การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตสำหรับองค์กร

Internet Security for Organization

นางสาวนิสา พัฒนพงษ์อนันต์

นางสาวสุนันท์ โชคจรัสกิจ

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2544

การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตสำหรับองค์กร

Internet Security for Organization

โดย

นางสาวนิสา พัฒนพงษ์อนันต์

นางสาวสุนันท์ โชคจรัสกิจ

อาจารย์ที่ปรึกษา

ดร. วรวัฒน์ ลิ้มโภคา

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2544

ปริญญานิพนธ์ปีการศึกษา 2544

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตสำหรับองค์กร

Internet Security for Organization

ผู้จัดทำ

1. นางสาวนิสา พัฒนพงษ์อนันต์ รหัสประจำตัว 41014230
2. นางสาวสุนันท์ โชคจรัสกิจ รหัสประจำตัว 41014477

อาจารย์ที่ปรึกษา

(ดร. วรวัฒน์ ลิ้มโภคา)

การรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตสำหรับองค์กร

น.ส. นิสา พัฒนพงษ์อนันต์ 41014230
น.ส. สุนันท์ โชคจรัสกิจ 41014477
อาจารย์ วรวัฒน์ ลิ้มโภคา อาจารย์ที่ปรึกษา
ปีการศึกษา 2544

บทคัดย่อ

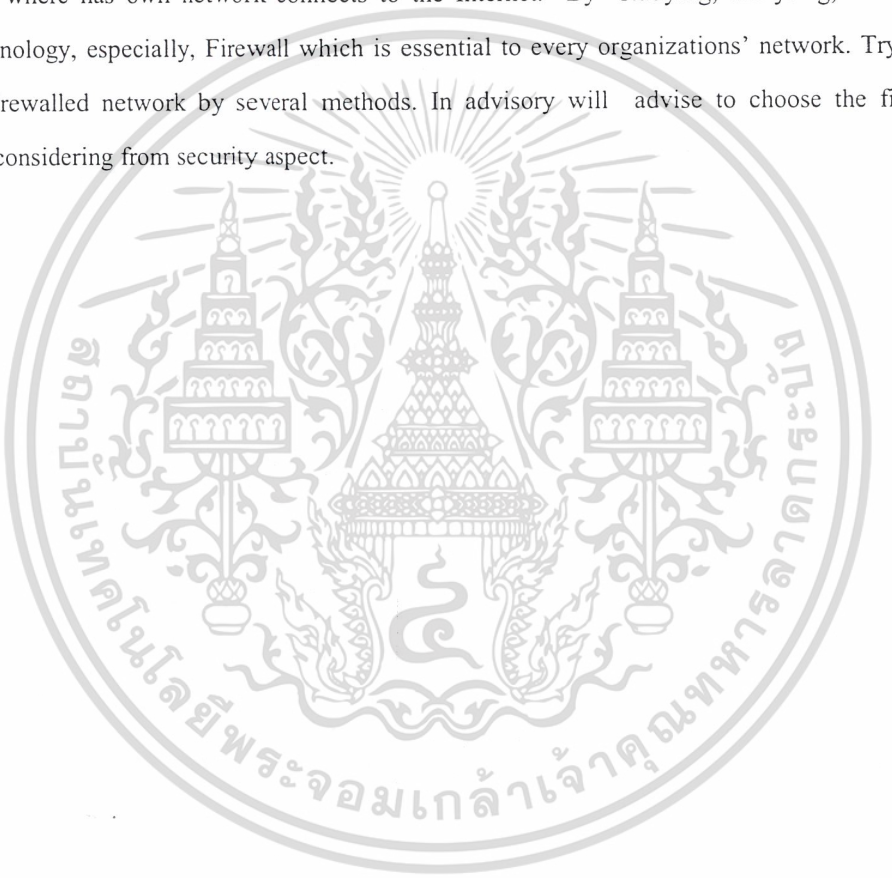
บทความฉบับนี้กล่าวถึงรายละเอียดของระบบรักษาความปลอดภัยบนเครือข่าย โดยเน้นไปที่องค์กรหรือหน่วยงานที่มีเครือข่ายเชื่อมต่อกับอินเตอร์เน็ต โดยศึกษา วิเคราะห์ เปรียบเทียบเทคโนโลยีในการรักษาความปลอดภัยต่างๆ พร้อมทั้งทดสอบผลิตภัณฑ์ไฟร์วอลล์ซึ่งเป็นเทคโนโลยีการรักษาความปลอดภัยที่จำเป็นอย่างยิ่งไม่ว่าจะสำหรับองค์กรขนาดใดๆ ก็ตาม โดยพยายามโจมตีเน็ตเวิร์กที่ติดตั้งไฟร์วอลล์ด้วยวิธีต่างๆ เพื่อค้นหาจุดบกพร่องและจุดดีในด้านความปลอดภัยของแต่ละผลิตภัณฑ์ จึงนำมาซึ่งคำแนะนำในการเลือกใช้ผลิตภัณฑ์ไฟร์วอลล์ อย่างชาญฉลาด ในที่สุด

Internet Security for Organization

Ms. Nisa Patanaponganan 41014230
Ms. Sunun Chokjaraskij 41014477
Mr. Worawat Limpoka Advisor

ABSTRACT

This article informs to the detail of Network Security System. By emphasizing for the organization where has own network connects to the Internet. By studying, analysing, comparing security technology, especially, Firewall which is essential to every organizations' network. Trying to attack the firewalled network by several methods. In advisory will advise to choose the firewall products by considering from security aspect.



กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้คงไม่อาจเสร็จได้ด้วยดี หากไม่ได้รับความช่วยเหลือ และร่วมมือจากหลาย ๆ ฝ่ายด้วยกัน บุคคลแรกที่ต้องกล่าวถึงเพราะเป็นส่วนสำคัญที่ทำให้วิทยานิพนธ์นี้เสร็จลงได้ก็คือ อาจารย์ วรวัฒน์ ลิ้มโภคา อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ให้ความเอาใจใส่ แนะนำ และช่วยเหลือเสมอมา ซึ่งต้องขอขอบพระคุณเป็นอย่างมาก

ขอขอบคุณอาจารย์ธนา ที่ให้คำปรึกษาแนะนำเกี่ยวกับการทำงาน

ขอขอบคุณ ป้อมที่ให้คำปรึกษาและให้ข้อมูลเกี่ยวกับไฟร์วอลล์ รวมไปถึงเทคโนโลยีทางด้านความปลอดภัยอื่นๆ ด้วย

พี่โจ้ที่ให้ยืมอุปกรณ์ต่างๆ ทางด้านเน็ตเวิร์กคือ สายครอส การ์ดแลน เพื่อมาทำการอิมพลีเมนท์ระบบ

ปอนที่ช่วยกู้ฮาร์ดดิสก์ให้

พี่ต๋องสำหรับสาย CAT 5 อันยาวเหยียด

หลิงที่ให้ยืมเครื่องในการใช้งาน

นุ้ยที่ให้ยืมเครื่องในการใช้งาน และให้ยืมหน่วยความจำมาใช้งาน

ฉุยที่พยายามหาหน่วยความจำและฮาร์ดดิสก์มาให้

พี่โกศลที่ให้คำแนะนำในการติดตั้งและใช้งานผลิตภัณฑ์ไฟร์วอลล์

พี่เชาวน์ที่ให้คำแนะนำในการโจมตีด้วย DoS และการเซ็ตอัพวินโดว์เอ็นที

ป๊อกสำหรับคำแนะนำเกี่ยวกับวินโดว์เอ็นที

ป้อม (ไอซีคิว) สำหรับคำแนะนำเกี่ยวกับลีนุกซ์และสาสตร์แห่งโลกมืด

โต (ไอซีคิว) สำหรับคำแนะนำเกี่ยวกับ Firewall-1

บัส เก่ง ที่ช่วยในการเซ็ตเครื่องเพื่อใช้งาน

เต้ จิ๊บ บอล และเพื่อนๆ พี่ๆ คนอื่นๆ ที่ไม่ได้กล่าวถึง

พี่อั๋น พี่อาร์ม พี่แอน พี่จูน ที่ให้คำแนะนำปรึกษา

ขอขอบคุณ นุชกับอ้อ ถ้าไม่มีเธอ 2 คน โปรเจ็คนี้คงไม่สำเร็จ

ขอขอบคุณ www.google.com และเว็บไซต์อื่นๆ ที่เป็นแหล่งค้นหาข้อมูล

และท้ายที่สุดนี้บุคคลที่สำคัญที่สุดที่ต้องขอขอบพระคุณก็คือ บิดา มารดา อันเป็นที่เคารพรักยิ่ง ซึ่งได้เลี้ยงดูข้าพเจ้ามาเป็นอย่างดี พร้อมทั้งให้โอกาสในการศึกษาอย่างเต็มที่ และยังให้กำลังใจ เอาใจใส่เสมอมา ในทุก ๆ ด้านอันหาที่เปรียบมิได้ ข้าพเจ้าขอระลึกในพระคุณอันสุดประมาณ และขอกราบขอบพระคุณมา ณ ที่นี้

นิสา พัฒนพงษ์อนันต์

สุนันท์ โชคจรัสกิจ

สารบัญ

สารบัญภาพประกอบ

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มา

ในปัจจุบันนี้อินเตอร์เน็ตได้เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์เป็นอย่างมาก เห็นได้จากการที่มีผู้ใช้งานคอมพิวเตอร์ที่เชื่อมต่อเข้ากับอินเตอร์เน็ตมีอัตราเพิ่มขึ้นอย่างรวดเร็ว มีการขยายตัวไปทั่วโลก อินเตอร์เน็ตทำให้คนที่อยู่กันคนละซีกโลกสามารถสนทนากันได้ ทำให้การสื่อสารทำได้อย่างรวดเร็วและประหยัดกว่าการที่จะต้องเดินทางไปเอง อินเตอร์เน็ตเป็นแหล่งข้อมูลมหาศาลที่ไม่มีวันที่ใครจะเรียนรู้ได้หมดสิ้น ดังนั้นไม่น่าแปลกที่ว่าองค์กรทั้งภาครัฐ และเอกชน ก็มีการเชื่อมต่อเข้ากับอินเตอร์เน็ตทำให้สามารถแลกเปลี่ยนข้อมูลกันทางคอมพิวเตอร์จากทุกๆ มุมโลกได้ ในขณะเดียวกันเครือข่าย(Network) ขององค์กรเหล่านั้นที่เชื่อมต่อกับอินเตอร์เน็ตก็สามารถเข้าถึงโดยใครก็ได้ที่ใช้งานอินเตอร์เน็ตอยู่ ไม่ว่าจะอยู่ห่างไกลกันแค่ไหนก็ตาม ซึ่งส่วนใหญ่องค์กรที่เชื่อมต่ออินเตอร์เน็ตอยู่นั้นมักมีข้อมูลที่สำคัญ และเป็นความลับ ทำให้ข้อมูลเหล่านี้อยู่ในสถานะที่เสี่ยงต่อผู้ไม่หวังดีต่อองค์กร ซึ่งอาจจะเป็นคู่แข่ง หรือใครก็ตามอย่างหลีกเลี่ยงไม่ได้ ด้วยเหตุนี้เองความปลอดภัยในเครือข่ายขององค์กรที่เชื่อมต่อกับอินเตอร์เน็ตจึงเป็นสิ่งที่จำเป็น และสำคัญสำหรับองค์กรเหล่านั้นเป็นอย่างมาก

ดังนั้นทางคณะผู้จัดทำจึงมีความสนใจเกี่ยวกับการรักษาความปลอดภัยบนระบบเครือข่ายที่เชื่อมต่อกับอินเตอร์เน็ต เพื่อเป็นการรักษาข้อมูลที่สำคัญ และเป็นความลับที่ไม่สามารถเปิดเผยได้ ไม่ให้ผู้ประสงค์ร้ายสามารถนำข้อมูลเหล่านั้นไปได้ หรือมาโจมตีระบบเครือข่ายของเราได้ ทางผู้จัดทำได้เล็งเห็นถึงความสำคัญในจุดนี้ จึงได้ทำการศึกษารายละเอียดเกี่ยวกับการรักษาความปลอดภัยบนระบบเครือข่าย เพื่อเป็นประโยชน์แก่ผู้ที่สนใจหรือต้องการเรียนรู้ ศึกษาเพื่อเป็นแนวทางในการนำไปใช้งาน หรือนำไปเป็นพื้นฐานในการค้นคว้าต่อไป

1.2 วัตถุประสงค์ของงานวิจัย

วัตถุประสงค์ของการทำโปรเจ็คนี้คือ

1. ศึกษาการทำงานของระบบรักษาความปลอดภัยบนอินเตอร์เน็ต เทคโนโลยีทางด้านความปลอดภัยแต่ละชนิด
2. ศึกษาเทคนิค เทคโนโลยี และวิธีการต่างๆ ในการรักษาความปลอดภัยให้แก่เครือข่ายขององค์กรที่เชื่อมต่อกับอินเตอร์เน็ต
3. เปรียบเทียบผลิตภัณฑ์ไฟร์วอลล์ โดยพิจารณาในด้านความปลอดภัยเป็นหลัก
4. ทดสอบไฟร์วอลล์ โดยโจมตีเครือข่ายที่ติดตั้งไฟร์วอลล์ ด้วย DoS (Denial of Service)
5. ทดสอบไฟร์วอลล์ โดยการสแกนเพื่อตรวจสอบโฮสต์และเครือข่าย

1.3 ขอบเขตของงานวิจัย

โครงงานนี้เริ่มต้นศึกษาที่ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์บนอินเตอร์เน็ต ครอบคลุมทุกประเภทของเทคโนโลยี การทำให้เครือข่ายขององค์กรปลอดภัยที่สุด เปรียบเทียบ และพยายามโจมตีผลิตภัณฑ์ไฟร์วอลล์ ซึ่งเป็นเทคโนโลยีการรักษาความปลอดภัยที่สำคัญยิ่งสำหรับทุกๆ เครือข่าย

1.4 วิธีการดำเนินงาน

ในขั้นแรกจะเริ่มต้นด้วยการศึกษาถึงความรู้เบื้องต้น และความปลอดภัยของระบบเครือข่ายอินเตอร์เน็ต จากนั้นก็นำไปสู่จุดประสงค์ที่ต้องมีการรักษาความปลอดภัย มีวิธีการโจมตีหรือใช้ช่องโหว่ในการโจมตีระบบเครือข่ายวิธีใดบ้าง รวมไปถึงการสำรวจและรวบรวมข้อมูลสำหรับการบุกรุกและหาช่องโหว่ของเครือข่ายในองค์กร

จากการโจมตีและการหาช่องโหว่ต่างๆ ในเครือข่ายอินเตอร์เน็ต จึงนำมาสู่ภาพรวมของการรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์ในองค์กร การนำเทคโนโลยีความปลอดภัยต่างๆ อันประกอบด้วยการเข้ารหัส, แอพพลิเคชันสำหรับการพิสูจน์ตน, ไฟร์วอลล์, พร็อกซีเซิร์ฟเวอร์, ระบบตรวจจับผู้บุกรุก, IPSec, VPN และ SSL มาใช้

เมื่อได้ศึกษาเทคโนโลยีความปลอดภัยต่างๆ แล้ว ทางกลุ่มของข้าพเจ้าได้เล็งเห็นว่าไฟร์วอลล์เปรียบเสมือนปราการด่านแรกขององค์กร เป็นสิ่งที่แต่ละองค์กรจำเป็นต้องมีในการรักษาความปลอดภัย จึงมุ่งประเด็นไปสู่การทดสอบไฟร์วอลล์ โดยพิจารณาในด้านความปลอดภัยเป็นหลัก

การทดสอบด้านความปลอดภัยจะแบ่งเป็น 2 ส่วนหลักๆ คือ การโจมตีด้วย DoS และการสแกนเพื่อตรวจสอบ โดยผลิตภัณฑ์ไฟร์วอลล์ที่นำมาศึกษานั้นมีทั้งเอ็นเตอร์ไพรส์ไฟร์วอลล์และเพอร์ซันนอลไฟร์วอลล์

จากนั้นได้ทำการสรุปผลการทดสอบผลิตภัณฑ์ไฟร์วอลล์ และสรุปการทำงาน

บทที่ 2
ความรู้เบื้องต้นและความปลอดภัยของระบบเครือข่ายอินเตอร์เน็ต

2.1 โพรโตคอลทีซีพี/ไอพี (TCP/IP Protocol)

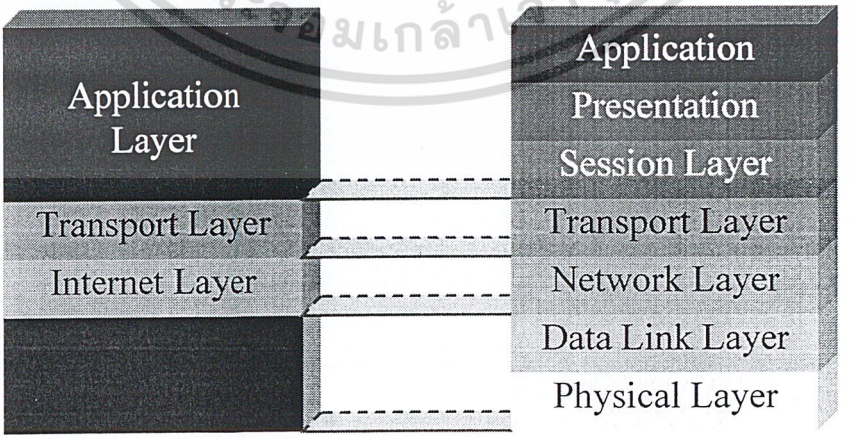
2.1.1 ความเป็นมาของโพรโตคอลทีซีพี/ไอพี

เป็นโพรโตคอลมาตรฐานที่ใช้กันอยู่ในระบบปฏิบัติการแบบยูนิกซ์ เริ่มพัฒนาโดยกระทรวงกลาโหมของสหรัฐใน ค.ศ. 1969 เพื่อเชื่อมต่อเครื่องคอมพิวเตอร์หลายชนิดที่อยู่ห่างไกลกัน เครือข่ายที่จัดตั้งในระยะแรกชื่อว่า อาร์พาเน็ต (ARPANET)

ต่อมาได้พัฒนาเป็นเครือข่ายอินเทอร์เน็ต โพรโตคอลนี้เหมาะสำหรับเชื่อมต่อคอมพิวเตอร์ทั้งใกล้และไกลเข้าด้วยกัน และมีมาตรฐานรองรับทำให้ผู้ผลิตฮาร์ดแวร์และซอฟต์แวร์ สามารถสร้างอุปกรณ์และโปรแกรมที่จะรองรับการทำงานของโพรโตคอลนี้ ทำให้เครื่องคอมพิวเตอร์สามารถรับส่งข้อมูลกันได้ไม่ว่าจะเป็นเครื่องขนาดเล็กหรือขนาดใหญ่ หรือใช้ระบบปฏิบัติการอะไรก็ตาม ทีซีพี/ไอพี (TCP/IP) เป็นชุดโพรโตคอลที่ประกอบด้วยโพรโตคอลต่างๆ หลายโพรโตคอล แต่ละโพรโตคอลมีคุณลักษณะ และมีความสามารถในการทำงานแตกต่างกัน โดยที่ในบทนี้ได้กล่าวถึงรายละเอียดและคุณสมบัติของโพรโตคอลที่สำคัญบางโพรโตคอล

2.1.2 การเชื่อมต่อของโพรโตคอลทีซีพี/ไอพี (TCP/IP Linking)

ทีซีพี/ไอพี (TCP/IP หรือ Transmission Control Protocol/Internet Protocol) เป็นโพรโตคอลในการสื่อสารในระบบอินเทอร์เน็ตและอินทราเน็ต การทำงานของทีซีพี/ไอพีสามารถเปรียบเทียบกับโมเดลอ้างอิงโอเอสไอ (Open System Interconnection Reference Model: OSI) ตามมาตรฐานไอเอสโอ (International Organization for Standardization: ISO) ได้ดังรูปที่ 2-1

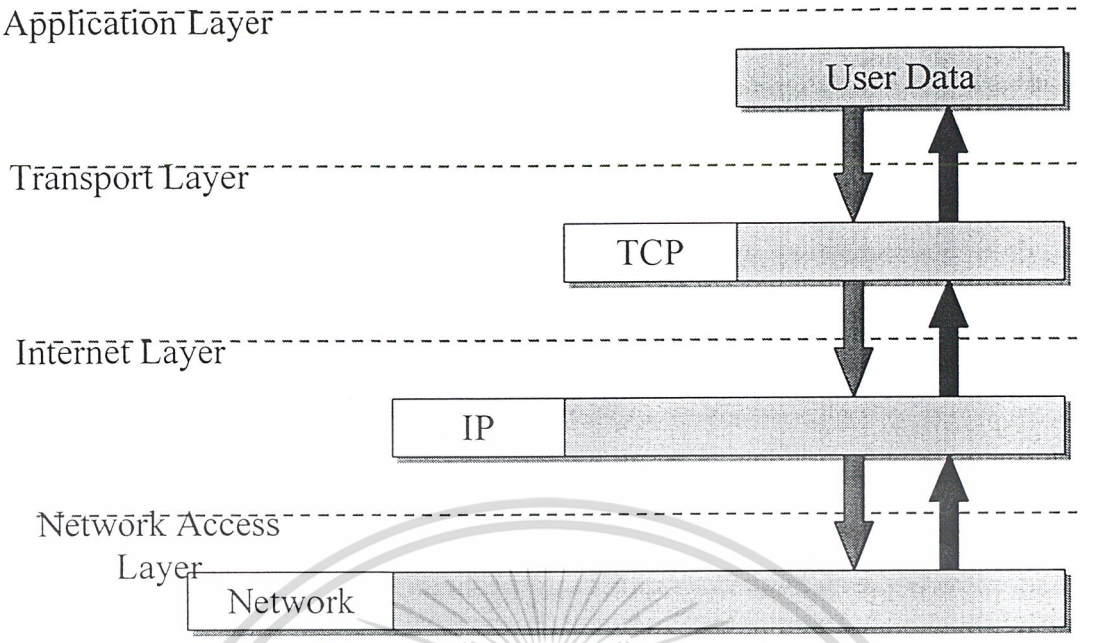


รูปที่ 2-1 แสดงการเปรียบเทียบเลเยอร์ของโอเอสไอกับเลเยอร์ของทีซีพี/ไอพี

ในแต่ละระดับชั้นของทีซีพี/ไอพีมีการทำงานที่แตกต่างกัน ตั้งแต่การติดต่อกับแอพพลิเคชันจนกระทั่งแปลงเป็นสัญญาณส่งไปตามสายสัญญาณ ซึ่งการทำงานในแต่ละระดับชั้นของทีซีพี/ไอพี มีดังตารางที่ 2-1

ชื่อระดับชั้น	หน้าที่
1. ชั้นแอพพลิเคชัน (Application Layer)	ชั้นนี้รองรับการทำงานของแอพพลิเคชันต่างๆ ที่ทำงานเป็นโพรเซสอยู่ในเครื่องต้นทางและปลายทาง โดยจัดการเชื่อมต่อระหว่างโพรเซส หรือแอพพลิเคชันที่อยู่ต่างเครื่องกัน โดยการทำงานของแอพพลิเคชันต่างๆมีการติดต่อกันตามแต่ละโพรโตคอลเฉพาะแล้วแต่แอพพลิเคชันที่ใช้งาน ซึ่งจะขอบริการจากชั้นทรานสปอร์ตอีกทีหนึ่ง
2. ชั้นทรานสปอร์ต (Transport Layer)	มีการสร้างการเชื่อมต่อกันระหว่างแอพพลิเคชันแบบ end-to-end โดยจุดที่เชื่อมต่อกันเพื่อรับส่งข้อมูลนี้เรียกว่า พอร์ต (port) หรือซ็อกเก็ต (Socket) ในชั้นนี้มีบริการหลักอยู่ 2 แบบ คือ Connection Oriented โดยเรียกผ่านโพรโตคอลทีซีพี (TCP: Transmission Control Protocol) และ Connectionless ซึ่งเรียกผ่านโพรโตคอลยูดีพี (UDP: User Datagram Protocol) ซึ่งกล่าวถึงในหัวข้อถัดไป
3. ชั้นอินเทอร์เน็ต (Internet Layer)	ชั้นนี้มีหน้านี้ส่งผ่านข้อมูลระหว่างเครือข่าย โดยมีโพรโตคอลที่ทำงานเป็นกลไกสำคัญในการส่งผ่านข้อมูลไปยังเครือข่ายใดๆ ในอินเทอร์เน็ต คือ ไอพี (Internet Protocol: IP) ซึ่งกล่าวถึงในหัวข้อถัดไป นอกจากนี้ในชั้นนี้ยังมีโพรโตคอลทำงานอยู่ด้วยอีก 2 ชนิด คือ ไอซีเอ็มพี (Internet Control Message Protocol: ICMP) และ เออาร์พี (Address Resolution Protocol: ARP)
4. ชั้นเน็ตเวิร์กอินเตอร์เฟส (Network Interface Layer)	ทำหน้าที่ในการแปลงข้อมูลให้อยู่ในรูปที่เหมาะสมกับเครือข่ายแต่ละแบบ ซึ่งแตกต่างกันออกไป และแปลงเป็นสัญญาณไฟฟ้าส่งไปยังเครือข่าย

ตารางที่ 2-1 การทำงานของแต่ละระดับชั้นของทีซีพี/ไอพี

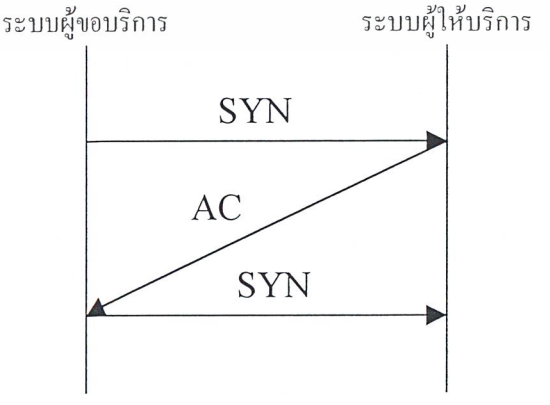


รูปที่ 2-2 แสดงการข้อมูลที่ส่งผ่านในโมเดลของทีซีพี/ไอพี

ในชุดโพรโตคอลทีซีพี/ไอพีนี้ มีโพรโตคอลหลักที่ขอกล่าวถึง 3 โพรโตคอล ได้แก่ โพรโตคอลทีซีพี โพรโตคอลยูดีพี ซึ่งทำงานในชั้นทรานสปอร์ต และโพรโตคอลไอพี ซึ่งทำงานในชั้นอินเทอร์เน็ต โดยมีรายละเอียดดังต่อไปนี้

2.1.3 โพรโตคอลทีซีพี (TCP: Transmission Control Protocol)

การทำงานที่สำคัญอย่างหนึ่งของโพรโตคอลทีซีพี คือ การทำ "3-way Handshake" ซึ่งเป็นกระบวนการเริ่มต้นในการสร้างการเชื่อมต่อในชั้นทรานสปอร์ต กล่าวคือ ในการติดต่อกันระหว่างระบบในเครือข่ายต้องมีการสร้างการเชื่อมต่อไปยังระบบที่ให้บริการก่อน โดยผู้ขอบริการส่งสัญญาณ SYN เพื่อขอบริการ จากนั้นผู้ให้บริการจะส่งสัญญาณ ACK เพื่อตอบรับการเชื่อมต่อที่ร้องขอมา จึงสามารถรับส่งข้อมูลกันได้ ดังรูปที่ 2-3



