ระบบจัดการไฟร์วอลล์อัตโนมัติ

Automatic Firewall Management System

โดย

นายเดชชัย ศรีหาคิม

รหัส 44067278

อาจารย์ที่ปรึกษา

ดร. จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2545

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิชาโครงการศึกษากรณีพิเศษ (Special Study Project)

เรื่อง

ระบบจัดการไฟร์วอลล์อัตโนมัติ

Automatic Firewall Management System

นายเดชชัย ศรีหาคิม

รหัส 44067278

รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ
การศึกษาวิชาโครงการศึกษากรณีพิเศษ หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
ภาคเรียนที่ 2 ปีการศึกษา 2545

..... อาจารย์ที่ปรึกษา
(ดร.จันทร์บูรณ์ สถิตวิริยวงศ์)

..... กรรมการสอบ
(ดร. ภัทรชัย ลลิตโรจน์วงศ์)

..... กรรมการสอบ
(ดร. พรฤดี เนติโสภากุล)

ชื่อหัวข้อ	ระบบจัดการไฟร์วอลล์อัตโนมัติ
นักศึกษา	นาย เดชชัย ศรีหาดิม
อาจารย์ที่ปรึกษา	ดร.จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2545

บทคัดย่อ

จากการที่องค์กรต่างๆมากมายได้มีการนำเอาข้อมูลสารสนเทศที่มีความสำคัญเก็บไว้บนระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นระบบเปิดไม่ว่าใครก็สามารถเข้าไปใช้ได้นั้น มีผลทำให้ระบบการรักษาความปลอดภัยสำหรับป้องกันและรักษาข้อมูลสารสนเทศดังกล่าว เพื่อรองรับการประกอบธุรกิจและการให้บริการอย่างมีประสิทธิภาพเป็นเรื่องที่สำคัญและจำเป็นอย่างมาก ซึ่งในปัจจุบันนี้ได้มีระบบติดตามและตรวจสอบการบุกรุก (Intrusion Detection System; IDS) เกิดขึ้นมาเพื่อตรวจจับและป้องกันการบุกรุกที่มีอยู่มากมาย แต่หากจะกล่าวถึงระบบ IDS ที่ราคาถูก และสามารถป้องกันการบุกรุกได้อย่างมีประสิทธิภาพแล้วนั้น ระบบที่มีอยู่คงเป็นไปได้ยากที่จะสนองตอบความต้องการได้ ดังนั้นแนวความคิดที่จะสร้างระบบซึ่งสามารถใช้ป้องกันการบุกรุกได้อย่างมีประสิทธิภาพจึงเกิดขึ้น โดยแนวทางคือใช้ความสามารถของระบบ IDS ที่มีอยู่แล้วเช่น Snort ประกอบกับโปรแกรม Automatic Firewall Management System ที่สร้างขึ้นมาใหม่เพื่อวิเคราะห์หาความเสี่ยงของการโจมตีแบบต่างๆ และสร้างกฎเกณฑ์ในการป้องกันที่เหมาะสมให้กับไฟร์วอลล์ โดยช่วยกำหนดกฎเกณฑ์ที่เหมาะสมได้

Title	Automatic Firewall Management System
Student	Mr. Dejchai Srihakim
Advisor	Dr. Chanboon Sathitviriyawong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2002

ABSTRACT

As organizations migrate their existing legacy system towards a more efficient and high technology information system via the Internet, data sensitivity as well as value is compromised. The requirement for security is of great necessity. An enhanced and efficient security system is critical to support business and their services. As of present, Intrusion Detection Systems (IDS) have been developed to detect and warn system administrators of unauthorized access into their network. Cheap IDS systems are always an option, but they do not serve the full functionality that the business requires. In order to satisfy the requirements an efficient and state-of-the-art system must be implemented in conjunction: "Snort", together with an "Automatic Firewall Management System" featuring a reliable to assist in determining the customized rules base and limitations in order to enhance the overall system's detection capability.

กิตติกรรมประกาศ

ในการจัดทำโครงการศึกษากรณีพิเศษเรื่องระบบจัดการไฟร์วอลล์อัตโนมัติ ได้รับคำแนะนำจากคณาจารย์หลายท่าน โดยเฉพาะอย่างยิ่ง ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ ผู้เป็นอาจารย์ที่ปรึกษา ที่ช่วยจัดหาแหล่งข้อมูล และแนะนำแหล่งข้อมูลเพื่อประกอบการค้นคว้า และขอขอบคุณไปยังทางกลุ่มนักพัฒนาซอฟท์แวร์ Snort ที่ได้ให้การสนับสนุนด้านข้อมูลของระบบเป็นอย่างดี ตลอดจนทุกท่านที่มีส่วนร่วมทำให้โครงการฉบับนี้สำเร็จไปได้ด้วยดี

ท้ายสุดขอกราบขอบพระคุณ บิดา มารดา ผู้ที่คอยให้กำลังใจ ให้ความช่วยเหลือ และผู้ที่มีส่วนเกี่ยวข้องที่ทำให้โครงการพิเศษฉบับนี้ให้สำเร็จลุล่วงไปด้วยดี

เดชชัย ศรีหาคิม

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญรูป

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

รูปที่

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ระบบตรวจจับผู้บุกรุก (Intrusion Detection System; IDS) เป็นระบบที่ใช้ตรวจจับข้อมูลที่น่าสงสัย ที่ถูกส่งผ่านมาภายในระบบคอมพิวเตอร์เครือข่าย ซึ่งได้รับความนิยมอย่างแพร่หลายในการใช้งาน ประกอบกับระบบรักษาความปลอดภัยอื่นๆ เช่น ไฟร์วอลล์เพื่อให้การรักษาความปลอดภัยแก่ระบบคอมพิวเตอร์เครือข่ายเป็นไปอย่างมีประสิทธิภาพสูงสุด

แต่ในขณะที่ IDS เองอาจจะไม่มีความสามารถที่จะทำการป้องกันการบุกรุกได้อย่างดี และการที่ระบบคอมพิวเตอร์ในปัจจุบัน ต่างมีหน้าที่การทำงานที่แตกต่างกันออกไป ทำให้การที่ผู้ดูแลระบบจะจัดการระบบให้เกิดความปลอดภัยได้อย่างทั่วถึงนั้น เป็นเรื่องที่ทำได้ยาก ถึงแม้จะมีการติดตั้งไฟร์วอลล์ให้กับระบบที่ต้องการรักษาความปลอดภัยแล้วก็ตาม บางครั้งการจัดการระบบที่มีคอมพิวเตอร์จำนวนมากนั้น ผู้ดูแลระบบก็อาจหลงลืม หรือมองข้ามช่องโหว่ต่างๆ ของระบบได้เช่นกัน

งานวิจัยฉบับนี้จะนำเสนอรูปแบบของการนำ IDS มาใช้งานกับไฟร์วอลล์ เพื่อช่วยให้ผู้ดูแลระบบคอมพิวเตอร์เครือข่าย สามารถรักษาความปลอดภัยให้กับระบบได้โดยสะดวก และมีประสิทธิภาพ โดยใช้แนวคิดของระบบการรักษาความปลอดภัยที่ทำงานจากศูนย์กลาง และมีการเปลี่ยนแปลงรูปแบบของการรักษาความปลอดภัย ปลอดภัยแบบอัตโนมัติ เพื่อให้การรักษาความปลอดภัยมีผลกระทบต่อการใช้งานของผู้ใช้น้อยที่สุด

1.2 วัตถุประสงค์ของการศึกษา

ในการศึกษาเกี่ยวกับระบบจัดการไฟร์วอลล์อัตโนมัติมีวัตถุประสงค์ในการศึกษา ดังนี้

1. เพื่อสร้างระบบที่ช่วยในการวิเคราะห์ความเสี่ยงของการบุกรุก และ นำข้อมูลที่เกี่ยวข้องมาสร้างเป็น Rules Base ที่เหมาะสมให้กับไฟร์วอลล์

2. เพื่อลดภาระงานของผู้บริหารระบบที่จะต้องคอยตรวจสอบการบุกรุกที่มีเข้ามา และหาวิธีป้องกันโดยให้ระบบจัดการให้

3. เพื่อลดความเสี่ยงที่เกิดจากการถูกบุกรุก โดยการที่ IDS สามารถ Update กฎเกณฑ์ของตัวเองจากแหล่งข้อมูลอื่นได้ง่าย ถึงแม้รูปแบบของการบุกรุกจะมีอยู่หลากหลาย และมีรูปแบบใหม่ๆ เพิ่มเข้ามาก็ตาม การบุกรุกก็จะถูกป้องกันโดยไฟร์วอลล์

4. เพื่อเพิ่มความปลอดภัยให้กับระบบ

5. เพื่อเพิ่มประสิทธิภาพให้กับการดูแลระบบคอมพิวเตอร์เครือข่าย โดยเฉพาะอย่างยิ่งระบบที่มีคอมพิวเตอร์จำนวนมากๆ

1.3 ขอบเขตของการสร้างระบบ

การสร้างระบบจัดการไฟร์วอลล์อัตโนมัติมีขอบเขตที่ครอบคลุมส่วนต่างๆ ที่สำคัญดังนี้คือ

1. เป็นระบบที่ทำงานกับโปรโตคอล TCP/ IP เท่านั้น

2. เป็นระบบที่ทำงานโดยอาศัยข้อมูลการของบุกรุกจาก Light weight IDS ที่ชื่อว่า Snort เท่านั้น

3. ระบบปฏิบัติการที่ติดตั้ง Firewall จะเป็นระบบปฏิบัติการ Linux และ Firewall ที่ใช้เป็น Ipchains

4. ระบบการป้องกันของไฟร์วอลล์จะทำงานอยู่ในระดับ Packets Filtering Firewall

5. การต่อเชื่อมจะกำหนดให้ไฟร์วอลล์ทำหน้าที่เป็น Router เพื่อเชื่อมโยงระหว่างเครือข่ายภายนอกกับระบบที่ต้องการป้องกัน

6. ระบบสามารถทำงานกับตัว Agent ที่ทำหน้าที่ปรับเปลี่ยนแก้ไข Configuration ของไฟร์วอลล์ ผ่านทาง โปรโตคอล HTTP ได้

7. ไฟร์วอลล์ Agents จะต้องมีระบบรักษาความปลอดภัยในระดับ Username/ Password เพื่อการป้องกันการสร้าง Rules Base ของ Firewall โดยผู้ที่ไม่ได้รับอนุญาต

8. การทำงานเพื่อการแก้ไข Rules Base ของไฟร์วอลล์มีการทำงานเป็นแบบอัตโนมัติ และการแก้ไขข้อมูลจะทำงานเป็นแบบ Batch โดยอาศัยความสามารถของระบบปฏิบัติการ (คำสั่ง crontab)

9. IP Address ของ Network ภายในกับภายนอกสามารถเชื่อมโยงกันได้โดยไม่ต้องทำ Network Address Translation (NAT)

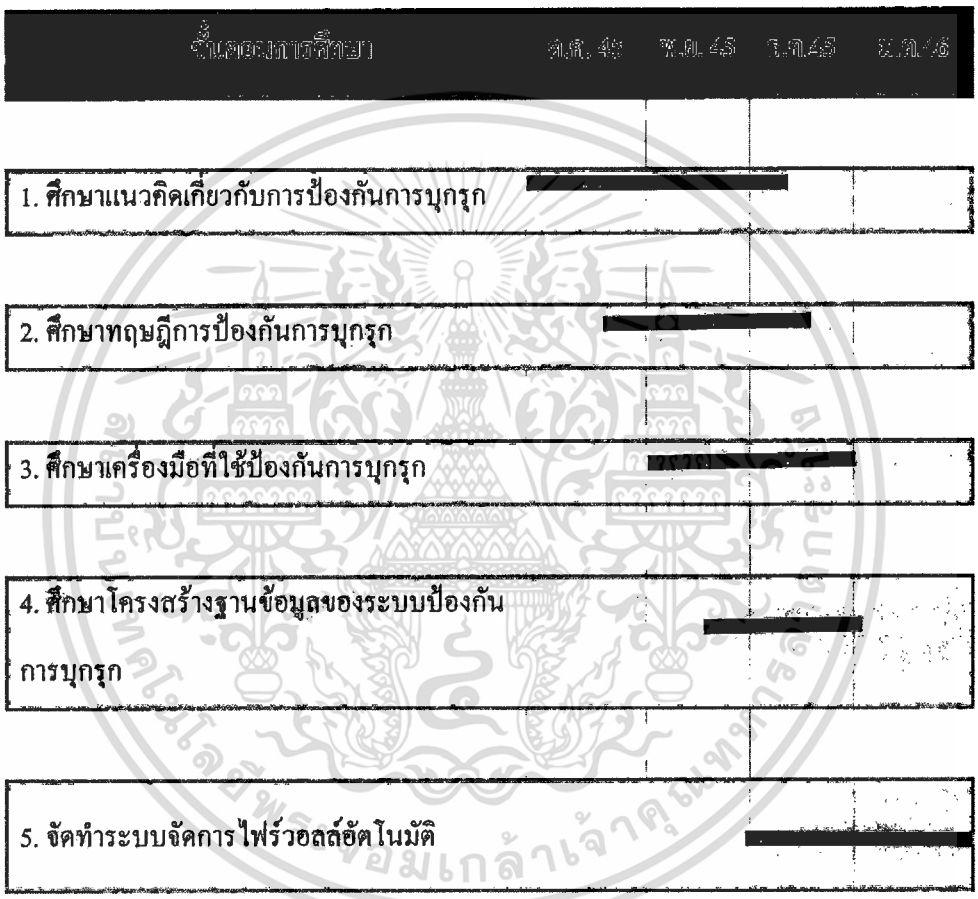
10. IDS มีความสามารถเพียงพอในการตรวจจับ Packets ที่ส่งผ่านอุปกรณ์ Network

11. Rules Base ที่อยู่บนตัว IDS จะไม่มีการเปลี่ยนแปลง

12. การทำการติดตั้ง Rules Base ให้กับ Firewall จะทำหลังจากที่ IDS ตรวจพบ Packets ต้องสงสัยในเวลา 10 นาที

1.4 ขั้นตอนการศึกษา

ในการศึกษาเกี่ยวกับการทำงานของระบบและออกแบบระบบมีขั้นตอนการดำเนินงานตามระยะเวลา ดังนี้



บทที่ 2

ทฤษฎีที่เกี่ยวข้อง

สำหรับการศึกษาเพื่อพัฒนาระบบงานนี้ได้ศึกษาและทบทวนแนวคิดรวมถึงทฤษฎีที่เกี่ยวข้องเพื่อนำมาเป็นกรอบกำหนดแนวทางการพัฒนาระบบงานเพื่อให้สำเร็จเป็นไปตามวัตถุประสงค์ โดยแบ่งออกเป็นหัวข้อดังนี้

2.1 กายวิภาคของการบุกรุกผ่านระบบคอมพิวเตอร์เครือข่าย (Anatomy of Hack)(Scambray, J. *et al*. 2001)

2.1.1 การแกะรอย (Foot Printing)

วัตถุประสงค์ของการแกะรอย เพื่อที่จะทำให้การบุกรุกของผู้ไม่ประสงค์ดี ได้มาซึ่งข้อมูลที่จำเป็นต่อการบุกรุก เช่นข้อมูลของเน็ตเวิร์คบล็อก, หมายเลข IP Address และ ชื่อโดเมน ผู้บุกรุกจะค้นหาข้อมูลที่เกี่ยวข้องกับระบบที่เป็นเป้าหมายเพื่อกำหนดขอบเขตของการบุกรุก โดยการระบุรูปแบบของการแกะรอยที่กระทำโดยผู้บุกรุกนั้น เป็นสิ่งที่ยากในการทำการตรวจสอบโดยผู้ดูแลระบบ เทคโนโลยีและข้อมูลสำคัญที่ผู้บุกรุกต้องการค้นหาได้แก่

อินเทอร์เน็ต (Internet) มีข้อมูลสำคัญคือ

- ชื่อโดเมน
- เน็ตเวิร์คบล็อค
- หมายเลข IP Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อโดยตรงกับอินเทอร์เน็ต
- เน็ตเวิร์คเซอร์วิสที่ทำงานบนโปรโตคอล TCP และ UDP, ประเภทของโปรเซสเซอร์ (เช่น SPARC, X86)
- Access Control List (ACL) ซึ่งเป็นกลไกการควบคุมการเข้าถึงทรัพยากรต่างๆ บนเครื่อง
- ระบบป้องกันผู้บุกรุก (Intrusion Detection Systems, IDS)
- การระบุรายละเอียดเกี่ยวกับระบบในแง่ต่างๆ (รายชื่อผู้ใช้และกลุ่มต่างๆ, แบนเนอร์, ตารางเราท์ติ้งของเราท์เตอร์, ข้อมูลของ SNMP)

อินทราเน็ต (Intranet) มีข้อมูลสำคัญคือ

- เน็ตเวิร์คโปรโตคอลที่ใช้งานอยู่ภายใน (เช่น โปรโตคอล IP, IPX, DecNet และอื่นๆ)
- ชื่อโดเมนภายใน
- เน็ตเวิร์คบล็อค
- หมายเลข IP Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อโดยตรงกับอินเทอร์เน็ต
- เน็ตเวิร์คเซอร์วิสที่ทำงานบนโปรโตคอล TCP และ UDP, ประเภทของโปรเซสเซอร์ (เช่น SPARC, X86)
- Access Control List (ACL) ซึ่งเป็นกลไกการควบคุมการเข้าถึงทรัพยากรต่างๆ บนเครื่อง
- ระบบป้องกันผู้บุกรุก (Intrusion Detection Systems, IDS)
- การระบุรายละเอียดเกี่ยวกับระบบในแง่ต่างๆ (รายชื่อผู้ใช้และกลุ่มต่างๆ, แบนเนอร์, ตารางเราท์ติ้งของเราท์เตอร์, ข้อมูลของ SNMP)

การเชื่อมต่อจากระยะไกล (Remote Access) มีข้อมูลสำคัญคือ

- เบอร์โทรศัพท์ในระบบ(อะนาล็อก/ ดิจิตอล)
- ประเภทของเซิร์ฟเวอร์ที่ให้บริการ
- กลไกการตรวจสอบผู้ใช้ (Authentication Mechanism)

เอ็กซ์ทราเน็ต (Extranet) มีข้อมูลสำคัญคือ

- คอนเน็กชั่นต้นทางและปลายทาง
- ประเภทของคอนเน็กชั่น
- กลไกควบคุมการเข้าถึงทรัพยากร (Access Control Mechanism)

2.1.2 การสแกนเพื่อตรวจสอบ (Scanning) วัตถุประสงค์ของการทำการสแกน เพื่อที่จะค้นหาเครื่องคอมพิวเตอร์ที่เปิดให้บริการอยู่ในระบบ นอกจากนี้ยังรวมไปถึงการค้นหาพอร์ตที่เครื่องคอมพิวเตอร์เปิดใช้งานอยู่ ผู้บุกรุกจะอาศัยข้อมูลที่ได้จากการสแกน มาวิเคราะห์เพื่อหาช่องโหว่ของระบบที่อาจจะเปิดไว้

2.1.3 การรวบรวมรายละเอียด (Enumeration) วัตถุประสงค์ของการรวบรวมรายละเอียด ก็เพื่อที่จะเก็บรายละเอียดของระบบคอมพิวเตอร์เป้าหมาย เพื่อที่จะช่วยทำให้ผู้บุกรุกเพิ่มโอกาสในการทำการบุกรุกได้สำเร็จ จากข้อมูลของช่องโหว่ต่างๆ ที่อาจจะถูกเปิดอยู่ โดยสามารถแบ่งข้อมูลที่ผู้บุกรุกส่วนใหญ่ต้องการเป็นกลุ่มๆ ดังนี้

- รายชื่อทรัพยากรในเน็ตเวิร์ค
- รายชื่อแอคเคานต์ของผู้ใช้งาน และชื่อกลุ่มต่างๆ
- รายชื่อแอปพลิเคชั่น และแบนเนอร์ของแอปพลิเคชัน

2.1.4 การรับสิทธิในการเข้าถึงระบบ (Gaining Access) จากการทำ Enumeration ผู้บุกรุกจะพยายามกระทำการต่างๆ เพื่อให้ได้มาซึ่งสิทธิในการเข้าถึงระบบ มีรูปแบบแตกต่างกันดังนี้

