โครงข่ายประสิทธิภาพสูงสำหรับกลุ่มการวิจัยการสื่อสารไร้สาย

High Performance Network for Wireless Communication Research Group

โดย

นางสาวศรัญญา วิจิตรสมบัติ

นางสาวสาวิตรี ฉ่ำมะณี

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมสารสนเทศ

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2549

High Performance Network for Wireless Communication Research Group

BY

Miss. Saranya Wichitsombat

Miss. Sawitree Chammanee

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENT FOR THE DEGREE OF

BACHELOR IN DEPARTMENT OF INFORMATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2006

หัวข้อปริญญานิพนธ์	โครงข่ายประสิทธิภาพสูงสำหรับกลุ่มการวิจัยการสื่อสารไร้สาย
ชื่อนักศึกษา	นางสาวศรัญญา วิจิตรสมบัติ รหัสนักศึกษา 46012196
	นางสาวสาวิตรี ฉ่ำมะณี รหัสนักศึกษา 46012204
อาจารย์ที่ปรึกษา	อาจารย์สถาพร พรหมวงศ์
	ผศ.พิชญ สุพรรณกูล
ระดับการศึกษา	ปริญญาตรี วิศวกรรมศาสตรบัณฑิต
	สาขาวิชาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2549

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง อนุมัติให้รับปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรบัณฑิต

.....

(อาจารย์สถาพร พรหมวงศ์)

อาจารย์ผู้ควบคุมปริญญานิพนธ์

.....

(ผศ.พิชญ สุพรรณกูล)

อาจารย์ผู้ควบคุมปริญญานิพนธ์

หัวข้อปริญญานิพนธ์	โครงข่ายประสิทธิภาพสูงสำหรับกลุ่มการวิจัยการสื่อสารไร้สาย
นักศึกษา	นางสาวศรัญญา วิจิตรสมบัติ รหัสนักศึกษา 46012196
	นางสาวสาวิตรี ฉ่ำมะณี รหัสนักศึกษา 46012204
อาจารย์ที่ปรึกษา	อาจารย์สถาพร พรหมวงศ์
อาจารย์ที่ปรึกษาร่วม	ผศ. พิชญ สุพรรณกูล
ระดับการศึกษา	ปริญญาตรีวิศวกรรมศาสตรบัณฑิต
	สาขาวิศวกรรมสารสนเทศ
ภาควิชา	วิศวกรรมสารสนเทศ
ปีการศึกษา	2549

บทคัดย่อ

โครงงานนี้ได้ทำการศึกษาและวางระบบโครงข่ายที่มีประสิทธิภาพสูงสำหรับกลุ่มการวิจัยการสื่อสารไร้สาย วัตถุประสงค์ของโครงงานนี้คือเพื่อออกแบบและพัฒนาโครงข่ายให้มีการทำงานอย่างมีประสิทธิภาพ มีเสถียรภาพ และปลอดภัยต่อข้อมูลในระดับสูง ได้มีการออกแบบและติดตั้งไฟร์วอลล์ (Firewall) DNS เซิร์ฟเวอร์ (DNS Server) เว็บเซิร์ฟเวอร์ (Web Server) และเซิร์ฟเวอร์ข้อมูลกลาง ไฟร์วอลล์ ใช้สำหรับป้องกันผู้บุกรุก รวมทั้งยังได้ออกแบบโฮมเพจ (Home Page) และเว็บบอร์ด (Web Board) สำหรับบริการและแลกเปลี่ยนข้อมูลไว้ในเว็บเซิร์ฟเวอร์ เซิร์ฟเวอร์ฐานข้อมูลกลางใช้สำหรับเก็บข้อมูลวิจัยในกลุ่มการวิจัยการสื่อสารไร้สาย

Thesis Title	**High Performance Network for Wireless Communication Research Group**
Student	**Miss Saranya Wichitsombat ID.46012196**
	Miss Sawitree Chammanee ID.46012204
Advisor	**Mr. Sathaporn Promwong**
	Asst.Prof.Pichaya Supanakoon
Graduate Level	**Bachelor Degree of Information Engineering**
Department	**Information Engineering**
Academic Year	**2006**

Abstract

In this project, high performance network for wireless communication research group is studied and managed. The purpose is to design and develop the network, which is high performance, stable and security. The firewall, DNS, web and central database server are designed and setup. The firewall is used to protect the hackers. The home page and web board are designed to service and exchange acknowledge in the web server. The central database server is used to store the research database inside the wireless communication research group.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้มิอาจสำเร็จลุล่วงได้ด้วยดี หากขาดความช่วยเหลือจากหลายๆ ฝ่าย ด้วยกัน ดังนั้นทางคณะผู้จัดทำจึงใคร่ขอขอบพระคุณบุคคลต่างๆ ดังต่อไปนี้

ขอขอบพระคุณ อาจารย์สถาพร พรหมวงศ์ และ ผศ. พิชญ สุพรรณกูล อาจารย์ที่ปรึกษาปริญญานิพนธ์ ที่ให้ความเอาใจใส่ แนะนำ และช่วยเหลือตลอดเวลาของการทำงาน ซึ่งต้องขอขอบพระคุณอาจารย์เป็นอย่างมาก

ขอขอบคุณพี่โจ้ พี่แป้ง พี่พร รวมถึงเพื่อนๆ ที่คอยให้ความช่วยเหลือ ให้คำแนะนำ รวมถึงการช่วยเหลือแก้ไขปัญหาต่างๆให้สำเร็จลุล่วง ตั้งแต่เริ่มทำโครงงาน

ขอขอบคุณ ภาควิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง สำหรับสิ่งอำนวยความสะดวกมากมาย ที่ใช้สำหรับการทำงาน ทั้งห้องทำงาน โต๊ะทำงาน อินเทอร์เน็ตสำหรับค้นคว้าหาข้อมูลต่างๆ ที่จำเป็นสำหรับโครงงานนี้

ขอกราบขอบพระคุณคณาจารย์ ภาควิชาวิศวกรรมสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้า เจ้าคุณทหารลาดกระบัง ทุกๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้กับผู้จัดทำ

และต้องขอบพระคุณบุคคลที่สำคัญที่สุดที่ทำให้ผู้จัดทำมีวันนี้ ก็คือ บิดา มารดา อันเป็นที่เคารพรักยิ่ง ซึ่งได้เลี้ยงดูผู้จัดทำมาเป็นอย่างดี พร้อมทั้งให้โอกาสในการศึกษาอย่างเต็มที่ และยังให้การสนับสนุน ให้กำลังใจ เอาใจใส่เสมอมา ในทุก ๆ ด้านอันหาที่เปรียบมิได้ ผู้จัดทำขอระลึกในพระคุณอันสุดประมาณและขอกราบขอบพระคุณมา ณ ที่นี้

คุณค่าและประโยชน์อันพึงมาจากวิทยานิพนธ์ฉบับนี้ คณะผู้จัดทำขอมอบแด่ผู้มีพระคุณทุกท่าน

นางสาวศรัญญา วิจิตรสมบัติ
นางสาวสาวิตรี ฉ่ำมะณี
ผู้จัดทำ

สารบัญ

สารบัญ(ต่อ)

สารบัญ(ต่อ)

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1.1 แนวความคิดและที่มา

เนื่องจากการจัดการระบบเน็ตเวิร์คภายในห้องกลุ่มการวิจัยการสื่อสารแบบไร้สายในแบบเดิม ยังคงขาดความปลอดภัยและเสถียรภาพในการใช้งาน ทำให้กลุ่มการวิจัยการสื่อสารไร้สายมีปัญหาในการใช้งานระบบโครงข่ายทั้งภายในและภายนอกรวมถึงเรื่องความปลอดภัยจากผู้บุกรุก จึงได้ออกแบบและจัดการกับระบบเน็ตเวิร์คภายในห้องกลุ่มการวิจัยไร้สายใหม่ โดยเน้นในเรื่องของความปลอดภัย ความมีเสถียรภาพในการใช้งาน รวมทั้งจัดทำเว็บแอพพลิเคชั่นสำหรับกลุ่มการวิจัยการสื่อสารไร้สายด้วย

1.1.1 ความปลอดภัย

ในเรื่องของความปลอดภัยในระบบเดิม ได้พบปัญหาหลายอย่างเช่น การใช้ IP สาธารณะเพียงอย่างเดียว ซึ่งจำนวนของหมายเลขเน็ตเวิร์คไม่เพียงต่อความต้องการของผู้ใช้ นอกจากนี้ยังทำให้ความปลอดภัยในระบบลดลงด้วย และเกิดปัญหาการชนกันของไอพีแอดเดรส เนื่องจากผู้ใช้เป็นคนกำหนดไอพีแอดเดรสกันเอง รวมถึงการจัดสรรไอพีแอดเดรสที่ไม่เป็นระบบ จึงได้คิดพิจารณาจัดทำโครงการนี้ขึ้นโดยได้ทำการออกแบบระบบเน็ตเวิร์คให้มีประสิทธิภาพทางด้านความปลอดภัยมากขึ้น

1.1.2 เสถียรภาพ

ในเรื่องของเสถียรภาพนั้นแบบเดิมใช้ เกตเวย์ไฟร์วอลล์เพียงตัวเดียว เมื่อเกิดความเสียหายทำให้ผู้ใช้ภายในไม่สามารถเชื่อมต่อกับเน็ตเวิร์คภายนอกได้ จึงได้ทำการออกแบบโครงข่ายให้มีประสิทธิภาพและเสถียรภาพมากขึ้น

1.1.3 ความปลอดภัยต่อข้อมูลภายในเซิร์ฟเวอร์

แบบเดิมภายในห้องวิจัยการสื่อสารไร้สายนั้นไม่ได้มีการจัดการใดๆเกี่ยวกับ ข้อมูล, ผลงานหรือผลการวิจัยของอาจารย์และนักศึกษา ซึ่งเป็นข้อมูลที่มีความสำคัญในระดับสูง จึงได้คิดพัฒนาให้มีการจัดการที่เป็นระบบมากขึ้น โดยจัดเก็บเป็นฐานข้อมูลให้มีความปลอดภัย

1.1.4 เว็บแอพพลิเคชั่น

ก่อนหน้านี้ภายในห้องวิจัยการสื่อสารไร้สายไม่มีระบบบริการภายในห้อง ทำให้เกิดความยุ่งยากต่างๆ เช่น การดาวน์โหลดงานวิจัย เป็นต้น จึงได้คิดสร้างเว็บไซด์ภายในห้องวิจัยการ

สื่อสารไร้สายขึ้น เพื่อให้มีการแจ้งข่าวสาร, ความรู้ต่างๆรวมทั้งทำการสร้างเว็บบอร์ด เพื่อให้ผู้ใช้ในห้องวิจัยได้ติดต่อหรือตั้งกระทู้ถาม- ตอบ เกี่ยวกับข่าวสาร หรือวิชาการความรู้ภายในห้องวิจัย

1.2 จุดประสงค์

- เพื่อพัฒนาการจัดระบบเน็ตเวิร์คภายในกลุ่มการวิจัยการสื่อสารไร้สาย
- เพื่อป้องกันการเข้าถึงระบบโครงข่ายจากภายนอก
- เพื่อเก็บรวบรวมผลการวิจัยและ thesis ของนักศึกษา ให้เป็นระบบ
- เพื่อแลกเปลี่ยนความรู้ ข่าวสาร ทั้งภายในและภายนอกกลุ่มการวิจัย

1.3 ขอบเขตของโครงงาน

- ศึกษาระบบโครงข่ายภายในห้องกลุ่มการวิจัยในแบบเดิม ว่ามีข้อดี- ข้อเสีย และส่วนที่บกพร่องตรงส่วนไหนบ้าง
- ศึกษาความต้องการ และพฤติกรรมการใช้งานในระบบโครงข่ายของผู้ใช้
- ทำการวางแผน ออกแบบ และวิเคราะห์ จัดการระบบเน็ตเวิร์คให้มีประสิทธิภาพ โดยมีการติดตั้ง ไฟร์วอล(Firewall), NAT, IPtables, Web Server, Mail Server และ FTP Server
- เพิ่มระบบความปลอดภัยของเซิร์ฟเวอร์ฐานข้อมูลกลาง (Central Database Server)
- ทำการตั้งค่าที่ใช้ในการวางระบบเน็ตเวิร์ค
- พัฒนาในส่วนของเซิร์ฟเวอร์ข้อมูลโดยการทำระบบฐานข้อมูล เพื่อสะดวกในการใช้งานยิ่งขึ้น
- เพิ่มระบบรักษาความปลอดภัยและระบบป้องกันการโจมตีที่มายังระบบเครือข่าย

1.4 ผลที่คาดว่าจะได้รับ

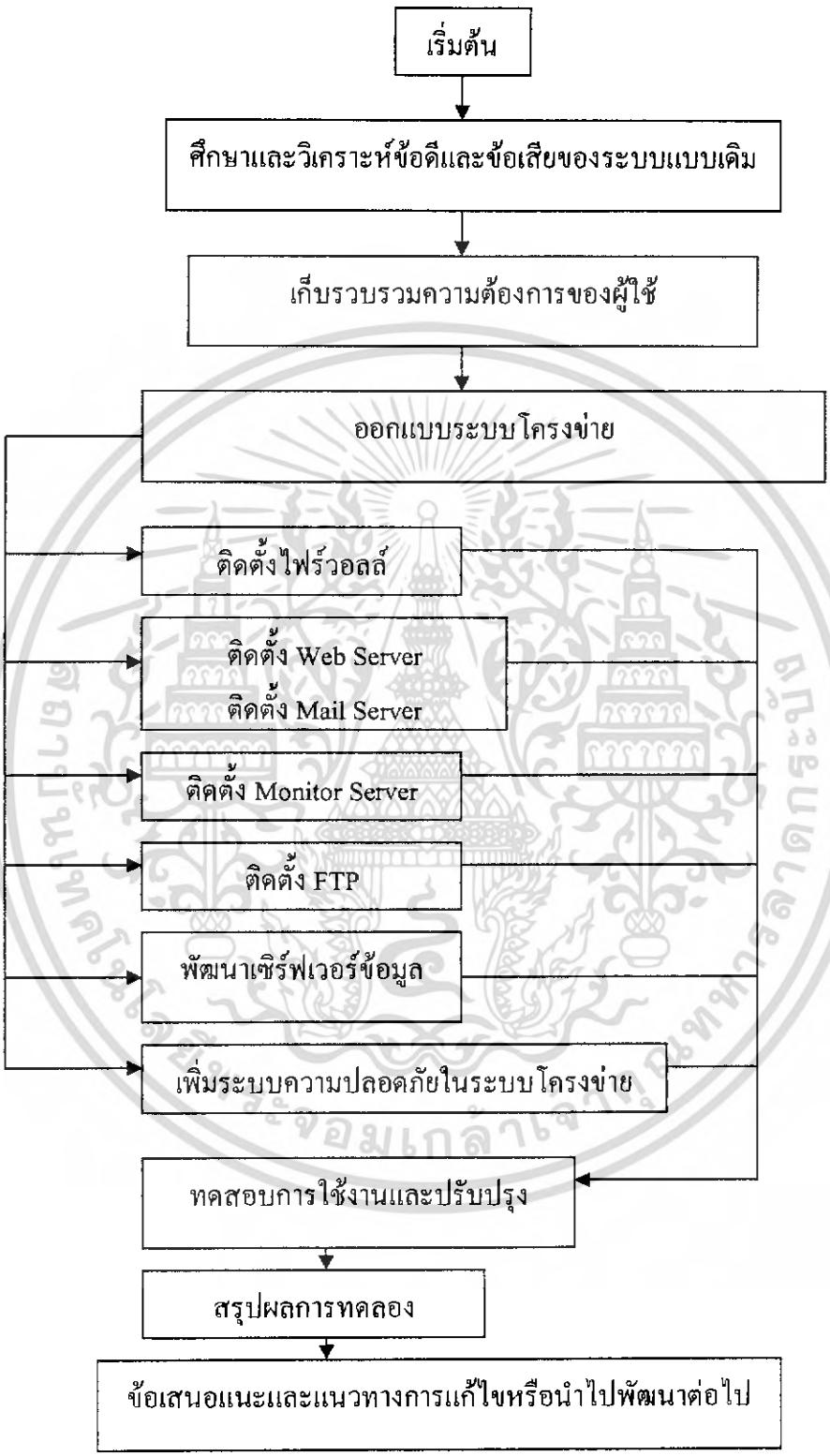
- มีระบบจัดการกับโครงข่ายในห้องการวิจัยที่มีคุณภาพ สามารถป้องกันการโจมตีจากโครงข่ายภายนอกที่ไม่หวังดีได้
- ผลงานหรือบทความทางการวิจัยของสมาชิกถูกจัดการให้เป็นระบบระเบียบมากขึ้น
- มีเว็บไซต์ที่เป็นศูนย์กลางเพื่อให้สมาชิกหรือผู้ที่เข้ามาชมได้รับความรู้และแลกเปลี่ยนความรู้ข่าวสารระหว่างกัน

1.5 ขั้นตอนดำเนินงาน

ในการจัดทำระบบเน็ตเวิร์คภายในห้องกลุ่มการวิจัยการสื่อสารไร้สายได้มีขั้นตอนในการจัดทำดังนี้

1. ทำการศึกษาระบบเน็ตเวิร์คภายในห้องกลุ่มการวิจัยแบบเดิม และวิเคราะห์ถึงข้อดีและข้อเสียของระบบ
2. เก็บรวบรวมข้อมูลความต้องการ และพฤติกรรมการใช้งานของผู้ใช้งานในระบบ
3. ทำการออกแบบระบบโครงข่ายให้สอดคล้องกับความต้องการของผู้ใช้
4. ติดตั้งไฟร์วอลล์
5. ติดตั้ง Web Server และ Mail Server
6. ติดตั้ง Monitor Server
7. ทำการพัฒนาในส่วนของเซิร์ฟเวอร์ข้อมูลโดยการทำระบบฐานข้อมูล
8. เพิ่มความปลอดภัยให้กับระบบโครงข่าย เพื่อป้องกันการโจมตีและสร้างความปลอดภัยให้แก่โครงข่าย

ขั้นตอนต่างๆสามารถแสดงได้ดังรูปที่ 1.1



รูปที่ 1.1 ขั้นตอนการดำเนินงาน

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 บทนำ

ในบทนี้จะกล่าวถึงทฤษฎีต่างๆ ที่เกี่ยวกับระบบโครงข่าย ที่จะใช้ในการทำโครงงานเรื่อง โครงข่ายประสิทธิภาพสูงสำหรับกลุ่มการวิจัยการสื่อสารไร้สาย ซึ่งประกอบไปด้วย

1. ไฟร์วอลล์จะทำหน้าที่ในการรักษาความปลอดภัยให้กับโครงข่าย ในการผ่านเข้า-ออกจากโครงข่าย

2. DHCP ทำหน้าที่ในการกำหนดไอพีแอดเดรสโดยอัตโนมัติให้แก่เครื่องไคลเอนต์ที่อยู่ในระบบ

3. DNS Server (Domain Name System) จะทำหน้าที่ในการแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปแบบของโดเมนเนม (Domain Name) หรือแปลงกลับจากโดเมนเนมไปเป็น ไอพีแอดเดรส

4. NAT (Network Address Translation) เป็นวิธีหนึ่งในการแปลงและแปลหมายเลขไอพีแอดเดรสของโครงข่ายภายในให้เป็นหมายเลขไอพีแอดเดรสสากลซึ่งเป็นที่ยอมรับในระบบการสื่อสารบนอินเตอร์เน็ต

5. IPtables เป็นโปรแกรมที่ใช้ในการควบคุมกฎในการผ่านเข้า-ออกของแพ็กเก็ตข้อมูล ซึ่งในที่นี้จะจัดเป็นส่วนหนึ่งในไฟร์วอลล์เพื่อเพิ่มเสถียรภาพและความปลอดภัยให้แก่ระบบโครงข่าย

6. Web Server ได้มีการจัดทำและอัพโหลดโฮมเพจ (home page) และแอพพลิเคชั่นต่างๆ โดยใช้ Professional Home Pages (PHP) ในการติดต่อระหว่างฝั่งเซิร์ฟเวอร์และไคลเอนต์

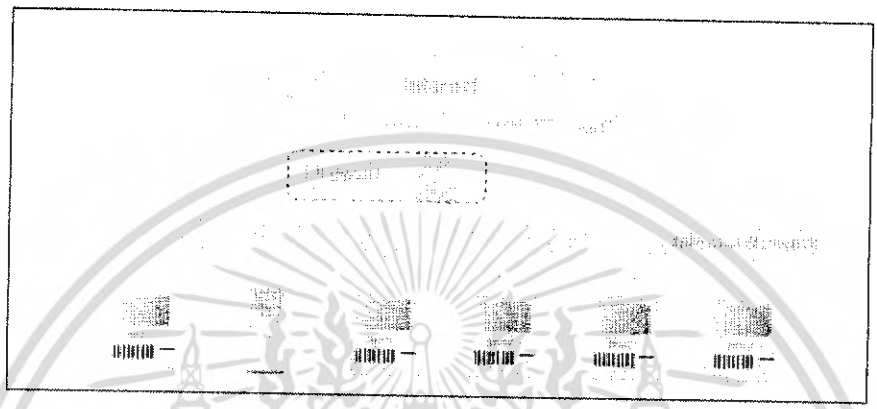
7. Mail Server ใช้ในการรับส่ง E-mail ในระบบโครงข่ายอินเทอร์เน็ต

8. FTP Server เป็นการถ่ายโอนแฟ้มข้อมูลระหว่างเครื่องคอมพิวเตอร์ 2 เครื่องที่อยู่ในระบบโครงข่าย

2.2 ไฟร์วอลล์ (Firewall)

ในความหมายทางด้านการก่อสร้างแล้วไฟร์วอลล์ จะหมายถึง กำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ส่วนทางด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆ กันก็คือ เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเทอร์เน็ตหรือเน็ตเวิร์คภายนอกนั่นเอง

ไฟร์วอลล์เป็นส่วนประกอบที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเน็ตเวิร์คภายนอกหรือเน็ตเวิร์คที่เราคิดว่าไม่ปลอดภัย กับเน็ตเวิร์คภายในหรือเน็ตเวิร์คที่เราต้องการจะป้องกัน โดยที่ส่วนประกอบนั้นอาจจะเป็นเราท์เตอร์คอมพิวเตอร์หรือเน็ตเวิร์คประกอบกันก็ได้ ขึ้นอยู่กับวิธีการหรือสถาปัตยกรรมไฟร์วอลล์ที่ใช้ ดังรูปที่ 2.1



รูปที่ 2.1 ไฟร์วอลล์กั้นระหว่างอินเทอร์เน็ตกับเน็ตเวิร์คภายใน

สิ่งที่ไฟร์วอลล์ช่วยได้

- บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้เซอร์วิสชนิดใด
- ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเน็ตเวิร์คภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของเน็ตเวิร์ค (Network-based Security)
- บันทึกข้อมูล กิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์คได้อย่างมีประสิทธิภาพ
- ป้องกันเน็ตเวิร์คบางส่วนจากการเข้าถึงของเน็ตเวิร์คภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้เซอร์วิส (เช่นถ้ามี Web Server) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามากรณีเช่นนี้ เราสามารถใช้ไฟร์วอลล์ช่วยได้
- ไฟร์วอลล์บางชนิด สามารถป้องกันไวรัสได้ โดยจะทำการตรวจไฟล์ที่โอนย้ายผ่านทางโปรโตคอล HTTP, FTP และ SMTP

อะไรที่ไฟร์วอลล์ช่วยไม่ได้

ถึงแม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความปลอดภัยให้กับเน็ตเวิร์คได้มากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่สิ่งเหล่านี้ไม่สามารถป้องกันได้จากการใช้ไฟร์วอลล์

- อันตรายที่เกิดจากเน็ตเวิร์คภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเน็ตเวิร์คเองไม่ได้ผ่านไฟร์วอลล์เข้ามา
- อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์ เช่น การ Dial-up เข้ามายังเน็ตเวิร์คภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์
- อันตรายจากวิธีใหม่ ๆ ที่เกิดขึ้น ทุกวันนี้มีการพบช่องทางใหม่ ๆ เกิดขึ้นทุกวัน เราไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วคิดว่าปลอดภัยตลอดไปดังนั้นต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ
- ไวรัสถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆ โปรโตคอล

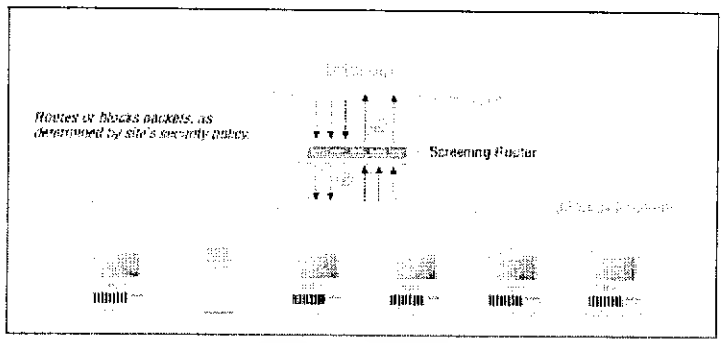
2.2.1 ชนิดและรูปแบบการทำงานของไฟร์วอลล์

ชนิดของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

- Packet Filtering
- Proxy Service
- Stateful Inspection

Packet Filter

Packet Filter คือเราท์เตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้ดังรูปที่ 2.2 ซึ่งเปรียบเสมือนว่าเป็นตัวกรองแพ็กเก็ต



รูปที่ 2.2 ใช้ Screening Router ทำหน้าที่ Packet Filtering

ซึ่งพอร์ตของทรานสปอร์ตเลเยอร์คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชั่นที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP, พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อ Packet Filter พิจารณาเฮดเดอร์ จึงทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ต หรือ ชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเน็ตเวิร์ค 203.154.207.0/24 , ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเน็ตเวิร์ค 203.154.207.0/24 ผ่านเราท์เตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น

Packet Filtering สามารถอิมพลีเมนต์ได้จาก 2 แพล็ตฟอร์ม คือ

- เราท์เตอร์ที่มีความสามารถในการทำ Packet Filtering (ซึ่งมีในเราท์เตอร์ส่วนใหญ่อยู่แล้ว
- คอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์

ซึ่งจะมีข้อดีและข้อเสียดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 เปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์ Packet Filtering

	ข้อดี	ข้อเสีย
เราท์เตอร์	ประสิทธิภาพสูงมีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลาง จำนวนอินเตอร์เฟสน้อย อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ข้อดี- ข้อเสียของ Packet Filtering

ข้อดี

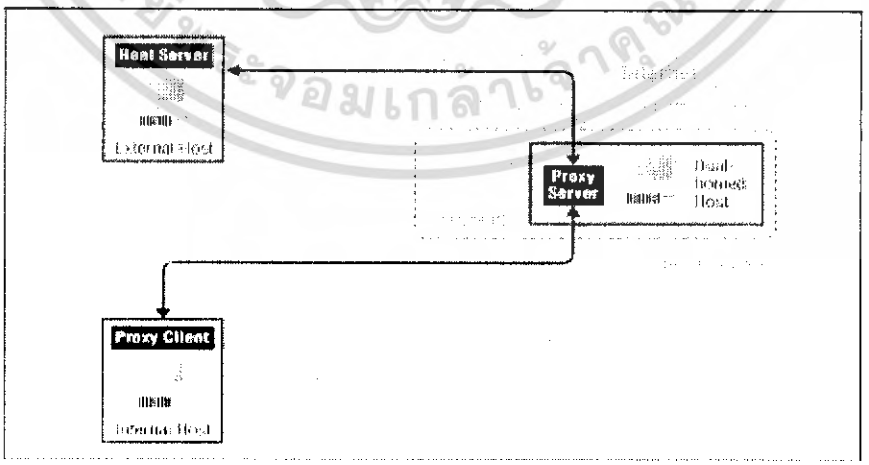
- ไม่ขึ้นกับแอพพลิเคชั่น
- มีความเร็วสูง
- รองรับการขยายตัวได้ดี

ข้อเสีย

- บางโปรโตคอลไม่เหมาะสมกับการใช้ Packet Filtering เช่น FTP, ICQ

Proxy

Proxy หรือ Application Gateway เป็นแอพพลิเคชั่นโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ค 2 เน็ตเวิร์ค ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์คโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์คภายในและภายนอก Proxy จะช่วยเพิ่มความปลอดภัยได้มากเนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชั่นเลเยอร์ เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยัง Proxy ก่อน ไคลเอนต์จะเจรจา กับ Proxy เพื่อให้ Proxy ติดต่อไปยังเครื่องปลายทางให้ เมื่อ Proxy ติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ (connection) 2 การเชื่อมต่อ คือ ไคลเอนต์กับ Proxy และ Proxy กับเครื่องปลายทาง ทั้งนี้ Proxy จะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่ดังรูปที่ 2.3



รูปที่ 2.3 ใช้ Dual-homed Host เป็น Proxy Server

ข้อดี-ข้อเสียของ Proxy

ข้อดี

- มีความปลอดภัยสูง
- รู้จักข้อมูลในระดับแอพพลิเคชั่น

ข้อเสีย

- ประสิทธิภาพต่ำ
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

Stateful Inspection Technology

โดยปกติแล้ว Packet Filtering แบบธรรมดา จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละแพ็กเก็ต นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น ดังนั้น Packet Filtering แบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือไม่ หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

Stateful Inspection เป็นเทคโนโลยีที่เพิ่มเข้าไปใน Packet Filtering โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว Stateful Inspection จะนำเอาส่วนข้อมูลของแพ็กเก็ต (message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้ นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

ตัวอย่างผลิตภัณฑ์ทางการค้าที่ใช้ Stateful Inspection Technology ได้แก่

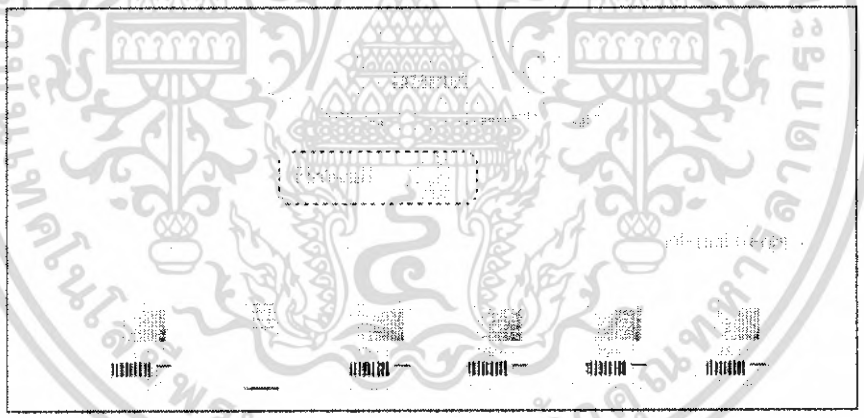
- Check Point Firewall-1
- Cisco Secure Pix Firewall
- SunScreen Secure Net

2.2.2 Firewall Architecture (สถาปัตยกรรมไฟร์วอลล์)

ในส่วนของสถาปัตยกรรมไฟร์วอลล์นั้น จะพูดถึงการจัดวางส่วนประกอบไฟร์วอลล์ในแบบต่างๆ เพื่อทำให้เกิดเป็นระบบไฟร์วอลล์ขึ้น

2.2.2.1 Single Box Architecture

Single Box Architecture เป็นสถาปัตยกรรมแบบง่ายๆ ที่มีส่วนประกอบทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเน็ตเวิร์คภายในกับเน็ตเวิร์คภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูลทำให้ดูแลได้ง่ายเป็นจุดสนใจในการดูแลความปลอดภัยเน็ตเวิร์ค ในทางกลับกันข้อเสียของวิธีนี้ก็คือ การที่มีเพียงจุดเดียวนี้ทำให้มีความเสี่ยงสูงหากมีการกำหนดผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อยการผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้



รูปที่ 2.4 Firewall Architecture แบบชั้นเดียว

คอมโพเน็นต์ที่ใช้ในสถาปัตยกรรมนี้อาจเป็น Screening Router , Dual-Homed Host หรือ Multi-purposed Firewall Box ก็ได้

- **Screening Router**

Screening Router เป็นการใช้เราท์เตอร์ทำ Packet Filtering ได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่ายเนื่องจากส่วนใหญ่จะใช้เราท์เตอร์ต่อกับเน็ตเวิร์คภายนอกอยู่แล้ว แต่วิธีนี้อาจไม่ยืดหยุ่นมากนักในการกำหนดค่าสถาปัตยกรรมแบบนี้เหมาะสำหรับ

  - เน็ตเวิร์คที่มีการป้องกันความปลอดภัยในระดับของโฮสต์ (Host security) เป็นอย่างดีแล้ว
  - มีการใช้โปรโตคอลไม่มาก และโปรโตคอลที่ใช้ก็เป็นโปรโตคอลที่ไม่ซับซ้อน
  - ต้องการไฟร์วอลล์ที่มีความเร็วสูง

- **Dual-Homed Host**

Dual-Homed Host (คอมพิวเตอร์ที่มีเน็ตเวิร์คอินเตอร์เฟสอย่างน้อย 2 อัน) ใช้การบริการเป็น Proxy ให้กับเครื่องภายในเน็ตเวิร์คสถาปัตยกรรมแบบนี้เหมาะสำหรับเน็ตเวิร์คที่มีการใช้งานอินเทอร์เน็ตค่อนข้างน้อยและ เน็ตเวิร์คที่ไม่ได้มีข้อมูลสำคัญๆ

2.2.2.2 Multi-purposed Firewall Box

มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆ เดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้ง Packet Filtering, Proxy แต่ก็อย่าลืมว่านี่คือสถาปัตยกรรมแบบชั้นเดียวซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งเน็ตเวิร์คได้

