟเวอร์ตกอยู่ในอันตราย โดยปรกติแล้วเว็บเซิร์ฟเวอร์จะเข้าใจสตริงและสามารถแบ่งสตริง "scripts/iis-admin" เพื่อจัดเตรียมสตริงก่อนส่งไปประมวลผล เมื่อระบบตรวจจับการบุกรุกมองว่าสตริงที่ถูกปรับแต่งไม่ตรงตามที่ได้กำหนดก็จะทำให้ระบบตรวจจับการบุกรุกไม่สามารถตรวจจับการบุกรุกได้ แต่ปัญหาดังกล่าวได้ถูกแก้ด้วย Preprocessor โดย Preprocessor จะสามารถทำการจัดเตรียมชุดของสตริงขึ้นมาใหม่เพื่อสามารถตรวจพบการบุกรุกดังกล่าว

การตรวจสอบข้อมูลที่มีขนาดใหญ่เกิน MTU (Maximum Transfer Unit) ระบบตรวจจับการบุกรุกจะต้องทำการรวมแพ็คเก็จย่อยก่อนที่จะนำแพ็คเก็จไปเปรียบเทียบกับกฎ หรือเปรียบ-เทียบกับรูปแบบตรวจจับบุกรุกที่กำหนด ขั้นตอนการรวมแพ็คเก็จย่อยก่อนนำไปตรวจสอบเป็นหน้าที่ของ Preprocessor ด้วยเช่นกัน

2.2.3 Detection Engine

Detection Engine เป็นส่วนประกอบที่สำคัญที่สุดของโปรแกรมสนอร์ต Detection Engine จะทำหน้าที่ในการตรวจจับการบุกรุกระบบเครือข่าย และกิจกรรมที่เป็นอันตรายต่อระบบเครือข่าย Detection Engine ของโปรแกรมสนอร์ตจะใช้การกำหนดกฎในการตรวจจับการบุกรุกระบบเครือข่าย ถ้าแพ็คเก็จที่เข้ามาตรงกับโครงสร้างของกฎที่กำหนดโปรแกรมจะมีตอบสนอง เช่น ละทิ้ง (Drop) แพ็คเก็จ เก็บประวัติของแพ็คเก็จ หรือสร้างการแจ้งเตือนไปยังผู้ดูแลระบบ

ระยะเวลาในการทำงานของ Detection Engine มีความสำคัญอย่างยิ่งต่อประสิทธิภาพการทำงานของโปรแกรมสนอร์ต ความเร็วในการทำงานของ Detection Engine ขึ้นอยู่กับปัจจัยดังต่อไปนี้

- จำนวนของกฎที่กำหนด
- ประสิทธิภาพของเครื่องที่ทำการติดตั้งโปรแกรมสนอร์ต
- ความเร็วระบบสื่อสารภายในของเครื่อง (Bus) ที่ติดตั้งโปรแกรมสนอร์ต
- ปริมาณทราฟฟิคภายในระบบเครือข่าย

Detection Engine จะทำงานหนักเมื่อมีปริมาณทราฟฟิคที่เกิดขึ้นในระบบเครือข่ายสูง โปรแกรมสนอร์ตจะทำการละทิ้งการตรวจสอบแพ็คเก็จ และอาจหยุดการทำงาน

2.2.4 Output Modules

Output Modules จะทำหน้าที่แสดงผลลัพธ์ที่ได้จากการทำงานของระบบตรวจจับการบุกรุกบนระบบเครือข่าย ผลลัพธ์ที่ได้จากระบบตรวจจับการบุกรุกบนระบบเครือข่ายจะแตกต่างกันออกไปขึ้นอยู่กับการกำหนดค่าของผู้ใช้งานโดยสามารถกำหนดค่าได้ดังต่อไปนี้

- การจัดเก็บไฟล์ประวัติโดยไฟล์ประวัติที่ถูกสร้างจะถูกเก็บอยู่ใน /var/log/snort/alerts

- ส่งผ่านโปรโตคอล SNMP
- จัดเก็บไฟล์ประวัติลงในฐานข้อมูล MySql หรือ Oracle
- สร้างเป็น XML (eXtensible Markup Language)
- ส่งข้อความแบบ SMB เพื่อส่งต่อไปยังเครื่องที่ใช้งานบนระบบปฏิบัติการ Windows

2.3 การตั้งค่าโปรแกรมสนอร์ต [2], [3], [14] [15], [19], [20], [22], [23] และ [28]

กฎของของโปรแกรมสนอร์ตจะถูกใช้ในการตรวจจับการบุกรุกระบบเครือข่าย การกำหนดโครงสร้างของกฎ (Syntax) มีความสำคัญอย่างยิ่ง กฎจะต้องถูกต้องและเหมาะสมกับปริมาณทราฟฟิคภายในระบบเครือข่าย ถ้านำกฎที่มีโครงสร้างของกฎไม่ถูกต้องไปใช้งานจะทำให้เกิดการแจ้งเตือนที่ผิดพลาดขึ้น และการแจ้งเตือนที่ผิดพลาดจำนวนมากจะทำให้ฐานข้อมูลการตรวจจับการบุกรุกต้องทำงานหนัก

กฎของสนอร์ตได้ถูกแบ่งออกเป็น 2 ส่วนคือ Rule Header และ Rule Option โดยได้แสดงในรูปที่

รูปที่ 2.4 โครงสร้างพื้นฐานกฎของโปรแกรมสนอร์ต

Rule Header จะเก็บข้อมูลเกี่ยวกับพฤติกรรมของกฎ ข้อมูลในส่วนของ Rule Header จะถูกนำมาใช้ในการตรวจสอบแพ็คเก็จ ในส่วนของ Rule Option ถูกใช้สำหรับเก็บข้อมูลการแจ้งเตือน

Action	Protocol	Address	Port	Direction	Address	Port

รูปที่ 2.5 โครงสร้างในส่วนของ Rule Header

ฟิลด์การกระทำ (Field Action) ทำหน้าที่กำหนดพฤติกรรมของกฎ ในการสอบสนองต่อการรับแพ็คเก็จที่เข้ามาแล้วมีลักษณะตรงกับกฎที่กำหนดซึ่งอาจจะเป็นการสร้างการแจ้งเตือน เก็บประวัติของแพ็คเก็จ หรือกระตุ้นให้กฎอื่นๆ ทำงาน

ฟิลด์โปรโตคอล (Field Protocol) ใช้ในการกำหนดประเภทของแพ็คเก็จที่เข้ามาตรวจสอบ โดยกฎจะทำการตรวจสอบเฉพาะแพ็คเก็จที่มีโปรโตคอลตรงตามที่กฎได้กำหนดเท่านั้น ค่าของฟิลด์โปรโตคอลถูกนำมาใช้ในการตรวจสอบแพ็คเก็จเป็นอันดับแรก โปรโตคอล

ในชั้นเน็ตเวิร์คเลเยอร์ (Network Layer) เลขพอร์ตจะไม่มีความสำคัญในการกำหนดกฎให้กับโปรโตคอล IP และ โปรโตคอล ICMP

ฟิลด์ที่อยู่ (Field Address) ใช้ในการกำหนดที่มาและปลายทางของเพ็คเก็จ ซึ่งสามารถกำหนดเป็นโฮสต์เดียวหรือหลายโฮสต์ หรือที่อยู่ของระบบเครือข่าย (Network Address) กฎของโปรแกรมสนอร์ตจะประกอบไปด้วยข้อมูลฟิลด์ที่อยู่จำนวน 2 ฟิลด์ คือ ฟิลด์ที่อยู่ต้นทาง และฟิลด์ที่อยู่ปลายทาง ซึ่งถูกกำหนดด้วยค่าจากฟิลด์ทิศทาง (Field Direction) ตัวอย่างเช่น ถ้าฟิลด์ทิศทาง เป็น "->" หมายความว่าฟิลด์ที่อยู่ด้านซ้ายจะเป็นที่มาของแพ็คก็จ และฟิลด์ที่อยู่ด้านขวาจะเป็นปลายทางของแพ็คเก็จ

ฟิลด์ทิศทางถูกใช้ในการกำหนดที่มาและปลายทางของแพ็คเก็จให้กับฟิลด์ที่อยู่ และฟิลด์พอร์ต (Field Port)

```
Alert icmp any any -> any (msg: "Ping with TTL=100"; \
ttl : 100;)
```

รูปที่ 2.6 ตัวอย่างกฎที่สร้างการแจ้งเตือนเมื่อกฎสามารถตรวจจับแพ็คเก็จจากโปรโตคอล ICMP ที่เกิดจากการใช้คำสั่ง Ping (ICMP ECHO REQUEST) ที่มีค่า TTL (Time to Live) เท่ากับ 100

กฎของโปรแกรมสนอร์ต จะทำการตรวจสอบในส่วนของ Rule Header (ข้อมูลที่อยู่ภายนอกวงเล็บ) ก่อนที่จะทำการตรวจสอบ Rule Option (ข้อความที่อยู่ในวงเล็บ) ข้อมูลในส่วนของ Rule Header ประกอบด้วยข้อมูลดังต่อไปนี้

- ฟิลด์การกระทำ จากกฎตัวอย่างค่าในฟิลด์การกระทำถูกกำหนดไว้เป็น "Alert" ซึ่งหมายความว่า การแจ้งเตือนจะถูกสร้างขึ้นเมื่อรูปแบบของแพ็คเก็จตรงตามเงื่อนไขที่กฎกำหนด การทำงานของฟิลด์การกระทำ ยังขึ้นอยู่กับการกำหนดกฎในส่วนของ Rule Option ด้วย
- ฟิลด์โปรโตคอล โปรโคตอลที่ใช้คือโปรโตคอล ICMP หมายความว่ากฎของโปรแกรมสนอร์ตจะทำการตรวจสอบเฉพาะแพ็คเก็จที่เป็นโปรโคตอล ICMP เท่านั้น ในส่วนของ Detection Engine ของโปรแกรมสนอร์ต เมื่อแพ็คเก็จที่ส่งเข้ามาไม่ใช้โปรโคคอล ICMP กฎก็จะไม่ทำการตรวจสอบต่อเพื่อลดการทำงานของ CPU
- ฟิลด์ที่อยู่และฟิลด์พอร์ตต้นทางได้ถูกกำหนดเป็น "any" หมายความว่า กฎจะทำการตรวจสอบทุกแพ็คเก็จที่เข้ามาในระบบเครือข่ายฟิลด์พอร์ตจะถูกนำมาใช้งานร่วมกับโปรโตคอล TCP และ UDP เท่านั้น
- ฟิลด์ทิศทางจากกฎตัวอย่างฟิลด์ทิศทางได้ถูกกำหนดค่าด้วยสัญลักษณ์ "->" แสดงว่าด้านซ้ายเป็นที่อยู่ไอพีและพอร์ตต้นทาง ด้านขวาเป็นที่อยู่ไอพีและพอร์ตปลายทาง

ผู้ใช้งานสามารถใช้สัญลักษณ์ "<-"ในฟิลด์ทิศทางได้ ซึ่งจะหมายความว่าด้านขวาเป็นที่อยู่ไอพีและพอร์ตต้นทาง ด้านซ้ายเป็นที่อยู่ไอพีและพอร์ตปลายทาง

- ฟิลด์ที่อยู่และฟิลด์พอร์ตต้นทางและปลายทาง จากกฎตัวอย่างได้ถูกกำหนดให้เป็น "Any" หมายความว่ากฎของโปรแกรมสนอร์ตจะตรวจสอบทุกแพ็คเก็จที่ผ่านเข้ามาในระบบเครือข่าย
- Rule Option จะประกอบไปด้วยข้อความที่อยู่ในวงเล็บ จากกฎตัวอย่างโปรแกรม – สนอร์ตจะสร้างการแจ้งเตือนเมื่อแพ็คเก็จมีค่า TTL = 100 และจะส่งข้อความ "Ping with TTL = 100" ไปยังผู้ดูแลระบบเครือข่าย

2.3.1 Rule Header

Rule Header จะทำหน้าที่ตรวจสอบแพ็คเก็จเป็นอันดับแรก ถ้ารูปแบบของแพ็คเก็จที่ผ่านเข้ามาตรงกับเงื่อนไขที่กำหนดไว้ใน Rule Header แพ็คเก็จจะถูกตรวจสอบในส่วนของ Rule Option ต่อไป Rule Header ประกอบด้วยส่วนต่าง ๆ ดังต่อไปนี้

- Rule Action

เป็นส่วนประกอบส่วนแรกของ Rule Header โดย Rule Action จะเป็นส่วนที่กำหนดพฤติกรรมของกฎเมื่อแพ็คเก็จที่เข้ามาตรงตามเงื่อนไขของกฎ การกำหนดค่า Rule Action สามารถกำหนดได้ 5 แบบ การกำหนดค่า Rule Action ของโปรแกรมสนอร์ตในเวอร์ชั่น 1.X และ 2.X นั้นจะมีความแตกต่างกันโดยโปรแกรมสนอร์ตเวอร์ชั่น 1.X ถ้าแพ็คเก็จที่เข้ามาตรงตามเงื่อนไขของกฎมากกว่าหนึ่งกฎ กฎแรก (กฎที่อยู่บนสุด) เท่านั้นที่จะนำไปใช้ในการตรวจสอบแพ็คเก็จโดยไม่สนใจกฎที่เหลือ สำหรับโปรแกรมสนอร์ตเวอร์ชั่น 2.X หากแพ็คเก็จที่เข้ามาตรงกับเงื่อนไขของกฎมากกว่าหนึ่งกฎ แพ็คเก็จจะถูกตรวจสอบด้วยกฎทุกกฎ และกฎที่มีความสำคัญมากที่สุด (Priority) จะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย

การกำหนดค่าทั้ง 5 แบบให้กับ Rule Action สามารถกำหนดได้ดังต่อไปนี้

- **Pass** เป็นการกำหนดให้โปรแกรมสนอร์ตไม่ต้องทำการตรวจสอบแพ็คเก็จที่เข้ามาในระบบเครือข่าย การกำหนดค่าของ Rule Action เป็น Pass นั้นจะทำให้โปรแกรมสนอร์ตทำงานได้เร็วขึ้น

- Log ใช้ในการเก็บประวัติของแพ็คเก็จ การเก็บประวัติของแพ็คเก็จสามารถเก็บได้หลายวิธีเช่น การจัดเก็บข้อความการแจ้งเตือนที่เกิดขึ้นในรูปแบบของไฟล์ประวัติ (Log File) หรือจัดเก็บลงในฐานข้อมูล

- Alert โปรแกรมสนอร์ตสร้างการแจ้งเตือนเมื่อแพ็คเก็จที่เข้ามานั้นตรงตามเงื่อนไขของกฎ การแจ้งเตือนสามารถทำได้หลายวิธีตัวอย่างเช่น ผู้ดูแลระบบสามารถส่งการแจ้งเตือนไปยังคอนโซล (Console) ที่ต้องการ ข้อแตกต่างระหว่างการกำหนดค่า Rule Action เป็น Log และ

Alert คือ Alert จะสร้างการแจ้งเตือน และเก็บประวัติของแพ็คเก็จ แต่ Log จะเก็บประวัติของแพ็คเก็จเพียงอย่างเดียว

- Activate จะถูกใช้ในการสร้างการแจ้งเตือน และกระตุ้นให้กฎที่กำหนดค่า Rule Action เป็น Dynamic ทำงาน การกำหนด Rule Action เป็น Activate จะถูกนำมาใช้เมื่อผู้ดูแลระบบเครือข่ายต้องการทดสอบแพ็คเก็จที่เข้ามาในระบบเครือข่าย

- Dynamic กฎที่ถูกกำหนดค่า Rule Action เป็น Dynamic จะสามารถทำงานต่อเมื่อถูกกระตุ้นด้วยกฎที่กำหนดค่า Rule Action เป็น Activate เท่านั้น

- Protocols

ฟิลด์โปรโตคอลใช้แสดงประเภทของแพ็คเก็จที่กฎทำการตรวจสอบ โดยโปรโตคอลที่โปรแกรมสนอร์ตสามารถตรวจสอบได้มีดังต่อไปนี้

- IP
- ICMP
- TCP
- UDP

นอกจากโปรโตคอลจะถูกใช้กำหนดเงื่อนไขในการตรวจสอบแพ็คเก็จในส่วนของ Rule Header แล้วโปรโตคอลยังถูกนำมากำหนดเงื่อนไขเพื่อใช้ในการตรวจสอบแพ็คเก็จในส่วนของ Rule Option อีกด้วย

```
alert icmp any any -> any any (msg: "Ping with TTL=100"; \
ttl: 100;)
```

รูปที่ 2.7 ตัวอย่างการกำหนดกฎให้มีการตรวจสอบค่า TTL ใน Rule Option

รูปที่ 2.7 ในส่วนของ Rule Option ได้กำหนดให้มีการตรวจสอบค่า TTL ซึ่งค่า TTL ไม่ได้เป็นส่วนประกอบในส่วนหัวของโปรโตคอล ICMP แต่ค่า TTL นั้นเป็นส่วนประกอบในส่วนหัวของโปรโตคอล IP หมายความว่าผู้ใช้งานสามารถกำหนดค่า Rule Option ให้สามารถตรวจสอบโปรโตคอลอื่นนอกเหนือจากโปรโตคอลใน Rule Header ได้

- Address

ฟิลด์ที่อยู่ใช้ในการตรวจสอบที่มาและปลายทางของแพ็คเก็จ การกำหนดค่าให้กับฟิลด์ที่อยู่จะกำหนดเพียงที่อยู่เดียว หรือกำหนดพร้อมกันหลายที่อยู่ก็ได้ ค่าในฟิลด์ที่อยู่จะเป็นที่อยู่ไอพีที่ใช้งานจริงในระบบเครือข่าย และจะตามด้วยเครื่องหมาย "/" เพื่อกำหนดจำนวนบิตของเน็ตมาร์ซ (netmark) ตัวอย่าง 192.168.2.0/24 แสดงการกำหนดที่อยู่ไอพีในคลาส C เน็ตเวิร์ค 192.168.2.0 มีจำนวนเน็ตมาร์ซ 24 บิตคือ 255.255.255.0

ผู้ใช้งานสามารถกำหนดจำนวนบิตของเน็ตมาร์ซได้ตามข้อกำหนดที่กำหนดของ Classless Inter-Domain Routing or CIDR โดยอ้างอิงจาก RFC 791 http://www.rfc.editor.org/rfc/rfc791.text โครงสร้างของที่อยู่ไอพีและเน็ตมาร์ซสามารถตรวจสอบได้จาก RFC 1519 ที่ http://www.rfc.editor.org/rfc/rfc1519.txt การกำหนดที่อยู่ไอพีในฟิลด์ที่อยู่ที่ผู้ใช้งานควรทราบมีรายละเอียดดังต่อไปนี้

ที่อยู่ 192.168.1.3/32 เป็นการกำหนดที่อยู่ไอพีให้กับโฮสต์เพียงโฮสต์เดียวที่ที่อยู่ไอพีคือ 192.168.1.3

ที่อยู่ 192.168.1.0/24 เป็นการกำหนดที่อยู่ไอพีในคลาส C ของระบบเครือข่ายที่มีที่อยู่ไอพีตั้งแต่ 192.168.1.0 ถึง 192.168.1.255 และมีเน็ตมาร์ซจำนวน 24 บิตคือ 255.255.255.0

ที่อยู่ 152.168.0.0/16 เป็นการกำหนดที่อยู่ไอพีในคลาส B ของระบบเครือข่ายที่มีที่อยู่ไอพีตั้งแต่ 152.168.0.0 ถึง 152.168.255.255 และมีเน็ตมาร์ซจำนวน16 บิตคือ 255.255.0.0

ที่อยู่ 10.0.0.0/8 เป็นการกำหนดที่อยู่ไอพีในคลาส A ของระบบเครือข่ายที่มีที่อยู่ไอพีตั้งแต่ 10.0.0.0 ถึง 10.255.255.255 และมีเน็ตมาร์ซจำนวน 8 บิตคือ 255.0.0.0

ที่อยู่ 192.168.1.16/28 เป็นการกำหนดที่อยู่ไอพีตั้งแต่ 192.168.1.16 ถึง 192.168.1.31 ซึ่งเน็ตมาร์ซจำนวน 28 บิตคือ 255.255.255.240 ประกอบไปด้วยที่อยู่ไอพีจำนวน 16 ไอพีแต่สามารถใช้งานได้เพียง 14 ไอพีเพราะว่า 2 ไอพีจะถูกกำหนดเป็น Network Address และ Broadcast Address ที่อยู่ไอพีแรกจะถูกกำหนดเป็น Network Address ในระบบเครือข่าย และที่อยู่ไอพีสุดท้ายของระบบเครือข่ายจะถูกกำหนดให้เป็น Broadcast Address สำหรับที่อยู่ไอพีที่ยกตัวอย่างมาที่อยู่ไอพี 192.168.1.16 เป็น Network Address และที่อยู่ไอพี 192.168.1.31 เป็น Broadcast Address

ตัวอย่างกำหนดกฎเพื่อสร้างการแจ้งเตือนของโปรโตคอล TCP ที่มีค่า TTL = 100 ที่เข้ามาเครื่องที่ให้เว็บเซริฟเวอร์ที่มีที่อยู่ไอพี192.168.1.10 และเลขพอร์ต 80 จากทุกๆ ที่อยู่ไอพีบนระบบเครือข่าย

```
alert tcp any any -> 192.168.1.10/32 80 (msg : "TTL=100"; \
ttl : 100;)
```

รูปที่ 2.8 ตัวอย่างการกำหนดกฎให้สร้างการแจ้งเตือนโปรโตคอล TCP ที่มีค่า TTL = 100

การกำหนดค่าที่อยู่ไอพีในฟิลด์ที่อยู่ต้นทาง และฟิลด์ที่อยู่ปลายทางสามารถกำหนดได้หลายรูปแบบ เช่น การกำหนดที่อยู่หลายระบบเครือข่ายภายในกฎเดียว หรือการกำหนดให้กฎไม่ต้องตรวจสอบที่อยู่ไอพีที่กำหนด

การกำหนดกฎเพื่อละเว้นการตรวจสอบที่อยู่ไอพีที่กำหนด (Address Exclusion) จะใช้เครื่องหมาย "!" ตัวอย่างการกำหนดกฎเพื่อละเว้นการตรวจสอบแพ็คเก็จที่มาจากคลาส C ของระบบเครือข่าย 192.168.2.0

```
alert icmp ![192.168.2.0/24] any -> any any \
(msg : "Ping with TTL = 100"; ttl: 100;)
```

รูปที่ 2.9 ตัวอย่างการกำหนดกฎเพื่อละเว้นการตรวจสอบที่อยู่ไอพีที่กำหนด

การกำหนดกฎเพื่อตรวจสอบหลายระบบเครือข่ายพร้อมกัน(Address Lists) จะใช้เครื่องหมาย "," เป็นตัวคั้นแต่ละระบบเครือข่ายตัวอย่าง ผู้ใช้งานมีระบบเครือข่ายภายในอยู่ 2 ระบบเครือข่ายซึ่งอยู่ในคลาส C คือ 192.168.2.0 และ 192.168.8.0 โดยผู้ใช้งานต้องการตรวจสอบทุกแพ็คเก็จยกเว้นจาก 2 เครือข่ายข้างต้น

```
alert icmp ![192.168.2.0/24, 192.168.8.0/24] any -> any \
any (msg: "Ping with TTL=100"; ttl: 100;)
```

รูปที่ 2.10 ตัวอย่างการกำหนดกฎเพื่อตรวจสอบระบบเครือข่ายหลายระบบเครือข่ายพร้อมกัน

- Port Number

เลขพอร์ตจะถูกนำมาตรวจสอบพอร์ตที่มาของแพ็คเก็จ หรือพอร์ตปลายทางของแพ็คเก็จ ตัวอย่าง ผู้ใช้งานกำหนดเลขพอร์ต 23 เป็นพอร์ตต้นทางเพื่อทำการตรวจสอบแพ็คเก็จที่มาจากเครื่องแม่ข่ายที่ให้บริการ Telnet (Telnet Server) โดยใช้คีย์เวิร์ด *any* การกำหนดเลขพอร์ตให้กับกฎของโปรแกรมสนอร์ตจะเป็นการกำหนดกฎเพื่อใช้ในการตรวจสอบโปรโตคอล TCP และ UDP เท่านั้น ตัวอย่างการกำหนดกฎเพื่อทำการตรวจสอบแพ็คเก็จที่มีข้อความ "confidential" ที่มาจากเครื่องให้บริการ Telnet มีและที่อยู่ 192.168.2.0/24 ในคลาส C

```
alert tcp 192.168.2.0/24 23 -> any any \
(content: "confidential"; msg: "Detected confidential")
```

รูปที่ 2.11 ตัวอย่างการกำหนดกฎเพื่อตรวจหาข้อความ "confidential" ในแพ็คเก็จ

ผู้ใช้งานสามารถกำหนดกฎให้ทำงานเหมือนกับกฎในรูปที่ 2.1 ได้โดยการแก้ไขในส่วนของ ฟิลด์ทิศทางซึ่งแสดงในรูปที่ 2.12

```
Alert tcp 192.168.2.0/24 23 <> any any \
(content: "confidential"; msg: "Detected confidential")
```

รูปที่ 2.12 ตัวอย่างการกำหนดกฎเพื่อตรวจหาข้อความ "confidential" ในแพ็คเก็จ

การกำหนดเลขพอร์ตให้กับกฎของโปรแกรมสนอร์ตสามารถกำหนดได้หลายรูปแบบ เช่น การกำหนดเป็นช่วงของเลขพอร์ต หรือกำหนดเลขพอร์ตที่ไม่ต้องการตรวจสอบ

การกำหนดเป็นช่วงของเลขที่พอร์ต (Port Rangs) จะใช้เครื่องหมาย (:) ในการแยกเลขพอร์ตแรกและเลขพอร์ตสุดท้ายออกจากกัน ตัวอย่างกำหนดกฎเพื่อสร้างการแจ้งเตือนแพ็คเก็จที่เป็นโปรโตคอล UDP และมาจากพอร์ต 1024 ถึง 2048 จากทุกโฮสต์บนระบบเครือข่าย

```
alert udp any 1024:2048 -> any any (msg: "UDP ports";)
```

รูปที่ 2.13 ตัวอย่างการกำหนดกฎโดยใช่ช่วงของเลขที่พอร์ต

การยกเว้นตรวจสอบเลขพอร์ตที่กำหนด (Negation Symbol) จะคล้ายกับการกำหนดในฟิลด์ที่อยู่ ตัวอย่าง การเก็บประวัติของทุกแพ็คเก็จที่เข้ามายกเว้นแพ็คเก็จที่มาจากพอร์ต 53

```
log udp any !53 -> any any log udp
```

รูปที่ 2.14 ตัวอย่างการกำหนดกฎเพื่อยกเว้นการเก็บประวัติพอร์ตที่กำหนด

เลขพอร์ตที่ผู้ใช้งานควรทราบแสดงในตารางที่ 2.1

ตารางที่ 2.1 เลขพอร์ตที่นำมาใช้งานร่วมกับโปรแกรมต่างๆ ที่ใช้งานบนระบบเครือข่าย

เลขพอร์ต	คำอธิบาย
20	ส่งข้อมูล FTP
21	FTP
22	SSH หรือ Secure Shell
23	Telnet
25	SMTP ใช้สำหรับ เครื่องให้บริการ E-Mail (Mail Server) คล้ายกับ Sendmail
37	NTP(Network Time Protocol) ใช้สำหรับซิงโครไนซ์เวลาของโฮสในระบบเครือข่าย
53	DNS Server
67	BootP/DHCP Client

68	BootP/DHCP Server
69	TFTP
80	HTTP ใช้สำหรับเครื่องให้บริการเว็บไซต์ (Web Server)
110	POP3 ใช้สำหรับใช้งาน mail เครื่องลูกข่าย คล้ายกับ Microsoft Outlook
161	SNMP
162	SNMP traps
443	HTTPS หรือ Secure HTTP
514	Syslog
3306	MySQL

ผู้ใช้งานสามารถดูข้อมูลของเลขที่พอร์ตที่ใช้งานได้จากไฟล์ /etc/service ในระบบปฏิบัติการยูนิตซึ่งอ้างอิงมาจาก RFC 1700 หากต้องการทราบรายละเอียดมากขึ้น สามารถตรวจสอบได้ที่ http://www.icann.org

- Direction

ฟิลด์ทิศทางจะใช้ในการกำหนดที่มาและปลายทางของแพ็คเก็จในฟิลด์ที่อยู่และฟิลด์พอร์ต การกำหนดค่าฟิลด์ทิศทางสามารถกำหนดได้ดังต่อไปนี้

สัญลักษณ์ "->" แสดงว่าที่อยู่และเลขพอร์ตที่อยู่ทางซ้ายมือของฟิลด์ทิศทางเป็นที่มาของแพ็คเก็จ และในส่วนขวามือของฟิลด์ทิศทางเป็นปลายทางของแพ็คเก็จ

สัญลักษณ์ "<-" แสดงว่าที่อยู่และพอร์ตที่อยู่ทางขวามือของฟิลด์ทิศทางเป็นที่มาของแพ็คเก็จ และในส่วนซ้ายมือของฟิลด์ทิศทางนั้นเป็นปลายทางของแพ็คเก็จ

สัญลักษณ์ "<>" แสดงว่ากฎจะทำการตรวจสอบทุกแพ็คเก็จที่เข้ามาและทุกแพ็คเก็จที่โฮสต์ส่งออกไป สัญลักษณ์ดังกล่าวจะเป็นประโยชน์เมื่อต้องการตรวจสอบแพ็คเก็จที่โฮสต์ได้รับและส่งออก

2.3.2 Rule Option

Rule Option จะอยู่ต่อจาก Rule Header ซึ่งอยู่ภายในเครื่องหมายวงเล็บการกำหนดเงื่อนไขใน Rule Option อาจกำหนดเพียงเงื่อนไขเดียวหรือหลายเงื่อนไข โดยแต่ละเงื่อนไขจะถูกแบ่งออกจากกันด้วยเครื่องหมาย (;) เงื่อนไขใน Rule Option จะประกอบไปด้วยส่วนที่เป็น คีย์เวิร์ด (Keyword) และอากิวเม็นท์ (Argument) ทั้งสองส่วนจะแยกออกจากกันด้วยเครื่องหมาย (:) แสดงในรูปที่ 2.15

msg: "Detected confidential"

รูปที่ 2.15 ตัวอย่างการกำหนดเงื่อนไขในส่วนของ Rule Option

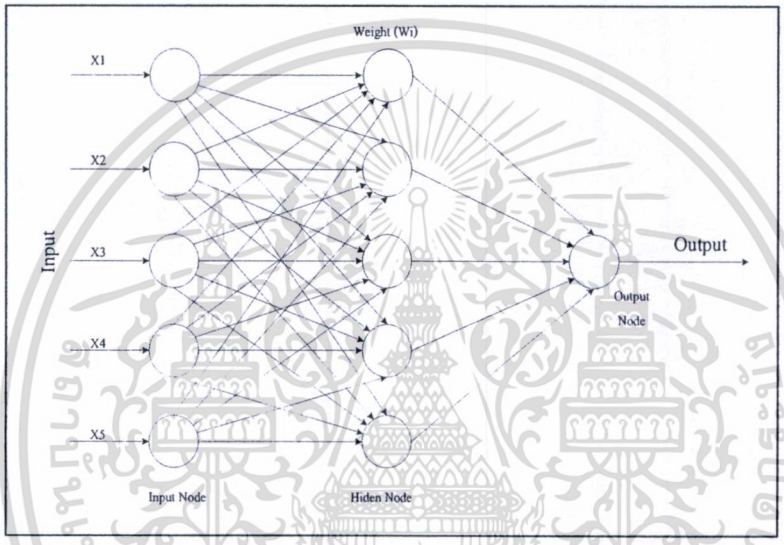
จากรูปที่ 2.15 "msg" เป็นคีย์เวิร์ดและ "Detected confidential" จะเป็นอากิวเม็นท์ของคีย์เวิร์ด "msg" การกำหนดคีย์เวิร์ด Rule Option ได้ถูกอธิบายไว้ใน ภาคผนวก ก

2.4 ระบบเครือข่ายใยประสาท (Neural Network) [9], [10] และ [24]

เครือข่ายใยประสาท (Neural Network) เป็นแบบจำลองสถาปัตยกรรมคอมพิวเตอร์ ที่พัฒนาขึ้นบนพื้นฐานการสังเกตพฤติกรรมทางชีวภาพของเซลล์ประสาทภายในสมองมนุษย์ โดยเชื่อมกระบวนการทำงานต่าง ๆ เข้าด้วยกันเพื่อให้สามารถประมวลผลข้อมูลโดยพร้อมเพียงกัน ระบบเครือข่ายใยประสาทจะมีการเลียนแบบความสามารถของสมอง เพื่อเพิ่มประสิทธิภาพให้กับการทำงานของระบบให้มีความสามารถในการเรียนรู้จากกลุ่มข้อมูลภายนอก ระบบเครือข่ายใยประสาทจะเรียนรู้จากการทดลองและข้อผิดพลาด ซึ่งส่วนมากแล้วเครือข่ายใยประสาทจะเป็นซอฟต์แวร์ซิมมูเลชั่น (software simulation) ที่ทำงานบนเครื่องคอมพิวเตอร์ ระบบเครือข่ายใยประสาทจะประกอบด้วยวงจรทรานซิสเตอร์ (transistor circuit) ทำหน้าที่เป็นเซลล์ประสาท (neural) และตัวต้านทานผันแปร (variable resistor) ทำการเชื่อมต่อเส้นประสาท (axons) เข้ากับปลายประสาท (dendrites) ซึ่งในแผงวงจรรวม (integrate circuit) ของเครือข่ายระบบประสาทจะประกอบด้วย 1,024 ซิลิกอน (silicon) รวมกันเป็นเซลล์ประสาทแต่ละเซลล์ประสาทในเครือข่ายจะมีข้อมูลนำเข้าเดียวหรือมากกว่า โดยระบบเครือข่ายใยประสาทจะรับข้อมูลนำเข้าเข้าไปคำนวณหาผลลัพธ์ออกมาซึ่งข้อมูลนำเข้าแต่ละตัวจะถูกให้ลำดับความสำคัญแตกต่างกัน ขณะป้อนข้อมูลน้ำเข้าแต่ละตัวเข้าสู่เซลล์ประสาทข้อมูลน้ำเข้านั้นจะถูกปรับค่าน้ำหนัก (weight) โดยเซลล์ประสาทจะทำการคำนวณค่าข้อมูลนำเข้า และนำผลลัพธ์ที่ได้ไปเปรียบเทียบกับผลลัพธ์ที่ได้ตั้งไว้ ถ้าค่าที่ออกมาเกิดความคลาดเคลื่อนก็จะนำไปสู่การปรับค่าน้ำหนักที่กำหนดไว้ในข้อมูลนำเข้าอีกครั้ง ซึ่งผลลัพธ์จากเซลล์ประสาทหนึ่งจะกลายมาเป็นผลลัพธ์ของเซลล์ประสาทตัวอื่นจนกระทั่งผลลัพธ์สุดท้ายนั้นมีค่าความคลาดเคลื่อนน้อยที่สุด

ระบบเครือข่ายใยประสาทโดยส่วนมากจะถูกนำไปใช้ในการพัฒนาซอฟต์แวร์ แต่ถ้าหากนำไปใช้กับคอมพิวเตอร์ฮาร์ดแวร์จะเรียกว่า "คอมพิวเตอร์เครือข่ายใยประสาท (neural computer)" จากรายละเอียดข้างต้นของคอมพิวเตอร์เครือข่ายใยประสาทนั้นจะเป็นการเชื่อมต่อโปรเซสเซอร์ (processor) หลายตัวเข้าด้วยกัน (multi-processor) ในหนึ่งเครื่องให้เครื่องประมวลผลเป็นแบบคู่ขนาน (parallel processing) และมีความสามารถในการจัดเก็บสิ่งที่รับรู้ ประสบการณ์และการกระทำ โดยจะมีลักษณะคล้ายการทำงานของสมองอยู่สองประการ

ประการแรกเป็นการรับรู้ของระบบบบ จะผ่านทางกระบวนการเรียนรู้ของเครื่อง (learning machine) ประการที่สองคือเซลล์ที่เชื่อมต่อถึงกัน (synapse) ถูกใช้ในการเก็บสิ่งที่รับรู้เข้ามา มนุษย์สามารถป้อนองค์ความรู้ไว้ในฮาร์ดแวร์ เพื่อให้ฮาร์ดแวร์ใช้ในการเรียนรู้และสร้างกลุ่มคำตอบได้ด้วยตนเองโดยปราศจากคนสอน คอมพิวเตอร์เครือข่ายใยประสาทจะมีความฉลาดในการเรียนรู้จากข้อมูลที่ไม่สมบูรณ์แล้วสามารถวิเคราะห์หาคำตอบได้ด้วยตนเอง แต่ก็ไม่ง่ายนักในการพัฒนาระบบเครื่องคอมพิวเตอร์ให้กลายเป็นคอมพิวเตอร์เครือข่ายใยประสาท เนื่องจากต้องใช้อุปกรณ์ต่าง ๆ ภายในตัวเครื่องจำนวนมากไม่ว่าจะเป็นจำนวนโปรเซสเซอร์ (processor) หรือหน่วยความจำ (memory) ที่ต้องการความจุที่มาก



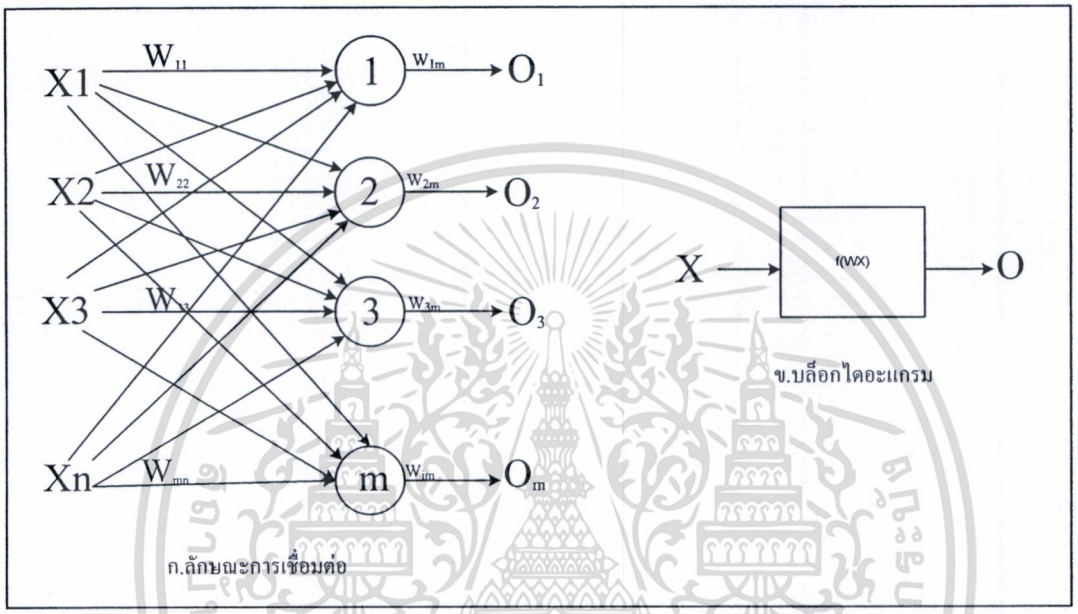
รูปที่ 2.16 โครงสร้างการทำงานของระบบเครือข่ายใยประสาท

ระบบเครือข่ายระบบประสาทมีโครงสร้างหลักประกอบด้วย 3 ส่วน ได้แก่ 1) weight (Wi) ทำหน้าที่ในการรับข้อมูลที่ถูกป้อนเข้ามาจาก input node จากนั้นป้อนเข้าไปให้กับ node 2) node เป็นการนำ processor หลายตัวมาเชื่อมต่อกันทำให้สามารถรับข้อมูลพร้อมกันได้โดย node จะจำแนกออกเป็น 3 กลุ่ม ได้แก่ input node จะรับข้อมูลจากภายนอก hidden node รับข้อมูลจากสิ่งที่รับรู้หรือจากเครือข่ายภายใน และ output node จะปรับผลลัพธ์ให้มีค่าความผิดพลาดน้อยที่สุดก่อนนำออกแสดงผลโดย node ทำหน้าที่ในการรวบรวมข้อมูลหรือจัดเก็บข้อมูลที่ถูกป้อนเข้ามา คำนวณและประมวลผลเสร็จแล้วส่งผลลัพธ์นั้นไปยัง hidden node 3) hidden node ทำหน้าที่แปลงข้อมูลที่ได้จากการประมวลผลและส่งไปที่ output node เพื่อให้ output node ปรับค่าความผิดพลาดและแสดงเป็นผลลัพธ์ตามต้องการ

2.4.1 ระบบเครือข่ายใยประสาทที่ส่งสัญญาณไปข้างหน้า (Feedforward Networks)

ระบบเครือข่ายใยประสาทที่ส่งสัญญาณไปข้างหน้าจะประกอบไปด้วยชั้นต่างๆ ของโครงข่ายโดยชั้นแรกจะเป็นข้อมูลนำเข้าและชั้นสุดท้ายจะเป็นผลลัพธ์ ส่วนระหว่างชั้นข้อมูลนำเข้า และผลลัพธ์จะมีหรือไม่มีชั้นแทรกอยู่ภายในก็ได้ขึ้นอยู่กับอัลกอลิทึมที่ใช้ในการสอน

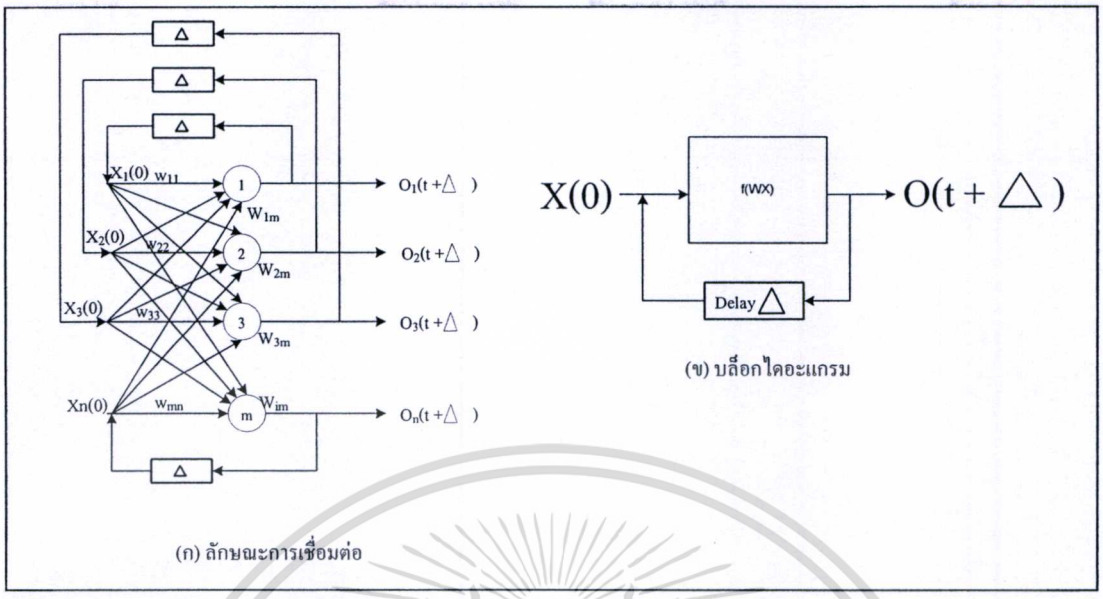
โครงข่ายใยประสาท เช่น ถ้าเป็นโครงข่ายเพอเซฟตรอนแบบหลายชั้น (Multilayer Perceotron) ก็จะมีชั้นที่อยู่ระหว่างข้อมูลนำเข้าและผลลัพธ์อีกซึ่งจะมากกว่าหนึ่งชั้นก็ได้ส่วน โครงข่ายเซลล์-ออแกไนซิงแมพ (Self-Organizing Map) ของโคโฮเคน (Kohoken) จะมีเพียงชั้นข้อมูลนำเข้ากับชั้นที่เป็นผลลัพธ์เท่านั้น การเชื่อมต่อระหว่างชั้นของโครงข่ายแบบโครงข่ายที่ส่งสัญญาณไปข้างหน้า จะมีค่าน้ำหนักเป็นตัวเชื่อม และสัญญาณนำเข้าที่เข้ามาจะถูกส่งไปตามทิศทางของลูกศรจนถึงชั้นที่เป็นผลลัพธ์โดยไม่มีการป้อนกลับ



รูปที่ 2.17 ระบบเครือข่ายใยประสาท Feedforward แบบชั้นเดียว (ก) ลักษณะการเชื่อมต่อ (ข) บล็อกไดอะแกรม

2.4.2 ระบบเครือข่ายใยประสาทที่มีการป้อนกลับ (Feedback Networks)

