

สำนักหอสมุดกลาง พระจอมเกล้าลาดกระบัง

การพัฒนาระบบเพื่อตรวจจับและวิเคราะห์การสื่อสารข้อมูล
แบบเพียร์ทูเพียร์

DEVELOPMENT OF DETECTING AND ANALYZING PEER TO PEER
COMMUNICATION SYSTEM



ชเนต ศิริเวชวรารุช
นิธิ ยอดมงคล
ยศพล จิตบรรเทิงพันธ์

เลขหมู่.....
เลขทะเบียน..... 73330
วัน,เดือน,ปี 1 2 ก.ค. 2550

b. 41900313
i.

ปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรบัณฑิต
ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2549

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**DEVELOPMENT OF DETECTING AND ANALYZING PEER TO PEER
COMMUNICATION SYSTEM**



**THANET SIRIWETWARAWUT
NITI YODMONGKOL
YOSAPHOL JITBANTERNGPAN**

**A SPECIAL PROJECT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF BACHELOR OF SCIENCE
DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
FACULTY OF SCIENCE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2006**

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปัญหาพิเศษ การพัฒนาระบบเพื่อตรวจจับและวิเคราะห์การสื่อสารข้อมูลแบบเพียร์ทูเพียร์
DEVELOPMENT OF DETECTING AND ANALYZING PEER TO PEER COMMUNICATION SYSTEM

ชื่อนักศึกษา นายธนศ ศิริเวชวรารุช 46050293
นายนิธิ ยอดมงคล 46050300
นายชสพล จิตบรรเทิงพันธ์ 46050313

ปริญญา วิทยาศาสตร์บัณฑิต
ภาควิชา คณิตศาสตร์และวิทยาการคอมพิวเตอร์
สาขาวิชา วิทยาการคอมพิวเตอร์
อาจารย์ที่ปรึกษา อ.สังกรศรีณย์ ถ่องชุมผล

ภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้นำปัญหาพิเศษนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร วิทยาศาสตร์บัณฑิต สาขาวิทยาการคอมพิวเตอร์ ประจำปีการศึกษา 2549

คณะกรรมการสอบ	ลายมือชื่อ
ประธานกรรมการ รศ. ไพโรบลย์ พันธรักษ์พงษ์	
กรรมการ อ. อัครเดช อุดมชัยพร	
กรรมการและอาจารย์ที่ปรึกษา อ. สังกรศรีณย์ ถ่องชุมผล	

(รองศาสตราจารย์ ดร. วีระ บุญจริง)

หัวหน้าภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์

ลิขสิทธิ์ของภาควิชาคณิตศาสตร์และวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อปัญหาพิเศษ	การพัฒนาระบบเพื่อตรวจจับและวิเคราะห์การสื่อสารข้อมูลแบบเพียร์ทูเพียร์ DEVELOPMENT OF DETECTING AND ANALYZING PEER TO PEER COMMUNICATION SYSTEM	
ชื่อนักศึกษา	นายชเนศ ศิริเวชวารวุธ	46050293
	นายนิธิ ยอดมงคล	46050300
	นายยศพล จิตบรรเทิงพันธ์	46050313
ปริญญา	วิทยาศาสตรบัณฑิต	
ภาควิชา	คณิตศาสตร์และวิทยาการคอมพิวเตอร์	
สาขาวิชา	วิทยาการคอมพิวเตอร์	
ปีการศึกษา	2549	
อาจารย์ที่ปรึกษา	อ.ศังกรศรีณีย์ ล่องชูผล	

บทคัดย่อ

ในปัจจุบันระบบอินเทอร์เน็ตมีบทบาทเป็นอย่างมากในด้านต่างๆไม่ว่าจะเป็นด้านธุรกิจ ด้านการศึกษา ด้านมัลติมีเดียและในอีกหลายๆด้าน ซึ่งในแต่ละวันจะมีผู้ใช้ระบบเครือข่ายมากมาย เพื่อติดต่อธุรกิจและค้นหาข้อมูลต่างๆ ซึ่งผลที่ตามมาก็คือ การขยายตัวและพัฒนาการของระบบเครือข่าย ซึ่งในปัจจุบันมีการสื่อสารแบบใหม่ที่เรียกว่า การสื่อสารแบบเพียร์ทูเพียร์ ซึ่งการสื่อสารรูปแบบนี้นั้นทำให้เกิดปริมาณการรับส่งข้อมูลจำนวนมาก ทำให้รบกวนปริมาณการรับส่งข้อมูลรวมทั้งหมดของการใช้งานเครือข่ายภายในองค์กร

ในการศึกษานี้เราจึงได้พยายามที่จะพัฒนาระบบที่สามารถตรวจสอบและแจ้งเตือนและทำการเก็บข้อมูลเหล่านั้น เพื่อนำไปใช้ในการพิจารณาและทำการกำจัดการสื่อสารแบบเพียร์ทูเพียร์ ซึ่งเป็นการอำนวยความสะดวกต่อผู้ดูแลระบบในการตรวจสอบการใช้งานแบบเพียร์ทูเพียร์ ซึ่งระบบนี้ได้นำเอาคุณสมบัติของระบบตรวจจับผู้บุกรุกมาใช้ในการพัฒนา

Special Topic	DETECTING AND ANALYZING PEER TO PEER COMMUNICATION SYSTEM DEVELOPMENT	
Students	Mr.Thanet Sriwetwarawut	46050293
	Mr.Niti Yodmongkol	46050300
	Mr.Yosaphol Jitbanterngphan	46050313
Degree	Bachelor of Science	
Department	Mathematics and Computer Science	
Programme	Computer Science	
Academic Year	2006	
Special Project Advisor	Sungkornsarun Longchupol	

ABSTRACT

Nowadays, the Internet has an importance in business, education, multimedia and others. Many people surf the Internet for many reasons, such as searching information, or business contact. The expansion of the internet causes a new kind of communication called P2P communication which it consumes a lot of bandwidth making traffic problems on the network.

The special problem "Detecting and Analyzing Peer to Peer communication system development" is developed to detect some protocols of P2P communication, then alert and store detected information into a database. Therefore, the system can help an administrator detects and tracks a source of the detected P2P communication later.

กิตติกรรมประกาศ

โครงการปัญหาพิเศษเรื่อง การพัฒนาระบบเพื่อจำกัดการสื่อสารข้อมูลแบบเพียร์ทูเพียร์ สามารถสำเร็จลุล่วงไปได้ด้วยดี ด้วยความช่วยเหลือและความร่วมมือจากหลายๆ ท่าน คณะผู้จัดทำ ต้องขอขอบพระคุณ อ.สังกรศรีณย์ ล่องพูล ซึ่งเป็นอาจารย์ที่ปรึกษาโครงการปัญหาพิเศษนี้ที่กรุณาให้คำแนะนำในการแก้ปัญหาค้างๆ คอยดูแลเอาใจใส่ และให้การสนับสนุนทางด้านทางด้าน ซอฟต์แวร์และฮาร์ดแวร์ รวมทั้งเป็นผู้ตรวจสอบความถูกต้องของโครงการพิเศษฉบับนี้ นอกจากนี้ ต้องขอขอบพระคุณศูนย์พัฒนาและวิจัยคอมพิวเตอร์ที่ให้ความช่วยเหลือทางด้านเครื่องมือและอุปกรณ์ที่ใช้สำหรับโครงการนี้ และต้องขอขอบพระคุณนายพงศกร ปิยะตระกูล (พีโก้ฟ) ที่ให้คำแนะนำและช่วยแก้ปัญหาค้างๆ ตลอดทั้งโครงการนี้

นอกจากนี้คณะผู้จัดทำต้องขอขอบพระคุณ บิดา มารดา ที่ได้ให้ความสนับสนุนทางด้าน กำลังใจและทุนทรัพย์ จนการทำปัญหาพิเศษนี้สำเร็จลุล่วงไปได้ด้วยดี รวมทั้งเพื่อนๆ พี่ๆ ทุกคนที่ให้ความช่วยเหลือในด้านต่างๆ เกี่ยวกับปัญหาพิเศษไว้ ณ ที่นี้

คณะผู้จัดทำ

มีนาคม 2550

สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	I
บทคัดย่อภาษาอังกฤษ	II
กิตติกรรมประกาศ	III
สารบัญ.....	IV
สารบัญตาราง	VII
สารบัญรูป	VIII
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของปัญหา.....	1
1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา.....	1
1.3 ขอบเขตของปัญหา.....	1
1.4 ประโยชน์ที่คาดว่าจะได้รับ	2
1.5 ขั้นตอนในการดำเนินงาน	2
1.6 อุปกรณ์ที่ใช้ในการทำปัญหาพิเศษ.....	2
1.6.1 รายละเอียดทางด้านอุปกรณ์.....	2
1.6.2 รายละเอียดทางด้านซอฟต์แวร์.....	3
บทที่ 2 ความรู้เบื้องต้น	4
2.1 การสื่อสารแบบเพียร์ทูเพียร์	4
2.2 ความรู้เบื้องต้นเกี่ยวกับระบบตรวจจับผู้บุกรุก	7
2.2.1 ส่วนประกอบของระบบตรวจจับผู้บุกรุก	7
2.2.2 ประเภทของระบบตรวจจับผู้บุกรุก	9
2.2.2.1 ระบบตรวจจับผู้บุกรุกบนพื้นฐานโฮสต์	9
2.2.2.2 ระบบตรวจจับผู้บุกรุกบนพื้นฐานเน็ตเวิร์ก	9
2.2.3 ข้อดีของการใช้ระบบตรวจจับผู้บุกรุก.....	10
2.2.3.1 การตอบสนองทันทีทันใด.....	10
2.2.3.2 การมีฐานความรู้ของการวิเคราะห์.....	10
2.2.3.3 การช่วยตรวจสอบข้อบกพร่องของระบบป้องกันอื่นๆ	11
2.2.4 ข้อเสียของการใช้ระบบตรวจจับผู้บุกรุก	11
2.2.4.1 การละเมิดความเป็นส่วนตัว.....	11
2.2.4.2 การตอบโต้อัตโนมัติ	12

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.2.4.3 การเตือนภัยผิดพลาด.....	13
2.2.5 สรุปความสามารถของระบบตรวจจับผู้บุกรุก.....	14
2.3 เทคนิคทางด้านเครือข่ายและ โพรโตคอล.....	14
2.3.1 ความหมายเบื้องต้นของโปรโตคอล.....	14
2.3.2 ความรู้เกี่ยวกับ โมเดลเครือข่ายแบบ โพรโตคอลที่ซีพี/ไอพี(TCP/IP)	14
2.3.2.1 ลำดับชั้นของโมเดลเครือข่ายแบบโปรโตคอลที่ซีพี/ไอพี	15
2.3.2.2 หลักการทำงานของโมเดลเครือข่ายแบบโปรโตคอลที่ซีพี/ไอพี	16
2.4 ลักษณะของโปรโตคอลที่ใช้ใน โปรแกรมประยุกต์เพียร์ทูเพียร์.....	17
บทที่ 3 วิธีดำเนินการวิจัย	21
3.1 รูปแบบโครงสร้างของระบบตรวจจับผู้บุกรุกที่ใช้ในการดำเนินการวิจัย	21
3.2 ลักษณะของโปรแกรมที่ทำการทดลอง	22
3.2.1 โปรแกรมที่ใช้ในการตรวจจับการบุกรุก.....	22
3.2.1.1 ส่วนประกอบของโปรแกรมสนอร์ต.....	23
3.2.1.2 สิ่งที่เป็นในการติดตั้งโปรแกรมสนอร์ต.....	25
3.2.1.3 การติดตั้งโปรแกรม.....	25
3.2.2 โปรแกรมเพียร์ทูเพียร์ประยุกต์(Peer-to-Peer Application).....	27
3.2.3 โปรแกรมที่ใช้ตรวจสอบรายละเอียดของแพ็กเก็ต.....	27
3.3 การทำงานของโปรแกรมสนอร์ต.....	27
3.3.1 กฎ (rules).....	27
3.3.2 โครงสร้างของกฎ.....	28
3.3.3 วิธีปรับแต่งโปรแกรมสนอร์ต.....	35
3.4 การทำงานและพฤติกรรมของการสื่อสารแบบเพียร์ทูเพียร์.....	36
3.4.1 องค์ประกอบของเพียร์ทูเพียร์.....	36
3.4.2 การทำงานของเพียร์ทูเพียร์.....	36
3.5 การทำงานของโปรแกรมอีเทอร์เรียล	37
3.6 การทำงานของระบบ.....	40
บทที่ 4 ผลการดำเนินงานวิจัย	42
4.1 เครื่องมือที่ใช้ในการทดสอบโปรแกรม	42
4.1.1 ความต้องการทางด้านฮาร์ดแวร์	42
4.1.2 ความต้องการทางด้านซอฟต์แวร์	42
4.2 ขั้นตอนการติดตั้งโปรแกรม.....	42

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3	การทำงานของโปรแกรม	42
4.3.1	เพย์โหลด ดีเทล(payload detail)	44
4.3.2	รายงานแสดงผลด้วยกราฟในเวลา 24 ชั่วโมงล่าสุด.....	45
4.3.3	การแสดงผลรายงานต่างๆ.....	48
4.4	การทดสอบระบบ	66
4.4.1	การทดสอบกับโปรโตคอลบิตทอร์เรนต์โดยใช้โปรแกรมบิทโคเม็ท.....	66
4.4.2	การทดสอบกับโปรโตคอลจิงูเทลล่าโดยใช้โปรแกรมเซคพีทูพี	68
4.4.3	การทดสอบกับโปรโตคอลอีคอนกี้โดยใช้โปรแกรมอีมูลล์	70
4.5	สรุปผลการทำงาน.....	72
บทที่ 5	สรุปผลและข้อเสนอแนะ	72
5.1	สรุปผลปัญหาพิเศษ	72
5.2	ข้อจำกัดปัญหาพิเศษ	72
5.3	ข้อเสนอแนะและแนวทางการศึกษาต่อ.....	73



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

ตารางที่

หน้า

3.1 ส่วนประกอบของสนอรัต..... 25



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป

รูปที่	หน้า
2.1 แบบจำลองเพียร์เพียร์ทูเพียร์.....	5
2.2 แบบจำลองไฮบริดเพียร์ทูเพียร์.....	6
2.3 แบบจำลองซูเปอร์เพียร์ทูเพียร์.....	7
2.4 ส่วนประกอบของไอดีเอส	8
2.5 โมเดลเครือข่ายแบบโปรโตคอลทีซีพี/ไอพี.....	15
2.6 Header ในแต่ละลำดับชั้นของ TCP/IP	17
2.7 ลักษณะเซคเตอร์ของ eDonkey Protocol.....	18
3.1 One-Arm Architecture.....	21
3.2 In-Line Architecture	22
3.3 ส่วนประกอบของสวิตช์.....	23
3.4 โครงสร้างพื้นฐานของกฏสวิตช์.....	28
3.5 โครงสร้างของเซคเตอร์ของกฏสวิตช์.....	28
3.6 ภาพแสดงองค์ประกอบของเพียร์ทูเพียร์.....	36
3.7 แสดงหน้าจอหลักของโปรแกรมอีเทอร์เรียล.....	37
3.8 แสดงหน้าจอตอนเลือก Network Card ที่จะจับแพ็กเก็ตที่ Network Card ไค.....	38
3.9 หน้าจอแสดงผลการเปรียบเทียบจำนวนแพ็กเก็ตที่จับได้ในแต่ละโปรโตคอล.....	38
3.10 หน้าจอแสดงรายละเอียดของแพ็กเก็ตต่างๆที่จับได้.....	39
3.11 แสดงรายละเอียดของแพ็กเก็ต.....	39
3.12 Flow chart การทำงานของระบบ.....	40
4.1 หน้าจอหลักของระบบ.....	43
4.2 หน้าจอแสดงกราฟแท่งแสดงความสัมพันธ์ระหว่างไอพีแอดเดรสต้นทางกับเพย์โหลดที่ใช้.....	44
4.3 หน้าจอแสดงกราฟแท่งแสดงความสัมพันธ์ระหว่างไอพีแอดเดรสปลายทางกับเพย์โหลดที่ใช้.....	44
4.4 หน้าจอแสดงกราฟเส้นแสดงความสัมพันธ์ระหว่างเพย์โหลดของโปรโตคอลเพียร์ทูเพียร์ทั้งหมดรวมกันกับเวลา 24 ชั่วโมงล่าสุด.....	45
4.5 หน้าจอแสดงการเลือกที่จะแสดงรายงานด้วยกราฟของโปรโตคอลตัวใด.....	46
4.6 หน้าจอแสดงกราฟเส้นแสดงความสัมพันธ์ระหว่างเพย์โหลดของแต่ละโปรโตคอลใน 24 ชั่วโมงล่าสุด.....	46
4.7 หน้าจอแสดงผลตามไอพีแอดเดรสต้นทาง.....	47

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.8	หน้าจอแสดงผลตามไอพีแอดเดรสปลายทาง.....	48
4.9	หน้าจอแสดงผลโดยเรียงแพ็กเก็ต 15 แพ็กเก็ตล่าสุด.....	49
4.10	หน้าจอแสดงผลของการตรวจจับ โดยแสดงซิกเนเจอร์ที่ไม่ซ้ำกันในวันนี้.....	50
4.11	หน้าจอแสดงผลของการตรวจจับทั้งหมดที่ตรวจจับได้ในวันนี้.....	51
4.12	หน้าจอแสดงผลของการตรวจจับวันนี้โดยพิจารณาจากไอพีแอดเดรสต้นทาง.....	52
4.13	หน้าจอแสดงผลของการตรวจจับในวันนี้โดยพิจารณาจากไอพีแอดเดรสปลายทาง.....	53
4.14	หน้าจอแสดงผลของการตรวจจับ โดยแสดงซิกเนเจอร์ที่ไม่ซ้ำกันและเป็นรายการที่เกิดขึ้นใน 24 ชั่วโมงล่าสุด.....	54
4.15	หน้าจอแสดงผลของการตรวจจับทั้งหมดที่ตรวจจับได้ใน 24 ชั่วโมงล่าสุด.....	55
4.16	หน้าจอแสดงผลของการตรวจจับ 24 ชั่วโมงล่าสุดโดยพิจารณาจากไอพีแอดเดรสต้นทาง.....	56
4.17	หน้าจอแสดงผลของการตรวจจับ 24 ชั่วโมงล่าสุดโดยพิจารณาจากไอพีแอดเดรสปลายทาง....	57
4.18	หน้าจอแสดงผลของการตรวจจับ โดยแสดงถึง 15 รายการล่าสุดที่พอร์ตต้นทางถูกแจ้งเตือน ...	58
4.19	หน้าจอแสดงผลของการตรวจจับ โดยแสดงถึง 15 รายการล่าสุดที่พอร์ตปลายทางถูกแจ้งเตือน.	59
4.20	หน้าจอแสดงผลของการตรวจจับ โดยแสดงประเภทของการแจ้งเตือนที่พบบ่อยที่สุด.....	60
4.21	หน้าจอแสดงผลของการตรวจจับ โดยแสดงหมายเลขพอร์ตของต้นทางที่ถูกแจ้งเตือนบ่อย ที่สุด 15 อันดับ.....	61
4.22	หน้าจอแสดงผลของการตรวจจับ โดยแสดงหมายเลขพอร์ตของปลายทางที่ถูกแจ้งเตือนบ่อย ที่สุด 15 อันดับ.....	62
4.23	หน้าจอแสดงผลการลบบันทึกการของแพ็กเก็ต.....	63
4.24	หน้าจอแสดงรูปแบบของแพ็กเก็ต และรายละเอียดที่มากับแพ็กเก็ต.....	64
4.25	หน้าจอแสดงผลการโหลดไฟล์ผ่านโปรแกรมบีทโคเมท.....	65
4.26	หน้าจอแสดงผลของโปรแกรมที่ได้หลังจากการโหลดไฟล์ผ่านโปรแกรมบีทโคเมท.....	66
4.27	หน้าจอแสดงผลการโหลดไฟล์ผ่านโปรแกรมแซดพีทูพี.....	67
4.28	หน้าจอแสดงผลของโปรแกรมที่ได้หลังจากการโหลดไฟล์ผ่านโปรแกรมแซดพีทูพี.....	68
4.29	หน้าจอแสดงผลการโหลดไฟล์ผ่านโปรแกรมอีมูลล์.....	69
4.30	หน้าจอแสดงผลของโปรแกรมที่ได้หลังจากการโหลดไฟล์ผ่านโปรแกรมอีมูลล์.....	70
ก 1	หน้าจอแสดงผลผลลัพธ์ที่ได้หลังจากเรียกโปรแกรมได้สำเร็จ.....	77

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการสื่อสารข้อมูลในลักษณะเพียร์ทูเพียร์ (P2P หรือ Peer to Peer) ได้รับความนิยมอย่างแพร่หลายเนื่องจากความนิยมในการกระจายซอฟต์แวร์และเนื้อหาของข้อมูลบันเทิงต่างๆ เช่น เพลงหรือภาพยนตร์ แต่โปรแกรมเพียร์ทูเพียร์กลายเป็นช่องทางของการแพร่กระจายของไวรัส (Virus) และเวิร์ม (Worm) ต่าง ๆ ตลอดจน โปรแกรมเพียร์ทูเพียร์มักจะมาพร้อมกับโปรแกรมแอดแวร์ (Adware) และโปรแกรมสปายแวร์ (Spyware) เพราะโปรแกรมเหล่านี้มีผลประโยชน์ทางธุรกิจร่วมกันอยู่ นอกจากนี้โปรแกรมเพียร์ทูเพียร์จะมีช่องโหว่ดังกล่าวแล้ว โปรแกรมเหล่านี้ยังใช้แบนด์วิธ (Bandwidth) ของระบบเครือข่ายอย่างมหาศาล ทำให้รบกวนการส่งข้อมูล (Traffic) ของการใช้งานเครือข่ายในองค์กรอย่างหลีกเลี่ยงไม่ได้

องค์กรควรกำหนด "นโยบายในการใช้งานระบบคอมพิวเตอร์ให้ปลอดภัย" ("Security Policy") ซึ่งคือการจัดสรรและการทำงานของเครือข่ายอย่างมีประสิทธิภาพเพื่อให้ผู้ใช้งานในรูปแบบอื่นอย่างข้อมูลสารสนเทศต่างๆ ที่ร่วมใช้เครือข่ายอินเทอร์เน็ตไม่ถูกแย่งชิงการใช้งานจากปริมาณข้อมูลของการสื่อสารแบบเพียร์ทูเพียร์ จัดการกับโปรแกรมเพียร์ทูเพียร์เหล่านี้ โดยการบล็อกช่องทางหรือพอร์ต (Port) ที่ใช้ในการสื่อสารแบบเพียร์ทูเพียร์เพื่อป้องกัน โปรแกรมแอดแวร์และ โปรแกรมสปายแวร์ และลดปัญหาการส่งข้อมูลภายในองค์กร

เนื่องจากในขณะนี้องค์กรต่างๆ ยังไม่มีระบบป้องกันการสื่อสารแบบเพียร์ทูเพียร์ คณะผู้จัดทำจึงคิดค้นระบบที่ใช้ตรวจจับและจำกัดการสื่อสารแบบเพียร์ทูเพียร์เพื่อเพิ่มความปลอดภัยภายในองค์กร โดยการพัฒนาระบบจากโปรแกรมโอเพน ซอร์ซ (Open Source)

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

- 1) เพื่อศึกษารูปแบบการสื่อสารแบบเพียร์ทูเพียร์
- 2) เพื่อสร้างระบบช่วยในการพิจารณาการจำกัดการใช้งานให้แก่ผู้ดูแลระบบเครือข่าย
- 3) เพื่อนำตัวจำกัดการสื่อสารแบบเพียร์ทูเพียร์ที่สร้างขึ้น ไปประยุกต์ใช้ในระบบงานจริง

1.3 ขอบเขตของปัญหา

- 1) การสร้างระบบตรวจจับการสื่อสารแบบเพียร์ทูเพียร์นั้นจะพัฒนาบนเครื่องคอมพิวเตอร์ส่วนบุคคลทั่วไป (PC-Based) ที่มีระบบปฏิบัติการลินุกซ์ (Linux)
- 2) ใช้โปรแกรมโอเพน ซอร์ซ ในการพัฒนาระบบจำกัดการสื่อสารแบบเพียร์ทูเพียร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- 3) เก็บข้อมูลการใช้งานโปรโตคอล(Protocol)เพียร์ทูเพียร์ของผู้ใช้งานในเครือข่าย
- 4) สามารถทำให้ระบบแจ้งเตือนการสื่อสารบนเพียร์ทูเพียร์ที่นิยม 3 ตัว คือ บิททอเรนต (BitTorrent) จีนูเทลต้า (Gnutella) และอีดอนกี้ (eDonkey) ที่เลือกโปรโตคอล 3 ตัวนี้เพราะมีแอปพลิเคชันที่สนับสนุนการทำงานของโปรโตคอลนี้อยู่เป็นจำนวนมาก
- 5) นำล็อกไฟล์ (log file) มาเขียนเป็นรายงานให้ผู้ดูแลระบบนำไปใช้ต่อไป

1.4 ประโยชน์ที่คาดว่าจะได้รับ

- 1) ลดต้นทุนในการซื้อฮาร์ดแวร์ราคาแพง
- 2) สามารถนำระบบนี้ไปพัฒนาต่อเพื่อเป็นระบบที่สมบูรณ์ยิ่งขึ้นได้
- 3) สามารถนำระบบนี้มาใช้ในระบบงานจริงได้เพื่อจำกัดการสื่อสารแบบเพียร์ทูเพียร์ที่มีอยู่ในเครือข่ายออกไป
- 4) สามารถนำข้อมูลการใช้งานของผู้ใช้งานในเครือข่ายไปวิเคราะห์ และนำไปแก้ปัญหาการใช้งานเครือข่าย

1.5 ขั้นตอนในการดำเนินการ

- 1) ศึกษาการทำงานและพฤติกรรมของเพียร์ทูเพียร์
- 2) ค้นคว้าหาโปรแกรมโอเพน ซอร์ซ หลายๆตัว แล้วเลือกตัวใดตัวหนึ่งมาพัฒนา
- 3) ศึกษาโปรแกรมโอเพน ซอร์ซ ที่ต้องการนำมาใช้ คือ โปรแกรมสนอร์ท อีเทอร์เรียด และเพียร์ทูเพียร์แอปพลิเคชันเช่น อีมูล์(Emule) , แซคพีทูพี(ZP2P)และบิต โทเรนต์(Bit Torrent)
- 4) สร้างระบบที่ต้องการขึ้น คือระบบตรวจจับและวิเคราะห์การสื่อสารแบบเพียร์ทูเพียร์
- 5) ทดสอบระบบที่สร้างขึ้น โดยทำการสร้างกฎของสนอร์ทและทดลองตรวจจับ
- 6) ปรับปรุงและแก้ไขข้อผิดพลาด

1.6 อุปกรณ์ที่ใช้ในการทำปัญหาพิเศษ

1.6.1 รายละเอียดด้านอุปกรณ์

- 1) คอมพิวเตอร์ 3 เครื่อง
- 2) เครื่องพิมพ์ 1 เครื่อง
- 3) กระดาษ 80 แกรม ขนาด A4
- 4) ซีดี-อาร์ (CD-R) 700 เมกะไบต์ (Megabytes)
- 5) ฮับ (Hub)
- 6) สายยูทีพี (UTP) 10/100 พร้อมหัวอาร์เจ-45 (RJ)-45

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

1.6.2 รายละเอียดทางด้านซอฟต์แวร์

1) โปรแกรมโอเพน ซอร์ซ ได้แก่ โปรแกรมสโนอร์ทเวอร์ชัน 2.6.0.2 , อาปาเช่ (Apache)เวอร์ชัน 2.2.4 , พีเอชพี(PHP)เวอร์ชัน 5.2.0 , อีเทอร์เรียล(Ethereal)เวอร์ชัน 0.99 และ มายเอสคิวแอล(mysql) เวอร์ชัน 5.0

2) ระบบปฏิบัติการลินุกซ์ฟีโดร่าคอร์4



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2

ความรู้เบื้องต้น

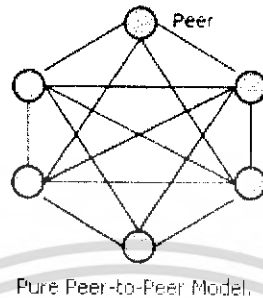
ก่อนที่จะเราเริ่มต้นการพัฒนาระบบเพื่อจัดการสื่อสารแบบเพียร์ทูเพียร์เราต้องมีความรู้พื้นฐานในเรื่องต่างๆที่เกี่ยวกับระบบก่อน

2.1 การสื่อสารแบบเพียร์ทูเพียร์

ในปัจจุบันเทคโนโลยีระบบเครือข่ายแบบเพียร์ทูเพียร์ได้รับความนิยม และเข้ามามีบทบาทในการใช้อินเทอร์เน็ตมากขึ้น เทคโนโลยีนี้ช่วยให้ผู้ใช้สามารถแลกเปลี่ยนข้อมูลบริการและทรัพยากรอื่นๆในเครื่องคอมพิวเตอร์ ที่อยู่บนเครือข่ายได้สะดวกมากยิ่งขึ้น ดังเช่น แนพสเตอร์(Napster), จินูเทลล่า(Gnutella) และ ฟรีเน็ต(Freenet) ซึ่งเป็นโปรแกรมประยุกต์ที่ยอมให้ใช้อินเทอร์เน็ตค้นหา และแลกเปลี่ยนไฟล์ข้อมูลต่างๆระหว่างคอมพิวเตอร์ซึ่งกันและกันได้ โดยไม่จำเป็นต้องมีคอมพิวเตอร์แม่ข่าย (Central Server) ซึ่งต่างจากระบบไคลเอนต์-เซิร์ฟเวอร์(Client-Server) ซึ่งต้องมีคอมพิวเตอร์แม่ข่าย (Server) คอยให้บริการตามคำขอของเครื่องลูกข่าย (Client) ในการขอข้อมูล บริการ และไฟล์ข้อมูล ดังตัวอย่างที่พบเห็นโดยทั่วไปคือ เวิลด์ ไรด์ เว็บ (www) ทั่วไปที่มีอยู่โดยใช้อินเทอร์เน็ตซึ่งเปรียบได้เสมือนเครื่องลูกข่ายจะใช้เว็บเบราว์เซอร์(Web Browser)ในการแสดงผลข้อมูลที่มาจากเครื่องแม่ข่าย (Web Server) โดยใช้ โพรโทคอล เซชทีทีพี(HTTP) เป็นมาตรฐานในการสื่อสารและมีรูปแบบการแสดงผลเป็นแบบ เซชทีเอ็มแอล(HTML) ซึ่งหากจะเปรียบไปแล้วเทคโนโลยีระบบเครือข่ายแบบเพียร์ทูเพียร์จะการทำงานในลักษณะที่เป็นดีเซ็นทรไลเซชัน(Decentralization) ส่วนระบบไคลเอนต์-เซิร์ฟเวอร์มีการทำงานเป็นแบบเซ็นทรไลเซชัน(Centralization) นั่นเอง เพียร์ทูเพียร์สามารถแบ่งออกได้เป็น 3 แบบ คือ เพียร์ทูเพียร์(Pure P2P), ไฮบริดเพียร์ทูเพียร์(Hybrid P2P), และซูเปอร์เพียร์ทูเพียร์(Super Peer)

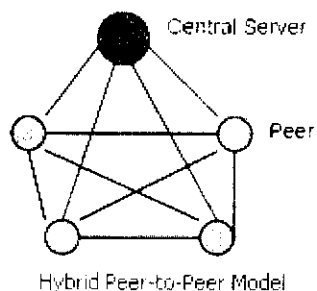
เพียร์ทูเพียร์ จะมีลักษณะที่ตรงข้ามกับ โมเดลแบบศูนย์กลางตรงที่ทุกๆเพียร์สามารถติดต่อและแลกเปลี่ยนข้อมูลกันได้โดยตรงโดยไม่ต้องผ่านเครื่องเซิร์ฟเวอร์กลาง จุดเด่นของโมเดลแบบนี้คือความสามารถในการขยายขนาดเครือข่าย, ความคงทน(Fault Tolerant) โดยถ้ามีเพียร์เสียหรือออกไปจากระบบก็จะไม่ส่งผลกระทบต่อระบบโดยรวม แต่โมเดลแบบนี้ก็มีข้อจำกัดตรงที่ควบคุมการไหลของข้อมูลได้ยากทำให้มีปัญหาเรื่องการใช้แบนด์วิธสิ้นเปลือง และโมเดลแบบนี้จะมีความปลอดภัยที่ต่ำเนื่องจากแต่ละเพียร์สามารถเข้าสู่เครือข่ายได้โดยไม่ต้องมีการยืนยันผู้ใช้งาน(Authentication) (โมเดล