รูปที่ 2-3 แสดงการทำ 3-way Handshake

การเชื่อมต่อแบบ 3-way handshake นี้ เป็นการตรวจสอบความพร้อมของทั้งฝ่ายส่งและฝ่ายรับ และการกำหนดค่าเริ่มต้นของพารามิเตอร์ต่างๆ ของทั้งสองฝ่ายให้ตรงกัน หลังจากกระบวนการทำ 3-way handshake สิ้นสุด ทั้งสองฝ่ายจึงสามารถรับและส่งข้อมูลซึ่งกันและกันได้

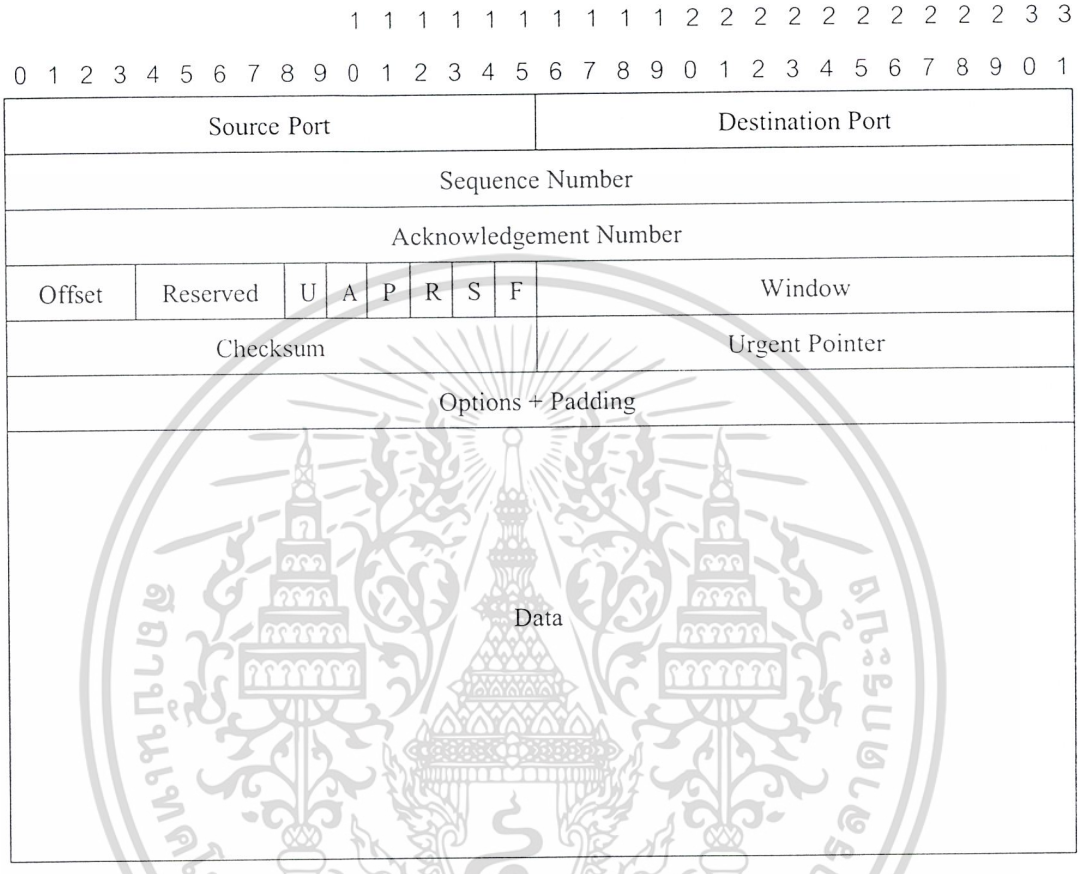
ดังนั้นโพรโตคอลทีซีพีจึงเป็นโพรโตคอลที่มีการรับส่งข้อมูลแบบ "Connection Oriented" ทำให้การทำงานของทีซีพีมีความน่าเชื่อถือมากขึ้น หน้าที่การทำงานของทีซีพีในการรับส่งข้อมูลมีหน้าที่หลัก 6 ข้อ คือ

1. ควบคุมการรับส่งข้อมูล (Basic Data Transfer)
2. ความน่าเชื่อถือในการรับส่งข้อมูล (Reliability)
3. ควบคุมการไหลของข้อมูล (Flow Control)
4. การทำมัลติเพล็ก (Multiplexing)
5. ควบคุมการเชื่อมต่อ (Connection)
6. ความปลอดภัยในการรับส่งข้อมูล (Security)

<u>ส่วนประกอบของทีซีพีเฮดเดอร์</u>

1. *Source Port* : เป็นหมายเลขพอร์ตของบริการที่เครื่องต้นทาง
2. *Destination Port* : เป็นหมายเลขพอร์ตของบริการเครื่องปลายทาง
3. *Sequence Number* : เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลของเครื่องที่ต้องการขอส่งข้อมูล
4. *Acknowledgement Number* : เป็นหมายเลขที่บอกลำดับของการรับส่งข้อมูลที่ฝั่งรับข้อมูลปกติ ค่าของ Acknowledgement Number มีค่าเท่ากับ Sequence Number (ของอีกฝั่งหนึ่ง) + 1 เสมอ
5. *Data Offset* : เป็นตัวบอกค่าออฟเซตของข้อมูล เพราะทีซีพีนั้นไม่มีการกำหนดความยาวที่แน่นอนของข้อมูล จึงต้องมีออฟเซตเป็นตัวบอก
6. *Flag* : เป็นบิตที่บอกชนิดของข้อมูล ได้แก่
    - URG : Urgent Pointer Field Significant - แสดง Urgent Pointer
    - ACK : Acknowledgement Field Significant – แสดงการ Acknowledgement
    - PSH : Push Function
    - RST : Reset The Connection - แสดงเมื่อรีเซ็ทการเชื่อมต่อ
    - SYN : Synchronize Sequence Number - หมายเลขแพ็กเก็ตที่ส่งแบบซิงโครนัส
    - FIN : No more data from sender - แสดงว่าไม่มีข้อมูลที่ส่งจากผู้ส่งแล้ว
7. *Window* : เป็นเลขบอกจำนวนของอ็อกเต็ต (octet) ของข้อมูล จัดการในส่วนของ end-to-end flow control
8. *Checksum* : เป็นส่วนที่ตรวจสอบความถูกต้องของข้อมูล
9. *Urgent Pointer* : เป็นตัวชี้ตำแหน่งของ Urgent Data

10. *Option and Padding* : เป็นตัวบอกออปชันของโพรเซสที่ใช้ทีซีพี
11. *Data* : เนื้อข้อมูลที่ต้องการสื่อสาร มีขนาดได้ไม่ต่ำกว่า 5 32-บิตเวิร์ด (6 บิตแรกสงวนไว้และกำหนดให้เป็นศูนย์)



รูปที่ 2-4 แสดงแพ็กเก็ตทีซีพี

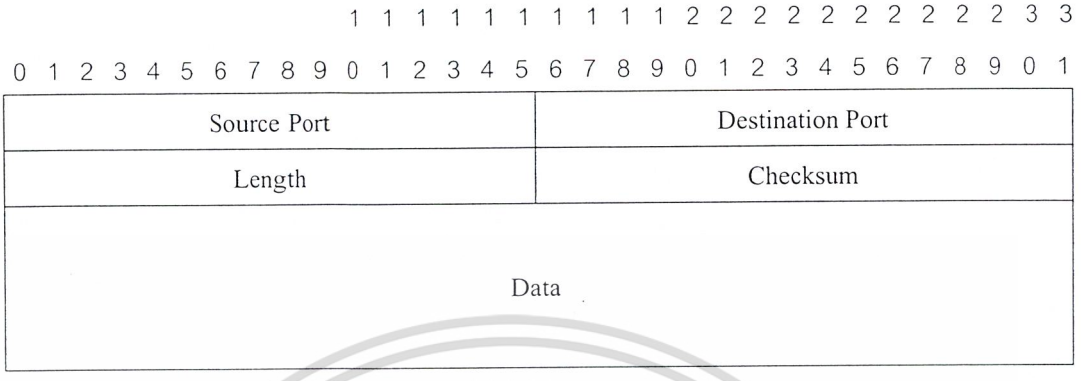
2.1.4 โพรโตคอลยูดีพี (UDP: User Datagram Protocol)

โพรโตคอลยูดีพีเป็นโพรโตคอลในการติดต่อสื่อสารในชั้นทรานสปอร์ต (Transport Layer) การทำงานคล้ายกับทีซีพีมาก คือ จัดการเกี่ยวกับการสื่อสารระหว่างเครื่อง แต่เป็นแบบ Connectionless คือ ทั้งฝ่ายส่งและฝ่ายรับไม่จำเป็นต้องอาศัยการสร้างช่องทางเชื่อมต่อกัน โดยไม่ต้องมีการแจ้งให้ฝ่ายรับข้อมูลเตรียมรับข้อมูลเหมือนโพรโตคอลทีซีพี และไม่มีการส่งสัญญาณตรวจสอบว่าข้อมูลถึงเครื่องปลายทางอย่างถูกต้องครบถ้วนในการส่งข้อมูลแต่ละครั้ง จึงไม่มีการส่งข้อมูลใหม่อีกในกรณีที่เกิดความผิดพลาดของการส่งข้อมูล

<u>ส่วนประกอบของ UDP Frame</u>

1. *Source Port* : เป็นค่าตัวเลข 16 บิต บอกพอร์ตของบริการที่เครื่องต้นทาง
2. *Destination Port* : เป็นค่าตัวเลข 16 บิต บอกพอร์ตของบริการที่เครื่องปลายทาง

3. *Length* : เป็นค่าตัวเลข 16 บิต บอกความยาวของข้อมูล
4. *Checksum* : เป็นค่าตัวเลข 16 บิต ตรวจสอบความถูกต้องของข้อมูลที่ส่ง

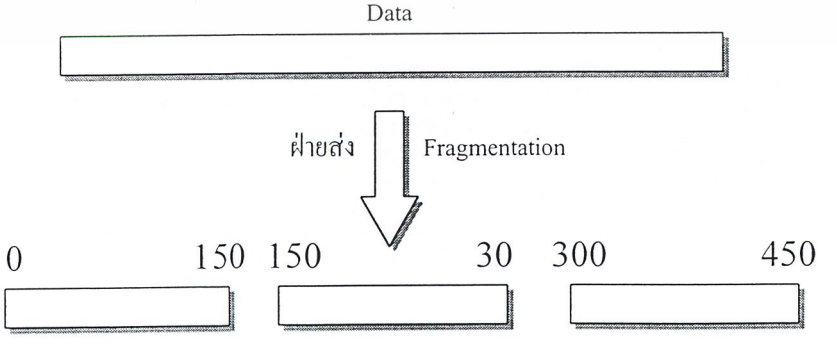


รูปที่ 2-5 แสดงแพ็กเก็ตยูดีพี

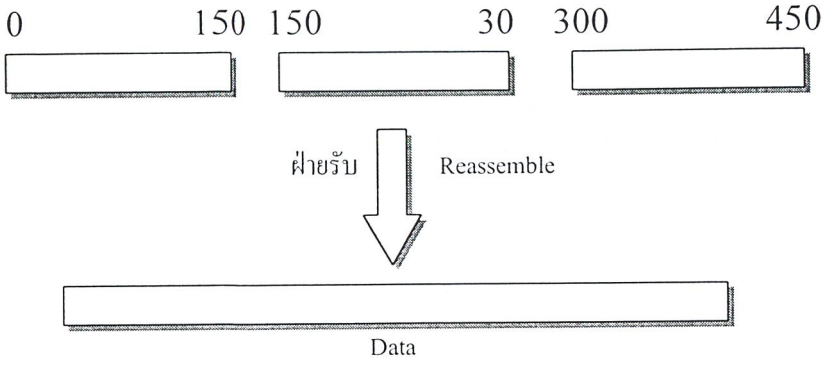
2.1.5 โพรโตคอลไอพี (IP: Internet Protocol)

โพรโตคอลไอพีเป็นโพรโตคอลที่จัดการเกี่ยวกับแอดเดรสของแต่ละแพ็กเก็ต เพื่อให้ส่งแพ็กเก็ตต่างๆ ไปยังเป้าหมายได้ถูกต้อง การทำงานของไอพีเป็นเพียงการส่งข้อมูลไปยังเครื่องเป้าหมายเท่านั้น ไม่มีการส่งสัญญาณขอบริการ หรือสัญญาณให้บริการระหว่างกันเหมือนทีซีพี เรียกว่าการเชื่อมต่อแบบ Connectionless ซึ่งระบบทั้งสองตั้งสมมติฐานว่าการเชื่อมต่อระหว่างกันไม่มีความผิดพลาดเกิดขึ้นแน่

เนื่องจากมาตรฐานในเครือข่ายมีหลากหลาย ขนาดของแพ็กเก็ตในแต่ละมาตรฐานจึงมีความแตกต่างกันออกไป ทำให้การส่งข้อมูลระหว่างอุปกรณ์ในเครือข่ายนั้นอาจมีการแบ่งข้อมูลออกเป็นแพ็กเก็ตย่อยๆ ในระหว่างการส่ง เรียกว่า การทำแฟร็กเมนเตชัน (Fragmentation) เช่น แพ็กเก็ตของ FDDI มีขนาด 4,500 ไบต์ หากเครื่องปลายอยู่ในเครือข่าย Ethernet ซึ่งมีขนาดของแพ็กเก็ตสูงสุดเพียง 1,500 ไบต์ ดังนั้นการส่งแพ็กเก็ตไปยังเครื่องปลายทางจึงต้องมีการแบ่งเป็นแพ็กเก็ตย่อย และเมื่อแพ็กเก็ตย่อยมาถึงเครื่องเป้าหมายก็จะมารวมกันเป็นแพ็กเก็ตเดิมที่มีขนาด 4,500 ไบต์อีกครั้ง เรียกการรวมกันนี้ว่า การรีแอสเซมเบิ้ล (Reassemble) ซึ่งทำให้ได้ข้อมูลเหมือนที่ส่งมาจากเครื่องต้นทาง



รูปที่ 2-6 แสดงการทำแฟร็กเมนเตชัน



รูปที่ 2-7 แสดงการรีแอสเซมเบิ้ล

ส่วนประกอบของแพ็กเก็ตไอพี

1. *version* : เป็นค่าตัวเลข 4 บิต บอกเวอร์ชันของมาตรฐานไอพีที่ใช้ โดยปกติมีค่าเป็น 4 ซึ่งหมายถึง IPv4
2. *Internet Header Length (IHL)* : เป็นตัวบอกความยาวเฮดเดอร์ของไอพี
3. *Type of Service* : เป็นส่วนที่บอกการทำงานของแพ็กเก็ตที่ส่งว่าทำหน้าที่อะไร มีทั้งหมด 8 บิต โดย

   Bit 0-2 : บอกรายละเอียดการทำงานของแพ็กเก็ตนั้นๆ

   111 - Network Control

   110 - Internetwork Control

   101 - CRITIC / ECP

   100 - Flash Override

   011 - Flash

   010 - Immediate

   001 - Priority

   000 - Routine

   Bit 3 : บอกถึงลักษณะของดีเลย์

   0 = Normal Delay - มีดีเลย์ปกติ

   1 = Low Delay - มีดีเลย์ต่ำ

   Bit 4 : บอกถึงประเภทของทรูพุต

   0 = Normal Throughput – มีทรูพุตปกติ

   1= High Throughput – มีทรูพุตสูง

Bit 5 : บอกถึงประเภทของความน่าเชื่อถือ

0 = Normal Reliability - มีความน่าเชื่อถือพอประมาณ

1 = High Reliability - มีความน่าเชื่อถือสูง

Bit 6-7 : กันไว้ใช้ในอนาคต

4. *Total Length* : มีขนาด 16 บิต บอกถึงความยาวในดาต้าแกรมของไอพี
5. *Identification field* : เป็นตัวเลข 16 บิต เป็นค่าประจำตัวของไอพีนั้น โดยโฮสต์ที่ส่งเป็นผู้กำหนด และเพิ่มค่าขึ้นหนึ่งเมื่อมีการส่งดาต้าแกรมของไอพีใหม่ ซึ่งใช้ในการประกอบกลับ
6. *Flag* : เป็นตัวเลข 3 bit บอกลักษณะของแพ็กเก็ตว่ามีการแฟร็กเมนต์หรือไม่

Bit 0 : สงวนไว้ ปกติเป็น 0

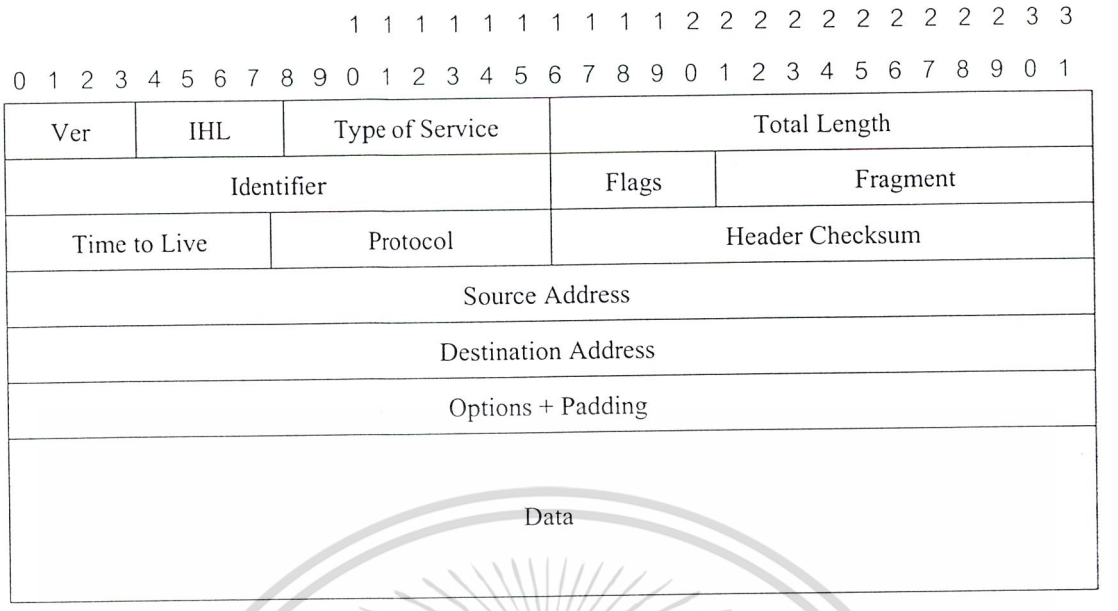
Bit 1 : 0 = บอกว่าแพ็กเก็ตมีการแตกแพ็กเก็ตย่อย

1 = บอกว่าแพ็กเก็ตไม่มีการแตกแพ็กเก็ตย่อย

Bit 2 : 0 = บอกว่าแพ็กเก็ตนั้นเป็นแพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย

1 = บอกว่าแพ็กเก็ตนั้นยังไม่ใช่แพ็กเก็ตสุดท้ายที่ได้จากการแตกแพ็กเก็ตย่อย

7. *Fragment Offset* : เป็นค่าตัวเลข 13 บิต บอกออฟเซตของแฟร็กเมนต์เมื่อเทียบในดาต้าแกรม
8. *Time To Live (TTL)* : เป็นตัวเลข 8 บิต บอกช่วงเวลาของแพ็กเก็ตที่ยังอยู่ในเครือข่ายได้ โดยกำหนดค่าเป็นจำนวนเราท์เตอร์สูงสุดที่ดาต้าแกรมผ่านได้ ซึ่งโดยทั่วไปทีค่าระหว่าง 32 ถึง 64 และลดค่าลงเรื่อยๆ เมื่อผ่านเราเตอร์ เพื่อเป็นการป้องกันแพ็กเก็ตล้นเครือข่าย
9. *Protocol* : เป็นตัวเลข 8 bit บอกถึงโพรโตคอลที่อยู่เหนือขึ้นไป ว่าเป็นโพรโตคอลระดับสูงกว่าประเภทใด
10. *Header Checksum* : เป็นค่าตัวเลข 32 บิต ใช้ตรวจสอบความถูกต้องของเฮดเดอร์
11. *Source Address* : เป็นค่าตัวเลข 32 บิต บอกถึงไอพีแอดเดรสของเครื่องต้นทาง
12. *Destination Address* : เป็นค่าตัวเลข 32 บิต บอกถึงไอพีแอดเดรสของเครื่องปลายทาง



รูปที่ 2-8 แสดงแพ็กเก็ตไอพี

2.2 ความรู้เบื้องต้นความปลอดภัยของระบบเครือข่ายอินเตอร์เน็ต (Internet Security Introduction)

ก่อนอื่น เรามาทำความเข้าใจกับประเภทของความปลอดภัยทั้งหลาย และขอบเขตของการรักษาความปลอดภัย ซึ่งโครงงานนี้ครอบคลุมถึงเสียก่อน ดังนี้

Information security หมายความถึง การรักษาความปลอดภัยทั่วๆ ไปของข้อมูล ป้องกันการขโมย แอบดูข้อมูล สามารถใช้ได้กับทั้งระบบคอมพิวเตอร์ หรือไม่ก็ได้ ซึ่งอาจรวมถึงข้อมูลในแฟ้มหรือกระดาษด้วย

Computer security หมายถึง การรักษาความปลอดภัยให้กับตัวคอมพิวเตอร์ ซึ่งเน้นไปที่เรื่องของข้อมูล เช่น การรักษาป้องกัน พาสเวิร์ด เป็นต้น

Network security หรือ **internet security** หมายถึง การรักษาความปลอดภัยให้กับเครือข่าย ปกป้องข้อมูลระหว่างการส่ง

สำหรับในความหมายที่ 2 และ 3 นั้นมีความคาบเกี่ยวกันอยู่ ยกตัวอย่างเช่น หนึ่งในประเภทของการโจมตีที่แพร่หลายที่สุด ก็คือ ไวรัสคอมพิวเตอร์ (Computer virus) ซึ่งมันจะอยู่ทั้งบนคอมพิวเตอร์ และยังอยู่ได้บนระบบเครือข่าย (internet) ด้วย ดังนั้น จึงมีเนื้อหาบางส่วนที่จำเป็นต้องเกี่ยวข้องกัน แยกกันไม่ออกโดยสิ้นเชิง

สำหรับโครงงานของเรา จะตั้งอยู่บนขอบเขตของ Network security (internet security) ซึ่งจะมีขอบเขตไปยังระบบเครือข่ายที่เชื่อมต่ออยู่บนเครือข่ายอินเตอร์เน็ต(Internet) จึงมาเป็นคำว่า **Internet Security** ในที่สุด

เนื่องจากการเพิ่มขึ้นอย่างมากมายของการบุกรุกเครือข่าย ผู้ใช้คอมพิวเตอร์ส่วนใหญ่จึงเริ่มหันมาสนใจระบบรักษาความปลอดภัยบนคอมพิวเตอร์กันมากขึ้น แต่อย่างไรก็ตาม ผู้ใช้ส่วนใหญ่ยังไม่เข้าใจระบบรักษาความปลอดภัยบนคอมพิวเตอร์ว่าสำคัญกับพวกเขาเพียงไร อาจเพราะว่าข่าวการบุกรุก

ต่างๆ เช่น หนอนคอมพิวเตอร์ (Worm) การจารกรรมบนอินเตอร์เน็ต ต่างๆ เป็นต้น นั้น ไม่ได้บอกถึงรายละเอียดของการบุกรุกต่างๆ จึงไม่สามารถสร้างความเข้าใจให้กับผู้ใช้ได้

2.2.1 เป้าหมายของการรักษาความปลอดภัย

บริการทางด้านความปลอดภัย (Security service) ทั้งหลายทั้งปวง เกิดขึ้นมา เพื่อจุดมุ่งหมายทั้ง6ข้อนี้

- **ความลับและความเป็นส่วนตัว (Confidentiality)**

  คือ ความสามารถในการปกป้อง รักษาความลับ และความเป็นส่วนตัว เช่น การเข้ารหัส (Encryption) ข้อความก่อนส่งออกไป

- **การพิสูจน์ตน (Authentication)**

  คือ การพิสูจน์ความเป็นตัวตน ของคอมพิวเตอร์ บุคคล หรือสิ่งของต่างๆ การยืนยันความเป็นตัวจริง

- **ความถูกต้อง (Integrity)**

  คือ การยืนยันความถูกต้อง รักษาความถูกต้องของข้อมูลว่า เช่นยืนยันได้ว่าไม่ได้มีการเปลี่ยนแปลงใดๆ ก่อนถึงมือผู้รับ

- **ความไม่สามารถปฏิเสธการกระทำได้ (Nonrepudiation)**

  คือ การที่ระบบสามารถยืนยันการกระทำต่างๆ ได้ว่า เกิดขึ้นจริงๆ หรือไม่ได้เกิดขึ้น เช่น เมื่อข้อความถึงมือผู้รับ (receiver)แล้ว ผู้ส่ง (sender) สามารถพิสูจน์ได้ว่าข้อความนั้นถูกรับโดยผู้รับจริงๆ ที่ผู้ส่งต้องการส่งให้

- **การควบคุมสิทธิการใช้งาน (Access control)**

  คือ การควบคุมสิทธิในการเข้าใช้ทรัพยากรต่างๆ ในส่วนที่พึงจะมีได้

- **ความสามารถคงการใช้งานอยู่ได้ (Availability)**

  คือ การทำให้ระบบสามารถให้บริการได้ต่อไป แม้ว่าจะถูกโจมตี

2.2.2 ประเภทของการโจมตี (Type of Attacks)

ประเภทของการคุกคาม (Type of Threat)	คำอธิบาย (Description)	รูปแบบการคุกคาม (Form of Threat)
การเปลี่ยนแปลงข้อมูลระหว่างส่ง	การเปลี่ยนแปลงของทรานส์แอ็กชัน(Transaction)ข้ามระบบเครือข่าย	หาจุดอ่อนของโพรโตคอลการสื่อสาร
Denial of Service	การโจมตีที่ทำให้เซิร์ฟเวอร์หรือระบบเครือข่ายแย่ลง	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยของโพรโตคอลการสื่อสาร และระบบปฏิบัติการ

การขโมยข้อมูล	การโจมตีที่ผลคือถูกขโมยข้อมูล	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยของตัวแอพพลิเคชัน ระบบปฏิบัติการ และเครื่องโฮสต์
การใช้ทรัพยากรโดยไม่ได้รับการยินยอม	ผู้โจมตีสามารถเข้าใช้บริการต่างๆ เช่น เครื่องคอมพิวเตอร์ได้	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยของตัวแอพพลิเคชัน ระบบปฏิบัติการ และเครื่องโฮสต์
การเข้าไปยุ่งกับข้อมูล(data tampering)	การแปลงเปลี่ยนของหน้าสถานะต่างๆเช่น ข้อมูลสุขภาพ, ทรานสคริปต์(transcripts) ของนักเรียน	หาจุดอ่อนเกี่ยวกับระบบความปลอดภัยบนเซิร์ฟเวอร์ เพื่อดัดแปลงหน้าเว็บเพจ หรือข้อมูลในฐานข้อมูล
การSpoof(Spoofing)	การปลอมแปลงหมายเลขไอพี เพื่อมีสิทธิในการเข้าใช้ทรัพยากร หรือการปลอมตัวเป็นผู้อื่นในการอีเมล์	หาจุดอ่อนของโพรโตคอลการสื่อสารที่จะยอมให้ผู้โจมตีปลอมตัวเป็นคนอื่นได้
การSniff(Sniffing)	การจับตาดูทราฟฟิก (traffic) ของระบบเครือข่าย เพื่อดูข้อมูลหรือรหัสผ่าน	ทราฟฟิกของระบบเครือข่ายถูกส่งเป็นข้อความต้นฉบับเลยอ่านได้ชัดเจน รหัสผ่านและข้อมูลต่างๆ สามารถถูกนำไปใช้ได้
ไวรัส (Virus)	โปรแกรมที่ประสงค์ร้ายอาจประกอบด้วยคอมโพเนนท์ที่ไม่อันตราย หรืออันตรายก็ได้	ความสะดวกของโปรแกรมที่ดาวน์โหลด(download) มา

