ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

Intrusion Detection for Electronics Mail System

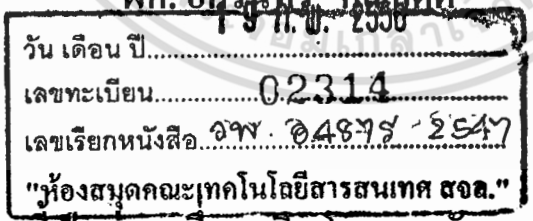
โดย

อังกูร ชูเชื้อ

รหัส 44067424

อาจารย์ที่ปรึกษา

ผศ. อัครินทร์ คณฑิตติ



รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2547

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	การพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์
นักศึกษา	นายอังกูร ชูเชื้อ
อาจารย์ที่ปรึกษา	ผศ. อัครินทร์ คุณกิตติ
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2547

บทคัดย่อ

จดหมายอิเล็กทรอนิกส์เป็นบริการหนึ่งในหลากหลายบริการบนเครือข่ายอินเทอร์เน็ต และได้รับความนิยมอย่างมาก เพราะสามารถทำได้ง่าย สะดวก รองรับข้อมูลได้หลายประเภททั้งแบบตัวอักษรธรรมดา หรือ แบบมัลติมีเดีย จะเห็นได้ว่าระบบจดหมายอิเล็กทรอนิกส์มีประโยชน์อย่างมาก แต่ก็มีบุคคลบางคนหรือบางกลุ่มที่กระทำการอันจะทำให้ระบบจดหมายอิเล็กทรอนิกส์ทำงานไม่ปกติ หรือไม่สามารถให้บริการได้ โดยการโจมตีระบบจดหมายอิเล็กทรอนิกส์ ด้วยวิธีการส่งจดหมายเข้ามาพร้อม ๆ กันเป็นจำนวนมากในลักษณะที่เรียกว่า Mail Bomb ดังนั้นจึงมีการสร้างระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ขึ้น ซึ่งนำหลักการของระบบตรวจจับการบุกรุก (Intrusion Detection) มาทำงานร่วมกับไฟร์วอลล์ (Firewall) โดยจะพิจารณาในสองประเด็น คือ พิจารณาจากจำนวนจดหมายที่ส่งมาจากผู้ส่งแหล่งเดียวกันในช่วงเวลาหนึ่งมีจำนวนเกินกว่าค่าที่กำหนดไว้หรือไม่ ส่วนประเด็นที่สองจะพิจารณาในส่วนของเลขทะเบียนจดหมาย (Message Id) ซึ่งเป็นค่าเฉพาะประจำตัวของจดหมายแต่ละฉบับ ดังนั้นจึงเป็นไปไม่ได้ที่จะมีเลขทะเบียนจดหมายซ้ำกันจากการส่งจากผู้ส่งแหล่งเดียวกัน ซึ่งหากเกิดเหตุการณ์ตรงกับทั้งสองประเด็น ระบบจะส่งคำสั่งไปให้ไฟร์วอลล์ทำการปฏิเสธการให้บริการผู้ส่งนั้น และการปฏิเสธการให้บริการจะเป็นในระยะเวลาหนึ่งเท่านั้น หากครบกำหนดเวลาดังกล่าว ระบบจะส่งคำสั่งไปให้ไฟร์วอลล์ยกเลิกการปฏิเสธการให้บริการนั้น เพื่อให้สามารถใช้งานได้ตามปกติต่อไป ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์พัฒนาบนระบบปฏิบัติการลีนุกซ์และใช้ภาษาเพิร์ลในการเขียนโปรแกรม โดยทำงานร่วมกับโปรแกรม Netfilter ซึ่งเป็นโปรแกรมประเภทไฟร์วอลล์และโปรแกรม Sendmail ผลการทำงานของระบบ สามารถตรวจจับการโจมตีและส่งคำสั่งเพื่อปฏิเสธการให้บริการไปยังไฟร์วอลล์ได้ และสามารถยกเลิกการปฏิเสธการให้บริการได้หากครบเวลาตามที่ได้กำหนดไว้

Title	Intrusion Detection for Electronics Mail System
Student	Mr. Ungkoon Chucheua
Advisor	Asst.Prof Akharin Khunkitti
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2004

Abstract

Electronics mail is one of various services in the world of internet. This service is so popular. Because of many excellent properties such as supports either normal text or multimedia data , easiness and more comfortable to use. But there are some people who use this service on the wrong way by sending a great amount of mails to electronics mail system , just like mail bomb. This causes the system works abnormally or the worst case , the system terminated. So , this project is developed to prevent or reduce this problem. The development is base on intrusion detection principle and works together with firewall system. There are two considerations for occurrence of attack. First is focused on amount of mails that sent from the same sender in the interval time. If the number of mails from same sender have more than a limit value. Then , it refers to the attack has occurred. The other is the same Message-Id attack. This Id is a specific unique value of each mail. So it is impossible that some mails from same sender have same Message-Id. This case refers to the attack has occurred, too. If the attacks have been occurred, the system sends commands to invoke firewall to deny the connection from the sender. And if the time for denying is expired, the system sends commands to the firewall to release blocking of the connection. That makes the sender can use the service normally. This system is developed on Linux OS with Netfilter and Sendmail program. Implementation uses perl language. It can detect the occurrence of attack and sends commands to firewall to deny connection and release after a timeout is expired.

กิตติกรรมประกาศ

ผู้จัดทำขอขอบพระคุณ ผศ. อัครินทร์ คุณกิตติ เป็นอย่างสูงที่ช่วยให้คำแนะนำแนวคิด ให้คำปรึกษาในด้านเนื้อหาที่เป็นประโยชน์ รวมทั้งให้ความช่วยเหลือในการตรวจสอบแก้ไขเอกสาร ตลอดจนขอขอบคุณผู้ที่มีส่วนเกี่ยวข้องทุกท่านที่ช่วยทำให้โครงการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์นี้สำเร็จลงได้

อังกูร ชูเชื้อ

กุมภาพันธ์ 2548

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

บทที่

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูป

หน้า

สารบัญรูป (ต่อ)

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

รูปที่

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของโครงการพัฒนาระบบ

ด้วยเทคโนโลยีการสื่อสารในปัจจุบันมีการพัฒนาไปอย่างมาก และได้มีการนำมาเชื่อมต่อเครื่องคอมพิวเตอร์เข้าด้วยกันเป็นระบบเครือข่าย และแต่ละเครือข่ายเชื่อมต่อกันเป็นเครือข่ายขนาดใหญ่ที่เรียกว่าอินเทอร์เน็ต ทำให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารซึ่งกันและกัน ซึ่งเป็นการสื่อสารในรูปแบบใหม่ จากแต่เดิมการติดต่อสื่อสารจะพิจารณาในเรื่องของเสียงเป็นส่วนใหญ่ ด้วยความต้องการการติดต่อสื่อสารผ่านเครือข่ายดังกล่าวก่อให้เกิดรูปแบบบริการอันหลากหลายเพื่อรองรับกับความต้องการการสื่อสารที่แตกต่างกันของแต่ละกลุ่มบุคคล จดหมายอิเล็กทรอนิกส์ก็เป็นอีกบริการหนึ่งที่เกิดขึ้นเพื่อตอบสนองกับความต้องการนั้น และได้รับความนิยมเป็นอย่างมาก อันเป็นเพราะคุณสมบัติของระบบจดหมายอิเล็กทรอนิกส์ ซึ่งมีความสะดวก รวดเร็วไม่ว่าผู้ส่งกับผู้รับจะอยู่คนละฟากโลกก็ตามที อีกทั้งยังสามารถรองรับข้อมูลได้หลากหลาย ไม่เฉพาะข้อมูลที่เป็นตัวอักษรเท่านั้น แต่ยังสามารถรองรับข้อมูลที่เป็นรูปภาพ หรือ ข้อมูลมัลติมีเดียได้ด้วย ทำให้มีผู้ใช้งานเป็นจำนวนมาก และในบรรดานั้นมีบุคคลบางกลุ่มที่ไม่ประสงค์ดีหรือแสวงหาผลประโยชน์โดยมิชอบ โดยอาศัยคุณสมบัติของระบบจดหมายอิเล็กทรอนิกส์เป็นช่องทาง เช่นการโฆษณาสินค้า ก่อให้เกิดความรำคาญในการใช้งาน หรือการโจมตีระบบจดหมายอิเล็กทรอนิกส์โดยการส่งจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลขนาดใหญ่ และปริมาณจำนวนมาก ทำให้ระบบเกิดความเสียหาย ไม่สามารถให้บริการ

จึงได้มีการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ เพื่อลดปัญหาการโจมตีระบบจดหมายอิเล็กทรอนิกส์ไม่ว่าจะเป็นในเรื่องการทำงานของเครื่องให้บริการจดหมายอิเล็กทรอนิกส์ หรือลดปัญหาตู้รับจดหมายอิเล็กทรอนิกส์เต็ม ซึ่งการพัฒนาจะมุ่งเน้นไปที่การป้องกันการโจมตีแบบ Mail Bomb

1.2 วัตถุประสงค์ของการพัฒนาระบบงาน

การพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ มีวัตถุประสงค์ดังต่อไปนี้

- เพื่อทำการศึกษาหลักการทำงานของระบบการรับส่งจดหมายอิเล็กทรอนิกส์

- เพื่อทำการศึกษาหลักการทำงานของการตรวจจับการบุกรุกและระบบไฟร์วอลล์
- เพื่อวิเคราะห์และออกแบบระบบการตรวจจับการบุกรุกระบบจดหมายอิเล็กทรอนิกส์
- เพื่อลดปัญหาการโจมตีระบบจดหมายอิเล็กทรอนิกส์ อันจะทำให้เครื่องที่ให้บริการจดหมายอิเล็กทรอนิกส์ (Mail Server) ทำงานหนักจนไม่สามารถให้บริการได้ และลดปัญหาตู้รับจดหมายอิเล็กทรอนิกส์ (Mailbox) เต็ม

1.3 ขอบเขตของการพัฒนาระบบงาน

การพัฒนาระบบตรวจจับการบุกรุกจดหมายอิเล็กทรอนิกส์ ครอบคลุมการทำงานส่วนต่าง ๆ ดังต่อไปนี้

- ส่วนของการตรวจสอบและเฝ้าดูการโจมตี โดยวิเคราะห์เป็น 2 ประเด็น ประเด็นแรกคือจำนวนจดหมายอิเล็กทรอนิกส์ที่มาจากต้นทางเดียวกันในช่วงเวลาหนึ่ง ๆ ว่าเกินกว่าที่กำหนดไว้หรือไม่ ซึ่งการกำหนดนี้ผู้ใช้สามารถกำหนดให้เหมาะสมกับระบบตัวเองได้ ส่วนประเด็นที่สองคือตรวจสอบจากเลขทะเบียนจดหมายอิเล็กทรอนิกส์ (Message-Id) ซึ่งจะมีลักษณะไม่ซ้ำกันในแต่ละฉบับของจดหมายอิเล็กทรอนิกส์ หากมีจดหมายอิเล็กทรอนิกส์ที่มีเลขทะเบียนซ้ำกันแสดงว่าเกิดการโจมตีเกิดขึ้น
- ส่วนของการจัดการ หากเกิดการโจมตีเกิดขึ้น จะทำการส่งสัญญาณไปยังไฟร์วอลล์ให้ทำการปฏิเสธจดหมายอิเล็กทรอนิกส์ โดยการปิดการติดต่อกับแหล่งที่มาของจดหมายอิเล็กทรอนิกส์นั้น และแจ้งเตือนผู้ดูแลระบบ
- ส่วนของการจัดการเมื่อข้อมูลถึงช่วงหมดเวลา (Timeout) โดยจะมีการลบข้อมูลออกจากระบบ และหากเป็นข้อมูลที่เกี่ยวกับไฟร์วอลล์ ก็จะส่งข้อมูลดังกล่าวให้ไฟร์วอลล์จัดการ

การพัฒนาระบบตรวจจับการบุกรุกจดหมายอิเล็กทรอนิกส์ จะพัฒนาภายใต้ระบบปฏิบัติการลีนุกซ์ โดยใช้โปรแกรม Sendmail เป็นโปรแกรมบริการจดหมายอิเล็กทรอนิกส์ และใช้ Netfilter เป็นไฟร์วอลล์ ซึ่ง Netfilter เป็นส่วนหนึ่งของระบบปฏิบัติการลีนุกซ์ ส่วนการเขียนโปรแกรมจะใช้ภาษาเพิร์ล (Perl)ในการพัฒนา

1.4 ขั้นตอนในการพัฒนาระบบงาน

- ศึกษารูปแบบของการโจมตีระบบจดหมายอิเล็กทรอนิกส์
- ศึกษารูปแบบและขั้นตอนการทำงานของระบบการรับส่งจดหมายอิเล็กทรอนิกส์
- ศึกษาการทำงานและการติดตั้งเครื่องบริการจดหมายอิเล็กทรอนิกส์ (Mail Server) โดยใช้โปรแกรม Sendmail

- ศึกษาการทำงานของไฟร์วอลล์
- ศึกษาวิธีการพัฒนาระบบบนระบบปฏิบัติลีนุกซ์
- ทำการวิเคราะห์และออกแบบโปรแกรมตรวจจับการบุกรุกระบบจดหมายอิเล็กทรอนิกส์
- พัฒนาโปรแกรมตรวจจับการบุกรุกระบบจดหมายอิเล็กทรอนิกส์
- ทดสอบการใช้งาน และปรับปรุงแก้ไขโปรแกรม
- สรุปผลการทดสอบจากการใช้งานที่เกิดขึ้น
- จัดทำเอกสารประกอบโครงงาน

1.5 รายละเอียดเนื้อหาของแต่ละบท

- บทที่ 2 นำเสนอความรู้เกี่ยวข้องกับการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ อันประกอบด้วยระบบตรวจจับการบุกรุก การทำงานของจดหมายอิเล็กทรอนิกส์ และหลักการทำงานของไฟร์วอลล์
- บทที่ 3 นำเสนอแนวทางการออกแบบและพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ โดยวิเคราะห์ความต้องการของระบบเพื่อนำไปสู่กระบวนการพัฒนาระบบต่อไป
- บทที่ 4 นำเสนอผลการทดสอบการใช้ระบบตรวจจับการบุกรุกระบบสำหรับจดหมายอิเล็กทรอนิกส์ว่าทำงานได้อย่างถูกต้อง
- บทที่ 5 นำเสนอสรุปการพัฒนาระบบงาน และข้อเสนอแนะ

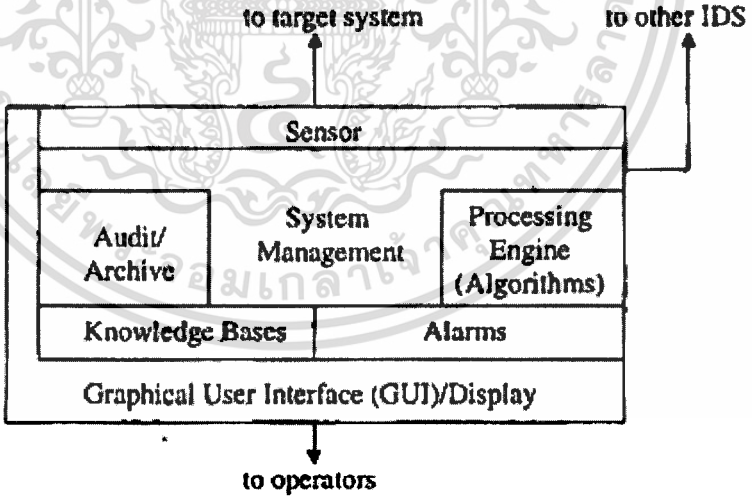
บทที่ 2

ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

2.1 ระบบตรวจจับการบุกรุก (Intrusion Detection System)

ระบบตรวจจับการบุกรุก คือระบบที่ใช้ในการตรวจจับกิจกรรมที่เกิดจากการใช้งานและความพยายามในการใช้งานทรัพยากรของเครือข่ายคอมพิวเตอร์ ซึ่งขัดต่อข้อบังคับของการใช้งาน ส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ โดยจะทำการวิเคราะห์เหตุการณ์ที่เกิดขึ้น และตอบสนองต่อเหตุการณ์นั้น ๆ ตามข้อกำหนด เช่นแจ้งเตือนผู้ดูแลระบบ หรือ แจ้งให้ระบบไฟร์วอลล์ทำการระงับเหตุการณ์นั้น ๆ หากเหตุการณ์นั้นเกิดจาก กิจกรรมที่ไม่เหมาะสม

2.1.1 โครงสร้างของระบบตรวจจับการบุกรุก



รูปที่ 2.1 แสดงโครงสร้างของระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุกมีส่วนประกอบต่าง ๆ หลายส่วนแสดงดังรูปที่ 2.1 ซึ่งมีรายละเอียดดังต่อไปนี้

- Sensor เป็นส่วนที่เฝ้าดูกระแสของข้อมูลที่ผ่านเข้าและออกจากระบบ
- System Management เป็นส่วนที่ควบคุมการทำงาน ของส่วนต่าง ๆ ของระบบ

- Process Engine เป็นส่วนประมวลผลข้อมูลที่รับเข้ามา เพื่อที่จะระบุได้ว่าข้อมูลไหนเป็นรูปแบบการบุกรุก โดยจะประมวลผลตาม algorithm ที่ได้กำหนดไว้
- Knowledge Base เป็นส่วนที่เก็บข้อมูลที่แสดงรูปแบบของการบุกรุกเพื่อที่จะใช้ในการเปรียบเทียบกับข้อมูลที่ต้องการตรวจสอบ ซึ่งข้อมูลเหล่านี้ต้องมีการปรับปรุงให้ทันสมัยให้มากที่สุด โดยอาจจะใช้กระบวนการวิเคราะห์ทางพฤติกรรมเข้ามาช่วยตรวจสอบรูปแบบพฤติกรรมที่เบี่ยงเบนไปจากรูปแบบปกติ และจดจำรูปแบบเหล่านี้เพื่อใช้อ้างอิงต่อไป
- Audit/Achieve เป็นส่วนในการเก็บข้อมูลกิจกรรมต่าง ๆ ที่เกิดขึ้น หรือ audit logs เพื่อจะได้นำมาวิเคราะห์ภายหลังได้
- Alarm เมื่อระบบตรวจจับการบุกรุกตรวจพบการบุกรุก ก็จะส่งสัญญาณเตือนไปยังส่วนต่าง ๆ ตามที่ได้กำหนดเอาไว้ เช่น เตือนให้ผู้ดูแลระบบผ่านทาง จดหมายอิเล็กทรอนิกส์ หรือ pager เป็นต้น
- Display เป็นส่วนใช้ในการติดต่อกับผู้ใช้ เพื่อใช้ในการกำหนดค่าของระบบ หรือ แจ้งให้ทราบว่าได้ตรวจพบมีการบุกรุกเกิดขึ้น

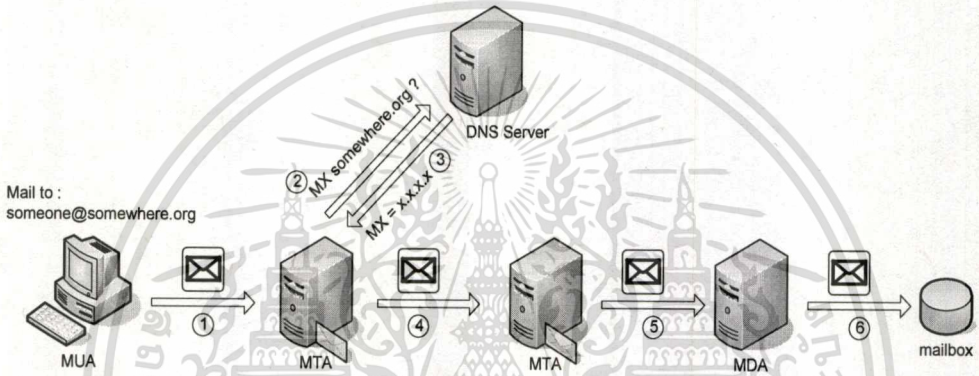
2.1.2 ประเภทของระบบตรวจจับการบุกรุก

โดยทั่วไประบบตรวจจับการบุกรุกจะแบ่งเป็นหลายประเภท ขึ้นอยู่กับลักษณะงาน แต่โดยทั่ว ๆ ไปจะแบ่งเป็น 2 ประเภทใหญ่ ๆ คือ

- ระบบตรวจจับที่ทำงานบนเครือข่าย (Network-based Intrusion Detection System) เป็นระบบตรวจจับการบุกรุกที่ทำงานเฝ้าดูกระแสข้อมูลบนระบบเครือข่ายที่รับผิดชอบ โดยที่จะเปรียบเทียบกับรูปแบบ signature ของระบบตรวจจับผู้บุกรุกว่ามีรูปแบบเหมือนกันหรือไม่ ถ้าเหมือนกับ signature ก็อาจสันนิษฐานได้ว่ามีความพยายามที่จะบุกรุก ซึ่ง signature จะแบ่งเป็น 3 ประเภทใหญ่ ๆ คือ
    - String signature ซึ่งจะบ่งบอกถึงการบุกรุกที่มีลักษณะเป็นข้อความหรือรูปแบบคำสั่งที่เป็นอันตรายต่อระบบ
    - Port signature มีลักษณะเป็นหมายเลข port ที่โปรแกรมของผู้บุกรุกใช้ เช่น NetBus ใช้ port หมายเลข 12345 หรือกรณี well-known port ที่เราไม่เปิดบริการให้ใช้ แต่มีความพยายามที่จะติดต่อเข้ามา แสดงว่าอาจมีพฤติกรรมที่ประสงค์ร้าย
    - Header signature โดยมีลักษณะ header ของ แพ็กเกต ที่มีรูปแบบที่ผิดปกติ เช่น TCP SYN , TCP FIN เป็นต้น

- ระบบตรวจจับการบุกรุกที่ทำงานเฉพาะเครื่อง (Host-based Intrusion Detection System) เป็นระบบตรวจจับการบุกรุกที่จะเฝ้าดูตรวจสอบกระแสข้อมูลที่ผ่านเข้าออกบนเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่รับผิดชอบ ว่ามีลักษณะที่เป็นการบุกรุกทรัพยากรภายในเครื่องหรือไม่ โดยจะเฝ้าดูความสมบูรณ์ของไฟล์ระบบ(system files) และเฝ้าดูกระบวนการประมวลผลที่น่าสงสัย

2.2 จดหมายอิเล็กทรอนิกส์



รูปที่ 2.2 แสดงการทำงานของระบบจดหมายอิเล็กทรอนิกส์

จดหมายอิเล็กทรอนิกส์เป็นบริการหนึ่งบนเครือข่ายอินเทอร์เน็ตที่ได้รับความนิยมอย่างอย่างสูง การทำงานจะเป็นไปในลักษณะที่เรียกว่า "ไคลเอนต์/เซอร์ฟเวอร์" โดยผู้ส่งจะทำหน้าที่เป็นไคลเอนต์ติดต่อไปยังเซอร์ฟเวอร์ ซึ่งทำหน้าที่เป็นเครื่องบริการจดหมายอิเล็กทรอนิกส์ของผู้รับเพื่อที่จะทำการขอส่งข้อมูลของจดหมาย โครงสร้างของระบบจดหมายอิเล็กทรอนิกส์จะแบ่งเป็น 3 ส่วน คือ

- MUA (Mail User Agent) ทำหน้าที่เป็นส่วนของผู้ส่งและส่วนของผู้รับของผู้ใช้งาน
- MTA (Mail Transfer Agent) ทำหน้าที่เป็นตัวกลางในการส่งจดหมายอิเล็กทรอนิกส์ ซึ่งการส่งจดหมายอิเล็กทรอนิกส์อาจจะอาศัย MTA หลายตัวส่งต่อกันเป็นทอด ๆ จนกว่าจะถึง MTA ตัวสุดท้ายที่ผู้รับจดหมายอิเล็กทรอนิกส์เป็นสมาชิกอยู่ และหากไม่สามารถส่งถึงผู้รับได้ ก็จะส่งจดหมายอิเล็กทรอนิกส์ที่แสดงข้อความผิดพลาด (Error Mail) กลับมายังผู้ส่ง
- MDA (Mail Delivery Agent) ทำหน้าที่ตรวจสอบว่าจดหมายอิเล็กทรอนิกส์ที่รับเข้ามาว่าตรงกับผู้รับที่เป็นสมาชิกหรือไม่ ถ้าตรงก็จะเก็บจดหมายอิเล็กทรอนิกส์ลงตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับ โดยทั่วไปของระบบจดหมายอิเล็กทรอนิกส์ MTA และ MDA มักจะอยู่รวมกัน