แบบนี้ทำการยืนยันผู้ใช้งานได้ยาก) และสามารถที่จะส่งข้อมูลที่อันตรายเข้าสู่เครือข่ายได้โดยง่าย เนื่องจากข้อเสียที่มากของโมเดลแบบนี้ทำให้โมเดลนี้ไม่เป็นที่นิยมเท่าที่ควร



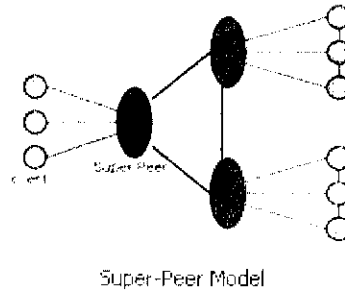
รูปที่ 2.1 แบบจำลองเพียร์เพียร์ทูเพียร์

ไฮบริดเพียร์ทูเพียร์ จะมีเครื่องเซิร์ฟเวอร์ ที่ทำหน้าที่ควบคุมรายละเอียดของข้อมูลที่อยู่ภายในเครือข่ายแต่การส่งข้อมูลจะเป็นแบบเดียวกับโมเดลเพียร์เพียร์ทูเพียร์ (ส่งถึงกันโดยตรง) โมเดลแบบนี้จะช่วยลดปัญหาเรื่องการจัดการข้อมูลที่ได้ยากในโมเดลแบบเพียร์เพียร์ทูเพียร์ โดยเครื่องเซิร์ฟเวอร์จะทำหน้าที่คอยตรวจสอบสถานะของทุกๆเพียร์ และควบคุมการไหลของข้อมูลในเครือข่ายแต่เพราะยังต้องใช้เครื่องเซิร์ฟเวอร์กลางอยู่ ดังนั้นถ้าเครื่องเซิร์ฟเวอร์กลางเสียไปก็จะเสียการควบคุมข้อมูลไปแต่ละเพียร์ แต่ยังคงสามารถแลกเปลี่ยนข้อมูลกันได้อยู่ เนื่องจากการควบคุมข้อมูลที่ติดตั้งโมเดลนี้จึงมีความสามารถในการขยายขนาดเครือข่ายได้ดีกว่าโมเดลเพียร์เพียร์ทูเพียร์ แต่ก็ยังมีขีดจำกัดของการขยายอยู่ที่จำนวนเครื่องลูกของเครื่องเซิร์ฟเวอร์ที่จะรับได้ โมเดลแบบนี้มีประสิทธิภาพที่จะนำไปใช้กับแอปพลิเคชันต่างๆ แต่ไม่สามารถนำไปใช้กับแอปพลิเคชันที่มีขนาดของปัญหาใหญ่ๆได้



รูปที่ 2.2 แบบจำลองไฮบริดเพียร์ทูเพียร์

ซูเปอร์เพียร์ทูเพียร์ เป็น โมเดลใหม่ที่จะเกิดขึ้นไม่นานมานี้ โดยเป็นการเอาระบบแบบ ศูนย์กลางไปรวมอยู่ในระบบแบบกระจาย โมเดลแบบซูเปอร์เพียร์ทูเพียร์จะช่วยลดปริมาณในการ จัดการของเซิร์ฟเวอร์ อีกทั้งช่วยเพิ่มความสามารถในเรื่องของการขยายขนาดและความคงทนของ เครื่องมือ และลดปัญหาอื่น ๆ ที่เกิดขึ้นในโมเดลแบบเพียร์ทูเพียร์และไฮบริดเพียร์ทูเพียร์ คือเพียร์ ที่ทำหน้าที่เหมือนเป็นเซิร์ฟเวอร์กลางให้กับกลุ่มของไคลเอนต์ แต่ละกลุ่มไคลเอนต์จะส่งคำร้องขอและ รับผลลัพธ์ของคำร้องขอนั้นจากซูเปอร์เพียร์ทูเพียร์ ในขณะที่ซูเปอร์เพียร์ทูเพียร์แต่ละเพียร์ก็จะ เชื่อมต่อกันด้วยเครือข่ายแบบเพียร์ทูเพียร์ โดยซูเปอร์เพียร์จะทำหน้าที่เป็นตัวควบคุม (Controller), ปรับแต่ง (Configuration), ดูแล (Administration) และรักษาความปลอดภัย (Security) ให้กับไคลเอนต์ ที่อยู่ในกลุ่มดังนั้นในแต่ละซูเปอร์เพียร์จะต้องมีโปรโตคอลในการติดต่อสื่อสารอยู่ 2 โปรโตคอล คือโปรโตคอลในการติดต่อสื่อสารระหว่างซูเปอร์เพียร์กับไคลเอนต์ และโปรโตคอลใน การติดต่อสื่อสารระหว่างซูเปอร์เพียร์กับซูเปอร์เพียร์อื่น โมเดลแบบซูเปอร์เพียร์มีจุดเด่นคือช่วย ลดเวลาและแบนด์วิธที่ใช้ในการค้นหา, แต่ละหน่วยจะมีความเป็นอิสระสูง, สามารถควบคุมและจัดการ ได้ง่าย, สามารถทำ Load Balancing ได้เป็นต้น แต่โมเดลซูเปอร์เพียร์นี้ถ้าซูเปอร์เพียร์เสียก็จะทำให้ ไคลเอนต์ที่อยู่ในกลุ่มนั้นไม่สามารถทำงานได้ แต่ปัญหานี้สามารถลดได้โดยการที่ให้มีซูเปอร์เพียร์ มากกว่าหนึ่งเพียร์ ในแต่ละกลุ่ม



รูปที่ 2.3 แบบจำลองซูเปอร์เพียร์เพียร์

2.2 ความรู้เบื้องต้นเกี่ยวกับระบบตรวจจับผู้บุกรุก (IDS: Intrusion Detection System)

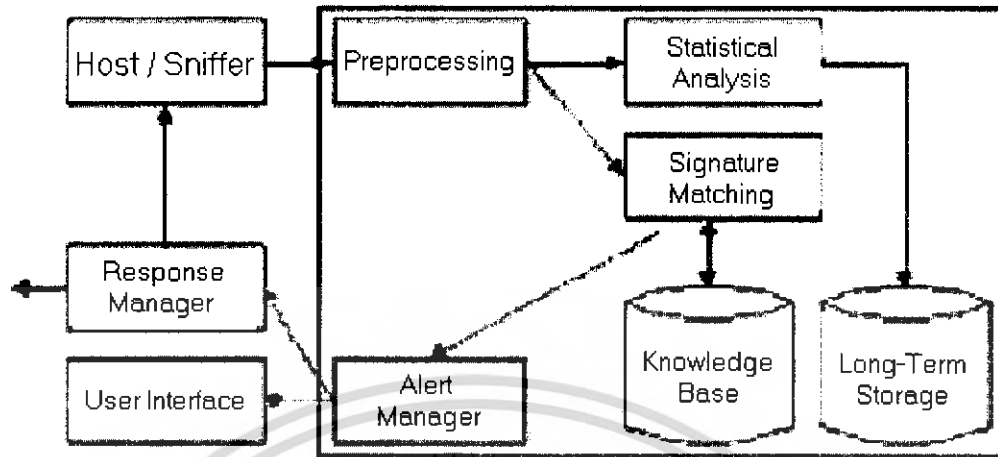
ระบบตรวจจับผู้บุกรุก คือ กระบวนการจำแนกและตอบสนองต่อกิจกรรมที่เกิดขึ้นในเน็ตเวิร์กที่มุ่งร้ายต่อระบบคอมพิวเตอร์และทรัพยากรที่อยู่บนเน็ตเวิร์กนั้น หรือหากอธิบายในภาษาง่าย ๆ ก็คือ เป็นกระบวนการตรวจจับการบุกรุกและการก่อวินาศกรรมที่เกิดขึ้นบนเครือข่ายนั่นเอง ดังนั้นระบบตรวจจับผู้บุกรุกก็คือระบบที่ประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์สำหรับทำหน้าที่คอยตรวจตราความเป็นไปและพฤติกรรมของข้อมูลที่ผ่านมาบนเน็ตเวิร์กว่าน่าสงสัยและมีสิ่งผิดปกติหรือไม่

ถ้าหน่วยงานใดมีการติดตั้งเครือข่ายภายใน (LAN) หรือเครือข่ายอินเทอร์เน็ต เพื่อใช้งานในองค์กร ถึงแม้ว่าระบบจะมีการติดตั้งไฟร์วอลล์ เพื่อป้องกันการบุกรุกจากบุคคลภายนอกแล้วก็ตาม ระบบก็ยังมีช่องโหว่ที่ทำให้เกิดความเสียหายได้ดังต่อไปนี้

ความเสี่ยงเนื่องจาก การเปิดบริการใช้งานบางประเภทที่ไฟร์วอลล์ ให้อำนาจบุคคลภายนอกที่มาจากอินเทอร์เน็ต เช่น การบริการเว็บแอปพลิเคชัน การบริการรับส่งเมลและการบริการถ่ายโอนข้อมูล (FTP) เป็นต้น เนื่องจาก ผู้ไม่ประสงค์ดี (Hacker) จะนิยมเข้ามาโจมตีและก่อให้เกิดความเสียหายแก่ระบบงานภายในองค์กร โดยเข้าทางที่ไฟร์วอลล์อนุญาตเป็นส่วนมาก

2.2.1 ส่วนประกอบของระบบตรวจจับผู้บุกรุก

โดยทั่วไป ไอดีเอส มีส่วนประกอบตามรูปข้างล่างนี้



รูปที่ 2.4 ส่วนประกอบของไอดีเอส

- โฮสต์ซิสเต็ม/เน็ตเวิร์กสไนฟเฟอร์ (Host System/Network Sniffer): ทำหน้าที่เป็นตัวตรวจจับเหตุการณ์ต่างๆ ที่เกิดขึ้นในโฮสต์ หรือเครือข่ายข้อมูลจากส่วนนี้เป็นเหมือนอินพุต ที่เข้าไปประมวลผลในไอดีเอส
- พร็ีโพรเซสซิ่ง (Pre-Processing) : จัดรูปแบบของอินพุต ที่รับเข้ามาเพื่อนำไปประมวลผลได้สะดวกต่อไป
- ส่วนวิเคราะห์ผลทางสถิติ (Statistical Analysis)
- ส่วนวิเคราะห์จากพฤติกรรมที่มีแบบแผน (Signature Matching): แนวความคิดตรงนี้นำมาจากที่ว่า การบุกรุกมักจะมีรูปแบบที่ค่อนข้างแน่นอน ส่วนนี้จะทำงานได้ดีต่อเมื่อมีข้อมูลมากพอที่จะวิเคราะห์ได้ว่าพฤติกรรมที่ปรากฏในระบบเป็นรูปแบบของการบุกรุกหรือไม่
- ฐานความรู้ (Knowledge Base): เป็นตัวเก็บข้อมูลเกี่ยวกับพฤติกรรมของการบุกรุก ข้อมูลนี้ถูกใช้โดยส่วนวิเคราะห์จากพฤติกรรมที่มีแบบแผน ข้อมูลส่วนนี้มีความสำคัญมากกับระบบเป็นตัวตัดสินเลยว่าระบบฉลาดพอที่จะตรวจจับการบุกรุกได้หรือไม่
- อลิร์ตแมนเนเจอร์ (Alert Manager): ทำหน้าที่เป็นตัวตัดสินใจว่าจะเหตุการณ์ที่เกิดขึ้นในระบบควรจะต้องเตือนหรือไม่ ระบบจะมีความอ่อนไหว มากน้อยแค่ไหนอยู่ที่ตัวนี้ด้วย
- ยูสเซอร์อินเตอร์เฟซ (User Interface): เป็นส่วนที่ได้ตอบกับผู้ใช้ อาจจะเป็นการแสดงผลที่หน้าจอ ส่งเสียงเตือนถึงการบุกรุก ส่งพิมพ์เป็นฮาร์ดค็อบปี หรือแม้แต่เชื่อมกับเพจเจอร์ / โทรศัพท์ นอกจากนี้ ยูสเซอร์อินเตอร์เฟซ ยังเป็นส่วน ได้ตอบระหว่างผู้ใช้กับระบบเพื่อ

เปลี่ยนแปลงหรือปรับปรุง ข้อมูลใน ฐานความรู้

- เรสพอนซ์แมนเนเจอร์ (Response Manager): รับข้อมูลจากเอเลิร์ตแมนเนเจอร์ เพื่อนำมาตัดสินใจว่าจะโต้ตอบกับการบุกรุกอย่างไร

2.2.2 ประเภทของระบบตรวจจับผู้บุกรุก ออกเป็นกลุ่มต่างๆ ได้ดังนี้

2.2.2.1 ระบบตรวจจับผู้บุกรุกบนพื้นฐานโฮสต์ (Host-Based Intrusion Detection System)

เป็นระบบไอดีเอสที่ออกแบบมาเพื่อจุดประสงค์ในการตรวจสอบการโจมตีที่เกิดขึ้นกับเครื่องใดเครื่องหนึ่งโดยเฉพาะ ซึ่งจะตรวจสอบการถูกโจมตีที่เกิดขึ้นกับบริการต่างๆ หรือแอปพลิเคชันแต่ละตัวได้ เช่น การพยายามที่จะเดารหัสผ่านเข้าสู่ระบบบริการ นอกจากนี้ระบบตรวจจับผู้บุกรุกบนพื้นฐานโฮสต์ยังสามารถที่จะตรวจสอบถึงการเข้ารหัสข้อมูลที่เครื่องนั้นๆ ติดต่อกับระบบอื่นๆ ในเครือข่ายได้เช่น ระบบเครือข่ายที่มีการเชื่อมต่อ VPN อีกทั้งตัวระบบก็ติดตั้งเข้ากับเครื่องเซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์ที่ต้องการจะป้องกันได้โดยตรง ดังนั้นไม่จำเป็นต้องเพิ่มฮาร์ดแวร์อื่นเข้าไปในระบบอีก

2.2.2.2 ระบบตรวจจับผู้บุกรุกบนพื้นฐานเน็ตเวิร์ก (Network-Based Intrusion Detection System)

เป็นระบบไอดีเอสที่ออกแบบมาทำการเฝ้าดูข้อมูลบนเครือข่ายโดยที่ระบบดังกล่าว จะทำการรับข้อมูลทั้งหมดที่อยู่บนส่วนของเครือข่ายที่รับผิดชอบนอกเหนือจากส่วนของเครือข่ายที่รับผิดชอบและชนิดของการสื่อสารอื่นๆ แล้วระบบดังกล่าวก็ไม่สามารถทำการตรวจจับแพ็กเก็ตต่างๆ ซึ่งจะถูกรวบรวมโดยเซ็นเซอร์ของระบบไอดีเอสและเซ็นเซอร์จะมองเห็นเฉพาะแพ็กเก็ตที่ผ่านส่วนของเครือข่ายที่เซ็นเซอร์นั้นติดตั้ง ดังนั้น แพ็กเก็ตต่างๆ จะเป็นที่น่าสนใจของเซ็นเซอร์ ก็ต่อเมื่อแพ็กเก็ตนั้นเข้ากับสัญญาณ (Signature) ที่กำหนดซึ่งปกติแล้ว สัญญาณ จะมี 3 ประเภท คือ

1) สัญญาณของสตริง (String Signature)

จะมองหาที่กซ์สตริง (Text String) ซึ่งอาจบ่งบอกถึงการโจมตีตัวอย่าง เช่น "cat" + + "7%rhost" อาจทำให้ระบบยูนิคซ์ เกิดช่องโหว่ต่อการโจมตีบนเครือข่าย

2) สัญญาณของพอร์ต (Port Signatures)

จะเฝ้าดูการพยายามติดต่อเข้ามาทางพอร์ตที่รู้จักกันดี และมักจะถูกโจมตี เช่น เทลเน็ต จะใช้ทีซีพีพอร์ต 23, เอฟทีพีจะใช้ทีซีพีพอร์ต 21/20, ซันอาร์พีซี (SUNRPC) ใช้ทีซีพี/ยูดีพีพอร์ต 111 และ ไอเอ็มเอป(IMAP) จะใช้ ทีซีพีพอร์ต 143 ซึ่งถ้าระบบของเราไม่ได้เปิดพอร์ตดังกล่าวแต่มีการพยายามเชื่อมต่อเข้ามาแสดงว่าแพ็กเก็ตดังกล่าวอาจจะมีประสงคร้ายก็ได้

3) สัญญาณของเฮดเดอร์ (Header Signatures)

พยายามมองหาคอมไบเนชัน (Combination) ที่อันตรายและผิดกฎหมายของแพ็กเก็ตเฮดเดอร์ ตัวอย่างที่เห็นได้ชัดของสัญญาณเฮดเดอร์ คือทีซีพีแพ็กเก็ต ซึ่งมีทั้งแฟล็ก (Flags) แบบซิน (SYN) และฟิน (FIN) ในการติดตั้งใช้งานไอดีเอส ในระบบเครือข่ายคอมพิวเตอร์นั้น การติดตั้งและใช้งานระบบไอดีเอส เพียงประเภทใดประเภทหนึ่งจะได้รับความปลอดภัยเพียงระดับหนึ่ง เพื่อความปลอดภัยที่สูงขึ้น จำเป็นต้องติดตั้งระบบไอดีเอส หลายประเภท รวมทั้ง ระบบไอดีเอส จะต้องมีความสามารถในการทำงานร่วมกัน กับระบบป้องกันรักษาความปลอดภัยประเภทอื่น

2.2.3 ข้อดีของการใช้ระบบตรวจจับผู้บุกรุก

2.2.3.1 การตอบสนองทันทีทันใด

จริงๆแล้วการวิเคราะห์การบุกรุกนั้นหากเป็นผู้เชี่ยวชาญที่มีความรู้ทางด้านเน็ตเวิร์กและโปรโตคอลเป็นอย่างดีก็จะสามารถวิเคราะห์ได้โดยอาศัยเครื่องมือเพียงเล็กน้อยเท่านั้นคือใช้เครื่องมือทำการจัดเก็บบันทึกข้อมูลทั้งหมดที่มีการสื่อสารบนเน็ตเวิร์ก แล้วนำข้อมูลที่ได้เหล่านั้นมาวิเคราะห์โดยพฤติกรรมและความสัมพันธ์ ก็จะสามารถหาสิ่งผิดปกติที่เกิดขึ้นได้ แต่การวิเคราะห์ในลักษณะดังกล่าวจะกระทำได้ก็ต่อเมื่อได้เกิดเหตุการณ์ไปแล้ว เนื่องจากการวิเคราะห์จะเป็นไปในลักษณะวิเคราะห์ข้อมูลย้อนหลัง ไม่สามารถกระทำได้ในทันที ซึ่งไอดีเอส จะช่วยแก้ไขข้อบกพร่องในส่วนนี้ เพราะไอดีเอส สามารถตรวจจับได้ทันทีที่มีความผิดปกติเกิดขึ้น และช่วยให้ทำการแก้ไขได้ทัน่วงที การทำงานพื้นฐานของไอดีเอส จะเหมือนกับการวิเคราะห์ที่ทำโดยคน เพียงแต่ไอดีเอสนั้นทำโดยอัตโนมัติและทำงานอยู่ตลอดเวลาไม่มีหยุด จึงสามารถตอบสนองต่อสิ่งผิดปกติได้รวดเร็วกว่า ซึ่งถ้าให้คนมานั่งตรวจจับก็ไม่สามารถทำได้ตลอดเวลา

2.2.3.2 การมีฐานความรู้ของการวิเคราะห์

จากที่ได้กล่าวมาข้างต้น การที่จะตรวจจับสิ่งผิดปกติและแยกแยะกิจกรรมเหล่านั้นออกจากการสื่อสารข้อมูลตามปกติได้นั้นต้องอาศัยความชำนาญ และเข้าใจรูปแบบการสื่อสารข้อมูลและการบุกรุกเป็นอย่างดี นั่นคือทักษะที่จำเป็นของนักวิเคราะห์การบุกรุก (Intrusion Analyst) ซึ่งผู้เชี่ยวชาญในระดับที่จะทำงานเช่นนี้ได้มีไม่มากนัก ประกอบกับเทคนิคและกลวิธีในการบุกรุกและก่อกรวนนั้นได้พัฒนาขึ้นทุกวัน วิธีตรวจจับและวิเคราะห์จำเป็นต้องพัฒนาตามให้สอดคล้องกันจึงจะตรวจจับได้อย่างมีประสิทธิภาพ ซึ่งในส่วนนี้ผู้เชี่ยวชาญอาจจะทำได้ไม่ดีเท่าไอดีเอส สามารถช่วยแบ่งเบาการวิเคราะห์ลงได้มาก โดยหากรู้พฤติกรรมแน่ชัดว่าเป็นการ มุ่งร้ายก็ให้จัดเก็บข้อมูลเหล่านี้ให้ไอดีเอส เสีย เมื่อกิจกรรมดังกล่าวเกิดขึ้นในเน็ตเวิร์ก ไอดีเอสก็สามารถตรวจพบได้ทันที และเมื่อค้นพบรูปแบบใหม่ก็จัดเก็บลงในไอดีเอสอีก ทำให้ไอดีเอสเสมือนมีฐานความรู้ในการวิเคราะห์การบุกรุกได้ดีในระดับหนึ่ง และขีดความสามารถก็จะเพิ่มขึ้นเรื่อยๆ ตามปริมาณที่เก็บอยู่ในฐานความรู้นั่นเอง หากมี

การบำรุงรักษาฐานความรู้ในตัว ไอดีเอส ได้ดีและนำไอดีเอสไปได้ ถึงขั้นนี้แล้วถึงแม้ว่าจะเป็นไอดีเอสแบบธรรมดาๆ ก็มีความสามารถมากกว่าผู้บริหารในระดับทั่วไปเสียอีก สำหรับนักวิเคราะห์แล้วเมื่อมีไอดีเอสจะทำให้ไม่ต้องห่วงหน้าพะวงหลัง เพราะการบุกรุกที่สามารถตรวจจับได้ง่ายๆ ก็สามารถตรวจพบได้โดยไอดีเอส อย่างน้อยไอดีเอสก็ช่วยกั้นกรองข้อมูลเบื้องต้นได้ในระดับหนึ่งและแบ่งเบาภาระได้ดีพอสมควร

2.2.3.3 การช่วยตรวจสอบข้อบกพร่องของระบบป้องกันอื่นๆ

เน็ตเวิร์กของผู้ใช้อาจจะมีการป้องกันการบุกรุกอยู่แล้วโดยใช้ไฟร์วอลล์ (Firewall) อย่างไรก็ตามไฟร์วอลล์มีใช้เครื่องมือที่จะป้องกันการบุกรุกได้โดยอัตโนมัติจะต้องอาศัยผู้ที่บริหารระบบกำหนดกฎให้เหมาะสมกับการใช้งาน อีกประการหนึ่ง ถึงแม้ว่าจะมีการตั้งกฎที่เหมาะสมแล้วก็ตาม แต่กฎเหล่านั้นอาจไม่สามารถป้องกันการบุกรุกได้ การบริหารไฟร์วอลล์ที่ดีก็ควรตรวจสอบย้อนหลัง (Audit) และการทดสอบเจาะระบบ (Penetration Test) เพื่อเป็นการตรวจทานระบบอีกครั้งหนึ่ง

ไอดีเอสสามารถช่วยได้มาก โดยติดตั้งไอดีเอสไว้หลังไฟร์วอลล์ และทำการทดสอบเจาะระบบด้วยวิธีการต่างๆ เพื่อดูว่าจะมีเทคนิคใดที่สามารถเจาะผ่านไฟร์วอลล์ได้บ้าง และหากมีแพ็คเกจใดผ่านเข้าไปไอดีเอส ก็จะตรวจพบ ทำให้ผู้บริหารระบบสามารถปรับปรุงกฎให้รัดกุมมากขึ้น

2.2.4 ข้อเสียของการใช้ระบบตรวจจับผู้บุกรุก

ถึงแม้ว่าไอดีเอส จะมีประโยชน์ค่อนข้างมากในการรักษาความปลอดภัย และเตือนภัย ล่วงหน้า แต่ก็ยังมีข้อเสียอยู่หลายประการซึ่งผู้ที่นำไปใช้จะต้องตระหนักไว้

2.2.4.1 การละเมิดความเป็นส่วนตัว

เนื่องจากไอดีเอส มีพื้นฐานจากการนำข้อมูลทั้งหมดที่ทำการสื่อสารกันมาทำการวิเคราะห์ ซึ่งข้อมูลเหล่านั้นจะต้องครอบคลุมข้อมูลทั่วไปที่มีการสื่อสารกันตามปกติ และการที่จะทราบว่ามีคามผิดปกติหรือไม่นั้นก็จะต้องอ่านข้อมูลทั้งหมดด้วย ดังนั้น ไม่ว่ากิจกรรมใดที่เกิดขึ้นในเน็ตเวิร์กไม่ว่าจะท่องเว็บ, การดาวน์โหลดข้อมูล, การแชทคุยกัน, โอซิทีว, อีเมล และกิจกรรมอื่นๆ ที่สื่อสารผ่านเน็ตเวิร์ก ก็จะเปิดอ่านได้จากไอดีเอส นั้นหมายความว่าไอดีเอส สามารถนำไปใช้งานในทางที่ผิดเพื่อละเมิดสิทธิส่วนบุคคลได้ การทำงานของ ไอดีเอส เปรียบเสมือนการที่ตำรวจต้องทำการตรวจสอบและดักจับผู้ไม่หวังดีที่คอยโทรศัพท์ก่อกรวนชาวบ้านในหมู่บ้าน และเพื่อการนี้ตำรวจจึงต้องทำการดักฟังโทรศัพท์ของทุกคนที่อยู่ในหมู่บ้านนั้น ซึ่งอาจจะมีเพียงหนึ่งในพื้นที่เป็นผู้ร้ายแต่ตำรวจผู้ทำหน้าที่ดักฟังก็จะรู้ความลับของคนทุกคน บางทีการที่มีคนมาดักฟัง ความลับของคนอาจจะ เป็นอันตรายกว่าการโดนผู้ร้ายก่อกรวนก็เป็นได้

ดังนั้นการนำไอดีเอส มาติดตั้งในเน็ตเวิร์กจะต้องได้รับอนุมัติจากหน่วยงานอย่างถูกต้องแล้วเท่านั้น และผู้ที่ทำหน้าที่ในด้านนี้ต้องเป็นผู้ที่ได้รับความไว้วางใจและมีความรับผิดชอบสูงอันที่จะไม่ละเมิดสิทธิส่วนบุคคลของผู้อื่น และหากเห็นข้อมูลใดๆ ก็ต้องไม่เปิดเผยข้อมูลเหล่านั้นแก่บุคคลอื่นโดยทั่วไปแล้วการติดตั้งอุปกรณ์ที่สามารถดักอ่านข้อมูลของผู้อื่นบนเน็ตเวิร์กได้นั้นจะ เป็นข้อห้ามอันคับตันๆ ในนโยบายรักษาความปลอดภัยเลยทีเดียว สิ่งที่เป็นข้อสังเกตคือ การกระทำในลักษณะนี้ยากต่อการป้องกันทางเทคนิค และมีบทลงโทษสำหรับผู้ละเมิดในขั้นรุนแรง

2.2.4.2 การตอบโต้อัตโนมัติ

ไอดีเอสที่มีจำหน่ายอยู่ในท้องตลาด จะมีส่วนหนึ่งที่ผู้ใช้สามารถกำหนดการดำเนินการอย่างหนึ่ง อย่างใดเมื่อตรวจพบการบุกรุกเกิดขึ้น เช่น ส่งจดหมายเตือนผู้ดูแลระบบ, เรียกวิทยุติดตามตัว, ส่งข้อมูลไปยังไฟร์วอลล์เพื่อจำกัดการเข้าออกของข้อมูล และสิ่งสำคัญที่สุดที่อาจจะเกิดผลเสียร้ายแรงมากที่สุดต่อเจ้าของได้ก็คือ การโจมตีกลับไปยังต้นกำเนิดของการบุกรุก (Counter Attack) โดยที่ไอดีเอสเองก็จะรู้จักวิธีการโจมตีต่างๆ คืออยู่แล้ว จึงมีโซ่เรื่องยากเย็นแต่อย่างใดที่จะทำการโจมตีผู้อื่น ผู้ผลิตจึงมักเพิ่มเติมส่วนนี้ให้แก่ไอดีเอส เสมือนหนึ่งติดอาวุธไว้ให้ต่อสู้กับแฮกเกอร์เลยทีเดียว ผู้ดูแลระบบบางส่วนอาจจะรู้สึกสะใจและคิดว่าเหมาะสมแล้วกับการโจมตีกลับไปยังแฮกเกอร์เหล่านั้นให้หลาบจำและไม่เข้ามาข้องแวะอีก เป็นนโยบายการรักษาความปลอดภัยแบบตาต่อตาฟันต่อฟัน และเชื่อว่าหากกำหนดให้การโจมตีกลับเป็นไปอย่างอัตโนมัติ แล้วน่าจะทำให้ปลอดภัยมากขึ้น ในคำคืนที่สงบใครจะไปรู้ว่าไอดีเอส กำลังต่อกรอยู่กับแฮกเกอร์ที่กำลังแอบเข้ามาในระบบอย่างสุดกำลัง และสู้รบตาเพื่อรักษามิให้แฮกเกอร์บุกรุกเข้ามาในเน็ตเวิร์กได้ ในความเป็นจริงแล้วการตัดสินใจว่าผู้ใดเป็นแฮกเกอร์อย่างชัดเจนมิได้ทำได้โดยง่ายและในเวลาอันรวดเร็ว การที่กำหนดให้ไอดีเอส ทำการตอบโต้กลับไปในทันทีโดยมีข้อมูลเพียงผิวเผินนั้น นอกจากจะไม่ช่วยให้เน็ตเวิร์กเราปลอดภัยแล้วยังจะทำให้เรากลายเป็นแฮกเกอร์ที่คอยโจมตีผู้อื่นเสียเองยกตัวอย่างความเสียหายเช่น

- การวิเคราะห์ผิดพลาดเข้าใจว่ากิจกรรมที่เกิดขึ้นเป็นการบุกรุกและไอดีเอสก็ดำเนินการโจมตีกลับไปในทันที กรณีนี้ผู้บริสุทธิ์ก็จะถูกโจมตีจากไอดีเอส ของเราโดยที่ไม่รู้เรื่องใดๆ
- การวิเคราะห์ถูกต้องแต่แอดเดรสปลายทางเป็นแอดเดรสปลอมกรณีนี้หากไอดีเอสไม่มีกลไกในการตรวจสอบแอดเดรสที่มีประสิทธิภาพ อาจไม่สามารถแยกแยะได้ว่าต้นทางของการโจมตีแท้จริงนั้นเป็นที่ไหน และเมื่อทำการโจมตีกลับไปที่อาจจะมิใช่ตัวการที่แท้จริง และเหตุการณ์จะเลวร้ายยิ่งขึ้นหากแอดเดรสที่ปลอมมานั้นเป็นหน่วยงานทางความมั่นคงหรือหน่วยงานทางการทหาร และเมื่อผู้ดูแลระบบอาจจะตระหนักได้ว่าไอดี

เอสตัวเดียวอาจจะทำให้เขาต้องไปนอนในคุกหลายคืน เทคนิคการปลอมแอดเดรสในลักษณะนี้อาจจะเป็นการขีมือ ไอดีเอสของเราไปโจมตีผู้อื่นอีกทอดหนึ่งได้เป็นอย่างดี

- การวิเคราะห์แอดเดรสที่ถูกต้อง และการโจมตีกลับไปก็ตรงไปยังแฮกเกอร์อย่างถูกต้องตามที่ต้องการ แต่ผลที่ได้ก็เพียงอาจจะทำให้แฮกเกอร์หยุดความพยายามไปชั่วขณะเท่านั้น อีกไม่นานก็จะหาวิธีกลับมาใหม่ และไม่เกิดผลใดๆ เลยนอกจากเป็นการช่วยผู้ให้เกิดความรุนแรงมากขึ้นเท่านั้นสิ่งที่สำคัญที่ผู้ทำหน้าที่ด้านความปลอดภัยและผู้บริหารระบบต้องตระหนักไว้คือท่านไม่มีสิทธิพิเศษที่จะตอบโต้ผู้บุกรุกโดยการโจมตีกลับไม่ว่าจะกรณีใดสิ่งที่ท่านจะทำได้ดีที่สุดคือทำให้ระบบแข็งแกร่งมั่นคงและปลอดภัยที่สุดเท่านั้น นั่นคือปิดประตูบ้านให้แน่น ตรวจสอบอย่างรัดกุม และใช้งานเท่าที่จำเป็น ส่วนผู้ที่กระทำผิดเหล่านั้นควรปล่อยให้ไปตามกฎหมายและกระบวนการยุติธรรมจะดีที่สุด เพราะการตอบโต้การกระทำผิดกฎหมายด้วยวิธีที่ผิดกฎหมายจะทำให้เรากลายเป็นจำเลยไปด้วยในที่สุด