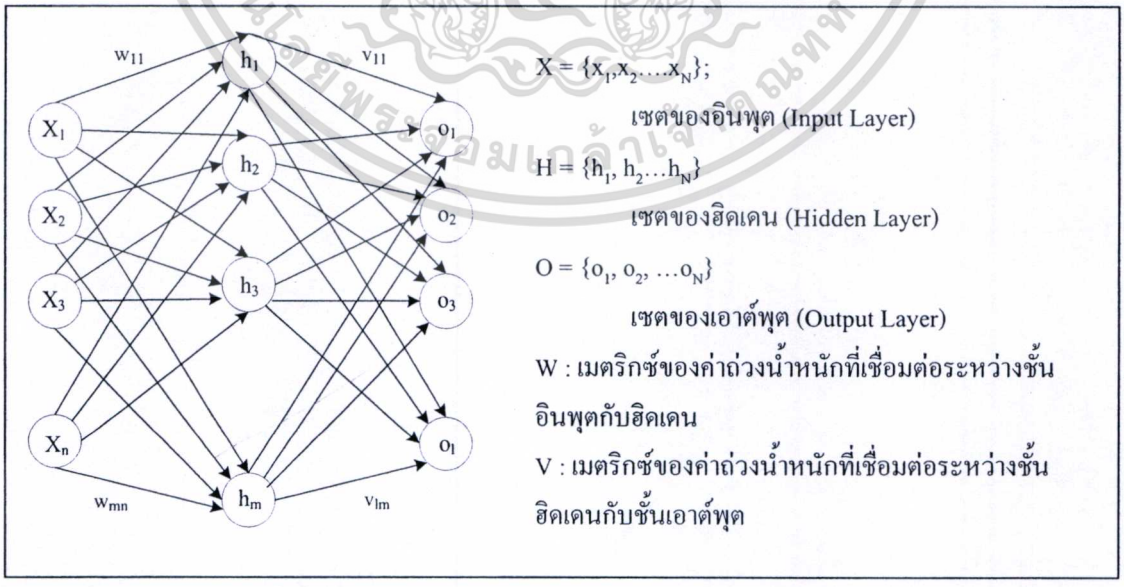
ในส่วนแรกของโครงข่ายใยประสาทจะเหมือนกับโครงข่ายที่ส่งสัญญาณไปข้างหน้า แต่มีส่วนที่เพิ่มขึ้นมาคือส่วนการป้อนกลับแสดงในรูปที่ 2.18 และการป้อนกลับจะมีหน่วงเวลาไปจากเวลาเดิม ซึ่งโครงข่ายใยประสาทในรูปที่ 2.18 จะเรียกกว่า รีเคอร์เรนท์ (Recurrent Networks)



2.18 ระบบเครือข่ายใยประสาทที่มีการป้อนกลับแบบไม่ต่อเนื่องชั้นเดียว (ก) ลักษณะการเชื่อมต่อ (ข) บล็อกไดอะแกรม

2.4.3 ระบบเครือข่ายใยประสาทแบบการแพร่กระจายกลับ (Back-propagation)

การแพร่กระจายกลับหรือแบ็คพร็อพพาเกชัน เป็นขั้นตอนที่ใช้ในการสอนระบบเครือข่ายใยประสาทแบบเพอเซฟตรอนแบบหลายชั้นซึ่งเป็นแบบจำลองโครงข่ายเซลล์ประสาทที่มีการเชื่อมโยงกันเป็นโครงข่ายแบบเป็นชั้น ๆ ดังรูปที่ 2.19



รูปที่ 2.19 โครงข่าย Multilayer Perception ที่มี 3 ชั้น

ซึ่งโครงข่ายที่มีการเชื่อมต่อกัน 3 ชั้น จะประกอบไปด้วยชั้นอินพุตซึ่งมีเซลล์ประสาทอยู่ N โหนดถัดมาเป็นชั้นของฮิดเดนหรือชั้นภายใน (Hidden Layer) ซึ่งประกอบไปด้วยโหนด (node) ต่าง ๆจำนวน M โหนด และชั้นสุดท้ายคือชั้นของเอาต์พุตซึ่งมีโหนดต่างๆ อยู่ L โหนด ระบบเครือข่ายใยประสาทแบบ Multilayer Perception ในรูปที่ 2.19 แต่ละโหนดในชั้นเดียวกันจะไม่มีการเชื่อมต่อกัน การเชื่อมโยงกันจะมีเฉพาะระหว่างชั้นเท่านั้น และการเชื่อมโยงนี้จะต่อถึงกันทุกโหนดโครงข่ายแบบ Multilayer Perception ไม่จำเป็นต้องมี 3 ชั้น อาจจะมี 4 ชั้น ก็ได้โดยการเพิ่มฮิดเดนเลเยอร์เข้าอีกชั้นก็ได้ หรือถ้าต้องการมากกว่านั้นก็สามารถทำได้โดยการเพิ่มฮิด-เดนเลเยอร์

ชั้นฮิดเดนเลเยอร์เป็นตัวเพิ่มความสามารถให้กับระบบเครือข่ายใยประสาทที่โครงข่ายเป็นแบบเพอเซฟตรอนแบบหลายชั้นถ้าไม่มีชั้นฮิดเดนเลเยอร์ก็จะกลายเป็นโครงข่ายแบบเพอ-เซฟตรอน

2.5 งานวิจัยที่เกี่ยวข้อง

การแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นจากระบบตรวจจับการบุกรุกบนระบบเครือข่ายได้สร้างปัญหาให้กับผู้ดูแลระบบเครือข่ายเป็นอย่างยิ่ง จึงได้มีผู้นำเสนอวิธีการลดการแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นด้วยวิธีที่แตกต่างกันออกไป โดยผู้วิจัยได้จำแนกวิธีลดการแจ้งเตือนที่ผิดพลาดของระบบตรวจจับการบุกกรุกบนระบบเครือข่ายไว้ 4 รูปแบบดังนี้

2.5.1 การวิเคราะห์ค่าทางสถิติ (Statistics) [8] และ [11]

เป็นวิธีที่ถูกนำมาใช้อย่างกว้างขวางโดยจะกำหนดพฤติกรรมปรกติที่เกิดขึ้นบนระบบเครือข่าย ซึ่งพฤติกรรมปรกติบนระบบเครือข่ายได้มาจากการจัดเก็บพฤติกรรมการใช้งานที่ไม่เป็นอันตรายต่อระบบเครือข่ายที่เกิดขึ้นจากผู้ใช้งาน และสภาพแวดล้อมภายในระบบเครือข่าย ตัวอย่างระบบตรวจจับการบุกรุกระบบเครือข่ายที่ใช้การวิเคราะห์ค่าทางสถิติในการทำงานคือ NIDES (Next – generation Intrusion Detection Expert System) การทำงานของ NIDES จะมีการทำงานอยู่สองแบบด้วยกันคือ การตรวจจับการบุกรุกบนระบบเครือข่ายในช่วงระยะเวลาสั้นๆ และการตรวจจับการบุกรุกบนระบบเครือข่ายในช่วงระยะเวลาที่นานขึ้น ผลลัพธ์ที่ได้จากการทำงานของ NIDES จะมีขนาดใหญ่ซึ่งเป็นผลมาจากที่ NIDES ต้องตรวจสอบทุกแพ็คเก็จที่ผ่านเข้ามาในระบบเครือข่ายแล้วนำมาเปรียบเทียบกับแพ็คเก็จต้นแบบ ข้อเสียในการใช้ค่าทางสถิติในระบบตรวจจับการบุกรุกบนระบบเครือข่ายคือจะทำงานได้ช้า และจะไม่สามารถตรวจจับการบุกรุกระบบเครือข่ายรูปแบบใหม่ได้ถ้าหากไม่มีการปรับปรุงชุดแพ็คเก็จต้นแบบอย่างสม่ำเสมอ

2.5.2 การเรียนรู้พฤติกรรม [8], [11] และ [12]

เป็นรูปแบบลดการแจ้งเตือนที่ผิดพลาดที่ทำงานโดยอัตโนมัติ ระบบจะมีการสร้างชุดของข้อมูลต้นแบบ (Training data sets) เพื่อกำหนดรูปแบบของพฤติกรรมปรกติบนระบบเครือข่าย ชุดข้อมูลต้นแบบจะใช้ในการตรวจสอบกิจกรรมที่เกิดขึ้นในระบบเครือข่าย หากมีกิจกรรมใดตรงกับชุดข้อมูลต้นแบบก็จะมีการสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย RIPPER เป็นตัวอย่างของการตรวจลดการแจ้งเตือนที่ผิดพลาด โดยใช้การเรียนรู้กฎของระบบตรวจจับการบุกรุกบนระบบเครือข่าย ชุดของข้อมูลต้นแบบจะต้องมีการปรับปรุงอยู่เสมอเพื่อให้สามารถตรวจจับการบุกรุกระบบเครือข่ายรูปแบบใหม่ได้

2.5.3 การตรวจหาร่องรอยการบุกรุกระบบเครือข่าย [13] และ [18]

การตรวจหาร่องรอยการบุกรุกระบบเครือข่ายได้แนวคิดมาจากวิธีการรักษาความปลอด-ภัยบนระบบเครือข่าย หากระบบเครือข่ายถูกบุกรุกหรือมีผู้พยายามสร้างความเสียหายให้กับระบบเครือข่าย ระบบจะต้องสามารถตรวจพบร่องรอยหรือความเสียหายที่เกิดขึ้นกับระบบเครือข่ายได้ ด้วยแนวคิดดังกล่าวการตรวจหาร่องรอยจึงเป็นการหาหลักฐานเพื่อนำมายืนยันว่าการแจ้งเตือนที่เกิดขึ้นเป็นการแจ้งเตือนที่ถูกต้อง ในการตรวจหาร่องรอยจากการบุกรุกบนระบบเครือข่ายมีอยู่หลายวิธีเช่น การใช้โปรแกรมเอเจ็นซึ่งถูกติดตั้งกระจายอยู่ทั่วระบบเครือข่ายและคอยตรวจหาร่องรอยในบริเวณที่ถูกกำหนด เป็นต้น

2.5.4 การประเมินคุณภาพการแจ้งเตือนที่เกิดขึ้น [1] และ [21]

การให้คะแนน (Score) กับการแจ้งเตือนที่เกิดขึ้น เมื่อเกิดการแจ้งเตือนของระบบตรวจจับการบุกรุกบนระบบเครือข่ายการแจ้งเตือนจะยังไม่ถูกส่งไปยังผู้ดูแลระบบโดยทันที แต่จะถูกส่งไปยังระบบการให้คะแนนและนำคะแนนที่ได้มาเปรียบเทียบกับเกณฑ์ที่กำหนด เพื่อชี้วัดว่าการแจ้งเตือนดังกล่าวมีแนวโน้มว่าเป็นการแจ้งเตือนถูกต้องหรือเป็นการแจ้งที่ผิดพลาด ผู้ดูแลระบบเครือข่ายจะนำการแจ้งเตือนที่มีคะแนนต่ำกว่าเกณฑ์ไปปรับลดกฎที่เป็นสาเหตุการเกิดการแจ้งเตือนที่ผิดพลาด

บทที่ 3
ระบบประเมินคุณภาพการแจ้งของโปรแกรมสนอร์ต

ปัจจุบันการรักษาความปลอดภัยบนระบบเครือข่ายมีความสำคัญอย่างยิ่ง ระบบตรวจจับการบุกรุกบนระบบเครือข่ายเป็นเทคนิคหนึ่งที่นำมาใช้ในการรักษาความปลอดภัยบนระบบเครือข่าย ปัญหาหลักของระบบตรวจจับการบุกรุกบนระบบเครือข่ายคือการแจ้งเตือนที่ผิดพลาด การแจ้งเตือนที่ผิดพลาดจำนวนมากมักจะส่งผลให้ระบบตรวจจับการบุกรุกทำงานหนักจนไม่สามารถทำงานได้ อันเป็นสาเหตุสำคัญทำให้ระบบเครือข่ายตกอยู่ในอันตรายจากผู้บุกรุกระบบเครือข่าย

การแก้ปัญหาข้างต้นผู้วิจัยได้สร้างระบบประเมินคุณภาพการแจ้งเตือนสำหรับโปรแกรมสนอร์ตโดยประยุกต์ใช้ระบบเครือข่ายใยประสาทที่ถูกฝึกด้วยชุดข้อมูลในกระบวนการเรียนรู้เพื่อนำมาใช้จำแนกประเภทการบุกรุกระบบเครือข่าย และประเมินระดับค่าบ่งชี้ของการแจ้งเตือนโปรแกรมสนอร์ตซึ่งค่าบ่งชี้นี้จะถูกนำไปคำนวณระดับคุณภาพการแจ้งเตือน การแจ้งเตือนที่มีระดับค่าคุณภาพต่ำจะถูกนำไปวิเคราะห์เพื่อนำไปปรับลดกฎที่เป็นสาเหตุทำให้เกิดการแจ้งเตือนที่ผิดพลาด

ในบทที่ 3 นี้จะกล่าวถึงสาเหตุการเกิดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต กลไกการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ค่าพารามิเตอร์และเงื่อนไขการกำหนดค่าพารามิเตอร์ของโมดูล Post Processor การจัดเก็บข้อมูลของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต การประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต การนำเสนอข้อมูลของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต และวิธีการอื่น ๆ [1] ที่นำมาเปรียบเทียบ

3.1 สาเหตุการเกิดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ต

การแจ้งเตือนที่ผิดพลาดของระบบตรวจจับการบุกรุกบนระบบเครือข่ายที่เกิดขึ้นเป็นจำนวนมากนั้นเป็นปัญหาหลักในการรักษาความปลอดภัยในระบบเครือข่าย และการทำธุรกรรมผ่านระบบอินเทอร์เน็ต ซึ่งการแจ้งเตือนที่ผิดพลาดเป็นจำนวนมากได้สร้างปัญหาให้แก่ผู้ดูแลระบบเครือข่ายเป็นอย่างยิ่งโดยเฉพาะการจำแนกว่าการเชื่อมต่อหรือกิจกรรมใดที่เกิดขึ้นในระบบเครือข่ายเป็นการบุกรุกหรือเป็นอันตรายต่อระบบเครือข่าย และกิจกรรมใดหรือการเชื่อมต่อใดเป็นการใช้งานปรกติบนระบบเครือข่าย

การแจ้งเตือนที่ผิดพลาดของระบบตรวจจับการบุกรุกบนระบบเครือข่ายสามารถแยกแยะได้ 2 สาเหตุหลักคือ กฎมีความผิดพลาด และการกำหนดกฎที่ใช้งานไม่เหมาะสมกับสภาพแวดล้อมของระบบเครือข่าย

3.1.1 กฎมีความผิดพลาด [21]

โปรแกรมสนอร์ตเป็นฟรีแวร์เมื่อมีการบุกรุกระบบเครือข่ายรูปแบบใหม่เกิดขึ้นผู้ใช้งานสามารถปรับปรุงชุดกฎของโปรแกรมสนอร์ตโดยการดาวน์โหลดจากเว็บไซต์ที่ให้บริการผู้ใช้งานที่ไม่มีความชำนาญจะไม่สามารถทราบได้เลยว่ากฎที่นำมาใช้งานนั้นมีประสิทธิภาพในการตรวจจับการบุกรุกบนระบบเครือข่าย หรือพบได้ก็ต่อเมื่อนำกฎเหล่านั้นมาใช้งานจริงเป็นผลให้การใช้งานโปรแกรมสนอร์ตนั้นมีความเสี่ยงสูงที่จะพบการแจ้งเตือนการบุกรุกที่ผิดพลาดขึ้น

3.1.2 การกำหนดกฎที่ใช้งานไม่เหมาะสมกับสภาพแวดล้อมของระบบเครือข่าย [21], [23], [24], [25] และ [26]

โครงสร้างระบบเครือข่ายภายในของแต่ละองค์กรย่อมแตกต่างกันขึ้นอยู่กับขนาดขององค์กรและนโยบายการรักษาความปลอดภัย ทำให้กิจกรรมและพฤติกรรมการใช้งานในแต่ละองค์กรมีความแตกต่างกันไป การกำหนดกฎให้เหมาะสมกับพฤติกรรมผู้ใช้งานบนระบบเครือข่ายจึงมีความสำคัญมากเพื่อป้องกันไม่ให้โปรแกรมสนอร์ตเข้าใจว่าพฤติกรรมปรกติในระบบเครือข่ายเป็นการบุกรุก งานวิจัยนี้จึงได้แบ่งพฤติกรรมที่โปรแกรมสนอร์ตมักพิจารณาว่าเป็นการบุกรุกระบบเครือข่ายเพื่อให้ผู้ใช้งานสามารถกำหนดชุดของกฎได้อย่างถูกต้องแสดงดังต่อไปนี้

การใช้งานคำสั่ง SQL ภายในระบบเครือข่าย การล็อคอินเข้าใช้งานที่มีความผิดพลาดสูง การทำงานของคำสั่ง SQL ที่ต้องใช้งานหน่วยความจำจำนวนมากในการประมวลผล รวมถึงการเกิดการโจมตีชนิด Password Brute Force เป็นต้น

ความถี่การสื่อสารของโปรโตคอลภายในระบบเครือข่ายสูง ความถี่ในการติดต่อสื่อสารของโปรโตคอล ตัวอย่างเช่น การตรวจจับ ARP Spoofing, Mac Address Flip-Flop, NETBIOS-SS Copy Executable File Attempt และ Invalid Response

การกำหนดค่าพารามิเตอร์ที่มีความยาวเกินกำหนด โปรแกรมสนอร์ตมองว่าชื่อที่ยาวเกินไปอาจเป็นสตริงที่แฮคเกอร์ใช้ในการบุกรุกระบบเครือข่าย ตัวอย่างเช่น SMB Overly Long Filename Creation, HTTP Parameter Length Too Long, IIS Command Execution, IIS cmd.exe Execution และ Attempt to Read Password File

การแจ้งเตือนที่เกิดจากส่วนหัวของโปรโตคอล (Header) ที่ใช้ในการส่งเมลล์และไฟล์ข้อมูล ตัวอย่างเช่น IM AIM (ICQ) File Transfer

การแบ่งย่อยแพ็คเก็จ (Fragments) ไม่ปรกติ พารามิเตอร์ที่ใช้ในการติดต่อมีค่าไม่ปรกติ รวมไปถึงพารามิเตอร์ที่ใช้ในการพิสูจน์ตัวเอง (Authentication) ที่มีความยาวกว่าปรกติ

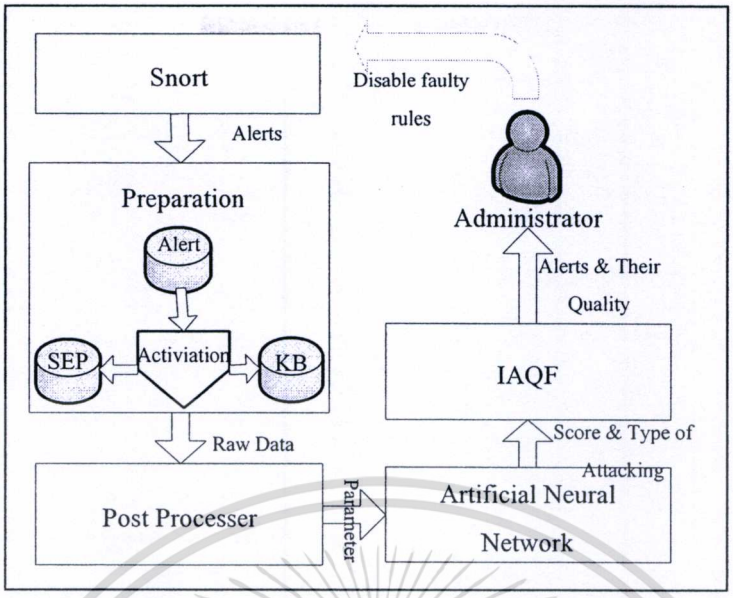
การใช้งานเครือข่ายภายในจากระยะไกล ตัวอย่างเช่น ผู้ใช้งานพยายามใช้งานเครือข่ายภายในจากระยะไกลด้วย REXEC (REXEC Account Login Attempt) หรือ MSRPC (Microsoft Remote Procedure Call) การพยายามใช้ RLOGIN ล็อกอินเข้าใช้งานเครือข่ายภายในจากระยะไกล (RLOGIN Root Account Attempt) การเข้าใช้งานเครือข่ายภายในด้วยชื่อผู้ใช้งานทั่วไปจากระยะไกลด้วย RSH (RSH Trusted Account) และการใช้ TTYPROMPT

ระดับความถี่ของความล้มเหลวการล็อกอินเข้าใช้งานระบบเครือข่ายสูงผิดปรกติ ไม่ว่าจะเป็นการเข้าใช้งานเครื่องแม่ข่ายที่เป็นเครื่องเมล์เซิร์ฟเวอร์ หรือเครื่องแม่ข่ายที่เก็บข้อมูล

3.2 กลไกการประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต [1], [13], [17] และ [18]

เนื่องจากโปรแกรมสนอร์ตเป็นโปรแกรมที่ใช้ในการตรวจจับการบุกรุกบนระบบเครือข่ายโดยไม่เสียค่าใช้จ่าย และการที่โปรแกรมสนอร์ตสามารถตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพทำให้มีผู้ใช้งานโปรแกรมสนอร์ตเพิ่มมากขึ้น จึงได้เกิดการรวมตัวกันเป็นสังคมของผู้ใช้งานโปรแกรมสนอร์ตขึ้น กลุ่มบุคคลเหล่านี้จะเขียนกฎของโปรแกรมสนอร์ตขึ้นมาเพื่อให้ผู้ใช้งานโปรแกรมสนอร์ตดาวน์-โหลดนำไปใช้ได้ แต่กฎของโปรแกรมสนอร์ตที่ดาวน์โหลดไปใช้งานนั้นอาจจะยังไม่ได้รับการตรวจสอบที่ดี หรือผู้ดูแลระบบกำหนดกฎที่นำไปใช้งานไม่เหมาะสมกับสภาพแวดล้อมของระบบเครือข่ายทำให้โปรแกรมสนอร์ตสร้างการแจ้งเตือนที่ผิดพลาดขึ้นจำนวนมาก

กลไกการประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตสามารถแสดงได้ดังรูปที่ 3.1 ระบบจะทำการจัดเก็บข้อมูลการแจ้งเตือนที่เกิดขึ้นลงในฐานข้อมูล และในขณะเดียวกันระบบก็จะทำการเก็บข้อมูลสภาพแวดล้อมภายในระบบเครือข่ายขณะที่เกิดการแจ้งเตือน เพื่อใช้กำหนดค่าพารามิเตอร์ซึ่งเป็นข้อมูลนำเข้าสำหรับระบบเครือข่ายใยประสาท ผลลัพธ์ที่ได้จะเป็นประเภทการบุกรุกระบบเครือข่ายและระดับคุณภาพการแจ้งเตือนที่เกิดขึ้น



รูปที่ 3.1 ขั้นตอนการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

Preparation เป็นกระบวนจัดเก็บข้อมูลเพื่อนำข้อมูลไปใช้งานในส่วนของ Post Processer เมื่อโปรแกรมสนอร์ตสร้างการแจ้งเตือน การแจ้งเตือนที่เกิดขึ้นจะถูกนำมาจัดเก็บไว้ในฐานข้อมูล Alert ขณะเดียวกันระบบจะกระตุ้นให้เกิดการจัดเก็บข้อมูลสถานะของโฮสต์และข้อมูลที่เกี่ยวข้อง โดยข้อมูลสถานะของโฮสต์จะถูกเก็บไว้ในฐานข้อมูลที่มีชื่อว่า SEP (Network/System Environment Parameter) ส่วน KB (Knowledge Base) จะเป็นข้อมูลฐานความรู้ของระบบ

Post Processer จะเป็นการนำข้อมูลจาก Preparation มาวิเคราะห์และเปรียบเทียบเพื่อกำหนดค่าให้กับพารามิเตอร์ที่ใช้งาน โดยค่าของพารามิเตอร์ที่ Post Processer กำหนดจะเป็นไปได้เพียง 2 ค่าเท่านั้นคือ 0 หรือ 1

Artificial Neural Network จุดประสงค์ของระบบเครือข่ายใยประสาทก็เพื่อจำแนกประเภทการบุกรุกระบบเครือข่ายและประเมินคุณภาพการแจ้งเตือนที่เกิดขึ้น ข้อมูลนำเข้าจะเป็นชุดข้อมูลจาก Post Processor ซึ่งเป็นพารามิเตอร์สถานะสภาพแวดล้อมของระบบเครือข่าย ผลลัพธ์ที่ได้จากระบบเครือข่ายใยประสาทคือ ประเภทการบุกรุกระบบเครือข่าย และระดับค่าบ่งชี้ประเภทการบุกรุกที่เกิดขึ้น

IAQF (Intrusion Alert Quality Framework) การนำเสนอข้อมูลที่ได้จากระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตให้อยู่ในรูปที่เข้าใจและใช้งานได้ง่ายต่อผู้ดูแลระบบเครือข่าย

3.3 พารามิเตอร์และการกำหนดค่าพารามิเตอร์ของ Post Processer

พารามิเตอร์แสดงสถานะและสภาพแวดล้อมของโฮสต์และระบบเครือข่ายถูกใช้เป็นข้อมูลนำเข้าสำหรับระบบเครือข่ายใยประสาท ค่าพารามิเตอร์จะถูกกำหนดโดย Post Processer ทำงานโดยการนำข้อมูลการแจ้งเตือนของโปรแกรมสนอร์ตมาเปรียบเทียบกับฐานความรู้ของระบบ ผลลัพธ์ที่ได้จาก Post Processor จะเป็นค่าชุดข้อมูลที่ประกอบไปด้วย 1 หรือ 0 โดยจะกำหนดค่าพารามิเตอร์เป็น 1 เมื่อพบช่องโหว่ที่เกิดจากการใช้งานไม่ว่าจะเกิดจากระบบเครือข่ายโฮสต์หรือระบบตรวจจับการบุกรุก และกำหนดค่าพารามิเตอร์เป็น 0 ก็ต่อเมื่อระบบเครือข่ายมีการป้องกันที่ดี เช่น การปิดช่องโหว่ที่ตรวจพบ หรือมีนโยบายการควบคุมการใช้งานระบบเครือข่ายที่ชัดเจน พารามิเตอร์ที่นำมาใช้งานกับระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตมีด้วยกัน 24 พารามิเตอร์โดยสามารถแบ่งพารามิเตอร์ออกเป็น 4 กลุ่มซึ่งมีรายละเอียดและเงื่อนไขในการกำหนดค่าพารามิเตอร์ดังต่อไปนี้

3.3.1 สถานะและสภาพแวดล้อมของโฮสต์ ตรวจสอบด้วยพารามิเตอร์ 9 พารามิเตอร์

- **สถานะของโฮสต์ (Correctness)** การคงอยู่ของโฮสต์ในระบบเครือข่าย หมายถึงโฮสต์เปิดใช้งานและสามารถติดต่อกับโฮสต์อื่น ๆ ภายในระบบเครือข่ายได้ สถานะของโฮสต์เป็นพารามิเตอร์อันดับแรกที่สามารถนำมาระบุได้ว่าการแจ้งเตือนที่เกิดขึ้นนั้นเป็นการแจ้งเตือนเมื่อมีการบุกรุกระบบเครือข่ายจริงหรือเป็นการแจ้งเตือนที่ผิดพลาด

เงื่อนไขในการกำหนดค่าพารามิเตอร์สำหรับการกำหนดให้โฮสต์เปิดทำงานและสามารถเชื่อมต่อกับโฮสต์อื่นๆภายในระบบเครือข่ายได้ให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- **ช่องโหว่บนระบบปฏิบัติการที่โฮสต์ทำงาน (Host_OS_Vulnerability)** [4], [6] และ [7] ระบบปฏิบัติการไม่ว่าจะเป็นวินโดว์หรือลีนุกซ์ โดยปรกติผู้ให้บริการจะมีซอฟท์แวร์ป้องกันช่องโหว่ (Patch) ตามออกมาเพื่อแก้ไขข้อผิดพลาด (Bug) หรือปิดช่องโหว่ของระบบปฏิบัติการที่จะนำไปสู่ช่องทางในการบุกรุกของผู้ไม่ประสงค์ดี เช่น Window XP จะมี Service Patch 1, 2 และ 3 หรือ Window Vista Service Patch 1 เป็นต้น ผู้ดูแลระบบเครือข่ายจำเป็นอย่างยิ่งที่จะต้องตรวจสอบข้อมูลช่องโหว่ของระบบปฏิบัติการและปิดช่องโหว่ดังกล่าวเพื่อไม่ให้ระ-บบเครือข่ายตกอยู่ในอันตราย ซอฟท์แวร์ที่นำมาปิดช่องโหว่สามารถดาวน์โหลดได้จากเว็บไซต์ของผู้ให้บริการโดยไม่เสียค่าใช้จ่าย

เงื่อนไขในการกำหนดพารามิเตอร์สำหรับการกำหนดให้ระบบปฏิบัติการที่โฮสต์ใช้งานไม่-ได้ปรับปรุงซอฟท์แวร์ป้องกันช่องโหว่ล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- **ช่องโหว่บนพอร์ตที่โฮสต์ทำงาน (Host_Port_Vulnerability)** [4], [6] และ [7] พอร์ตสื่อสารของโปรโตคอล TCP และ UDP ในชั้น Transport Layer หมายเลขพอร์ตจะมีค่าแตกต่างกันไปตามลักษณะการใช้งาน เช่น พอร์ต 80 ใช้สำหรับเปิดเว็บเพจ พอร์ต 25 สำหรับรับส่งอีเมล

หรือ พอร์ต 23 สำหรับใช้ Telnet ในการเข้าใช้งานระบบเครือข่ายภายในจากระยะไกล ช่องโหว่ที่เกิดขึ้นกับพอร์ตที่ใช้งานสามารถตรวจสอบข้อมูลได้ที่ CERT [5] และ CVE Mire [3]

เงื่อนไขในการกำหนดพารามิเตอร์สำหรับการกำหนดให้พอร์ตที่โฮสต์ใช้งานมีช่องโหว่ให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- ช่องโหว่บนโปรแกรมที่โฮสต์ใช้งาน (Host_App_Vulnerability) [4], [6] และ [7] โปรแกรมที่ใช้ออกอินเทอร์เน็ตหรือโปรแกรมที่ต้องมีกิจกรรมเกี่ยวข้องกับอินเทอร์เน็ตซึ่งเป็นช่องทางหนึ่งที่ผู้ไม่ประสงค์ดีใช้เป็นเครื่องมือในการบุกรุกระบบเครือข่าย ดังนั้นผู้ดูแลระบบเครือข่ายจำเป็นต้องตรวจสอบช่องโหว่ข้อบกพร่องของโปรแกรมและปิดช่องโหว่เหล่านั้น เช่น โปรแกรม Internet Explorer เป็นโปรแกรมในการใช้งานอินเทอร์เน็ตบนระบบปฏิบัติการวินโดว์ ไมโครซอฟท์ได้มีซอฟท์แวร์ปิดช่องโหว่ของโปรแกรม Internet Explorer จำนวนมากออกมาให้ดาวน์โหลดโดยไม่เสียค่าจ่ายที่เว็บไซต์ของไมโครซอฟท์

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้โปรแกรมที่โฮสต์ใช้งานไม่ได้ปรับ-ปรุงด้วยซอฟท์แวร์ปิดช่องโหว่ของโปรแกรมเวอร์ชันล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- สถานะของหน่วยความจำ (Host _Memory_Status) หน่วยความจำ (Ram) จะถูกโจมตีในลักษณะ DoS เพื่อทำให้โฮสต์ไม่สามารถทำงานได้หรือทำงานช้ากว่าปรกติ การโจมตีหน่วยความจำสามารถทำได้หลายวิธี เช่น โฮสต์ถูกบุกรุกด้วยมัลแวร์ (Malware) เซอร์วิสที่ถูกติดตั้งโดยสปายแวร์ (Spyware) หรือการถูกโจมตีแบบ flooding เป็นต้น

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้หน่วยความจำถูกใช้งานมากกว่าปรก-ติให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- สถานะของหน่วยประมวลผล (Host_CPU_Status) สถานะของหน่วยประมวลผล (CPU) จะถูกโจมตีในลักษณะ DoS เช่นเดียวกับหน่วยความจำซึ่งจะส่งผลให้ CPU ทำงานหนักกว่าปรกติ การโจมตีหน่วยประมวลผลจะมีวิธีคล้ายคลึงกับการโจมตีหน่วยความจำ

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้หน่วยประมวลผลทำงานไม่ปรกติให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- การติดตั้งโปรแกรมตรวจจับไวรัส (Host_AV_Installation) โปรแกรมตรวจจับไวรัสเป็นวิธีพื้นฐานในการป้องกันการบุกรุกของโฮสต์ โปรแกรมตรวจจับไวรัสจะทำหน้าที่ป้องกันไวรัส เวิร์ม มัลแวร์ และสปายแวร์ (ความสามารถของโปรแกรมตรวจจับไวรัสขึ้นอยู่กับผู้ให้บริการจะเป็นผู้กำหนด) ที่มาจากอินเทอร์เน็ตหรืออุปกรณ์ต่อพ่วง (floppy disk, External Hard Drive และ CD Rom) ดังนั้นโปรแกรมป้องกันไวรัสจึงมีความสำคัญอย่างยิ่งต่อโฮสต์ที่เชื่อมต่อกับระบบเครือข่ายหรือโฮสต์ที่ทำงานเพียงเครื่องเดียว (Stand Alone)

เงื่อนไขในการกำหนดพารามิเตอร์สำหรับการกำหนดให้โฮสต์ที่ไม่ได้ติดตั้งโปรแกรมป้อง-กันไวรัสให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- การอัพเดทรูปแบบการตรวจจับไวรัสเวอร์ชันล่าสุด (Host_AV_Uptodate) ไวรัส เวิร์ม และ มัลแวร์ ได้ถูกพัฒนารูปแบบการบุกรุกอยู่ตลอดเวลาดังนั้นโปรแกรมที่ทำงานจำเป็นต้องปรับปรุงรูปแบบการตรวจจับการบุกรุกด้วยเช่นกัน เพื่อให้สามารถตรวจจับการบุกรุกรูปแบบใหม่ ๆ ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ

เงื่อนไขในการกำหนดพารามิเตอร์สำหรับการกำหนดให้โฮสต์ที่ไม่ได้ปรับปรุงรูปแบบการตรวจจับการบุกรุกเวอร์ชันล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- กำหนดสิทธิ์การใช้งานโฮสต์ (Host_Permission_Control) การกำหนดสิทธิ์ใช้งานโฮสต์เพื่อป้องกันไม่ให้โฮสต์ตกอยู่ในอันตราย เช่น ผู้ใช้งานลบไฟล์ที่ใช้ในการเปิดเครื่อง หรือผู้ใช้งานทำให้ไฟล์ระบบปฏิบัติการเสียหาย เป็นต้นการกำหนดสิทธิ์ในการใช้งานยังช่วยให้ระบบเครือข่ายไม่ตกอยู่ในอันตรายเนื่องจากการที่ผู้ใช้งานแอบติดตั้งโปรแกรมที่เป็นอันตรายต่อระบบเครือข่าย เช่น โปรแกรมสแกนระบบเครือข่าย หรือโปรแกรมสแกนรหัสผ่าน เป็นต้น

เงื่อนไขการกำหนดพารามิเตอร์ด้วยการกำหนดให้โฮสต์ที่ไม่มีการกำหนดสิทธิ์ในการเข้าใช้งานโฮสต์ให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

3.3.2 สภาพแวดล้อมของระบบตรวจจับการบุกรุกบนระบบเครือข่าย [27], [29] และ [30] ตรวจสอบด้วยพารามิเตอร์ 4 พารามิเตอร์

- การกำหนดกฎบนระบบตรวจจับการบุกรุกระบบเครือข่าย (IDS_Rule_Reliability) การนำกฎมาใช้งานกับระบบตรวจจับการบุกรุกบนระบบเครือข่ายจะต้องไม่ทำให้เกิดการแจ้งเตือนที่ผิดพลาดจำนวนมาก และต้องไม่ทำงานล้มเหลวโดยตรวจสอบไม่พบการบุกรุก (False Negative) โดยในงานวิจัยนี้จะมุ่งเน้นปรับปรุงในส่วนของการลดการแจ้งเตือนที่ผิดพลาด

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้กฎที่ดาวน์โหลดมาใช้งานไม่ได้ถูกทดสอบก่อนใช้งานจริงให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- ระบบตรวจจับการบุกรุกมีการปรับปรุงชุดกฎสม่ำเสมอ (IDS_Rule_ Sensitivity) การบุกรุกระบบเครือข่ายได้มีการพัฒนารูปแบบมาโดยตลอดเพื่อให้ระบบตรวจจับการบุกรุกระบบเครือข่ายได้อย่างมีประสิทธิภาพ ระบบตรวจจับการบุกรุกระบบเครือข่ายจำเป็นต้องปรับปรุงชุดกฎให้สามารถตรวจจับการบุกรุกรูปแบบใหม่ได้ สำหรับโปรแกรมสนอร์ตผู้ใช้งานสามารถดาวน์โหลดชุดของกฎได้ที่ www.snort.org

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้ชุดกฎที่ใช้งานไม่ได้รับการปรับปรุงล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- ช่องโหว่บนระบบปฏิบัติการที่รองรับระบบตรวจจับการบุกรุกบนระบบเครือข่ายทำงาน (IDS_OS_Vulnerability) ช่องโหว่บนระบบปฏิบัติการที่ระบบตรวจจับการบุกรุกบนระบบเครือข่ายทำงานเป็นสิ่งสำคัญมาก หากระบบตรวจจับการบุกรุกบนระบบเครือข่ายไม่สามารถทำงานได้จะทำให้ระบบเครือข่ายตกอยู่ในอันตราย

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้ระบบปฏิบัติการที่ระบบตรวจจับการบุกรุกระบบเครือข่ายทำงานไม่ได้ปรับปรุงซอฟท์แวร์ป้องกันช่องโหว่ล่าสุดให้มีค่าเท่ากับ 1 ถ้า ไม่ใช่ให้มีค่าเท่ากับ 0

- **เวอร์ชันของระบบตรวจจับการบุกรุกบนระบบเครือข่าย (IDS_Version_Uptodate)** โปรแกรมสนอร์ตได้ถูกพัฒนาจนกลายเป็นโปรแกรมตรวจจับการบุกรุกบนระบบเครือข่ายที่นิยมใช้งานกันทั่วโลก ความสามารถในการตรวจจับการบุกรุกบนระบบเครือข่ายก็ได้ถูกพัฒนาขึ้นมาด้วยเช่นกันเพื่อปิดช่องโหว่ ข้อผิดพลาดในการใช้งาน (Bug) และเพิ่มประสิทธิภาพในการทำงานให้กับโปรแกรมสนอร์ตโดยเวอร์ชันล่าสุดของโปรแกรมสนอร์ตคือ เวอร์ชัน 2.8.4.1 อัพเดท ณ วันที่ 27 เมษายน พ.ศ. 2552

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้โปรแกรมสนอร์ตเวอร์ชันที่ใช้งานไม่-ใช่เวอร์ชันล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

3.3.3 การป้องกันการบุกระบบเครือข่ายจากภายนอกองค์กร ตรวจสอบด้วยพารามิเตอร์ 5 พารามิเตอร์ [23] และ [30]

- **ไฟร์วอลล์บนระบบเครือข่าย (Firewall_Availiability)** ไฟร์วอลล์เป็นอุปกรณ์ป้องกันการบุกรุกระบบเครือข่ายจากภายนอกองค์กร และเป็นอุปกรณ์พื้นฐานที่ทุกองค์กรสมควรติดตั้ง สำหรับไฟร์วอลล์ที่ใช้ในงานวิจัยมีชื่อว่า IPCop โดย IPCop เป็นฟรีแวร์ที่สามารถนำมาใช้งานโดยไม่เสียค่าใช้จ่าย และทำงานได้อย่างมีประสิทธิภาพ

เงื่อนไขในการกำหนดพารามิเตอร์สำหรับการกำหนดให้ระบบเครือข่ายไม่มีไฟร์วอลล์ให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- **ช่องโหว่บนระบบปฏิบัติการที่รองรับไฟร์วอลล์ (Firewall_OS_Vulnerability)** มีลักษณะคล้ายกับระบบปฏิบัติการที่ระบบตรวจจับการบุกรุกระบบเครือข่ายทำงาน หากไฟร์วอลล์ไม่สามารถทำงานได้ระบบเครือข่ายจะตกอยู่ในอันตรายด้วยเช่นกัน

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้ระบบปฏิบัติการที่รองรัไฟร์วอลล์ไม่ได้อัพเดทซอฟท์แวร์ป้องกันช่องโหว่ล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- **เวอร์ชันของไฟร์วอลล์ (Firewall_Version_Uptodate)** IPcop ได้ถูกพัฒนามาจนถึงเวอร์ชัน 1.4.2.1 ณ วันที่ 23/07/2008 สามารถดาวน์โหลดมาใช้งานได้ที่ www.ipcop.org

เงื่อนไขการกำหนดพารามิเตอร์ด้วยการกำหนดให้โปรแกรม IPCop ที่ใช้งานไม่ใช่เวอร์ชันล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- **คัดกรองการใช้งานอินเทอร์เน็ต (Firewall_URL_Filtering)** อินเทอร์เน็ตมีทั้งข้อดีและข้อเสียถ้าผู้ใช้งานนำอินเทอร์เน็ตมาเพิ่มประสิทธิภาพในการทำงานก็จะมีประโยชน์ต่อองค์กร แต่ถ้าผู้ใช้งานนำไปใช้ผิดวิธี เช่น ใช้อินเทอร์เน็ตภายในองค์กรเข้าใช้งานเว็บไซต์ที่ให้บริการรูปและเนื้อหาไม่เหมาะสม ทำให้องค์กรสูญเสียแบนด์วิดท์โดยไม่เกิดประโยชน์ต่อองค์กร ในกรณีของ

เว็บไซค์ดังกล่าวอาจจะมี สปายแวร์ เวิร์ม ไวรัส หรือมัลแวร์ฝังตัวอยู่ เมื่อผู้ใช้งานเข้าถึงเว็บนี้จะทำให้ระบบเครือข่ายขององค์กรตกอยู่ในอันตรายได้

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้ระบบเครือข่ายภายในองค์กรไม่มีการคัดกรองการใช้งานอินเทอร์เน็ตให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- สถานะการอัพเดทฐานข้อมูลเว็บไซต์ต้องห้าม (Firewall_URL_Uptodate) การใช้งานอินเทอร์เน็ตได้รับความนิยมอย่างสูง ทำให้มีเว็บไซต์เกิดขึ้นใหม่ทุกวันเป็นจำนวนมาก ดังนั้นการควบคุมการเข้าใช้งานอินเทอร์เน็ตจะทำได้อย่างมีประสิทธิภาพ ก็ต่อเมื่อฐานข้อมูลที่ใช้จัดเก็บเว็บไซต์ที่องค์กรห้ามเข้าถึงมีการปรับปรุงอยู่เสมอ

เงื่อนไขการกำหนดพารามิเตอร์ด้วยการกำหนดให้ฐานข้อมูลจัดเก็บเว็บไซต์ไม่ได้ถูกปรับปรุงให้มีสถานะใหม่ล่าสุดให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

3.3.4 นโยบายการรักษาความปลอดภัยบนระบบเครือข่าย ตรวจสอบด้วยพารามิเตอร์ 6 พารามิเตอร์ [30]

- การกำหนดนโยบายรักษาความปลอดภัยบนระบบเครือข่าย (Security_Policy) นโยบายรักษาความปลอดภัยบนระบบเครือข่ายเป็นเครื่องมือพื้นฐานที่ช่วยให้เกิดความปลอดภัยในการใช้งาน นโยบายรักษาความปลอดภัยรวมไปถึงระบบการรักษาความปลอดภัยทางกายภาพ เช่น การใช้ Smart Card ในการพิสูจน์ตัวตน หรือการใช้ไบโอเมทริกซ์ (Biometrics) เป็นต้น

เงื่อนไขในการกำหนดค่าพารามิเตอร์สำหรับการกำหนดให้องค์กรไม่มีการกำหนดนโยบายด้านความปลอดภัยบนระบบเครือข่ายให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- การกำหนดชื่อผู้ใช้งานมีรูปแบบที่แน่นอน (Username_Pattern) การกำหนดรูปแบบชื่อผู้ใช้งานที่แน่นอนจะทำให้ผู้ดูแลระบบเครือข่ายทราบพฤติกรรมการใช้งานบนระบบเครือข่ายได้อย่างชัดเจน ตัวอย่างรูปแบบการกำหนดชื่อผู้ใช้งาน ชื่อตามด้วยเครื่องหมาย “_” แล้วตามด้วยนามสกุลสามตัวแรก เป็นต้น

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้การเข้าใช้งานระบบเครือข่ายไม่มีการกำหนดรูปแบบชื่อผู้ใช้งานที่ชัดเจนให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- ความซับซ้อนของรหัสผ่าน (Password_ Complexity) การตั้งรหัสผ่านมีความสำคัญอย่างยิ่งถ้าตั้งรหัสผ่านง่ายเกินไปเช่น “123456” หรือนำวันเดือนปีเกิดของผู้ใช้งานมาทำเป็นรหัสผ่านจะทำให้ง่ายต่อการคาดเดาของผู้ไม่ประสงค์ดี รหัสผ่านที่ดีควรมีความยาวเกิน 6 ตัวอักษร ควรมีตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ ประกอบเข้าด้วยกัน