ตารางที่ 2-2 แสดงประเภทของการโจมตี (Type of Attack)

หรืออาจจำแนกตามจุดประสงค์ของการคุกคาม ได้ดังนี้

จุดประสงค์การคุกคาม (Threat Purpose)	**การคุกคาม (Threats)**	**ผลกระทบ (Consequence)**	**มาตรการรับมือ (Countermeasures)**
ความถูกต้อง (Integrity)	- การเปลี่ยนแปลงข้อมูล - ม้าโทรจัน(Trojan horse) - การแปลงข้อมูลระหว่างส่ง	- สูญเสียข้อมูล - เป็นช่องโหว่(Vulnerability) ต่อทุกการคุกคาม	Cryptographic Checksum
ความลับและความเป็นส่วนตัว (Confidentiality)	- การแอบดูข้อมูลบนเน็ต - ขโมยข้อมูล	- ข้อมูลสูญหาย - สูญเสียความเป็นส่วนตัว	การเข้ารหัส (Encryption), Web proxies
Denial Of Service	- การทำลายThreads - การฟลัดดิ้ง(Flooding)	- ภาวะแตกแยก (Disruptive)	ยากที่จะป้องกัน

	- การทำให้หน่วยความจำเต็ม - โจมตีดีดีเอ็นเอสเซิร์ฟเวอร์(DNS Server)เพื่อปล่อยให้เครื่องโดดเดี่ยว	- ทำให้ผู้ใช้ทำงานไม่เสร็จ - ทำให้รำคาญ	
การพิสูจน์ตน (Authentication)	- การปลอมตัวเป็นผู้ใช้ที่มีสิทธิ์ - การปลอมแปลงเอกสารข้อมูล ปลอมลายเซ็น	- เชื่อว่าข้อมูลที่ผิดนั้นถูกต้อง - การแสดงอย่างผิดๆ ของผู้ใช้	Cryptographic Technique

ตารางที่ 2-3 แสดงประเภทของการโจมตีจำแนกตามจุดประสงค์ของการคุกคาม

2.2.3 ความบกพร่อง (Vulnerability)

คือเป็นจุดอ่อน ช่องโหว่ รูรั่ว ที่สามารถนำไปสู่การบุกรุกหรือคุกคามคอมพิวเตอร์ได้ แน่นอนว่าคอมพิวเตอร์ทุกเครื่องนั้นย่อมมีความบกพร่องที่จะนำไปสู่การบุกรุกได้ แต่นโยบายการรักษาความปลอดภัย (Security Policies) และผลิตภัณฑ์ต่างๆ ก็สามารถช่วยลดความบกพร่องต่างๆ ของระบบได้ หรืออีกนัยหนึ่งคือสามารถทำให้ผู้บุกรุกต้องใช้ความพยายามมากขึ้นในการบุกรุกเข้ามาในระบบนั้นๆ นั่นหมายถึงว่า ไม่มีระบบรักษาความปลอดภัยที่สมบูรณ์ที่สุด ความบกพร่องทั่วๆ ไปของระบบคอมพิวเตอร์อาจจัดได้ดังนี้

- **ความบกพร่องทางกายภาพ (Physical Vulnerabilities)**

  ได้แก่ การที่ตึก หรือห้องที่มีคอมพิวเตอร์อยู่ภายในนั้น สามารถถูกบุกรุกเข้าไปได้ โดยวิธีเดียวกับที่ขโมยบุกเข้าไปปล้นบ้านได้ วิธีการป้องกัน ได้แก่การใช้ระบบรักษาความปลอดภัยของอาคารเช่น กุญแจล็อกห้อง พนักงานรักษาความปลอดภัย สัญญาณเตือนภัย

- **ความบกพร่องจากธรรมชาติ (Natural Vulnerabilities)**

  ได้แก่ ภัยธรรมชาติต่างๆ เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว ตึกถล่ม ฯลฯ ภัยเหล่านี้สามารถทำให้ข้อมูลในคอมพิวเตอร์เสียหายได้ อีกทั้งสภาพแวดล้อมต่างๆ เช่น ฝุ่น ความชื้น อุณหภูมิ ก็อาจทำความเสียหายให้กับคอมพิวเตอร์ได้

- **ความบกพร่องของซอฟต์แวร์และฮาร์ดแวร์ (Hardware and Software Vulnerabilities)**

  ได้แก่ความผิดพลาดในการทำงานของฮาร์ดแวร์ เช่นการจัดการหน่วยความจำผิดพลาดในการที่จะควบคุมการเข้าถึงหน่วยความจำของระบบที่ไม่อนุญาตให้ผู้ใช้ปกติเข้าถึงได้ ทำให้ผู้ใช้ปกติสามารถเข้าไปถึงหน่วยความจำของระบบนั้นๆ ได้

- **ความบกพร่องของสื่อ (Media Vulnerabilities)**

  ได้แก่ แผ่นดิสก์ เทป และเอกสารต่างๆ สามารถถูกขโมยได้ อีกทั้งยังอาจเสื่อมสภาพตามกาลเวลาทำให้ข้อมูลเสียหายได้ด้วย

- **ความบกพร่องของการส่งผ่านข้อมูล (Communication Vulnerabilities)**

  ได้แก่ การที่ข้อมูลที่ส่งผ่านกันนั้น สามารถถูกดักจับ หรือถูกขัดขวางได้ เช่นบนเครือข่ายคอมพิวเตอร์ข้อมูลที่ส่งผ่านไปยังสายสัญญาณนั้นอาจถูกขัดขวางหรือดังข้อมูลนั้นๆ ได้

- **ความบกพร่องที่เกี่ยวกับมนุษย์ (Human Vulnerabilities)**

  ได้แก่ การที่ผู้ควบคุมระบบนั้นๆ ไม่มีความรู้ความสามารถเพียงพอที่จะควบคุมระบบนั้นๆ ได้ หรือมีความหละหลวมในระบบรักษาความปลอดภัย เช่น ติดสินบนเพื่อใช้รหัสผ่าน การติดสินบนเพื่อเข้าใช้ห้องคอมพิวเตอร์ สิ่งเหล่านี้เป็นความบกพร่องที่เป็นอันตรายอย่างยิ่ง

2.2.4 ช่องโหว่ภายในระบบ (Internal Vulnerabilities)

เมื่อผู้บุกรุก (Intruder) ต้องการบุกรุกระบบ สามารถทำได้โดยหาช่องโหว่ภายในระบบ แล้วพยามยามเข้าสู่ระบบทางช่องโหว่นั้นๆ ช่องโหว่ของระบบมีดังนี้

- **ข้อบกพร่องของโปรแกรม หรือระบบปฏิบัติการ**

เกิดจากบัก(Bug) ที่อยู่ในโปรแกรมซึ่งทำงานในเครื่องเซิร์ฟเวอร์ , เครื่องไคลเอ็นต์, บนระบบปฏิบัติการ, หรือ สแต็กของเครือข่าย ช่องโหว่ของระบบซึ่งพบที่โปรแกรมจำแนกเป็นประเภทต่างๆ ดังนี้

- บัฟเฟอร์โอเวอร์โฟลว์(Buffer Overflow) ช่องโหว่ที่พบในปัจจุบันเกิดจากบัฟเฟอร์โอเวอร์โฟลว์แทบทั้งสิ้น การเกิดบัฟเฟอร์โอเวอร์โฟลว์ เช่น สมมุติว่าโปรแกรมเมอร์เขียนโปรแกรมรับอินพุตเป็นชื่อผู้ใช้ และจองพื้นที่256 ตัวอักษรสำหรับเก็บอินพุตนี้ โปรแกรมเมอร์คาดไว้ว่าไม่มีผู้ใช้คนใดที่มีชื่อยาวกว่านี้แน่ ส่นในมุมมองของผู้บุกรุกนั้นจะพิจารณาว่าหากใส่อินพุตที่ยาวกว่า 256 ตัวอักษรแล้ว ตัวอักษรที่เกินมาจะถูกวางในส่วนใดในหน่วยความจำ ผู้บุกรุกจึงพยายามส่งตัวอักษรมากกว่า 256 ตัวอักษรติดกัน พร้อมกับแทรกโค้ดที่สามารถทำงานได้ไว้ในอินพุตนั้นด้วย ถ้าโปรแกรมเกิดแครช (Crash) ขึ้น ผู้บุกรุกสามารถนำมาใช้เป็นจุดที่เข้าไปบุกรุกระบบได้ ซึ่งผู้บุกรุกสามารถหาช่องโหว่นี้ได้หลายทาง เช่นจากซอร์สโค้ดของเซอร์วิสต่างๆ ที่มีแจกในอินเตอร์เน็ต ผู้บุกรุกเพียงแค่ค้นหาโปรแกรมตัวที่มีช่องโหว่นี้ จากนั้นก็ศึกษาซอร์สโค้ดแอสเซมบลีในการค้นหาช่องโหว่และทดลองใส่ข้อมูลสุ่มเพื่อหาข้อบกพร่อง มีข้อสังเกตว่าปัญหานี้มักเกิดกับโปรแกรมที่เขียนด้วยซี (C) หรือซี พลัส พลัส (C++) และพบได้น้อยมากในโปรแกรมที่เขียนด้วยจาวา (JAVA) เนื่องจากจาวาไม่ยอมให้โปรแกรมเมอร์เข้าถึงหน่วยความจำโดยตรง
- การใช้โปรแกรมหลายโปรแกรมทำงานร่วมกันทำให้เกิดสิ่งที่ไม่คาดคิดขึ้นในการเขียนโปรแกรม (Unexpected combinations) โปรแกรมเมอร์เขียนโดยใช้โค้ดหลายๆ ระดับสร้างโปรแกรมขึ้นมา โดยมีระดับระบบปฏิบัติการเป็นระดับล่างสุด ตัวอย่างช่องโหว่แบบนี้ที่สามารถเห็นได้คือ โปรแกรมที่เขียนด้วยภาษาเพิร์ล(Perl) ซึ่งสามารถส่งอินพุตไปยังโปรแกรมอื่นๆได้ เช่น

  " | mail </etc/passwd" เมื่อโปรแกรมทำงานที่คำสั่งนี้ ทำให้ระบบส่งไฟล์ /etc/passwd ไปให้ผู้บุกรุกผ่านทางอีเมล์

- อินพุตที่ไม่สามารถควบคุมได้ (Unhadled input) โปรแกรมเมอร์โดยส่วนใหญ่พิจารณาถึงเฉพาะอินพุตที่ใส่อย่างถูกต้องเท่านั้น โดยไม่ได้คิดถึงการใส่อินพุตที่เป็นไปไม่ได้ด้วย นี่เป็นช่องโหว่อีกทางหนึ่งที่สามารถใช้ในการบุกรุกระบบได้
- สภาพที่มีการแข่งขัน (Race condition) ระบบปัจจุบันเป็นระบบแบบมัลติทาร์กกิ้ง (Multitasking) และ มัลติเธรด (Multithread) คือในขณะใดๆ สามารถมีโปรแกรมมากกว่าหนึ่งโปรแกรมทำงานอยู่ได้ ซึ่งเป็นอันตรายต่อระบบถ้าสองโปรแกรมกำลังเข้าถึงข้อมูลเดียวกันในเวลาเดียวกัน กรณีนี้อาจทำให้ข้อมูลของโปรแกรมหนึ่งไม่สามารถเขียนได้อย่างสมบูรณ์ เหตุการณ์นี้เกิดขึ้นน้อยมาก ผู้บุกรุกต้องใช้เวลานานสำหรับการบุกรุกด้วยช่องทางนี้

■ **ข้อบกพร่องของการกำหนดค่าของระบบ (Misconfiguration)**

ข้อบกพร่องจากการกำหนดค่าของระบบเกิดได้จากหลายสาเหตุดังนี้

- การตั้งค่าโดยใช้ค่าเดิมที่ระบบกำหนดมาให้ (Default Configure) โปรแกรมส่วนใหญ่ที่ลูกค้าซื้อมาได้กำหนดค่าการทำงานต่างๆ มาแล้ว และเป็นค่าที่ทำให้โปรแกรมใช้งานได้ง่าย ซึ่งการใช้งานง่ายซึ่งง่ายต่อการบุกรุกระบบด้วย
- เกิดจากผู้ดูแลระบบเกียจคร้าน ไม่ได้ใส่รหัสผ่านของรูต (root) หรือผู้ใช้ใดๆ ในระบบ ทำให้เป็นช่องโหว่ที่ผู้บุกรุกใช้บุกรุกเข้าระบบโดยง่าย
- โปรแกรมอาจมีช่องโหว่จากเซอร์วิสที่ทำงานอยู่ในระบบ ผู้ดูแลระบบควรปิดเซอร์วิสของระบบทุกตัวที่ไม่ได้ใช้งานเพื่อหลีกเลี่ยงช่องโหว่ที่อาจเกิดขึ้นได้ในภายหลัง ในส่วนนี้มีโปรแกรมสำหรับตรวจสอบความปลอดภัย ซึ่งสามารถตรวจสอบและแจ้งเตือนผู้ดูแลระบบให้ไปแก้ไขได้
- เครื่องที่เชื่อถือกัน (Trust relationships) ผู้บุกรุกอาศัยช่องโหว่จากเครื่องที่ติดต่อกันแบบทรัสต์ โดยสามารถเข้าไปยังเครื่องอื่นๆ ที่ยกเว้นการตรวจสอบสิทธิของกันและกันได้ ตัวอย่างการบุกรุกทางช่องโหว่ตรงนี้คือ การบุกรุกโดยใช้ .rhost

■ **ช่องโหว่ของรหัสผ่าน**

ส่วนใหญ่เกิดจากผู้ใช้ส่วนใหญ่จะใช้ชื่อที่ผู้ใช้คุ้นเคย เช่นชื่อตัวเอง ชื่อเพื่อน เป็นรหัสผ่าน (Password) มีความหละหลวมในการตั้งรหัสผ่าน ทำให้ผู้บุกรุกสามารถเดารหัสผ่านได้ง่าย ผู้บุกรุกอาจเดารหัสผ่านได้จากคำในพจนานุกรม หรืออาจใช้วิธีการบรูทฟอร์ซ (Brute force attack) เป็นอีกวิธีที่ผู้บุกรุกใช้ในการเดารหัสผ่าน ผู้บุกรุกเดารหัสที่เป็นไปด้าที่เกิดขึ้นจากการสร้างรหัสผ่าน เช่นสมมติว่ารหัสผ่านที่เป็นไปได้ของระบบเป็นตัวอักษรภาษาอังกฤษตัวพิมพ์เล็กจำนวน 4 ตัว ผู้บุกรุกก็พยายามล็อกอินเข้าสู่ระบบโดยใช้รหัสผ่านที่เป็นไปได้ทั้งหมดจากการผสมคำ ในกรณีนี้ รหัสผ่านที่เป็นไปได้คือ 26x26x26x26 ตัว ซึ่งถ้าตั้งรหัสผ่านมีการผสมกันระหว่าง ตัวอักษรทั้งเล็กและใหญ่ ตัวเลขและเครื่องหมายต่างๆ จะทำให้คำที่เป็นไปได้ทั้งหมดมีจำนวนมากขึ้น ดังนั้นหากผู้บุกรุกใช้วิธีนี้ในการเดารหัสผ่านก็จะใช้เวลานานยิ่งขึ้น

นอกจากนี้ผู้บุกรุกสามารถได้รหัสผ่านโดยวิธีต่อไปนี้

- การดักจับข้อมูลที่ไม่ได้เข้ารหัส (clear text sniffing) เซอร์วิสที่รันบนโพรโตคอล TCP/IP เช่น Telnet มีการส่งรหัสผ่านที่ไม่เข้าหัส ซึ่งอาจมีการดักจับโดยใช้ตัววิเคราะห์โพรโตคอล(protocol analyzer) ระหว่างทางของการส่งแพ็กเก็ตผ่านไปในเครือข่าย ผู้บุกรุกสามารถเอารหัสผ่านที่ได้ไปล็อกอินเข้าระบบในภายหลัง
- การดักจับข้อมูลเข้ารหัส (Encrypt sniffing) ถึงแม้ว่ารหัสผ่านถูกเข้ารหัสไว้ ผู้บุกรุกสามารถทราบรหัสผ่านเหล่านั้นได้โดยนำรหัสผ่านจากคำในพจนานุกรม หรือจากการเดาคำไปเข้ารหัสเพื่อมาเปรียบเทียบกับรหัสผ่านที่ถูกเข้ารหัสไว้ (Brute force) หากผู้บุกรุกสามารถทราบรหัสผ่านเข้าสู่ระบบแล้ว ผู้นั้นก็เหมือนกับผู้ใช้ทั่วๆ ไป โดยที่ไม่อาจทราบได้ว่า ผู้ที่ล็อกอินเข้ามานั้นเป็นผู้ที่มีสิทธิ์คนนั้นจริงหรือไม่
- การบุกรุกโดยการส่งข้อมูลซ้ำ (Replay Attack) ผู้บุกรุกไม่จำเป็นต้องถอดรหัสรหัสผ่านเพื่อแต่ดักจับแพ็กเก็ตนั้น และสร้างโปรแกรมที่สามารถส่งแพ็กเก็ตของรหัสผ่านที่เข้ารหัสของผู้ที่มีสิทธิ์ในการใช้งานที่ดักจับได้ไว้ก่อนหน้านั้น แล้วส่งแพ็กเก็ตนั้นอีกครั้งไปยังเซิร์ฟเวอร์ขณะที่กำลังตรวจสอบสิทธิ์ ทำให้การติดต่อนั้นสำเร็จด้วยโดยใช้สิทธิ์ของผู้ใช้คนอื่น
- การขโมยไฟล์รหัสผ่าน(Password file stealing) ในระบบของเครื่องเซิร์ฟเวอร์ทั่วๆ ไปจะเก็บฐานข้อมูลรหัสผ่านของผู้ใช้อยู่ในไฟล์ ซึ่งในระบบปฏิบัติการลีนุกซ์อยู่ที่ไฟล์ /etc/password หรือสำหรับระบบปฏิบัติการวินโดว์เอ็นที (WindowNT)เก็บไว้ในไฟล์ชื่อ SAM เมื่อผู้บุกรุกกระทำการใดๆ ก็ตามทำให้ได้ไฟล์รหัสผ่านเหล่านี้แล้ว ผู้บุกรุกสามารถนำไฟล์นี้ไปถอดรหัสโดยให้โปรแกรมถอดรหัส(Crack) หากรหัสผ่านที่ใช้เข้าสู่ระบบ
- การเฝ้าสังเกต (Observation) ปัญหาพื้นฐานของระบบการรักษาความปลอดภัย คือการขโมยใช้รหัสผ่าน หากผู้ใช้ในระบบมีการกำหนดรหัสผ่านของตนให้เป็นรหัสผ่านที่ยากต่อการเดา ปัญหาที่จะเกิดกับผู้ใช้นั้นคือ ผู้ใช้ต้องจำรหัสผ่านที่ตัวเองตั้งขึ้นมาด้วย ผู้ใช้บางคนอาจเผอเรอเขียนรหัสผ่านไว้บนกระดาษแล้วทิ้งไว้ ทำให้ผู้บุกรุกได้เอกสารที่มีรหัสผ่านนั้นไปได้ อีกวิธีหนึ่งคือถามรหัสผ่านผู้ที่รู้โดยใช้วิธีหลอกถามรหัสผ่านจากผู้ที่มีสิทธิ์จริงๆ โดยอ้างเหตุผลต่างๆ

2.2.5 ช่องทางพื้นฐานสำหรับการบุกรุกระบบคอมพิวเตอร์

สคริปต์ซีจีไอ(CGI Script)

เป็นที่รู้จักกันดีว่าการใช้งานสคริปต์ซีจีไอไม่ปลอดภัย เนื่องจากผู้บุกรุกสามารถสอดแทรกโปรแกรมแปลกปลอมผ่านเข้าไปกับฟิลด์ที่รับอินพุตให้ทำงานจากเชลล์ได้ ซึ่งโปรแกรมแปลกปลอมนั้นสามารถซ่อนไว้โดยการกำหนดตัวแปรแทนได้ ช่องโหว่ที่เป็นที่รู้จักกันดีตัวหนึ่งคือ phf ซึ่งเป็นไลบรารีที่มากับ httpd ของ NCSA

การบุกรุกผ่านทาง เว็บเซิร์ฟเวอร์

เว็บเซิร์ฟเวอร์หลายตัวที่สามารถเขียนตัวเองได้ เช่น IIS มีจุดบกพร่องในการระบุชื่อของไฟล์ สามารถเรียกได้โดยใช้ "../"(เป็นการย้อนกลับไปในไดเรกทอรีนอกหนึ่งชั้น) ทำให้สามารถเข้าไปเรียกใช้ได้ทุกไดเรกทอรีในระบบไฟล์ ช่องทางการบุกรุกอื่นๆ เช่นใช้ บัฟเฟอร์โอเวอร์โฟลว์

การบุกรุกผ่านทางโดเมนเนมเซิร์ฟเวอร์ (DNS)

ช่องโหว่เกิดจากโดเมนเนมเซิร์ฟเวอร์ (Domain Name Server) มีการทำงานแบบรีเคอร์ซีฟ (Recursive) โดยส่งคำถามไปยังโดเมนเนมเซิร์ฟเวอร์ที่อยู่ในลำดับขั้นที่สูงขึ้นไป ผู้บุกรุกอาจส่งคำร้องขอเข้าไปยังโดเมนเนมเซิร์ฟเวอร์ตัวแรก ซึ่งโดเมนเนมเซิร์ฟเวอร์ตัวนั้นจะส่งคำถามขึ้นไปยังโดเมนเนมเซิร์ฟเวอร์ในลำดับสูงขึ้นถัดไป ผู้บุกรุกสามารถปลอมที่อยู่ทางอินเตอร์เน็ตให้เป็นโดเมนเนมเซิร์ฟเวอร์ที่ตอบสนองตัวแรก และส่งคำตอบผิดๆ กลับมา ทำให้โปรแกรมที่เป็นผู้ถามในลำดับแรกได้รับคำตอบที่ผิดๆ ไป ซึ่งอาจเกิดการติดต่อไปยังเครื่องที่ผู้บุกรุกจัดเตรียมไว้ก่อนแล้วได้

Remote Procedure Call (RPC)

RPC อนุญาตให้สามารถรันโปรแกรมบนเครื่องคอมพิวเตอร์เครื่องอื่นได้ เป็นอันตรายอย่างยิ่งเมื่อผู้บุกรุกเข้ามารันโปรแกรมที่เครื่องเป้าหมาย เช่น ลงโปรแกรม Back door เอาไว้เพื่อเป็นช่องทางในการเข้าไปยังเครื่องเป้าหมายอีกครั้ง ซึ่ง RPC ในเวอร์ชันเก่าๆ จะมีการกำหนดสิทธิ์เป็น full control

การบุกรุกผ่านโพรโตคอล SMTP (Sendmail)

Sendmail เป็นโปรแกรมที่ใช้กันอย่างแพร่หลาย และซับซ้อนโปรแกรมหนึ่ง ซึ่งมีข้อบกพร่องอยู่มาก ในประวัติศาสตร์มีผู้บุกรุกพบบักที่เกิดจากการใช้คำสั่ง DEBUG หรือฟีเจอร์ WIZ ที่ซ่อนไว้ เป็นตัวช่วยเจาะระบบผ่านทาง SMTP

Sadmind และ mountd

Sadmind ถูกใช้งานอยู่ในระบบ SUN Solaris อนุญาตให้ผู้ดูแลระบบสามารถทำการควบคุมเครื่องเซิร์ฟเวอร์จากระยะไกลได้ส่วน mountd มีการอนุญาตให้มีการแชร์ไฟล์ระหว่างเครือข่าย ซึ่งเป็นช่องทางให้ผู้บุกรุกสามารถลงโปรแกรม เช่น DDOS (Distributed Denial Of Service) เพื่อโจมตีเครื่องเป้าหมายเครื่องอื่นได้

การเปิดแชร์ไฟล์

เครื่องคอมพิวเตอร์ที่มีการเปิดแชร์ไฟล์เอาไว้ เช่นใน Network neighborhood (Windows), Appleshare (Macintoch) และ NFS(Unix) อาจเป็นช่องทางให้ผู้บุกรุกเข้าไปเอาข้อมูลที่สำคัญออกมา เช่น อีเมล์ เอกสารสำคัญที่เก็บเอาไว้ในเครื่องคอมพิวเตอร์หรือได้ Account และรหัสผ่านสำหรับล็อกอินไปยังเซิร์ฟเวอร์อื่นได้

Account ที่ไม่มีรหัสผ่าน หรือรหัสผ่านที่ง่ายต่อการเดา

เมื่อผู้บุกรุกทราบว่ามี Username นั้นอยู่จริงๆ ภายในระบบ จะทำการเชื่อมต่อไปยังเครื่องคอมพิวเตอร์ หรือเซิร์ฟเวอร์เป้าหมายโดยทำการล็อกอินด้วย Usernameนั้น และทำการเดารหัสผ่าน หรือในบางครั้ง ระบบจะไม่มีการถามรหัสผ่าน สามารถเข้าไปในระบบได้เลย นับว่าเป็นอันตรายอย่างยิ่ง

IMAP และ POP

เป็นโพรโตคอลที่อนุญาตให้ผู้ใช้งานไม่ว่าจะอยู่ที่ไหนก็ตาม สามารถเข้ามาอ่านอีเมล์จากเมล์เซิร์ฟเวอร์ได้ เป็นช่องทางให้ผู้บุกรุกสามารถผ่านเข้าไปถึงเมล์เซิร์ฟเวอร์ในระบบ โดยไม่ถูกกันจากไฟร์วอล

Simple Network Management Protocol (SNMP)

อุปกรณ์จำพวกเราเตอร์, สวิตช์, ฮับ หรืออุปกรณ์ที่เปิดให้มีควบคุม และบริหารในเครือข่ายระยะใกล้ และไกลได้ มักจะมีการตั้งค่ารหัสผ่านของผู้ดูแลระบบ เป็นค่าเดิมจากโรงงานที่ผลิต นับเป็นช่องทางให้ผู้บุกรุกเข้ามาควบคุมระบบเครือข่ายขององค์กรได้

2.2.6 การสำรวจระบบ และรวบรวมข้อมูล เพื่อการโจมตีของผู้บุกรุก

- **วิธีการที่ผู้บุกรุกใช้สำรวจระบบ และรวบรวมข้อมูล**

Ping sweeps

การส่งคำสั่ง ping ไปยังเครื่องแบบสุ่ม เพื่อค้นหาว่ามีเครื่องใดเปิดให้บริการอยู่ ค้นหาตำแหน่โฮสต์ที่ต้องการและตรวจสอบการเข้าถึงได้ การกระทำในทำนองนี้อาจใช้โพรโตคอลอื่นๆ เช่น **SNMP sweep** สามารถนำมาใช้เพื่อตรวจสอบดูตารางการจัดเส้นทาง (routing table)ของเราเตอร์ที่ไม่รักษาความปลอดภัยเพื่อเรียนรู้รายละเอียดเกี่ยวกับโทโปโลยี(Topology) ของเครือข่ายขององค์กรเป้าหมาย

TCP scan

การเข้าไปตรวจดูพอร์ตทีซีพีว่ามีช่องทางใดที่เปิดให้บริการอยู่ และเป็นช่องที่ผู้บุรุกสามารถใช้เจาะระบบเข้าไปได้ รูปแบบในการสแกนพอร์ตต่างๆ เป็นไปได้ทั้งการสแกนพอร์ตแบบต่อเนื่อง (เรียงตามหมายเลขพอร์ตที่เป็นไปได้) แบบสุ่ม และแบบกำหนดหมายเลขพอร์ตที่ต้องการสแกนไว้ล่วงหน้า