2.2.4.3 การเตือนภัยผิดพลาด

ข้อนี้อาจจะไม่ใช่ข้อเสียที่สำคัญที่สุดของการใช้ ไอดีเอส หากผู้ใช้มีความรู้ในการใช้งานที่ดีพอและเข้าใจหลักการวิเคราะห์การบุกรุกของไอดีเอส ได้ดีอย่างที่ได้อ่านมาแล้วข้างต้นก็คือ อาจจะมีกิจกรรมหลายอย่างที่มีลักษณะใกล้เคียงหรือบางครั้งเหมือนกับการบุกรุก ซึ่งแน่นอนว่า หากไอดีเอสถูกกำหนดให้ตรวจจับกิจกรรมประเภทดังกล่าวแล้ว ก็จะมีการเตือนในทันทีที่ตรวจพบและเป็นหน้าที่ของนักวิเคราะห์ที่จะทำการสืบค้นข้อมูลด้านอื่นๆ มาประกอบการวินิจฉัยอีกครั้งหนึ่งว่าพฤติกรรมที่ตรวจพบนั้นเป็นการบุกรุกหรือไม่ อย่างไร ไอดีเอสที่ถูกกำหนดให้มีความว่องไวเป็นพิเศษมักจะสามารถตรวจจับพฤติกรรมที่ก้าวกึ่งนั้น ได้มากเป็นพิเศษ

ตัวอย่างเช่น ไอดีเอสได้ถูกกำหนดไว้ว่า เมื่อได้รับบิงแพ็กเก็ต (Ping Packet) จากแอดเดรสเดิมติดต่อกัน 10 แพ็กเก็ตภายใน 30 วินาที ให้เตือนว่าเป็นการพยายามโจมตีโดยเทคนิคบิงฟlood (Ping Flood) เป็นต้นหากเน็ตเวิร์กดังกล่าวเป็นเน็ตเวิร์กที่ใช้งานโดยวิศวกรระบบ และมีการทดสอบการบิง (Ping) บ่อยๆ อาจจะทำให้ ไอดีเอส เตือนอยู่แทบตลอดเวลาโดยไม่ได้มีการบุกรุกที่แท้จริง

การเตือน โดยมิได้มีการบุกรุกจริงนั้น อาจจะถูกมองว่าไม่ส่งผลเสียหาประการใดและน่าจะเกิดประโยชน์เสียด้วยซ้ำ เพราะจะทำให้ผู้ดูแลระบบมีความตื่นตัวตลอดเวลาแต่ในความเป็นจริงแล้วธรรมชาติของมนุษย์มีแนวโน้มจะละเลยต่อสิ่งเหล่านี้ หากมีการเตือนแล้วไม่มีการบุกรุกจริงอยู่บ่อยครั้งเข้า ความน่าเชื่อถือของไอดีเอสจะลดลงตามลำดับ และเมื่อมีความบุกรุกจริงก็จะไม่ได้ให้ความสนใจเท่าที่ควรและไม่ได้หาทางป้องกันอย่างเหมาะสม นั่นคือไอดีเอสจะกลายเป็นเด็กเลี้ยงแกะที่เวลา

หมาป่าเข้ามาจริงก็ไม่มีผู้ได้รับฟัง ดูเฉินๆ อาจจะเหมือนว่ายังดีกว่าถ้าไม่มีไอดีเอสเสียเลย แต่การมีไอดีเอสอยู่ในระบบโดยไม่นำมาปรับแต่งอย่างเหมาะสม และเชื่อมั่นว่าไอดีเอสสามารถจะคอยระแวดระวังและเก็บหลักฐานต่างๆ ไว้ให้มันจะทำให้ผู้บริหารระบบนิ่งนอนใจ และคลายความเคร่งครัดในการปฏิบัติงานลง อาจถึงขั้นหย่อนยานกว่าการป้องกันในระดับปกติที่ไม่มีไอดีเอสได้

นอกจากนี้หากปล่อยให้ไอดีเอสมีการเตือนอย่างไม่เหมาะสมจะทำให้เกิดข้อมูลในลักษณะที่เป็นการบงกชจริงและการเตือนผิดพลาดผสมกันอยู่ อาจทำให้การเตือนที่เป็นของจริงถูกกลบไปและยากต่อการสังเกต อย่างลึ้มว่าแฮกเกอร์ที่มีความสามารถจะทิ้งร่องรอยไว้เพียงเล็กน้อยอาจจะมีเพียง 2-3 ร่องรอยเท่านั้นที่ไอดีเอสสามารถตรวจพบได้ หากร่องรอยเหล่านี้ถูกนำไปผสมปะปนกับการตรวจจับอื่นๆ อีกนับพัน ย่อมมีโอกาสูงที่จะถูกมองเลยไปโดยไม่มีผู้ใดให้ความสนใจ

2.2.5 สรุปความสามารถของระบบตรวจจับผู้บุกรุก

ไอดีเอสเป็นเครื่องมือสำคัญในการรักษาความปลอดภัยในเน็ตเวิร์ก ทำหน้าที่ในเชิงรุก (Proactive) สามารถทำให้ผู้ดูแลระบบสามารถป้องกันภัยคุกคามได้ล่วงหน้าก่อนที่การบุกรุกจะเกิดขึ้น หรือก่อนที่การบุกรุกจะกระทำสำเร็จ นอกจากนี้ไอดีเอสยังสามารถช่วยในการเก็บหลักฐานทางอิเล็กทรอนิกส์ของการบุกรุกที่เกิดขึ้น สามารถนำไปวิเคราะห์และสืบค้นผู้กระทำผิดได้ในภายหลัง แต่ทั้งนี้ไอดีเอสมิใช่เครื่องมืออัตโนมัติที่สามารถจับการบุกรุกได้อย่างถูกต้อง 100 เปอร์เซ็นต์การนำไปใช้งานต้องอาศัยความเข้าใจ และการปรับแต่ง อย่างถูกต้องเหมาะสมกับสิ่งแวดล้อมรวมทั้งต้องอาศัยการบำรุงรักษาและตรวจสอบอยู่เสมอสม่ำเสมอ

นอกจากนี้ไอดีเอสเองก็มีทั้งข้อดีและข้อเสียในตัวเองซึ่งผู้ที่นำไปใช้จะต้องตระหนักให้มาก และต้องคัดเลือกบุคคลากรที่มีความชำนาญและมีความรับผิดชอบที่เหมาะสมให้เป็นผู้ดูแล เพื่อเป็นการป้องกันมิให้ไอดีเอสถูกนำไปใช้ในทางที่ผิดและส่งผลร้ายต่อบุคคลอื่นมากกว่าจะใช้ในการป้องกันระบบของตนเอง

2.3 เทคนิคทางด้านเครือข่ายและโปรโตคอล

2.3.1 ความหมายเบื้องต้นของโปรโตคอล

โปรโตคอล คือ เป็นตัวที่มีหน้าที่สำหรับคอยตกลงระเบียบวิธี ที่กำหนดขึ้นสำหรับสื่อสารข้อมูล โดยสามารถส่งผ่านข้อมูลไปยังปลายทางได้อย่างถูกต้อง เมื่อคอมพิวเตอร์เครื่องหนึ่งต้องการรับส่งข้อมูลกับคอมพิวเตอร์อีกเครื่องหนึ่งที่มีระบบแตกต่างกัน หรือคนละผู้ผลิตเป็นสิ่งที่ทำให้การติดต่อทำได้ยากมาก จึงต้องมีตัวที่เป็นมาตรฐานส่วนกลาง ที่จำเป็นต้องใช้ในการรับส่งข้อมูล

2.3.2 ความรู้เกี่ยวกับโมเดลเครือข่ายแบบโปรโตคอลทีซีพี/ไอพี(TCP/IP)

โปรโตคอลทีซีพี/ไอพี เป็นโปรโตคอลที่ใช้กันแพร่หลายที่สุด โดยเฉพาะเมื่อถูกนำไปใช้กับเครือข่ายบนอินเทอร์เน็ต ทีซีพี/ไอพี มีการแบ่ง โปรโตคอลสื่อสารออกเป็นชั้นๆ โดยจะมีการเรียกลำดับชั้นของทีซีพี/ไอพีว่า ทีซีพี/ไอพี สแต็ก(TCP/IP Stack) โดยทีซีพี/ไอพี สแต็ก มีทั้งหมด 4 ชั้น คือ

2.3.2.1 ลำดับชั้นของโมเดลเครือข่ายแบบโปรโตคอลทีซีพี/ไอพี

1) ลำดับชั้นที่ 4: โพรเซสสเลเยอร์(Process Layer)

จะเป็นแอปพลิเคชัน โปรโตคอล(Application Protocol) ที่ทำหน้าที่เชื่อมต่อกับผู้ใช้ และให้บริการต่างๆ เช่น เอฟทีพี(FTP) , เทลเน็ต(Telnet) , เอสเอ็นเอ็มพี(SNMP) เป็นต้น

2) ลำดับชั้นที่ 3: โฮสต์ทูโฮสต์เลเยอร์(Host to Host Layer)

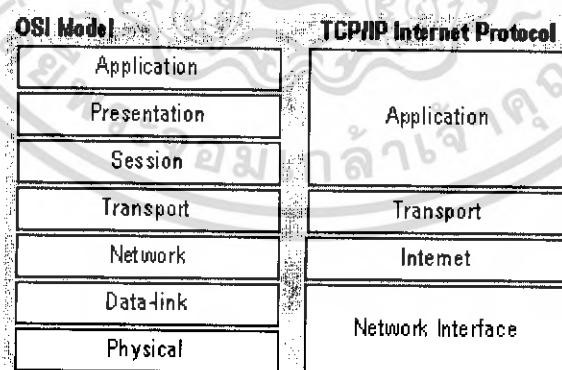
จะเป็นทีซีพี หรือยูดีพี(UDP) ที่ทำหน้าที่คล้ายกับเลเยอร์ที่สี่ของแบบจำลองโอเอสไอ(OSI Model) ควบคุมการรับส่งข้อมูลจากปลายด้านส่งถึงปลายด้านรับข้อมูล

3) ลำดับชั้นที่ 2: อินเทอร์เน็ตเวิร์ก(Internet network)

ได้แก่ ส่วนของโปรโตคอลไอพี(IP) ซึ่งทำหน้าที่คล้ายกับเลเยอร์ที่สามของแบบจำลองโอเอสไอเชื่อมต่อคอมพิวเตอร์ของด้านรับ และด้านส่งเข้าหากันผ่านระบบเครือข่ายพร้อมทั้งเลือก หรือ กำหนดเส้นทางที่จะใช้ในการรับส่งข้อมูลระหว่างกัน และส่งผ่านข้อมูลที่ได้รับไปยังอุปกรณ์ในเครือข่ายต่างๆ จนกระทั่งถึงปลายทาง ข้อมูลที่รับส่งกันจะอยู่ในรูปแพ็กเก็ต หรือเฟรมข้อมูล

4) ลำดับชั้นที่ 1: เน็ตเวิร์กอินเทอร์เฟซ(Network Interface)

ทำหน้าที่คล้ายกับเลเยอร์ที่หนึ่งและสองของแบบจำลองโอเอสไอ คือเชื่อมต่อการรับส่งข้อมูลในระดับฮาร์ดแวร์ โดยทำหน้าที่แปลคำสั่งนั้นๆ ให้เป็นคำสั่งควบคุมฮาร์ดแวร์ และแก้ไขข้อผิดพลาดที่ตรวจพบนั้น ซึ่งที่ใช้กันอยู่จะเป็นตามมาตรฐาน IEEE ข้อมูลในชั้นนี้จะอยู่ในรูปเฟรม



รูปที่ 2.5 โมเดลเครือข่ายแบบโปรโตคอลทีซีพี/ไอพี

2.3.2.2 หลักการทำงานของโมเดลเครือข่ายแบบโปรโตคอลทีซีพี/ไอพี

แนวคิดหลักของระบบเครือข่ายคอมพิวเตอร์ ก็คือ การเชื่อมโยงอุปกรณ์เข้าด้วยกัน ไม่ว่าจะ เป็นเครื่องเซิร์ฟเวอร์ และอุปกรณ์ในเครือข่ายอื่นๆ จึงจะต้องมีการไอพีแอดเดรส(IP Address) ที่เป็น ค่าที่อยู่ไว้อ้างอิงถึงที่ที่จะส่งข้อมูลผ่าน

1) ไอพีแอดเดรส

ไอพีแอดเดรสถูกกำหนดขึ้นมาให้เป็นหมายเลขอ้างอิงประจำตัวของอุปกรณ์ต่างๆ ที่ เชื่อมต่ออยู่ในเครือข่ายอินเทอร์เน็ต โดยการกำหนดไอพีแอดเดรสให้แต่ละเครื่อง หรือแต่ละอุปกรณ์นี้ จะต้องไม่ซ้ำกัน ซึ่งไอพีแอดเดรสนี้จะไม่ถูกผูกติดกับตัวฮาร์ดแวร์ จึงสามารถกำหนดใหม่ หรือแก้ไข เปลี่ยนแปลงได้เมื่อมีการเปลี่ยนแปลงตัวฮาร์ดแวร์

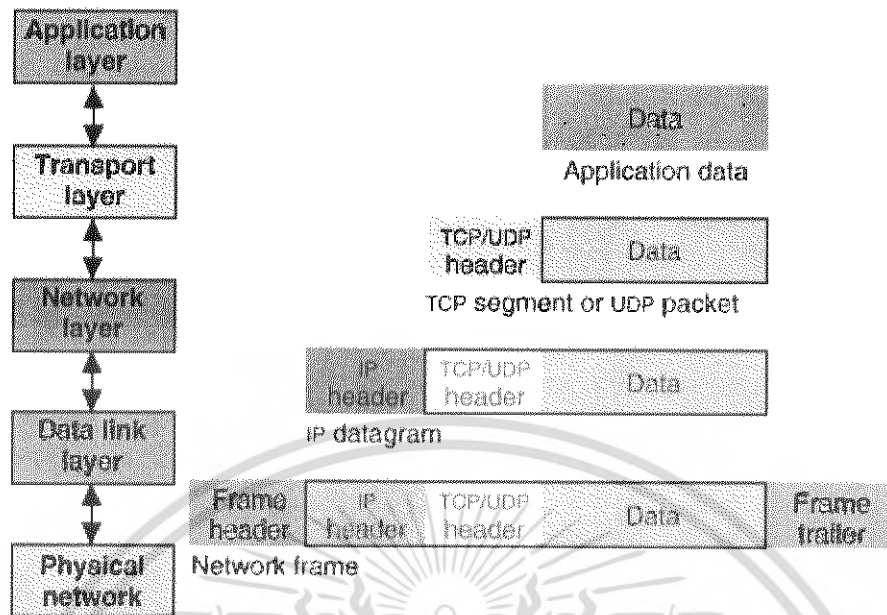
โปรโตคอลไอพีจำเป็นต้องอาศัยไอพีแอดเดรสเพื่อระบุถึงอุปกรณ์ต่างๆ ที่อยู่ในเครือข่าย ไม่ว่าจะ เป็นเว็บเซิร์ฟเวอร์ เมล์เซิร์ฟเวอร์ อุปกรณ์เราเตอร์ ไอพีแอดเดรสจะเป็นค่าตัวเลขขนาด 32 บิต ถูกแบ่งออกเป็น 4 ส่วน ส่วนละ 8 บิต และถูกคั่นแต่ละส่วนด้วยเครื่องหมายจุด(.)

2) แพ็กเก็ตข้อมูล (Data Packet)

เมื่อมีการส่งข้อมูลบนเครือข่ายอินเทอร์เน็ตนั้น ที่แสดงออกมาทางบราวเซอร์ ข้อมูล จำเป็นต้องมีการทำให้มีขนาดเล็กลง โดยแบ่งออกเป็นย่อยๆ เรียกว่าแพ็กเก็ตข้อมูลหรือคาต้าแกรม (Datagram) โดยข้อมูลจะถูกแบ่งออกเป็นย่อยๆ มีประโยชน์ คือ ทำให้เครือข่ายนั้นสามารถรองรับการ ติดต่อ และรับส่งข้อมูลกันได้อย่างราบรื่นไม่ติดขัด หรือถ้าเกิดปัญหาเครือข่ายทำงานช้า เมื่อมีการรับส่ง ข้อมูลขนาดใหญ่ เนื่องจากสายสัญญาณเชื่อมโยงเป็นสื่อที่ต้องแบ่งกันใช้ นอกจากนี้การแบ่งข้อมูล ออกเป็นส่วนย่อยๆ ยังทำให้สามารถเพิ่มกระบวนการตรวจทานความถูกต้องของข้อมูลที่ปลายทาง และ แก้ไขเมื่อข้อมูลผิดพลาด หรือตกหล่นได้โดยง่ายอีกด้วย

3) การห่อหุ้ม (Encapsulation)

การผนึกข้อมูลหนึ่งให้ไปเป็นอีกรูปแบบหนึ่งนี้ จะเป็นกลไกที่สำคัญของการใช้งาน โปรโตคอลทีซีพี/ไอพีมาก โดยที่กระบวนการที่ใช้จะมีขั้นตอนคร่าวๆ ดังรูป



รูปที่ 2.6 Header ในแต่ละลำดับชั้นของ TCP/IP

2.4 ลักษณะของโปรโตคอลที่ใช้ในโปรแกรมประยุกต์เพียร์ทูเพียร์

โปรแกรมประยุกต์เพียร์ทูเพียร์นั้นมีหลากหลายโปรแกรมมาก เช่น Bitcomet , LimeWire , Kazaa เป็นต้น ซึ่งแต่ละ โปรแกรมมีการใช้ซิกเนเจอร์ (Signature) ที่มีลักษณะเฉพาะสำหรับแต่ละ โปรโตคอลที่ โปรแกรมนั้นใช้เป็นช่องทางในการติดต่อสื่อสาร ในที่นี้จะยกตัวอย่างซิกเนเจอร์ของแพ็กเก็ตของ โปรโตคอลที่มีความนิยมมากกว่าตัวอื่นๆ คือ Gnutella , eDonkey , DirectConnect , BitTorrent และ Kazaa

1) Gnutella Protocol

จะมีเฮดเดอร์ของคำร้องขอ (request header) ดังนี้

```
GET /get/<File Index>/<File Name>
```

```
/HTTP/1.0 \r \n
```

```
Connection: Keep-Alive\r\n
```

```
Range: byte=0-\r\n
```

```
User-Agent: <Name>\r\n
```

```
\r\n
```

73330

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ส่วนเฮดเดอร์ของคำตอบกลับ(response header) จะเป็นดังนี้

HTTP 200 OK\r\n

Server: <Name>\r\n

Content-type: \r\n

Content-length: \r\n

\r\n

ฉะนั้นถ้าเฮดเดอร์ใดมีสตริงต่อไปนี้ ถือว่าเป็นแพ็กเก็ตของ Gnutella

- เฮดเดอร์ที่ขึ้นต้นด้วยคำว่า GET หรือ HTTP หรือ GNUTELLA

- ถ้าเฮดเดอร์ใดที่ขึ้นต้นด้วย GET หรือ HTTP จะต้องตามด้วยสตริงต่อไปนี้

- User-Agent: <Name>

- UserAgent: <Name>

- Server: <Name>

โดยที่ <Name> อาจจะเป็น LimeWire, Bear-Share, Gnucleus, MorpheusOS, XoloX, MorpheusPE, gtkgnutella,Acquisition, Mutella-0.4.1, MyNapster, Mutella-0.4.1, MyNapster, Mutella-0.4, Qtella, AquaLime, NapShare,Comebaek, Go, PHEX, SwapNut, Mutella-0.4.0, Shareaza,Mutella-0.3.9b, Morpheus, FreeWire, Opencxt, Mutella-0.3.3,Phex.

2) eDonkey Protocol

เฮดเดอร์ของมันจะต่อจากเฮดเดอร์ของพีซีพีมีลักษณะดังนี้คือ

```

1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8
+-----+
|  Number  |
+-----+
| packet Length (4 bytes) |
+-----+
| Message type |
+-----+

```

รูปที่ 2.7 ลักษณะเฮดเดอร์ของ eDonkey Protocol

- 1 ไบต์แรกจะเป็นมาร์กเกอร์ซึ่งมีค่า 0xE3 (เลขฐาน 16)
- 4 ไบต์ต่อมาเป็นขนาดของแมสเสจ(message)
- 1 ไบต์สุดท้ายเป็นแมสเสจไอดี(message ID)ที่เป็นเอกลักษณ์ไม่ซ้ำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3) DirectConnect Protocol

ลักษณะเฮดเดอร์ของมัน จะเป็นดังนี้

Scommand_type field1 field2 ...|

ฉะนั้นถ้าเฮดเดอร์ใดมีสตริงต่อไปนี้ ถือว่าเป็นแพ็กเก็ตของ DirectConnect

- ไบต์แรกที่อยู่ก่อนเฮดเดอร์ของโปรโตคอลที่ซีพี/ไอพีเป็น "\$" และ ไบต์สุดท้ายเป็น "|"

- ตัวที่อยู่ก่อน "\$" จะเป็น command_type ได้แก่ MyNick, Lock, Key, Direction, GetListLen, ListLen, MaxedOut, Error, Send, Get, FileLength, Canceled, HubName, ValidateNick, ValidateDenide, GetPass, Mypass, BadPass, Version, Hello, Logedin, MyINFO, GetINFO, GetNickList, NickList, OpList, To, Connect-ToMe, MultiConnectToMe, RevConnectToMe, Search, MultiSearch, SR, Kick, OpForceMove, ForceMove, Quit.

4) BitTorrent Protocol

เฮดเดอร์ของมันมีรูปแบบดังนี้

<a character(1 byte)><a string(19 byte)>

ฉะนั้นถ้าเฮดเดอร์ใดมีสตริงต่อไปนี้ ถือว่าเป็นแพ็กเก็ตของ BitTorrent

- ไบต์แรกจะเป็นตัวอักษร 19 (0x13)

- 19 ไบต์ต่อมาจะมีคำว่า "BitTorrent Protocol" อยู่

5) Kazaa Protocol

เฮดเดอร์ของคำร้องขอ จะมีลักษณะดังนี้

GET /.files HTTP/1.1\r\n

Host: IP address/port\r\n

UserAgent: KazaaClient\r\n

X-Kazaa-Username: \r\n

X-Kazaa-Network: KaZaA\r\n

X-Kazaa-IP: \r\n

X-Kazaa-SupernodeIP: \r\n

เฮดเดอร์ของคำตอบกลับจะมีลักษณะดังนี้

HTTP/1.1 200 OK\r\n

Content-Length: \r\n

Server: KazaaClient\r\n

X-Kazaa-Username: \r\n

X-Kazaa-Network: \r\n

X-Kazaa-IP: \r\n

X-Kazaa-SupernodeIP: \r\n

Content-Type: \r\n

ฉะนั้นการที่จะระบุว่าเป็นเซคเตอร์ของ Kazaa Protocol จะต้องมียกยณะดังนี้

- มีคำว่า GET หรือ HTTP

- ต้องมีฟิลด์ที่เป็นคำว่า X-Kazaa



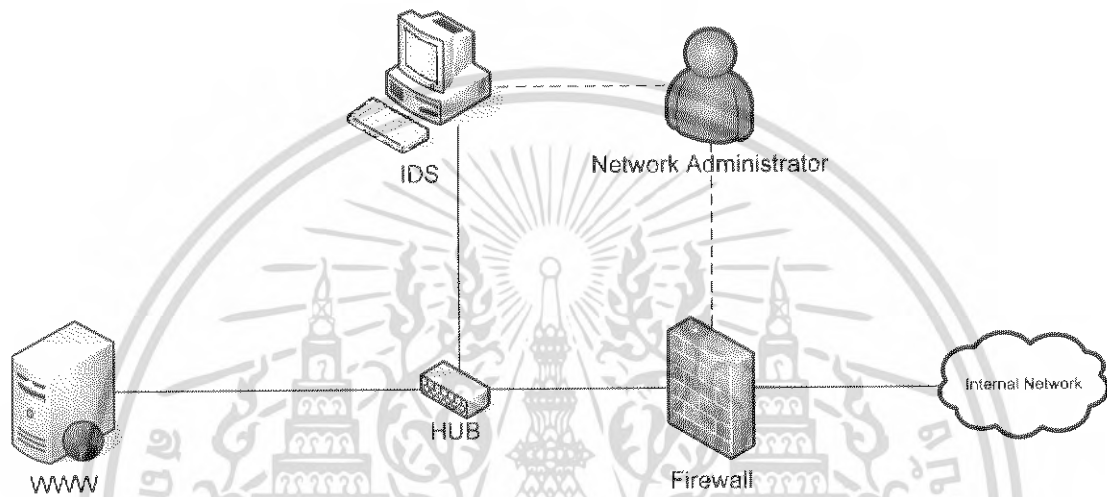
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

วิธีดำเนินการวิจัย

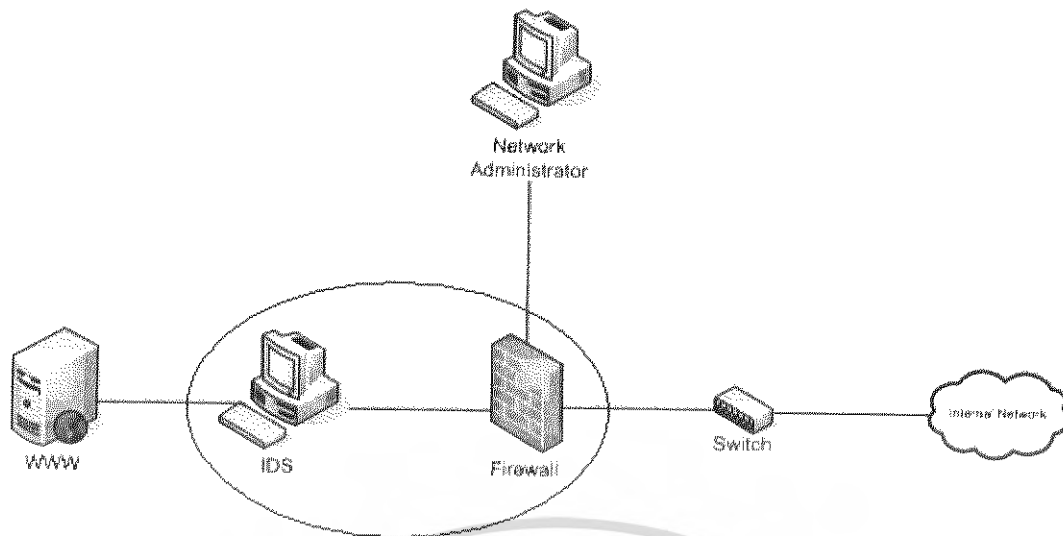
3.1 รูปแบบโครงสร้างของระบบตรวจจับผู้บุกรุกที่ใช้ในการดำเนินการวิจัย

ระบบตรวจจับผู้บุกรุกจะมีลักษณะโครงสร้างอยู่ 2 รูปแบบ คือ อินไลน์(In-Line Architecture) และ วันอาร์ม(One-Arm Architecture) ดังรูป



รูปที่ 3.1 One-Arm Architecture

ในการทำงานแบบวันอาร์ม แพ็กเก็ตข้อมูลจะวิ่งผ่านสวิตช์(Switch)หรือฮับ(Hub) และถูกทำสำเนาส่งไปให้ระบบตรวจจับผู้บุกรุก ตรวจสอบแพ็กเก็ตนั้นว่ามีซิกเนเจอร์ตรงกับซิกเนเจอร์ของเพิร์ทูเพียร์หรือไม่ ถ้าตรงก็จะส่งให้ไฟร์วอลล์ (Firewall) ให้บล็อกไอพี(IP) นั้นในระยะเวลาหนึ่ง ดังภาพที่ 3.1



รูปที่ 3.2 In-Line Architecture

ในการทำงานแบบออนไลน์ แพ็กเก็ตจะวิ่งจากเครือข่ายอินเทอร์เน็ตไปยังเครือข่ายแลนหรือจากเครือข่ายแลนไปยังเครือข่ายอินเทอร์เน็ตโดยผ่านระบบตรวจจับผู้บุกรุกที่ทำงานร่วมกับไฟร์วอลล์หรือสวิตช์ ถ้าหากพบว่ามีแพ็กเก็ตที่มีซิกเนเจอร์เป็นแพ็กเก็ตของเพิร์ทูเพียร์ จะสั่งให้ไฟร์วอลล์บล็อกหมายเลขไอพีนั้นในระยะเวลาหนึ่ง

ในการวิจัยเราได้ใช้ระบบตรวจจับผู้บุกรุกแบบวันอาร์ม เพราะข้อดีของมันคือ ถ้าหากตัวระบบตรวจจับผู้บุกรุกเกิดความเสียหายไม่สามารถทำงานต่อได้ เครือข่ายแลนและเครือข่ายอินเทอร์เน็ตยังคงสามารถติดต่อสื่อสารกันได้ แต่ถ้าเป็นแบบออนไลน์เมื่อระบบตรวจจับผู้บุกรุกเสียหาย เครือข่ายแลนและเครือข่ายอินเทอร์เน็ตจะไม่สามารถติดต่อสื่อสารกันได้

3.2 ลักษณะของโปรแกรมที่ทำการทดลอง

3.2.1 โปรแกรมที่ใช้ในการตรวจจับการบุกรุก

โปรแกรมที่นำมาใช้คือโปรแกรมสนอร์ต(Snort) ซึ่งเป็นระบบตรวจจับผู้บุกรุกแบบ โอเพน ซอร์ซ สามารถดาวน์โหลดโปรแกรมสนอร์ตเวอร์ชันล่าสุดได้จาก <http://www.snort.org/>

เหตุผลที่เลือกใช้โปรแกรมสนอร์ต เนื่องจากมีประสิทธิภาพในการตรวจจับผู้บุกรุกได้ดี เหมาะในการนำมาใช้ในการพัฒนาระบบ เป็นฟรีแวร์(Freeware) สามารถนำไปใช้หรือพัฒนาต่อโดยไม่เสียค่าใช้จ่ายใดๆ มีผู้ใช้เป็นจำนวนมากทำให้มีเอกสารอ้างอิงในการแก้ปัญหาเยอะ

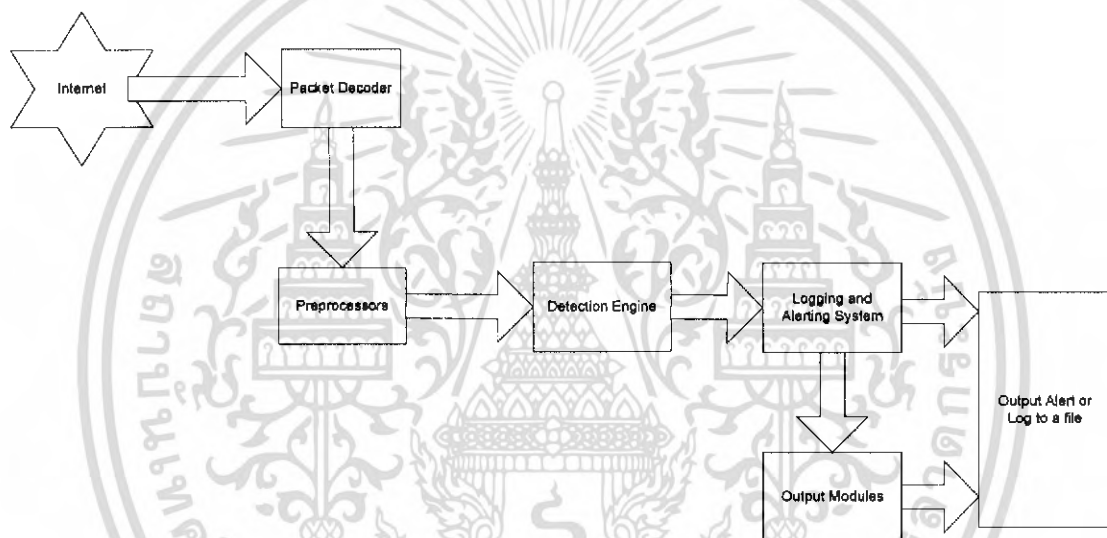
สนอร์ต มีการทำงานแบบเอ็นไอดีเอส (NIDS : Network Intrusion Detection System) คือจะเป็นการทำงานโดยตรวจสอบข้อมูลที่วิ่งอยู่ในเน็ตเวิร์ก แบบเรียลไทม์(Realtime) ว่าตรงกับรูปแบบของกฎ (Rule) ที่เก็บไว้ในฐานข้อมูลหรือไม่ ในการบุกรุกจะมีรูปแบบสัญญาณ (Signature) หลายประเภท ข้อมูลเกี่ยวกับรูปแบบเหล่านี้จะถูกใช้ในการสร้างกฎสนอร์ต (Snort Rules) เราใช้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปแบบการบุกรุก ตรวจสอบว่ามีใครพยายามหาประโยชน์จากจุดที่เป็นช่องโหว่ รูปแบบเหล่านี้อาจอยู่ในส่วนเฮดเดอร์(Header) ของแพ็กเก็ต หรือในเพย์โหลด (Payload) ระบบตรวจจับสแนร์ด จะมีพื้นฐานมาจากกฎ ซึ่งกฎเหล่านี้มาจากรูปแบบการบุกรุก กฎของสแนร์ด ตรวจสอบได้หลายส่วนของแพ็กเก็ตข้อมูล สแนร์ดสามารถวิเคราะห์เฮดเดอร์ของชั้นเลเยอร์ที่ 3 , 4 (แอปพลิเคชันเลเยอร์) ได้ กฎจะถูกประยุกต์ใช้ทันสมัยกับทุกแพ็กเก็ต กฎอาจใช้ในการสร้างข้อความเตือน (Alert Message) , บันทึกข้อความ (Log Message) หรือในรูปแบบของสแนร์ด การผ่าน Pass) ของแพ็กเก็ตข้อมูล