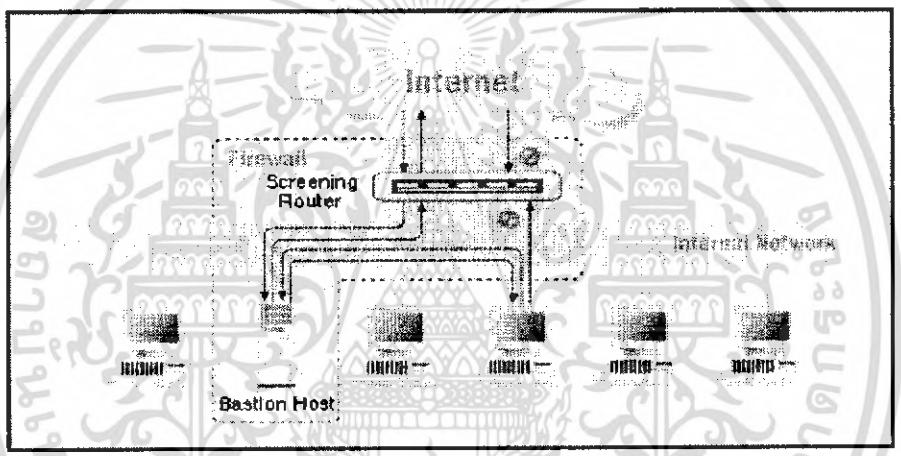
- **Screened Host Architecture**

Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการ Proxy เหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่า โฮสต์นั้นจะอยู่ภายในเน็ตเวิร์ค ไม่ต่ออยู่กับเน็ตเวิร์คภายนอกอื่น ๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้ Dual Homed Host) และจะมี เราท์เตอร์ที่ทำหน้าที่ Packet Filtering ช่วยบังคับให้เครื่องภายในเน็ตเวิร์คต้องติดต่อเซอร์วิสผ่าน Proxy โดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะ Bastion host (คือโฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเทอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ) เท่านั้น ในสถาปัตยกรรมแบบนี้จะประกอบไปด้วยเราท์เตอร์ทำ

หน้าที่ Packet Filtering และภายในเน็ตเวิร์คจะมี Bastion Host ให้บริการ Proxy อยู่ โดยที่เราท์เตอร์นั้นอาจจะถูกกำหนดค่าดังนี้

- อาจจะอนุญาตให้เครื่องภายในใช้เซอร์วิสบางอย่างได้โดยตรง
- ส่วนเซอร์วิสอื่นๆ จะไม่ยอมให้เครื่องภายในติดต่อผ่านออกไปโดยตรง ยกเว้น Bastion Host เท่านั้นที่สามารถติดต่อกับเน็ตเวิร์คภายนอกได้ทั้งนี้เพื่อเป็นการบังคับให้ใช้บริการ Proxy ผ่านทาง Bastion Host เท่านั้น

หรืออาจจะเซ็ตให้เซอร์วิสส่วนใหญ่ผ่านเราท์เตอร์ออกไปได้โดยตรงแล้ว ให้บางส่วนต้องใช้เซอร์วิสผ่าน Proxy ก็แล้วแต่นโยบายและความเหมาะสมขององค์กร



รูปที่ 2.5 Screened Host Architecture

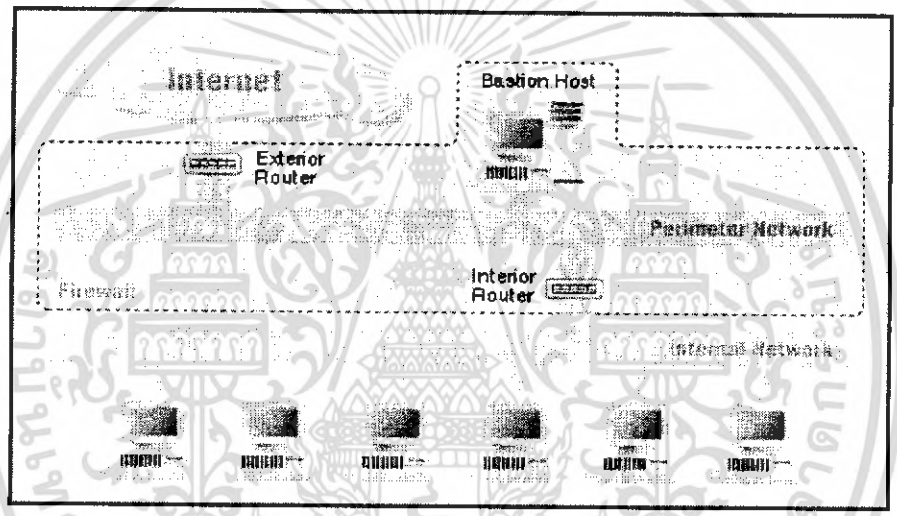
จากรูปที่ 2.5 จะเห็นว่าวิธีนี้ถึงแม้ว่าจะมีทั้ง Proxy และเราท์เตอร์ทำหน้าที่ Packet Filtering แต่ก็ยังคงอันตรายอยู่ เพราะว่าเราท์เตอร์ต้องยอมให้ภายนอกสามารถติดต่อกับ Bastion Host ได้อยู่แล้ว หากแฮกเกอร์สามารถเจาะเข้ามายัง Bastion Host ได้ก็เสร็จ

สถาปัตยกรรมนี้เหมาะสำหรับ

- เน็ตเวิร์คที่มีการติดต่อกับเน็ตเวิร์คภายนอกน้อย
- เน็ตเวิร์คที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดีแล้ว

ในสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากส่วนประกอบหลายๆส่วนทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลด

ความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้นหากในชั้นแรกถูกเจาะก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่นๆ ในการป้องกันอันตรายและยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกัน เพื่อให้เกิดความหลากหลายเป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรมแบบหลายชั้นจะเป็นการต่อกันเป็นซีรี่โดยมี Perimeter Network อยู่ตรงกลาง เรียกว่า Screened Subnet Architecture ดังแสดงในรูปที่ 2.6



รูปที่ 2.6 Screened Subnet Architecture

- **Screened Subnet Architecture**

Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่ม Perimeter Network เข้าไปกั้นระหว่างอินเทอร์เน็ตกับเน็ตเวิร์คภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เน็ตเวิร์คภายในมีความปลอดภัยมากขึ้นในรูปที่ 2.6 แสดง Screened Subnet Architecture อย่างง่ายประกอบไปด้วยเราท์เตอร์ 2 ตัวตัวหนึ่งอยู่ระหว่างอินเทอร์เน็ตกับ Perimeter Network ส่วนอีกตัวหนึ่งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์คภายในถ้าหากแฮกเกอร์จะเจาะเน็ตเวิร์คภายในต้องผ่านเราท์เตอร์เข้ามาถึง 2 ตัวด้วยกันถึงแม้ว่าจะเจาะชั้นแรกเข้ามายัง Bastion host ได้แต่ก็ยังต้องผ่านเราท์เตอร์ตัวในอีกถึงจะเข้ามายังเน็ตเวิร์คภายในได้

- Perimeter Network เป็นเน็ตเวิร์คที่เพิ่มเข้ามาเพื่อความปลอดภัยอยู่ระหว่างเน็ตเวิร์คภายนอกกับเน็ตเวิร์คภายในประโยชน์ของ Perimeter Network ที่เห็นได้ชัดก็คือ การแบ่งเน็ตเวิร์คออกเป็นส่วนๆ ทำให้การไหลของข้อมูลถูกแบ่งออกเป็นส่วนๆตามเน็ตเวิร์คด้วย เนื่องจากโดยทั่วไปแล้ว เน็ตเวิร์คที่เป็นแลนนั้นจะเป็นแบบ Ethernet ซึ่งจะมีการส่งข้อมูลแบบ Broadcast ดังนั้นถ้ามีใครคอยดักจับข้อมูลอยู่ในเน็ตเวิร์คนั้นก็จะได้พาสเวิร์ดข้อมูลต่างๆ ไปหมด ดังนั้นหากไฟร์วอลล์เรามีชั้นเดียวและแฮกเกอร์สามารถเข้ามาได้ โดนดักจับข้อมูลก็เสร็จหมด แต่ถ้าเรามี Perimeter Network ถึงจะดักจับข้อมูลได้แต่ก็จะได้เพียงที่อยู่บน Perimeter Network เท่านั้น
- Bastion Host ตั้งอยู่บน Perimeter Network ทำหน้าที่ให้บริการ Proxy กับเน็ตเวิร์คภายในและให้บริการต่างๆ กับผู้ใช้บนอินเทอร์เน็ต Bastion Host นั้นจะมีความเสี่ยงต่อการโจมตีสูง จึงต้องมีการดูแลความปลอดภัยเป็นพิเศษ
- Interior Router ตั้งอยู่ระหว่าง Perimeter Network กับเน็ตเวิร์คภายใน ทำหน้าที่ Packet Filtering ป้องกันเน็ตเวิร์คภายในจาก Perimeter Network ในการตั้งค่าระหว่างเน็ตเวิร์คภายในกับ Perimeter Network ควรกำหนดอย่างรอบคอบอนุญาตเฉพาะเซอร์วิสที่จำเป็นเท่านั้นอย่างเช่น DNS, SMTP
- Exterior Router ตั้งอยู่ระหว่างเน็ตเวิร์คภายนอกกับ Perimeter Network เนื่องจาก Exterior Router นี้เป็นจุดที่ต่ออยู่กับเน็ตเวิร์คภายนอกจึงมีหน้าที่ที่สำคัญอย่างหนึ่งคือการป้องกันแพ็กเก็ตที่มีการ Forged IP Address เข้ามา โดยอ้างว่ามาจากเน็ตเวิร์คภายในทั้งๆ ที่จริงๆ แล้วมาจากเน็ตเวิร์คภายนอก

2.3 DHCP (Dynamic Host Configuration Protocol)

DHCP เป็นเน็ตเวิร์ค Protocol อันหนึ่งที่เมื่อติดตั้งบน Server (เรียกว่า DHCP Server) แล้วจะทำให้ Server นั้นมีความสามารถในการจัดสรรหรือจ่าย ไอพีแอดเดรส เป็นแบบอัตโนมัติให้กับเครื่องคอมพิวเตอร์ (Client) ที่มี TCP/IP stack software ซึ่ง DHCP จะกำหนดไอพีแอดเดรสเป็นแบบไดนามิกจากช่วงหรือ scope ที่ถูกกำหนดบน Server ให้กับโครงข่ายเครื่องคอมพิวเตอร์เครื่องลูก (Client computer) ที่ถูกตั้งค่าให้มีการกำหนดไอพีแอดเดรสด้วยการรับค่าจาก DHCP Server ก็ไม่ต้องมีการกำหนดไอพีแอดเดรสเป็นแบบ Static ซึ่งการกำหนดไอพีแอดเดรสมาจาก DHCP Server ยังรวมถึง Default Gateway, DNS Server และ WIN Server ด้วย นั่นคือค่า ไอพีแอดเดรส, Default Gateway, DNS Server, และ WIN Server ของเครื่องไคล์เอนต์จะถูกจ่ายมาจาก DHCP Server ทั้งหมด (ค่าบางค่าอาจจะไม่ถูกตั้งค่าให้จ่ายได้)

2.3.1 การจัดสรร TCP/IP Address โดยใช้ DHCP

จะมีขึ้นเมื่อระบบเริ่มทำงานซึ่งโดยทั่วไปแล้วจะมีขั้นตอนของการทำงานเป็นดังนี้

- เครื่องไคลเอนต์ทำการหาตำแหน่งที่อยู่ของ DHCP Server บนระบบโครงข่ายโดยการส่งข่าวสาร DHCP Discover ออกไปโครงข่ายเพื่อร้องขอไอพีแอดเดรส
- เครื่อง DHCP Server ทำการค้นหาไอพีแอดเดรสจากฐานข้อมูลในเครื่องเพื่อไม่ให้ซ้ำกัน และส่งข่าวสาร DHCP Offer กลับไปให้เครื่องไคลเอนต์ที่ร้องขอ
- เมื่อเครื่องไคลเอนต์ได้รับหมายเลขไอพีแอดเดรสเรียบร้อยแล้ว ไคลเอนต์จะส่งสัญญาณตอบกลับ DHCP Request มาให้ทราบ
- เครื่อง DHCP Server จะส่งสัญญาณ DHCP Ack กลับไปยังเครื่องไคลเอนต์เพื่อให้เริ่มใช้งาน (และเซิร์ฟเวอร์ DHCP จะเก็บหมายเลขไอพีแอดเดรส นั้นเอาไว้ไม่ให้เครื่องอื่นใช้ซ้ำ)

2.3.2 การกำหนดหมายเลขไอพีแอดเดรส

สามารถนำค่าที่กำหนดจากการวางแผนมาใช้ในการกำหนดในเครื่อง หรือโฮสต์ได้ ซึ่งค่าที่กำหนดสามารถกำหนดด้วย Manual หรือ Automatic

การกำหนดด้วย Manual ทำโดยไปกำหนดที่ Internet Protocol (TCP/IP) ในเน็ตเวิร์ค Card และต้องไม่ซ้ำกัน ในองค์กรใหญ่ต้องมีการกำหนดรายการในเครื่องแต่ละเครื่องตายตัว หรือมีเลเบลติดเพื่อไม่ให้มีปัญหากำหนดหมายเลขชนกัน การกำหนดอัตโนมัติก็จำเป็นต้องมี DHCP Server ซึ่งติดตั้งและกำหนดสโคปที่ต้องการใน Active Directory ต้องมีการ Authorized ด้วย

การกำหนดของ DHCP สามารถที่กำหนดจองได้สามแบบดังนี้

- จองแบบไดนามิก คือลูกข่ายมีรอบเวลาที่กำหนดขอต่ออายุในไอพีแอดเดรส
- จองแบบอัตโนมัติมีการกำหนดให้หมายเลขที่ถาวรไม่ต้องกำหนดเปลี่ยนไปเรื่อยๆ ใช้กับเครื่องที่ไม่เคลื่อนย้ายบ่อย
- จองแบบตายตัวหรือกำหนดตามเครื่อง เป็นการระบุค่าที่แน่นอนหรือเรียกว่า Reservations ใช้กับ Web Server หรือค่าที่ต้องการหมายเลขตายตัว

2.3.3 การวางแผน DHCP

เราสามารถที่กำหนดค่าต่างๆได้โดยใช้ DHCP ทั้ง ไอพีแอดเดรส, Subnet Mask หรือ DHCP Options ต่าง ๆ นอกจากการแจกค่าต่าง ๆ แล้ว DHCP Server สามารถแจกหมายเลขข้าม

โครงข่ายได้ด้วยเพียงต้องมี DHCP Relay agent หรือเราท์เตอร์สามารถผ่าน BOOTP ได้ซึ่งเรียกว่า Multiple Networks กับหนึ่ง DHCP Server

DHCP Relay Agent เป็นเครื่องที่ทำหน้าที่ลงทะเบียนแทน DHCP Server โดย DHCP Client ติดต่อผ่านแล้วนำค่าที่ติดต่อร้องขอไปขอใน DHCP Server จริงซึ่งในการกำหนดต้องระบุ DHCP Server ที่ร้องขอด้วยโดยไม่จำเป็นต้องนำมาจาก DHCP Server เดียว (ออกแบบตามกฎ 80/20 ได้) เพื่อ Fault tolerance

2.3.4 ข้อดีของ DHCP Server

การตั้งค่าคอมพิวเตอร์ด้วยการกำหนดไอพีแอดเดรสแบบ Static ในกรณีที่ไม่สามารถขอ IP จาก Administrator ได้จะมีข้อเสียคือไม่รู้ว่าจะใช้หมายเลขไอพีแอดเดรสเป็นอะไรเพราะกลัวจะไปชนกับ IP ที่มีอยู่แล้วหลายคนพยายามจะ Ping ดูก่อนเพื่อหา IP ที่ว่างจากการใช้งานซึ่งถ้าเครื่องทุกเครื่องเปิดใช้งานหมดก็โชคดีไปแต่ถ้ายังมีบางเครื่องที่ยังไม่เปิดเครื่องใช้งานก็อาจจะเป็นไปได้ที่จะทำให้เกิดการตั้งค่า IP ที่ตรงกันวิธีการแก้ไขปัญหาที่ค่อนข้างได้ผลดีก็คือการตั้งค่าไอพีแอดเดรสให้เป็นแบบรับค่ามาจาก DHCP Server ซึ่งจะได้ค่าของไอพีแอดเดรสที่จะไม่ไปชนกับเครื่องอื่น ๆ แน่นอนเพราะการจัดสรร IP ของ DHCP Server จะไม่ปล่อย IP ที่ซ้ำกันออกไป

2.4 DNS Server (Domain Name System)

บนโครงข่ายอินเทอร์เน็ตที่มีการเชื่อมโยงจากผู้คนมากมายเข้าด้วยกัน จะมีหน่วยงาน InterNIC (Inter Network Information Center) เป็นผู้ดูแลเกี่ยวกับการจดทะเบียนเน็ตเวิร์คหรือโดเมนที่มีการเชื่อมต่อกับอินเทอร์เน็ต โดยจะดูแลรายชื่อและหมายเลขไอพีแอดเดรสทั้งหมดทุกเครื่องจะต้องเชื่อมต่อผ่านโปรโตคอล TCP/IP ซึ่งต้องใช้ไอพีแอดเดรสในการอ้างถึง เช่น การเข้าสู่ Web Server ถ้า Web Server มีไอพีแอดเดรสเป็น 203.247.62.173 จะต้องใช้หมายเลขนี้ในการติดต่อ แต่เนื่องจากไอพีแอดเดรสของเซิร์ฟเวอร์นั้นมีอยู่หลายหมายเลขเป็นเรื่องยากในการจดจำตัวเลขว่าเป็นเซิร์ฟเวอร์หรือเว็บไซต์ใดจึงมีการกำหนดมาตรฐานระบบชื่อโดเมนหรือ DNS มาใช้

DNS เป็นระบบแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปแบบของโดเมนเนม หรือ แปลงกลับจากโดเมนเนมเป็นไอพีแอดเดรสได้ หลังจากได้จดทะเบียนชื่อโดเมนเนมผ่าน ISP จะใช้เวลาประมาณสองวันในการกระจายชื่อโดเมนนี้ไปทั่วโลก ในการตั้งชื่อโดเมนส่วนมากจะใช้ชื่อหน่วยงาน บริษัท หรือ สถานศึกษาเพื่อให้ง่ายต่อการจดจำมาตรฐานระบบ DNS ประกอบไปด้วยชื่อโครงข่าย ชื่อสับโดเมน และชื่อโดเมน เช่น ไอพีแอดเดรส

2.5 NAT (Network Address Translation)

NAT เป็นวิธีการหนึ่งในการแปลงและแปลไอพีแอดเดรสของโครงข่ายภายในให้เป็นไอพีแอดเดรสซึ่งเป็นที่ยอมรับและสื่อสารบนอินเทอร์เน็ต

NAT มีข้อดีหลายอย่าง เช่น สามารถใช้ไอพีแอดเดรสที่ตั้งขึ้นมาเองได้ (ซึ่งเป็นไอพีแอดเดรสที่ไม่ต้องจดทะเบียนบนอินเทอร์เน็ต) เพียงแต่ใช้ไอพีแอดเดรสที่ผู้ให้บริการอินเทอร์เน็ตให้มาก็พออีกทั้งยังสามารถซ่อนไอพีแอดเดรสที่อยู่ในโครงข่ายได้ ทำให้มีความปลอดภัย รวมทั้งไม่จำเป็นต้องอ้างไอพีแอดเดรสซ้ำๆ อีกเมื่อต้องการติดต่อกับอินเทอร์เน็ต หรือโครงข่ายขององค์กร อย่างไรก็ดีการใช้ NAT ไม่ใช่ทางเลือกการเชื่อมต่อที่ดีที่สุด

การใช้ NAT เพื่อจุดมุ่งหมายขั้นพื้นฐาน มีดังนี้

- NAT สามารถซ่อนไอพีแอดเดรสของโครงข่ายภายในองค์กรด้วยจุดประสงค์เพื่อรักษาความปลอดภัยเมื่อบุคคลภายนอกไม่สามารถล่วงรู้ IP จริงภายใน ก็ย่อมมีความปลอดภัยมากขึ้น
- หากมีโครงข่ายภายในที่มีการตั้งค่าให้ใช้ ไอพีแอดเดรสที่ไม่ได้จดทะเบียนให้ใช้บนอินเทอร์เน็ต หรือจาก ISP การใช้ NAT จะช่วยให้การเชื่อมต่อโครงข่ายภายในองค์กรกับอินเทอร์เน็ตซึ่งถือว่าเป็นโครงข่ายสาธารณะนั้นมีความปลอดภัยเนื่องจาก NAT จะทำการแปลงไอพีแอดเดรสของโครงข่ายในองค์กรให้ใช้ไอพีแอดเดรสที่จดทะเบียนถูกต้องบนอินเทอร์เน็ตเสียก่อนที่จะส่งข้อมูลข่าวสารออกไปที่ อินเทอร์เน็ต
- คอมพิวเตอร์ภายในองค์กรที่ได้รับการจัดตั้งไอพีแอดเดรสแบบ Static NAT (เช่น Mail Servers เป็นต้น) สามารถที่จะถูกแปลแอดเดรสเมื่อติดต่อกับภายนอกโดยไม่ต้องมีการ Update ข้อมูลบันทึกบน NAT

- **การทำงานของ NAT**

NAT เป็นระบบการ Interface กับอินเทอร์เน็ตที่ไม่ขึ้นอยู่กับโปรโตคอล และแอพพลิเคชั่นรวมทั้งอุปกรณ์ Hardware ใดๆ ซึ่งหมายความว่า NAT สามารถถูกนำมาประยุกต์ใช้งานกับเราท์เตอร์หรือคอมพิวเตอร์ที่ทำหน้าที่เป็นเราท์เตอร์ใดๆ ที่มีลักษณะการเชื่อมต่อโดยมีด้านหนึ่งสำหรับโครงข่ายภายในและอีกด้านหนึ่งกับโครงข่ายภายนอกดังเช่นอินเทอร์เน็ต ตัวอย่างการเชื่อมต่อ เช่น ก ารติดตั้ง NAT ที่ Border เราท์เตอร์ซึ่งเป็นเราท์เตอร์ที่เชื่อมต่อโครงข่ายย่อย ๆ ต่าง ๆ ภายในองค์กรกับโครงข่ายภายนอก

NAT สามารถทำงานได้ในรูปแบบ 2 ทาง หรือการเชื่อมต่อสื่อสารทั้งในแบบ Inbound และ Outbound หมายความว่า สามารถจัดการกับไอพีแอดเดรสที่วิ่งเข้ามา หรือไอพีแอดเดรสที่วิ่งออกไป โดยสามารถจัดการกับไอพีแอดเดรสต้นทางและปลายทางได้เป็นอย่างดี NAT สามารถทำงานในสถานการณ์ 3 ประการ ดังนี้

- ทำหน้าที่แปลงและแปลไอพีแอดเดรสต้นทางที่มาจากโครงข่ายภายใน
- ทำหน้าที่แปลงและแปลไอพีแอดเดรสต้นทางที่มาจากโครงข่ายภายนอก เช่น อินเทอร์เน็ต เป็นต้น
- ทำหน้าที่แปลงและแปลไอพีแอดเดรสปลายทางภายในโครงข่าย

แม้ว่า NAT สามารถใช้ กับไอพีแอดเดรสภายนอกก็ตาม แต่โดยทั่วไป NAT มีไว้เพื่อการแปลไอพีแอดเดรส ภายในโครงข่าย จุดประสงค์ก็เพื่อที่จะซ่อนไอพีแอดเดรสภายในโครงข่าย และ / หรือการแปลไอพีแอดเดรสที่ไม่ได้จดทะเบียนถูกต้อง (หรือ ไอพีแอดเดรสส่วนตัว) ไปใช้เป็นไอพีแอดเดรสที่จดทะเบียนถูกต้อง ที่สามารถวิ่งไปตามเส้นทางบนอินเทอร์เน็ต การที่จะให้ทำเช่นนี้ได้ จำเป็นต้องมีการจัดตั้งค่าที่ถูกต้องก่อนการใช้งานเสมอ

- **สามารถขจัดการเสียเวลาจากการอ้างแอดเดรสซ้ำซาก**

สมมติว่ามีโครงข่ายที่ประกอบด้วยไอพีแอดเดรสที่ไม่ได้จดทะเบียนถูกต้อง และต้องการให้โครงข่ายของท่านนี้เชื่อมต่อกับอินเทอร์เน็ต และหากต้องการให้แพ็กเก็ตจากโครงข่ายสามารถวิ่งบนอินเทอร์เน็ตได้ไอพีแอดเดรสที่เป็นต้นทางและปลายทางจะต้องได้รับการจดทะเบียนถูกต้องบนอินเทอร์เน็ตเสียก่อน ดังนั้น หากต้องการให้คอมพิวเตอร์เครื่องใดเครื่องหนึ่งรับและส่งข้อมูลผ่านอินเทอร์เน็ต จะต้องอ้างแอดเดรสทุกครั้ง ซึ่งไม่เพียงแต่ทำให้ต้องเสียเวลาและค่าใช้จ่ายยังจะต้องมีไอพีแอดเดรสที่ถูกต้องเป็นจำนวนมากเพื่อนำมาใช้

NAT จะช่วยให้สามารถใช้ไอพีแอดเดรสเดิมที่มีอยู่ ถึงแม้ไม่ได้จดทะเบียนถูกต้องก็ตาม เพียงแต่จะต้องมีไอพีแอดเดรสที่ถูกต้องจำนวนหนึ่งก็พอ ซึ่งไอพีแอดเดรสจำนวนน้อยนี้ สามารถนำไปใช้สร้างเป็นไอพีแอดเดรส Pool (ไอพีแอดเดรสที่คอมพิวเตอร์บนโครงข่ายนำมาแบ่งใช้งานร่วมกัน) ด้วยวิธีนี้ คอมพิวเตอร์ภายในโครงข่ายสามารถใช้ไอพีแอดเดรสที่ถูกต้องติดต่อกับอินเทอร์เน็ตได้ และการร้องขอเข้ามาเพื่อเชื่อมต่อกับคอมพิวเตอร์ในโครงข่ายจากภายนอก จะใช้ไอพีแอดเดรสของ NAT เป็นแอดเดรสปลายทาง ซึ่ง NAT จะทำการแปลและนำเอาไอพีแอดเดรสของ NAT ในแอดเดรส Pool นี้ไปเป็นไอพีแอดเดรสที่ใช้งานภายในโครงข่ายต่อไป

- **ขั้นตอนการทำงานของ NAT**

สิ่งที่ NAT ทำงาน ได้แก่การแปลไอพีแอดเดรสในลักษณะแบบฉบับที่เรียก ว่าหนึ่งต่อหนึ่ง หรือจำนวนมากต่อจำนวนมาก โดยไอพีแอดเดรสที่อยู่ภายในโครงข่ายจะถูก Map ให้เป็นไอพีแอดเดรสภายนอก หมายความว่าไอพีแอดเดรสภายในจะถูกแปลงเป็นไอพีแอดเดรสสำหรับการสื่อสารกับภายนอกที่เหมาะสม หรือในทางกลับกัน

ขั้นตอนในการแปลแอดเดรสมีดังนี้

- ไอพีแอดเดรสที่อยู่ใน IP Header จะถูกแทนที่ด้วยไอพีแอดเดรสจากภายนอก หรือภายใน (ขึ้นอยู่กับทิศทางการวิ่งของแพ็กเก็ต) และหมายเลขพอร์ตใน TCP หรือ UDP Header จะถูกเปลี่ยนเป็นเลขหมายพอร์ตอันใหม่ หากมีการกำหนดให้ NAT จะต้องทำการแปลหมายเลขพอร์ตด้วย
- ค่า Checksum สำหรับ IP Packet จะถูกคำนวณใหม่ และตรวจสอบเพื่อความถูกต้อง
- ที่ Header ของ TCP จะได้รับการคำนวณใหม่เช่นกัน หลังจากที่ได้รับการคำนวณมาแล้วก่อนหน้านี้ครั้งแรก จากเครื่องคอมพิวเตอร์ที่เป็นเจ้าของภายในโครงข่าย (หรือเจ้าของที่มาจากโครงข่ายภายนอก)

จากที่กล่าวมาแล้วจะเห็นได้ว่า NAT ทำหน้าที่แปลไอพีแอดเดรสของเครื่องต้นทางและเครื่องปลายทางขึ้นอยู่กับทิศทางของ Traffic ในการที่จะแปลงไอพีแอดเดรสนั้น NAT จะต้องตรวจสอบที่ช่องไอพีแอดเดรสของแพ็กเก็ตซึ่งแพ็กเก็ตในที่นี้ เราเรียกว่า IP Datagram โดยที่ IP Datagram เป็นรูปแบบของข่าวสารที่ใช้ห่อหุ้มข้อมูลและโปรโตคอลในระดับสูงที่ใช้จัดการขนถ่ายข้อมูลอย่างเช่น TCP โดยให้บริการขนถ่ายข้อมูลจาก User File จากเว็บเพจหรือข่าวสาร E- mail เป็นต้น

- **ชนิดของ NAT**

NAT มีอยู่ 2 ชนิดหลักๆ ได้แก่

- Static NAT
- Dynamic NAT

Static NAT

Static NAT เป็นการแปลไอพีแอดเดรสชนิดกำหนดค่าแอดเดรสตายตัวจากโครงข่ายภายในไปยังโครงข่ายภายนอก ส่วนแอดเดรสภายนอกจะไม่มีการเปลี่ยนแปลง ดังนั้นความสัมพันธ์ระหว่างไอพีแอดเดรสของโครงข่ายภายนอกและภายในจะเป็นแบบแน่นอนตายตัว

ข้อดีและข้อเสียของการใช้ Static NAT

แม้ Static NAT จะเป็นระบบที่เรียบง่ายและตรงไปตรงมาก็ตาม แต่ก็มีข้อเสียหลายประการ ที่ทำให้ Static NAT กลายเป็นระบบที่เหมาะสำหรับโครงข่ายที่มีข้อจำกัดมาก แต่ไม่เหมาะกับโครงข่ายขนาดใหญ่ ด้วยเหตุผลหลายประการดังนี้

- ต้องการการดูแลอย่างมาก การ Map แอดเดรสโดยวิธีการของ Static Map นี้ จะไม่มีการเปลี่ยนแปลงเลขหมายไอพีแอดเดรสโดยอัตโนมัติ หากมีการเปลี่ยนแปลงแอดเดรสภายในหรือภายนอกเกิดขึ้น เช่น หากต้องการเพิ่มหรือแก้ไขแอดเดรสใดๆแล้ว ผู้ดูแลโครงข่ายจะต้องเข้ามาจัดตั้งตารางการแปลแอดเดรสกันใหม่ ซึ่งจะทำให้เกิดความผิดพลาดขณะที่มีการจัดตั้งตารางการแปลแอดเดรส

- มีการใช้งานแอดเดรสอย่างมากในโครงข่ายขนาดใหญ่ การใช้แอดเดรสภายในและภายนอกแบบชนิดหนึ่งต่อหนึ่งนี้ ทำให้ใช้แอดเดรสภายนอกค่อนข้างมาก หากมีเครื่องคอมพิวเตอร์ภายในโครงข่ายเป็นจำนวนมากเพราะต้องกำหนด 1 เครื่องต่อหนึ่งไอพีแอดเดรสที่ถูกต้อง

- มีการเลือกเส้นทางที่แน่นอนตายตัว ในกรณีที่มีการเชื่อมต่อกับอินเทอร์เน็ตแบบหลายๆ Connection เช่น เชื่อมต่อพร้อมกันหลาย ISP เมื่อมีการใช้ Static NAT เกิดขึ้น ระบบนี้จะเลือกเส้นทางที่แน่นอนตายตัว ตามที่ Static NAT กำหนดไว้

ข้อเสียของ Static NAT คือไม่ได้หมายความว่า ระบบนี้ไม่เหมาะสมกับโครงข่ายสมัยใหม่ในปัจจุบัน แต่ Static NAT เหมาะสำหรับระบบโครงข่ายขนาดเล็กต่อไปนี้เป็นรายละเอียดที่แสดงถึงข้อดีของการใช้ Static NAT มีดังนี้

- จำกัดความต้องการใช้ NAT ภายในโครงข่ายที่ซึ่งมีการจำกัดจำนวนของ PC ที่ใช้ NAT ระบบ Static NAT ดูจะเป็นเครื่องมือที่มีประสิทธิภาพที่จะควบคุมการ Access ไปที่ภายนอก หมายความว่า การจำกัดจำนวนคอมพิวเตอร์ที่จะออกไปที่อินเทอร์เน็ต ทำได้โดยการจำกัดไอพีแอดเดรสสำหรับที่จะออกไปที่อินเทอร์เน็ตเท่านั้นเอง สำหรับโครงข่ายใดที่ส่วนใหญ่มีการสื่อสารเฉพาะภายใน และมีบางครั้งที่มี Access ไปที่ภายนอกบ้างเป็นจำนวนน้อย ระบบนี้จึงเป็นระบบที่ดีกว่า

- การบริหารจัดการโครงข่าย ปัจจุบันมีระบบโครงข่ายอยู่มากมายที่ต้องการบริหารจัดการกับ Traffic ภายนอก เพื่อต้องการดูว่ามีคอมพิวเตอร์เครื่องใดบ้างที่ติดต่อกับภายนอก ทั้งนี้ก็เพื่อให้ง่ายต่อการตรวจสอบที่มาของปัญหาว่ามาจากโครงข่ายภายในหรือภายนอก การใช้ Static NAT จะช่วยให้สามารถติดตามดูได้ว่า คอมพิวเตอร์แต่ละเครื่องมี Traffic ไปไหนมาไหนบ้าง

- สามารถเข้ากันได้แอพพลิเคชั่นโดยทั่วไปมีแอพพลิเคชั่นบางตัวที่ฝังไอพีแอดเดรสไว้ที่ช่องเก็บข้อมูลของ IP Datagram ซึ่งการทำเช่นนี้จะทำให้ NAT โดยทั่วไปไม่สามารถสังเกตเห็นแอดเดรสที่อยู่ในช่องนี้ ซึ่งหมายความว่าแอพพลิเคชั่นบางรายการไม่สามารถทำงานได้ตามปกติภายใต้ NAT แต่ Static NAT สามารถถูกจัดตั้งค่าให้ทำงานร่วมกับ Application Level Gateway เพื่อตรวจสอบ IP Datagram ดังกล่าวได้