- การดักจับข้อมูลจากเน็ตเวิร์ค (Packets Sniff) จากที่ Address Resolution Protocol (ARP) (RFC 826) เป็นโปรโตคอลที่ทำหน้าที่ค้นหา MAC Address ขนาด 48 บิตของเครื่องคอมพิวเตอร์ โดยทราบหมายเลข IP Address ขนาด 32 บิตของเครื่องคอมพิวเตอร์ นั้นๆ เมื่อเครื่องต้นทางต้องการติดต่อกับเพื่อนบ้านที่อยู่ในเน็ตเวิร์คเซ็กเมนต์เดียวกัน (รวมทั้งดีฟอลต์เราท์เตอร์ที่เครื่องต้นทางใช้ด้วย) เครื่องต้นทางจะทำต้องส่งแพคเก็ต ARP Broadcast Request ออกไปถามทุกๆ เครื่องในเซ็กเมนต์นั้น ว่าใครทราบบ้างว่าเครื่องที่มีหมายเลข IP Address เบอร์นี้มี MAC Address เป็นอะไร เครื่องที่เป็นเจ้าของหมายเลข IP Address นั้นๆ จะเป็นผู้ตอบกลับมาว่าตัวเองมี MAC Address เป็นอะไร หลังจากนั้นการสนทนาก็เริ่มขึ้น
  แต่ ARP สามารถที่จะเปลี่ยนทิศทางได้ ทำให้โอกาสที่จะเกิดการฉวยโอกาสของผู้บุกรุกที่ฉกฉวยเอาข้อมูลมาดูได้ ตัวอย่างของข้อมูลที่อาจจะถูกลักลอบดูโดยที่ผู้ใช้งานไม่รู้ตัว เช่น Username, Password และ ข้อความใน email เป็นต้น
- การบุกรุกโดยใช้กำลังเพื่อเอาชนะ (Brute Force Hacking) เป็นวิธีการบุกรุกเพื่อให้ได้มาซึ่งสิทธิในการเข้าถึงระบบ โดยการเดาสุ่มอย่างมีหลักการ ด้วยรูปแบบของการเดาสุ่มด้วยวิธีต่างๆ

2.1.5 การยกระดับให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบ (Escalating Privilege) จุดประสงค์ที่ผู้บุกรุกต้องการคือต้องการที่จะยกระดับตัวเองให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบ เพราะในบางครั้ง

ระบบปฏิบัติการที่มีการรักษาความปลอดภัยที่ดี จะมีการกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนให้อยู่ในระดับที่แตกต่างกัน การที่จะสามารถเข้าถึงข้อมูลทุกส่วนได้ จะมีเพียงผู้ดูแลระบบเท่านั้น และในบางระบบเช่น ระบบฐานข้อมูล จะมีการรักษาความปลอดภัยของตัวเอง โดยผู้ใช้งานที่สามารถเข้าถึงฐานข้อมูลทั้งหมดได้ก็คือ Database Administrator ของระบบฐานข้อมูลนั้น ในขณะที่ผู้ใช้งานอื่นจะได้รับอนุญาตให้ใช้งานตามที่ถูกกำหนดไว้เท่านั้น ดังนั้นสิทธิในการเข้าถึงข้อมูลในระดับผู้ดูแลระบบ จึงเป็นสิ่งที่ผู้บุกรุกปรารถนามาก

วิธีการที่ผู้บุกรุกใช้ในการได้มาซึ่งสิทธิของผู้ดูแลระบบมีดังนี้

- การใช้ช่องโหว่ของระบบปฏิบัติการแอปพลิเคชั่น โดยใช้เทคนิคการทำให้ Buffer ของโปรแกรมล้นและทำงานผิดพลาด แล้วอาศัยชุดคำสั่งเพื่อทำงานด้วยสิทธิของผู้ดูแลระบบ เหตุการณ์ที่ทำให้เกิดการล้นของข้อมูล เกิดจากขนาดของ Buffer ถูกเรียกว่าการทำ Buffer Over Flow
- การวางกับดักเพื่อดักจับรหัสผ่าน (Password Trojan) เป็นการสร้างโปรแกรมที่รอให้ผู้ดูแลระบบมา Execute และหลอกถามรหัสผ่าน ผู้ดูแลระบบที่ขาดประสบการณ์อาจจะหลงกลไป Execute เข้า โปรแกรมจะทำงานโดยสร้าง Prompt ของการใส่รหัสผ่าน หากผู้ดูแลระบบหลงกลใส่รหัสผ่านของตนไป โปรแกรมที่ผู้บุกรุกสร้างไว้ก็จะส่งรหัสผ่านไปยังปลายทางที่ผู้บุกรุกต้องการ เช่น ส่ง email ไปยัง email ของผู้บุกรุก เป็นต้น
- การถอดรหัสข้อมูลเพื่อหารหัสผ่าน (Password cracking) เป็นการใช้โปรแกรมถอดรหัส เพื่อถอดรหัสของแฟ้มข้อมูลสำคัญที่เก็บรหัสผ่านของผู้ดูแลระบบ

2.1.6 การขโมยข้อมูลเพิ่มเติม (Pilfering) เมื่อผู้บุกรุกสามารถยกระดับของตนเองให้ได้รับสิทธิในการเข้าถึงข้อมูลที่มีความสำคัญแล้ว นั่นก็หมายความว่าเกราะป้องกันข้อมูลที่ถูกป้องกันไว้ได้ถูกทำลายลง ผู้บุกรุกก็อาจจะมองหาช่องทาง เพื่อจะบุกรุกไปยังระบบอื่นต่อไป โดยใช้สิทธิในการเข้าถึงแฟ้มข้อมูลสำคัญ ซึ่งผู้บุกรุกสามารถค้นหาข้อมูลได้ไม่ยาก ยกตัวอย่างเช่น การดูข้อมูลใน Registry, การสำรวจ Configuration Files ต่างๆ

2.1.7 การปิดบัง อำพรางตัว (Covering Tracks) เป็นวิธีการซ่อนตัวที่ทำโดยผู้บุกรุก ทำเพื่อหลีกเลี่ยงการตรวจพบจากผู้ดูแลระบบตัวจริง ทำให้ผู้ดูแลระบบที่ขาดประสบการณ์ ไม่ทราบถึง

การบุกรุกที่ถูกกระทำไปแล้ว โดยผู้บุกรุกจะใช้การลบ แก้ไข เปลี่ยนแปลง ข้อมูลที่บ่งบอกถึงการบุกรุกเช่น Log Files ต่างๆ

2.1.8 การสร้างประตูลับ (Back Door) การที่ผู้บุกรุกสามารถเข้ามายังระบบได้แล้วนั้น ผู้บุกรุกจะพยายามครอบครองระบบไว้ให้ได้นานที่สุดเท่าที่จะสามารถทำได้ ผู้ดูแลระบบอาจจะมีการแก้ไขเปลี่ยนแปลง Configuration หรือซ่อมแซมช่องโหว่ของระบบ โดยที่ไม่ทราบว่าระบบถูกบุกรุกเข้ามาก่อนนี้แล้ว และได้ปิดช่องโหว่เก่าไป ผู้บุกรุกที่มีความสามารถจะสร้างช่องทางลับไว้ตามที่ต่างๆ ของระบบ เพื่อให้มั่นใจว่าถึงแม้ผู้ดูแลระบบจะปรับเปลี่ยน Configuration ของระบบไปอย่างใด หรือได้พยายามปิดช่องโหว่ไปแล้วก็ตาม ผู้บุกรุกก็จะสามารถอาศัยช่องทางลับกลับเข้ามายังระบบ และมีสิทธิเท่าเทียมผู้ดูแลระบบได้อีกครั้ง

2.1.9 การทำให้ระบบไม่สามารถให้บริการได้ เป็นการบุกรุกแบบที่ต้องการให้ระบบเป้าหมายไม่สามารถให้บริการได้ โดยการบุกรุกจะใช้วิธีการที่ระบบไม่สามารถปฏิเสธการให้บริการได้ (Denial of Services; DoS) ตัวอย่างของการบุกรุกแบบนี้เช่น การอาศัยช่องโหว่ของ Three way hand shake communication, Overlapping IP Fragment เป็นต้น

2.2 การใช้ภาษาสคริปต์ PHP (The PHP Group. 2001)

ภาษา PHP (Professional Home Page) เป็นภาษาที่ใช้ในการพัฒนาเว็บเพจที่มีความสามารถสูง และเรียนรู้ได้ง่ายภายในระยะเวลาสั้น นับเป็นภาษาที่นำความสามารถของ ASP ที่เรียนรู้ได้ง่ายและพัฒนาได้เร็ว มารวมกับความสามารถหลากหลายและทำงานได้เร็วของ Perl ทำให้ปัจจุบันภาษา PHP เป็นภาษาที่กำลังได้รับความนิยมและเป็นที่ต้องการของตลาดเพิ่มขึ้น จากการที่ PHP เป็นภาษาที่แจกให้ฟรี ไม่ต้องเสียค่าลิขสิทธิ์ สามารถทำงานได้กับ Server ที่เป็น NT, Linux หรือ Unix มีความสามารถในการติดต่อกับฐานข้อมูลได้หลายชนิด และสามารถติดต่อผ่าน ODBC ได้ รวมทั้งมีความสามารถที่เด่นกว่าภาษาอื่น คือทำงานด้านกราฟฟิกได้เป็นอย่างดี เป็นการเพิ่มความน่าสนใจให้กับเว็บเพจมากขึ้น ด้วยเหตุนี้เองทำให้ PHP เป็นภาษาที่น่าศึกษามากที่สุดสำหรับนักพัฒนาเว็บไซต์ยุคใหม่

ภาษา PHP พัฒนาโดย Rasmus Lerdorf (rasmus@lerdorf.on.ca) ทั้งนี้เพราะ Rasmus เคยเขียนเว็บเพจด้วยภาษา Perl มาก่อน แล้วพบว่าเว็บเพจผลลัพธ์ที่ได้นั้นยังไม่เป็นที่น่าพอใจ เขาจึงได้พัฒนาภาษาสคริปต์ขึ้นมาเพื่อใช้ในการเขียนเว็บเพจเอง และได้อาศัยเค้าโครงของภาษา Perl เป็น

ต้นแบบในการสร้างภาษาสคริปต์ดังกล่าวขึ้นมา โดยใช้โปรแกรมภาษา C++ เป็นเครื่องมือพัฒนาแรกเริ่มเดิมทีเขาเรียกภาษาสคริปต์นี้ว่า Personal Home Page

ต่อมาได้มีผู้ร่วมงานอีกหลายคนเข้ามาช่วยพัฒนา PHP โดยเพิ่มขีดความสามารถมากยิ่งๆขึ้น จนถูกกล่าวขานว่าน่าจะเป็น Professional Home Page มากกว่า Personal Home Page ดังนั้นถ้าพูดถึง PHP ในปัจจุบันจะหมายถึงคำที่ย่อมาจาก Professional Home page

ทั้งนี้ไม่เพียงเพราะ PHP เป็นโปรแกรมที่แจกจ่ายให้ใช้ฟรีเท่านั้น แต่มีประสิทธิภาพและสามารถทำงานได้หลากหลายรูปแบบ คือใช้ได้กับระบบปฏิบัติการหลายระบบ และทำงานร่วมกับโปรแกรมเว็บเซิร์ฟเวอร์ได้หลากหลาย ไม่ว่าจะเป็น Personal Web Server (PWS) ซึ่งใช้กับระบบปฏิบัติการวินโดว์ส 95 หรือ 98 หรือ Internet Information Server (IIS) ซึ่งใช้กับวินโดว์ส เอ็นที หรือจะใช้กับ Apache Web Server ภายใต้ระบบปฏิบัติการ Linux และระบบปฏิบัติการอื่นๆ ก็ได้

แต่นอกจากความสามารถความสามารถที่กล่าวมาในข้างต้น PHP ยังเป็นภาษาที่ถูกนำมาพัฒนา Script ที่สามารถใช้กับ Shell ของระบบ Operating System ได้ด้วย โดยการทำงานจะคล้ายกับการทำงานของภาษา Perl

การใช้ภาษา PHP เพื่อทำงานกับ Operating System Shell

ลักษณะการเขียนเว็บเพจให้มีสคริปต์ PHP จะอาศัยวิธีการเขียนซอร์ดโค้ดให้อยู่ในรูปแบบของภาษาสคริปต์ PHP ทั้งหมดเลยก็ได้ (เหมือนกับที่เขียนเว็บเพจด้วยภาษา Perl) สคริปต์ PHP จะใช้แท็กในการกำหนดขอบเขตของสคริปต์ ซึ่งอาจเรียกว่า PHP Script Tag โดยประกอบด้วยแท็กเปิดและแท็กปิด

แท็กเปิดของ PHP เขียนได้ 2 แบบคือ <? หรือ <? Php ส่วนแท็กปิดเขียนอยู่ในรูป ?>
ในกรณีที่ต้องเขียนสคริปต์ PHP ร่วมกับสคริปต์ XML (Extensible Markup Language) จะ ต้องเขียนแท็กเปิดของ PHP เป็น <? Php เพื่อความแตกต่าง แต่ไม่ว่าจะเปิดแบบ <? หรือ <? Php ก็ตาม วิธีการเขียนเว็บเพจแบบนี้เรียกว่าเป็นการเขียนในลักษณะฝังสคริปต์ หรือ Embedded Script นั่นเอง

เราจะพบเป็นการนำวิธีการฝังสคริปต์มาใช้ในการเขียนเว็บเพจมาขึ้นเรื่อยๆ ตัวอย่างเช่นการเขียนสคริปต์ ASP (Active Server Pages) ฝังลงในเว็บเพจ ก็จะมีเครื่องหมาย <% และ %> ใช้กำกับในการเปิดและปิดส่วนที่เป็นสคริปต์ ASP เป็นต้น ทั้งนี้เพราะเป็นวิธีการเขียนเว็บเพจที่สะดวกต่อผู้เขียนในการตรวจสอบการทำงานของเว็บเพจ โดยส่วนของเว็บเพจที่ไม่ได้กำกับด้วยสคริปต์ใดๆ ก็จะแสดงผลไปตามข้อความนั้นๆโดยตรงหากเราจะเปลี่ยนแปลงแก้ไขข้อความใดๆก็จะกระทำได้เลย โดยไม่ต้องกลัวว่าเว็บเพจจะทำไม่ถูกต้อง และเมื่อเว็บเพจแจ้งข้อความว่าเกิดข้อผิดพลาด อันเนื่องมาจากการทำงานของสคริปต์ เราก็เพียงไปแก้ไขหรือปรับปรุงเฉพาะจุดที่สคริปต์นั้นๆ

ข้อแตกต่างของสคริปต์ PHP กับสคริปต์ภาษา HTML คือสคริปต์ PHP เป็น Server Side Script โดยถูกเรียกให้ทำงานทางฝั่งเซิร์ฟเวอร์ ส่วนสคริปต์ ภาษา HTML เป็น Client Side Script นั่นคือ สคริปต์จะถูกเรียกทำงานทางฝั่งไคลเอนต์หรือฝั่งของบราวเซอร์

โดยทั่วไปเวลาเขียนเว็บเพจเรามักจะกำหนดนามสกุลของไฟล์เว็บเพจให้สื่อความหมายในตัว เช่น เป็น .html เพื่อให้ทราบว่าเป็นไฟล์ที่เขียนโดยมีแท็กคำสั่งของภาษา HTML อยู่ข้างใน เช่นเดียวกันเมื่อเราเขียนเว็บเพจให้มีสคริปต์ภาษา PHP ปกติเราจะกำหนดนามสกุลของไฟล์ให้เป็น .php3 ซึ่งหมายถึงไฟล์เว็บเพจที่เขียนขึ้นเพื่อใช้กับ PHP เวอร์ชัน 3 แต่ก็ไม่ได้เป็นกฎเกณฑ์บังคับตายตัวว่าจะต้องระบุนามสกุลของไฟล์เป็นแบบนี้ เราอาจกำหนดเป็น .php เฉยๆก็ได้ ทั้งนี้ขึ้นอยู่กับเราว่าจะกำหนดให้เว็บเซิร์ฟเวอร์ของเรารับรู้นามสกุลของไฟล์เว็ลเพจ PHP เป็นอะไร

2.3 ดาต้าเบสเซิร์ฟเวอร์ MySQL (The PHP Group. 2001)

PHP มีฟังก์ชันที่จะติดต่อกับโปรแกรมดาต้าเบสเซิร์ฟเวอร์ได้หลายหลากตระกูล อย่างเช่น Adabas D, MySQL, Oracle, PostgraSQL, Sybase, FilePro, mSQL, Velocis, Informix, Unix dbm และ ODBC เป็นต้น ซึ่งดาต้าเบสเซิร์ฟเวอร์แต่ละโปรแกรมก็จะใช้ฟังก์ชันในการติดต่อทำงานที่แตกต่างกันออกไป

MySQL เป็นโปรแกรมด้านดาต้าเบสเซิร์ฟเวอร์ที่ทำงานภายให้ระบบปฏิบัติการหลายระบบ มีทั้ง Linux หรือ UNIX และ Windows NT สามารถเลือกดาวน์โหลดได้ที่ www.mysql.com ซึ่งจะมีคำอธิบายวิธีการติดตั้งให้มาด้วย

ผู้ใช้งานดาต้าเบสเซิร์ฟเวอร์ของ MySQL มีอยู่เป็นจำนวนมาก นับว่าเป็นดาต้าเบสเซิร์ฟเวอร์ที่มีผู้ใช้งานมากที่สุดโปรแกรมหนึ่งในบรรดาดาต้าเบสเซิร์ฟเวอร์ที่มีใช้กันอยู่ ทั้งนี้นอกเหนือจากเพราะว่าเป็นโปรแกรมแจกจ่ายฟรีแล้ว ประสิทธิภาพก็ไม่ด้อยไปกว่าดาต้าเบสเซิร์ฟเวอร์อื่นๆ ที่ทำงานในระดับเดียวกันหรือเหมือนๆกัน แต่ต้องใช้งบประมาณซื้อหามาในราคาที่ค่อนข้างสูง

และหากเครื่องที่เป็นเซิร์ฟเวอร์มีศักยภาพที่สูง เช่น มีความจุหน่วยความจำมาก, มีซีพียูความเร็วสูงๆ, มีฮาร์ดดิสก์ที่ทำงานค้นหาข้อมูลได้เร็วๆ แล้วละก็ เราจะได้ประโยชน์จากดาต้าเบสเซิร์ฟเวอร์มากยิ่งขึ้น

2.4 ระบบปฏิบัติการลีนุกซ์ (Linux) (Red Hat, Inc. 2003)

ลีนุกซ์ คือระบบปฏิบัติการแบบ 32 บิต ที่เป็นยูนิกซ์โคลน สำหรับเครื่องพีซี และแจกจ่ายให้ใช้ฟรี สนับสนุนการใช้งานแบบหลากงาน หลายผู้ใช้ (Multi User - Multi Tasking) มีระบบ X วินโดวส์ ซึ่งเป็นระบบการติดต่อผู้ใช้แบบกราฟฟิก ที่ไม่ขึ้นกับโอเอสหรือฮาร์ดแวร์ใดๆ (มักใช้กัน

มากในระบบยูนิกซ์) และมาตรฐานการสื่อสาร TCP/IP ที่ใช้เป็นมาตรฐานการสื่อสารใน อินเตอร์เน็ต ลีนุกซ์มีความเข้ากันได้ กับ มาตรฐาน POSIX ซึ่งเป็นมาตรฐานอินเทอร์เฟสที่ระบบยูนิกซ์ส่วนใหญ่จะต้องมีและมีรูปแบบบางส่วนที่คล้ายกับระบบปฏิบัติการยูนิกซ์จากค่าย Berkeley และ System V

โดยความหมายทางเทคนิค ลีนุกซ์ เป็นเพียงเคอร์เนล (kernel) ของระบบปฏิบัติการ ซึ่งจะทำหน้าที่ในด้านของการจัดสรรและบริหารโพรเซสงาน การจัดการไฟล์และอุปกรณ์ I/O ต่างๆ แต่ผู้ใช้ทั่วๆไปจะรู้จักลีนุกซ์ผ่านทางแอพพลิเคชั่นและระบบอินเทอร์เฟสที่เขาเหล่านั้นเห็น (เช่น Shell หรือ X วินโดวส์) และนอกจากแพลตฟอร์มอินเทลแล้ว ปัจจุบันลีนุกซ์ยังได้ทำการพัฒนาระบบเพื่อให้สามารถใช้งานได้บนแพลตฟอร์มอื่นๆด้วย เช่น DEC Alpha, Motorolla Power-PC , MIPS เมื่อคุณสร้างแอพพลิเคชั่นขึ้นมาบนแพลตฟอร์มใดแพลตฟอร์มหนึ่งแล้ว เราสามารถย้ายแอพพลิเคชั่น ของคุณไปทำงานบนแพลตฟอร์มอื่นได้ไม่ยาก

2.4.1 คุณสมบัติของลีนุกซ์

- เป็นระบบปฏิบัติการฟรี ที่สามารถขอจากผู้ที่มีลีนุกซ์ หรือจะดาวน์โหลดจากอินเตอร์เน็ตหรือบีบีเอสได้โดยไม่ผิดกฎหมาย
- ลีนุกซ์สามารถใช้งานได้บนตัวประมวลผลกลางหลากหลายตั้งแต่อินเทล, โมโตโรลา, ดิจิตอลอัลฟา, พาวเวอร์พีซี, ไปจนถึง สปาร์คของซัน นอกจากนี้ยังมีผู้พัฒนาโปรแกรมประยุกต์ออกมากันมากมาย
- ลีนุกซ์เป็นระบบปฏิบัติการ 32 บิตเต็มรูปแบบ ซึ่ง สามารถจะดึงเอาพลังของเครื่องคอมพิวเตอร์ออกมาได้อย่างเต็มกำลัง
- มีคุณลักษณะของระบบ UNIX เป็นระบบหลากผู้ใช้ หลายงาน มีระบบอินเทอร์เฟสแบบกราฟฟิกเรียกว่า X Windows เป็นมาตรฐานของระบบยูนิกซ์ทั่ว ๆ ไป นอกจากนี้ยังสนับสนุนโปรโตคอลแบบ TCP/IP,SLIP, PPP, UUCP และอื่น ๆ
- สามารถหาข้อมูลเพิ่มเติมได้ง่าย และผู้คนมากมายคอยสนับสนุนผ่านอินเตอร์เน็ต