3.2.1.1 ส่วนประกอบของโปรแกรมสแนร์ด

ส่วนประกอบของสแนร์ดเป็นดังรูป



รูปที่ 3.3 ส่วนประกอบของสแนร์ด

1) ตัวถอดแพ็กเก็ต (Packet Decoder) เป็นส่วนที่ทำหน้าที่เกี่ยวกับการนำแพ็กเก็ตจากหลายๆ โปรโตคอลและเตรียมแพ็กเก็ต โดยตัดเอาแพ็กเก็ตส่วนที่ฟรีโพรเซสเซอร์รู้จักออกมาเพื่อทำการฟรีโพรเซส (Preprocess) หรือส่งไปยังดีเทคชันเอนจิน (Detection Engine)

2) ฟรีโพรเซสเซอร์ (Preprocessor) เป็นส่วนประกอบหรือปลั๊กอิน(Plug-In) ที่ใช้ในสแนร์ดเพื่อการจัดเรียงหรือเปลี่ยนแปลงแพ็กเก็ตข้อมูล ก่อนที่ ดีเทคชันเอนจิน จะทำการค้นหาแพ็กเก็ตที่เป็นการบุกรุกฟรีโพรเซสเซอร์บางตัว จะทำการตรวจสอบโดยการหาเฮดเดอร์ของแพ็กเก็ตที่ไม่ปกติและทำการเตือนขึ้นมา ฟรีโพรเซสเซอร์เป็นสิ่งที่ยิ่งสำคัญอย่างยิ่งสำหรับระบบตรวจจับผู้บุกรุก คือ เตรียมแพ็กเก็ตข้อมูลเพื่อการตรวจสอบกับกฎที่อยู่ในดีเทคชันเอนจิน ตัวอย่างเช่น แอส

เกอร์โจมตีในเซกที่พีแพ็กเก็ต (HTTP packet) วิธีแก้คือเราสร้างกฎที่ค้นหารูปแบบของคำว่า “scripts/iisadmin” (แพ็กเก็ตเพย์โหลด (Packet payload)) แต่ถ้าแฮกเกอร์ เปลี่ยนสตริงเช่น

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

ระบบตรวจจับผู้บุกรุกจะไม่สามารถตรวจจับได้เลยจึงต้องมีฟรี โพรเซสเซอร์ที่ช่วยในการ จัดเรียงสตริงเพื่อตรวจจับการบุกรุกประเภทนี้

3) ดีเทคชันแอนจิ้น เป็นส่วนที่ทำหน้าที่ในการใช้ กฎในการตรวจจับแพ็กเก็ต ถ้าแพ็กเก็ต เกิดเป็นการบุกรุก โดยกฎจะทำการอ่านโครงสร้างภายในของข้อมูล ถ้ามีแพ็กเก็ตที่ตรงกับกฎ จะมีการกระทำเกิดขึ้นโดยอาจจะเป็นการบันทึกแพ็กเก็ต (Log Packet) หรือ การเตือน (Alert) ถ้าไม่ใช้ การบุกรุกแพ็กเก็ตนั้น จะถูกพาส(Pass)ไป ในส่วนของดีเทคชันแอนจิ้น ระยะเวลาที่ใช้ในการ ตรวจจับจะขึ้นอยู่กับ

- ประสิทธิภาพของเครื่องคอมพิวเตอร์ที่ใช้โปรแกรมสนอร์ต
- จำนวนกฎที่กำหนด
- ความเร็วของอินเทอร์เน็ทบัส (Internal Bus) ของเครื่องคอมพิวเตอร์
- จำนวนการจราจร (Traffic) ที่อยู่บนเครือข่าย

4) ระบบการบันทึกและเตือน (Logging and Alerting System) อาจะบันทึกหรือ แจ้งเตือนก็ได้ โดยการบันทึก จะเก็บเป็นเท็กซ์ไฟล์ หรือฐานข้อมูล ก็ได้

5) เอาท์พุทโมดูล (Output Modules) ควบคุมประเภทของการสร้างเอาท์พุทโดยจะ เป็นการบันทึกหรือแจ้งเตือนคือ

- ไฟล์บันทึก (Log file)
- ส่งเอสเอ็นเอ็มพีแทร็ป (SNMP (Simple Network Management Protocol) Traps)
- ไฟล์บันทึก ไปยังฐานข้อมูล
- สร้างเอ็กซ์เอ็มแอล (XML Output)
- ปรับเปลี่ยนค่าของเราเตอร์ (Router) และไฟร์วอลล์ (Firewall)
- ส่งข้อความเอสเอ็มบี (SMB :Server Message Block) ไปยังเครื่องคอมพิวเตอร์ที่เป็น วินโดวส์

ชื่อ	คำอธิบาย
Packet Decoder	เตรียมแพ็กเก็ตสำหรับประมวลผล
Preprocessor or Input Plugins	ใช้ในการปรับเสดเดอร์ของโปรโตคอลให้อยู่ในสภาวะปกติ, ตรวจสอบแพ็กเก็ตที่ผิดปกติ, รวมแพ็กเก็ตและทีซีพีสตรีม(TCP Stream ขึ้นมาใหม่
Detection Engine	ตรวจสอบว่าตรงกับแพ็กเก็ตใด
Logging and Alerting System	สร้างอเลิร์ตและล็อกเมสเสจ
Output Modules	ประมวลผลอเลิร์ตและล็อกเพื่อสร้างเอาต์พุตสุดท้าย

ตารางที่ 3.1 ส่วนประกอบของสนอร์ต

3.2.1.2 สิ่งจำเป็นในการติดตั้งโปรแกรมสนอร์ต

- Libpcap library (<ftp://ftp.ee.lbl.gov/libpcap.tar.Z>)
- C Compiler ซึ่งปกติจะมีติดตั้งไว้ในทุก OS อยู่แล้ว หรืออาจจะพิจารณาใช้ GNU C (<ftp://ftp.gnu.org/gnu/gcc/>)
- Utility ที่ใช้สำหรับขยายไฟล์ เช่น GZIP (<ftp://ftp.gnu.org/gnu/gzip/>)
- MD5 Cryptographic Checksum Program เพื่อใช้เช็ควอร์ซโค้ด(Source code) ที่ได้มานั้นไม่ได้ถูกแก้ไขไปก่อนหน้านี้โดยผู้ไม่ประสงค์ดี

3.2.1.3 การติดตั้งโปรแกรม

ขยายไฟล์ที่ดาวน์โหลดมา

```
#tar xzf snort-x.x.x.tar.gz -C /usr/local
```

ย้ายไดเรกทอรีไปยังเป้าหมายที่ขยายไป จากนั้นใช้คำสั่ง

```
#!/configure (ใช้ ./configure --help เพื่อดู Option ทั้งหมด)
```

```
#make
```

```
#make install
```

โดยปกติสนอร์ตจะเก็บข้อมูลล็อกอยู่ในรูปของล็อกไฟล์คล้ายๆ กับ Syslog แต่เราสามารถสั่งให้สนอร์ตเก็บข้อมูลที่ต้องการไว้ใน Database เช่น MySQL, PostgreSQL หรือ MSSQL ได้ เพื่อให้สามารถดึงข้อมูลมาตรวจสอบได้สะดวกยิ่งขึ้นผ่านทางปลั๊กอิน เช่น ACID ทั้งนี้จะมีตัวอย่างการคอมไพล์(Compile) เพื่อให้ใช้งานกับ MySQL อีกครั้งในบทความฉบับต่อไป

Create Directory for Snort Log Files

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สร้างไดเรกทอรีเพื่อเก็บล็อกไฟล์ของสนอร์ดทั้งหมดแยกต่างหาก และควรป้องกันไม่ให้บุคคลอื่น Access เข้ามาที่ไดเรกทอรีนั้นๆ โดยปกติแล้วจะสร้างไว้ที่ /var/log/snort

```
#mkdir /var/log/snort
#chmod 700 /var/log/snort
```

ทดสอบโปรแกรม

ทดลองรันคำสั่ง snort -? เพื่อแสดง Hclp ของสนอร์ดทั้งหมด

สร้างไฟล์ Configuration และ Rules

จริงๆ แล้ว ขั้นตอนนี้จะไม่ถือว่าเป็นการสร้างเป็นเพียงการประกอบข้อมูลที่สนอร์ดให้เรามาแล้วนั้น นำมาจัดให้เป็นระเบียบเรียบร้อยเท่านั้นเอง ซึ่งอาจจะไม่จำเป็น ในที่นี้จะสร้างโฟลเดอร์ขึ้นมาที่ /etc/snort เพื่อใช้เก็บ Configuration และ Rules Files ของสนอร์ดไว้ต่างหาก

```
#mkdir /etc/snort
จากนั้นให้ก๊อปปี้ข้อมูล Configuration และ Rules Files จากซอร์ซของสนอร์ด
```

```
#cd /usr/local/src/snort
#cp snort.conf /etc/snort
#cp *.rules /etc/snort
#cp classification.config /etc/snort
```

แก้ไข /etc/snort/snort.conf

เราจะใช้ไฟล์ snort.conf เป็นไฟล์หลักในการรันสนอร์ดโดยจำเป็นต้องแก้ไขข้อมูลในบางส่วนดังต่อไปนี้ (vi snort.conf)

แก้ไข HOME_NET ให้เป็นเน็ตเวิร์ก แอดเดรส(Network Address) ของเครือข่ายที่ต้องการมอนิเตอร์(Monitor) เช่น var HOME_NET 10.10.10.0/24

แก้ไขค่า Network IP Address อื่นให้ตรงกับความต้องการ เช่น SMTP , SQL_SERVERS

ค่าที่ควรแก้ไขคือ VAR DNS_SERVERS แก้ให้เป็น DNS Server ที่ใช้ภายในหน่วยงาน เพื่อป้องกัน Fault Alarm

สำหรับพารามิเตอร์(Parameter) อื่นๆ นั้น ท่านสามารถหาข้อมูลเพิ่มเติมได้ที่ www.snort.org พร้อมกับคู่มือการเขียนกฎ (โดยปกติแล้ว ไม่มีความจำเป็นต้องเขียนกฎเอง เพียงแต่หมั่นติดตามข่าวกฎใหม่ๆ ที่ www.snort.org เท่านั้นเอง)

การรันสนอร์ด (Daemon)

ทดลองรัน `/usr/local/bin/snort -c /etc/snort/snort.conf` ถ้าไม่มีข้อผิดพลาด(Error) ใดๆ แสดงว่าสามารถใช้งานได้ เพียงแต่การใช้งานจริงนั้นจะรันใน Daemon Mode โดยจะใช้คำสั่งดังนี้

```
#/usr/local/bin/snort -D -c /etc/snort/snort.conf
```

ถ้าต้องการให้ snort รันใน Daemon Mode ทุกครั้งที่บูตเครื่องขึ้นมา ก็ให้แก้ไขไฟล์ `/etc/rc.local` แล้วใส่คำสั่งด้านบน เพื่อให้ snort ทำงานเมื่อมีการบูตเครื่องใหม่

3.2.2 โปรแกรมเพียร์ทูเพียร์ประยุกต์(Peer-to-Peer Application)

โปรแกรมเพียร์ทูเพียร์(เช่น BitTorrent , BitComet) ใช้สำหรับกระจาย หรือเผยแพร่ไฟล์ โดยเฉพาะไฟล์ใหญ่ๆ แบบเครื่องสู่เครื่องได้อย่างรวดเร็วมาก ซึ่งการกระทำเช่นนี้เป็นการเพิ่มความคับคั่งให้ระบบเครือข่ายส่วนรวม ซึ่งมีหลายโปรแกรมให้เลือกใช้ แต่เราจะใช้โปรแกรมบิตโคเม็ต 0.71 , อิมูลล์และแซลเพียร์ทูเพียร์

3.2.3 โปรแกรมที่ใช้ตรวจสอบรายละเอียดของแพ็กเก็ต

ส่วนนี้จะใช้โปรแกรมอีเทอเรียล (Ethereal) ซึ่งเป็นฟรีแวร์ที่มีประสิทธิภาพสูงใช้ตรวจจับทราฟฟิกแบบเรียลไทม์ โดยสามารถตรวจจับและถอดรหัสโปรโตคอลต่าง ๆ ได้มากมายถึง 400 โปรโตคอล เพื่อนำมาวิเคราะห์เครือข่ายหรือเน็ตเวิร์ก ทราฟฟิก (Network Traffic) นำแพ็กเก็ตที่ดักจับได้มาทำการถอดรหัส และแสดงผลข้อมูลออกมาในรูปแบบที่สามารถอ่านและเข้าใจได้ง่าย สามารถทำงานได้ทั้งบนวินโดวส์(Windows) หรือ ยูนิกซ์(Unix) รวมทั้งลินุกซ์(Linux)

3.3 การทำงานของโปรแกรม snort

3.3.1 กฎ(rules)

snort จะเขียนกฎในไวยากรณ์ (Syntax) ที่เข้าใจง่าย กฎส่วนใหญ่จะเขียนบรรทัดเดียว แต่เราก็สามารถเขียนได้หลายบรรทัดโดยใช้ `\` (backslash) กันเมื่อจบหนึ่งบรรทัด กฎปกติจะอยู่ในไฟล์คอนฟิกเกอร์เรชัน (Configuration File : `snort.conf`)

ตัวอย่างกฎ

```
alert ip any any -> any any ( msg : " IP Packet detected " ; )
```

- คำว่า " alert " แสดงให้เห็นว่ากฎนี้จะสร้างข้อความเตือน (Alert Message) เมื่อเจอแพ็กเก็ตเกิดแบบเดียวกับที่เราสร้างเงื่อนไขที่เป็นมาตรฐานไว้ ซึ่งเงื่อนไขที่เป็นมาตรฐานจะนิยามด้วยคำที่ตามมา

- ส่วน " ip " แสดงให้เห็นว่ากฎนี้ ใช้ได้กับทุกไอพีแพ็กเก็ต (IP Packets)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- " any " แรกถูกใช้สำหรับไอพีแอดเดรสต้นทาง (Source IP Address)
- " any " ตัวที่สองใช้สำหรับหมายเลขพอร์ต เพราะหมายเลขพอร์ต ไม่เกี่ยวกับไอพีแอดเดรส
- เครื่องหมาย -> แสดงทิศทางของแพ็กเก็ต
- " any " ตัวที่สามถูกใช้สำหรับไอพีแอดเดรสปลายทาง (Destination IP Address)
- " any " ตัวที่สี่ถูกใช้สำหรับพอร์ตปลายทาง (Destination Port)
- ส่วนสุดท้าย เป็นส่วนออปชันของกฎ (Rule Options) และบรรจุข้อความ ที่ไว้แจ้งเตือนตอนเกิดการแจ้งเตือน

3.3.2 โครงสร้างของกฎ

กฎสนอร์ต ทุกอันจะมี 2 ส่วนหลักคือ คือ เฮดเดอร์ของกฎ (Rule Header) และส่วนออปชันของกฎ (Rule Options) ดังรูป

Rule Header	Rule Option
-------------	-------------

รูปที่ 3.4 โครงสร้างพื้นฐานของกฎสนอร์ต

1) **เฮดเดอร์ของกฎ** บรรจุข้อมูลเกี่ยวกับการกระทำ (Action) ที่กฎจะได้รับ รวมถึงเงื่อนไขที่เป็นมาตรฐานสำหรับไว้จับคู่กันระหว่างกฎกับแพ็กเก็ตข้อมูล ส่วนออปชันของกฎ บรรจุข้อความแจ้งเตือนและข้อมูลที่เกี่ยวข้องกับส่วนแพ็กเก็ต ที่จะถูกใช้ในการสร้างข้อความแจ้งเตือน และยังเพิ่มเงื่อนไขที่เป็นมาตรฐานสำหรับไว้จับคู่กันระหว่างกฎกับแพ็กเก็ตข้อมูล กฎหนึ่งสามารถตรวจพบการบุกรุกได้ตั้งแต่หนึ่งถึงหลายประเภท กฎที่ฉลาดจะประยุกต์ใช้ได้กับหลาย รูปแบบการบุกรุกโครงสร้างทั่วไปของเฮดเดอร์ของกฎสนอร์ต เป็นดังนี้

Action	Protocol	Address	Port	Direction	Address	Port
--------	----------	---------	------	-----------	---------	------

รูปที่ 3.5 โครงสร้างของเฮดเดอร์ของกฎสนอร์ต

ส่วนแอ็คชัน จะพิจารณาว่าทำการกระทำแบบไหน เมื่อตรงกับเงื่อนไขที่เป็นมาตรฐาน และ กฎตรงกับแพ็กเก็ตข้อมูล โดยปกติการกระทำจะสร้างการแจ้งเตือนหรือบันทึกข้อความหรือเรียกกฎอื่น

ส่วนโปรโตคอล กฎหรือแพ็กเก็ตจะประยุกต์ใช้กับสำหรับ โปรโตคอลนั้นๆ โปรโตคอลที่ใช้เช่น ไอพี , ไอซีเอ็มพี , ยูดีพี ฯลฯ

ส่วนแอดเดรส จะกำหนดแอดเดรสต้นทางและปลายทาง แอดเดรสต้นทางและปลายทางจะพิจารณาจากไดเรกชันฟิลด์ (Direction Field) ตัวอย่างเช่น ถ้าไดเรกชันฟิลด์ เป็น -> ตำแหน่งด้านซ้ายจะเป็นต้นทางส่วนด้านขวาเป็นปลายทาง

ส่วนพอร์ต ในกรณีของทีซีพีหรือยูดีพี พอร์ตจะใช้ในการพิจารณาต้นทางและปลายทาง ส่วนในกรณีของไอพีและไอซีเอ็มพี หมายเลขพอร์ตไม่มีความสำคัญ

ส่วนทิศทาง (Direction) ใช้พิจารณาแอดเดรสและพอร์ตว่า อันไหนเป็นต้นทางอันไหนเป็นปลายทาง

ตัวอย่าง พิจารณากฎ ที่จะสร้างข้อความแจ้งเตือนเมื่อพบไอซีเอ็มพีปิงแพ็กเก็ต (ICMP Ping Packet) ด้วย ทีทีแอล (TTL)= 100

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

- แอคชัน ในกฎนี้แอคชันคือการแจ้งเตือนเมื่อมีการตรวจพบการบุกรุก

- โพรโตคอล ในกฎนี้โพรโตคอลคือไอซีเอ็มพี หมายความว่ากฎนี้ใช้ได้แค่แพ็กเก็ตประเภทไอซีเอ็มพี

- แอดเดรสและพอร์ตต้นทาง ในตัวอย่างนี้ใช้ได้กับทุกไอซีเอ็มพีแพ็กเก็ต ส่วนหมายเลขพอร์ตไม่เกี่ยวกับไอซีเอ็มพีแพ็กเก็ต

- ทิศทาง ใช้สัญลักษณ์ ->

- แอดเดรสและพอร์ตปลายทาง ในตัวอย่างนี้ใช้ได้กับทุกไอซีเอ็มพีแพ็กเก็ต

ส่วนออพชัน จะอยู่ในวงเล็บ () ซึ่งจะแสดงให้เห็นว่าข้อความแจ้งเตือนที่จะสร้างที่ชัดเจน " Ping with TTL=100 " เมื่อเกิดทีทีแอล (TTL:Time To Live) = 100

เฮดเดอร์ของกฎจะประกอบไปด้วย

1.1) แอคชันของกฎ (Rule Action) ทำแอคชันเมื่อกฎเป็นจริง ประกอบด้วย 5 แอคชัน

1.1.1) การผ่าน (Pass)

ทำการเพิกเฉยต่อแพ็กเก็ต ใช้ในกรณีที่ต้องการหาช่องโหว่ในระบบ เพราะมันจะทำได้รวดเร็วกว่าแอคชันอื่น

1.1.2) การบันทึก (Log)

ทำการบันทึกแพ็กเก็ต เช่นข้อความจะถูกบันทึกให้เป็นไฟล์หรือเก็บในฐานข้อมูลก็ได้ สามารถเก็บ รายละเอียด ได้หลายระดับตามที่กำหนดไว้ในคอมมานด์ไลน์อาร์กิวเมนต์ (Command Line Argument) และไฟล์คอนฟิกเกอร์เรชัน (Configuration File)

1.1.3) การแจ้งเตือน (Alert)

ใช้สำหรับส่งข้อความแจ้งเตือนเมื่อกฎเป็นจริง การส่งส่งได้หลายวิธี เช่น เตือนผ่านทางไฟล์หรือเตือนผ่านทางคอนโซล ข้อแตกต่างระหว่างการบันทึกกับการแจ้งเตือนคือ การแจ้งเตือนจะมีข้อความขึ้นมาและบันทึกแพ็กเก็ต ส่วนการบันทึกจะทำแค่การบันทึกแพ็กเก็ต

1.1.4) พลวัต (Dynamic)

ถูกเรียกใช้เมื่อถูกอื่นใช้ “activate” action” ตามปกติมันจะไม่ทำงาน มันจะทำงานก็ต่อเมื่อ แอคทีเวทแอ็คชัน (activate action) เรียกใช้เท่านั้น

1.1.5) ยูสเซอร์ดีไฟน์แอ็คชัน (User Defined Actions)

สามารถกำหนดแอ็คชันได้เอง เช่น

- ส่งข้อความไปยังซิสล็อก(Syslog) ซิสล็อกคือตัวบันทึกของระบบที่เป็นเดมอนโพรเซส(Daemon Process) และสร้างไฟล์บันทึกที่ / var / log syslog เปรียบได้กับตัวบันทึกเหตุการณ์ของวินโดวส์

- ส่งเอสเอ็นเอ็มพีแทร็ป (SNMP Traps) เอสเอ็นเอ็มพีแทร็ปจะถูกส่งไปยังระบบจัดการเครือข่าย

- ทำงานหลายๆแอ็คชัน บน 1 แพ็กเก็ตเช่น ส่งเอสเอ็นเอ็มพีแทร็ปและ ข้อมูลบันทึกการแจ้งเตือน(Log Alert Data) ไว้ที่ซิสล็อก

- ข้อมูลการบันทึก (Log Data) ให้เป็นเอ็กซ์เอ็มแอลไฟล์ (XML Files)

สนอร์คสามารถบันทึกข้อความเก็บไว้ในฐานข้อมูลของมายเอสคิวแอล(MySQL), โพสต์เกรสคิวแอล(PostgreSQL) , ออราเคิล(Oracle) และ ไมโครซอฟต์เอสคิวแอลเซิร์ฟเวอร์ (Microsoft SQL Server)

แอ็คชันจะถูกกำหนดไว้ในไฟล์คอนฟิกเกอร์ชัน (snort.conf) การกำหนดแอ็คชันทำได้ดังนี้

```
rule type action_name
{
  action definition
}
ตัวอย่างของกฎ
rule type smb_db_alert
{
  type alert
  output alert_smb : workstation.list
  output database : log ,mysql,user = rr password=rr \
  dbname = snort hshot = localhost
}
```

1.2) โพรโตคอล ส่วนนี้จะแสดงให้เห็นว่ากฎจะจับแพ็กเก็ตบนโปรโตคอลไหน

1.3) แอดเดรส แบ่งเป็น 2 ส่วน คือส่วนแรกเป็นแอดเดรสต้นทาง ส่วนหลังเป็นแอดเดรสปลายทาง จะเป็นไอพีแอดเดรสหรือเน็ตเวิร์กแอดเดรสก็ได้ คำสำคัญ “any ” คือ ทุกๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

แอดเดรส ตัวอย่างเช่น ถ้าต้องการสร้างการแจ้งเตือนสำหรับทุกๆ ทีซีพีแพ็กเก็ตที่มีค่าทีทีแอล (TTL:Time To Live) = 100 ที่วิ่งไปยังเว็บเซิร์ฟเวอร์ 192.168.1.10 ที่ พอร์ต 80 จากต้นทางใดๆ เขียนกฎได้ดังนี้

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

1.3.1) แอดเดรสที่ถูกยกเว้น (Address Exclusion)

ใช้สำหรับแอดเดรสที่ถูกยกเว้น ตัวอย่างเช่น จับทุกแพ็กเก็ตที่มาจาก 192.168.2.0

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

ประโยชน์คือใช้ในการทดสอบแพ็กเก็ตที่ไม่ได้มาจากโฮมเน็ตเวิร์ก (Home Network)

1.3.2) รายชื่อแอดเดรส (Address List)

ใส่แอดเดรสเป็นรายชื่อ ตัวอย่างเช่น โฮมเน็ตเวิร์กประกอบด้วยไอพี 192.168.2.0 , 192.168.8.0 เพิ่มในกฎที่แล้ว ทำได้ดังนี้

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

: ใช่มั้ย !

1.4) หมายเลขพอร์ต (Port Number) ใช้ในการจับแพ็กเก็ต ว่ามาจากพอร์ตไหน และจะไปยังพอร์ตหรือช่วงของพอร์ตอะไร เช่นใช้พอร์ตต้นทาง หมายเลข 23 ไว้ตรวจจับแพ็กเก็ตที่มาจากเทลเน็ตเซิร์ฟเวอร์

2) ส่วนออปชันของกฎ (Rules Option)

ทางเลือก (Option) ของกฎ จะอยู่ต่อจากเฮดเดอร์ของกฎและอยู่ในวงเล็บ ซึ่งจะมีทางเลือกเดียวหรือหลายทางเลือกก็ได้ โดยแต่ละทางเลือกจะถูกกั้นด้วยเซมิโคลอน (;) ถ้าคุณเลือกให้หลายทางเลือกมันจะเหมือนกับการแอนด์ (And) ทางลोजิก การกระทำของเฮดเดอร์ของกฎ จะเกิด ขึ้นเมื่อทางเลือกทุกๆทางเป็นจริงขึ้นมา ทุกๆทางเลือกจะถูกประกาศโดยใช้คำสำคัญหรือ บางตัวก็บรรจุกิวเมนต์(Argument) อยู่ข้างใน โดยทั่วไปแล้ว ทางเลือกนั้นอาจจะมี 2 ส่วนคือ ส่วนคำสำคัญ (Keyword) และส่วนอากิวเมนต์ (Argument) อากิวเมนต์จะถูกแยกจากคำสำคัญโดย โคลอน (:) เช่นmsg : " Detected confidential " ;

2.1) คำสำคัญ "ack"

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เฮดเดอร์ของทีซีพีจะบรรจุด้วย แถวของตัวเลขที่บอกถึงสิ่งต่างๆ ด้วยความยาวขนาด 32 บิต แถวของตัวเลขนั้นจะแสดงถึงกระบวนการการรับแพ็กเก็ตต่อไปจากผู้ส่ง แถวตัวเลขนี้จะปรากฏที่ต่อเมื่อแฟลกแอค (ACK Flag) ในทีซีพีเฮดเดอร์ที่ได้ถูกกำหนดไว้

2.2) คำสำคัญ “classtype”

กฎที่สามารถที่จะถูกแบ่งได้ตามชนิด และ ความสำคัญ โดยดูรายละเอียดได้จากไฟล์ Classification.conf ซึ่งแต่ละบรรทัดจะบรรจุไวยากรณ์ไว้ คือ ชื่อ คำอธิบาย และเลขลำดับความสำคัญ (Priority)

2.3) คำสำคัญ “content”

คุณลักษณะสำคัญของสเนอร์ตซ์หนึ่งคือสามารถค้นหาข้อมูลในแพ็กเก็ตได้ โดยข้อมูลนั้นอาจอยู่ในรูปของ แอสกี (ASCII) หรือตัวอักษร เช่น ไรต์ส, ผู้บุกรุก ซึ่งได้มีคำสำคัญ “content” และสัญลักษณ์ ในการค้นหาพวกมันในแพ็กเก็ตอยู่แล้ว

2.4) คำสำคัญ “offset”

ใช้ร่วมกับคำสำคัญ “content” สามารถที่จะเริ่มต้นหาได้ตั้งแต่ส่วนที่เป็นข้อมูลจุดเริ่มต้นของแพ็กเก็ตจะมีการใช้ตัวเลข และอักขระในคำสำคัญนี้

2.5) คำสำคัญ “depth”

ใช้ร่วมกับคำสำคัญ “content” เช่นเดียวกัน เพื่อที่จะใช้กำหนดขอบเขตมากที่สุดของการจับคู่ สามารถที่จะระบุทิศทางจากจุดเริ่มของแพ็กเก็ตได้ ข้อมูลหลังจากทิศทางที่ระบุไว้จะไม่ถูกตรวจหาข้อมูลในแพ็กเก็ตถ้าใช้ทิศทาง 2 ทางร่วมกันก็จะสามารถบอกถึงขนาดความยาวของแพ็กเก็ตได้

2.6) คำสำคัญ “content-list”

ใช้กับชื่อของไฟล์ซึ่งเหมือนเป็นอักขระของคำสำคัญแบบนี้ เท็กซ์ไฟล์ตัวนี้จะบรรจุตัวอักษรซึ่งจะใช้ในการค้นหาภายในแพ็กเก็ต แต่ละอักขระจะแบ่งเป็นบรรทัด

2.7) คำสำคัญ “dsize”

จะถูกใช้เพื่อหาความยาวของส่วนที่เป็นข้อมูลในแพ็กเก็ต การโจมตีหลายๆครั้งจะใช้วิธีบัพเฟอร์โอเวอร์โฟลว์ที่จะทำการส่งแพ็กเก็ตข้อมูลจำนวนมากเข้ามา ด้วยการใช้คำสำคัญนี้ทำให้เราสามารถระบุได้ว่าแพ็กเก็ตที่เข้ามามีขนาดเท่าไรและตรงกับการโจมตีแบบใดหรือเปล่า

2.8) คำสำคัญ “flags”

ใช้ตรวจสอบว่าแฟลกใดในทีซีพีเฮดเดอร์ที่ส่งมาถูกเซตไว้บ้าง แต่ละแฟลกสามารถใช้เป็นอักขระสำหรับ กฎของสเนอร์ตซ์ได้

2.9) คำสำคัญ “flagbits”

ในทีซีพีเฮคเตอร์นั้นบรรจุด้วย 3 แฟล็กบิต ซึ่งใช้สำหรับการแบ่งส่วนของข้อมูล และการทำรีแอสเซมบลี (Reassembly) บางบิตจะถูกใช้โดย แสคเกอร์เพื่อที่จะบุงกรุกและ ใช้ ตรวจสอบข้อมูลบนเครือข่ายนั้น

2.10) คำสำคัญ “icmp_id”

ใช้ตรวจจับเลขไอดีเจาะจงที่ใช้ร่วมกับไอซีเอ็มพีแพ็กเก็ต จะมีประโยชน์มากเมื่อ ค้นหาว่าแพ็กเก็ตใดถูกตอบกลับในการร้องแบบเจาะจง

2.11) คำสำคัญ “icmp_seq”

ใช้ในการช่วยหาจำนวนตัวเลขที่เจาะจง เพื่อที่จะเอาไปเทียบกับกฎว่าตรงกับกฎ ไหนหรือไม่

2.12) คำสำคัญ “itype”

ไอซีเอ็มพีเฮคเตอร์เข้ามาหลังจากไอพีเฮคเตอร์ และบรรจุด้วยแถวของ ชนิดของ ไอซีเอ็มพีนั้นๆ ซึ่งคำสำคัญ นี้จะใช้ตรวจจับการบุงกรุกซึ่งใช้ แถวของชนิด ในไอซีเอ็มพีเฮคเตอร์