Dynamic NAT

Dynamic NAT เป็นแบบตรงกันข้าม ที่มีการนำเอาไอพีแอดเดรสจากกลุ่มของไอพีแอดเดรส ที่แชร์หรือร่วมใช้งานกัน หรือที่เรียกว่าแอดเดรส Pool มาทำการแปลจากแอดเดรส Pool ภายใน ให้เป็นแอดเดรส Pool สำหรับโครงข่ายภายนอก หรือในทางกลับกัน รูปแบบนี้จะต้องได้รับการจัดตั้งค่าโดยผู้ดูแลระบบโครงข่าย แต่หลังจากที่จัดตั้งค่าเป็นที่เรียบร้อยแล้ว เราท์เตอร์ที่สนับสนุน NAT จะเป็นผู้จ่ายไอพีแอดเดรสให้กับคอมพิวเตอร์อย่างเหมาะสม และเพื่อให้เกิดความรวดเร็วในการทำงาน ผู้บริหารจัดการโครงข่ายจะต้องทำการ Map ระยะของไอพีแอดเดรสหากเป็นไปได้ ลักษณะนี้คล้ายๆกับการทำงานของ DHCP Server ที่ไม่ได้กำหนดเครื่องคอมพิวเตอร์แต่ละเครื่องให้มีไอพีแอดเดรสที่ตายตัว โดยผู้จัดการโครงข่ายจะกำหนดแอดเดรสขึ้นมาจำนวนหนึ่ง เป็นระยะหรือช่วงของแอดเดรส เช่น 192.80.20.15 - 192.80.20.50 เป็นต้น ดังนั้นใครที่เข้ามาที่โครงข่ายก่อนก็จะได้รับแจกแอดเดรสไปใช้งานก่อน โดยเครื่องคอมพิวเตอร์จะไม่ได้รับ IP ที่ซ้ำกัน ข้อแตกต่างกันระหว่าง NAT กับ DHCP Server ตรงที่ไอพีแอดเดรสของ NAT เป็นไอพีแอดเดรสที่ได้รับการจดทะเบียนแล้ว เพื่อแจกให้กับเครื่องคอมพิวเตอร์ที่เข้าและออกบนโครงข่ายไปยังภายนอก

หาก Static NAT เป็นส่วนที่เรียกว่า หัวในเหรียญบาท ดังนั้น Dynamic NAT ก็จะถือได้ว่าเป็นส่วนก้อยของเหรียญบาท เช่นกัน ตรงที่ว่า Dynamic NAT มีการกำหนดแอดเดรสให้กับภายนอกแบบพลวัตร หมายความว่า แทนที่จะใช้ระบบกำหนดแอดเดรสภายในกับภายนอกแบบหนึ่งต่อหนึ่ง Dynamic NAT จะกำหนดว่าแอดเดรสที่ใช้จะเปลี่ยนแปลงไปเรื่อยๆ และจะมีการเปลี่ยนแปลงทุกครั้งที่คอมพิวเตอร์ภายในโครงข่ายมีการสถาปนาการเชื่อมต่อกับคอมพิวเตอร์ภายนอกโครงข่าย หรืออาจจะมีการเปลี่ยนเป็นระยะเวลาก็เป็นได้

ในเวลาเดียวกัน IP Datagram ที่มาจากคอมพิวเตอร์เครื่องที่สองบนโครงข่าย ที่ส่งข่าวสารไปที่โครงข่ายภายนอก จะได้รับการปฏิบัติในทำนองเดียวกันโดย NAT Router ตัวอย่าง เช่น NAT Router อาจแปล ไอพีแอดเดรส ต้นทาง ที่อยู่ใน IP Header ที่ติดต่อออกไปเพื่อต้องการใช้งาน FTP Application จากเครื่องคอมพิวเตอร์ที่ใช้แอดเดรส 192.168.10.4 ไปที่แอดเดรสต่อไปใน NAT

Address Pool ซึ่งประกอบด้วยแอดเดรสจำนวนหนึ่ง ซึ่งต่อมา NAT Router จะแปลแอดเดรส 192.168.10.4 ให้เป็น 192.112.36.3 ส่วน อีกเครื่องหนึ่งคือ 192.168.10.5 จะได้รับการแปลเป็น 192.112.36.2 หากเครื่องพีซีทั้งสองต้องการติดต่อกับโครงข่ายภายนอก

เมื่อคอมพิวเตอร์แต่ละเครื่องได้เสร็จสิ้นจากภารกิจในการสื่อสารข้อมูลกับโครงข่ายภายนอกแล้ว ตัว NAT Router ก็จะเรียกแอดเดรสภายนอกคืนกลับเข้าไปที่แอดเดรส Pool เพื่อให้ผู้อื่นใช้ต่อไป

Dynamic NAT พร้อมด้วย IP Overload

เป็นที่ทราบดีว่า Port Address Translation (PAT) สามารถทำการ Map บรรดาแอดเดรสต่างๆหลายแอดเดรสให้เป็นแอดเดรสเดียวที่เป็นแอดเดรสสำหรับติดต่อกับภายนอกและเนื่องจากการที่ PAT สามารถ Map แอดเดรสสำหรับเครือข่ายภายในหลาย ๆ แอดเดรสให้เป็นแอดเดรสเดียวนี่เอง จึงทำให้เลขหมายของพอร์ตที่ทำงานบน TCP หรือ UDP นั้น มีมากเพียงพอที่จะให้บริการโดยไม่เกิดปัญหาได้

ส่วนคำว่า "Overload" ในที่นี้ใช้ในสถานการณ์ ที่ไอพีแอดเดรสในแอดเดรส Pool มีไม่เพียงพอที่จะให้บริการ จึงต้องอาศัยพอร์ตเพื่อแยกความแตกต่างระหว่างการเชื่อมต่อเข้ามาทั้ง 2 Connection ซึ่งโดยทั่วไปหมายเลขของพอร์ตที่กำหนดให้ใช้งานคือ 1024 ถึง 4999 ซึ่งเท่ากับมีจำนวนพอร์ตใช้งานมากถึง 4000 พอร์ต

Dynamic NAT ที่มีการจัดตั้ง Redundant ที่ Interface ภายนอก

หากมีการเชื่อมต่อกับโครงข่ายภายนอก เช่น อินเทอร์เน็ต โดยทาง Interface ทั้งสอง เช่น การเชื่อมต่อผ่าน ISP 2 แห่งพร้อมกัน สามารถใช้ NAT เพื่อการแปลแอดเดรสภายในให้เป็นไอพีแอดเดรสภายนอก สำหรับการเชื่อมต่อกับ ISP ทั้งสองเพื่อออกอินเตอร์เน็ต โดย NAT จะสามารถใช้ไอพีแอตเดรสภายนอก 2 ชุดเพื่อสื่อสารผ่านทั้งสอง Interface และออกไปทางอินเทอร์เน็ตได้

2.6 IPTABLES

Iptables เป็นไฟร์วอลล์ประเภท Packet Filtering ที่พัฒนาโดยกลุ่ม Netfilter Project และยังสนับสนุนการทำ NAT (Network Address Translation) อีกด้วย Iptables ถูกนำมาใช้งานบน Linux 2.4 Kernel

รูปแบบคำสั่ง

iptables [table] <command> <match> <target/jump>

- **[table]** หมายถึง ตารางที่ต้องการระบุ เช่น Iptables -t nat หมายถึงให้ทำงานกับ nat table ในกรณีที่ไม่ได้ระบุตาราง Iptables จะถือว่าคำสั่งดังกล่าวระบุถึง filter table โดยอัตโนมัติ
- **<command>** จะเป็นตัวสั่งให้ Iptables ทำในสิ่งที่ต้องการ เช่น Iptables -A INPUT ซึ่งหมายถึงให้สร้างกฎต่อท้าย INPUT chain ใน filter table
- **<match>** เป็นส่วนที่ใช้ตรวจสอบว่าแพ็กเก็ตมีข้อมูลตรง (match) กับที่ระบุไว้หรือไม่ เช่น มี source ไอพีแอดเดรสเป็น 1.2.3.4
- **<target/jump>** เป็นตัวระบุว่าเมื่อเจอแพ็กเก็ตที่ match ก็จะกระทำ (action) ตามที่ระบุไว้ เช่น ถ้าแพ็กเก็ตใดมี source ไอพีแอดเดรสเป็น 1.2.3.4 ให้ DROP แพ็กเก็ตนั้นทิ้งไป

Table หมายถึง ตารางที่ต้องการจะใช้งาน โดยจะต้องใส่ Option table ลงไปแล้วตามด้วยตารางที่ต้องการ Iptables จะมีอยู่ 3 ตารางด้วยกันคือ

Filter เป็นตารางปริยายโดยจะระบุค่าของ built in chains เอาไว้ คือ INPUT, OUTPUT, FORWORD

Nat การแปลงไอพีแอดเดรสตามกระบวนการ Network Address Translation โดยจะมี built in chains อยู่ 3 ตัวคือ PREROUTER, POSTROUTER,OUTPUT

Mangle เป็นตารางที่ใช้สำหรับแพ็กเก็ตพิเศษ

Command หมายถึง คำสั่งที่สั่งให้ Iptables ทำงานตามต้องการ จะเป็นตัวอักษรย่อ

-A เพิ่มกฎใหม่ต่อท้าย chain (Append rule)

-D ลบกฎ (Delete rule)

-I เพิ่มกฎใหม่ใน chain (Insert rule)

-R แทนที่กฎเดิม ด้วยกฎใหม่ (Replace rule)

-L แสดงกฎทั้งหมดใน chain

-F ลบกฎทั้งหมดใน chain ทิ้ง

-Z ใช้ reset byte counter สำหรับทุกกฎใน chain ที่กำหนด

-N ใช้สร้าง chain ใหม่

-X ลบ chain ที่ไม่มีกฎซึ่งสามารถลบ user-defined chain ที่ไม่มีกฎได้ แต่ไม่สามารถลบ built-in chain ได้

-P เปลี่ยน default policy ของ chain ค่าที่ใช้ได้คือ ACCEPT, DROP ทั้งนี้ค่านี้มีความสำคัญอย่าง มากเพราะหากแพ็กเก็ต ถูกส่งเข้ามาใน chain แล้ว และไม่ match กับกฎใด ๆ เลยแพ็กเก็ตนั้นก็ต้องถูกตัดสินใจโดย policy ของchain นั้นๆ ซึ่งหากแพ็กเก็ตถูกส่งเข้ามายัง FORWARD chain และไม่ match กับกฎใดๆ ใน FORWARD chain นี้เลย มันก็จะถูก DROP ทันที

-E ใช้เปลี่ยนชื่อ chain ใหม่การใช้ command ด้านบนนั้นสามารถใช้ร่วมกับ Option บางอย่างได้

-V, --verbose ใช้ร่วมกับ -L, -A, -I, -D, -R เพื่อให้แสดงจำนวน byte ที่ match กับกฎออกมาด้วย (หน่วยเป็นได้ทั้ง K (x1, 000), M (x1, 000, 000), G (x1, 000, 000, 000))

-x, --exact ใช้ร่วมกับ -L และ -v เพื่อให้แสดงจำนวนแพ็กเก็ต และจำนวนของ byte ข้อมูลที่ match โดยไม่ให้แสดงผลในหน่วยของ K, M, G

-n, --numeric ใช้ร่วมกับ -L เพื่อสั่งให้ Iptables แสดงข้อมูลไอพีแอดเดรสและพอร์ตเป็นตัวเลขเท่านั้น

--line-numbers ใช้ร่วมกับ -L เพื่อแสดงเลขบรรทัดของ rule ซึ่งตัวเลขที่แสดงนี้จะสามารถใช้ได้ กับคำสั่ง insert rule ที่ระบุเป็นลำดับที่ของกฎ

--modprobe=*command* เพื่อโหลด module ที่เกี่ยวข้อง

Match การตั้งเงื่อนไขของการ match นั้นจะต้องอาศัยความเข้าใจในเรื่อง IP, TCP, UDP และ ICMP มาบ้างพอสมควร จึงจะสามารถตั้งเงื่อนไขที่เหมาะสมและตรงตามความต้องการได้ ซึ่งมีรายละเอียดดังนี้

- การระบุ source, destination IP address

  สามารถระบุ source ไอพีแอดเดรสของแพ็กเก็ตโดยใช้ -s หรือ --source หรือ --src และสำหรับ destination ไอพีแอดเดรสก็ใช้ -d หรือ --destination หรือ --dst การระบุไอพีแอดเดรสนั้นสามารถทำได้ 4 แบบด้วยกันคือ

  1. ใช้ชื่อเต็มแทน เช่น localhost หรือ www.kmitl.ac.th
  2. ระบุไอพีแอดเดรสโดยตรง เช่น 127.0.0.1 หรือ 202.44.204.33
  3. ระบุเป็น group ของไอพีแอดเดรส เช่น 202.44.204.0/24 ซึ่งหมายถึงไอพีแอดเดรสตั้งแต่ 202.44.204.0 - 202.44.204.255
  4. หรืออาจจะใช้ 202.44.204.0/255.255.255.0 แทน 202.44.204.0/24 ได้

- การทำ Inversion

ในบางกรณีนั้นหากต้องการระบุเป็น inverse เช่น อนุญาตให้ทุก IP ยกเว้น IP ที่ระบุไว้ ซึ่งการใช้คำสั่งดังกล่าวนั้นสามารถทำได้โดยการใช้เครื่องหมาย ! นำหน้า argument ที่ต้องการ (เครื่องหมาย ! หมายถึง NOT) เช่น -p ! TCP ซึ่งจะ match กับโปรโตคอลทุก ๆ ตัวที่ไม่ใช่ TCP หรือ -s ! localhost ซึ่งหมายถึงแพ็กเก็ตที่มี source ไอพีแอดเดรสอื่นๆ ยกเว้น localhost (127.0.0.1)

- การระบุโปรโตคอล

  สามารถระบุโปรโตคอลที่ต้องการได้ดังนี้คือ TCP, UDP, ICMP หรือสามารถใช้ตัวเลขแทนได้ (สำหรับ *NIX อ้างอิงได้จาก /etc/protocols) และยังสามารถใช้ได้ทั้งตัวอักษรเล็กหรือใหญ่ (ใช้ได้ทั้ง tcp และ TCP) เช่น -p TCP หรือ -p ! tcp

- การระบุ Interface

-i หรือ --in-interface ตามด้วยชื่อ Interface ใช้เพื่อระบุ incoming interface ซึ่งหมายถึงว่าแพ็กเก็ตที่จะ match กับกฎนี้ต้องเข้ามาจาก Interface ที่กำหนด เช่น -i eth0 หมายความว่าทุกแพ็กเก็ตที่เข้ามาทาง eth0 จะ match กับกฎนี้ ทั้งนี้ชื่อ Interface ที่สามารถใช้ได้นั้นสามารถตรวจสอบได้โดยใช้คำสั่ง ifconfig

Target เป็นข้อกำหนดของกฎบนไฟร์วอลล์ในกรณีที่แพ็กเก็ตไม่เข้ากัน (Match) กับกฎข้อแรกแล้วก็จะมีการตรวจสอบกฎข้อที่สองต่อไป แต่ถ้าแพ็กเก็ตนั้นไม่มีความเข้ากันกับทุกกฎเคอร์เนลจะตรวจสอบกับ Chain policy แล้วส่งต่อไปกำหนด target สำหรับแพ็กเก็ตนั้นๆ หรือจะใช้ user-defined chain (ที่ user สร้าง chain ขึ้นมาเอง) ก็ได้ target มีอยู่ 5 ข้อด้วยกัน คือ

ACCEPT การยอม หรืออนุญาตให้แพ็กเก็ตผ่านเข้าได้

DROP การปฏิเสธ หรือไม่อนุญาตให้แพ็กเก็ตผ่านเข้ามา

REJEC การปฏิเสธแพ็กเก็ตเหมือนกับ DENY แต่มีการส่ง ICMP กลับไปยังต้นทาง

QUEUE การส่งแพ็กเก็ตไปยัง userspace

RETURN กระโดดไปยัง Chain สุดท้าย และจัดการด้วยค่า default target

Iptables จะมีนโยบาย (policy) ด้านความปลอดภัยอยู่ 3 ข้อคือ INPUT, OUTPUT และ FORWARD

INPUT เป็นการรับค่าต่าง ๆ จากภายนอกเข้ามายังเซิร์ฟเวอร์หมายความว่า แพ็กเก็ตข้อมูลใด ๆ ที่วิ่งเข้ามายังเซิร์ฟเวอร์ จะผ่าน INPUT Chain

OUTPUT เป็นการส่งค่าต่าง ๆ จากเซิร์ฟเวอร์ไปยังภายนอก หมายความว่าแพ็กเก็ตข้อมูลใด ๆ ที่วิ่งออกไปจากเซิร์ฟเวอร์จะผ่าน OUTPUT Chain

FORWARD เป็นส่วนที่ใช้ควบคุมการติดต่อระหว่าง Private IP กับโครงข่ายอินเทอร์เน็ต หมายความว่า แพ็กเก็ตข้อมูลใด ๆ ที่วิ่งผ่านเข้ามายังเซิร์ฟเวอร์ แล้วถูกส่งต่อออกไปยังโครงข่ายอื่น จะผ่าน FORWARD Chain

ความแตกต่างระหว่าง Iptables และ Ipchains

- ชื่อของ built-in chain (ประกอบไปด้วย INPUT, OUTPUT, FORWARD) เปลี่ยนจากตัวอักษรเล็ก (lowercase) เป็นตัวอักษรใหญ่ (uppercase)
- การใช้งานที่ต้องระบุพอร์ตทั้ง TCP และ UDP นั้น ต้องใช้คำว่า --source-port หรือ --sport (--destination-port หรือ –dport) และต้องใช้ตามหลังจาก -p tcp หรือ -p udp
- TCP -y flag เปลี่ยนเป็น --syn และต้องใช้ร่วมกับ -p tcp
- target จาก DENY เปลี่ยนเป็น DROP
- chain ที่ไม่มีกฎใดๆ เลยก็สามารถทำงานได้
- การทำ zeroing built-in chain จะทำให้ byte counter ถูกล้างค่าไปด้วย
- ชื่อของ chain ยาวสูงสุดได้ 31 ตัวอักษร
- MASQ เปลี่ยนเป็น MASQUERADE และมีรูปแบบการใช้งานเปลี่ยนไป รวมทั้ง REDIRECT ก็มีการเปลี่ยนแปลงรูปแบบใหม่

2.7 Web Server

คือ เครื่องบริการเว็บไซต์ หรือเว็บเพจผ่านเว็บบราวเซอร์เพื่อให้ได้ข้อมูลทั้งภาพ เสียงจากผู้ให้บริการ เช่นบริการ http://www.google.com ที่เปิดบริการเว็บจากเครื่องให้บริการที่เรียกว่า Web Server บริการ Web Server จะมีบริการเสริมต่าง ๆ สำหรับนักพัฒนา ที่ทำให้เว็บไซต์สมบูรณ์ เช่น บริการภาษา หรือระบบฐานข้อมูล ซึ่งแต่ละโปรแกรมมีความแตกต่างกันไป เช่นภาษา html, perl, php, asp หรือ jsp เป็นต้น ส่วนฐานข้อมูลอาจใช้ MSAccess, Mysql, MSSQL หรือ Oracle เป็นต้น สำหรับรายละเอียดของบริการเสริม ในที่นี้จะขอกล่าวถึง Apache Web Server และ PHP พอสังเขป

- Apache WebServer เป็นโปรแกรมที่ใช้รองรับการให้บริการที่เรียกว่า World Wide Web (WWW) ซึ่งผู้ใช้งานอินเทอร์เน็ตโดยทั่วไปรู้จักคุ้นเคยกันเป็นอย่างดี ทั้งยังเป็นบริการหนึ่งที่มีผู้ใช้งานสูงสุดบนโครงข่ายอินเทอร์เน็ตอีกด้วย ผู้ใช้ทั่วไปนิยมใช้บริการ WWW นี้เพื่อค้นหา หรือเลือกดูข้อมูลที่สนใจ และดึงเอาข้อมูลที่ต้องการมาใช้งาน ส่วนองค์กรต่างๆนิยมใช้เพื่อการประชาสัมพันธ์ข้อมูล หรือใช้เป็นช่องทางการติดต่อสื่อสารกับผู้ใช้งานอีกทางหนึ่ง ให้ประโยชน์ใน

การส่งผ่านข้อมูลทั่วไป หรือใช้ในการทำธุรกรรมพาณิชย์อิเล็กทรอนิกส์ ทั้งนี้เนื่องมาจากการติดตั้ง Web Server ขึ้นมาเพื่อใช้งานนั้นสามารถทำได้โดยไม่ยุ่งยาก และเสียค่าใช้จ่ายไม่มากนัก

อย่างไรก็ตาม การรักษาความปลอดภัยให้กับเครื่อง Web Server ถือเป็นสิ่งจำเป็นซึ่งผู้ดูแลระบบไม่ควรมองข้าม เพราะเว็บเพจของแต่ละองค์กรก็เปรียบเสมือนหน้าตาขององค์กร หากถูกผู้ไม่ประสงค์ดีบุกรุกโจมตีก็จะเป็นการทำลายชื่อเสียงหรือความน่าเชื่อถือขององค์กรไปด้วย

Directive ที่ควรได้รับการพิจารณากำหนดค่าให้เหมาะสม เพื่อเพิ่มความปลอดภัยให้กับโปรแกรม Apache และเครื่อง Web Server ประกอบด้วย

ServerType standalone [standalone | inetd]

ServerType ใช้กำหนดชนิดของ Web Server ที่จะให้บริการว่าจะให้ทำงานด้วยตนเอง หรือทำงานผ่านเดมอนชื่อ inetd (หรือ xinetd) ข้อดีของการทำงานแบบ standalone คือ หลังจากสั่งให้ Web Server เริ่มทำงาน จะเกิดการสร้างโพรเซสขึ้นมาล่วงหน้ารอรับการขอใช้งาน ทำให้การให้บริการทำได้เร็วและนิยมใช้งานทั่วไป ส่วนข้อดีของการทำงานแบบ inetd คือ เป็นการประหยัดทรัพยากร เนื่องจากโพรเซสที่รองรับการขอใช้งานจะเกิดขึ้นเมื่อมีการร้องขอการใช้งานเกิดขึ้นจริง เหมาะสำหรับเครื่องที่มีทรัพยากรจำกัดเท่านั้น และไม่นิยมใช้ในกรณีทั่วไป

User nobody [username | #user_id]

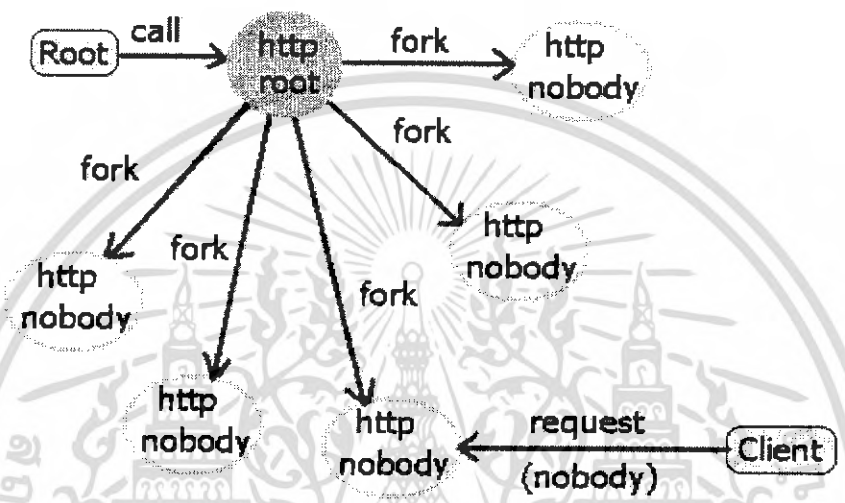
เป็นการกำหนดชื่อหรือรหัสผู้ใช้ที่จะกำหนดให้เป็นเจ้าของโพรเซสที่ถูกสร้างขึ้นเพื่อรอรับการขอเข้าใช้งานจากผู้ใช้ภายนอก ดังนั้นผู้ใช้จากภายนอกที่ขอเข้าใช้งานจะได้รับสิทธิ์เป็นผู้ใช้ตามที่กำหนดนี้ด้วย

Group nobody [groupname | #group_ip]

เป็นการกำหนดกลุ่มหรือรหัสของกลุ่มผู้ใช้ที่จะกำหนดให้เป็นเจ้าของโพรเซสที่ถูกสร้างขึ้นเพื่อรอรับการขอเข้าใช้งานจากผู้ใช้ภายนอก ดังนั้นผู้ใช้จากภายนอกที่ขอเข้าใช้งานจะได้รับสิทธิ์ให้อยู่ในกลุ่มตามที่กำหนดนี้ด้วย

การกำหนดชื่อผู้ใช้และกลุ่มของผู้ใช้เกี่ยวข้องกับการสร้างโพรเซสเพื่อรอรับการขอเข้าใช้งาน เนื่องจากโพรเซสของ Apache หรือ http จะถูกสั่งให้เริ่มทำงานโดยผู้ดูแลระบบ (root)

หลังจากนั้น โพรเซสดังกล่าวจะสั่งให้สร้างโพรเซสเพิ่มขึ้นอีกตามจำนวนที่กำหนด โพรเซสที่ถูกสร้างขึ้นในภายหลังนี้เองจะมีเจ้าของโพรเซสตามที่กำหนดใน directive ด้านบนและอนุญาตให้ผู้ใช้จากภายนอกเข้ามาใช้งาน ดังนั้น ผู้ที่เข้ามาใช้งานจึงได้สิทธิ์ตามนั้นดังแสดงในรูปที่ 2.7



รูปที่ 2.7 การทำงานของโพรเซส Apache (http)

ข้อแนะนำสำหรับการกำหนดชื่อและกลุ่มผู้ใช้สำหรับ directive ทั้งสองข้อด้านบนคือ ผู้ดูแลระบบสามารถกำหนดค่าเป็นผู้ใช้คนใด หรือกลุ่มผู้ใช้กลุ่มใดก็ได้ แต่จะต้องเป็นผู้ใช้และกลุ่มผู้ใช้ที่มีสิทธิ์การใช้งานเครื่องต่ำ และไม่ควรเป็นผู้ใช้หรือกลุ่มผู้ใช้ที่ได้รับสิทธิ์ในการใช้งานไฟล์อื่นๆ นอกเหนือจากไฟล์ที่ต้องการแสดงผลผ่านเว็บ รวมไปถึงจะต้องไม่ได้รับอนุญาตให้แก้ไขเปลี่ยนแปลงไฟล์ใดๆ ในระบบ เนื่องจากผู้ดูแลระบบไม่สามารถตรวจสอบหรือพิสูจน์ตัวตนได้ว่าจะมีการขอเข้าใช้งานเครื่อง Web Server จากที่ใดบ้าง จึงควรให้สิทธิ์การใช้งานแก่ผู้ที่เข้าใช้งานดังกล่าวให้น้อยที่สุดเท่าที่จะเป็นไปได้ และไม่ควรเป็นผู้ใช้และกลุ่มผู้ใช้ที่ถูกสร้างขึ้นเพื่อใช้งานอื่นๆ อีก

- PHP ในปัจจุบันเว็บไซต์ต่าง ๆ ได้มีการพัฒนาในด้านด่างๆ อย่างรวดเร็ว อาทิเช่น เรื่องของความสวยงามและแปลกใหม่, การบริการข่าวสารข้อมูลที่ทันสมัย, เป็นสื่อกลางในการติดต่อ และสิ่งหนึ่งที่กำลังได้รับความนิยมเป็นอย่างมากซึ่ง PHP ช่วยให้เป็นการพัฒนาเว็บไซต์และความสามารถที่โดดเด่นอีกประการ-หนึ่งของ PHP นั้น คือ database-enabled web page ทำให้

เอกสารของ HTML สามารถที่ จะเชื่อมต่อกับระบบฐานข้อมูล (database)ได้อย่างมีประสิทธิภาพ และรวดเร็ว จึงทำให้ ความต้องการในเรื่องการจัดรายการสินค้าและรับรายการสั่งของตลอดจนการจัดเก็บ ข้อมูลต่าง ๆ ที่สำคัญผ่านทางอินเทอร์เน็ตเป็นไปได้อย่างง่ายดาย

PHP เป็นภาษาจำพวก scripting language คำสั่งต่างๆจะเก็บอยู่ในไฟล์ที่เรียกว่า สคริปต์ (script) และเวลาใช้งานต้องอาศัยตัวแปลชุดคำสั่ง ตัวอย่างของภาษาสคริปก็เช่น JavaScript, Perl เป็นต้น ลักษณะของ PHP ที่แตกต่างจากภาษาสคริปต์แบบอื่นๆ คือ PHP ได้รับการพัฒนาและออกแบบมา เพื่อใช้งานในการสร้างเอกสารแบบ HTML โดยสามารถสอดแทรกหรือแก้ไขเนื้อหาได้โดยอัตโนมัติ ดังนั้นจึงกล่าวว่า PHP เป็นภาษาที่เรียกว่า server-side หรือ HTML- embedded scripting language เป็นเครื่องมือที่สำคัญชนิดหนึ่งที่ช่วยให้เราสามารถสร้างเอกสารแบบ Dynamic HTML ได้อย่างมีประสิทธิภาพและมีลูกเล่นมากขึ้นเนื่องจากว่า PHP ไม่ได้เป็นส่วนหนึ่งของตัว Web Server ดังนั้นถ้าจะใช้ PHP ก็จะต้องดูก่อนว่า Web Server นั้นสามารถใช้สคริปต์ PHP ได้หรือไม่ ในกรณีของ Apache เราสามารถใช้ PHP ได้สองรูปแบบคือ ในลักษณะของ CGI และ Apache Module ความแตกต่างอยู่ตรงที่ว่า ถ้าใช้ PHP เป็นแบบโมดูล PHP จะเป็นส่วนหนึ่งของ Apache หรือเป็นส่วนขยายในการทำงานนั่นเอง ซึ่งจะทำงานได้เร็วกว่าแบบที่เป็น CGI เพราะว่า ถ้าเป็น CGI แล้ว ตัวแปลชุดคำสั่งของ PHP ถือว่าเป็นแค่โปรแกรมภายนอก ซึ่ง Apache จะต้องเรียกขึ้นมาทำงานทุกครั้ง ที่ต้องการใช้ PHP ดังนั้น ถ้ามองในเรื่องของประสิทธิภาพในการทำงาน การใช้ PHP แบบที่เป็นโมดูลหนึ่งของ Apache จะทำงานได้มีประสิทธิภาพมากกว่า

ลักษณะเด่นของ PHP

- ใช้ได้ฟรี
- PHP เป็นโปร แกรมวิ่งข้างเซิร์ฟเวอร์ ดังนั้นขีดความสามารถไม่จำกัด
- Conlatfun นั่นคือ PHP วิ่งบนเครื่อง UNIX, Linux, Windows ได้หมด
- เรียนรู้ง่าย เนื่องจาก PHP ฝังเข้าไปใน HTML และใช้โครงสร้างและไวยากรณ์ภาษาง่ายๆ
- เร็วและมีประสิทธิภาพ โดยเฉพาะเมื่อใช้กับ Apach Xerve เพราะไม่ต้องใช้โปรแกรมจากภายนอก
- ใช้ร่วมกับ XML ได้ทันที
- ใช้กับระบบแฟ้มข้อมูลได้
- ใช้กับข้อมูลตัวอักษรได้อย่างมีประสิทธิภาพ
- ใช้กับโครงสร้างข้อมูลใช้ได้แบบ Scalar, Array, Associative array

- ใช้กับการประมวลผลภาพได้

2.8 Mail Server

E- mail หรือ จดหมายอิเล็กทรอนิคส์เป็นบริการอย่างหนึ่งที่นิยมใช้กันอย่างแพร่หลายมาก จนทำให้บางคนคิดว่า E- mail คือ อินเทอร์เน็ต และอินเทอร์เน็ตคือ E- mail วิธีใช้งาน E- mail ก็ง่าย และมีประโยชน์มาก การทำงานของ E- mail มีลักษณะคล้ายกับระบบไปรษณีย์ปกติ (หมายถึง ระบบที่ใช้กระดาษในการเขียนจดหมาย) กล่าวคือในระบบไปรษณีย์ปกติมีหน่วยงานที่ทำหน้าที่ใน การรับส่งจดหมายคือเป็นบุรุษไปรษณีย์ ถ้าเป็นในอินเทอร์เน็ตสิ่งที่ทำหน้าที่คอยรับส่งจดหมายคือ บรรดาคอมพิวเตอร์ทั้งหลายที่ทำหน้าที่เป็น E- mail Server (คอมพิวเตอร์ที่ทำหน้าที่ให้บริการด้าน จดหมายอิเล็กทรอนิคส์) ดังนั้นถ้าท่านต้องการใช้ E- mail สิ่งแรกที่ท่านต้องทำคือไปสมัครเป็น สมาชิกหรือไปทำการลงทะเบียนกับ E- mail Server จะเป็น Server ใดก็ได้ บรรดา E- mail Server ทั้งหลายนี้สามารถจัดแบ่งออกได้เป็นสามประเภทดังนี้

- E- mail Server ของหน่วยงานที่ทำการศึกษาอยู่หรือทำงานอยู่ เช่น นิสิต อาจารย์ ข้าราชการ ของจุฬาลงกรณ์มหาวิทยาลัย ก็สามารถลงทะเบียนหรือสมัครเป็นสมาชิกได้กับ คอมพิวเตอร์ที่เป็น E- mail Server ของจุฬา ฯ ได้
- E- mail Server ของ ISP (Internet Service Provider - หน่วยงานที่ให้บริการอินเทอร์เน็ต) เช่น KSC เป็นต้น ท่านสามารถสมัครหรือลงทะเบียนกับหน่วยงานประเภทนี้ได้ แต่ต้องเสีย ค่าสมาชิกให้แก่หน่วยงานประเภทนี้ด้วย
- E- mail Server ของหน่วยงานที่ให้บริการฟรี เป็นบริการฟรีที่เปิดโอกาสให้ผู้ที่สนใจ สามารถเข้าไปลงทะเบียนหรือสมัครเป็นสมาชิกได้โดยไม่ต้องเสียค่าใช้จ่าย เช่น hotmail เป็นต้น

attachment (สิ่งที่ส่งมากับ E- mail)อาจเป็นไฟล์ประเภทไหนก็ได้ เช่น ไฟล์ที่เป็นข้อความ ล้วน ๆ (text) ไฟล์ที่ข้อมูลรูปภาพ กล่าวคือเป็นสื่ออะไรก็ได้

ประโยชน์ที่เป็นผู้ใช้ E- mail จะได้รับมีดังนี้

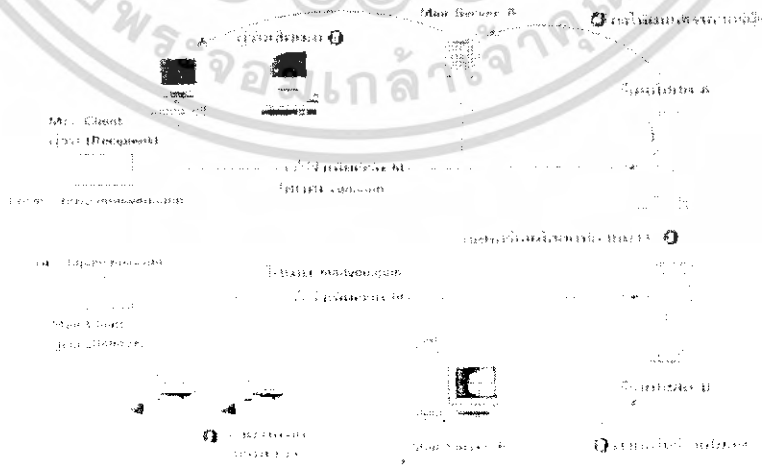
- สามารถส่งจดหมายอิเล็กทรอนิกส์เมื่อไรก็ได้ตามที่ต้องการ จะเป็นเวลากลางคืนหรือเวลา กลางวันก็ได้