2.4.2 แอพพลิเคชั่นบนลีนุกซ์

มีผู้ใช้งานลีนุกซ์หลากหลายระดับ ไม่ว่าจะเป็นระดับเดอร์นัลแฮกเกอร์ ที่ศึกษาเกี่ยวกับการทำงานของระบบปฏิบัติการในระดับลึก ไปจนถึงผู้ใช้ทั่วไป แอพพลิเคชั่นที่พัฒนามาเพื่อใช้งานบน

- Emacs, Tex และ LaTeX เป็นซอฟท์แวร์ที่ใช้จัดเตรียม และพิมพ์เอกสารต่างๆ
- Web Browser เช่น เนตสเคป และ โมเสค
- เกมส์ต่างๆ เช่น DOOM เป็นต้น

แอปพลิเคชั่นที่กล่าวถึงข้างต้นนี้ ส่วนใหญ่จะเป็นแอพพลิเคชั่นที่แจกจ่ายฟรี ผ่านทางอินเตอร์เน็ต แต่ในปัจจุบันสำหรับลีนุกซ์แล้วก็เริ่มที่จะมีตลาดของตัวเองมากขึ้นเรื่อยๆ ทำให้มีบริษัทต่างๆได้เริ่มทำการพัฒนาแอพพลิเคชั่นที่เป็นคอมเมอร์เชียลแวร์ ที่จะต้องจ่ายเงินซื้อหาถ้าหากต้องการใช้งานแอพพลิเคชั่น เหล่านี้ และผู้พัฒนาก็มีทั้งในยุโรปและอเมริกา ตัวอย่างเช่น คาต้าเบสเซอร์ฟเวอร์ YardSQL, JustLogic SQL สเปรตชีต NEXUS และเวิร์ดโพรเซสเซอร์ WordPerfect นอกจากนี้ยังมีผู้รวบรวมแอพพลิเคชั่นที่จำเป็น หลายๆชนิดเข้าด้วยกัน และมีการใช้งานบนระบบเดสก์ทอปวินโดวส์ ที่น่าประทับใจ เช่น GNOME โดยระบบนี้จะมี ระบบควบคุมเนตเวอร์ก เวปบราวเซอร์ และ เวิร์ดโพรเซสเซอร์ ฯลฯ เราสามารถจะสื่อสารกับอินเตอร์เน็ต ทำบีบีเอสส่วนตัว ทำระบบงานแบคออฟฟิศที่ใช้งานจริง ใช้ทำการศึกษา หรือแม้แต่ใช้เป็นอินเตอร์เน็ตเซอร์ฟเวอร์ หรือ เวปเซอร์ฟเวอร์ก็ได้ นอกจากนี้ยังสามารถประยุกต์การใช้งานให้ลีนุกซ์เป็นอินเตอร์เน็ตเกตเวย์ และเวปเซอร์ฟเวอร์ ซึ่งลีนุกซ์ก็จะมียูทิลิตีต่างๆเตรียมไว้ให้และที่จำเป็นในการติดตั้งทุกอย่าง ก็หาได้ง่ายจากอินเตอร์เน็ต

2.4.3 การนำ Linux ไปใช้งานในองค์กร

Linux มีจุดแข็งตรงที่นำมาใช้งานเป็นเซอร์ฟเวอร์ ชนิดต่างๆ และทำงานได้ดีทางด้าน Network TCP/IP ดังเช่น

1. Internet gateway คือ นำ Linux มาติดตั้ง บน PC แต่ต้องมี LAN card และ modem ทำให้สามารถเข้าไปใช้ internet พร้อม ๆ กัน หลาย ๆ จอได้โดยใช้ account เดียว และ internet gateway ที่ run ด้วย Linux ถือได้ว่า stable มาก และมีความเร็วสูง

2.E-mail server ในองค์กรที่มีผู้ทำงานต้องการใช้ e-mail ประมาณ 100 กว่าคน ถ้าจะใช้ win NT + MS exchange ก็คงเสียค่าลิขสิทธิ์

3.Web server เพื่อใช้เป็นแหล่งเผยแพร่ข้อมูลขององค์กร ส่วน program ที่ run web server ก็เป็น Apache ที่แจกมาพร้อมกับ CD ที่ติดตั้ง Linux

4.FTP server เอาไว้เก็บโปรแกรมที่น่าสนใจโดย download จาก internet หรือข้อมูลอื่นมาเก็บไว้ที่ Server เพื่อให้บริการ

5.File server โดยติดตั้ง software ที่ชื่อ SAMBA ไว้ที่เครื่อง server ซึ่งจะทำให้เป็นเหมือน PC ที่ run window และเปิด share file เอาไว้ ซึ่งสามารถจะ copy และ paste ได้เหมือนปกติที่ทำงานกับ PC ที่ run window ทำให้นำไปใช้เป็นตัว backup ข้อมูลของ PC ที่ run window ได้

6. Print server

7.Terminal server เอาไว้ link modem เข้ามาที่office เพื่อ check e-mail หรือ browse ไป internet โดยอาศัย card ที่เรียกว่า multi serial card ในกรณีที่มีความจำเป็นต้องใช้ port มากกว่า 2 port

8.Proxy server เอาไว้ช่วยทำ cache ของข้อมูล ของ web site ที่ใช้บ่อยๆ ทำให้ไม่ไป load traffic ที่ link ไป ISP และ ฝั่ง browser ทำงานได้เร็วขึ้น กรณีที่ข้อมูลมีอยู่ใน cache แล้ว โดยใช้ software ที่ชื่อว่า squid

9.ใช้ Linux ทำเป็น TCP/IP router เชื่อม LAN 2 วงเข้าด้วยกัน

2.4.4 ระบบการจัดเก็บแฟ้มข้อมูลของ Linux

มีการทำงานที่รวดเร็ว มีชื่อเรียกว่า Extended File System Version 2 (EXT2) ซึ่งพัฒนาขึ้นโดย Remy Card คุณสมบัติและข้อมูลต่าง ๆ ในระบบปฏิบัติการลินุกซ์ถูกเก็บไว้ในรูปแบบของไฟล์ ซึ่งสามารถแยกประเภทของไฟล์ออกมาได้ดังนี้

- ไฟล์ทั่วไป (Ordinary Files) เป็นที่รวบรวมข้อมูลที่เป็นรูปแบบ ตัวอย่างเช่น Source Code File, Document File.
- Directory Files คือ Node ที่เป็นเส้นทางให้ไฟล์นั้นสามารถเชื่อมถึงกันโดยเราสามารถที่จะท่องไปในยังส่วนต่าง ๆ ของโครงสร้างไฟล์ (Tree)
- FIFO files คือ ไฟล์ที่ยอมไม่ให้มีความสัมพันธ์กับกระบวนการในการติดต่อกับส่วนอื่น ๆ
- Special Files คือ ไฟล์ที่ถูกสร้างขึ้นเป็นส่วนหนึ่งทางกายภาพ เช่น Tape หรือ Disk ดังนั้น ไฟล์พิเศษนี้จึงไม่ได้เป็นไฟล์ที่แท้จริงแต่เป็นเพียงการแทนที่
- Directories directories ก็เป็น file ๆ หนึ่ง เพียงแต่มีรูปแบบการเก็บข้อมูลที่พิเศษ แต่ละไดเร็คทอรี่จะประกอบด้วย list ของ directory entries ยังมีไดเร็คทอรี่พิเศษอีก 2 ชนิด คือ "." และ ".." ก็จะมีการเก็บ file ชื่อ "." และ ".." ภายในไดเร็คทอรี่นั้นๆ โดยมีจุดพิเศษ คือ ทั้ง 2 file นี้จะถูกสร้าง โดยอัตโนมัติ ในขณะที่สร้างไดเร็คทอรี่ใหม่ โครงสร้างของระบบไฟล์และไดเรกทอรีในระบบยูนิกซ์ทำการเก็บข้อมูลโดยใช้ ไฟล์ และ ไดเรกทอรี เข้ามาช่วย โดยจะมีลักษณะเป็นรูปแบบของ hierarchy หรือ

โครงสร้างแบบต้นไม้ คล้ายกับดอส จะเห็นว่ามีรูปแบบการเก็บข้อมูลที่คล้ายกัน เพียงแต่การใช้งานจะแตกต่างกันบ้าง ไดเรกทอรีจะเปรียบเสมือนแฟ้มที่สามารถเก็บไฟล์ต่างๆ ในไดเรกทอรีลำดับบนๆ ก็เหมือนกับแฟ้มขนาดใหญ่ ซึ่งนอกจากจะเก็บไฟล์ได้แล้วก็ยังสามารถเก็บไดเรกทอรีอื่นๆ ได้ด้วย ไดเรกทอรีลำดับบนสุดจะถูกเรียกว่า ไดเรกทอรีราก (root directory) ซึ่งจะประกอบไปด้วยไฟล์และไดเรกทอรีต่างๆ ในไดเรกทอรีที่ย่อยลงมาก็อาจจะประกอบไปด้วยไฟล์และไดเรกทอรีไปเรื่อยๆ

โครงสร้างไดเร็คทอรี่ของ / (Root) ไดเร็คทอรี่ราก

bin	ไฟล์คำสั่งทั่วไปของระบบ
boot	ไฟล์สำหรับการ boot ระบบ เช่น ไฟล์ของเคอร์เนล (vmlinuz)
dev	ไฟล์อุปกรณ์ (device file) ที่ใช้สำหรับติดต่อกับระบบ
etc	ไฟล์ configuration ของระบบ
home	โฮมไดเร็คทอรี่ของผู้ใช้งานทั่วไปของระบบ
lib	แชร์ไลบรารี่และเคอร์เนลโมดูล
mnt	ไดเร็คทอรี่สำหรับทำการ mount พาร์ทิชั่นขึ้นมาชั่วคราว
lost+found	เก็บข้อมูลผิดพลาดต่าง ๆ ที่เกิดกับ hard disk
proc	เก็บ system info หรือข้อมูลของระบบ
root	โฮมไดเร็คทอรี่สำหรับผู้ดูแลระบบ
sbin	ไฟล์คำสั่งสำหรับการจัดการระบบ
tmp	ไฟล์ชั่วคราว
usr	เก็บโปรแกรมและข้อมูลที่สามารถใช้งานร่วมกันกับเครื่องอื่น ๆ
var	ข้อมูลทั่วไปของระบบที่ถูกใช้โดยโปรแกรมต่าง ๆ

2.4.5 File permissions and Ownership

คือ การแสดงสถานะในลักษณะต่างๆ ของไฟล์ หรือไดเรกทอรี่ เพื่ออนุญาตให้บุคคลภายนอก หรือแม้แต่เจ้าของ (หรือผู้สร้าง) ไฟล์หรือไดเรกทอรี่นั้นได้ทราบว่า ไฟล์หรือไดเรกทอรี่นั้นๆ สามารถที่จะดำเนินการแบบใดได้บ้าง เช่น สามารถแก้ไข (หรือเขียนทับได้) สามารถเปิดอ่านได้ หรือสามารถทำงานได้

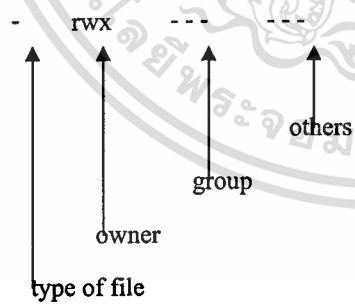
การกำหนด File Permissions and Ownership นี้ ผู้ใช้ (หรือบุคคลทั่วไป) ไม่สามารถกำหนดได้ตามใจชอบ ผู้ที่สามารถกำหนดได้มีเพียงเจ้าของ หรือผู้สร้างไฟล์ หรือไดเรกทอรี่นั้น

เท่านั้น ซึ่งสามารถที่จะกำหนดให้เป็นแบบใดก็ได้ตามแต่ที่ต้องการ โดยใช้คำสั่ง chmod และตามด้วย option แบบต่างๆ ที่ต้องการกำหนด เช่น chmod 755 filename ผลที่ได้จากคำสั่งนี้จะได้ไฟล์ที่สามารถอ่านได้สำหรับผู้ใช้ทุกคน และดำเนินการกับตัวไฟล์หรือไดเรกทอรี่นั้นได้ แต่ผู้สร้างเท่านั้นที่สามารถแก้ไขได้

เมื่อใช้คำสั่ง ls –l หรือ ls –la ที่หน้าจอจะมีลักษณะดังนี้

```
$ ls –l
total 16
drwx------  8 sc404896  student    2048  Jun 24  13:18  cal.p
```

โดยที่ 10 ตัวแรกจะแสดง permission ของ file จะแบ่งได้เป็น 4 กลุ่ม กลุ่มแรก 1 ตัว อีก 3 กลุ่ม ๆ ละ 3 ตัว ดังรูปข้างล่างนี้



<u>กลุ่มแรก</u> จะบอกให้เราทราบว่าเป็น file หรือ directory ถ้าเป็นตัว d หมายความว่าเป็น directory แต่ถ้าเป็นเครื่องหมาย - หมายความว่าเป็น file

<u>กลุ่มที่สอง, สาม และสี่</u> จะประกอบด้วยตัวอักษรกลุ่มละ 3 ตัว คือ r,w,x ซึ่งจะใช้เป็นตัวแสดง สถานะของไฟล์ว่า ไฟล์นั้นสามารถที่จะดำเนินการได้กับตัวมันเองอย่างไรบ้าง ตามเงื่อนไขที่กำหนดไว้ดังนี้

ถ้ามี r ในกลุ่มใดๆ แสดงว่ากลุ่มนั้นสามารถที่จะอ่านได้

ถ้ามี w ในกลุ่มใดๆแสดงว่ากลุ่มนั้นสามารถที่จะเขียนหรือแก้ไขไฟล์นั้นได้

ถ้ามี x ในกลุ่มใดๆแสดงว่ากลุ่มนั้นสามารถที่จะดำเนินการ(execute)กับไฟล์นั้นได้โดย กลุ่มที่สองหมายถึงเกี่ยวกับเจ้าของ (หรือผู้สร้างไฟล์) กลุ่มที่สามคือกลุ่ม(ที่ทำงานหรือถูกจัดให้อยู่ในกลุ่มเดียวกัน) และกลุ่มที่สี่คือกลุ่มบุคคลอื่น ๆ เช่น -rwxr- - r- -
หมายความว่าเป็น file โดยที่เจ้าของสามารถอ่านได้เขียนได้และ execute ได้ ในขณะที่กลุ่มและคนอื่นๆสามารถอ่านได้อย่างเดียว

2.5 หลักการพื้นฐานของแพ็คเกจฟิลเตอร์ (Rusty Russell. 2000)

การส่งข้อมูลในระบบเน็ตเวิร์คจะอยู่ในรูปแบบของแพ็คเกจ ซึ่งแต่ละแพ็คเกจจะประกอบไปด้วยส่วนที่เรียกว่าเฮดเดอร์และบอดี้ เฮดเดอร์จะเก็บข้อมูลเกี่ยวกับคอมพิวเตอร์ต้นทางและปลายทางที่แพ็คเกจจะถูกจัดส่งไป รวมไปถึงรายละเอียดการจัดการอื่นๆ ส่วนบอดี้จะบรรจุข้อมูลแท้จริงที่ใช้ส่ง การดาวโหลดแพ็คเกจแต่ละแพ็คเกจไม่สามารถทำได้ภายในครั้งเดียว ตัวอย่างเช่น แพ็คเกจที่มีความยาว 50 k อาจจะต้องดาวโหลดครั้งละ 1460 ไบต์ ต่อเนื่องกันไป 36 ครั้ง เพื่อจะได้ข้อมูลทั้งหมดโปรโตคอลบางประเภท เช่น TCP ซึ่งถูกใช้สำหรับการส่งข้อมูลในเว็บไซต์ ส่งเมลหรือ Remote Login ใช้หลักการที่เรียกว่า คอนเนคชั่น นั่นคือก่อนที่จะมีการส่งผ่านข้อมูลแต่ละครั้ง แต่ละแพ็คเกจจะต้องมีการแลกเปลี่ยนข้อมูลในส่วนของเฮดเดอร์เพื่อบอกถึงความพร้อมในการส่งจากต้นทางและรับข้อมูลจากปลายทางเสียก่อน การรับส่งแพ็คเกจถึงจะเริ่มขึ้นได้

IPCHAINS แพ็คเกจฟิลเตอร์ คือ ซอฟแวร์ที่ใช้สำหรับอ่านข้อมูลของเฮดเดอร์แล้วทำการตัดสินว่าจะทำการอนุญาตหรือปฏิเสธแพ็คเกจที่ถูกส่งมา การตัดสินแพ็คเกจจะมีอยู่ 3 กรณี

กรณีแรก แพ็คเกจจะถูกปฏิเสธสมือนหนึ่งคอมพิวเตอร์ปลายทางไม่เคยได้รับแพ็คเกจนั้นมาก่อน

กรณีที่สอง แพ็คเกจฟิลเตอร์จะอณุญาตให้แพ็คเกจผ่านเข้ามาในระบบได้และ

กรณีที่สาม แพ็คเกจจะถูกปฏิเสธเหมือนกรณีแรกแต่จะทำการส่งข้อมูลตอบกลับไปยังแหล่งต้นทางเพื่อบอกถึงการปฏิเสธแพ็คเกจนั้นๆ

ภายใต้ระบบปฏิบัติการลีนุกซ์ แพ็คเกจฟิลเตอร์จะถูกสร้างอยู่ในส่วนของเคอร์เนล และทำการประมวนผลข้อมูลบางอย่างได้มากกว่าระบบปฏิบัติการอื่นๆ แต่หลักการในการตัดสินแพ็คเกจยังคงยึดหลักการที่ได้กล่าวมาแล้วข้างต้น

การใช้งาน IPCHAINS เพื่อควบคุม Packets

ถ้าผู้ใช้เลือกใช้ระบบปฏิบัติการลีนุกซ์สำหรับทำการติดต่อระหว่างเนตเวิร์คภายในกับเนตเวิร์คภายนอก เช่นอินเตอร์เนต ผู้ใช้สามารถที่จะกำหนดเงื่อนไขในการควบคุมการส่งข้อมูลได้ ยกตัวอย่างเช่นสามารถป้องกันไม่ให้แพ็คเกจถูกส่งไปยังเส้นทางที่กำหนดไว้ หรือจำกัดโปรโตคอลที่ใช้ในการส่ง นั่นหมายถึง แพ็คเกจที่จะถูกจัดส่งออกไปทั้งหมดต้องผ่านเงื่อนไขที่ถูกกำหนดไว้ในส่วนของลีนุกซ์ก่อน หรือในกรณีการควบคุมการรับข้อมูลจากภายนอกเข้ามายังเนตเวิร์คภายในเช่น ใช้เบราเซอร์เนตสเคปเพื่อที่จะเข้าไปอ่านข้อมูลของคอมพิวเตอร์เครื่องหนึ่งนอกระบบ แต่ทุกครั้งก่อนที่จะอ่านข้อมูลได้ คอมพิวเตอร์เครื่องนั้นได้กำหนดให้มีการดาวโหลดข้อมูลจากอีกเว็บไซต์หนึ่งเสียก่อน ซึ่งเราสามารถหลีกเลี่ยงการดาวโหลดนี้ได้โดยการกำหนดให้แพ็คเกจฟิลเตอร์ไม่อนุญาตให้มีการรับข้อมูลที่มาจากเว็บไซต์นั้น

ตัวอย่างกฎของ ipchains

/sbin/ipchains –p icmp –s 0/0 –j DENY

ความหมายของกฎข้างต้นคือ ปฏิเสธโปรโตคอล icmp ทุกตัวที่เรียกเข้ามาจากทุกๆ IP

2.6 Snort IDS (Roesch, M;Green, C. 2002)

Snort เป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่าย (network intrusion detection) โดย Martin Roesch (http://www.snort.org) การทำงานของ Snort จะใช้ไลบรารี (library) พื้นฐานชื่อ libpcab ซึ่งใช้กันโดยทั่วไปในบรรดา network sniffer และ network analyzer ทั้งหลาย สำหรับ Snort นั้นสามารถทำ protocol analysis, content searching/matching, ตรวจจับการบุกรุกและ probe เช่น buffer overflow, stealth port scan, CGI attack, SMB probe, OS Fingerprint และอื่นๆ นอกจากนี้ยังมีคุณสมบัติในการทำ real-time alerting อีกด้วย นอกเหนือจากการเก็บล็อกไปที่ syslog หรือเก็บแยกไฟล์ต่างหาก และยังสามารถ alert ผ่าน winpopup ผ่านทาง Samba's client ได้อีกด้วย(ต้อง compile ด้วย option --enable-smbalerts)

Snort และ Database

Snort สนับสนุนฐานข้อมูล MySQL, Postgresql, unixODBC และ Oracle ในกรณีที่ท่านใช้ฐานข้อมูลอื่น เช่น DB2, Informix หรืออื่นๆ ท่านสามารถใช้ unixODBC เป็นตัวกลางในการเชื่อมต่อได้