2.2.1 ขั้นตอนการทำงานของระบบจดหมายอิเล็กทรอนิกส์

จากรูปที่ 2.2 แสดงขั้นตอนการส่งจดหมายอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

- ขั้นตอนที่ 1 ผู้ส่งใช้ MUA ในการเขียนจดหมายส่งไปถึง someone@somewhere.org โดยส่งผ่าน MTA ตัวแรก
- ขั้นตอนที่ 2 เมื่อ MTA ตัวแรกได้รับจดหมายอิเล็กทรอนิกส์ ก็จะสอบถาม DNS ว่าหากต้องการส่งจดหมายอิเล็กทรอนิกส์ไปยังโดเมน somewhere.org นั้นจะส่งไปที่ MTA ใด โดย DNS มีเรคอร์ดของ MTA ที่เรียกว่า MX (Mail Exchange)
- ขั้นตอนที่ 3 DNS ตอบกลับการสอบถามของ MTA ตัวแรก ด้วยหมายเลข IP address ของ MTA ที่มีโดเมนเป็น somewhere.org
- ขั้นตอนที่ 4 MTA ตัวแรกส่งจดหมายอิเล็กทรอนิกส์ไปยัง MTA ที่ได้จากการสอบถาม DNS
- ขั้นตอนที่ 5 MTA ของโดเมน somewhere.org ทำการตรวจสอบจดหมายอิเล็กทรอนิกส์เป็นโดเมนของตนหรือไม่ ถ้าใช่ก็จะตรวจสอบว่าผู้รับว่าเก็บอยู่ในส่วนของ MDA ใด จากนั้นก็จะส่งให้ MDA นั้น
- ขั้นตอนที่ 6 MDA ตรวจสอบชื่อผู้รับ และนำจดหมายอิเล็กทรอนิกส์เก็บเป็นไฟล์ไว้ที่ตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับ

2.2.2 รูปแบบของจดหมายอิเล็กทรอนิกส์

ในส่วนของรูปแบบของจดหมายอิเล็กทรอนิกส์แบ่งเป็น 2 ส่วนคือ

- Header ส่วนนี้จะถูกสร้างโดย MUA และ MTA เพื่อใช้เป็นข้อมูลในการส่งจดหมายอิเล็กทรอนิกส์ Header มีรูปแบบมาตรฐานที่หน่วยงาน IEFT เป็นผู้กำหนด ได้แก่ RFC 822 , RFC 1123 และ RFC 2822 (822bis) โดยประกอบด้วยฟิลด์หลายฟิลด์รวมกัน ซึ่งแต่ละฟิลด์ประกอบด้วยชื่อฟิลด์ตามด้วยเครื่องหมาย : ตามด้วยเว้นวรรคและค่าที่เป็นไปได้ของแต่ละฟิลด์ ดังตัวอย่างแสดงในรูปที่ 2.3 เป็นการแสดงถึงฟิลด์ที่ชื่อ Date มีค่าเป็น 30 Jul 2000 11:54:54 +0007

Date: 30 Jul 2000 11:54:54 +0007

รูปที่ 2.3 แสดงตัวอย่างแสดงฟิลด์ของ Header

ส่วนฟิลด์อื่น ๆ แสดงในตารางที่ 2.1

ตารางที่ 2.1 แสดงฟิลด์ต่าง ๆ ใน Header

หมวด	ฟิลด์	รายละเอียด
Recipients	To	ระบุถึงผู้รับปลายทาง
	Cc	ระบุถึงผู้รับคนอื่นๆโดยที่ผู้รับสามารถมองเห็นชื่อผู้รับอื่นๆได้
	Bcc	ระบุถึงผู้รับคนอื่นๆ โดยที่ผู้รับไม่สามารถมองเห็นชื่อผู้รับอื่นๆได้
Senders	From	ผู้ส่งจดหมายอิเล็กทรอนิกส์
	Sender	เหมือนกับ From แต่มีการ authentication ผู้ส่ง มักใช้ใน USENET news
Response	Reply-To	ระบุถึงปลายทางที่จะส่งจดหมายอิเล็กทรอนิกส์กลับ
Threading	Message-Id	หมายเลขกำกับจดหมายอิเล็กทรอนิกส์ เป็น unique number
	In-Reply-To	ข้อมูลของจดหมายอิเล็กทรอนิกส์สำหรับการตอบกลับ
Date	Date	เวลาที่แท้จริงเมื่อจดหมายอิเล็กทรอนิกส์มีการยืนยันที่จะส่ง โดยมีการเทียบเวลากับ UTC
Trace	Path	รายชื่อ MTA ที่จดหมายอิเล็กทรอนิกส์ผ่าน
	Receive	MTA ตัวสุดท้ายที่รับจดหมายอิเล็กทรอนิกส์
	Return-Path	เส้นทางในการตอบกลับของจดหมายอิเล็กทรอนิกส์
Miscellaneous	Subject	หัวข้อของจดหมายอิเล็กทรอนิกส์ หรือข้อความสรุปที่แสดงถึงเนื้อหาของจดหมาย
	Comment	ถูกสร้างขึ้นโดย MUA เช่น Pegasus มักจะระบุถึงผู้ส่งที่ผ่านการ authentication
	Encrypted	ข้อมูลของกระบวนการเข้ารหัสจดหมายอิเล็กทรอนิกส์ หากจดหมายอิเล็กทรอนิกส์มีการเข้ารหัส

- Body คือส่วนของเนื้อหาของจดหมาย โดยจะมีบรรทัดว่างเป็นตัวแยก Header กับ Body หากเนื้อหาเป็นตัวอักษรจะเป็นรหัส ASCII 7 บิต แต่หากเป็นข้อมูลที่เป็นรูปภาพหรือมัลติมีเดีย จะใช้ วิธีการตามข้อกำหนดที่เรียกว่า MIME (Multipurpose Internet Mail Extension)

2.2.3 SMTP

SMTP (Simple Mail Transfer Protocol) เป็นข้อตกลงมาตรฐานในการส่งจดหมายอิเล็กทรอนิกส์บนเครือข่าย TCP/IP ซึ่งมีการกำหนดไว้ใน RFC 821 จดหมายอิเล็กทรอนิกส์ที่มีการส่งข้อมูลผ่าน SMTP นั้นต้องมีการทำตามรูปแบบที่กำหนดไว้ใน RFC 822 SMTP ยังมีการจัดการเกี่ยวกับความผิดพลาดที่เกิดขึ้น บางครั้งจุดหมายปลายทางอาจจะไม่สามารถติดต่อได้ หรือเกิดล้มเหลวระหว่างที่กำลังถ่ายข้อมูล SMTP ที่ส่งสามารถที่จะนำกลับเข้าคิวใหม่เพื่อส่งภายหลังหรือแจ้งความผิดพลาดแก่ผู้ส่ง โปรโตคอล SMTP นั้นใช้ในการรับส่งระหว่าง SMTP สองฝั่งคือฝั่งส่งและฝั่งรับ ผ่านทาง TCP พอร์ตหมายเลข 25 และเป็นบริการที่ให้ความน่าเชื่อถือของข้อมูลแต่ไม่สามารถรับรองที่จะแก้คืนจดหมายที่เกิดการสูญหายได้ SMTP ที่ทำหน้าที่รับจดหมายแต่ละอันที่มาถึงและทำการนำไปเก็บไว้ที่ตู้จดหมายของผู้รับ หรือไม่ก็ทำการคัดลอกเพื่อเก็บไว้ในคิวที่จะทำการส่งออก ถ้าจดหมายนั้นต้องมีการส่งต่อ SMTP รับผิดชอบสำหรับส่งจดหมายเพียงจากจุดหนึ่งถึงผู้รับอีกจุดหนึ่งที่สามารถบ่งบอกได้ว่าการถ่ายข้อมูลสมบูรณ์ แต่ไม่ได้หมายความว่า จะส่งถึงมือผู้รับแน่นอน ในแต่ละขั้นตอนการทำงานของ SMTP ประกอบไปด้วย ชุดของคำสั่งและรหัสที่ตอบกลับมา ระหว่าง SMTP ของฝั่งส่งและฝั่งรับ โดยรูปแบบคำสั่งและรหัสที่ตอบกลับมา รายละเอียดแสดงในตารางที่ 2.2 และ 2.3 ตามลำดับ เมื่อ SMTP ฝั่งส่งเริ่มทำการเชื่อมต่อผ่านทาง TCP จะมีชุดคำสั่งส่งออกไปในทางที่เชื่อมต่อ แต่ละคำสั่งที่ส่งออกไปก็จะมีการตอบรับกลับมาหนึ่งครั้งเสมอ เมื่อมีการส่งคำสั่ง SMTP ต่าง ๆ ไปแล้วนั้นก็จะมีการตอบกลับถึงสถานะของคำสั่ง ว่าสามารถปฏิบัติตามได้หรือไม่

ตารางที่ 2.2 แสดงคำสั่งของ SMTP

คำสั่ง	รายละเอียด
HELO	เริ่มต้นการเชื่อมต่อกับเครื่องบริการจดหมายอิเล็กทรอนิกส์
MAIL	ระบุผู้ส่งจดหมายอิเล็กทรอนิกส์
RCPT	ระบุรับส่งจดหมายอิเล็กทรอนิกส์
DATA	เนื้อหาของจดหมายอิเล็กทรอนิกส์
RSET	ยกเลิกการเชื่อมต่อกับเครื่องบริการจดหมายอิเล็กทรอนิกส์

ตารางที่ 2.2 (ต่อ)

คำสั่ง	รายละเอียด
NOOP	ไม่มีผลใด ๆ เพียงแต่บังคับให้เครื่องบริการจดหมายอิเล็กทรอนิกส์ส่ง OK (code 200) กลับมา
QUIT	ปิดการเชื่อมต่อ
SEND	ส่งข้อความถึงเครื่องผู้รับ
SAML	ส่งข้อความถึงเครื่องผู้รับและตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับด้วย
SOML	หากเครื่องผู้รับอยู่ในสถานะพร้อมรับข้อความให้ส่งข้อความถึงเครื่องผู้รับ หากไม่อยู่ในสถานะพร้อมรับข้อความให้ส่งข้อความไปที่ตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับแทน
VRFY	ร้องขอการตรวจสอบที่อยู่ของผู้รับ
EXPN	กำหนดมีการใช้ mailing list
HELP	ขอความเชื่อเหลือ
TURN	เปลี่ยนจากสภาพผู้รับเป็นผู้ส่ง

ตารางที่ 2.3 แสดงรหัสตอบกลับของ SMTP

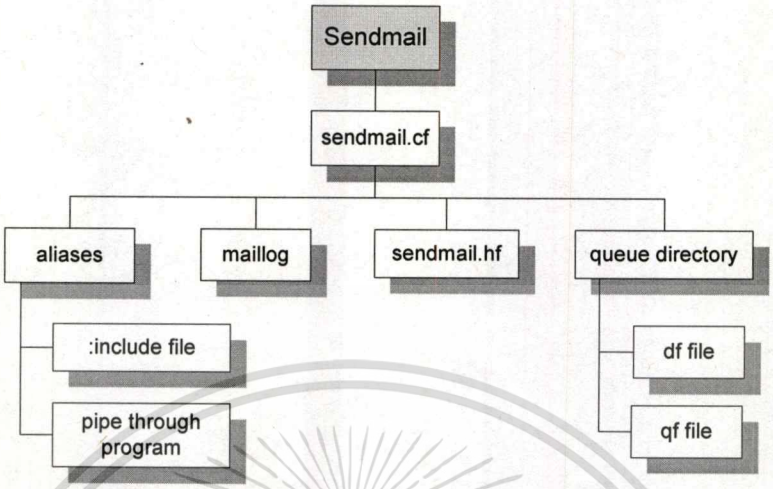
รหัส	รายละเอียด
211	สถานะของระบบ
214	ข้อความช่วยเหลือ
220	พร้อมให้บริการ
221	ปิดการเชื่อมต่อ
250	การร้องขอเสร็จเรียบร้อย
251	ผู้รับไม่ใช่สมาชิกของเครื่องบริการจดหมายอิเล็กทรอนิกส์ แต่จะส่งต่อไปให้เครื่องบริการจดหมายอิเล็กทรอนิกส์อื่น (forward-path)
354	เป็นการตอบกลับคำสั่ง DATA ว่าพร้อมจะรับข้อความจนกว่าจะพบ “carriage return . carriage return ”
421	ไม่พร้อมให้บริการ
450	ตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับไม่พร้อมให้บริการ
451	ระบบเกิดความผิดพลาดขึ้นไม่สามารถปฏิบัติตามคำสั่งได้

ตารางที่ 2.3 (ต่อ)

รหัส	รายละเอียด
452	ไม่สามารถปฏิบัติตามคำสั่งได้ เนื่องจากเกิดปัญหากับระบบจัดเก็บข้อมูล
500	รูปแบบคำสั่งไม่ถูกต้อง
501	รูปแบบพารามิเตอร์ของคำสั่งไม่ถูกต้อง
502	ไม่สามารถปฏิบัติตามคำสั่งได้
503	ลำดับของคำสั่งไม่ถูกต้อง
504	ไม่สามารถปฏิบัติตามคำสั่งที่มีค่าพารามิเตอร์นี้ได้
550	ไม่สามารถหาตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับได้
551	ผู้รับไม่ใช่สมาชิกของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ให้ส่งไปที่เครื่องบริการจดหมายอิเล็กทรอนิกส์อื่น ตามข้อมูลที่ส่งไปให้
552	ไม่สามารถปฏิบัติตามคำสั่งได้ เนื่องจากหน่วยเก็บข้อมูลเต็ม
553	รูปแบบของที่อยู่ผู้รับไม่ถูกต้อง
554	การเชื่อมต่อเกิดความล้มเหลว โดยไม่ทราบสาเหตุ

2.2.4 Sendmail

Sendmail เป็นโปรแกรมประเภท MTA ที่ได้รับความนิยมมากที่สุด ด้วยคุณสมบัติที่มีความยืดหยุ่นสูง สามารถปรับแต่งให้สามารถรองรับกับต้องการได้หลากหลาย Sendmail ถูกพัฒนามาจากโปรแกรมส่งข่าวสารบนระบบปฏิบัติการยูนิกซ์ที่เรียกว่า UUCP (Unix to Unix Copy) แต่ด้วยเหตุที่ UUCP สามารถส่งข่าวสารได้เฉพาะในเครือข่ายเดียวกันเท่านั้น ไม่สามารถส่งข่าวสารข้ามเครือข่ายได้ ดังนั้นจึงมีการพัฒนาโปรแกรมใหม่เพื่อแก้ปัญหานี้โดย Eric Allman ซึ่งมีชื่อว่า delivermail ต่อมาก็ได้พัฒนามาเรื่อย ๆ และเปลี่ยนชื่อเป็น Sendmail ปัจจุบัน Sendmail ถูกพัฒนาอยู่ในลำดับที่ 8 หรือเรียกว่า V8 โดยการทำงานอยู่บนพื้นฐานของ RFC หลายตัว เช่น RFC821 (SMTP) , RFC822 (Header and Body of Mail) , RFC819 (Domain Naming Convention) , RFC1123 (Extension of RFC821 and RFC822) เป็นต้น



รูปที่ 2.4 แสดงไฟล์ระบบของโปรแกรม Sendmail

ไฟล์ระบบที่สำคัญดังแสดงดังรูปที่ 2.4 มีรายละเอียดดังต่อไปนี้

- sendmail.cf เป็นไฟล์ที่ใช้ในการกำหนดค่าเริ่มต้นการทำงานของโปรแกรม Sendmal โดยจะแบ่งเป็น 2 ส่วนใหญ่ ๆ คือ
  - ส่วนของการกำหนดค่า ซึ่งจะขึ้นต้นด้วยอักษรตัวใหญ่ดังแสดงในตารางที่ 2.4

ตารางที่ 2.4 แสดงรูปแบบการกำหนดค่าในไฟล์ sendmail.cf

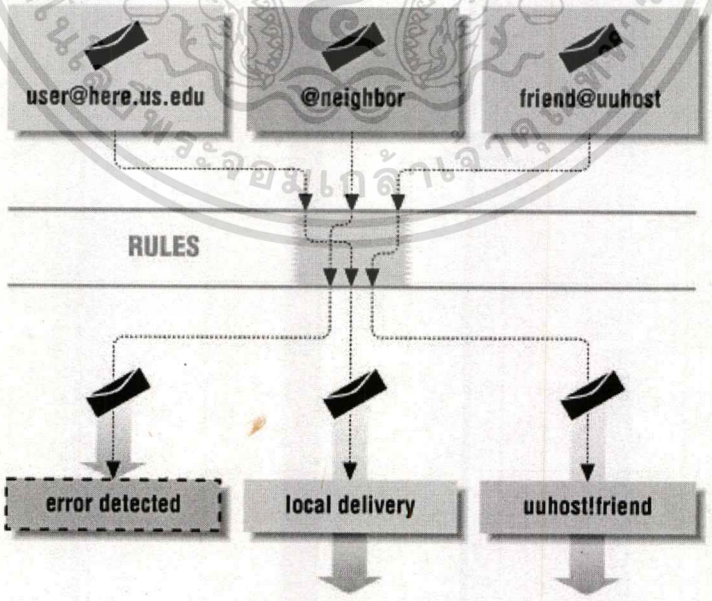
คำสั่ง	รายละเอียด
V	กำหนด version ของ Sendmail
M	กำหนด mail delivery agent
D	กำหนด macro
R	กำหนด rewrite rule
S	ประกาศการใช้ rule-set
C	กำหนด class macro
O	กำหนด option
H	กำหนด header
T	กำหนด trusted users
E	กำหนด environment variable

ตัวอย่างการกำหนดค่าแสดงดังรูปที่ 2.5 ซึ่งเป็นการกำหนด mail delivery agent ประเภทท้องถิ่น (local) หรือภายใน นั่นคือถ้าหากมีจดหมายอิเล็กทรอนิกส์เข้ามาเป็นประเภทท้องถิ่น โปรแกรม Sendmail จะทำการปฏิบัติกับจดหมายอิเล็กทรอนิกส์ตามเงื่อนไขที่ได้กำหนดไว้ ตามตัวอย่าง

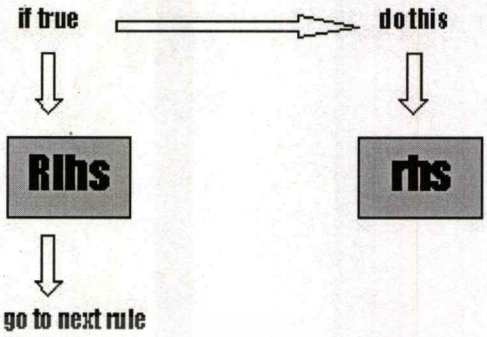
```
Mlocal, P=/bin/mail, F=lsDFMAw5:/|@rmn, S=10, R=20/40, A=mail -d $u
```

รูปที่ 2.5 แสดงตัวอย่างการกำหนดค่าในไฟล์ sendmail.cf

- ส่วนของกฎ (Rules) ในส่วนนี้เป็นส่วนที่สำคัญที่ใช้ในการสร้างแอดเดรสใหม่ (rewrite address) ของจดหมายอิเล็กทรอนิกส์ให้ถูกต้อง เพราะว่าระบบจดหมายอิเล็กทรอนิกส์มีรูปแบบของแอดเดรสที่แตกต่างกันขึ้นอยู่กับการที่ได้กำหนดดังที่กล่าวไว้ในส่วนแรก ดังแสดงดังรูป 2.6 ซึ่งจะเห็นได้ว่าเมื่อมีจดหมายอิเล็กทรอนิกส์เข้ามา Sendmail จะใช้กฎในการสร้างแอดเดรสใหม่ ให้ถูกต้องตามระบบของผู้ใช้ เช่น ถ้าหากเป็นแบบ UUCP จะมีรูปแบบเป็น user!host หรือในระบบทั่วไปจะเป็นแบบ user@host



รูปที่ 2.6 แสดงการสร้างแอดเดรสใหม่

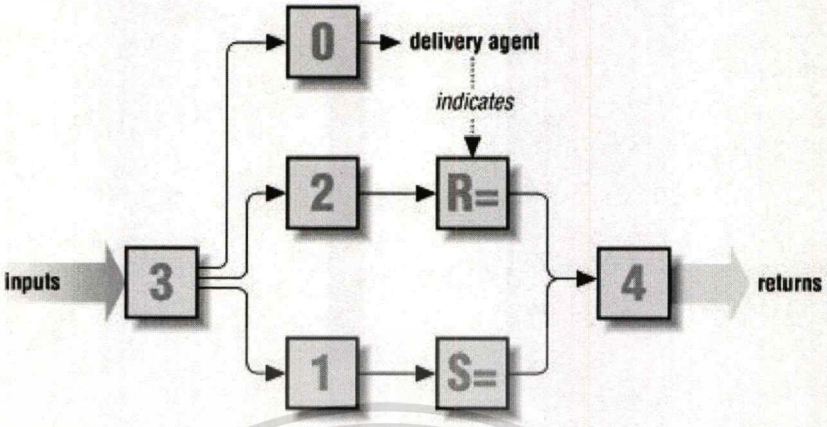


รูปที่ 2.7 แสดงการเปรียบเทียบกฎ

รูปแบบของกฎ จะมี 2 ด้าน คือ LHS (Left – Hand Side) กับ RHS (Right – Hand Side) และการกำหนดกฎจะขึ้นต้นด้วยตัวอักษร R ส่วนการใช้งานเริ่มจาก Sendmail จะตรวจสอบแอดเดรสของจดหมายอิเล็กทรอนิกส์กับกฎที่กำหนดไว้ โดยจะเปรียบกับด้าน LHS ซึ่งถ้าตรง Sendmail จะสร้างแอดเดรสขึ้นมาใหม่ตามรูปแบบด้าน RHS หากไม่ตรงก็จะเปรียบกฎข้อต่อไปดังแสดงในรูป 2.7 และเพื่อการใช้งานที่สะดวกจึงมีการนำกฎที่กำหนดขึ้นมารวมกันเป็นหมวดหมู่เรียกว่า rule set โดยที่ Sendmail จะมีมาตรฐานของ rule set อยู่ 5 ประเภทรายละเอียดดัง ตารางที่ 2.5 และรูปที่ 2.8

ตารางที่ 2.5 แสดงรายละเอียดของ Rule Set

Rule Set	รายละเอียด
0	เป็นตัวกำหนดการเลือก delivery agent
1	เป็นตัวกำหนดการ rewrite address ของผู้ส่ง
2	เป็นตัวกำหนดการ rewrite address ของผู้รับ
3	การทำงานจะเป็นลักษณะ pre-processing คือจดหมายอิเล็กทรอนิกส์ต้องผ่านเป็นอันดับแรก
4	การทำงานจะเป็นลักษณะ post-processing คือจะส่งจดหมายอิเล็กทรอนิกส์กลับไป rule set 3



รูปที่ 2.8 แสดง Rule Set ของโปรแกรม Sendmail

- aliases เมื่อมีจดหมายอิเล็กทรอนิกส์เข้ามา โปรแกรม Sendmail จะเข้าไปอ่านไฟล์ aliases ว่าจดหมายอิเล็กทรอนิกส์ควรจะส่งไปที่ใด ทั้งนี้ขึ้นอยู่กับจุดประสงค์ของการใช้งานอันได้แก่

ตารางที่ 2.6 แสดงการกำหนดค่าในไฟล์ aliases

จุดประสงค์	ตัวอย่าง	รายละเอียด
ใช้กำหนดนามแฝง	kchai: somchai	การกำหนดว่าหากมีจดหมายอิเล็กทรอนิกส์ส่งมาถึง kchai@host ให้ส่งจดหมายฉบับนี้ไปที่ตู้รับจดหมายที่ชื่อ somchai
ใช้กำหนดนามแฝงของผู้ใช้แบบเป็นกลุ่ม	all: ka, kb, kc	การกำหนดว่าหากมีจดหมายอิเล็กทรอนิกส์ส่งมาถึง all@host ให้ส่งจดหมายฉบับนี้ถึง ka@host , kb@host และ kc@host
ใช้กำหนดการเก็บจดหมายอิเล็กทรอนิกส์ไว้เป็นไฟล์	kchai: /savefile	การกำหนดว่าหากจดหมายอิเล็กทรอนิกส์ส่งมาถึง kchai@host ให้เก็บไว้เป็นไฟล์ชื่อ savefile
ใช้กำหนดการส่งจดหมายอิเล็กทรอนิกส์ไปยังโปรแกรม	kchai: |/filter	การกำหนดว่าหากมีจดหมายอิเล็กทรอนิกส์ส่งมาถึง kchai@host ให้ส่งจดหมายฉบับนี้ไปที่โปรแกรมชื่อ filter
ใช้กำหนดการส่งจดหมายอิเล็กทรอนิกส์ใช้ข้อมูลจาก mailing list	all: :include:/mail.list	การกำหนดว่าหากมีจดหมายอิเล็กทรอนิกส์ส่งมาถึง all@host ให้ส่งจดหมายฉบับนี้ไปยังรายชื่อที่อยู่ในรายการที่ชื่อว่า mail.list