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้ผู้ดูแลระบบไม่ได้กำหนดให้รหัสผ่านต้องมีความซับซ้อนให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- การกำหนดอายุให้กับรหัสผ่าน (Password_Expiration) การเปลี่ยนรหัสผ่านบ่อยๆ จะเป็นการเพิ่มความปลอดภัยให้กับระบบเครือข่าย ผู้ดูแลระบบเครือข่ายจำเป็นต้องกำหนดให้ผู้ใช้งานมีการเปลี่ยนรหัสผ่านทุก 3 เดือนเป็นอย่างน้อย

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้ผู้ดูแลระบบไม่มีการกำหนดให้รหัสผ่านหมดอายุให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- ระบบจัดการชื่อผู้ใช้งานและรหัสผ่าน (Username_Systematic) เมื่อมีพนักงานลาออกหรือย้ายแผนก ชื่อผู้ใช้งานจะต้องไม่สามารถเข้าใช้งานระบบเครือข่ายได้เพื่อป้องกันไม่ให้พนักงานกลับมาลบข้อมูล หรือนำข้อมูลที่เป็นความลับขององค์กรออกไป เมื่อพนักงานย้ายแผนกความสามารถในการเข้าใช้งานจะต้องเปลี่ยนตามไปด้วย

เงื่อนไขการกำหนดพารามิเตอร์สำหรับการกำหนดให้หากไม่มีระบบการจัดการชื่อผู้ใช้-งานและรหัสผ่านให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

- ควบคุมการใช้งานอุปกรณ์ต่อพ่วง (External_Drive_Control) การใช้งานอุปกรณ์ต่อพ่วง (Floppy Disk, CD-Rom และ External Hard Drive) ในปัจจุบันได้รับความนิยมเป็นอย่างมาก เนื่องจากสะดวกในการใช้งาน ง่ายต่อการติดตั้งเคลื่อนย้าย และสามารถจัดเก็บข้อมูลได้เป็นจำนวนมาก การนำอุปกรณ์ต่อพ่วงมาใช้งานในองค์กรจะต้องมีการควบคุมที่ดีเนื่องจากอุปกรณ์ต่อพ่วงได้ถูกนำไปใช้งานกับโฮสต์อื่นๆ ภายนอกองค์กรทำให้อุปกรณ์ต่อพ่วงอาจติดไวรัสแล้วมาแพร่กระจายภายในองค์กรได้ และการที่อุปกรณ์ต่อพ่วงสามารถจัดเก็บข้อมูลได้เป็นจำนวนมากจึงง่ายที่พนักงานจะนำข้อมูลที่เป็นความลับขององค์กรออกไปโดยไม่ได้รับอนุญาต

เงื่อนไขการกำหนดพารามิเตอร์ด้วยการกำหนดให้องค์กรไม่มีการควบคุมการใช้งานอุป-กรณ์ต่อพ่วงให้มีค่าเท่ากับ 1 ถ้าไม่ใช่ ให้มีค่าเท่ากับ 0

3.4 การจัดเก็บข้อมูลของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

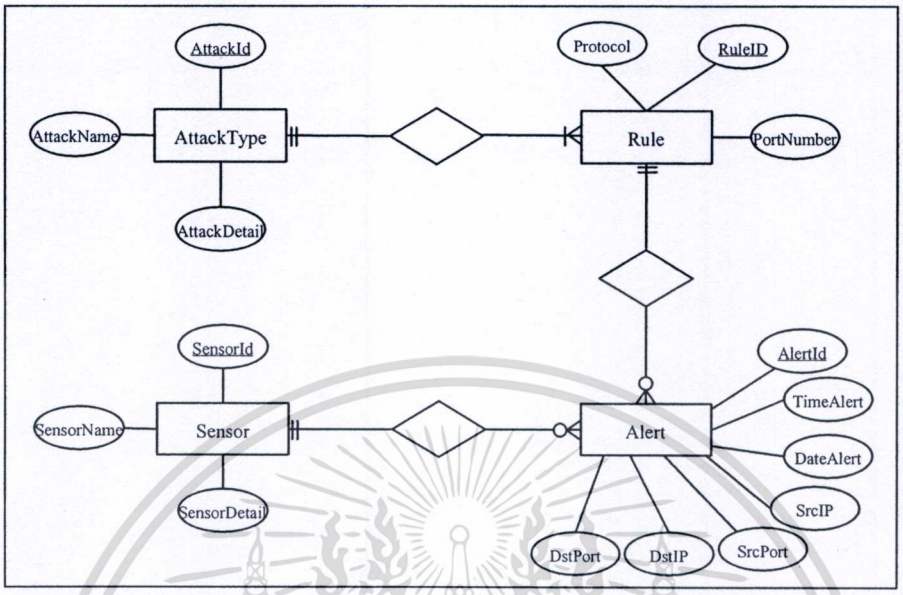
Preparation จะทำหน้าที่จัดเตรียมข้อมูลเพื่อนำไปใช้ใน Post Processer โดย Preparation จะนำข้อมูลที่ใช้ในระบบประเมินคุณภาพของโปรแกรมสนอร์ตมาจัดเก็บไว้ในฐานข้อมูลของระบบ ฐานข้อมูลที่นำมาใช้งานคือ MySql เวอร์ชัน 5.01 ข้อมูลที่ถูกจัดเก็บจะประกอบไปด้วยข้อมูลการแจ้งเตือนที่เกิดขึ้นของโปรแกรมสนอร์ต ข้อมูลฐานความรู้ของระบบ และข้อมูลสถานะของโฮสต์ซึ่งมีรายละเอียดดังต่อไปนี้

3.4.1 ข้อมูลการแจ้งเตือนของโปรแกรมสนอร์ต

โปรแกรมสนอร์ตมีฐานข้อมูลในการจัดเก็บการแจ้งเตือนที่เกิดขึ้น โดยสามารถจัดเก็บข้อมูลลงในฐานข้อมูลที่เป็น MySql, Oracle และ SQLServer ผู้ใช้งานสามารถดาวน์โหลดโครงสร้างฐานข้อมูลได้จากเว็บไซต์ของโปรแกรมสนอร์ต

การจัดเก็บข้อมูลการแจ้งเตือนที่เกิดขึ้นโปรแกรมสนอร์ตนั้นมีความซับซ้อนและมีความละเอียดของข้อมูลสูง เช่น การเก็บข้อมูลส่วนหัวของแพ็คเก็จ (ค่าความยาว, ค่า TTL, ค่า Flags เป็นต้น) ซึ่งในงานวิจัยนี้ใช้เพียงบางส่วนของข้อมูลเหล่านั้น ดังนั้นทางผู้วิจัยจึงได้จัดสร้างฐานข้อมูลขึ้นมาใช้งานเองเพื่อให้สามารถนำข้อมูลออกมาใช้งานได้อย่างมีประสิทธิภาพ รูปที่ 3.2

เป็น ER Diagram แสดงโครงสร้างฐานข้อมูลเพื่อบันทึกข้อมูลการแจ้งเตือนที่โปรแกรมสนอร์ตได้สร้างขึ้น



รูปที่ 3.2 ER Diagram แสดงโครงสร้างฐานข้อมูลสำหรับบันทึกข้อมูลการแจ้งเตือนของโปรแกรมสนอร์ต

พจนานุกรมข้อมูล (Data Dictionary) ที่ใช้อธิบาย ER Diagram ซึ่งเป็นโมเดลฐานข้อมูลที่ใช้รองรับข้อมูลการแจ้งเตือนของโปรแกรมสนอร์ต

ตารางที่ 3.1 รายละเอียดการจัดเก็บข้อมูลตาราง AttackType

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
AttackId	Int(Autonumber)	Primary Key	รหัสประเภทการบุกรุกระบบเครือข่าย
AttackName	Char(150)		ชื่อประเภทการบุกรุก
AttackDetail	Char(255)		รายละเอียดการบุกรุก

ตารางที่ 3.2 รายละเอียดการจัดเก็บข้อมูลตาราง Rule

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
RuleId	Int(Autonumber)	Primary Key	เลขที่กฎที่โปรแกรมสนอร์ตใช้งาน
Protocol	Char(255)		โปรโตคอลที่กฎตรวจสอบ
PortNumber	Char(255)		พอร์ตที่กฎตรวจสอบ
Attackid	Int	Foreign Key	รหัสประเภทการบุกรุกระบบเครือข่าย

ตารางที่ 3.3 รายละเอียดการจัดเก็บข้อมูลตาราง Alert

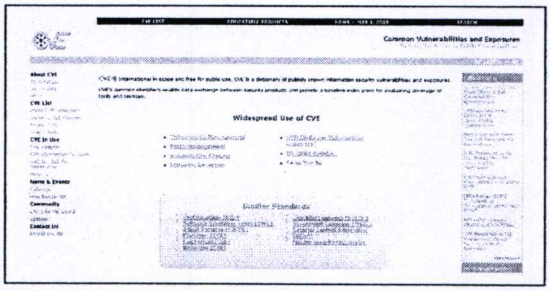
ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
AlertId	Int(Autonumber)	Primary Key	รหัสการแจ้งเตือนที่เกิดขึ้น
DateAlert	Date/Time		วันที่เกิดการแจ้งเตือน
TimeAlert	Date/Time		เวลาที่เกิดการแจ้งเตือน
SrcIP	Char(30)		ไอพีต้นทาง
SrcPort	Char(10)		พอร์ตต้นทาง
DstIP	Char(30)		ไอพีปลายทาง
DstPort	Char(10)		พอร์ตปลายทาง
SensorId	Int	Foreign Key	รหัสเซ็นเซอร์ของโปรแกรมสนอร์ต
RuleId	int	Foreign Key	เลขที่กฎที่โปรแกรมสนอร์ตใช้งาน

ตารางที่ 3.4 รายละเอียดการจัดเก็บข้อมูลตาราง Sensor

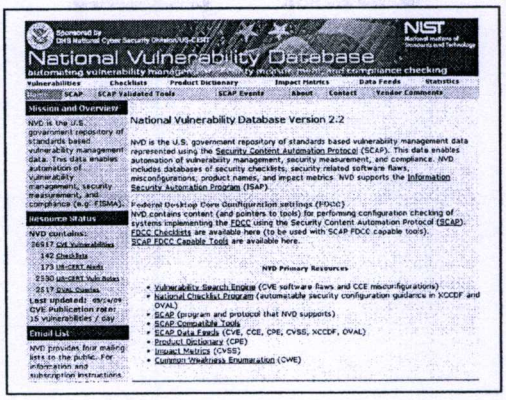
ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
SensorId	Int(Autonumber)	Primary Key	รหัสเซ็นเซอร์ของโปรแกรมสนอร์ต
SensorName	Char(50)		ชื่อเซ็นเซอร์
SensorDetail	Char(200)		ที่ตั้งและรายละเอียดเกี่ยวกับเซ็นเซอร์

3.4.2 ข้อมูลฐานความรู้ของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

ข้อมูลฐานความรู้ของระบบจะถูกนำมาใช้ในการกำหนดค่าพารามิเตอร์ประกอบไปด้วยข้อมูล 2 ส่วน ส่วนแรกเป็นข้อมูลช่องโหว่ที่จะถูกผู้บุกรุกระบบเครือข่ายนำมาใช้บุกรุกระบบเครือข่ายอันประกอบไปด้วยช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของโปรโตคอลและช่องโหว่ของโปรแกรมที่ใช้งานซึ่งเป็นข้อมูลที่ได้มาจาก CVE Mitre [5], CERT [3] และเว็บไซต์ที่ให้บริการ ส่วนที่สองเป็นข้อมูลที่เกี่ยวข้องกับโปรแกรมที่ใช้งาน เช่น หมายเลขเวอร์ชันล่าสุดของโปรแกรมที่ใช้งาน รูปแบบการตรวจจับการบุกรุกล่าสุดที่สามารถดาวน์โหลดมาใช้งาน เป็นต้น



รูปที่ 3.3 ข้อมูลช่องโหว่ที่สามารถตรวจสอบได้ที่เว็บไซต์ http://cve.mitre.org

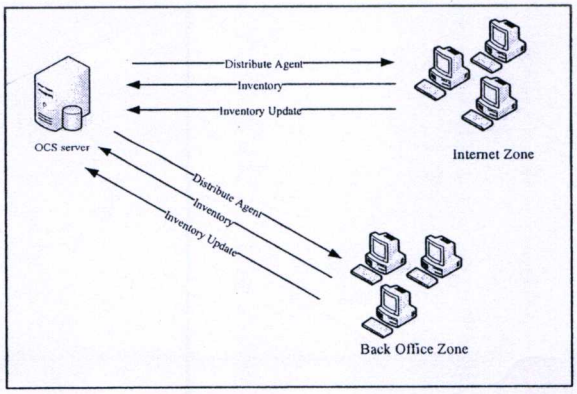


รูปที่ 3.4 ข้อมูลช่องโหว่ที่สามารถตรวจสอบได้ที่เว็บไซต์ http://nvd.nist.gov

3.4.3 ข้อมูลสถานะของโฮสต์

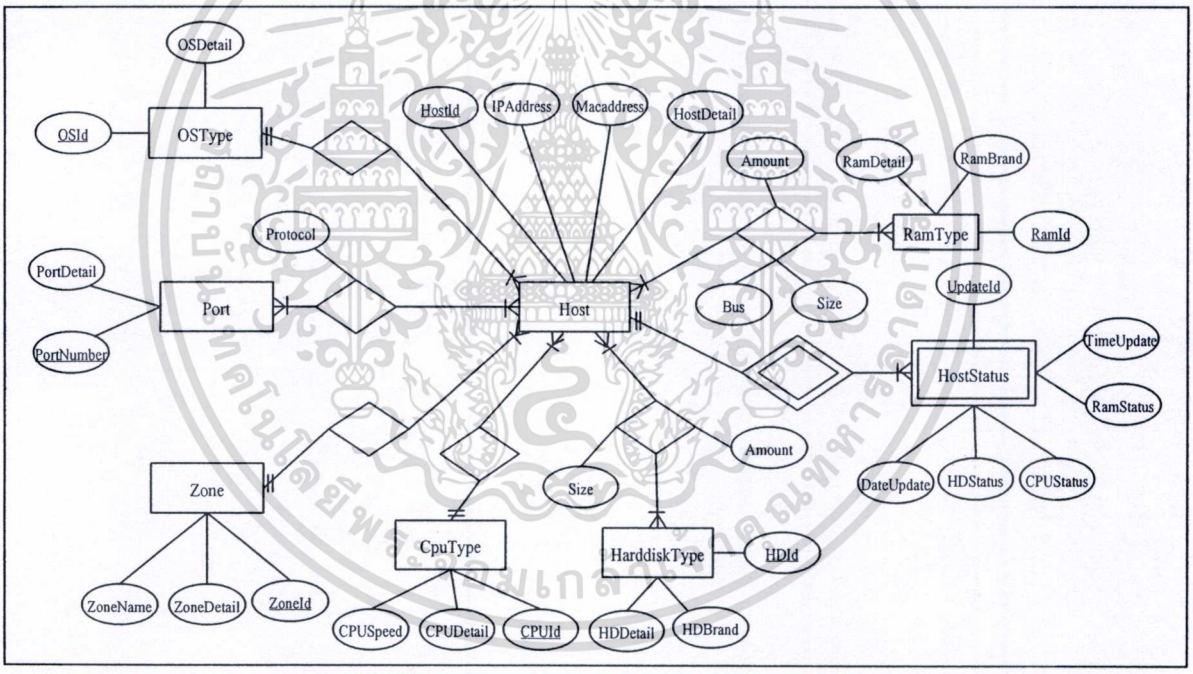
ข้อมูลสถานะของโฮสต์ที่นำมาใช้ในระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตประกอบไปด้วย ข้อมูลหน่วยความจำที่โฮสต์ใช้งาน และข้อมูลหน่วยประมวลผลที่โฮสต์ใช้งานในขณะที่เกิดการแจ้งเตือน การจัดเก็บข้อมูลสถานะของโฮสต์เป็นหน้าที่ของโปรแกรมเอเจ็นต์โดยโปรแกรมเอเจ็นต์จะถูกติดตั้งที่โฮสต์และจะส่งข้อมูลสถานะของโฮสต์มาจัดเก็บในฐานข้อมูลของระบบเป็นระยะๆ โดยโปรแกรมเอเจ็นต์นั้นประยุกต์ใช้โปรแกรม OCS Inventory [16] ในการจัดเก็บข้อมูล

โปรแกรม OCS (Open Computer and Software) Inventory เป็นฟรีแวร์ที่ใช้งานกันอย่างแพร่หลาย เนื่องด้วยประสิทธิภาพในการทำงานสูงและสามารถทำงานได้บนระบบปฏิบัติการหลายแบบ เช่น วินโดว์หรือลีนุกซ์ ผู้ที่ต้องการใช้งานสามารถดาวน์โหลดมาใช้งานได้จาก www.ocs.org โปรแกรม OCS Inventory ทำงานได้โดยการกระจาย (Distribute) โปรแกรมเอเจ็นต์ไปติดตั้งยังโฮสต์ต่างๆ จากนั้นให้โปรแกรมเอเจ็นต์จะทำการตรวจสอบข้อมูลของโฮสต์แล้วจัดส่งข้อมูลกลับมายัง OCS Inventory เครื่องแม่ข่าย (OCS Inventory server) โดย OCS Inventory เครื่องแม่ข่ายจะทำหน้าที่จัดเก็บข้อมูลลงฐานข้อมูล และจะถูกผู้ดูแลระบบเครือข่ายเรียกใช้ในการเฝ้าติดตามการเปลี่ยนแปลงที่เกิดขึ้นกับโฮสต์



รูปที่ 3.5 ขั้นตอนการทำงานของโปรแกรม OCS Inventory

หน้าที่หลักของโปรแกรม OCS Inventory คือการจัดเก็บข้อมูลโฮสต์ (เครื่องลูกข่ายและเครื่องแม่ข่าย) การจัดเก็บประวัติการซ่อมบำรุงของโฮสต์ ข้อมูลฮาร์ดแวร์ เช่น ขนาดของหน่วยความจำ ความเร็วของ CPU ความจุของฮาร์ดดิสก์ รวมไปถึงยี่ห้ออุปกรณ์ ข้อมูลซอฟท์แวร์ที่ติดตั้งบนโฮสต์ และหากเกิดการเปลี่ยนแปลงของซอฟท์แวร์หรือฮาร์ดแวร์ โปรแกรม OCS Inventory ก็จะสร้างการแจ้งเตือนไปยังผู้ดูแลระบบเครือข่าย ความสามารถของโปรแกรม OCS Inventory จะช่วยให้ผู้ดูแลระบบสามารถทำงานได้ง่ายขึ้นในการจัดการโฮสต์ที่อยู่ในระบบเครือข่าย ทางผู้วิจัยจึงได้นำโปรแกรมดังกล่าวมาปรับใช้ในงานวิจัยโดยจะใช้ข้อมูลด้านฮาร์ดแวร์ที่ได้จากโปรแกรมมาตรวจสอบสถานะของโฮสต์ เพื่อนำมากำหนดค่าให้กับพารามิเตอร์ โดยผู้วิจัยได้สร้างฐานข้อมูลจัดเก็บข้อมูลทางด้านฮาร์ดแวร์แยกจากฐานข้อมูลของโปรแกรม OCS Inventory เพื่อป้องกันไม่ให้โปรแกรมทำงานผิดพลาด โครงสร้างฐานข้อมูลที่ใช้ในการจัดเก็บข้อมูลสถานะของโฮสต์แสดงในรูปที่ 3.6



รูปที่ 3.6 ER Diagram ฐานข้อมูลสถานะของโฮสต์

พจนานุกรมข้อมูลที่ใช้อธิบายของ ER Diagram ซึ่งเป็นโมเดลฐานข้อมูลที่ใช้รองรับข้อมูลสถานะของโฮสต์ แสดงดังต่อไปนี้

ตารางที่ 3.5 รายละเอียดการจัดเก็บข้อมูลตาราง Host

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
HostId	Int(Autonumber)	Primary Key	รหัสของโฮสต์
IpAddress	Char(30)		ที่อยู่ไอพีของโฮสต์

MacAddress	Char(45)		ที่อยู่ MAC การ์ดสื่อสารของโฮสต์
HostDetail	Char(250)		รายละเอียดของโฮสต์
OSId	Char(5)	Foreign Key	รหัสของ OS
ZoneId	Char(5)	Foreign Key	รหัสของโซน
CPUId	Char(5)	Foreign Key	รหัส CPU

ตารางที่ 3.6 รายละเอียดการจัดเก็บข้อมูลตาราง Port

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
PortNumber	Char(10)	Primary Key	เลขที่พอร์ต
PortDetail	Char(250)		รายละเอียดของเลขที่พอร์ต

ตารางที่ 3.7 รายละเอียดการจัดเก็บข้อมูลตาราง Zone

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
ZoneId	Int(Autonumber)	Primary Key	รหัสของโซน
ZoneName	Char(30)		ชื่อโซน
ZoneDetail	Char(100)		รายละเอียดของโซน

ตารางที่ 3.8 รายละเอียดการจัดเก็บข้อมูลตาราง HostStatus

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
UpdateId	Int(Autonumber)	Primary Key	เลขที่การอัพเดพ
TimeUpdate	Date/Time		เวลาที่อัพเดท
DateUpdate	Date/Time		วันที่อัพเดท
RamStatus	Char(30)		สถานะของ Ram (หน่วยความจำที่ใช้งาน)
HDStatus	Char(30)		สถานะของ Harddisk (เนื้อที่เหลือ)
CPUStatus	Char(30)		สถานะของ CPU (% CPU ที่ใช้งาน)
HostId	Int	Foreign Key	รหัสของโฮสต์

ตารางที่ 3.9 รายละเอียดการจัดเก็บข้อมูลตาราง IntitalRam

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
Ramid	Char(5)	Primary Key	รหัสของ Ram
HostId	Int	Primary Key	รหัสของโฮสต์
Amount	Int		จำนวน Ram
Bus	Char(10)		ความเร็วบัส

Size	Int		ขนาดความจุของ Ram

ตารางที่ 3.10 รายละเอียดการจัดเก็บข้อมูลตาราง IntitalHarddisk

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
HostId	Int	Primary Key	รหัสของโฮสต์
HDdetail	Char(5)	Primary Key	รหัสของ Harddisk
Size	Int		ความจุของ Harddisk
Amount	Int		จำนวนของ Harddisk

ตารางที่ 3.11 รายละเอียดการจัดเก็บข้อมูลตาราง IntitalPort

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
HostId	Int	Primary Key	รหัสของโฮสต์
PortNumber	Char(10)	Primary Key	เลขที่พอร์ต
Protocol	Char(10)		โปรโตคอลที่ใช้งาน

ตารางที่ 3.12 รายละเอียดการจัดเก็บข้อมูลตาราง RamType

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
RamId	Int(Autonumber)	Primary Key	รหัสของ Ram
RamDetail	Char(100)		รายละเอียด Ram
RamBrand	Char(50)		ยี่ห้อของ Ram

ตารางที่ 3.13 รายละเอียดการจัดเก็บข้อมูลตาราง CPUType

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
CPUId	Int(Autonumber)	Primary Key	รหัสของ CPU
Cpudetail	Char(100)		รายละเอียดของ CPU
Cpuspeed	Int		ความเร็วของ CPU

ตารางที่ 3.14 รายละเอียดการจัดเก็บข้อมูลตาราง HarddiskType

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
HDId	Int(Autonumber)	Primary Key	รหัสของ Harddisk
HDDetail	Char(250)		รายละเอียดของ Harddisk
HDBrand	Char(50)		ยี่ห้อของ Harddisk

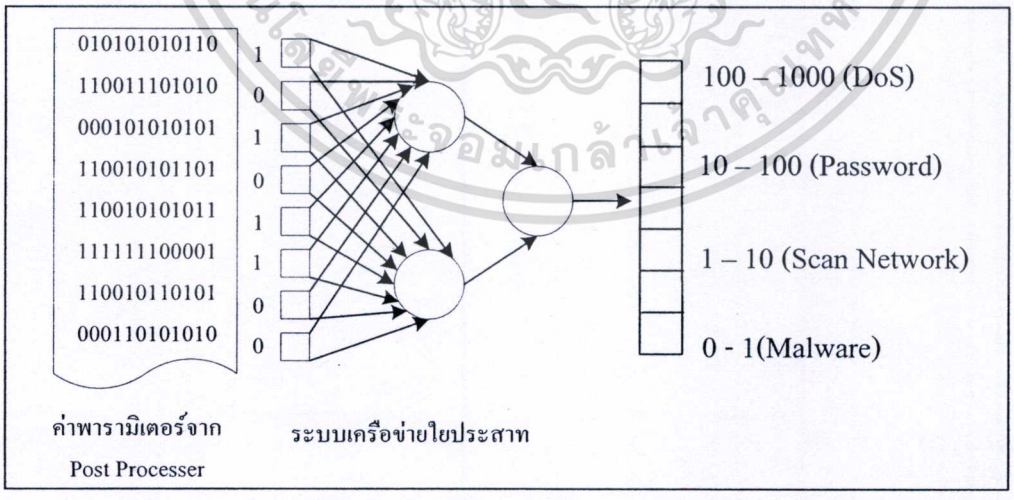
ตารางที่ 3.15 รายละเอียดการจัดเก็บข้อมูลตาราง OSType

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
OSId	Int(Autonumber)	Primary Key	รหัสของ OS
Osdetail	Char(250)		รายละเอียดของ OS

3.5 การประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต [8], [9], [10] และ [11]

การแจ้งเตือนของโปรแกรมสนอร์ตจะถูกจำแนกประเภทการบุกรุกระบบเครือข่าย และประเมินระดับค่าบ่งชี้ประเภทการบุกรุกด้วยระบบเครือข่ายใยประสาท ระบบเครือข่ายใยประสาทจะมีโครงสร้างชนิดที่ส่งสัญญาณไปข้างหน้า (Feed Forward) เมื่อโมดูล Preparation ได้จัดเตรียมข้อมูลที่เกี่ยวข้องให้โมดูล Post Processer กำหนดค่าพารามิเตอร์ทั้ง 24 พารามิเตอร์ ชุดค่าพารามิเตอร์จะถูกส่งต่อไปยังระบบเครือข่ายใยประสาทซึ่งผลลัพธ์ที่ได้จะเป็นประเภทการบุกรุกระบบเครือข่าย และระดับค่าบ่งชี้ประเภทการบุกรุกจะมีค่าอยู่ระหว่าง 0 – 1,000 โดยขั้นตอนการทำงานของโมดูล Artificial Neural Network แสดงรูปที่ 3.7

การฝึกระบบเครือข่ายใยประสาทให้มีความสามารถในการจำแนกประเภทการบุกรุกระบบเครือข่าย และประเมินระดับค่าบ่งชี้การแจ้งเตือนนั้นผู้วิจัยได้จัดเตรียมชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้ (Training Set) จำนวน 1,500 ระเบียน สำหรับประเภทการบุกรุกระบบเครือข่ายแต่ละประเภท และฝึกจนระบบเครือข่ายใยประสาทมีค่า RMSE Ratio น้อยกว่าหรือเท่ากับค่าที่กำหนด (0) หรือฝึกจนครบรอบจำนวนครั้งที่กำหนดสูงสุด (Maximum Epoch)



รูปที่ 3.7 การประเมินคุณภาพการแจ้งเตือนของ Artificial Neural Network

คุณสมบัติของระบบเครือข่ายใยประสาท คือ ความสามารถในการเรียนรู้จากตัวอย่างโดยพยายามคำนวณหาความสัมพันธ์ระหว่างข้อมูลนำเข้าและผลลัพธ์ การเรียนรู้นี้จะเริ่มจากการสุ่มค่าน้ำหนัก (Weight) และค่าเบี่ยงเบนเริ่มต้น (Bias) ค่าผลลัพธ์ที่ได้จากค่าเริ่มต้นจะถูกนำมา

เปรียบเทียบกับผลลัพธ์จริง ค่าที่แตกต่างจะถูกนำมาปรับค่าน้ำหนักและค่าเบี่ยงเบนโดยวิธีลองผิดลองถูก (Trial and Error) จนได้ผลลัพธ์ที่ใกล้เคียงหรือตรงกับผลลัพธ์จริง ค่าน้ำหนักและค่าเบี่ยงเบนสุดท้ายจะถูกนำมาใช้ในการพยากรณ์ผลลัพธ์ที่เกิดขึ้นจากข้อมูลนำเข้าชุดใหม่

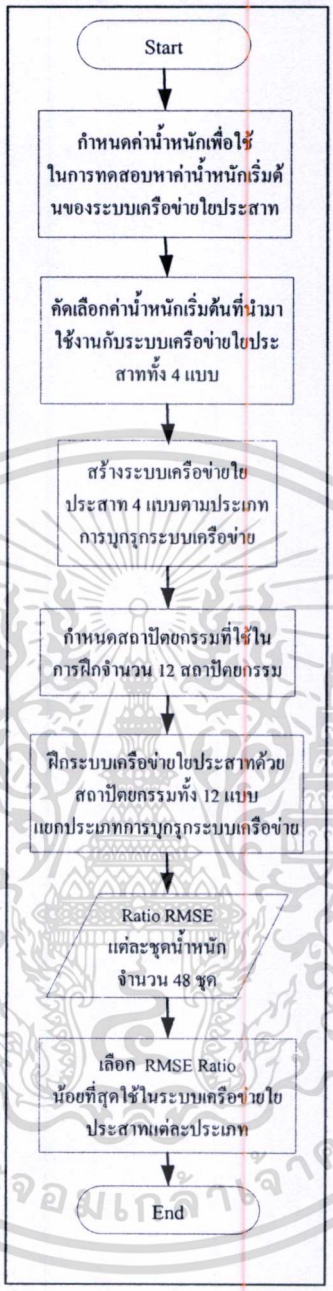
จากการศึกษาระบบเครือข่ายใยประสาท ซึ่งได้ทดสอบความสัมพันธ์ด้วยการกำหนดจำนวนหน่วย (Node) ของชั้นรับข้อมูล (Layer) ชั้นฮิดเดน (Hidden Layer) และชั้นแสดงผล (Output Layer) รวมถึงจำนวนรอบของการคำนวณที่มีโครงสร้างและมีจำนวนรอบการทำงานต่างกัน ซึ่งทั้งหมดได้ประกอบขึ้นเป็นระบบเครือข่ายใยประสาท โดยสถาปัตยกรรมของระบบเครือข่ายใยประสาทที่มีความเหมาะสมในการทำงาน (Optimum ANN) จะขึ้นอยู่กับปัญหาที่นำมาวิเคราะห์ในกระบวนการออกแบบสถาปัตยกรรมของระบบเครือข่ายใยประสาทที่เหมาะสมของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ผู้วิจัยได้แบ่งข้อมูลออกเป็น 2 ชุดคือ

(1) ชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้ (Training Set)

(2) ชุดข้อมูลที่ใช้ในกระบวนการทดสอบ (Testing Set)

3.5.1 การจัดเตรียมชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้

กระบวนการเรียนรู้ของระบบเครือข่ายใยประสาทในขั้นตอนแรกจะเป็นการกำหนดค่าชุดน้ำหนักเริ่มต้นจำนวน 5 ชุดดังตารางที่ 3.20 ตารางที่ 3.21 ตารางที่ 3.22 และตารางที่ 3.2 ให้กับระบบเครือข่ายใยประสาทโดยแบ่งตามประเภทการบุกรุกระบบเครือข่ายทั้ง 4 แบบ จัดสร้างระบบเครือข่ายใยประสาทจำนวน 4 แบบอันประกอบด้วย ระบบเครือข่ายใยประสาทที่ใช้ตรวจจับการบุกรุกแบบ DoS (NN DoS) ระบบเครือข่ายใยประสาทที่ใช้ตรวจจับการบุกรุกโดยพยายามค้นหารหัสผ่าน (NN Password) ระบบเครือข่ายใยประสาทที่ใช้ตรวจจับการบุกรุกแบบสแกนระบบเครือข่าย (NN Scan) และระบบเครือข่ายใยประสาทที่ใช้ตรวจจับการบุกรุกโดยมัลแวร์ (NN Malware) ฝึกระบบเครือข่ายใยประสาททั้ง 4 แบบตามสถาปัตยกรรมที่กำหนดทั้ง 12 สถาปัตยกรรม และคัดเลือกสถาปัตยกรรมที่มีค่า Ratio RMSE น้อยที่สุดมาใช้งานกับระบบเครือข่ายใยประสาททั้ง 4 แบบโดยกระบวนการฝึกระบบเครือข่ายใยประสาทแสดงในรูปที่ 3.8



รูปที่ 3.8 ขั้นตอนการฝึกระบบเครือข่ายที่นำมาใช้งาน

การจัดเตรียมชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้มีขั้นตอนการทำงานอยู่สองขั้นตอนคือ ขั้นตอนแรกการแบ่งกลุ่มชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้ และขั้นตอนสองเป็นการกำหนดค่าน้ำหนักให้กับพารามิเตอร์โดยค่าน้ำหนักทั้งหมดจะถูกนำมาเปรียบเทียบกับคุณภาพการแจ้งเตือนที่ได้จากระบบเครือข่ายใยประสาท

- ขั้นตอนการแบ่งกลุ่มชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้

ประเภทการบุกรุกระบบเครือข่ายสามารถจำแนกประเภทได้เป็น 4 ประเภท ซึ่งรายละเอียดได้กล่าวในหัวข้อที่ 2.12 วิธีการบุกรุกระบบเครือข่ายที่แตกต่างกันย่อมส่งผลกระทบที่

แตกต่างกันออกไปด้วยเช่นกัน ทำให้การจัดเตรียมชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้จำเป็นต้องแยกชุดข้อมูลที่ใช้ในการะบวนการเรียนรู้ออกเป็นกลุ่มตามประเภทการบุกรุกระบบเครือข่าย ชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้ทั้ง 4 แบบได้แสดงในตารางที่ 3.16

ตารางที่ 3.16 ชุดข้อมูลที่ใช้ในกระบวนการเรียนรู้ของระบบเครือข่ายใยประสาท

ชุดข้อมูลแพ็คเก็จที่ได้จากการบุกรุก	รายละเอียด	จำนวนระเบียน
ตรวจสอบการโจมตี DoS	สำหรับตรวจจับการบุกรุกแบบ DoS ทั้งการโจมตีด้วยโปรโตคอล ICMP หรือ TCP	1500
ตรวจสอบการโจมตี Password	สำหรับตรวจจับการบุกรุกที่เกี่ยวข้องกับรหัสผ่านทั้งที่เป็นการบุกรุกแบบ Remote to user attack และ U2R	1500
ตรวจสอบการโจมตี Scan	สำหรับตรวจจับการบุกรุกที่เป็นการหาข้อมูลเหยื่อไม่ว่าจะเป็นช่องโหว่ของระบบปฏิบัติการ หรือพอร์ตที่ใช้งาน	1500
ตรวจสอบการโจมตี Malware	สำหรับตรวจจับตรวจจับการบุกรุกของไวรัส เวิร์ม มัลแวร์ และ สปายแวร์	1500

ชุดข้อมูลแพ็คเก็จที่ใช้ในกระบวนการเรียนรู้ของระบบเครือข่ายใยประสาทได้ถูกแบ่งออกเป็น 4 กลุ่มตามประเภทการบุกรุกระบบเครือข่าย ซึ่งในแต่ละประเภทการบุกรุกมีความสัมพันธ์กับพารามิเตอร์แสดงในตารางที่ 3.17

ตารางที่ 3.17 การแบ่งพารามิเตอร์ตามประเภทชุดข้อมูลในกระบวนการเรียนรู้

พารามิเตอร์	ชื่อพารามิเตอร์	ชุดข้อมูล DoS	ชุดข้อมูล Password	ชุดข้อมูล Scan	ชุดข้อมูล Malware
P1	Correctness	Y	Y	Y	Y
P2	Host_OS_Vulnerability	Y	-	Y	-
P3	Host_Port_Vulnerability	Y	-	Y	-
P4	Host_App_Vulnerability	Y	-	Y	-
P5	Host _Memory_Status	Y	-	-	-
P6	Host_CPU_Status	Y	-	-	-
P7	Host_AV_Installation	-	-	-	Y
P8	Host_AV_Uptodate	-	-	-	Y
P9	Host_Permission_Control	Y	Y	Y	Y
P10	IDS_Rule_Reliability	Y	Y	Y	Y
P11	IDS_Rule_ Sensitivity	Y	Y	Y	Y

P12	IDS_OS_Vulnerability	Y	Y	Y	Y
P13	IDS_Version_Uptodate	Y	Y	Y	Y
P14	Firewall_Availiability	Y	Y	Y	-
P15	Firewall_OS_Vulnerability	Y	Y	Y	-
P16	Firewall_Version_Uptodate	Y	Y	Y	-
P17	Firewall_URL_Filtering	Y	Y	Y	-
P18	Firewall_URL_Uptodate	Y	Y	Y	-
P19	Security_Policy	Y	Y	Y	Y
P20	Username_Pattern	-	Y	-	-
P21	Password_ Complexility	-	Y	-	-
P22	Password_Expiration	-	Y	-	-
P23	Username_Systematic	-	Y	-	-
P24	External_Drive_Control	Y	Y	Y	Y

* ให้ Y แสดงพารามิเตอร์ที่พิจารณาให้เป็นชุดข้อมูลในกระบวนการเรียนรู้

จากตารางที่ 3.17 แสดงให้เห็นว่าชุดข้อมูลในกระบวนการเรียนรู้ได้มีการใช้งานค่าพารามิเตอร์ร่วมกัน และมีพารามิเตอร์บางตัวมีความสัมพันธ์กับการบุกรุกระบบเครือข่ายเพียงรูปแบบเดียวเท่านั้นตัวอย่าง พารามิเตอร์ P7 และ P8 มีความสัมพันธ์เฉพาะการบุกรุกระบบเครือข่ายด้วยมัลแวร์ ส่วน P1, P9, P10, P11, P12, P13, P19 และ P24 มีความสัมพันธ์กับการบุกรุกระบบเครือข่ายทุกรูปแบบ

- การกำหนดน้ำหนักให้กับพารามิเตอร์

ค่าน้ำหนักที่กำหนดให้กับพารามิเตอร์ในชุดข้อมูลในกระบวนการเรียนรู้จะถูกนำมาเปรียบเทียบกับคุณภาพการแจ้งเตือนที่ได้จากระบบเครือข่ายใยประสาท ค่าน้ำหนักที่เหมาะสมที่สุดจะนำมาใช้ในชุดข้อมูลสำหรับการเรียนรู้ที่ได้ถูกกำหนดขึ้น โดยค่าน้ำหนักที่เหมาะสมที่สุดหาได้โดยใช้หลักเกณฑ์ดังนี้

1. พารามิเตอร์ที่สัมพันธ์กับการบุกรุกระบบเครือข่ายหลายรูปแบบจะกำหนดให้มีค่าน้ำหนักน้อยกว่าพารามิเตอร์ที่สัมพันธ์กับการบุกรุกระบบเครือข่ายเพียงรูปแบบเดียว
2. พารามิเตอร์ Correctness จะมีความสำคัญมากที่สุด เนื่องจากพารามิเตอร์ Correctness สามารถใช้ตรวจสอบเบื้องต้นว่าการแจ้งเตือนที่เกิดขึ้นเป็นการแจ้งเตือนที่ถูกต้องหรือการแจ้งเตือนที่ผิดพลาด
3. กำหนดตามความสำคัญของพารามิเตอร์ตามกลุ่มชุดข้อมูลในกระบวนการเรียนรู้ แสดงในตารางที่ 3.21 โดยค่าพารามิเตอร์ที่มีค่าลำดับความสำคัญ (Priority) เท่ากับ 1

มีความสำคัญสูงสุด ลำดับความสำคัญของพารามิเตอร์จะนำมาใช้เปรียบเทียบเมื่อพารามิเตอร์มีความสัมพันธ์กับรูปแบบการบุกรุกระบบเครือข่ายที่เท่ากัน

ตารางที่ 3.18 ค่าลำดับความสำคัญของพาราเมิเตอร์ในชุดข้อมูลในกระบวนการเรียนรู้

พารามิเตอร์	ชื่อพารามิเตอร์	ชุดข้อมูล DoS	ชุดข้อมูล Password	ชุดข้อมูล Scan	ชุดข้อมูล Malware
P1	Correctness	1	1	1	1
P2	Host_OS_Vulnerability	4	-	2	-
P3	Host_Port_Vulnerability	5	-	3	-
P4	Host_App_Vulnerability	6	-	4	-
P5	Host _Memory_Status	2	-	-	-
P6	Host_CPU_Status	3	-	-	-
P7	Host_AV_Installation	-	-	-	2
P8	Host_AV_Uptodate	-	-	-	3
P9	Host_Permission_Control	15	14	13	4
P10	IDS_Rule_Reliability	12	11	10	7
P11	IDS_Rule_ Sensitivity	13	12	11	8
P12	IDS_OS_Vulnerability	14	13	12	9
P13	IDS_Version_Uptodate	18	17	16	10
P14	Firewall_Availiability	7	6	5	-
P15	Firewall_OS_Vulnerability	10	9	8	-
P16	Firewall_Version_Uptodate	11	10	9	-
P17	Firewall_URL_Filtering	8	7	6	-
P18	Firewall_URL_Uptodate	9	8	7	-
P19	Security_Policy	16	15	14	6
P20	Username_Pattern	-	5	-	-
P21	Password_ Complexility	-	2	-	-
P22	Password_Expiration	-	3	-	-
P23	Username_Systematic	-	4	-	-
P24	External_Drive_Control	17	16	15	5

การกำหนดค่าน้ำหนักให้กับพารามิเตอร์ในแต่ละกลุ่ม ค่าน้ำหนักจะถูกแบ่งออกเป็นช่วงกว้าง ๆ เพื่อให้ระบบเครือข่ายใยประสาทสามารถจำแนกประเภทการบุกรุกระบบเครือข่ายได้ โดยการกำหนดระดับให้กับค่าน้ำหนักของชุดข้อมูลได้แสดงในตารางที่ 3.19

ตารางที่ 3.19 การแบ่งระดับค่าน้ำหนักเริ่มต้นที่ใช้ในชุดข้อมูลกระบวนการเรียนรู้ตามประเภทการบุกรุกระบบเครือข่าย

ชุดข้อมูลกระบวนการเรียนรู้	ช่วงค่าน้ำหนัก
ตรวจสอบการโจมตี DoS	100 - 1000
ตรวจสอบการโจมตี Password	10 - 100
ตรวจสอบการโจมตี Scan	1 - 10
ตรวจสอบการโจมตี Malware	0 - 1

ค่าน้ำหนักจะถูกนำมาใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทให้มีความเชี่ยวชาญในการจำแนกประเภทการบุกรุกระบบเครือข่ายและประเมินระดับค่าบ่งชี้ประเภทการบุกรุก ค่าน้ำหนักจะถูกทดสอบกับระบบเครือข่ายใยประสาทที่มีสถาปัตยกรรมชั้นแฝง 1 ชั้น และมี 10 หน่วย ค่าน้ำหนักที่มีค่า RMSE Ratio น้อยที่สุดในแต่ละประเภทการบุกรุกจะถูกใช้เป็นค่าน้ำหนักเริ่มต้นในฝึกระบบเครือข่ายใยประสาทแต่ละประเภท ผู้วิจัยได้เลือกใช้ค่าน้ำหนักที่นำมาทดสอบจำนวน 5 ชุดในแต่ละละเภทการบุกรุกระบบเครือข่าย โดยเกณฑ์การกำหนดค่าน้ำหนักได้อธิบายในหัวข้อที่ผ่านมา

ค่าน้ำหนักทั้ง 5 ชุดที่นำมาใช้ในการทดสอบเพื่อใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทในแต่ละประเภทการบุกรุกระบบเครือข่ายได้แสดงในตารางที่ 3.20, ตารางที่ 3.21, ตารางที่ 3.22 และตารางที่ 3.23

ตารางที่ 3.20 ชุดค่าน้ำหนักจำนวน 5 ชุดที่ใช้ในการตรวจสอบการโจมตี DoS

พารามิเตอร์	ชื่อพารามิเตอร์	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
P1	Correctness	1	1	1	1	1
P2	Host_OS_Vulnerability	90.8	142.2	98.6	86.3	74
P3	Host_Port_Vulnerability	85.6	130.7	90.1	85.9	69
P4	Host_App_Vulnerability	82.4	120.3	84.2	76.4	61
P5	Host _Memory_Status	195.2	145.2	273.1	212.8	165
P6	Host_CPU_Status	192.4	135.3	218.3	183.4	159
P9	Host_Permission_Control	20.5	15.2	8.2	16.2	33

P10	IDS_Rule_Reliability	28.5	19.1	11.8	19.2	41
P11	IDS_Rule_ Sensitivity	28.1	17.2	10.3	18.4	37
P12	IDS_OS_Vulnerability	21.1	15.4	9.4	17.7	35
P13	IDS_Version_Uptodate	14.7	13.9	3.8	13.9	22
P14	Firewall_Availiability	52.4	82.1	46.2	52.3	57
P15	Firewall_OS_Vulnerability	32.2	24.5	31.1	45.7	47
P16	Firewall_Version_Uptodate	30.1	22.3	29.9	42.1	43
P17	Firewall_URL_Filtering	50.9	55.2	40.1	51.3	52
P18	Firewall_URL_Uptodate	44.2	32.1	31.9	49.2	50
P19	Security_Policy	15.8	14.9	7.3	15	30
P24	External_Drive_Control	15.1	14.4	5.7	14.2	25