บทที่ 3

การออกแบบระบบ

3.1 ระบบการทำงานปัจจุบัน

การตรวจสอบว่าระบบเครือข่ายมีการบุกรุกด้วยวิธีใด จากที่ไหน และกระทำต่อใครนั้น IDS สามารถติดตามได้โดยอาศัย Rules Base ที่อยู่ในตัว IDS เอง และ Rules Base นี้จะเป็นหัวใจของการตรวจจับการบุกรุก เพื่อแจ้งเตือนให้ผู้ดูแลระบบทราบถึงภัยที่มาถึง ข้อมูลที่ได้จากการแจ้งเตือนซึ่งเป็นผลลัพธ์ของ IDS จะถูกระบบ Automatic Firewall Management System นำไปวิเคราะห์เพื่อหาระดับความเสี่ยงของการบุกรุก เพื่อสร้าง Rules Base ที่เหมาะสมให้กับ Firewall และติดตั้ง Rules Base ดังกล่าวให้แก่ไฟร์วอลล์โดยอัตโนมัติ จากแต่เดิมเมื่อมีการตรวจพบการบุกรุกและแจ้งเตือนจาก IDS ผู้ดูแลระบบต้องคอยตรวจสอบข้อมูลที่ IDS ส่งมาให้เพื่อทำการวิเคราะห์และกำหนด Rules base ที่เหมาะสมให้กับไฟร์วอลล์ พร้อมทั้งต้องนำ Rules Base ดังกล่าวไปติดตั้งให้กับไฟร์วอลล์ ซึ่งบางครั้งการที่ผู้ดูแลระบบจะทราบถึงการแจ้งเตือนจาก IDS ก็อาจจะกินเวลาหลายชั่วโมง หรือในบางครั้งอาจกินเวลาถึงหลายวัน ทำให้การป้องกันการบุกรุกทำได้ไม่ดีเท่าที่ควร

รูปแบบของการบุกรุกที่เกิดขึ้นมีได้หลากหลายรูปแบบ และมีความเสี่ยงของการโจมตีที่แตกต่างกันด้วย ข้อมูลของการบุกรุกต่างๆ จะเป็นหัวใจของการวิเคราะห์ผลกระทบที่อาจเกิดขึ้นจากการบุกรุกนั้นๆ เพื่อนำไปใช้หาแนวทางในการป้องกันการบุกรุกที่เหมาะสม เพื่อให้เกิดผลกระทบต่อการใช้งานของผู้ใช้งานโดยรวมให้น้อยที่สุดด้วย

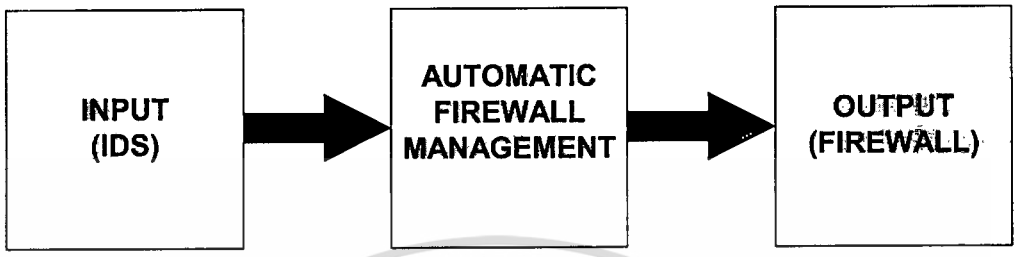
3.2 การออกแบบระบบ

แนวทางการออกแบบระบบ จะแบ่งการทำงานออกเป็นสามส่วนใหญ่ๆ ตามรูปที่ 3.1 โดยมีรายละเอียดดังนี้

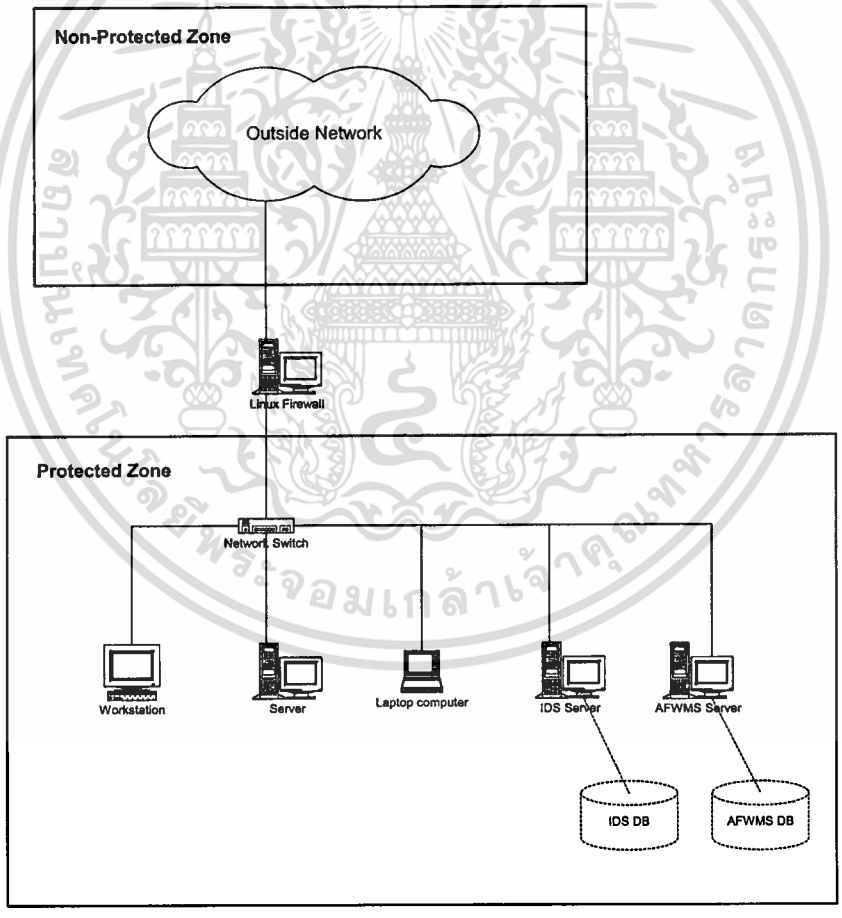
1. ภาคอินพุตของระบบ จะเป็นการทำงานในลักษณะ การไปดึงข้อมูลของการบุกรุกจากระบบฐานข้อมูลของ IDS

2. ระบบไฟร์วอลล์อัตโนมัติ จะเป็นตัววิเคราะห์ความเสี่ยงของการบุกรุก เพื่อหา Rules Base ของไฟร์วอลล์ ที่เหมาะสมที่สุดและปลอดภัยต่อการบุกรุกที่ระบบตรวจจับการบุกรุกตรวจพบในข้างต้น

3. ภาคเอาท์พุต จะเป็นการนำเอา Rules Base ของไฟร์วอลล์ ที่ได้มากจากการวิเคราะห์ ไปติดตั้งใช้กับระบบไฟร์วอลล์ที่มีอยู่ โดยการทำงานเป็นแบบ Batch



รูปที่ 3.1 Process Diagram

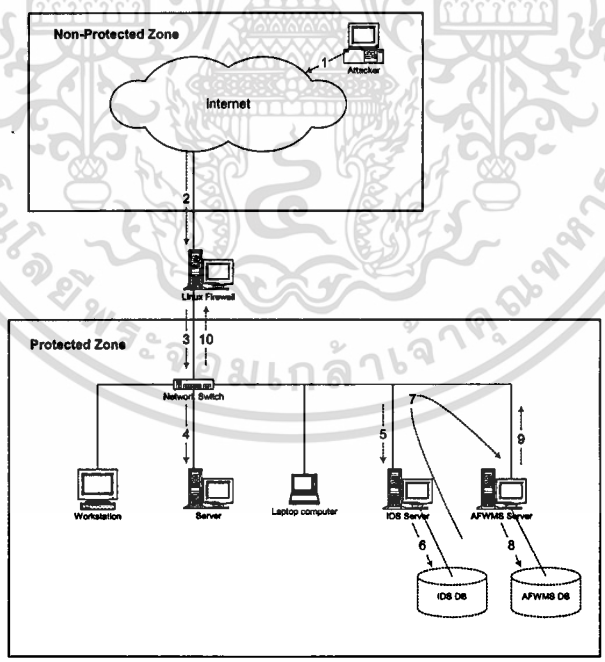


รูปที่ 3.2 Network Diagram

การทำงานของระบบสามารถทำงานได้กับระบบ Network ที่มีการออกแบบตามรูปที่ 3.2 เพื่อความง่ายในการทดสอบการทำงานของระบบ จึงใช้ระบบที่มีความซับซ้อนของระบบไม่มาก และวัตถุประสงค์ในการทำงานของระบบไฟร์วอลล์ก็เพื่อวัตถุประสงค์ในการป้องกันเครือข่ายคอมพิวเตอร์ภายในที่ต้องการป้องกัน (Protected Zone) จากการบุกรุกของผู้บุกรุกที่มาจาก Network ภายนอกซึ่งเราไม่ เชื่อถือซึ่งเรามองว่าเป็นส่วนที่ไม่ได้รับการป้องกัน (Non-Protected Zone)

การออกแบบ Rules Base ของไฟร์วอลล์เป็นเรื่องที่สลับซับซ้อน หากกำหนดเงื่อนไขได้ไม่ดี ก็อาจจะทำให้ระบบทำงานช้า แต่หากมีการออกแบบที่หละหลวมจนเกินไป ก็อาจทำให้การรักษาความปลอดภัยทำได้ไม่ดีเท่าที่ควร

แนวทางการออกแบบจึงเน้นไปในการกำหนดการทำงานของไฟร์วอลล์ ที่ทำงานในแบบ Packets filtering เพื่อให้การกำหนดเงื่อนไขไม่ซับซ้อนมากนักและให้ความปลอดภัยกับระบบได้ โดยการปฏิเสธการขอใช้งาน หากมีการตรวจจับจากระบบตรวจจับการบุกรุกได้ว่าเครื่องคอมพิวเตอร์ที่เข้ามาขอใช้บริการระบบมีความพยายามในการบุกรุก ซึ่งเงื่อนไขของการปฏิเสธที่จะไม่ให้บริการแก่เครื่องคอมพิวเตอร์เครื่องใด และระดับของการปฏิเสธเป็นอย่างใดนั้น จะอาศัยความสามารถของระบบเป็นตัวระบุ



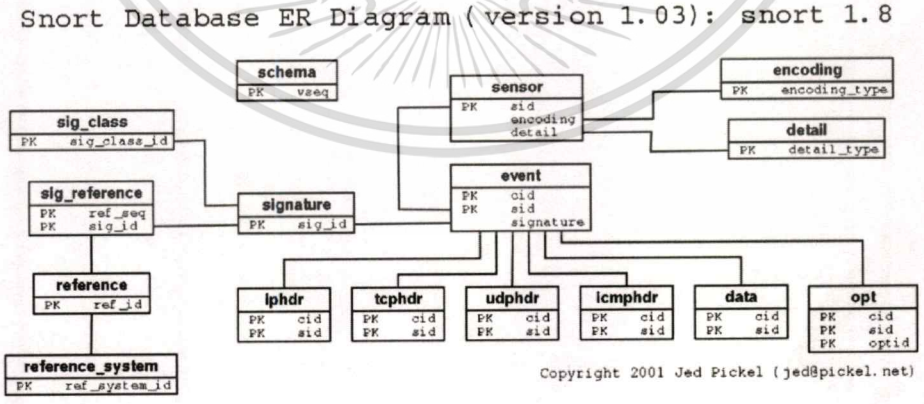
รูปที่ 3.3 ลำดับขั้นการทำงาน

จากรูปที่ 3.3 (ลำดับที่ 1-4) เมื่อ Attacker ส่ง Packets เข้ามาจาก Network ภายนอก โดยเป็น Packets ที่มีวัตถุประสงค์ไม่ดีต่อระบบคอมพิวเตอร์ที่เราต้องการป้องกัน Packets จะถูกส่งผ่าน ไฟร์วอลล์ เข้ามายังอุปกรณ์เชื่อมต่อภายใน ในที่นี้คือ Network Switch และ Packets จะถูก Broadcast เพื่อให้เครื่องปลายทางได้รับตามมาตรฐานของ Ethernet เครื่องคอมพิวเตอร์ปลายทางจะรับเอา Packets ที่ถูกส่งมาทำการประมวลผล

จากรูปที่ 3.3 (ลำดับที่ 4-6) ในขณะเดียวกัน IDS ที่ทำงานอยู่ในลักษณะ Passive Mode ซึ่งจะคอยรับทุก Packets ที่ถูกส่งผ่านอุปกรณ์ Network Switch ข้างต้นมาวิเคราะห์ และเมื่อ IDS ได้รับ Packets ต้องสงสัยที่มี Pattern ตรงกับเงื่อนไขที่อยู่บน Rules Base ของตัว IDS เองแล้ว IDS ก็จะทำการแจ้งเตือนอยู่ ซึ่งรูปแบบของการแจ้งเตือนจะถูกจัดเก็บให้อยู่ในรูปของข้อมูล ที่ถูกเก็บไว้ในระบบฐานข้อมูล RDBMS

จากรูปที่ 3.3 (ลำดับที่ 6-10) Automatic Firewall Management System จะอ่านข้อมูลจากระบบฐานข้อมูลที่ถูกจัดเก็บโดย IDS มาประมวลผลทุกๆ 5 นาที โดย Automatic Firewall Management System จะเอา Records ที่เกิดขึ้นในช่วงเวลา 5 นาทีสุดท้ายมาผ่านระบบผู้เชี่ยวชาญเพื่อวิเคราะห์หา Rules Base ที่เหมาะสมให้แก่ Firewall จากนั้นระบบจะเก็บข้อมูล Rules Base ของ Firewall ลงสู่ระบบฐานข้อมูลของตน และ Automatic Firewall Management System จะทำการนำข้อมูล Rules Base ที่มีอยู่ในฐานข้อมูลทั้งหมดไปติดตั้งให้กับ Firewall ในกรณีที่มีข้อมูลเปลี่ยนแปลงไปจากเดิม

จากการศึกษา Database Schema ของ Snort เห็นว่ามี Table ที่เกี่ยวข้องและสามารถนำมาใช้เป็นข้อมูลในภาคอินพุตของ AFWMS ได้ โดยมีการเลือกข้อมูลมาจากการศึกษาจาก Schema ดังนี้



รูปที่ 3.4 Snort Database ER Diagram

3.3 การออกแบบโครงสร้างของโปรแกรม

แบ่งการทำงานของโปรแกรมเป็นสองส่วนดังนี้

3.3.1 AFWMS MASTER SERVER

มีการทำงานคือเป็นส่วนที่ติดต่อกับฐานข้อมูล Snort เพื่อดึงข้อมูลมาทำการวิเคราะห์ และสร้างแฟ้มข้อมูลที่จะนำไปเป็น Rules base ของ Firewall ต่อไป

3.3.2 AFWMS REMOTE SERVER

มีการทำงานคือเป็นส่วนที่นำไปติดตั้งไว้ยัง Firewall Server เพื่อให้ Firewall สามารถ Update ข้อมูลของ Rules base ที่เปลี่ยนแปลงจากการวิเคราะห์ข้อมูลของการบุกรุกที่ได้จากการตรวจจับของ Snort

3.4 การออกแบบโครงสร้าง Directory ของ Program

การออกแบบจะจัดวาง Directory ของ AFWMS ไปที่ root directory ของระบบ เพื่อให้ง่ายต่อการอ้างอิงถึงโปรแกรมทำได้สะดวก และมีการแยก Directory ออกเป็นสาม Directory หลักๆ ดังนี้

/AFWMS-CONFIG คือ ส่วนที่ใช้เก็บข้อมูล และ Configuration ที่จำเป็นของโปรแกรม

/AFWMS-MS คือ ส่วนที่ใช้เก็บโปรแกรมที่ทำงานเป็น Master Server

/AFWMS-RS คือ ส่วนที่ใช้เก็บโปรแกรมที่ทำงานเป็น Remote Server

นอกจาก Directory หลักทั้งสามที่กล่าวมาข้างต้นแล้ว ยังมี Directory ที่มีความเกี่ยวข้องต่อการทำงานของโปรแกรมอีกดังนี้

/etc/sysconfig คือ Directory ที่เก็บแฟ้ม ipchains ที่จะถูก update ให้กับตัว Firewall เพื่อนำ Configuration ดังกล่าวไปใช้งาน

/etc/rc.d/init.d คือ Directory ที่จะเก็บแฟ้ม ipchains ที่งานเป็น script ในการ restart ตัวไฟร์วอลล์

/var/www/html/ms คือ Directory ที่ตัว Master Server ใช้เก็บแฟ้มข้อมูล ที่เกี่ยวข้องในขั้นตอนการ Update ตัว Rules base ของไฟร์วอลล์ ผ่าน HTTPD

3.5 การออกแบบโปรแกรมเพื่อตรวจสอบการทำงานของ Remote Server

โปรแกรมในส่วนนี้จะคอยทำหน้าที่เพื่อตรวจสอบว่า Server ที่มี Remote Server ที่ติดตั้งไว้กับไฟร์วอลล์ เพื่อทำการ Update ตัว Rules base จากส่วนที่เป็น Master Server นั้นทำงานอยู่หรือเปล่าโดย โปรแกรมจะอ่านข้อมูลที่ถูกเก็บไว้ใน Server Configuration File ว่ามีเครื่องใดบ้างที่ถูกลงทะเบียนไว้กับระบบ

การทดสอบไฟร์วอลล์ จะใช้สมมติฐานที่ว่าไฟร์วอลล์ที่ติดตั้ง Rules base ที่สร้างจาก Master Server จะอนุญาตให้เครื่อง Master Server ติดต่อเข้าไปยังตัวไฟร์วอลล์โดยไม่มีการ Block ดังนั้น เครื่อง Master Server จะคอยตรวจสอบการทำงานด้วยการใช้คำสั่ง ping เพื่อตรวจสอบการตอบสนองการทำงานของไฟร์วอลล์ หากมีการตรวจพบว่ามีไฟร์วอลล์ที่ไม่ตอบสนองคำสั่ง Ping ในเวลาที่กำหนด ระบบจะบันทึกเป็น Error Message ไว้ใน Log file

3.6 การออกแบบในเรื่องเกี่ยวกับ Rules base เพื่อ Minimize ตัว Rules base

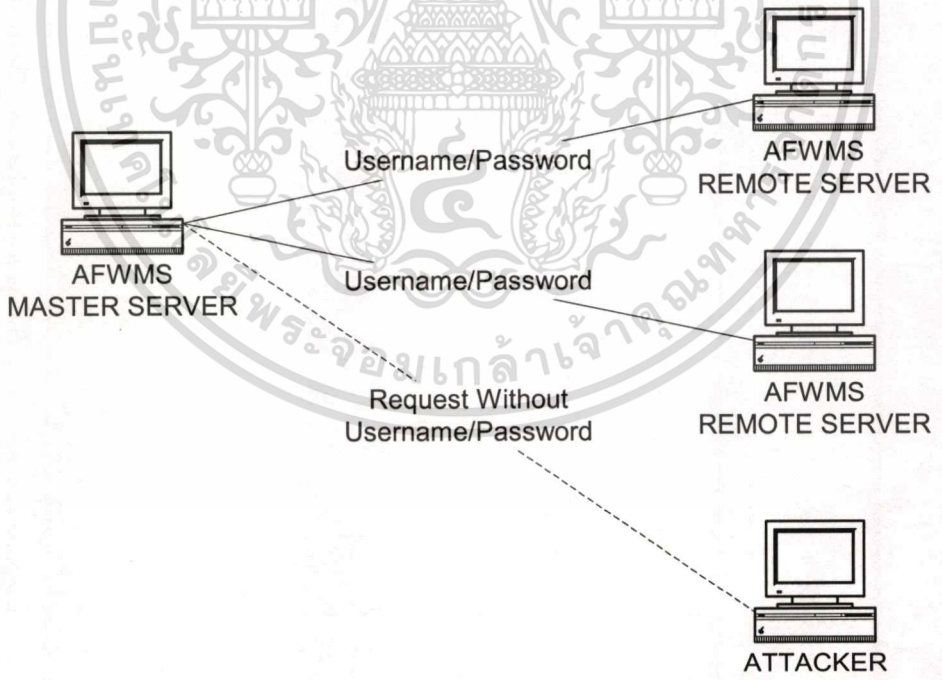
เนื่องจากการที่ระบบมีโอกาสที่จะเกิดการบุกรุกเข้ามามากๆ และอาจส่งผลให้ขนาดของข้อมูลของการบุกรุกเพิ่มเข้ามามากๆ Rules base ของตัวไฟร์วอลล์ ก็อาจจะมีจำนวนมากขึ้นด้วย และเมื่อ Rules base ของตัวไฟร์วอลล์มีจำนวนมากขึ้น ก็จะส่งผลให้การทำงานของไฟร์วอลล์ช้าลงได้

แนวความคิดเพื่อให้การทำงานเป็นไปได้ดีนั้นก็คือจะต้องมีการ Minimize ตัว Rules base แต่เนื่องจากการที่จะทำให้ Rules base ของไฟร์วอลล์ มีขนาดเล็กเป็นเรื่องที่เรายังไม่ได้ให้ความสำคัญมาก แต่อย่างไรก็ดีจะต้องมีวิธีการที่จะทำให้ระบบสามารถทำงานได้ และ ยังสามารถป้องกันการบุกรุกที่อาจก่อให้เกิดความเสียหายให้กับระบบที่ต้องการป้องกัน ดังนั้นจึงเกิดแนวคิดที่จะจำกัด Rules base ของไฟร์วอลล์ โดยการเลือกข้อมูลที่อยู่ในฐานข้อมูลของระบบ Automatic Firewall Management System มาบางส่วนเพื่อที่จะนำมาสร้างเป็น Rules base ของไฟร์วอลล์ ต่อไป โดยมีเงื่อนไขอยู่ว่าข้อมูลที่เลือกมานั้นจะเป็นข้อมูลล่าสุดที่ถูกสร้างขึ้น แต่ไม่เกินจำนวนไม่เกิน 100 Records ด้วยเหตุผลที่กล่าวมาข้างต้น