- maillog เป็นไฟล์ที่ใช้บันทึกเหตุการณ์ที่เกี่ยวข้องกับระบบจดหมายอิเล็กทรอนิกส์ทั้งหมด ไม่ว่าจะเป็นวันเวลาที่จดหมายอิเล็กทรอนิกส์เข้า หรือ ออก ใครเป็นผู้ส่ง แล้วส่งถึงใคร รวมทั้งข้อความที่แสดงถึงความผิดพลาดต่าง ๆ (error message) เป็นต้น
- queue directory เป็นไดเร็คทรอรีที่ใช้เก็บจดหมายอิเล็กทรอนิกส์ที่รอการส่ง โดยจดหมายอิเล็กทรอนิกส์แต่ละฉบับจะแบ่งเป็น 2 ไฟล์คือ ไฟล์ที่เก็บ header จะขึ้นต้นด้วย qf ส่วนอีกไฟล์ใช้เก็บเนื้อหาของจดหมายอิเล็กทรอนิกส์ ซึ่งจะขึ้นต้นด้วย df

2.3 ไฟร์วอลล์ (Firewall)

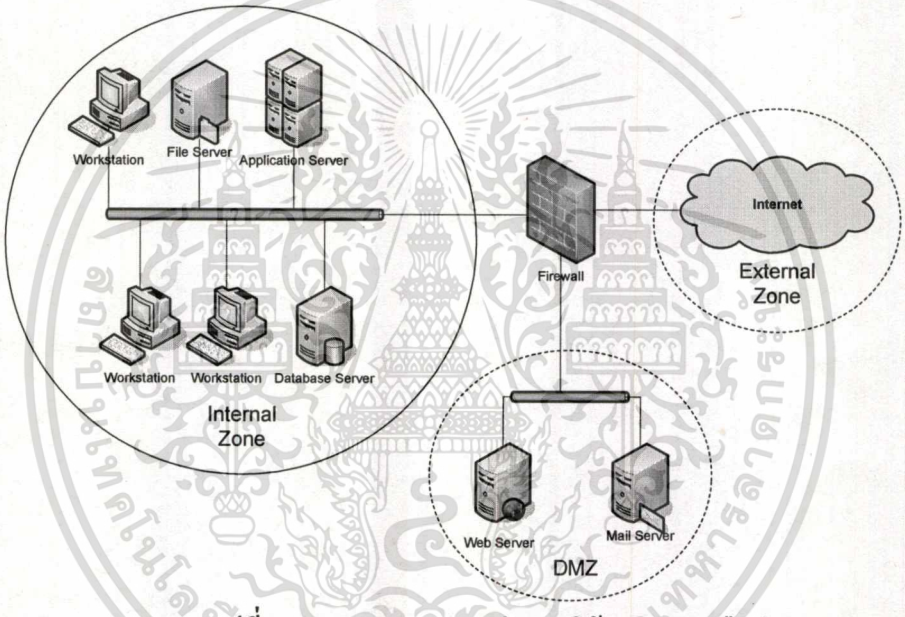
ไฟร์วอลล์เป็นระบบหรือกลุ่มระบบที่ทำหน้าที่ควบคุมการสื่อสารที่เกิดขึ้นระหว่างเครือข่ายอย่างน้อยสองเครือข่าย เพื่อให้การสื่อสารที่เกิดขึ้นเป็นไปตามนโยบายการเข้าถึง (Access Control Policy) ทรัพยากรของเครือข่าย

2.3.1 องค์ประกอบของระบบไฟร์วอลล์

การนำไฟร์วอลล์มาใช้งานให้บังเกิดผลในการป้องกันอย่างแท้จริงนั้น มิใช่อาศัยเพียงการจัดหาไฟร์วอลล์มาติดตั้งเท่านั้น ยังต้องอาศัยองค์ประกอบหลายประการที่สอดคล้องกัน ได้แก่

- นโยบายความปลอดภัย (Policy) เป็นสิ่งสำคัญขั้นพื้นฐานในการป้องกันและรักษาความปลอดภัยของการใช้งานทรัพยากรบนเครือข่าย โดยจะระบุเป็นข้อปฏิบัติ , ข้อห้าม ,ข้อจำกัด และหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง นโยบายที่ดีต้องมีความชัดเจนเข้าใจได้ง่ายและต้องคำนึงถึงความสมดุลระหว่างการใช้งานและในแง่ความปลอดภัย เพราะว่าทั้งสองประเด็นมักจะขัดแย้งกันเสมอ
- การออกแบบเครือข่าย เป็นขั้นตอนที่นำนโยบายมาดำเนินการให้เป็นรูปธรรม นอกจากนโยบายความปลอดภัยจะระบุให้มีการใช้ไฟร์วอลล์แล้ว ยังต้องคำนึงถึงตำแหน่งที่จะติดตั้งไฟร์วอลล์ที่เหมาะสม เพื่อที่ไฟร์วอลล์จะทำงานได้อย่างมีประสิทธิภาพ สามารถควบคุมความปลอดภัยของเครือข่ายได้อย่างเต็มที่ ดังนั้นก่อนที่จะนำไฟร์วอลล์ไปควบคุมจุดใด ๆ บนเครือข่าย จะต้องพิจารณาภาพรวมของเครือข่าย โดยมีหลักการดังต่อไปนี้
    - เครือข่ายจะต้องมีอาณาเขตที่ชัดเจน กล่าวคือในเครือข่ายมีการกำหนด IP address จากช่วงใดถึงช่วงใด มีช่องทางใดบ้างที่ใช้ในการติดต่อสื่อสารกันระหว่างภายในเครือข่ายและภายนอกเครือข่าย เพื่อที่จะได้นำไฟร์วอลล์ไปควบคุมช่องทางการติดต่อสื่อสารเหล่านั้นได้อย่างเหมาะสม

- การติดต่อสื่อสารที่เกิดขึ้นระหว่างภายในและภายนอกเครือข่ายจะต้องผ่านไฟร์วอลล์เท่านั้น
- แยกเครื่องบริการที่มีลักษณะการใช้งานต่างกันออกจากกัน เช่นเครื่องบริการที่เปิดบริการให้เฉพาะภายในเครือข่าย และเครื่องบริการที่เปิดให้บริการให้ทั้งภายในและภายนอกเครือข่าย ซึ่งควรจะแยกกลุ่มออกจากกันเป็นเครือข่ายย่อย โดยทั่วไปการออกแบบเครือข่ายจะแบ่งกลุ่มของเครื่องบริการออกเป็นโซน (Zone) คือ โซนภายใน , โซนภายนอก และดีมิลิทาไรซ์โซน (DeMilitarized Zone , DMZ) ดังแสดงในรูป 2.9



รูปที่ 2.9 แสดงการแยกกลุ่มการใช้งานของเครือข่าย

- การกำหนดกฎของไฟร์วอลล์ (Access Rule) เป็นส่วนที่สำคัญที่สุดเพราะเป็นแนวป้องกันของเครือข่ายที่จะทำการตรวจสอบกระแสข้อมูลที่ผ่านเข้าออกเครือข่าย โดยทั่วไปองค์ประกอบกฎของไฟร์วอลล์จะพิจารณาจากหลายปัจจัย ได้แก่ ต้นทางการสื่อสาร (Source) , ปลายทางการสื่อสาร (Destination) , บริการที่การสื่อสารใช้อยู่ (Service) และการปฏิบัติต่อการสื่อสารนั้น ๆ (Action) ในการตรวจสอบการสื่อสารที่ผ่านไฟร์วอลล์จะเปรียบเทียบกับกฎที่กำหนดขึ้นซึ่งจะเปรียบเทียบกับกฎที่ละข้อตามลำดับ

2.3.2 ประเภทของไฟร์วอลล์

ไฟร์วอลล์โดยทั่วไปแบ่งเป็น 2 ประเภทคือ

- Network Level ไฟร์วอลล์ประเภทนี้จะควบคุมการจราจรบนเครือข่าย โดยอาศัยข้อมูลจากเฮดเดอร์ของไอพีแพ็กเกต (IP packet) มาเปรียบเทียบกับกฎที่ผู้ดูแลระบบกำหนดขึ้น ว่าควรจะอนุญาตให้ แพ็กเกต ใดบ้างสามารถผ่านเข้าออกเครือข่ายได้ ด้วยเหตุที่ไฟร์วอลล์ประเภทนี้จะตรวจสอบข้อมูลจากแพ็กเกต ดังนั้นไฟร์วอลล์ประเภทนี้จึงเรียกอีกอย่างว่า "Packet Filtering"
- Application Level ไฟร์วอลล์ประเภทนี้เป็นโปรแกรมประยุกต์ที่ถูกพัฒนาขึ้นมาโดยเฉพาะทำงานบนเครื่องบริการที่ทำหน้าที่เป็นไฟร์วอลล์ (Firewall Host) โดยจะตั้งอยู่ระหว่างเครือข่าย คอยตรวจสอบกระแสข้อมูลที่ผ่าน ซึ่งการตรวจสอบของไฟร์วอลล์ประเภทนี้จะทำการตรวจสอบถึงระดับของแอพพลิเคชั่น (Application Layer) และไฟร์วอลล์ประเภทนี้เรียกอีกอย่างว่า " Proxy Service"

การทำงานของไฟร์วอลล์ประเภทนี้ เริ่มจากไคลเอนต์ต้องการใช้บริการจากภายนอกเครือข่าย ไคลเอนต์จะทำการติดต่อไปยังไฟร์วอลล์ก่อน ไคลเอนต์จะเจรจา (Negotiate) กับไฟร์วอลล์ เพื่อให้ไฟร์วอลล์ ติดต่อไปยังเครื่องบริการที่อยู่อีกเครือข่ายหนึ่งให้ เมื่อไฟร์วอลล์ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อสองการเชื่อมต่อ คือระหว่าง ไคลเอนต์กับไฟร์วอลล์ และ ไฟร์วอลล์กับเครื่องบริการที่อยู่อีกเครือข่ายหนึ่ง โดยที่ไฟร์วอลล์ จะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ในสองทิศทาง ทั้งนี้ไฟร์วอลล์จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันได้หรือไม่

2.3.3 ไฟร์วอลล์บนระบบปฏิบัติการลีนุกซ์

ระบบปฏิบัติการลีนุกซ์สามารถใช้งานเป็นไฟร์วอลล์ได้ตั้งแต่เคอร์เนล 1.1 ซึ่งเป็นเวอร์ชันแรก โดยอาศัยไฟร์วอลล์จากระบบปฏิบัติการบีเอสดี ที่มีชื่อว่า ipfw ต่อมาเคอร์เนล 2.0 ได้ถูกพัฒนาและปรับปรุงใหม่เรียกว่า ipfwadm และต่อมาเคอร์เนล 2.2 ก็ได้สร้างเครื่องมือตัวใหม่ชื่อ ipchains ซึ่งเผยแพร่ในปี 1998 ทั้งนี้ ipchains นี้ถือได้ว่าเป็นพัฒนาการขั้นที่สามของลีนุกซ์ไฟร์วอลล์ จนกระทั่งในปัจจุบันมีการพัฒนาไฟร์วอลล์สำหรับระบบปฏิบัติการลีนุกซ์ซึ่งมีชื่อเรียกว่า netfilter

2.3.4 Netfilter

Netfilter เป็นไฟร์วอลล์สำหรับระบบปฏิบัติการลีนุกซ์เคอร์เนลตั้งแต่เวอร์ชัน 2.4 และสามารถใช้งานร่วมกับ ipchains และ ipfwadm ซึ่งเป็นไฟร์วอลล์สำหรับระบบปฏิบัติการลีนุกซ์ที่มีเคอร์เนลต่ำกว่าเวอร์ชัน 2.4 ส่วนรูปแบบกฎของ Netfilter จะเป็นลักษณะเป็นสายของคำสั่ง (

chain) โดยการทำงานของ Netfilter จะเปรียบเทียบข้อมูลที่ผ่านไฟร์วอลล์กับกฎที่กำหนดจากลำดับแรกจนถึงลำดับสุดท้าย หากไม่ตรงกับกฎที่กำหนด Netfilter จะปฏิบัติตามกฎที่เป็นค่าปริยาย

รูปแบบการใช้งานคำสั่งของ Netfilter มีรูปแบบดังแสดงในรูปที่ 2.10

iptables [-t |- -table ***table*** **] –*command* [chain] [-i** ***interface*** **] [-p** ***protocol*** **[port [:** ***por t*** **]]] [-s** ***address*** **[port [:** ***port*** **]]] [-d** ***address*** **[port [:** ***port*** **]]] [-j** ***policy*** **]**

รูปที่ 2.10 แสดงรูปแบบคำสั่งของ Netfilter

จากรูปที่ 2.10 แสดงความหมายของค่าต่าง ๆ ของคำสั่ง Netfilter ดังต่อไปนี้

- iptables เป็นคำสั่งในการเรียกใช้งาน Netfilter
- -t or –table เป็นพารามิเตอร์ที่หมายถึงตารางที่รวบรวมกฎของไฟร์วอลล์ไว้ โดยแบ่งออกเป็น 4 ประเภท ดังแสดงในตารางที่ 2.7

ตารางที่ 2.7 แสดงรูปแบบตารางของ Netfiler

table	รายละเอียด
filter	เป็นตารางมาตรฐานประกอบด้วย 3 build – in chain คือ INPUT , OUTPUT และ FORWARD chain
NAT	ใช้ในการแปลงไอพีแอดเดรส (Network Address Translation)
mangle	ใช้ในเรื่องคุณภาพการใช้บริการ (Quality Of Service)
(กำหนดขึ้นเอง)	เป็นตารางที่ผู้ใช้กำหนดขึ้นเอง

- command หมายถึงตัวที่ระบุให้ Netfilter ทำอะไร ซึ่งมีรายละเอียดดังตารางที่ 2.8

ตารางที่ 2.8 แสดงรูปแบบพารามิเตอร์คำสั่งของ Netfilter

command	รายละเอียด
-A	ระบุการเพิ่มกฎแบบต่อท้ายกฎที่มีอยู่แล้ว (Append)
-D	ระบุการลบกฎ (Delete)
-I	ระบุการเพิ่มกฎแบบให้อยู่ลำดับแรกของกฎที่มีอยู่ (Insert)
-R	ระบุการแทนที่กฎเดิมด้วยกฎใหม่ (Replace)

ตารางที่ 2.8 (ต่อ)

command	รายละเอียด
-F	ระบุการลบกฎทั้งหมดในสายคำสั่ง (Flush)
-Z	ระบุการ reset byte counter สำหรับทุกกฎ
-L	ระบุการแสดงกฎทั้งหมดในสายคำสั่ง (List)
-N	ระบุการสร้างสายของคำสั่งใหม่ (New)
-X	ระบุการลบสายคำสั่งที่ผู้ใช้กำหนดขึ้นเอง ซึ่งจะไม่สามารถลบ build – in chain ได้
-P	ระบุค่าปริยายของสายคำสั่ง ซึ่งจะมีค่าได้ 2 ค่า คือ ACCEPT และ DROP (Policy)
-E	ระบุการเปลี่ยนชื่อของสายคำสั่ง

- -i interface เป็นการระบุ network interface ที่แพ็กเกตผ่าน
- -p protocol เป็นการระบุโปรโตคอล เช่น ทีซีพี , ยูดีพี หรือ ไอซีเอ็มพี เป็นต้น
- port เป็นการระบุหมายเลขพอร์ต
- -s และ –d address เป็นการระบุไอพีแอดเดรสของต้นทางและปลายทางตามลำดับ
- -j policy เป็นการระบุว่าถ้าแพ็กเกตที่ผ่านเข้ามา ตรงกับกฎที่กำหนดไว้จะต้องทำอย่างไรต่อแพ็กเกตนั้น โดยมีรายละเอียดดังตารางที่ 2.9

ตารางที่ 2.9 แสดงการปฏิบัติต่อแพ็กเกตเมื่อผ่านไฟร์วอลล์

policy	รายละเอียด
ACCEPT	ให้แพ็กเกตที่เข้ามาสามารถผ่านได้
DROP	ปฏิเสธแพ็กเกตที่เข้ามา
REJECT	คล้ายกับ DROP แต่จะส่งข้อความของไอซีเอ็มพีกลับไปยังต้นทาง
RETURN	การเปรียบเทียบแพ็กเกตกับกฎ ให้ออกจากสายคำสั่งปัจจุบันไปที่ค่าปริยาย
MASQUERADE	เปลี่ยนไอพีแอดเดรส โดยใช้กับ DHCP
QUEUE	ส่งแพ็กเกตไปที่โปรแกรมที่กำหนดขึ้น
REDIRECT	ส่งแพ็กเกตไปที่ที่กำหนดเช่นจากพอร์ตหมายเลข 80 ไปหมายเลข 8080

ตารางที่ 2.9 (ต่อ)

policy	รายละเอียด
SNAT	ให้เปลี่ยนไอพีแอดเดรสของแพ็กเกตที่จะส่งออกไป หรือเรียกว่า Post-routing
DNAT	ให้เปลี่ยนไอพีแอดเดรสของแพ็กเกตที่จะรับเข้ามา หรือเรียกว่า Pre-routing
LOG	มีการบันทึกว่ามีแพ็กเกตเข้ามา โดยจะมีการใช้งาน 2 รูปแบบคือ –log-level เป็นการระบุลำดับก่อนหลัง ส่วนอีกรูปแบบหนึ่งคือ –log-prefix เป็นการระบุอักษรหรือประโยคให้ปรากฏในบันทึก

2.3.5 ตัวอย่างคำสั่งของ Netfilter

ตัวอย่างคำสั่งของ Netfilter ดังแสดงในตารางที่ 2.10

ตารางที่ 2.10 แสดงตัวอย่างการใช้คำสั่งของ Netfilter

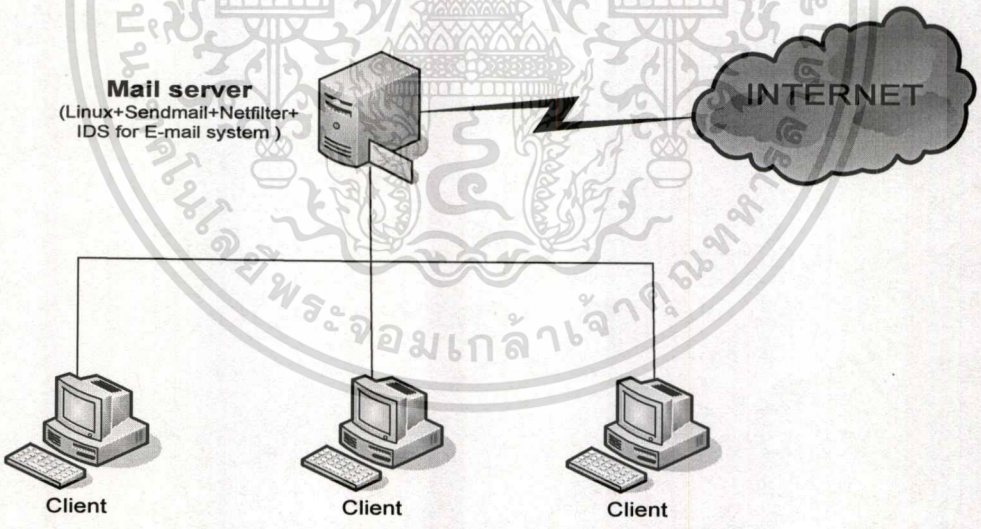
รูปแบบคำสั่ง	รายละเอียด
iptables –L	แสดงกฎทั้งหมดของสายคำสั่ง
iptables –A INPUT –p ALL –I eth0 –j DROP	การเพิ่มกฎในรูปแบบต่อท้ายกฎเดิมของ build – in chain ที่ชื่อ INPUT โดยระบุให้ปฏิเสธทุกแพ็กเกตที่เข้ามาทาง interface eth0
iptables –D INPUT –p ALL –I eth0 –j DROP	การลบกฎของ build – in chain ที่ชื่อ INPUT โดยที่กฎนั้นเป็นการปฏิเสธทุกแพ็กเกตที่เข้ามาทาง interface eth0
iptables –F INPUT	ลบกฎทั้งหมดของสายคำสั่ง INPUT
iptables –N mychains	สร้างสายคำสั่งใหม่ที่ชื่อ mychains
iptables –X mychains	ลบสายคำสั่งที่ชื่อ mychains
iptables –E myoldchain mynewchain	เปลี่ยนชื่อสายคำสั่งที่ชื่อ myoldchain เป็น mynewchain

บทที่ 3

การวิเคราะห์และออกแบบระบบ

เนื้อหาในบทที่ 2 ได้นำเสนอรายละเอียดในสิ่งที่จำเป็นต่อการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ ส่วนในบทที่ 3 จะได้กล่าวถึงขั้นตอนการออกแบบระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ โดยจะอธิบายถึงภาพรวมของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ สถานะของจดหมายอิเล็กทรอนิกส์ที่เข้าสู่ระบบ การไหลของกระแสข้อมูลภายในระบบ และสุดท้ายจะกล่าวถึงขั้นตอนการทำงานของระบบ

3.1 ภาพรวมของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

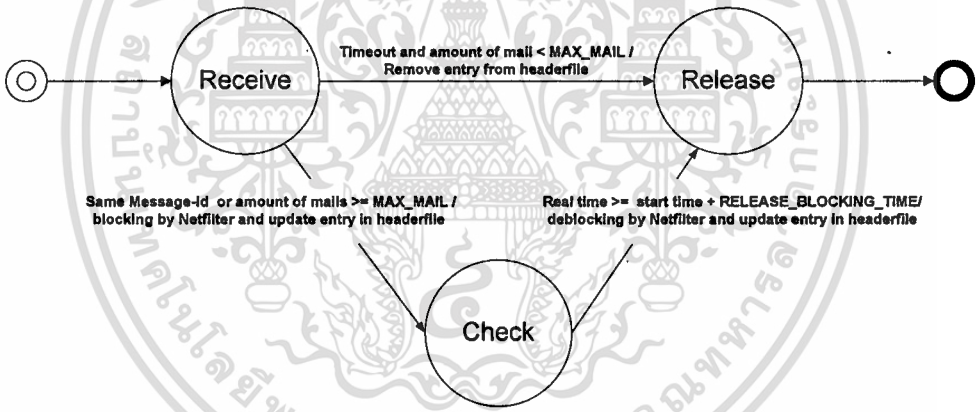


รูปที่ 3.1 แสดงตำแหน่งที่ติดตั้งระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

รูปที่ 3.1 เป็นการแสดงตำแหน่งที่ใช้ในการติดตั้งระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์และสภาพแวดล้อมของการทำงาน โดยจะติดตั้งบนเครื่องบริการจดหมายอิเล็กทรอนิกส์ที่ทำงานบนระบบปฏิบัติการลีนุกซ์ ส่วนโปรแกรมประเภท MTA ที่ใช้คือโปรแกรม Sendmail และโปรแกรม Netfilter ซึ่งเป็นโปรแกรมประเภทไฟร์วอลล์ การทำงานของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ เริ่มจากเมื่อมีจดหมายเข้ามา ระบบจะทำ