- จดหมายจะถึงมือผู้รับภายในเวลาอันรวดเร็ว อาจภายในไม่กี่นาที หรือภายในไม่กี่ชั่วโมง ไม่ว่าผู้รับจดหมายนั้นจะอยู่ใกล้หรือไกล
- ผู้รับจดหมายก็สามารถรับและเปิดอ่านจดหมายได้เมื่อไรก็ได้ตามที่ต้องการ
- สามารถส่งจดหมายไปยังผู้รับคนเดียว หลายคน หรือจำนวนมากเป็นร้อยคน เป็นพันคนได้ ซอฟต์แวร์ของ E- mail ส่วนใหญ่จะมีวิธีช่วยให้เก็บรายชื่อพร้อมทั้ง E- Mail Address ของผู้ที่ต้องการส่งจดหมายไปหา และช่วยจัดเป็นกลุ่มด้วย ถ้าต้องการส่งจดหมายไปยังกลุ่มก็หมายความว่าทุกคนในกลุ่มก็ได้รับจดหมายนั้น
- สามารถเก็บจดหมายที่ได้รับ(จากเพื่อน ผู้ร่วมงาน หรือหัวหน้า)บางฉบับไว้ได้ ถ้าเห็นว่าจดหมายนั้นมีความสำคัญ เช่น ไว้เตือนความจำว่ามีงานอะไรต้องทำ หรือ ได้ตกลงเรื่องอะไรไว้กับใครบ้าง

ปัญหาที่อาจพบในการใช้ E-mail

- จดหมายหาย ปัญหานี้อาจเกิดได้จากหลายสาเหตุ เช่น ความผิดพลาดของคน ความผิดพลาดของซอฟต์แวร์ ความล้มเหลวของ hardware เป็นต้น
- จดหมายส่งไปผิด คือไปยังผู้รับผิดคน ปัญหานี้อาจเกิดการที่ระบุ E-Mail Address ของผู้รับผิด
- การปลอมจดหมาย

การทำงานของ Mail Server



รูปที่ 2.8 ลักษณะการทำงานของระบบ E- mail

จากรูปที่ 2.8 สามารถอธิบายได้โดยเริ่มจากที่เมล์ถูกส่งไปยังเครื่องคอมพิวเตอร์ ที่เป็น Mail Server ซึ่งจะทำหน้าที่ต่อ ในการส่งไปยัง E- Mail Address ที่ระบุ เมื่อผู้รับเข้ามารับ E- mail นั้น Mail Server จะแจ้งให้ทราบว่ามี E- mail ใหม่กี่ฉบับแล้ว Mail Server จะรู้ได้อย่างไรว่า Mail Server ตัวไหนที่จะส่งเมล์ไป คือมันจะดูจาก DNS (Domain Name Service) สิ่งที่มันทำมันจะหา MX (Mail Exchange Record) ซึ่งจะถูกกำหนดขึ้นมาเมื่อสร้าง domain ในตอนแรก ซึ่ง Server นั้นมักจะถูกเรียกว่า "mail.domain" เป็นเครื่องที่ใช้รับเมล์ในโดเมนเนมนี้ถามว่า ถ้า Mail Server เกิดปัญหาในขณะส่งจะเกิดอะไรขึ้นไม่ต้องกังวล ถ้าไม่สามารถส่งถึงผู้รับ E- mail จะถูกส่งกลับมาพร้อมการแจ้งสาเหตุที่ไม่สามารถส่งถึงผู้รับได้โดยอัตโนมัติ ส่วนใหญ่การรับและส่งเมล์จะใช้ Server เดียวกันโปรโตคอลสำหรับรับ E- mail ที่เกี่ยวข้องที่ใช้งานกันแพร่หลาย มีอยู่ 4 แบบ คือ โปรโตคอล POP, SMTP , IMAP และ MIME

2.8.1 POP (Post Office Protocol)

POP หรือ Post Office Protocol เป็นโปรโตคอลที่ออกแบบมาให้ใช้สำหรับการรับเมลล์จากเครื่องที่เป็น Mail Server มายังเครื่องของผู้ใช้ โดยทางฝั่งเซิร์ฟเวอร์จะมีโปรเซสที่เป็น POP Server ขณะทางฝั่งผู้ใช้มี POP Client ซึ่งในบางโปรแกรมที่ผู้ใช้อ่านและเขียนเมล์นั้นจะมี POP Client ฝังอยู่ในตัวอยู่แล้ว ไม่ได้แยกออกมาเป็นโปรแกรมหนึ่ง เมื่อผู้ใช้เชื่อมต่อไปที่ POP Server อีเมล์ที่อยู่บน Mail Server จะถูกส่งมาเก็บไว้ในเครื่องของผู้ใช้เลย ดังนั้นเมื่อผู้ใช้จัดการกับเมล์ เช่น ลบเมล์หรือส่งต่อเมล์ก็จะทำกับเมล์ที่อยู่บนเครื่องของผู้ใช้เอง ส่วนเมล์บน Mail Server จะถูกลบทิ้งไปเมื่อมีการส่งให้ผู้ใช้เรียบร้อยแล้ว ยกเว้นจะมีการกำหนดเพิ่มเติมไว้ที่โปรแกรม Mail Client ว่าอย่าให้ลบเมล์ออกจากเซิร์ฟเวอร์ (Leave a copy of message on the server)

ในปัจจุบันโปรโตคอลมีออกมาหลายเวอร์ชัน แต่ที่นิยมกันคือ POP3 ซึ่งก็ยังมีข้อจำกัดในการใช้ คือขณะรับและส่ง E- mail ฝั่งผู้ใช้จะส่งรหัสผ่านของผู้ใช้ในรูปของข้อความหรือเท็กซ์ไป ทำให้ไม่ปลอดภัยนักหากมีการลอบดักข้อมูล ฉะนั้นดอนเซ็ท POP client เช่น MS outlook หรือโปรแกรมอื่น ๆ ควรจะเลือกใช้งาน Log on using Secure Password Authentication (SPA) ด้วย แต่ต้องให้ Mail Server มีสนับสนุนการใช้ SPA ถึงจะใช้งานได้ ปัจจุบันได้พัฒนามาจนถึง version 3 แล้ว หรือเรียกย่อๆว่า POP3 โปรโตคอลนี้เป็นตัวแรกที่ถูกออกแบบมาเพื่อใช้รับ E- mail และเพื่อให้สนับสนุนการทำงานแบบ Offline ซึ่งกลไกของ POP3 นี้จะทำงานในแบบ Offline โดยดิดต่อเข้าไปยัง Mail Server แล้วดาวน์โหลดE-mail ทั้งหมดมาไว้ที่ User Agent จากนั้นจะลบ E- mail ที่

เซิร์ฟเวอร์นั้นทิ้งไป เพื่อป้องกันการดาวน์โหลดซ้ำ แต่ผู้ใช้จะทำงานแบบ Online กับเซิร์ฟเวอร์ไม่ได้ เนื่องจากการอ่าน E- mail จะดึง E - mail ที่เก็บไว้ใน User Agent ขึ้นมาให้อ่านหลังจากที่ download

โปรโตคอลของ POP3 นี้จะทำงานในแบบของไคลเอนต์เซิร์ฟเวอร์ คือ มีโปรแกรม POP Server ใน Mail Server และ POP Client ในเครื่องของผู้รับ ซึ่งปกติจะฝังอยู่ในโปรแกรมที่เป็น user Agent เลย โปรแกรมทั้ง2 จะติดต่อกันโดยใช้คำสั่งที่เป็นรหัส ASCII คือเมื่อด้านที่รับทำคำสั่งก็จะทำงานตามคำสั่งนั้น แล้วตอบกลับมามีค่าเป็น (+OK) หมายถึง ทำงานได้เรียบร้อย หรือ (-ERR) หมายถึง เกิดปัญหาขึ้นทำงานไม่ได้ ซึ่งในคำสั่งที่ต้องมีการตอบกลับและส่งข้อมูลกลับมา โดยประกอบด้วยข้อมูลหลาย ๆ บรรทัดนั้น POP3 จะให้บรรทัดสุดท้ายเป็นเครื่องหมาย (.) ตามด้วย Carriage Return และ Line Feed หมายถึงการสิ้นสุดชุดข้อมูล แต่ในกรณีที่ข้อมูลบรรทัดสุดท้าย มีข้อมูลที่เป็นจุดด้วย จะใช้เทคนิคที่เรียกว่า Character Stuffing เพื่อแก้ปัญหา โดยจะเติมจุดลงไปอีก 1 ตัว เพื่อเป็นตัวบ่งชี้ว่าข้อมูลนั้นเป็นจุด ซึ่งจะแตกต่างจากสัญลักษณ์แสดงการสิ้นสุดของข้อมูล

การทำงานของ POP3 จะทำงานร่วมกับโปร โตคอล TCP (Transmission Control Protocol) โดยทั่วไปจะใช้พอร์ต 110 ในการติดต่อขั้นตอนการทำงานของ POP3 จะประกอบด้วย 3 สถานะ คือ สถานะขออนุมัติ, สถานะรับส่งรายการ และสถานะปรับปรุงข้อมูล ซึ่งในแต่ละสถานะจะรับรู้คำสั่งดังนี้

1. สถานะขออนุมัติ (Authorization State) เมื่อเริ่มต้นติดต่อกับเซิร์ฟเวอร์จะเป็นการเข้าสู่สถานะการขออนุมัติ โดยไคลเอนต์จะต้องแจ้งชื่อผู้ใช้ และรหัสผ่าน (Password) เพื่อขออนุมัติจากเซิร์ฟเวอร์ก่อน โดยไคลเอนต์จะใช้คำสั่ง USER เพื่อระบุชื่อผู้ใช้ หรือคำสั่ง PASS เพื่อกำหนด Password แต่ในกรณีที่ชื่อ Password ถูกเข้ารหัสไว้ และไม่ได้เป็นค่า ASCII ทั่วไป ไคลเอนต์จะใช้คำสั่ง POP ทำงานแทนคำสั่ง USER และ PASS

2. สถานะรับส่งรายการ (Transaction State) หลังจากที่ได้รับอนุมัติจากเซิร์ฟเวอร์แล้ว ก็จะเข้าสู่สถานะที่ใช้คำสั่งในการทำงานต่างๆ

3. สถานะปรับปรุงข้อมูล (Update State) เมื่อ User Agent เลิกใช้งานด้วยคำสั่ง QUIT ของ POP3 Server ก็จะเข้าสู่สถานะปรับปรุงข้อมูล เพื่อลบ E- mail ที่ดาวน์โหลดเรียบร้อยแล้วออกไป จากนั้นก็จะเข้าสู่สถานะขออนุมัติใหม่โดยอัตโนมัติ เพื่อรอรับการทำงานครั้งต่อไป

สถานะขออนุมัติ (Authorization State)

เมื่อ POP3 Client ติดต่อกับ POP3 Server ก็จะแสดงบรรทัดติดต่อขึ้นมาบรรทัดหนึ่ง และบอกจุดสิ้นสุดด้วย CRLF (Carriage Return Line Feed) ตัวอย่างเช่น

s :+OK POP3 server read

เป็นการตอบรับของ POP3 ซึ่ง POP3 Server จะแสดงเครื่องหมาย + บอกการตอบรับว่าในขณะนั้นสามารถให้บริการแก่ไคลเอนต์ตามที่ร้องขอ

เมื่อ POP3 อยู่ในฐานะ Authorization State แล้วก็จะทำการยืนยันแก่ POP3 Server โดยมีวิธีการยืนยันอยู่สองวิธี คือ

- คำสั่ง USER รวมกับคำสั่ง PASS

- คำสั่ง APOP

การใช้คำสั่ง USER และคำสั่ง PASS ในขั้นแรก Client ต้องใช้คำสั่ง USER ก่อนถ้า POP3 Server ตอบมาด้วยสถานะบ่งชี้ว่าเป็นเครื่องหมาย + ("+OK") เครื่องไคลเอนต์จะใส่คำสั่ง PASS เข้าไปในการทำงานหรือคำสั่ง QUIT เพื่อบอกสถานะว่าหยุดการทำงานถ้าหากสถานะบ่งชี้เป็นเครื่องหมาย - ("ERR") เครื่องไคลเอนต์ต้องส่งคำสั่งไปใหม่หรือยกเลิกโดยใช้คำสั่ง Quit ไปเลยก็ได้ เมื่อเครื่องไคลเอนต์ส่งคำสั่ง PASS แล้ว POP3 Server จะใช้ทั้งคำสั่ง USER และ PASS เพื่อพิจารณาว่าเครื่องไคลเอนต์ใดสามารถเข้าไปใช้งานภายใน Maildrop ได้

POP3 Server ได้มีการจำกัดการเข้าถึงใน Maildrop เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าไปทำการเปลี่ยนแปลงหรือลบข้อมูลใน Maildrop ก่อนจะเข้าสู่ช่วง Update State ถ้าการ lock สำเร็จ POP3 Server ก็จะตอบสนองด้วยสถานะการบ่งชี้ เป็น + ขณะนี้ POP3 ก็จะเข้าสู่ช่วง Transaction State ซึ่งไม่มี Message ที่ถูกทำเครื่องหมาย Delete ถ้าไม่สามารถเปิด Maildrop เนื่องจากเหตุผลบางประการ เช่น lock ไม่ได้, ไคลเอนต์ปฏิเสธการเข้าถึง Maildrop ที่เหมาะสม หรือ Maildrop ไม่สามารถกระจายข้อมูลได้, Mail Server จะแสดงสถานะบ่งชี้เป็นเครื่องหมาย - ถ้ามีการ lock แต่ POP3 Server ยังแสดงสถานะบ่งชี้เป็นเครื่องหมายลบอยู่ จะต้องดูที่สำดับการ lock ในการปฏิเสธคำสั่งหลังจากได้รับตัวบ่งชี้สถานะเป็นเครื่องหมายลบเซิร์ฟเวอร์ก็จะปิดการติดต่อถ้าเซิร์ฟเวอร์ยังไม่ปิดการติดต่อเครื่องไคลเอนต์ก็จะส่งคำสั่งมาอีก หรือไม่ก็ใช้คำสั่ง Quit ออกไปเลยเมื่อ POP3 Server ได้เปิด Maildrop ก็จะส่งหมายเลข Message ไปยังแต่ละ Message ซึ่งขนาดของแต่ละ Messagee จะอยู่ในรูปของเลขฐาน 8 ข้อความแรกใน Maildrop จะได้รับหมายเลข Message เป็น 1 ลำดับที่สอง ก็เป็น 2 ตามลำดับไปเรื่อยๆ คำสั่ง POP3 และหมายเลขจะเป็นเลขฐาน 10

2.8.2 Simple Mail Transfer Protocol (SMTP)

SMTP หรือ Simple Mail Tranfer Protocol เป็นโปรโตคอลที่ติดต่อกันระหว่างเครื่องที่เป็น host กับ host โดย host ในที่นี้ทำหน้าที่เป็น Mail Server หรือผู้ให้บริการ E- mail ซึ่งจะมีโปรเซสที่ทำหน้าที่เป็น Mail transfer agent ทำงานอยู่บนทั้ง 2 ด้าน และรับส่งข้อมูลระหว่างกันโดยใช้

SMTP เมื่อได้รับเมล์มาแล้วก็จะเก็บเมล์เหล่านั้นไว้ในไดเร็คทอรี่ที่เป็น Mailbox หรือตู้ไปรษณีย์ในเครื่องนั้น และรอจนกว่าผู้ใช้มาเปิดอ่าน ซึ่งมีได้ 3 วิธีด้วยกันคือ

- ผู้ใช้มี Account บนเครื่อง Mail Server ก็สามารถเปิดอ่านได้โดยใช้คำสั่งต่าง ๆ ของ Linux/Unix เช่น เมล์, pine และเมล์ที่ถูกอ่านจะถูกย้ายไปเก็บไว้ใน Mailbox ของผู้ใช้แทน Mailbox ของระบบได้
- ผู้ใช้อยู่บนเครื่องลูกข่าย จะต้องโหลดเมล์ไปไว้ในเครื่องของตัวเองก่อน แล้วจึงเปิดอ่านได้
- ผู้ใช้รับส่งเมล์ผ่านตัวกลางที่เป็น Web Server ซึ่งเมล์จะยังคงถูกเก็บไว้ที่เครื่อง Mail Server

การทำงานของ SMTP จะทำหน้าที่ในการกำหนดว่า MTA แต่ละตัวจะติดต่อกันได้อย่างไรผ่านทาง TCP/IP จดหมายที่ส่งไปนั้นอาจจะส่งตรงไปยัง MTA ปลายทางเลย หรือว่าผ่าน MTA หลายเครื่อง (หมายถึงผ่านรีเลย์โฮสต์หลายเครื่อง) โดยผ่านกระบวนการ Store and Forward ก็ได้เช่นกัน

โปรโตคอล SMTP จะไม่สนใจข้อความในจดหมาย แต่จำกัดว่า SMTP สามารถส่งได้แต่ข้อมูลที่เป็นข้อความ ASCII เท่านั้น ไม่สามารถส่งไฟล์ที่เป็นเพลง, หนัง, รูปภาพ หรืออื่น ๆ ได้ ซึ่งถ้าเราต้องการส่งไฟล์เหล่านั้นผ่านทาง SMTP จะต้องแปลงไฟล์เหล่านั้นให้อยู่ในรูปของข้อความเสียก่อน และเมื่อส่งไปถึงปลายทางแล้วค่อยทำการแปลงกลับอีกที

นอกจากการใช้ SMTP เพื่อรับส่งเมล์ระหว่าง Mail Server ด้วยกันแล้ว ยังใช้ในขณะที่เป็นไคลเอนต์ส่งเมล์ไปยังเครื่องที่เป็น Mail Server ด้วย

Simple Mail Transfer Protocol (SMTP) เป็นโปรโตคอล ของ TCP/IP ใช้ในการส่งและรับ E-mail แต่ SMTP มีความจำกัดในด้านแถวคอย (Queue) ของข้อความในด้านรับ ตามปกติจะใช้ร่วมกับโปรโตคอลอื่นอีกตัว เช่น POP3 หรือ Internet Message Access Protocol เพื่อให้ผู้ใช้สามารถเก็บเมล์ไว้ใน Server Mailbox และ ดาวน์โหลดจากเซิร์ฟเวอร์ในอีกความหมายคือ SMTP ใช้สำหรับการส่งเมล์ของผู้ใช้ และ POP3 หรือ IMAP ใช้สำหรับเมล์แล้วเก็บไว้ในเครื่องแม่ข่าย โปรแกรม E- mail ส่วนใหญ่ เช่น Eudora ให้ผู้ใช้ระบุได้ทั้ง SMTP Server และ POP Server บนระบบ UNIX การส่งเมล์ใช้ SMTP Server ส่วนแพ็คเก็ตการส่งเมล์เชิงพาณิชย์ได้รวม POP Server และมาพร้อมกับ Window NT

SMTP ได้รับสนับสนุนให้กำกับพอร์ต 25 ของ Transmission Control Protocol รายละเอียดของ SMTP อยู่ใน Request for Comment 821 ของ Internet Engineering Task Force (IETF) ตัวเลือกอื่นนอกจาก SMTP คือ X.400 ซึ่งใช้กันอย่างกว้างขวางในยุโรป

Simple mail transfer protocol server คือเครื่องบริการส่ง E- mail ไปยังเครื่องบริการอื่น ๆ สำหรับ SMTP ส่วนใหญ่จะไม่ยอมให้คนนอกองค์กรหรือ IP ที่อยู่นอกองค์กรใช้งาน SMTP เพราะอาจมีการลักลอบใช้งานทำให้บริการ SMTP ทำงานหนักให้กับคนภายนอกโดยไม่เกิดประโยชน์ใดๆ หากเครื่องมีบริการ SMTP แก่คนนอก แสดงว่าไม่ได้มีการกำหนด RELAY ไว้เพราะอาจมีการใช้เครื่องมือค้นหา " OPEN RELAY" แล้วพบว่าเครื่องนั้นเป็นเครื่องหนึ่งที่ไม่ได้ทำ RELAY ไว้ก็ได้และที่อันตรายคือ อาจมีการใช้โปรแกรม MOBI+ กำหนดให้เครื่อง SMTP Bomb Mail ไปยัง Mail Box ของเป้าหมาย และหมายเลขเครื่องที่โจมตี ก็คือ เครื่องSMTP นั่นเอง

2.8.3 Internet Message Access Protocol (IMAP)

IMAP เป็นมาตรฐานโปรโตคอลสำหรับการเข้าถึง E- mail จากเครื่อง Local Service โดย IMAP เป็นโปรโตคอลแบบ Client/Service ซึ่ง E- mail จะได้รับและเก็บไว้ในเครื่องแม่ข่ายอินเตอร์เน็ต ผู้ใช้สามารถดูหัวข้อ และผู้ส่งของจดหมายแล้วจึงตัดสินใจดาวน์โหลดผู้ใช้สามารถสร้างและควบคุมโฟลเดอร์ หรือ Mail Box บนเครื่องแม่ข่ายลบจดหมายหรือค้นหา IMAP ต้องการเข้าถึงแม่ข่ายอย่างต่อเนื่องตลอดช่วงเวลาการใช้ E- mail

โปรโตคอล ที่มีความซับซ้อนน้อยกว่า คือ Post Office Protocol 3 (POP3) การใช้ POP3 ทำให้ E- mail ของผู้ใช้ได้รับการเก็บไว้ใน Mail Box บนโครงข่ายเมื่อต้องการอ่าน E- mail สามารถทำการดาวน์โหลดมายังคอมพิวเตอร์ของผู้ใช้ และไม่จำเป็นต้องเก็บไว้บนแม่ข่าย POP และ IMAP เกี่ยวข้องกับการรับ E- mail ของผู้ใช้ในเครื่อง Local Server และอย่าสับสนกับ Simple Mail Transfer Protocol (SMTP) ซึ่งเป็นโปรโตคอลสำหรับการส่ง E-mail ระหว่างจุดบนอินเทอร์เน็ต การส่ง E- mail ใช้ SMTP การอ่าน E- mail ใช้ POP และ IMAPIMAP เป็นโปรโตคอลที่มีลักษณะคล้ายคลึงกับ POP3 แต่จะแก้ปัญหาของ POP3 ได้ดีขึ้นคือ

POP จะมีวิธีการทำงานในลักษณะ "เก็บและส่งต่อ" (store-and-forward) ดังนั้นกระบวนการจัดการจดหมายต่าง ๆ จึงยังไม่ดีมากพอ IMAP จะแตกต่างจาก POP ในเรื่องของการตรวจสอบ E-mail ซึ่ง IMAP จะสามารถตรวจสอบเมล์ได้ 3 แบบคือ

1. offline access คือ ดึง E-mail ทั้งหมดมาเก็บไว้ที่เครื่อง และลบ E- mail ออกจากเครื่อง Server (POP3) จะตรวจสอบด้วยวิธีนี้และการใช้โปรแกรมดึงE- mail บางตัวเราสามารถจะสั่งให้เก็บ E- mail ที่เราอ่านแล้วไว้ที่เครื่องเซิร์ฟเวอร์ได้

2. Online-access อ่าน E- mail แบบออนไลน์โดยใช้เครื่องเราเป็นตัวอ่าน E- mail ส่วนตัว E-mail ก็อยู่ที่เซิร์ฟเวอร์

3. Disconnected access คือ การผสมระหว่าง 2 วิธีแรกคือ สามารถเลือกเมล์ที่ต้องการนำมาเก็บเครื่องก่อนได้โดยไม่ต้องดาวโหลดมาทั้งหมดที่สำคัญสามารถรู้ได้ว่าได้มีการลบ E- mail ไปเท่าไหร่แล้วโดย IMAP จะสามารถจดจำเอาไว้ได้ว่าเราได้ลบ E- mail ฉบับไหนออกไปเมื่อมีการติดต่อกับเซิร์ฟเวอร์ในครั้งถัดไปจำนวน E- mail ในเครื่องกับเครื่องเซิร์ฟเวอร์ก็จะถูกปรับให้เข้ากันได้โดยอัตโนมัติ (คือการทำ Synchronized) ด้วยเทคนิคนี้ทำให้สามารถตรวจสอบ E- mail ได้จากเครื่องคอมพิวเตอร์หลาย ๆ เครื่องโดยไม่สับสน

สามารถสรุปจุดเด่นของ IMAP ได้ดังนี้

- IMAP สามารถให้บริการในรูปแบบ remote ได้ดีกว่า (คือการควบคุมการใช้ E- mail จากเครื่องไปยังเซิร์ฟเวอร์) เช่น อ่าน E- mail แบบออนไลน์ แยก E- mail กับส่วนประกอบเอกสาร (Attachment) ออกจากกันได้ซึ่งเราสามารถเลือกดาวน์โหลด E- mail มาเก็บไว้เครื่องโดยทิ้งส่วนประกอบเอกสารไว้ที่เซิร์ฟเวอร์ เพื่อดาวน์โหลดในภายหลังหรือยามว่าง
- IMAP สนับสนุนโฟลเดอร์แบบลำดับชั้นและสามารถแบ่งโฟลเดอร์ให้ใช้งานร่วมกันได้ (folder hierarchies and folder sharing) ในขณะที่ POP ไม่สามารถทำได้
- IMAP อนุญาตให้ทำการค้นหา E- mail หรือบางส่วนของ E- mail รวมทั้งเลือก E- mail ที่เราต้องการจะนำมาเก็บไว้ที่เครื่องได้ (การค้นหานี้จะทำโดยเซิร์ฟเวอร์ไม่ใช่ไคลเอนต์) แต่ถึงยังไงก็แล้วแต่ IMAP protocol ก็ยังไม่ได้รับความนิยมในปัจจุบันโดยนักเล่นอินเทอร์เน็ตทั้งหลายยังคงใช้ POP กันอยู่เนื่องจากสาเหตุหลายประการ ดังนี้

• POP3 นั้นได้ติดตั้งอยู่ในโปรแกรมชื่อดังที่มีความสามารถลูกเล่นแปลกใหม่ที่ได้รับความนิยมของผู้ใช้ทั่วไปในขณะที่ IMAP นั้นยังไม่ค่อยมีโปรแกรมที่พัฒนามากนัก

• การใช้ IMAP นั้นจะต้องใช้ทรัพยากรของเครื่องเซิร์ฟเวอร์มากขึ้นทำให้เครื่องที่เป็นเซิร์ฟเวอร์ต้องทำงานหนักขึ้นอย่างมากจึงต้องเสียค่าบริการราคาแพง แต่ POP นั้นมีให้บริการฟรี

• IMAP นั้นจะต้องใช้เวลาในการติดต่อนานกว่า เนื่องจากมีกิจกรรมที่จะต้องส่งข้อมูลระหว่างไคลเอนต์กับเซิร์ฟเวอร์เพื่อปรับเปลี่ยนข้อมูลให้ตรงกันซึ่งต่างกับ POP คือดึงข้อมูลมาแล้วก็หมด

ข้อเสียของโปรโตคอล IMAP

โปรโตคอลมีความซับซ้อนและยากในการ Implement มีซอฟแวร์ที่สนับสนุนน้อยกว่า POP IMAP เหนือกว่า POP ใน 3 ส่วนหลักๆ คือ

- มีคำสั่งในการจัดการตู้จดหมายจำนวนมาก มีความสามารถในการจัดการ folder อื่นๆ นอกเหนือจาก inbox มีจุดเด่นในการเพิ่มประสิทธิภาพของแบบออนไลน์ โดยเฉพาะกับจดหมายที่เป็น MIME และเพราะว่าขณะนี้
- มีการแจก development libraries ของ IMAP ฟรี ดังนั้นความซับซ้อนของมันคงไม่มีผลต่อความนิยมใช้ที่จะเพิ่มมากขึ้นในอนาคตโดยเน็ตสเคปวางแผนที่จะรวม IMAP เข้าไว้ใน Mail-Server รุ่นต่อไปของตนซึ่งน่าจะออกมาได้ในปีนี้
- ยิ่งไปกว่านั้น SunSoft ก็มี IMAP Server และไคลเอนต์ขณะที่ยังมี IMAP Client ที่ชื่อว่า Embla ของ ICL และ ICL/Team Ware ที่ให้ Internet Messaging Server ที่สนับสนุน POP และ IMAP ส่วนผลิตภัณฑ์อื่นๆ ที่ร่วมขบวนของ IMAP ก็ได้แก่ Control Data Mail Hub server, NetManage Z-Mail Pro และ messaging server ที่มาจาก Software.com

2.8.4 Multipurpose Internet Mail Extensions (MIME)

MIME เป็นมาตรฐานสำหรับระบุชนิดของข้อมูลมาตรฐาน MIME ถูกสร้างขึ้นมาเพื่อใช้สำหรับการส่งไฟล์แนบไปกับ E- mail แต่ภายหลังได้ถูกนำไปใช้ในหลาย ๆ งานรวมทั้ง Web Server ด้วยโดยการแบ่งชนิดของข้อมูลใน MIME นั้นจะแบ่งออกเป็น 2 ระดับโดยใช้เครื่องหมาย / คั่น เช่น text/plain หมายถึงข้อมูลที่เป็นตัวอักษร (Text) และเป็นข้อความธรรมดา ส่วน text/html หมายถึง ข้อมูลที่เป็นตัวอักษรและเป็นข้อมูล HTML หรือ image/jpg หมายถึงข้อมูลรูปภาพและเป็นรูปภาพแบบ JPG เป็นต้น การทำงานหลาย ๆ อย่างของเว็บไซต์นั้นขึ้นอยู่กับ MIME เช่น การที่บราวเซอร์ได้รับข้อมูลที่เป็น Plug-in ประเภท application/x-shockwave-flash ก็จะทำการเรียก Plug-in Shockwave Flash ขึ้นมา

การเข้ารหัสและ MIME (Multipurpose Internet Mail Extension)

การรับส่ง E-mail ผ่านเครือข่ายนั้นคอมพิวเตอร์ที่เชื่อมต่ออยู่ในโครงข่ายมักจะมีหลากหลายชนิด ดังนั้นข้อมูลที่ส่งผ่านจึงจะต้องเป็นข้อมูลที่อยู่ในรูปแบบกลาง ๆ ซึ่งคอมพิวเตอร์จะรับรู้และเข้าใจได้เหมือนกันเพื่อไม่ให้ข้อมูลที่รับหรือส่งเหล่านั้นผิดเพี้ยนไปจากความเป็นจริง และสามารถส่งข้อมูลทั้งที่เป็นข้อความและไม่เป็นข้อความ (เช่น ข้อมูลที่เป็นรูปภาพและเสียง) รวมกันไปใน E- mail ฉบับเดียวกันได้ดังนั้นจึงได้นำเทคนิคการเข้ารหัสที่เรียกว่า MIME มาใช้เพื่อเข้ารหัสและถอดรหัสในการรับส่ง E- mail โดยทั่วไป

เทคนิคของ MIME (Multipurpose Internet Mail Extensions) นี้เป็นเทคนิคที่แปลงรหัสแอสกี้ทั่วไปซึ่งมี 8 บิตให้เป็นค่า 7 บิต (ให้บิตที่ 0 มีค่าเป็น 0 เสมอ) โดยที่เทคนิคของ MIME นี้จะ

สามารถใช้รับส่งข้อมูลได้ทุก ๆ รูปแบบไม่ว่าจะเป็นข้อมูลของ E- mail หรือไฟล์ประเภทต่างๆ ที่แนบไปกับ E- mail ซึ่ง E- mail บนอินเทอร์เน็ตในยุคแรกๆ ในกรณีที่ต้องการรับส่งข้อมูลที่มีรูปแบบไฟล์แตกต่างไปจากค่าแอสกี้โดยทั่วไปผู้ส่งจะต้องแปลงรหัสข้อมูลก่อนส่งด้วยคำสั่ง UUENCODE เพื่อแปลงข้อมูลให้อยู่ในรูปแบบของ MIME ในด้านผู้รับก็จะต้องถอดรหัสข้อมูลกลับมาอยู่ในรูปแบบเดิมโดยใช้คำสั่ง UUDECOCE ซึ่งทั้ง 2 คำสั่งนี้เริ่มพัฒนาขึ้นมาพร้อมกับระบบปฏิบัติการ UNIX และภายหลังจึงมีการให้ใช้แพร่หลายในระบบปฏิบัติการอื่นๆ แต่ในปัจจุบันโปรแกรมที่ทำหน้าที่รับส่ง E- mail จะทำหน้าที่แปลงและถอดรหัสข้อมูลให้อัตโนมัติโดยไม่จำเป็นต้องอาศัยคำสั่ง UUENCODE และ UUDECODE อีกต่อแล้ว

ลักษณะข้อมูลของ MIME ประกอบด้วย 2 ส่วน คือ ส่วนหัวหรือเรียกว่า Content Transfer Encode ซึ่งจะเก็บรายละเอียดของไฟล์ที่เข้ารหัสไว้ เช่น ประเภทของไฟล์เป็นต้น ส่วนที่ 2 เป็นส่วนของข้อมูลที่เข้ารหัสแล้วการเข้ารหัสและการถอดรหัสของ MIME นี้จะถูกระบุไว้ในส่วนหัวเพื่อให้ผู้รับและผู้ส่งเข้าใจตรงกันว่า E- mail นี้เข้ารหัสและถอดรหัสด้วยวิธีใดซึ่งมีอยู่ด้วยกัน 6 วิธี คือ