OS identification

กระทำโดยการส่งแพ็กเก็ตไอซีเอ็มพี (ICMP) หรือทีซีพี(TCP) ไปยังเครื่องเป้าหมาย ทำให้ผู้บุกรุกทราบชนิด และเวอร์ชันของระบบปฏิบัติการและชนิดของเครื่อง

TraceRoute

โปรแกรม TraceRoute สามารถเปิดเผยหมายเลขเครือข่ายและเราเตอร์ในเส้นทางไปสู่โฮสต์ที่ระบุ

Finger

โพรโตคอล Finger สามารถเปิดเผยข้อมูลในรายละเอียดเกี่ยวกับผู้ใช้ (ชื่อล็อกอิน หมายเลขโทรศัพท์ เวลาที่ล็อกอินครั้งสุดท้าย เป็นต้น) ของโฮสต์ที่ระบุได้

DNS Server

เซิร์ฟเวอร์ดีเอ็นเอสสามารถเข้าถึงรายการไอพีแอดเดรสของโฮสต์และชื่อโฮสต์ที่ตรงกันได้

Whois

โพรโตคอล Whois เป็นบริการข้อมูลชนิดหนึ่งที่สามารถให้ข้อมูลเกี่ยวกับโดเมน DNSทั้งหมดและผู้ดูแลระบบที่รับผิดชอบแต่ละโดเมน อย่างไรก็ตาม ข้อมูลนี้มักจะล้าสมัย

2.2.7 การสำรวจจุดอ่อนในการรักษาความปลอดภัยของระบบเครือข่าย

หลังจากรวบรวมข้อมูลเกี่ยวกับเครือข่ายขององค์กรเป้าหมายแล้ว ผู้บุกรุกจะพยายามสำรวจจุดอ่อนในการรักษาความปลอดภัยของแต่ละโฮสต์ มีเครื่องมือจำนวนมากที่ผู้บุกรุกสามารถใช้เพื่อตรวจโฮสต์แต่ละตัวบนเครือข่ายโดยอัตโนมัติ ตัวอย่างเช่น

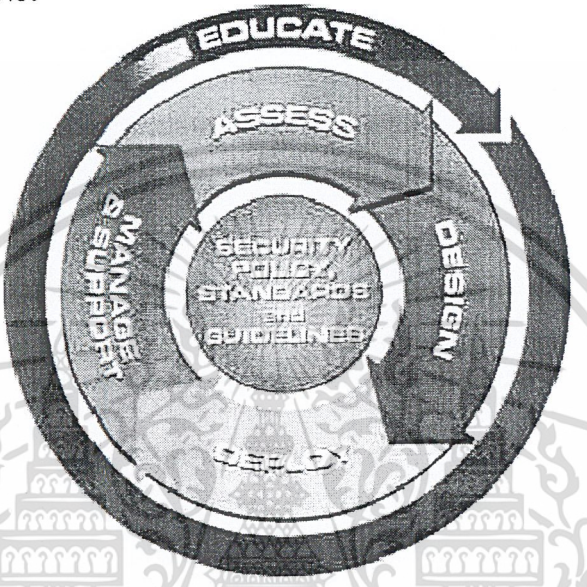
- เนื่องจากบริการที่มีจุดอ่อนซึ่งเป็นที่รู้กันมีอยู่ไม่มาก ผู้บุกรุกหรือแฮ็กเกอร์ที่มีความรู้จึงสามารถเขียนโปรแกรมขนาดเล็กที่พยายามเชื่อมต่อกับพอร์ตของบริการที่กำหนดบนโฮสต์ เป้าหมายเอาท์พุตของโปรแกรมคือรายการโฮสต์ที่สนับสนุนบริการนั้นซึ่งเปิดกว้างต่อการโจมตี
- มีเครื่องมือที่ใช้โดยทั่วไปหลายตัว เช่น Security Administrator Tool for Analysing Network (SATAN) ที่ตรวจสอบโดเมนหรือเครือข่ายย่อย(Subnetwork) ทั้งหมด และค้นหาจุดอ่อนในการรักษาความปลอดภัย โปรแกรมเหล่านี้ระบุจุดอ่อนของแต่ละระบบซึ่งอาจถูกโจมตีในหลายๆ จุด ผู้บุกรุกใช้ข้อมูลที่รวบรวมจากการตรวจสอบเหล่านี้เพื่อเข้าถึงระบบขององค์กรเป้าหมายโดยไม่ได้รับอนุญาต

ผู้ดูแลระบบที่ชาญฉลาดสามารถใช้เครื่องมือเหล่านี้ภายในเครือข่ายส่วนตัวของพวกเขาเพื่อค้นหาจุดอ่อนในการรักษาความปลอดภัย และตรวจดูว่าโฮสต์ใดต้องได้รับการปรับปรุงด้วยซอร์ฟแวร์ที่แก้ไขใหม่

บทที่3

หลักการและขั้นตอนการรักษาความปลอดภัยระบบเครือข่ายขององค์กร

3.1 วัฏจักรความปลอดภัย (Security lifecycle)



รูปที่3-1 แสดงวัฏจักรความปลอดภัย

- **ประเมิน (Assess)**

พิจารณามูลค่าของสินทรัพย์ข้อมูลขององค์กร ขนาดของการคุกคาม(Size of threats) ช่องโหว่และความบกพร่องของข้อมูล(Vulnerabilities) และความสำคัญของความเสี่ยงโดยรวมขององค์กร(Risk = Threat + Vulnerability) เหล่านี้เป็นการล่วงรู้ถึงสถานะปัจจุบันของความเสี่ยงที่มีต่อสินทรัพย์ข้อมูลของ

- **ออกแบบ (Design)**

เปลี่ยนข้อมูลที่ประเมินมาได้เป็นรายการของแอพพลิเคชันเกี่ยวกับการรักษาความปลอดภัยเครือข่าย (Network security Application) จัดลงในตำแหน่งที่เหมาะสม กระทำตามกลยุทธ์ต่างๆ และปรับแต่งค่าต่างๆตามคำแนะนำ สำหรับแต่ละอุปกรณ์เครือข่ายหรือ แต่ละแอพพลิเคชันความปลอดภัย ณ จุดที่ขั้นตอนนี้เสร็จสมบูรณ์ นโยบายทางด้านความปลอดภัย (Security Policy) ต้องจัดเป็นเอกสารเรียบร้อยตามด้วยแผนงานเรียบเรียง (deployment plan) สำหรับทุกๆ เทคโนโลยีที่จำเป็น

- **เรียบเรียง (Deploy)**

เป็นขั้นตอนในการจัดทำแผนงานที่คิดขึ้นมาในขั้นตอนการออกแบบ พร้อมทั้งการติดตั้ง การทดสอบ การฝึกอบรม และแปลงไปเป็นโปรดักต์ (production)

- **จัดการและสนับสนุน (Manage and Support)**

การวัดประสิทธิภาพของข้อมูลของโครงสร้างพื้นฐานการรักษาความปลอดภัยระบบเครือข่าย (Network security infrastructure) network security ที่ขัดแย้งกับสถานะจุดประสงค์ (goals state) ในนโยบายความปลอดภัย พิจารณาว่าควรจะประเมินนโยบายใหม่หรือยัง และจะเริ่มต้นขั้นตอนการสร้างนโยบายใหม่หรือยัง

- **ศึกษาหาข้อมูล (Education)**

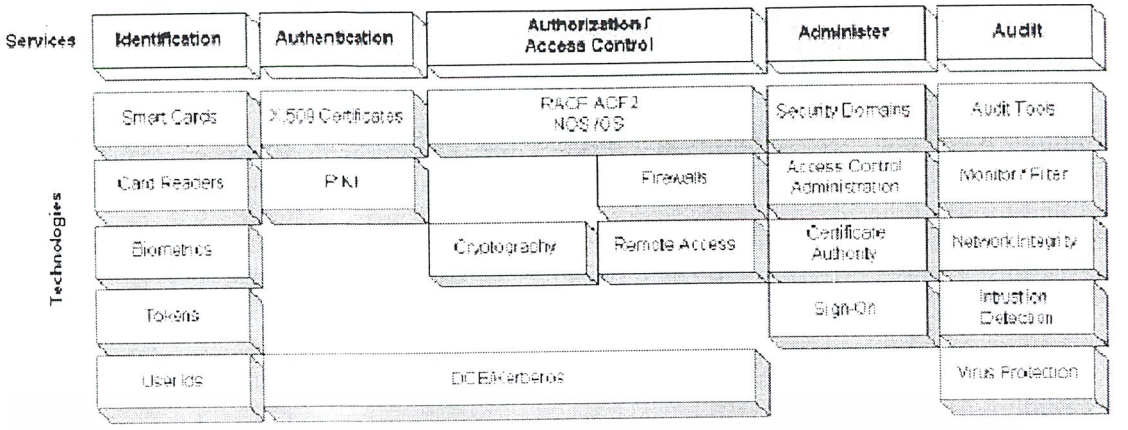
ความพยายามต่อเนื่องที่จะรับรู้ถึงสิ่งจำเป็นสำหรับความปลอดภัยระบบเครือข่ายทั้งที่การบริหารการจัดการ ที่ผู้ดูแลระบบ(Administrator) และที่ระดับผู้ใช้(User) ขั้นตอนนี้จะตัดข้ามทุกๆขั้นตอน และรวมไปถึงทั้งการฝึกอบรมผู้ดูแลระบบให้พร้อมสำหรับการคุกคามที่จะเกิดขึ้นได้ตลอด และการตระหนักถึงข้อได้เปรียบของการทำงานในความปลอดภัยในหมู่ผู้ใช้เองด้วย

หลังจากได้นำเอาแผนการต่างๆไปปฏิบัติ (Implementation) แล้ว ต้องมีกระบวนการตรวจสอบ (Audit) ควบคู่ไปด้วย ซึ่งเป็นการทำให้แน่ใจว่าการควบคุมถูกปรับแต่งค่าต่างๆ อย่างถูกต้องตรงตามนโยบายที่วางไว้ด้วย

3.2 ภาพรวมระบบรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ในองค์กร

บริการทางด้านความปลอดภัย (Security services) ที่พึงมีในการปกป้องข้อมูลและเครือข่ายขององค์กร มีดังนี้

- **การชี้ตัว (Identification)** เป็นกระบวนการจำแนกผู้ใช้ หนึ่งจากทั้งหมด
- **การพิสูจน์ตน (Authentication)** กระบวนการตรวจสอบความจริง (verifying) ลักษณะจำเพาะของผู้ใช้นั้นๆ
- **การอนุญาตและการควบคุมสิทธิการใช้งาน (Authorization and access control)** การมอบและ บังคับ สิทธิ์ และ อภิสิทธิ์ ที่อนุญาตแก่ผู้ใช้
- **การจัดการบริหาร (Administration)** เป็นการจัดการ จัดตั้ง และทำให้ความปลอดภัยนั้นคงอยู่ได้
- **การตรวจสอบ (Audit)** กระบวนการในการสังเกต ตรวจตรากิจกรรมของระบบว่าตรงตามนโยบายขององค์กรหรือไม่



รูปที่ 3-2 แสดงความสัมพันธ์ระหว่างบริการทางด้านความปลอดภัยและเทคโนโลยีของมัน

3.2.1 การชี้ตัว (Identification)

ในการจำแนกแยกแยะ ให้ระบบรู้ว่า เป็น ผู้ใช้ คนใดเข้ามา หมายรวมถึงการรับการเข้าสู่ทรัพยากรขององค์กร เช่น workstations , ระบบเครือข่าย (networks), หรือแอพพลิเคชัน ซึ่งมันมีความใกล้เคียงต่อไปกับ การพิสูจน์ตนมาก ซึ่ง การพิสูจน์ตนคือการตรวจสอบลักษณะเฉพาะของผู้ใช้ นั้นๆ ตัวอย่างของการ การชี้ตัว เช่น ยูสเซอร์ไอดี (userID) และ รหัสผ่าน, สมาร์ทการ์ด(smart card) , ไบโอเมทริกต์ (biometrics) (ลายนิ้วมือ, DNA,ลายเซ็น) เป็นต้น

3.2.2 การพิสูจน์ตน (Authentication)

การพิสูจน์ตน เป็นการตอบคำถามที่ว่า "คุณคือคนที่คุณแสดงตนหรือไม่" **(Are you who you say you are?)** วิธีการง่ายๆ ก็คือใช้ **รหัสผ่าน** แต่ทว่า รหัสผ่าน นั้นมี จุดอ่อน(weakness) ที่หลากหลายมาก เป็นอันตรายอย่างยิ่ง มักขาดการจัดการบริหารที่ดีพอ หรืออาจขาดความใส่ใจในการเลือกรหัสผ่าน อาจหันมาใช้ **ลายเซ็นดิจิตอล (Digital signature)** ซึ่งก็เทียบเท่ากับ ลายเซ็น ที่เป็นลายมือของเจ้าตัวนั่นแหละ บางเทคนิคเช่น certificateของพับลิคคีย์ **(Public Key Certificates)** ก็ได้รับการพัฒนาเพื่อใช้กับการกการพิสูจน์ตน ที่เข้มงวดได้อย่างดี ซึ่งเป็นเทคนิคที่ใช้หลักการของศาสตร์แห่งการเข้ารหัส (Cryptography)

3.2.3 การอนุญาตและการควบคุมสิทธิการใช้งาน (Authorization and Access Control)

การอนุญาต ตอบคำถามที่ว่า "คุณได้รับอนุญาตให้ทำในสิ่งที่คุณกำลังขอหรือพยายามจะทำหรือไม่" ความต้องการที่จะใช้หรือ ข้อห้ามไม่ให้ใช้ ทรัพยากรที่หลายหลากอันกระจายอยู่ข้ามหน่วยงานกัน ข้อมูลบางอย่าง เข้าถึง (access) ได้ทุกๆ ผู้ใช้ แต่บางอย่างเข้าถึงได้แค่บางคนเท่านั้น การอนุญาตนี้เป็นการยินยอมที่จะให้ใช้ทรัพยากรทางคอมพิวเตอร์ ส่วนการเข้าถึง เป็น ความสามารถในการทำบางสิ่งบางอย่างกับทรัพยากรนั้นการควบคุมสิทธิการใช้งาน (Access control)เป็นความหมายทางเทคนิค คือการบังคับใช้การอนุญาตนั้น (enforce permission) การควบคุมสิทธิการใช้งานนี้ สามารถฝังอยู่ในระบบ

ปฏิบัติการ อาจรวมอยู่ในโปรแกรมแอพพลิเคชัน หรือโปรแกรมยูทิลิตี้หลักๆ หรืออาจจะถูกกระทำการใน add-on security packages ที่ติดตั้งอยู่กับระบบปฏิบัติการ การควบคุมสิทธิการใช้งานอาจถูกแสดงในคอมโพเนนต์ (component) ที่ ควบคุมการติดต่อสื่อสารระหว่างคอมพิวเตอร์ ก็ได้

สำหรับเทคโนโลยีที่จะใช้ในการป้องกันองค์กรจากการไม่ได้รับอนุญาต(unautherized)ทั้งการเข้าถึงจากภายนอกและภายใน อีกทั้งรักษาความถูกต้องและ ความลับของข้อมูลขององค์กร ประกอบด้วย :

- **ศาสตร์แห่งการเข้ารหัส (Cryptography)** ดังที่ได้กล่าวแล้ว
- **ศาสตร์แห่งการเข้ารหัสแบบซีเคร็ตคีย์ (Secret Key Cryptography)** - สำหรับ อัลกอริทึม(algorithms) ของมัน เช่น DES, 3DES, RC2,RC4 ,IDEA และ CAST เป็นต้น
- **โพรโตคอลรักษาความปลอดภัย (Security Protocols)** - ที่สำคัญๆ มีดังนี้

  - **Secure Sockets Layer (SSL)** ใช้กันอย่างกว้างขวางซึ่งเป็นการติดต่อกันอย่างปลอดภัย ระหว่างเว็บเซิร์ฟเวอร์ และ เว็บบราวเซอร์ SSL สร้างการเชื่อมต่อที่ถูกเข้ารหัส ระหว่างไคลเอ็นต์กับเซิร์ฟเวอร์ ที่ต้องการติดต่อกันอย่างปลอดภัย เป็นไปได้ทั้งการ การพิสูจน์เครื่องไคลเอ็นต์ และเซิร์ฟเวอร์ ด้วย SSL สามารถถูกใช้กับแอพพลิเคชัน อื่นๆ ได้เช่น เอฟทีพี(FTP), เทลเน็ต (Telnet) เป็นต้น

    มาตรฐาน : SSL v3

  - **Simple Key Management for Internet Protocols (SKIP)** เป็น โพรโตคอลการแลกเปลี่ยนซีเคร็ตคีย์ ที่ทำงานภายใต้ชั้น IP ใน โพรโตคอลTCP/IP วิธีนี้สามารถถูกใช้จัดทำความปลอดภัยแบบระบบที่ไม่รู้สึกถึงว่ามีอยู่(Transparent Security ระหว่าง entities)

  - **Security Multiparts for MIME : S/MIME** เป็นโปรแกรมแอพพลิเคชันคโพรโตคอลรักษาความปลอดภัยสำหรับอีเมล์ แต่มันกว้างกว่าแบบ store-and-forward messaging

    มาตรฐาน : S/MIME v3

  - **Internet Protocol Security extensions : IPSec** เป็นโพรโตคอลรักษาความปลอดภัยที่นิยามสำหรับเครือข่าย IPที่งานบนระดับชั้นเน็ตเวิร์ก (network layer) ใน โพรโตคอลTCP/IP IPSec จะเพิ่มเฮดเดอร์ขยาย เข้าไปใน IP แพ็กเก็ต ออกแบบมาให้ทำความปลอดภัยที่ปลายทางสู่ปลายทาง (end-to-end security) สำหรับการท่องไปของแพ็กเก็ตบน อินเตอร์เน็ต

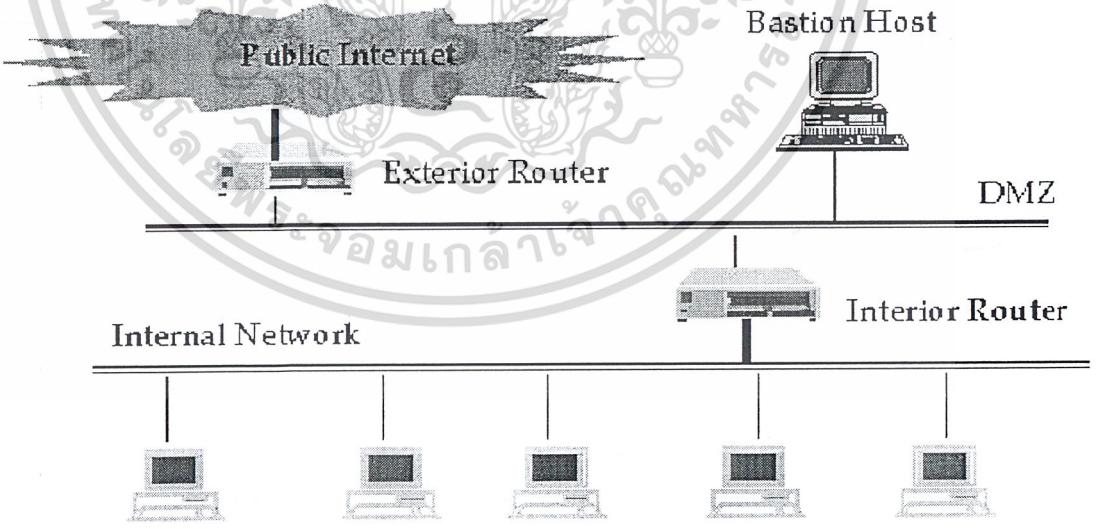
    มาตรฐาน : IPSec

  - **Internet Key Exchange : IKE** แลกเปลี่ยนคีย์ในการเข้ารหัส ระหว่าง distant device ซึ่ง เป็นมาตรฐานของกลไกการแลกเปลี่ยนคีย์ สำหรับ IPSec

Email	Web Browser	Tax Application
S/MIME	SSL	
IPSEC		
SKIP		
Physical Layer Security		

รูป3-3 แสดงโพรโตคอลรักษาความปลอดภัยและแอพพลิเคชัน

- ไฟร์วอล (Firewalls) เป็นคำเรียกของอุปกรณ์ทางกายภาพ(Physical device), ซอฟต์แวร์ และ สถาปัตยกรรมระบบเครือข่าย (network architectures) ออกแบบมาเพื่อขวางกั้น(Block) หรือ กรอง การผ่านเข้าออก ระหว่าง เครือข่ายส่วนตัว (Private network) กับ เครือข่ายสาธารณะ (Public network) เช่น อินเตอร์เน็ต มันสามารถถูกใช้ทำการควบคุมสิทธิการใช้งานระหว่างเครือข่ายภายในที่แยกกัน (Separate internal networks)



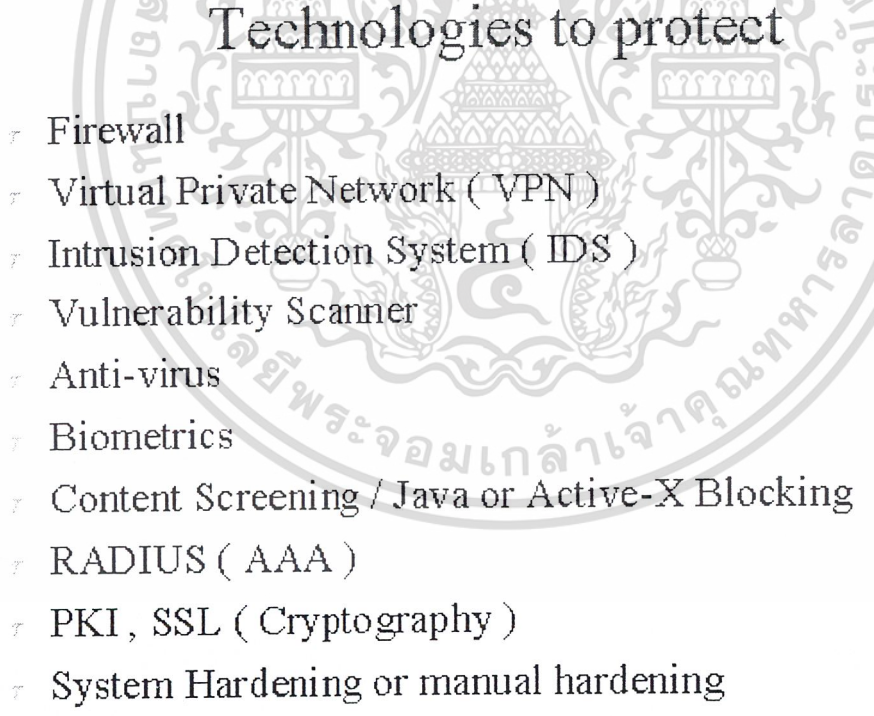
รูป 3-4 แสดงไฟร์วอลล์ชนิด screened Subnet

- **Virtual Private Networks (VPNs)** เป็นเส้นทางของการเชื่อมต่อระหว่าง 2 เครือข่าย ที่ต้องติดต่อกัน ข้ามผ่านเครือข่ายที่ไม่ปลอดภัย เช่น อินเตอร์เน็ต ซึ่ง VPN จะสร้างความปลอดภัยด้วยการใช้ IPSec การเชื่อมต่อนี้ จะทำระหว่างไฟร์วอล แต่บาง VPN ก็ใช้โพรโตคอลอื่นแทน

IPSec เช่น ใช้ PPTP, L2TP, L2F ซึ่งจะเหมาะกว่าในกรณีที่เป็นแอพพลิเคชันที่เข้าถึงในระยะไกล(remote-access applications) และทราฟฟิก ที่ไม่ใช่ไอพี (non –IP traffic) ข้ามอินเตอร์เน็ต

มาตรฐานที่ใช้กันในตอนนี้

1. บริการที่จัดอยู่บนอินเตอร์เน็ต เช่น แอพพลิเคชันเว็บ-เอนเนเบิล (Web-enabled application) , เอฟทีพี, เมล์ ,ข่าวสาร, ดีเอ็นเอส เหล่านี้ต้อง ให้อยู่บน DMZ (Demilitarized Zone) หรือ พร็อกซี (Proxied) จาก DMZ (โฮสต์ที่ไม่น่าเชื่อถือ และ มีความปลอดภัยต่ำ)
2. ใช้ S/MIME v3 ในการรักษาความปลอดภัยในการติดต่อทางอีเมล์ (secure email communication)
3. ใช้ IPSec
4. ศาสตร์แห่งการเข้ารหัสต้องอยู่บนมาตรฐานที่เปิด เช่น พับลิคคีย์ / ไพรเวทคีย์ ก็ต้องใช้มาตรฐาน คือ RSA, ECC ไพรเวทคีย์ก็ต้องใช้ DES, 3DES เป็นต้น Message digest ก็ต้องใช้ MD5, SHA-1 เป็นต้น
5. SSL v3



รูปที่3-5 แสดงเทคโนโลยีที่จะใช้ในการรักษาความปลอดภัยซึ่งสมบูรณ์ที่สุด

(Countermeasure Technologies)

บทที่ 4
เทคโนโลยีของความปลอดภัย
บนเครือข่ายอินเตอร์เน็ตและเครือข่ายขององค์กร

4.1 การเข้ารหัส (Encryption)

4.1.1 ศาสตร์แห่งการเข้ารหัสแบบซีเคร็ตคีย์ (Secret Key Cryptography)

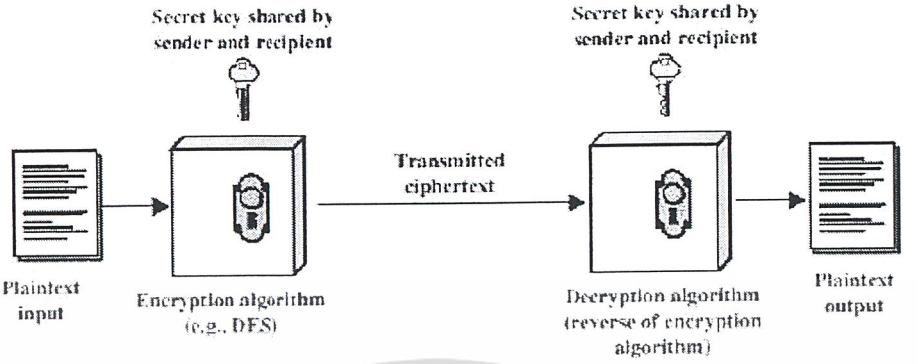
การเข้ารหัสแบบซีเคร็ตคีย์หรือเรียกว่าการเข้ารหัสแบบสมมาตร (symmetric encryption) สำหรับสาเหตุที่เรียกว่าสมมาตร เพราะมีกระบวนการเข้ารหัสและถอดรหัสที่เป็นกระบวนการเดียวกัน และในกระบวนการเข้ารหัสแบบนี้ บางครั้งจะเรียกว่าคีย์เดี่ยว (single key)

4.1.1.1 หลักการของซีเคร็ตคีย์

ในกระบวนการเข้ารหัสของซีเคร็ตคีย์ จะมีส่วนประกอบอยู่ด้วยกันทั้งหมด 5 ส่วนด้วยกันคือ