3.7 การออกแบบระบบรักษาความปลอดภัยภายใน AFWMS

ไฟร์วอลล์เป็นอุปกรณ์ที่มีความสำคัญต่อการใช้งานระบบคอมพิวเตอร์เครือข่าย เพราะนอกจากจะช่วยป้องกันการบุกรุกจากภายนอกแล้วไฟร์วอลล์ยังสามารถทำให้ผู้ใช้งาน ไม่สามารถติดต่อกับระบบอื่นๆได้ด้วย ดังนั้นหากผู้บุกรุกสามารถเข้าถึงระบบ AFWMS ก็อาจจะมีการเปลี่ยนแปลงแก้ไข Rules base ของตัวไฟร์วอลล์ได้ แนวคิดของระบบคือจะต้องมีการตรวจสอบการทำงานระหว่าง Master Server และ Remote Server โดยก่อนการปรับปรุงแก้ไขตัว Rules base ของไฟร์วอลล์ จะต้องมีการยืนยันโดยใช้ Username และ Password เพื่อเข้าสู่การบวนการส่งถ่ายข้อมูล ทั้งนี้เพื่อที่จะป้องการ Update ข้อมูลจากเครื่องที่ไม่ได้รับอนุญาติเพื่อนำข้อมูลที่ติดตั้งในตัวไฟร์วอลล์ ไปวิเคราห์ได้

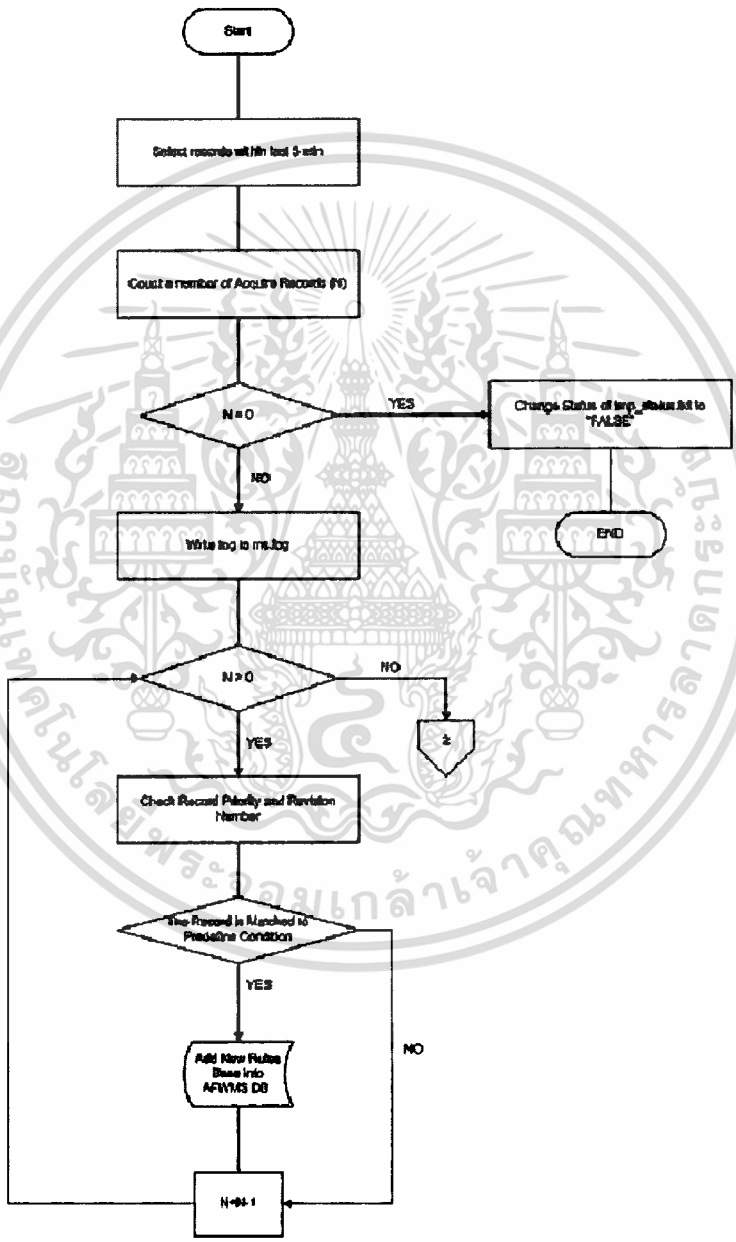
นอกเหนือจากที่มีการกำหนด Username และ Password เพื่อเข้ามาขอ Rules base แล้วนั้นเรายังสามารถที่จะเพิ่มความปลอดภัย ได้อีกทางโดยใช้ ipchains เป็นตัวกำหนดว่าเครื่องใดสามารถที่จะเข้ามาติดต่อยัง Automatic Firewall Management System ได้บ้าง



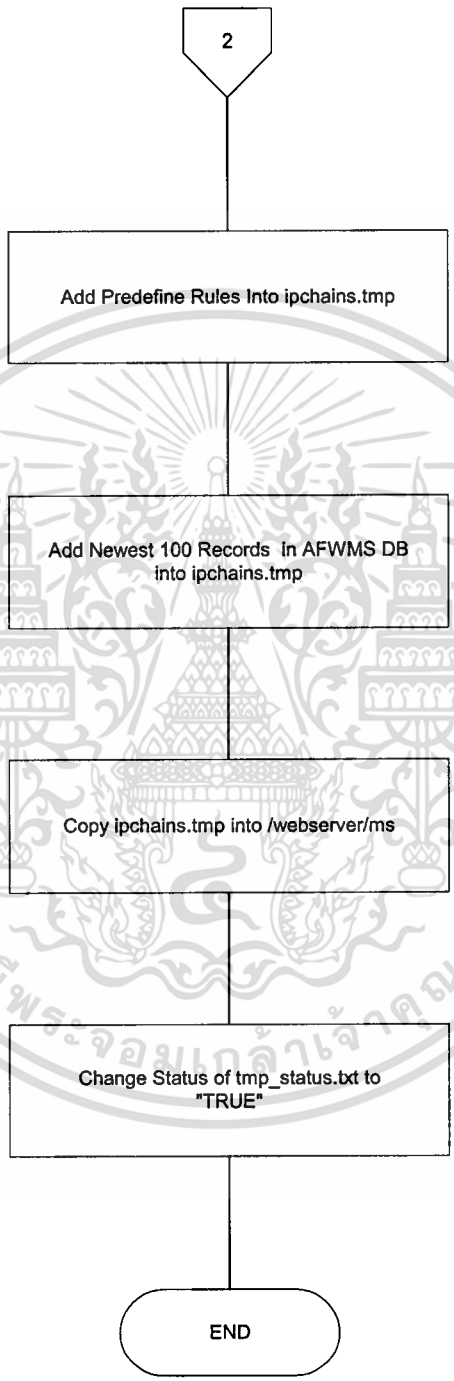
รูปที่ 3.5 แสดงการติดต่อจาก Client เข้ามายัง Server

3.8 การออกแบบลำดับขั้นการทำงานของโปรแกรม

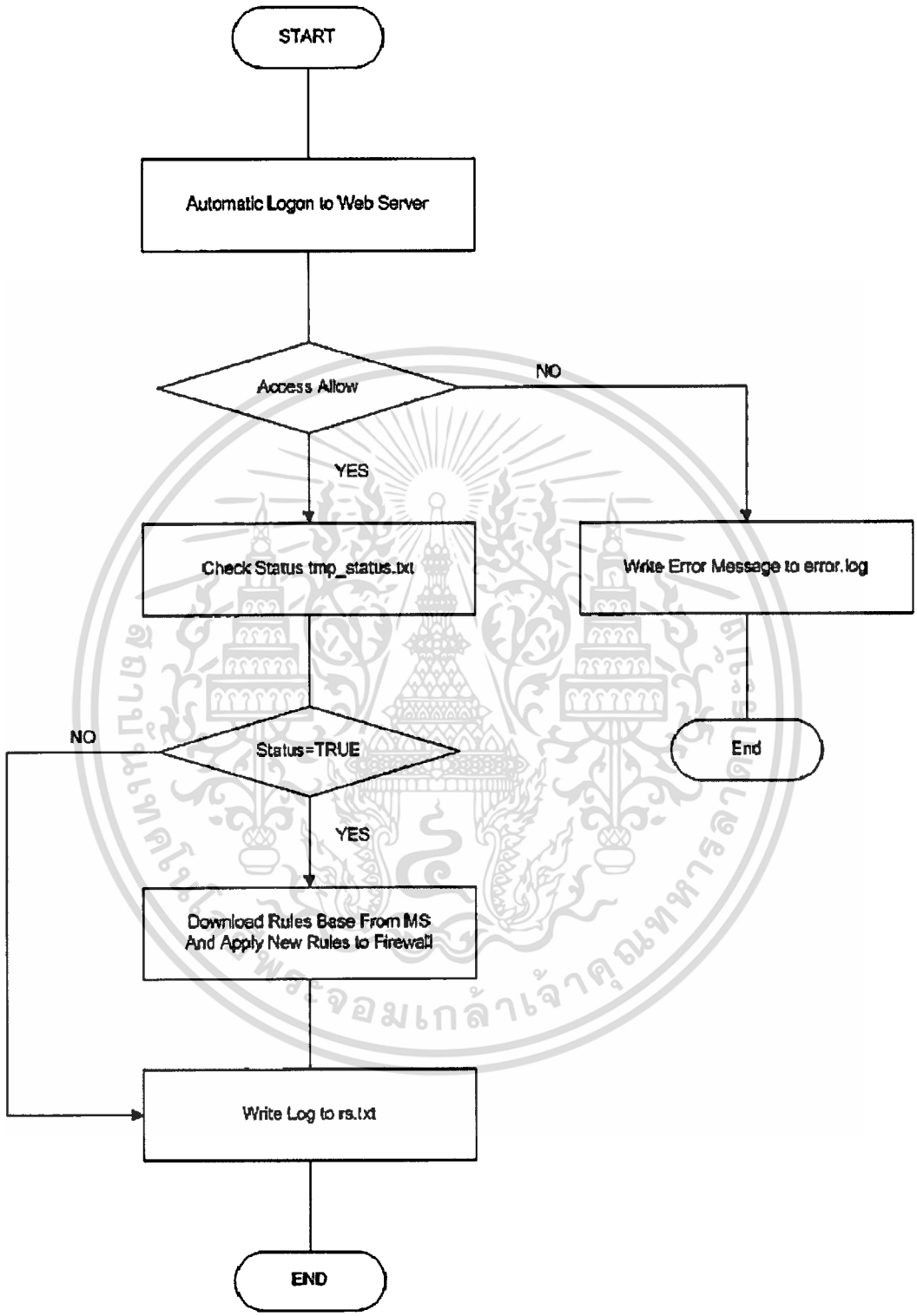
การออกแบบการทำงานของโปรแกรม ทำโดยนำเงื่อนไขที่อยู่ในขอบเขตของระบบมาวิเคราะห์ เพื่อหาแนวทางที่เหมาะสมในการที่จะนำไปสร้างโปรแกรมต่อ โดยมีรายละเอียดของการออกแบบดังแสดงดังในรูป



รูปที่ 3.6 ลำดับขั้นการทำงานของโปรแกรม MS (1)



รูปที่ 3.7 ลำดับขั้นการทำงานของโปรแกรม MS (2)



รูปที่ 3.8 ลำดับขั้นการทำงานของโปรแกรม RS

บทที่ 4
การพัฒนาระบบ

4.1 ขั้นตอนการพัฒนา

เมื่อได้ดำเนินการออกแบบโครงสร้างระบบโครงสร้างและลำดับการทำงานของโปรแกรมในการใช้งานในบทที่ 3 เสร็จเรียบร้อยแล้วในขั้นตอนต่อไปจะเป็นการสร้างระบบนี้ ซึ่งจะใช้ Linux ที่เป็นระบบปฏิบัติการ และใช้ MySQL เป็นโปรแกรมฐานข้อมูลจำลองของ Snort ที่ติดตั้งบนเครื่องแม่ข่ายไว้เรียบร้อยแล้วมาเป็นเครื่องมือในการพัฒนาต่อไป สาเหตุที่ใช้ MySQL มาใช้งานเนื่องจาก Snort จะเก็บข้อมูลของการบุกรุกไว้ในฐานข้อมูลดังกล่าว และ MySQL เป็นฟรีแวร์ที่สนับสนุนการใช้งานในคำสั่ง SQL ได้ทั้งหมด

การดำเนินงานเริ่มต้นจากการติดตั้งระบบปฏิบัติการ Linux และ สร้างฐานข้อมูลสำหรับเก็บข้อมูลของ Snort จากนั้นจึงสร้างตารางต่างๆ ขึ้นบนฐานข้อมูลดังกล่าว ซึ่งสามารถทำได้ทำได้โดยใช้ SQL สคิปต์ที่มากับโปรแกรม Snort เป็นตัวสร้าง Schema ของฐานข้อมูล เมื่อดำเนินการสร้างฐานข้อมูลเป็นที่เรียบร้อยแล้ว ก็จะเป็นขั้นตอนการติดตั้งซอร์ฟแวร์ที่เกี่ยวข้องต่างๆ เริ่มจากติดตั้ง PHP4 ลงบนเครื่องเซิร์ฟเวอร์ ซึ่งจะใช้เป็น Shell Script ที่ใช้ในการพัฒนาระบบงานนี้ต่อไป

เมื่อติดตั้งโปรแกรมต่างๆ เรียบร้อยแล้ว ก็ดำเนินการออกแบบ Environment, File Permission, Network Configuration, เพื่อรองรับการใช้งาน และทำการพัฒนาโปรแกรมให้สามารถใช้งานได้ตรงตามความต้องการโดยการเขียนโปรแกรม PHP4 เพื่อเป็นการพัฒนาการทำงานของระบบไฟร์วอลล์อัตโนมัติ

4.2 การติดตั้งระบบปฏิบัติการ Linux

<u>ความต้องการด้านฮาร์ดแวร์</u>

1. ซีพียูตั้งแต่รุ่น 80486 ขึ้นไป ที่เป็นของ Intel หรือ Intel Compatible เช่น AMD เป็นต้น
2. หน่วยความจำ (RAM) ขนาด 64 MB ขึ้นไป (Install แบบ Graphic mode)
3. ฮาร์ดดิสก์ขนาด 4 GB ขึ้นไป
4. การ์ดแสดงผลและมอนิเตอร์แบบVGA หรือ Super VGA
5. ซีดีรอมไดร์ฟ
6. Network Interface Card

Partition ของ Hard disk

Partition table คือ ส่วนที่เก็บรายละเอียดเกี่ยวกับโครงสร้าง Partition ของ Hard disk และเก็บอยู่ในส่วนหนึ่งของ boot sector หรือ master boot record ซึ่งก็คือ logical sector 0 ของ Hard disk โดยที่จะถูกจำกัดให้มีเพียง 4 Primary Partition บนเครื่องตระกูล PC แต่ถ้าเป็นเครื่องที่เป็น minicomputer ที่ run UNIX จะมีวิธีจัดการ Partition table ที่แตกต่างจากเครื่องตระกูล PC

Partition ก็คือพื้นที่ ต่อเนื่องใน Hard disk ที่ถูกกำหนดตำแหน่งเอาไว้ว่า เริ่มต้นที่ใด และสิ้นสุดที่ใดโดยแต่ละ Partition จะอยู่แยกกันอิสระไม่มีการทับซ้อนกัน และสามารถจะลง OS หรือ File System คนละชนิดกันได้ ใน Hard disk ตัวเดียวกัน

ประโยชน์ของการแบ่ง Partition มีอยู่หลายประการ เช่น

- ลง OS หลายตัวใน Hard disk ตัวเดียวกัน
- ต้องการแบ่งพื้นที่ของ Hard disk เพื่อใช้ File System คนละชนิดกัน เช่น ทำเป็น SWAP Partition, หรือทำเป็น FAT 16 เพื่อเป็นตัวกลางในการส่งผ่าน ข้อมูลระหว่าง NT กับ Linux
- ต้องการจำกัดพื้นที่ของการใช้งาน เช่นพื้นที่ของ User อาจจะแยกเป็น อีก Partition หนึ่ง เพื่อป้องกันการใช้พื้นที่ของ Hard disk แบบมากมายผิดปกติ
- ต้องการแยกส่วนระหว่าง OS กับ data ออกจากกัน เอาไว้เวลาเราทำการติด ตั้ง OS ที่มี Version ใหม่กว่า เราก็สามารถจะ Clear พื้นที่ disk เฉพาะในส่วน ที่เป็นของ System ได้ โดยไม่มีผลกระทบกับ data ที่อยู่อีก Partition

การอ้างอิงอุปกรณ์ของ Linux

Linux มีวิธีการอ้างอิงถึงอุปกรณ์ต่าง ๆ เป็นแฟ้มข้อมูลโดยมีอักษรนำหน้าและตามด้วยตัวเลข เช่น /dev/ttyS0, /dev/ttyS1, /dev/psaux เหล่านี้เป็นการอ้างถึง COM1, COM2 และ PS2 ตามลำดับ

/dev/fd0, /dev/df1 อ้างอิงถึง diskette drive ตัวที่ 1 และ 2 หรือ A: หรือ B:

/dev/hda, /dev/hdb อ้างอิงถึง Hard disk Primary EIDE/IDE ตัวที่ 1 และ 2

/dev/hdc, /dev/hdd อ้างอิงถึง Hard disk Secondary EIDE/IDE ตัวที่ 1 และ 2

การอ้างอิง Partition ของ Linux

โดยจะเติมตัวเลขต่อท้ายชื่ออุปกรณ์ (1 – 4 แทน Primary/Extended Partition และ 5 แทน Logical Partition) เช่น /dev/hda1, /dev/hda2, /dev/hda5 อ้างถึง Primary Partition ที่ 1, Extended

Partition และ Logical Partition ของ Primary EIDE/IDE Hard disk ตัวที่ 1 เป็นต้น

การเตรียมแผ่น Boot

การเตรียมแผ่น Boot สามารถดำเนินการได้หลายวิธี แต่จะแนะนำวิธีการติดตั้งเพียง 2 วิธี คือ การเตรียมแผ่น Boot จาก CD-ROM และ จากแผ่น Diskette

- การเตรียมแผ่น Boot จาก CD-ROM

สำหรับโปรแกรม Red Hat 7.3 จะบรรจุอยู่ใน CD-ROM จำนวน 3 แผ่น โดยแผ่นแรกได้บรรจุโปรแกรมสำหรับการ Boot ด้วยตัวเองอยู่แล้ว เพียงแต่ผู้ใช้ จะต้องกำหนดให้เครื่อง คอมพิวเตอร์ที่จะใช้ในการติดตั้ง ทำการ Boot จาก CD-ROM Drive เท่านั้น โดยทำการแก้ไข BIOS ขณะเปิดเครื่องคอมพิวเตอร์ ในส่วนของ Boot Sequence ในหมวด BIOS FEATURES SETUP ซึ่งวิธีนี้เหมาะกับเครื่องคอมพิวเตอร์รุ่นใหม่ ๆ หรือเครื่องที่สามารถหนด BIOS ให้ Boot จาก CD ROM ได้

- การเตรียมแผ่น Boot จากแผ่น Diskette

Boot เครื่องคอมพิวเตอร์ด้วยแผ่น Dos หรือ Windows ให้เห็น Drive A: และ CD ROM Drive สมมุติว่าระบบ มองเห็น CD ROM เป็น d: ให้ใช้คำสั่งต่อไปนี้

d:\dosutils\rawrite.exe

โปรแกรมจะถามตำแหน่งที่จัดเก็บ Image File ที่ต้องการ ให้ระบุเป็น

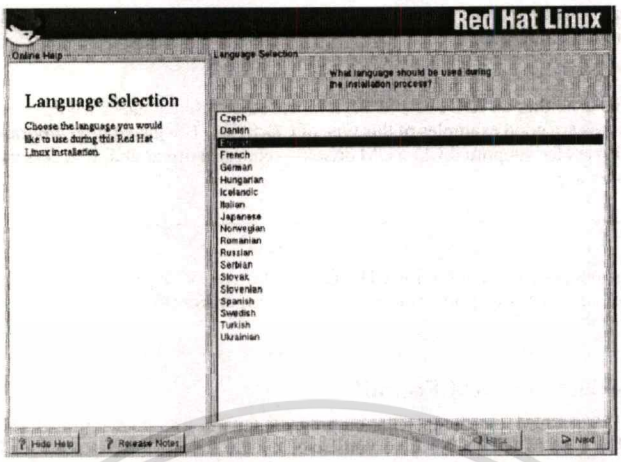
d:\images\boot.img

โปรแกรมจะถาม Drive ที่ต้องการให้โปรแกรมทำการสร้างแผ่นบูต ให้ระบุเป็น ไดรฟ์ A: จากนั้นโปรแกรมจะคัดลอก Image File เพื่อทำการสร้างแผ่น Boot จนเสร็จ