2.13) คำสำคัญ “icode”

ไอซีเอ็มพีเฮคเตอร์เข้ามาหลังจากไอพีเฮคเตอร์และบรรจุด้วยแถวของรหัส(Code) ซึ่งคำสำคัญตัวนี้จะใช้ตรวจสอบตัวรหัสที่บรรจุใน ไอซีเอ็มพีเฮคเตอร์

2.14) คำสำคัญ “id”

ใช้สำหรับจับคู่ส่วนของไอดีของไอพีแพ็กเก็ตเฮคเตอร์เพื่อตรวจจับการบุงกรุกที่ทำการคงค่า(Fix) เลขไอดีเอาไว้ ถ้าไอดีเป็น 0 ก็จะหมายถึงตำแหน่งสุดท้ายของไอพีแพ็กเก็ต

2.15) คำสำคัญ “ipopts”

โดยปกติไอพีวี4 (IPv4) จะมีความยาวของเฮคเตอร์เท่ากับ 20 ไบต์แต่อาจจะยาวได้ถึง 40 ไบต์ ไอพีออปชันใช้โดยมีหลายจุดประสงค์ เช่น บันทึกเส้นทาง บันทึกเวลา หรือใช้หาเส้นทาง แสคเกอร์สามารถใช้ส่วนนี้หาข้อมูลจากเครือข่ายที่ใช้ได้

2.16) คำสำคัญ “ip_proto”

ใช้ปลั๊กอินของไอพีโปรโต เพื่อที่จำจำนวนเลขโปรโตคอลที่อยู่ในไอพีเฮคเตอร์ คำสำคัญนี้ต้องใช้เลขโปรโตคอลเป็นอาร์กิวเมนต์หรือสามารถใช้ชื่อของโปรโตคอลก็ได้

2.17) คำสำคัญ “logto”

ใช้เพื่อเก็บแพ็กเก็ตไปยังไฟล์พิเศษ อย่างสิมระบุพาร(Path) ของไฟล์ที่จะเก็บด้วย

2.18) คำสำคัญ “msg”

ใช้เพื่อใส่ตัวอักษรหรือข้อความลงไปนีส็อก(Logs) และการแจ้งเตือน โดยใส่ข้อความลงไปนีส็อก

2.19) คำสำคัญ “nocase”

ใช้ร่วมกับคำสำคัญ “content” โดยตัวมันเองไม่มีอาทิวเมนต์ จุดประสงค์หลักคือ ต้องการค้นหาข้อมูลที่อยู่ในรูปแบบอินเซนซิทีฟ (Insensitive) ในแพ็กเก็ต

2.20) คำสำคัญ “priority”

ใช้ใส่ค่าความสำคัญลงไปในกลุ่ม โดยที่ค่าความสำคัญเท่ากับ 1 จะเป็นค่าที่ทำให้กฎนั้นมีความสำคัญสูงสุด ใช้ในการแยกการแข่งขันแบบต่างๆออกจากกัน

2.21) คำสำคัญ “react”

ใช้ในการทำลายเซสชัน (Session) ปิดกั้นบางเว็บไซต์ หรือบางเซอร์วิส (Service) โดยจะใส่ไว้ส่วนท้ายสุดของกฎ

2.22) คำสำคัญ “reference”

ใช้ในการเพิ่มคำอธิบายลงไปในกลุ่ม

2.23) คำสำคัญ “resp”

เป็นคำสำคัญที่สำคัญมาก มันสามารถจัดการกับกิจกรรมที่มาจากแฮกเกอร์โดยส่งแพ็กเก็ต ไปยังโฮสต์ที่ส่งแพ็กเก็ตมาตรงกับกฎที่กำหนดไว้

2.24) คำสำคัญ “rev”

ใช้เพื่อที่จะแสดงจำนวนรีวิชัน (revision) สำหรับกฎ ถ้าคุณปรับปรุงกฎ คุณสามารถใช้คำสำคัญนี้ในการแสดงจำนวนกฎที่เปลี่ยนไปได้

2.25) คำสำคัญ “rpc”

ใช้ตรวจจับการร้องขออาร์พีซี (RPC) โดยใช้ 3 อาทิวเมนต์คือเลขของแอปพลิเคชัน เลขโปรซีเยอร์ และเลข เวอร์ชัน

2.26) คำสำคัญ “sameip”

ใช้เพื่อเช็ค ไอพีของจุดกำเนิดกับ ไอพีปลายทางตรงกันหรือเปล่า เนื่องจากมีการทำการปลอมแปลงไอพีได้

2.27) คำสำคัญ “seq”

ใช้ทดสอบลำดับตัวเลขของทีซีพีแพ็กเก็ต ซึ่งอาทิวเมนต์ของตัวมันคือ เลขลำดับ

2.28) คำสำคัญ “flow”

ใช้เพื่อคำนวณทิศทางของแพ็กเก็ต

2.29) คำสำคัญ “session”

ใช้ในการแสดงแพ็กเก็ตทั้งหมดที่มาจากทีซีพีเซสชันหรือเฉพาะแค่บางตัวก็ได้ ถ้าใช้ “all” จะเป็นการแสดงทั้งหมด

2.30) คำสำคัญ “sid”

ใช้ในการใส่ไอดีของสนอร์ตลงไปยังกฎ เพื่อที่จะให้ส่วนแสดงผลหรือส่วนเก็บข้อมูลเรียกใช้กฎได้ถูก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.31) คำสำคัญ “tag

เป็นคำสำคัญที่สำคัญอีกตัวหนึ่ง ซึ่งจะใช้เป็นเก็บข้อมูลที่เข้าหรือออกจากโฮสต์ของผู้บุกรุก เมื่อถูกได้ถูกดำเนินการ เพื่อใช้ในการวิเคราะห์พฤติกรรมของผู้บุกรุกในภายหลัง

2.32) คำสำคัญ “tos”

ใช้ตรวจสอบค่าที่เจาะจงของรูปแบบการให้บริการ ในไอพีเซคเตอร์

2.33) คำสำคัญ “ttl”

ใช้ตรวจสอบค่าเวลาที่ยังอยู่ (Time To Live) ในไอพีเซคเตอร์ของแพ็กเก็ต ตัวค่าสำคัญควรจะต้องมีค่าเท่ากับค่าที่ประมาณไว้พอดี สามารถใช้ได้กับทุกๆ โพรโตคอลใช้ในการตรวจสอบว่ามีคนพยายามจะทำการ ติดตามเส้นทาง (Traceroute) มายังเครือข่ายของเราหรือไม่

2.34) คำสำคัญ “uricontent”

เหมือนกับคำสำคัญ “content” จะแตกต่างตรงที่มันจะคอยตรวจสอบความผิดปกติที่ส่วนยูอาร์ไอ (URI) ในแพ็กเก็ตเท่านั้น

3.3.3 วิธีปรับแต่งโปรแกรมสนอร์ต

- แก้ไฟล์ snort.conf ที่ตัวแปร RULE_PATH ให้ตรงกับ path ที่เก็บกฎ(rules)ไว้ดังนี้

```
var RULE_PATH /rules
```

 หรือถ้าใช้กับระบบปฏิบัติการวินโดวส์ให้เซตเป็นลักษณะดังนี้

```
var RULE_PATH c:\snort\rules
```
- เมื่อกำหนดพารามิเตอร์ของกฎเรียบร้อยแล้วให้ทำการเรียกใช้กฎนั้นโดยพิมพ์คำสั่ง

```
Include something.rules
```

 เช่น

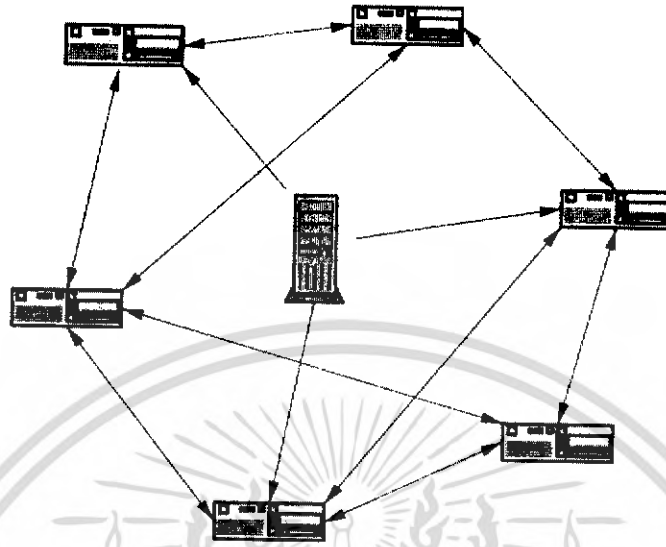
```
include $RULE_PATH/p2p.rules
```


 หรือถ้าในไฟล์ snort.conf มีคำสั่งอยู่แล้ว ให้เอาเครื่องหมาย “#” ออก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.4 การทำงานและพฤติกรรมของการสื่อสารแบบเพียร์ทูเพียร์

3.4.1 องค์ประกอบของเพียร์ทูเพียร์



รูปที่ 3.6 ภาพแสดงองค์ประกอบของเพียร์ทูเพียร์

ไคลเอนต์ คือโปรแกรมที่จะนำมาใช้ในการใช้งานการสื่อสารแบบเพียร์ทูเพียร์ ซึ่งมีอยู่หลายตัว เช่น Bitcomet , BitTomado , Azureus , TorrentStorm โปรแกรมเหล่านี้จะใช้ในการดาวน์โหลดไฟล์และอัปโหลดไฟล์

แทร็กเกอร์ เซิร์ฟเวอร์(Tracker server) คือเซิร์ฟเวอร์ที่ทำหน้าที่เป็นแม่ข่ายกลางระหว่างไคลเอนต์

ทอร์เรนต์ ไฟล์(Torrent file) เป็นไฟล์ที่เก็บข้อมูลเพื่อใช้ในการดาวน์โหลด ซึ่งประกอบไปด้วย แอดเดรสของแทร็กเกอร์ , Check sum เพื่อเอาไว้ใช้ในการตรวจสอบความถูกต้องของไฟล์

3.4.2 การทำงานของเพียร์ทูเพียร์

มีกระบวนการทำงานทั้งหมด ดังต่อไปนี้

- 1) ค้นหาไฟล์ .torrent มาจากเว็บไซต์ แล้วนำมาเปิดด้วยโปรแกรมที่ใช้ในการสื่อสารแบบเพียร์ทูเพียร์(บิต โคมิต , อิมูลท์ และแซคพิททูพี เป็นต้น)
- 2) โปรแกรมจะอ่านค่าแอดเดรสของแทร็กเกอร์ เซิร์ฟเวอร์ในไฟล์ที่เปิด แล้วทำการติดต่อไปหาแทร็กเกอร์เพื่อทำการส่งข้อมูลเกี่ยวกับไฟล์ .torrent
- 3) แทร็กเกอร์ เซิร์ฟเวอร์จะตรวจสอบว่าไฟล์ที่ขอมามีการลงทะเบียนไว้ในระบบหรือไม่ ถ้ามีจะตรวจสอบว่ามีไอพีแอดเดรสอะไรบ้างที่มีการอัปโหลดและดาวน์โหลดไฟล์นี้อยู่

4) ส่งรายการไอพีแอดเรสของคนที่มีการติดต่ออยู่กลับไป และทำการเก็บไอพีแอดเรสของเราไว้ด้วย (เก็บไว้ส่งให้คนอื่น)

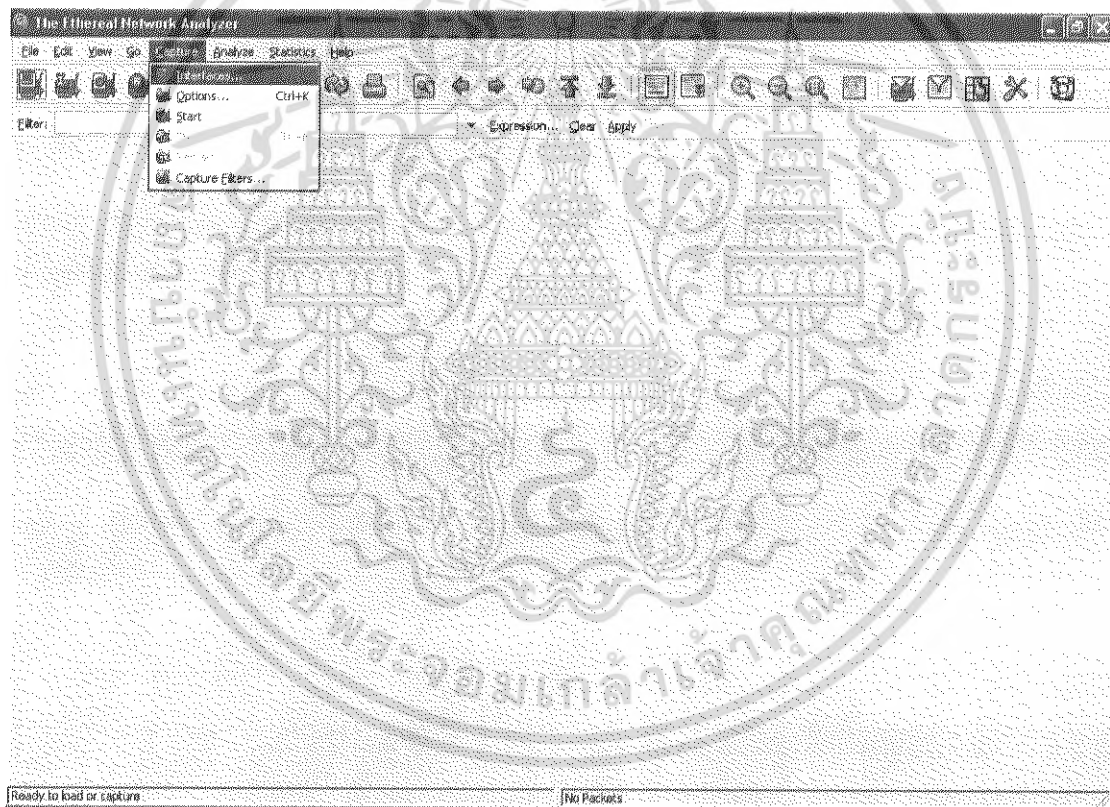
5) เมื่อทอร์เรนต์ไคลเอนต์(Torrent client) ได้ไอพีแอดเรสแล้ว มันก็จะทำการติดต่อไปยังไอพีแอดเรสที่ได้มาโดยจะส่งคำร้องขอไปสอบถามว่าแต่ละ ไอพีแอดเรสนั้นมีส่วนไหนของไฟล์ที่ต้องการนี้อยู่บ้าง

6) แล้วปลายทางก็จะบอกว่าส่วนไหนของไฟล์ที่ปลายทางมีอยู่ แล้วส่งไปบอกต้นทาง

7) ต้นทางก็จะทำการตรวจว่ามีส่วนไหนของไฟล์ที่ยังขาดอยู่บ้าง แล้วส่งคำขอเฉพาะส่วนที่ต้องการ แล้วปลายทางก็จะส่งส่วนของไฟล์ที่ต้องการนั้นมาให้

3.5 การทำงานของโปรแกรมอีเทอร์เรียด

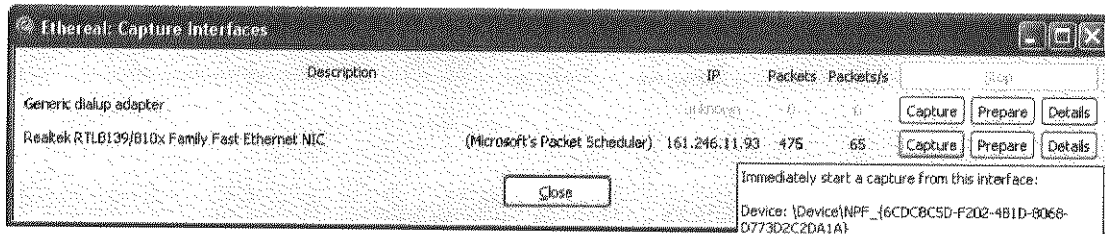
มีการทำงานดังนี้



รูปที่ 3.7 แสดงหน้าจอหลักของโปรแกรมอีเทอร์เรียด

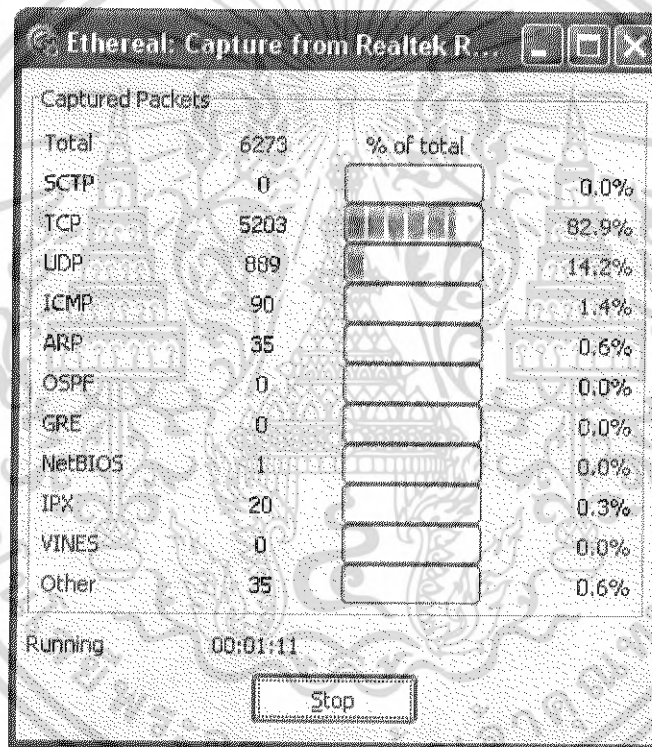
ให้เปิดไปที่เมนู Capture -> Interface จากนั้นจะปรากฏหน้าจอดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 3.8 แสดงหน้าจอตอนเลือก Network Card ที่จะจับแพ็กเก็ตที่ Network Card ได้

ซึ่งจะแสดงถึง Network Card ที่มีอยู่ แล้วให้คลิกไปที่ปุ่ม Capture ของ Network Card ที่เราต้องการใช้ในการตรวจจับ Packet แล้วจะมีหน้าจอแสดงถึง Packet ต่าง ๆ ที่ผ่านเข้าออกผ่าน Network Card นี้



รูปที่ 3.9 หน้าจอแสดงผลการเปรียบเทียบจำนวนแพ็กเก็ตที่จับได้ในแต่ละโปรโตคอล

Packet ต่าง ๆ ที่ผ่านเข้าออกจะแสดงออกมาเป็นประเภท ๆ จากนั้นให้คลิก Stop แล้วจะมีหน้าจอแสดงรายละเอียดต่าง ๆ ของแต่ละ Packet ที่ผ่าน

The screenshot shows a Wireshark interface with a list of network packets. The selected packet (No. 6091) is a BitTorrent handshake. The details pane shows the protocol name as 'BitTorrent protocol' and the reserved extension bytes as '6578000000000000'. The hex data pane shows the raw bytes of the packet, with ASCII characters visible on the right side, including '/Z.Y..E.', '.|.|.@... ..]', and 'R.3...-B C0084-(

รูปที่ 3.10 หน้าจอแสดงรายละเอียดของแพ็กเก็ตต่างๆที่จับได้

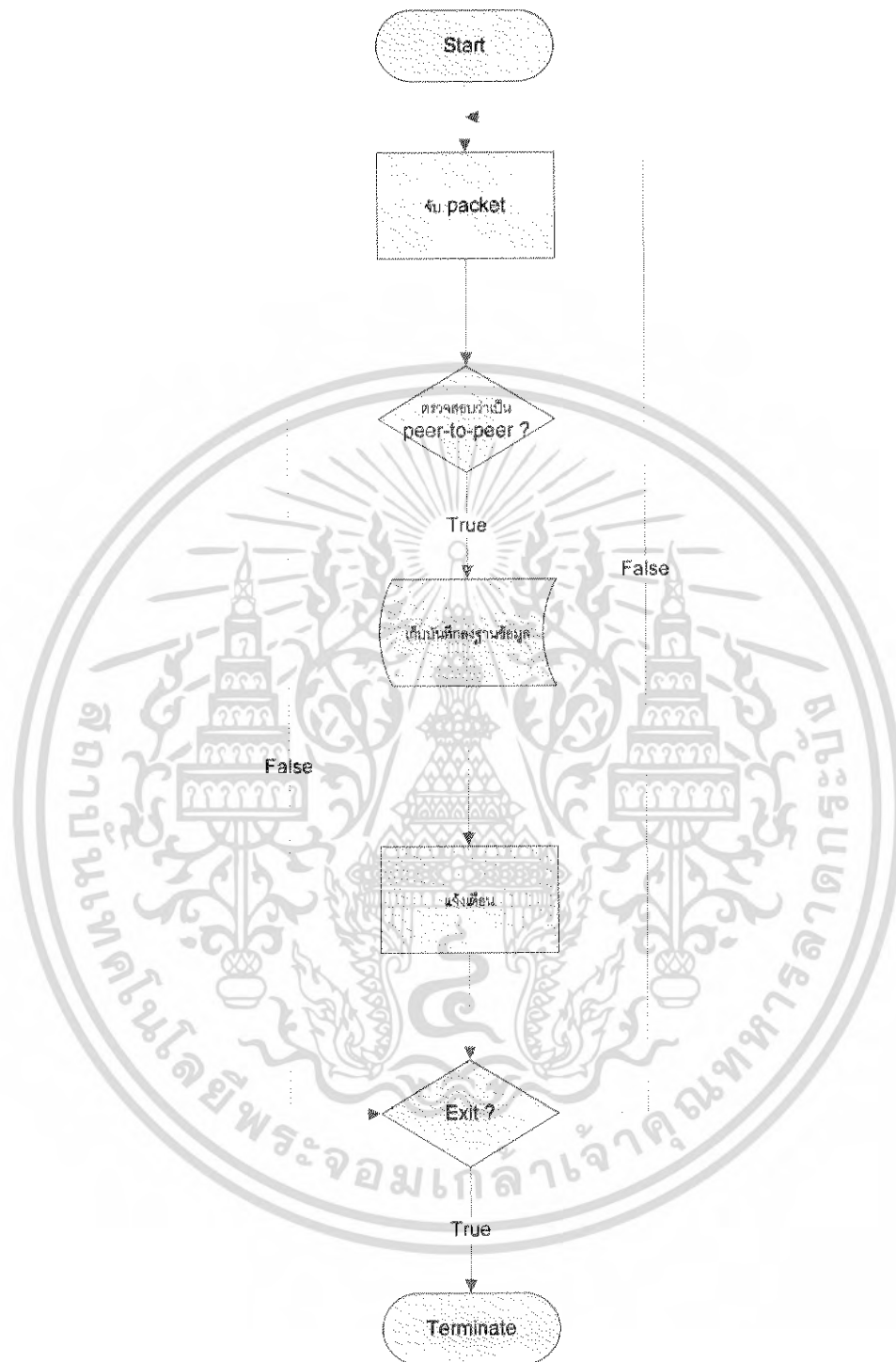
ซึ่งด้านบนจะแสดงถึง Packet ต่างๆที่โปรแกรมจับได้ พร้อมทั้งแสดงไอพีแอดเดรสของผู้ส่งและผู้รับ และแสดง Protocol ที่ Packet นั้นใช้ เมื่อคลิกไปที่ Packet จะมีข้อมูลด้านล่างซึ่งก็คือรายละเอียดของ Packet

This image shows a close-up of the hex data view from the previous screenshot. It displays hexadecimal values in columns, with corresponding ASCII characters on the right. The ASCII characters include '/Z.Y..E.', '.|.|.@... ..]', 'R.3...-B C0084-(', and 'A#'. The hex values are: 0000 00 d0 95 9f 17 14 00 11 2f 5a db 59 08 00 45 00, 0010 00 6c 7c d9 40 00 80 06 f7 d1 a1 f6 0b 5d 3a b6, 0020 9d d7 05 2c c0 03 40 9f 6d 90 23 d7 32 ba 50 18, 0030 44 70 ce 22 00 00 13 42 69 74 59 6f 72 72 65 6e, 0040 74 20 70 72 6f 74 6f 63 6f 6c 65 78 00 00 00 00, 0050 00 00 da 0f 24 24 a2 08 0f 4c 58 95 de ab d9 8b, 0060 52 19 33 b1 95 f3 2d 42 43 30 30 38 34 2d fc 28, 0070 7d 1e ca ca af 7e 09 2e 5e 23.

รูปที่ 3.11 แสดงรายละเอียดของแพ็กเก็ต

ใน Packet ที่มีการใช้งาน BitTorrent Protocol จะมี Header ใน Packet ต่าง ๆ ที่มีลักษณะเหมือนกันคือ จะมีคำว่า "BitTorrent protocol" เป็นต้น

3.6 การทำงานของระบบ



รูปที่ 3.12 Flow chart การทำงานของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เริ่มแรกจะทำการตรวจจับและตรวจสอบแพ็คเกจที่วิ่งเข้ามาในระบบว่าตรงกับกฎที่กำหนดไว้หรือไม่ซึ่งก็คือเป็นแพ็คเกจข้อมูลที่เป็นการสื่อสารแบบเพียร์ทูเพียร์หรือไม่ ถ้าใช่ก็จะทำการบันทึกข้อมูลของแพ็คเกจนั้นลงในฐานข้อมูลและแจ้งเตือนบนหน้าจอ ถ้าไม่ใช่ก็จะตรวจจับและตรวจสอบแพ็คเกจข้อมูลต่อไป



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

ผลการดำเนินงานวิจัยวิจัย

4.1 เครื่องมือที่ใช้ในการทดสอบโปรแกรม

4.1.1 ความต้องการทางด้านฮาร์ดแวร์

- 1) เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นระบบตรวจจับผู้บุกรุก
 - คอมพิวเตอร์ที่มีหน่วยประมวลผลกลางรุ่นเพนเทียมทรี ขึ้นไป
 - สามารถเชื่อมต่อกับเครือข่ายทีซีพี / ไอพีได้
 - หน่วยความจำขนาด 128 เมกะไบต์ ขึ้นไป
 - พื้นที่ว่างในฮาร์ดดิสก์ 10 กิกะไบต์ ขึ้นไป
- 2) อุปกรณ์ทางด้านเครือข่าย
 - ฮับ (Hub)
 - สายยูทีพี (UTP) 10/100 พร้อมหัวอาร์เจ-45 (RJ)-45

4.1.2 ความต้องการทางด้านซอฟต์แวร์

- ระบบปฏิบัติการฟิโดราคอร์ 4 (Fedora Core 4)
- โปรแกรมอาปาเช่ เวอร์ชัน 2.2.4 (Apache v.2.2.4) , มายเอสคิวแอล เวอร์ชัน 4.1.20 (MySQL v.4.1.20) และพีเอชพีเวอร์ชัน 5.2.0 (PHP v.5.2.0)

4.2 ขั้นตอนการติดตั้งโปรแกรม

ทำการติดตั้งระบบปฏิบัติการ และซอฟต์แวร์ ทั้งหมดที่จำเป็นต้องใช้ลงในเครื่องที่กำหนดให้เป็นเครื่องตรวจจับ

4.3 การทำงานของโปรแกรม

ในการพัฒนาระบบจะทำการสร้างส่วนติดต่อกับผู้ใช้งาน (User Interface) โดยผ่านทางเว็บเพจ (Web Page) สามารถเรียกใช้งานได้โดยเปิดบราวเซอร์ (Browser) และพิมพ์ในช่องแอดเดรสว่า

http://localhost/acid/acid_main.php



Peer-to-Peer Alert

Payload Detail In Last 20 Seconds

(Warning = 5000)

Warning at: _____

OK

Source IP	Sum Payload
85.17.40.174	1650

Graph

Destination IP	Sum Payload
60.190.113.235	836
61.194.108.8	832
64.131.238.201	272
81.9.140.138	272
83.149.112.85	862
85.17.40.39	1692
85.17.40.42	1650
85.1243.69	136
191.128.250.234	850
212.227.102.119	854

Graph

Added 7 alerts to the Alert cache

Source IP	Destination IP	Sum Payload
85.17.40.174	60.190.113.235	836
85.17.40.174	61.194.108.8	832
85.17.40.174	64.131.238.201	272
85.17.40.174	81.9.140.138	272
85.17.40.174	83.149.112.85	862
85.17.40.174	85.17.40.39	1692
85.17.40.174	85.17.40.42	1650
85.17.40.174	85.1243.69	136
85.17.40.174	191.128.250.234	850
85.17.40.174	212.227.102.119	854

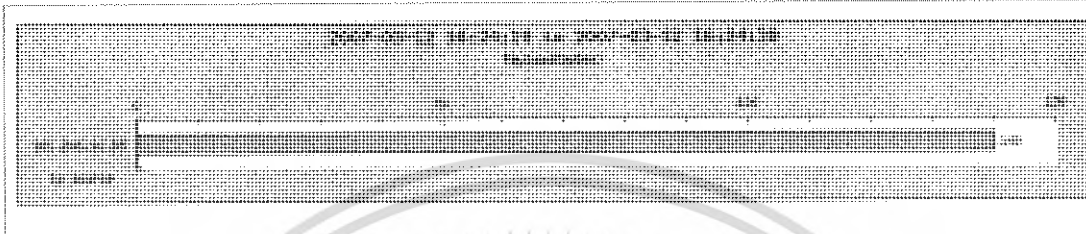
Queried on Mon March 12, 2007 16:31:28

รูปที่ 4.1 หน้าจอหลักของระบบ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.1 เพย์โหลด ดีเทล(payload detail)

โดยจะพิจารณาจากต้นทางและปลายทางที่ตรวจจับได้ว่าแต่ละแอดเดรสใช้เพย์โหลดไปเท่าไร ถ้าเกิน 2,000 ไบต์ จะแสดงเป็นแถบสีแดง(ปกติเป็นแถบสีเหลือง) โดยจะทำการรีเฟรช (Refresh)หน้าจอใหม่ทุกๆ 20 วินาที เมื่อต้องการดูกราฟให้คลิกที่ปุ่ม “Graph” จะได้ผลดังรูปที่ 4.2 และ 4.3



รูปที่ 4.2 หน้าจอแสดงกราฟแท่งแสดงความสัมพันธ์ระหว่างไอพีแอดเดรสต้นทางกับเพย์โหลดที่ใช้



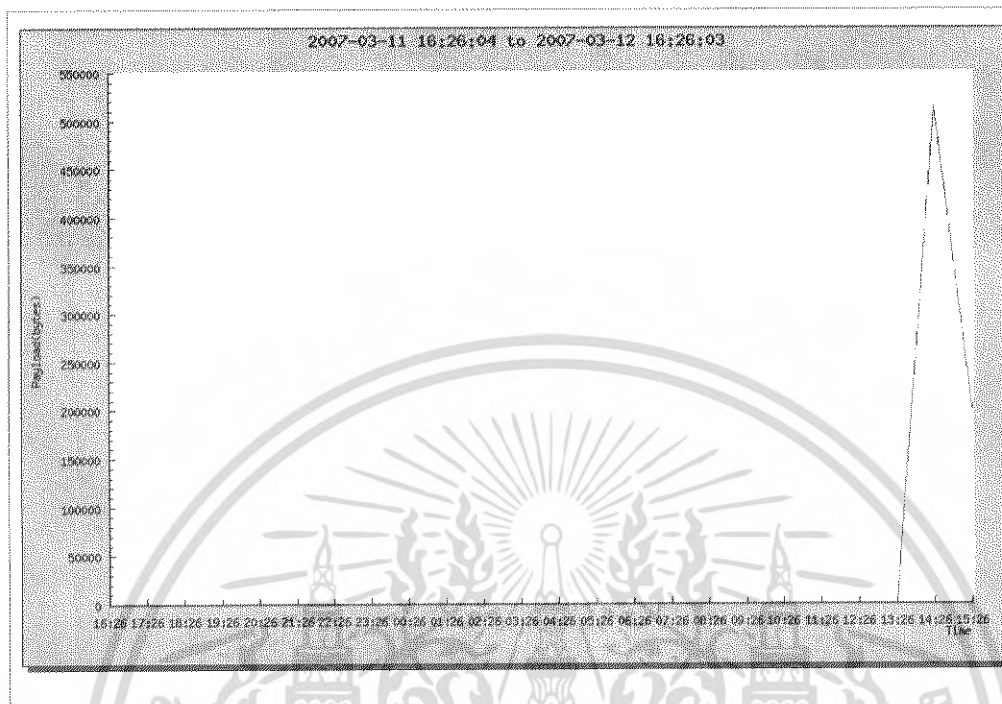
รูปที่ 4.3 หน้าจอแสดงกราฟแท่งแสดงความสัมพันธ์ระหว่างไอพีแอดเดรสปลายทางกับเพย์โหลดที่ใช้