- *เพลนเท็กซ์ (plaintext)* หมายถึง ข้อความเริ่มแรกที่ยังไม่ได้เข้ารหัส และมีความต้องการที่จะเข้ารหัส
- *อัลกอริทึมในการเข้ารหัส (encryption algorithm)* เป็นกระบวนการแปลงเพลนเท็กซ์ไปเป็นข้อความที่ไม่สามารถอ่านได้ โดยจะเน้นที่การสลับบิต หรือการแทนที่ เพื่อให้ข้อมูลมีความยุ่งเหยิง
- *ซีเคร็ตคีย์* เป็นรหัสที่ต้องป้อนเข้าไปในกระบวนการเข้ารหัส โดยรูปแบบการแปลงข้อความของอัลกอริทึมในการเข้ารหัส จะขึ้นกับซีเคร็ตคีย์ที่ป้อนเข้าไป
- *ไซเฟอร์เท็กซ์ (ciphertext)* เป็นผลลัพธ์ที่ได้จากการเข้ารหัสโดยจะขึ้นกับเพลนเท็กซ์ และซีเคร็ตคีย์ ที่ป้อนเข้าไป ข้อความที่เหมือนกัน แต่มีคีย์ต่างกัน จะให้ผลลัพธ์ที่ต่างกันด้วย
- *อัลกอริทึมในการถอดรหัส (decryption algorithm)* เป็นกระบวนการย้อนกลับของการเข้ารหัส โดยเมื่อใส่ไซเฟอร์เท็กซ์ และคีย์ที่ถูกต้องเข้าไป จะต้องได้ข้อความเดิมหรือเพลนเท็กซ์ออกมา

สำหรับรูปแบบของการเข้ารหัสแบบซีเคร็ตคีย์สามารถดูได้ตามรูปที่ 4-1 ในหน้าถัดไป



รูปที่ 4-1 แสดงรูปแบบของการเข้ารหัสแบบซีเคร็ตคีย์

4.1.1.2 ความจำเป็นในการเข้ารหัสแบบซีเคร็ตคีย์

ในการใช้งานการเข้ารหัสแบบซีเคร็ตคีย์นี้ จะมีความจำเป็น 2 ประการเพื่อให้การใช้งานได้ผลดี คือ

- อัลกอริทึมในการเข้ารหัสจะต้องมีความแข็งแกร่ง (strong)

ทั้งนี้เนื่องจากอัลกอริทึมที่เป็นซีเคร็ตคีย์ มักจะมีการเปิดเผยวิธีการอยู่แล้ว ดังนั้นผู้อื่นก็ย่อมจะรู้วิธีการเข้ารหัสและถอดรหัสเช่นเดียวกัน ดังนั้นจากส่วนประกอบของกระบวนการเข้ารหัส ผู้อื่นก็จะรู้ไซเฟอร์เท็กซ์เพราะสามารถดักจากกระบวนการส่งได้ และสามารถรู้อัลกอริทึม แต่สิ่งที่ผู้อื่นไม่รู้คือคีย์ ดังนั้นเพื่อให้ได้ข้อความต้นฉบับกลับมา ก็จะต้องหาคีย์เพื่อจะใช้ในการถอดรหัสได้ ดังนั้นอัลกอริทึมนี้จะต้องมีความแข็งแกร่งมากพอที่จะปิดบังคีย์เอาไว้ แม้ว่าจะได้ทั้งเพลนเท็กซ์และไซเฟอร์เท็กซ์ก็ไม่สามารถหาคีย์ได้

- การรักษาความลับของคีย์

หัวใจของกระบวนการเข้ารหัสแบบนี้คือ คีย์ ซึ่งจะได้เห็นว่าแม้ว่าจะทราบถึงส่วนประกอบต่าง ๆ ทั้งหมดแต่ไม่ทราบคีย์ ก็ไม่สามารถจะยับยั้ง (brake) กระบวนการเข้ารหัสได้ ดังนั้นการรักษาคีย์จึงมีความสำคัญอย่างยิ่ง และกระบวนการรับส่งหรือแจกจ่ายคีย์จะต้องมีความปลอดภัย เพราะหากมีผู้อื่นได้คีย์ไป กระบวนการเข้ารหัสเพื่อรักษาความลับ ก็จะไม่เป็นความลับอีกต่อไป

จากที่กล่าวมา จะเห็นว่าความปลอดภัยของการเข้ารหัส คือ การรักษาความลับของคีย์ ไม่ใช่ความลับของอัลกอริทึม ทั้งนี้เนื่องจากการได้มาซึ่งอัลกอริทึมสักหนึ่งตัวนั้นเป็นเรื่องไม่ง่ายนัก ดังนั้นหากใช้วิธีให้ความลับอยู่ที่อัลกอริทึมแล้ว หากถูกเปิดเผยก็จะต้องสร้างอัลกอริทึมใหม่ขึ้นมา ในขณะที่ใช้วิธีให้ความลับอยู่ที่คีย์แล้ว หากคีย์มีการการเปิดเผย ก็เพียงแต่สร้างคีย์ใหม่ขึ้นมาเท่านั้น ซึ่งเป็นเรื่องที่ง่ายกว่ามาก

และการเปิดเผยอัลกอริทึมนี้เอง ที่ทำให้การใช้งานการเข้ารหัสซีเคร็ตคีย์สามารถใช้งานได้ในวงกว้าง เพราะไม่จำเป็นที่แต่ละคนจะต้องสร้างอัลกอริทึมเข้ารหัสของตัวเองขึ้นมา แต่ใช้สิ่งที่เป็นมาตรฐานเหมือนๆ

กัน โดยใช้คีย์ที่ต่างกัน และจากการเปิดเผยอัลกอริทึมก็ไม่จำเป็นที่จะต้องบอกวิธีการให้อีกฝ่ายทราบ เพียงแต่เข้าใจตรงกันว่ากำลังใช้อัลกอริทึมไหนและใช้คีย์อะไรอยู่ก็พอแล้ว นอกจากนั้นยังสามารถสร้างการเข้ารหัสในรูปของฮาร์ดแวร์ได้ด้วย

4.1.1.3 ปัญหาของการเข้ารหัสแบบซีเคร็ตคีย์

ในการเข้ารหัสแบบซีเคร็ตคีย์นั้น ปัญหาใหญ่ที่สุดก็คือ เรื่องของการส่งคีย์ระหว่างผู้รับและผู้ส่งที่จำเป็นต้องใช้คีย์เดียวกัน ประกอบกับคีย์ที่ใช้จะต้องเป็นคีย์ลับ ดังนั้นจะเปิดเผยไม่ได้ คราวนี้ปัญหาก็เกิดจากตอนเริ่มต้นที่ยังไม่มีช่องทางลับ แล้วจะส่งคีย์ลับไปทางไหนจึงจะไม่สามารถถูกลอบดักเอาไปได้ซึ่งเป็นปัญหาค่อนข้างมาก ด้วยเหตุนี้จึงได้มีการออกแบบการเข้ารหัสอีกรูปแบบหนึ่งคือพับลิคคีย์(public key)

4.1.2 ศาสตร์แห่งการเข้ารหัสแบบแบบพับลิคคีย์ (Public Key Cryptography)

4.1.2.1 หลักการของพับลิคคีย์

การเข้ารหัสแบบพับลิคคีย์หรือเรียกว่า การเข้ารหัสไม่แบบสมมาตร (asymmetric encryption) สำหรับสาเหตุที่เรียกว่าไม่สมมาตร เพราะมีกระบวนการเข้ารหัสและถอดรหัสคนละกระบวนการกัน ในกระบวนการเข้ารหัสแบบนี้ บางครั้งจะเรียกว่าคีย์คู่(two key)

การใช้คีย์ 2 คีย์นี้เองที่ทำให้ปัญหาในเรื่องของการรับส่งคีย์ง่ายขึ้นมาก นอกจากนี้การเข้ารหัสแบบพับลิคคีย์ยังมีลักษณะการเข้ารหัสที่ต่างจากเดิม โดยจากเดิมจะเน้นที่การสลับบิตของข้อมูลหรือการแทนที่ แต่สำหรับพับลิคคีย์จะใช้วิธีฟังก์ชันทางคณิตศาสตร์เข้ามาประมวลผล ทำให้การถอดรหัสทำได้ยากมากขึ้น

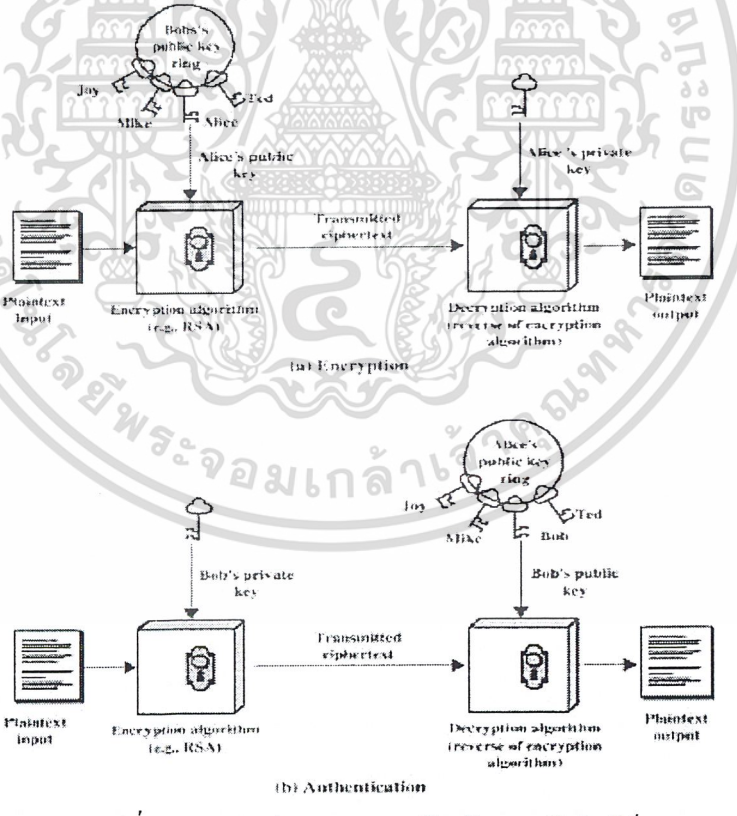
แต่ไม่ได้หมายความว่าพับลิคคีย์จะปลอดภัยกว่าซีเคร็ตคีย์ เพราะความปลอดภัยของการเข้ารหัสจะขึ้นกับปัจจัย 2 ประการคือ ความยาวของคีย์และความเร็วของเครื่องที่ใช้ในการถอดรหัส นอกจากนั้นพับลิคคีย์ก็ไม่ได้สร้างมาเพื่อใช้แทนซีเคร็ตคีย์ด้วย โดยการเกิดขึ้นของพับลิคคีย์ก็ไม่ได้ทำให้ซีเคร็ตคีย์หายไป เนื่องจากพับลิคคีย์ใช้ฟังก์ชันทางคณิตศาสตร์ในการประมวลผล จึงทำให้การเข้ารหัสและถอดรหัสข้อมูลแต่ละครั้งจะใช้เวลามาก

สำหรับการทำงานของพับลิคคีย์ได้แสดงไว้ตามรูปที่ 4-2 โดยการทำงานก็จะคล้ายกับการทำงานของซีเคร็ตคีย์ แต่จะต่างกันตรงที่จะมีคีย์จำนวน 2 คีย์ คือไพรเวทคีย์ (private key) ซึ่งเป็นคีย์ที่จะเก็บเอาไว้กับตัว โดยคีย์ตัวนี้จะเป็นคีย์ลับที่จะต้องเก็บเอาไว้อย่างดี สำหรับอีกคีย์หนึ่งคือพับลิคคีย์ โดยเป็นคีย์ที่ใช้แจกจ่ายออกไป ซึ่งคีย์ทั้ง 2 ตัวนี้จะทำงานคู่กันคือหากเข้ารหัสด้วยไพรเวทคีย์ ก็จะต้องถอดออกด้วยพับลิคคีย์ของคู่มันเท่านั้น และหากเข้ารหัสด้วยพับลิคคีย์ ก็จะต้องถอดด้วยไพรเวทคีย์ของคู่มันเท่านั้น

4.1.2.2 การนำการเข้ารหัสแบบพับลิคคีย์ไปใช้งาน

หากมองในแง่ของการนำไปใช้งานแล้ว จะแบ่งออกเป็น 3 กรณีคือ

- **การพิสูจน์ตน (authentication)** โดยเข้ารหัสด้วยไพรเวทคีย์และถอดรหัสด้วยพับลิคคีย์ กล่าวคือ ข้อมูลที่เข้ารหัสด้วยไพรเวทคีย์จะถอดรหัสได้ด้วยพับลิคคีย์ที่เป็นคู่ของมันเท่านั้น ดังนั้นเราจึงใช้ในการยืนยันต้นทางว่ามาจากบุคคลนั้นจริงๆ ได้ เพราะหากคนนั้นไม่ได้เข้ารหัสมาแล้วก็จะใช้พับลิคคีย์ของคนนั้นถอดไม่ได้ ซึ่งมักจะเรียกว่าการไซน์ (sign)เพื่อเป็นลายเซ็นดิจิตอล (digital signature) นั่นเอง
- **ความลับในทิศทางเดียว (one-way confidential)** โดยเข้ารหัสด้วยพับลิคคีย์และถอดรหัสด้วยไพรเวทคีย์ กล่าวคือข้อมูลที่เข้ารหัสด้วยพับลิคคีย์จะถอดรหัสได้ด้วยไพรเวทคีย์ที่เป็นคู่ของมันเท่านั้น ดังนั้นความเป็นความลับจะเกิดขึ้นทิศทางเดียวคือทิศทางที่เข้ารหัสด้วยพับลิคคีย์จากผู้อื่น เพราะการถอดรหัสจะต้องอาศัยไพรเวทคีย์ ซึ่งจะมีเฉพาะเจ้าของเท่านั้นที่มี
- **ความลับในสองทิศทาง (two-way confidential)** โดยใช้คีย์จำนวน 2 คู่



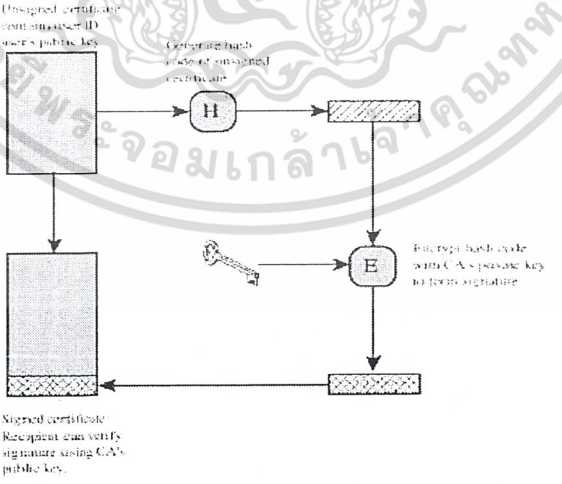
รูปที่ 4-2 แสดงรูปแบบของการเข้ารหัสแบบพับลิคคีย์

4.1.2.3 ปัญหาของการเข้ารหัสแบบแบบพับลิคคีย์

- พับลิคคีย์ใช้ฟังก์ชันทางคณิตศาสตร์ในการประมวลผล จึงทำให้การเข้ารหัสและถอดรหัสข้อมูลแต่ละครั้งใช้เวลามาก ดังนั้นในทางปฏิบัติเราจึงใช้พับลิคคีย์ในการรับส่งคีย์ที่เป็นซีเคร็ตคีย์ ซึ่งสามารถแก้ปัญหาในเรื่องการกระจายคีย์ของซีเคร็ตคีย์ลงได้ ดังนั้นพับลิคคีย์จึงทำหน้าที่เสริมการทำงานของซีเคร็ตคีย์ให้สมบูรณ์แบบมากขึ้น
- ในการใช้พับลิคคีย์อาจอาศัยการแจกจ่ายกันเป็นส่วนตัวก็ได้ โดยอาจส่งทางอีเมล์หรือช่องทางอื่นๆ และจากช่องทางในการส่งนี่เองที่ทำให้เกิดจุดอ่อนขึ้น เช่น สมมติว่าสุนันท์ส่งพับลิคคีย์ของตนเองไปให้นิสา หากมีผู้ดักจับจดหมายดังกล่าวกลางทางก็อาจจะทำการเปลี่ยนพับลิคคีย์เสียใหม่ โดยสร้างพับลิคคีย์ขึ้นมาใหม่ได้ จากนั้นหากสุนันท์ส่งข้อความใดๆ ถึงนิสาอีกโดยมีการไซน์ ผู้ดักจับก็จะแอบเปลี่ยนข้อความแล้วไซน์ใหม่โดยอาศัยไพรเวทคีย์ที่มีอยู่ และเมื่อนิสาได้รับ แล้วนับพับลิคคีย์(ปลอม)ที่ได้รับในครั้งก่อนมาตรวจสอบ ก็อาจคิดว่าเป็นจดหมายจริง จึงได้มีการนำเอา CA (Certificate Authority) มาใช้

4.1.2.4 การนำเอา CA (Certificate Authority) มาใช้ในการเข้ารหัสแบบพับลิคคีย์

CA เป็นตัวกลางในการแจกจ่ายคีย์ โดยแทนที่สุนันท์จะต้องคอยส่งพับลิคคีย์ของตนเองไปในช่องทางต่างๆ เช่น อีเมล์ ก็จะส่งไปเก็บไว้ที่ CA โดยจะเก็บไว้ในรูปแบบของใบรับรอง (certificate) จากนั้นก็ให้ผู้ติดต่อด้วยคือนิสาไปขอใบรับรอง (certificate) จาก CA ซึ่งในกระบวนการส่งพับลิคคีย์จะมีการไซน์จากCA เพื่อยืนยันว่าพับลิคคีย์นี้เป็นพับลิคคีย์ที่ถูกต้อง ดังนั้นจึงสามารถแก้ปัญหาข้างต้นได้ ในรูปที่4-3 จะแสดงกระบวนการในการส่งคีย์ โดยจะใช้มาตรฐาน PKI (x.509)



รูปที่ 4-3 แสดงกระบวนการในการส่งคีย์

4.1.3 ระบบการเข้ารหัส

ในการเข้ารหัสนั้น โดยทั่วไปจะมีการพิจารณาใน 3 มุมมองด้วยกันคือ

4.1.3.1 รูปแบบของการกระทำที่ใช้ในการแปลงจากเพลนเท็กซ์ไปเป็นไซเฟอร์เท็กซ์

ในอัลกอริทึมของการเข้ารหัส มักจะตั้งอยู่บนหลักการ 3 หลักด้วยกันคือ

- *การแทนที่ (substitution)* โดยหลักการแทนที่นั้น จะใช้วิธีแทนส่วนประกอบของเพลนเท็กซ์ (บิต, กลุ่มของบิต หรือไบต์ หรือตัวอักษร) ด้วยส่วนประกอบอีกกลุ่มหนึ่ง
- *การสลับที่ (transposition)* จะเป็นการจัดลำดับของบิต, กลุ่มของบิต หรือไบต์ หรือตัวอักษรให้มีรูปแบบที่เปลี่ยนไป โดยในระหว่างกระบวนการนั้น จะต้องไม่มีข้อความใด ๆ หายไป
- *การใช้ฟังก์ชันทางคณิตศาสตร์*

4.1.3.2 จำนวนคีย์

- *คีย์เดี่ยว* หรือซีเคร็ตคีย์ หรือการเข้ารหัสแบบสมมาตร
- *คีย์คู่* หรือพับลิคคีย์ หรือการเข้ารหัสแบบไม่สมมาตร

4.1.3.3 ลักษณะทีอัลกอริทึมกระทำกับข้อความต้นฉบับ

- *บล็อกไซเฟอร์ (block cipher)* คือการแบ่งข้อมูลออกเป็นส่วน ๆ ที่มีความยาวเท่ากันแล้วจึงประมวลผลข้อมูลไปทีละบล็อก โดยจะได้ผลลัพธ์เป็นบล็อกเช่นเดียวกัน
- *สตรีมไซเฟอร์ (stream cipher)* ซึ่งมีการประมวลผลไปทีละกลุ่ม (อาจเป็นบิต, ไบต์หรือกลุ่มของบิต) โดยผลลัพธ์ออกมาในทำนองเดียวกัน

4.2 แอพพลิเคชันสำหรับการพิสูจน์ตน (Authentication Application)

4.2.1 เคอร์บีรอส (Kerberos)

4.2.1.1 จุดประสงค์ที่นำเคอร์บีรอสมาใช้งาน

ในยุคเริ่มต้นการใช้งานคอมพิวเตอร์ มักจะอยู่ในลักษณะของการใช้งานในแบบที่เรียกว่า เครื่องใครเครื่องมัน (stand alone) ดังนั้นการป้องกันข้อมูลสามารถทำได้โดยป้องกันการเข้าใช้งานในเครื่องพีซีแต่ละเครื่อง

ต่อมามีการเชื่อมต่อเป็นระบบเครือข่ายโดยมีเซิร์ฟเวอร์อยู่ตรงกลาง การป้องกันข้อมูลก็ได้กลายเป็นหน้าที่ของระบบปฏิบัติการ โดยระบบปฏิบัติการจะทำหน้าที่ควบคุมนโยบายการเข้าใช้งาน ซึ่งโดยส่วนใหญ่จะใช้การล็อกออน (logon) เพื่อระบุตัวผู้ใช้

แต่เมื่อมาถึงปัจจุบันลักษณะการเชื่อมต่อของคอมพิวเตอร์ผ่านทางเครือข่ายได้เปลี่ยนไป โดยเซิร์ฟเวอร์ซึ่งเดิมเป็นคอมพิวเตอร์เครื่องเดียวทำทุกอย่าง ก็ได้เปลี่ยนเป็นคอมพิวเตอร์1 เครื่องให้บริการไม่กี่อย่าง (อาจจะอย่างเดียวก็ได้) เช่น เซิร์ฟเวอร์ที่ทำหน้าที่เป็นเมลล์เซิร์ฟเวอร์ ไฟล์เซิร์ฟเวอร์, เวปเซิร์ฟเวอร์,

เอฟทีพีเซิร์ฟเวอร์, ดาต้าเบสเซิร์ฟเวอร์ และอื่นๆ อีกมากมาย ซึ่งหมายความว่าผู้ใช้ 1 คน อาจต้องใช้เซิร์ฟเวอร์มากกว่า 1 เครื่องในขณะเดียวกัน จึงเป็นที่มาของแอพพลิเคชันสำหรับการพิสูจน์ตนนั่นเอง สำหรับการพิสูจน์สิทธิ์จะเป็นไปในลักษณะดังนี้

1. ผู้ใช้จะต้องพิสูจน์สิทธิ์กับไคลเอ็นต์หรือแสดงตัวกับเซิร์ฟเวอร์โดยผ่านไคลเอ็นต์อีกที(อาจจะทำโดยการล็อกออน) ซึ่งอาจต้องผ่านนโยบายของการเข้าใช้ระบบด้วย
2. ไคลเอ็นต์จะต้องพิสูจน์สิทธิ์กับเซิร์ฟเวอร์
3. และในบางกรณี ผู้ใช้จะต้องพิสูจน์สิทธิ์การใช้งานในระดับของการให้บริการ(service) ด้วย

ในระบบที่มีขนาดไม่ใหญ่นัก ซึ่งเครื่องทั้งหมดทำงานในองค์กรเดียวกัน อาจต้องการการพิสูจน์สิทธิ์เพียง 2 ข้อแรก แต่หากเป็นองค์กรใหญ่ๆ แล้วอาจต้องมีการพิสูจน์สิทธิ์ในข้อ 3 ด้วย ซึ่งเคอร์บีรอสก็ได้ออกแบบมาเพื่อการพิสูจน์สิทธิ์ทั้ง 3 ระดับนี้ โดยเคอร์บีรอสจะสามารถใช้งานกับระบบเครือข่ายที่ทำงานในแบบไคลเอ็นต์/เซิร์ฟเวอร์ (client/server) ที่มีจำนวนเท่าไรก็ได้ และสามารถมี เคอร์บีรอส ได้หลายเครื่องอีกด้วย

4.2.1.2 เงื่อนไขการออกแบบของเคอร์บีรอส

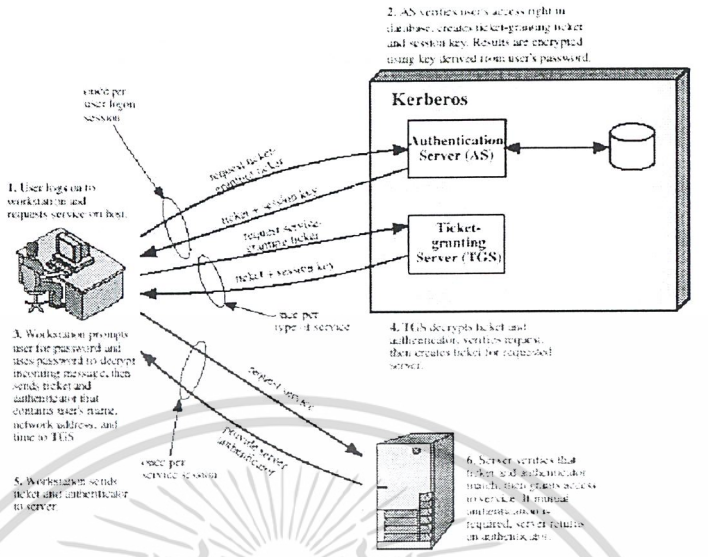
- **ความปลอดภัย (Secure)** ระบบจะป้องกันการลอบดักข้อมูลในระบบเครือข่าย โดยมีการรับประกันว่าข้อมูลที่ถูกดักเอาไป จะไม่สามารถทำให้เกิดการปลอมเป็นผู้ใช้คนอื่นได้ หรืออีกนัยหนึ่งคือเคอร์บีรอสจะต้องแข็งแกร่งมากพอที่ฝ่ายตรงข้ามจะไม่สามารถหาจุดอ่อนจากการส่งข้อมูลได้
- **ความเชื่อถือได้ (Reliable)** เนื่องจากเคอร์บีรอสเป็นแกนกลางของการพิสูจน์สิทธิ์ ดังนั้นหากเคอร์บีรอสไม่สามารถใช้งานได้ในขณะใดขณะหนึ่ง การเข้าใช้งานก็จะไม่สามารถทำได้ ดังนั้นเคอร์บีรอสจึงต้องมีเสถียรภาพสูงมาก โดยจะยอมให้มี2 ระบบสำรองการทำงานกันได้
- **ความไม่รู้สึกว่ามีอยู่ (Transparent)** โดยเคอร์บีรอสจะต้องไม่แสดงการทำงานในระดับของผู้ใช้ ซึ่งหมายความว่าผู้ใช้จะไม่รู้ว่ามีการใช้งานเคอร์บีรอสอยู่ โดยผู้ใช้ต้องทำแค่เพียงป้อนรหัสผ่านเท่านั้น ไม่ต้องรับรู้ถึงความกลไกการทำงานของเคอร์บีรอส
- **รองรับขนาดของระบบได้ไม่จำกัด (Scalable)** ระบบเคอร์บีรอสจะต้องสามารถสนับสนุนระบบขนาดใหญ่ที่มีจำนวนคอมพิวเตอร์มากๆ ได้ ไม่ว่าระบบคอมพิวเตอร์จะมีจำนวนเครื่องมากเท่าไหร่ก็ตาม

จากเงื่อนไขที่ได้กล่าวมาจึงทำให้ระบบเคอร์บีรอสเป็นลักษณะของผู้ให้บริการพิสูจน์สิทธิ์ ซึ่งทั้งเซิร์ฟเวอร์และไคลเอ็นต์จะต้องทรัสต์ (trust) กับระบบเคอร์บีรอส โดยยอมให้เคอร์บีรอสทำการพิสูจน์สิทธิ์การใช้งานให้ ดังนั้นตราบใดที่ระบบเคอร์บีรอสมีความปลอดภัยก็จะหมายความว่าการพิสูจน์สิทธิ์มีความปลอดภัยด้วย