- วิธีเข้ารหัสแบบ Quoted-Printable
  เทคนิคการเข้ารหัสวิธีนี้จะแปลงข้อมูลให้อยู่ในลักษณะที่อ่านได้เสมอซึ่งหากข้อมูลเป็นแอสกี้ 7 บิต อยู่แล้วก็จะไม่มีการแปลงข้อมูลแต่ถ้าเป็นค่าบิตที่ศูนย์มีค่าเป็น 1 จะถูกแปลงให้มาอยู่ในรูปค่าของเลขฐาน 16 (01234567890ABCDEF) และนำหน้าด้วยเครื่องหมายเท่ากับ (=) ตัวอย่าง เช่น ข้อมูลที่เขารหัสแล้วมีค่าเป็น = A1 หมายถึงข้อมูลที่ค่า แอสกี้ เป็น 161 (ในภาษาไทยคือ ค่า 'ก') หรือค่า Hex เป็น A1 เป็นต้น
- วิธีเข้ารหัสแบบ Base64
  เป็นเทคนิคการเข้ารหัสโดยจะแปลงข้อมูลจำนวน 24 บิต (ข้อมูล 8 บิตจำนวน 3 ไบต์) ออกเป็นข้อมูล 6 บิตจำนวน 4 ชุด โดยหลังจากที่เข้ารหัสแล้วข้อมูลจะถูกแปลงให้อยู่ในรูปของตัวอักษร 64 ตัว มีค่าตามตาราง Base64 Alphabet แต่ข้อมูลดังกล่าวจะไม่เปลี่ยนแปลงค่าของ Carriage Return และ Line Feed และปิดท้ายข้อมูลด้วยเครื่องหมาย = ซึ่งเรียกว่า PAD Binary เป็นข้อมูลที่ต่อเนื่องกันเป็นค่าไบนารีไม่แบ่งออกเป็นบรรทัดซึ่งข้อมูลประเภทนี้จะส่งโดยไม่มีการเข้ารหัสข้อมูล
- วิธีเข้ารหัสแบบ Seven-Bit
  เป็นข้อมูลที่มีค่าแอสกี้ 7 บิต ซึ่งข้อมูลประเภทนี้จะส่งโดยไม่มีการเข้ารหัสข้อมูล
- วิธีเข้ารหัสแบบ Eight-Bit
  เป็นข้อมูลที่มีค่าแอสกี้ 8 บิต ซึ่งข้อมูลประเภทนี้จะส่งโดยไม่มีการเข้ารหัสข้อมูล
- วิธีเข้ารหัสแบบ X-Token

เป็นเทคนิคการเข้ารหัสที่ต้องมีการติดต่อและตกลงกันระหว่างด้านผู้ส่งและผู้รับของ SMTP Server ก่อนเป็นเทคนิคการเข้ารหัสที่ต้องมีการติดต่อและตกลงกันระหว่างด้านผู้ส่งและผู้รับของ SMTP Server ก่อน

- การรักษาความปลอดภัยและการเข้ารหัส E- mail

  การที่ต้องให้ E- mail มีความปลอดภัยในการรับส่งข้อมูลมากขึ้นก็เพื่อป้องกันไม่ให้ผู้อื่นลักลอบอ่านข้อความได้และในการแปลงรหัสตามวิธีของ MIME เน้นได้มีข้อกำหนดเพิ่มเติมเรียกว่า S/MIME ซึ่งพัฒนาขึ้นโดย RSA Data Security Inc. โดยเพิ่มเติมในส่วนของระบบรักษาความปลอดภัยขึ้นจากมาตรฐานของ MIME แบบเดิมกระบวนการของ S/MIME ที่ได้เพิ่มในส่วนการทำหน้าที่เข้ารหัสข้อมูล (Encryption) และการส่งลายเซ็นดิจิตอล (Digital Signature) เข้าไปในข้อมูล E- mail การเข้ารหัสข้อมูลนั้น S/MIME จะใช้วิธีการ Public-Key โดยใช้คีย์ที่มีความยาวได้สูงสุด 2,048 บิตและวิธีการเข้ารหัสข้อมูลนั้นมีใช้ทั้งวิธีการเข้ารหัสข้อมูลนั้นมีใช้ทั้งวิธีของ DES (Data Encryption Standard) และ Triple DES ในกรณีการเข้ารหัสของลายเซ็นดิจิตอลนั้น RSA ได้พัฒนาไลบรารีภาษา C ที่เรียกว่า TIPEM เพื่อให้ผู้พัฒนา Software ต่าง ๆ นำไปพัฒนาตามมาตรฐานของ S/MIME

ในปัจจุบันถึงแม้ว่า S/MIME จะยังไม่ถูกกำหนดให้เป็นโปรโตคอลมาตรฐานในการรักษาความปลอดภัยของ E- mail แต่ก็ถือว่าได้รับการยอมรับเป็นมาตรฐานไปโดยปริยายเพราะมีการใช้งานมาก (De facto Standard) เนื่องจากบริษัทพัฒนา Software ชั้นนำหลายแห่ง ไม่ว่าจะเป็น Microsoft, Nescape, Lotus, Verisgn หรือ Novell ก็ตามได้นำเอาโปรโตคอล S/MIME นี้ไปใช้งานแล้ว ในขณะที่โปรโตคอล S/MIME กำลังรอการรับรองมาตรฐานอยู่นี้การเข้ารหัสแบบ MOSS หรือ MIME Object Security Services หรือที่เรียกอีกอย่างหนึ่งว่า PEM-MIME (Privacy Enhanced Mail MIME) ก็กำลังมีการพัฒนาตาม RFC 1848 อยู่ โดย MOSS ได้พยายามแก้ไขจุดอ่อนของ S/MIME จากการที่โปรโตคอล S/MIME จะใช้มาตรฐานการเข้ารหัสแบบเดียวในทุก ๆ ส่วนของ E- mail แต่ MOSS จะแบ่ง E- mail ออกเป็นส่วน ๆ แต่ละส่วนจะใช้วิธีการเข้ารหัสและคีย์ที่แตกต่างกันไป ซึ่งจะช่วยให้ E- mail มีความปลอดภัยมากยิ่งขึ้นแต่อย่างไรก็ดีความซับซ้อนของโปรโตคอล MOSS ก็ทำให้การกำหนดมาตรฐานและการพัฒนาผลิตภัณฑ์ออกมามีความยุ่งยากมากขึ้นตามไปด้วย

2.9 FTP Server

FTP ย่อมาจาก File Transfer Protocol เป็นบริการรับส่งไฟล์ระหว่างเครื่องคอมพิวเตอร์ FTP Server เป็นคอมพิวเตอร์ที่ทำหน้าที่เป็นผู้ให้บริการ FTP บริการของ FTP มีอยู่สองอย่างด้วยกันคือ

- download เป็นบริการรับไฟล์หรือคัดลอกไฟล์จากเครื่องคอมพิวเตอร์ที่เป็น FTP Server มายังเครื่องคอมพิวเตอร์ของผู้ใช้
- upload เป็นบริการส่งไฟล์หรือคัดลอกไฟล์จากเครื่องคอมพิวเตอร์ของท่านไปยังเครื่องคอมพิวเตอร์ที่เป็น FTP Server

บริการ FTP มักนำมาใช้ประโยชน์ในเรื่องของ Freeware และ Shareware

- Freeware หมายถึงซอฟต์แวร์ที่ผู้ผลิตแจกให้ใช้ฟรี
- ส่วน Shareware หมายถึง ซอฟต์แวร์ที่ผู้ผลิตแจกให้ลองไปใช้ดูก่อนและเมื่อใช้แล้วพอใจจะนำไปใช้จริงก็ค่อยส่งเงินมาชำระทีหลัง ถ้าไม่นำไปใช้จริงก็ไม่ต้องส่งเงินมาชำระ

ผู้ผลิต Freeware และ ผู้ผลิต Shareware จะทำการส่งซอฟต์แวร์ของตนเองที่ต้องการแจกจ่ายไปไว้ที่คอมพิวเตอร์ที่เป็น FTP Server และใครก็ตามที่สนใจจะลองนำไปซอฟต์แวร์ของผู้ผลิตไปใช้ดูก็ให้ไปทำการดาวน์โหลดจากคอมพิวเตอร์ที่เป็น FTP Server เครื่องนั้นมายังเครื่องคอมพิวเตอร์ของตนเอง ในบางกรณีถ้าท่านมีข้อมูลที่น่าสนใจและต้องการเผยแพร่ ท่านก็สามารถส่งข้อมูลนั้นไปไว้ที่ FTP Server ได้ ตัวอย่าง FTP Server เช่น ftp.kmitl.ac.th

ทิศทางการถ่ายโอนข้อมูล

การใช้คำสั่ง FTP จะถือว่าเครื่องคอมพิวเตอร์ที่เรียกใช้ FTP เป็น เครื่องคอมพิวเตอร์ต้นทาง (Local Host Computer) และเครื่องคอมพิวเตอร์ ที่ถูกเรียกด้วยคำสั่ง FTP เป็นเครื่องคอมพิวเตอร์ปลายทาง

คำสั่งต่างๆที่ใช้ใน FTP

- คำสั่ง dir

  dir เป็นคำสั่งสำหรับดูชื่อแฟ้มข้อมูลและชื่อไดเรคทอรีในเครื่องคอมพิวเตอร์ปลายทาง

- คำสั่ง cd

  cd เป็นคำสั่งที่ใช้เปลี่ยนไปยังไดเรคทอรีย่อยของเครื่องคอมพิวเตอร์ปลายทาง ที่ต้องการ

- คำสั่ง cd .. หรือ cdup

  cd .. หรือ cdup เป็นคำสั่งที่ใช้เปลี่ยนไดเรคทอรีขึ้นไปอีกหนึ่งระดับของเครื่องคอมพิวเตอร์ปลายทาง

- คำสั่ง get [ชื่อแฟ้มต้นทาง] [ชื่อแฟ้มปลายทาง]

  get เป็นคำสั่งที่ใช้คัดลอกแฟ้มจากคอมพิวเตอร์ปลายทางไปยังคอมพิวเตอร์ต้นทางในกรณีที่ไม่พิมพ์ชื่อแฟ้มปลายทางเครื่องจะตั้งชื่อแฟ้มปลายทางเหมือนกับชื่อแฟ้มต้นทาง

- คำสั่ง mget [ชื่อแฟ้ม] [ชื่อแฟ้ม] mget

  เป็นคำสั่งคัดลอกแฟ้มหลาย ๆ แฟ้มจาก คอมพิวเตอร์ปลายทางตามรูปแบบที่กำหนดมาที่คอมพิวเตอร์ต้นทางโดยเครื่องจะถามความต้องการที่ละแฟ้มข้อมูล

- คำสั่ง quit หรือ bye quit หรือ bye

  เป็นคำสั่งที่ใช้ออกจาก ftp

สรุปคำสั่งใน FTP

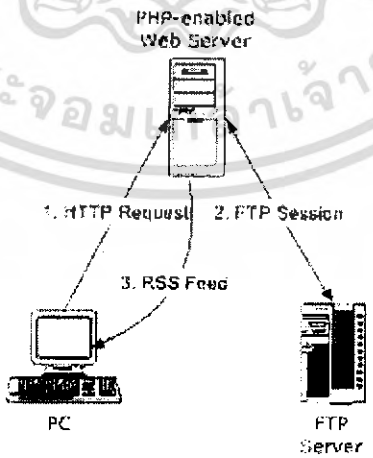
ตาราง 2.2 ตารางสรุปคำสั่งใน FTP

[คำสั่ง] / help [คำสั่ง]	แสดงข้อความช่วยเหลือ อธิบายคำสั่งใน ftp
asscii	คัดลอกแฟ้มข้อมูลแบบแอสกี้
binary	คัดลอกแฟ้มข้อมูลแบบไบนารี
bell	ให้ส่งเสียงเมื่อคัดลอกแฟ้มข้อมูลเสร็จ
bye	จบการทำงานและออกจาก FTP
cd [ไดเรกทอรี]	เปลี่ยนไดเรคทอรี ของคอมพิวเตอร์ปลายทาง
cd .. หรือ cdup	เปลี่ยนไดเรคทอรีของคอมพิวเตอร์ปลายทางขึ้นไปหนึ่งระดับ
Lcd [ไดเรคทอรี]	เปลี่ยนไดเรคทอรีของคอมพิวเตอร์ปลายทาง
close หรือ disconnect	จบการเชื่อต่อกับคอมพิวเตอร์ปลายทางแต่ยังไม่ออกจาก FTP
dir [ชื่อแฟ้ม]	แสดงรายชื่อแฟ้มของคอมพิวเตอร์ปลายทาง
Get [ชื่อแฟ้ม] [ชื่อแฟ้ม]	คัดลอกแฟ้มจากคอมพิวเตอร์ปลายทางมาที่คอมพิวเตอร์ต้นทาง

mget [ชื่อแฟ้ม] [ชื่อแฟ้ม]	คัดลอกแฟ้มจากคอมพิวเตอร์ปลายทางมาที่คอมพิวเตอร์ต้นทางแบบหลายแฟ้ม
Put [ชื่อแฟ้ม] [ชื่อแฟ้ม]	คัดลอกแฟ้มจากคอมพิวเตอร์ต้นทางไปไว้ที่คอมพิวเตอร์ปลายทาง
mput [ชื่อแฟ้ม] [ชื่อแฟ้ม]	คัดลอกแฟ้มจากคอมพิวเตอร์ต้นทางไปไว้ที่ คอมพิวเตอร์ปลายทางแบบหลายแฟ้ม
prompt [on] [off]	กำหนดให้มีการโต้ตอบกับผู้ใช้เพื่อเลือกแฟ้มเมื่อใช้ mget, mput
pwd	แสดงไดเรคทอรีของรีโมตโฮสต์

การทำงานของ FTP

FTP ทำงานแบบ Client / Server โดยสร้างการเชื่อมต่อ (connection oriented) ขึ้นมาก่อนทุกครั้ง เครื่องไคลเอนต์จะต้องระบุหมายเลขไอพีแอดเดรสของเครื่อง FTP Server ที่อยู่ปลายทางแล้วใส่ชื่อผู้ใช้และรหัสผ่านจากนั้นเครื่องไคลเอนต์จะเป็นเสมือนเทอร์มินัลของ FTP Server เว็บไซต์ที่แสดงแอดเดรส URL ขึ้นต้นด้วย ftp:// แสดงว่าเป็น FTP Server ที่คอยบริการดาวน์โหลดไฟล์ต่างๆ ซึ่งมีหลักการทำงานพื้นฐานดังรูปที่ 2.9



รูปที่ 2.9 การทำงานพื้นฐานของ FTP Server

2.10 รูปแบบการโจมตีและการป้องกัน

จุดประสงค์ของการโจมตีโครงข่ายทั้งจากทางอินเทอร์เน็ตหรือโครงข่ายองค์กรมีมากมายหลายประการ ซึ่งพอที่จะแบ่งประเภทการโจมตีออกเป็นระดับชั้นดังนี้

- Denial of Service Attack
- Null Session
- Buffered Overflow
- Rootkits
- IP Spoofing
- Sniffing
- SSH Brute Force
- Back door
- Zero Day Attacks

2.10.1 การโจมตีแบบ Denial of Service Attack

Denial of Service Attack (DOS) เป็นรูปแบบการโจมตีที่มีจุดประสงค์เพื่อการทำให้โครงข่ายหรือโฮมเพจรวมทั้งเซิร์ฟเวอร์บนโครงข่ายปฏิเสธการให้บริการหรือไม่สามารถดำเนินการต่อไปได้ลักษณะการโจมตีแบบนี้เป็นการทำให้โครงข่ายเต็มไปด้วย Traffic ขนาดมหาศาลซึ่งคล้ายกับการที่มีบุคคลเป็นจำนวนมากต่างพร้อมใจกันโทรศัพท์ติดต่อเข้ามาที่โทรศัพท์หมายเลขเดียวกันทำให้สายโทรศัพท์ไม่ว่างตลอดเวลาจุดประสงค์ของการโจมตีแบบ DOS นี้อาจเกิดขึ้นจากความสนุกความที่ต้องการลองวิชาหรือเจตนาในเชิงแข่งขันทางธุรกิจรวมทั้งเจตนามุ่งร้ายอื่นๆ การโจมตีในลักษณะนี้ไม่เพียงแค่ทำให้โครงข่ายติดขัดเนื่องจากปริมาณ Traffic ที่เพิ่มขึ้นเท่านั้นแต่ยังมีการส่งแพ็กเกิดพิเศษที่ถูกจัดทำขึ้นเพื่อให้โปรโตคอลการทำงานของเครื่องคอมพิวเตอร์เป้าหมายเกิดความสับสนหรือทำให้แอพพลิเคชั่นรวมทั้งการให้บริการต่าง ๆ บนเครื่องเป้าหมายหยุดทำงานหรือไม่สามารถทำงานต่อไปได้

ความเสียหายที่เกิดโดยการโจมตีในรูปแบบ DoS

ความเสียหายที่เกิดจาก DoS ส่งผลให้ผู้ใช้งานแต่ละส่วนไม่เหมือนกันแล้วแต่ว่าจะอยู่ในส่วนใด เช่น เป็นผู้เข้าไปใช้งาน, เป็นพนักงานในองค์กรที่โดนโจมตี หรือเป็นเจ้าของเครื่องที่ถูกใช้ในการโจมตี หรือจะมองในแง่ขององค์กรที่โดนโจมตีทุกๆ ฝ่ายล้วนแล้วแต่เป็นฝ่ายเสียทั้งนั้น

ยกเว้นคนที่ทำให้เหตุการณ์นี้เกิดขึ้นหรือคนที่เป็นคนบงการอยู่เบื้องหลังเท่านั้นที่ได้ประโยชน์จากการโจมตีนั้นถ้าเราจะจัดความเสียหายของ DoS นั้นก็สามารถจัดได้ตามประเภทของการทำงานของตัว DoS เอง ซึ่งสามารถแบ่งได้เป็นสองประเภทด้วยกันคือ

ความเสียหายกับเครื่องคอมพิวเตอร์

ในส่วนความเสียหายของเครื่องคอมพิวเตอร์นั้นก็สามารถมองได้สองมุมด้วยกันคือ ในมุมของเครื่องที่ถูกใช้ในการโจมตีกับในมุมของเครื่องที่โดนโจมตี

- เครื่องที่ถูกใช้เป็นเครื่องมือในการโจมตีอันดับแรกคือเราสูญเสียการควบคุมของเครื่องเราเองทำให้คนอื่นสามารถเข้ามาบงการเครื่องของเราให้ไปทำอย่างโน้นทำอย่างนี้ตามที่เขาต้องการได้อันดับสองคือการเสียทรัพยากรของเครื่องเองไม่ว่าจะเป็น ซีพียู, เมโมรี หรือแบนด์วิดธ์ เป็นต้น ทรัพยากรต่างๆ ของเครื่องที่กล่าวไปแล้วนั้นจะถูกใช้ไปรันโปรแกรมที่จะใช้ในการเข้าไปโจมตีเครื่องเหยื่อทำให้เครื่องคอมพิวเตอร์นั้นไม่สามารถใช้งานได้อย่างเต็มที่
- เครื่องที่เป็นเหยื่อในการโจมตีครั้งนี้แน่นอนว่าทำให้เครื่องนั้นไม่สามารถให้บริการต่อไปได้เพราะจุดประสงค์หลักของ DoS ก็คือสิ่งนี้เพราะเครื่องนั้นมัวแต่ประมวลผล Request จำนวนมากที่ถูกส่งเข้ามาทำให้เครื่องนั้นทำงานหนักจนไม่สามารถรับงานได้อีกต่อไปบางเครื่องอาจจะแฮงก์ไปเฉยๆ หรือระบบอาจจะ Crash เลยก็เป็นไปได้ทำให้เครื่องนั้นไม่สามารถให้บริการได้อีก

ความเสียหายกับระบบเน็ตเวิร์ค

ความเสียหายที่เกิดขึ้นกับระบบเน็ตเวิร์คนั้นเราก็สามารถมองได้สองมุมเช่นกันคือมองในมุมของผู้ที่ถูกใช้เป็นเครื่องมือในการโจมตีและผู้ที่ถูกโจมตี

- มุมที่ผู้ถูกใช้เป็นเครื่องมือ ทำให้แบนด์วิดธ์ที่เราควรจะมีเหลือไว้ใช้นั้นถูกใช้ไปกับการโจมตีเสียหมดบางครั้งก็กินแบนด์วิดธ์ทั้งหมดที่เรามีอยู่เพื่อใช้ในการโจมตีทำให้เครื่องหรือระบบที่ถูกใช้เป็นเครื่องมือในการโจมตีนั้นไม่สามารถใช้งานระบบเน็ตเวิร์คได้อีกต่อไป
- มุมที่ผู้ถูกโจมตี เช่นเดียวกับแบนด์วิดธ์ของผู้ที่ถูกโจมตีนั้นก็จะใช้ไปอย่างรวดเร็วจนหมดทำให้บริการที่เตรียมไว้ที่เครื่องที่ถูกโจมตีนั้นไม่สามารถใช้งานได้อีกต่อไปเครื่องที่ต้องการที่จะติดต่อเข้ามาที่เครื่องนี้หรือผ่านเครื่องนี้เพื่อเข้าไปในระบบข้างใน(ในกรณีที่

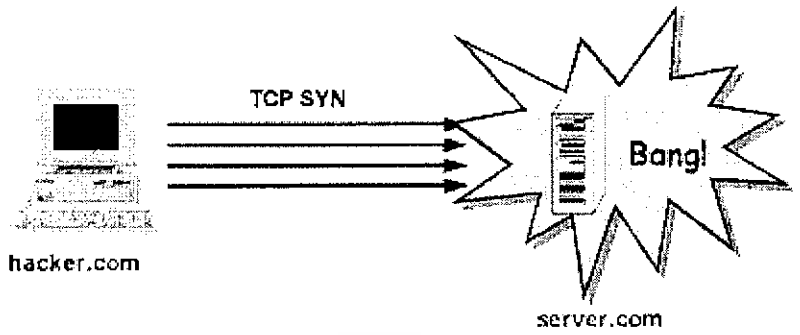
เป็นไฟร์วอลล์)ไม่สามารถใช้งานได้ผู้ที่อยู่ด้านในของระบบก็จะไม่สามารถเชื่อมต่อกับระบบภายนอกได้เช่นเดียวกันแต่ระบบแลน ภายในก็ยังสามารถใช้งานได้ตามปกติ

ความเสียหายกับองค์กร

- เมื่อเกิดการโจมตีขึ้นแล้วก็มีแต่เสียกับเสียเท่านั้นยิ่งองค์กรที่ถูกโจมตีด้วยแล้วความเสียหายนั้นก็เกิดขึ้นอย่างมากมายทีเดียวเริ่มตั้งแต่ความเสียหายของตัวเครื่องคอมพิวเตอร์หรือระบบที่โดนโจมตีเองทำให้ต้องเสียเวลาเสียค่าใช้จ่ายในการซ่อมแซมเพื่อที่ให้สามารถกลับมาให้บริการได้อย่างเดิม
- เสียโอกาสทางธุรกิจโอกาสที่จะทำธุรกรรมกับเครื่องที่โดนโจมตีหรือการทำธุรกรรมอื่น ๆ กับระบบภายในที่จำเป็นต้องต่อเชื่อมกับอินเทอร์เน็ตสูญเสีย,โอกาสที่จะทำธุรกรรมทางอินเทอร์เน็ต,โอกาสที่ลูกค้าจะเข้ามาในเว็บโอกาสที่จะปิดการขาย,โอกาสที่จะสร้างรายได้ และอีกหลาย ๆ โอกาสที่ทางองค์กรจะต้องเสียไป
- เสียภาพลักษณ์ขององค์กร องค์กรที่ถูกโจมตีด้วยการโจมตีประเภท DoS นั้นทำให้การบริการที่องค์กรนั้นเตรียมพร้อมไว้ให้บริการไม่สามารถให้บริการได้ทำให้ภาพลักษณ์ขององค์กรนั้นเสียไปเพราะไม่สามารถป้องกันเหตุที่เกิดขึ้นได้หรือไม่มีวิธีการแก้ไขที่รวดเร็วจนทำให้เกิดความเสียหายขึ้นทำให้ลูกค้าขาดความเชื่อมั่นในองค์กรว่าจะสามารถตอบสนองความต้องการของตนได้อาจเป็นเหตุให้ลูกค้าเปลี่ยนใจไปใช้บริการขององค์กรอื่นแทนในที่สุด

2.10.1.1 การโจมตีแบบ SYN Flood

การโจมตีแบบ SYN Flood เป็นการโจมตีบนพื้นฐานของโปรโตคอล TCP ผู้บุกรุกจะใช้วิธีการโจมตีด้วยในรูปแบบการเชื่อมต่อที่เรียกว่าการเปิดการเชื่อมต่อแบบครึ่งทาง (Half Open Attack) การทำเช่นนี้จะทำให้เครื่องคอมพิวเตอร์เป้าหมายไม่สามารถให้บริการในขณะที่เกิดการโจมตี หรือหลังจากที่การโจมตีเสร็จสิ้นแล้ว ซึ่งแสดงได้ดังรูปที่ 2.10



รูปที่ 2.10 ลักษณะการโจมตีแบบ TCP SYN Flood

ลักษณะการโจมตีได้แก่การส่งข่าวสารที่เกี่ยวกับการร้องขอการสถาปนาการเชื่อมต่อบนโปรโตคอลของ TCP ไปยังเครื่องเป้าหมายอย่างรวดเร็วและมากมายเกินกว่าที่เครื่องเป้าหมายจะสามารถทำงานได้ทัน

- ผู้โจมตีจะใช้ซอฟต์แวร์เพื่อจัดสร้างแอดเดรสต้นทางแบบสุ่มไม่เรียงลำดับขึ้นสำหรับแต่ละแพ็กเก็ตที่จะร้องขอไปยังเครื่องเป้าหมาย
- ในแต่ละแพ็กเก็ตที่จะส่งออกไปได้มีการตั้งค่า Flag หรือสถานะของ TCP ให้เป็น SYN เพื่อขอเปิดการเชื่อมต่อไปยังเครื่องปลายทางโดยแต่ละแพ็กเก็ตนี้ยังได้ใส่แอดเดรสลวงอีกด้วย
- เมื่อเครื่องปลายทางได้รับแพ็กเก็ตเป็นที่เรียบร้อยแล้วเครื่องปลายทางจะรอการยืนยันจากเครื่องต้นทางที่ไม่มีวันจะเกิดขึ้น (เนื่องจากเครื่องต้นทางเป็นเครื่องลวง) การรอจะเกิดขึ้นประมาณ 3 นาที
- เครื่องปลายทางจะทำการสำรองหน่วยความจำจำนวนหนึ่งเป็นบัฟเฟอร์เพื่อเก็บตารางการเชื่อมต่อไว้และรอการตอบสนองจากเครื่องต้นทางในขณะนั้นถ้ามีใครติดต่อเข้ามาเพื่อขอเปิดการเชื่อมต่อก็จะไม่มีการตอบสนองใด ๆ เกิดขึ้นซึ่งในขณะนั้นหากเครื่องเป้าหมายเป็นเซิร์ฟเวอร์ดังนั้นผู้ใดก็ตามที่ติดต่อกับเซิร์ฟเวอร์ในขณะนั้นจะไม่ได้รับความสนใจยกเว้นจะมีผู้มาขอเปิดการเชื่อมต่อเท่านั้น
- เมื่อเวลาล่วงเลยไปสักระยะหนึ่ง (เวลาสั้น ๆ) ถ้าไม่มีการตอบสนองจากเครื่องต้นทางอีกทั้งหมดเวลาการรอคอยแล้ว เครื่องที่เป็นเป้าหมายการโจมตีก็จะยกเลิกการเชื่อมต่อและคืนหน่วยความจำให้แก่ระบบ
- การโจมตีในลักษณะนี้เป็นการทำให้เซิร์ฟเวอร์เหมือนคนที่เกิดอารมณ์ค้างอย่างต่อเนื่องโดยการโจมตีจะเกิดขึ้นอย่างต่อเนื่องติด ๆ กันด้วยความเร็วสูงและทุกครั้งที่โจมตีโดยขอเปิดการเชื่อมต่อนี้เครื่องเป้าหมายจะต้องสำรองหน่วยความจำเพื่อใช้ในการตอบสนองการขอเชื่อมต่อทุก

ครั้ง และหากการโจมตีเกิดขึ้นอย่างต่อเนื่องและความเร็วสูงมากก็จะทำให้เครื่องเป้าหมายไม่สามารถจัดสรรหน่วยความจำมาใช้เพื่อการนี้ได้ทัน ส่งผลทำให้เครื่องเป้าหมายอาจไม่มีหน่วยความจำมาให้บริการแอพพลิเคชั่นอื่น ๆ ได้

ระบบปฏิบัติการสมัยใหม่สามารถจัดสรรทรัพยากร เช่น หน่วยความจำได้ดีกว่าแต่ก่อน ดังนั้นจึงเป็นเรื่องยากที่ทำให้เกิดปัญหา Overflow แต่ SYN Flood ก็ยังเป็นการโจมตีที่อันตราย อย่างไรก็ดี SYN Flood อาจไม่ได้เป็นเครื่องมือหลักในการโจมตี เพียงแต่เป็นตัวเสริมเท่านั้น

เทคนิคการตรวจสอบ TCP SYN Flood

ผู้ใช้งานเซิร์ฟเวอร์ที่กำลังถูกโจมตีอาจไม่รู้สึกถึงความผิดปกติที่เกิดขึ้น เนื่องจากการขอเชื่อมต่อแบบลวงโลกนี้ไม่ได้สร้างความผิดปกติใด ๆ เกิดขึ้นอย่างชัดเจน แต่ผู้ใช้งานเซิร์ฟเวอร์อาจรู้สึกถึงปัญหาที่เกิดขึ้นหากเขาพยายามที่จะ Access เข้าไปที่บริการใดบริการหนึ่งของเซิร์ฟเวอร์

เพื่อที่จะพิสูจน์ว่าเซิร์ฟเวอร์กำลังถูกโจมตีหรือไม่ ให้ตรวจสอบสถานะ Traffic ของเซิร์ฟเวอร์ตัวอย่าง หากท่านใช้ยูนิกซ์ เช่น SunOS ท่านอาจต้องใช้คำสั่งดังนี้

netstat -a -f inet (Inet หมายถึงไอพีแอดเดรสของเซิร์ฟเวอร์)

หากผลที่แสดงออกมาปรากฏว่ามีสถานะที่เรียกว่า "SYN_RECEIVED" ปรากฏบนหน้าจอขึ้นมากมาย นั่นคือสัญญาณบอกเหตุว่าท่านกำลังถูกโจมตีแล้ว

รายละเอียด

เป็นการโจมตีโดยการส่งแพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมายเสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายังไอพีแอดเดรสต้นทางที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุในไอพีแอดเดรสต้นทางไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมากก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็มทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมากยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย การโจมตีแบบ SYN Flood เป็นการโจมตีบนพื้นฐานของโปรโตคอล TCP ผู้บุกรุกจะใช้วิธีการโจมตีด้วยในรูปแบบการเชื่อมต่อที่เรียกว่าการเปิดการเชื่อมต่อแบบครึ่งทาง (Half Open Attack) การทำเช่นนี้จะทำให้เครื่อง

คอมพิวเตอร์เป้าหมายไม่สามารถให้บริการในขณะที่เกิดการโจมตี หรือหลังจากที่การโจมตีเสร็จสิ้นแล้ว ลักษณะการโจมตีได้แก่การส่งข่าวสารที่เกี่ยวกับการร้องขอการสถาปนาการเชื่อมต่อบนโปรโตคอลของ TCP ไปยังเครื่องเป้าหมายอย่างรวดเร็วและมากมายเกินกว่าที่เครื่องเป้าหมายจะสามารถทำงานได้ทัน

ระบบปฏิบัติการสมัยใหม่สามารถจัดสรรทรัพยากร เช่น หน่วยความจำได้ดีกว่าแต่ก่อน ดังนั้นจึงเป็นเรื่องยากที่ทำให้เกิดปัญหา Overflow แต่ SYN Flood ก็ยังเป็นการโจมตีที่อันตราย อย่างไรก็ดี SYN Flood อาจไม่ได้เป็นเครื่องมือหลักในการโจมดี เพียงแต่เป็นตัวเสริมเท่านั้น

การป้องกัน

- โดยใช้ iptables

Protect Syn Flood

[root@localhost]#iptables-N syn-flood

[root@localhost]#iptables -A syn-flood -i ppp0 -m limit --limit 75/s --limit-burst 100 -j RETURN

[root@localhost]#iptables -A syn-flood -j LOG --log-prefix "SYN-FLOOD: "

[root@localhost]#iptables -A syn-flood -j DROP

เปิดการใช้งาน IP Forward ป้องกัน Syn Flood และ อนุญาตให้มีการใช้งานแบบ Dynamic IP)

[root@localhost]#echo 1 > /proc/sys/net/ipv4/ip_forward

[root@localhost]#echo 1 > /proc/sys/net/ipv4/tcp_syncookies

[root@localhost]#echo 1 > /proc/sys/net/ipv4/ip_dynaddr

- Cisco Router

เราท์เตอร์ของ Cisco มีฟังก์ชันการทำงานชื่อ TCP Intercept ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood โดย TCP intercept software จะพยายามสร้างการเชื่อมต่อกับไคลเอ็นต์ หากสำเร็จการเชื่อมต่อดังกล่าวก็จะถูกส่งไปให้กับเครื่องให้บริการต่อไป ดังนั้นการโจมตีแบบ SYN flood จะไม่สามารถเข้าไปถึงเครื่องเป้าหมายจริงๆ ได้ และเราท์เตอร์ก็ถูกออกแบบให้รองรับการเชื่อมต่อได้มากกว่าเครื่องให้บริการ (Server) อีกด้วย แต่ก็มีข้อเสียคือจะทำให้เราท์เตอร์ใช้ทรัพยากรมากกว่าปกติ รายละเอียดเพิ่มเติมศึกษาได้

นอกจากนี้เราท์เตอร์ของ Cisco ยังมีฟังก์ชันชื่อ Committed Access Rate (CAR) ซึ่งใช้ในการจำกัดแบนด์วิดธ์ที่ใช้สำหรับแต่ละบริการได้ (แก้ไขได้ผ่านทาง extended access control list) ซึ่งไม่เพียงแต่ป้องกันการโจมตีแบบ SYN flood ยังป้องกันการเชื่อมต่อที่ถูกต้องไม่ให้ใช้แบนด์วิดธ์

มากเกินไป ซึ่งข้อเสียในการนำไปใช้งานคือในขณะที่เครื่องเป้าหมายถูกโจมตีจะทำให้การเชื่อมต่อจากผู้ใช้ธรรมดาไม่สามารถทำได้ เทคนิคหนึ่งในการนำ CAR ไปใช้งานคือการจำกัดการเข้าถึงโดยระบุเป็นจำนวนไคลเอ็นต์ที่สามารถเข้าใช้งานได้

- Checkpoint FW-1

Checkpoint เป็น ผลิตภัณฑ์ระดับ Enterprise Firewall

Checkpoint FW-1

FW-1 มีฟังก์ชั่นชื่อ SYN Defender ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood โดยใช้หลักการเช่นเดียวกันกับ Cisco's TCP Intercept ซึ่งจะทำให้ SYN packet ถูกหยุดยั้งไว้ที่ FW-1 เช่นเดียวกันกับ Cisco's TCP Intercept ตัว FW-1 เองก็จะใช้ทรัพยากรมากกว่าปกติในการทำงานในลักษณะดังกล่าว