4.3.2 รายงานแสดงผลด้วยกราฟในเวลา 24 ชั่วโมงล่าสุด

มีให้เลือก 2 แบบคือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

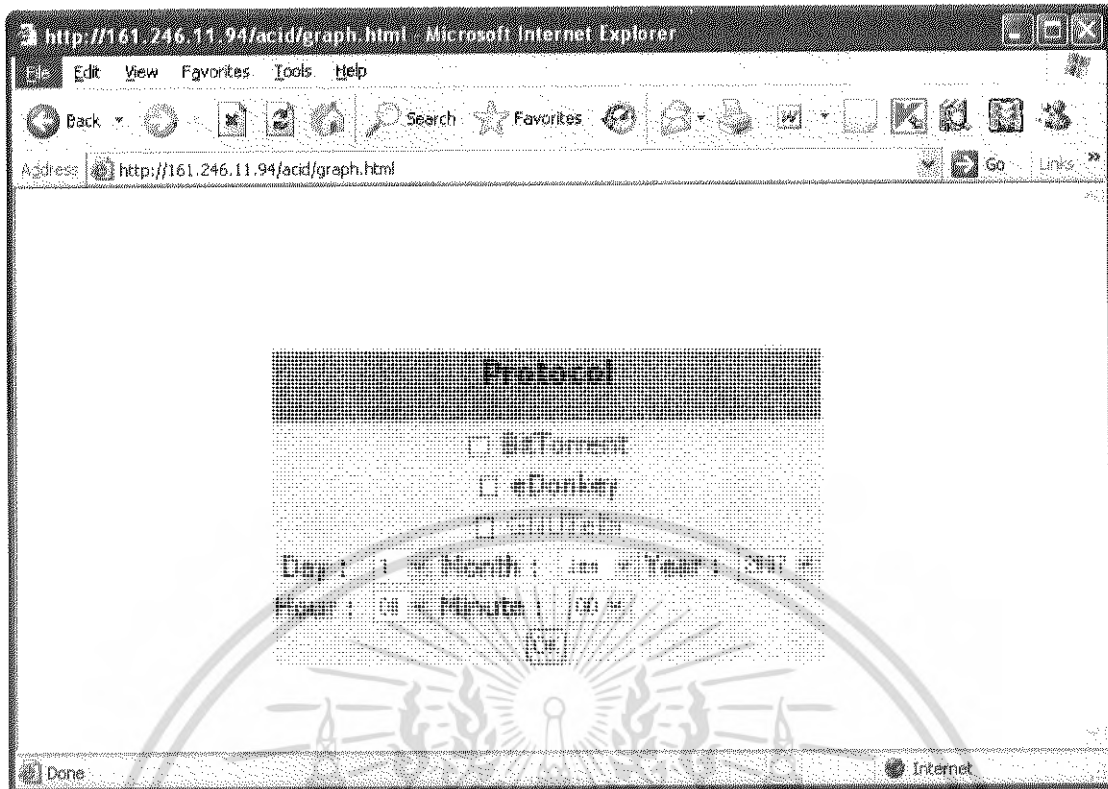
1) กราฟเส้นแสดงเพย์โหลดของโปรโตคอลเพียร์ทูเพียร์ทั้งหมดรวมกัน ใน 24 ชั่วโมงล่าสุด ดังรูปที่ 4.4



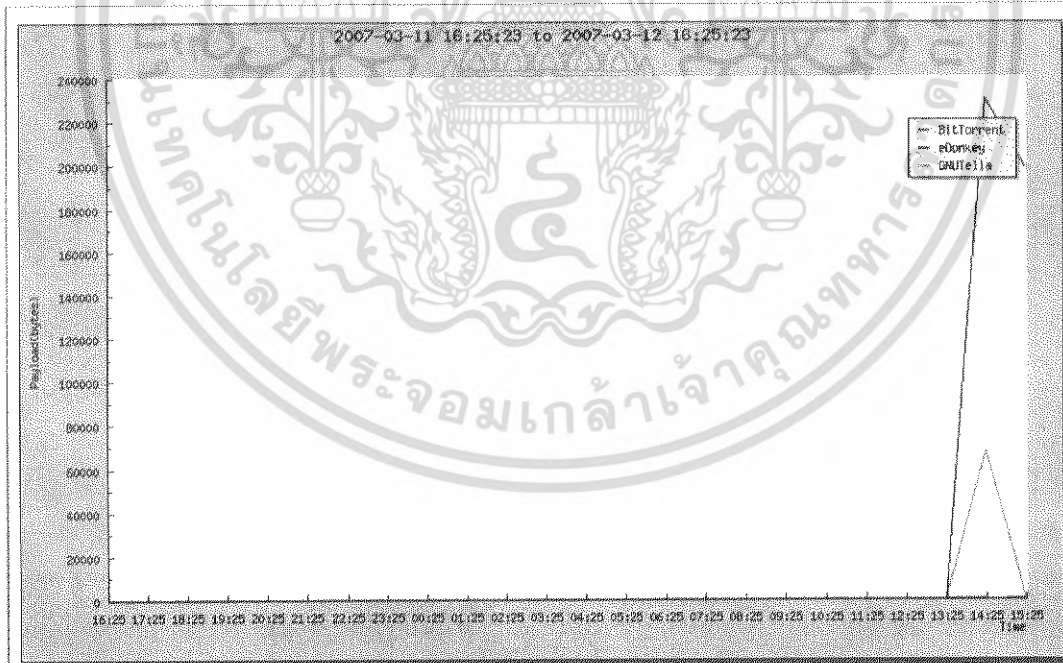
รูปที่ 4.4 หน้าจอแสดงกราฟเส้นแสดงความสัมพันธ์ระหว่างเพย์โหลดของโปรโตคอลเพียร์ทูเพียร์ทั้งหมดรวมกันกับเวลา 24 ชั่วโมงล่าสุด

2) กราฟเส้นแสดงเพย์โหลดของโปรโตคอลเพียร์ทูเพียร์ตามแต่ผู้ใช้จะเลือก ใน 24 ชั่วโมงล่าสุด ดังรูปที่ 4.5 และ 4.6

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.5 หน้าจอแสดงการเลือกที่จะแสดงรายงานด้วยกราฟของโปรโตคอลตัวใดและวันเวลาใด



รูปที่ 4.6 หน้าจอแสดงกราฟเส้นแสดงความสัมพันธ์ระหว่างเพียร์โหนดของแต่ละโปรโตคอลใน 24 ชั่วโมงล่าสุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.3.3 การแสดงรายงานต่างๆ

มีรายละเอียดดังนี้

สามารถแสดงผลตามไอพีแอดเดรสต้นทางได้โดยระบบจะแสดงว่าไอพีแอดเดรส
นั้นๆใช้งานทั้งหมดก็แพ็กเก็ต ใช้งานกี่รูปแบบ และ ไอพีแอดเดรสปลายทางมีจำนวนเท่าไร ดังรูป

The screenshot shows a web interface for 'ALERT Unique Source Address(es)'. It includes a search bar, a 'Home' link, and a '[Back]' link. Below the search bar, it says 'Queried DB on: Tue March 06, 2007 14:50:36' and 'Displaying alerts 1-28 of 28 total'. The main content is a table with the following columns: Src IP address, FQDN, Total #, Unique Alerts, and Dest Addr. The table lists various IP addresses and their corresponding FQDNs, along with the number of total alerts, unique alerts, and destination addresses for each.

Src IP address	FQDN	Total #	Unique Alerts	Dest Addr
24.19.249.158	c-24-19-249-160.hsd1.mi.comcast.net	1	1	1
74.243.176.228	cpe-24-243-176-228.sit.res.rr.com	1	1	3
81.184.109.81	Unable to resolve address	26	1	1
72.62.30.123	pool-72-62-30-123.prispa.east.verizon.net	23	1	1
77.152.135.65	85.135.192.77.rev.pooland.net	3	1	1
87.231.253.19	lin51-1-62-231-253-19.fbx.proxad.net	61	1	1
83.38.5.91	box31.neoplus.adsl.tpnet.pl	96	1	1
84.35.167.191	Unable to resolve address	103	1	2
84.90.139.278	Unable to resolve address	11	1	1
84.90.11.87	Unable to resolve address	20	1	1
84.192.107.114	57.1130-84.rev.pooland.net	17	1	1
85.75.428.169	d540c667c.access.telenet.bg	17	1	1
86.296.229.89	ath0d1-276748.oranet.gr	35	1	1
88.138.207.21	ALyon-25-1-102-69-w66-206.abo.wanadoo.fr	4	1	1
89.139.42.43	68-139-207-81.bb.netvision.net.il	13	1	1
89.139.42.43	89-139-42-43.bb.netvision.net.il	44	1	1
89.139.72.235	89-139-72-235.bb.netvision.net.il	75	1	1
161.246.11.59	jaruay-crc.kmitl.ac.th	42	1	7
161.246.11.58	001-crc.kmitl.ac.th	1	2	1
161.246.11.57	krasama-crc.kmitl.ac.th	417	3	116
161.246.11.53	160-crc.kmitl.ac.th	1	2	3
161.246.11.95	poohich-crc.kmitl.ac.th	66	4	18
161.246.11.96	ip-rags-crc.kmitl.ac.th	1111	7	233
161.246.11.97	first-crc.kmitl.ac.th	1970	7	122
161.246.11.98	richy-crc.kmitl.ac.th	120	4	24
166.203.229.5	Unable to resolve address	3	1	1
213.172.779.109	Unable to resolve address	1	1	1
219.93.34.281	211.31.85.219.kj81.hondatv.net.my	9	1	1
295.255.255.255	Unable to resolve address	1	1	1

[Loaded in 0 seconds]

รูปที่ 4.7 หน้าจอแสดงผลตามไอพีแอดเดรสต้นทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบยังสามารถแสดงผลการตรวจจับ โดยเรียงแพ็กเก็ต 15 แพ็กเก็ตล่าสุดที่บันทึกไว้

ดังรูป

ALERT Query Results: 15 Last TCP

Accepted (starting) in the Alert Cache

Displaying 15 Last TCP

ID	Signature	Timestamp	Source Address	Dest Address
#0 (2-375)	[snort] BitTorrent announce request	2007-03-06 14:52:06	161.246.11.98:2841	64.72.112.47:80
#1 (2-376)	[snort] BitTorrent announce request	2007-03-06 14:52:06	161.246.11.98:2840	205.234.195.10:80
#2 (2-373)	[snort] BitTorrent announce request	2007-03-06 14:50:59	161.246.11.98:2830	64.72.112.47:80
#3 (2-374)	[snort] BitTorrent announce request	2007-03-06 14:50:59	161.246.11.98:2829	205.234.195.10:80
#4 (2-371)	[snort] BitTorrent announce request	2007-03-06 14:50:00	161.246.11.98:2805	64.72.112.47:80
#5 (2-372)	[snort] BitTorrent announce request	2007-03-06 14:50:00	161.246.11.98:2806	205.234.195.10:80
#6 (2-369)	[snort] BitTorrent transfer	2007-03-06 14:50:00	161.246.11.98:2799	89.136.207.83:37332
#7 (2-378)	[snort] BitTorrent transfer	2007-03-06 14:50:00	61.184.100.8:67566	161.246.11.98:10737
#8 (2-368)	[snort] BitTorrent announce request	2007-03-06 14:49:58	161.246.11.98:2797	61.184.100.8:98
#9 (2-364)	[snort] BitTorrent announce request	2007-03-06 14:49:27	161.246.11.98:2792	64.72.112.47:80
#10 (2-366)	[snort] BitTorrent announce request	2007-03-06 14:49:27	161.246.11.98:2793	205.234.195.10:80
#11 (2-361)	[snort] BitTorrent announce request	2007-03-06 14:49:23	161.246.11.98:2786	61.184.100.8:98
#12 (2-360)	[snort] BitTorrent announce request	2007-03-06 14:49:21	89.136.207.83:1910	161.246.11.98:10737
#13 (2-357)	[snort] BitTorrent announce request	2007-03-06 14:49:56	161.246.11.98:2774	64.72.112.47:80
#14 (2-356)	[snort] BitTorrent announce request	2007-03-06 14:49:56	161.246.11.98:2773	205.234.195.10:80

[Loaded in 0 seconds]

Delete start(s) Select All on Screen Entire Query

รูปที่ 4.9 หน้าจอแสดงผลโดยเรียงแพ็กเก็ต 15 แพ็กเก็ตล่าสุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับได้ในวันนี้ โดยแสดงผลที่ไม่ซ้ำกันออกมา ดัง

รูป

ALERT

Alert Listing

Home

[Back]

Added 6 alert(s) to the Alert cache

Queried DB on Tue March 06, 2007 14:53:40

Displaying alerts 1-5 of 5 total

	Signature	Total #	Src Addr	Dest Addr	First	Last
<input type="checkbox"/>	[snort] (portscan) TCP PortswEEP	4 (0%)	1	1	2007-03-06 14:26:15	2007-03-06 14:49:23
<input type="checkbox"/>	[snort] (portscan) Open Port	11 (0%)	1	8	2007-03-06 14:26:16	2007-03-06 14:49:29
<input type="checkbox"/>	[snort] BitTorrent transfer	26 (1%)	3	2	2007-03-06 14:40:12	2007-03-06 14:53:33
<input type="checkbox"/>	[snort] BitTorrent announce request	101 (2%)	1	10	2007-03-06 14:39:59	2007-03-06 14:53:11
<input type="checkbox"/>	[snort] (snort decoder) Bad Traffic Same Src/Dst IP	1 (0%)	1	1	2007-03-06 14:00:58	2007-03-06 14:00:58

Delete alert(s) Selected ALL on Screen

[Loaded in 1 seconds]

รูปที่ 4.10 หน้าจอแสดงผลของการตรวจจับโดยแสดงซิกเนเจอร์ที่ไม่ซ้ำกันในวันนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับในวันนี้ได้ทั้งหมด ค้างรูป



Query Results

Home

[Back]

Added 2 alerts to the Alert cache

Displaying alerts 1-50 of 145 total

ID	Signature	Timestamp	Source Address	Dest Address
#1 (2-238)	[snort] smart decoder) Bad Traffic Same Src/Dst IP	2007-03-06 14:00:58	255.255.255.255	255.255.255.255
#1 (2-239)	[snort] (portscan) TCP Portscan	2007-03-06 14:26:15	161.246.11.98	217.14.78.234
#2 (2-240)	[snort] (portscan) Open Port	2007-03-06 14:26:16	161.246.11.98	72.5.236.31
#3 (2-241)	[snort] (portscan) Open Port	2007-03-06 14:26:16	161.246.11.98	87.176.47.237
#4 (2-242)	[snort] BitTorrent announce request	2007-03-06 14:39:59	161.246.11.98:2496	205.234.195.18:80
#5 (2-243)	[snort] BitTorrent announce request	2007-03-06 14:39:59	161.246.11.98:2493	193.138.230.239:2710
#6 (2-244)	[snort] BitTorrent announce request	2007-03-06 14:40:00	161.246.11.98:2496	64.72.142.42:80
#7 (2-245)	[snort] BitTorrent announce request	2007-03-06 14:40:01	161.246.11.98:2494	85.17.46.43:80
#8 (2-246)	[snort] BitTorrent announce request	2007-03-06 14:40:02	161.246.11.98:2473	248.93.248.254:8000
#9 (2-247)	[snort] BitTorrent announce request	2007-03-06 14:40:02	161.246.11.98:2464	193.138.230.239:2710
#10 (2-248)	[snort] BitTorrent announce request	2007-03-06 14:40:02	161.246.11.98:2487	85.17.46.43:80
#11 (2-249)	[snort] BitTorrent announce request	2007-03-06 14:40:02	161.246.11.98:2488	85.17.46.43:80
#12 (2-250)	[snort] BitTorrent announce request	2007-03-06 14:40:02	161.246.11.98:2463	193.138.230.239:2710
#13 (2-251)	[snort] BitTorrent announce request	2007-03-06 14:40:02	161.246.11.98:2481	193.138.230.239:2710
#14 (2-252)	[snort] BitTorrent announce request	2007-03-06 14:40:03	161.246.11.98:2501	64.72.142.42:80
#15 (2-253)	[snort] BitTorrent announce request	2007-03-06 14:40:03	161.246.11.98:2483	83.149.112.85:9999
#16 (2-254)	[snort] BitTorrent announce request	2007-03-06 14:40:03	161.246.11.98:2484	212.227.402.119:8000
#17 (2-255)	[snort] BitTorrent announce request	2007-03-06 14:40:03	161.246.11.98:2495	85.17.46.43:80
#18 (2-256)	[snort] BitTorrent announce request	2007-03-06 14:40:05	161.246.11.98:2474	193.138.230.239:2710
#19 (2-257)	[snort] BitTorrent announce request	2007-03-06 14:40:05	161.246.11.98:2475	193.138.230.239:2710
#20 (2-258)	[snort] BitTorrent announce request	2007-03-06 14:40:05	161.246.11.98:2481	193.138.230.239:2710
#21 (2-259)	[snort] BitTorrent announce request	2007-03-06 14:40:05	161.246.11.98:2480	85.17.46.43:80
#22 (2-260)	[snort] BitTorrent announce request	2007-03-06 14:40:11	161.246.11.98:2475	193.138.230.239:2710
#23 (2-261)	[snort] BitTorrent announce request	2007-03-06 14:40:11	161.246.11.98:2476	193.138.230.239:2710
#24 (2-262)	[snort] BitTorrent announce request	2007-03-06 14:40:11	161.246.11.98:2478	193.138.230.239:2710
#25 (2-263)	[snort] BitTorrent announce request	2007-03-06 14:40:11	161.246.11.98:2480	85.17.46.43:80
#26 (2-264)	[snort] BitTorrent announce request	2007-03-06 14:40:11	161.246.11.98:2481	193.138.230.239:2710
#27 (2-265)	[snort] BitTorrent transfer	2007-03-06 14:40:12	161.246.11.98:2504	85.17.46.43:80
#28 (2-266)	[snort] BitTorrent transfer	2007-03-06 14:40:15	161.246.11.98:2504	85.17.46.43:80
#29 (2-267)	[snort] BitTorrent announce request	2007-03-06 14:40:16	161.246.11.98:2511	205.234.195.18:80
#30 (2-268)	[snort] BitTorrent announce request	2007-03-06 14:40:17	161.246.11.98:2508	248.93.248.254:8000
#31 (2-269)	[snort] BitTorrent announce request	2007-03-06 14:40:17	161.246.11.98:2510	85.17.46.43:80
#32 (2-270)	[snort] BitTorrent announce request	2007-03-06 14:40:17	161.246.11.98:2510	85.17.46.43:80
#33 (2-271)	[snort] BitTorrent announce request	2007-03-06 14:40:20	161.246.11.98:2508	248.93.248.254:8000
#34 (2-272)	[snort] BitTorrent announce request	2007-03-06 14:40:23	161.246.11.98:2474	193.138.230.239:2710
#35 (2-273)	[snort] BitTorrent announce request	2007-03-06 14:40:23	161.246.11.98:2475	193.138.230.239:2710
#36 (2-274)	[snort] BitTorrent announce request	2007-03-06 14:40:23	161.246.11.98:2480	85.17.46.43:80
#37 (2-275)	[snort] BitTorrent announce request	2007-03-06 14:40:37	161.246.11.98:2528	85.17.46.43:80
#38 (2-276)	[snort] BitTorrent announce request	2007-03-06 14:40:38	161.246.11.98:2523	85.17.46.43:80
#39 (2-277)	[snort] BitTorrent announce request	2007-03-06 14:40:40	161.246.11.98:2527	64.72.142.42:80
#40 (2-278)	[snort] BitTorrent announce request	2007-03-06 14:40:40	161.246.11.98:2525	205.234.195.18:80
#41 (2-279)	[snort] BitTorrent announce request	2007-03-06 14:40:40	161.246.11.98:2522	248.93.248.254:8000
#42 (2-280)	[snort] BitTorrent announce request	2007-03-06 14:40:40	161.246.11.98:2525	85.17.46.43:80
#43 (2-281)	[snort] BitTorrent announce request	2007-03-06 14:40:41	161.246.11.98:2516	217.14.78.234:8088
#44 (2-282)	[snort] BitTorrent announce request	2007-03-06 14:40:41	161.246.11.98:2533	202.214.210.16:8088
#45 (2-283)	[snort] BitTorrent announce request	2007-03-06 14:40:47	161.246.11.98:2474	193.138.230.239:2710
#46 (2-284)	[snort] BitTorrent announce request	2007-03-06 14:40:47	161.246.11.98:2475	193.138.230.239:2710
#47 (2-285)	[snort] BitTorrent announce request	2007-03-06 14:40:47	161.246.11.98:2481	193.138.230.239:2710
#48 (2-286)	[snort] BitTorrent announce request	2007-03-06 14:40:47	161.246.11.98:2480	85.17.46.43:80
#49 (2-287)	[snort] BitTorrent announce request	2007-03-06 14:41:09	161.246.11.98:2642	64.72.142.42:80

Query Results
[1] [2]

Delete alert(s): Selected ALL on Screen Entire Query

[Loaded in 0 seconds]

รูปที่ 4.11 หน้าจอแสดงผลของการตรวจจับทั้งหมดที่ตรวจจับได้ในวันนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับวันนี้โดยพิจารณาจากไอพีแอดเดรสต้นทาง
ดังรูป

ALERT Unique Source Address(es) Home

Added 2 alert(s) to the Alert cache [Back]

Queried DB on Tue March 06, 2007 14:56:11

Displaying alerts 1-4 of 4 total

Src IP address	FQDN	Total #	Unique Alerts	Dest. Addr.
161.246.11.98	nchy.crs.c.irmill.ac.th	130	4	24
89.138.207.83	99-138-207-83.bb.netvision.net.il	17	1	1
61.184.180.8	Unable to resolve address	1	1	1
255.255.255.255	Unable to resolve address	1	1	1

[Loaded in 0 seconds]

รูปที่ 4.12 หน้าจอแสดงผลของการตรวจจับวันนี้โดยพิจารณาจากไอพีแอดเดรสต้นทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับในวันนี้โดยพิจารณาจากไอพีแอดเดรส
ปลายทาง ดังรูป

Dest IP address	FQDN	Total #	Unique Alerts	Src. Addr.
193.139.236.239	Unable to resolve address	26	2	1
91.184.198.6	Unable to resolve address	25	3	1
205.234.195.10	server.ahssoft.com	21	2	1
64.72.142.42	Unable to resolve address	21	2	1
161.249.11.58	nctry.disc.kmit.ac.th	21	2	1
89.136.207.83	89.136-207-83.bb.netvision.net.il	18	1	2
218.93.748.244	Unable to resolve address	15	2	1
86.17.46.43	Unable to resolve address	3	1	1
85.214.105.231	Unable to resolve address	2	1	1
218.93.135.114	hpd-crew.homelip.net	2	1	1
193.139.231.146	Unable to resolve address	2	1	1
222.214.218.76	Unable to resolve address	2	1	1
64.72.119.195	76.218.214.222.broadband.spectrum.net	2	1	1
216.17.218.42	hosted-by.liquidnet.com	2	1	1
72.6.236.34	es-19-215-12-218-42.easervers.net	1	1	1
717.13.706.147	hans.skle.com	1	1	1
61.176.77.231	Unable to resolve address	1	1	1
211.56.76.734	Unable to resolve address	1	1	1
83.149.142.65	marier.manahost.ru	1	1	1
85.12.12.5	tracker.paradise-tracker.com	1	1	1
68.190.113.238	ms113-koccl-group.com	1	1	1
85.17.48.34	Unable to resolve address	1	1	1
85.17.48.38	Unable to resolve address	1	1	1
255.255.255.255	Unable to resolve address	1	1	1
85.17.48.40	Unable to resolve address	1	1	1
719.227.682.119	316201373.dnshome-server.nfo	1	1	1

[Loaded in 18 seconds]

รูปที่ 4.13 หน้าจอแสดงผลของการตรวจจับในวันนี้โดยพิจารณาจากไอพีแอดเดรสปลายทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับที่เกิดขึ้นภายใน 24 ชั่วโมงล่าสุด โดยแสดงผลที่ไม่ซ้ำกันออกมา ดังรูป

ALERT

Alert Listing

Home

[Back]

Added 2 alerts to the Alert cache

Queried DB on Tue March 06, 2007 14:57:46

Displaying alerts 1-10 of 10 total

	Signature	Total #	Src Addr	Dest Addr	First	Last
<input type="checkbox"/>	[snort] (portscan) TCP PortswEEP	53 (1%)	8	75	2007-03-04 23:09:34	2007-03-06 14:49:23
<input type="checkbox"/>	[snort] (portscan) Open Port	506 (14%)	8	155	2007-03-04 23:09:43	2007-03-06 14:49:25
<input type="checkbox"/>	[snort] (portscan) UDP PortswEEP	1 (0%)	1	1	2007-03-04 23:14:06	2007-03-04 23:14:06
<input type="checkbox"/>	[snort] (portscan) TCP Portscan	3 (0%)	3	2	2007-03-04 23:17:03	2007-03-04 23:52:32
<input type="checkbox"/>	[snort] BitTorrent transfer	1268 (30%)	20	14	2007-03-01 23:03:13	2007-03-06 14:57:36
<input type="checkbox"/>	[snort] BitTorrent announce request	1174 (28%)	4	31	2007-03-01 23:03:11	2007-03-06 14:57:44
<input type="checkbox"/>	url[snort] eDonkey transfer	46 (1%)	2	5	2007-03-01 18:16:26	2007-03-02 00:23:18
<input type="checkbox"/>	[snort] Outbound GNU/Tella client request	458 (11%)	3	288	2007-03-01 18:14:56	2007-03-04 23:37:11
<input type="checkbox"/>	[snort] GNU/Tella client request	625 (15%)	5	289	2007-03-01 18:14:56	2007-03-04 23:37:14
<input type="checkbox"/>	[snort] (snort decoder) Bad Traffic Same Src/Dst IP	1 (0%)	1	1	2007-03-06 14:00:58	2007-03-06 14:00:58


Delete alert(s) Delete Selected ALL on Screen

[Loaded in 1 seconds]

รูปที่ 4.14 หน้าจอแสดงผลของการตรวจจับโดยแสดงซิกเนเจอร์ที่ไม่ซ้ำกันและเป็นรายการที่เกิดขึ้น ใน 24 ชั่วโมงล่าสุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับที่เกิดขึ้นภายใน 24 ชั่วโมงล่าสุดโดยแสดงรายการที่ตรวจจับได้ทั้งหมดทั้งหมด ดังรูป



Query Results

[Home](#)
[\[Back \]](#)

Added 0 alert(s) to the Alert cache

Displaying alerts 1-50 of 4247 total

#	ID	Signature	Timestamp	Source Address	Dest Address
<input type="checkbox"/>	#0 (1-1813)	[snort] GNUtella client request	2007-03-01 18:26:43	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#1 (1-1812)	[snort] Outbound GNUtella client request	2007-03-01 18:26:43	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#2 (1-1811)	[snort] GNUtella client request	2007-03-01 18:26:43	161.246.11.92:2365	24.58.251.151:12157
<input type="checkbox"/>	#3 (1-1810)	[snort] Outbound GNUtella client request	2007-03-01 18:26:43	161.246.11.92:2365	24.58.251.151:12157
<input type="checkbox"/>	#4 (1-1809)	[snort] GNUtella client request	2007-03-01 18:26:41	161.246.11.92:2368	74.56.124.224:9256
<input type="checkbox"/>	#5 (1-1808)	[snort] GNUtella client request	2007-03-01 18:26:38	161.246.11.92:2358	74.56.124.224:9256
<input type="checkbox"/>	#6 (1-1807)	[snort] GNUtella client request	2007-03-01 18:26:37	161.246.11.92:2358	74.56.124.224:9256
<input type="checkbox"/>	#7 (1-1806)	[snort] Outbound GNUtella client request	2007-03-01 18:26:37	161.246.11.92:2358	74.56.124.224:9256
<input type="checkbox"/>	#8 (1-1805)	[snort] GNUtella client request	2007-03-01 18:26:36	161.246.11.92:2360	82.254.192.48:6346
<input type="checkbox"/>	#9 (1-1804)	[snort] Outbound GNUtella client request	2007-03-01 18:26:36	161.246.11.92:2360	82.254.192.48:6346
<input type="checkbox"/>	#10 (1-1803)	[snort] GNUtella client request	2007-03-01 18:26:33	161.246.11.92:2355	222.101.90.252:6346
<input type="checkbox"/>	#11 (1-1802)	[snort] Outbound GNUtella client request	2007-03-01 18:26:33	161.246.11.92:2355	222.101.90.252:6346
<input type="checkbox"/>	#12 (1-1801)	[snort] GNUtella client request	2007-03-01 18:26:30	161.246.11.92:2355	222.101.90.252:6346
<input type="checkbox"/>	#13 (1-1800)	[snort] Outbound GNUtella client request	2007-03-01 18:26:30	161.246.11.92:2355	222.101.90.252:6346
<input type="checkbox"/>	#14 (1-1799)	[snort] GNUtella client request	2007-03-01 18:26:23	161.246.11.92:2350	82.247.63.234:6346
<input type="checkbox"/>	#15 (1-1798)	[snort] Outbound GNUtella client request	2007-03-01 18:26:23	161.246.11.92:2350	82.247.63.234:6346
<input type="checkbox"/>	#16 (1-1797)	[snort] GNUtella client request	2007-03-01 18:26:23	161.246.11.92:2349	81.220.224.77:6346
<input type="checkbox"/>	#17 (1-1796)	[snort] Outbound GNUtella client request	2007-03-01 18:26:23	161.246.11.92:2349	81.220.224.77:6346
<input type="checkbox"/>	#18 (1-1795)	[snort] GNUtella client request	2007-03-01 18:26:21	161.246.11.92:2343	71.75.33.216:15246
<input type="checkbox"/>	#19 (1-1794)	[snort] Outbound GNUtella client request	2007-03-01 18:26:21	161.246.11.92:2343	71.75.33.216:15246
<input type="checkbox"/>	#20 (1-1793)	[snort] GNUtella client request	2007-03-01 18:26:19	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#21 (1-1792)	[snort] Outbound GNUtella client request	2007-03-01 18:26:19	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#22 (1-1791)	[snort] GNUtella client request	2007-03-01 18:26:18	161.246.11.92:2349	71.75.33.216:15246
<input type="checkbox"/>	#23 (1-1790)	[snort] Outbound GNUtella client request	2007-03-01 18:26:18	161.246.11.92:2343	71.75.33.216:15246
<input type="checkbox"/>	#24 (1-1789)	[snort] GNUtella client request	2007-03-01 18:26:12	161.246.11.92:2323	24.76.181.148:6346
<input type="checkbox"/>	#25 (1-1788)	[snort] Outbound GNUtella client request	2007-03-01 18:26:09	161.246.11.92:2323	24.76.181.148:6346
<input type="checkbox"/>	#26 (1-1787)	[snort] GNUtella client request	2007-03-01 18:26:08	161.246.11.92:2323	24.76.181.148:6346
<input type="checkbox"/>	#27 (1-1786)	[snort] Outbound GNUtella client request	2007-03-01 18:26:08	161.246.11.92:2323	24.76.181.148:6346
<input type="checkbox"/>	#28 (1-1785)	[snort] GNUtella client request	2007-03-01 18:26:07	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#29 (1-1784)	[snort] Outbound GNUtella client request	2007-03-01 18:26:07	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#30 (1-1783)	[snort] GNUtella client request	2007-03-01 18:26:05	161.246.11.92:2223	82.228.62.12:6346
<input type="checkbox"/>	#31 (1-1782)	[snort] Outbound GNUtella client request	2007-03-01 18:26:01	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#32 (1-1781)	[snort] GNUtella client request	2007-03-01 18:26:01	161.246.11.92:2322	85.179.162.93:6346
<input type="checkbox"/>	#33 (1-1780)	[snort] Outbound GNUtella client request	2007-03-01 18:25:59	161.246.11.92:2320	210.49.253.73:19218
<input type="checkbox"/>	#34 (1-1779)	[snort] GNUtella client request	2007-03-01 18:25:58	161.246.11.92:2320	210.49.253.73:19218
<input type="checkbox"/>	#35 (1-1778)	[snort] Outbound GNUtella client request	2007-03-01 18:25:58	161.246.11.92:2320	210.49.253.73:19218
<input type="checkbox"/>	#36 (1-1776)	[snort] GNUtella client request	2007-03-01 18:25:55	161.246.11.92:2317	217.172.241.24:6346
<input type="checkbox"/>	#37 (1-1775)	[snort] Outbound GNUtella client request	2007-03-01 18:25:57	161.246.11.92:2317	217.172.241.24:6346
<input type="checkbox"/>	#38 (1-1775)	[snort] Outbound GNUtella client request	2007-03-01 18:25:55	161.246.11.92:2317	217.172.241.24:6346
<input type="checkbox"/>	#39 (1-1774)	[snort] GNUtella client request	2007-03-01 18:25:54	161.246.11.92:2316	128.2.25.171:6346
<input type="checkbox"/>	#40 (1-1773)	[snort] Outbound GNUtella client request	2007-03-01 18:25:54	161.246.11.92:2316	128.2.25.171:6346
<input type="checkbox"/>	#41 (1-1772)	[snort] GNUtella client request	2007-03-01 18:25:45	161.246.11.92:2305	58.104.150.240:17717
<input type="checkbox"/>	#42 (1-1771)	[snort] Outbound GNUtella client request	2007-03-01 18:25:45	161.246.11.92:2305	58.104.150.240:17717
<input type="checkbox"/>	#43 (1-1770)	[snort] GNUtella client request	2007-03-01 18:25:45	161.246.11.92:2130	68.106.185.191:6346
<input type="checkbox"/>	#44 (1-1769)	[snort] Outbound GNUtella client request	2007-03-01 18:25:45	161.246.11.92:2130	68.106.185.191:6346
<input type="checkbox"/>	#45 (1-1768)	[snort] GNUtella client request	2007-03-01 18:25:40	161.246.11.92:2223	82.228.62.12:6346
<input type="checkbox"/>	#46 (1-1767)	[snort] Outbound GNUtella client request	2007-03-01 18:25:38	161.246.11.92:2291	74.57.99.106:6346
<input type="checkbox"/>	#47 (1-1766)	[snort] GNUtella client request	2007-03-01 18:25:38	161.246.11.92:2291	74.57.99.106:6346
<input type="checkbox"/>	#48 (1-1765)	[snort] Outbound GNUtella client request	2007-03-01 18:25:35	161.246.11.92:2291	74.57.99.106:6346
<input type="checkbox"/>	#49 (1-1764)	[snort] GNUtella client request	2007-03-01 18:25:35	161.246.11.92:2291	74.57.99.106:6346