ขั้นตอนการติดตั้ง Linux

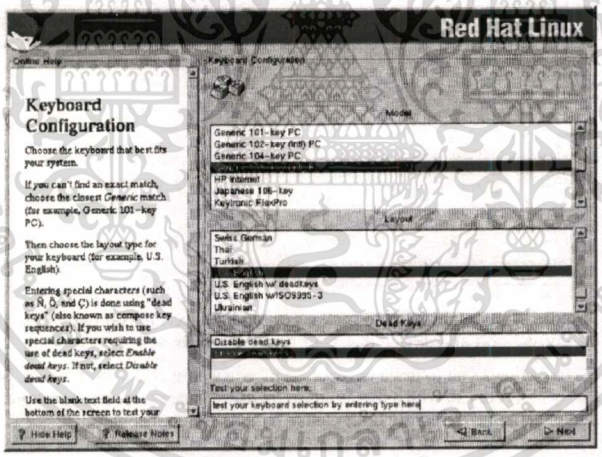
เริ่มติดตั้งโปรแกรมโดย Boot เครื่องคอมพิวเตอร์ด้วยแผ่น CD-ROM หรือ แผ่น Boot ที่ได้จัดเตรียมไว้ พร้อมทั้งใส่แผ่น Red Hat 7.3 แผ่นที่ 1 ไว้ใน Drive CD-ROM ด้วย จะปรากฏหน้าจอ

หน้าจอ Welcome to Red Hat Linux 7.3 และปรากฏ Prompt ที่ชื่อ “boot :” ให้ กดปุ่ม <Enter> เพื่อเลือกการติดตั้ง แบบ Graphic Mode หรือ พิมพ์คำว่า “text” และกดปุ่ม <Enter> เพื่อเลือกการติดตั้งในลักษณะ Text Mode ในที่นี้ให้เลือกกดปุ่ม <Enter> เพื่อเลือกการติดตั้ง แบบ Graphic Mode โปรแกรมจะทำการ Load File System ต่างๆ เข้าสู่ระบบ พร้อมทั้งตรวจเช็ค Hardware ของระบบด้วย หลังจากนั้นจะเข้าสู่หน้าจอเริ่มต้นการติดตั้งอื่น ๆ ต่อไป



รูปที่ 4.1 หน้าจอ Language Selection เลือกภาษาที่ใช้ในขณะติดตั้ง

เลือกภาษาที่ใช้เป็น English แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ



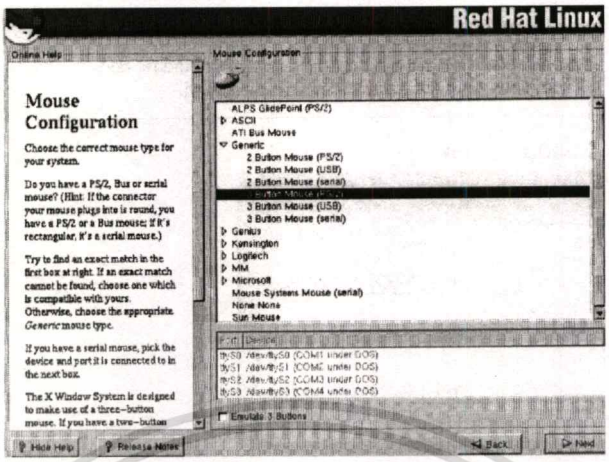
รูปที่ 4.2 หน้าจอ Keyboard Selection

เลือก Model แบบ Generic 101-key PC

เลือก Layout แบบ US English

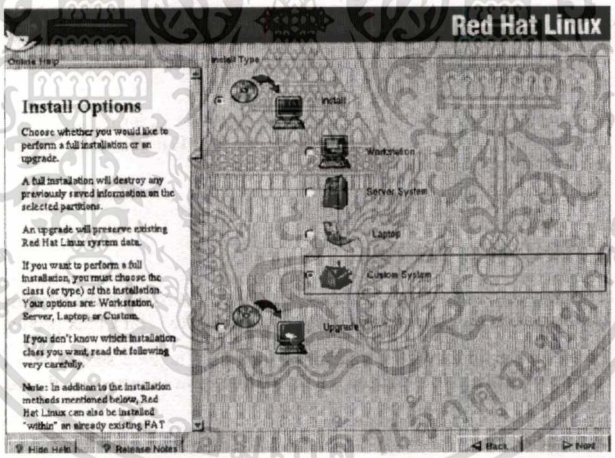
เลือก Dead Keys แบบ Disable Dead Keys (ในกรณีที่ Keyboard ไม่มี อักขระพิเศษ)

แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ



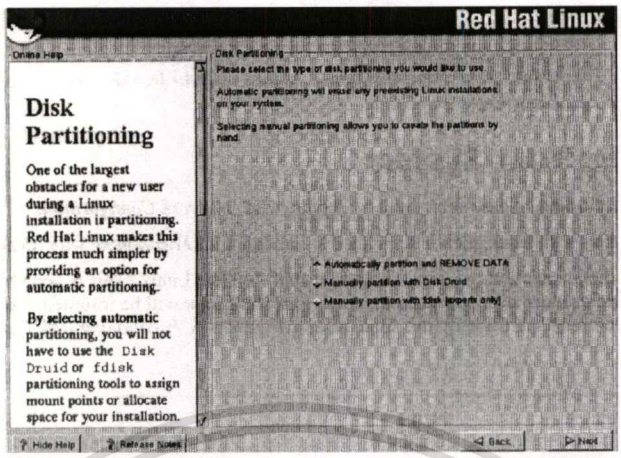
รูปที่ 4.3 หน้าจอ Mouse Configuration เลือกชนิดของ Mouse ที่เหมาะสม

เลือก Generic2 Button Mouse (PS/2) แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ



รูปที่ 4.4 หน้าจอ Install Options

เลือกติดตั้งโปรแกรมหรือPackageให้เหมาะกับความต้องการใช้งาน มีหลายชนิด เช่น Workstation, Server System, Laptop, Custom System หรือ Upgrade เลือก Custom system เพื่อเลือก Package ที่จะติดตั้งตามต้องการ แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ



รูปที่ 4.5 หน้าจอ Disk Partitioning

เลือกวิธีการจัดแบ่งพื้นที่ใน Hard Disk มี 3 วิธี คือ

- Automatically Partition and Remove Data แบ่งเนื้อที่แบบอัตโนมัติ
- Manually Partition with Disk Druid มีการแบ่งเนื้อที่ใน Hard disk แล้ว
- Manually Partition with fdisk (Expert Only) แบ่งเนื้อที่ตามต้องการ

เลือก Manually Partition with fdisk (Expert Only) แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อจะพบหน้าจอ using fdisk เลือก Hard disk ที่ต้องการสร้างหรือแก้ไข Partition

เลือก hda หมายถึง Primary Hard Disk จะเข้าสู่โหมด Command Line เพื่อเริ่มต้นสร้างหรือแก้ไข Partition โดยมีคำสั่งที่ต้องใช้ดังนี้

m	แสดงรายละเอียดของคำสั่งทั้งหมด
p	แสดงรายละเอียดของ Partition ที่จัดแบ่งแล้ว
n	สร้าง Partition ใหม่ e = extended, p = primary partition
d	ลบ Partition
t	เปลี่ยนหมายเลขเพื่อกำหนดชนิดของ Partition
w	บันทึกการเปลี่ยนแปลง Partition ทั้งหมด และออกจาก Command Mode
q	ออกจากโหมด Command Line โดยไม่บันทึก

โดยปกติ การสร้าง Partition ใน Hard disk ควรมีอย่างน้อย 2 Partition ได้แก่ Partition ชนิด Linux Native สำหรับติดตั้งโปรแกรม และชนิด Linux Swap สำหรับใช้เป็นหน่วยความจำเสมือน (โดยปกติจะมีขนาดเป็น 2 เท่าของ Main Memory (RAM))

<u>การสร้าง Partition ที่ทำหน้าที่หน่วยความจำเสมือน (Linux Swap)</u>

- กด n เพื่อเข้าสู่กระบวนการสร้าง Partition ใหม่
- กด p เพื่อสร้าง Primary Partition (มีได้ไม่เกิน 4 Partition)
- กด 2 เพื่อสร้าง Primary Partition ลำดับที่ 2
- กด 1 เพื่อบอกตำแหน่งพื้นที่เริ่มต้นที่ใช้ใน Hard disk (First Cylinder)
- กด +128M เพื่อบอกขนาดพื้นที่หน่วยความจำเสมือน (ปกติใช้พื้นที่ขนาด 2 เท่าของหน่วยความจำ ตัวเลข 128 คือ RAM 64 MB x 2)
- กด t เพื่อเข้าสู่กระบวนการเปลี่ยนสถานะของ Partition
- กด 2 เพื่อระบุ Partition ลำดับที่ 2 ที่จะเปลี่ยนสถานะ
- กด 82 เพื่อเปลี่ยนสถานะ Partition เป็นหน่วยความจำเสมือน (Linux Swap)

<u>การสร้าง Partition สำหรับติดตั้งระบบปฏิบัติการ Linux</u>

- กด n เพื่อเข้าสู่กระบวนการสร้าง Partition ใหม่
- กด p เพื่อสร้าง Primary Partition (มีได้ไม่เกิน 4 Partition)
- กด 1 เพื่อสร้าง Primary Partition ลำดับที่ 1
- กดตัวเลข เช่น 67 เพื่อบอกตำแหน่งพื้นที่เริ่มต้นที่ใช้ใน Hard disk สังเกตจากตัวเลขหลังข้อความ First Cylinder (67-621)
- กดตัวเลข เช่น 621 เพื่อบอกตำแหน่งสุดท้ายของพื้นที่ใน Hard Disk สังเกตจากตัวหลังข้อความ Last Cylinder (67-621)

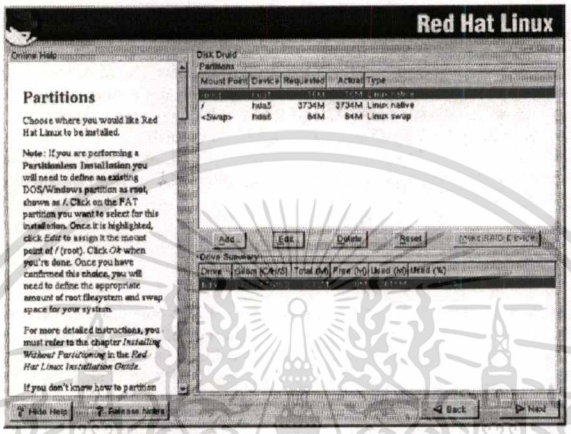
<u>การกำหนด Boot Partition ให้กับระบบ</u>

- กด a เพื่อกำหนดเป็น Boot Partition (toggle a bootable flag) พร้อมทั้ง กดตัวเลขลำดับที่ Partition ในตัวอย่างนี้คือ 1

ที่ Command mode กด p เพื่อแสดงรายชื่อ Partition ใน Column Boot จะมีเครื่องหมาย "*" แสดงอยู่

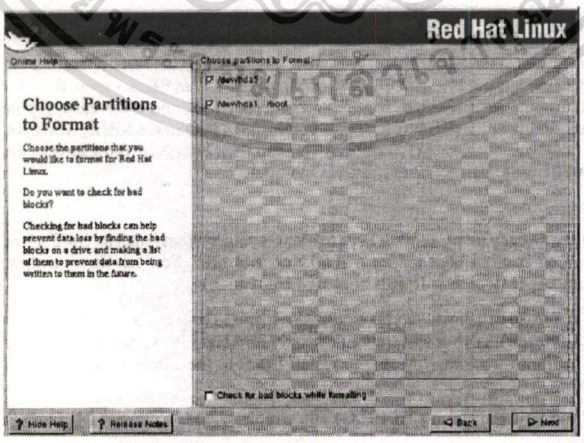
การสร้างบันทึกและออกจาก Command mode

- กด w เพื่อบันทึกการสร้าง Partition และออกจาก Command mode หรือ กด ออกจาก Command mode โดยไม่บันทึก หลังจากทำการสร้าง Partitions เสร็จเลือกปุ่ม NEXT เพื่อทำงานต่อ



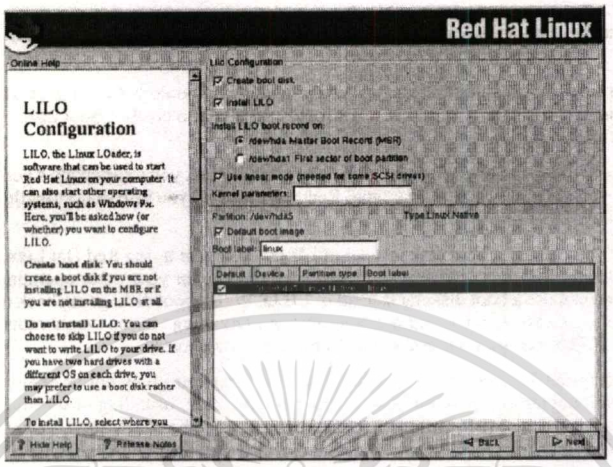
รูปที่ 4.6 หน้าจอ Partitions ให้เลือก Partition สำหรับ Install Red Hat Linux

กำหนด Mount Point โดยเลือก Partition ที่เป็นชนิด Linux Native ให้ทำแถบสีน้ำเงิน และกดปุ่ม Edit และใส่เครื่องหมาย / (หมายถึงให้ Partition นี้ทำหน้าที่เป็น root directory) ในช่อง Mount Point กดปุ่ม OK และเลือกปุ่ม NEXT เพื่อทำงานต่อ



รูปที่ 4.7 หน้าจอ Choose Partitions to Format เลือก Partition ที่ต้องการจะ format

เลือก Partition ที่ต้องการ Formant แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ



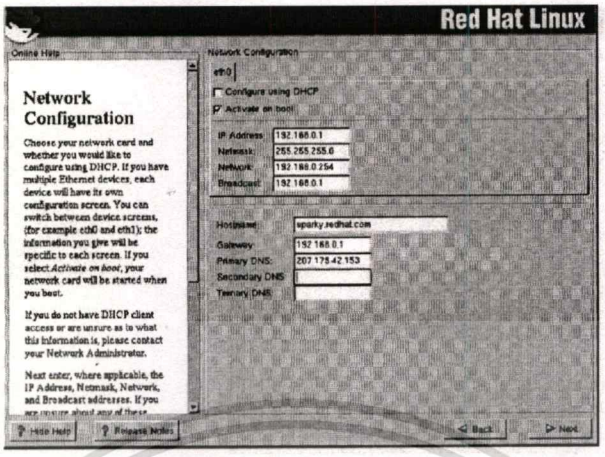
รูปที่ 4.8 หน้าจอ LILO Configuration

หน้าจอ LILO Configuration เป็นการเลือกติดตั้งโปรแกรม Linux Loader เพื่อจัด การกับระบบ boot ของเครื่องคอมพิวเตอร์ ในกรณีที่มีการลงระบบปฏิบัติการหลายตัวหรือตัวเดียวในเครื่องเดียวกันให้สามารถเลือกใช้ได้ตามต้องการ มีหัวข้อให้เลือกดังนี้

- Create boot Disk สำหรับสร้างแผ่น Boot เพื่อใช้ในยามฉุกเฉิน หรือไม่สามารถ boot จาก hard disk ได้
- Install LILO ใน Master Boot Record สามารถเลือก OS ได้มากกว่า 1 ระบบ

  -Install LILO ใน First Sector of Boot Partition ถ้าต้องการใช้ Boot Loader อื่น แทน LILO
- Use Linear Mode สำหรับ Hard Disk แบบ SCSI
- Default Boot Image สำหรับระบุ OS แรกที่ boot เครื่อง

แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ

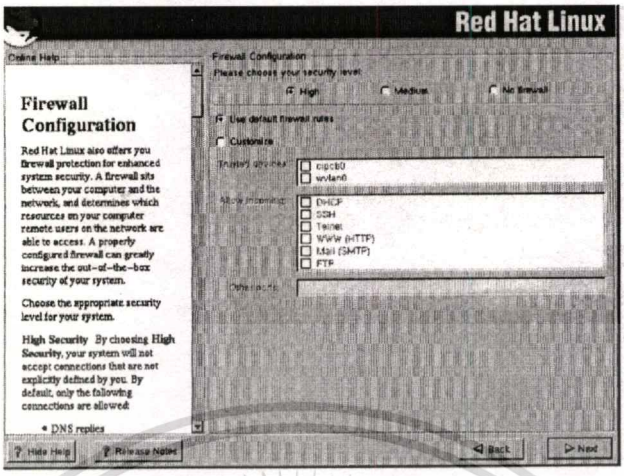


รูปที่ 4.9 หน้าจอ Network Configuration สำหรับการกำหนดค่าเครือข่ายต่าง ๆ

เลือก Active on boot และกำหนดค่าต่าง ๆ ที่ได้จากผู้บริหารระบบ ดังนี้

IP ADDRESS	:	เช่น 172.17.81.66
NETMASK	:	เช่น 255.255.255.0
NETWORK	:	เช่น 172.17.81.60
BOARDCAST	:	เช่น 172.17.81.255
HOSTNAME	:	เช่น spider.reptile.net
GATEWAY	:	เช่น 172.17.81.253
PRIMARY DNS	:	เช่น 172.17.100.1
SECOUNDARY DNS	:	เช่น 172.17.100.2

แล้วเลือกปุ่ม NEXT เพื่อทำงานต่อ



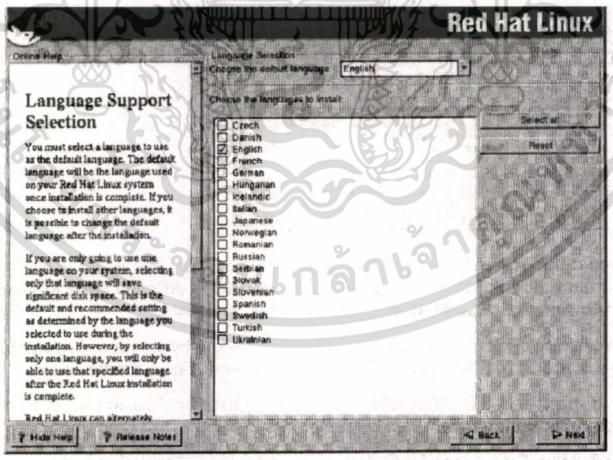
รูปที่ 4.10 หน้าจอ Firewall Configuration

สำหรับติดตั้งระบบการป้องกันความปลอดภัย

เลือก Medium

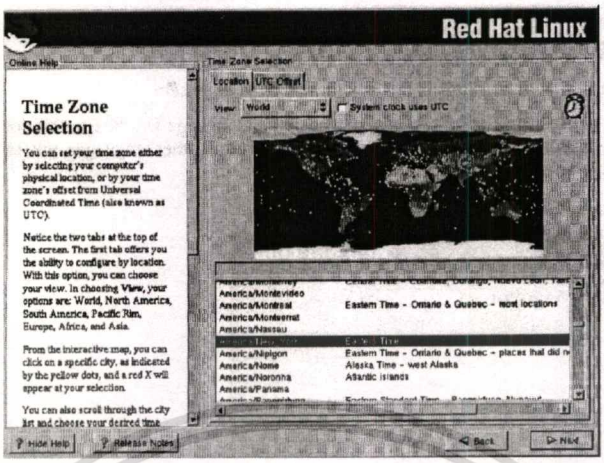
เลือก Use Default Firewall Roles

เสร็จแล้ว เลือกปุ่ม NEXT เพื่อทำงานต่อไป



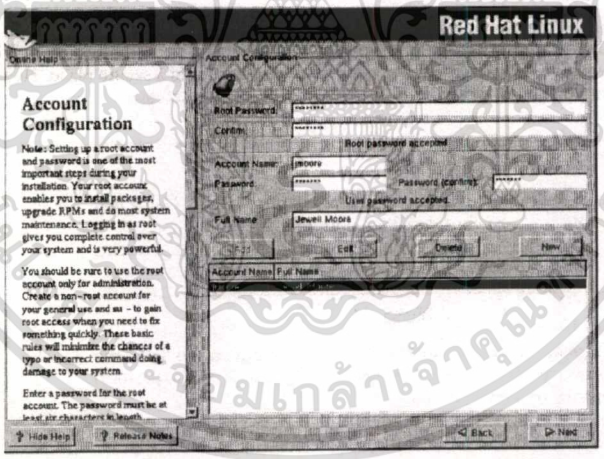
รูปที่ 4.11 หน้าจอ Language Support Selection

เลือกภาษาที่จะใช้เลือก English เสร็จแล้ว เลือกปุ่ม NEXT เพื่อทำงานต่อไป



รูปที่ 4.12 หน้าจอ Time Zone Selection

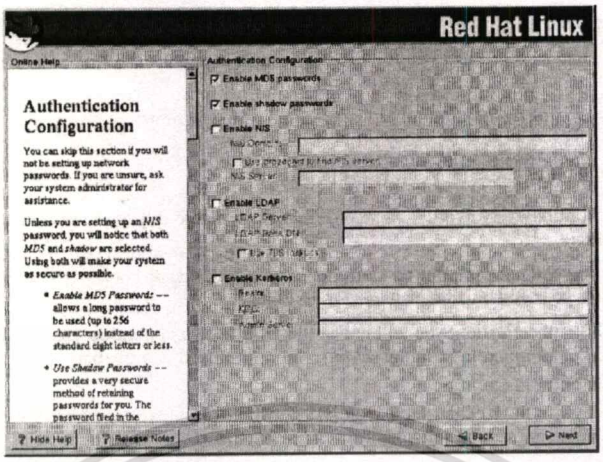
เลือกใช้เวลาให้ตรงกับประเทศนั้น ๆ โดยเลือกเป็น Asia/Bangkok เสร็จแล้ว เลือกปุ่ม NEXT เพื่อทำงานต่อไป