FW-1 มีฟังก์ชั่นชื่อ SYN Defender ซึ่งถูกออกแบบมาเพื่อต่อต้านการโจมตีแบบ SYN flood โดยใช้หลักการเช่นเดียวกันกับ Cisco's TCP Intercept ซึ่งจะทำให้ SYN packet ถูกหยุดยั้งไว้ที่ FW-1 เช่นเดียวกันกับ Cisco's TCP Intercept ตัว FW-1 เองก็จะใช้ทรัพยากรมากกว่าปกติในการทำงานในลักษณะดังกล่าว

2.10.1.2 การโจมตีแบบ ICMP Flood

ลักษณะการโจมตีจะใช้ข้อบกพร่องของ Fragment ในการโจมตีโดยส่ง ICMP Echo Request ที่ Fragment ไปยังเป้าหมายเรื่อยๆ เพื่อให้ผลรวมของ Fragment นั้นเกินกว่าขนาด 64 K (เกิด Overflow) โปรแกรมทำงานผิดเพี้ยน / เครื่องหยุดทำงาน

รายละเอียด

เป็นการส่งแพ็คเก็ต ICMP จำนวนมากไปยังเป้าหมายทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่ การป้องกันระบบส่วนใหญ่สามารถทำงานได้โดยไม่ต้องใช้ ICMP Echo Request ซึ่งสามารถป้องกันการใช้งานได้โดยใช้คำสั่งที่เราท์เตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ ปรับปรุง OS ให้มีกลไกในการควบคุมขนาดและความต่อเนื่องของแพ็กเก็ตที่รัดกุมเพียงพอ

2.10.1.3 การโจมตีแบบ UDP Flood

เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมายซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่ หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมดโดยจะส่ง UDP packet ไปยังพอร์ตที่กำหนดไว้เช่น 53 (DNS)

การป้องกัน

เราท์เตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop แพ็คเก็ตที่มุ่งโจมตีมายังพอร์ตที่ไม่เป็นที่ต้องการได้ เช่น โจมตีมายังพอร์ตที่ไม่ได้ให้บริการในพอร์ตดังกล่าวในกรณีที่เป็นการโจมตีเฉพาะพอร์ตที่เปิดให้บริการ เช่น พอร์ต 53 ก็สามารถป้องกันระบบเป้าหมายได้โดยใช้ CAR เพื่อจำกัดจำนวนข้อมูล

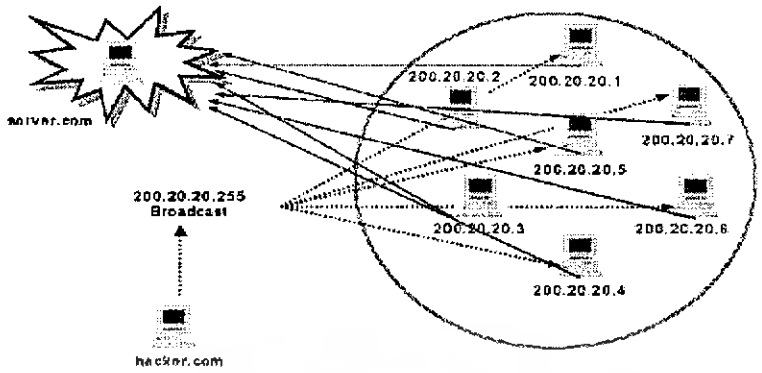
2.10.1.4 การโจมตีแบบ Teardrop

โดยปกติแล้วการที่เราจะส่ง Packet ข้อมูลขนาดใหญ่ผ่านเราท์เดอร์ออกไปยัง Layer ระดับล่างนั้นโดยที่ Packet มีขนาดต่างๆ กันไปนั้นเราท์เตอร์จะไม่ยอมให้ผ่านจะต้องทำ Fragment เสียก่อน จึงจะยอมให้ผ่านได้และเมื่อผ่านไปแล้วเครื่องของผู้รับปลายทางจะนำแพ็กเก็ตที่ถูกแบ่งออกเป็นชิ้นส่วนต่างๆ ด้วยวิธีการ Fragment มารวมเข้าด้วยกันเป็นแพ็กเก็ตที่สมบูรณ์การที่สามารถนำมารวมกันได้นี้จะต้องอาศัยค่า Offset ที่ปรากฏอยู่ในแพ็กเก็ตแรกและแพ็กเก็ตต่อๆ ไปสำหรับการโจมตีแบบ Teardrop นี้ผู้โจมตีจะส่งค่า Offset ในแพ็กเก็ตที่สองและต่อๆ ไปที่จะทำให้เครื่องรับปลายทางเกิดความสับสนหากระบบปฏิบัติการไม่สามารถรับมือกับปัญหานี้ก็จะทำให้ระบบหยุดการทำงานในทันที

2.10.1.5 การโจมตีแบบ Smurf

ลักษณะการโจมตีแบบนี้ผู้โจมตีจะใช้วิธีการที่เรียกว่ายืมมือฆ่ากันพูดง่าย ๆ คือการยุแหย่ให้เกิดการรุมตีกันบนโครงข่ายวิธีการโจมตีได้แก่การส่ง IP Ping ไปที่ไอพีแอดเดรสหนึ่งได้แก่ IP ที่ลงท้ายด้วย .255 ซึ่งเป็นแอดเดรสเพื่อการ Broadcasting เฉพาะโครงข่ายนั้นและแน่นอนผู้โจมตีจะต้องสร้างไอพีแอดเดรสลวงขึ้นมาซึ่งเป็นไอพีแอดเดรส ของเซิร์ฟเวอร์ที่ต้องการจะถูกโจมตี

หลังจากที่มีการ Ping ไปที่แอดเดรสดังกล่าวแล้วแอดเดรสที่เป็น Broadcasting นี้จะทำการ Broadcast ไปที่คอมพิวเตอร์ทุกตัวบนโครงข่ายซึ่งเมื่อทุกเครื่องได้รับการ Ping แล้วก็จะเข้าใจว่าเป็นการ Ping มาจากเครื่องที่เป็นเซิร์ฟเวอร์ดังนั้นทุกเครื่องก็จะส่งข่าวสาร Echo สนองตอบกลับมาที่เซิร์ฟเวอร์เพียงเครื่องเดียวในเวลาเดียวกันซึ่งจะทำให้เซิร์ฟเวอร์ทำงานช้าลงเนื่องจากถูกถล่มและหาก Hacker ทำการส่ง Ping ออกมาอย่างต่อเนื่องและมีข่าวสารขนาดใหญ่ผลก็คือ เซิร์ฟเวอร์แทบจะใช้งานไม่ได้ลักษณะการโจมตีแบบ Smurf นี้ แสดงได้ดังรูปที่ 2.11



รูปที่ 2.11 ลักษณะการโจมตีแบบ Smurf

การป้องกัน

เช่นเดียวกันกับการโจมตีแบบ ICMP flood เราท์เตอร์และอุปกรณ์กรองแพ็คเก็ตอื่นๆ สามารถ drop ICMP Echo Reply ซึ่งในกรณีนี้ควร drop ICMP Echo Reply ที่ส่งเข้ามาโดยไม่ได้มีการส่ง ICMP Echo Request ออกไปก่อนซึ่งการทำงานลักษณะนี้อาจจะทำให้อุปกรณ์ packet filtering ใช้ทรัพยากรเพิ่มขึ้นและในกรณีที่เกิดการโจมตีขึ้นแล้วยังสามารถบล็อกไอพีแอดเดรสต้นทางของ ICMP Echo Reply ได้เพราะผู้โจมตีไม่สามารถเปลี่ยนแปลงข้อมูลส่วนนี้ได้

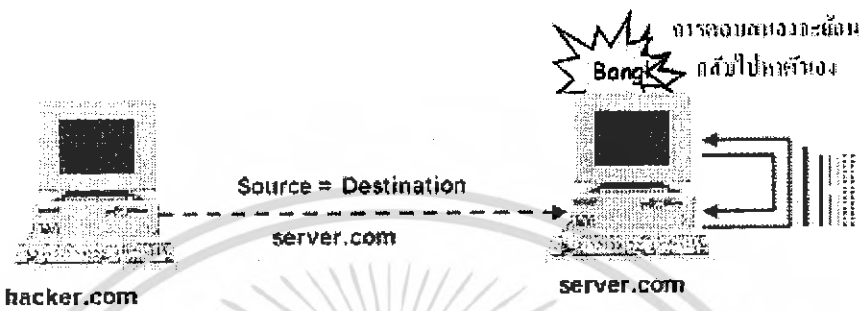
สำหรับผู้ดูแลระบบทั่วไปควรป้องกันไม่ให้ระบบของตัวเองถูกใช้เป็นตัวกรองแพ็กเก็ตโดยการไม่ตอบสนองต่อแพ็กเก็ตที่ส่งเข้ามายัง broadcast address ซึ่งวิธีการแก้ไขแยกตามระบบที่ใช้

2.10.1.6 การโจมตีแบบ Land Attack

ลักษณะการโจมตีประเภทนี้เป็นการส่ง SYN ไปที่เครื่องเป้าหมายเพื่อขอสถาปนาการเชื่อมต่อซึ่งเครื่องที่เป็นเป้าหมายจะต้องตอบรับคำขอการเชื่อมต่อด้วย SYN ACK ไปที่เครื่องคอมพิวเตอร์ต้นทางเสมอแต่เนื่องจากว่าไอพีแอดเดรสของเครื่องต้นทางกับเครื่องที่เป็นเป้าหมายนี้มีไอพีแอดเดรสเดียวกันโดยการใช้วิธีการสร้างไอพีแอดเดรสลวง (โดยข้อเท็จจริงแล้วเครื่องของ Hacker จะมีไอพีแอดเดรสที่ต่างกับเครื่องเป้าหมายอยู่แล้วแต่จะใช้วิธีการทางซอฟต์แวร์ในการส่งแพ็กเก็ตที่ประกอบด้วยคำขอการเชื่อมต่อพร้อมด้วยไอพีแอดเดรสปลอม) ซึ่งโปรโตคอลของเครื่องเป้าหมายไม่สามารถแยกแยะได้ว่าไอพีแอดเดรสที่เข้ามาเป็นเครื่องปัจจุบันหรือไม่ก็จะทำการตอบสนองด้วย SYN ACK ออกไป

หากแอดเดรสที่ขอเชื่อมต่อเข้ามาเป็นแอดเดรสเดียวกับเครื่องเป้าหมาย ผลก็คือ SYN ACK นี้จะย้อนเข้าหาตนเอง และเช่นกันที่การปล่อย SYN ACK แต่ละครั้งจะต้องมีการปันส่วนของ

หน่วยความจำเพื่อการนี้จำนวนหนึ่งซึ่งหากผู้โจมตีส่งคำขอเชื่อมต่อออกมาอย่างต่อเนื่องก็จะเกิดปัญหาการจัดสรรหน่วยความจำอีกทั้งต้องมาประมวลผลในส่วนของการเชื่อมต่อก็จะทำให้เครื่องเป้าหมายทำงานช้าลงหรือหยุดทำงานได้ซึ่งการโจมตีแบบ Land Attack แสดงดังรูปที่ 2.12



รูปที่ 2.12 ลักษณะการโจมตีแบบ Land Attack

การป้องกัน

- ปรับปรุง TCP Stack ให้รัดกุมขึ้น
- ป้องกันการปลอม IP
- ปรับปรุงระบบการปฏิบัติการของ Host ให้ทันสมัย

2.10.1.7 การโจมตีแบบ Fraggle

รายละเอียด

เป็นอีกรูปแบบหนึ่งของการโจมตีแบบ Smurf โดยผู้โจมตีจะส่ง UDP Echo Request (UDP พอร์ต 7) ไปยัง broadcast address ของ amplifier network โดยไอพีแอดเดรสต้นทางไปเป็นไอพีแอดเดรสของเป้าหมายซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่และทำให้มีการใช้ทรัพยากรของเป้าหมายจนหมดไปซึ่งการโจมตียังสามารถใช้ได้กับ UDP, TCP services อื่น เช่น Chargen อีกด้วย

การป้องกัน

สามารถป้องกันได้คล้ายๆ กับการป้องกันการโจมตีแบบ Smurf attack โดยใช้เราท์เตอร์หรืออุปกรณ์กรองแพ็คเก็ตอื่นๆ drop แพ็คเกต UDP/TCP ที่ใช้โจมตีเข้ามาหรืออาจจะใช้วิธีบล็อกไอพีแอดเดรสต้นทางได้เช่นเดียวกัน สำหรับผู้ดูแลระบบทั่วไปควรป้องกันไม่ให้ระบบของตัวเองถูกใช้เป็น amplifier โดยการไม่ตอบสนองต่อแพ็กเก็ตที่ส่งเข้ามายัง broadcast address ซึ่งมีวิธีการแก้ไขแยกตามระบบ

อย่างไรก็ตามผู้ดูแลระบบควรยกเลิกการใช้งาน UDP, TCP service บางตัวเช่น Echo, Chargen, Discard ซึ่งไม่มีความจำเป็นในการใช้งานอีกแล้วซึ่งสำหรับเราท์เตอร์ของ Cisco แล้วสามารถใช้คำสั่งด้านล่างนี้เพื่อยกเลิกบริการดังกล่าว

no service udp-small-servers

no service tcp-small-servers

2.10.1.8 Distributed Denial of Services (DDOS)

DDOS เป็นวิธีการโจมตีแบบ DOS ที่น่ากลัวที่สุดและหาที่มาของผู้โจมตีได้ค่อนข้างยากมีการนำมาใช้อย่างแพร่หลายบนอินเทอร์เน็ตการโจมตีแบบนี้สามารถมีที่มาได้จากหลาย ๆ จุดทำให้ยากต่อการตรวจสอบและป้องกันเนื่องจากการปิดกั้นไอพีแอดเดรสโดยลำพังหรือการปิดกั้นไอพีแอดเดรสทั้งโครงข่ายก็ยังไม่สามารถป้องกันได้เนื่องจากการโจมตีสามารถเกิดขึ้นได้จากคอมพิวเตอร์หลายร้อยหลายพันเครื่อง

การตรวจสอบหาการโจมตีแบบ DDOS

การตรวจสอบหาการโจมตีแบบนี้สามารถทำได้โดยสังเกตการร้องขอเข้ามาในลักษณะเป็นห้วงเวลาหากการร้องขอติดต่อเข้ามานั้นเป็นไปอย่างต่อเนื่องมาจากจุดเดียวกัน รวมทั้งขนาดของข่าวสารการร้องขอเท่ากันทั้งหมดแสดงให้เห็นว่าเป็นการโจมตีและสามารถสร้างฟิลเตอร์จากโปรแกรมประเภทไฟร์วอลล์เพื่อปิดกั้นเฉพาะข้อมูลที่มีขนาดดังกล่าวรวมทั้งไอพีแอดเดรสที่เป็นผู้ติดต่อเข้ามาโดยเฉพาะอย่างไรก็ดีผู้โจมตีแต่ละคนต่างก็อาจใช้รูปแบบการร้องขอที่ต่างกันยิ่งโดยเฉพาะขณะที่กำลังถูกโจมตีอยู่นั้นจะไม่สามารถป้องกันได้ทันท่วงที

การโจมตีแบบ DDOS

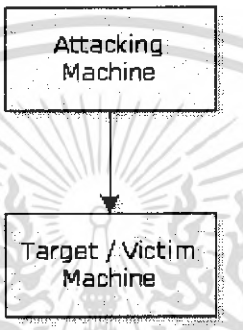
มีการสร้าง Traffic ในปริมาณมากออกมาให้สามารถหลั่งไหลท่วมท้นไปที่เครื่องเป้าหมายปลายทางโดยเฉพาะเว็บไซต์บนอินเทอร์เน็ตรูปแบบของการโจมตีได้แก่การสร้างเครื่องคอมพิวเตอร์ที่ทำงานในลักษณะของ Zombie ขึ้นมาในที่นี้หมายความว่าผู้โจมตีจะต้องใช้ซอฟต์แวร์ที่ทำให้เครื่องคอมพิวเตอร์อื่นๆ จะต้องรับคำสั่งจากเครื่องคอมพิวเตอร์ของผู้โจมตีซึ่งซอฟต์แวร์ประเภทนี้ได้ถูกฝังตัวอยู่ในเครื่องคอมพิวเตอร์เหล่านั้นเป็นที่เรียบร้อยโดยที่ผู้ใช้งานก็ไม่รู้ตัว

วิธีการฝังโปรแกรมเหล่านี้ลงไปที่เครื่องของเหยื่อเป็นเรื่องที่ทำได้ไม่ยากเพียงแต่ฝังโปรแกรมดังกล่าวลงไปไว้ในโปรแกรมที่ผู้โจมตีเสนอตัวให้คัดลอกฟรีหรือฟรีแวร์เป็นต้น ซึ่งเมื่อผู้ใดนำไปติดตั้งที่เครื่องและระเบิดออกมาใช้งาน ก็เท่ากับว่าได้รันโปรแกรม Zombie นี้แล้ว

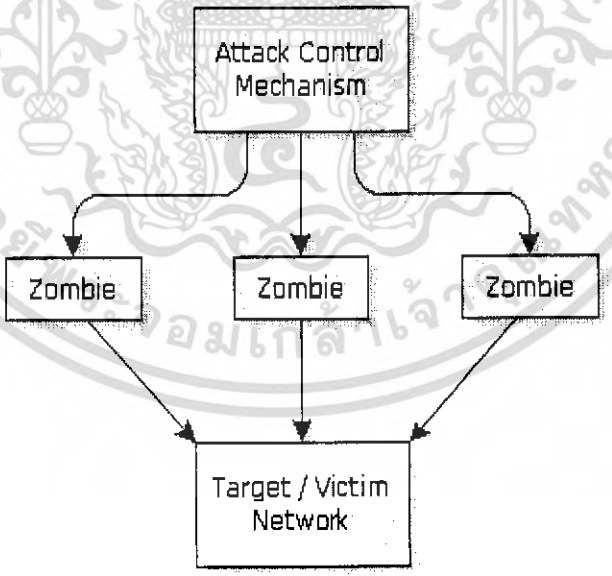
ขั้นตอนต่อไปผู้โจมตีจะทำการสแกนดูว่าเครื่องคอมพิวเตอร์ที่เป็นเหยื่อต่างๆ เหล่านี้ได้รันโปรแกรม Zombie นี้แล้วหรือยัง หากรันเรียบร้อยแล้วก็สามารถสั่งการให้เครื่องคอมพิวเตอร์เหล่านี้

เริ่มการโจมตีเครื่องคอมพิวเตอร์เป้าหมายที่แท้จริงในลักษณะบงการอยู่เบื้องหลังซึ่งคอมพิวเตอร์ที่ตกอยู่ในสภาวะเป็น Zombie นี้อาจมีเป็นร้อยหรือพันก็ได้

การเปรียบเทียบการโจมตีระหว่างรูปที่ 2.13 ซึ่งเป็นการแสดงการโจมตีแบบ DOS กับรูปที่ 2.14 ซึ่งเป็นการแสดงการโจมตีแบบ DDOS



รูปที่ 2.13 การโจมตีแบบ DOS



รูปที่ 2.14 การโจมตีแบบ DDOS

2.10.2 การโจมตีแบบ NULL Session (SMB)

Services ที่ถูกใช้บ่อยที่สุด อย่างหนึ่งของระบบปฏิบัติการ Windows ก็คือ Server Message Block (SMB) ซึ่งรองรับการทำงานของบริการ File and Print Sharing Services ของไมโครซอฟท์ จากนี้ไปจะแสดงให้เห็นถึง null session ซึ่งแสดงให้เห็นถึงเทคนิคในการดึงเอา session ของผู้ใช้ในระบบ Windows ออกไปโดยที่ไม่ต้องล็อกออนแต่อย่างใด

รูปแบบการโจมตี

หนึ่งในช่องโหว่ที่สุดของระบบปฏิบัติการตระกูล NT นั่นคือการที่ค่า default ยังคงต้องพึ่งพาโปรโตคอล Common Internet File System/Server message Block ที่ทำงานผ่านทางพอร์ต TCP 139 และ 445 ถึงแม้ว่าผู้ใช้จะไม่มีการล็อกออนเลยก็ตามขั้นแรกสุดในการเข้าถึง API ตัวนี้คือการสร้างการเชื่อมต่อที่ไม่จำเป็นต้องผ่านการตรวจสอบหรือ Null Session

คำสั่งข้างต้นนี้จะเชื่อมต่อไปยังแชร์ที่ถูกซ่อนไว้สำหรับฟังก์ชันการสื่อสารระหว่างโพรเซสด้วยกัน (IPC$) ของไอพีแอดเดรส 192.168.1.3 ในฐานะของ Account แบบ Anonymous (/u"") ด้วยรหัสผ่านเป็นค่าว่าง หากสำเร็จนั่นหมายถึงว่าแฮกเกอร์ได้เตรียมเปิด Session เตรียมไว้สำหรับดึงข้อมูลออกจากเครื่องเป้าหมายด้วยเทคนิคต่างๆ ด้วย Null Session ที่ถูกสร้างขึ้นมาสามารถแชร์โฟลเดอร์ของเครื่องเป้าหมายด้วยคำสั่งง่ายๆดังนี้

หากว่าโฟล์เดอร์ในเครื่องของ Target ไม่ได้มีการเซต Policy อย่างเหมาะสมจะสามารถดู Resource และ นำไปสู่วิธีการ Hack ในแบบอื่นๆ ได้

การป้องกัน NULL SESSION

- บล็อกการเข้าถึง TCP พอร์ต 139 และ 445 ที่ระดับเน็ตเวิร์คหรือที่ Host โดยใช้ Personal Firewall หรือ เซต ACL ใน Cisco Router
- ยกเลิก Administrative Shares (หรือ แชร์ที่ขึ้นต้นด้วย driveletter$) ด้วยการเขียน Registry เพิ่ม
- ลบ ADMIN$ และแชร์ที่ขึ้นต้นด้วย driveletter$ จาก Computer Management Control Panel ภายใต้ Shared Foldersshares

2.10.3 การโจมตีแบบ Buffer Overflow

Buffer Overflow นั้นเป็นปัญหาที่เกิดจากปริมาณพื้นที่ที่ได้เตรียมไว้สำหรับการรับข้อมูลนั้นน้อยกว่าข้อมูลที่ได้รับมาทำให้ข้อมูลใหม่นั้นไปทับกับข้อมูลของเก่าที่มีอยู่ซึ่งข้อมูลที่ถูกทับไปนั้นอาจจะเป็นคำสั่งหรือว่าข้อมูลอื่นก็ได้ถ้าข้อมูลที่ถูกทับไปนั้นเป็นคำสั่งที่เตรียมไว้ให้ทำงานต่อไปเครื่องก็จะนำเอาข้อมูลชุดใหม่มาใช้ประมวลผลแทนซึ่งถ้าข้อมูลใหม่นั้นสามารถตีความเป็นคำสั่งได้ก็จะทำให้เครื่องของเราทำงานผิดพลาดไปสาเหตุ

โดยทั่วไปการเกิด Buffer Overflow ในเว็บนั้นเกิดจากการที่มีการรอรับค่าจากผู้ใช้แล้วไม่ได้ทำการกำหนดลักษณะของข้อมูลที่ต้องการ เช่น ความยาวประเภท เป็นต้น ทำให้ผู้ใช้สามารถที่จะใส่ข้อมูลอะไรมาก็ได้

ตัวอย่างที่ 1 Buffer-Overflow Attacks แบบเบื้องต้น

ในตัวอย่างแรกนี้เป็นตัวอย่างโปรแกรมภาษา C ง่ายๆ ที่เมื่อถูก Overflow จะทำให้การทำงานบางอย่างผิดไปในที่นี้คือตัวแปร age ซึ่งเป็นตัวแปรเก็บตัวเลขจะถูก Overflow จนค่าที่ได้เปลี่ยนไปดังในตัวอย่างจะพบว่าอายุเปลี่ยนจาก 15 เป็น 49 (ทั้งที่ไม่ได้ทำการกำหนดค่าตัวแปร age เป็น 49)

```
#include <stdio.h>
int main(char argc,char *argv[])

{
    int age;
    char name[7];
    char tmp[20];
    printf("Enter your age:");
    gets(tmp);
    age=atoi(tmp);
    printf("Enter your name:");
    gets(name);  /* 1 */
    printf("---------- ");
    printf("%s is %d years old " ,name,age);
}
```

ผลลัพธ์ที่ได้ คือ

[root@localhost]./a.out

Enter your age:15

Enter your name: yoshijo

---

yoshijo is 49 years old

ค่าที่ได้อาจจะแตกต่างกันไป ขึ้นอยู่กับ Processor, ระบบปฏิบัติการ และ ตัว compiler

สิ่งที่เกิดขึ้นคือ คำสั่ง gets(name) (1) ซึ่งรับข้อมูล input ที่มีขนาด 8 ตัว (7 ตัวอักษร "yoshijo" และ 1 terminator) มาเก็บไว้ในตัวแปร name แต่ตัวแปร name นั้นมีขนาดเพียง 7 ตัวอักษรทำให้ข้อมูลที่ได้มาเกิด Overflow ไปทับ age ผลที่ตามมาคือตัวแปร age ซึ่งเดิมเก็บตัวเลข 15 ถูกเปลี่ยนเป็นเก็บตัวอักษร '1' แทน เมื่อ age ถูกอ้างอิงอีกครั้ง ตัวอักษร '1' จึงถูกอ้างอิงเป็นตัวเลขซึ่งมีค่าเป็น 49 (ในที่นี้ถือตามมาตรฐานรหัสแอสกี้)

วิธีป้องกัน :

สาเหตุที่ทำให้เกิด Buffer Overflow นั้นก็มาจากข้อมูลที่รับเข้ามาจากผู้ใช้งานมีลักษณะไม่ตรงตามที่ต้องการ ดังนั้นสิ่งที่ทำได้คือ

- กำหนดลักษณะของข้อมูลที่ต้องการ
- ตรวจสอบความยาวของข้อมูลไม่ให้ยาวเกินกว่าพื้นที่ที่ได้เตรียมไว้
- ตรวจสอบรูปแบบของข้อมูลให้ตรงความต้องการ
- ทำการ encode สัญลักษณ์ต่าง ๆ ก่อนที่จะนำไปประมวลผล เช่น เปลี่ยนเป็น > เพื่อให้เครื่องคิดว่าเป็นตัวอักษรตัวหนึ่งเท่านั้น

หลักการสำคัญของ Buffer-Overflow

ถึงตรงนี้อาจจะตั้งข้อสังเกตว่า Buffer Overflow ดูเหมือนจะเป็นปัญหาที่เกิดขึ้นจากภาษา C ซึ่งไม่มีระบบ Bound Checking แต่ในความเป็นจริงคือทุกภาษาในปัจจุบันมักจะถูกแปลงลงมาเป็นภาษาเครื่องหรือติดต่อกับระบบปฏิบัติการ ซึ่งส่วนประกอบต่างๆ มักเขียนในภาษา C (และ assembly) ตัวอย่างที่เห็นได้ชัดเช่น Buffer-overflow attacks ที่พบใน Java, Perl, หรือแม้แต่ .Net

2.10.4 การโจมตีแบบ Rootkits

ไม่เพียงแต่การเข้าถึงทรัพยากรต่างๆ ในเซิร์ฟเวอร์เป้าหมายเท่านั้นแฮกเกอร์ยังมีวิธีการที่จะฝังโปรแกรมบางอย่างไว้เพื่อการย้อนกลับมายังเซิร์ฟเวอร์นี้อีกครั้งในภายหลังโดยหลบซ่อนอยู่ในรูปของโปรแกรม Utility ของระบบเองซึ่งผู้ดูแลระบบไม่อาจทราบได้ว่ามีสิ่งแปลกปลอมเหล่านั้นอยู่ที่ใดบ้างเราเรียกโปรแกรมประเภทนี้ว่า Rootkits

เมื่อใดที่ Rootkits ถูกติดตั้งลงสู่ระบบการตรวจสอบเพื่อค้นหาความเปลี่ยนแปลงที่เกิดขึ้นเป็นสิ่งที่กระทำได้ยากหากไม่มีการเตรียมการล่วงหน้าไว้ก่อน Rootkits จะอาศัยอยู่ในระบบและทำงานราวกับเป็นส่วนหนึ่งของระบบแต่ก็อาจจะมีข้อสังเกตบางประการที่ทำให้เราเห็นได้ยกตัวอย่าง เช่น โปรแกรม Rootkits รุ่นล่าสุดของ Linux โปรแกรมล็อกอินที่ถูกลักลอบเข้ามาแล้วจะมีทำงานคล้ายกับโปรแกรมล็อกอินเดิมของระบบทุกอย่างยกเว้นจะทำงานช้าลงกว่าปกติเท่านั้น

Rootkits ในระบบปฏิบัติการ UNIX และ Linux จะประกอบไปด้วยโปรแกรม Utilityเป็นจำนวนมากส่วนหนึ่งจะเป็นโปรแกรมพื้นฐานของระบบเองแต่ถูกดัดแปลงให้มีการทำงานบางอย่างที่เอื้อประโยชน์ต่อแฮกเกอร์ เช่น login, top, sshd, netstat, ifconfig เป็นต้น โดยส่วนใหญ่แล้วจะเป็นคำสั่งที่มีลักษณะดังนี้

- ต้องถูกเรียกใช้งานบ่อยเพื่อเปิดโอกาสให้แก่แฮกเกอร์มากขึ้นนั่นเอง เช่น mount
- เกี่ยวข้องกับข้อมูลสำคัญเพื่อการดักเก็บข้อมูลที่เป็นประโยชน์ต่อการโจมตีหรือเจาะระบบต่อไปในอนาคต เช่น โปรแกรมล็อกอินจะดักจับรหัสผ่านของ User เป็นต้น
- เป็นคำสั่งที่ถูกใช้งานโดยผู้ดูแลระบบเองเพื่อการยกระดับสิทธิขึ้นสู่ผู้ดูแลระบบและทำงานที่ส่งผลสำคัญต่อระบบโดยตรง
- เป็นคำสั่งหรือโปรแกรมที่สัมผัสกับระบบโครงข่ายโดยตรงและทำงานในลักษณะรอคอยอยู่ในระบบเพื่อให้แฮกเกอร์สามารถอาศัยเป็นช่องทางในการเข้าสู่ระบบอีกครั้งตามที่ต้องการหรือสามารถทำงานบางอย่างให้แก่ แฮกเกอร์ได้อย่างต่อเนื่อง (เช่น ทำ Denial of Services) เช่น sshd, in.ftpd, top, rshd

ค้นหาและกำจัดหน่วยแทรกซึมในระบบ Linux

เครื่องมือป้องกันระบบจากปัญหาของการฝังตัว Rootkits นี้เรานิยมใช้ซอฟต์แวร์ระบบรักษาความปลอดภัยที่เรียกว่า ntrusion Detection System หรือ IDS ซึ่งมีโปรแกรมโอเพ่นซอร์สในกลุ่มนี้อยู่มากมายโปรแกรมที่นิยมใช้กันมากที่สุด คือ โปรแกรม chkrootkit ซึ่งเป็นโปรแกรมประเภท rootkits detection เวอร์ชั่นปัจจุบันคือ 0.39a พัฒนาขึ้นโดย Nelson Murilo และ Klaus Steding-Jessen เริ่มตั้งแต่ปี คศ.1997 เป็นต้นมาและรีลีสอัพเดตความสามารถในการตรวจจับ

Rootkits รุ่นใหม่ๆ มาอย่างต่อเนื่อง chkrootkit สร้างขึ้นจากเชลล์สคริปต์ธรรมดาทั้งนี้เพื่อให้มีความคล่องตัวสูงในการนำไปใช้งานและสามารถทำงานได้ทุกกับยูนิกซ์ทุกตระกูลนอกจากนี้ยังมีโปรแกรมยูทิลิตี้ขนาดเล็กที่เขียนด้วยภาษาซีอีกจำนวนหนึ่งเพื่อใช้ตรวจหาร่องรอยของแฮกเกอร์ในไฟล์ binary ซึ่งเชลล์สคริปต์ไม่สามารถกระทำได้ไว้ด้วย ตัวอย่างเช่น ifpromisc.c หนึ่งในโปรแกรมภาษา C นี้จะทำหน้าที่ตรวจสอบและยืนยันว่าการ์ดอินเทอร์เฟสของเราจะไม่ทำงานใน promiscuous mode ซึ่งจะเอื้อประโยชน์แก่ Sniffer จริงอยู่ที่คุณสามารถตรวจสอบได้ง่ายกว่าด้วยคำสั่ง ifconfig แต่น่าเสียดายที่ Rootkits ส่วนใหญ่จะทำการโมดิฟายเจ้าคำสั่ง ifconfig นี้ไปเรียบร้อยแล้ว ดังนั้นคำตอบที่ได้อาจจะไม่จริงเสมอไป

โปรแกรม chkrootkit สามารถตรวจค้นหาการถูกแก้ไขโปรแกรมไบนารี่ต่าง ๆ ได้ เช่น sshd, ifconfig, telnet, top รู้จักกับ Rootkits นานาชนิดกว่า 30 ตัว ตั้งแต่ t0rn, lrk3, lrk4, lrk5, lrk6 รวมทั้ง "เจ้าหนอน" อย่างเช่น Adore, Lion, Ramen

โดยปกติแล้วระบบปฏิบัติการจะมีกลไกที่จะบันทึกการเข้ามาของผู้ใช้ไว้ใน Last Log (wtmp) แต่ตัวแสบที่แวะเข้ามาเยี่ยมเซิร์ฟเวอร์ของเราก็ฉลาดพอที่จะกลบเกลื่อนร่องรอยเหล่านั้นก่อนจะจากไปโปรแกรม chkrootkit ยังมีโปรแกรมภาษา C อีกจำนวนหนึ่งคือ check_wtmpx.c, chkdirs.c, chklastlog.c, chkproc.c, chkwtmp.c ซึ่งจะช่วยตรวจสอบว่ามีผู้ไม่ประสงค์ดีเข้ามาในระบบและทำการลบ Log ต่าง ๆ ไปหรือไม่

วิธีการป้องกัน

- ใช้โปรแกรม chkrootkits

เนื่องจากโปรแกรม chkrootkit เองเป็นโปรแกรมเชลล์สคริปต์ดังนั้นจึงต้องทำงานโดยอาศัยคำสั่งต่าง ๆ ที่มีอยู่ระบบปฏิบัติการด้วยเช่นกัน เช่น find, awk, grep, netstat หากไฟล์เหล่านั้นถูกแทนที่ด้วย Rootkits ไปแล้วย่อมส่งผลต่อการทำงานของ chkrootkit เองด้วยดังนั้นจึงควรกำหนดให้ chkrootkit ใช้คำสั่งที่เราแน่ใจว่าเป็นของแท้ไม่มีการปลอมแปลงมาก่อนได้ด้วย พารามิเตอร์