Query Results

(0) [1] [2] [3] [4] [5] >>

Delete alert(s) Selected All on Screen Entire Query

[Loaded in 0 seconds]

รูปที่ 4.15 หน้าจอแสดงผลของการตรวจจับทั้งหมดที่ตรวจจับได้ใน 24 ชั่วโมงล่าสุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับใน 24 ชั่วโมงล่าสุดโดยพิจารณาจากไอพีแอดเดรสต้นทาง ดังรูป


Src IP address	FQDN	Total #	Unique Alerts	Dest. Addr.
161.246.11.97	first.crc.kmitl.ac.th	1870	7	122
161.246.11.96	ip-regis.crc.kmitl.ac.th	1111	7	233
161.246.11.92	Kasama.crc.kmitl.ac.th	417	3	116
89.139.72.238	89-139-72-238.bb.netvision.net.il	156	2	1
161.246.11.98	richy.crc.kmitl.ac.th	132	4	24
84.36.202.151	Unable to resolve address	103	1	2
161.246.11.95	poolinch.crc.kmitl.ac.th	66	4	18
82.231.253.19	tm51-1-82-231-253-19.lbx.proxad.net	64	1	1
83.30.8.91	lbc91.neoplus.adsl.tpnet.pl	56	1	1
89.139.42.43	89-139-42-43.bb.netvision.net.il	44	1	1
161.246.11.58	jeruay.crc.kmitl.ac.th	42	3	7
85.73.128.170	athedsl-276748.atenet.gr	35	1	1
61.184.100.8	Unable to resolve address	26	1	3
89.138.207.83	89-138-207-83.bb.netvision.net.il	23	1	1
72.92.30.123	pool-72-92-30-123.phlpa.eas1.verizon.net	21	1	1
84.98.14.91	91.11.98.84.rev.gadland.net	20	1	1
84.192.184.124	d54C0657C.access.telenet.be	17	1	1
84.96.139.228	Unable to resolve address	11	1	1
219.95.31.211	211.31.95.219.kj01.home.tn.net.my	8	1	1
161.246.11.58	oui.crc.kmitl.ac.th	7	2	1
196.203.221.5	Unable to resolve address	5	1	1
86.206.220.99	ALyon-251-1-102-69-w65-206.abo.wanadoo.fr	4	1	1
213.172.232.109	Unable to resolve address	3	1	1
161.246.11.93	lec.crc.kmitl.ac.th	3	2	3
77.192.435.85	85.135.192-77.rev.gadland.net	3	1	1
74.19.249.158	c-24-19-249-158.hsd1.wa.comcast.net	1	1	1
24.243.126.228	cpe-24-243-126-228.six.res.r.com	1	1	1
755.255.255.255	Unable to resolve address	1	1	1

[Loaded in 0 seconds]

รูปที่ 4.16 หน้าจอแสดงผลของการตรวจจับ 24 ชั่วโมงล่าสุดโดยพิจารณาจากไอพีแอดเดรสต้นทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับใน 24 ชั่วโมงล่าสุดโดยพิจารณาจากไอพีแอดเดรสปลายทาง ดังรูป



Home

[Back]

Added 0 alerts to the Alert cache

Queried DB on Tue March 06, 2007 14:59:34

Displaying alerts 1-50 of 462 total

Dest IP address	FQDN	Total #	Unique Alerts	Src. Addr
161.246.11.96	ip-regis.crc.kmitl.ac.th	298	1	12
161.246.11.97	first.crc.kmitl.ac.th	281	1	7
64.72.112.42	Unable to resolve address	259	2	4
295.234.195.10	senet.ukisok.com	248	2	3
193.138.230.239	Unable to resolve address	241	2	3
89.139.72.238	89-139-72-238.bb.netvision.net.il	219	3	1
84.90.139.278	Unable to resolve address	199	3	1
61.184.109.8	Unable to resolve address	195	3	3
89.138.42.43	89-138-42-43.bb.netvision.net.il	82	1	1
84.152.401.124	d54C0657C.access.lanet.be	69	1	1
217.132.163.01	Unable to resolve address	57	2	1
85.230.52.62	c-3e34e655-56-1-64736c11.cust.broadbandsolaget.se	51	2	1
85.17.40.49	Unable to resolve address	46	2	4
193.138.231.146	Unable to resolve address	43	2	3
80.190.113.235	Unable to resolve address	39	3	3
222.214.273.76	76.218.214.222.broadle.sc.dynamic.163data.com.cn	15	2	3
218.93.248.254	Unable to resolve address	29	3	3
64.72.119.195	hosted by liquidnet.com	28	3	3
212.222.102.119	s15201973.onlinehome-server.info	28	2	3
87.149.112.85	tracker.paradise-tracker.com	26	2	3
85.17.40.45	Unable to resolve address	25	2	2
161.246.11.88	nchy.crc.kmitl.ac.th	24	1	2
62.241.53.2	Unable to resolve address	24	1	2
87.52.162.18	ircs-67-52-107-18.net.biz.ir.com	24	3	3
161.246.11.94	sundaras.crc.kmitl.ac.th	23	1	1
793.150.238.73	host73.porai.com	21	2	1
85.17.40.85	Unable to resolve address	21	2	2
79.129.83.174	cpe-70-120-83-174.satx.res.llnwd.net	20	2	1
72.34.50.138	Unable to resolve address	20	2	1
85.17.40.34	Unable to resolve address	19	2	3
58.215.89.113	Unable to resolve address	18	2	2
85.17.41.3	ns1.tue-ivcd-group.com	18	2	2
62.241.53.4	Unable to resolve address	17	1	1
60.4.38.236	www.bay110.hotmail.com	16	2	1
221.178.125.228	Unable to resolve address	15	2	1
217.13.205.147	Unable to resolve address	14	2	3
63.236.73.144	Unable to resolve address	14	2	1
89.138.207.83	Unable to resolve address	13	2	2
85.17.40.37	Unable to resolve address	13	2	2
85.214.65.231	tpd-craw.hotmailp.net	13	1	2
203.121.182.204	Unable to resolve address	13	1	1
201.209.212.183	201-209-212-183.genericrev.cdnv.net	12	2	1
85.17.40.41	Unable to resolve address	12	2	1
213.245.87.81	FR-OZQIR-1954-6462-8737.voip.upchance.com	11	2	3
87.11.27.44	host44-27-dynamic.11-874.retail.telecomitalia.it	11	2	1
218.5.72.126	Unable to resolve address	11	2	1
65.209.8.52	uuvaehp2.dnubioclick.net	11	2	1
82.253.216.143	line-bzn-46-62-253-216-143.adel.proxad.net	10	2	1
68.186.14.139	68-186-14-139.dhcp.csby.or.charter.com	10	2	1
207.46.225.60	www.kktest4.microsoft.com	10	1	1


Query Results
[1 2 3 4 5] >>

[Loaded in 34 seconds]

รูปที่ 4.17 หน้าจอแสดงผลของการตรวจจับ 24 ชั่วโมงล่าสุดโดยพิจารณาจากไอพีแอดเดรสปลายทาง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับโดยแสดงหมายเลขพอร์ตของต้นทางที่ถูกตรวจจับนั้น จำนวนที่ถูกแจ้งเตือน วันและเวลาที่เพิ่งเกิดแรกและสุดท้ายที่ถูกตรวจจับ ซึ่งจะแสดง 15 รายการล่าสุดที่ถูกตรวจจับ ดังรูป



Unique TCP Source Port(s): 15 Last Ports

[Home](#)

[Back]

Added 4 alerts to the Alert cache

Queried DB on Tue March 06 2007 15:00:53

Displaying 15 Last Ports


Port	Occurrences	Unique Alerts	Source IP	Dest IP	First	Last
3057 / tcp	1	1	1	1	2007-03-06 15:00:53	2007-03-06 15:00:53
3058 / tcp	4	2	2	2	2007-03-02 00:28:20	2007-03-06 15:00:53
3028 / tcp	1	1	1	1	2007-03-06 15:00:22	2007-03-06 15:00:22
3037 / tcp	1	1	1	1	2007-03-06 15:00:22	2007-03-06 15:00:22
3011 / tcp	4	1	1	1	2007-03-06 14:59:44	2007-03-06 15:00:05
2988 / tcp	3	1	1	1	2007-03-06 14:59:45	2007-03-06 15:00:03
3021 / tcp	1	1	1	1	2007-03-06 15:00:01	2007-03-06 15:00:01
3023 / tcp	1	1	1	1	2007-03-06 15:00:01	2007-03-06 15:00:01
3024 / tcp	1	1	1	1	2007-03-06 15:00:01	2007-03-06 15:00:01
2989 / tcp	5	3	2	2	2007-03-04 23:36:47	2007-03-06 14:59:50
2987 / tcp	1	1	1	1	2007-03-06 14:59:46	2007-03-06 14:59:46
2984 / tcp	2	1	1	1	2007-03-06 14:59:43	2007-03-06 14:59:46
3067 / tcp	1	1	1	1	2007-03-06 14:59:44	2007-03-06 14:59:44
2997 / tcp	1	1	1	1	2007-03-06 14:59:44	2007-03-06 14:59:44
2996 / tcp	1	1	1	1	2007-03-06 14:59:44	2007-03-06 14:59:44

[Loaded in 1 seconds]

รูปที่ 4.18 หน้าจอแสดงผลของการตรวจจับโดยแสดงถึง 15 รายการล่าสุดที่พอร์ตต้นทางถูกแจ้งเตือน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับ โดยแสดงหมายเลขพอร์ตของปลายทางที่ถูกตรวจจับนั้น จำนวนที่ถูกแจ้งเตือน วันและเวลาที่แพ็กเก็ตแรกและสุดท้ายที่ถูกตรวจจับ ซึ่งจะแสดง 15 รายการล่าสุดที่ถูกตรวจจับ ดังรูป



Unique TCP Destination Port (s): 15 Last Ports

[Home](#)

[\[Back \]](#)

Added 0 alerts to the Alert cache

Queried DB on Tue March 06, 2007 15:01:48

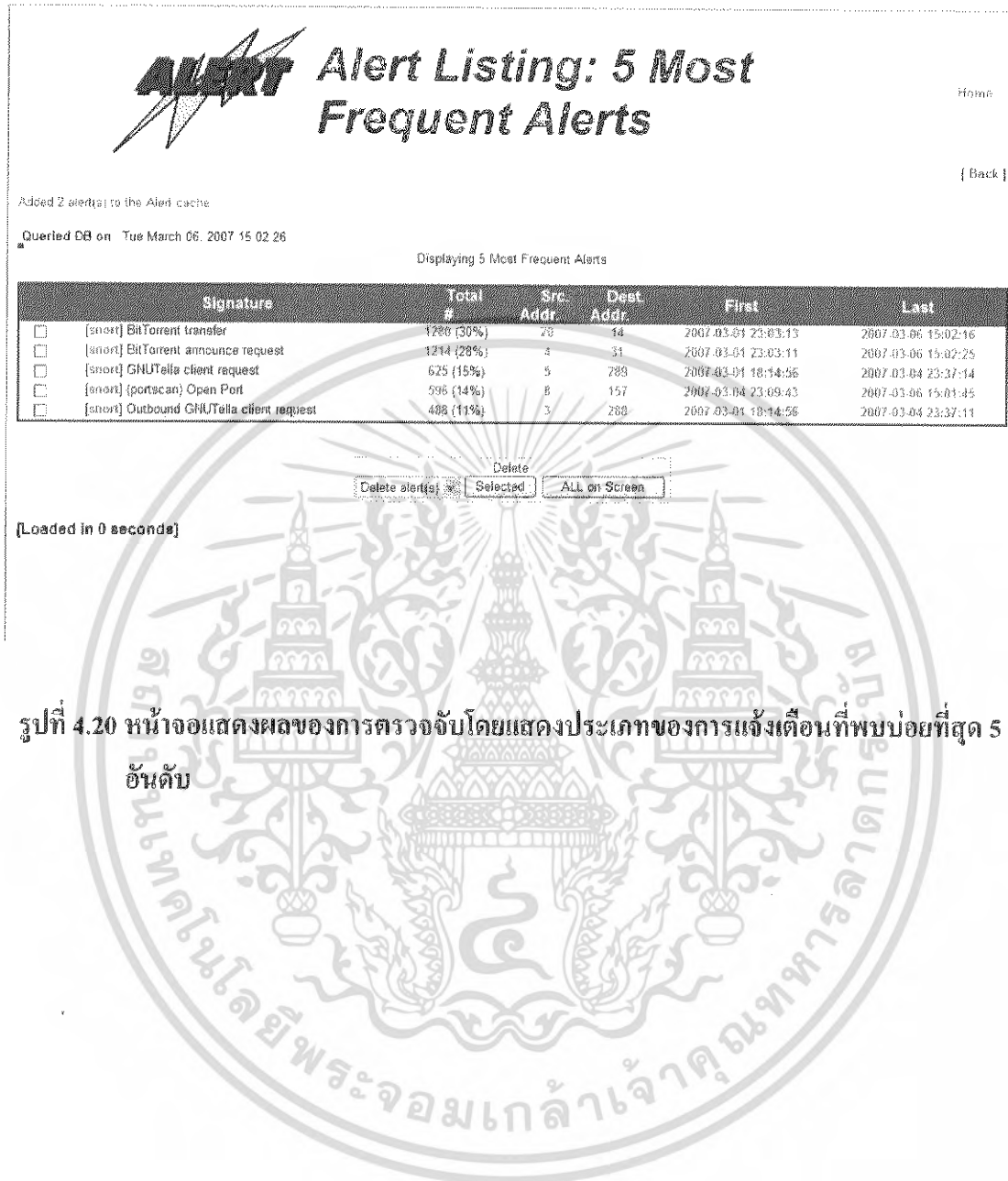
Displaying 15 Last Ports

Port	Occurrences	Unique Alerts	Source IP	Dest. IP	First	Last
37337 / tcp	348	1	3	4	2007-03-01 23:03:22	2007-03-06 15:01:48
80 / tcp	643	1	4	16	2007-03-01 23:03:11	2007-03-06 15:01:44
2719 / tcp	271	1	3	3	2007-03-01 23:03:11	2007-03-06 15:00:03
8006 / tcp	61	1	3	6	2007-03-01 23:03:18	2007-03-06 15:00:01
8088 / tcp	33	1	3	1	2007-03-01 23:03:20	2007-03-06 14:59:44
9999 / tcp	22	1	2	1	2007-03-01 23:03:18	2007-03-06 14:59:43
16737 / tcp	992	1	17	3	2007-03-01 23:03:13	2007-03-06 14:58:20
98 / tcp	142	1	1	1	2007-03-02 00:25:01	2007-03-06 14:49:58
8080 / tcp	22	1	3	5	2007-03-01 23:03:16	2007-03-06 14:48:18
6969 / tcp	15	1	3	3	2007-03-01 23:03:15	2007-03-06 14:40:41
32459 / tcp	5	1	1	1	2007-03-05 20:44:04	2007-03-05 20:44:49
49366 / tcp	189	1	1	1	2007-03-04 23:03:24	2007-03-05 01:20:52
1258 / tcp	1	1	1	1	2007-03-05 01:07:38	2007-03-05 01:07:38
2646 / tcp	1	1	1	1	2007-03-05 00:53:16	2007-03-05 00:53:16
3079 / tcp	2	1	1	1	2007-03-05 00:37:29	2007-03-06 00:30:17

[Loaded in 1 seconds]

รูปที่ 4.19 หน้าจอแสดงผลของการตรวจจับโดยแสดงถึง 15 รายการล่าสุดที่พอร์ตปลายทางถูกแจ้งเตือน

ระบบสามารถแสดงผลของการตรวจจับ โดยแสดงประเภทของการแจ้งเตือนที่ตรวจจับ พบบ่อยที่สุด 5 อันดับ ดังรูป



ALERT Alert Listing: 5 Most Frequent Alerts

Home

[Back]

Added 2 alert(s) to the Alert cache

Queried DB on Tue March 06, 2007 15:02:26

Displaying 5 Most Frequent Alerts

	Signature	Total #	Src. Addr.	Dest. Addr.	First	Last
<input type="checkbox"/>	[short] BitTorrent transfer	1288 (30%)	29	14	2007-03-01 23:03:13	2007-03-06 15:02:16
<input type="checkbox"/>	[short] BitTorrent announce request	1214 (28%)	4	31	2007-03-01 23:03:11	2007-03-06 15:02:25
<input type="checkbox"/>	[short] GNUTella client request	625 (15%)	5	789	2007-03-01 18:14:56	2007-03-04 23:37:14
<input type="checkbox"/>	[short] (portscan) Open Port	596 (14%)	8	157	2007-03-04 23:09:43	2007-03-06 15:01:45
<input type="checkbox"/>	[short] Outbound GNUTella client request	488 (11%)	3	268	2007-03-01 18:14:56	2007-03-04 23:37:11

Delete


Delete alert(s): Selected ALL on Screen

[Loaded in 0 seconds]

รูปที่ 4.20 หน้าจอแสดงผลของการตรวจจับโดยแสดงประเภทของการแจ้งเตือนที่พบบ่อยที่สุด 5 อันดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับโดยแสดงหมายเลขพอร์ตของต้นทางที่ถูกแจ้งเดือนบ่อยที่สุด 15 อันดับ ดังรูป



Unique TCP Source Port(s): 15 Most Frequent Ports

Home

[Back]

Added 1 alert(s) to the Alert cache

Queried DB on Tue March 06 2007 15:03:06

Displaying 15 Most Frequent Ports


Port	Occurrences	Unique Alerts	Source IP	Dest IP	First	Last
10737 / tcp	21	1	2	6	2007-03-02 00:27:09	2007-03-05 01:07:38
2305 / tcp	14	2	2	2	2007-03-01 18:26:46	2007-03-04 23:25:31
1243 / tcp	12	3	2	2	2007-03-01 22:33:08	2007-03-02 00:29:40
2130 / tcp	11	3	2	2	2007-03-01 19:24:16	2007-03-05 01:20:34
1223 / tcp	11	1	3	3	2007-03-01 22:32:45	2007-03-05 00:58:25
1202 / tcp	11	2	2	2	2007-03-01 22:32:24	2007-03-04 23:07:27
1252 / tcp	11	3	2	2	2007-03-01 22:33:16	2007-03-05 00:59:00
3219 / tcp	11	1	1	1	2007-03-02 00:16:41	2007-03-02 00:18:16
2645 / tcp	10	2	2	2	2007-03-02 01:17:51	2007-03-05 01:18:50
2649 / tcp	10	3	2	2	2007-03-01 18:29:16	2007-03-04 23:05:27
1188 / tcp	10	2	2	2	2007-03-01 22:32:13	2007-03-04 23:07:24
1295 / tcp	10	2	1	1	2007-03-04 23:08:02	2007-03-04 23:09:32
1113 / tcp	10	7	1	1	2007-03-01 22:30:44	2007-03-01 22:31:29
3969 / tcp	10	1	2	2	2007-03-02 00:40:02	2007-03-02 00:42:39
1219 / tcp	10	3	2	3	2007-03-01 22:32:40	2007-03-05 00:58:34

[Loaded in 0 seconds]

รูปที่ 4.21 หน้าจอแสดงผลของการตรวจจับโดยแสดงหมายเลขพอร์ตของต้นทางที่ถูกแจ้งเดือนบ่อยที่สุด 15 อันดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลของการตรวจจับโดยแสดงหมายเลขพอร์ตของปลายทางที่ถูก
แจ้งเตือนบ่อยที่สุด 15 อันดับ ดังรูป



Unique TCP Destination Port (s): 15 Most Frequent Ports

Name

[\[Back \]](#)

Added 1 alert(s) to the Alert cache

Queried DB on Tue March 06, 2007 15:03:41

Displaying 15 Most Frequent Ports

Port	Occurrences	Unique Alerts	Source IP	Dest. IP	First	Last
80 / tcp	648	1	4	16	2007-03-01 23:03:11	2007-03-06 15:03:26
6246 / tcp	641	2	3	166	2007-03-01 18:18:37	2007-03-04 23:37:14
18737 / tcp	597	1	17	3	2007-03-01 23:03:13	2007-03-06 15:03:15
37332 / tcp	355	1	3	4	2007-03-01 23:03:22	2007-03-06 15:03:40
2746 / tcp	273	1	3	3	2007-03-01 23:03:11	2007-03-06 15:00:03
49366 / tcp	188	1	1	1	2007-03-04 23:03:24	2007-03-05 01:20:52
98 / tcp	142	1	3	1	2007-03-02 00:25:04	2007-03-06 14:49:58
36967 / tcp	66	1	1	1	2007-03-02 00:25:04	2007-03-02 01:18:20
8009 / tcp	61	1	3	6	2007-03-01 23:03:18	2007-03-06 15:00:01
11795 / tcp	50	1	1	1	2007-03-04 23:03:25	2007-03-04 23:40:56
4242 / tcp	46	1	2	2	2007-03-01 18:16:26	2007-03-02 00:23:18
3088 / tcp	33	1	3	1	2007-03-01 23:03:20	2007-03-06 14:59:44
8080 / tcp	22	1	3	8	2007-05-01 23:03:16	2007-03-06 14:48:18
9999 / tcp	22	1	3	1	2007-03-01 23:03:18	2007-03-06 14:59:43
42771 / tcp	22	2	3	1	2007-03-01 18:14:56	2007-03-04 23:28:47

[Loaded in 0 seconds]

รูปที่ 4.22 หน้าจอแสดงผลของการตรวจจับโดยแสดงหมายเลขพอร์ตของปลายทางที่ถูกแจ้งเตือนบ่อยที่สุด 15 อันดับ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถทำการลบบันทึกรายการได้จากช่องแอ็คชัน (Action) ซึ่งสามารถเลือกได้ว่าจะลบรายการที่เลือกไว้ หรือรายการที่ปรากฏบนหน้าจอ หรือรายการที่ได้มาจากการดึงข้อมูลนี้ ดังรูป

The screenshot displays a web browser window showing a table of BitTorrent transfer records. The table has several columns, including an ID column with checkboxes, an 'Action' column, a date column, and numerical data columns. Below the table, there are navigation and control buttons: 'Delete alert(s)', 'Selected', 'Delete ALL on Session', and 'Entire Query'. The page title is 'Query Results' and it indicates 'Loaded in 1 seconds'.

ID	Action	Date	Value 1	Value 2
<input type="checkbox"/> 1019 (3-24756)	[ลบ] BitTorrent transfer	2007-03-07 00:15:59	161,246,11,93:2286	38,100,25,178:35483
<input type="checkbox"/> 1020 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:01	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1021 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:01	161,246,11,93:2286	38,100,25,178:35483
<input type="checkbox"/> 1022 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:04	161,246,11,93:2286	34,162,198,00:18334
<input type="checkbox"/> 1023 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:05	81,101,11,17:61584	161,246,11,93:24902
<input type="checkbox"/> 1024 (3-24755)	[ลบ] BitTorrent transfer	2007-03-07 00:16:05	161,246,11,93:2272	39,132,37,116:39500
<input type="checkbox"/> 1025 (3-24756)	[ลบ] BitTorrent transfer	2007-03-07 00:16:07	81,101,11,17:62965	161,246,11,93:24902
<input type="checkbox"/> 1026 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:07	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1027 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:07	161,246,11,93:2274	39,132,37,116:39500
<input type="checkbox"/> 1028 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:07	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1029 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:07	161,246,11,93:2274	39,132,37,116:39500
<input type="checkbox"/> 1030 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:08	161,246,11,93:2273	38,100,25,178:35483
<input type="checkbox"/> 1031 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:12	82,101,11,17:61584	161,246,11,93:24902
<input type="checkbox"/> 1032 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:12	71,99,198,00:60483	161,246,11,93:24902
<input type="checkbox"/> 1033 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:12	71,99,198,00:62965	161,246,11,93:24902
<input type="checkbox"/> 1034 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:14	87,101,11,17:61584	161,246,11,93:24902
<input type="checkbox"/> 1035 (3-24756)	[ลบ] BitTorrent transfer	2007-03-07 00:16:15	71,245,98,00:62965	161,246,11,93:24902
<input type="checkbox"/> 1036 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:15	38,100,25,16:61514	161,246,11,93:24902
<input type="checkbox"/> 1037 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:18	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1038 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:20	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1039 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:23	161,246,11,93:2303	39,132,37,116:39500
<input type="checkbox"/> 1040 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:23	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1041 (3-24753)	[ลบ] BitTorrent transfer	2007-03-07 00:16:25	161,246,11,93:2309	38,100,25,178:35483
<input type="checkbox"/> 1042 (3-24773)	[ลบ] BitTorrent transfer	2007-03-07 00:16:25	199,198,00:62965	199,198,00:62965
<input type="checkbox"/> 1043 (3-24773)	[ลบ] BitTorrent transfer	2007-03-07 00:16:28	87,101,11,17:61584	161,246,11,93:24902
<input type="checkbox"/> 1044 (3-24773)	[ลบ] BitTorrent transfer	2007-03-07 00:16:28	161,246,11,93:2309	38,100,25,178:35483
<input type="checkbox"/> 1045 (3-24773)	[ลบ] BitTorrent transfer	2007-03-07 00:16:28	62,224,1,169:4322	161,246,11,93:24902
<input type="checkbox"/> 1046 (3-24773)	[ลบ] BitTorrent transfer	2007-03-07 00:16:28	199,198,00:60152	161,246,11,93:24902
<input type="checkbox"/> 1047 (3-24773)	[ลบ] BitTorrent transfer	2007-03-07 00:16:28	161,246,11,93:2286	34,162,198,00:18334
<input type="checkbox"/> 1048 (3-24775)	[ลบ] BitTorrent transfer	2007-03-07 00:16:29	161,246,11,93:2286	38,100,25,187:45779
<input type="checkbox"/> 1049 (3-24780)	[ลบ] BitTorrent transfer	2007-03-07 00:16:31	62,224,1,169:4322	161,246,11,93:24902

รูปที่ 4.23 หน้าจอแสดงการลบบันทึกรายการของแพ็กเก็ต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ระบบสามารถแสดงผลเป็นรายละเอียดเหตุการณ์ของแพ็กเก็ตที่ได้มา โดยจะแสดงรายละเอียดของแพ็กเก็ตนั้นด้วย เช่น เวลาที่แพ็กเก็ตผ่านเข้ามา ซิกเนเจอร์ (Signature) ไอพีต้นทาง และไอพีปลายทาง เป็นต้น

Alert

Queried DB on Tue March 06, 2007 15:06:50
Added 0 alert(s) to the Alert cache

Alert #6
<< Previous #5 (1-1807) >> Next #6 (1-1805)

ID #	Time	Triggered Signature
2 - 478	2007-03-05 15:04:32	[none] BitTorrent announce request

Source	name	interface	filter
localhost.localdomain	eth0	eth0	none

Alert Group: none

source addr	dest addr	Ver	dir	Len	TOS	length	ID	flags	ttl	ttl_remain
151.246.11.96	205.234.39.10	4	S	5	0	500	61767	0	0	128 51564

Source Name	Dest Name
richy.crc.kmit.ac.th	server.ufsok.com

Options: none

source port	dest port	R	R	U	R	A	R	C	R	S	R	T	seq #	ack	offset	res	window	urg	chksum
761	80												3769230775	3138568460	5	0	17520	0	46524

Options: none

length = 465

```

000 47 45 54 20 2F 74 72 61 63 68 65 72 2F 61 6E 6E GET /tracker/ann
010 6F 78 6E 53 65 2E 70 68 70 3F 69 62 66 6F 5F 68 ounce.php?info=
020 61 73 60 3D 25 42 36 26 37 42 25 41 41 25 42 35 ash*H6C279LAAZ95
030 25 38 37 25 41 38 25 38 44 25 3D 41 25 45 39 63 %87%48%2B%4A%2B%
040 25 38 42 25 42 38 25 32 32 25 43 44 25 41 33 25 205B%42%2D%33%
050 43 3D 25 43 37 45 69 25 45 4E 26 70 65 65 72 5F CB%27%1%2E%2E%
060 69 64 3D 25 32 44 42 43 3D 3D 37 3D 25 3E 44 4D id=%2F%6C%07%2D%2D
070 25 44 42 25 43 41 25 3D 45 43 41 25 35 43 25 46 %B%6A%6C%6A%6C%6E
080 45 3D 25 42 3D 25 3D 44 45 2D 7D 6F 72 74 3D 31 5E%4B%4D%4E%41
090 3D 37 35 37 26 6E 61 74 6D 61 7D 70 65 64 3D 31 0737&atmapped=1
0a0 25 6F 6F 63 61 6C 69 7D 3D 31 32 37 2E 3D 2E 3D &localip=127.0.0.1
0b0 2E 31 26 75 7D 6F 61 64 65 64 3D 3D 26 6C 6C 66 74 3D %sloaded%&do
0c0 72 6E 6C 6F 61 64 65 64 3D 3D 26 6C 6C 66 74 3D &loaded=0&left=
0d0 39 36 32 35 32 36 35 36 65 75 6D 77 63 6E 74 3D %2E265&navent=
0e0 32 3D 3E 26 63 6F 6D 7D 61 67 74 3D 31 25 6E 5F 200&compete=&no
0f0 5F 7D 65 65 72 5F 69 64 3D 31 26 6B 65 79 3D 32 %serv_id%&serv=1
100 39 36 37 31 26 65 76 65 6E 74 2D 73 74 61 72 74 %57%&event=stat
110 65 64 2D 48 54 54 5D 2F 31 2E 31 0D 04 41 63 63 md HTTP/1.1 Acc
120 65 7D 74 3A 2D 2A 2F 2A 6D 0A 41 63 63 65 7D 74 mp: see: scope
130 2D 45 6E 61 6F 64 69 6E 67 3A 2D 67 7A 69 7D 0D -Encoding: gzip
140 04 43 6F 6E 65 63 74 69 6F 6E 3A 2D 63 6C 6F -Connection: clo
150 75 65 6D 0A 40 6F 73 74 3D 77 77 77 2E 61 6D ee: Host: www.af
160 60 69 6C 69 61 74 68 6E 6E 54 66 7D 6F 74 2E 6E file: /codepot.o
170 65 74 3A 3D 3D 0D 0A 65 73 65 72 2D 41 67 65 6E ot: 80 User-Agent:
180 74 3A 2D 4D 6F 7A 68 6C 6C 61 2F 34 2E 3D 2D 2D ct: Accept: */*
190 63 6F 6D 7D 61 74 65 62 6C 65 3D 3D 4D 53 49 4E compatible: MSN
1a0 2D 36 2E 3D 3D 2D 57 69 6E 64 6F 77 73 2D 4E 54 6.0; Windows NT
1b0 2D 35 2E 3D 3D 2D 4E 45 54 2D 43 4C 52 2D 51 5.0; NET CLR 1
1c0 2E 31 2E 14 33 37 32 29 0A 0D 0A