ตารางที่ 3.21 ชุดค่าน้ำหนักจำนวน 5 ชุดที่ใช้ในการตรวจสอบการพยายามค้นหารหัสผ่าน

พารามิเตอร์	**ชื่อพารามิเตอร์**	**ชุดที่ 1**	**ชุดที่ 2**	**ชุดที่ 3**	**ชุดที่ 4**	**ชุดที่ 5**
P1	Correctness	1	1	1	1	1
P9	Host_Permission_Control	1.95	1.17	0.71	0.9	1.5
P10	IDS_Rule_Reliability	3.21	1.74	1.05	1.37	2.2
P11	IDS_Rule_ Sensitivity	3.15	1.52	0.95	1.23	1.9
P12	IDS_OS_Vulnerability	2.94	1.33	0.87	0.97	1.8
P13	IDS_Version_Uptodate	1.59	0.87	0.24	0.71	0.9
P14	Firewall_Availiability	7.45	7.25	7.58	8.24	9.5
P15	Firewall_OS_Vulnerability	5.94	3.99	5.92	4.38	4.3
P16	Firewall_Version_Uptodate	4.01	2.83	4.59	2.74	3.2
P17	Firewall_URL_Filtering	7.11	5.27	7.44	5.31	8.5
P18	Firewall_URL_Uptodate	6.84	5.21	6.01	4.99	5.2
P19	Security_Policy	1.89	1.01	0.53	0.95	1.1
P20	Username_Pattern	12.01	13.21	10.01	14.73	13.9
P21	Password_ Complexility	13.85	18.11	18.99	19.35	15.7
P22	Password_Expiration	13.69	17.62	17.97	17.31	14.9
P23	Username_Systematic	12.74	17.89	16.82	16.01	14.4
P24	External_Drive_Control	1.63	0.98	0.32	0.81	1

ตารางที่ 3.22 ชุดค่าน้ำหนักจำนวน 5 ชุดที่ใช้ในการตรวจสอบการสแกนระบบเครือข่าย

พารามิเตอร์	ชื่อพารามิเตอร์	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
P1	Correctness	1	1	1	1	1
P2	Host_OS_Vulnerability	1.784	1.874	1.778	1.834	1.93
P3	Host_Port_Vulnerability	1.705	1.796	1.696	1.823	1.61
P4	Host_App_Vulnerability	1.698	1.627	1.677	1.602	1.57
P9	Host_Permission_Control	0.199	0.234	0.175	0.215	0.18
P10	IDS_Rule_Reliability	0.255	0.278	0.226	0.243	0.32
P11	IDS_Rule_ Sensitivity	0.239	0.261	0.213	0.237	0.29
P12	IDS_OS_Vulnerability	0.234	0.254	0.187	0.219	0.25
P13	IDS_Version_Uptodate	0.177	0.132	0.092	0.096	0.13
P14	Firewall_Availiability	0.787	0.843	1.092	1.005	0.85
P15	Firewall_OS_Vulnerability	0.617	0.531	0.521	0.522	0.6
P16	Firewall_Version_Uptodate	0.511	0.449	0.331	0.499	0.51
P17	Firewall_URL_Filtering	0.772	0.823	1.003	0.746	0.75
P18	Firewall_URL_Uptodate	0.651	0.545	0.781	0.632	0.69
P19	Security_Policy	0.189	0.201	0.121	0.192	0.17
P24	External_Drive_Control	0.182	0.152	0.107	0.135	0.15

ตารางที่ 3.23 ชุดค่าน้ำหนักจำนวน 5 ชุดที่ใช้ในการตรวจสอบการบุกรุกระบบเครือข่ายด้วย-มัลแวร์

พารามิเตอร์	ชื่อพารามิเตอร์	ชุดที่ 1	ชุดที่ 2	ชุดที่ 3	ชุดที่ 4	ชุดที่ 5
P1	Correctness	1	1	1	1	1
P7	Host_AV_Installation	0.3299	0.4307	0.3017	0.4571	0.32
P8	Host_AV_Uptodate	0.2988	0.3292	0.3002	0.4229	0.306
P9	Host_Permission_Control	0.0784	0.0534	0.0726	0.0248	0.095
P10	IDS_Rule_Reliability	0.0766	0.0338	0.0503	0.0237	0.051
P11	IDS_Rule_ Sensitivity	0.0568	0.0272	0.0483	0.0183	0.032
P12	IDS_OS_Vulnerability	0.0459	0.0205	0.0481	0.0154	0.022
P13	IDS_Version_Uptodate	0.0412	0.0196	0.0469	0.0133	0.018

P19	Security_Policy	0.0401	0.0375	0.061	0.013	0.074
P24	External_Drive_Control	0.0323	0.0481	0.0709	0.0115	0.082

กระบวนการเรียนรู้และกระบวนการทดสอบนี้ได้ทดลองใช้สถาปัตยกรรมของระบบเครือข่ายใยประสาทจำนวน 48 แบบ โดยแต่ละแบบจะมีจำนวนหน่วยในชั้นแฝง จำนวนชั้นแฝง และชุดของค่าน้ำหนักที่แตกต่างกันดังแสดงในตารางที่ 3.24

ตารางที่ 3.24 สถาปัตยกรรมของระบบเครือข่ายใยประสาทที่ใช้ในการทดลอง

แบบที่	สถาปัตยกรรมระบบเครือข่ายใยประสาท	ชุดค่าน้ำหนัก
1	ชั้นแฝง 1 ชั้น มี 10 หน่วย	ชุดข้อมูล DoS
2	ชั้นแฝง 1 ชั้น มี 15 หน่วย	ชุดข้อมูล DoS
3	ชั้นแฝง 1 ชั้น มี 20 หน่วย	ชุดข้อมูล DoS
4	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล DoS
5	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล DoS
6	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล DoS
7	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล DoS
8	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล DoS
9	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล DoS
10	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล DoS
11	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล DoS
12	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล DoS
13	ชั้นแฝง 1 ชั้น มี 10 หน่วย	ชุดข้อมูล Password
14	ชั้นแฝง 1 ชั้น มี 15 หน่วย	ชุดข้อมูล Password
15	ชั้นแฝง 1 ชั้น มี 20 หน่วย	ชุดข้อมูล Password
16	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Password
17	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Password
18	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Password
19	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Password
20	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Password
21	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Password
22	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Password
23	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Password
24	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Password

25	ชั้นแฝง 1 ชั้น มี 10 หน่วย	ชุดข้อมูล Scan
26	ชั้นแฝง 1 ชั้น มี 15 หน่วย	ชุดข้อมูล Scan
27	ชั้นแฝง 1 ชั้น มี 20 หน่วย	ชุดข้อมูล Scan
28	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Scan
29	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Scan
30	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Scan
31	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Scan
32	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Scan
33	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Scan
34	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Scan
35	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Scan
36	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Scan
37	ชั้นแฝง 1 ชั้น มี 10 หน่วย	ชุดข้อมูล Malware
38	ชั้นแฝง 1 ชั้น มี 15 หน่วย	ชุดข้อมูล Malware
39	ชั้นแฝง 1 ชั้น มี 20 หน่วย	ชุดข้อมูล Malware
40	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Malware
41	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Malware
42	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Malware
43	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Malware
44	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Malware
45	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Malware
46	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	ชุดข้อมูล Malware
47	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	ชุดข้อมูล Malware
48	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	ชุดข้อมูล Malware

ข้อมูลที่ใช้ในกระบวนการเรียนรู้จะถูกนำมาป้อนให้กับระบบเครือข่ายใยประสาททั้ง 48 แบบเพื่อคำนวณหาความสัมพันธ์ระหว่างพารามิเตอร์ที่เป็นข้อมูลนำเข้ากับค่าระดับคุณภาพการแจ้งเตือน โดยค่าความสัมพันธ์จะอยู่ในค่าน้ำหนักและค่าเบี่ยงเบนดังที่ได้กล่าวแล้วข้างต้น ค่าดังกล่าวจะถูกนำมาใช้ในกระบวนการทดสอบเพื่อหาคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตและสถาปัตยกรรมที่สามารถพยากรณ์ได้ถูกต้องแม่นยำที่สุดโดยพิจารณาจากค่า Root Mean Square Error (RMSE) Ratio ซึ่งสามารถหาได้ด้วยสมการที่ 3.1

$$\text{RMSE Ratio} = \frac{\sqrt{\frac{\sum_{i=1}^{N}(x_i - t_j)^2}{N}}}{t_j} \qquad (3.1)$$

N คือ จำนวนชุดข้อมูลการแจ้งเตือนที่นำมาใช้ในกระบวนการฝึกสอน

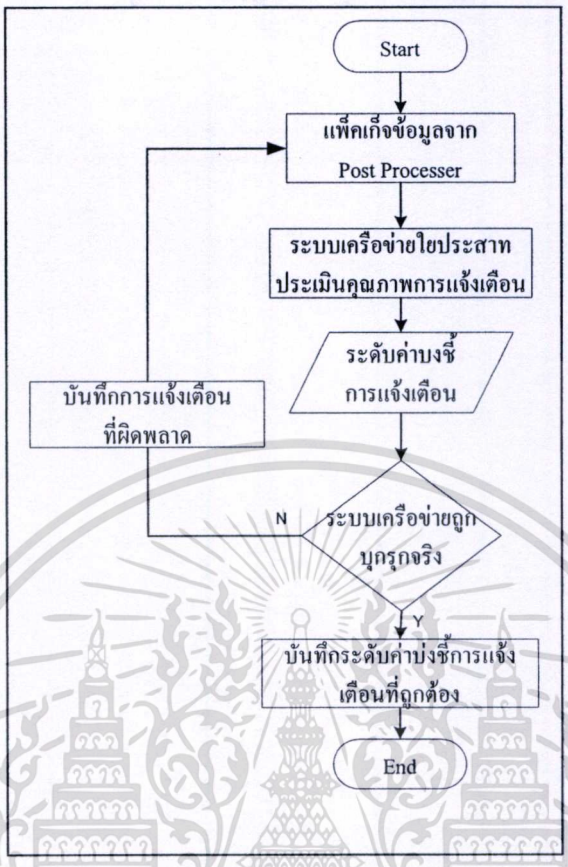
x_i คือ ค่าบ่งชี้ประเภทการแจ้งเตือนที่ i โดย i = {1,2,3…N} ที่ได้ขากระบบเครือข่ายใยประสาท

t_j คือ ค่าบ่งชี้ประเภทการแจ้งเตือนที่ได้จากสมมุติฐานโดย j = {DoS = 1000, Password = 100, Scan = 10 และ Malware = 1}

3.5.2 การจัดเตรียมชุดข้อมูลที่ใช้ในกระบวนการทดสอบ

โมดูล Artificial Neural Network จะประกอบไปด้วยระบบเครือข่ายใยประสาทจำนวน 4 สถาปัตยกรรม คือ ระบบเครือข่ายใยประสาทใช้ในการประเมินคุณภาพการแจ้งเตือนแบบ Dos ระบบเครือข่ายใยประสาทใช้ในการประเมินคุณภาพการแจ้งเตือนที่เป็นการพยายามเข้าใช้งานเกินสิทธิ์ที่ได้รับอนุญาต ระบบเครือข่ายใยประสาทใช้ในการประเมินคุณภาพการแจ้งเตือนที่เป็นการบุกรุกแบบสแกนระบบเครือข่าย และระบบเครือข่ายใยประสาทใช้ในการประเมินคุณภาพการแจ้งเตือนที่เป็นการบุกรุกของมัลแวร์ โดยระบบเครือข่ายใยประสาทแต่ละแบบจะมีความชำนาญเฉพาะด้านในการตรวจจับการบุกรุกระบบเครือข่าย

การแจ้งเตือนที่ถูกต้องจะต้องอยู่ในเกณฑ์ของระดับค่าบ่งชี้การแจ้งเตือนที่กำหนด ผู้วิจัยจะพิจารณาค่าบ่งชี้ต่ำสุดซึ่งสามารถระบุได้ว่าเป็นการแจ้งเตือนถูกต้อง ผู้วิจัยจะนำระดับค่าบ่งชี้การแจ้งเตือนมาตรวจสอบว่าการแจ้งเตือนดังกล่าวเป็นการบุกรุกระบบเครือข่ายจริงหรือไม่ ถ้าไม่ใช่นำระดับค่าบ่งชี้การแจ้งเตือนที่มีค่าสูงกว่ามาตรวจสอบใหม่ จนกว่าค่าระดับค่าบ่งชี้การแจ้งเตือนที่นำมาตรวจสอบจะเป็นการแจ้งเตือนที่ถูกต้อง ขั้นตอนการกำหนดเกณฑ์การแจ้งเตือนที่ถูกต้องมีขั้นตอนแสดงในรูปที่ 3.9



รูปที่ 3.9 ขั้นตอนการกำหนดเกณฑ์ระดับค่าบ่งชี้การแจ้งเตือนที่ถูกต้อง

เกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้องของการบุกรุกระบบเครือข่ายแต่ละประเภทแสดงใน ตารางที่ 3.25

ตารางที่ 3.25 การกำหนดค่าการแจ้งเตือนที่ถูกต้อง

ระบบเครือข่ายแต่ละประเภท	เกณฑ์การแจ้งเตือน ที่ถูกต้อง
ระบบเครือข่ายใยประสาท DoS	780 - 1000
ระบบเครือข่ายใยประสาท Password	75 - 100
ระบบเครือข่ายใยประสาท Scan Network	8 - 10
ระบบเครือข่ายใยประสาท Malware	0.8 - 1

เมื่อแพ็คเก็จข้อมูลถูกส่งมาจากโมดูล Post Processer ระบบจะทำการตรวจสอบค่าพารามิเตอร์ Correctness ถ้ามีค่าเท่ากับ 0 ระบบจะสรุปทันทีว่าการแจ้งเตือนดังกล่าวเป็นการ

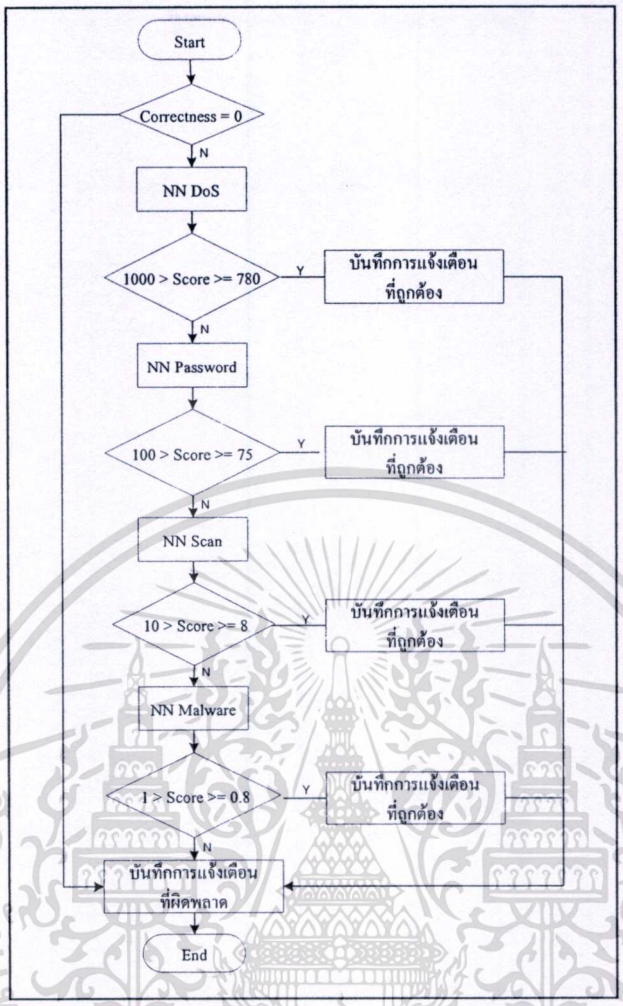
แจ้งเตือนที่ผิดพลาด ถ้าค่าพารามิเตอร์ Correctness มีค่าเท่ากับ 1 ชุดแพ็คเก็จข้อมูลจะถูกส่งไปตรวจสอบคุณภาพข้อมูลที่โมดูล

- ระบบเครือข่ายใยประสาทใช้ในการประเมินระดับค่าบ่งชี้การแจ้งเตือนแบบ Dos (NN Dos) หากค่าดังกล่าวมีค่าระหว่าง 780 - 1000 ระบบจะสรุปว่าเป็นการแจ้งเตือนที่ถูกต้อง ประเภทการบุกรุกระบบเครือข่ายแบบ DoS ถ้าไม่ใช่ แพ็คเก็จข้อมูลจะถูกส่งไปตรวจสอบค่าระดับค่าบ่งชี้การแจ้งเตือนด้วยระบบเครือข่ายใยประสาท NN Password
- ระบบเครือข่ายใยประสาทใช้ในการประเมินระดับค่าบ่งชี้การแจ้งเตือนที่เป็นการพยายามเข้าใช้งานเกินสิทธิ์ที่ได้รับอนุญาต (NN Password) หากค่าดังกล่าวมีค่าระหว่าง 75 - 100 ระบบจะสรุปว่าเป็นการแจ้งเตือนที่ถูกต้อง เป็นประเภทการบุกรุกระบบเครือข่ายแบบการพยายามเข้าใช้งานเกินสิทธิ์ที่ได้รับอนุญาต ถ้าไม่ใช่ แพ็คเก็จข้อมูลจะถูกส่งไปตรวจสอบค่าระดับค่าบ่งชี้การแจ้งเตือนด้วยระบบเครือข่ายใยประสาท NN Scan
- ระบบเครือข่ายใยประสาทใช้ในการประเมินระดับค่าบ่งชี้การแจ้งเตือนที่เป็นการบุกรุกแบบสแกนระบบเครือข่าย (NN Scan) หากค่าดังกล่าวมีค่าระหว่าง 8 – 10 ระบบจะสรุปว่าเป็นการแจ้งเตือนที่ถูกต้อง เป็นประเภทการบุกรุกระบบเครือข่ายแบบการสแกนระบบเครือข่าย ถ้าไม่ใช่ แพ็คเก็จข้อมูลจะถูกส่งไปตรวจสอบค่าระดับค่าบ่งชี้การแจ้งเตือนด้วยระบบเครือข่ายใยประสาท NN Malware
- ระบบเครือข่ายใยประสาทใช้ในการประเมินระดับค่าบ่งชี้การแจ้งเตือนที่เป็นการบุกรุกของมัลแวร์ (NN Malware) หากค่าดังกล่าวมีค่าระหว่าง 0.8 - 1 ระบบจะสรุปว่าการแจ้งเตือนดังกล่าวเป็นการแจ้งเตือนที่ถูกต้อง ประเภทการบุกรุกระบบเครือข่ายของมัลแวร์ ถ้าไม่ใช่ แพ็คเก็จข้อมูลของการแจ้งเตือนจะถูกสรุปว่าเป็นการแจ้งเตือนที่ผิดพลาด ขั้นตอนการทำงานของระบบได้แสดงในรูปที่ 3.10

ค่า RMSE Ratio ที่ได้จากการทดสอบค่าน้ำหนัก เพื่อนำมาใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทแต่ละประเภทแสดงในตารางที่ 3.26

ตารางที่ 3.26 ผลการทดสอบหาค่าน้ำหนักเริ่มต้นที่นำมาฝึกระบบเครือข่ายใยประสาท

ระบบเครือข่ายใยประสาท	ชุดค่าน้ำหนักที่ 1	ชุดค่าน้ำหนักที่ 2	ชุดค่าน้ำหนักที่ 3	ชุดค่าน้ำหนักที่ 4	ชุดค่าน้ำหนักที่ 5
ระบบเครือข่ายใยประสาท DoS	0.9584	0.2358	1.1127	0.8521	1.3568
ระบบเครือข่ายใยประสาท Password	0.0025	0.6521	0.8543	0.7561	0.1128
ระบบเครือข่ายใยประสาท Scan Network	0.0928	0.0475	0.0221	0.0858	0.7525
ระบบเครือข่ายใยประสาท Malware	0.2587	0.3598	0.4587	0..2568	0.0945



รูปที่ 3.10 ขั้นตอนการประเมินคุณภาพการแจ้งเตือนของโมดูล Artificial Neural Network

จากตารางที่ 3.26 ค่าหนักชุดที่ 2 จะถูกนำมาใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทในการประเมินระดับค่าบ่งชี้การแจ้งเตือนแบบ Dos ค่าหนักชุดที่ 1 จะถูกนำมาใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทในการประเมินระดับค่าบ่งชี้การแจ้งเตือนแบบพยายามค้นหารหัสผ่าน ค่าหนักชุดที่ 3 จะถูกนำมาใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทในการประเมินระดับค่าบ่งชี้การแจ้งเตือนแบบสแกนระบบเครือข่าย และค่าหนักชุดที่ 5 จะถูกนำมาใช้เป็นค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทในการประเมินระดับค่าบ่งชี้การแจ้งเตือนด้วยมัลแวร์

ตัวอย่างการคำนวณหาระดับค่าบ่งชี้การแจ้งเตือนของระบบเครือข่ายใยประสาท โดยสมมติชุดข้อมูลที่ถูกส่งมาจากโมดูล Post Processer คือ [110000101110110100111111] และใช้ค่าชุดน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาทแต่ละประเภท จะได้ระดับค่าบ่งชี้การแจ้งเตือนแสดงได้ดังตาราง 3.27

ตารางที่ 3.27 คุณภาพการแจ้งเตือนของระบบเครือข่ายใยประสาทแต่ละประเภทที่ใช้ชุดค่าน้ำหนักเริ่มต้นในการฝึกระบบเครือข่ายใยประสาท

ระบบเครือข่ายใยประสาทแต่ละประเภท	ช่วงค่าบ่งชี้ที่ถูกต้อง	ระดับค่าบ่งชี้การแจ้งเตือนที่คำนวณได้
ระบบเครือข่ายใยประสาท DoS	780 - 1000	573
ระบบเครือข่ายใยประสาท Password	75 - 100	87.4
ระบบเครือข่ายใยประสาท Scan Network	8 - 10	5.02
ระบบเครือข่ายใยประสาท Virus	0.8 - 1	0.711

จากตารางที่ 3.27 แสดงให้เห็นการแจ้งเตือนที่ได้จากระบบเครือข่ายใยประสาทแต่ละชนิดการแจ้งเตือนที่ได้จากระบบเครือข่ายใยประสาท Password อยู่ในเกณฑ์การแจ้งเตือนที่ถูกต้องแสดงว่าชุดแพ็คเก็จข้อมูลเป็นการแจ้งเตือนที่เกิดจากการบุกรุกระบบเครือข่ายแบบค้นหารหัสผ่านที่มีคุณภาพการแจ้งเตือน ในระดับ 87.4

คุณภาพการแจ้งเตือนที่ได้จากระบบเครือข่ายใยประสาทจะถูกจัดเก็บไว้ในตาราง Quality ซึ่งประกอบด้วยฟิลด์ข้อมูลแสดงในตารางที่ 3.28

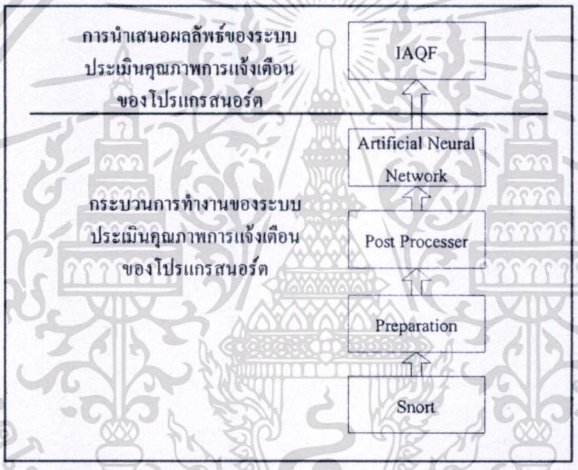
ตารางที่ 3.28 รายละเอียดการจัดเก็บข้อมูลตาราง Quality

ฟิลด์	ประเภทข้อมูล	ประเภท Key	รายละเอียด
QualityId	Int(Autonumber)	Primary Key	รหัสคุณภาพการแจ้งเตือน
RuleId	Char(10)	Foreign Key	รหัสกฎการแจ้งเตือน
QualityAlert	Char(10)		คุณภาพการแจ้งเตือน
AttackId	Char(10)	Foreign Key	รหัสประเภทการบุกรุก

3.6 ระบบนำเสนอคุณภาพการแจ้งเตือนที่เกิดขึ้น

การแจ้งเตือนและประเภทการบุกรุกระบบเครือข่ายเป็นผลลัพธ์ที่ได้มาจากระบบเครือข่ายใยประสาท IAQF (Intrusion Alert Quality Framework) จะทำหน้าที่นำเสนอผลลัพธ์ที่ได้จากระบบเครือข่ายใยประสาทต่อผู้ดูแลระบบเครือข่าย การแจ้งเตือนที่ผิดพลาดควรได้รับการพิจารณาเพื่อนำไปปรับลดกฎที่เป็นสาเหตุของการแจ้งเตือนนั้น

ระบบนำเสนอการแจ้งเตือนที่เกิดขึ้นจะทำหน้าที่นำเสนอข้อมูลประเภทการบุกรุกระบบเครือข่าย และข้อมูลระดับคุณภาพการแจ้งเตือนที่ได้ต่อผู้ดูแลระบบเครือข่าย ขั้นตอนการทำงานทั้งหมดของกลไกลดการแจ้งเตือนที่ผิดพลาดของโปรแกรมสนอร์ตอาจแบ่งได้เป็นสองส่วน ส่วนแรกคือการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ส่วนที่สองคือการนำเสนอผลลัพธ์ที่ได้จากการทำงานต่อผู้ดูแลระบบเครือข่ายแสดงในรูปที่ 3.11



รูปที่ 3.11 ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

ในการนำเสนอข้อมูลการแจ้งเตือน ผู้ดูแลระบบสามารถที่จะแบ่งย่อยระดับของการแจ้งเตือนที่ถูกต้องออกเป็นสองระดับแสดงดังตัวอย่างในตารางที่ 3.29 – 3.32 หรือแบ่งตามเปอร์เซ็นการแจ้งเตือนที่ถูกต้องแสดงในตารางที่ 3.33

ตารางที่ 3.29 การแบ่งย่อยระดับค่าบ่งชี้การแจ้งเตือนแบบ DoS

เงื่อนไข	ระดับคุณภาพการแจ้งเตือน
การแจ้งเตือนมีคุณภาพ = 1000	เป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพอยู่ระหว่าง 780 <= คุณภาพการแจ้งเตือน < 1000	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพ < 780	เป็นการแจ้งเตือนที่ผิดพลาด

ตารางที่ 3.30 การแบ่งย่อยระดับค่าบ่งชี้การแจ้งเตือนแบบพยายามค้นหารหัสผ่าน

เงื่อนไข	ระดับคุณภาพการแจ้งเตือน
การแจ้งเตือนมีคุณภาพ = 100	เป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพอยู่ระหว่าง 75 <= คุณภาพการแจ้งเตือน < 100	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพ < 75	เป็นการแจ้งเตือนที่ผิดพลาด

ตารางที่ 3.31 การแบ่งย่อยระดับค่าบ่งชี้การแจ้งเตือนแบบสแกนระบบเครือข่าย

เงื่อนไข	ระดับคุณภาพการแจ้งเตือน
การแจ้งเตือนมีคุณภาพ = 10	เป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพอยู่ระหว่าง 8 <= คุณภาพการแจ้งเตือน < 10	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพ < 8	เป็นการแจ้งเตือนที่ผิดพลาด

ตารางที่ 3.32 การแบ่งย่อยระดับค่าบ่งชี้การแจ้งเตือนด้วยมัลแวร์

เงื่อนไข	ระดับคุณภาพการแจ้งเตือน
การแจ้งเตือนมีคุณภาพ = 1	เป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพอยู่ระหว่าง 0.8 <= คุณภาพการแจ้งเตือน < 1	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง
การแจ้งเตือนมีคุณภาพ < 0.8	เป็นการแจ้งเตือนที่ผิดพลาด

ตารางที่ 3.33 การแบ่งระดับค่าบ่งชี้การแจ้งเตือนออกเป็นเปอร์เซ็นต์ความถูกต้อง

ประเภทการบุกรุกระบบเครือข่าย	ความถูกต้อง 100%	ความถูกต้อง 90%	ความถูกต้อง 80%	ความถูกต้อง 70%
เกณฑ์ระดับค่าบ่งชี้การบุกรุกแบบ DoS	1000	900 – 1000	800 – 900	780 - 800
เกณฑ์ระดับค่าบ่งชี้การบุกรุกแบบค้นหารหัสผ่าน	100	90 - 100	80 - 90	75 - 80
เกณฑ์ระดับค่าบ่งชี้การบุกรุกแบบสแกนระบบเครือข่าย	10	9 - 10	8 – 9	-
เกณฑ์ระดับค่าบ่งชี้การบุกรุกด้วยมัลแวร์	1	0.9 - 1	0.8 – 0.9	-

3.7 ระบบ False Positive Reduction via Intrusion Alert Quality Framework (FPAF) [1]

การแจ้งเตือนที่ผิดพลาดเป็นปัญหาอันดับต้น ๆ ของระบบตรวจจับการบุกรุกบนระบบเครือข่าย จึงได้มีผู้นำเสนอวิธีการลดปัญหาดังกล่าว ด้วยวิธีการที่แตกต่างกันออกไปดังที่ได้อธิบายไว้ในหัวข้อ 2.5 วิธีการลดการแจ้งเตือนที่ผิดพลาดแต่ละวิธีมีข้อดี ข้อเสียแตกต่างกัน ผู้ใช้งานสามารถเลือกใช้งานได้ตามความเหมาะสม

ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตที่ผู้วิจัยได้นำเสนอได้ใช้วิธีการประเมินคุณภาพการแจ้งเตือน การลดการแจ้งเตือนที่ผิดพลาดด้วยวิธีนี้มีผู้วิจัยท่านอื่นได้นำมาใช้ด้วยเช่นกัน ผู้วิจัยได้เลือกงานวิจัยที่มีชื่อว่า “False Positive Reduction via Intrusion Alert Quality Framework” (FPAF) มาเปรียบเทียบประสิทธิภาพการทำงานกับงานวิจัยที่นำเสนอ

การทำงานของระบบดังกล่าวจะเป็นการเก็บรวบรวมข้อมูลการแจ้งเตือนที่เกิดขึ้น และข้อมูลของโฮสต์เพื่อนำมากำหนดคะแนนให้กับการแจ้งเตือนที่เกิดขึ้น โดยข้อมูลที่ระบบทำการจัดเก็บแสดงในตารางที่ 3.34

ตารางที่ 3.34 การจัดเก็บข้อมูลการแจ้งเตือนที่เกิดขึ้นของระบบตรวจจับการบุกรุกบนระบบเครือข่าย

ตัวแปร	คำอธิบาย
SensorId	เซ็นเซอร์ที่เกิดการแจ้งเตือน
EventId	ลำดับการเกิดการแจ้งเตือน
AlertID	จำนวนครั้งการเกิดการแจ้งเตือน
AlertTye	ประเภทการแจ้งเตือน
EventDate	วันและเวลาที่เกิดการแจ้งเตือน
SrcIP	ที่อยู่ไอพีต้นทาง
SrcPort	พอร์ตต้นทาง
DstIp	ที่อยู่ไอพีปลายทาง
DstPort	พอร์ตปลายทาง

เมื่อระบบจัดเก็บข้อมูลการแจ้งเตือนที่เกิดขึ้นแล้ว ระบบจะนำข้อมูลดังกล่าวมาคำนวณหาค่าให้กับพารามิเตอร์ เพื่อใช้คำนวณหาคะแนนให้กับการแจ้งเตือนที่เกิดขึ้น เงื่อนไขการกำหนดค่าพารามิเตอร์และค่าน้ำหนักที่นำมาคำนวณหาคะแนนให้กับการแจ้งเตือนได้แสดงในตารางที่ 3.35

ตารางที่ 3.35 การกำหนดค่าพารามิเตอร์และค่าน้ำหนักของพารามิเตอร์

Quality Parameter	Rule	Wight(W)
Correctness	If the target host alive, score = 1 else score = 0	1.0
Os_Accuracy	If the DstIP running OS vulnerable to the attack, score = 1 else score = 0	0.3
Port_Accuracy	If the DstIP open port(s) vulnerable to the attack, score = 1 else score = 0	0.3
App_Accuracy	If the running application(s) vulnerable to the attack, score = 1 else score = 0	0.3
Aggregated Accuracy Score	OS_Accuracy_score * W_{os} + Post_Accuracy_score * W_p + App-Accuracy-score * W_a	
Reliability	If the sensor rules are frequently optimized, score = 1 else score = 0	0.05
Sensitivity	If the sensor signatures are frequently update, score = 1 else score = 0	0.05
Total Alert Quality Score	Correctness_score * (Aggregate_Accuracy_score + Reliability_score * W_r + Sensitivity_score * W_s)	

การเปรียบเทียบการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตกับระบบ PFAF ได้แสดงในตารางที่ 3.36

ตารางที่ 3.36 เปรียบเทียบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตกับระบบ PFAF

รายละเอียด	ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต	ระบบ PFAF
1. พารามิเตอร์ที่ใช้ในระบบ	24 พารามิเตอร์	5 พารามิเตอร์
2. ค่าน้ำหนักที่ใช้ในระบบ	สุ่มจากระบบเครือข่ายใยประสาท	ค่าน้ำหนักถูกกำหนดคงที่
3. วิธีการทำงานของระบบ	ระบบเครือข่ายใยประสาท	คำนวณด้วยมือ
4. ผลลัพธ์ของระบบ	0 – 1000	0 - 10

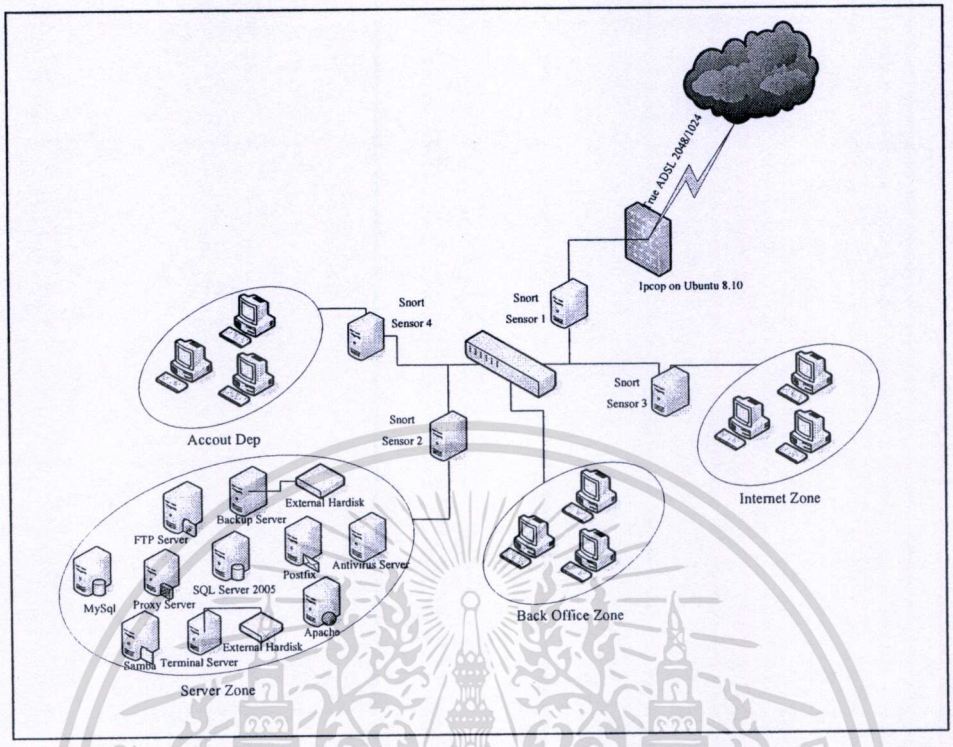
บทที่ 4
ผลการทดลองของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

ในบทนี้จะกล่าวถึง สภาพแวดล้อมบนระบบเครือข่ายที่ใช้ในการทดสอบระบบประเมินคุณภาพการแจ้งของโปรแกรมสนอร์ต ผลการทดสอบระบบเครือข่ายใยประสาท ผลการทดลองของระบบเมื่อเปรียบเทียบกับวิธีพื้นฐาน ผลการทดลองของระบบเมื่อเทียบกับวิธีการ False Positive Reduction via Intrusion Alert Quality Framework [1]

4.1 สภาพแวดล้อมบนระบบเครือข่ายที่ใช้ในการทดสอบระบบ

ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตได้ถูกทดสอบใช้งานด้วยข้อมูลการแจ้งเตือนการบุกรุกจากระบบเครือข่ายจริงขององค์กรแห่งหนึ่งที่มีโครงสร้างของระบบเครือข่ายในรูปที่ 4.1 ระบบเครือข่ายจะถูกแบ่งตามลักษณะการใช้งานออกเป็น 4 ระบบเครือข่ายย่อยอันประกอบไปด้วย เครือข่ายย่อยสำหรับแผนกบัญชี เครือข่ายย่อยสำหรับการใช้งานอินเทอร์เน็ต เครือข่ายย่อยสำหรับเครื่องแม่ข่าย (Server) และเครือข่ายย่อยสำหรับการใช้งานอินทราเน็ต (Intranet) โดยระบบประกอบไปด้วยเครื่องแม่ข่ายจำนวน 10 เครื่อง และเครื่องลูกข่าย (client) จำนวน 144 เครื่อง รายละเอียดของเครือข่ายย่อยได้แสดงดังต่อไปนี้

- **เครือข่ายย่อยสำหรับแผนกบัญชี** การใช้งานโปรแกรมบัญชีที่ทำงานติดต่อกับเครื่องแม่ข่าย SQL 2005 และการใช้งานโปรแกรมที่โปรแกรมเมอร์พัฒนาขึ้นใช้งานภายในองค์กรโดยจะติดต่อกับเครื่องแม่ข่าย MySQL การใช้งานเครื่องแม่ข่าย Samba เครื่องแม่ข่าย Antivirus และเครื่องแม่ข่าย Postfix เครือข่ายย่อยสำหรับแผนกบัญชีจะไม่สามารถใช้งานอินเทอร์เน็ต และประกอบไปด้วยเครื่องลูกข่ายจำนวน 22 เครื่อง มีรายละเอียดดังนี้ เครื่องลูกข่ายของฝ่ายการเงิน 7 เครื่อง เครื่องลูกข่ายของฝ่ายจัดซื้อ 5 เครื่อง เครื่องลูกข่ายของฝ่ายสต็อก 3 เครื่อง และเครื่องลูกข่ายของฝ่ายบัญชี 7 เครื่อง การกำหนดที่อยู่ไอพีเครือข่ายย่อยสำหรับแผนกบัญชีมีหมายเลขที่อยู่ไอพีในช่วง 192.168.10.51/24 – 192.168.10.90/24



รูปที่ 4.1 โครงสร้างระบบเครือข่ายที่ใช้ทดสอบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

- **เครือข่ายย่อยสำหรับการใช้งานอินทราเน็ต** โดยมากเป็นการใช้งานโปรแกรมที่โปรแกรมเมอร์พัฒนาขึ้นใช้งานภายในองค์กรโดยจะติดต่อกับเครื่องแม่ข่าย MySQL การใช้งานเครื่องแม่ข่าย Samba เครื่องแม่ข่าย Postfix เครื่องแม่ข่าย Antivirus และโปรแกรม Payroll ติดต่อกับเครื่องแม่ข่าย SQL 2005 ซึ่งจะใช้งานเฉพาะฝ่ายบุคคล เครื่องลูกข่ายจะไม่สามารถใช้งานอินเทอร์เน็ตได้ เครือข่ายย่อยสำหรับการใช้งานอินทราเน็ตประกอบไปด้วยเครื่องลูกข่ายจำนวน 83 เครื่อง มีรายละเอียดดังนี้ เครื่องลูกข่ายของแผนกธุรการ 25 เครื่อง เครื่องลูกข่ายของพนักงานประเมิน 38 เครื่อง เครื่องลูกข่ายของฝ่ายบุคคล 7 เครื่อง เครื่องลูกข่ายของฝ่ายการตลาด 8 เครื่อง และเครื่องลูกข่ายของการใช้งานทั่วไป 5 เครื่อง การกำหนดที่อยู่ไอพีสำหรับเครือข่ายย่อยสำหรับการใช้งานอินทราเน็ตมีหมายเลขที่อยู่ไอพีในช่วง 192.168.10.91/24 – 192.168.10.190/24

- **เครือข่ายย่อยสำหรับการใช้งานอินเทอร์เน็ต** การใช้งานโปรแกรมที่โปรแกรมเมอร์พัฒนาขึ้นใช้งานภายในองค์กรโดยจะติดต่อกับเครื่องแม่ข่าย MySQL การใช้งานเครื่องแม่ข่าย Samba เครื่องแม่ข่าย Postfix เครื่องแม่ข่าย Antivirus เครื่องแม่ข่าย Proxy และโปรแกรมบัญชี Formula ติดต่อกับเครื่องแม่ข่าย SQL 2005 สำหรับผู้บริหาร เครือข่ายย่อยสำหรับการใช้งานอินเทอร์เน็ตประกอบไปด้วยเครื่องลูกข่ายจำนวน 39 เครื่องมีรายละเอียดดังนี้ เครื่องลูกข่ายของการใช้งานอินเทอร์เน็ตของพนักงาน 20 เครื่อง เครื่องลูกข่ายของผู้บริหาร หัวหน้าแผนกและหัวหน้า

ฝ่าย 13 เครื่อง และเครื่องลูกข่ายของแผนกคอมพิวเตอร์ 6 เครื่อง การกำหนดที่อยู่ไอพีสำหรับเครือข่ายย่อยการใช้งานอินเทอร์เน็ตมีหมายเลขที่อยู่ไอพีในช่วง 192.168.10.191/24 – 192.168.10.245/24

- **เครือข่ายย่อยสำหรับเครื่องแม่ข่าย** การทำงานของเครื่องแม่ข่ายทั้งหมดภายในองค์ มีการกำหนดที่อยู่ไอพีสำหรับเครือข่ายย่อยเครื่องแม่ข่ายในช่วง 192.168.10.1/24 – 192.168.10.30/24จำนวน 10 เครื่องมีรายละเอียดดังต่อไปนี้

- เครื่องแม่ข่าย Samba ทำหน้าที่เป็น file sharing server ให้พนักงานใช้งานในการจัดเก็บข้อมูลที่เป็นความลับ และการใช้งานข้อมูลรวมกันเครื่องแม่ข่าย Samba จะมีการทำ Profile Control ในการเข้าใช้งานเครื่องคอมพิวเตอร์ภายในองค์กร เครื่องแม่ข่าย Samba ทำงานอยู่บน Fedora Core 5 เวอร์ชันของโปรแกรมคือ Samba 3.0 ที่อยู่ไอพีของเครื่องแม่ข่าย Samba มีหมายเลขที่อยู่ไอพี 192.168.10.3/24
- เครื่องแม่ข่าย Terminal ใช้สำหรับผู้ดูแลระบบเครือข่าย และพนักงานที่ได้รับสิทธิ์ในการเข้าใช้งานระบบเครือข่ายจากระยะไกล เครื่องแม่ข่าย Terminal ได้ถูกกำหนดค่าให้สามารถใช้งานเครือข่ายส่วนบุคคล (VPN) ได้การสำรองข้อมูลของเครื่องแม่ข่าย Terminal จะทำการสำรองข้อมูลในเวลา 2.00 น. ของทุกวันลงในอุปกรณ์ต่อพ่วง (External Hard Drive) เครื่องแม่ข่าย Terminal ทำงานด้วยระบบปฏิบัติการ Window 2008 ที่อยู่ไอพีของเครื่องแม่ข่าย Terminal มีหมายเลขที่อยู่ไอพี 192.168.10.5/24
- เครื่องแม่ข่าย Backup จัดเก็บไฟล์สำหรับกู้ระบบ (Image) ของเครื่องแม่ข่ายภายในองค์ ไฟล์สำหรับกู้ระบบ จะถูกนำมาใช้เมื่อเครื่องแม่ข่ายไม่สามารถทำงานได้ ไม่ว่าจะเป็นปัญหาด้านฮาร์ดแวร์หรือซอฟต์แวร์ ผู้ดูแลระบบจะนำไฟล์สำหรับกู้ระบบ มากู้คืน (Restore) ให้กับเครื่องแม่ข่าย การสำรองข้อมูลจะใช้โปรแกรม Acronic ในการจัดทำไฟล์สำหรับกู้ระบบของเครื่องแม่ข่าย และนำมาจัดเก็บในเครื่องแม่ข่ายสำรองข้อมูล (Backup) เครื่องแม่ข่ายสำรองข้อมูลทำงานด้วยระบบปฏิบัติการ Ubuntu 8.10 ที่อยู่ไอพีของเครื่องแม่ข่ายสำรองข้อมูลมีหมายเลขที่อยู่ไอพี 192.168.10.4/24
- เครื่องแม่ข่าย Postfix ทำหน้าที่เป็นเครื่องแม่ข่ายให้บริการอีเมลที่ใช้ในการติดต่อสื่อสารทั้งภายในองค์กรและภายนอกองค์กร เครื่องแม่ข่าย Postfix ทำงานอยู่บน Fedora Core 5 เวอร์ชันของโปรแกรมคือ Postfix 2.2 ที่อยู่ไอพีของเครื่องแม่ข่าย Postfix มีหมายเลขที่อยู่ไอพี 192.168.10.7/24
- เครื่องแม่ข่าย SQL 2005 ทำหน้าที่จัดเก็บข้อมูลของโปรแกรมบัญชี Formula และโปรแกรม Payroll โปรแกรม Formula จะนำมาใช้ในงานบัญชีของแผนกบัญชี และใช้สำหรับผู้บริหารดูข้อมูลโดยรวมขององค์กร โปรแกรม Payroll ใช้ในการจัดทำเงินเดือนของฝ่ายบุคคล เครื่องแม่ข่าย Sql 2005 ทำงานอยู่บน Windows 2003 R2 ฐานข้อมูลที่ใช้