การตรวจสอบ header ของจดหมาย โดยจะค้นหาเลขทะเบียนจดหมายอิเล็กทรอนิกส์ (Message-Id) , ไอพีแอดเดรสของผู้ส่ง และไอพีแอดเดรสของเครื่องบริการที่ส่งผ่านจดหมาย (RELAY) เก็บไว้ในไฟล์ที่ชื่อ headerfile ซึ่งไฟล์นี้จะใช้ในการตรวจสอบเลขทะเบียนจดหมายอิเล็กทรอนิกส์ และไอพีแอดเดรสของผู้ส่ง หากตรวจพบกรณีใดกรณีหนึ่งดังนี้ จะส่งคำสั่งให้โปรแกรม Netfilter ปฏิเสธการเชื่อมต่อกับผู้ส่งนั้น กรณีแรกคือจดหมายที่เข้ามามีเลขทะเบียนจดหมายอิเล็กทรอนิกส์มีค่าซ้ำกันจากผู้ส่งแหล่งเดียวกัน เพราะว่าเลขทะเบียนจดหมายอิเล็กทรอนิกส์เป็นค่าเฉพาะไม่ซ้ำกัน กรณีที่สองคือ มีจำนวนจดหมายจากผู้ส่งแหล่งเดียวกันเข้ามาในช่วงเวลาที่กำหนดเกินกว่าจำนวนที่ได้กำหนดไว้ หลังจากนั้นหากครบเวลาที่ได้กำหนดไว้ ระบบจะส่งคำสั่งให้โปรแกรม Netfilter ยกเลิกการปฏิเสธการเชื่อมต่อจากผู้ส่งนั้น เพื่อให้สามารถใช้งานได้ตามปกติ

3.2 สถานะของการตรวจจับการบุกรุก



รูปที่ 3.2 แสดงสถานะของการตรวจจับการบุกรุก

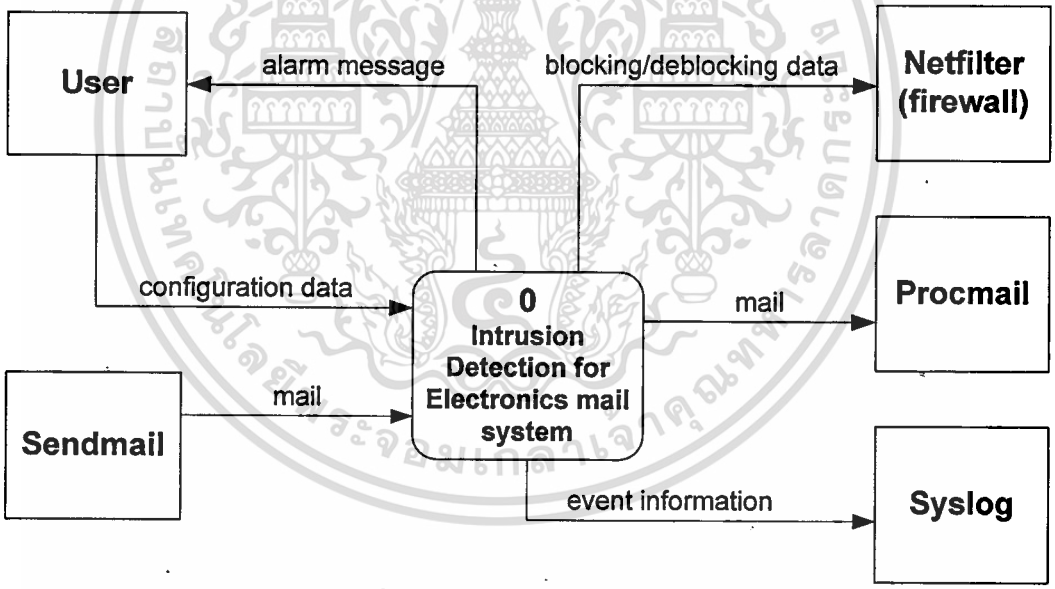
จากรูปที่ 3.2 สามารถอธิบายการเปลี่ยนสถานะของจดหมายอิเล็กทรอนิกส์ได้ดังนี้

- Receive เป็นสถานะของจดหมายที่ถูกส่งมาถึงผู้รับที่เป็นสมาชิกของระบบจดหมายอิเล็กทรอนิกส์ (Local)
- Check เป็นสถานะที่ระบบตรวจพบว่ามีการส่งจดหมายอิเล็กทรอนิกส์เข้ามาเข้ามาใน2 ลักษณะคือ
    - จำนวนจดหมายที่ส่งมาจากผู้ส่งแหล่งเดียวกันเข้ามามีค่าเกินกว่าค่าที่กำหนดไว้ในช่วงเวลาหนึ่ง ๆ หรือ
    - จดหมายที่ส่งมาจากผู้ส่งแหล่งเดียวกันมีเลขทะเบียนจดหมายซ้ำกัน
- Release การจะเปลี่ยนเป็นสถานะ Release ได้จะต้องเป็นกรณีใดกรณีหนึ่งในสองกรณีนี้

- มีสถานะ Receive มาก่อนและตรวจพบว่าจำนวนจดหมายที่ส่งเข้ามาจากผู้ส่งแหล่งเดียวกันมีค่าน้อยกว่าค่าที่ได้กำหนดไว้ และเวลาครบตามค่าเวลาที่ได้กำหนดไว้ (timeout)
- มีสถานะ Check มาก่อนและเวลาครบตามค่าเวลาที่ได้กำหนดไว้ (Release blocking time)

3.3 การออกแบบระบบตรวจจับการการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

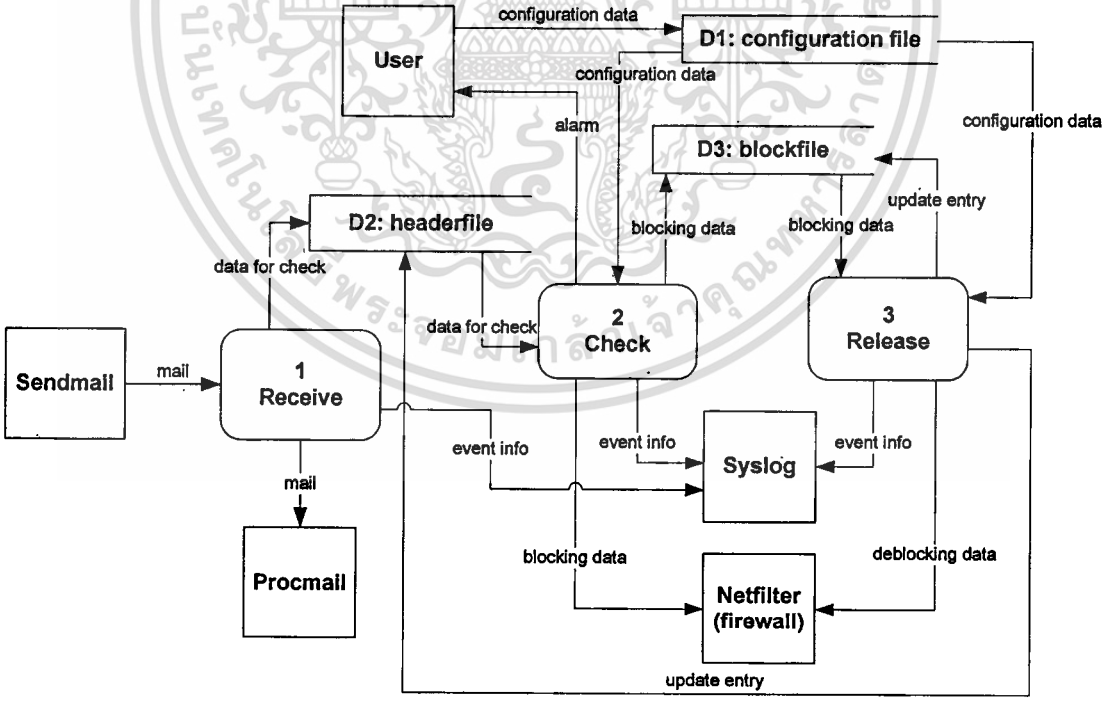
เมื่อทราบสถานะของการส่งจดหมายอิเล็กทรอนิกส์จากหัวข้อที่ผ่านมา สามารถวิเคราะห์และออกแบบระบบ โดยเขียนเป็นแผนภาพแบบ Context Diagram แสดงถึงการติดต่อระหว่างระบบกับสภาพแวดล้อมอันได้แก่ โปรแกรม Sendmail , โปรแกรม Netfilter , โปรแกรม Procmail , โปรแกรม Syslog และผู้ใช้ ดังแสดงในรูปที่ 3.3



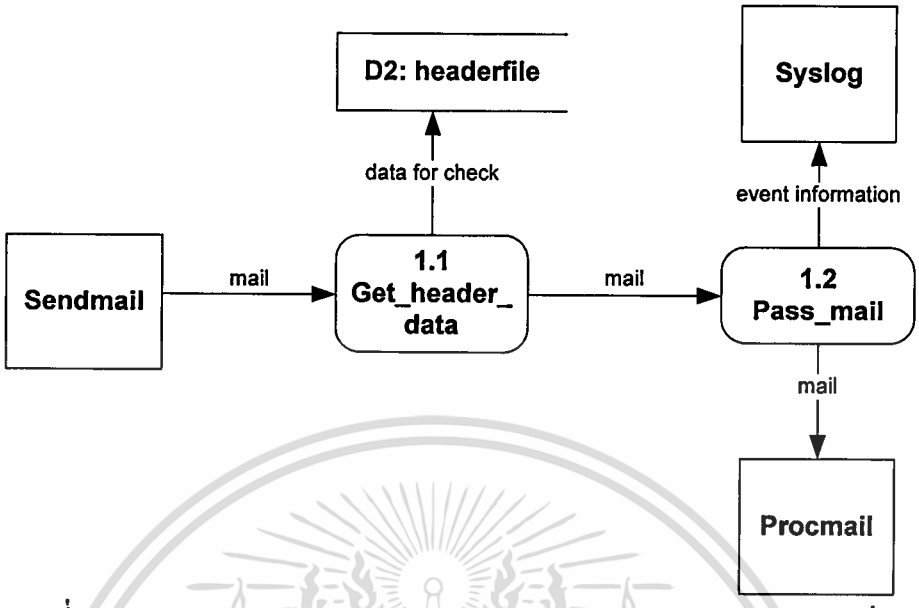
รูปที่ 3.3 แสดง Context Diagram
ของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

และเพื่อให้เห็นถึงรายละเอียดของกระบวนย่อยของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์มากขึ้น จะแสดงด้วยแผนภาพในระดับ 0 ดังรูปที่ 3.4 โดยประกอบด้วยกระบวนการย่อย 3 กระบวนการคือ

- Receive เป็นกระบวนการที่ทำหน้าที่รับจดหมายมาจากโปรแกรม Sendmail พร้อมกับเก็บข้อมูล header ของจดหมายไว้ในไฟล์ headerfile จากนั้นก็ส่งจดหมายให้โปรแกรม Procmail
- Check เป็นกระบวนการที่ตรวจสอบจดหมายที่เข้ามาเป็นการโจมตีหรือไม่ ถ้าหากเป็นการโจมตี กระบวนการนี้จะเรียกใช้โปรแกรม Netfilter ทำการปฏิเสธการให้บริการและบันทึกข้อมูลการปฏิเสธการให้บริการเก็บไว้ในไฟล์ blockfile พร้อมทั้งส่งข้อความเตือนผู้ดูแลระบบ
- Release เป็นกระบวนการที่ทำหน้าที่ตรวจสอบการยกเลิกการปฏิเสธการให้บริการโดยอาศัยข้อมูลจากไฟล์ blockfile และจัดการกับข้อมูลในไฟล์ headerfile ที่ถึงเวลา timeout เพื่อไม่ให้ไฟล์มีขนาดใหญ่จนเกินไป



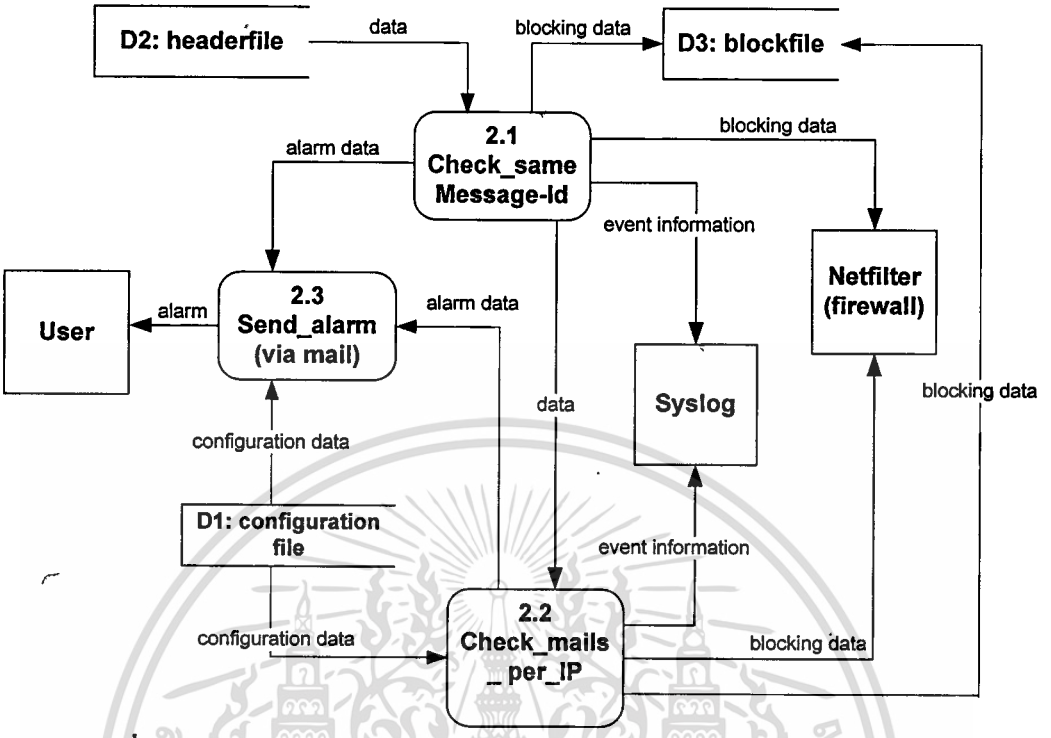
รูปที่ 3.4 แสดงแผนภาพการไหลของกระแสข้อมูลในระดับ 0



รูปที่ 3.5 แสดงแผนภาพการไหลของกระแสข้อมูลในระดับ 1 กระบวนการที่ 1

จากรูปที่ 3.5 แสดงรายละเอียดการไหลของกระแสข้อมูลในระดับ 1 กระบวนการที่ 1 ซึ่งมีกระบวนย่อยคือ

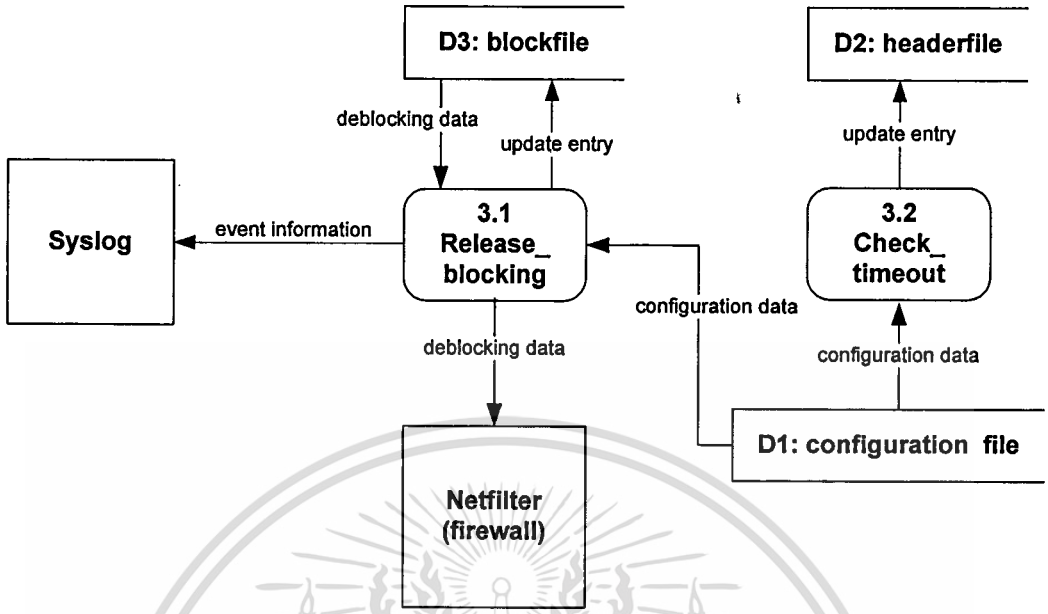
- Get_header_data เป็นกระบวนการจัดเก็บข้อมูลจาก header ของจดหมายไว้ในไฟล์ headerfile
- Pass_mail เป็นกระบวนการส่งจดหมายที่ได้รับมาส่งต่อให้โปรแกรม Procmail และบันทึกเหตุการณ์โดยอาศัยกลไกของ Syslog



รูปที่ 3.6 แสดงแผนภาพการไหลของกระแสข้อมูลในระดับ 1 กระบวนการที่ 2

จากรูปที่ 3.6 แสดงรายละเอียดการไหลของกระแสข้อมูลในระดับ 1 กระบวนการที่ 2 ซึ่งมีกระบวนย่อยคือ

- Check_same_Message-Id เป็นกระบวนการตรวจสอบการโจมตีในรูปแบบของเลขทะเบียนจดหมายอิเล็กทรอนิกส์ที่ซ้ำกัน จากการส่งจากผู้ส่งแหล่งเดียวกัน หากตรวจพบว่ามีการโจมตีเกิดขึ้น จะส่งคำสั่งให้โปรแกรม Netfilter ทำการปฏิเสธการให้บริการแก่ผู้ส่งนั้น และทำการบันทึกข้อมูลการปฏิเสธการให้บริการไว้ในไฟล์ blockfile
- Check_mails_per_IP เป็นกระบวนการตรวจสอบการโจมตีในรูปแบบการส่งจดหมายในจำนวนที่เกินกว่าที่กำหนดไว้ จากการส่งจากผู้ส่งแหล่งเดียวกันในช่วงเวลาหนึ่ง หากตรวจพบว่ามีการโจมตีเกิดขึ้น ก็จะปฏิบัติเช่นเดียวกับกระบวนการ Check_same_Message-Id
- Send_alarm เป็นกระบวนการส่งข้อความเตือนแก่ผู้ดูแลระบบหากมีการโจมตีเกิดขึ้น

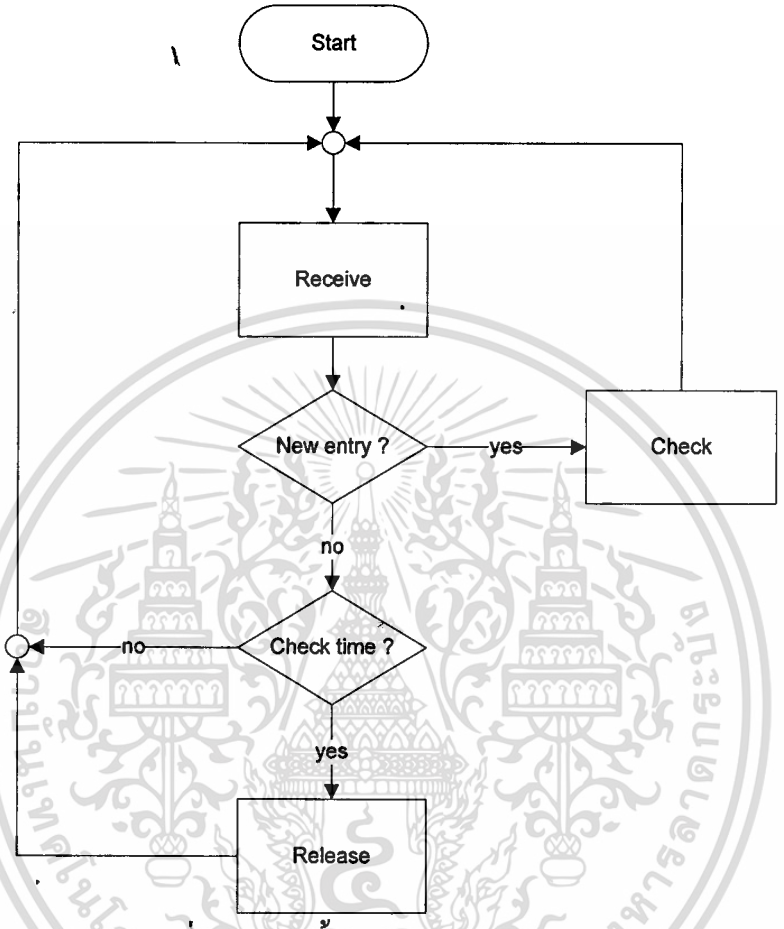


รูปที่ 3.7 แสดงแผนภาพการไหลของกระแสข้อมูลในระดับ 1 กระบวนการที่ 3

จากรูปที่ 3.6 แสดงรายละเอียดการไหลของกระแสข้อมูลในระดับ 1 กระบวนการที่ 3 ซึ่งมีกระบวนย่อยคือ

- Release_blocking เป็นกระบวนการที่ตรวจสอบการยกเลิกการปฏิเสธการให้บริการ หากถึงเวลาที่กำหนดจะส่งคำสั่งเรียกใช้โปรแกรม Netfilter ยกเลิกการปฏิเสธการให้บริการ โดยอาศัยข้อมูลจาก blockfile
- Check_timeout เป็นกระบวนการที่จัดการข้อมูลในไฟล์ headerfile ที่ถึงเวลา timeout เพื่อมิให้ไฟล์มีขนาดใหญ่จนเกินไป

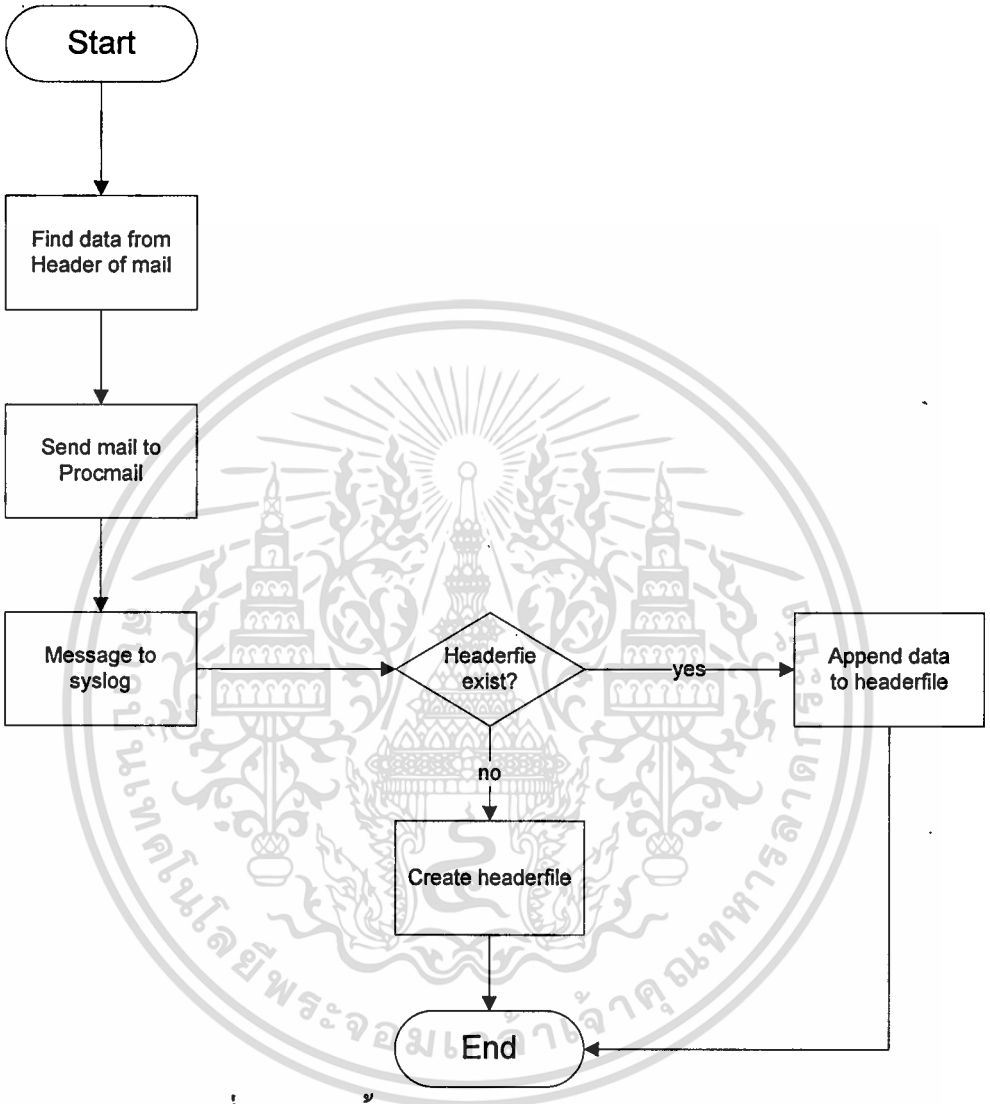
3.4 ขั้นตอนการทำงานของระบบตรวจจับการการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์