สำหรับในสังคมโอเพ่นซอร์สแล้วทั้งโปรแกรม Rootkits และโปรแกรมที่ใช้ค้นหาและกำจัด Rootkits ล้วนแล้วแต่เป็นโปรแกรมที่มีการเปิดเผยโปรแกรมต้นฉบับด้วยกันทั้งนั้นในโลกของคอมพิวเตอร์และอินเทอร์เน็ตจึงไม่แตกต่างอะไรกับในโลกของความเป็นจริงที่มีการสร้างอาวุธที่ใช้ทำลายล้างกันอยู่ตลอดเวลาหากเรารู้จักนำความรู้นั้นมาพัฒนาอย่างสร้างสรรค์ซอฟต์แวร์ระบบปฏิบัติการของเราก็จะเข้มแข็งขึ้นได้ซอฟต์แวร์ที่มีคุณภาพดียิ่งขึ้นแต่หากนำความรู้เหล่านั้นมาใช้ในทางตรงกันข้ามย่อมสร้างความเดือดร้อนปราศจากความสงบสุขได้เช่นกัน

2.10.5 การโจมตีแบบ IP Spoofing

IP spoofing เป็นหนึ่งในวิธีการโดยทั่วไปที่ใช้เพื่อโจมตีโครงข่ายเพื่อให้สามารถเข้าถึงระบบคอมพิวเตอร์ที่ไม่ได้รับอนุญาตโดยการส่งข้อความปลอมๆ ที่ดูเหมือนจะจากเครื่องที่ได้รับการเชื่อถือ (trusted machine) อาศัยการปลอม ไอพีแอดเดรสของเครื่องนั้นซึ่งจะมีเทคนิคในการโจมตีด้วย IP Spoofing อยู่ 3 แบบหลักๆ คือ

Non-Blind Spoofing

เป็นวิธีการที่แฮกเกอร์จะใช้ ต่อเมื่อเครื่องของแฮกเกอร์เองนั้นอยู่ภายใน Subnet เดียวกันกับเป้าหมายโดยจะอาศัยหมายเลข Acknowledge No. ที่แฮกเกอร์นั้น Sniff มาได้และทำการส่งแพ็กเก็ตออกไปโดยเซต Acknowledge No. ใหม่ ให้เป็นลำดับถัดจากที่ Sniff มาได้

Blind Spoofing

จะเป็นการสุ่มเอา Acknowledge No. ออกไปยังเครื่องเป้าหมายเนื่องจากวิธีเดิมนั้นไม่สามารถที่จะ Sniff Packet ของ Users ที่อยู่ห่าง Subnet กันออกไปได้

Man-in-Middle Attack

ในการโจมตีแบบ Man-in-Middle ผู้โจมตีจะลวงให้ผู้ใช้เชื่อมต่อเข้ากับโฮสต์ของผู้โจมตีซึ่งจะทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลที่ผู้ใช้รับส่งอยู่ได้และนำไปสู่การโจมตีโฮสต์ที่ทำการ Trusts กับโฮสต์ที่ทางแฮกเกอร์นั้นโจมตีมาได้

วิธีการป้องกัน

- Filter IP Address คลาสที่ไม่ได้ใช้ออกจาก ACL เช่น 172.16.0.0/12 10.0.0.0/24 เป็นต้น
- Implements IPSec ในโครงข่าย

2.10.6 การโจมตีแบบ Sniffer

Sniffer หรือที่เรียกว่า Network wiretap เป็นโปรแกรมซึ่งทำหน้าที่ดักจับแพ็กเก็ตในโครงข่ายโปรแกรม Sniffer จะถอดข้อมูลในแพ็กเก็ตและเก็บบันทึกไว้ให้ผู้ติดตั้งนำไปใช้งาน Sniffer จึงเป็นโปรแกรมหนึ่งที่แฮกเกอร์นิยมใช้เมื่อเจาะเข้าไปในเครื่องคอมพิวเตอร์ปลายทางเพื่อใช้ดักจับข้อมูลโดยเฉพาะอย่างยิ่งชื่อบัญชีและรหัสผ่านเพื่อนำไปใช้เจาะระบบอื่นต่อไป

โดยส่วนมากแล้วจะมีการใช้โปรแกรม Sniffer อยู่สองรูปแบบคือใช้ในการบำรุงรักษาโครงข่ายหรือใช้วิเคราะห์การบุกรุกตัวอย่างเช่น การวิเคราะห์ ปัญหาของโครงข่ายว่า ทำไมเครื่องที่ 1 ไม่สามารถติดต่อกับเครื่องที่ 2 ได้หรือใช้วิเคราะห์ประสิทธิภาพของระบบเพื่อแก้ปัญหาคอขวดหรือใช้ในการตรวจจับหาผู้บุกรุกระบบ

การทำงานของ Sniffer

Ethernet Topology นั้นสร้างมาจากหลักการ Shared คือทุกเครื่องบนโครงข่ายภายในโครงข่ายเดียวกันจะใช้ Shared Media เดียวกันซึ่งหมายความว่าทุกเครื่องจะรับแพ็กเก็ตทั้งหมดบน Shared Media นั้นได้ดังนั้น Hardware จึงถูกสร้างมาพร้อมกับ Filter ซึ่งจะไม่สนใจแพ็กเก็ตที่ไม่ได้ส่งถึงมันเองโดยการตรวจ MAC Address แต่ Sniffer จะปิดการทำงานของ Filter นั้นและบังคับให้ Network Card เข้าสู่ภาวะการทำงานที่เรียกว่า "promiscuous mode"

โปรแกรม Sniffer ส่วนใหญ่ทำงานได้กับ NIC Card แทบทุกแบบและเมื่อจับเฟรมข้อมูลขึ้นมาได้แล้วก็จะนำไปใส่ในบัฟเฟอร์โดยการจับข้อมูลมีอยู่ 2 โหมดจับข้อมูลจนกระทั่งบัฟเฟอร์เต็มหรือใช้บัฟเฟอร์แบบ round-robin (เขียนข้อมูลใหม่ทับข้อมูลที่เก่าที่สุด) โปรแกรมบางชนิด (เช่น BlackICE Sentry IDS ของ Network ICE) สามารถใช้ Disk เป็นบัฟเฟอร์แบบ round-robin ในการจับข้อมูลที่ความเร็วเต็มที่ 100 mbps ได้ ซึ่งทำให้มีบัฟเฟอร์ขนาดหลายกิกะไบต์แทนที่จะใช้เฉพาะหน่วยความจำที่มีขนาดจำกัด

วิธีการป้องกัน

เราสามารถป้องกันการดักจับข้อมูลจากภายในโครงข่ายได้หรือทำให้การดักจับยากขึ้นแต่ไม่สามารถป้องกันการดักจับข้อมูลจากภายนอกโครงข่ายได้วิธีที่ดีที่สุดในการป้องกันข้อมูลคือ การเข้ารหัสข้อมูลเพราะถึงแม้ว่าผู้อื่นสามารถดักจับข้อมูลได้แต่ก็ไม่สามารถอ่านข้อมูลได้วิธีที่ใช้ในการเข้ารหัสข้อมูล มีดังนี้ คือ

- SSL (Secure Socket Layer)

  นิยมใช้อย่างแพร่หลายในเว็บเพราะใช้ในการเข้ารหัสข้อมูลผ่านเว็บโดยส่วนใหญ่จะใช้ในธุรกรรมอิเล็กทรอนิกส์เช่นการกรอกข้อมูลของเครดิตการ์ด

- Ssh (Secure Shell)

  ใช้สำหรับการล็อกอินเข้าไปใช้งานบนระบบยูนิกซ์ ssh จะใช้ในการเข้ารหัสข้อมูลเพื่อป้องกันการดักจับ ssh เป็นโปรแกรมที่ออกแบบมาใช้แทน telnet

2.10.7 การโจมตีแบบ Phishing Web Sites

Phishing คือ การโจมตีในรูปแบบของการปลอมแปลง E- mail (Email Spoofing) และทำการสร้างเว็บไซต์ปลอมเพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับ E- mail เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิตบัญชีผู้ใช้และรหัสผ่านหมายเลขบัตรประจำตัวประชาชนหรือข้อมูลส่วนบุคคลอื่นๆ

Phishing สามารถทำได้โดยการขโมยหรือนำเครื่องหมายหรือสัญลักษณ์ตลอดจนรูปลักษณ์ของธนาคารหรือสถาบันการเงินที่มีชื่อเสียงและบัตรเครดิตประเภทต่างๆ ของผู้ประกอบการ การให้สินเชื่อทางอินเทอร์เน็ตมาประกอบเข้ากับการหลอกลวงเหยื่อหรือผู้ใช้ให้เปิดเผยข้อมูล ซึ่งมีการประเมินเบื้องต้นว่าการโจมตีในรูปแบบของ phishing สามารถหลอกให้เหยื่อร้อยละ 5 ของทั้งหมดเปิดเผยข้อมูลที่ต้องการนอกจากนี้ผู้โจมตี (แฮกเกอร์ หรือ Spammer) ยังใช้ยุทธวิธีการหลอกลวงแบบ Social Engineering ประกอบเพิ่มเติมเพื่อให้มีความน่าเชื่อถือยิ่งขึ้น เช่น การหลอกลวงชื่อ E-mail เป็นต้นว่าเป็นเรื่องด่วนจากธนาคารการหลอกลวงว่าบัญชีที่ใช้งานจะหมดอายุการเสนอสินค้าที่มีดอกเบี้ยต่ำต่างๆ เป็นต้น

วิธีการป้องกันและรับมือกับการถูกโจมตีแบบ phishing

- หยุดคิดและพิจารณาข้อมูลที่ได้รับทาง E- mail หรือข้อมูลที่เข้าไปดูในเว็บไซต์ทุกครั้ง
- ควรลบข้อมูลที่น่าสงสัยนั้นทิ้งทันที
- หากมีความจำเป็นต้องกรอกหรือส่งข้อมูลใดทางเว็บไซต์ต้องพิจารณาความน่าเชื่อถือของเว็บไซต์ดังกล่าวว่ามีตัวตนหรือมีการรับรองหรือไม่หากไม่แน่ใจควรติดต่อไปยังเจ้าของ

เว็บไซต์หรือเจ้าของสถาบันการเงินดังกล่าวเพื่อสอบถามข้อมูลและยืนยันข้อมูลก่อนการดำเนินการใดๆ

- ไม่ควรเข้าไปในเว็บไซต์หรือรันไฟล์ที่แนบมากับ E- mail ซึ่งมาจากบุคคลที่ไม่รู้จักหรือไม่มั่นใจว่าผู้ส่งเป็นใครหรือไม่ทราบว่าไฟล์ดังกล่าวเป็นไฟล์อะไร ตลอดจนเว็บไซต์หรือไฟล์ที่ถูกส่งมาด้วยโปรแกรมสนทนาประเภทต่างๆ เช่น IRC, ICQ, MSN หรือ PIRCH เป็นต้น
- ติดตั้งโปรแกรมปรับปรุงช่องโหว่ (patch) ของทุกซอฟต์แวร์ที่มีการใช้อยู่ในเครื่องคอมพิวเตอร์ของท่านอยู่เสมอ
- ติดตามข่าวสารและการแจ้งเตือนทางด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ผ่านทาง E- mail ของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

2.10.8 การโจมตีแบบ SSH Brute Forces

สำหรับเครื่องเซิร์ฟเวอร์ที่เป็น Public IP ทั้งหลาย จะประสบกับปัญหานี้กันมากคือถูกโจมตีด้วย ssh brute force ในกรณีที่ที่ผู้บุกรุกสามารถบุกรุกเข้าไปในระบบได้สำเร็จ ผู้บุกรุกจะ

- ติดตั้ง rootkits ซึ่งช่วยในการซ่อนตัวจากการตรวจจับและปกปิดร่องรอยการบุกรุก
- ติดตั้ง SSH ที่เป็น rootkits (ผู้บุกรุกปรับแต่ง source code ของ SSH)
- ติดตั้งเครื่องมือที่ใช้ในการ scan เครื่องอื่นๆ ว่ามีช่องโหว่เดียวกันนี้หรือไม่โดยโปรแกรมดังกล่าวนี้จะอาศัยข้อมูลเวอร์ชันจาก banner ที่ปรากฏใน SSHD service

2.10.9 การโจมตีแบบ Backdoor

Backdoor เป็นวิธีการหนึ่งที่ทางแฮกเกอร์ต้องการที่จะสร้างช่องทางพิเศษไว้ในการที่จะกลับไปควบคุมเครื่องเป้าหมายอีกครั้งหรืออาจจะเพื่อสามารถควบคุมเป้าหมายได้ดีขึ้น

Feature ที่เด่นๆ ของ SubSeven

- ดักจับคีย์ที่พิมพ์ลงไปบน Keyboard (Keystroke Logging)
- การส่งคีย์เพื่อรับคำสั่ง
- การ Sniffing
- การค้นหาไฟล์จาก Drive

- การดาวน์โหลดรหัสผ่านจากเครื่อง เช่น รหัสของ RAS Server
- Registry Editor
- เปลี่ยนทิศทางพอร์ต (Port Redirection)
- แสกนพอร์ตระยะไกล
- Monitoring โปรแกรมประเภท IM ต่างๆ (MSN)

2.10.10 การโจมตีแบบ Zero Day Attack

ช่องโหว่ใหม่ๆ ที่ถูกค้นพบในแต่ละวันหลังจากช่องโหว่ถูกค้นพบและขณะนั้นยังไม่มี "Patch" ออกมาแก้ไขในช่วงเวลานั้นถือเป็นช่วงเวลาอันตรายของระบบเราเพราะหากมี ผู้บุกรุกทำการบุกรุกเข้ามาสร้างโปรแกรม Exploit หรือ Malware ที่ขึ้นระบบที่เราใช้อยู่ก็สามารถถูกโจมตีได้อย่างง่ายดาย เนื่องจากยังไม่มี "Patch" ออกมาปิดช่องโหว่ดังกล่าว เราเรียกว่าช่วง Zero-Day

วิธีแก้ไข

- Proactive Vulnerability Management หรือ การ กระตือรือร้นในการปิดช่องโหว่ที่เกิดขึ้นอย่างทันท่วงที และการเตรียมแผนระยะสั้น- ยาวในการบริหารจัดการเมื่อเกิด Zero Day Attack ขึ้น
- Patch Management Systems หรือ ระบบติดตั้ง Patch อัตโนมัติโดยใช้ฟังก์ชันนี้ได้จาก Windows Server หรือ Enterprise IPS (Intrusion Prevention Systems)
- ใน IPS ระดับสูง จะมี ฟังก์ชัน ZDI (Zero Day Initiative) ที่สามารถตรวจจับและป้องกันช่องโหว่ใน Application หรือ OS ที่เกิดปัญหาขึ้นได้

บทที่ 3
การออกแบบโครงงาน

3.1 ขั้นตอนการออกแบบระบบโครงข่าย

1. วิเคราะห์ความต้องการของผู้ใช้ในระบบโครงข่ายห้องวิจัยการสื่อสารไร้สาย ความต้องการของผู้ใช้ ได้แก่

- ต้องการระบบโครงข่ายภายในที่เป็นสัดส่วนแยกจากโครงข่ายภายนอกอย่างชัดเจน
- ต้องการความปลอดภัยจากผู้บุกรุกซึ่งเป็นบุคคลภายนอกที่ไม่หวังดี
- ต้องการความปลอดภัยในระดับสูงแก่เซิร์ฟเวอร์ฐานข้อมูล
- ต้องการความสะดวกสบายในการใช้งานโครงข่ายไม่พบปัญหาในการใช้งาน เช่น การชนกันของไอพีแอดเดรส
- มีการดูแลเครื่องไคลเอ็นต์ภายในระบบโครงข่าย เช่น การแจ้งเตือนไวรัส
- ต้องการให้มีบริการเก็บรวบรวมผลการวิจัยและ thesis ของนักศึกษาให้เป็นระบบ
- ต้องการให้มีเว็บไซต์ภายในห้องวิจัยการสื่อสารไร้สาย เพื่อให้มีการแจ้งข่าวสาร, ความรู้ต่าง ๆ รวมทั้งทำเว็บบอร์ด (Webboard) เพื่อให้ผู้ใช้ในห้องวิจัยได้ติดต่อหรือตั้งกระทู้ ถาม- ตอบ เกี่ยวกับข่าวสารหรือวิชาการความรู้ภายในห้องวิจัย

2. ศึกษาข้อบกพร่องของระบบโครงข่ายเดิมเพื่อทำการพัฒนาให้ดีขึ้น

- เดิมมีการใช้ Public IP เพียงอย่างเดียวทำให้หมายเลขไอพีแอดเดรสไม่เพียงพอต่อความต้องการของผู้ใช้
- มีการชนกันของ IP เนื่องจากผู้ใช้เป็นคนตั้งค่ากันเอง
- โครงข่ายแบบเดิมภายในห้องวิจัยการสื่อสารไร้สายนั้นไม่ได้มีการจัดการใด ๆเกี่ยวกับข้อมูล ผลงานหรือ ผลการวิจัย ของอาจารย์ และนักศึกษา ซึ่งเป็นข้อมูลที่มีความสำคัญในระดับสูง
- โครงข่ายของระบบยังขาดประสิทธิภาพและเสถียรภาพ

3. ออกแบบระบบโครงข่ายเพื่อใช้งานในห้องวิจัยการสื่อสารไร้สาย โดยได้คำนึงถึง

- ประสิทธิภาพ
- ความน่าเชื่อถือ
- ระดับความปลอดภัย
- เสถียรภาพของโครงข่าย

- ความเป็นประโยชน์
- งบประมาณ
- ความยากง่ายในการจัดการและตั้งค่า
- ความสะดวกสบายของผู้ใช้

3.2 การออกแบบส่วนของโครงข่ายภายในที่ทำงานผ่านไฟร์วอลล์ภายนอก

- Web Server
- ได้ทำการสร้าง Web Server สำหรับให้บริการการใช้งานต่าง ๆ ให้กับอาจารย์ และนักศึกษาที่อยู่ภายในห้องกลุ่มการวิจัยการสื่อสารไร้สาย เช่น การสร้างโฮมเพจให้กับห้องวิจัย ภายใต้ชื่อ www.wis.ite.kmitl.ac.th ขึ้นเพื่อให้อาจารย์ และนักศึกษาของกลุ่มการวิจัยได้สามารถเข้ามาค้นหาหรือดาวน์โหลดข้อมูลเกี่ยวกับเทคโนโลยีการสื่อสารไร้สายได้ง่ายและสะดวกขึ้น และยังได้จัดทำเว็บบอร์ดขึ้นมาเพื่อให้มีการแจ้งข่าวสาร, ความรู้ต่าง ๆ เพื่อให้ผู้ใช้ในห้องวิจัยได้ติดต่อหรือตั้งกระทู้ ถาม- ตอบ เกี่ยวกับปัญหา, คำถาม หรือวิชาการความรู้ ในเรื่องของเทคโนโลยีการสื่อสารไร้สาย

- DNS Server

DNS เป็นระบบแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปของ โดเมนเนมหรือแปลงจากโดเมนเนมไปเป็นไอพีแอดเดรสได้ ในโครงงานนี้ได้ทำการลงทะเบียนชื่อโดเมนผ่าน ISP เรียบร้อยแล้ว โดยใช้หมายเลขไอพีแอดเดรสเป็น 161.246.73.75 และทำการประกาศสับโดเมน (Subdomain) ชื่อ wis.ite.kmitl.ac.th

- Mail Server

Mail Server จะเป็นตัวที่ทำหน้าที่ในด้านการจัดการรับและส่ง E- mail ของผู้ใช้ที่เป็นสมาชิกในห้องกลุ่มการวิจัยการสื่อสารไร้สายทำให้การใช้งานในส่วนของ E- mail มีความยืดหยุ่นและมีประสิทธิภาพมากขึ้น โดยสมาชิกทุกคนจะมีอีเมล์แอดเดรสเป็นของตัวเอง ซึ่งส่งผลให้ดูเป็นทางการมากขึ้น โดยสมาชิกจะมีแอดเดรสเป็น user@wis.ite.kmitl.ac.th

ในโครงการนี้ได้จัดทำโดยใช้คอมพิวเตอร์ส่วนบุคคล ทำหน้าที่เป็นเซิร์ฟเวอร์โดยมีคุณสมบัติของเครื่องเป็นดังนี้

- ซีพียู : Pentium4 3.0 GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 80 GHz

เทคโนโลยีที่เลือกใช้

- ใช้ระบบปฏิบัติการ Linux เนื่องจากเป็นระบบปฏิบัติการที่เป็นโอเพ่นซอร์ส และเป็นระบบปฏิบัติการที่มีประสิทธิภาพและเสถียรภาพสูงมีฟังก์ชั่นในการทำงานที่เหมาะที่จะเป็นเซิร์ฟเวอร์ และทำหน้าที่เป็นไฟร์วอลล์ได้ดี
- Apache Web Server ใช้เป็นเว็บเซิร์ฟเวอร์เพราะเป็นโอเพ่นซอร์สและใช้งานได้ง่าย สะดวกต่อการติดตั้ง
- โปรแกรม PHP ใช้เพื่อเป็น Script ในการเขียนไฟล์ *.php
- MySQL สำหรับจัดการฐานข้อมูลต่าง ๆของเว็บเซิร์ฟเวอร์
- PHPMyAdmin สำหรับการจัดการส่วนที่เป็น PHP กับ MySQL
- ใช้ Bin 9.2.4 เป็น DNS Server เนื่องจากเป็น Open Source และง่ายต่อการติดตั้ง
- ใช้โปรแกรม Postfig ในการจัดการบริการ SMTP
- ใช้โปรแกรม ClamAV เป็น Antivirus
- ใช้โปรแกรม Amavist-New เป็น Antivirus Scanner สำหรับเป็นตัวกลางระหว่าง Postfig และ ClamAV
- ใช้โปรแกรม Squirrel Mail ในการบริหารจัดการเว็บเบสสำหรับติดต่อกับผู้ใช้เมล์ผ่านเว็บ

3.3 การออกแบบมอนิเตอร์เซิร์ฟเวอร์

เป็นเซิร์ฟเวอร์ที่ทำหน้าที่ดูแลและจัดการคอมพิวเตอร์ของผู้ใช้ภายในโครงข่าย ทำหน้าที่เป็น DHCP Server สำหรับแจก ไอพีแอดเดรสโดยอัตโนมัติให้แก่เครื่องคอมพิวเตอร์ที่เป็นเครื่องไคลเอ็นต์ เครื่อง DHCP เซิร์ฟเวอร์ทำการค้นหาหมายเลขไอพีแอดเดรสจากฐานข้อมูลในเครื่องเพื่อไม่ให้ซ้ำกัน และส่ง message DHCP Offer กลับไปให้เครื่องไคลเอ็นต์ที่ร้องขอ และมีโปรแกรมตรวจจับไวรัสในโครงข่ายภายใน สามารถแจ้งเตือนให้แก่ผู้ใช้งานในระบบได้ทราบ มีการเก็บล็อกข้อมูลต่าง ๆ ของการใช้งานระบบโครงข่ายของบุคลากร เพื่อป้องกันและตรวจสอบข้อผิดพลาดในการใช้งาน

ในโครงงานนี้ได้ใช้คอมพิวเตอร์ส่วนบุคคล ทำหน้าที่เป็นมอนิเตอร์เซิร์ฟเวอร์โดยมีคุณสมบัติของเครื่องคอมพิวเตอร์ดังนี้

- ซีพียู : Pentium4 3.0 GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 40 GHz

เทคโนโลยีที่เลือกใช้

- ใช้ระบบปฏิบัติการ Windows Server 2003 เนื่องจากเป็นระบบปฏิบัติการที่สามารถติดต่อกับผู้ใช้ได้สะดวก และมีโปรแกรมสนับสนุนมาก
- ใช้โปรแกรม Trend Micro ในการตรวจจับไวรัสบนโครงข่าย
- OfficeScan ทำหน้าที่ป้องกันไวรัสบนโครงข่าย โดยผู้บริหารสามารถจัดการเครื่องลูกข่ายต่าง ๆ เหล่านี้ได้จากจุดศูนย์กลาง เพื่อง่ายต่อการจัดการ

3.4 การออกแบบเซิร์ฟเวอร์ข้อมูล

เป็นเซิร์ฟเวอร์ที่ทำหน้าที่ในการเก็บข้อมูลต่างๆ เกี่ยวกับห้องกลุ่มการวิจัยการสื่อสารไร้สาย เช่น ข้อมูลหรือประวัติต่าง ๆ ของสมาชิก รวมทั้งเป็นแหล่งรวบรวม Thesis หรือบทความทางการวิจัย ของอาจารย์และนักศึกษา ซึ่งเป็นข้อมูลที่มีความสำคัญในระดับสูง

ในโครงงานนี้ได้ใช้คอมพิวเตอร์ส่วนบุคคล ทำหน้าที่เป็น Monitor Server โดยมีคุณสมบัติของเครื่องคอมพิวเตอร์ดังนี้

- ซีพียู : Pentium4 3.0 GHz
- แรม : 512 MHz
- ฮาร์ดดิสก์ : 40 GHz

เทคโนโลยีที่เลือกใช้

- ใช้ระบบปฏิบัติการ Linux เนื่องจากเป็นระบบปฏิบัติการที่เป็นโอเพ่นซอร์สและเป็นระบบปฏิบัติการที่มีประสิทธิภาพและเสถียรภาพสูง
- VSFTP (Very Secure FTP) สำหรับจัดการด้าน FTP ที่มีความปลอดภัยในระดับสูง

- MySQL ในการจัดเก็บข้อมูลต่าง ๆ เนื่องจากเป็นโอเพ่นซอร์สและง่ายต่อการใช้งาน

3.5 การออกแบบโฮมเพจ

เนื่องจากภายในห้องวิจัย Wireless Communication Research Group ต้องการโฮมเพจเพื่อให้บุคคลภายในและภายนอกได้สามารถเข้ามาใช้เว็บไซต์เพื่อศึกษาความรู้เทคโนโลยีการสื่อสารไร้สายได้อย่างสะดวก

ดังนั้นในโครงการนี้จึงได้สร้างโฮมเพจสำหรับห้องวิจัย Wireless Communication Research Group ขึ้นมา โดยในโฮมเพจจะประกอบไปด้วย

- Member (สมาชิก) จะมีรายชื่อและข้อมูลของบุคลากรที่เป็นสมาชิกของห้องวิจัยการสื่อสารไร้สายนี้
- Public list (ผลงานการวิจัย) จะมีรายละเอียดของบทความการวิจัยที่มีการตีพิมพ์ลงในวารสารทั้งในประเทศและต่างประเทศ
- Link (ลิ้งค์) ภายในมี link เพื่อ link ไปยังเว็บไซต์ต่างๆ ที่สำคัญและมีประโยชน์สำหรับห้องวิจัย
- Webmail (เว็บเมล์) ซึ่งจะ link ไปยังเว็บเมล์ที่โครงงานนี้ได้สร้างขึ้นมาเพื่อให้บริการเกี่ยวกับการรับและส่ง E- mail

นอกจากนี้ยังได้สร้างหน้าล็อกอินเพื่อให้ผู้ที่เป็นสมาชิกของห้องกลุ่มวิจัยเท่านั้นที่จะสามารถเข้าไปยังหน้าที่สามารถตั้งเว็บบอร์ดและดาวน์โหลดผลการวิจัยต่าง ๆ ได้ โดยหน้าล็อกอินจะให้กรอกชื่อ และ password ถ้าบุคคลใดยังไม่ได้เป็นสมาชิกจะต้องมีการลงทะเบียนใหม่ (New Register) โดยจะต้องกรอกข้อมูลตามแบบฟอร์มที่มีให้เพื่อเป็นการกำหนด Username และ password เมื่อลงทะเบียนเรียบร้อยแล้วจึงจะสามารถล็อกอินเข้าสู่ระบบได้

ผู้ที่ล็อกอินเข้ามาได้นั้นสามารถจะเข้ามาเพื่ออ่านหรือดาวน์โหลดผลงานการวิจัย หรือ thesis มาศึกษาได้ และสามารถเข้าไปตั้งกระทู้ในเว็บบอร์ดที่ได้จัดทำขึ้นโดยที่กระทู้ต่าง ๆ จะอยู่ในความดูแลของผู้ดูแลระบบ ผู้ดูแลระบบเท่านั้นที่จะสามารถทำการลบกระทู้ที่ไม่เหมาะสมออกได้

เมื่อทำการสร้างโฮมเพจเรียบร้อยแล้วจะนำไปลงที่ Web Server โดยใช้ Apache Web Server เนื่องจากเป็น Web Server ที่มีประสิทธิภาพสูง และนิยมใช้มากที่สุด นอกจากนี้ยังใช้ Script

language คือ PHP เพราะเป็นโอเพ่นซอร์สและสามารถติดต่อกับฐานข้อมูล (MySQL) ที่ใช้ในโครงงานได้

3.6 การออกแบบไฟร์วอลล์เพื่อป้องกันการโจมตี

เป็นการคอนฟิกค่าต่าง ๆ โดยใช้ Iptables เพื่อเขียนกฎในการผ่านเข้าออกของแพ็กเก็ตข้อมูล และควบคุมการทำงานของโปรโตคอล เพื่อตรวจจับการโจมตีจากผู้ไม่หวังดีจากภายนอก โดยให้สามารถมีการป้องกันการโจมตีในหลายรูปแบบดังต่อไปนี้

- ป้องกันการโจมตีแบบ SYN Flood

จัดการป้องกันโดยการป้องกันการปลอมแปลงไอพีแอดเดรสจากเครื่องผู้บุกรุก และจำกัดการส่งแพ็กเก็ต TCP ที่ตั้งค่า SYN ไว้ไม่ให้มีการส่งมากจนเกินไป โดยกำหนดให้สามารถส่งได้แค่ 1 ครั้งต่อนาที

- ป้องกันการโจมตีแบบ ICMP Flood

ทำได้โดยการ คอนฟิกผ่าน Iptables โดยจะอนุญาตให้แพ็กเก็ตข้อมูลที่เป็นโปรโตคอล ICMP ชนิด echo - request ผ่านเข้ามาได้จำกัดแค่ 10 ครั้งต่อนาที

- ป้องกันการโจมตีแบบ UDP Flood

ทำการป้องกันได้โดยการ drop แพ็กเก็ตที่ส่งมายังพอร์ตที่ไม่ได้เปิดให้บริการ และจำกัดข้อมูลในการส่ง TCP ชนิด UDP

- ป้องกันการโจมตีแบบ Smurf

ทำการป้องกันโดยการกำหนดให้แพ็กเก็ต ICMP Echo Reply ที่ส่งเข้ามาโดยที่ไม่มีการส่งแพ็กเก็ต ICMP Echo Request ออกไป ไม่สามารถผ่านเข้ามายังโครงข่ายได้

- ป้องกันการโจมตีแบบ Land Attack

การโจมตีในรูปแบบนี้เกิดจากการที่ผู้บุกรุกใช้ไอพีแอดเดรสปลอมในการร้องขอการเชื่อมต่อเข้ามา จึงได้ทำการเขียนกฎในการป้องกันการปลอมแปลงไอพีแอดเดรส แล้วติดต่อเข้าในเครือข่ายที่เรียกว่า Ip spoofing

- ป้องกันการโจมตีแบบ IP Spoofing

ได้ทำการเขียนกฎในการป้องกันการปลอมแปลงไอพีแอดเดรส ที่จะเข้าในโครงข่ายโดยที่จะไม่อนุญาตให้แพ็กเก็ตที่มาจาก Interface ภายนอกบาง IP ผ่านเข้ามาได้

- ป้องกันการโจมตีแบบ SSH Brute Forces

  ใช้ iptables ในการกำหนดค่าการทำงานของไฟร์วอลล์โดยใช้คำสั่ง

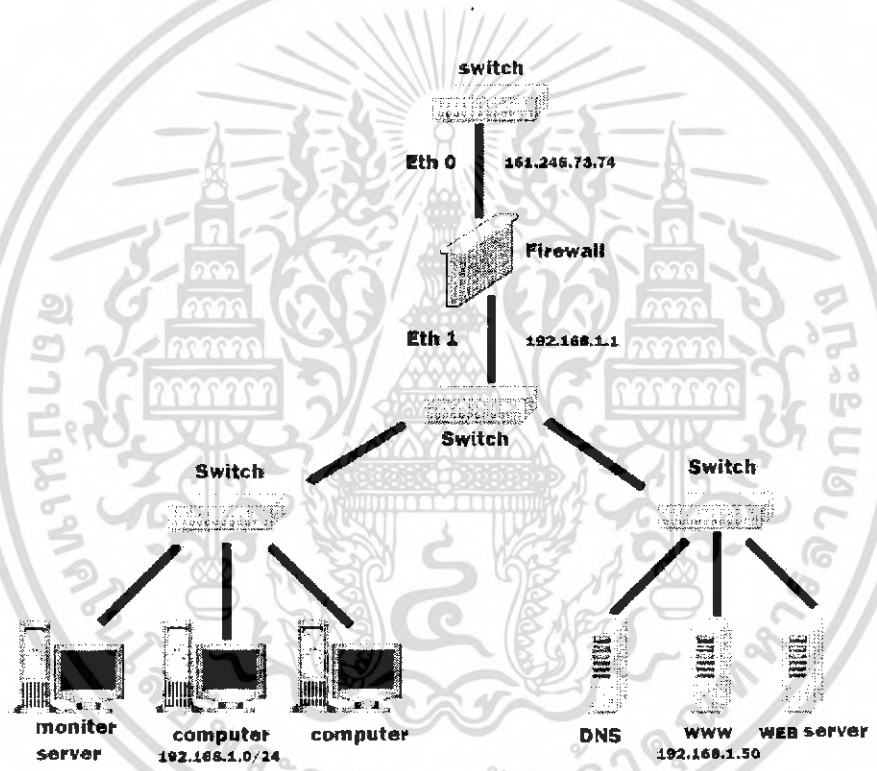
iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --set

iptables -I INPUT -p tcp --dport 22 -i eth0 -m state --state NEW -m recent --update --seconds 600 --hitcount 2 -j DROP