งานคือโปรแกรม Microsoft Sql Server 2005 SP 1 ที่อยู่ไอพีของเครื่องแม่ข่าย Sql 2005 มีหมายเลขที่อยู่ไอพี 192.168.10.13/24

- เครื่องแม่ข่าย MySql ทำหน้าที่จัดเก็บข้อมูลเหมือนกับเครื่องแม่ข่าย SQL 2005 แต่ เครื่องแม่ข่าย MySql จะใช้จัดเก็บข้อมูลจากโปรแกรมที่ได้ถูกพัฒนาขึ้นมาใช้ภายในองค์เท่านั้น เครื่องแม่ข่าย MySql ทำงานอยู่บน Ubuntu 8.04 ฐานข้อมูลที่ใช้งานคือ MySql 5.0 ที่อยู่ไอพีของเครื่องแม่ข่าย MySql มีหมายเลขที่อยู่ไอพี 192.168.10.12/24
- เครื่องแม่ข่าย FTP ให้บริการข้อมูลกับสาขาขององค์กร ที่อยู่ไอพีของเครื่องแม่ข่าย FTP มีหมายเลขที่อยู่ไอพี 192.168.10.9/24
- เครื่องแม่ข่าย Apache ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์เพื่อการใช้งานโปรแกรมบนเว็บเพจ (Web Application) ภายในองค์กร เครื่องแม่ข่าย Apache ทำงานอยู่บน Ubuntu 8.10 ที่อยู่ไอพีของเครื่องแม่ข่าย Apache มีหมายเลขที่อยู่ไอพี 192.168.10.17/24
- เครื่องแม่ข่าย Antivirus ทำหน้าที่ดาวน์โหลดรูปแบบการตรวจจับการบุกรุกจากเว็บไซต์ที่ให้บริการ และทำการกระจายรูปแบบการตรวจจับการบุกรุกไปยังเครื่องลูกข่ายโดยเครื่องแม่ข่าย Antivirus ทำงานอยู่ Microsoft Window 2003 Server ที่อยู่ไอพีของเครื่องแม่ข่าย Antivirus มีหมายเลขที่อยู่ไอพี 192.168.10.19/24
- ไฟร์วอลล์ ทำหน้าที่คัดกรองแพ็คเก็จที่ผ่านเข้า-ออกบนระบบเครือข่าย โปรแกรมที่ทำหน้าที่เป็นไฟร์วอลล์คือ IPCop ซึ่งทำงานอยู่บน Ubuntu 8.04 เวอร์ชันของโปรแกรม IPCop คือ IPCop 1.4.2.1 ที่อยู่ไอพีของไฟร์วอลล์ มีหมายเลขที่อยู่ไอพี 192.168.10.16/24

- การตั้งค่าของ สนอร์ตเซ็นเซอร์ (Snort Sensor) ทั้ง 4 ตัว

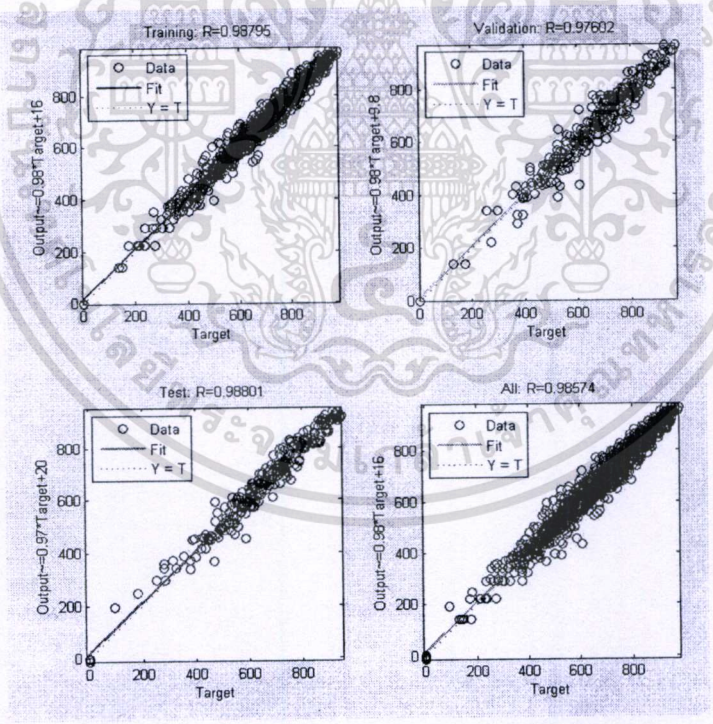
- สนอร์ตเซ็นเซอร์หมายเลข 1 ทำงานอยู่หลังไฟร์วอลล์ทำหน้าที่ในการตรวจสอบทราฟฟิคที่ผ่านเข้ามาในระบบเครือข่าย สนอร์ตเซ็นเซอร์หมายเลข 1 ทำงานอยู่บน Ubuntu 8.10 เวอร์ชันของโปรแกรมสนอร์ต คือ Snort 2.8.4 ที่อยู่ไอพีของสนอร์ตเซ็นเซอร์หมายเลข 1 มีหมายเลขที่อยู่ไอพี 192.168.10.21/24
- สนอร์ตเซ็นเซอร์หมายเลข 2 ตรวจสอบทราฟฟิคที่ผ่านเข้าไปยังเครือข่ายย่อยสำหรับเครื่องแม่ข่าย สนอร์ตเซ็นเซอร์หมายเลข 2 ทำงานอยู่บน Ubuntu 8.04 เวอร์ชันของโปรแกรมสนอร์ต คือ Snort 2.8.4 ที่อยู่ไอพีของสนอร์ตเซ็นเซอร์หมายเลข 2 มีหมายเลขที่อยู่ไอพี 192.168.10.22/24
- สนอร์ตเซ็นเซอร์หมายเลข 3 ตรวจสอบทราฟฟิคที่ผ่านเข้าไปยังเครือข่ายย่อยสำหรับการใช้งานอินเทอร์เน็ต สนอร์ตเซ็นเซอร์หมายเลข 3 ทำงานอยู่บน Ubuntu 8.04 เวอร์ชันของโปรแกรมสนอร์ต คือ Snort 2.8.3 ที่อยู่ไอพีของสนอร์ตเซ็นเซอร์หมายเลข 3 มีหมายเลขที่อยู่ไอพี 192.168.10.23/24

- สนอร์ตเซ็นเซอร์หมายเลข 4 ตรวจสอบทราฟฟิคที่ผ่านเข้าไปยังเครือข่ายย่อยสำหรับแผนกบัญชี สนอร์ตเซ็นเซอร์หมายเลข 4 ทำงานอยู่บน Ubuntu 8.04 เวอร์ชันของโปรแกรมสนอร์ต คือ Snort 2.8.3 ที่อยู่ไอพีของสนอร์ตเซ็นเซอร์หมายเลข 4 มีหมายเลขที่อยู่ไอพี 192.168.10.24/24

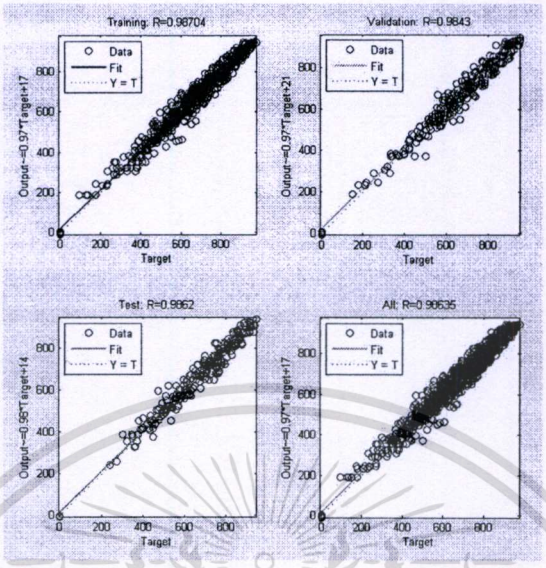
4.2 ผลการทดสอบสถาปัตยกรรมระบบเครือข่ายใยประสาท

จากการทดสอบระบบเครือข่ายใยประสาทที่มีสถาปัตยกรรม 1 และ 2 ชั้นแฝงโดยในแต่ละชั้นแฝงจะมีจำนวนหน่วย 10, 15 และ 20 หน่วยประสาทเทียม และทำการฝึกสอนกับชุดค่าน้ำหนักเริ่มต้นจำนวน 5 เพื่อดูความสามารถในการพยากรณ์ของแต่ละสถาปัตยกรรม เมื่อทำการทดสอบระบบเครือข่ายใยประสาทตามสถาปัตยกรรมที่กำหนดสามารถวาดกราฟได้ดังนี้

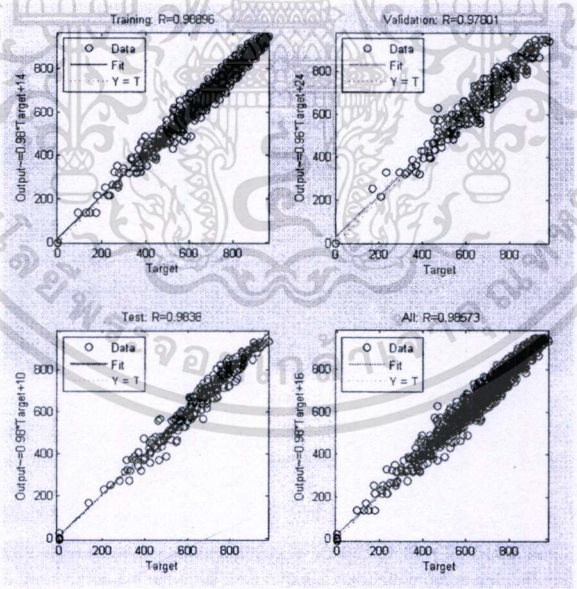
4.2.1 ผลการทดสอบระบบเครือข่ายใยประสาทที่ใช้ประเมินคุณภาพการแจ้งเตือนการบุกรุกแบบ DoS



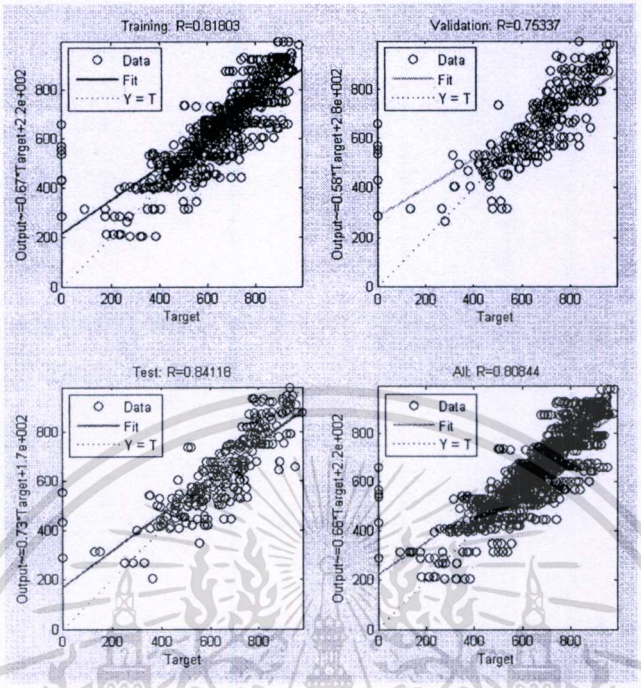
รูปที่ 4.2 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น จำนวน 10 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบ DoS



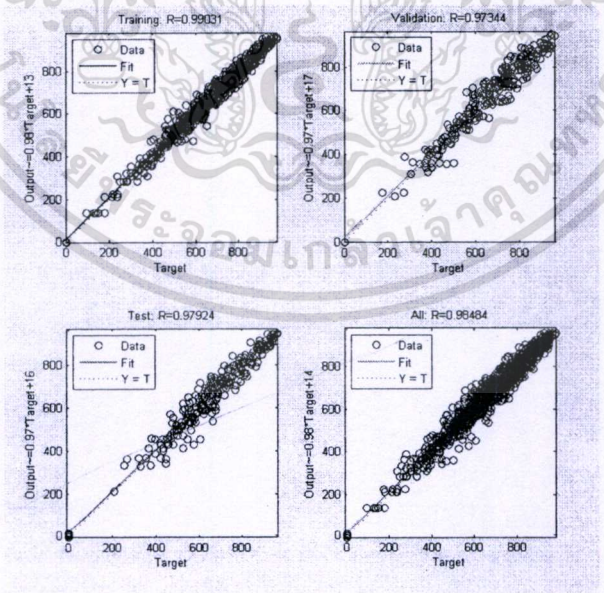
รูปที่ 4.3 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น จำนวน 15 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบ DoS



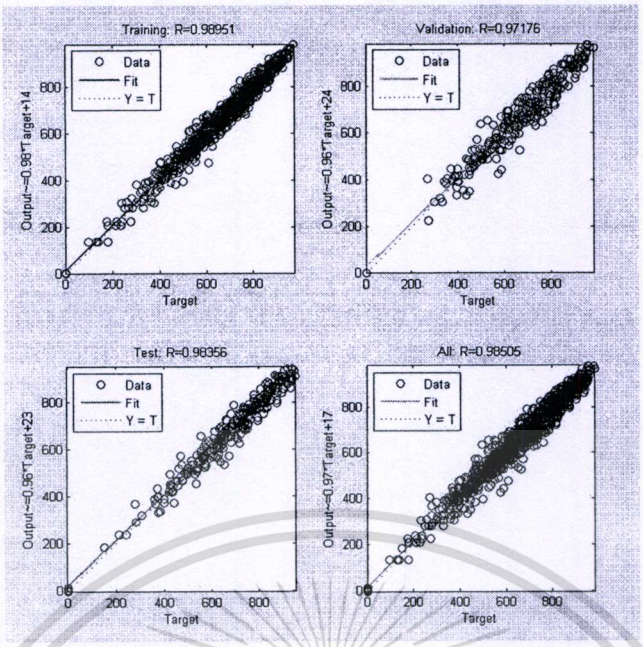
รูปที่ 4.4 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น จำนวน 20 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบ DoS



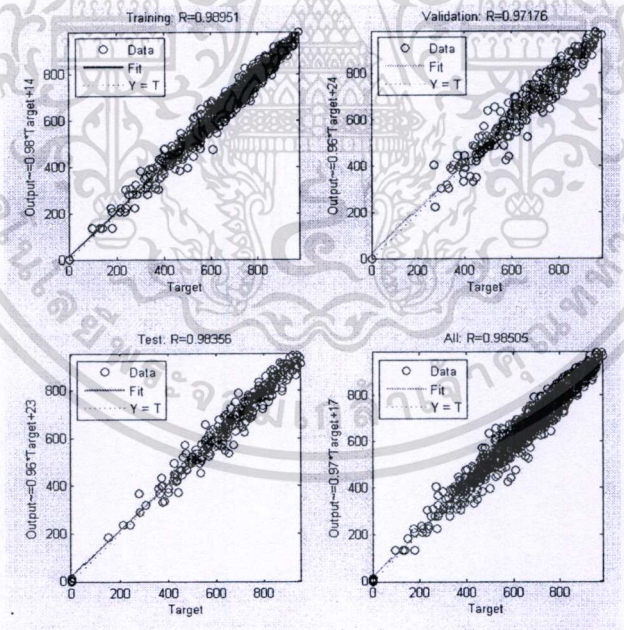
รูปที่ 4.5 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



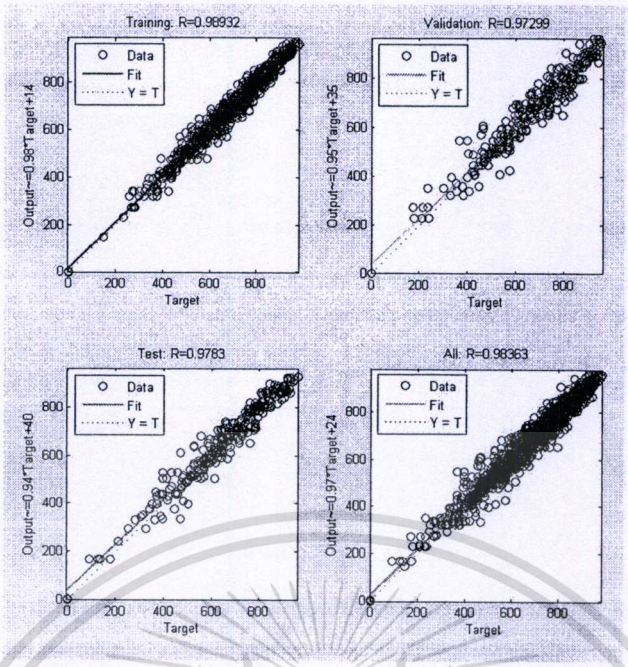
รูปที่ 4.6 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



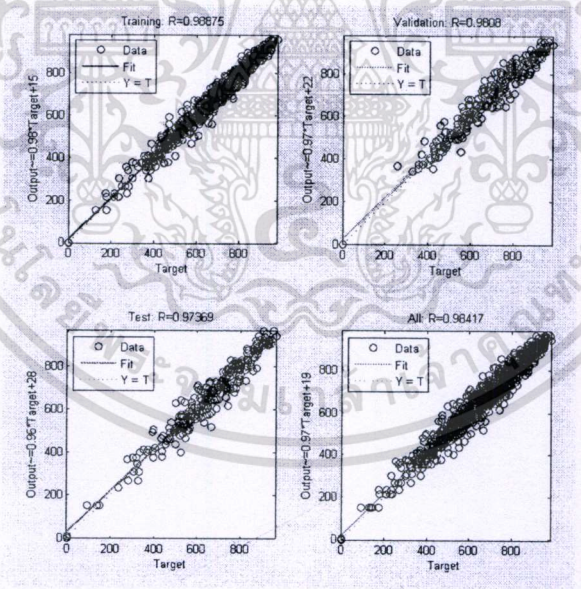
รูปที่ 4.7 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



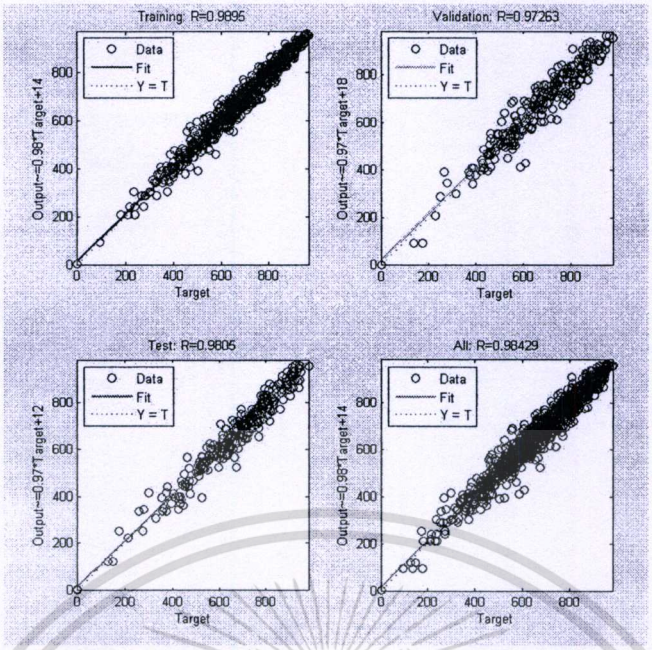
รูปที่ 4.8 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



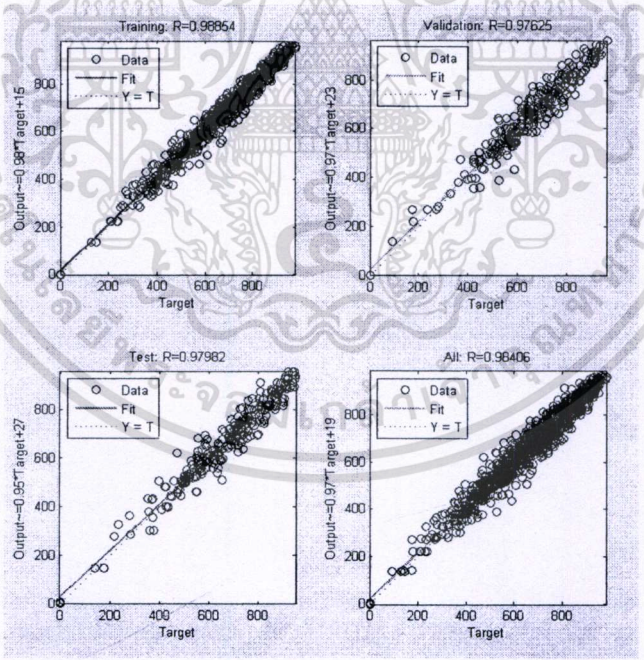
รูปที่ 4.9 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



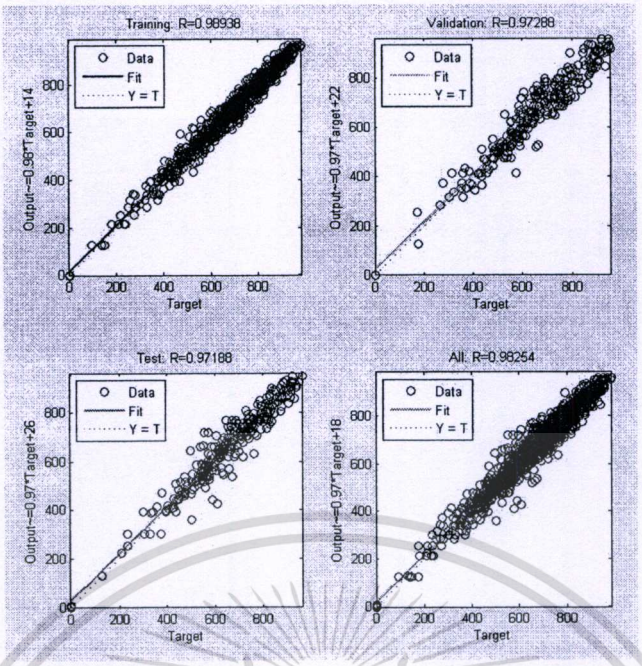
รูปที่ 4.10 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



รูปที่ 4.11 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



รูปที่ 4.12 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS



รูปที่ 4.13 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบ DoS

จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบ Dos สามารถแสดงตารางค่าประสิทธิภาพซึ่งวัดจากค่า RMSE Ratio ได้ดังนี้

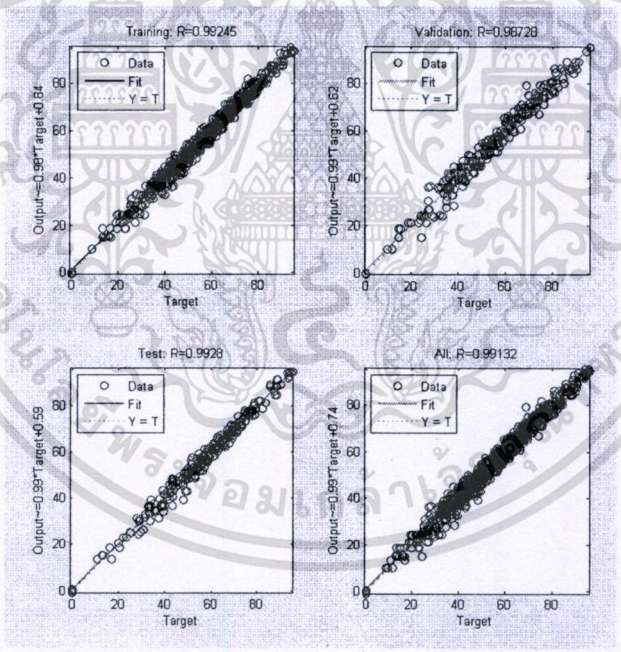
ตารางที่ 4.1 ค่า RMSE Ratio จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบ DoS

แบบที่	สถาปัตยกรรมระบบเครือข่ายใยประสาท	ค่า RMSE Ratio
1	ชั้นแฝง 1 ชั้น มี 10 หน่วย	0.9929
2	ชั้นแฝง 1 ชั้น มี 15 หน่วย	1.0125
3	ชั้นแฝง 1 ชั้น มี 20 หน่วย	1.1400
4	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	17.5737
5	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	1.3780
6	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	1.5426
7	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	1.5479
8	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	1.7713
9	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	1.6207
10	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	1.9642

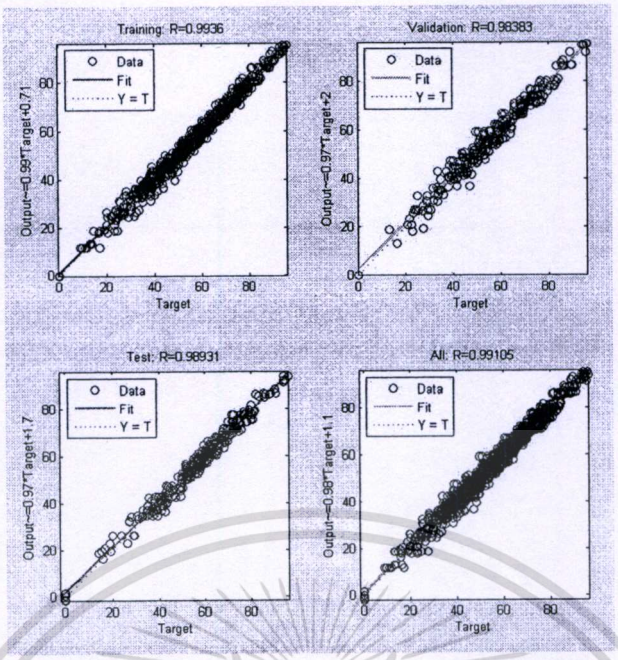
11	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	1.6871
12	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	2.0636

จากผลการทดลองจะเห็นได้ว่าค่า RMSE Ratio ของค่าความผิดพลาดจะมีค่าไม่เท่ากันในแต่ละสถาปัตยกรรม เมื่อนำผลการทดลองที่ได้มาเปรียบเทียบจะพบว่าสถาปัตยกรรมที่มีชั้นแฝง 1 ชั้น มี 10 หน่วย มีค่า RMSE Ratio น้อยที่สุดคือ 0.9929 และสถาปัตยกรรมที่มีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วยมีค่า RMSE Ratio มากที่สุดคือ 2.0636 ดังนั้นจึงเลือกใช้งานระบบเครือข่ายใยประสาทที่มีสถาปัตยกรรมชั้นแฝง 1 ชั้นมีจำนวน 10 หน่วย ในการประเมินคุณภาพการแจ้งเตือนแบบ DoS

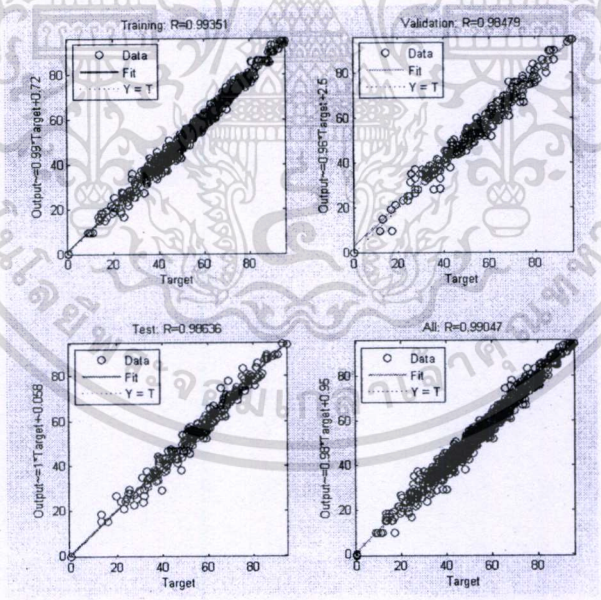
4.2.2 ผลการทดสอบระบบเครือข่ายใยประสาทที่ใช้ประเมินคุณภาพการแจ้งเตือนการบุกรุกแบบพยายามค้นหารหัสผ่าน



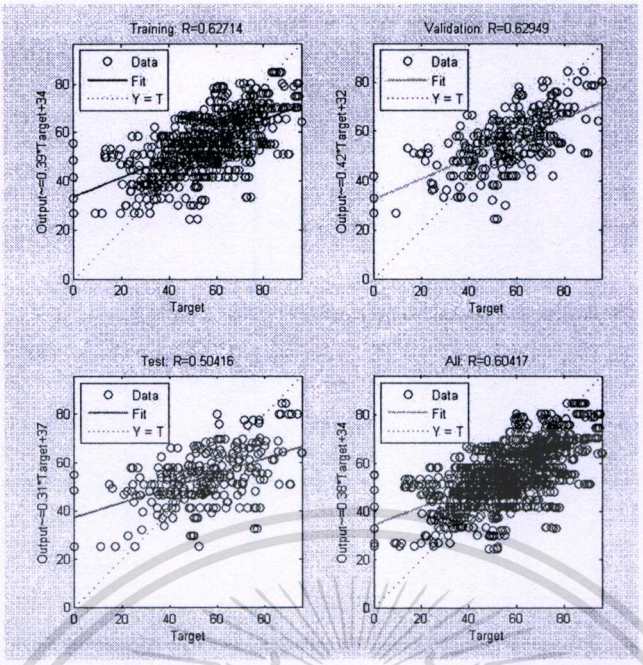
รูปที่ 4.14 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 10 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



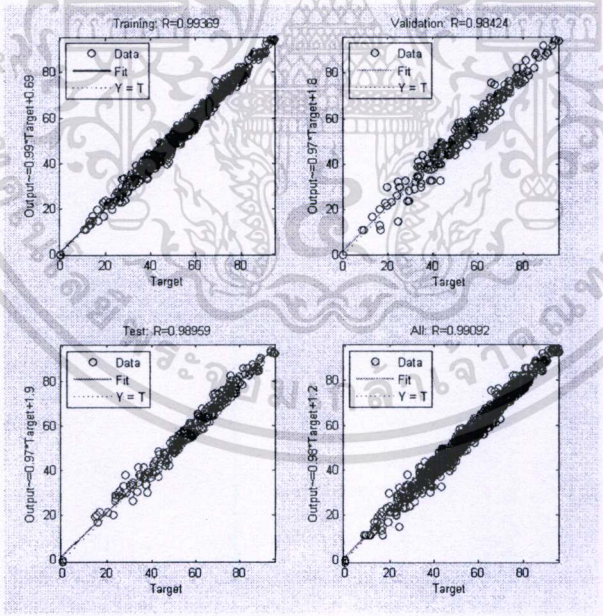
รูปที่ 4.15 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 15 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



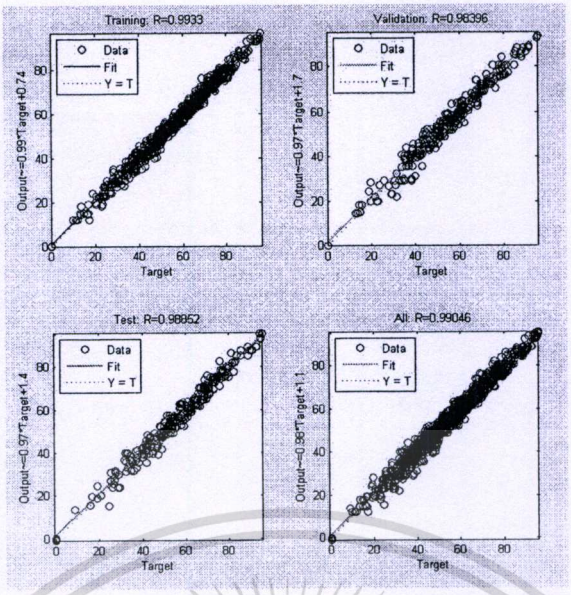
รูปที่ 4.16 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 20 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



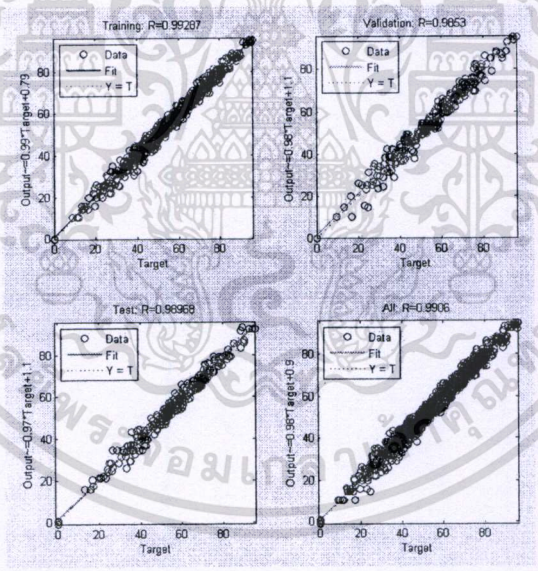
รูปที่ 4.17 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



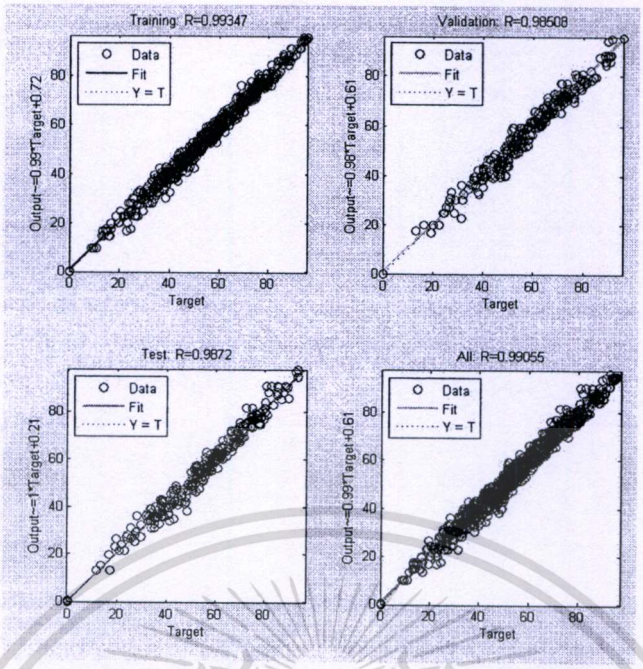
รูปที่ 4.18 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



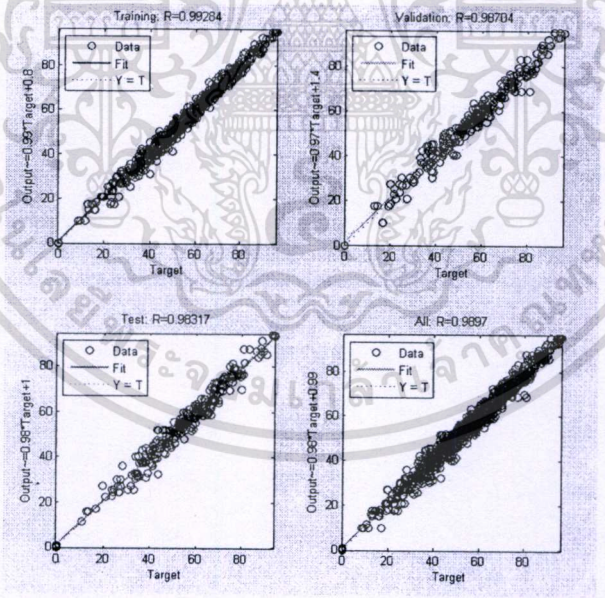
รูปที่ 4.19 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



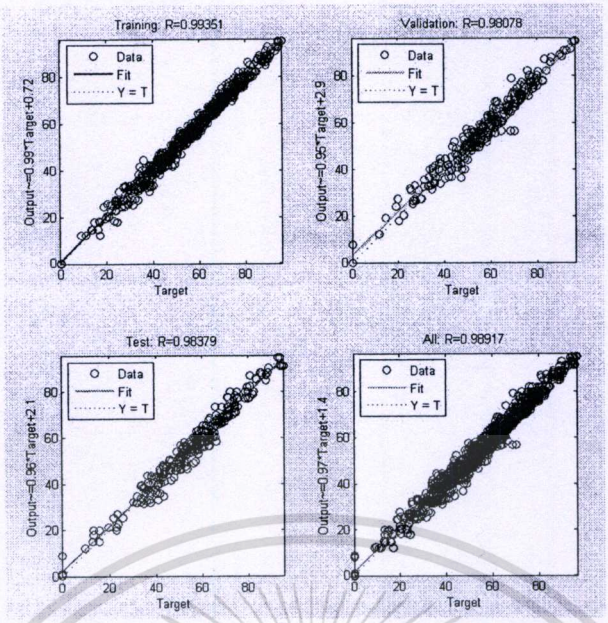
รูปที่ 4.20 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



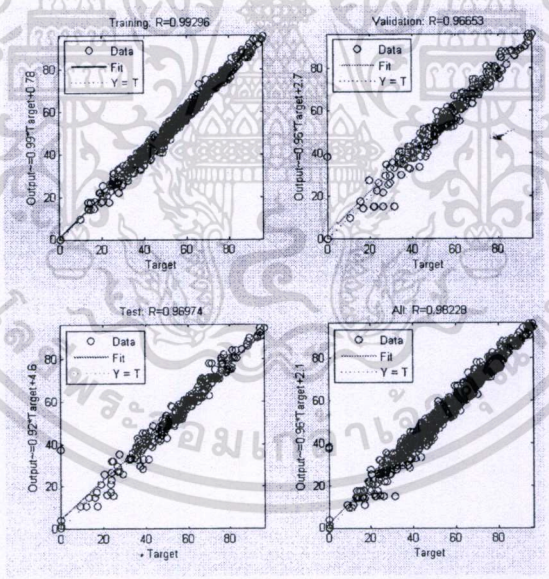
รูปที่ 4.21 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



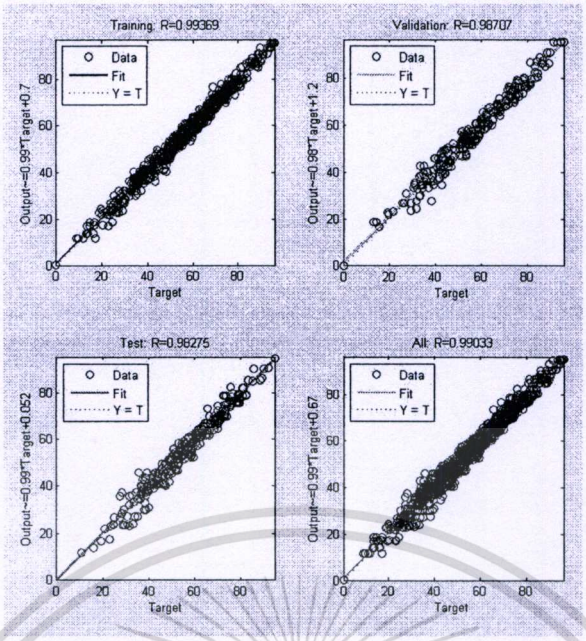
รูปที่ 4.22 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



รูปที่ 4.23 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



รูปที่ 4.24 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน



รูปที่ 4.25 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน

จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน สามารถแสดงตารางค่าประสิทธิภาพซึ่งวัดจากค่า RMSE Ratio ได้ดังนี้

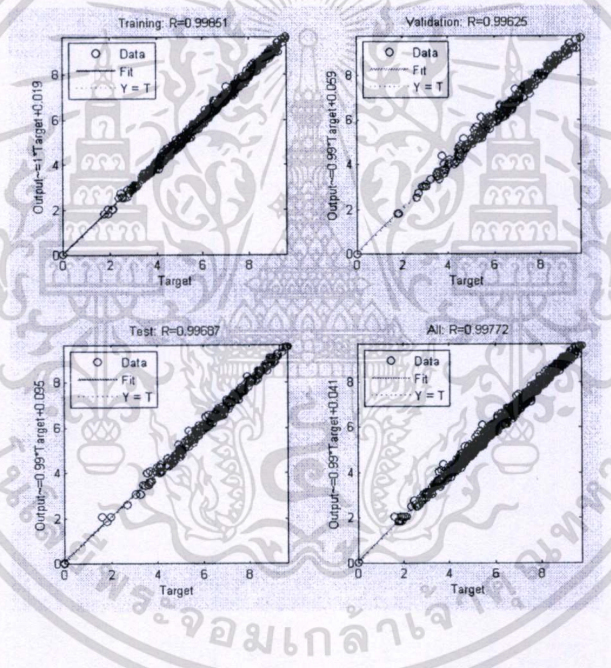
ตารางที่ 4.2 ค่า RMSE Ratio จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน

แบบที่	สถาปัตยกรรมระบบเครือข่ายใยประสาท	ค่า RMSE Ratio
1	ชั้นแฝง 1 ชั้น มี 10 หน่วย	0.0065
2	ชั้นแฝง 1 ชั้น มี 15 หน่วย	0.0055
3	ชั้นแฝง 1 ชั้น มี 20 หน่วย	0.0073
4	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	1.7943
5	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0076
6	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0076
7	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0079
8	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0071
9	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0088
10	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0115
11	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0203

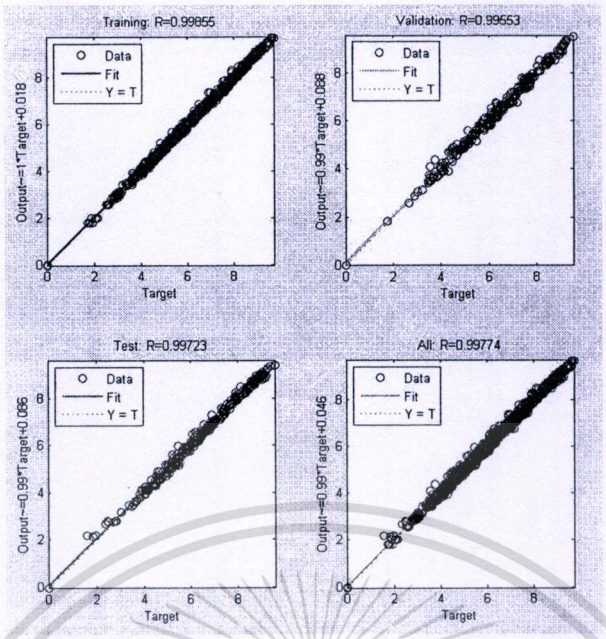
12	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0086

จากผลการทดลองจะเห็นได้ว่า RMSE Ratio ของค่าความผิดพลาดจะมีค่าไม่เท่ากันในแต่ละสถาปัตยกรรม เมื่อนำผลการทดลองที่ได้มาเปรียบเทียบจะพบว่าสถาปัตยกรรมที่มีชั้นแฝง 1 ชั้น มี 15 หน่วยมีค่า RMSE Ratio น้อยที่สุดคือ 0.0055 และสถาปัตยกรรมที่มีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วยมีค่า RMSE Ratio มากที่สุดคือ 0.1794 ดังนั้นจึงเลือกใช้งานระบบเครือข่ายใยประสาทที่มีสถาปัตยกรรมชั้นแฝง 1 ชั้นจำนวน 15 หน่วยในการประเมินคุณภาพการบุกรุกระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน

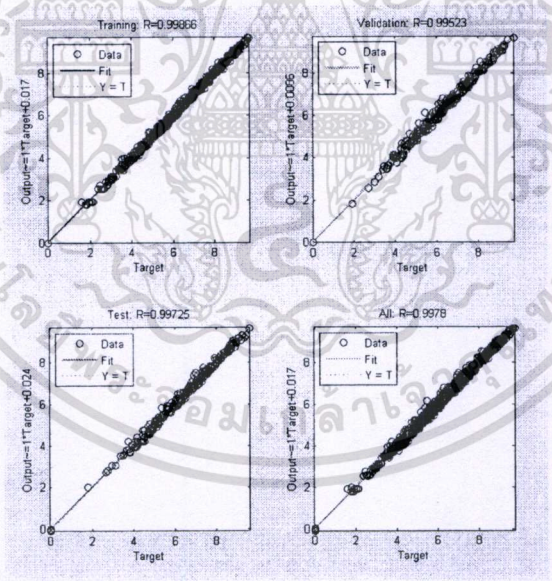
4.2.3 ผลการทดสอบระบบเครือข่ายใยประสาทที่ใช้ประเมินคุณภาพการแจ้งเตือนการบุกรุกแบบสแกนระบบเครือข่าย