รูปที่ 3.8 แสดงขั้นตอนการทำงานโดยรวมของระบบ

จากรูปที่ 3.8 แสดงภาพรวมการทำงานของระบบ โดยลักษณะการทำงานมีการวนซ้ำเพื่อตรวจสอบจดหมายที่เข้ามายังระบบจดหมายอิเล็กทรอนิกส์ โดยประกอบด้วยกระบวนการย่อย 3 ส่วน คือ Receive , Check และ Release ซึ่งรายละเอียดจะได้กล่าวในหัวข้อต่อไป

3.4.1 ขั้นตอนการทำงานในส่วนของกระบวนการย่อย Receive



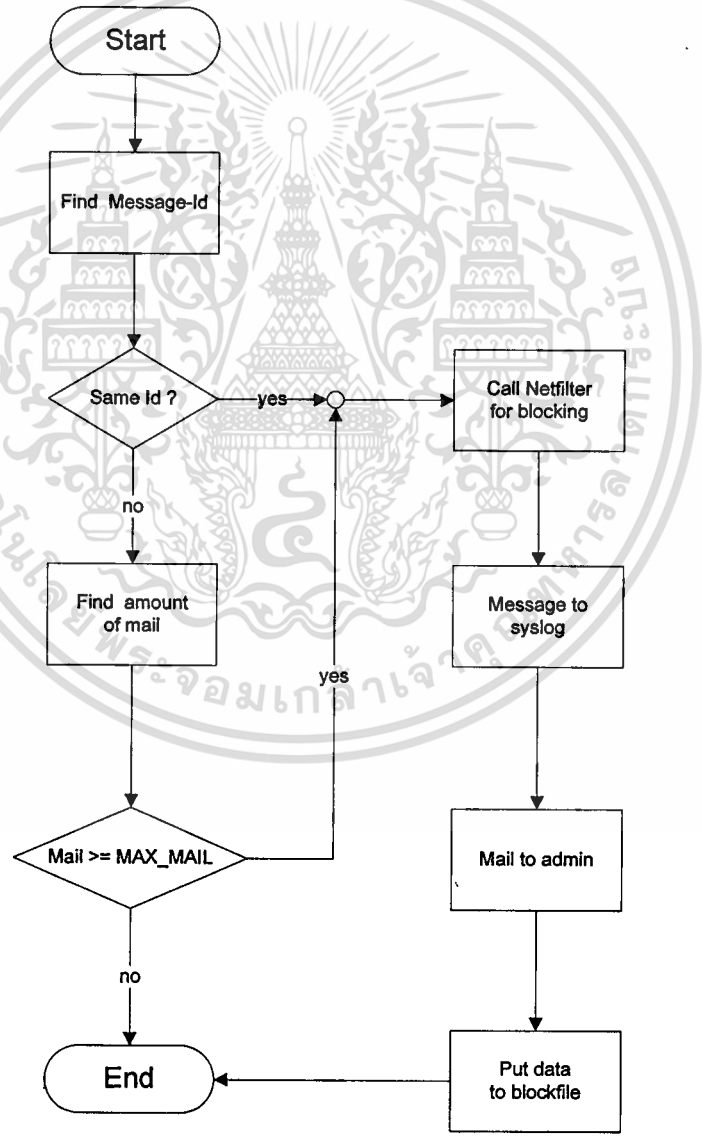
รูปที่ 3.9 แสดงขั้นตอนการทำงานของกระบวนการย่อย Receive

จากรูปที่ 3.9 แสดงขั้นตอนการทำงานของกระบวนการย่อย Receive จากแผนภาพการไหลของกระแสข้อมูลในระดับ 0 ซึ่งสามารถอธิบายลำดับการทำงานได้ดังต่อไปนี้

1) เมื่อจดหมายเข้ามา ระบบจะค้นหาข้อมูลของ Header อันได้แก่ เลขทะเบียนจดหมายอิเล็กทรอนิกส์ และไอพีแอดเดรสของผู้ส่ง
2) ส่งต่อจดหมายที่เข้ามาให้แก่โปรแกรม Promail
3) บันทึกเหตุการณ์การส่งจดหมาย โดยใช้กลไกของ Syslog

4) ตรวจสอบว่ามีไฟล์ที่ชื่อ /etc/guardmail/headerfile หรือไม่ หากพบว่ามีให้ทำข้อ 5) หากไม่พบให้ทำในข้อ 6)
5) นำข้อมูลที่ได้จากข้อ 1) มาเก็บไว้ในไฟล์ headerfile แบบต่อท้ายข้อมูลใหม่
6) สร้างไฟล์ headerfile และนำข้อมูลที่ได้จากข้อ 1) มาเก็บ
7) สิ้นสุดการทำงานของส่วนย่อยนี้

3.4.2 ขั้นตอนการทำงานในส่วนของกระบวนการย่อย Check

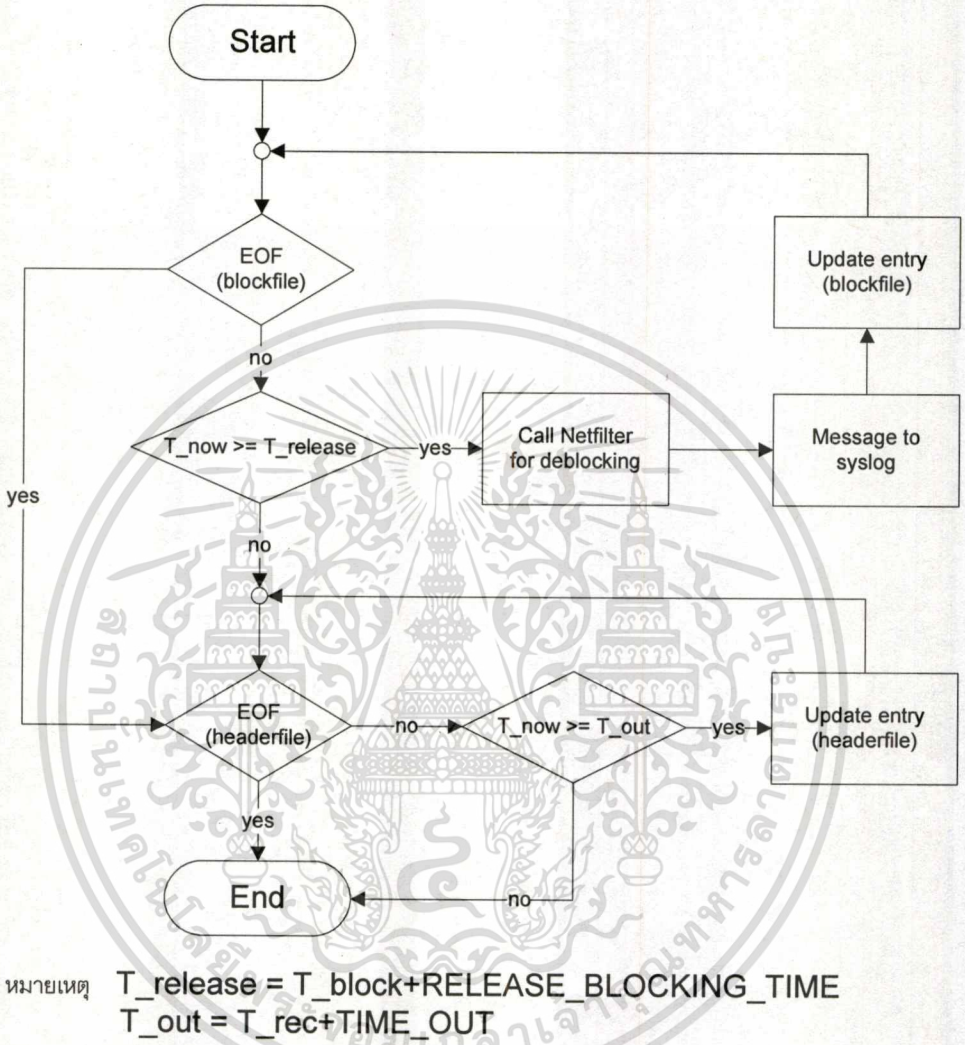


รูปที่ 3.10 แสดงขั้นตอนการทำงานในส่วนของกระบวนการย่อย Check

จากรูปที่ 3.10 แสดงขั้นตอนการทำงานของกระบวนการย่อย Check จากแผนภาพการไหลของกระแสข้อมูลในระดับ 0 ซึ่งสามารถอธิบายลำดับการทำงานได้ดังต่อไปนี้

1) ตรวจสอบข้อมูลในไฟล์ headerfile ว่ามีจดหมายที่ส่งจากผู้ส่งเดียวกัน มีเลขทะเบียนซ้ำกันหรือไม่ ถ้าพบว่ามีซ้ำกันให้ทำในข้อ 2) และหากไม่พบให้ทำในข้อ 7)
2) ส่งคำสั่งไปให้โปรแกรม Netfilter ปฏิเสธการให้บริการจากผู้ส่งจดหมายนั้น
3) บันทึกเหตุการณ์การปฏิเสธการให้บริการ โดยใช้กลไกของ Syslog
4) ส่งจดหมายเตือนไปยังผู้ดูแลระบบ เกี่ยวกับเหตุการณ์ที่เกิดขึ้น
5) เก็บข้อมูลในไฟล์ blockfile
6) สิ้นสุดการทำงานของส่วนการทำงานย่อย Check
7) ตรวจสอบจดหมายที่ส่งจากผู้ส่งแหล่งเดียวกันมีจำนวนมากเกินกว่าค่าที่ได้กำหนดในช่วงเวลาที่กำหนด ตามเงื่อนไข mails >= MAX_MAIL หากพบว่าตรงกับเงื่อนไข ให้วนไปทำในข้อ 2) หากไม่ตรงกับเงื่อนไข ให้ทำในข้อ 6)

3.4.3 ขั้นตอนการทำงานในส่วนของกระบวนการย่อย Release



รูปที่ 3.11 แสดงขั้นตอนการทำงานในส่วนของกระบวนการย่อย Release

จากรูปที่ 3.11 แสดงขั้นตอนการทำงานของกระบวนการย่อย Release จากแผนภาพการไหลของกระแสข้อมูลในระดับ 0 ซึ่งสามารถอธิบายลำดับการทำงานได้ดังต่อไปนี้

1) ตรวจสอบว่าข้อมูลใน blockfile ได้รับการตรวจหมดหรือยัง ถ้าตรวจหมดทั้งไฟล์แล้วให้ทำในข้อ 6) หากยังตรวจไม่หมดให้ทำในข้อ 2)
2) ตรวจสอบข้อมูลใน blockfile ว่ามีข้อมูลที่เป็นการปฏิเสธการให้บริการถึงเวลาที่จะยกเลิกหรือยัง (T_now >= T_release) ถ้ายังไม่ถึงเวลาให้ไปทำในข้อ 6) แต่ถ้าหากถึงเวลาที่ยกเลิกให้ไปทำในข้อ 3)

3) เรียกใช้โปรแกรม Netfilter ทำการยกเลิกการปฏิเสธการให้บริการ

4) บันทึกเหตุการณ์ โดยอาศัยกลไกของ Syslog

5) ลบข้อมูลที่ได้ทำการยกเลิกการปฏิเสธการให้บริการในไฟล์ blockfile แล้ววนกลับไปทำในข้อ 1)

6) ตรวจสอบข้อมูลในไฟล์ headerfile ได้รับการตรวจหมดหรือยัง ถ้าตรวจหมดแล้วให้ทำในข้อ 9) แต่หากยังไม่หมดให้ไปทำในข้อ 7)

7) ตรวจสอบข้อมูลในไฟล์ headerfile ว่าถึงเวลา timeout หรือยัง (T_now >= T_out) ถ้ายังให้ไปทำในข้อ 9) แต่หากถึงเวลา timeout แล้วให้ไปทำในข้อ 8)

8) ลบข้อมูลที่ครบกำหนดเวลา timeout ออกจาก headerfile แล้ววนกลับไปทำในข้อ 6)

9) สิ้นสุดการทำงานของการบวนการย่อย Release

3.5 รูปแบบข้อมูลที่ใช้ในการทำงานของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

จากการออกแบบระบบ มีไฟล์ที่ใช้ในการจัดเก็บข้อมูล 3 ไฟล์ ซึ่งแต่ละไฟล์มีรูปแบบของข้อมูลที่ใช้ในกระทำงานของระบบดังต่อไปนี้

- Configuration file เป็นไฟล์ที่ใช้จัดเก็บข้อมูลสำหรับเป็นค่าเริ่มต้นการทำงานของระบบ ซึ่งประกอบด้วยฟิลด์ต่าง ๆ โดยมีรายละเอียดดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 แสดงความหมายและประเภทข้อมูลของ Configuration file

ฟิลด์	ประเภท	รายละเอียด
RELEASE_BLOCKING_TIME	เลขจำนวนเต็มบวก	เป็นค่าเวลาที่ใช้ในการยกเลิกการปฏิเสธการให้บริการ มีหน่วยเป็นวินาที
INTERVAL_TIME	เลขจำนวนเต็มบวก	เป็นค่าช่วงเวลาที่ใช้ในการตรวจสอบจดหมายที่เข้ามา มีหน่วยเป็นวินาที
MAX_MAIL	เลขจำนวนเต็มบวก	เป็นจำนวนจดหมายมากที่สุดที่สามารถส่งมาได้ ในช่วงเวลา INTERVAL_TIME
TIME_OUT	เลขจำนวนเต็มบวก	เป็นค่าเวลาที่ใช้ในการจัดการกับข้อมูลที่เกิดจากระบบ เพื่อไม่ให้ไฟล์มีขนาดใหญ่จนเกินไป

ตารางที่ 3.1 (ต่อ)

ฟิลด์	ประเภท	รายละเอียด
MAIL_TO	อักษร	เป็นค่าที่เก็บที่อยู่ ที่จะส่งข้อความเตือน เช่น root@localhost

- headerfile เป็นไฟล์ที่จัดเก็บข้อมูลที่ได้จากส่วน header ของจดหมายอิเล็กทรอนิกส์และระบบสร้างขึ้นเองเพื่อใช้ในการทำงาน โดยมีรายละเอียดดังแสดงในตารางที่ 3.2

ตารางที่ 3.2 แสดงความหมายและประเภทข้อมูลของ headerfile

ฟิลด์	ประเภท	รายละเอียด
Message-Id	อักษร	เก็บค่าของเลขทะเบียนจดหมายอิเล็กทรอนิกส์
Host_Relay	เลขจำนวนเต็มบวก (คั่นด้วย .)	เก็บค่าไอดีแอดเดรสของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ให้บริการ RELAY
Host_Source	เลขจำนวนเต็มบวก (คั่นด้วย .)	เก็บค่าไอดีแอดเดรสของเครื่องที่ส่งจดหมายอิเล็กทรอนิกส์
Time	เลขจำนวนเต็มบวก	เก็บค่าเวลารับจดหมายเข้ามา หน่วยเป็นวินาที
Checked	อักษร	เก็บค่าสถานะ มี 2 ค่า คือ NO หมายถึงจดหมายที่ส่งมามีจำนวนไม่เกินที่กำหนด ส่วน YES หมายถึงจดหมายที่ส่งมามีจำนวนที่เท่ากับหรือมากกว่าค่าที่ได้กำหนด

- blockfile เป็นไฟล์ที่จัดเก็บข้อมูลที่เกี่ยวกับการปฏิเสธการให้บริการ ซึ่งประกอบด้วยฟิลด์ต่าง ๆ โดยมีรายละเอียดดังแสดงในตารางที่ 3.3

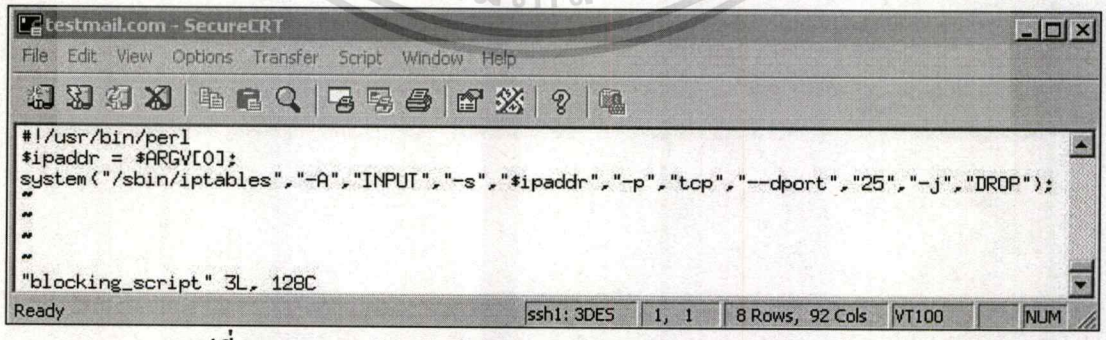
ตารางที่ 3.3 แสดงความหมายและประเภทข้อมูลของ blockfile

ฟิลด์	ประเภท	รายละเอียด
IP_Address	เลขจำนวนเต็มบวก (คั่นด้วย .)	เก็บค่าไอดีแอดเดรสของเครื่องที่โจมตีระบบจดหมายอิเล็กทรอนิกส์
Time	เลขจำนวนเต็มบวก	เก็บค่าเวลาที่เริ่มต้นการปฏิเสธการให้บริการ มีหน่วยเป็นวินาที
Alarm	อักษร	เก็บค่าสถานะ มี 2 ค่าคือ NO หมายถึงยังไม่ได้ส่งข้อความเตือน ส่วน YES หมายถึงได้ส่งข้อความเตือนแล้ว

3.6 รูปแบบการส่งคำสั่งให้โปรแกรม Netfilter

- การปฏิเสธการให้บริการ

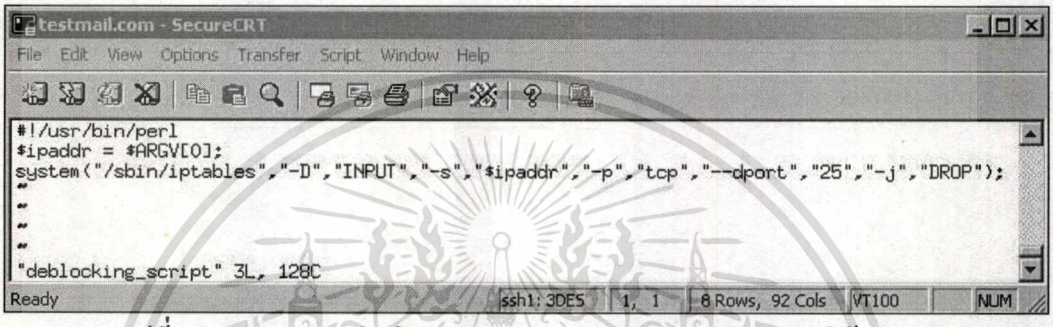
  การส่งคำสั่งให้โปรแกรม Netfilter ทำการปฏิเสธการให้บริการ จะเรียกใช้โปรแกรมที่ถูกสร้างขึ้นมาเพื่อเรียกใช้โปรแกรม Netfilter ซึ่งเป็นสคริปต์ที่เขียนด้วยเพิร์ล โดยอาศัยข้อมูลในไฟล์ blockfile คือค่าไอพีแอดเดรส ที่ต้องการให้ระงับการให้บริการ ส่งให้โปรแกรมนี้ทำการเรียกใช้โปรแกรม Netfilter ตัวอย่างโปรแกรมจัดการการปฏิเสธการให้บริการแสดงในรูปที่ 3.12



รูปที่ 3.12 แสดงตัวอย่างโปรแกรมจัดการการปฏิเสธการให้บริการ

- การยกเลิกการปฏิเสธการให้บริการ

การส่งคำสั่งให้โปรแกรม Netfilter ทำการยกเลิกการปฏิเสธการให้บริการ จะเรียกใช้โปรแกรมที่ถูกสร้างขึ้นมาเพื่อเรียกใช้โปรแกรม Netfilter โดยการทำงานจะเหมือนกับกรณีการจัดการการปฏิเสธการให้บริการ ตัวอย่างโปรแกรมจัดการการยกเลิกการปฏิเสธการให้บริการดังแสดงในรูปที่ 3.13



รูปที่ 3.13 แสดงตัวอย่างโปรแกรมจัดการยกเลิกการปฏิเสธการให้บริการ

บทที่ 4

การพัฒนาและการทดสอบระบบงาน

ในบทนี้จะกล่าวถึงการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ ซึ่งประกอบด้วยการพัฒนาบนสภาวะแวดล้อมของระบบปฏิบัติการ ภาษาที่เลือกใช้ และเครื่องที่จำเป็นต่าง ๆ ที่ใช้ในการพัฒนาระบบ ส่วนการทดสอบการทำงานของระบบได้จำลองการใช้งานแบบปกติและสร้างสถานการณ์จำลองการโจมตีระบบจดหมายอิเล็กทรอนิกส์

4.1 การพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ ต้องอาศัยส่วนประกอบและเครื่องมือที่ใช้ในการพัฒนาระบบ ดังต่อไปนี้

4.1.1 ระบบปฏิบัติการ

ระบบปฏิบัติการที่เลือกในการพัฒนาระบบงานคือ ลีนุกซ์ ซึ่งมีพื้นงานมาจากระบบปฏิบัติงานยูนิกซ์ เหตุผลที่เลือกใช้ระบบปฏิบัติการลีนุกซ์ เพราะว่าเป็นระบบปฏิบัติการที่สามารถทำงานบน CPU ได้หลายตระกูล ไม่ว่าจะเป็นของ INTEL , DIGITAL ALPHA , SUN SPARC หรือ MACINTOSH เป็นต้น และที่สำคัญลีนุกซ์ยังเป็นระบบปฏิบัติการที่ได้ชื่อว่าฟรี ไม่ว่าจะเป็นในเรื่องค่าใช้จ่าย และการใช้งานภายใต้ลิขสิทธิ์แบบ GPL (GNU General Public License) ซึ่งเป็นลิขสิทธิ์ที่ยอมให้มีการเปลี่ยนแก้ไขต้นฉบับได้อย่างอิสระทั้งยังสามารถแจกจ่ายได้โดยไม่จำกัดสิทธิ์ ส่วนอีกเหตุผลหนึ่งที่เลือกใช้ระบบปฏิบัติการลีนุกซ์ คือมีเครื่องมือและโปรแกรมที่จำเป็นที่ใช้ในการพัฒนาระบบงานติดตั้งมาด้วย ไม่ว่าจะเป็น เพิร์ล (perl) ซึ่งเป็นภาษาในการพัฒนาโปรแกรม หรือ โปรแกรม Sendmail ซึ่งจะได้กล่าวในหัวข้อต่อไป

4.1.2 โปรแกรมที่ใช้รับส่งจดหมายอิเล็กทรอนิกส์

โปรแกรมที่เลือกใช้คือ โปรแกรม Sendmail ซึ่งเป็นโปรแกรมประเภท MTA ที่ได้รับความนิยมอย่างแพร่หลายในการใช้งาน โดยรายละเอียดได้กล่าวไว้ในบทที่ 2

4.1.3 ภาษาและเครื่องมือที่ใช้ในการพัฒนาระบบงาน

- ภาษาที่ใช้คือเพิร์ล (Perl) เป็นภาษาในการพัฒนาโปรแกรมที่พัฒนามาจากภาษาซี โดยได้ตัดคุณสมบัติบางประการออกไปเช่น การกำหนดประเภทของข้อมูล ทำให้การใช้งานได้ง่าย และที่สำคัญภาษาเพิร์ลมีความความสามารถในแง่ของการจัดการข้อความได้เป็นอย่างดี เช่น Pattern Matching ซึ่งคุณสมบัตินี้มีความจำเป็นมากในการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์
- VI / VIM เป็นอิดิเตอร์ใช้ในการสร้างและแก้ไขโปรแกรม
- Microsoft Word ใช้ในการจัดการด้านเอกสารประกอบโครงงาน
- Visio และ Adobe Photoshop ใช้ในการจัดการด้านภาพประกอบเอกสารโครงงาน

4.2 โปรแกรมระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

โปรแกรมและไฟล์ต่าง ๆ ที่ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ใช้ในการทำงาน แบ่งเป็น 2 กลุ่ม ได้แก่ โปรแกรมที่ถูกพัฒนาขึ้นมาและไฟล์ที่ระบบสร้างขึ้น โดยรายละเอียดมีดังนี้