รูปที่ 4.13 หน้าจอ Account Configuration

กำหนดชื่อและรหัสผ่านสำหรับผู้ดูแลระบบ ใส่รหัสผ่าน (Password) ในช่อง Root Password ใส่ชื่อผู้ดูแลระบบ ในช่อง Account Name, Password และ ชื่อเต็มของผู้ดูแลระบบ ในช่อง Full Name เลือกปุ่ม ADD เข้าสู่ระบบ

เสร็จแล้ว เลือกปุ่ม NEXT เพื่อทำงานต่อไป

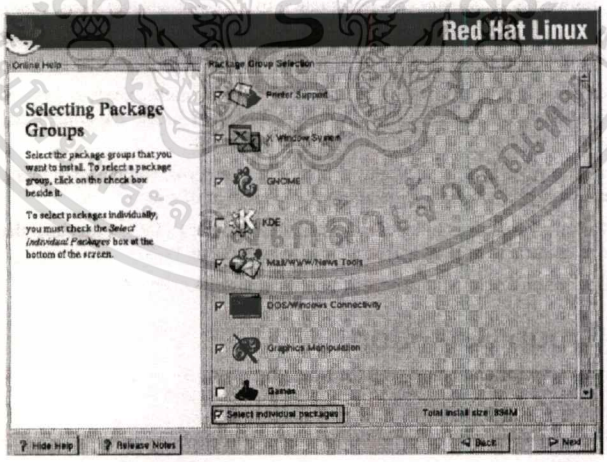


รูปที่ 4.14 หน้าจอ Authentication Configuration

กำหนด Authentication Configuration เพื่อเลือกระบบรักษาความปลอดภัยใน การตรวจสอบชื่อและรหัสผ่าน ก่อนอนุญาตให้ใช้งานในระบบ

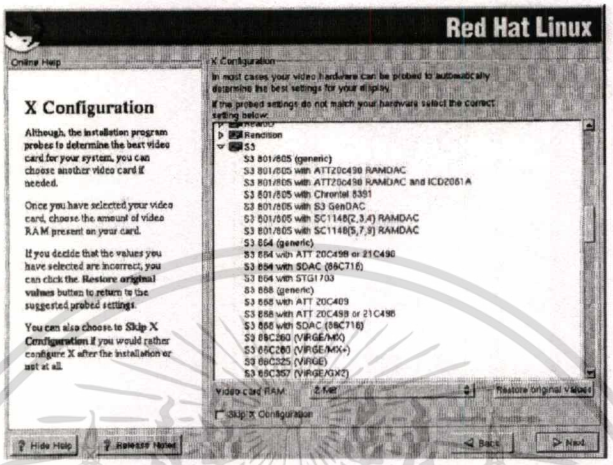
เลือก Use Shadow Password เพื่อรักษาความปลอดภัยให้กับ password

เลือก Enable MD5 Password เพื่อ encryption รหัส แบบ MD5 ซึ่งสนับสนุนการตั้งรหัสถึง 256 ตัวอักษร เสร็จแล้ว เลือกปุ่ม NEXT เพื่อทำงานต่อไป



รูปที่ 4.15 หน้าจอ Selecting Package Group

สำหรับเลือก Package ต่าง ๆ ที่ต้องการติดตั้งระบบ เสร็จแล้ว เลือกปุ่ม NEXT เพื่อทำงานต่อไป

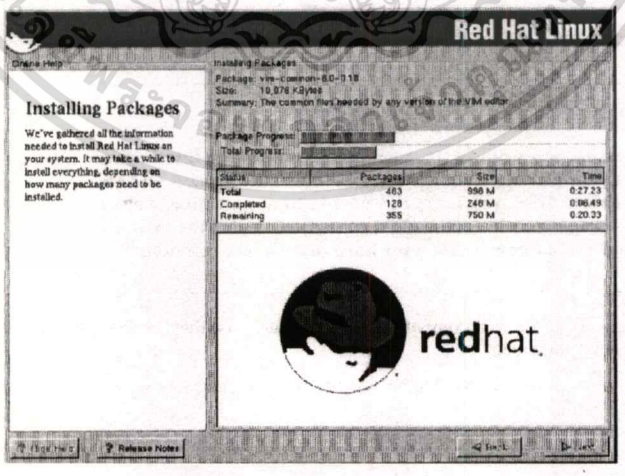


รูปที่ 4.16 หน้าจอ X Configuration

หน้าจอ X Configuration เป็นขั้นตอนการติดตั้งระบบ X Windows

เลือกปุ่ม Skip X Configuration เพื่อข้ามการติดตั้ง X Windows เลือกปุ่ม NEXT เพื่อเข้าสู่หน้าจอ about to install เป็นการยืนยันการติดตั้ง ถ้ายังไม่พร้อมสามารถยกเลิกได้โดยการกดปุ่ม Ctrl + Alt + Del ซึ่งโดยปกติเราจะไม่ทำการยกเลิกการติดตั้ง

เลือกปุ่ม NEXT เพื่อทำงานต่อไป



รูปที่ 4.17 หน้าจอ Installing Package

ระบบจะทำการ Format Partition และติดตั้งโปรแกรมทั้งหมดที่เลือกไว้
เมื่อเสร็จแล้ว เลือกปุ่ม Exit เพื่อจบการติดตั้ง

การ Login, logout และ Shutdown

- การ Login

  ใส่ชื่อผู้ใช้ Login : root

  ใส่รหัสผ่าน Password : ********

- การ Logout

  ทำได้โดยโดยการกดปุ่ม Ctrl + d หรือ ใช้คำสั่ง logout หรือ exit

- การปิดเครื่อง

  # /sbin/shutdown -h now ยุติการทำงานระบบ และหยุดเครื่อง

  # /sbin/shutdown -r now ให้ระบบทำการบูตใหม่

4.3 การติดตั้ง Snort

4.3.1 ขั้นตอนการติดตั้ง Snort

ก่อนการติดตั้ง Snort จะต้องมีการติดตั้ง libraries ที่จำเป็นเสียก่อน ในกรณีที่ระบบของท่านยังไม่ได้ติดตั้ง libpcap สามารถที่จะดาวน์โหลด library ดังกล่าวได้จาก ftp://ftp.ee.lbl.gov/libpcap.tar.Z หรือผู้ที่ใช้ Red Hat สามารถดาวน์โหลดเวอร์ชั่นที่เป็น rpm ได้จากเว็บไซต์ของ Red Hat http://www.redhat.com , ดาวน์โหลด Snort เวอร์ชั่นล่าสุดจาก http://www.snort.org จากนั้นให้ขยายไฟล์ออก ดังนี้

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

ให้ compile โดยเพิ่ม option ดังนี้ --with-mysql-includes=DIR และ --with-mysql-libraries=DIR ดังตัวอย่าง เช่น

```
#cd /usr/local/snort
#./configure --with-mysql-includes=/usr/include/mysql --with-mysql-libraries=/usr/lib/mysql
#make
#make install
```

ทั้งนี้ในขณะที่โปรแกรมกำลังคอมไพล์อยู่นั้น ท่านควรจะสังเกตเห็นคำว่า "checking for mysql... yes" ปรากฏขึ้น 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
```

สร้างไดเร็คทอรีเพื่อเก็บล็อกไฟล์ของ Snort ทั้งหมดแยกต่างหาก และควรป้องกันไม่ให้บุคคลอื่น access เข้ามาที่ไดเร็คทอรีนั้นๆ โดยปกติแล้วจะสร้างไว้ที่ /var/log/snort

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

สร้าง Database structure สำหรับ Snort โดยล็อกอินเข้าไปยัง MySQL และ สร้าง database ชื่อ snort ขึ้นมา

```
#mysql –u root -p
mysql>CREATE DATABASE snort;
```

จากนั้นให้สร้าง MySQL account ขึ้นมาเพื่อให้มีสิทธิในการจัดการกับฐานข้อมูล

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

จากนั้นก็ต้องสร้าง database structure ตามที่ Snort กำหนดไว้