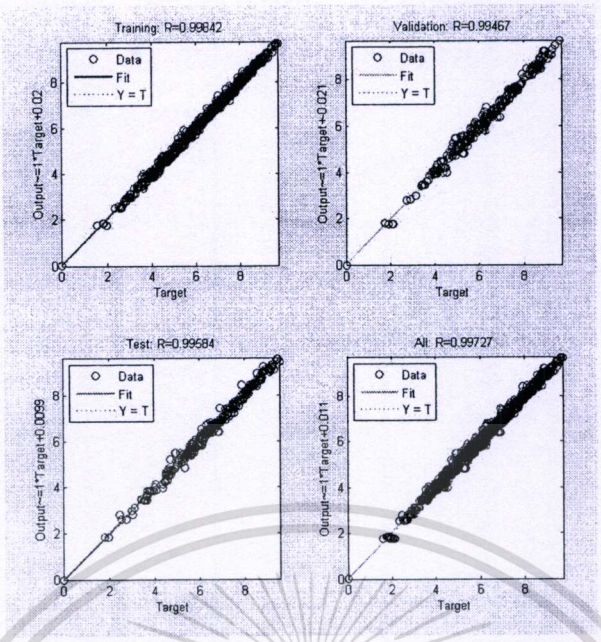
รูปที่ 4.26 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 10 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



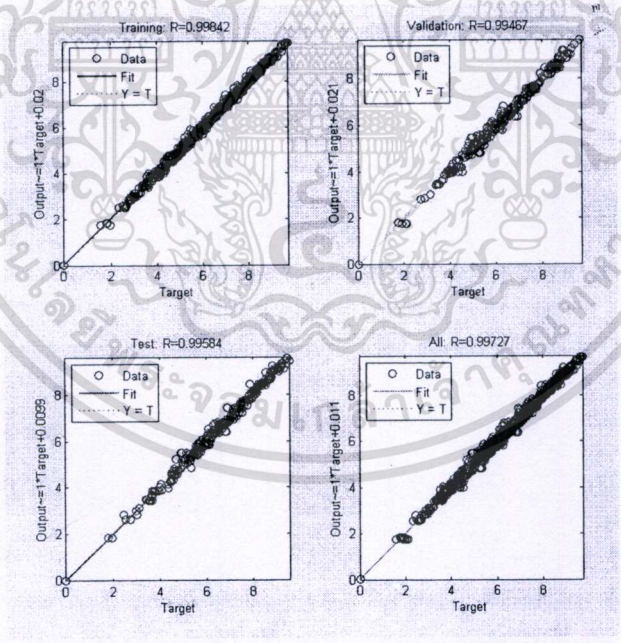
รูปที่ 4.27 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 15 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



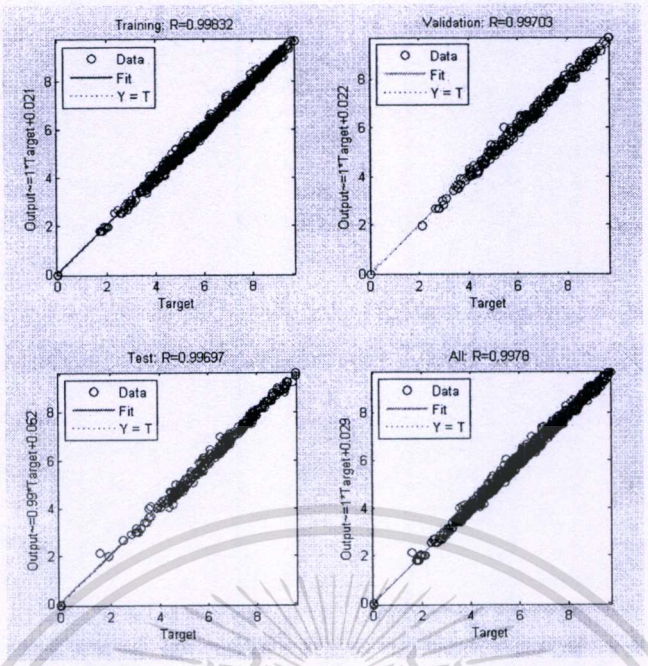
รูปที่ 4.28 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 20 หน่วย สำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



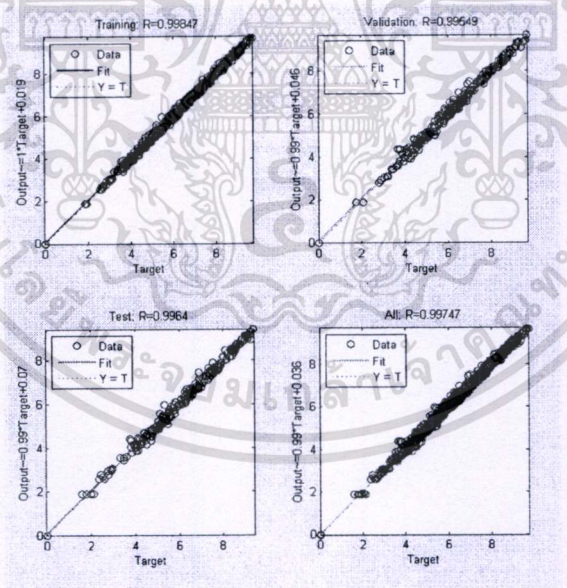
รูปที่ 4.29 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



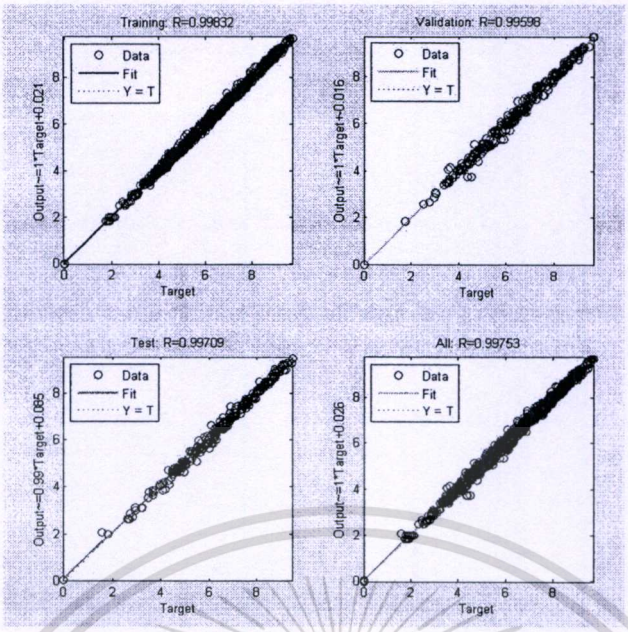
รูปที่ 4.30 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



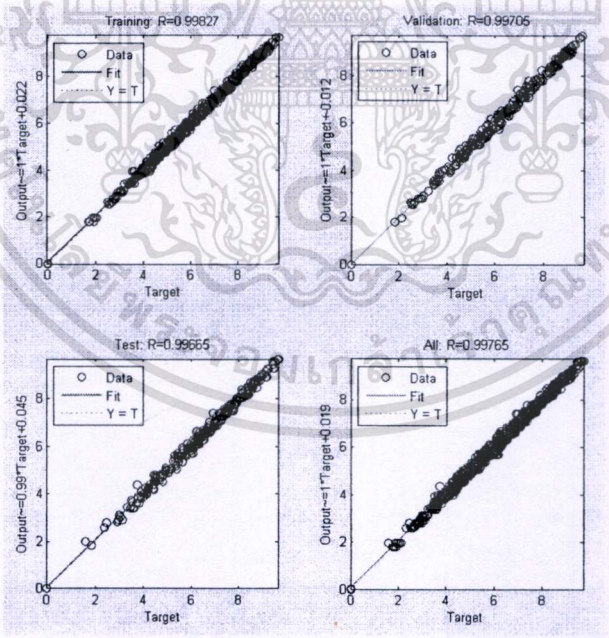
รูปที่ 4.31 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



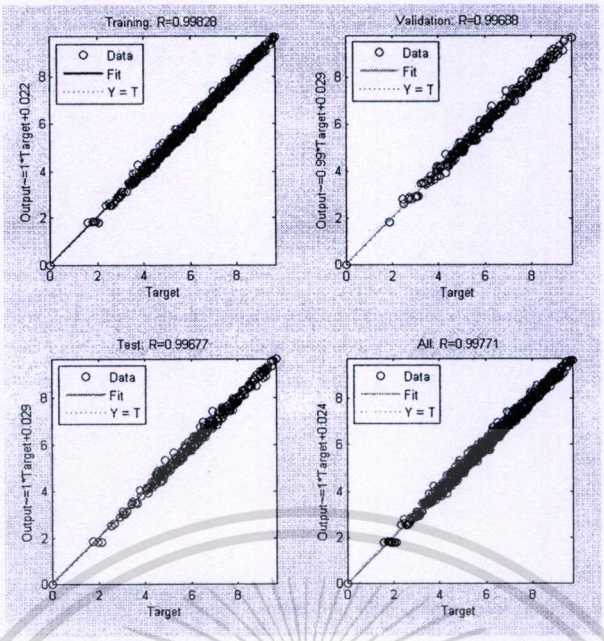
รูปที่ 4.32 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



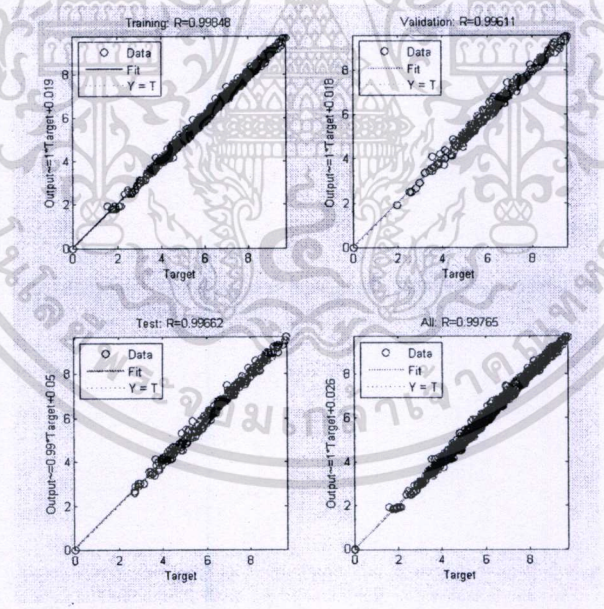
รูปที่ 4.33 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



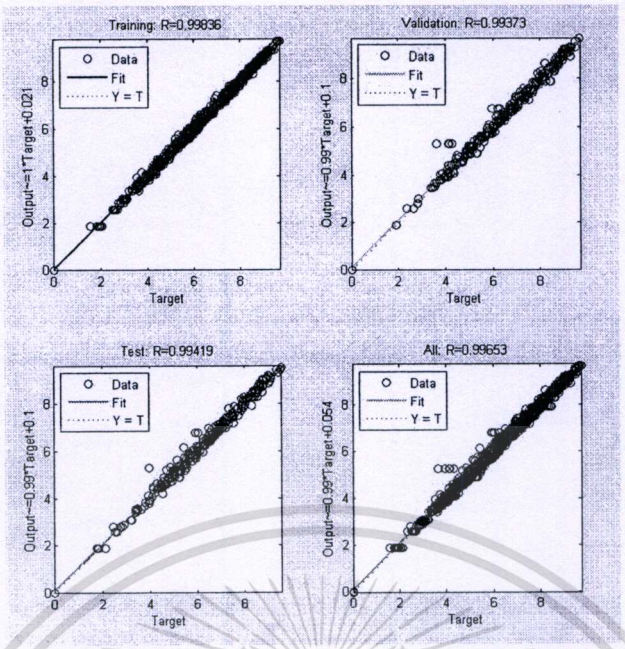
รูปที่ 4.34 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



รูปที่ 4.35 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 10 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



รูปที่ 4.36 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 15 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย



รูปที่ 4.37 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และชั้นที่ 2 มี 20 หน่วยสำหรับการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย

จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่ายสามารถแสดงตารางค่าประสิทธิภาพซึ่งวัดจากค่า RMSE Ratio ได้ดังนี้

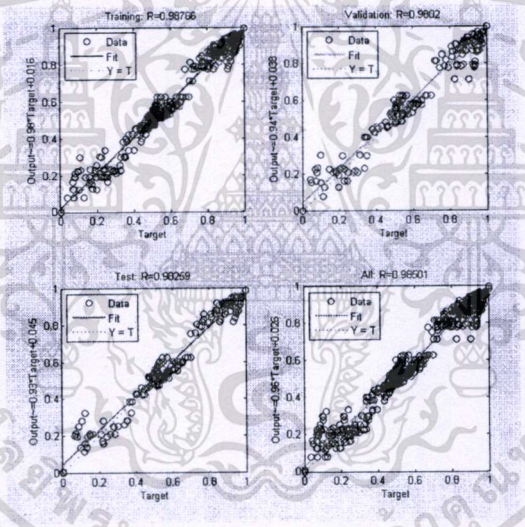
ตารางที่ 4.3 ค่า RMSE Ratio จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย

แบบที่	สถาปัตยกรรมระบบเครือข่ายใยประสาท	ค่า RMSE Ratio
1	ชั้นแฝง 1 ชั้น มี 10 หน่วย	0.0018
2	ชั้นแฝง 1 ชั้น มี 15 หน่วย	0.0001
3	ชั้นแฝง 1 ชั้น มี 20 หน่วย	0.0018
4	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0029
5	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0014
6	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0015
7	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0025
8	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0021
9	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0021
10	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0020
11	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0023

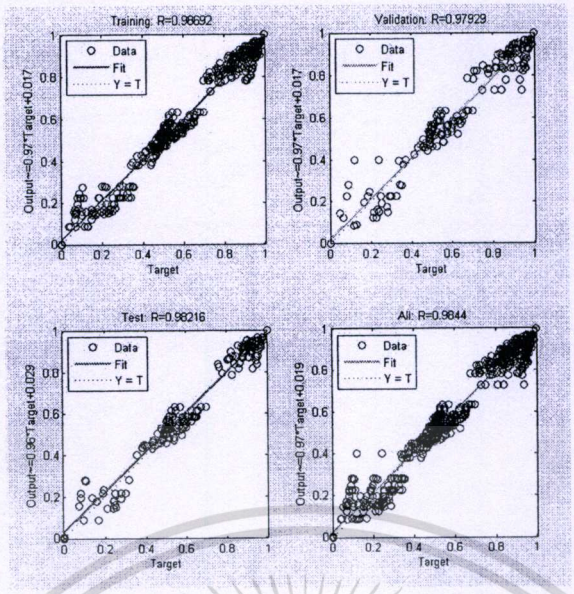
12	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0045

จากผลการทดลองจะเห็นได้ว่า Ratio RMSS ของค่าความผิดพลาดจะมีค่าไม่เท่ากันในแต่ละสถาปัตยกรรมต่อค่าชุดน้ำหนัก เมื่อนำผลการทดลองที่ได้มาเปรียบเทียบจะพบว่าสถาปัตยกรรมที่มีชั้นแฝง 1 ชั้น มี 15 หน่วยมีค่า RMSE Ratio น้อยที่สุดคือ 0.0001 และสถาปัตยกรรมที่มีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วยมีค่า RMSE Ratio มากที่สุดคือ 0.0045 ดังนั้นจึงเลือกใช้งานระบบเครือข่ายใยประสาทที่มีสถาปัตยกรรมชั้นแฝง 15 หน่วย ในการประเมินคุณภาพการบุกรุกระบบเครือข่ายแบบสแกนระบบเครือข่าย

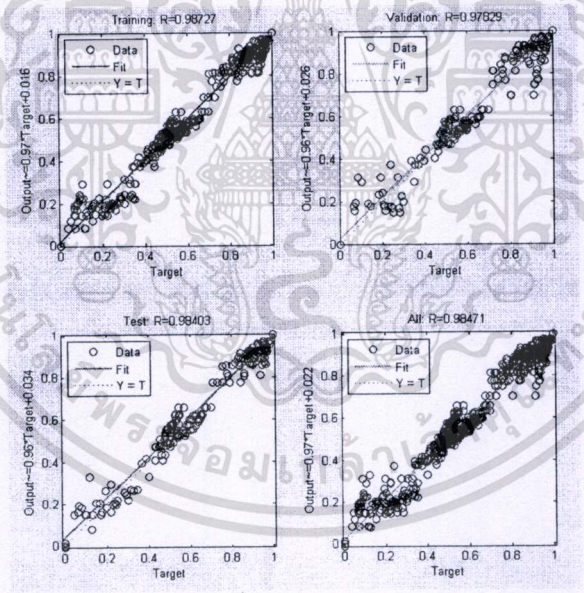
4.2.4 ผลการทดสอบระบบเครือข่ายใยประสาทที่ใช้ประเมินคุณภาพการแจ้งเตือน การบุกรุกระบบเครือข่ายด้วยมัลแวร์



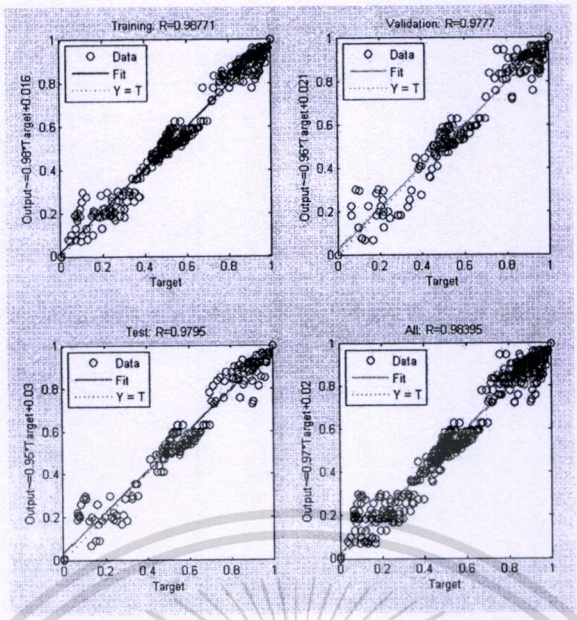
รูปที่ 4.38 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 10 หน่วย ด้วย การบุกรุกระบบเครือข่ายด้วยมัลแวร์



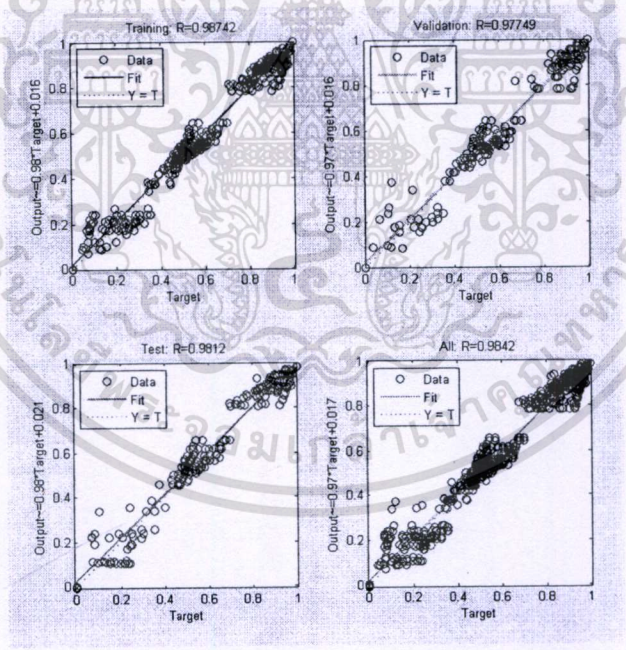
รูปที่ 4.39 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 15 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



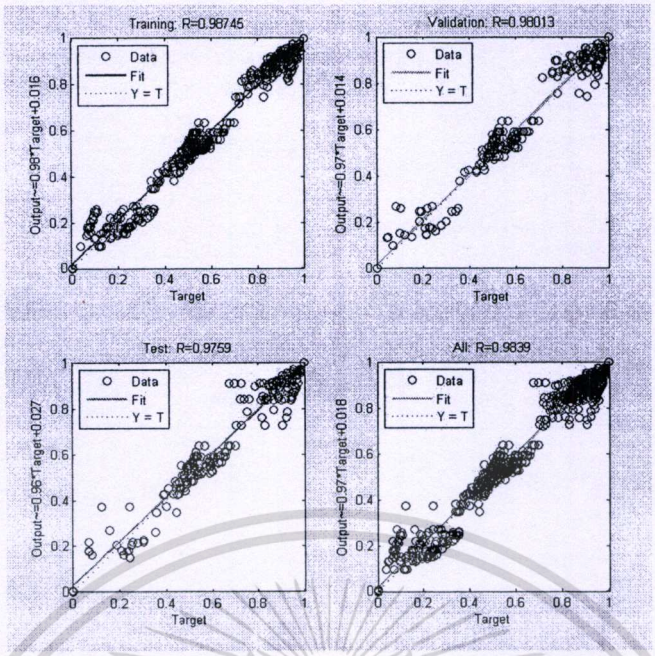
รูปที่ 4.40 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 1 ชั้น ชั้นที่ 1 มี 20 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



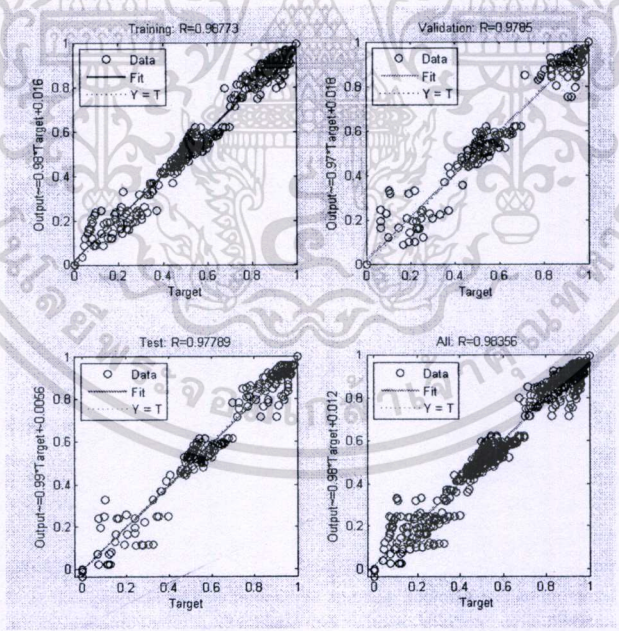
รูปที่ 4.41 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



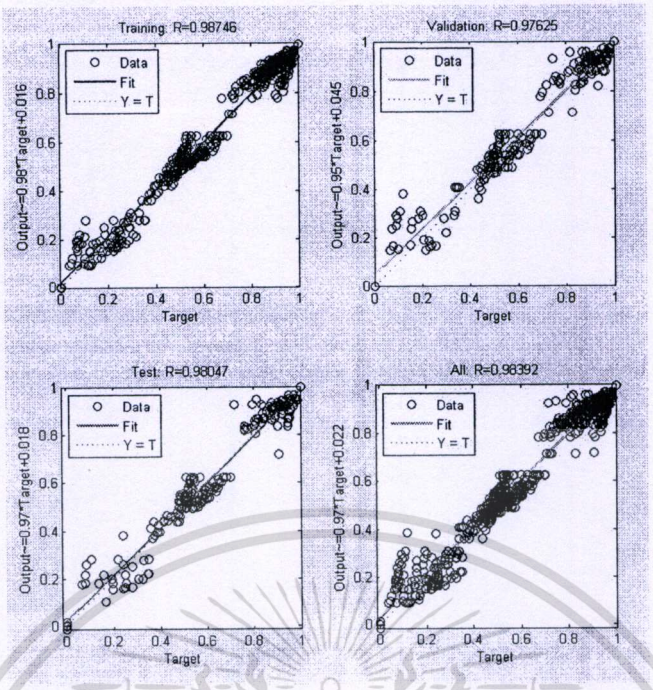
รูปที่ 4.42 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



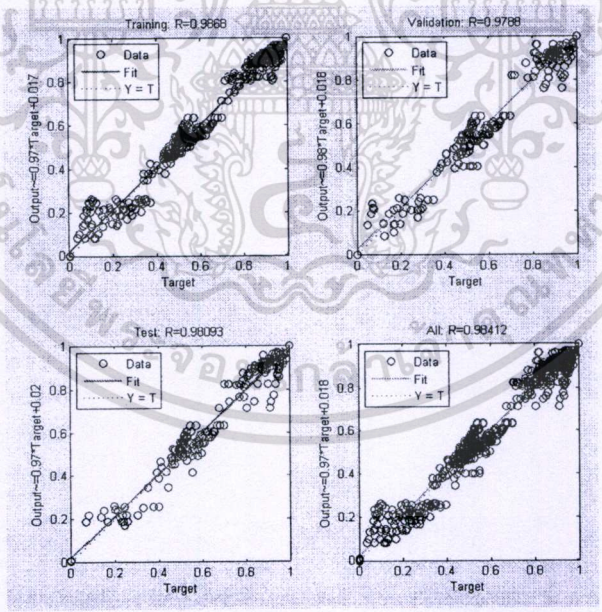
รูปที่ 4.43 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



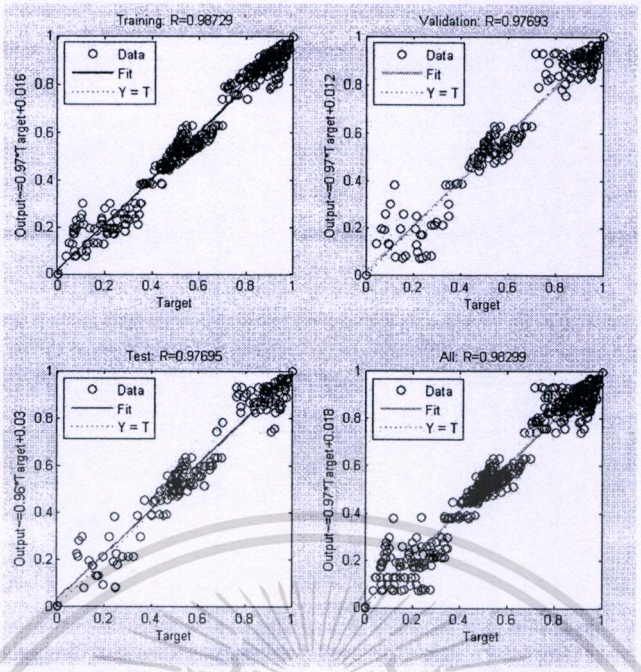
รูปที่ 4.44 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15หน่วย และ ชั้นที่ 2 มี 10 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



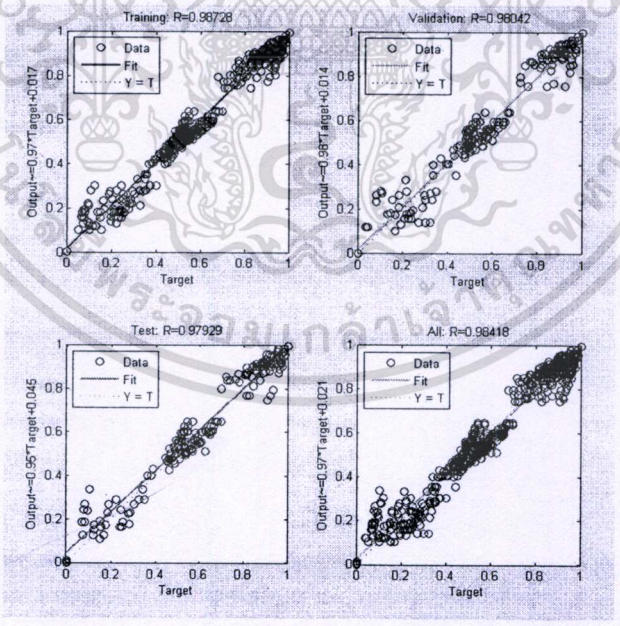
รูปที่ 4.45 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



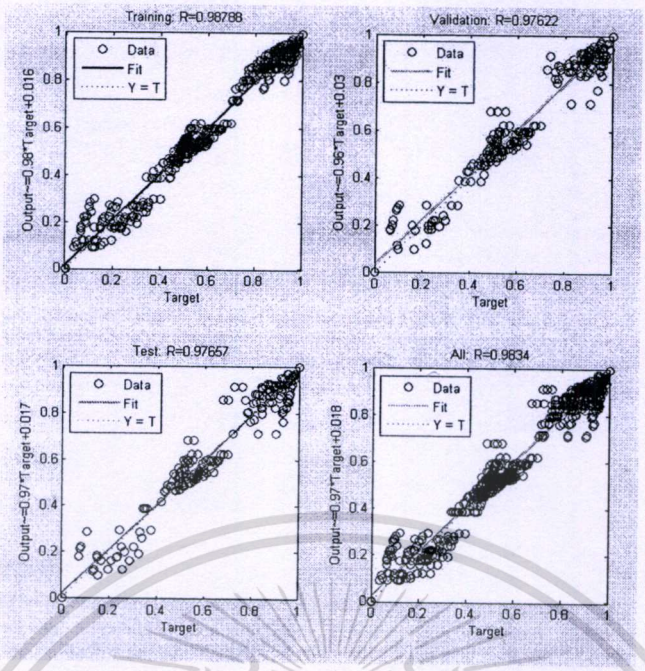
รูปที่ 4.46 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



รูปที่ 4.47 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



รูปที่ 4.48 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์



รูปที่ 4.49 ผลการทดลองระบบเครือข่ายใยประสาทมีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย ของการบุกรุกระบบเครือข่ายด้วยมัลแวร์

จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายด้วยมัล-แวร์ สามารถแสดงตารางค่าประสิทธิภาพซึ่งวัดจากค่า RMSE Ratio ได้ดังนี้

ตารางที่ 4.4 ค่า RMSE Ratio จากการทดสอบระบบเครือข่ายใยประสาทกับชุดข้อมูลการบุกรุกระบบเครือข่ายแบบมัลแวร์

แบบที่	สถาปัตยกรรมระบบเครือข่ายใยประสาท	ค่า RMSE Ratio
1	ชั้นแฝง 1 ชั้น มี 10 หน่วย	0.0022
2	ชั้นแฝง 1 ชั้น มี 15 หน่วย	0.0026
3	ชั้นแฝง 1 ชั้น มี 20 หน่วย	0.0027
4	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0029
5	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0027
6	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 10 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0026
7	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0032
8	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0030
9	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 15 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0027
10	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วย	0.0034

11	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 15 หน่วย	0.0028
12	ชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 20 หน่วย	0.0030

จากผลการทดลองจะเห็นได้ว่าค่า RMSE Ratio ของค่าความผิดพลาดจะมีค่าไม่เท่ากันในแต่ละสถาปัตยกรรมต่อค่าชุดน้ำหนัก เมื่อนำผลการทดลองที่ได้มาเปรียบเทียบจะพบว่าสถาปัตยกรรมที่มีชั้นแฝง 1 ชั้น มี 10 หน่วยมีค่า RMSE Ratio น้อยที่สุดคือ 0.0022 และสถาปัตยกรรมที่มีชั้นแฝง 2 ชั้น ชั้นที่ 1 มี 20 หน่วย และ ชั้นที่ 2 มี 10 หน่วยมีค่า RMSE Ratio มากที่สุดคือ 0.0034 ดังนั้นจึงเลือกใช้งานระบบเครือข่ายใยประสาทที่มีสถาปัตยกรรมชั้นแฝง 1 ชั้นจำนวน 10 หน่วย ในการประเมินคุณภาพการบุกรุกระบบเครือข่ายด้วยมัลแวร์

จากผลการทดลองหาสถาปัตยกรรมที่เหมาะสมที่ใช้ในการประเมินคุณภาพการแจ้งเตือนการบุกรุกระบบเครือข่ายทั้ง 4 แบบสามารถแสดงได้ในตารางที่ 4.5

ตารางที่ 4.5 สรุปสถาปัตยกรรมของระบบเครือข่ายใยประสาทที่ใช้ในการประเมินคุณภาพการแจ้งเตือนแต่ละประเภท

ระบบเครือข่ายใยประสาท	**สถาปัตยกรรมระบบเครือข่ายใยประสาท**	**ค่า RMSE Ratio**
การบุกรุกแบบ DoS	ชั้นแฝง 1 ชั้น มี 10 หน่วย	0.9929
การบุกรุกแบบพยายามค้นหารหัสผ่าน	ชั้นแฝง 1 ชั้น มี 15 หน่วย	0.0055
การบุกรุกแบบสแกนระบบเครือข่าย	ชั้นแฝง 1 ชั้น มี 15 หน่วย	0.0001
การบุกรุกด้วยมัลแวร์	ชั้นแฝง 1 ชั้น มี 10 หน่วย	0.0022

4.3 ผลการทดลองของระบบเมื่อเทียบกับวิธีพื้นฐาน

การแจ้งเตือนที่เกิดขึ้นของสนอร์ตเซ็นเซอร์ทั้ง 4 ตัวบนระบบเครือข่ายตั้งแต่วันที่ 20 เมษายน 2552 ถึงวันที่ 20 พฤษภาคม 2552 รวมเป็นระยะเวลา 1 เดือน ได้เกิดการแจ้งเตือนทั้งสิ้น แสดงดังต่อไปนี้

ตารางที่ 4.6 การแจ้งเตือนที่เกิดจากสนอร์ตเซ็นเซอร์ทั้ง 4 ตัวบนระบบเครือข่าย

Snort Sensor	Alert
Snort Sensor 1	2279
Snort Sensor 2	1055
Snort Sensor 3	476
Snort Sensor 4	429
รวม	4239

การแจ้งเตือนที่เกิดขึ้นจากสนอร์ตเซ็นเซอร์ทั้ง 4 ตัวรวมกัน 4239 ครั้งโดย สนอร์ตเซ็นเซอร์หมายเลข 1 สร้างการแจ้งเตือน 2279 ครั้งมากกว่าสนอร์ตเซ็นเซอร์ตัวอื่น ๆ มีสาเหตุมาจาก การที่สนอร์ตเซ็นเซอร์หมายเลข 1 ทำหน้าที่ตรวจสอบทราฟฟิคภายนอกที่เข้ามายังภายในระบบเครือข่ายทั้งหมด

เมื่อนำการแจ้งเตือนที่เกิดขึ้นทั้งหมดมาตรวจสอบ โดยการตรวจสอบข้อมูลของแพ็คเก็จรวมกับสถานะและสภาพแวดล้อมของระบบเครือข่ายทำให้สามารถจำแนกการแจ้งเตือนที่ถูกต้องและการแจ้งเตือนที่ผิดพลาดได้ดังต่อไปนี้

ตารางที่ 4.7 ผลการจำแนกการแจ้งเตือนที่ถูกต้องและการแจ้งเตือนที่ผิดพลาด

Snort Sensor	Alert	การแจ้งเตือนที่ถูกต้อง	การแจ้งเตือนที่ผิดพลาด
Snort Sensor 1	2279	1931	348
Snort Sensor 2	1055	919	136
Snort Sensor 3	476	353	123
Snort Sensor 4	429	346	83
รวม	**4239**	**3549**	**690**

ผลการจำแนกคุณภาพการแจ้งเตือนของสนอร์ตเซ็นเซอร์ทั้ง 4 ที่เกิดขึ้นภายในระบบเครือข่ายทำให้ทราบว่าการแจ้งเตือนทั้งหมด 4239 ครั้งเป็นการแจ้งเตือนที่ถูกต้องจำนวน 3549 ครั้งซึ่งคิดเป็นร้อยละ 83.72 และการแจ้งเตือนที่ผิดพลาด 690 ครั้งซึ่งคิดเป็นร้อยละ 16.28 ของการแจ้งเตือนทั้งหมด

เมื่อนำการแจ้งเตือนที่ถูกต้องมาแยกตามประเภทการบุกรุกระบบเครือข่ายจะพบว่าการบุกรุกระบบเครือข่ายด้วยมัลแวร์ถูกตรวจพบมากที่สุดเป็นจำนวน 1760 ครั้ง และการพยายามทำให้ระบบเครือข่ายไม่สามารถทำงานได้ (DoS) ถูกตรวจพบจำนวน 871 ครั้ง คิดเป็นร้อยละ 54.74 และ 24.93 ตามลำดับ แสดงในตารางที่ 4.8

ตารางที่ 4.8 การจำแนกการแจ้งเตือนที่ถูกต้องตามประเภทการบุกรกระบบเครือข่าย

Snort Sensor	การบุกรุกแบบ DoS	ค้นหารหัสผ่าน	สแกนระบบเครือข่าย	มัลแวร์	รวม
Snort Sensor 1	314	284	224	1109	**1931**
Snort Sensor 2	379	96	87	357	**919**
Snort Sensor 3	87	83	25	158	**353**
Snort Sensor 4	91	77	42	136	**346**
รวม	**871**	**540**	**378**	**1760**	**3549**

ผลการทดสอบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต โดยการนำการแจ้งเตือนที่เกิดขึ้นทั้ง 4239 ครั้งมาทดสอบกับระบบ ผลลัพธ์ที่ได้จากระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตแสดงในตารางที่ 4.9

ตารางที่ 4.9 คุณภาพการแจ้งเตือนที่ได้จากระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

Sensor	Alert	High Quality Alert		Number of High Quality Alert	Low Quality Alert	Number of Low Quality Alert
		เป็นการแจ้งเตือนที่ถูกต้อง	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง		การแจ้งเตือนที่ผิดพลาด	
Snort Sensor 1	2279	713	1338	**2051**	228	**228**
Snort Sensor 2	1055	299	674	**973**	82	**82**
Snort Sensor 3	476	154	223	**377**	99	**99**

Snort Sensor 4	429	111	258	**369**	60	**60**
รวม	**4239**			**3770**		**469**

ระดับค่าบ่งชี้การแจ้งเตือนที่ได้จากระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตทำให้ผู้ดูแลระบบเครือข่ายทราบได้ทันทีว่าการแจ้งเตือนที่เกิดขึ้นมีระดับค่าบ่งชี้การแจ้งเตือนเป็นแบบใด จากตารางที่ 4.9 สามารถสรุปได้ว่า สนอร์ตเซ็นเซอร์ทั้ง 4 ตัวสร้างการแจ้งเตือนที่ถูกต้องจำนวน 3770 ครั้ง ในขณะที่สร้างการแจ้งเตือนที่ผิดพลาดจำนวน 469 ครั้ง การแจ้งเตือนที่ผิดพลาดคิดเป็นคิดเป็นร้อยละ 11.06 ของการแจ้งเตือนทั้งหมด โดยสนอร์ตเซ็นเซอร์หมายเลข 1 ทำงานอยู่หลังไฟร์วอลล์นั้นถูกตรวจพบว่าได้สร้างการแจ้งเตือนที่ผิดพลาดจำนวน 228 ครั้ง สนอร์ตเซ็นเซอร์หมายเลข 2 ทำงานตรวจสอบทราฟฟิคระบบเครือข่ายย่อยเครื่องแม่ข่ายนั้นถูกตรวจพบว่าได้สร้างการแจ้งเตือนที่ผิดพลาดจำนวน 82 ครั้ง สนอร์ตเซ็นเซอร์หมายเลข 3 ตรวจสอบทราฟฟิคระบบเครือข่ายย่อยสำหรับการใช้งานอินเทอร์เน็ตนั้นถูกตรวจพบว่าได้สร้างการแจ้งเตือนที่ผิดพลาดจำนวน 99 ครั้ง และสนอร์ตเซ็นเซอร์หมายเลข 4 ทำงานตรวจสอบทราฟฟิคแผนกบัญชีนั้นถูกตรวจพบว่าได้สร้างการแจ้งเตือนที่ผิดพลาดจำนวน 60 ครั้ง

การแจ้งเตือนที่ผิดพลาดที่ระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตสามารถตรวจพบและคัดกรองได้ เมื่อนำมาตรวจสอบความถูกต้องแม่นยำในการทำงานของระบบพบว่าจำนวนการแจ้งเตือนที่ถูกต้องที่ถูกคัดกรองว่าเป็นการแจ้งเตือนผิดพลาด (False Negative) ที่ตรวจพบนั้นได้แสดงในตารางที่ 4.10

ตารางที่ 4.10 การแจ้งเตือนที่ถูกต้องที่ระบบไม่สามารถตรวจพบ

Sensor	การแจ้งเตือนทั้งหมด	การแจ้งเตือนที่ผิดพลาดที่ระบบตรวจพบ	การแจ้งที่ถูกต้องที่ระบบไม่สามารถตรวจพบ
Snort Sensor 1	2279	228	9
Snort Sensor 2	1055	82	6
Snort Sensor 3	476	99	4
Snort Sensor 4	429	60	2
รวม	**4239**	**469**	**21**

ประสิทธิภาพการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตที่สามารถตรวจพบการแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นภายในระบบเครือข่ายแสดงในตารางที่ 4.11

ตารางที่ 4.11 ประสิทธิภาพการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

Snort Sensor	การแจ้งเตือนทั้งหมด	การแจ้งเตือนที่ผิดพลาด	การแจ้งเตือนที่ผิดพลาดที่ระบบตรวจพบ	ประสิทธิภาพในการลดการแจ้งเตือนที่ผิดพลาด
Snort Sensor 1	2279	348	228	**62.93%**
Snort Sensor 2	1055	136	82	**55.88%**
Snort Sensor 3	476	123	99	**77.24%**
Snort Sensor 4	429	83	60	**67.47%**
รวม	**4239**	**690**	**469**	**64.92%**

จากตารางที่ 4.11 ประสิทธิภาพในการตรวจพบการแจ้งเตือนที่ผิดพลาดของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตเพียงร้อยละ 64.92 ซึ่งมีประสิทธิภาพค่อนข้างต่ำ ผู้วิจัยจึงปรับเปรุงเกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้องในระบบเครือข่ายใยประสาทใหม่ โดยเพิ่มระดับค่าบ่งชี้การแจ้งเตือนประเภทการบุกรุกให้มีค่าสูงขึ้นเพื่อให้ระบบเกิดการแจ้งเตือนที่ผิดพลาดลดลง เกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้องหลังการปรับปรุงแสดงในตารางที่ 4.12

ตารางที่ 4.12 เกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้องก่อนการปรับปรุง และหลังการปรับปรุง

ระบบเครือข่ายแต่ละประเภท	เกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้อง	เกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้องที่ผ่านการปรับปรุง
ระบบเครือข่ายใยประสาท DoS	780 – 1000	815 – 1000
ระบบเครือข่ายใยประสาท Password	75 – 100	75 - 100
ระบบเครือข่ายใยประสาท Scan Network	8 – 10	8 – 10
ระบบเครือข่ายใยประสาท Malware	0.8 – 1	0.83 - 1

การปรับเกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้องได้พิจารณาจากสาเหตุความผิดพลาดในการประเมินระดับค่าบ่งชี้การแจ้งเตือนจากการบุกรุกระบบเครือข่ายในรูปแบบต่างๆ การประเมินระดับค่าบ่งชี้การแจ้งเตือนที่เกิดจากการบุกรุกโดยมัลแวร์และการพยายามทำให้ระบบเครือข่ายไม่สามารถทำงานได้มีการแจ้งเตือนที่ผิดพลาดเกิดขึ้นเป็นจำนวนมาก ซึ่งเป็นสาเหตุหลักที่ทำให้ประสิทธิภาพของระบบต่ำ ดังนั้นผู้วิจัยจึงได้ทำการปรับระดับการแจ้งเตือนที่ถูกต้องในการ

ประเมินระดับค่าบ่งชี้การแจ้งเตือนของการบุกรุกระบบเครือข่ายด้วยมัลแวร์ และการพยายามทำให้ระบบเครือข่ายไม่สามารถใช้งานได้เท่านั้น

ผลการทดสอบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตที่ผ่านการปรับปรุงเกณฑ์การแจ้งเตือนที่ถูกต้องแสดงในตารางที่ 4.13

ตารางที่ 4.13 คุณภาพการแจ้งเตือนที่ได้จากระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตที่ผ่านการปรับปรุงเกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้อง

Sensor	Alert	High Quality Alert		Number of High Quality Alert	Low Quality Alert	Number of Low Quality Alert
		เป็นการแจ้งเตือนที่ถูกต้อง	เกือบจะเป็นการแจ้งเตือนที่ถูกต้อง		การแจ้งเตือนที่ผิดพลาด	
Snort Sensor 1	2279	713	1259	**1972**	307	**307**
Snort Sensor 2	1055	299	641	**940**	115	**115**
Snort Sensor 3	476	154	219	**373**	103	**103**
Snort Sensor 4	429	111	243	**354**	75	**75**
รวม	**4239**			**3639**		**600**

ผลการทดลองตารางที่ 4.13 แสดงให้เห็นว่าเมื่อทำการปรับเกณฑ์การแจ้งเตือนที่ถูกต้องของการตรวจจับการบุกรุกระบบเครือข่ายด้วยมัลแวร์ และการพยายามทำให้ระบบเครือข่ายไม่สามารถทำงานได้ ระบบจะสามารถตรวจพบการแจ้งเตือนที่ผิดพลาดได้เพิ่มขึ้นจากเดิมจำนวน 469 ครั้ง เป็น 600 ครั้ง คิดเป็นร้อยละ 27.93

เมื่อนำการแจ้งเตือนที่ผิดพลาดมาตรวจหาการแจ้งเตือนที่เป็นการบุกรุกระบบเครือข่ายจริงที่ระบบไม่สามารถตรวจพบ แสดงในตารางที่ 4.14