4.2.1 โปรแกรมที่ถูกพัฒนาขึ้นประกอบไปด้วย 5 ไฟล์ได้แก่

- gmail.conf เป็น configuration file เก็บค่ากำหนดการทำงานของระบบ
- gmail_agent เป็นไฟล์ที่ทำหน้าที่รับจดหมายจากโปรแกรม Sendmail และตรวจสอบรูปแบบการโจมตีของจดหมายที่รับเข้ามา
- gmaild เป็นไฟล์ที่ทำหน้าที่ในการจัดการข้อมูลที่เกิดขึ้นจากระบบ เพื่อไม่ให้ไฟล์ที่เก็บข้อมูลมีขนาดใหญ่จนเกินไป
- blocking_script เป็นไฟล์ที่เรียกใช้โปรแกรม Netfilter เพื่อปฏิเสธการให้บริการ
- deblocking_script เป็นไฟล์ที่เรียกใช้โปรแกรม Netfilter เพื่อยกเลิกการปฏิเสธการให้บริการ

4.2.2 ไฟล์ที่ระบบสร้างขึ้น

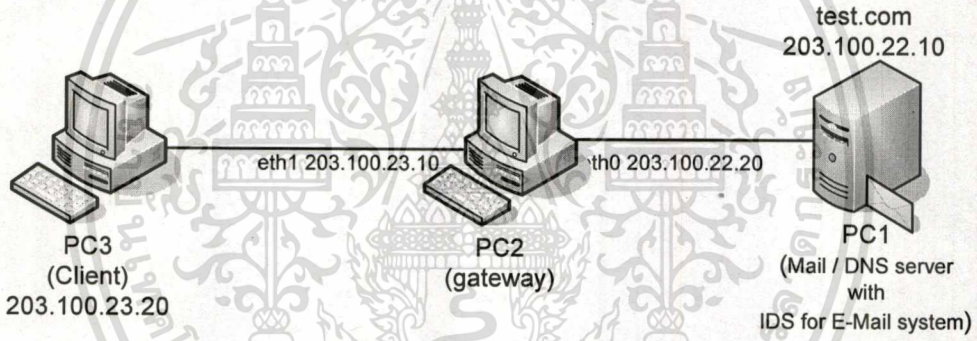
- headerfile เป็นไฟล์ที่ใช้จัดเก็บข้อมูล header ของจดหมาย ซึ่งรายละเอียดได้กล่าวไว้ในหัวข้อ 3.5

- blockfile เป็นไฟล์ที่ใช้จัดเก็บข้อมูลของการปฏิเสธการให้บริการ ซึ่งรายละเอียดได้กล่าวไว้ในหัวข้อ 3.5 เช่นกัน

4.3 การทดสอบระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

การทดสอบการทำงานของโปรแกรม จะจำลองการโจมตีระบบจดหมายอิเล็กทรอนิกส์ในรูปแบบที่ติดตั้งและไม่ได้ติดตั้งระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ ก่อนจะทำการทดสอบ ต้องติดตั้งโปรแกรมตรวจจับการบุกรุกจดหมายอิเล็กทรอนิกส์บนเครื่องบริการจดหมายอิเล็กทรอนิกส์ก่อน โดยการติดตั้งได้อธิบายไว้ที่ภาคผนวก ก สำหรับรูปแบบการทดสอบได้กำหนดรูปแบบการทดสอบไว้ 3 รูปแบบ ดังต่อไปนี้

4.3.1 การทดสอบที่ 1

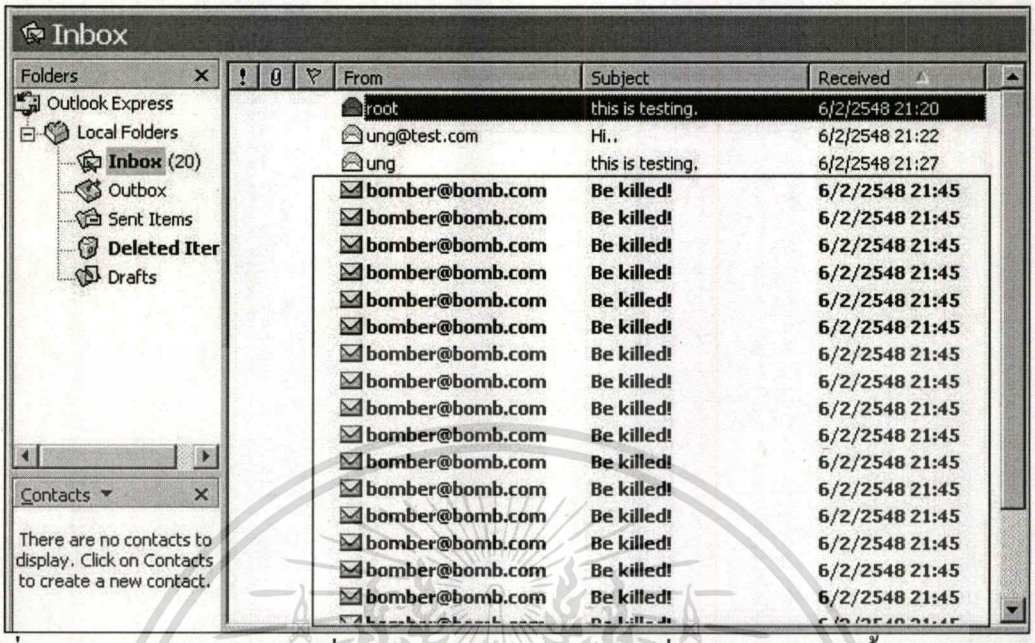


รูปที่ 4.1 แสดงการทดสอบที่ 1

เป็นการทดสอบการส่งจดหมายอิเล็กทรอนิกส์จากไคลเอนต์ถึงเซอร์ฟเวอร์โดยไม่ผ่านเครื่องที่ เป็นตัวส่งผ่าน (RELAY) ซึ่งรูปแบบของเครือข่ายแสดงในรูปที่ 4.1 โดยให้ PC1 ซึ่งได้ติดตั้งโปรแกรมระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ทำงานพร้อมรับการร้องขอบริการ และทำการส่งจดหมายอิเล็กทรอนิกส์จาก PC3 ใน 2 รูปแบบคือ

- การทดสอบการโจมตีระบบจดหมายอิเล็กทรอนิกส์แบบไม่ได้ติดตั้งระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

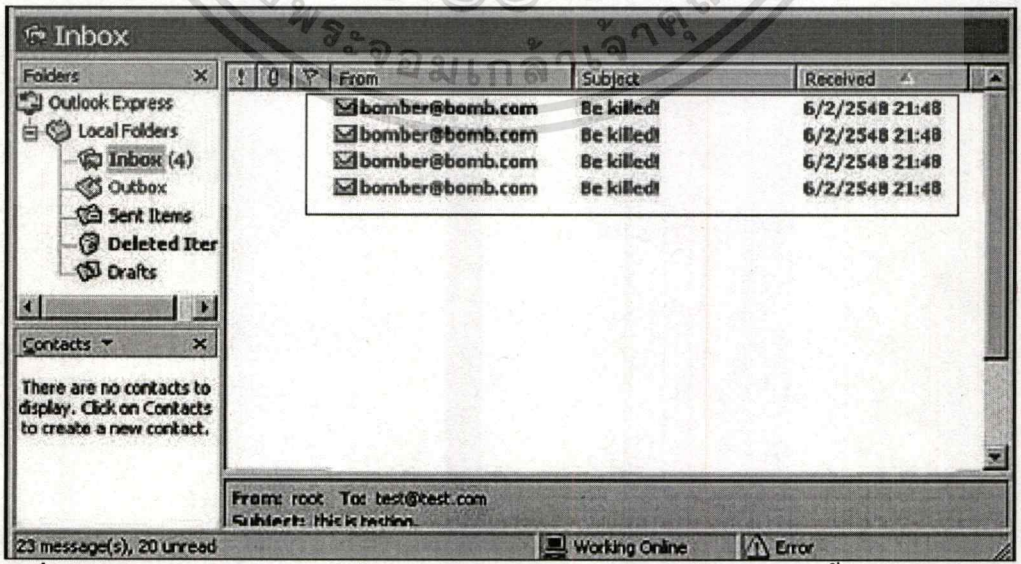
ผลการทดสอบที่ได้จากการโจมตีด้วยการส่งจดหมายจาก PC3 ไปยัง PC1 แสดงผลในรูปที่ 4.3 ซึ่งแสดงให้เห็นว่ามีจำนวนจดหมายจำนวนมากในตู้รับจดหมายของผู้รับใน PC1



รูปที่ 4.2 แสดงจำนวนจดหมายที่โจมตีระบบของการทดสอบที่ 1(แบบไม่ได้ติดตั้งระบบตรวจจับ)

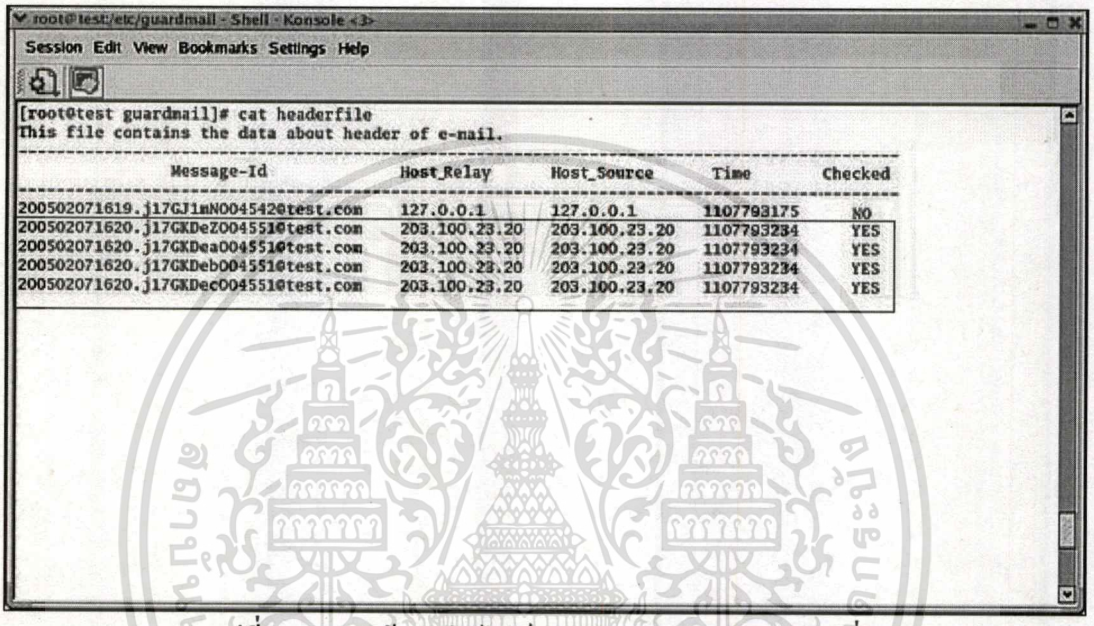
- การทดสอบการโจมตีระบบจดหมายอิเล็กทรอนิกส์แบบติดตั้งระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

ผลการทดสอบจากการที่ PC3 โจมตีระบบจดหมายอิเล็กทรอนิกส์ของ PC1 เมื่อทำการตรวจดูในตู้รับจดหมายจะพบว่ามีจดหมายที่โจมตีเข้ามาเป็นจำนวนที่น้อยเมื่อเปรียบเทียบกับกรณีแรก ซึ่งจดหมายเหล่านี้ได้ทำการปลอมแปลงชื่อผู้ส่งด้วย ดังแสดงในรูปที่ 4.3

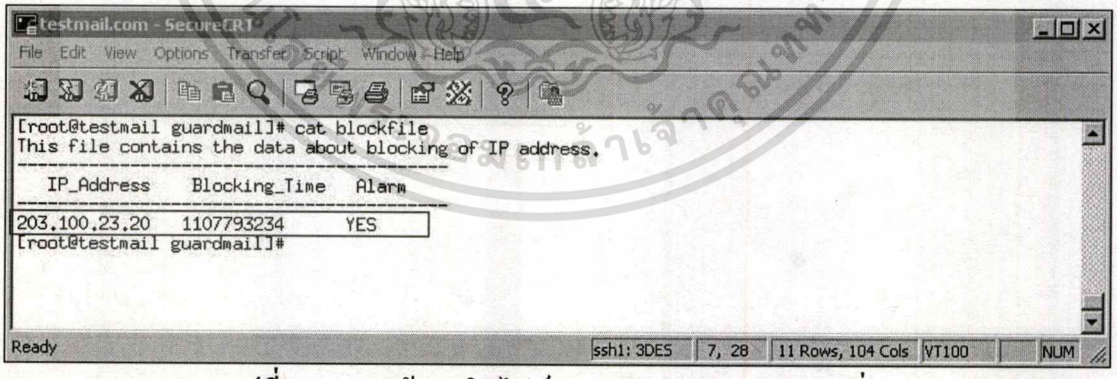


รูปที่ 4.3 แสดงจำนวนจดหมายที่โจมตีระบบของการทดสอบที่ 1(แบบติดตั้งระบบตรวจจับ)

เมื่อเข้าไปตรวจดูไฟล์ headerfile พบว่ามีการส่งจดหมายมาจากไอพีแอดเดรส 203.100.23.20 ดังแสดงในรูปที่ 4.4 และระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ ได้ตรวจสอบพบว่าจำนวนจดหมายที่รับเข้ามามีมากกว่าค่าที่ได้กำหนดไว้ในช่วงเวลาหนึ่ง สังเกตได้จากคอลัมน์ Checked มีค่าเป็น YES

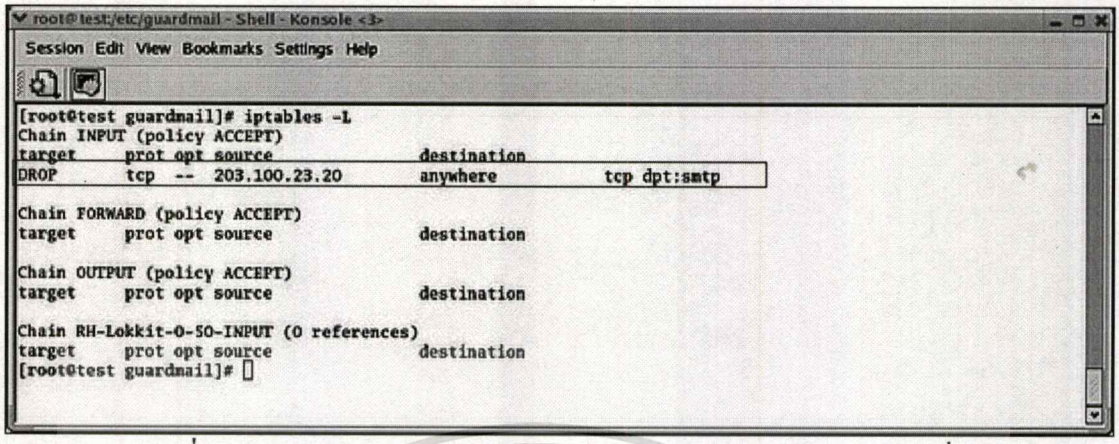


รูปที่ 4.4 แสดงข้อมูลในไฟล์ headerfile ของการทดสอบที่ 1



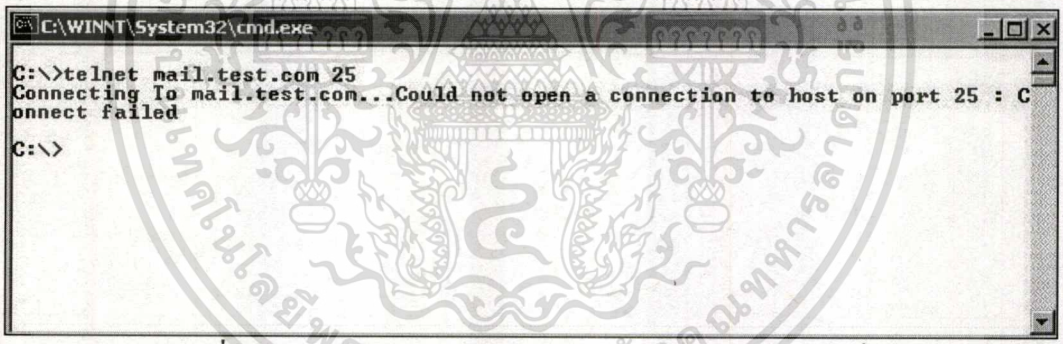
รูปที่ 4.5 แสดงข้อมูลในไฟล์ blockfile ของการทดสอบที่ 1

รูปที่ 4.5 แสดงข้อมูลในไฟล์ blockfile โดยจะเห็นว่ามีไอพีแอดเดรส 203.100.23.20 ได้ถูกปฏิเสธการให้บริการ และระบบได้ส่งข้อความเตือนผู้ดูแลระบบแล้ว สังเกตุได้จากฟิลด์ Alarm มีค่าเป็น YES และรูปที่ 4.6 แสดงการปฏิเสธการให้บริการของโปรแกรม Netfilter

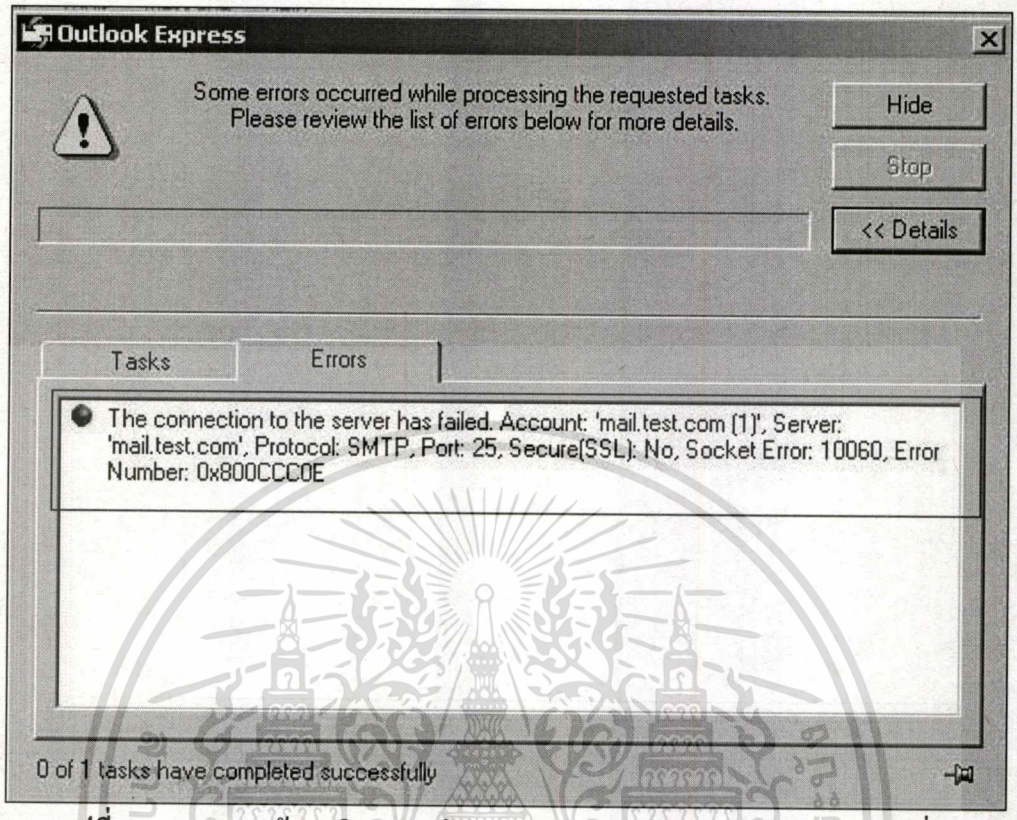


รูปที่ 4.6 แสดงการปฏิเสธการให้บริการของ Netfilter ของการทดสอบที่ 1

หลังจากนั้นทดสอบว่า Netfilter งานได้ถูกต้องหรือไม่ ด้วยการ telnet ไปที่พอร์ตหมายเลข 25 ของ PC1 หรือใช้โปรแกรมประเภท MUA ส่งจดหมายจาก PC3 ไปยัง PC1 อีกครั้ง ซึ่งจะพบว่าไม่สามารถที่จะร้องขอบริการได้ดังแสดงในรูปที่ 4.7 และ 4.8 ตามลำดับ

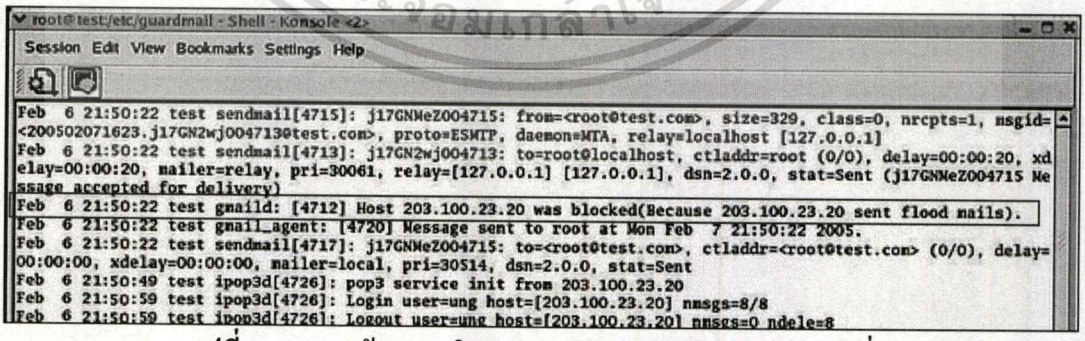


รูปที่ 4.7 แสดงการร้องขอบริการจาก telnet ของการทดสอบที่ 1



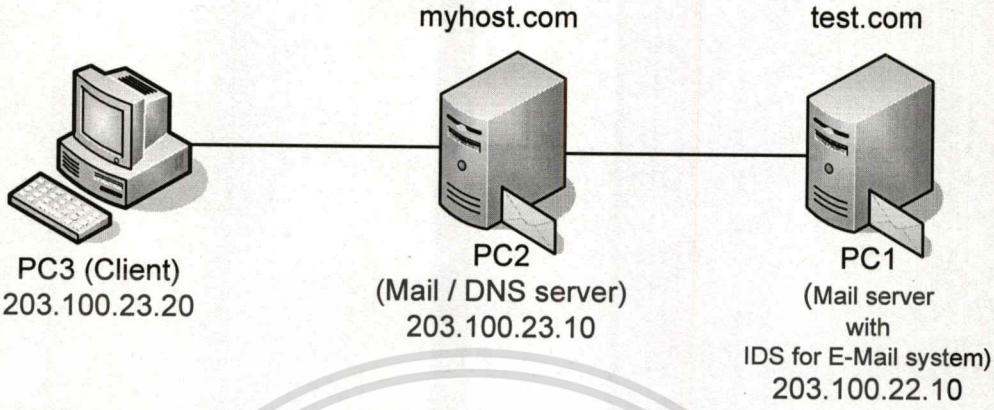
รูปที่ 4.8 แสดงการร้องบริการจากโปรแกรมประเภท MUA ของการทดสอบที่ 1

เมื่อไปตรวจสอบดูใน System log file ของระบบที่ /var/log/maillog จะพบว่ามีข้อความเตือนจาก gmaild ว่าได้ทำการปฏิเสธการให้บริการแก่ไอพีแอดเดรสหมายเลข 203.100.23.20 ดังแสดงในรูปที่ 9



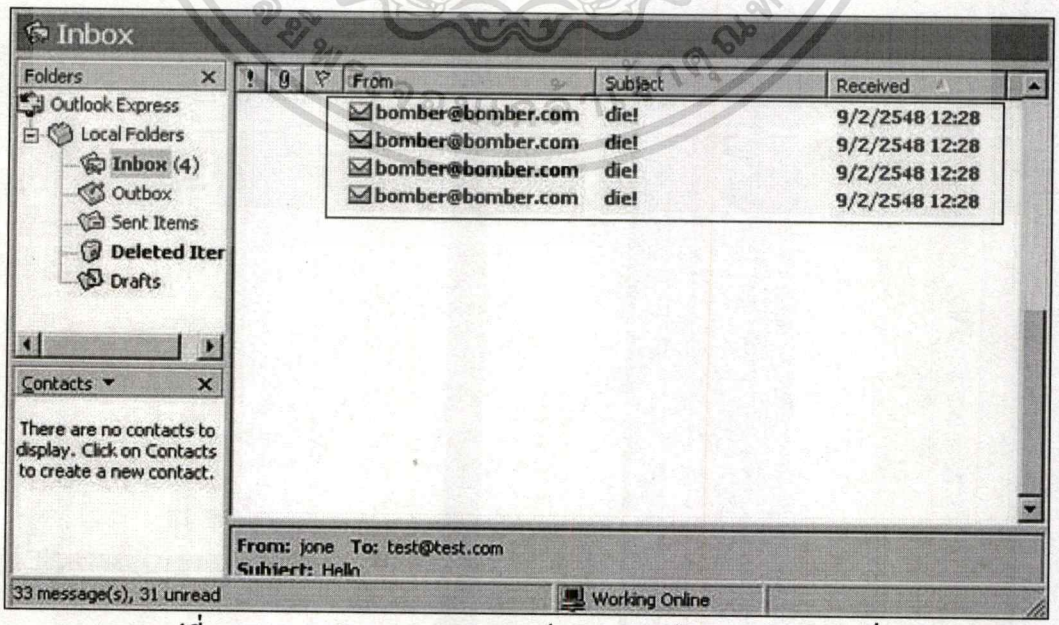
รูปที่ 4.9 แสดงข้อความใน System log file ของการทดสอบที่ 1