บทที่ 4
ผลการทดลอง

4.1 การจัดการระบบโครงข่ายภายใน

ในโครงงานนี้ได้จัดการออกแบบโครงข่ายที่จะต้องใช้งานในระบบได้ดังนี้



รูปที่ 4.1 ระบบเน็ตเวิร์ค

จากรูปเป็นการออกแบบระบบเน็ตเวิร์คที่จะใช้ในกลุ่มการวิจัยการสื่อสารไร้สายโดยที่มีรายละเอียดของระบบดังต่อไปนี้

4.1.1 ไฟร์วอลล์

ประกอบด้วย 2 Interface สำหรับใช้ในการติดต่อ ได้แก่

- Eth0 ซึ่งกำหนดให้มี IP Address เป็น 161.246.73.74 ได้กำหนดให้ Interface Eth0 นี้ใช้เพื่อติดต่อกับโครงข่ายภายนอก มี netmark เป็น 255.255.255.0
- Eth1 ซึ่งกำหนดให้มี IP Address เป็น 192.168.1.1 ได้กำหนดให้ Interface Eth1 นี้ใช้เพื่อติดต่อกับโครงข่ายภายใน มี netmark เป็น 255.255.255.0

โดยจะทำหน้าที่เป็น

1. ใช้เป็นเราท์เตอร์ในการหาเส้นทาง โดยพิจารณาจากเฮดเดอร์ของแพ็กเก็ต
2. ใช้กำหนดกฎการเข้า- ออกของแพ็กเก็ตข้อมูล และกำหนดกฎให้กับไฟร์วอลล์จะอนุญาตหรือไม่ให้ใช้เซอร์วิสชนิดใด
3. ป้องกันเน็ตเวิร์คบางส่วนจากการเข้าถึงของเน็ตเวิร์คภายนอก
4. NAT สำหรับแปลงไอพีแอดเดรสของโครงข่ายภายในให้เป็นไอพีแอดเดรสซึ่งเป็นที่ยอมรับและสามารถทำการสื่อสารบนอินเทอร์เน็ตได้

สามารถป้องกันการโจมตีดังนี้

- การโจมตีแบบ SYN Flood
- การโจมตีแบบ ICMP Flood
- การโจมตีแบบ UDP Flood
- การโจมตีแบบ Smurf
- การโจมตีแบบ Land Attack
- การโจมตีแบบ IP Spoofing
- การโจมตีแบบ SSH Brute Forces

4.1.2 เว็บเซิร์ฟเวอร์

มีไอพีแอดเดรสเป็น 192.168.0.50 netmark เป็น 255.255.255.0 จะทำการแปลงไอพีแอดเดรสแบบ Static NAT จาก 161.246.73.75 เป็น 192.168.1.50 ก่อนที่โครงข่ายภายนอกจะเข้าสู่เว็บเซิร์ฟเวอร์ได้

โดยจะทำหน้าที่เป็น

1. โฮมเพจและเว็บแอพพลิเคชั่น เพื่อให้บริการแก่ผู้ใช้
2. มีการแจ้งข่าวสาร ความรู้ต่าง ๆ ในเรื่องของเทคโนโลยีการสื่อสารไร้สาย

3. เป็นที่ตั้งของเว็บบอร์ด (Webboard) ให้ผู้ใช้ในกลุ่มการวิจัยได้ติดต่อหรือตั้งกระทู้ ถาม- ตอบ เกี่ยวกับข่าวสาร หรือวิชาการความรู้ภายในห้องวิจัย
4. ที่ที่ให้สามารถเข้ามาค้นหาหรือดาวน์โหลดข้อมูลเกี่ยวกับ ความรู้ในเรื่องเทคโนโลยีการสื่อสารไร้สาย หรือ thesis ต่าง ๆ เพื่อการเพื่อศึกษาได้

4.1.3 DNS Server

ใช้สำหรับแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปของ โดเมนเนมหรือแปลงจากโดเมนเนมไปเป็นไอพีแอดเดรสได้ ได้ทำการลงทะเบียนชื่อโดเมนผ่าน ISP เรียบร้อยแล้ว และทำการประกาศโดเมนลูก (Subdomain) เป็น "wis.ite.kmitl.ac.th"

4.1.4 Mail Server

มีไอพีแอดเดรสเป็น 192.168.0.50 netmark เป็น 255.255.255.0 โดยจะทำหน้าที่ จัดการรับและส่ง E- mail ของผู้ใช้ที่เป็นสมาชิกในกลุ่มการวิจัยการสื่อสารไร้สาย โดยสมาชิกทุกคนจะมีอีเมล์แอดเดรสเป็นของตัวเอง ซึ่งจะมีแอดเดรสเป็น user@wis.ite.kmitl.ac.th

4.1.5 มอนิเตอร์เซิร์ฟเวอร์

กำหนดให้มีไอพีแอดเดรสเป็น 192.168.1.51 netmark เป็น 255.255.255.0

โดยจะทำหน้าที่เป็น

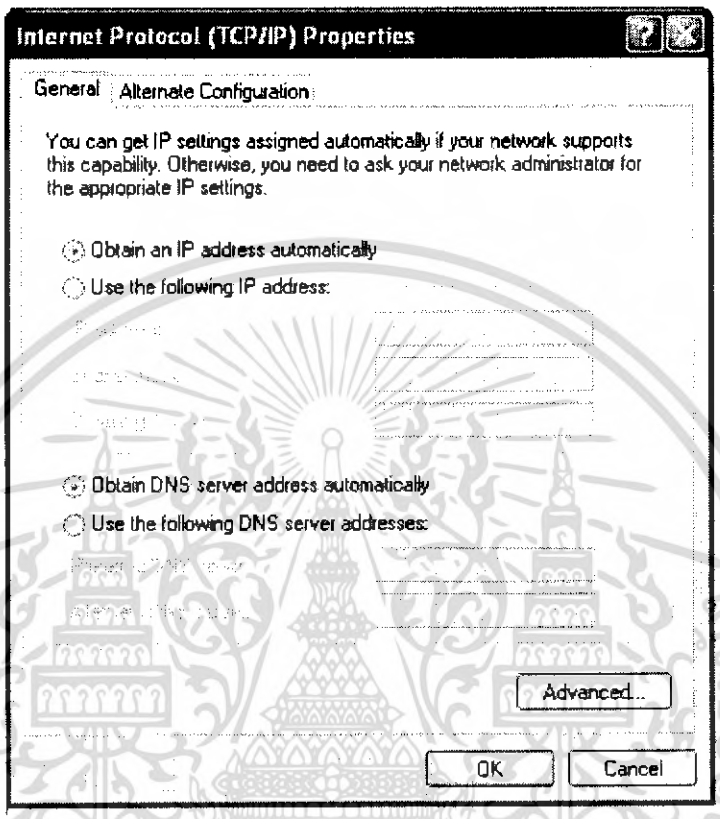
1. ดูแลจัดการคอมพิวเตอร์ของผู้ใช้ภายในโครงข่าย
2. มีโปรแกรมตรวจจับไวรัสในโครงข่ายภายใน สามารถแจ้งเตือนกับผู้ใช้ภายในระบบได้เมื่อเกิดปัญหา
3. มีการเก็บล็อกข้อมูลต่างๆ ของการใช้งานระบบโครงข่ายของผู้ใช้ เมื่อเกิดปัญหาจะได้ทราบสาเหตุ
4. DHCP Server จัดการแจกไอพีแอดเดรส ให้แก่เครื่องไคลเอ็นต์โดยอัตโนมัติ

4.1.6 เซิร์ฟเวอร์ข้อมูล

กำหนดให้มีไอพีแอดเดรสเป็น 192.168.1.51 netmark เป็น 255.255.255.0 โดยจะทำหน้าที่เก็บข้อมูลของผู้ใช้ภายในโครงข่ายให้มีความปลอดภัยในระดับสูง

4.2 ผลการทดลองระบบโครงข่าย

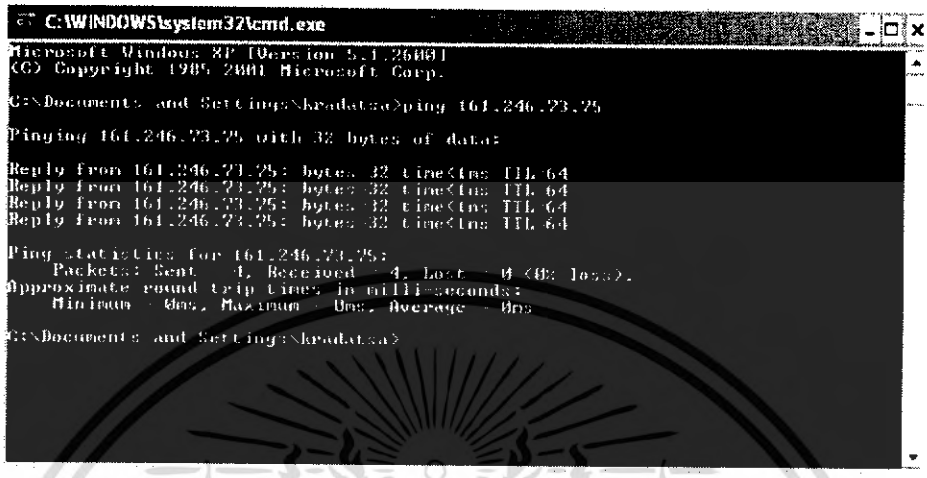
4.2.1 DHCP Server



รูปที่ 4.2 การใช้งาน DHCP

รูปที่ 4.2 แสดงการใช้ DHCP เมื่อผู้ใช้ที่เป็นเครื่องไคลเอ็นต์เข้าไปที่ Internet Protocol (TCP/IP) Properties และเลือก Obtain an IP address automatically เพื่อรับ IP Address แบบอัตโนมัติจาก DHCP Server

4.2.2 NAT และไฟล์วอลล์

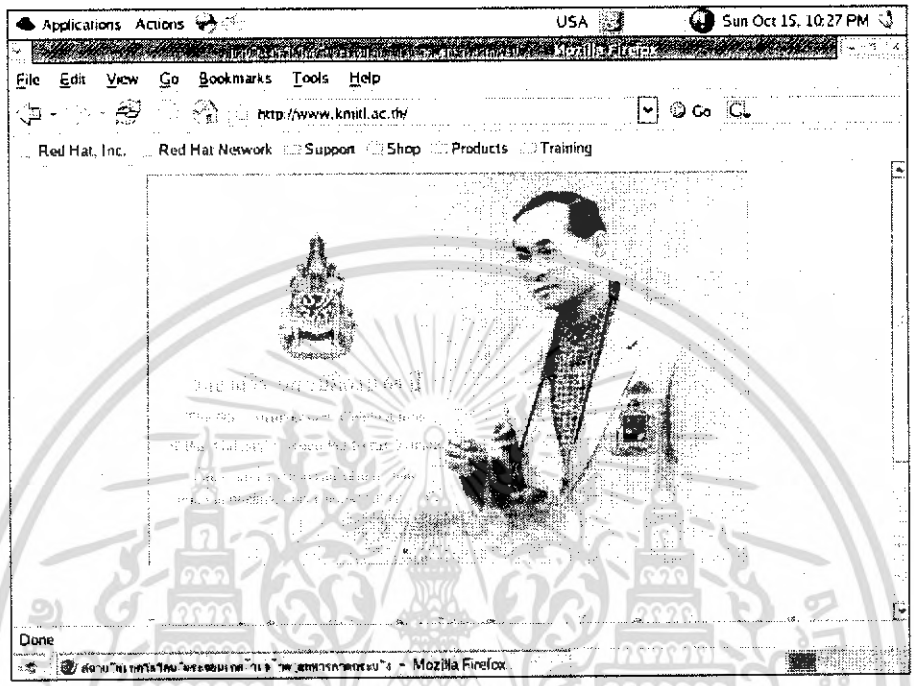


รูปที่ 4.3 การ ping เข้าสู่เครื่องที่เป็นเซิร์ฟเวอร์

จากรูปที่ 4.3 เป็นจากทดลอง ping เข้าสู่เครื่องที่เป็นเซิร์ฟเวอร์จากโครงข่ายภายนอก แสดงให้เห็นว่าโครงข่ายภายนอกสามารถมองเห็น IP 161.246.73.75

รูปที่ 4.4 การ ping จากเซิร์ฟเวอร์ออกสู่โครงข่ายภายนอก

จากรูปที่ 4.4 เป็นจากทดลอง ping ออกสู่เครื่องที่เป็นโครงข่ายภายนอกระบบเพื่อเช็คว่าระบบได้ถูกเชื่อมต่อเรียบร้อยแล้ว

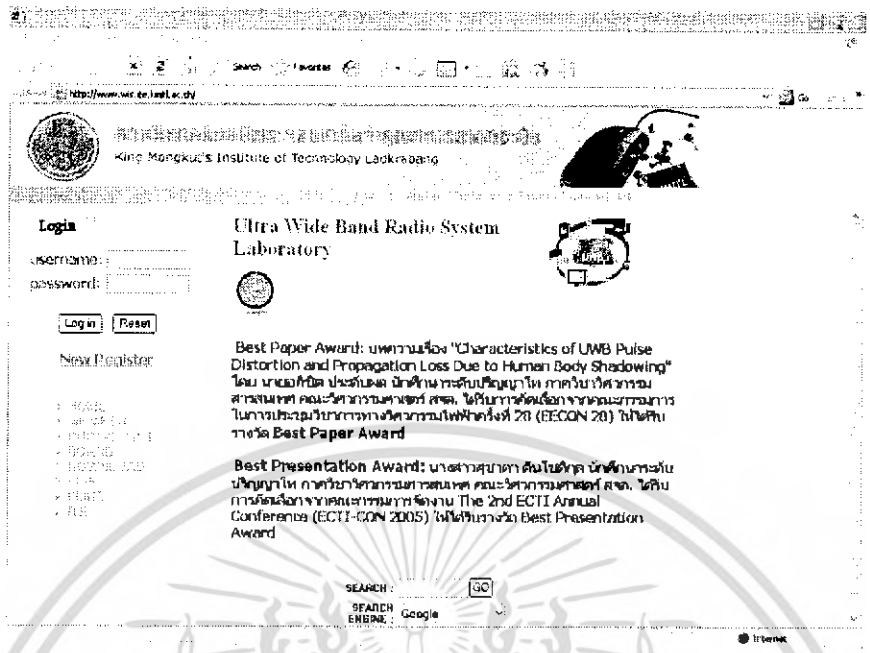


รูปที่ 4.5 การติดต่อกับโครงข่ายภายนอก

หลังจากที่ได้สร้าง NAT และไฟร์วอลล์เพื่อให้ผู้ใช้ที่อยู่ในโครงข่ายภายใน สามารถติดต่อกับโครงข่ายภายนอกได้อย่างสะดวก ปลอดภัย และโครงข่ายภายนอกไม่สามารถเห็นโครงข่ายภายในได้ ซึ่งในกรณีนี้จะมีกฎการเข้า- ออกแพ็กเก็ตเปิดให้โครงข่ายจากภายนอกติดต่อกับเฉพาะ Web Server เท่านั้น จากรูปที่ 4.5 ได้แสดงการติดต่อกับโครงข่ายภายนอกโดยผ่าน NAT และไฟร์วอล์ที่สร้างขึ้น

4.2.3 Web Server

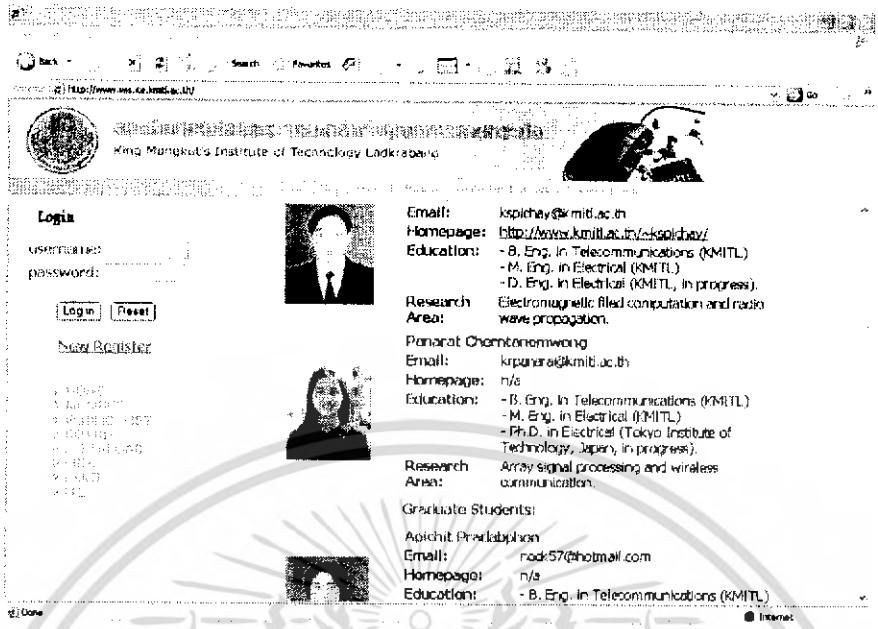
ในส่วนของ Web Server ได้มีการจัดทำเว็บไซต์ขึ้นมาเพื่อให้บริการแก่สมาชิกในห้องวิจัยโดยที่ได้จัดทำหน้าเว็บเพจดังต่อไปนี้



รูปที่ 4.6 หน้าโฮมเพจของ Web Server

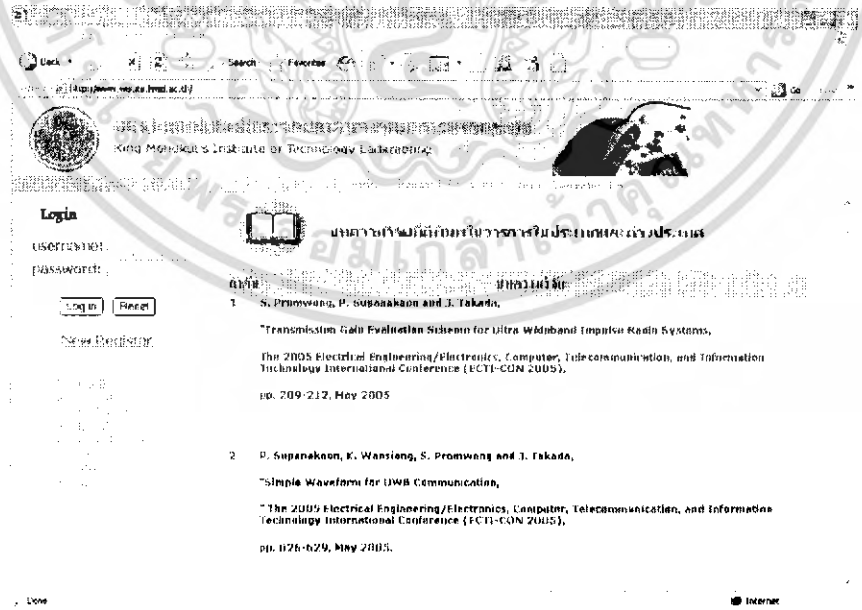
จากรูปเป็นหน้าแรกของ Web Server หน้านี้จะประกอบไปด้วย

- มีการประกาศข่าวต่าง ๆ เกี่ยวกับห้องวิจัยหรือเรื่องราวความรู้ใหม่ ๆ ที่เกี่ยวกับเทคโนโยลีการสื่อสารไร้สาย
- เป็นหน้าที่ให้สมาชิกของกลุ่มการวิจัยการสื่อสารเข้ามาล็อกอินเพื่อเข้าสู่ระบบ
- มี Link ไปยังเว็บไซต์ต่าง ๆ ที่มีความสำคัญและให้ความรู้เกี่ยวกับเทคโนโลยีการสื่อสารไร้สาย



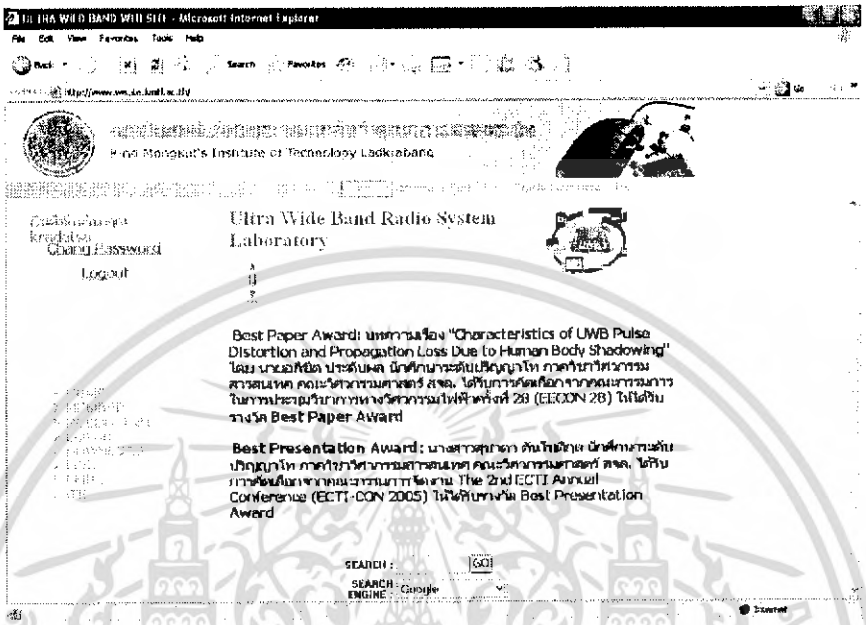
รูปที่ 4.7 หน้าสมาชิกของห้องวิจัย

จากรูป 4.7 หน้านี้จะเป็นหน้าที่แสดงรายชื่อ และข้อมูลประวัติทางการศึกษาของสมาชิกภายในกลุ่มการวิจัย และจากหน้านี้ผู้เข้าชมสามารถที่จะ link ไปยังโฮมเพจส่วนตัวของสมาชิกแต่ละท่านได้อีกด้วย



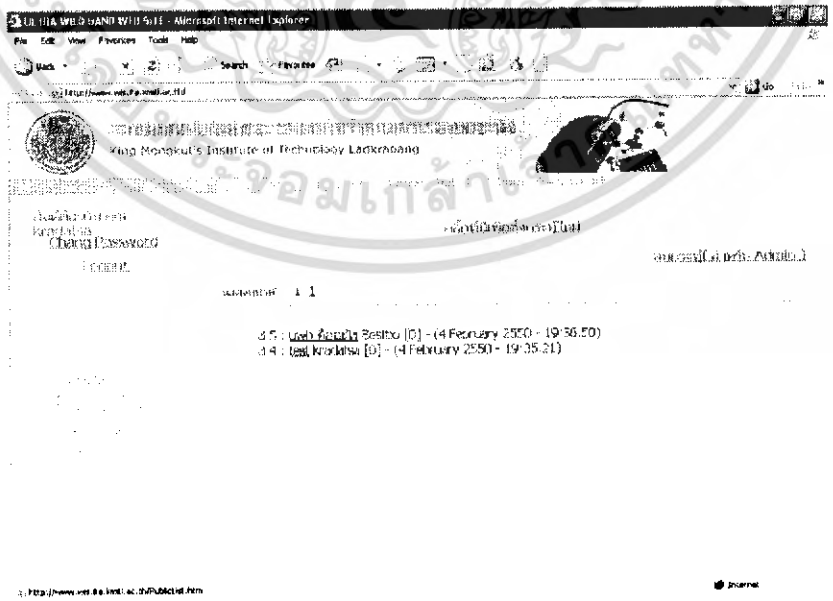
รูปที่ 4.8 บทความหรืองานวิจัยที่ตีพิมพ์

จากรูปที่ 4.8 ผู้ที่ผ่านเข้ามาจะสามารถเข้ามาชมผลงานของสมาชิกภายในกลุ่มการวิจัยซึ่งเป็นบทความและงานวิจัยที่ได้รับการตีพิมพ์ในวารสารทั้งในประเทศและต่างประเทศ



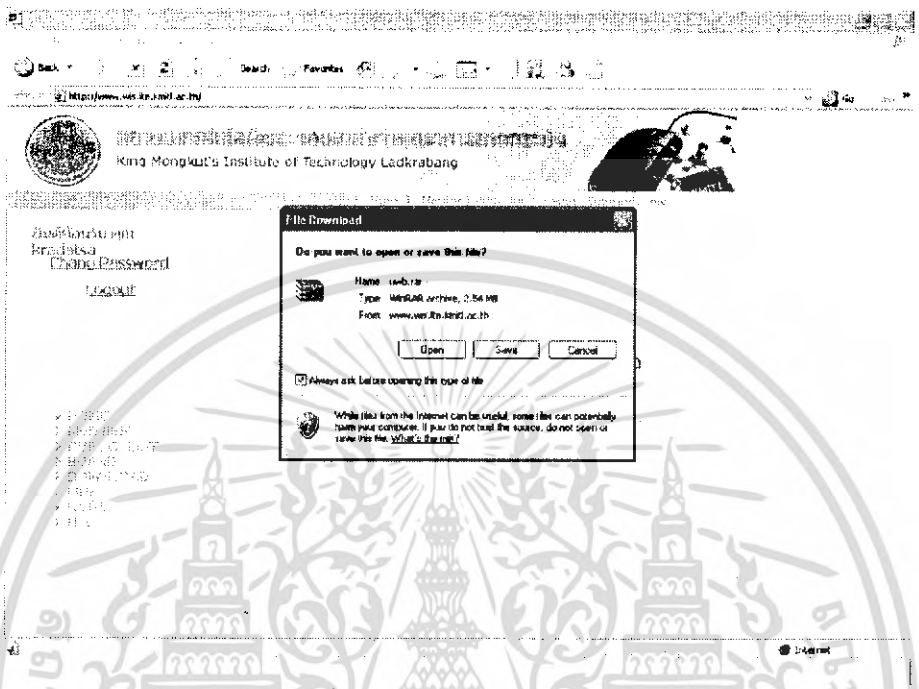
รูปที่ 4.9 หลังจากการล็อกอิน

รูปที่ 4.9 หลังจากที่สมาชิกได้มีการล็อกอินเพื่อผ่านเข้ามาในส่วนของสมาชิก ซึ่งจะสามารถทำการดาวน์โหลดงานวิจัยและใช้งานเว็บบอร์ดได้



รูปที่ 4.10 เว็บบอร์ด

จากรูปที่ 4.10 เมื่อสมาชิกได้ทำการล็อกอินจะสามารถทำการตั้งกระทู้ในเว็บบอร์ด เพื่อเป็นการแลกเปลี่ยนความรู้และข่าวสารระหว่างสมาชิกด้วยกัน

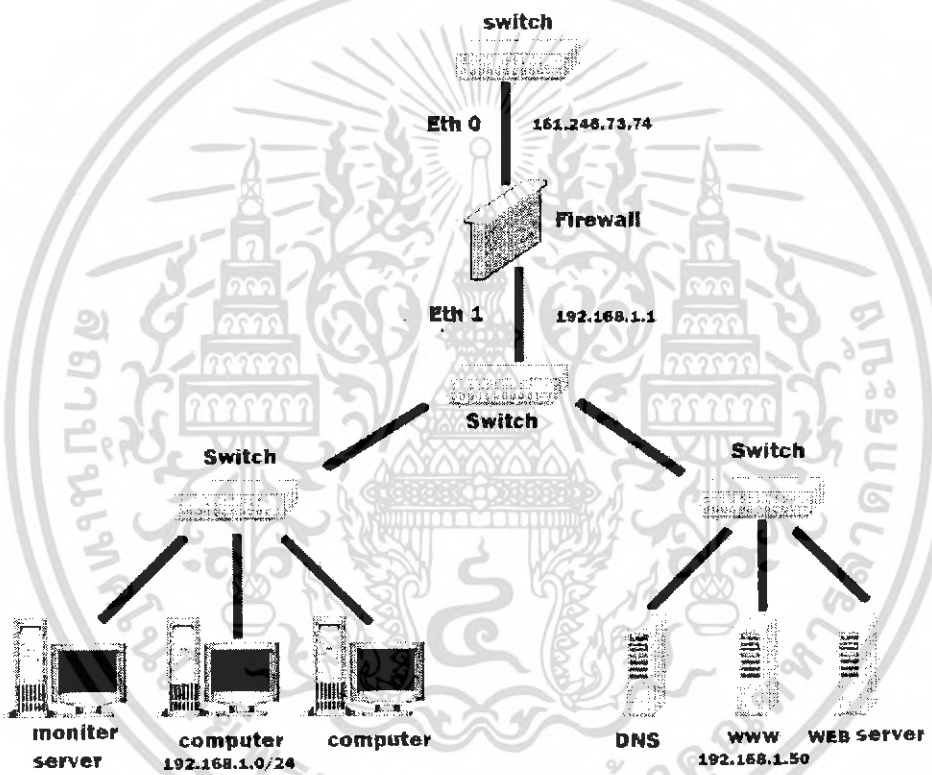


รูปที่ 4.11 ดาวน์โหลดงานวิจัย

ในหน้านี้จะอนุญาตให้เฉพาะสมาชิกเท่านั้นที่จะสามารถเข้ามาและทำการดาวน์โหลดงานวิจัย รวมทั้งปริญญานิพนธ์เพื่อนำไปศึกษา

บทที่ 5
บทสรุปของโครงงาน

5.1 สรุปการออกแบบเน็ตเวิร์ค



รูปที่ 5.1 สรุปการออกแบบเน็ตเวิร์ค

จากโครงงานเรื่องโครงข่ายประสิทธิภาพสูงสำหรับกลุ่มการวิจัยการสื่อสารไร้สายซึ่งได้จัดทำการวางระบบเน็ตเวิร์คที่มีประสิทธิภาพให้แก่กลุ่มการวิจัยสรุปผลการออกแบบได้ดังนี้

- ไฟร์วอลล์ ที่ใช้เป็นเกตเวย์ติดต่อกับโครงข่ายภายนอก มีการกำหนดกฎเพื่อควบคุมการผ่านเข้าออกของแพ็กเก็ตข้อมูล และทำ NAT สำหรับแปลงแอดเดรสจาก Private IP เป็น Public IP
- DNS Server สำหรับแปลงหมายเลขไอพีแอดเดรสให้อยู่ในรูปของโดเมนเนมหรือแปลงจากโดเมนเนมไปเป็นไอพีแอดเดรสได้ ได้ทำการลงทะเบียนชื่อโดเมนผ่าน ISP เรียบร้อยแล้ว และทำการประกาศโดเมนลูก (Subdomain) เป็น "wis.ite.kmitl.ac.th"
- เว็บเซิร์ฟเวอร์สำหรับให้บริการด้านโฮมเพจและแอพพลิเคชั่นต่างๆ ที่เทคโนโลยีการสื่อสารไร้สายให้แก่อาจารย์ นักศึกษาและสมาชิกทุกท่านในกลุ่มการวิจัยการสื่อสารไร้สาย
- DHCP Server สำหรับแจกไอพีแอดเดรสให้แก่เครื่องไคลเอ็นต์แบบอัตโนมัติ
- มอนิเตอร์เซิร์ฟเวอร์ สำหรับดูแลจัดการคอมพิวเตอร์ของผู้ใช้ภายในโครงข่าย มีโปรแกรมตรวจจับไวรัสในโครงข่ายภายใน สามารถแจ้งเตือนกับผู้ใช้ภายในระบบได้เมื่อเกิดปัญหา และมีการเก็บล็อกข้อมูลต่างๆ ของการใช้งานระบบโครงข่ายของผู้ใช้ เมื่อเกิดปัญหาจะได้ทราบสาเหตุ
- สร้างเว็บแอพพลิเคชั่น ซึ่งผู้ใช้สามารถเข้ามาล็อกอินเพื่อดาวน์โหลดและตั้งกระทู้เกี่ยวกับในกลุ่มการวิจัยได้ และบริการงานด้านต่างๆ ให้แก่ผู้ใช้งานภายในกลุ่มการวิจัย

5.2 ผลที่ได้รับ

- ระบบโครงข่ายภายในมีประสิทธิภาพ เสถียรภาพ และมีความปลอดภัยของโครงข่ายค่อนข้างสูงสามารถป้องกันการโจมตีจากโครงข่ายภายนอกได้
- มีการใช้ Antivirus Gateway เพื่อกรองแพ็กเก็ตก่อนเข้ามายังโครงข่าย เพื่อป้องกันไวรัสมารบกวนการทำงาน
- สามารถใช้งานโดเมนลูกชื่อ "wis.ite.kmitl.ac.th" ได้เป็นอย่างดีสามารถใช้ติดต่อกับโครงข่ายภายนอกได้
- เว็บเซิร์ฟเวอร์สามารถใช้งานได้ มีการประกาศข่าวสารต่างๆ ให้สมาชิกได้รับรู้
- ผู้ใช้สามารถศึกษาและดาวน์โหลดบทความจากงานวิจัยได้
- DHCP สามารถทำงานได้อย่างมีประสิทธิภาพ ผู้ใช้ไม่เกิดปัญหาเรื่องการเซตไอพีแอดเดรสซ้ำซ้อน ไม่เกิดการชนกันของไอพีแอดเดรส

5.3 ปัญหาที่พบ

- ปัญหาเรื่องการติดตั้งไฟร์วอลล์เกิดปัญหาในการตั้งค่า และในการเขียน IPtables หรือกฎการผ่านเข้า- ออกของแพ็กเก็ตข้อมูล
- ปัญหาในเรื่องงบประมาณ เนื่องจากซอฟต์แวร์บางตัวที่ประสิทธิสูง แต่จำเป็นต้องจ่ายค่าลิขสิทธิ์ จึงมีความจำเป็นต้องเลือกซอฟต์แวร์ที่เป็นโอเพ่นซอร์สซึ่งจะด้อยกว่าในเรื่องของประสิทธิภาพการทำงาน

5.4 แนวทางการทำงานในส่วนต่อไป

- สามารถทำการสำรองข้อมูล (backup) ในกรณีที่เกิดความสูญหายของข้อมูล และกรณีเกิดความเสียหายของระบบโครงข่าย
- พัฒนาในส่วนของเซิร์ฟเวอร์ข้อมูลโดยการรวบรวมปริญญานิพนธ์ และงานวิจัยต่างๆให้หลากหลายมากขึ้น

บรรณานุกรม

อ.บัณฑิต จามรภูติ. 2546. **คัมภีร์ Linux Redhat เล่ม 1.** กรุงเทพฯ : สำนักพิมพ์ Bandhit

สมศักดิ์ โชคชัยชุติกุล. 2547. **PHP5.** กรุงเทพฯ : บริษัท โปรวิชั่น จำกัด

กิตติ ภักดีวัฒนะกุล. 2546. **คัมภีร์ PHP.** กรุงเทพฯ : สำนักพิมพ์ KTP

http://linux.thai.net

http://linux.org

http://ciberthai.com

http://nectec.or.th

http://thaicert.nectec.or.th