ตารางที่ 4.14 การแจ้งเตือนที่ถูกต้องที่ระบบไม่สามารถตรวจพบหลังการปรับปรุงเกณฑ์การแจ้งเตือนที่ถูกต้อง

Sensor	การแจ้งเตือนทั้งหมด	การแจ้งเตือนที่ผิดพลาดที่ระบบตรวจพบ	การแจ้งที่ถูกต้องที่ระบบไม่สามารถตรวจพบ
Snort Sensor 1	2279	307	10
Snort Sensor 2	1055	115	7
Snort Sensor 3	476	103	5
Snort Sensor 4	429	75	4

รวม	**4239**	**600**	**26**

ตารางที่ 4.14 แสดงให้เห็นว่าระบบจะทำให้ไม่สามารถตรวจพบการบุกรุกระบบเครือข่ายจริงจากจำนวน 21 ครั้งเป็นจำนวน 26 ครั้ง

ประสิทธิภาพการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตที่ผ่านการปรับปรุงเกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้อง สามารถตรวจพบการแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นภายในระบบเครือข่ายแสดงในตารางที่ 4.15

ตารางที่ 4.15 ประสิทธิภาพการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตที่ผ่านการปรับปรุงเกณฑ์คุณภาพการแจ้งเตือนที่ถูกต้อง

Snort Sensor	**การแจ้งเตือนทั้งหมด**	**การแจ้งเตือนที่ผิดพลาด**	**การแจ้งเตือนที่ผิดพลาดที่ระบบตรวจพบ**	**ประสิทธิภาพในการลดการแจ้งเตือนที่ผิดพลาด**
Snort Sensor 1	2279	348	307	85.34%
Snort Sensor 2	1055	136	115	79.41%
Snort Sensor 3	476	123	103	79.67%
Snort Sensor 4	429	83	75	85.54%
รวม	**4239**	**690**	**600**	**83.19%**

ผลการทดลองในตารางที่ 4.15 ประสิทธิภาพของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตเพิ่มขึ้นจากร้อยละ 64.92 เป็นร้อยละ 83.19 เมื่อทำการปรับปรุงระดับคุณภาพการแจ้งเตือนที่ถูกต้องของการตรวจจับการบุกรุกระบบเครือข่ายโดยมัลแวร์ และการพยายามทำให้ระบบเครือข่ายไม่สามารถทำงานได้ ประสิทธิภาพการทำงานของสนอร์ตเซ็นเซอร์หมายเลข 1 สามารถตรวจจับการบุกรุกระบบเครือข่ายได้ร้อยละ 85.34 ประสิทธิภาพการทำงานของสนอร์ตเซ็นเซอร์หมายเลข 2 สามารถตรวจจับการบุกรุกระบบเครือข่ายได้ร้อยละ 79.71 ประสิทธิภาพการทำงานของสนอร์ตเซ็นเซอร์หมายเลข 3 สามารถตรวจจับการบุกรุกระบบเครือข่ายได้ร้อยละ 79.67 และประสิทธิภาพการทำงานของสนอร์ตเซ็นเซอร์หมายเลข 4 สามารถตรวจจับการบุกรุกระบบเครือข่ายได้ร้อยละ 85.54

ข้อผิดพลาดจากการทำงานของระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตคิดจากการที่ระบบไม่สามารถตรวจพบการบุกรุกจริงบนระบบเครือข่าย (False Negative) และการแจ้งเตือนที่ผิดพลาดที่ระบบสร้างขึ้น (False Positive) โดยข้อผิดพลาดของระบบได้แสดงในตารางที่ 4.16

ตารางที่ 4.16 ค่าความผิดพลาดที่เกิดจากการทดสอบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต

Snort Sensor	การแจ้งเตือนทั้งหมด	การแจ้งเตือนที่ถูกต้อง	การแจ้งเตือนที่ระบบสร้างขึ้น	การแจ้งเตือนที่ผิดพลาด %	การแจ้งเตือนที่ถูกต้อง ที่ระบบไม่สามารถตรวจพบ	การตรวจไม่พบ %
Snort Sensor 1	2279	1931	**1972**	14.60	10	0.44
Snort Sensor 2	1055	919	**940**	20.59	7	0.66
Snort Sensor 3	476	353	**373**	20.33	5	1.05
Snort Sensor 4	429	346	**354**	14.46	4	0.93
รวม	**4239**	**3549**	**3639**	**16.81**	**26**	**0.61**

ผลการทดสอบระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต ทำให้ทราบว่าระบบดังกล่าวจะสามารถลดการแจ้งเตือนที่ผิดพลาดที่เกิดขึ้นบนระบบเครือข่ายได้ร้อยละ 83.19 ข้อผิดพลาดที่เกิดจากการทำงานของระบบสามารถแยกออกเป็นสองส่วน คือส่วนแรกระบบไม่สามารถคัดกรองการแจ้งเตือนที่ถูกต้องได้ร้อยละ16.81 และส่วนที่สองระบบไม่สามารถตรวจพบการแจ้งเตือนที่เป็นการบุกรุกระบบเครือข่ายจริงได้ร้อยละ 0.61

การแจ้งเตือนที่เกิดขึ้นทั้งหมดผู้ดูแลระบบเครือข่ายจะไม่ทราบได้โดยทันทีว่าการแจ้งเตือนใดเป็นการแจ้งเตือนที่ผิดพลาด หรือการแจ้งเตือนใดเป็นการแจ้งเตือนที่ถูกต้อง ผู้ดูแลระบบเครือข่ายต้องทำการวิเคราะห์สาเหตุการแจ้งเตือนที่เกิดขึ้น และทำการปิดช่องโหว่เมื่อมีการบุกรุกระบบเครือข่ายจริง การแจ้งเตือนที่เกิดขึ้นจำนวนมากทำให้ผู้ดูแลระบบเครือข่ายจะต้องเสียเวลามากในการวิเคราะห์ถึงสาเหตุการแจ้งเตือนที่เกิดขึ้น หากทำการปิดช่องโหว่ที่เกิดจากการบุกรุกเครือข่ายไม่ทันเวลาจะทำให้ระบบเครือข่ายตกอยู่ในอันตรายต่อผู้ไม่ประสงค์ดีได้

เมื่อนำระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตไปใช้งานจริงจะทำให้ผู้ดู-แลระบบเครือข่ายสามารถจำแนกประเภทการบุกรุกระบบเครือข่าย และคุณภาพของการแจ้งเตือนที่เกิดขึ้นได้อย่างมีประสิทธิภาพ และสามารถป้องกันอันตรายที่จะเกิดขึ้นกับระบบเครือข่ายได้อย่างทันท่วงที

4.4 ผลการทดลองของระบบเมื่อเทียบกับวิธีการอื่น

ตารางที่ 4.17 ผลการทดลองที่ได้จากระบบ False Positive Reduction via Intrusion Alert Quality Framework

Sensor	Alert	High Quality Alert			Sum of High Quality	Low Quality Alert		Sum of Low Quality
		S = 10	8<= S < 10	5<= S<8		0 < S < 5	S = 0	
Snort Sensor 1	2279	554	764	752	**2070**	124	85	**209**
Snort Sensor 2	1055	237	258	469	**964**	59	32	**91**
Snort Sensor 3	476	68	177	157	**402**	30	24	**74**
Snort Sensor 4	429	94	173	119	**386**	24	19	**43**
รวม	**4239**				**3822**			**417**

* S แทนคะแนนที่ระบบคำนวณได้

ตรวจสอบการแจ้งเตือนที่ผิดพลาดที่ระบบสามารถคัดกรองได้ ไม่พบว่าการแจ้งเตือนใดเป็นการแจ้งเตือนเมื่อเกิดการบุกรุกระบบเครือข่ายจริง ประสิทธิภาพการทำงานของระบบแสดงในตารางที่ 4.18

ตารางที่ 4.18 ประสิทธิภาพการทำงานของระบบที่นำมาเปรียบเทียบ

Snort Sensor	การแจ้งเตือนทั้งหมด	การแจ้งเตือนที่ผิดพลาด	การแจ้งเตือนที่ผิดพลาดที่ระบบตรวจพบ	ประสิทธิภาพในการลดการแจ้งเตือนที่ผิดพลาด
Snort Sensor 1	2279	348	209	60.06%
Snort Sensor 2	1055	136	91	66.91%
Snort Sensor 3	476	123	74	60.12%
Snort Sensor 4	429	83	43	51.81%
รวม	**4239**	**690**	**417**	**60.43%**

ตารางที่ 4.18 แสดงประสิทธิภาพการทำงานของระบบที่นำมาเปรียบเทียบกับระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต พบว่าระบบดังกล่าวสามารถลดการแจ้งเตือนที่ผิดพลาดได้ร้อยละ 60.43 ค่าความผิดพลาดที่ระบบไม่สามารถคัดกรองการแจ้งเตือนที่ผิดพลาดออกจากการแจ้งเตือนที่ถูกต้องคิดเป็นร้อยละ 39.57 และค่าความผิดพลาดที่ระบบไม่สามารถตรวจพบการแจ้งเตือนที่ถูกต้องคิดเป็นร้อยละ 0

ตารางที่ 4.19 เปรียบเทียบประสิทธิภาพและค่าความผิดพลาดของระบบที่นำเสนอ

การเปรียนเทียบ	ระบบที่นำเสนอ	ระบบที่นำมาเปรียบเทียบ[1]
1. ประสิทธิภาพของระบบ	83.19 %	60.43%
2. ความผิดพลาดในการคัดกรอง การแจ้งเตือนที่ผิดพลาด	16.81 %	39.57 %
3. ความผิดพลาดในการตรวจคัดกรองการแจ้งเตือนที่ถูกต้อง	0.61 %	0 %

จากตารางที่ 4.19 แสดงให้เห็นว่าระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตสามารถลดการแจ้งเตือนที่ผิดพลาดได้ดีกว่าระบบที่นำมาเปรียบเทียบถึงร้อยละ 22.76 และมีข้อผิดพลาดในการคัดกรองการแจ้งเตือนที่ผิดพลาดน้อยกว่าร้อยละ 22.76 แต่ระบบที่นำเสนอมีข้อผิดพลาดในการคัดกรองการแจ้งเตือนที่ถูกต้องร้อยละ 0.61 ซึ่งระบบที่นำมาเปรียบเทียบไม่เกิดข้อผิดพลาดดังกล่าว

บทที่ 5
สรุปผลการวิจัย และข้อเสนอแนะ

การรักษาความปลอดภัยบนระบบเครือข่ายมีอยู่หลายวิธีด้วยกันดังที่ได้กล่าวข้างต้น แต่เนื่องจากอุปกรณ์รักษาความปลอดภัยบนระบบเครือข่ายมีราคาสูง โปรแกรมสนอร์ตจึงเป็นทางเลือกหนึ่งในการรักษาความปลอดภัยบนระบบเครือข่ายสำหรับองค์กรที่มีขนาดกลางและขนาดเล็ก โปรแกรมสนอร์ตเป็นฟรีแวร์ที่ใช้ในการตรวจจับการบุกรุกบนระบบเครือข่ายที่ผู้ใช้งานสามารถนำมาใช้โดยไม่เสียค่าใช้จ่าย โปรแกรมสนอร์ตตรวจจับการบุกรุกโดยใช้กฎที่ถูกกำหนดโดยผู้ดูแลระบบเครือข่าย หากมีการกำหนดกฎที่ไม่ดีจะทำให้โปรแกรมสนอร์ตสร้างการแจ้งเตือนที่ผิดพลาดขึ้น การแจ้งเตือนที่ผิดพลาดได้สร้างความวุ่นวายให้กับผู้ดูแลระบบเครือข่ายที่จะต้องวิเคราะห์หาสาเหตุดังกล่าว

ในวิทยานิพนธ์ฉบับนี้จึงได้นำเสนอวิธีการลดการแจ้งเตือนของโปรแกรมสนอร์ตด้วยระบบประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต โดยระบบจะทำหน้าที่จำแนกประเภทการบุกรุกระบบเครือข่าย และประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ต จากนั้นนำผลลัพธ์ที่ได้นำเสนอต่อผู้ดูแลระบบเครือข่าย ผู้ดูแลระบบเครือข่ายจะเป็นผู้นำระดับคุณภาพการแจ้งเตือนที่ได้ไปทำการปรับลดกฎของโปรแกรมสนอร์ต การประเมินคุณภาพการแจ้งเตือนของโปรแกรมสนอร์ตระบบจะทำการจัดเก็บการแจ้งเตือนที่เกิดขึ้น และข้อมูลที่เกี่ยวข้องในขณะที่เกิดการแจ้งเตือนลงในฐานข้อมูลของระบบ ข้อมูลจะถูกวิเคราะห์เพื่อนำมากำหนดค่าให้กับพารามิเตอร์นำไปใช้เป็นข้อมูลนำเข้าในระบบเครือข่ายใยประสาท ระบบเครือข่ายใยประสาทจะทำหน้าที่จำแนกประเภทการบุกรุกระบบเครือข่าย และการประเมินระดับค่าบ่งชี้การแจ้งเตือนระดับค่าบ่งชี้การแจ้งเตือนที่ได้จะถูกนำมานำเสนอต่อผู้ดูแลระบบเครือข่าย ซึ่งจากการทดลองแสดงให้เห็นว่าเมื่อนำวิธีการที่นำเสนอมาใช้ในการประเมินคุณภาพการแจ้งเตือนที่เกิดขึ้นของโปรแกรมสนอร์ต จะทำให้โปรแกรมสนอร์ตเกิดการแจ้งเตือนที่ผิดพลาดน้อยลง กฎที่เป็นสาเหตุที่ทำให้เกิดการแจ้งเตือนที่ผิดพลาดจะถูกปรับลดโดยผู้แลระบบเครือข่าย ส่งผลให้โปรแกรมสนอร์ตทำงานได้มีประสิทธิภาพดีกว่าเมื่อเปรียบเทียบกับวิธีพื้นฐาน วิธีการที่นำเสนอสามารถลดการแจ้งเตือนเตือนที่ผิดพลาดของโปรแกรมสนอร์ตได้ถึงร้อยละ 83.27

ระบบควรมีความยืดหยุ่นในการทำงานเพื่อรองรับรูปแบบการบุกรุกระบบเครือข่ายรูปแบบใหม่ ๆ ที่เกิดขึ้น และควรใช้ระยะเวลาในการทำงานที่น้อยลงเนื่องจากปัจจุบันความเร็วในการรับส่งข้อมูลได้ถูกพัฒนาให้สามารถรับส่งข้อมูลได้เร็วขึ้น หากระบบทำงานโดยใช้เวลาในการทำงานสูงก็จะทำให้ระบบไม่สามารถตรวจสอบแพ็คเก็จที่ผ่านเข้ามาในระบบเครือข่ายทั้งหมดได้

วิธีการที่นำเสนอในวิทยานิพนธ์เป็นเทคนิคหนึ่งเท่านั้นที่ช่วยเพิ่มประสิทธิภาพในการทำงานของระบบตรวจจับการบุกรุกบนระบบเครือข่าย แต่ก็ยังมีเทคนิควิธีการอื่นที่น่าสนใจไม่ว่า

จะเป็นการประยุกต์ใช้ Fuzzy logical [5] การทำงานด้วยเอเจ็น [13] การวิเคราะห์ค่าทางสถิติ [17] หรือการนำหลายวิธีมาทำงานร่วมกัน [12] เป็นต้น การรักษาความปลอดภัยบนระบบเครือข่ายจะมีประสิทธิภาพสูงสุดจะต้องเป็นทำงานร่วมกันทั้งอุปกรณ์รักษาความปลอดภัยบนระบบเครือข่ายและการรักษาความปลอดภัยทางด้านกายภาพ ด้วยเช่นกัน

บรรณานุกรม

[1] A. Samsudin, B. Belaton, and N. Abu Bakar, **"Intrusion Alert Quality Framework,"** School of Computer Science University Science, Malaysia Penang Malaysia, IEEE, 2005.

[2] B. Caswell, J. Bealeand, J. C. Foster, and J. Faircloth, **"Snort 2.0 Intrusion Detection,"** Syngress, Feburary 2003.

[3] J. Koziol, **"Intrusion Detection with Snort,"** Mark Taber Associate Publisher Sams Publishing 201 West 103rd Street Indianapolis, IN 462090 USA, 1998.

[4] "**CERT/CC Advisories**", http://www.cert.org/advisories/ (27 July 2005).

[5] C. Kruegel and W. Robertson. **"Alert Verification - Determining the Success of Intrusion Attempts**" in Proc. First Workshop the Detection of Intrusions and Maiware & Vulnerability Assessment (DIMVA), 2004.

[6] **"Common Vulnerabilities and Exposures- The Standard for Information Security Vulnerability Names"**, http://www.cve.mitre.org (27 July 2005).

[7] D. E. Denning, **"An Intrusion-Detection Model,"** IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp.222-232,1987.

[8] E. Hooper, "**An Intelligent Detection and Response Strategy to False Positives and Network Attacks,**" Information Security Group, University of London Royal Holloway, Egham, Surrey, TW20 OEX, UK., 2006.

[9] I.V.M. Lima, **"A Simplified Accost of Intrusion Detection Based in Artificial Neural Networks,"** in portuguese, Master's thesis, Federal University of Santa Catarina, February, 2005.

[10] J. Cannady, **"Artificial Neural Networks to Misuse Detection,"** First International Workshop on the Recent Advances in Intrusion Detection, 1998.

[11] G. Helmer, J. Wong, V. Honavar and L. Miller, **"Automated discovery of concise predictive rules for intrusion detection,"** The Journal of Systems and Software, issue 60, pp. 165-175, 2002.

[12] K. Timm, **"Strategies to Reduce False Positives and False Negatives in NIDS,"** SecurityFocus Article, 2001, http:H/www.securityfocus.com/infocus/l463 (27 July 2005).

[13] K. Kono and M. Shimamura, "**Using Attack Information to Reduce False Positives in Network IDS**," Department of Information and Computer Science, Keio University,

IEEE, 2006.

[14] M. Norton and D. Roelker, **"Snort 2.0 Rule Optimizer,"** Sourcefire Network Security White Paper, April 2004.

[15] M. Roesch. **"Snort: Lightweight intrusion detection for networks,"** In Proc. of the 13th USENIX Conference on Systems Administration (LISA '99), pp. 229–238, 1999.

[16] **"OCS Inventory"**, http://www.OCSInventory.org (13 April 2009)

[17] P. A. Porras, M. W. Fong, and A. Valdes, **"A Mission Impact-Based Approach to INFOSEC Alarm Correlation,"** in Proc. 5th International Symposium, Recent Advances in Intrusion Detection (RAID) 2002, Springer Verlag Lecture Notes in Computer Science, October 2002.

[18] P. Ning, Y. Cui, and D. Reeves, **"Constructing Attack Scenarios through Correlation of Intrusion Alerts,"** CCS'02 Washington DC, US, 2002. R. Y. Wang, M. Ziad, and Y. W. Lee, Data Quality. Kluwer 2001.

[19] R. Ur Rehman, **"Intrusion Detection System with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP and ACID,"** Prentice Hall PTR, May 2003.

[20] R. Alder, J. Babbin, J. Beale, A. Doxtaer, Jame C. Foster, T. Konenberg and M. Rash, **"Snort 2.1 Intrusion Detecton Second Edition,"** Syngress Publishing, Inc. 800 Hingham Street Rockland, MA 02370, 2004.

[21] R. Goodman, **"Rule-Based Neural Networks for Classification and Probability Estimation,"**Neural Computation 4, pp. 781-804, 1992.

[22] Roesch and Martin, **"Snort – Lightweight Intrusion Detection for Network,"** In Proc. of the USENIX LISA Conference, November 1999.

[23] S. B. Cho and S. J. Han, **"Rule-based Integration of Multiple Measure-models for Effective Intrusion Detection,"** Yonsei University, Korea, 2003.

[24] S. M. Bridges and R. B. Vaughn, **"Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection,"** Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, 2000.

[25] S. Staniford-Chen, B. Tung, and D. Schnackenberg, **"The Common Intrusion Detection Framework (CIDF),"** Information Survivability Workshop,Orlando FL, October 1998.

[26] **"TIAA: A Toolkit for Intrusion Alert Analysis (Version 0.4),"** http:/discovery.csc.-ncsu.edu/software/correlator/ver0.4 (27 July 2005).

[27] V. Paxson. "**Bro: a System for Detecting Network Intruders in Realtime**". Computer-Networks, 31(23–24):2435–2463, 1999.

[28] W. Metcalf. **Snort-inline**. http://snort-inline.sourceforge.net/.

[29] W. Lee, S. J. Stolfo, and K. W. Mok, **"A Data Mining Framework for Building Intrusion Detection Models,"** In Proc. 1999 IEEE Symposium on Security and Privacy, May 1999.

[30] W. Yurcik, **"Controlling Intrusion Detection Systems by Generating False Positives: Squealing Proof-of-Concept,"** 27th Annual IEEE Conference on Local Computer Networks, 2002.

ภาคผนวก ก.

การกำหนด Rule Option ที่ใช้ในการกำหนดกฎของโปรแกรสนอร์ต

The ack Keyword

ส่วนหัวแพ็คเก็จของโปรโตคอล TCP จะมีค่าของฟิลด์ Acknowledgement Number ขนาด 32 บิตทำหน้าที่แสดงเลข Sequence Number เพื่อให้โฮสต์ที่ส่งแพ็คเก็จทราบ ผู้ใช้งานสามารถดูรายละเอียดในการกำหนดค่าได้จาก RFC793

การทำงานส่วนหัวของโปรโตคอล TCP nmap (http://www.nmap.org) ได้มีการนำเทคนิดดังกล่าวมาพัฒนาใช้กับคำสั่ง ping เมื่อ namp ใช้คำสั่ง ping ไปยังอุปกรณ์ต่างๆ ในระบบเครือข่าย nmap ทำการส่งแพ็คเก็จ TCP ไปยังพอร์ต 80 กำหนดค่า ACK flag และ Sequence Number ให้เป็น 0 ซึ่งแพ็คเก็จที่ส่งออกไปจะถูกปฏิเสธจากฝ่ายรับตามหลักการทำงานของโปรโตคอล TCP จากนั้นฝ่ายรับจะส่งแพ็คเก็จ RST กลับมาเมื่อ nmap ได้รับ RST แพ็คเก็จ nmap จะทราบทันที่ว่าโฮสต์นั้นมีอยู่จริง โดยวิธีการดังกล่าวจะถูกนำมาใช้งานเมื่อโฮสต์นั้นไม่ตอบสนอง “ICMP ECHO REQUEST” ของ ping แพ็คเก็จ การกำหนดกฎเพื่อตรวจจับการ ping โดยใช้ TCP แสดงรูปที่ ก.1

```
alert tcp any any -> 192.168.1.0/24 any (flags: A; \
ack:0; msg: “TCP ping detected”)
```

รูปที่ ก.1 กำหนดกฎเพื่อตรวจจับการ ping โดยใช้โปรโตคอล TCP

จากรูปที่ ก.1 จะมีการสร้างการแจ้งเตือนเมื่อเครื่องให้บริการได้รับแพ็คเก็จของโปรโตคอล TCP ที่มีการกำหนดค่า flag เป็น A และค่าของ Acknowledgement มีค่าเป็น 0 การกำหนดค่า flag ของโปรโตคอล TCP สามารถดูได้จากตารางที่ ก.1 โดยทั่วไปแล้วเมื่อมีการกำหนดค่า flag เป็น A ค่าของ ACK นั้นจะไม่เท่ากับ 0

The classtype Keyword

กฎของโปรแกรมสนอร์ตจะถูกแบ่งออกเป็นกลุ่มและตามลำดับความสำคัญของกฎ เพื่อให้เข้าใจการทำงานของคีย์เวิร์ด classtype อันดับแรกให้ผู้ใช้งานดูที่ไฟล์ classification.config ซึ่งถูกรวมอยู่ในไฟล์ snort.conf การกำหนดค่าของ classification.config มีรูปแบบแสดงดังรูปที่ ก.2

```
config classification: name,description,priority
```

รูปที่ ก.2 การกำหนดค่าของ classification.config

name จะถูกใช้ตั้งชื่อประเภทของกฎโดย *name* จะนำมาใช้งานร่วมกับคีย์เวิร์ด classtype *description* จะเป็นการอธิบายประเภทของกฎ *priority* จะเป็นตัวเลขแสดงถึงลำดับความสำคัญของกฎซึ่งเป็นค่าตั้งต้นที่ผู้ใช้งานสามารถแก้ไขได้ด้วยคีย์เวิร์ด priority รูปที่ ก.3 แสดงการกำหนดค่าใน classification.config

```
Config classification : DoS, Denial of Service Attack,2
```

รูปที่ ก.3 กำหนดประเภทและความสำคัญของกฎในไฟล์ classification.config

จากรูปที่ ก.3แบ่งประเภทของกฎเป็น DoS และมีลำดับความสำคัญเป็น 2 ผู้ใช้งานสามารถใช้ ACID ในการตรวจสอบประเภทของกฎซึ่ง ACID เป็นเครื่องที่ใช้ในการวิเคราะห์ข้อมูลการแจ้งเตือนทางเว็บไซต์ รูปที่ ก.4 ตัวอย่างการกำหนดกฎให้อยู่ในกลุ่ม DoS และใช้ค่าลำดับความสำคัญเดิม

```
Alert udp any any -> 192.168.1.0/24 6838 (msg: "DoS"; \
Content: "server"; classtype:DoS;)
```

รูปที่ ก.4 กำหนดให้กฎอยู่ในกลุ่ม DoS ที่มีลำดับความสำคัญเท่ากับค่าในไฟล์ classification.config

```
Alert udp any any -> 192.168.1.0/24 6838 (msg: "DoS"; \
Content: "server"; classtype:DoS; priority:1)
```

รูปที่ ก.5 กำหนดให้กฎอยู่ในกลุ่ม DoS ที่มีลำดับความสำคัญเท่ากับ 1

การจัดกลุ่มและกำหนดความสำคัญให้กับกฎทำให้ผู้ใช้งานสามารถแยกระหว่างการแจ้งเตือนที่มีความเสี่ยงสูงและการแจ้งเตือนที่มีความเสี่ยงต่ำได้อย่างมีประสิทธิภาพ

The content Keyword

คีย์เวิร์ด content เป็นคีย์เวิร์ดที่มีความสำคัญในการกำหนดกฎให้กับโปรแกรมสนอร์ต คีย์เวิร์ด content ใช้ในการค้นหาชุดข้อมูลภายในแพ็คเก็จโดยรูปแบบของชุดข้อมูลอาจอยู่ในรูปของ ASCII หรือไบนารีของเลขฐาน 16 ตัวอย่างเป็นกฎที่ใช้ในการตรวจหาสตริง "Get" ในแพ็คเก็จของโปรโตคอล TCP ออกมาจากระบบเครือข่าย192.168.1.0 ไปยังทุกระบบเครือข่ายที่ไม่ได้อยู่ในระบบเครือข่ายเดียวกันแสดงในรูปที่ ก.6

```
alert tcp 192.168.1.0/24 any -> ![192.168.1.0/24] any \
(content : "Get"; msg: "Get matched";)
```

รูปที่ ก.6 กำหนดกฎเพื่อตรวจหาสตริง "Get" ในแพ็คเก็จโปรโตคอล TCP

รูปที่ ก.7 เป็นกฎที่ทำงานเหมือนกับกฎรูปที่ ก.6 แต่เปลี่ยนรูปแบบในการค้นหาจากชุดสตริงเป็นเลขฐาน 16

```
alert tcp 192.168.1.0/24 any -> ![192.168.1.0/24] any \
        (content : "|47 45 54|"; msg: "Get matched";)
```

รูปที่ ก.7 กำหนดเพื่อตรวจสอบสตริง "Get" ในรูปแบบของเลขฐาน 16

47 ในเลขฐาน 16 จะมีค่าเท่ากับ G, 45 จะมีค่าเท่ากับ E และ 54 จะมีค่าเท่ากับ T ผู้ใช้งานสามารถกำหนดค่ารูปแบบการค้นหาในรูปแบบของ ASCII และไบนารีในรูปแบบของเลขฐาน 16 ได้ทั้ง 2 รูปแบบภายในกฎกฎเดียว การกำหนดรูปแบบของข้อมูลเป็นเลขฐาน 16 จะต้องคลอบด้วยเครื่องหมาย "| |" การใช้งานคีย์เวิร์ด content ต้องคำนึงถึงผลกระทบดังต่อไปนี้

-ในการเปรียบชุดข้อมูลจะใช้ประมาณหน่วยความจำในการประมวลสูงดังนั้นผู้ใช้งานจะต้องระมัดระวังในการกำหนดชุดข้อมูลให้กับกฎ

- การกำหนดชุดข้อมูลเป็น ASCII ผู้ใช้งานควรหลีกเหลี่ยงการอ้างอิงซ้ำ 2 ครั้ง,
- สามารถใช้งานคีย์เวิร์ด content ในการค้นหารูปแบบของข้อมูลได้มากกว่าหนึ่งชุดข้อมูลภายในหนึ่งกฎ
- การเปรียบเทียบชุดข้อมูลจะต้องคำนึงถึงกรณี เคสเซนซิทีฟ (case-sensitive)

มีคีย์เวิร์ดอยู่ 3 คีย์เวิร์ดที่ใช้งานร่วมกับคีย์เวิร์ด content โดยทั้ง 3 คีย์เวิร์ดจะใช้ในการเพิ่มเกณฑ์ในการค้นหารูปแบบข้อมูลภานในแพ็คเก็จ ซึ่งประกอบไปด้วย คีย์เวิร์ด offset, คีย์เวิร์ด depth และ คีย์เวิร์ด nocase

The offset Keyword

คีย์เวิร์ด offset จะนำมาใช้งานร่วมกับคีย์เวิร์ด content คีย์เวิร์ด offset จะถูกนำมากำหนดค่าเริ่มต้นในการค้นหาสตริงภายแพ็คเก็จ การกำหนดอากิวเม็นต์ให้กับคีย์เวิร์ด office จะเป็นเลขจำนวนเต็ม ตัวอย่างกำหนดกฎเพื่อค้นหาคำว่า "HTTP" ตั้งบิตที่ 5 ของแพ็คเก็จแสดงรูปที่ ก.8

```
Alert tcp 192.168.1.0/24 any -> any any \
        (content: "HTTP"; offset: 4; msg: "HTTP matched";)
```

รูปที่ ก.8 กำหนดกฎโดยใช้ คีย์เวิร์ด offset ในการค้นหาสตริง "HTTP"

The depth Keyword

คีย์เวิร์ด depth จะนำมาใช้งานร่วมกับคีย์เวิร์ด content เพื่อใช้กำหนดจุดสิ้นสุดในการตรวจสอบข้อมูล ผู้ใช้งานสามารถนำ คีย์เวิร์ด depth มาใช้งานร่วมกับ คีย์เวิร์ด offset เพื่อกำหนดขอบเขตในการค้นหาสตริงภายในแพ็คเก็จที่ชัดเจน ตัวอย่างกำหนดกฎเพื่อใช้ในการค้นหาคำว่า "HTTP" ที่อยู่ระหว่างตำแหน่งที่ 4 ถึง 40 ในส่วนข้อมูลแพ็คเก็จของโปรโตคอล TCP

```
alert tcp 192.168.1.0/24 any -> any any (content: \
        "HTTP"; offset: 4; depth: 40; msg: "HTTP matched";)
```

รูปที่ ก.9 กำหนดกฎเพื่อตรวจสอบ "HTTP" ที่อยู่ระหว่างตำแหน่งที่ 4 ถึง 40 ในส่วนข้อมูลแพ็คเก็จของโปรโตคอล TCP

The content-list Keyword

คีย์เวิร์ด content-list จะถูกใช้ในการตรวจสอบชื่อไฟล์ ชื่อไฟล์จะถูกใช้กำหนดเป็นอากิวเม็นท์ของคีย์เวิร์ด content-list ชื่อไฟล์จะประกอบไปด้วยรายชื่อของสตริงที่นำมาใช้ค้นหาสตริงภายในแพ็คเก็จ การกำหนดรายชื่อของสตริงจะต้องกำหนดให้อยู่กันคนละบรรทัด ตัวอย่างเช่น ไฟล์ชื่อว่า "porn" ประกอบด้วยสตริง 3 ชุดดังต่อไปนี้

"porn"
"hardcore"
"under 18"

```
alert ip any any -> 192.168.1.0/24 any (content-list: \
        "porn"; msg: "Porn word matched";)
```

รูปที่ ก.10 กำหนดกฎเพื่อใช้ในการตรวจสอบไฟล์ที่มีชื่อว่า "porn"

ผู้ใช้งานสามารถใช้เครื่องหมาย "!" ในการกำหนดเพื่อสร้างการแจ้งเตือนในกรณีที่ไม่พบสตริงตรงตามที่กำหนด

The dsize Keyword

คีย์เวิร์ด desize จะใช้ในการตรวจสอบขนาดของแพ็คเก็จ การโจมตีไปยังจุดอ่อนของระบบเครือข่ายแบบบัฟเฟอร์โอเวอร์โฟว์ (Buffer Overflow) ผู้บุกรุกจะส่งแพ็คเก็จที่มีขนาดใหญ่ทำให้ระบบเครือข่ายทำงานหนักจนไม่สามารถทำงานได้ ตัวอย่างกำหนดกฎเพื่อตรวจสอบแพ็คเก็จที่มีขนาดใหญ่กว่า 6,000 ไบต์แสดงรูปที่ ก.11

```
alert ip any any -> 192.168.1.0/24 any (dsize: > 6000; \
msg: "Large size IP packet detected";)
```

รูปที่ ก.11 กำหนดกฎเพื่อตรวจสอบแพ็คเก็จที่มีขนาดใหญ่กว่า 6,000 ไบต์

The flags Keyword

คีย์เวิร์ด flags จะใช้ในการตรวจสอบค่า flag bits ส่วนหัวแพ็คเก็จของโปรโตคอล TCP รายละเอียด flag bits ของโปรโตคอล TCP แสดงอยู่ใน RFC793 ที่ http://www.rfc.editor.org/rfc-editor.org/rfc/rfc793.txt ค่า flag bits ถูกนำมาใช้ในเครื่องมือรักษาความปลอดภัยบนระบบเครือข่ายตามวัตถุประสงค์ที่แตกต่างต่างกันออกไปเช่น เครื่องมือที่ใช้ในการสแกนพอร์ต nmap เป็นต้น

ตารางที่ ก.1 ค่าอาถิวเมนท์ที่นำมากำหนด flag bits ของโปรโตคอล TCP ที่นำมาใช้กับกฎของโปรแกรมสนอร์ต

Flag	อาถิวเม็นท์ที่ใช้งาน
FIN or Finish Flag	F
SYN or Sync Flag	S
RST or Reset Flag	R
PSH or Push Flag	P
ACK or Acknowledge Flag	A
URG or Urgent Flag	U
Reserved Bit 1	1
Reserved Bit 2	2
No Flag set	0

```
Alert tcp any any -> 192.168.1.0/24 any (flags: SF; \
Msg: "SYNC-FIN packet detected";)
```

รูปที่ ก.12 กำหนดกฎเพื่อตรวจสอบค่า flag bits ในส่วนหัวของโปรโตคอล TCP

The fragbits Keyword

ในส่วนหัวของโปรโตคอล IP จะประกอบไปด้วยค่า flag จำนวน 3 บิตมีหน้าที่ในการแบ่งย่อยแพ็คเก็จและ รวมแพ็คเก็จ (re-assembly) เข้าด้วยกัน โดยทั้ง 3 บิตมีรายละเอียดดังนี้

- Reserved Bit (RB) ใช้ในการสำรองบิตเพื่อนำไปใช้งานในอนาคต
- Don't Fragment Bit(DF) ถ้ามีการกำหนดค่าของ DF บิต แสดงว่าไม่มีการย่อยแพ็คเก็จของโปรโตคอล IP
- More Fragments Bit (MF) ถ้ามีการกำหนดค่าของ MF บิต แสดงแพ็คเก็จย่อยของโปรโตคอล IP แต่ถ้า MF บิตไม่ได้ถูกกำหนดค่าแสดงว่าเป็นแพ็คเก็จย่อยชิ้นสุดท้ายขนาด ขนาดของแพ็คเก็จที่สามารถส่งได้จะขึ้นอยู่กับค่า MTU ที่กำหนด

ข้อมูลเพิ่มเติมเกี่ยวข้องกับค่า Flag สามารถดูรายละเอียดได้จาก RFC791 ที่ http://www.rfc-editor.org/rfc/rfc791.txt บางครั้งผู้บุกรุกระบบเครือข่ายได้ใช้ค่า flag ในการโจมตีระบบเครือข่ายและค้นหาข้อมูลบนระบบเครือข่ายโดย DF บิตจะถูกใช้ในการค้นหาค่าต่ำสุดและค่าสูงสุดของ MTU ที่ใช้ในการรับส่งข้อมูล คีย์เวิร์ด fragbits ใช้ในการตรวจสอบค่า flag ของแพ็คเก็จ ตัวอย่างกำหนดกฎที่ใช้ในการตรวจหาค่า DF ที่ถูกกำหนดค่าไว้ในแพ็คเก็จของโปรโตคอล ICMP แสดงในรูปที่ ก.13

```
Alert icmp any any -> 192.168.1.0/24 any (fragbits: D; \
Msg: "Don't Fragment bit set";)
```

รูปที่ ก.13 กำหนดกฎเพื่อตรวจสอบค่า DF flag

จากรูปที่ ก.13 คีย์เวิร์ด fragbits ถูกกำหนดค่าเป็น "D" สำหรับการกำหนดค่าของ DF บิต "R" สำหรับการกำหนดค่า RB บิตและ "M" สำหรับการกำหนดค่า MF บิต โดยผู้ใช้งานสามารถใช้เครื่องหมาย "!" ในการกำหนดค่าคีย์เวิร์ด fragbits เพื่อตรวจสอบค่า flag ที่ไม่ได้ถูกกำหนดค่า ตัวอย่าง การกำหนดกฎที่ใช้ในการตรวจจับแพ็คเก็จถ้า DF บิตไม่ได้ถูกตั้งค่าแสดงในรูปที่ ก.14

```
Alert icmp any any -> 192.168.1.0/24 any (fragbits: !D; \
Msg: "Don't Fragment bit not set";)
```

รูปที่ ก.14 กำหนดกฎเพื่อตรวจสอบค่า DF บิตที่ไม่ได้ถูกกำหนด

โลจิค AND และ OR สามารถนำมาใช้ในการตรวจสอบบิตในกรณีที่มีการกำหนดค่าหลายค่าโดยแทนด้วยสัญลักษณ์ "+" ซึ่งจะใช้ในการตรวจสอบทุกๆบิต (AND) และสัญลักษณ์ "*" จะใช้ในการตรวจสอบบางบิต (OR)

The icmp_id Keyword

คีย์เวิร์ด icmp_id จะถูกใช้ในการตรวจสอบค่าในฟิลด์ ID แพ็คเก็จของโปรโตคอล ICMP รูปแบบของการใช้งานคีย์เวิร์ด icmp_id แสดงในรูปที่ ก.15

```
icmp_id : <ICMP_id_number>
```

รูปที่ ก.15 รูปแบบการกำหนดค่าอากิวเม็นต์ให้กับคีย์เวิร์ด icmp_id

ใน ICMP แพ็คเก็จจะพบฟิลด์ "ICMP ECHO REQUEST" และ "ICMP ECHO REPLY" ได้ถูกอธิบายไว้ใน RFC792 โดยฟิลด์นี้จะใช้ในการเปรียบเทียบกับ "ECHO REQUEST" และ "ECHO REPLY" เมื่อผู้ใช้งานใช้คำสั่ง "ping" โปรโตคอล ICMP ส่งข้อมูลแลกเปลี่ยนระหว่างผู้ส่งข้อมูลและผู้รับข้อมูล ผู้ส่งข้อมูลจะส่งแพ็คเก็จ "ECHO REQUEST" และผู้รับจะตอบกลับด้วยแพ็คเก็จ "ECHO REPLY" ตัวอย่างการกำหนดกฎที่ใช้ในการตรวจสอบค่าฟิลด์ ID ในส่วนหัวของโปรโตคอล ICMP ที่มีค่าเท่ากับ 100 แสดงในรูปที่ ก.16

```
alert icmp any any -> any any (icmp_id: 100; \
        msg: "ICMP ID=100";)
```

รูปที่ ก.16 กำหนดกฎเพื่อตรวจสอบค่าฟิลด์ id ในส่วนหัวของโปรโตคอล ICMP

The icmp_seq Keyword

คีย์เวิร์ด icmp_seq จะมีลักษณะการทำงานคล้ายกับคีย์เวิร์ด icmp_id การกำหนดค่าให้กับคีย์เวิร์ด icmp_seq แสดงในรูปที่ ก.17

```
icmp_seq: <ICMP_seq_number>
```

รูปที่ ก.17 กำหนดค่าอากิวเมนต์ให้กับคีย์เวิร์ด icmp_seq

ฟิลด์ sequence number จะอยู่ในส่วนหัวของแพ็คเก็จโปรโตคอล ICMP มันจะถูกนำเปรียบเทียบกับ ICMP ECHO REQUEST และ ICMP ECHO REPLY ซึ่งสามารถอ้างอิงได้จาก RFC792 คีย์เวิร์ด icmp_seq ถูกใช้ในการตรวจสอบค่าในฟิลด์ sequence number ที่มีลักษณะเฉพาะ ตัวอย่างกำหนดกฎใช้ในการตรวจสอบค่าในฟิลด์ sequence number ที่มีค่าเท่ากับ 100 แสดงในรูปที่ ก.18

```
alert icmp any any -> any any (icmp_seq: 100; \
msg: "ICMP Sequence=100";)
```

รูปที่ ก.18 กำหนดกฎเพื่อตรวจสอบค่าในฟิลด์ sequence number ที่มีค่าเท่ากับ 100

The itype Keyword

ส่วนหัวของโปรโตคอล ICMP จะถูกส่งมาหลังจากส่วนหัวของโปรโตคอล IP ภายในส่วนหัวของโปรโตคอล ICMP จะประกอบด้วยฟิลด์ type รายละเอียดของฟิลด์ type ได้ถูกอธิบายไว้ใน RFC792 ที่ http://www.rfc-editor.org/rfc/rfc792.txt คีย์เวิร์ด itype ถูกใช้ในการตรวจสอบค่าของฟิลด์ type ในส่วนหัวของแพ็คเก็จของโปรโตคอล ICMP การกำหนดค่าอากิวเม็นท์ให้กับคีย์เวิร์ด itype แสดงในรูปที่ ก.19

```
itype : "ICMP_type_number"
```

รูปที่ ก.19 กำหนดค่าอากิวเม็นต์ให้กับคีย์เวิร์ด itype

ฟิลด์ type ในส่วนหัวของแพ็คเก็จโปรโตคอล ICMP จะเป็นตัวกำหนดประเภทแพ็คเก็จของโปรโตคอล ICMP แสดงในตารางที่ ก.2

ตารางที่ ก.2 ค่าฟิลด์ type ในส่วนหัวแพ็คเก็จของโปรโตคอล ICMP

ค่า	ประเภทของ ICMP แพ็คเก็จ
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect
8	Echo request
11	Time exceed
12	Parameter problem
13	Timestamp request
14	Timestamp reply
15	Information request
16	Information reply

```
alert icmp any any -> any any (itype:4; \
        msg: "ICMP Source Quench Message received";)
```

รูปที่ ก.20 การกำหนดค่าเพื่อตรวจสอบค่าฟิลด์ type ในส่วนหัวแพ็คเก็จของโปรโตคอล ICMP

The icode Keyword

ส่วนหัวของโปรโตคอล ICMP จะถูกส่งมาหลังจากส่วนหัวของโปรโตคอล IP ซึ่งภายในของส่วนหัวโปรโตคอล ICMP จะประกอบด้วยฟิลด์ code ผู้ใช้งานสามารถดูรายละเอียดของฟิลด์ code ได้ที่ RFC792 ที่ http://www.rfc-editor.org/rfc/rfc792.txt คีย์เวิร์ด icode จะใช้ในการตรวจสอบค่าฟิลด์ code ที่อยู่ในส่วนหัวของโปรโตคอล ICMP การกำหนดค่าอากิวเม็นท์ให้กับคีย์เวิร์ด icode จะเป็นตัวเลขเท่านั้นแสดงในรูปที่ ก.21

```
Icode: "ICMP_codee_number"
```

รูปที่ ก.21 กำหนดค่าอากิวเม็นต์ให้กับคีย์เวิร์ด icode

ฟิลด์ type ในส่วนหัวของโปรโตคอล ICMP จะใช้แสดงประเภทข้อความของโปรโตคอล ICMP ฟิลด์ code จะถูกนำมาใช้ในการอธิบายฟิลด์ type ตัวอย่าง ถ้าฟิลด์ type มีค่าเท่ากับ 5 แสดงว่าแพ็คเก็จของโปรโตคอล ICMP จะเป็นแบบ "ICMP redirect" ซึ่งมีหลายสาเหตุสาเหตุดังกล่าวได้ถูกกำหนดไว้ในฟิลด์ code แสดงดังต่อไปนี้