4.3.2 การทดสอบที่ 2

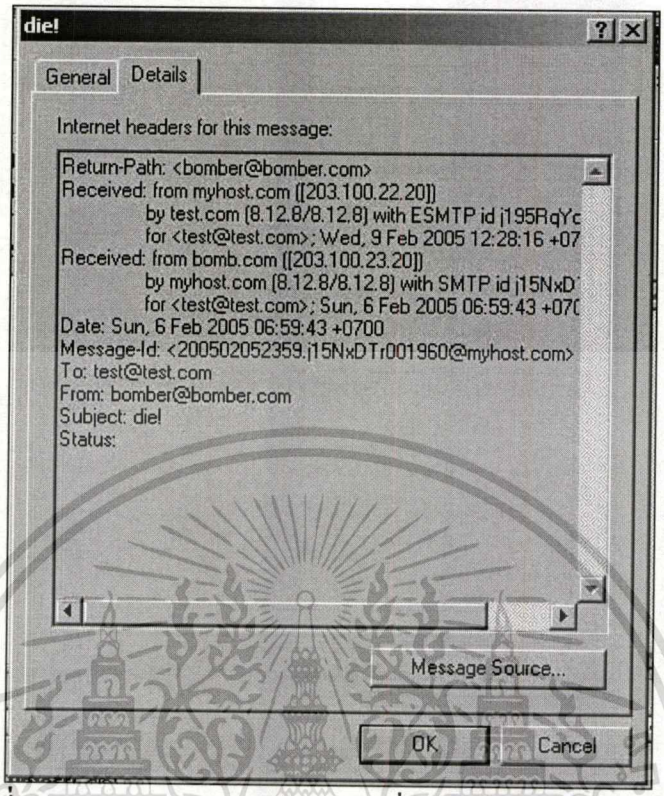


รูปที่ 4.10 แสดงการทดสอบที่ 2

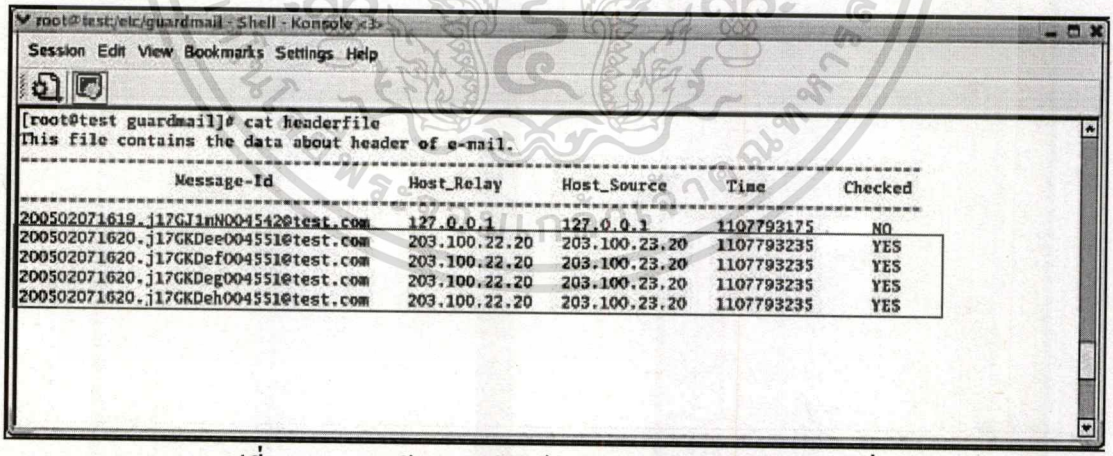
สำหรับการทดสอบที่ 2 นี้เป็นการทดสอบการส่งจดหมายอิเล็กทรอนิกส์โดยผ่านเครื่องที่ให้บริการผ่านได้ (RELAY) ดังแสดงในรูปที่ 4.10 โดยการทดสอบจะทดสอบในรูปแบบการโจมตีระบบจดหมายอิเล็กทรอนิกส์แบบติดตั้งระบบตรวจจับการบุกรุก โดยจะทดสอบแบบการโจมตี เริ่มจาก PC3 ส่งจดหมายโจมตี PC1 โดยผ่าน PC2 เมื่อเข้าไปตรวจดูตู้รับจดหมายอิเล็กทรอนิกส์ จะพบว่ามีจำนวนจดหมายที่โจมตีไม่มากนัก ดังรูปที่ 4.11 และพบว่า header ของจดหมายที่ส่งมามีการปลอมชื่อผู้ส่งจดหมายและเครื่องที่ให้บริการเป็น bomber@bomber.com และ bomb.com ตามลำดับ ดังรูปที่ 4.12



รูปที่ 4.11 แสดงจำนวนจดหมายอิเล็กทรอนิกส์ของการทดสอบที่ 2

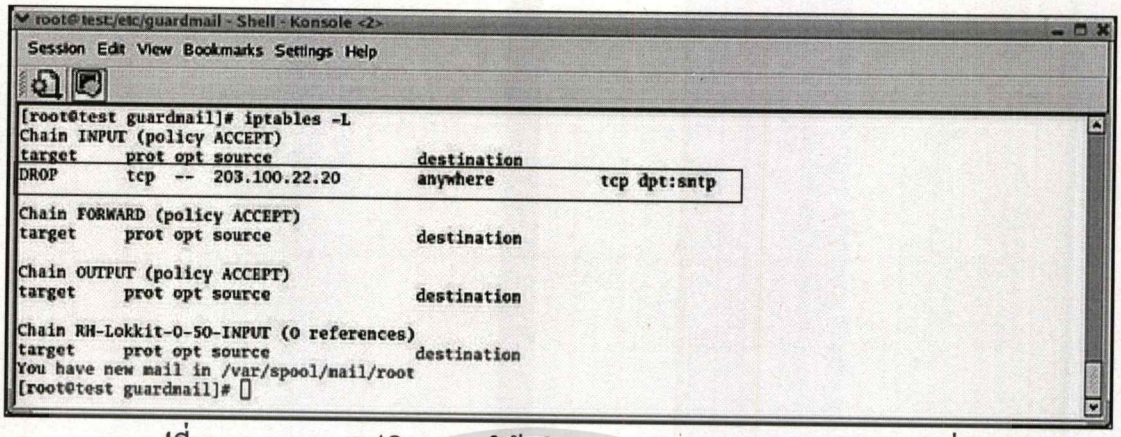


รูปที่ 4.12 แสดง header ของจดหมายที่โจมตีของการทดสอบที่ 2

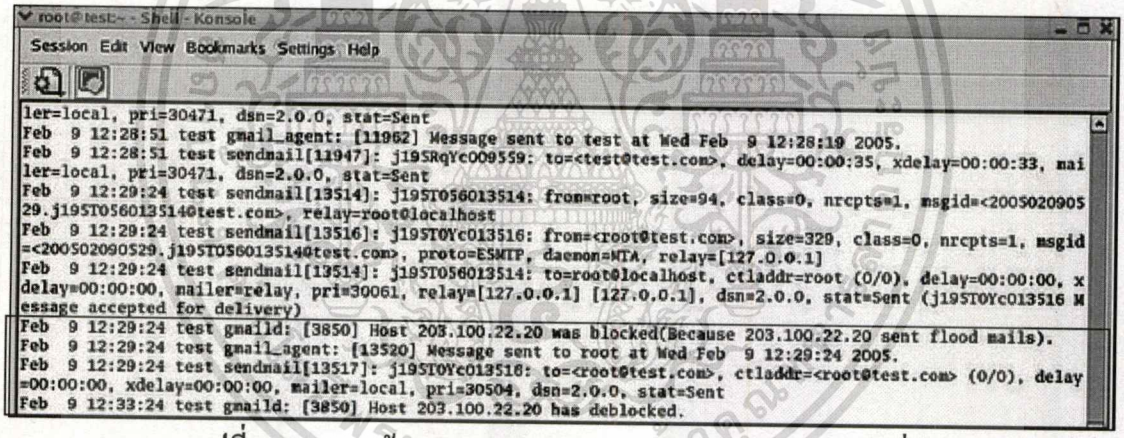


รูปที่ 4.13 แสดงข้อมูลในไฟล์ headerfile ของการทดสอบที่ 2

จากรูปที่ 4.13 เมื่อระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ทำงาน พบว่ามีจดหมายที่ส่งมาโจมตีจากไอพีแอดเดรส 203.100.23.20 โดยผ่านไอพีแอดเดรส 203.100.22.20 และได้ทำการปฏิเสธให้บริการแก่ไอพีแอดเดรส 203.100.22.20 ซึ่งเป็นตัวให้ผ่านการโจมตี ดังรูปที่ 4.14

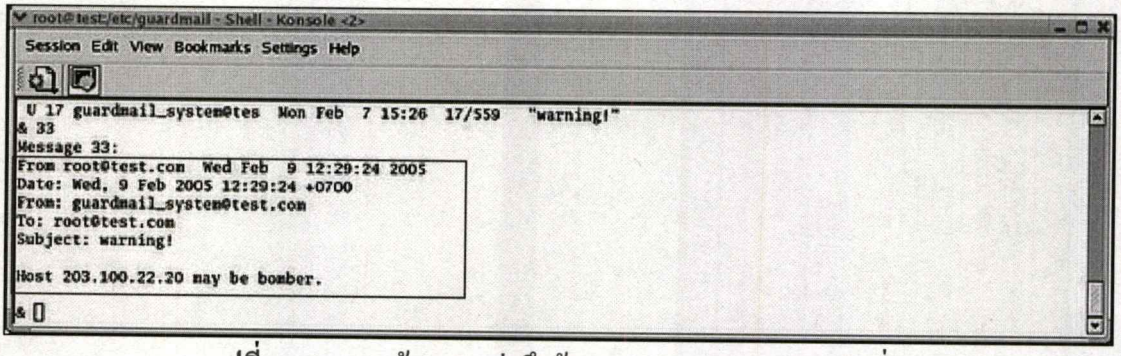


รูปที่ 4.14 แสดงการปฏิเสธการให้บริการของ Netfilter ของการทดสอบที่ 2



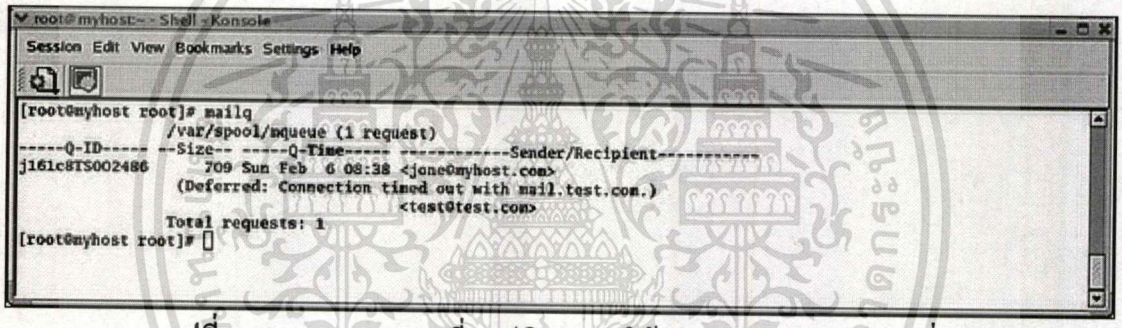
รูปที่ 4.15 แสดงข้อความของ System log file ของการทดสอบที่ 2

จากรูปที่ 4.15 เป็นการแสดงข้อความของ System log file โดยมีข้อความระบุว่ามีการโจมตีจากไอพีแอดเดรส 203.100.22.20 และได้มีการส่งจดหมายเตือนไปถึงผู้ดูแลระบบ โดยมีเนื้อหาดังรูปที่ 4.16 จากนั้นเมื่อครบกำหนดเวลาในการเปิดให้บริการตามที่ได้กำหนดไว้ ก็จะมีการเรียกใช้โปรแกรม Netfilter อนุญาตให้มีการเชื่อมต่อจากไอพีแอดเดรส 203.100.22.20 ต่อไป



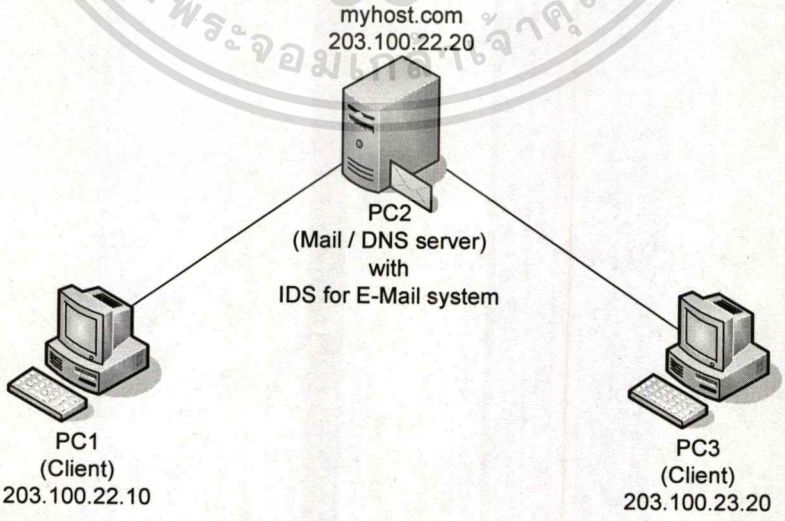
รูปที่ 4.16 แสดงข้อความส่งถึงผู้ดูแลระบบของการทดสอบที่ 2

ในระหว่างการปฏิเสธการให้บริการ เมื่อเข้าไปตรวจสอบ PC2 ซึ่งเป็นตัวส่งผ่าน พบว่าไม่สามารถที่จะส่งจดหมายอิเล็กทรอนิกส์ถึง PC3 ได้ดังรูปที่ 4.17



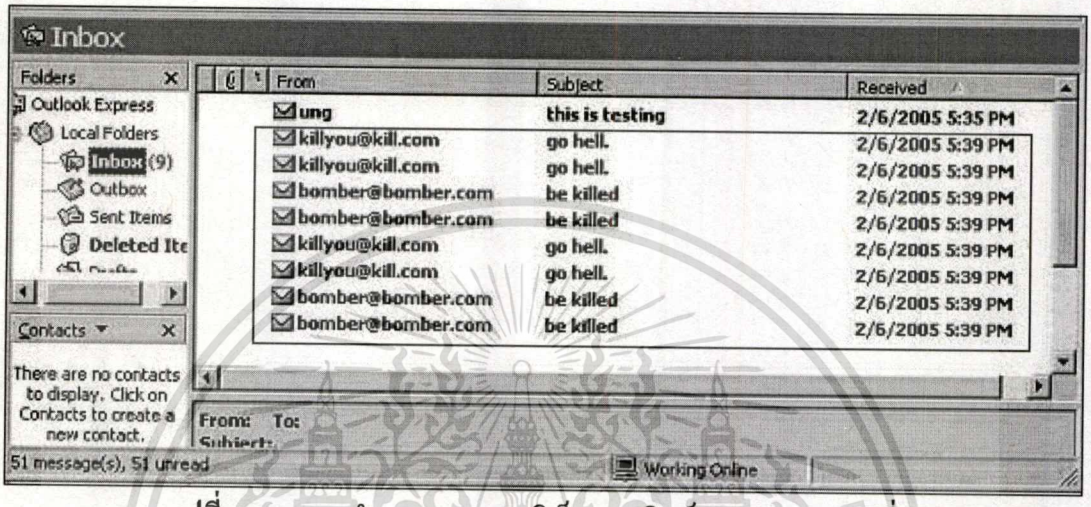
รูปที่ 4.17 แสดงจดหมายที่ถูกปฏิเสธการให้บริการของการทดสอบที่ 2

4.3.3 การทดสอบที่ 3

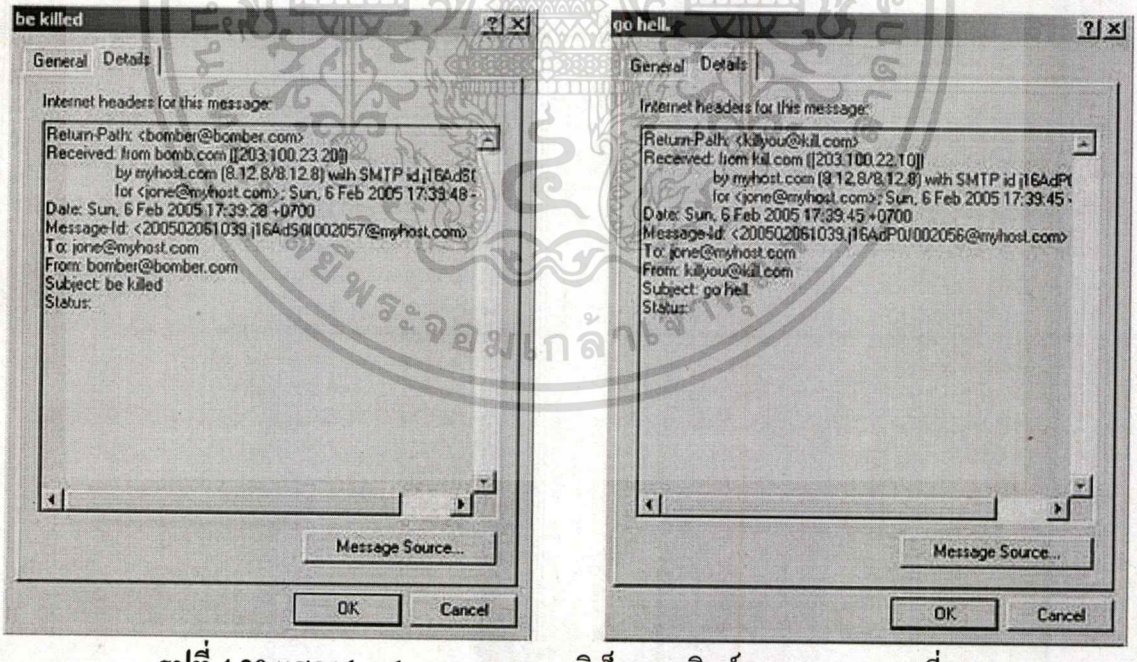


รูปที่ 4.18 แสดงการทดสอบที่ 3

สำหรับการทดสอบที่ 3 เป็นการทดสอบการโจมตีจากหลายเครื่อง โดยจะใช้จำนวน 2 เครื่อง คือ PC1 และ PC3 ทำการโจมตี PC2 ผลการทดสอบเมื่อเข้าไปตรวจตู้รับจดหมายอิเล็กทรอนิกส์ของผู้รับที่ PC2 พบว่ามีจดหมายถูกส่งมาในเวลาไล่เลี่ยกันดังรูปที่ 4.19

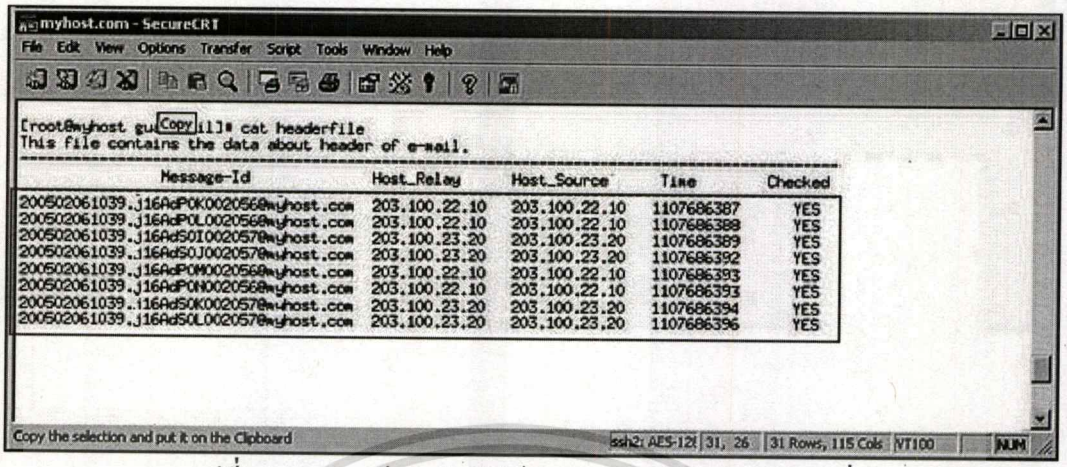


รูปที่ 4.19 แสดงจำนวนจดหมายอิเล็กทรอนิกส์ของการทดสอบที่ 3



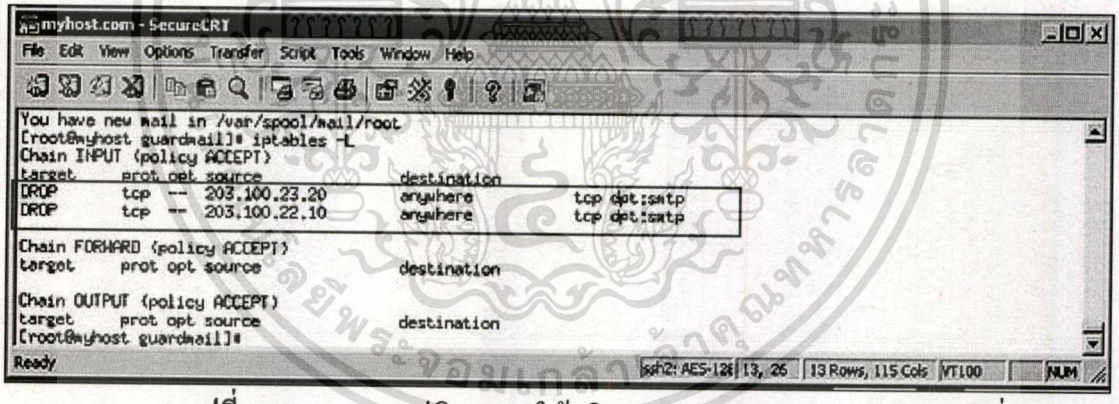
รูปที่ 4.20 แสดง header ของจดหมายอิเล็กทรอนิกส์ของการทดสอบที่ 3

จากรูปที่ 4.20 เป็นการแสดง header ของจดหมายอิเล็กทรอนิกส์ที่โจมตี PC2 จาก PC1 และ PC3 โดยจะมีการปลอมแปลงชื่อผู้ส่ง