4.2.1.3 การทำงานของเคอร์บีรอส

แสดงตามรูปที่ 4-4 ในหน้าถัดไป โดยมีลำดับการทำงานดังนี้

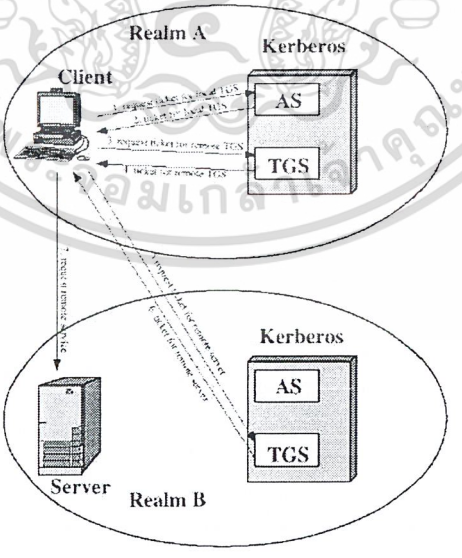
1. ไคลเอ็นต์จะขอ Ticket Granting Ticket โดยผู้ใช้จะต้องส่งชื่อผู้ใช้(user ID) ไปให้กับ AS (Authentication Server) โดยมีการส่งค่า TGS ID ไปด้วย เพื่อยืนยันว่าต้องการติดต่อกับเซิร์ฟเวอร์นั้นจริงและต้องการติดต่อกับ TGS (Ticket granting Server)
2. เครื่อง AS จะส่งตั๋ว (Ticket) ที่เข้ารหัสด้วยซีเคร็ตคีย์ของไคลเอ็นต์เอง โดยซีเคร็ตคีย์นี้จะเป็นคีย์ที่สร้างขึ้นมาใช้ในแต่ละครั้งเท่านั้น โดยสร้างมาจากรหัสผ่านของผู้ใช้ที่เก็บไว้ใน ASกับวิธีการของ AS เอง ทำให้แต่ละครั้งจะได้คีย์ที่ต่างออกไป จากนั้นเมื่อไคลเอ็นต์ได้รับตั๋วเรียบร้อยแล้วก็จะถามรหัสผ่านจากผู้ใช้ เพื่อนำมาทำการถอดรหัส ซึ่งหากผู้ใช้ป้อนรหัสผ่านตรงกับที่เก็บไว้ใน AS ก็จะสามารถถอดรหัสได้ และได้ตั๋วออกมา
3. เมื่อไคลเอ็นต์ต้องการใช้บริการก็จะขอ Service Granting Ticket ไปยัง TGS ซึ่งที่ TGS ก็จะมีการตรวจสอบว่าชื่อผู้ใช้ที่ให้มาด้วยเป็นชื่อเดียวกับในตั๋วหรือไม่และเน็ตเวิร์กแอดเดรส (network address) ตรงกันกับในกับตั๋วหรือไม่ และถ้าตั๋วยังสามารถใช้งานได้อยู่ก็จะให้ตั๋วอีกใบที่จะนำไปเข้าใช้บริการตามที่ไคลเอ็นต์ขอมา
4. เครื่อง TGS จะส่งตั๋วสำหรับเซิร์ฟเวอร์ให้กับเครื่องไคลเอ็นต์ โดยตั๋วนี้จะเข้ารหัสด้วยซีเคร็ตคีย์ที่รู้เฉพาะ TGS และเซิร์ฟเวอร์เครื่องนั้นเท่านั้น โดยตั๋วจะประกอบด้วยชื่อของผู้ใช้, เน็ตเวิร์กแอดเดรสของเครื่องผู้ใช้, ชื่อของเซิร์ฟเวอร์ที่ขอใช้บริการ และไทม์สแตมป์กับระยะเวลาที่ใช้ ตั๋วนี้ได้
5. เมื่อไคลเอ็นต์ได้รับตั๋วแล้ว ก็จะส่งตั๋วนี้เพื่อไปขอใช้บริการยังเซิร์ฟเวอร์ โดยจะส่งชื่อผู้ใช้ไปด้วย
6. เซิร์ฟเวอร์จะถอดรหัสตั๋วออกมา จากนั้นจะดูว่าชื่อผู้ใช้ตรงกับในตั๋วหรือไม่ และมีเน็ตเวิร์กแอดเดรสตรงกับในตั๋วหรือไม่ และถ้าตั๋วนั้นยังสามารถใช้งานได้อยู่ ก็จะยอมให้ผู้ใช้คนนั้นเข้าใช้บริการเซิร์ฟเวอร์นั้นได้



รูปที่ 4-4 การทำงานของเคอร์บีรอส

4.2.1.4 การขอให้บริการข้าม Realm ของเคอร์บีรอส

สำหรับเคอร์บีรอสวง ๆ หนึ่งจะเรียกว่า Realm โดยเคอร์บีรอสจะยอมให้มีการขอใช้บริการข้าม Realm กันด้วย โดยมีเงื่อนไขการทำงานเพิ่มเติมคือเครื่องเคอร์บีรอสเซิร์ฟเวอร์ที่อยู่ต่างRealm กันจะใช้ซีเคร็ตคีย์ร่วมกัน โดยเคอร์บีรอสเซิร์ฟเวอร์ทั้งสองจะต้องเข้ามาลงทะเบียนซึ่งกันและกันเอาไว้ โดยการทำงานข้าม Realm จะแสดงในรูปที่ 4-5 จะเห็นได้ว่าเมื่อมีความต้องการใช้งานเซิร์ฟเวอร์ที่อยู่ Realm อื่น ก็จะต้องร้องขอตั๋วไปยังเคอร์บีรอสของ Realm ที่ตนเองสังกัดก่อน เพื่อขอตั๋วที่จะเข้าไปใช้ในเคอร์บีรอสที่อยู่ต่าง Realm



รูปที่ 4-5 การทำงานข้าม Realm

4.2.2 Public Key Infrastructure (PKI)

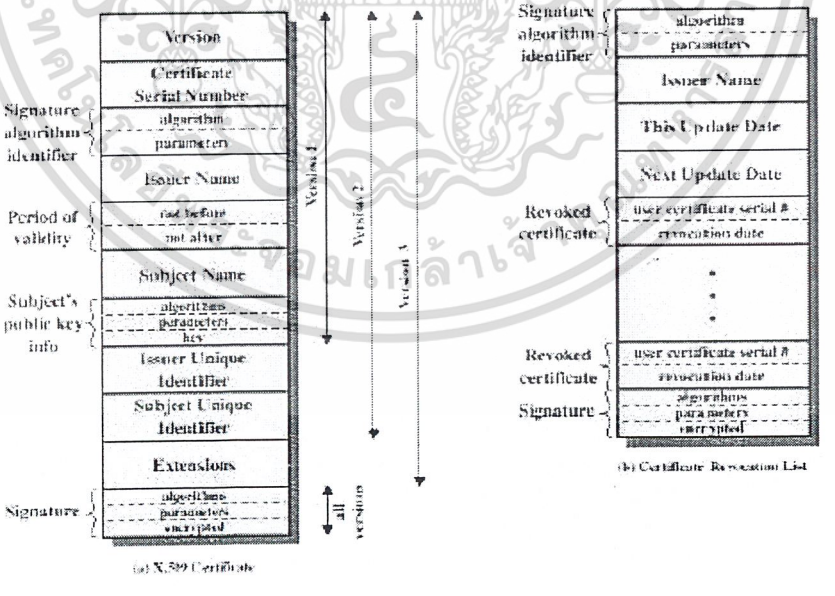
สำหรับเคอร์บีรอสจะเน้นไปที่การพิสูจน์สิทธิ์เพื่อเข้าใช้บริการ ซึ่งมักเป็นการพิสูจน์สิทธิ์ภายในองค์กรเดียวกัน แต่ PKI จะเน้นไปที่การพิสูจน์บุคคล เพื่อยืนยันการติดต่อมากกว่า

PKI หรือรู้จักกันในมาตรฐาน X.509 จะมีโครงสร้างการทำงานที่เป็นไดเร็กทอรี โดยในที่นี้ไดเร็กทอรีจะทำหน้าที่เก็บข้อมูลที่ใช้ในการยืนยัน โดยทั่วไปจะอยู่ในรูปของใบรับรอง(Certificate) ซึ่งในใบรับรองจะเก็บพับลิคคีย์ของผู้ใช้ที่ไซน์โดยไพรเวทคีย์ขององค์กรที่จ่ายใบรับรองมาให้ สำหรับการทำงานของ PKIจะมีขอบเขตการนำไปใช้งานที่กว้างขวางมาก เช่น ใช้ในการรักษาความปลอดภัยทางเมล์(mail security), ใช้ในการรักษาความปลอดภัยในระดับ ไอพี (IP Security), ใช้ในการรักษาความปลอดภัยทางเว็บ (web security) หรืออาจกล่าวว่า เมื่อต้องการพิสูจน์หรือยืนยันบุคคลหรือยืนยันเครื่องคอมพิวเตอร์แล้ว ก็มักจะอยู่ในขอบข่ายการทำงานของ PKI เสมอ

การทำงานของ PKI จะใช้การเข้ารหัสแบบพับลิคคีย์และใช้มาตรฐานลายเซ็นดิจิตอล สำหรับอัลกอริทึมนั้นไม่ได้ระบุแน่นอน โดยสามารถเลือกใช้ได้หลายตัว

ใบรับรอง (Certificate)

เนื่องจาก PKI นั้นจะเปรียบเสมือนกับโครงสร้างที่ทำหน้าที่เก็บใบรับรอง ซึ่งทำหน้าที่เป็นใบรับรองพับลิคคีย์ของแต่ละบุคคลหรือแต่ละเครื่อง ว่าเป็นพับลิคคีย์ที่ทำหน้าที่เป็นตัวแทนของบุคคลนั้นหรือเครื่องนั้นจริง โดยใบรับรองจะสร้างขึ้นโดย CA ที่เชื่อถือได้ รูปแบบทั่วไปของใบรับรอง จะแสดงในรูปที่ 4-6



รูปที่ 4-6 รูปแบบทั่วไปของใบรับรอง

4.2.2.1 ระบบการทรัสต์ของ CA

อย่างไรก็ตาม เนื่องจากระบบเครือข่ายในปัจจุบันมีขนาดกว้างขวางมาก ดังนั้นการที่ผู้ใช้ทุกคนจะมาใช้ CA เดียวกันก็เป็นเรื่องที่ยาก ดังนั้นหากผู้ใช้ 2 คนที่เป็นสมาชิกในคนละ CA กัน ก็จะไม่สามารถตรวจสอบ CA ของอีกฝ่ายว่าเป็นฉบับจริงหรือไม่ ซึ่งในกรณีเช่นนี้ก็อาจจะใช้วิธีก๊อบปี้พับลิคคีย์ของCA ของผู้ใช้อีกคนหนึ่งมาทำการตรวจสอบเองก็สามารถทำได้ แต่เราก็ไม่สามารถมั่นใจได้อีกว่าใบรับรองที่ได้รับมานั้นเป็นฉบับที่ถูกต้องหรือไม่

เช่นมี CA-A และ CB-B โดยให้บริการกับผู้ใช้ A และ B แต่เนื่องจากครั้งแรกที่ A ก๊อปปี้พับลิคคีย์ของ CA-B มานั้น อาจเกิดการปลอมได้ เพราะสิ่งที่เรามีอยู่คือพับลิคคีย์ ของ CA-A ของเรา แต่ใบรับรองของ CA-B ซึ่งบรรจุพับลิคคีย์ของ CA-B นั้นจะไซน์ด้วยไพรเวทคีย์ของ CA-B ทำให้เราไม่สามารถตรวจสอบว่าใบรับรองที่ได้รับมานั้นเป็นฉบับที่ถูกต้องหรือไม่ ดังนั้นวิธีดังกล่าวจึงถือว่ามีความปลอดภัยไม่เพียงพอ

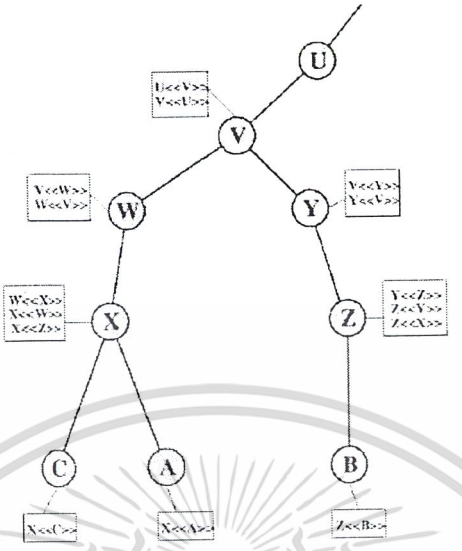
สำหรับวิธีการอีกแบบคือให้ CA-A เก็บใบรับรองของ CA-B เอาไว้ด้วย และ CA-B ก็เก็บใบรับรองของ CA-A เอาไว้เช่นกัน ด้วยวิธีนี้เราก็จะสามารถให้ CA ตรวจสอบใบรับรองได้ ไม่ว่าใบรับรองนั้นจะไซน์มาจาก CA-A หรือ CA-B ก็ตาม เช่น ผู้ใช้ A ต้องการตรวจสอบใบรับรองที่ไซน์โดย CA-A ก็สามารถทำได้เลยเพราะรู้พับลิคคีย์ ของ CA-A อยู่แล้วเนื่องจากเป็นสมาชิกของ CA-A และหากผู้ใช้ A ต้องการตรวจสอบใบรับรองที่ไซน์โดย CA-B ผู้ใช้ A ก็จะขอใบรับรองของ CA-B จาก CA-A โดยใบรับรองดังกล่าวจะไซน์โดย CA-A ดังนั้นจึงแน่ใจได้ว่าใบรับรองของ CA-B ที่ได้รับนั้นเป็นของจริงและพับลิคคีย์ของCA-B ก็เป็นของจริง จากนั้นจึงนำเอาพับลิคคีย์ของCA-B ไปตรวจสอบใบรับรองอีกที ก็จะทราบได้ว่าใบรับรองนั้นเป็นของจริงหรือไม่

และนอกเหนือจาก CA-A และ CA-B แล้ว การทำการทรัสต์กันเช่นนี้ยังสามารถกระทำกับ CAอื่นๆ ไปเรื่อยๆ อย่างไรก็ตามหาก CA มีจำนวนมากๆแล้ว ก็มีความจำเป็นที่จะต้องจัดโครงสร้างการทรัสต์กันของ CA ให้เป็นระบบ ไม่เช่นนั้นก็อาจมีการทรัสต์กันยุ่งเหยิง และทำให้การทำงานเป็นไปอย่างไม่มีประสิทธิภาพ

มาตรฐาน X.509 ก็ได้แนะนำให้มีการทรัสต์ CA ให้อยู่ในรูปความสัมพันธ์แบบระดับชั้น (Hierachical) ซึ่งรูปที่ 4-7 จะแสดงความสัมพันธ์แบบระดับชั้นของ CA ต่างๆ โดยส่วนที่เป็นวงกลมจะหมายถึงความสัมพันธ์ระหว่าง CA และในกล่องจะหมายถึงใบรับรองที่เก็บไว้ในไดเร็กทอรี ของแต่ละ CA โดย CA จะมีใบรับรอง 2 แบบ ได้แก่

- *Forward Certificates* หมายถึงใบรับรองของ X ที่สร้างโดย CA อื่นๆ
- *Reverse Certificates* หมายถึงใบรับรองที่สร้างโดย X ซึ่งก็จะกลายเป็น ใบรับรอง ของ CA อื่นๆด้วย เช่น ตัวอย่าง ผู้ใช้ A ได้ขอใบรับรองจาก CA-B จะได้ Certificate Path ดังนี้

X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>>

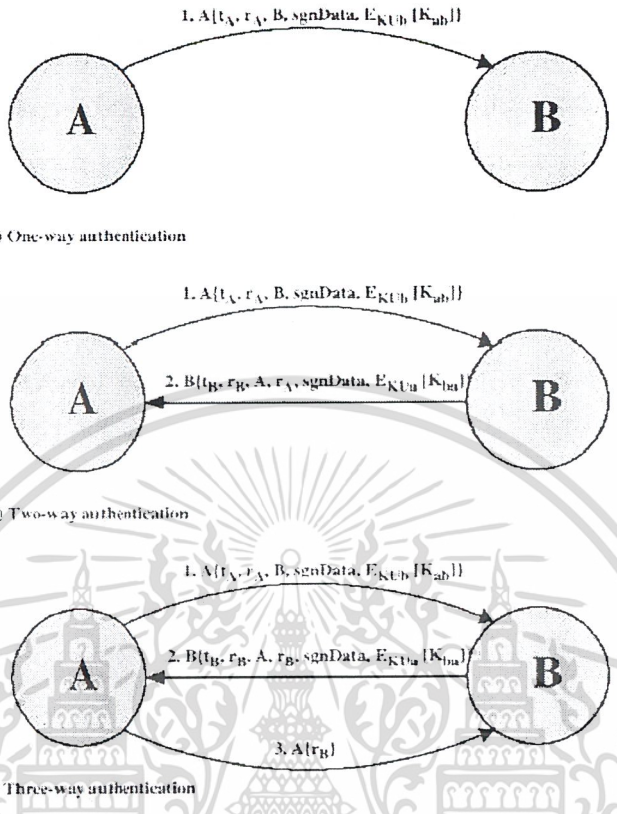


รูปที่ 4-7 การทรัสต์ของ CA ตามความสัมพันธ์ระดับชั้น

4.2.2.2 วิธีการพิสูจน์ตน (Authentication Procedure) ใน มาตรฐานX.509

ใน PKI ได้ให้วิธีการพิสูจน์ตนเอาไว้ 3 วิธีด้วยกัน ดังแสดงในรูปที่4-8 โดยในขั้นแรกจะถือว่าทั้ง 2 ฝ่าย ได้รับพับลิคคีย์มาอย่างถูกต้องและมีการตรวจสอบพับลิคคีย์เรียบร้อยแล้ว โดยวิธีแรกจะเรียกว่า

1. **การพิสูจน์ตนทางเดียว (One-way authentication)** โดยจะใช้ในกรณีที่มีการส่งข้อมูลจากผู้ใช้คนหนึ่งไปยังผู้ใช้อีกคนหนึ่งในทิศทางเดียว เช่น ในรูปจะเป็นการส่งจาก A ไป B ก็จะเป็นการยืนยันว่าข้อมูลที่ส่งเป็นการส่งจาก A จริงๆ ใช้สำหรับการพิสูจน์ความเป็นต้นฉบับ โดย tA จะเป็น ไทม์แสตมป์ และ rA จะเป็นข้อมูลสุ่ม(Nonce) และมีการระบุว่าส่งให้ B โดยมีการไซน์ข้อมูลด้วยไพรเวทคีย์ของ A
2. **การพิสูจน์ตนสองทาง (Two-way authentication)** โดยจะมีการใช้งานในกรณีที่มีข้อมูลรับส่งสองทาง โดยการทำงานก็จะเป็นเช่นเดียวกับการพิสูจน์ตนทางเดียว แต่จะเป็นการทำงานย้อนกลับทางกัน
3. **การพิสูจน์ตนสามทาง (Three-way authentication)** จะเหมือนกับการการพิสูจน์ตนสองทาง แต่จะเพิ่มการตอบกลับไปอีกทีว่าได้รับข้อมูลแล้ว

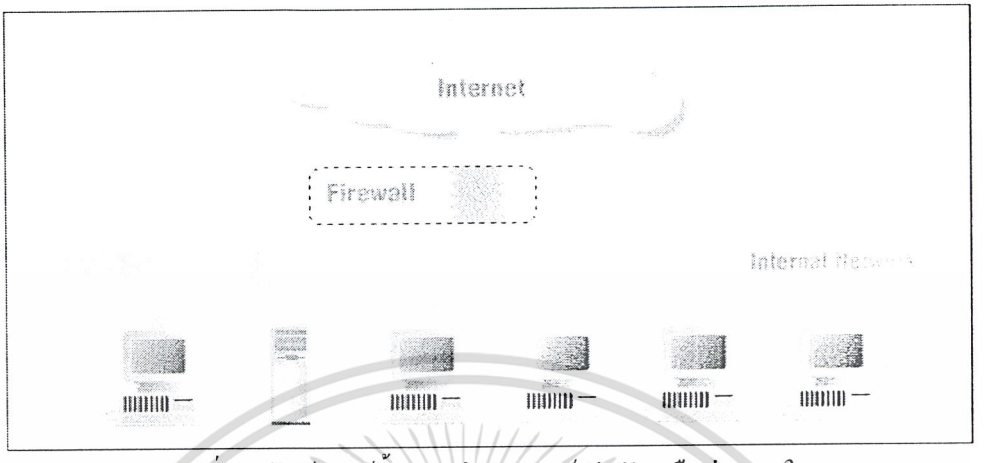


รูปที่ 4-8 กระบวนการพิสูจน์ตนของ PKI

4.3 ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์หมายถึงกำแพงที่เอาไว้ป้องกันไฟไม่ให้ลุกลามไปยังส่วนอื่นๆ ส่วนทางด้านคอมพิวเตอร์นั้นก็จะมีความหมายคล้ายๆกันก็คือ เป็นระบบที่เอาไว้ป้องกันอันตรายจากอินเตอร์เน็ตหรือเครือข่ายภายนอกนั่นเอง

ไฟร์วอลล์เป็นคอมโพเน็นต์หรือกลุ่มของคอมโพเน็นต์ที่ทำหน้าที่ในการควบคุมการเข้าถึงระหว่างเครือข่ายภายนอกหรือเครือข่ายที่เราคิดว่าไม่ปลอดภัยกับเครือข่ายภายในหรือเครือข่ายที่เราต้องการจะป้องกัน โดยที่คอมโพเน็นต์นั้นอาจจะเป็นเราเตอร์, คอมพิวเตอร์,หรือเครือข่ายประกอบกันก็ได้ ขึ้นอยู่สถาปัตยกรรมของไฟร์วอลล์ รูปที่4-9 จะแสดงการใช้ไฟร์วอลล์กั้นระหว่างอินเตอร์เน็ตกับเครือข่ายภายใน



รูปที่ 4-9 ไฟร์วอลล์กั้นระหว่างอินเตอร์เน็ตกับเครือข่ายภายใน

การควบคุมการเข้าถึงของไฟร์วอลล์นั้น สามารถทำได้ในหลายระดับและหลายรูปแบบขึ้นอยู่ชนิดหรือเทคโนโลยีของไฟร์วอลล์ที่นำมาใช้ เช่น เราสามารถกำหนดได้ว่าจะให้มีการเข้ามาใช้เซอร์วิสอะไรได้บ้าง จากที่ไหน เป็นต้น

4.3.1 สิ่งที่ไฟร์วอลล์ช่วยได้

ไฟร์วอลล์สามารถช่วยเพิ่มความปลอดภัยให้กับระบบได้โดย

- บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตให้ใช้หรือไม่ให้ใช้เซอร์วิสชนิดใด
- ทำให้การพิจารณาดูแลและการตัดสินใจด้านความปลอดภัยของระบบเป็นไปได้ง่ายขึ้น เนื่องจากการติดต่อทุกชนิดกับเครือข่ายภายนอกจะต้องผ่านไฟร์วอลล์ การดูแลที่จุดนี้เป็นการดูแลความปลอดภัยในระดับของเครือข่าย (Network-based Security)
- บันทึกข้อมูล กิจกรรมต่างๆที่ผ่านเข้าออกเครือข่ายได้อย่างมีประสิทธิภาพ
- ป้องกันเครือข่ายบางส่วนจากการเข้าถึงของเครือข่ายภายนอก เช่นถ้าหากเรามีบางส่วนที่ต้องการให้ภายนอกเข้ามาใช้เซอร์วิส(เช่น ถ้ามีเว็บเซิร์ฟเวอร์) แต่ส่วนที่เหลือไม่ต้องการให้ภายนอกเข้ามา กรณีเช่นนี้เราสามารถใช้ไฟร์วอลล์ช่วยได้
- ไฟร์วอลล์บางชนิดสามารถป้องกันไวรัสได้ โดยจะทำการตรวจไฟล์ที่โอนย้ายผ่านทางโพรโตคอล HTTP, FTP และ SMTP

4.3.2 สิ่งที่ไฟร์วอลล์ช่วยไม่ได้

ถึงแม้ว่าไฟร์วอลล์จะสามารถช่วยเพิ่มความปลอดภัยให้กับเครือข่ายได้มากโดยการตรวจดูข้อมูลที่ผ่านเข้าออก แต่อย่าลืมว่าสิ่งเหล่านี้ไม่สามารถป้องกันได้จากการใช้ไฟร์วอลล์

- อันตรายที่เกิดจากเครือข่ายภายใน ไม่สามารถป้องกันได้เนื่องจากอยู่ภายในเครือข่ายเอง ไม่ได้ผ่านไฟร์วอลล์เข้ามา
- อันตรายจากภายนอกที่ไม่ได้ผ่านเข้ามาทางไฟร์วอลล์ เช่นการไดอัล-อัพ (Dial-up) เข้ามายังเครือข่ายภายในโดยตรงโดยไม่ได้ผ่านไฟร์วอลล์
- อันตรายจากวิธีใหม่ๆที่เกิดขึ้น ทุกวันนี้มีการพบช่องโหว่ใหม่ๆเกิดขึ้นทุกวัน เราไม่สามารถไว้ใจไฟร์วอลล์โดยการติดตั้งเพียงครั้งเดียวแล้วก็หวังให้มันปลอดภัยตลอดไป เราต้องมีการดูแลรักษาอย่างต่อเนื่องสม่ำเสมอ
- ไวรัส ถึงแม้จะมีไฟร์วอลล์บางชนิดที่สามารถป้องกันไวรัสได้ แต่ก็ยังไม่มีไฟร์วอลล์ชนิดใดที่สามารถตรวจสอบไวรัสได้ในทุกๆโพรโตคอล

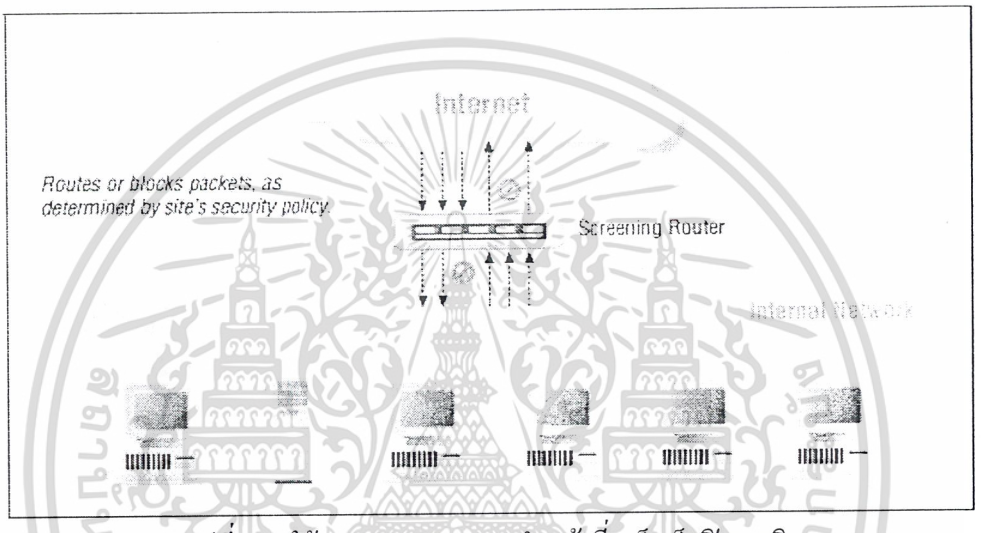
4.3.3 ชนิดของไฟร์วอลล์

ชนิดของไฟร์วอลล์แบ่งตามเทคโนโลยีที่ใช้ในการตรวจสอบและควบคุม แบ่งได้เป็น

- แพ็กเก็ตฟิลเตอริง (Packet Filtering)
- พร็อกซี (Proxy)
- สเตตฟูลอินสเปกชัน (Stateful Inspection)