- ฟิลด์ code มีค่าเท่ากับ 0 แสดงว่าระบบเครือข่ายส่งแพ็คเก็จ ICMP ซ้ำ
- ฟิลด์ code มีค่าเท่ากับ 1 แสดงว่าโฮสต์ส่งแพ็คเก็จซ้ำ
- ฟิลด์ code มีค่าเท่ากับ 2 แสดงว่ามีการส่งแพ็คเก็จซ้ำระหว่างประเภทการให้บริการ(Type of Service) กับระบบเครือข่าย
- ถ้า code ฟิลด์มีค่าเท่ากับ 2 แสดงว่ามีการส่งแพ็คเก็จซ้ำระหว่างประเภทการให้บริการกับโฮสต์

คีย์เวิร์ด icode จะถูกใช้ในตรวจสอบค่าฟิลด์ code ในส่วนหัวของโปรโตคอล ICMP การกำหนดอากิวเม็นต์ให้กับคีย์เวิร์ด icode แสดงในรูปที่ ก.22

```
alert icmp any any -> any any (itype: 5; \
        icode: 1; msg: "ICMP ID=100";)
```

รูปที่ ก.22 กำหนดกฎใช้ในการตรวจสอบค่าฟิลด์ code ในส่วนหัวของโปรโตคอล ICMP

จากรูปที่ ก.22 จะเป็นการกำหนดกฎโดยใช้คีย์เวิร์ด itype และคีย์เวิร์ด icode คีย์เวิร์ด icode เพียงค่าเดียวจะไม่สามารถทำให้กฎทำงานได้

The id Keyword

คีย์เวิร์ด id จะถูกใช้ในการเปรียบเทียบกับฟิลด์ ID ของแพ็คเก็จที่ถูกแบ่งย่อยออกมาของส่วนหัวของ IP แพ็คเก็จ ซึ่งคีย์เวิร์ด id จะถูกใช้ในการตรวจจับการบุกรุกที่มีการกำหนดค่าฟิลด์ ID ในส่วนหัวของ IP รูปแบบการใช้งานคีย์เวิร์ด id แสดงในรูปที่ ก.23

```
id : "id_number"
```

รูปที่ ก.23 รูปแบบการกำหนดค่าให้กับคีย์เวิร์ด id

ถ้าค่าของฟิลด์ id ในส่วนหัวของ IP มีค่าเป็นศูนย์แสดงว่าเป็นส่วนสุดท้ายของแพ็คเก็จที่ถูกแบ่งย่อยออกมาจาก IP แพ็คเก็จ (ในกรณีที่แพ็คเก็จนั้นถูกแบ่งออก) ถ้าแพ็คเก็จนั้นมีเพียงแพ็คเก็จเดียวไม่ได้ถูกแบ่งย่อยค่าของฟิลด์ id ก็จะมีค่าเป็นศูนย์ด้วยเช่นกันคีย์เวิร์ด id ของโปรแกรมสนอร์ตสามารถนำมาใช้กำหนดส่วนสุดท้ายของแพ็คเก็จที่ถูกแย่งย่อยออกมาจาก IP แพ็คเก็จ

The ipopts Keyword

ในไอพีเวอร์ชัน 4 ส่วนหัวของแพ็คเก็จจะมีความยาว 20 ไบต์ผู้ใช้งานสามารถเพิ่มอ๊อพชั่นให้กับส่วนหัวของ IP โดยความยาวของส่วนหัวที่เป็นส่วนของอ๊อพชั่นสามารถเพิ่มได้จนถึง 40 ไบต์ โดยอ๊อพชั่นที่ใช้จะถูกใช้ในวัตถุประสงค์ที่แตกต่างกันแสดงดังต่อไปนี้

- Record Route(rr)
- Time Stams(ts)
- Loose Source Routiong(lsrr)
- Strict Source Routing(ssrr)

รายละเอียดของอ๊อพชั่นในส่วนหัวของ IP นั้นสามารถดูได้จาก RFC791 ที่ http://www.rfc-editor.org/rfc/rfc791.txt อ๊อพชั่นจะถูกใช้ในการกำหนดกฎของของโปรแกรมสนอร์ตโดยอ๊อพชั่นในส่วนหัวของ IP ผู้บุกรุกระบบเครือข่ายจะใช้ในการค้นหาข้อมูลเกี่ยวกับระบบเครือข่ายตัวอย่างเช่น Loose Source Routing (lsrr) และ Strict Source Routing(ssrr) จะถูกผู้บุกรุกระบบเครือข่ายใช้ในการค้นหาเส้นทางของระบบเครือข่ายถ้าระบบเครือข่ายนั้นมีอยู่จริง ตัวอย่างเป็นการกำหนดกฎที่ใช้ในการตรวจจับผู้ที่พยายามบุกรุกระบบเครือข่ายโดยใช้ Loose Source Routing

```
Alert ip any any -> any any (ipopts: lsrr; \
        Msg: "Loose source routing attempt";)
```

รูปที่ ก.24 กำหนดกฎโดยใช้คีย์เวิร์ด ipopts ตรวจจับการบุกรุกระบบเครือข่ายที่ใช้อ๊อพชั่น "Loose Secure Routing"

The ip_proto Keyword

คีย์เวิร์ด ip_proto ใช้ปลั๊กอิน (Plug-In) ใน IP Proto เพื่อกำหนดเลขโปรโตคอลในส่วนหัวของ IP คีย์เวิร์ด ip_proto จะใช้หมายเลขโปรโตคอลในการกำหนดอากิวเม็นท์ ผู้ใช้งานสามารถดูชื่อและเลขโปรโตคอลได้ที่ไฟล์ /etc/protocols บนระบบปฏิบัติการยูนิค

ตารางที่ ก.3 ตัวอย่างชื่อโปรโตคอลและเลขโปรโตคอลในไฟล์ /etc/protocols

ax.25	93	AX.25	# AX.25 Frames
ipip	94	IPIP	# Yet Another IP encapsulation
micp	95	MICP	# Mobile Internetworking Control Pro.
scc-sp	96	SCC-SP	# Semaphore Communications Sec. Pro.
etherip	97	ETHERIP	# Ethernet-within-IP Encapsulation
encap	98	ENCAP	# Yet Another IP encapsulation
#	99		# any private encryption scheme
gmtp	100	GMTP	# GMTP
ifmp	101	IFMP	# Ipsilon Flow Management Protocol
pnni	102	PNNI	# PNNI over IP

```
Alert ip any any -> any any (ip_proto: ipip; \
        Msg : "IP-IP tunneling detected";)
```

รูปที่ ก.25 การกำหนดกฎใช้คีย์เวิร์ด ip_proto โดยใช้ชื่อโปรโตคอลเป็นค่าอากิวเม็นต์

```
Alert ip any any -> any any (ip_proto: 94; \
        Msg : "IP-IP tunneling detected";)
```

รูปที่ ก.26 การกำหนดใช้คีย์เวิร์ด ip_proto โดยใช้หมายเลขโปรโตคอลเป็นค่าอากิวเม็นต์

เลขโปรโตคอลได้ถูกกำหนดไว้ใน RFC1700 ที่ http://www.rfc-editor.org/rfc/rfc1700.txt เลขโปรโตคอลเลขล่าสุดสามารถดูข้อมูลได้จาก ICANN หรือที่เว็บไซต์ http://www.icann.org หรือ IANA ที่เว็บไซต์ http://www.iana.org

The logto Keyword

คีย์เวิร์ด logto จะใช้ในการเก็บประวัติของแพ็คเก็จไปไว้ในไฟล์ที่ต้องการ โดยรูปแบบการใช้งานคีย์เวิร์ด logto แสดงในรูปที่ ก.27

```
logto : logto_log
```

รูปที่ ก.27 การกำหนดคีย์เวิร์ด logto

```
alert icmp any any -> any any (logto: logto_log; ttl: 100;)
```

รูปที่ ก.28 การกำหนดกฎเพื่อเก็บข้อมูลของแพ็คเก็จโปรโตคอล ICMP ที่มีค่า TTL เท่ากับ 100 ไปยังไฟล์ logto_log โดยข้อมูลในไฟล์ logto_log ได้แสดงในรูปที่ ก.29

```
[root@conformix] # cat logto_log
07/03-03:57:56.496845 192.168.1.101 -> 192.168.1.2
ICMP TTL:100 TOS:0x0 ID:33822 IPLen:20 DgmLen:60
Type:8      Code:0      ID:768      Seq:9217      ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70      abcdefghijklmnop
71 72 73 74 75 76 77 61 62  63 64 65  66  67 68 69      qrstuvwabcdefghi

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[root@conformix] #
```

รูปที่ ก.29 ข้อมูลที่อยู่ในไฟลล์ logto_log

รายละเอียดของข้อมูล logto_log ไฟล์ที่ใช้ในการเก็บข้อมูลแสดงดังต่อไปนี้

- แสดงข้อมูลวันและเวลาของแพ็คเก็จที่เก็บข้อมูล
- ไอพีแอ็คเดซต้นทาง 192.168.1.101
- ไอพีแอ็คเดซปลายทาง 192.168.1.2
- โปรโตคอลที่ใช้งานคือโปรโตคอล ICMP
- ค่า TTL ในส่วนหัวของไอพีมีค่าเท่ากับ 100

- ค่า TOS (Type Of Service) ในส่วนหัวของไอพีมีค่าเท่ากับ 100 โดยค่า TOS เท่ากับ 0 แสดงว่าแพ็คเก็จที่เข้ามานั้นปรกติ รายละเอียดของค่า TOS สามารถหาข้อมูลได้จาก RFC791
- ID ของไอพีแพ็คเก็จ เป็น 33822
- ความยาวในส่วนหัวของไอพี มีขนาด 20 ไบต์
- ความยาวของแพ็คเก็จมีขนาด 60 ไบต์
- ฟิลด์ ICMP Type มีค่าเป็น 8
- ICMP Code มีค่าเป็น 0
- ICMP ID มีค่าเป็น 768
- ฟิลด์ ICMP Sequence มีค่าเป็น 9217
- ในส่วนของ ECHO แสดงว่าเป็น ICMP ECHO แพ็คเก็จ
- ส่วนที่เหลือเป็นส่วนของข้อมูลในส่วนหัวของ ICMP

สิ่งที่ต้องคำนึงถึงเมื่อใช้งานคีย์เวิร์ด logto หากไม่ระบุพาร์ทที่ใช้ในการจัดเก็บไฟล์ ไฟล์จะถูกสร้างขึ้น และจัดเก็บโดยอัตโนมัติในไดเร็กเทอรี่ /var/log/snort และจะต้องไม่เว้นวรรคหลังเครื่องหมาย "," หากเว้นวรรคโปรแกรมสนอร์ตจะคิดว่าการเว้นวรรคจะเป็นส่วนหนึ่งของชื่อไฟล์ หากผู้ใช้งานต้องการเว้นวรรคผู้ใช้งานจะต้องปิดชื่อของไฟล์ด้วยเครื่องหมาย ("")

The msg Keyword

คีย์เวิร์ด msg จะใช้ในการแสดงข้อความแจ้งเตือนและจัดเก็บประวัติโดยกำหนดข้อความแจ้งเตือนภายในเครื่องหมาย ("") รูปแบบการใช้งานคีย์เวิร์ด msg แสดงในรูปที่ ก.30

```
Msg : "Your message text here"
```

รูปที่ ก.30 การกำหนดค่าให้กับคีย์เวิร์ด msg

The nocase Keyword

คีย์เวิร์ด nocase จะถูกใช้งานร่วมกับคีย์เวิร์ด content ซึ่งคีย์เวิร์ด nocase จะไม่มีการกำหนดค่าอากิวเม็นต์ให้กับตัวมัน จุดประสงค์การใช้งานคีย์เวิร์ด nocase จะใช้ในการค้นหารูปแบบของข้อมูลในแพ็คเก็จที่เป็นเคสเซนซิทิฟ

The priority Keyword

คีย์เวิร์ด priority จะถูกใช้ในการกำหนดความสำคัญของกฎในการกำหนดอากิวเม็นท์ให้กับคีย์เวิร์ด priority จะต้องเป็นตัวเลขเท่านั้นโดยเลข "1" จะมีลำดับความสำคัญสูงสุด คีย์เวิร์ด priority จะใช้งานร่วมกับคีย์เวิร์ด classtype รูปที่ ก.31 ตัวอย่างการกำหนดกฎโดยใช้คีย์เวิร์ด priority ที่มีค่าอากิวเม็นเท่ากับ 10

```
Alert ip any any -> any any (ipopts: lsrr; \
        Msg: "Loose source routing attempt"; priority: 10;)
```

รูปที่ ก.31 กำหนดกฎด้วยคีย์เวิร์ด priority ให้มีค่าอากิวเม็นต์เท่ากับสิบ

The react Keyword

คีย์เวิร์ด react จะถูกใช้ในการบล็อกเว็บไซต์หรือเซอร์วิสต่าง แต่จะสามารถบล็อกได้เพียงบางส่วนเท่านั้น รูปที่ ก.32 กำหนดกฎเพื่อบล็อกการใช้งาน HTTP จากระบบเครือข่ายภายใน 192.168.1.0/24 ในการบล็อกการเข้าใช้งาน HTTP กฎจะทำการส่งแพ็คเก็จ TCP FIN ไปยังโฮสต์ที่ทำการส่งและรับแพ็คเก็จแทน เมื่อแพ็คเก็จตรงตามเงื่อนไขที่กฎกำหนด

```
alert tcp 192.168.1.0/24 any -> any 80 (msg: "Outgoing \
        HTTP connection"; react: block;)
```

รูปที่ ก.32 กำหนดกฎเพื่อบล็อกการใช้งาน HTTP ด้วยคีย์เวิร์ด react

รูปที่ ก.32 เป็นการกำหนดค่าให้คีย์เวิร์ด react ด้วยอากิวเม็นต์ "block" ผู้ใช้งานสามารถกำหนดค่าอากิวเม็นต์เป็น "warn" เมื่อต้องการส่งข้อความแจ้งเตือนไปยังผู้ใช้งานซึ่งสามารถนำมาใช้งานร่วมกับคีย์เวิร์ด msg เพื่อสร้างข้อความแจ้งเตือนไปยังผู้ใช้งาน แสดงรูปที่ ก.33

```
alert tcp 192.168.1.0/24 any -> any 80 (msg: "Outgoing \
        HTTP connection"; react: warn, msg;)
```

รูปที่ ก.33 การกำหนดกฎโดยการนำคีย์เวิร์ด msg มาใช้งานร่วมกับคีย์เวิร์ด react

The reference Keyword

คีย์เวิร์ด reference ใช้ในการเพิ่มข้อมูลอ้างอิงให้กับกฎโดยนำข้อมูลมาจากอินเทอร์เน็ตคีย์เวิร์ด reference จะไม่เกี่ยวข้องกับการกำหนดกฎ คีย์เวิร์ด reference จะไม่มีผลกระทบต่อการทำงานของโปรแกรมสอร์ต ตัวอย่างข้อมูลอ้างอิงที่สามารถนำมาใช้ในคีย์เวิร์ด reference เช่น CVE และ Bugtraq รูปที่ ก.34 การกำหนดกฎโดยใช้คีย์เวิร์ด reference และรูปที ก.35 แสดงผลลัพธ์ที่ได้จากรูปที่ ก.34

```
alert udp $EXTERNAL_NET any -> $HOME_NET 1900 \
(msg: "MISC UPNP malformed advertisement"; \
Content : "NOTIFY * "; nocase; classtype:misc-attack; \
Reference : cve, CAN-2001-0876; reference:cve, \
CAN-2001-0877; sid:1384; rev:2;)
```

รูปที่ ก.34 กำหนดกฎโดยใช้คีย์เวิร์ด reference

```
[**]  [1:1384:2] MISC UPNP malformed advertisement [**]
[Classification: Misc Attack] [Priority: 2]
12/01-15:25:21.792758  192.168.1.1:1901 -> 239.255.255.255.250:1900
UDP TTL:150 TOS: 0x0  ID:9  IpLen:20  DgmLen:341
Len: 321
[Xref => cve CAN-2001-0877] [Xref => cve CAN-2001-0876]
```

รูปที่ ก.35 ผลลัพธ์ที่ได้จากการกำหนดกฎด้วยคีย์เวิร์ด reference จากรูปที่ ก.34

บรรทัดสุดท้ายของการแจ้งเตือนแสดงถึงที่มาของข้อมูลอ้างอิงอื่น ๆ ที่เกี่ยวข้องกับการแจ้งเตือนที่เกิดขึ้น โดยไฟล์ reference.config มีความสำคัญอย่างยิ่งในการกำหนดข้อมูลอ้างอิงให้กับกฎของโปรแกรมสนอร์ตเนื่องจากข้อมูลในไฟล์ reference.config จะประกอบไปด้วย URL ที่ใช้ในการแสดงข้อมูลอ้างอิง รูปที่ ก.36 เป็นตัวอย่างข้อมูลอ้างอิงในไฟล์ reference.config

```
Config reference: cve http://cve.mitre.org/cgi-bin/cvename.cgi?name=
```

รูปที่ ก.36 ตัวอย่างข้อมูลในไฟล์ reference.config

เมื่อผู้ใช้งานเพิ่ม CAN-2001-0876 ไปยังส่วนสุดท้ายของ URL ผู้ใช้งานจะสามารถเปิดเว็บเพจที่จัดเก็บข้อมูลที่เกี่ยวข้องกับการแจ้งเตือนได้ทันทีโดยเว็บเพจที่แสดงขึ้นมาจะมี URL ดังรูปที่ ก.37

```
http://cve.mite.org/cgi-bin/cvename.cgi?name=CAN-2001-0876.
```

รูปที่ ก.37 การกำหนดค่าให้กับ URL เมื่อผู้ใช้งานต้องการดูข้อมูลอ้างอิง CAN-2001-0876

The resp Keyword

คีย์เวิร์ด resp เป็นคีย์เวิร์ดที่มีความสำคัญอย่างยิ่งคีย์เวิร์ด resp จะใช้ในการหยุดกิจกรรมที่เกิดขึ้นจากผู้บุกรุกระบบเครือข่าย คีย์เวิร์ด resp จะส่งแพ็คเก็จตอบโต้ไปยังโฮสต์ต้นทางที่ส่งแพ็คเก็จมาตรงตามเงื่อนไขที่กฎกำหนด คีย์เวิร์ด resp จะมีความสามารถในการตอบโต้การบุกรุกที่มีความยืดหยุ่น (Flexible Response) หรือเรียกแบบสั้นๆว่า FlexResp คีย์เวิร์ด resp อาศัยปลั๊กอินของ FlexResp ในการทำงานโดยปลั๊กอิน FlexResp นั้นถูกคอมไพล์โดยโปรแกรมสนอร์ต รูปที่ ก.38 เป็นตัวอย่างการกำหนดกฎโดยใช้คีย์เวิร์ด resp ในการส่งแพ็คเก็จ TCP Reset กลับไปยังบุกรุกระบบเครือข่ายที่พยายามบุกรุกมายังเลขพอร์ต 8080 ด้วยโปรโตคอล TCP

```
alert tcp any any -> 192.168.1.0/24 8080 (resp: rst_snd;)
```

รูปที่ ก.38 การกำหนดกฎโดยใช้คีย์เวิร์ด resp

ในการใช้งานคีย์เวิร์ด resp ผู้ใช้งานสามารถส่งแพ็คเก็จตอบโต้ไปยังผู้บุกรุกระบบเครือข่ายได้พร้อมกันหลายรูปแบบโดยค่าของแต่ละอากิวเม็นท์จะถูกคั้นด้วยเครื่องหมาย “,”

ตารางที่ ก.4 อากิวเม็นท์นำมาใช้งานกับคีย์เวิร์ด resp

อากิวเม็นท์	รายละเอียดของแต่ละอากิวเม็นท์
rst_snd	ส่ง TCP Reset แพ็คเก็จไปยังผู้ส่งแพ็คเก็จ
rst_rcv	ส่ง TCP Reset แพ็คเก็จไปยังผู้รับแพ็คเก็จ
rst_all	ส่ง TCP Reset แพ็คเก็จไปยังผู้รับและผู้ส่งแพ็คเก็จ
icmp_net	ส่ง ICMP Network Unreachable แพ็คเก็จไปยังผู้ส่ง
icmp_host	ส่ง ICMP Host Unreachable แพ็คเก็จไปยังผู้ส่ง
icmp_port	ส่ง ICMP Port Unreachable แพ็คเก็จไปยังผู้ส่ง
icmp_all	ส่งแพ็คเก็จทั้งหมดที่แสดงมาไปยังผู้ส่ง

The rev Keyword

คีย์เวิร์ด rev ใช้แสดงจำนวนครั้งในการแก้ไขกฎ เมื่อผู้ใช้งานแก้ไขกฎผู้ใช้งานสามารถใช้คีย์เวิร์ด rev แสดงความแตกต่างของกฎที่ได้แก้ไข รูปที่ ก.39 แสดงการกำหนดกฎเพื่อใช้งานคีย์เวิร์ด rev

```
Alert ip any any -> any any (ipopts : lsrr; \
        Msg: “Loose source routing attempt”; rev: 2;)
```

รูปที่ ก.39 การกำหนดเพื่อใช้งานคีย์เวิร์ด rev โดยกฎดังกล่าวได้ถูกแก้ไขมาแล้วสองครั้ง

The rpc Keyword

คีย์เวิร์ด rpc ใช้ในการตรวจจับการร้องขอ RPC โดยอากิวเม็นท์ของคีย์เวิร์ด rpc จะกำหนดด้วยตัวเลข 3 จำนวนแสดงดังต่อไปนี้

- Application number
- Procedure number
- Version number

ค่าของอากิวเม็นท์จะถูกแยกด้วยเครื่องหมาย "," ผู้ใช้งานสามารถใช้เครื่องหมาย "*" แทนค่าตัวเลขในการกำหนดอากิวเม็นท์ รูปที่ ก.40 แสดงการกำหนดกฎใช้งานคีย์เวิร์ด rpc

```
alert ip any any -> 192.168.1.0/24 any (rpc: 1000,*,3; \
        Msg: "RPC request to local network";)
```

รูปที่ ก.40 กำหนดเพื่อตรวจจับการร้องขอของ RPC ที่มีโปรโตคอล TCP จำนวน 1000, ทุกโพรซีเยอร์และมีเลขเวอร์ชันเท่ากับ 3

The sameip Keyword

คีย์เวิร์ด sameip ถูกใช้ในการตรวจสอบที่อยู่ไอพีต้นทางและปลายทางโดย คีย์เวิร์ด sameip จะไม่มีการกำหนดอากิวเม็นท์ให้กับตัวมัน ประโยชน์ของคีย์เวิร์ด sameip จะใช้ในตรวจจับการปลอมแปลงที่อยู่ไอพีเพื่อเข้าไปดูข้อมูลที่เป็นความลับ หรือบุกรุกไปยังเครื่องแม่ข่าย รูปที่ ก.41 กำหนดกฎโดยใช้คีย์เวิร์ด sameip

```
Alert ip any any -> 192.168.1.0/24 any (msg: "Same IP"; \
        sameip;)
```

รูปที่ ก.41 กำหนดกฎใช้งานคีย์เวิร์ด sameip

The seq Keyword

คีย์เวิร์ด seq จะใช้ในการตรวจสอบค่า sequence number ของแพ็คเก็จโปรโตคอล TCP อากิวเม็นท์ที่ใช้ในการกำหนดคีย์เวิร์ด seq คือ "sequence number" คีย์เวิร์ด seq มีรูปแบบค่าอากิวเม็นท์ดังต่อไปนี้

```
seq: "sequence_number";
```

รูปที่ ก.42 การกำหนดค่าให้กับคีย์เวิร์ด seq

The session Keyword

session คีย์เวิร์ด จะใช้ในการคัดลอกข้อมูลทั้งหมดจากเซ็คชั่นของโปรโตคอล TCP คีย์เวิร์ด session สามารถคัดลอกข้อมูลจากทุกเซ็คชั่น และนำข้อมูลออกมาพิมพ์ได้ตัวอย่างการกำหนดกฎด้วยคีย์เวิร์ด session

```
log tcp any any -> 192.168.1.0/24 110 (session: printable;)
```

รูปที่ ก.43 กำหนดกฎเพื่อคัดลอกข้อมูลจากเซ็คชั่น POP3 ออกมาพิมพ์

กำหนดกฎค่าคีย์เวิร์ด session ให้มีค่าเป็น "all" จะสามารถคัดลอกข้อมูลทั้งหมดภายในเซ็คชั่น และหากต้องการเก็บประวัติของทราฟฟิคที่เข้ามาสามารถใช้งานรวมกับคีย์เวิร์ด logto

The sid Keyword

คีย์เวิร์ด sid จะถูกใช้ในการเพิ่ม "Snort ID" ให้กับกฎซึ่งจะเป็นประโยชน์ในส่วนของ Output modules หรือการตรวจหาประวัติยผู้เขียนได้แบ่งช่วงของ SID สำหรับการกำหนดกฎเพื่อง่ายต่อการใช้งานแสดงดังต่อไปนี้

- ในช่วง 0 – 99 ถูกสำรองไว้ใช้งานในอนาคต
- ช่วง 100 – 1,000,000 ถูกสำรองไว้สำหรับกฎของโปรแกรมสนอร์ตที่ใช้งานกันอยู่ทั่วไป
- มากกว่า 1,000,000 ใช้สำหรับการกำหนดกฎใช้ภายในระบบเครือข่ายภายใน

```
alert ip any any -> any any (ipopts: lsrr; \
        msg: "Loose source routing attempt"; sid: 1000001;)
```

รูปที่ ก.44 การกำหนดกฎให้มีค่า sid เท่ากับ 1000001

The tag Keyword

คีย์เวิร์ด tag เป็นคีย์เวิร์ดที่มีความสำคัญเป็นอย่างยิ่งเพราะคีย์เวิร์ด tag จะถูกนำไปใช้สำหรับการเก็บข้อมูลประวัติการบุกรุกระบบเครือข่าย การกำหนดค่าให้กับคีย์เวิร์ด tag มีรูปแบบดังนี้

```
tag: <type>, <count>, <metric>[,direction]
```

รูปที่ ก.45 รูปแบบการใช้งานคีย์เวิร์ด tag

อากิวเม็นท์ที่นำมาใช้งานกับคีย์เวิร์ด tag ได้อธิบายไว้ในตารางที่ ก.5

ตารางที่ ก.5 อากิวเม็นท์ที่ใช้งานกับคีย์เวิร์ด tag

อากิวเม็นท์	รายละเอียดของอากิวเม็นท์
Type	กำหนดการเก็บประวัติของเพ็คเก็จจาก เซสชัน (session) หรือโฮสต์
Count	แสดงให้เห็นถึงจำนวนแพ็คเก็จที่เก็บประวัติ หรือระยะเวลาที่ใช้ในการเก็บประวัติของแพ็คเก็จ ซึ่งความแตกต่างระหว่างการจัดเก็บทั้งสองแบบจะถูกกำหนดโดยอากิวเม็นท์ metric
Metric	รูปแบบการเก็บประวัติของแพ็คเก็จ จะเป็นแบบ “packet” หรือ “second” ซึ่งจะนำมาใช้งานร่วมกับอากิวเม็นท์ Count
Direction	อากิวเม็นท์ที่เพิ่มขึ้นมาเพื่อให้ผู้ใช้งานเลือกว่าจะเก็บประวัติของแพ็คเก็จที่เข้ามายังโฮสต์กำหนดเป็น “src” หรือเก็บประวัติของแพ็คเก็จที่โฮสต์ส่งออกไปกำหนดเป็น “dst”

```
alert tcp 192.168.2.0/24 23 -> any any \
    (content: “boota”; msg: “Detected boota”; \
    tag session, 100, packets;)
```

รูปที่ ก.46 กำหนดกฎเพื่อจัดเก็บประวัติของแพ็คเก็จจำนวน 100 แพ็คเก็จหลังจากกฎเริ่มทำงาน

The tos Keyword

คีย์เวิร์ด toe ใช้ในการตรวจสอบค่า TOS (Type of Service) ในส่วนหัวของแพ็คเก็จที่เป็นโปรโตคอล IP มีรูปแบบการกำหนดค่าดังนี้

```
tos: 1;
```

รูปที่ ก.47 กำหนดค่าคีย์เวิร์ด toe

ข้อมูลเพิ่มเติมเกี่ยวกับค่า TOS สามารถตรวจสอบได้จาก RFC791

The ttl Keyword

คีย์เวิร์ด ttl ใช้สำหรับการตรวจสอบค่า Time to Live ในส่วนหัวแพ็คเก็จของโปรโตคอล IP การกำหนดค่าให้กับคีย์เวิร์ด ttl จะต้องเป็นค่าที่แน่นอนเพื่อใช้ในการตรวจสอบค่า TTL คีย์เวิร์ด ttl สามารถนำไปใช้งานได้กับทุกโปรโตคอล คีย์เวิร์ด ttl มีรูปแบบการใช้งานแสดงรูปที่ – ก.48

```
ttl: 100;
```

รูปที่ ก.48 รูปแบบการกำหนดค่าคีย์เวิร์ด ttl

traceroute จะใช้ค่า TTL ในการค้นหาเส้นทางของฮ็อพ (hop) ถัดไปโดย traceroute จะส่งแพ็คเก็จของโปรโตคอล UDP ที่มีการเพิ่มค่าของ TTL ค่า TTL จะมีค่าลดลงทุกๆฮ็อพเมื่อค่า TTL มีค่าเป็น 0 เร้าเตอร์จะส่งแพ็คเก็จของโปรโตคอล ICMP กลับมา แพ็คเก็จของโปรโตคอล ICMP จะทำให้ทราบไอพีแอ็คเดซของเร้าเตอร์ ตัวอย่าง การค้นหาฮ็อพของเร้าเตอร์ลำดับที่ 5 traceroute จะส่งแพ็คเก็จ UDP ที่มีค่า TTL เท่ากับ 5 เมื่อแพ็คเก็จถูกส่งมาถึงฮ็อพอันดับที่ 5 ค่า TTL ก็จะมีค่าเป็น 0 แล้วแพ็คเก็จของโปรโตคอล ICMP จะถูกส่งกลับ คีย์เวิร์ด ttl จะใช้สำหรับตรวจจับผู้ที่พยายามใช้ traceroute บนระบบเครือข่าย ปัญหาที่เกิดขึ้นกับการใช้งานคีย์เวิร์ด ttl คือจะต้องกำหนดค่า TTL ที่แน่นอน

The uricontent Keyword

คีย์เวิร์ด uricontent จะทำงานคล้ายกับคีย์เวิร์ด content แต่คีย์เวิร์ด uricontent จะใช้ในการค้นหาสตริงใน URI ของแพ็คเก็จเพียงอย่างเดียว

ภาคผนวก ข.

โปรแกรมที่ใช้ในการออกแบบระบบเครือข่ายใยประสาท

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
%สร้างระบบเครือข่ายใยประสาท ที่ใช้ในการประเมินคุณการแจ้งเตือนที่เป็นการบุกรุกระบบ
เครือข่ายแบบ DoS
% Clear หน้าจอ Output
clc;
% เปิดไฟล์ข้อมูล
fid = fopen('private/crabdata.csv');
% กำหนดประเภทของข้อมูล
C =
textscan(fid,'%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f64','delimi
ter',',');
%ปิดการเชื่อมต่อ
fclose(fid);
%สร้างชุดข้อมูล Input
physchars = [C{1} C{2} C{3} C{4} C{5} C{6} C{7} C{8} C{9} C{10} C{11} C{12} C{13}
C{14} C{15} C{16} C{17} C{18} C{19} C{20} C{21} C{22} C{23} C{24}];
%สร้างชุดข้อมูล Output
alarm = [C{25}];
 %Convert Row to Colum
physchars = physchars';
alarm = alarm';
%สร้างการสุ่มข้อมูล
rand('seed', 491218382)
 %สร้าง Neural Network
s1 =20;
s2 = 20;
net = newff(physchars,alarm,[s1,s2]);
 %กำหนดประสิทธิภาพการทกงานของ Neural Network
net=init(net);
net.trainparam.epochs=2000;
net.trainparam.goal = 0;
net.trainparam.max_fail = 500;
net.trainParam.min_grad = 1e-15;
```

```
net.trainparam.mu_max = 1e+200;
net.trainparam.show=10;
net.performParam.ratio = 0.5;
[net,tr] = train(net,physchars,alarm);
%กำหนดค่าน้ำหนักและค่าเบี่ยงเบน
w1=net.IW{1,1};
b1=net.b{1};
%ทดสอบผลลัพธ์
testInputs = physchars(:,tr.testInd);
testTargets = alarm(:,tr.testInd);
out = round(sim(net,testInputs));
N = size(testInputs,2);
% แสดงจำนวนชุดทดสอบ
fprintf('Total testing samples: %d\n', N);
%จัดเก็บข้อมูลที่ได้จาก Neural Network
save NNDoS.mat net w1 b1 s1 s2
fprintf('\nFINISHED...\n');

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
%สร้างระบบเครือข่ายใยประสาท ที่ใช้ในการประเมินคุณการแจ้งเตือนที่เป็นการบุกรุเครือข่าย
แบบพยายามค้นหารหัสผ่าน
% Clear หน้าจอ Output
clc;
% เปิดไฟล์ข้อมูล
fid = fopen('private/crabdata.csv');
% กำหนดประเภทของข้อมูล
C =
textscan(fid,'%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f64','delimi
ter',',');
%ปิดการเชื่อมต่อ
fclose(fid);
%สร้างชุดข้อมูล Input
```

```
physchars = [C{1} C{2} C{3} C{4} C{5} C{6} C{7} C{8} C{9} C{10} C{11} C{12} C{13}
C{14} C{15} C{16} C{17} C{18} C{19} C{20} C{21} C{22} C{23} C{24}];
%สร้างชุดข้อมูล Output
alarm = [C{25}];
 %Convert Row to Colum
physchars = physchars';
alarm = alarm';
%สร้างการสุ่มข้อมูล
rand('seed', 491218382)
 %สร้าง Neural Network
s1 =20;
s2 = 20;
net = newff(physchars,alarm,[s1,s2]);
 %กำหนดประสิทธิภาพการทกงานของ Neural Network
net=init(net);
net.trainparam.epochs=2000;
net.trainparam.goal = 0;
net.trainparam.max_fail = 500;
net.trainParam.min_grad = 1e-15;
net.trainparam.mu_max = 1e+200;
net.trainparam.show=10;
net.performParam.ratio = 0.5;
[net,tr] = train(net,physchars,alarm);
%กำหนดค่าน้ำหนักและค่าเบี่ยงเบน
w1=net.IW{1,1};
b1=net.b{1};
%ทดสอบผลลัพธ์
testInputs = physchars(:,tr.testInd);
testTargets = alarm(:,tr.testInd);
out = round(sim(net,testInputs));
N = size(testInputs,2);
% แสดงจำนวนชุดทดสอบ
fprintf('Total testing samples: %d\n', N);
```

```
%จัดเก็บข้อมูลที่ได้จาก Neural Network
save NNPassword.mat net w1 b1 s1 s2
fprintf('\nFINISHED...\n');
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
%สร้างระบบเครือข่ายใยประสาท ที่ใช้ในการประเมินคุณการแจ้งเตือนที่เป็นการบุกรุกระบบ
เครือข่ายแบบสแกนระบบเครือข่าย
% Clear หน้าจอ Output
clc;
% เปิดไฟล์ข้อมูล
fid = fopen('private/crabdata.csv');
% กำหนดประเภทของข้อมูล
C =
textscan(fid,'%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f64','delimi
ter',',');
%ปิดการเชื่อมต่อ
fclose(fid);
%สร้างชุดข้อมูล Input
physchars = [C{1} C{2} C{3} C{4} C{5} C{6} C{7} C{8} C{9} C{10} C{11} C{12} C{13}
C{14} C{15} C{16} C{17} C{18} C{19} C{20} C{21} C{22} C{23} C{24}];
%สร้างชุดข้อมูล Output
alarm = [C{25}];
 %Convert Row to Colum
physchars = physchars';
alarm = alarm';
%สร้างการสุ่มข้อมูล
rand('seed', 491218382)
 %สร้าง Neural Network
s1 =20;
s2 = 20;
net = newff(physchars,alarm,[s1,s2]);
 %กำหนดประสิทธิภาพการทกงานของ Neural Network
net=init(net);
net.trainparam.epochs=2000;
```

```
net.trainparam.goal = 0;
net.trainparam.max_fail = 500;
net.trainParam.min_grad = 1e-15;
net.trainparam.mu_max = 1e+200;
net.trainparam.show=10;
net.performParam.ratio = 0.5;
[net,tr] = train(net,physchars,alarm);
%กำหนดค่าน้ำหนักและค่าเบี่ยงเบน
w1=net.IW{1,1};
b1=net.b{1};
%ทดสอบผลลัพธ์
testInputs = physchars(:,tr.testInd);
testTargets = alarm(:,tr.testInd);
out = round(sim(net,testInputs));
N = size(testInputs,2);
% แสดงจำนวนชุดทดสอบ
fprintf('Total testing samples: %d\n', N);
%จัดเก็บข้อมูลที่ได้จาก Neural Network
save NNScan.mat net w1 b1 s1 s2
fprintf('\nFINISHED...\n');
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
%สร้างระบบเครือข่ายใยประสาท ที่ใช้ในการประเมินคุณการแจ้งเตือนที่เป็นการบุกรุกระบบ
เครือข่ายด้วยมัลแวร์
% Clear หน้าจอ Output
clc;
% เปิดไฟล์ข้อมูล
fid = fopen('private/crabdata.csv');
% กำหนดประเภทของข้อมูล
C =
textscan(fid,'%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f64','delimi
ter',',');
%ปิดการเชื่อมต่อ
fclose(fid);
```

```
%สร้างชุดข้อมูล Input
physchars = [C{1} C{2} C{3} C{4} C{5} C{6} C{7} C{8} C{9} C{10} C{11} C{12} C{13}
C{14} C{15} C{16} C{17} C{18} C{19} C{20} C{21} C{22} C{23} C{24}];
%สร้างชุดข้อมูล Output
alarm = [C{25}];
 %Convert Row to Colum
physchars = physchars';
alarm = alarm';
%สร้างการสุ่มข้อมูล
rand('seed', 491218382)
 %สร้าง Neural Network
s1 =20;
s2 = 20;
net = newff(physchars,alarm,[s1,s2]);
 %กำหนดประสิทธิภาพการทกงานของ Neural Network
net=init(net);
net.trainparam.epochs=2000;
net.trainparam.goal = 0;
net.trainparam.max_fail = 500;
net.trainParam.min_grad = 1e-15;
net.trainparam.mu_max = 1e+200;
net.trainparam.show=10;
net.performParam.ratio = 0.5;
[net,tr] = train(net,physchars,alarm);
%กำหนดค่าน้ำหนักและค่าเบี่ยงเบน
w1=net.IW{1,1};
b1=net.b{1};
%ทดสอบผลลัพธ์
testInputs = physchars(:,tr.testInd);
testTargets = alarm(:,tr.testInd);
out = round(sim(net,testInputs));
N = size(testInputs,2);
%แสดงจำนวนชุดทดสอบ
```

```
fprintf('Total testing samples: %d\n', N);
%จัดเก็บข้อมูลที่ได้จาก Neural Network
save NNMalware.mat net w1 b1 s1 s2
fprintf('\nFINISHED...\n');
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
%การเรียกใช้งานระบบเครือข่ายใยประสาทและประเมินระดับบ่งชี้การแจ้งเตือนที่เกิดขึ้น
% Clear หน้าจอ Output
clc;
% เปิดไฟล์ข้อมูล
fid = fopen('private/crabdata.csv');
% กำหนดประเภทของข้อมูล
C =
textscan(fid,'%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f%f64','delimi
ter',',');
%ปิดการเชื่อมต่อ
fclose(fid);
%สร้างชุดข้อมูล Input
physchars = [C{1} C{2} C{3} C{4} C{5} C{6} C{7} C{8} C{9} C{10} C{11} C{12} C{13}
C{14} C{15} C{16} C{17} C{18} C{19} C{20} C{21} C{22} C{23} C{24}];
%คำนวณหาระดับบ่งชี้คุณภาพการแจ้งเตือนด้วยระบบเครือข่ายใยประสาทที่ใช้ในการบุกรุก
ระบบเครือข่ายแบบ DoS
OutputDoS = call(NNDoS.mat(Inputdata));
If 1000 < OutputDoS >= 815
Then
fprint('DoS Attacking and Quality =:%d\n',OutputDoS)
Else;
Exit sub;
%คำนวณหาระดับบ่งชี้คุณภาพการแจ้งเตือนด้วยระบบเครือข่ายใยประสาทที่ใช้ในการบุกรุก
ระบบเครือข่ายแบบพยายามค้นหารหัสผ่าน
OutputPassword = call(NNPassword.mat(Inputdata));
If 100 < OutputPassword >= 75
Then
fprint('Password Attacking and Quality =:%d\n',OutputPassword)
```

Else;

Exit sub;

%คำนวณหาระดับบ่งชี้คุณภาพการแจ้งเตือนด้วยระบบเครือข่ายใยประสาทที่ใช้ในการบุกรุกระบบเครือข่ายแบสแกนระบบเครือข่าย

OutputScan = call(NNScan.mat(Inputdata));

If 10 < OutputScan >= 8

Then

fprint('Scan Network Attacking and Quality =:%d\n', OutputScan)

Else;

Exit sub;

%คำนวณหาระดับบ่งชี้คุณภาพการแจ้งเตือนด้วยระบบเครือข่ายใยประสาทที่ใช้ในการบุกรุกระบบเครือข่ายด้วย มัลแวร์

OutputMalware = call(NNMalware.mat(Inputdata));

If 1000 < OutputMalware >= 815

Then

fprint('Malware Attacking and Quality =:%d\n', OutputMalware)

Else;

Exit sub;

++

ภาคผนวก ค.

ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่

เรื่อง การลดการแจ้งเตือนที่ผิดพลาดสำหรับการตรวจจับของโปรแกรมสนอร์ต

ตีพิมพ์ใน วิศวกรรมสารมหาวิทยาลัยขอนแก่น ปีที่ 36 ฉบับที่ 3

ประจำเดือน กรกฎาคม – กันยายน 2552

ที่ ศธ.0514.4.1.7/[illegible]

คณะวิศวกรรมศาสตร์
มหาวิทยาลัยขอนแก่น
จังหวัดขอนแก่น
40002

29 กันยายน 2552

เรื่อง แจ้งการตีพิมพ์บทความ

เรียน นายสิรานาถ เทียนงาม

ตามที่ท่านได้ส่งบทความเรื่อง **"การถดการแจ้งเตือนที่ผิดพลาดสำหรับการตรวจจับของโปรแกรมสนอร์ต"** เพื่อพิจารณาลงตีพิมพ์ในวิศวกรรมสาร มข. นั้น

บัดนี้ กองบรรณาธิการพิจารณาแล้ว เห็นสมควรตีพิมพ์บทความของท่านลงในวิศวกรรมสาร มข. ปีที่ 36 ฉบับที่ 3 ประจำเดือนกรกฎาคม – กันยายน 2552 จะนับถึงขอแจ้งให้ท่านชำระเงินเพื่อเป็นค่าตีพิมพ์บทความ จำนวน 1,000 บาท (หนึ่งพันบาทถ้วน) โดยโอนเข้าบัญชีเงินรายได้ มหาวิทยาลัยขอนแก่น กระแสรายวัน เลขที่บัญชี 551-3-00039-5 ธนาคารไทยพาณิชย์ สาขามหาวิทยาลัยขอนแก่น พร้อมทั้งส่งหลักฐานการโอนเงินมายังกองบรรณาธิการวิศวกรรมสาร มข. หมายเลขโทรสาร 043-362142 E-mail: enjournal@kku.ac.th หรือชำระเป็นเงินสดที่เจ้าหน้าที่ประจำวิศวกรรมสาร มข. ตึกเพียรวิจิตร ชั้น 7 ภายในระยะเวลา 2 สัปดาห์ หากพ้นระยะเวลาที่กำหนด จะถือว่าท่านสละสิทธิ์ในการตีพิมพ์บทความ

จึงเรียนมาเพื่อทราบและดำเนินการต่อไป

ขอแสดงความนับถือ

(ศาสตราจารย์ปริญญา จินดาประเสริฐ)
บรรณาธิการ

วิศวกรรมสาร มข.
โทร. 043-362145-6 ต่อ 708 โทรสาร 043-362142
หมายเหตุ : หากมีข้อสงสัยหรือต้องการข้อมูลเพิ่มเติมกรุณาติดต่อ คุณภูวิชญา ภูเหม็ดบุตร (เจ้าหน้าที่ประจำวิศวกรรมสาร มข.)
ที่อยู่ : กองบรรณาธิการวิศวกรรมสาร มข. ชั้น 7 คณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น จังหวัดขอนแก่น 40002
E-mail : enjournal@kku.ac.th

ประวัติผู้เขียน

นายศิวนาถ เทียงงาม เกิดเมื่อวันที่ 27 พฤศจิกายน พ.ศ.2525 ที่จังหวัดอ่างทอง สำเร็จการศึกษาปริญญาตรีวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันราชภัฏพระนครศรีอยุธยา ในปีการศึกษา 2547 และเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมสารสนเทศ ภาควิชาวิศวกรรมสารสนเทศ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2547