```

<< Previous #5 (1-1807) >> Next #6 (1-1805)

Delete
Delete alert(s): Selected

[Loaded in 0 seconds]

รูปที่ 4.24 หน้าจอแสดงรูปแบบของแพ็กเก็ต และ รายละเอียดที่มากับแพ็กเก็ต

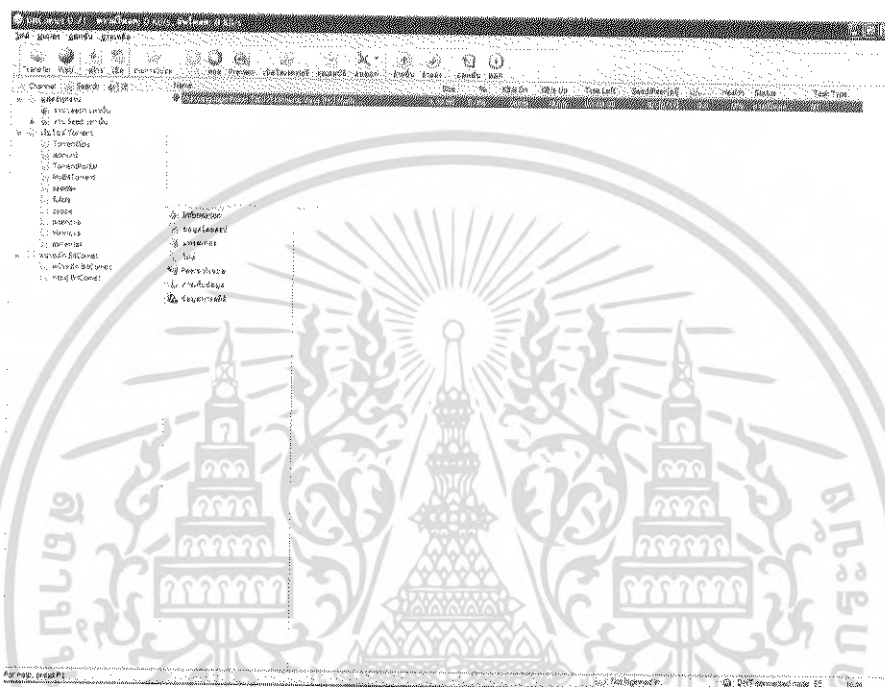
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.4 การทดสอบระบบ

การทดสอบโปรแกรมเราจะใช้โปรแกรมบิทโคเมท เวอร์ชัน 0.72 แชนด์พีทูพี (ZP2P) และอีมูลส์ (eMule) ซึ่งเป็นโปรแกรมแลกเปลี่ยนไฟล์ (File-Sharing) ผ่านโปรโตคอลบิททอร์เรนท์ จินูเทลล่า และอีตอว์นก็

4.4.1 การทดสอบกับโปรโตคอลบิททอร์เรนท์โดยใช้โปรแกรมบิทโคเมท

โดยเราจะทำการโหลดไฟล์ผ่านโปรแกรมบิทโคเมท ดังรูป



รูปที่ 4.25 หน้าจอแสดงการโหลดไฟล์ผ่านโปรแกรมบิทโคเมท

ซึ่งการโหลดไฟล์ผ่านโปรแกรมบิทโคเมทนั้นจะเป็นการใช้งาน โปรโตคอลบิททอร์เรนท์ ซึ่งระบบของเราจะทำการตรวจจับได้ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



Query Results

Added
0 alerts to the Alert cache

Home Back

Displaying alerts 1-50 of 1437 total

ID	Signature	Date	Source Address	Dest Address
80 (1-583)	[alert] BitTorrent transfer	2007-03-12 15:33:10	161.246.11.96:2676	84.203.141.93:83670
81 (1-125)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2710	60.190.113.205:80
82 (1-124)	[alert] BitTorrent transfer	2007-03-12 14:51:22	161.246.11.96:2676	194.186.192.129:30067
83 (1-121)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2696	193.138.230.239:2710
84 (1-122)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2702	212.227.167.119:8000
85 (1-123)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2693	218.93.246.254:8000
86 (1-119)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2604	193.138.230.239:2710
87 (1-117)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2603	193.138.230.239:2710
88 (1-120)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2694	193.138.230.239:2710
89 (1-118)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2656	193.138.230.239:2710
90 (1-115)	[alert] BitTorrent announce request	2007-03-12 14:51:22	161.246.11.96:2705	85.17.40.40:80
91 (1-115)	[alert] BitTorrent transfer	2007-03-12 14:51:21	161.246.11.96:2680	80.139.40.30:52743
92 (1-114)	[alert] BitTorrent announce request	2007-03-12 14:51:21	161.246.11.96:2674	86.191.39.63:60500
93 (1-113)	[alert] BitTorrent transfer	2007-03-12 14:51:21	161.246.11.96:2676	24.66.22.195:30544
94 (1-112)	[alert] BitTorrent transfer	2007-03-12 14:51:21	161.246.11.96:2676	85.218.161.96:65000
95 (1-111)	[alert] BitTorrent announce request	2007-03-12 14:51:20	161.246.11.96:2696	218.93.246.254:8000
96 (1-110)	[alert] BitTorrent announce request	2007-03-12 14:51:20	161.246.11.96:2672	85.17.40.40:80
97 (1-109)	[alert] BitTorrent announce request	2007-03-12 14:51:20	161.246.11.96:2670	212.227.167.119:8000
98 (1-107)	[alert] BitTorrent announce request	2007-03-12 14:51:17	161.246.11.96:2682	60.190.113.205:80
99 (1-108)	[alert] BitTorrent announce request	2007-03-12 14:51:20	161.246.11.96:2667	193.138.230.239:2710
100 (1-102)	[alert] BitTorrent transfer	2007-03-12 14:51:15	161.246.11.96:2607	89.233.228.87:65535
101 (1-103)	[alert] BitTorrent transfer	2007-03-12 14:51:15	161.246.11.96:2606	201.258.113.128:47785
102 (1-106)	[alert] BitTorrent transfer	2007-03-12 14:51:17	161.246.11.96:2603	82.81.111.213:19418
103 (1-105)	[alert] BitTorrent announce request	2007-03-12 14:51:16	161.246.11.96:2620	85.17.40.40:80
104 (1-104)	[alert] BitTorrent transfer	2007-03-12 14:51:15	161.246.11.96:2608	218.230.239.239:65535
105 (1-101)	[alert] BitTorrent transfer	2007-03-12 14:51:15	161.246.11.96:2606	60.233.93.171:8106
106 (1-100)	[alert] BitTorrent transfer	2007-03-12 14:51:15	161.246.11.96:2604	188.157.265.102:42934
107 (1-99)	[alert] BitTorrent announce request	2007-03-12 14:51:08	161.246.11.96:2526	85.17.40.40:80
108 (1-96)	[alert] BitTorrent transfer	2007-03-12 14:51:05	161.246.11.96:2603	87.61.111.713:19418
109 (1-97)	[alert] BitTorrent announce request	2007-03-12 14:51:04	161.246.11.96:2620	60.190.113.98
110 (1-98)	[alert] BitTorrent announce request	2007-03-12 14:51:03	161.246.11.96:2610	193.138.230.239:2710
111 (1-95)	[alert] BitTorrent announce request	2007-03-12 14:51:03	161.246.11.96:2617	193.138.230.239:2710
112 (1-94)	[alert] BitTorrent announce request	2007-03-12 14:51:03	161.246.11.96:2618	193.138.230.239:2710
113 (1-95)	[alert] BitTorrent announce request	2007-03-12 14:51:03	161.246.11.96:2603	218.230.239.239:65535
114 (1-92)	[alert] BitTorrent transfer	2007-03-12 14:51:03	161.246.11.96:2616	193.138.230.239:2710
115 (1-87)	[alert] BitTorrent transfer	2007-03-12 14:51:03	161.246.11.96:2604	188.157.265.102:42934
116 (1-88)	[alert] BitTorrent transfer	2007-03-12 14:51:03	161.246.11.96:2605	89.233.228.87:65535
117 (1-89)	[alert] BitTorrent transfer	2007-03-12 14:51:03	161.246.11.96:2607	89.233.228.87:65535
118 (1-90)	[alert] BitTorrent transfer	2007-03-12 14:51:03	161.246.11.96:2606	201.258.113.128:47785
119 (1-85)	[alert] BitTorrent transfer	2007-03-12 14:50:59	161.246.11.96:2603	82.81.111.213:19418
120 (1-80)	[alert] BitTorrent announce request	2007-03-12 14:51:09	161.246.11.96:2622	85.17.40.40:80
121 (1-82)	[alert] BitTorrent announce request	2007-03-12 14:50:57	161.246.11.96:2619	193.138.230.239:2710
122 (1-83)	[alert] BitTorrent announce request	2007-03-12 14:50:57	161.246.11.96:2610	193.138.230.239:2710
123 (1-84)	[alert] BitTorrent announce request	2007-03-12 14:50:58	161.246.11.96:2620	85.17.40.40:80
124 (1-81)	[alert] BitTorrent announce request	2007-03-12 14:50:57	161.246.11.96:2617	193.138.230.239:2710
125 (1-82)	[alert] BitTorrent transfer	2007-03-12 14:50:57	161.246.11.96:2618	193.138.230.239:2710
126 (1-77)	[alert] BitTorrent transfer	2007-03-12 14:50:57	161.246.11.96:2606	218.230.239.239:65535
127 (1-78)	[alert] BitTorrent announce request	2007-03-12 14:50:57	161.246.11.96:2654	60.190.113.205:80
128 (1-79)	[alert] BitTorrent announce request	2007-03-12 14:50:57	161.246.11.96:2616	193.138.230.239:2710

Query Results

1 2 3 4 5 >>

Delete

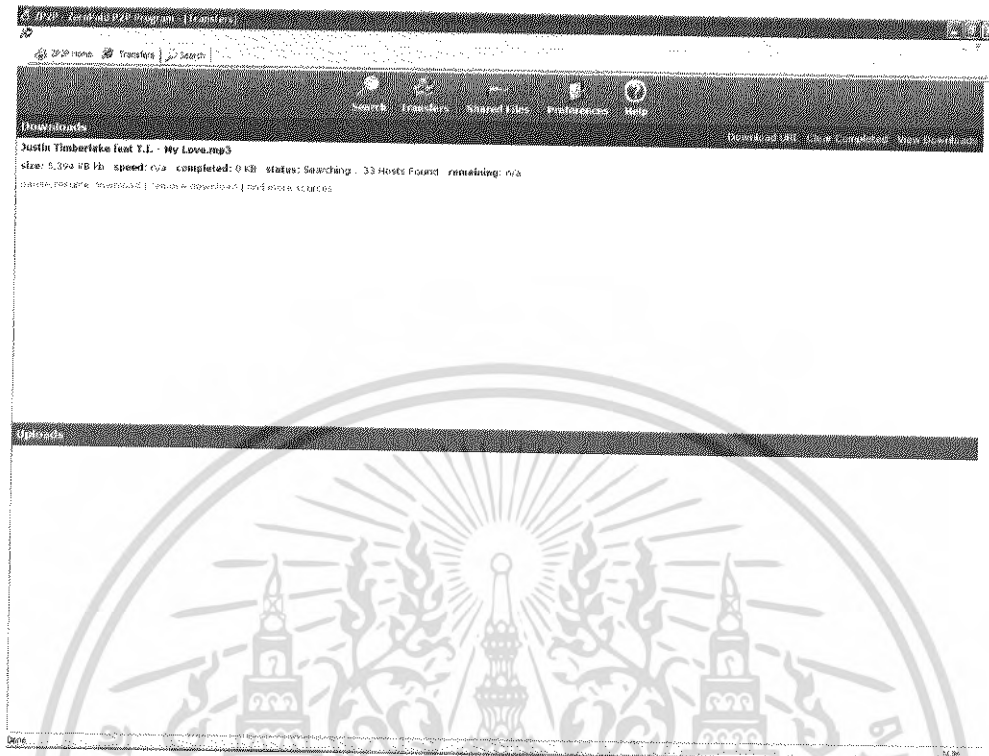
Delete alerts: Selected All on Screen Entire Query

[Loaded in 1 seconds]

รูปที่ 4.26 หน้าจอแสดงผลของโปรแกรมที่ได้หลังจากการโหลดไฟล์ผ่านโปรแกรมมิดคอมเท

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

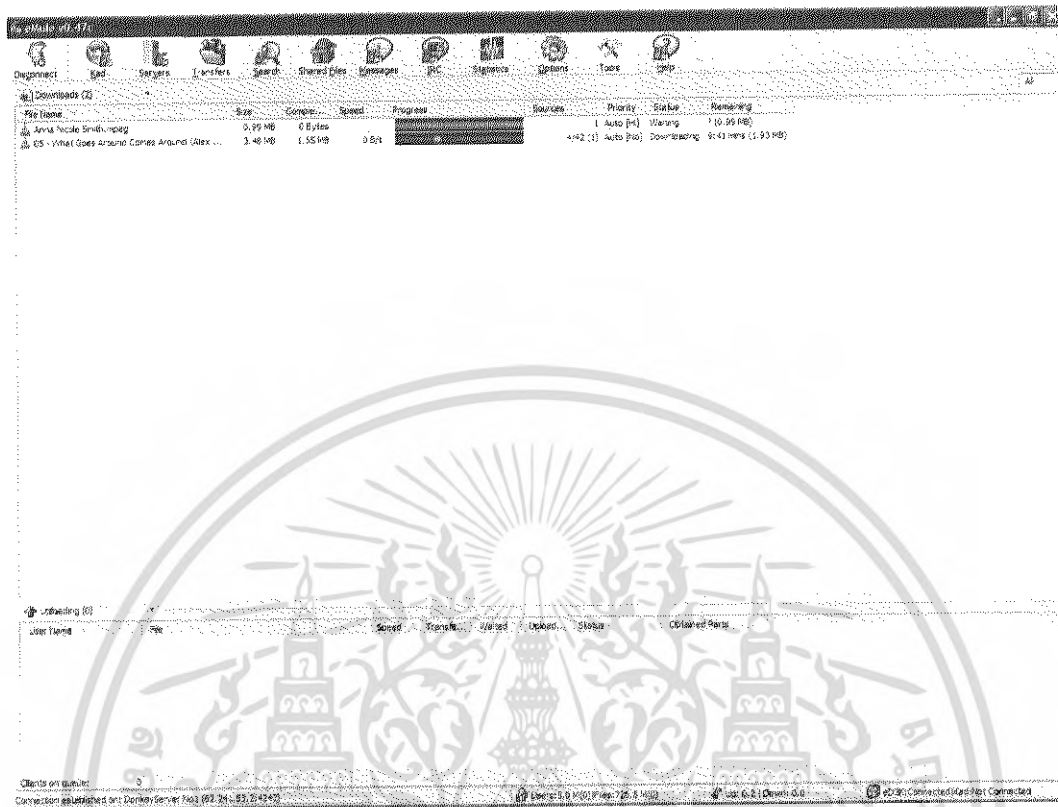
4.4.2 การทดสอบกับโปรโตคอลสัญญาณต่ำโดยใช้โปรแกรมเซดพิทูพี โดยทำการ โหลดไฟล์ด้วยโปรแกรมเซดพิทูพี ดังรูป



รูปที่ 4.27 หน้าจอแสดงการโหลดไฟล์ผ่านโปรแกรมเซดพิทูพี
ซึ่งการโหลดไฟล์ผ่านโปรแกรมเซดพิทูพีนั้นจะเป็นการใช้งานโปรโตคอลสัญญาณต่ำซึ่ง
ระบบของเราจะทำการตรวจจับได้ ดังรูป

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.4.3 การทดสอบกับโปรโตคอลอื่นที่โดยใช้โปรแกรมอีมูเลต โดยเราจะทำการ โหลดไฟล์ผ่าน โปรแกรมอีมูเลต ดังรูป



รูปที่ 4.29 หน้าจอแสดงการโหลดไฟล์ผ่านโปรแกรมอีมูเลต

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โดยรายชื่อแพ็คเกจที่พบทั้งหมด แสดงได้ดังนี้

- BitTorrent announce request
- BitTorrent transfer
- Outbound GNUTella client request
- GNUTella client request
- cDonkey transfer

4.5 สรุปผลการทำงาน

จากการทดลองข้างต้นทำให้เราทราบได้ว่าเครื่องคอมพิวเตอร์ถูกข่ายเครื่องไหนที่ทำการใช้การสื่อสารแบบพีียร์ทูพีียร์ ใช้ผ่านโปรโตคอลไหน และใช้เมื่อเวลาเท่าไร ซึ่งเราสามารถนำข้อมูลที่ได้มาพิจารณาเพื่อทำการจำกัดการสื่อสารเครื่องคอมพิวเตอร์ถูกข่าย ซึ่งระบบนี้สามารถนำไปพัฒนาต่อในส่วนของการจำกัดการใช้งานเครือข่ายเพิ่มเติมเพื่อให้ผู้ดูแลระบบสามารถจำกัดการใช้งานได้ในระบบเดียวเลย



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 สรุปผลปัญหาพิเศษ

การดำเนินงานตามปัญหาพิเศษนี้มีวัตถุประสงค์คือ ต้องการตรวจจับแพ็กเก็ตที่เป็นโปรโตคอลเพียร์ทูเพียร์ คือ โปรโตคอลบิททอว์เรนท อีคอนกี้ และจีนูเทลล่า เนื่องจากการสื่อสารประเภทนี้ใช้แบนด์วิธมาก และสามารถแจ้งเตือนไปยังผู้ดูแลระบบเมื่อเครื่องลูกข่ายใช้การสื่อสารแบบเพียร์ทูเพียร์ โดยสามารถแสดงถึงข้อมูลการใช้งานต่างๆของเครื่องลูกข่ายที่อยู่ในระบบได้โดยจะรันโปรแกรมอยู่ตลอดเวลา

จากการศึกษาปัญหาพิเศษการพัฒนาาระบบเพื่อป้องกันการสื่อสารแบบเพียร์ทูเพียร์โดยใช้โปรแกรมโอเพนซอร์ซที่รันบนระบบปฏิบัติการลินุกซ์นั้น ระบบมีความสามารถดังนี้

1. สามารถตรวจจับแพ็กเก็ตต่างๆที่เป็นของโปรโตคอลเพียร์ทูเพียร์
2. สามารถแจ้งเตือน(alert) ให้กับผู้ควบคุมและดูแลระบบ เมื่อระบบมีการใช้การสื่อสารแบบเพียร์ทูเพียร์
3. สามารถแสดงข้อมูลการใช้งานของเครื่องลูกข่ายต่างๆที่อยู่ภายในระบบเมื่อใช้การสื่อสารแบบเพียร์ทูเพียร์กับเครื่องอื่นๆที่อยู่ทั้งภายในและภายนอกของระบบ

ระบบที่ทางคณะผู้จัดทำพัฒนาขึ้นนั้นมีข้อดีกว่าระบบอื่นๆคือ มีความยืดหยุ่นกว่า สามารถปรับเปลี่ยนรูปแบบการตรวจจับ(update)ให้ทันกับซิกเนเจอร์ของโปรโตคอลเพียร์ทูเพียร์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา และเป็นระบบที่พัฒนามาจากโอเพนซอร์ซเสียค่าใช้จ่ายในการพัฒนาน้อย

5.2 ข้อจำกัดปัญหาพิเศษ

ปัญหาพิเศษการพัฒนาาระบบเพื่อจำกัดการสื่อสารแบบเพียร์ทูเพียร์นั้นยังมีข้อจำกัดในการทำงานอยู่คือ การทำงานของระบบ ระบบยังไม่สามารถที่จะตรวจจับโปรโตคอลเพียร์ทูเพียร์ได้ครอบคลุมทุกชนิดเนื่องจากโปรโตคอลเพียร์ทูเพียร์มีการแก้ไขตัวเองอยู่เสมอเพื่อไม่ให้ระบบสามารถตรวจจับโปรโตคอลเพียร์ทูเพียร์ของตนได้ และไม่สามารถที่จะทำลายการสื่อสารแบบเพียร์ทูเพียร์ที่เกิดขึ้นในระบบออกไปได้ ทำได้แค่เพียงตรวจจับและแจ้งเตือนไปยังผู้ควบคุมและดูแลระบบ อีกทั้งการสื่อสารแบบเพียร์ทูเพียร์มักจะมาพร้อมกับแอดแวร์, สปายแวร์ และไวรัส ซึ่งระบบทำได้แค่เพียงแจ้งเตือนผู้ควบคุมและดูแลระบบ แต่ไม่สามารถที่จะทำลายสิ่งเหล่านั้นได้

5.3 ข้อเสนอแนะและแนวทางการศึกษาต่อ

เนื่องจากมีข้อจำกัดบางประการ ฉะนั้นระบบควรมีความสามารถดังนี้

1. ระบบควรมีความสามารถในการตรวจจับโปรโตคอลเพิร์ทูเพียร์ได้ครอบคลุมทุกชนิด โดยการจับแพ็คเก็ตของเพิร์ทูเพียร์มาวิเคราะห์หาสิ่งที่เป็นจุดเด่นของโปรโตคอลชนิดต่างๆอยู่เสมอ เพื่อนำมาเขียนกฎในระบบไอดีเอสและเป็นการอัปเดตกฎให้มีความทันสมัยอยู่เสมอ
2. ระบบควรมีความสามารถในการหยุดการสื่อสารแบบเพิร์ทูเพียร์ออกไปจากระบบได้โดยทำงานร่วมกับไฟร์วอลล์โดยบล็อกไอพีแอดเดรสที่มีการสื่อสารแบบเพิร์ทูเพียร์
3. ระบบควรมีความสามารถในการกำจัดพวกแอดแวร์, สปายแวร์ และไวรัส โดยสามารถทำงานร่วมกับโปรแกรมแอนติไวรัสได้(anti-virus)



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

หนังสือ

- [1] ประภาพร ช่างไม้, “Linux redhat ฉบับผู้เริ่มต้น” , Info Press , 2547
- [2] ก่อกิจ วีระอาชากุล, “ติดตั้งและปรับแต่งเซิร์ฟเวอร์ Linux สำหรับ Admin Linux โดยเฉพาะ” , Info Press , 2546
- [3] Rafeeq Rehman , “Intrusion Detection with SNORT” , Prentice Hall PTR , 2546
- [4] สมประสงค์ ชิตินิลนิต, “เรียนลัด PHP 4 : ครอบคลุมเวอร์ชัน 4.2” , โปรวิชั่น จำกัด, 2547
- [5] ณัฐพล เหลืองวัฒนไพศาล พรชัย ประสิทธิ์สุวรรณ และพิริยะ อรรถทวีสิน . 2547. “ระบบตรวจจับผู้บุกรุกบนเครือข่ายคอมพิวเตอร์ขนาดเล็ก.” วิทยานิพนธ์วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

บทความ

- [1] ภูวศล ตำนระหาญ , “การติดตั้ง Snort ร่วมกับ ACID (+MySQL)”, <http://www.thaicert.nectec.or.th/paper/ids/snort2.php>, เผยแพร่เมื่อ : 3 สิงหาคม 2544
- [2] Subhabrata Sen, Oliver Spatscheck, Dongmei Wang, “Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures”, [http:// etd.lib.nsysu.edu.tw/ETD-db/ETD-search/getfile?URN=etd-0706105-135129&filename=etd-0706105-135129.pdf](http://etd.lib.nsysu.edu.tw/ETD-db/ETD-search/getfile?URN=etd-0706105-135129&filename=etd-0706105-135129.pdf)

เว็บไซต์ที่เกี่ยวข้อง

- [1] <http://www.snort.org>
- [2] <http://www.thaicert.nectec.or.th>
- [3] <http://acidlab.sourceforge.net/>
- [4] <http://www.php.net>
- [5] <http://www.w3schools.com/>
- [6] <http://www.google.co.th>

ภาคผนวก

1. คู่มือการติดตั้งโปรแกรม

1.1 การติดตั้ง Httpd (Web server)

เปิดโปรแกรม Terminal และใช้คำสั่งดังต่อไปนี้

```
tar -zxvf httpd-2.2.4 -C /usr/local/
```

```
cd /usr/local/httpd-2.2.4
```

```
./configure
```

```
make
```

```
make install
```

- เพื่อตรวจสอบการทำงานของ Httpd ควรเรียกใช้คำสั่งดังต่อไปนี้

```
/sbin/chkconfig httpd on
```

```
/sbin/service httpd start
```

```
/sbin/chkconfig mysqld on
```

```
/sbin/service mysqld start
```

- ตั้งค่ารหัสผ่านของ mysql

```
mysqladmin -u root password '123456'
```

1.2 การติดตั้ง PHP

```
tar -zxvf php-5.2.0.tar.gz
```

```
cd php-5.2.0
```

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

```
make
```

```
/sbin/service httpd stop
```

```
make install
```

```
vi /etc/httpd/conf/httpd.conf
```

หา LoadModule php5_module /usr/lib/httpd/modules/libphp5.so และเพิ่ม # ก่อน

หน้าข้อความนั้น

```
# LoadModule php5_module /usr/lib/httpd/modules/libphp5.so
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กด escape และ พิมพ์ :wq

/sbin/service httpd restart

1.3 การติดตั้งโปรแกรมส่วนติดต่อผู้ใช้งาน

นำไฟล์เตอร์ p2p-alert ไปไว้ใน /var/www/html/

1.4 การติดตั้ง ADODB

เปิดโปรแกรม Terminal และใช้คำสั่งดังต่อไปนี้

```
tar -zxvf adodb493a.tgz -C /var/www/html/
```

1.5 การติดตั้ง Snort

เปิดโปรแกรม Terminal และใช้คำสั่งดังต่อไปนี้

```
tar -zxvf snort-2.6.0.2.tar.gz -C /usr/local/
```

```
cd /usr/local/snort
```

```
./configure --with-mysql-includes=/usr/include/mysql --with-mysql-libraries=/usr/lib/mysql
```

```
make
```

```
make install
```

จากนั้นให้ก๊อปปี้ข้อมูล configuration และ rules files จาก source ของ Snort ไปยัง /etc/snort เพื่อความเป็นระเบียบ

```
mkdir /etc/snort
```

```
cd /usr/local/src/snort
```

```
cp snort.conf /etc/snort
```

```
cp *.rules /etc/snort
```

```
cp classification.config /etc/snort
```

สร้างไดเรกทอรีเพื่อเก็บล็อกไฟล์ของ Snort ทั้งหมดแยกต่างหาก และควรป้องกันไม่ให้บุคคลอื่น access เข้ามาที่ไดเรกทอรีนั้นๆ โดยปกติแล้วจะสร้างไว้ที่ /var/log/snort

```
mkdir /var/log/snort
```

```
chmod 700 /var/log/snort
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

-สร้าง database structure สำหรับ Snort

ให้ล็อกอินเข้าไปยัง MySQL และสร้าง database ชื่อ snort ขึ้นมา

```
#mysql -uroot -p
123456
mysql>CREATE DATABASE snort;
```

จากนั้นให้สร้าง MySQL account ขึ้นมาเพื่อให้มีสิทธิในการจัดการกับฐานข้อมูล

```
mysql>grant insert,delete,select,create,update on snort.* to snort@localhost;
mysql>flush privileges;
```

จากนั้นก็สร้าง database structure ตามที่ Snort กำหนดไว้

```
cd /usr/local/snort
vi contrib/create_mysql แล้วเพิ่มคำว่า USE snort; ไว้ที่บรรทัดบนสุด
mysql < ./contrib/create_mysql -uroot -p
```

- นำไฟล์ snort.conf ไปไว้ในโฟลเดอร์ /etc/snort/

- นำไฟล์ p2p.rules ไปไว้ในโฟลเดอร์ /etc/snort/rules

รัน Snort (daemon)

ทดสอบรัน /usr/local/bin/snort -c /etc/snort/snort.conf ถ้าไม่มี error ใดๆ แสดงว่าสามารถใช้งานได้ เพียงแต่การใช้งานจริงนั้นจะรันใน daemon mode โดยจะใช้คำสั่งดังนี้

```
/usr/local/bin/snort -D -c /etc/snort/snort.conf
```

2. การเปิดโปรแกรมเริ่มต้นการทำงาน

ต้องทำการเริ่มต้นการทำงานของ Httpd ก่อน โดยใช้คำสั่ง

```
/sbin/service httpd restart
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

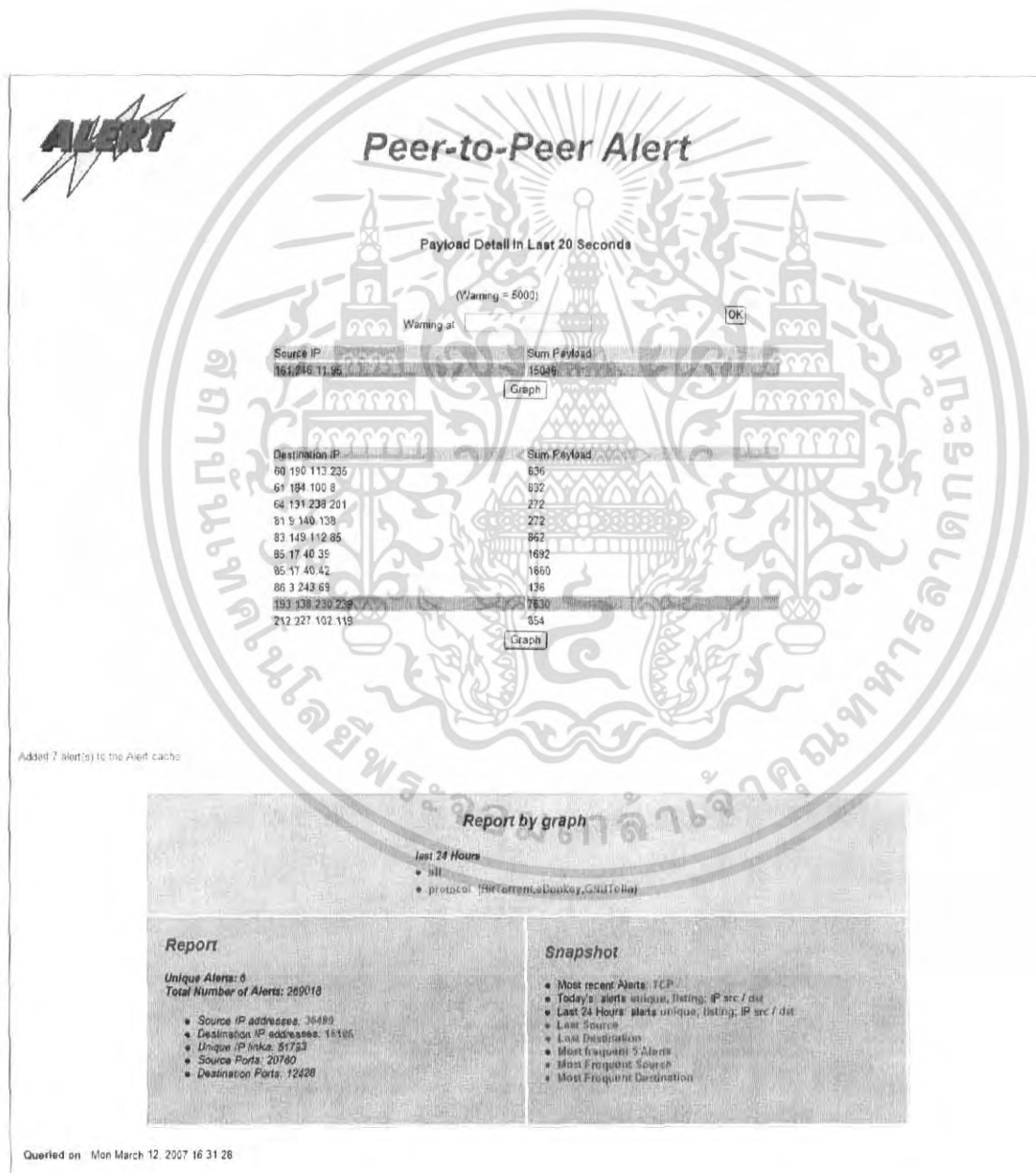
หลังจากนั้นก็เริ่มการทำงานของสเนอร์

```
/usr/local/bin/snort -D -c /etc/snort/snort.conf
```

เปิดโปรแกรมใช้งานได้จากบราวเซอร์ โดยเรียกไปที่แอดเดรสนี้

http://localhost/p2p-alert/acid_main.php

จะได้ผลดังภาพ



รูปที่ ก 1 หน้าจอแสดงผลที่ได้หลังจากเรียกโปรแกรมนี้ได้สำเร็จ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้