4.3.3.1 แพ็กเก็ตฟิลเตอริง

แพ็กเก็ตฟิลเตอ คือเราเตอร์ที่ทำการหาเส้นทางและส่งต่อ (route) อย่างมีเงื่อนไข โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามาเทียบกับกฎ(rules) ที่กำหนดไว้และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้ ในรูปที่ 4-10 จะแสดงการใช้ Screening Router ทำหน้าที่แพ็กเก็ตฟิลเตอริง



รูปที่ 4-10 ใช้ Screening Router ทำหน้าที่ แพ็กเก็ตฟิลเตอริง

ในการพิจารณาเฮดเดอร์ แพ็กเก็ตฟิลเตอจะตรวจสอบในระดับของอินเตอร์เน็ตเลเยอร์ (Internet Layer) และทรานสปอร์ตเลเยอร์ (Transport Layer) ในอินเตอร์เน็ตโมเดล ซึ่งในอินเตอร์เน็ตเลเยอร์จะมีแอตทริบิวต์ที่สำคัญต่อ แพ็กเก็ตฟิลเตอริง ดังนี้

- ไอพีต้นทาง
- ไอพีปลายทาง
- ชนิดของโพรโตคอล (TCP, UDP และ ICMP)

และในระดับของทรานสปอร์ตเลเยอร์ มีแอตทริบิวต์ที่สำคัญคือ

- พอร์ตต้นทาง
- พอร์ตปลายทาง
- แฟล็ก (มีเฉพาะในเฮดเดอร์ของแพ็กเก็ตTCP)
- ชนิดของ ICMP message (ในแพ็กเก็ต ICMP)

พอร์ตของทรานสปอร์ตเลเยอร์คือทั้ง TCP และ UDP นั้นจะเป็นสิ่งที่บอกถึงแอพพลิเคชันที่แพ็กเก็ตนั้นต้องการติดต่อด้วยเช่น พอร์ต 80 หมายถึง HTTP,พอร์ต 21 หมายถึง FTP เป็นต้น ดังนั้นเมื่อแพ็กเก็ตฟิลเตอพิจารณาเฮดเดอร์ จะทำให้สามารถควบคุมแพ็กเก็ตที่มาจากที่ต่างๆ และมีลักษณะต่างๆ (ดูได้จากแฟล็กของแพ็กเก็ตหรือชนิดของ ICMP ในแพ็กเก็ต ICMP) ได้ เช่น ห้ามแพ็กเก็ตทุกชนิดจาก crack.cracker.net เข้ามายังเครือข่าย 192.168.0.0/24 , ห้ามแพ็กเก็ตที่มีไอพีต้นทางอยู่ในเครือข่าย 192.168.0.0/24 (โดยสมมติว่าเป็นเครือข่ายของเรา) ผ่านเราเตอร์เข้ามา (ในกรณีนี้เพื่อเป็นการป้องกัน ip spoofing) เป็นต้น

แพ็กเก็ตฟิลเตอริง สามารถอิมพลีเมนต์ได้จาก 2 แพลี็ตฟอร์ม คือ

- เราเตอร์ที่มีความสามารถในการทำ แพ็กเก็ตฟิลเตอริง(ซึ่งมีในเราเตอร์ส่วนใหญ่อยู่แล้ว)
- คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์

ซึ่งจะมีข้อได้เปรียบเสียเปรียบกันดังนี้

	ข้อดี	ข้อเสีย
เราเตอร์	ประสิทธิภาพสูง มีจำนวนอินเตอร์เฟสมาก	เพิ่มเติมฟังก์ชันการทำงานได้ยาก, อาจต้องการหน่วยความจำมาก
คอมพิวเตอร์ที่ทำหน้าที่เป็นเราเตอร์	เพิ่มฟังก์ชันการทำงานได้ไม่จำกัด	ประสิทธิภาพปานกลาง, จำนวนอินเตอร์เฟสน้อย, อาจมีความเสี่ยงจากระบบปฏิบัติการที่ใช้

ตารางที่ 4-1 เปรียบเทียบข้อดีข้อเสียในการเลือกอุปกรณ์มาทำหน้าที่ แพ็กเก็ตฟิลเตอริง

ข้อดี-ข้อเสียของ แพ็กเก็ตฟิลเตอริง

ข้อดี

- ไม่ขึ้นกับแอพพลิเคชัน
- มีความเร็วสูง
- รองรับการขยายตัวได้ดี

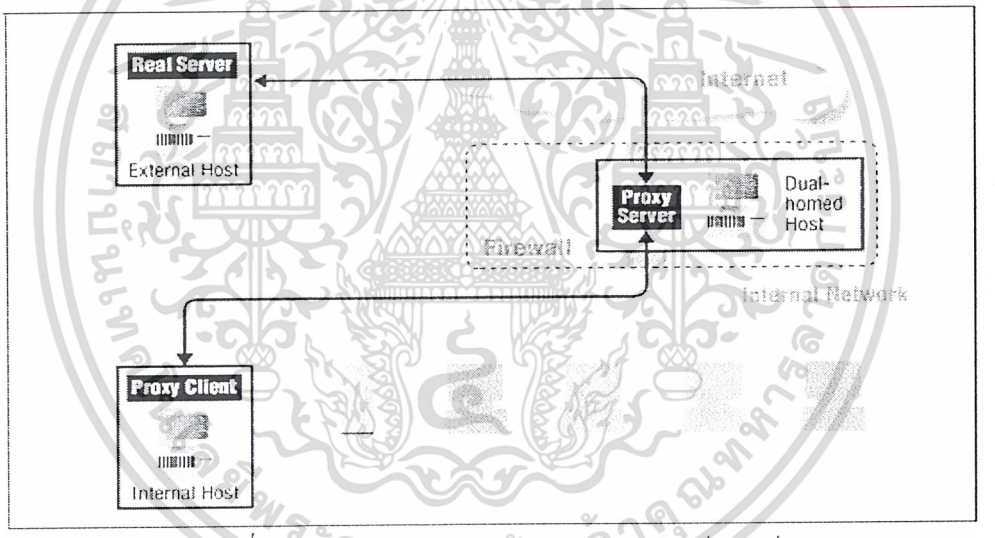
ข้อเสีย

- บางโพรโตคอลไม่เหมาะสมกับการใช้แพ็กเก็ตฟิลเตอริง เช่น FTP, ICQ

4.3.3.2 พร็อกซี

พร็อกซี หรือแอพพลิเคชันเกตเวย์ (Application Gateway) เป็นแอพพลิเคชันโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเครือข่าย 2 เครือข่าย ทำหน้าที่เพิ่มความปลอดภัยของระบบเครือข่ายโดยการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายในและภายนอก แอพพลิเคชันพร็อกซีจะช่วยเพิ่มความปลอดภัยได้มาก เนื่องจากมีการตรวจสอบข้อมูลถึงในระดับของแอพพลิเคชันเลเยอร์(Application Layer)

เมื่อไคลเอนต์ต้องการใช้เซอร์วิสภายนอก ไคลเอนต์จะทำการติดต่อไปยังพร็อกซีก่อน ไคลเอนต์จะเจรจา(negotiate)กับพร็อกซี เพื่อให้พร็อกซีติดต่อไปยังเครื่องปลายทางให้ เมื่อพร็อกซีติดต่อไปยังเครื่องปลายทางให้แล้วจะมีการเชื่อมต่อ(connection) 2การเชื่อมต่อ คือ ไคลเอนต์กับพร็อกซี และพร็อกซีกับเครื่องปลายทาง โดยที่พร็อกซีจะทำหน้าที่รับข้อมูลและส่งต่อข้อมูลให้ใน 2ทิศทาง ทั้งนี้พร็อกซีจะทำหน้าที่ในการตัดสินใจว่าจะให้มีการเชื่อมต่อกันหรือไม่ จะส่งต่อแพ็กเก็ตให้หรือไม่



รูปที่ 4-11 ใช้ Dual-homed Host เป็นพร็อกซีเซิร์ฟเวอร์

ข้อดี-ข้อเสียของ พร็อกซี

ข้อดี

- มีความปลอดภัยสูง
- รู้จักข้อมูลในระดับแอพพลิเคชัน

ข้อเสีย

- ประสิทธิภาพต่ำ
- แต่ละบริการมักจะต้องการโปรเซสของตนเอง
- สามารถขยายตัวได้ยาก

4.3.3.3 สเตตฟูลอินสเป็กชัน

โดยปกติแล้วแพ็กเก็ตฟิลเตอริงแบบธรรมดา(ที่เป็น Stateless แบบที่มีอยู่ในเราเตอร์ทั่วไป) จะควบคุมการเข้าออกของแพ็กเก็ตโดยพิจารณาข้อมูลจากเฮดเดอร์ของแต่ละแพ็กเก็ต นำมาเทียบกับกฎที่มีอยู่ ซึ่งกฎที่มีอยู่ก็จะเป็นกฎที่สร้างจากข้อมูลส่วนที่อยู่ในเฮดเดอร์เท่านั้น ดังนั้นแพ็กเก็ตฟิลเตอริงแบบธรรมดาจึงไม่สามารถทราบได้ว่า แพ็กเก็ตนี้อยู่ส่วนใดของการเชื่อมต่อ เป็นแพ็กเก็ตที่เข้ามาติดต่อใหม่หรือเปล่า หรือว่าเป็นแพ็กเก็ตที่เป็นส่วนของการเชื่อมต่อที่เกิดขึ้นแล้ว เป็นต้น

สเตตฟูลอินสเป็กชันเป็นเทคโนโลยีที่เพิ่มเข้าไปในแพ็กเก็ตฟิลเตอริง โดยในการพิจารณาว่าจะยอมให้แพ็กเก็ตผ่านไปนั้น แทนที่จะดูข้อมูลจากเฮดเดอร์เพียงอย่างเดียว สเตตฟูลอินสเป็กชันจะนำเอาส่วนข้อมูลของแพ็กเก็ต(message content) และข้อมูลที่ได้จากแพ็กเก็ตก่อนหน้านี้ที่ได้ทำการบันทึกเอาไว้นำมาพิจารณาด้วย จึงทำให้สามารถระบุได้ว่าแพ็กเก็ตใดเป็นแพ็กเก็ตที่ติดต่อเข้ามาใหม่ หรือว่าเป็นส่วนหนึ่งของการเชื่อมต่อที่มีอยู่แล้ว

ตัวอย่างผลิตภัณฑ์ทางการค้าที่ใช้ สเตตฟูลอินสเป็กชัน ได้แก่

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

และส่วนผลิตภัณฑ์ที่ให้ใช้ฟรี ได้แก่

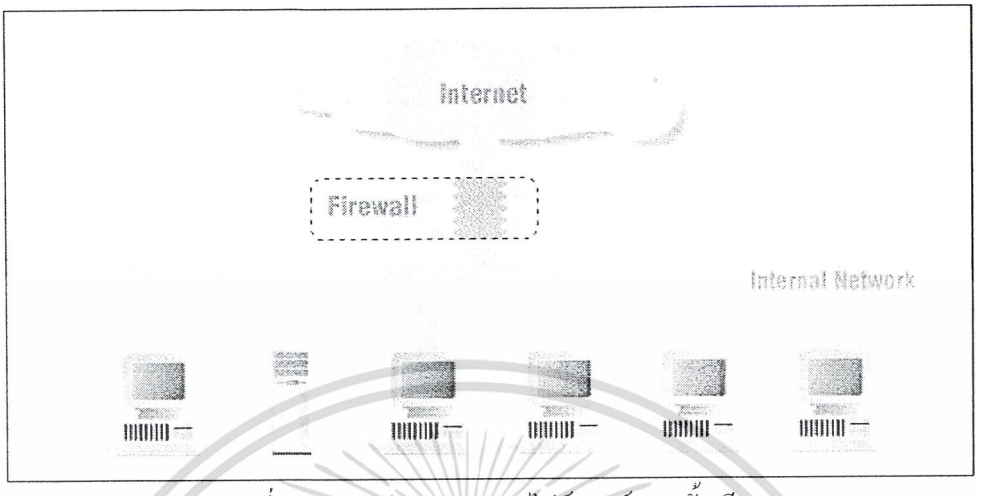
- NetFilter ใน Linux (iptables ในลีนุกซ์เคอร์เนล 2.3เป็นต้นไป)

4.3.4 สถาปัตยกรรมของไฟร์วอลล์ (Firewall Architecture)

ในส่วนของสถาปัตยกรรมของไฟร์วอลล์นั้น จะพูดถึงการจัดวางไฟร์วอลล์คอมโพเน็นต์ในแบบต่างๆเพื่อทำให้เกิดเป็นระบบไฟร์วอลล์ขึ้น

4.3.4.1 สถาปัตยกรรมของไฟร์วอลล์แบบชั้นเดียว (Single Box Architecture)

สถาปัตยกรรมของไฟร์วอลล์แบบชั้นเดียวเป็นสถาปัตยกรรมแบบง่ายๆ ที่มีคอมโพเน็นต์ทำหน้าที่เป็นไฟร์วอลล์เพียงอันเดียวตั้งอยู่ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก ข้อดีของวิธีนี้ก็คือการที่มีเพียงจุดเดียวที่หน้าที่ไฟร์วอลล์ทั้งหมด ควบคุมการเข้าออกของข้อมูล ทำให้ดูแลได้ง่ายเป็นจุดสนใจในการดูแลความปลอดภัยเครือข่าย ในทางกลับกันข้อเสียของวิธีนี้ก็คือการที่มีเพียงจุดเดียวนี้ทำให้มีความเสี่ยงสูง หากมีการคอนฟิกูเรชันผิดพลาดหรือมีช่องโหว่เพียงเล็กน้อย การผิดพลาดเพียงจุดเดียวอาจทำให้ระบบถูกเจาะได้



รูปที่ 4-12 สถาปัตยกรรมของไฟร์วอลล์แบบชั้นเดียว

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

1. Screening Router

เราสามารถใช้เราเตอร์ทำแพ็กเก็ตฟิลเตอริงได้ วิธีนี้จะทำให้ประหยัดค่าใช้จ่ายเนื่องจากส่วนใหญ่จะใช้เราเตอร์ต่อกับเครือข่ายภายนอกอยู่แล้ว แต่วิธีนี้อาจไม่ยืดหยุ่นมากนักในการคอนฟิก

สถาปัตยกรรมแบบนี้เหมาะสำหรับ

- เครือข่ายที่มีการป้องกันความปลอดภัยในระดับของโฮสต์ (Host security) เป็นอย่างดีแล้ว
- มีการใช้โพรโตคอลไม่มาก และโพรโตคอลที่ใช้ก็เป็นโพรโตคอลที่ไม่ซับซ้อน
- ต้องการไฟร์วอลล์ที่มีความเร็วสูง

2. Dual-Homed Host

เราสามารถใช้ Dual-Homed Host (คอมพิวเตอร์ที่มีเครือข่ายอินเตอร์เฟสอย่างน้อย 2 อัน) ในการบริการเป็นพร็อกซีให้กับเครื่องภายในเครือข่าย

สถาปัตยกรรม แบบนี้เหมาะสำหรับ

- เครือข่ายที่มีการใช้งานอินเตอร์เน็ตค่อนค่างน้อย
- เครือข่ายที่ไม่ได้มีข้อมูลสำคัญๆ

3. Multi-purposed Firewall Box

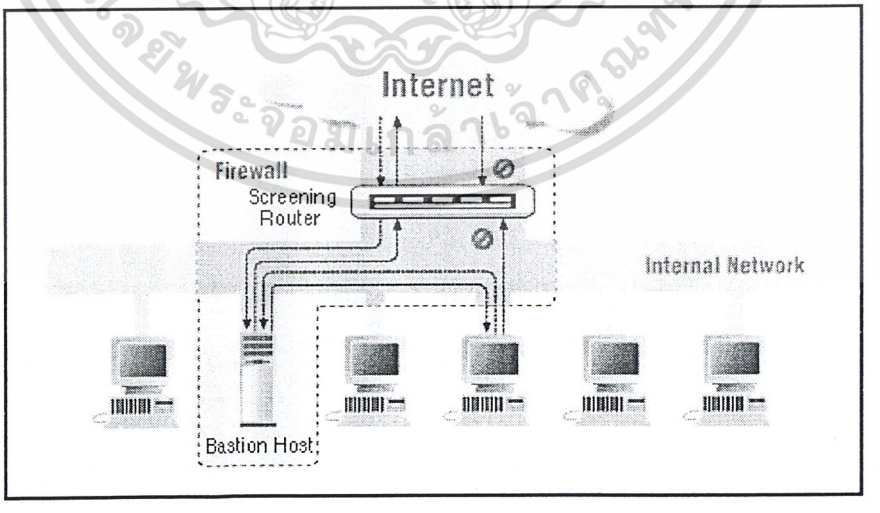
มีผลิตภัณฑ์หลายชนิดที่ผลิตออกมาเป็นกล่องๆเดียว ซึ่งทำหน้าที่ได้หลายอย่าง ทั้งแพ็กเก็ตฟิลเตอริง, พร็อกซี แต่ก็อย่าลืมว่านี่คือสถาปัตยกรรมแบบชั้นเดียว ซึ่งถ้าพลาดแล้วก็จะเสียหายทั้งเครือข่ายได้

4. Screened Host Architecture

Screened Host Architecture จะมีโฮสต์ซึ่งให้บริการพร็อกซีเหมือนกับใน Single Box Architecture ที่เป็น Dual-homed Host แต่จะต่างกันตรงที่ว่าโฮสต์นั้นจะอยู่ภายในเครือข่ายไม่ต่ออยู่กับเครือข่ายภายนอกอื่นๆ (ดังนั้นก็ไม่จำเป็นที่จะต้องใช้Dual Homed Host) และจะมีเราเตอร์ที่ทำหน้าที่แพ็กเก็ตฟิลเตอริง ช่วยบังคับให้เครื่องภายในเครือข่ายต้องติดต่อเซอร์วิสผ่านพร็อกซีโดยไม่ยอมให้ติดต่อใช้เซอร์วิสจากภายนอกโดยตรง และก็ให้ภายนอกเข้าถึงได้เฉพาะแบสชั่นโฮสต์เท่านั้น (แบสชั่นโฮสต์คือโฮสต์ที่มีความเสี่ยงสูงต่อการถูกโจมตี มักจะเป็นโฮสต์ที่เปิดให้บริการกับอินเตอร์เน็ต ดังนั้นโฮสต์นี้ต้องมีการดูแลเป็นพิเศษ)

จากรูปที่ 4-13 ในสถาปัตยกรรมแบบนี้จะประกอบไปด้วยเราเตอร์ทำหน้าที่แพ็กเก็ตฟิลเตอริง และภายในเครือข่ายจะมีแบสชั่นโฮสต์ให้บริการพร็อกซีอยู่ โดยที่เราเตอร์นั้นอาจจะถูกเซ็ตดังนี้

- อาจจะอนุญาตให้เครื่องภายในใช้เซอร์วิสบางอย่างได้โดยตรง
- ส่วนเซอร์วิสอื่นๆ จะไม่ยอมให้เครื่องภายในติดต่อผ่านออกไปโดยตรง ยกเว้นแบสชั่นโฮสต์เท่านั้นที่สามารถติดต่อกับเครือข่ายภายนอกได้ ทั้งนี้เพื่อเป็นการบังคับให้ใช้บริการพร็อกซีผ่านทางแบสชั่นโฮสต์เท่านั้น
- หรืออาจจะเซ็ตให้เซอร์วิสส่วนใหญ่ผ่านเราเตอร์ออกไปได้โดยตรงแล้ว ให้บางส่วนต้องใช้เซอร์วิสผ่านพร็อกซีก็แล้วแต่นโยบายและความเหมาะสมขององค์กร



รูปที่ 4-13 Screened Host Architecture

วิธีนี้ถึงแม้ว่าจะมีทั้งพร็อกซีและเราเตอร์ทำหน้าที่แพ็กเก็ตฟิลเตอริงแต่ก็ยังคงอันตรายอยู่ เพราะว่าเราเตอร์ต้องยอมให้ภายนอกสามารถติดต่อกับแบสชั่นโฮสต์ได้อยู่แล้ว หากแฮกเกอร์สามารถเจาะเข้ามายังแบสชั่นโฮสต์ได้ก็เสร็จ

สถาปัตยกรรม นี้เหมาะสำหรับ

- เครือข่ายที่มีการติดต่อกับเครือข่ายภายนอกน้อย
- เครือข่ายที่มีการป้องกันความปลอดภัยในระดับของโฮสต์เป็นอย่างดีแล้ว

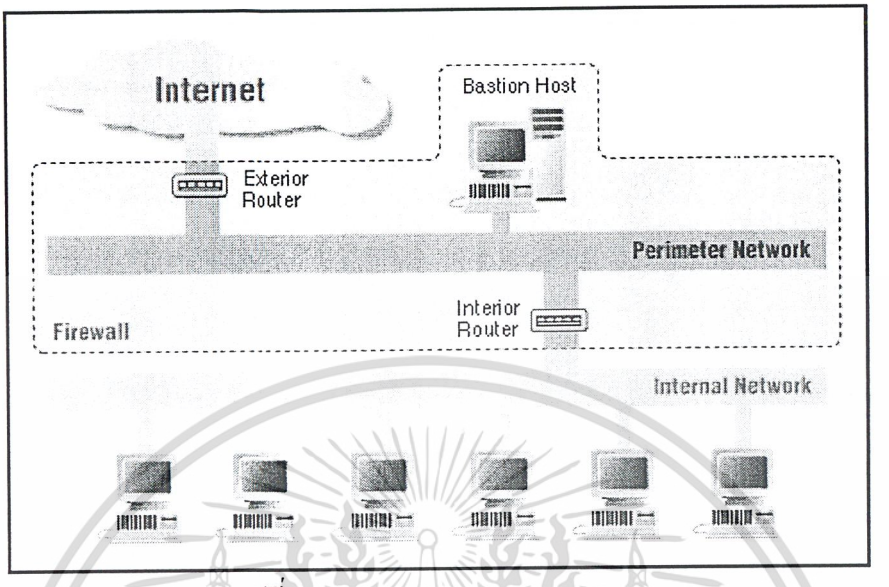
4.3.4.2 สถาปัตยกรรมของไฟร์วอลล์แบบหลายชั้น (Multi Layer Architecture)

ในสถาปัตยกรรมแบบหลายชั้น ไฟร์วอลล์จะเกิดขึ้นจากคอมโพเน็นต์หลายๆส่วนมาทำหน้าที่ประกอบกันขึ้นเป็นระบบ วิธีการนี้สามารถเพิ่มความปลอดภัยได้มาก เนื่องจากเป็นการลดความเสี่ยงต่อความผิดพลาดที่อาจเกิดขึ้น ถ้าหากมีไฟร์วอลล์เพียงจุดเดียวแล้วมีเกิดความผิดพลาดเกิดขึ้น ระบบทั้งหมดก็จะเป็นอันตราย แต่ถ้ามีการป้องกันหลายชั้น หากในชั้นแรกถูกเจาะก็อาจจะมีความเสียหายเพียงบางส่วน ส่วนที่เหลือระบบก็ยังคงมีชั้นอื่นๆ ในการป้องกันอันตราย และยังลดความเสี่ยงได้โดยการที่แต่ละชั้นนั้นมีการใช้เทคโนโลยีที่แตกต่างกันเพื่อให้เกิดความหลากหลาย เป็นการหลีกเลี่ยงการโจมตีหรือช่องโหว่ที่อาจมีในเทคโนโลยีชนิดใดชนิดหนึ่ง โดยทั่วไปแล้วสถาปัตยกรรมแบบหลายชั้นจะเป็นการต่อกันเป็นซีรี โดยมีเพอริมิเตอร์เน็ตเวิร์ก (Perimeter Network หรือบางทีเรียกว่า DMZ Network) อยู่ตรงกลาง เรียกว่า Screened Subnet Architecture

Screened Subnet Architecture

Screened Subnet Architecture เป็นสถาปัตยกรรมที่มีการเพิ่มเพอริมิเตอร์เน็ตเวิร์กเข้าไปกั้นระหว่างอินเตอร์เน็ตกับเครือข่ายภายในไม่ให้เชื่อมต่อกันโดยตรง ทำให้เครือข่ายภายในมีความปลอดภัยมากขึ้น

ในรูปที่ 4-14 แสดง Screened Subnet Architecture อย่างง่าย โดยประกอบไปด้วยเราเตอร์ 2 ตัว ตัวนึงอยู่ระหว่างอินเตอร์เน็ตกับเพอริมิเตอร์เน็ตเวิร์ก ส่วนอีกตัวหนึ่งอยู่ระหว่างเพอริมิเตอร์เน็ตเวิร์กกับเครือข่ายภายใน ถ้าหากแฮกเกอร์จะเจาะเครือข่ายภายในต้องผ่านเราเตอร์เข้ามาถึง2 ตัวด้วยกัน ถึงแม้ว่าจะเจาะชั้นแรกเข้ามายังแบสชั่นโฮสต์ได้ แต่ก็ยังต้องผ่านเราเตอร์ตัวในอีก ถึงจะเข้ามายังเครือข่ายภายในได้



รูปที่4-14 Screened Subnet Architecture

คอมโพเน็นต์ของ Screened Subnet Architecture ในรูปที่ 4-14

- เพอริมิเตอร์เน็ตเวิร์กเป็นเครือข่ายที่เพิ่มเข้ามาเพื่อความปลอดภัย โดยตั้งอยู่ระหว่างเครือข่ายภายนอกกับเครือข่ายภายใน ประโยชน์ของเพอริมิเตอร์เน็ตเวิร์กที่เห็นได้ชัดก็คือ การแบ่งเครือข่ายออกเป็นส่วนๆ ทำให้การไหลของข้อมูลถูกแบ่งออกเป็นส่วนๆตามเครือข่ายด้วย เนื่องจากโดยทั่วไปแล้วเครือข่ายที่เป็นแลนนั้นจะเป็นแบบอีเทอร์เน็ตซึ่งจะมีการส่งข้อมูลแบบบรอดคาสท์ (Broadcast)ดังนั้นถ้ามีใครคอยดักจับข้อมูลอยู่ในเครือข่ายนั้นก็จะได้พาสเวิร์ดและข้อมูลต่างๆไปหมด ดังนั้นหากไฟร์วอลล์เรามีชั้นเดียวและแฮกเกอร์สามารถเข้ามาทำการดักจับข้อมูล ก็จะได้ข้อมูลไปทั้งหมด แต่ถ้าเรามีเพอริมิเตอร์เน็ตเวิร์ก ถึงจะดักจับข้อมูลได้แต่ก็จะได้เพียงที่อยู่บนเพอริมิเตอร์เน็ตเวิร์กเท่านั้น

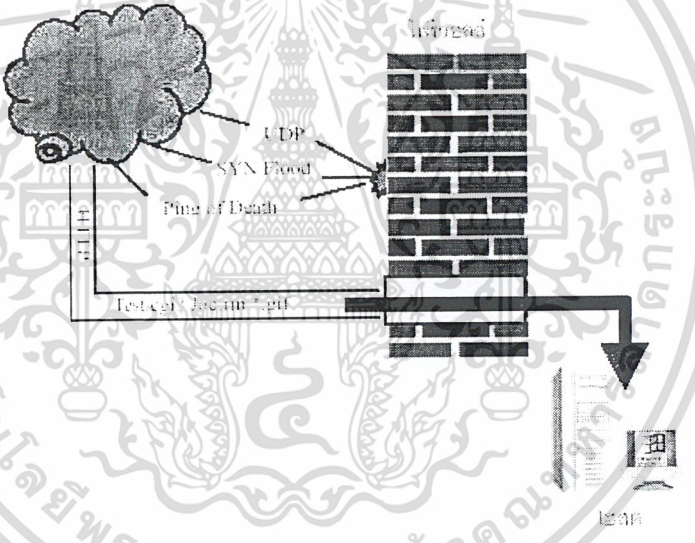
- แบสชันโฮสต์ตั้งอยู่บนเพอริมิเตอร์เน็ตเวิร์ก ทำหน้าที่ให้บริการพร็อกซีกับเครือข่ายภายในและให้บริการต่างๆกับผู้ใช้บนอินเตอร์เน็ต โดยแบสชั่นโฮสต์นั้นจะมีความเสี่ยงต่อการโจมตีสูง จึงต้องมีการดูแลความปลอดภัยเป็นพิเศษ