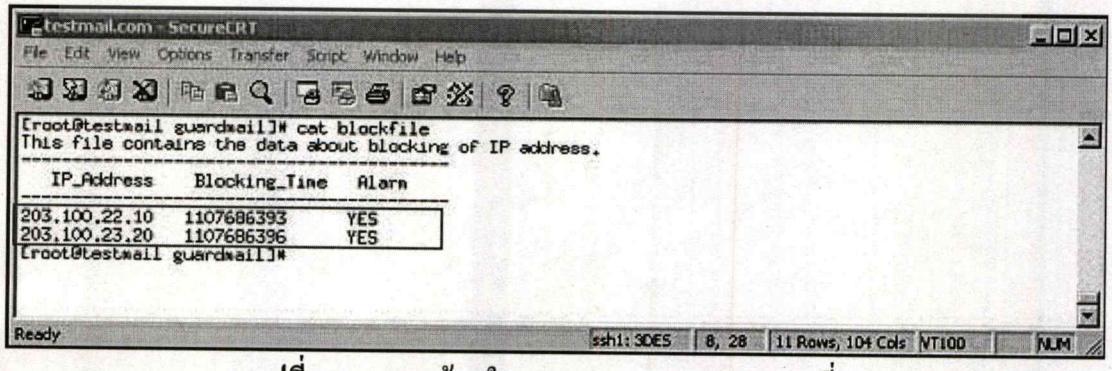


รูปที่ 4.21 แสดงข้อมูลในไฟล์ headerfile ของการทดสอบที่ 3

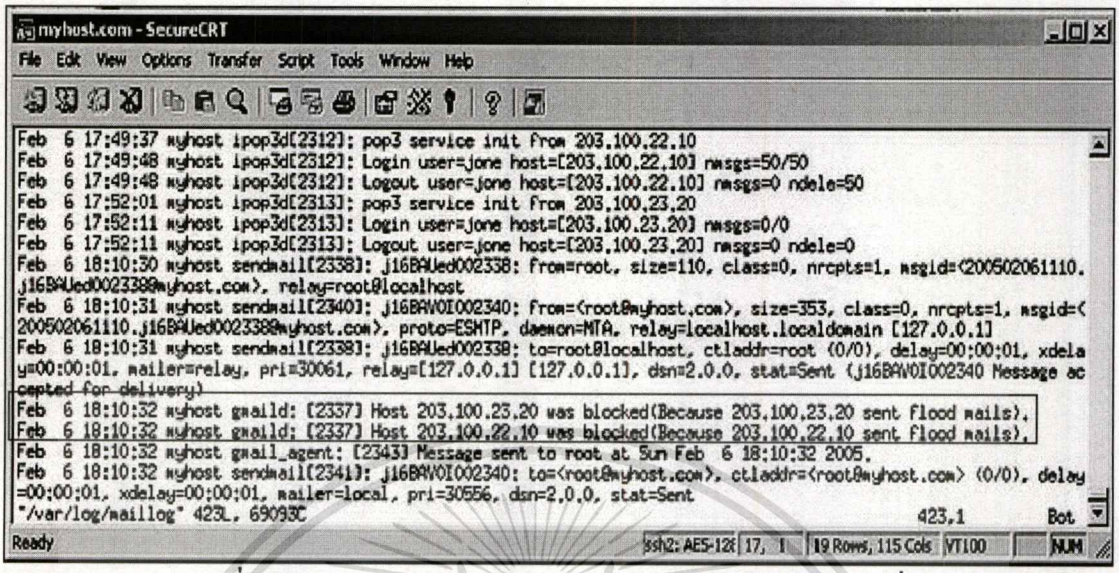
รูปที่ 4.21 แสดงการตรวจพบการส่งจดหมายจากไอพีแอดเดรส 203.100.22.10 และ 203.100.23.20 มากกว่าค่าที่ได้กำหนดไว้ ดังนั้นจึงได้ปฏิเสธการให้บริการจากทั้งสอง โดยเรียกการทำงานของโปรแกรม Netfilter ดังรูปที่ 4.22 และข้อมูลใน blockfile ดังรูปที่ 4.23



รูปที่ 4.22 แสดงการปฏิเสธการให้บริการของ Netfilter ของการทดสอบที่ 3

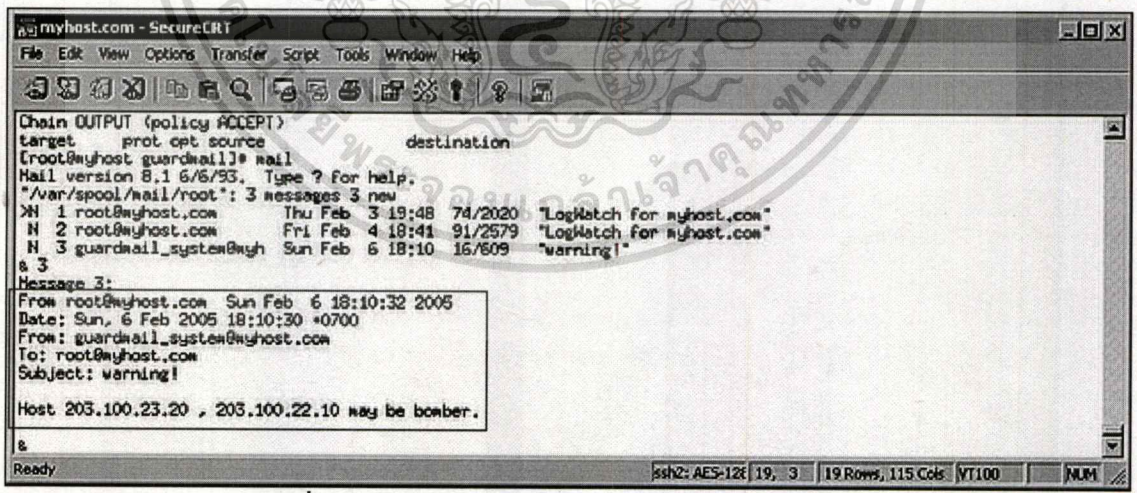


รูปที่ 4.23 แสดงข้อูลใน blockfile ของการทดสอบที่ 3

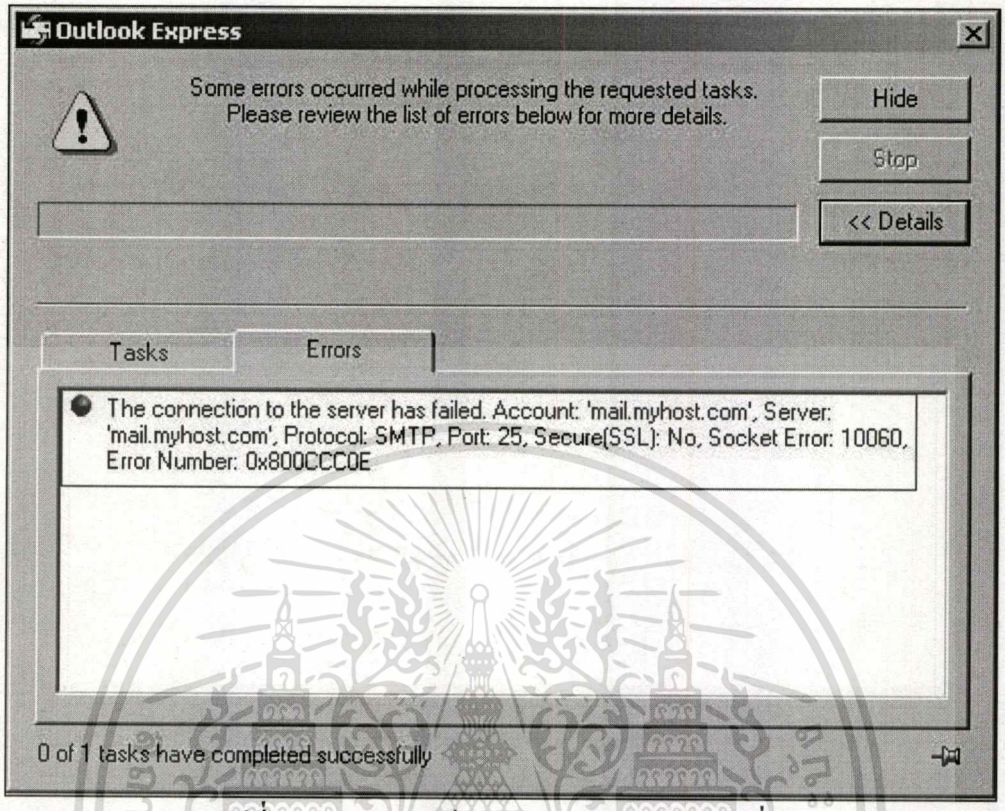


รูปที่ 4.24 แสดงข้อความของ System log file ของการทดสอบที่ 3

จากรูปที่ 4.24 แสดงถึงข้อความของ System log file โดยมีข้อความระบุว่าได้ทำการปฏิเสธการให้บริการจากไอพีแอดเดรส 203.100.22.10 และ 203.100.23.20 เนื่องจากทั้งสองไอพีแอดเดรสได้โจมตีระบบจดหมายอิเล็กทรอนิกส์ และเมื่อตรวจสอบดูจดหมายที่ส่งมาจากระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ถึงผู้ดูแลระบบ โดยมีเนื้อหาดังรูปที่ 4.25



รูปที่ 4.25 แสดงข้อความส่งถึงผู้ดูแลระบบของการทดสอบที่ 3



รูปที่ 4.26 แสดงการร้องบริการของการทดสอบที่ 3

จากรูปที่ 4.26 เป็นการแสดงการร้องขอบริการจาก PC2 หลังจากการปฏิเสธการให้บริการ จะเห็นได้ว่าจะมีข้อความที่บอกว่าไม่สามารถใช้บริการได้

บทที่ 5
สรุปและข้อเสนอแนะ

เนื้อหาในบทนี้จะเป็นสรุปของการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ พร้อมทั้งข้อเสนอแนะสำหรับผู้ที่สนใจนำระบบงานไปทำการพัฒนาต่อไป

5.1 สรุปผลการทำงานและประโยชน์ที่ได้รับ

จากการพัฒนาระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ และการทดสอบ พบว่าสามารถป้องกันการโจมตีระบบจดหมายอิเล็กทรอนิกส์ได้ตามวัตถุประสงค์ของโครงการได้ กล่าวคือสามารถตรวจสอบการโจมตีระบบจดหมายอิเล็กทรอนิกส์ อันทำให้ระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถทำงานได้อย่างปกติ หรือในกรณีที่ร้ายแรงคือไม่สามารถให้บริการได้เลย เมื่อตรวจพบว่าเกิดการโจมตีขึ้นระบบสามารถเรียกใช้โปรแกรมภายนอก ซึ่งเป็นโปรแกรมประเภทไฟร์วอลล์ ในโครงงานพัฒนาระบบงานนี้ ได้เลือกใช้โปรแกรม Netfilter ทำหน้าเป็นไฟร์วอลล์ โดยส่งคำสั่งให้โปรแกรม Netfilter ปฏิเสธการให้บริการผู้ที่ส่งจดหมายโจมตี พร้อมทั้งบันทึกเหตุการณ์ที่เกิดขึ้นโดยอาศัยกลไกของ System log file (Syslog) และส่งข้อความเตือนผู้ดูแลระบบในรูปแบบจดหมายอิเล็กทรอนิกส์ หากครบกำหนดระยะเวลาหนึ่ง ระบบจะส่งคำสั่งไปให้โปรแกรม Netfilter ยกเลิกการปฏิเสธการให้บริการจากผู้ส่งนั้น ๆ เพื่อให้สามารถใช้งานได้ตามปกติ

ดังนั้นเครื่องบริการจดหมายอิเล็กทรอนิกส์ที่ต้องการป้องกันการโจมตีในลักษณะเดียวกันนี้ สามารถนำระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์มาใช้ประโยชน์ได้

5.2 ข้อเสนอแนะ

ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์สามารถนำไปพัฒนาต่อเพื่อให้สามารถนำไปใช้ให้เกิดประโยชน์มากขึ้น โดยเพิ่มคุณสมบัติดังต่อไปนี้

- เพิ่มส่วนติดต่อผู้ใช้ (interface) เพื่อใช้กำหนดค่าเริ่มต้นของการทำงาน , การเรียกการใช้งาน , การหยุดการทำงาน , การตรวจสอบสถานะของระบบ หรือดูข้อความเหตุการณ์ที่เกิดขึ้นใน System log file

- พัฒนาในส่วนการตรวจสอบจดหมายขยะ (Spam Mail) ทั้งในรูปแบบของเนื้อหา หรือตรวจสอบแหล่งที่มาของจดหมายขยะ
- พัฒนาในส่วนการตรวจสอบไฟล์ที่แนบมากับจดหมาย ซึ่งอาจจะเป็นไฟล์ที่ไม่พึงประส่ง เช่น ไวรัส , เวิร์ม หรือ โทรจัน เป็นต้น
- เพิ่มส่วนในการรองรับข้อผิดพลาดที่เกิดขึ้น (Error Handle) เช่นเมื่อมีการปฏิเสธการให้บริการของไอพีแอดเดรสหมายเลขหนึ่ง แล้วผู้ดูแลระบบยกเลิกการปฏิเสธด้วยตัวเอง เมื่อระบบทำงานครบกำหนดเวลาที่ต้องยกเลิกการปฏิเสธการให้บริการ แต่ผู้ดูระบบยกเลิกไปแล้ว ทำให้เกิดข้อผิดพลาดขึ้นในลักษณะที่ว่าไม่สามารถยกเลิกการปฏิเสธการให้บริการได้เพราะกฎการปฏิเสธนั้นไม่มีอยู่ เป็นต้น

บรรณานุกรม

สุรศักดิ์ สงวนพงษ์. 2545. **สถาปัตยกรรมและโปรโตคอลทีซีพี/ไอพี.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

อังกูร ชูเชื้อ. 2546. **ระบบตรวจสอบและป้องกันระบบจดหมายอิเล็กทรอนิกส์.** บทความสัมมนา 2. คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง.

Costales, B. and Allman, E. **Sendmail**. CA : O'Reilly & Associates.

Simple Mail Transfer Protocol. **SMTP.** [Online]. Available: http://www.networksorcery.com/enp/protocol/smtp.htm.

Stateful Firewall. 2544. **IPTABLES.** [Online]. Available : http://thaicert.nectec.or.th/paper/firewall/iptables.php.

Till, D. 2538. **Teach Yourself PERL in 21 Days**. Indiana : SAMS.

Volkerding, P. 2541. **LINUX configuration and installation**. CA : M&T Books.

ภาคผนวก

การติดตั้งและใช้งาน
ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

1. การติดตั้งระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

ก่อนที่ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์จะสามารถทำงานได้ ต้องมีการติดตั้งตามขั้นตอนต่อไปนี้

1.1 ขยายไฟล์ gmail.tar.gz ไว้ที่ directory ที่ต้องการเช่น /tmp โดยใช้คำสั่งดังนี้

```
# tar  zxvf  gmail.tar.gz
```

1.2 ตรวจสอบว่ามีไฟล์จำนวน 6 ไฟล์ดังต่อไปนี้หรือไม่ gmail.conf , gmail_agent , gmaild , blocking_script , deblocking_script และ setup.pl ด้วยคำสั่งดังนี้

```
# ls -l
```

1.3 ติดตั้งโปรแกรม โดยใช้คำสั่งดังนี้

```
# ./setup.pl
```

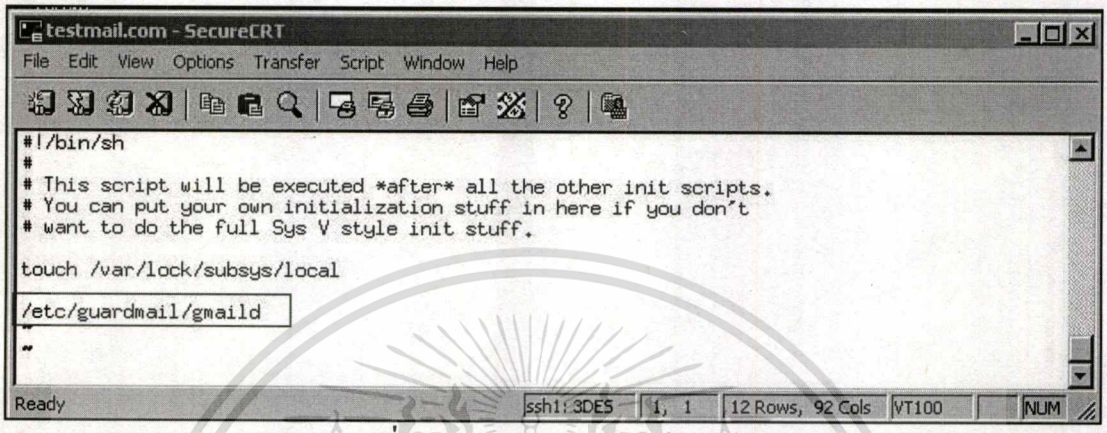
1.4 ตรวจสอบว่ามีไฟล์ gmail.conf , gmail_agent , gmaild , blocking_script และ deblocking_script อยู่ใน directory /etc/guardmail หรือไม่ ด้วยคำสั่ง

```
# ls   /etc/guardmail
```

1.5 สร้าง symbolic link ไว้ที่ directory /usr/sbin เพื่อให้สามารถเรียกใช้งานได้ง่าย ด้วยคำสั่งดังนี้

```
# ln –s /etc/guardmail/gmaild
```

หรือถ้าจะให้โปรแกรมทำงานตั้งแต่ตอน boot ให้เพิ่มข้อความ /etc/guardmail/gmail ลงในไฟล์ /etc/rc.d/rc.local ดังรูปที่ ก.1



รูปที่ ก.1 แสดงข้อมูลในไฟล์ rc.local

1.6 แก้ไขไฟล์ /etc/mail/sendmail.cf ดังรูปที่ ก.1 เป็น รูปที่ ก.2

```
Mlocal,          P=/usr/bin/procmail, F=lsDFMAw5:/|@qSPfhn9, S=EnvFromL/HdrFromL,
 R=EnvToL/HdrToL,
                 T=DNS/RFC822/X-Unix,
                 A=procmail -t -Y -a $h -d $u
```

รูปที่ ก.2 แสดงไฟล์ sendmail.cf ก่อนการแก้ไข

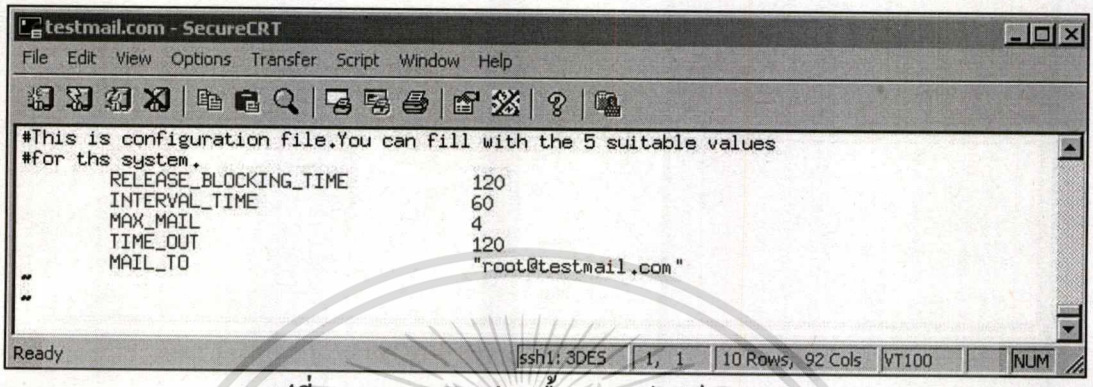
```
Mlocal,          P=/etc/guardmail/gmail_agent, F=lsDFMAw5:/|@qSPfhn9, S=EnvFromL/
HdrFromL, R=EnvToL/HdrToL,
                 T=DNS/RFC822/X-Unix,
                 A=gmail_agent -t -Y -a $h -d $u
```

รูปที่ ก.3 แสดงไฟล์ sendmail.cf หลังการแก้ไข

1.7 หลังจากแก้ไขไฟล์ /etc/mail/sendmail.cf ให้ทำการ restart การทำงานของโปรแกรม Sendmail ใหม่ ดังคำสั่งต่อไปนี้

```
# service sendmail restart
```

2. การกำหนดค่าเริ่มต้นการทำงานของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์



รูปที่ ก.4 แสดงตัวอย่างเนื้อหาของไฟล์ gmail.conf

การกำหนดค่าเริ่มต้นการทำงานของระบบ จะแก้ไขในไฟล์ /etc/guardmail/gmail.conf ดังแสดงดังรูปที่ ก.4 โดยที่พารามิเตอร์ที่ต้องกำหนดมีดังต่อไปนี้

2.1 RELEASE_BLOCKING_TIME เป็นค่าระยะเวลา(วินาที) ที่ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ใช้ปฏิเสธการให้บริการ หากครบกำหนดเวลาดังกล่าวระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ จะส่งคำสั่งให้โปรแกรม Netfilter ยกเลิกการปฏิเสธการให้บริการนั้น หากไม่กำหนดค่านี้ระบบจะใช้ค่าปริยายคือ 86400 (1 วัน)

2.2 INTERVAL_TIME เป็นช่วงระยะเวลา (วินาที) ที่ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ใช้ในการตรวจสอบปริมาณจดหมายที่เข้ามายังระบบ หากไม่กำหนดค่านี้ระบบจะใช้ค่าปริยายคือ 60

2.3 MAX_MAIL เป็นค่าของจำนวนจดหมายมากที่สุดจากผู้ส่งแหล่งเดียวกันที่สามารถส่งเข้ามาในช่วง INTERVAL_TIME ได้ หากเกินกว่าค่า ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์จะส่งคำสั่งให้โปรแกรม Netfilter ปฏิเสธการให้บริการจากผู้ส่งนั้น โดยมีค่าปริยายคือ 4 ฉบับ

2.4 TIME_OUT เป็นค่าระยะเวลา (วินาที) ที่ใช้ในการลบข้อมูลในไฟล์ headerfile เพื่อไม่ให้ไฟล์นี้มีขนาดใหญ่ เพราะว่าถ้าหากมีจดหมายเข้ามา ระบบจะเพิ่มข้อมูลของจดหมายในไฟล์นี้ ทำให้ไฟล์มีขนาดใหญ่ขึ้น หากไม่กำหนดค่านี้ระบบจะใช้ค่าปริยายคือค่า 86400 (1 วัน)

2.5 MAIL_TO เป็นที่อยู่ที่จะให้ระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ ส่งจดหมายเตือนให้ทราบว่ามีการโจมตีระบบจดหมายอิเล็กทรอนิกส์ หากไม่กำหนดค่านี้ระบบจะใช้ค่าปริยายคือ root@localhost

3. การใช้งานระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์

3.1 หากมีการสร้าง symbolic link ดังข้อ 1.5 แล้ว สามารถเรียกใช้คำสั่งได้เลย ดังนี้

```
# gmaild
```

หากยังไม่ได้สร้าง symbolic link ให้เข้าไปที่ directory /etc/guardmail/ แล้วใช้คำสั่งดังนี้

```
# ./gmaild
```

3.2 ตรวจสอบว่ามีการทำงานของโปรแกรมหรือไม่ ด้วยคำสั่งดังนี้

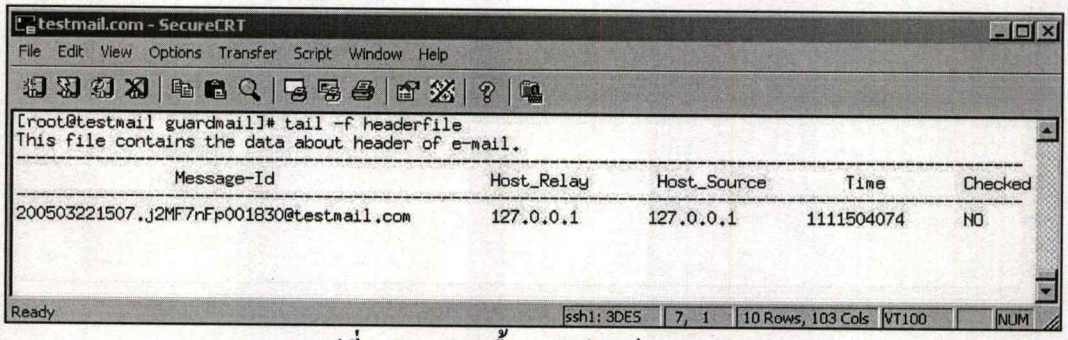
```
# ps –aux|grep gmaild
```

3.3 ตรวจสอบการทำงานของระบบตรวจจับการบุกรุกสำหรับระบบจดหมายอิเล็กทรอนิกส์ใน ด้วยการทดลองส่งจดหมายเข้าสู่ระบบ ด้วยคำสั่ง

```
# sendmail –v user
```

หมายเหตุ user คือชื่อของผู้รับที่เป็นสมาชิกของระบบจดหมายอิเล็กทรอนิกส์

และตรวจสอบว่ามีไฟล์ /etc/guardmail/headerfile หรือไม่ ถ้ามีจะมีเนื้อหาลักษณะคล้ายรูปที่ ก.5



รูปที่ ก.5 แสดงเนื้อหาในไฟล์ headerfile

3.4 ตรวจสอบเหตุการณ์ต่างที่เกิดขึ้นกับระบบจดหมายอิเล็กทรอนิกส์ใน System log file ดังคำสั่งต่อไปนี้

```
# tail –f  /var/mail/maillog
```

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายอังกูร ชูเชื้อ
วันเกิด	วันพุธ 21 สิงหาคม พ.ศ. 2517
สถานที่เกิด	อ.แม่จัน จ.เชียงราย
ประวัติการศึกษา	
ระดับประถมศึกษา	โรงเรียนบ้านแม่คี จ.เชียงราย
ระดับมัธยมศึกษา	โรงเรียนสามัคคีวิทยาคม จ.เชียงราย
ระดับปริญญาตรี	มหาวิทยาลัยเทคโนโลยีสุรนารี จ.นครราชสีมา