```
#cd /usr/local/snort
#vi contrib/create_mysql แล้วเพิ่มคำว่า USE snort; ไว้ที่บรรทัดบนสุด
#mysql < ./contrib/create_mysql –u root –p
```

4.3.2 Snort Plugin Configuration

ให้แก้ไขไฟล์ /etc/snort/snort.conf เพื่อให้ snort เก็บข้อมูลเข้า database โดยมีลักษณะดังนี้

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

Arguments:

[log | alert] - ระบุว่าจะเก็บข้อมูลในส่วนของ alert หรือ log ปกติแล้วจะใช้ log

[type of database] - เช่น mysql, postgresql และ unixodbc.

[parameter list] - รูปแบบคือ key=value คั่นแต่ละ key ด้วย space

dbname - the name of the database you are connecting to

host - the host the RDBMS is on

port - the port number the RDBMS is listening on

user - connect to the database as this user

password - the password for given user

sensor_name - specify your own name for this snort

sensor. If you do not specify a name one will be generated automatically.

encoding - มีสามชนิดคือ hex, base64, ascii

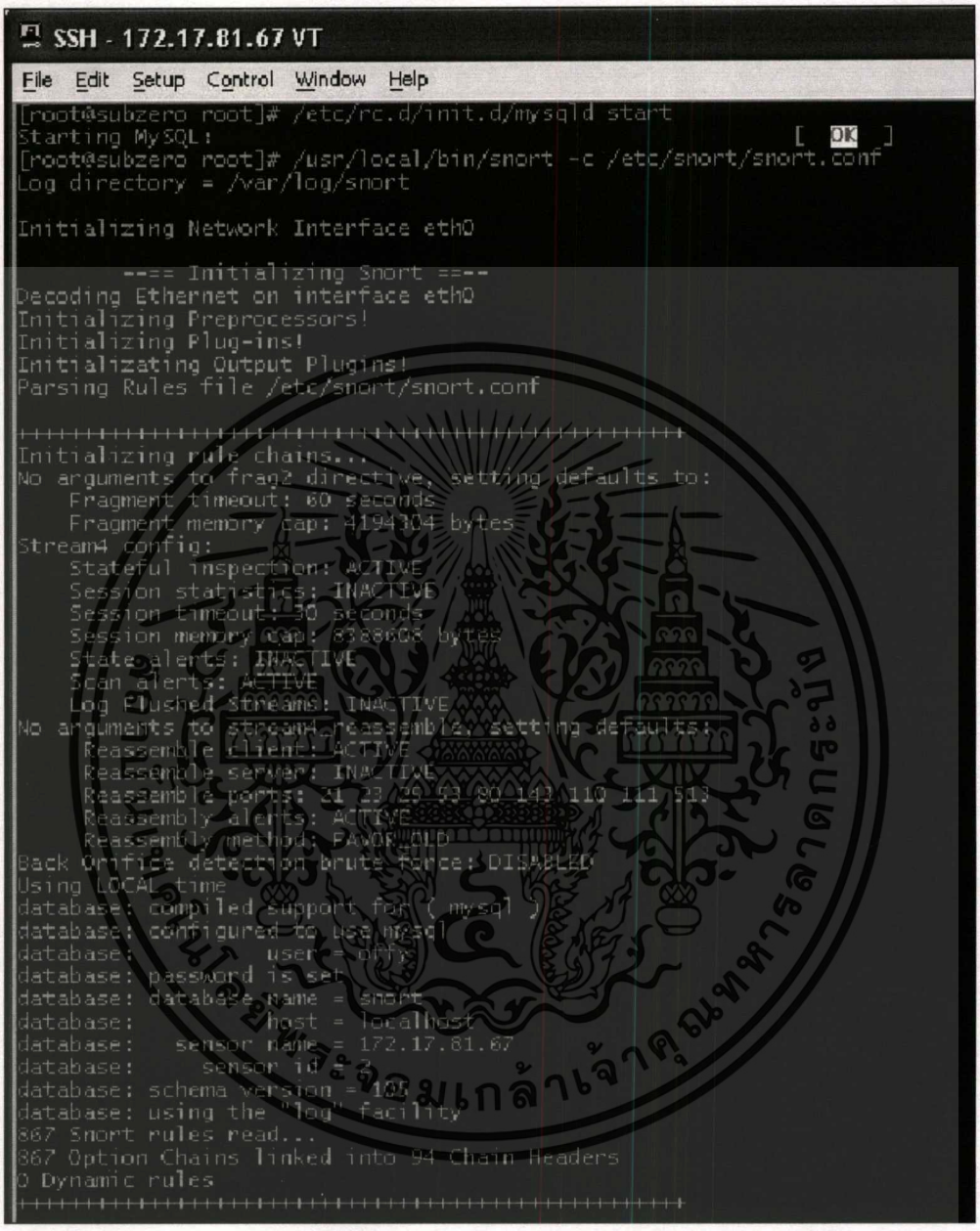
detail - รายละเอียดการเก็บข้อมูล มี full และ fast(default)

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

- Start Snort (daemon)

ทดลอง Start โปรแกรม Snort /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

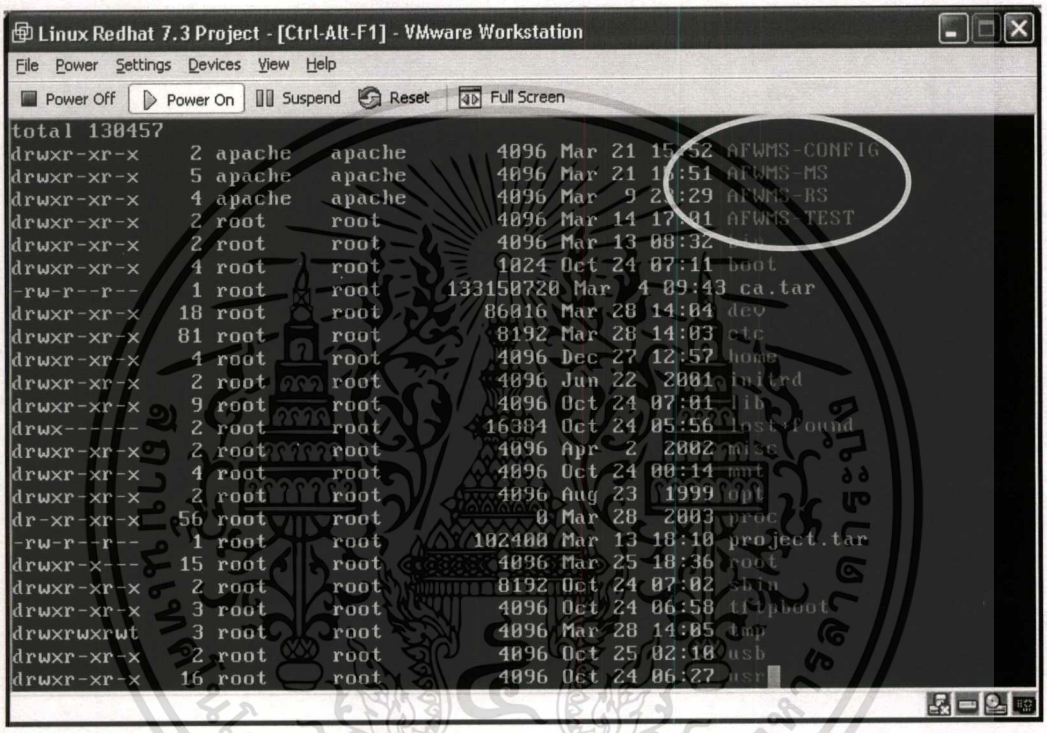


รูปที่ 4.18 หน้าจอผลลัพธ์ของการ Start Snort

จากรูปที่ 4.18 ก่อนที่จะทำการ Start Snort จะต้องทำการ Start MySQL ก่อน จากนั้นจึง Start Snort ตามลำดับ ซึ่งจากรูปจะเห็นว่ามี Rules Base ของ Snort ทั้งหมด 867 Rules ที่ถูกอ่านเข้ามา ซึ่ง Rules base เหล่านี้ สามารถดาวน์โหลด ได้จาก http://www.snort.org

4.4 การเซ็ตอัพ Environment ของระบบ

การเซ็ตอัพ Environment ของระบบ ประกอบไปด้วยการกำหนดโครงสร้างของ Directory ตามที่ได้ออกแบบไว้, การกำหนด File Permission ของระบบโครงสร้างของ Directory และการสร้าง crontab ให้โปรแกรมทำงานตาม Schedule ที่ตั้งเอาไว้ มีรายละเอียดดังนี้



รูปที่ 4.19 หน้าจอแสดง Directory หลักของโปรแกรม

การติดตั้งโปรแกรมระบบจัดการไฟร์วอลล์อัตโนมัติ จะติดตั้งไปยังใดก็ได้ root directory ของ Linux เพื่อให้การ อ้างอิงถึง PATH ของการ run program ทำได้ง่าย

อีกประการคือ Owner ของ Directory ทั้งสามจะใช้ User ที่ Run ตัว Web Server ทั้งนี้เพื่อรองรับคำสั่งบางอย่างที่ต้องทำงานผ่าน CGI ได้

การสร้าง Directory เพื่อนำ Script ไปเก็บไว้ เพื่อให้การทำงานเป็นไปตามเวลาที่กำหนด สามารถทำได้ดังนี้

สิ่งที่เราต้องการก็คือ ต้องการให้โปรแกรมทำงานทุกๆ 5 นาที เพื่อให้เกิด Process ต่างๆ ตามที่ออกแบบไว้ โดยการที่จะทำให้ระบบทำงานตามที่กำหนดไว้โดยใช้ crond สามารถทำได้ดังนี้

Login โดยใช้สิทธิของ root เพื่อ สร้าง Directory ที่ชื่อ /etc/cron.5min แล้วเรียก vi editor เพื่อแก้ไขแฟ้ม /etc/crontab โดยสิ่งที่ต้องทำคือเพิ่ม

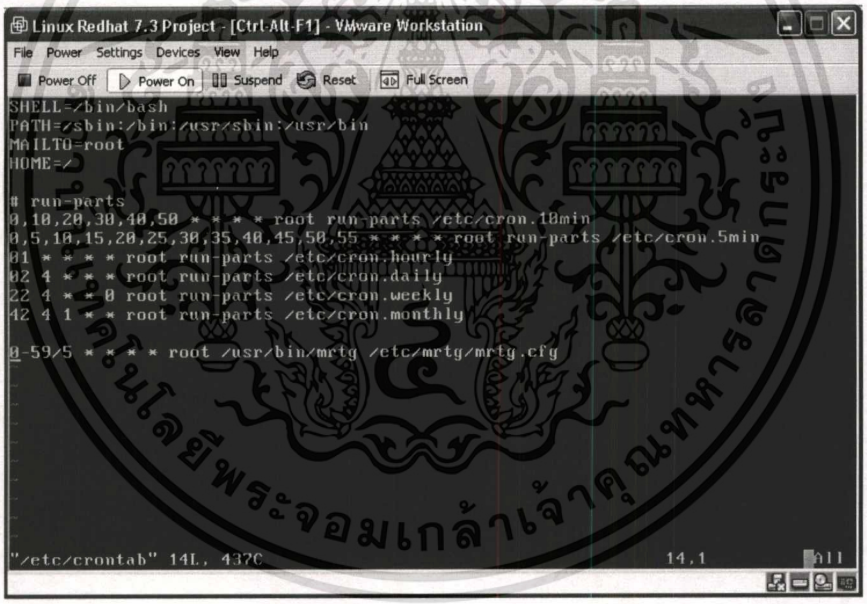
5,10,15,20,25,30,35,40,45,50,55 root run-parts /etc/cron.5min

เข้าไปในแฟ้ม จากนั้นพิมพ์

:wq

เพื่อ save และออกจากโปรแกรม

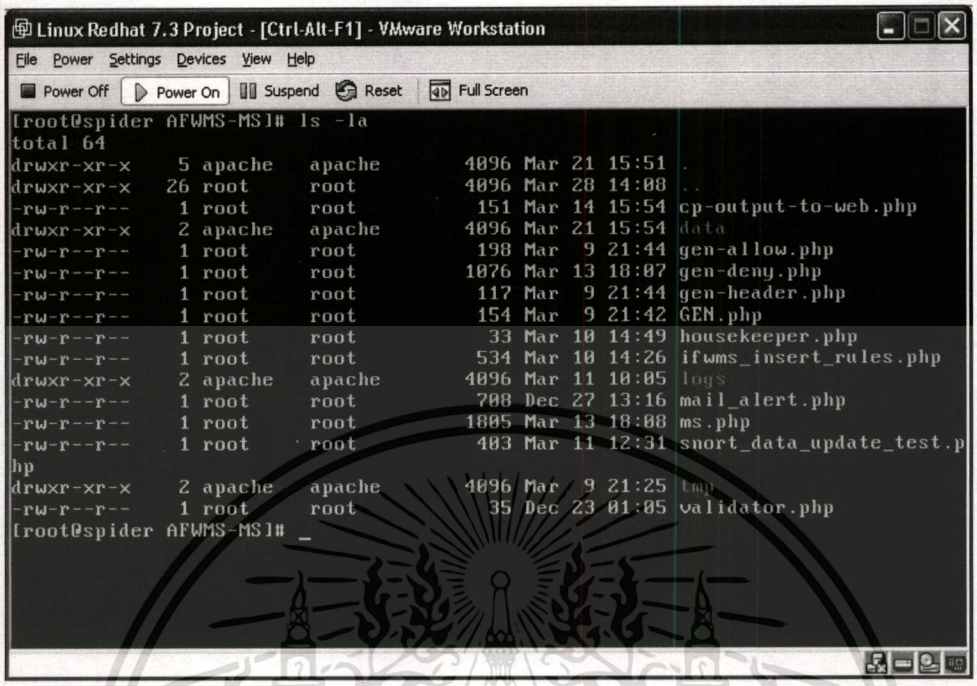
จากนั้น shell script ที่ถูกเก็บไว้ภายใต้ /etc/cron.5min จะถูกเรียกให้ทำงานทุกๆ 5 นาที



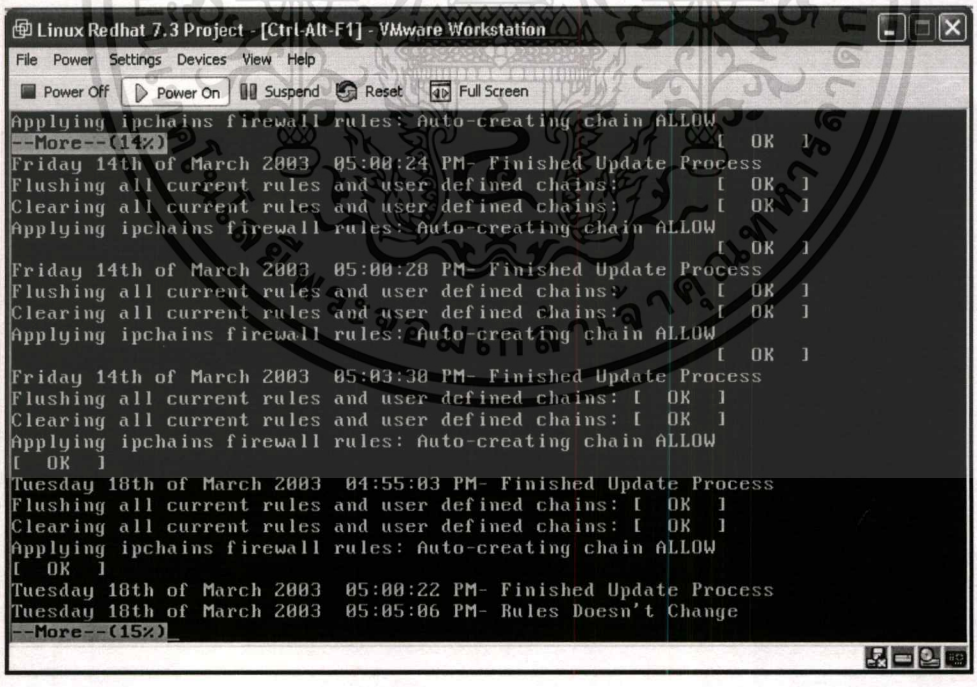
รูปที่ 4.20 หน้าจอแสดงการแก้ไขแฟ้ม /etc/crontab

4.5 ตัวอย่างการตรวจสอบ Log file

ระบบ Automatic Firewall Management System เป็นระบบที่ทำงานอยู่เบื้องหลัง ซึ่งการทำงานจะมีการเก็บ Log ไว้ใน Directory หลักของโปรแกรม ได้แก่ /AFWMS-MS/logs และ /AFWMS-RS/logs ดังรูปที่ 4.21



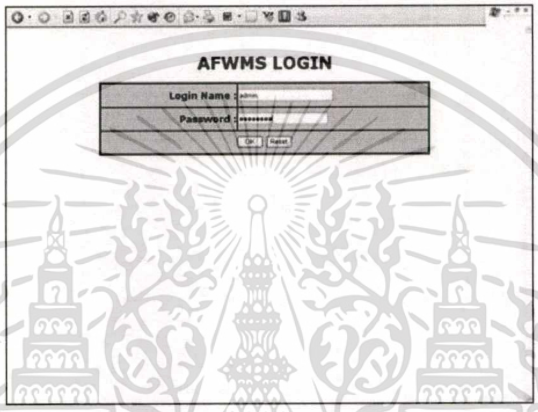
รูปที่ 4.21 หน้าจอแสดง Log Directory



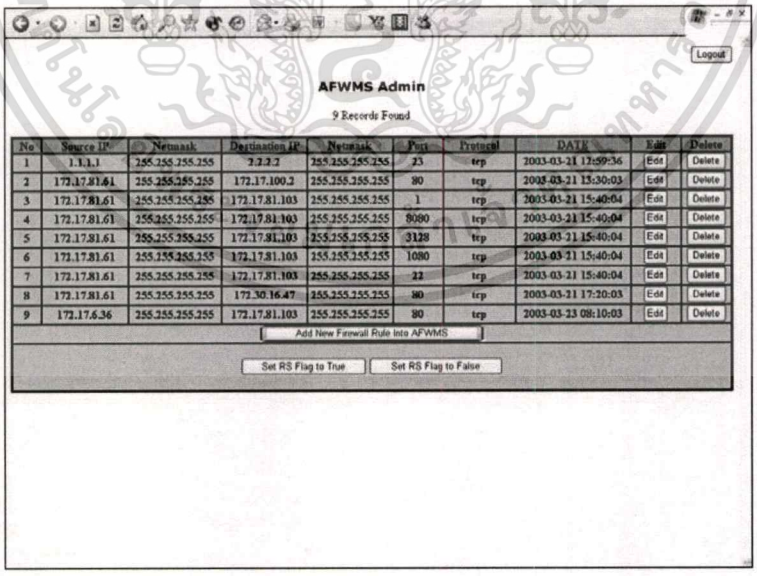
รูปที่ 4.22 หน้าจอแสดงข้อมูลภายในแฟ้ม /AFWMS-RS/logs/rs.log

4.6 การใช้งาน AFWMS ADMIN

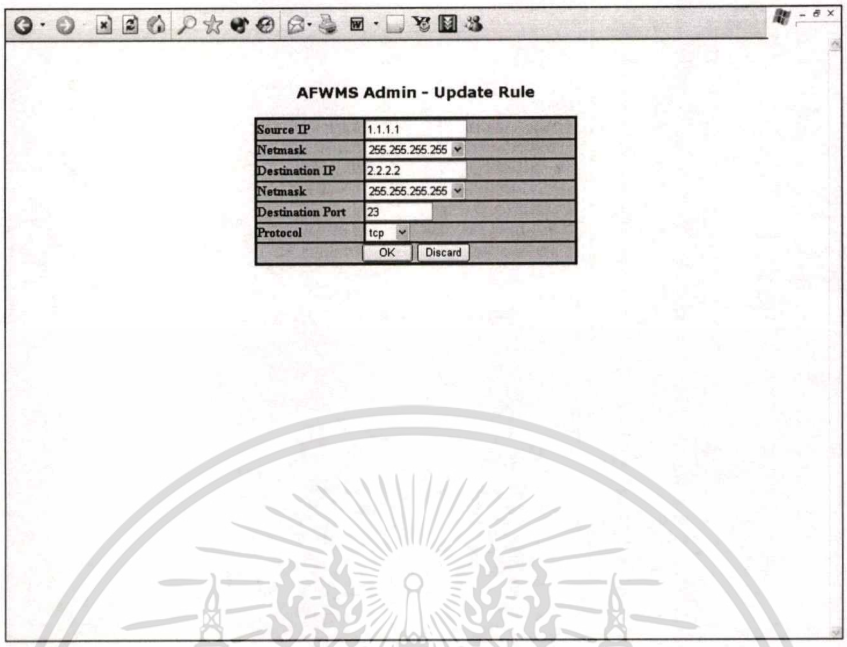
AFWMS ADMIN คือหน้าจอ User Interface (UI) ของระบบ Automatic Firewall Management System ซึ่งอนุญาตให้ผู้ดูแลระบบ สามารถแก้ไขปรับเปลี่ยน ลบ และ เพิ่มเติม ข้อมูลที่อยู่ในฐานข้อมูลของระบบ Automatic Firewall Management System ที่จะถูกนำไปสร้าง Rules base ให้กับไฟร์วอลล์ ทั้งนี้เนื่องจากบางครั้งการทำงานจริง มีโอกาสที่ผู้ดูแลระบบจะมีความต้องการที่จะแก้ไข ข้อมูลรวมถึงการลบ DENY Rules ที่ถูกสร้างขึ้นโดยระบบ



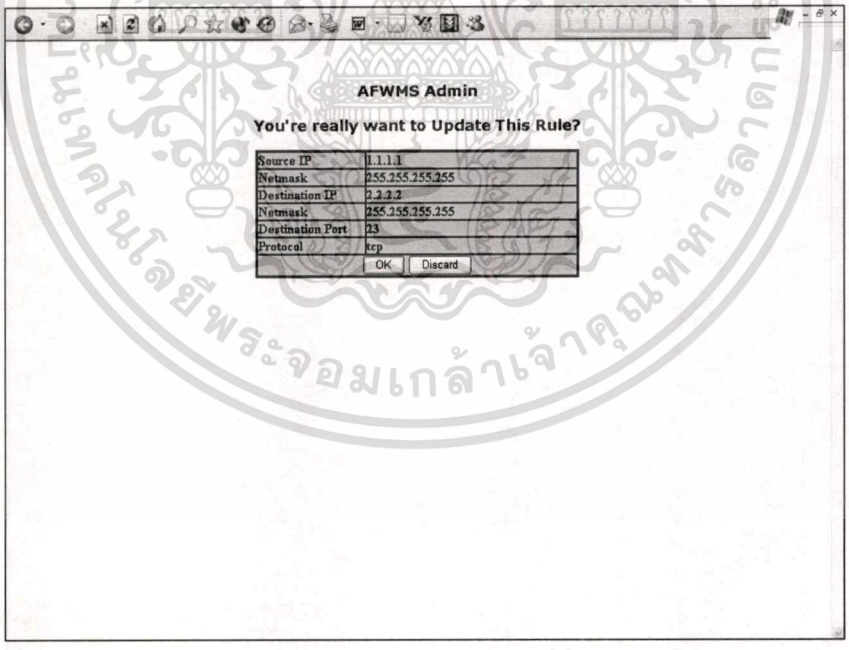
รูปที่ 4.23 หน้าจอ Login เข้าสู่ระบบ



รูปที่ 4.24 หน้าจอแสดงรายการข้อมูล



รูปที่ 4.25 หน้าจอแสดงหน้าจอ Edit

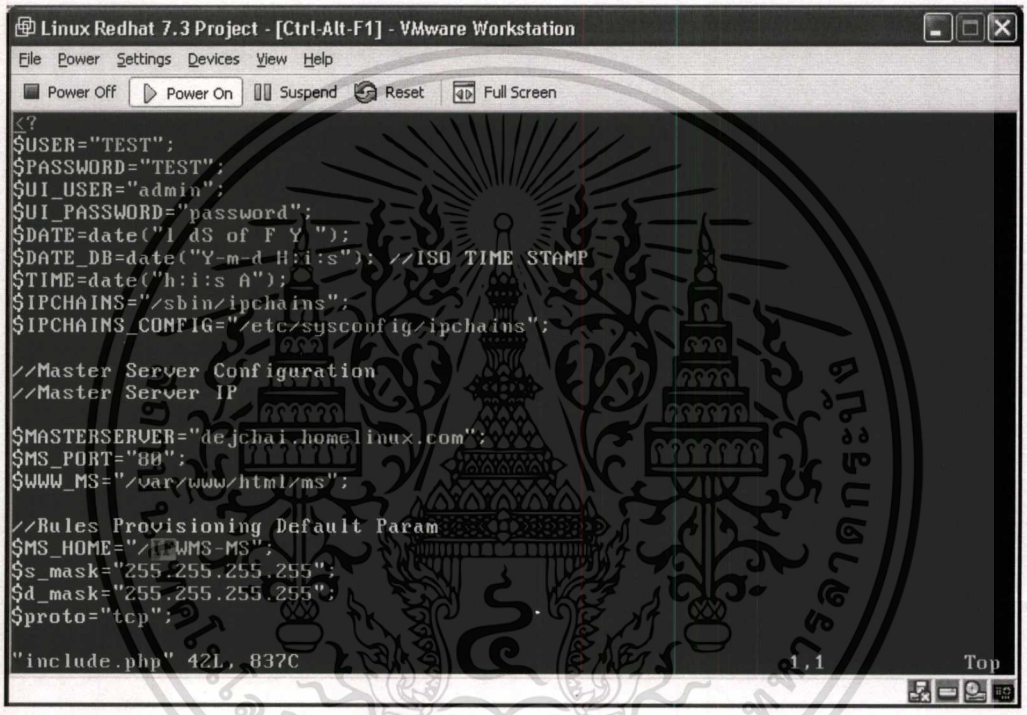


รูปที่ 4.26 หน้าจอแสดงการยืนยัน การแก้ไข หรือลบข้อมูล

4.7 การกำหนด Configuration ให้กับระบบ

ระบบมีการติดต่อกันระหว่างส่วนที่เป็น Master Server ซึ่งอยู่ที่ตัว Server ของระบบ Automatic Firewall Management System และ Remote Server ซึ่งติดตั้งไว้ที่ตัวไฟร์วอลล์ ดังนั้น จะต้องมีการกำหนด Parameters ต่างๆ ให้กับระบบ เพื่อที่จะทำให้ระบบรู้ว่าเครื่อง ที่มันต้องการจะติดต่อด้วยนั้นมีชื่อว่าอะไร และมี ip address เป็นอะไร เป็นต้น

นอกเหนือจากรายละเอียดของเครื่องคอมพิวเตอร์ในระบบแล้ว Configuration File



รูปที่ 4.27 หน้าจอแสดง Configuration ของระบบ

บทที่ 5
สรุปและข้อเสนอแนะ

5.1 สรุป

ระบบ Automatic Firewall Management System มีจุดมุ่งหมายเพื่อช่วยผู้ดูแลระบบในการป้องกันระบบที่ต้องการรักษาความปลอดภัย จากการบุกรุกภายนอกได้อย่างทันท่วงที โดยอาศัยการนำเอาข้อมูลที่ต้องสงสัยที่ IDS ตรวจจับได้ไปปรึกษากับระบบผู้เชี่ยวชาญ ที่มีความรู้ในการป้องกันการบุกรุกแบบต่างๆ เพื่อหาวิธีป้องกันที่เหมาะสมกับรูปแบบการบุกรุกแล้วนำเอาวิธีการป้องกันที่ได้จากระบบผู้เชี่ยวชาญไปกำหนด Rules Base ให้กับไฟร์วอลล์เพื่อไม่ให้การบุกรุกสามารถกระทำต่อระบบที่ต้องการป้องกันได้

จากการทดสอบโครงการพัฒนาระบบ Automatic Firewall Management System เห็นว่าน่าจะมีประโยชน์กับองค์กรดังนี้ คือ

1. ช่วยทำการวิเคราะห์ความเสี่ยงของการบุกรุกจากข้อมูลที่ IDS ตรวจพบ และ นำผลของการวิเคราะห์มาสร้างเป็น Rules Base ที่เหมาะสมให้กับไฟร์วอลล์
2. ลดภาระงานของผู้บริหารระบบที่จะต้องคอยตรวจสอบการบุกรุกที่มีเข้ามา และหาวิธีป้องกันการบุกรุกที่เกิดขึ้น
3. ลดความเสี่ยงที่เกิดจากการถูกบุกรุกรูปแบบต่าง เพราะการบุกรุกที่มีความเสี่ยงสูงจะถูกป้องกันโดยไฟร์วอลล์
4. เพิ่มความปลอดภัยให้กับระบบ
5. เพิ่มประสิทธิภาพให้กับการดูแลระบบคอมพิวเตอร์เครือข่าย โดยเฉพาะอย่างยิ่งระบบที่มีคอมพิวเตอร์จำนวนมากๆ

โดยสรุป ระบบ Automatic Firewall Management System มีจุดมุ่งหมายเพื่อช่วยผู้ดูแลระบบในการป้องกันระบบที่ต้องการรักษาความปลอดภัย จากการบุกรุกภายนอกได้อย่างทันท่วงที โดยอาศัยการนำเอาข้อมูลที่ต้องสงสัยที่ IDS ตรวจจับได้ ไปวิเคราะห์หาเงื่อนไขในการป้องกันการบุกรุกแบบต่างๆ เพื่อให้ได้มาซึ่งวิธีป้องกันที่เหมาะสมกับรูปแบบการบุกรุกนั้นๆ แล้วนำเอาวิธีการป้องกันที่ได้ไปกำหนด Rules Base ให้กับไฟร์วอลล์ เพื่อไม่ให้การบุกรุกสามารถกระทำต่อระบบที่ต้องการป้องกันได้

5.2 ข้อเสนอแนะ

1. ระบบทำงานผ่าน HTTP ซึ่งสามารถทำการแก้ไขให้การสื่อสารระหว่างส่วนที่เป็น Master Server และ Remote Server ผ่านทางโปรโตคอล ที่มีความปลอดภัยสูงกว่าได้ เช่น HTTPS
2. การสร้าง Rules base ให้กับไฟร์วอลล์เป็นเรื่องที่ยุ่งยาก และหากมีการพัฒนาโปรแกรมส่วนที่ทำการลดรูปของ Rules base ก็จะทำให้จำนวน Rules base ที่ติดตั้งให้กับไฟร์วอลล์ลดลง ทำให้ Performance ของระบบ ไฟร์วอลล์ดีขึ้นด้วย
3. ระบบจะติดตั้ง Rules Base ที่ทำการป้องกันการบุกรุกแบบ Packet Filtering Firewall ซึ่งอาจมีการทำให้ระบบสามารถทำการป้องกันได้ละเอียดมากขึ้นได้
4. ควรติดตั้งโปรแกรมที่ช่วยจัดการเวลาของเครื่องที่เป็น Client และ Server ให้ตรงกันเพื่อประโยชน์ในการตรวจสอบ Log File
5. การพัฒนาให้ระบบสามารถทำงานกับไฟร์วอลล์ ที่มีการติดตั้งรูปแบบอื่นได้ จะช่วยทำให้ระบบน่าใช้มากขึ้น
6. การแก้ปัญหาเรื่องของการบุกรุกแบบ DDoS (Distributed Denial of Service) เป็นเรื่องที่น่าสนใจว่าการติดตั้ง Rules Base จะทำอย่างไรจึงจะมีความเหมาะสมกับระบบที่สุด
7. ระบบยังไม่ได้คำนึงถึงการจัดการเรื่องขนาดของ Log Files จึงมีโอกาสที่ขนาดของ Log File จะขยายไปมากหากมีการทำงานไปเป็นระยะเวลานานๆ รวมถึงมีความผิดพลาดซึ่งเกิดจากการทำงานอยู่มากๆ ระบบก็จะบันทึก Error Messages ไว้ด้วย

บรรณานุกรม

Grammp, F. T. and Morris, R. H.1984. "Unix Operating System Security." **AT&T Bell Laboratories Technical Journal**. 63(8): 1649-1672.

Hall, D. V. 1992. **Microprocessors and Interfacing Programming and Hardware**. Second Edition. Singapore: McGraw-Hill.

Held, G. 1996. **Understanding Data Communications**. Fifth Edition. Indianapolis, IN: Sams Publishing.

Rob, P. and Coronel, C. 2000. **Database Systems: Design, Implementation, and Management**. Fourth Edition. Cambridge, MA: Course Technology.

Scambray, J. et al. 2001. **Hacking Exposed: Network Security Secrets & Solutions**. Second Edition. New York, NY: Mc Graw-Hill.

Stalling, W. 1999. **Cryptography and Network Security Principles and Practice**. Upper Saddle River, NJ: Prentice Hall.

The PHP Group. 2001. **PHP Manual**. [Online].Available: http://www.php.net/manual/en/.

Red Hat, Inc. 2003. **Redhat Support and Documents.** [Online].Available: http://www.redhat.com/apps/support/.

Rusty Russell. 2000. **Linux IPCHAINS-HOWTO.** [Online].Available: http://www.netfilter.org/ipchains/HOWTO.txt

Roesch, M and Green, C. 2002. **Snort Users Manual.** [Online].Available: http://www.snort.org/docs/writing_rules/.

ประวัติผู้เขียน

ชื่อ : นายเดชชัย ศรีหาคิม

ประวัติการศึกษา : 2536- 2541 ครุศาสตร์อุตสาหกรรมกรรม (4ปี)

สาขาวิชาวิศวกรรมไฟฟ้า

สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ประวัติการทำงาน : 2540 – 2544 สำนักเทคโนโลยีสารสนเทศ กระทรวงสาธารณสุข และโรงพยาบาลขอนแก่น

ตำแหน่ง วิศวกรระบบ

ฝ่าย เทคโนโลยีและวิศวกรรมการแพทย์

2545-ปัจจุบัน บริษัท ฮัทชิสัน CAT ไวร์เลส มัลติมีเดีย จำกัด

ตำแหน่ง Fraud & Security Developer

ฝ่าย Fraud and Security