- เราท์เตอร์ภายใน (Interior Router) ตั้งอยู่ระหว่างเพอริมิเตอร์เน็ตเวิร์กกับเครือข่ายภายใน ทำหน้าที่แพ็กเก็ตฟิลเตอริงป้องกันเครือข่ายภายในจากเพอริมิเตอร์เน็ตเวิร์ก ในการเซ็ตคอนฟิกูเรชันระหว่างเครือข่ายภายในกับเพอริมิเตอร์เน็ตเวิร์กต้องมีการกำหนดอย่างรอบคอบ อนุญาตเฉพาะเซอร์วิสที่จำเป็นเท่านั้นอย่างเช่น DNS, SMTP

- เราท์เตอร์ภายนอก (Exterior Router) ตั้งอยู่ระหว่างเครือข่ายภายนอกกับเพอริมิเตอร์เน็ตเวิร์ก เนื่องจากเราท์เตอร์ภายนอกนี้เป็นจุดที่ต่ออยู่กับเครือข่ายภายนอก จึงมีหน้าที่ที่สำคัญอย่างหนึ่งคือ การป้องกันแพ็กเก็ตที่มีการปลอมไอพีแอดเดรสเข้ามา โดยอ้างว่ามาจากเครือข่ายภายในทั้งๆที่จริงๆแล้วมาจากเครือข่ายภายนอก

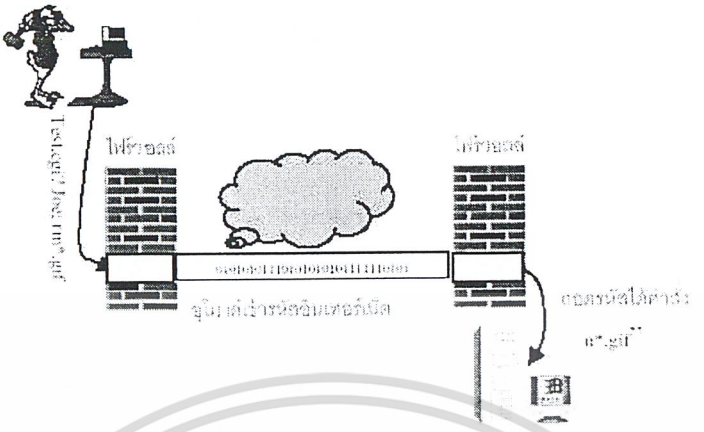
4.3.5 ปัญหาของไฟร์วอลล์

- ไฟร์วอลล์ไม่สามารถป้องการบุกรุกที่อาศัยช่องโหว่ของแอพพลิเคชันได้ดังแสดงในรูปที่ 4-15 พบว่าไฟร์วอลล์กรองแพ็กเก็ตตามที่ถูกระบุไว้สามารป้องกันการส่งSYN เป็นจำนวนมาก (SYN Flood) ได้ แต่ยอมให้แพ็กเก็ตของ HTTP ผ่าน ทำให้สามารถส่งไฟล์ใดๆ ที่มีนามสกุล cgi เข้ามาในระบบได้ เช่นในตัวอย่าง ผู้บุกรุกส่งไฟล์ชื่อ test.cgiเข้ามาในระบบเพื่อลบไฟล์ทั้งหมดที่มีนามสกุล gif ในเว็บเซิร์ฟเวอร์ซึ่งทำให้โฮมเพจในนั้นเสียหาย



รูปที่ 4-15 การบุกรุกระบบโดยอาศัยจุดอ่อนของแอพพลิเคชัน

- ไฟร์วอลล์กรองแพ็กเก็ตต่างๆ โดยพิจารณาจากโพรโตคอลในชั้นเน็ตเวิร์ก ถ้าข้อมูลที่ผู้บุกรุกส่งมามีรูปแบบถูกต้องตามโพรโตคอล ไฟร์วอลล์จะยอมให้แพ็กเก็ตนั้นผ่านเข้ามาได้ ซึ่งผู้บุกรุกสามารถซ่อนข้อมูลใด ๆ เข้ามาดังแสดงในรูปที่ 4-16ผู้บุกรุกส่ง test.cgi?Joe;rm *.gif ผ่านอุโมงค์การเข้ารหัสในอินเตอร์เน็ตโพรโตคอล ทำให้แพ็กเก็ตนี้สามารถผ่านไฟร์วอลล์ได้ เมื่อถอดรหัสแล้วได้คำสั่ง “rm *.gif“ แก่เซิร์ฟเวอร์ ทำให้ไฟล์รูปภาพที่มีนามสกุล gif ถูกลบออกจากระบบ

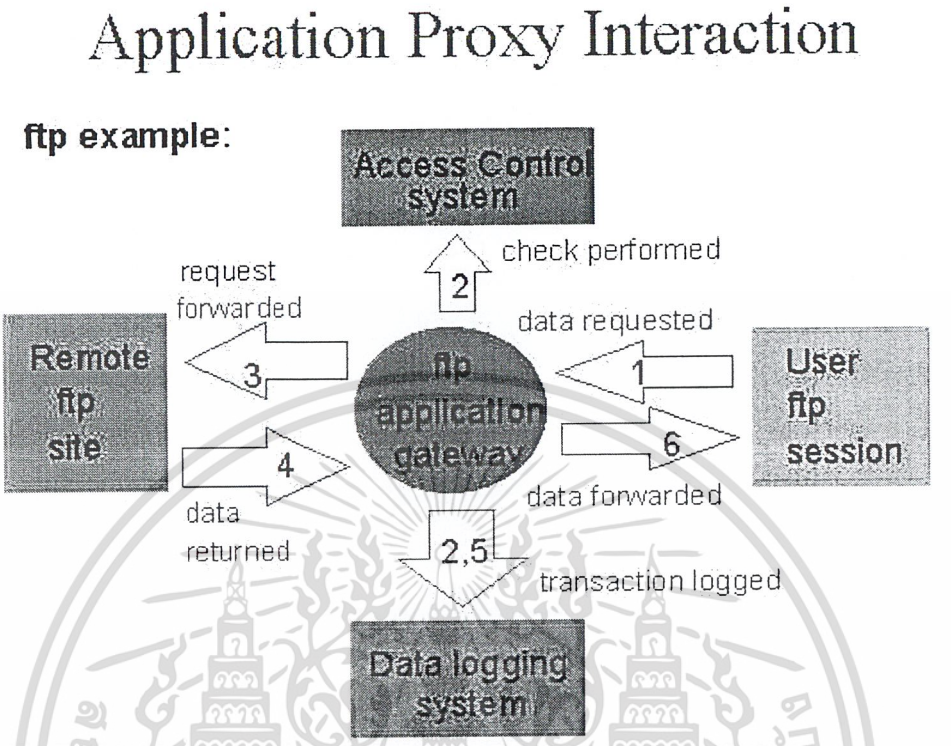


รูปที่ 4-16 การบุกรุกระบบโดยอาศัยอุโมงค์ของอินเตอร์เน็ตโพรโตคอล

4.4 พร็อกซีเซิร์ฟเวอร์ (Proxy Server)

พร็อกซีเซิร์ฟเวอร์มีหน้าที่รับการร้องขอ (request) บริการในเครือข่ายอินเตอร์เน็ตจากผู้ใช้(การร้องขอจากผู้ใช้ ก็อย่างเช่น เว็บเพจ นั่นเอง) และถ้าการร้องขอเว็บเพจผ่าน กล่าวคือไม่ผิดกับข้อห้ามใดๆ(อาจจะมีการกำหนดข้อห้าม เช่น ห้ามเข้าเว็บโป๊ หรือเว็บที่เกี่ยวกับการพนัน เป็นต้น) พร็อกซีเซิร์ฟเวอร์ก็จะไปดูในแคชก่อน ถ้าหากเว็บเพจที่ร้องขอมามีอยู่ในแคช, มันก็จะทำการตอบรับการร้องขอนั้นเองเลยโดยไม่ต้องไปร้องขอกับเซิร์ฟเวอร์จริงๆ แต่ถ้าหากเว็บเพจนั้นไม่มีอยู่ในแคช, พร็อกซีเซิร์ฟเวอร์ก็จะแสดงตัวเป็นผู้ใช้เพื่อไปร้องขอกับเซิร์ฟเวอร์จริงๆ (real server) และเมื่อพร็อกซีเซิร์ฟเวอร์ได้รับเพจนั้นมาแล้ว, พร็อกซีเซิร์ฟเวอร์ก็จะฟอร์เวิ ร์ดไปให้ผู้ใช้

สำหรับผู้ใช้แล้วจะไม่รู้ถึงการมีอยู่ของพร็อกซีเซิร์ฟเวอร์เลย การทำงานของพร็อกซีเซิร์ฟเวอร์จะแสดงให้เห็นในรูปที่ 4-17 โดยจะเป็นตัวอย่างของแอพพลิเคชันพร็อกซีที่ให้บริการเอฟทีพีนั่นเอง



รูปที่ 4-17 แอพพลิเคชันพร็อกซีที่ให้บริการเอฟทีพี

ฟังก์ชันการทำงานของพร็อกซี, ไฟร์วอลล์ และแคชชิ่ง สามารถรวมเป็นแพ็กเกจเดียวกันได้ ตัวอย่าง เช่น พร็อกซีเซิร์ฟเวอร์อาจจะเป็นแมชีน (machine)เดียวกับไฟร์วอลล์ หรืออาจจะแยกเป็นเซิร์ฟเวอร์คนละ ตัว แล้วพร็อกซีเซิร์ฟเวอร์จะฟอร์เวิร์ดการร้องขอไปให้ไฟร์วอลล์ต่อไป

พร็อกซีเซิร์ฟเวอร์ก็จะแบ่งออกเป็นหลายชนิดโดยจะมีความสามารถในการทำงานต่างกัน พร็อกซี เซิร์ฟเวอร์บางชนิดสามารถซ่อนไอพีแอดเดรสจริง ๆ ได้ด้วย

4.4.1 จุดประสงค์หลักของพร็อกซีเซิร์ฟเวอร์

พร็อกซีเซิร์ฟเวอร์มีจุดประสงค์หลัก 2 ประการ คือ

1. เพิ่มประสิทธิภาพในการทำงาน

พร็อกซีเซิร์ฟเวอร์สามารถเพิ่มประสิทธิภาพในการทำงานในระบบที่มีผู้ใช้เป็นจำนวนมาก เพราะ พร็อกซีเซิร์ฟเวอร์จะเก็บผลลัพธ์ของการร้องขอเอาไว้ กล่าวคือสมมติว่ามีผู้ใช้ 2 คนคือสุนันท์กับนิสาเข้ามา ใช้บริการเวิลด์ไวด์เว็บผ่านทางพร็อกซีเซิร์ฟเวอร์ ในครั้งแรกสมมติว่าสุนันท์ได้ทำการร้องขอเว็บเพจชื่อว่า

เพจ 1 ต่อมานิสาได้ทำการร้องขอเพจ 1 เหมือนกัน ในการรีร้องขอครั้งที่ 2 (โดยนิสา) พร็อกซีเซิร์ฟเวอร์ก็จะรีเทิร์นเพจ 1 ที่ร้องขอไปแล้วโดยสุนันท์ โดยไม่ต้องทำการติดต่อไปยังเซิร์ฟเวอร์จริง ๆ

2. กำหนดสิทธิในการใช้งานเว็บเพจ เช่น ไม่ให้เข้าเวปโป๊หรือเว็บที่เกี่ยวกับการพนัน เป็นต้น

4.5 ระบบตรวจจับผู้บุกรุก (Intrusion Detection System)

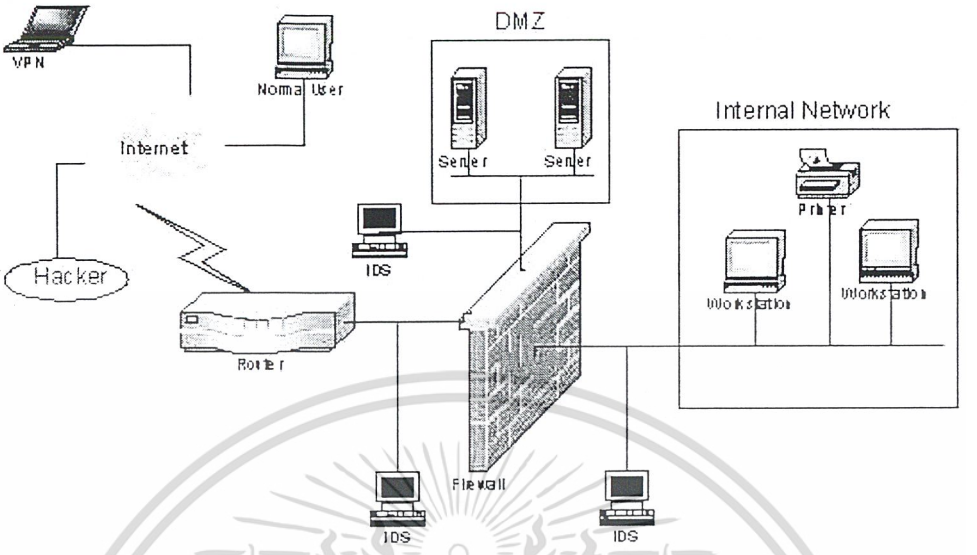
4.5.1 ความสำคัญของระบบตรวจจับผู้บุกรุก

ผู้บุกรุกระบบคอมพิวเตอร์ (Intruder) หมายถึง บุคคลที่พยายามบุกรุกหรือได้บุกรุกเข้ามาในระบบโดยที่ไม่ได้รับอนุญาติ โดยหมายความรวมถึงบุคคลที่เรียกว่าแฮ็กเกอร์ (Hacker) คือผู้ที่ชอบเข้าไปศึกษาบางสิ่งบางอย่างในระบบ เช่น เข้าไปศึกษาหลักการทำงานของระบบและโปรแกรม การบุกรุกถ้าแบ่งจากสถานที่ที่ติดต่อเข้ามาของผู้บุกรุก สามารถแบ่งได้เป็น 2 ประเภท คือ การบุกรุกจากภายในเครือข่ายเอง และการบุกรุกจากภายนอกเครือข่าย

การบุกรุกจากภายนอกเป็นการบุกรุกที่มาจากภายนอกเครือข่ายของระบบ และเข้ามาทำความเสียหายให้แก่ระบบ เช่น เข้ามาเปลี่ยนข้อมูลในโฮมเพจ หรือพยายามบุกรุกผ่านไฟร์วอลล์เข้ามาทำความเสียหายให้กับเครื่องที่อยู่ภายในเครือข่าย โดยผู้บุกรุกจากภายนอกสามารถเข้ามาโดยผ่านบริการ(services) ของระบบหรือติดต่อผ่านโมเด็มเข้ามาก็ได้

การบุกรุกจากภายในเป็นการบุกรุกโดยผู้ที่มีสิทธิ์อันชอบธรรมที่เข้ามาใช้ทรัพยากรในระบบ แต่ใช้งานทรัพยากรอย่างไม่ถูกต้อง หรือพยายามแอบอ้างไปใช้สิทธิ์ของผู้ใช้อื่นที่มีสิทธิ์การใช้งานเหนือกว่า

ถึงแม้ว่าระบบมีการติดตั้งไฟร์วอลล์เพื่อป้องกันการบุกรุก แต่การมีไฟร์วอลล์เพียงอย่างเดียวก็เหมือนกับการมีเครื่องกีดขวางมากั้นระหว่างระบบคอมพิวเตอร์ภายในเครือข่าย (Intenal network) กับระบบภายนอก (Internet) เท่านั้น ไม่สามารถป้องกันการบุกรุกจากภายในระบบได้ ดังนั้นการใช้ไฟร์วอลล์แต่เพียงอย่างเดียวจึงไม่เพียงพอสำหรับการรักษาความปลอดภัยในระบบคอมพิวเตอร์ จำเป็นต้องมีระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์เข้ามาช่วยเสริมการทำงาน เปรียบเสมือนกับการที่มีรั้วกั้นและมียามเฝ้าประตูคอยตรวจสอบกับบุคคลไม่พึงประสงค์ ผู้บุกรุกอาจใช้วิธีปลอมแปลงหรือหาช่องทางพิเศษเล็ดลอดเข้ามาได้ และตัวไฟร์วอลล์เองไม่สามารถบอกได้เลยว่าภายในระบบกำลังมีอะไรเกิดขึ้นบ้าง จึงต้องมีโทรทัศน์วงจรปิดทำงานร่วมกับสัญญาณกันขโมยคอยรวบรวมข้อมูลจากแหล่งต่างๆ มาวิเคราะห์ ช่วยให้สามารถตรวจจับการบุกรุกที่มาจากภายในระบบ รวมทั้งผู้บุกรุกที่เล็ดลอดผ่านไฟร์วอลล์เข้ามาได้ซึ่งก็คือ ระบบตรวจจับผู้บุกรุกระบบคอมพิวเตอร์นั่นเอง ตัวอย่างการใช้งานก็ตามรูปที่4-18 นั่นเอง



รูปที่ 4-18 ตัวอย่างการวางระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุกคือ ระบบที่ใช้ในการตรวจจับการใช้งานและความพยายามในการใช้งานคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ซึ่งขัดกับข้อบังคับและเจตุจำนงค์การใช้งาน ส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ 3 ประการคือความถูกต้อง (Integrity), ความลับ (Confidentiality) และความสามารถคงการใช้งานอยู่ได้ (Availability)

4.5.2 ประเภทของระบบตรวจจับการบุกรุกแบ่งตามขอบเขตของการตรวจจับ

ประเภทของระบบตรวจจับการบุกรุกระบบคอมพิวเตอร์แบ่งตามขอบเขตของการตรวจจับได้ 2ชนิด ดังนี้

1. ระบบตรวจจับการบุกรุกบนโฮสต์ (Host-based Intrusion Detection)

ระบบตรวจจับการบุกรุกบนโฮสต์ทำการตรวจจับข้อมูลที่ไหลเข้าและออกคอมพิวเตอร์แต่ละเครื่อง นอกจากนั้นก็จะทำการตรวจสอบความสมบูรณ์ของซิสเต็มไฟล์ และเฝ้าดูโพรเซสที่น่าสงสัย ระบบตรวจจับการบุกรุกบนโฮสต์ มี 2 ประเภทใหญ่คือ

- *Host Wrappers หรือเพอร์ซันนอลไฟร์วอลล์ (personal firewall)*
  เราสามารถที่จะทำการปรับแต่งให้ IDS ชนิดนี้ทำการตรวจสอบทุกๆ แพ็กเก็ตบนเครือข่าย การพยายามที่จะเชื่อมต่อเข้ามาหรือการที่จะพยายามล็อกอินเข้ามาซึ่งรวมถึงการเชื่อมต่อแบบไดอัลอิน (dial-in) Host wrappers ที่รู้จักกันดีคือ TCP Wrapper

- *Agent-based Software*

สามารถที่จะเฝ้าตรวจการเข้าถึง (access) และการเปลี่ยนแปลงของซิสเต็มไฟล์ รวมทั้งการเปลี่ยนแปลงสิทธิ (privilege) ของผู้ใช้ IDS ประเภทนี้ที่รู้จักกันดีคือ Tripwire

ซึ่งทั้งสองชนิดจะมีประสิทธิภาพในการตรวจจับการบุกรุกจากภายในได้ดีกว่าระบบตรวจจับการบุกรุกบนเครือข่าย (network-based IDS) แต่ประสิทธิภาพการตรวจจับการโจมตีจากภายนอกนั้นจะทำได้ดีพอๆ กัน

2. ระบบตรวจจับการบุกรุกบนเครือข่าย (Network based IDS)

ระบบตรวจจับการบุกรุกบนเครือข่ายนั้นจะทำการเฝ้าดูข้อมูลบนเครือข่าย โดยที่ระบบดังกล่าวจะทำการรับข้อมูลทั้งหมดที่อยู่บนส่วนของเครือข่ายที่รับผิดชอบ นอกเหนือจากส่วนของเครือข่ายที่รับผิดชอบและชนิดของการสื่อสารอื่นๆ แล้วระบบดังกล่าวก็ไม่สามารถทำการตรวจจับ แพ็กเก็ตต่างๆจะถูกตรวจจับโดยเซ็นเซอร์ (sensor) ของ IDS ซึ่งเซ็นเซอร์จะมองเห็นเฉพาะแพ็กเก็ตที่ผ่านส่วนของเครือข่ายที่เซ็นเซอร์นั้นติดอยู่ แพ็กเก็ตต่างๆจะเป็นที่สนใจของเซ็นเซอร์ก็ต่อเมื่อแพ็กเก็ตนั้นเข้ากับซิกเนเจอร์(signature) ที่หนด ซึ่งปกติแล้วจะแบ่งได้เป็น 3 ประเภทคือ

- *สตริงซิกเนเจอร์ (String signature)*

จะมองหาสตริงที่เป็นข้อความ (text string) ซึ่งอาจบ่งบอกถึงการโจมตีตัวอย่างเช่น " cat " + + " 7% rhost " อาจทำให้ระบบยูนิกซ์เกิดช่องโหว่ต่อการโจมตีบนเครือข่าย

- *พอร์ตซิกเนเจอร์ (Port signatures)*

จะเฝ้าดูการพยายามติดต่อเข้ามาทางพอร์ตที่รู้จักกันดีและมักจะถูกโจมตี เช่น telnetจะใช้ TCP พอร์ต 23. FTP จะใช้ TCP พอร์ต 21/20 ซึ่งถ้าระบบของเราไม่ได้เปิดพอร์ตดังกล่าว แต่มีการพยายามเชื่อมต่อเข้ามาแสดงว่าแพ็กเก็ตดังกล่าวอาจจะมีความประสงค์ร้ายก็ได้

- *เฮดเดอร์ซิกเนเจอร์ (Header signatures)*

พยายามมองหารูปแบบที่อันตรายและผิดกฎของแพ็กเก็ตเฮดเดอร์ (packet header)ตัวอย่างที่เห็นได้ชัดของเฮดเดอร์ซิกเนเจอร์คือ TCPแพ็กเก็ตซึ่งมีทั้ง SYN และ FIN Flags

4.5.3 ประเภทของระบบตรวจจับการบุกรุกแบ่งตามแหล่งข้อมูล

ระบบตรวจจับการบุกรุกระบบคอมพิวเตอร์แบ่งตามแหล่งข้อมูลได้ 3 ชนิด ดังนี้

1. ระบบตรวจจับผู้บุกรุกทางเครือข่าย (Network Intrusion Detection System : NIDS)

เป็นระบบตรวจจับแพ็กเก็ตที่วิ่งอยู่ในเน็ตเวิร์ก โดยพยายามตรวจสอบว่ามีผู้บุกรุกพยายามบุกรุกเข้าสู่ระบบหรือไม่ ตัวอย่างของระบบนี้คือระบบที่ตรวจสอบว่ามีแพ็กเก็ตของการเชื่อมต่อแบบTCP/ไอพี ที่ชื่อว่า SYN ส่งเข้ามาเป็นจำนวนมากอย่างผิดปกติในเครื่องเป้าหมาย ซึ่ง NIDS นั้นอาจจะถูกติดตั้งบนเครื่องเป้าหมายเอง และจะคอยตรวจทุกทราฟฟิกของตัวเองหรืออาจจะถูกติดตั้งบนเครื่องที่แยกอยู่ต่างหากและจะคอยตรวจทุกแพ็กเก็ตที่ผ่านมาในเครือข่ายก็ได้

2. ระบบตรวจสอบความถูกต้องของข้อมูลในระบบ (System Integrity Verifiers : SIV)

ตรวจสอบความถูกต้องของข้อมูลในระบบ เพื่อค้นหาว่ามีผู้บุกรุกพยายามเปลี่ยนแปลงข้อมูลของซิสเต็มไฟล์หรือส่วนประกอบอื่น ๆ (component) เช่น ไฟล์ที่เป็นรีจิสตรี(registry) ของวินโดว์สหรือครอน (cron) ในระบบปฏิบัติการยูนิกซ์หรือไม่

3. ระบบตรวจสอบล็อกไฟล์ (Log File Monitors : LFM)

จะทำการเฝ้าดูล็อกไฟล์ต่างๆที่สร้างขึ้นมาโดยบริการในเครือข่าย โดยดูรูปแบบของล็อกไฟล์ที่เกิดขึ้นว่าตรงกับพฤติกรรมการบุกรุกที่เคยเกิดขึ้นแล้วหรือไม่ ถ้าตรงก็สามารถตั้งข้อสงสัยว่าเข้าข่ายการบุกรุกระบบ

4.5.4 ประเภทของระบบตรวจจับการบุกรุกแบ่งตามกระบวนการตรวจจับ

ระบบตรวจจับการบุกรุกระบบคอมพิวเตอร์แบ่งตามกระบวนการตรวจจับได้ 2 ชนิด ดังนี้

1. ระบบตรวจจับการบุกรุกแบบอาศัยข้อมูลที่มีอยู่ (Knowledge-based IDS)

จะอาศัยข้อมูลที่เกี่ยวกับการโจมตีชนิดต่างๆ พร้อมทั้งช่องโหว่ของระบบในการตรวจจับการบุกรุกเมื่อความพยายามในการโจมตีนั้นถูกจับได้ IDS ก็จะทำการแจ้งเตือน เพราะฉะนั้นจะเห็นได้ว่าความสมบูรณ์ และประสิทธิภาพของ IDS ชนิดนี้ จะขึ้นอยู่กับความทันสมัยของข้อมูลเกี่ยวกับการโจมตีต่างๆ

ข้อดี ของวิธีการแบบนี้คือ อัตราการเกิดการแจ้งเตือนผิดๆ นั้นจะต่ำ และข้อมูลที่ได้จาก IDS นั้นจะมีรายละเอียดที่ดีทำให้ง่ายต่อผู้ใช้ในการป้องกันและแก้ไขการโจมตี

ข้อเสีย ของวิธีนี้คือ ความยากในการรวบรวมข้อมูลเกี่ยวกับรูปแบบการโจมตีและการปรับปรุงข้อมูลเกี่ยวกับช่องโหว่ต่างๆ ให้ทันสมัยอยู่เสมอ เนื่องจากข้อมูลต่างๆ นั้นขึ้นอยู่กับระบบปฏิบัติการ, เวอร์ชั่น, แพลตฟอร์มและแอพพลิเคชัน นอกจากชั้นการตรวจจับการโจมตีจากภายในนั้นทำได้ยากเนื่องจาก การโจมตีจากภายในเกี่ยวกับการละเมิดสิทธิของผู้ใช้ซึ่งไม่ได้เกี่ยวข้องกับช่องโหว่แต่อย่างใด

2. ระบบตรวจจับการบุกรุกแบบตรวจสอบพฤติกรรม (Behavior-based IDS)

แนวความคิดของการตรวจจับการบุกรุกแบบนี้คือ จะมีการแจ้งเตือนเมื่อระบบมีการตรวจพบความเบี่ยงเบนและความผิดปกติของระบบหรือของผู้ใช้จากการใช้ระบบปกติ ซึ่งรูปแบบของพฤติกรรมที่เป็นปกตินั้นจะถูกรวบรวมจากข้อมูลอ้างอิงต่างๆ หลังจากนั้น IDS จะทำการเปรียบเทียบระหว่างพฤติกรรมในขณะนั้นกับรูปแบบอ้างอิง ดังนั้นจะเห็นได้ว่าการแจ้งเตือนที่ผิดพลาด(false alarm) จะเกิดขึ้นได้บ่อยครั้ง

ข้อดี ของการตรวจจับโดยใช้เทคนิคลักษณะนี้คือสามารถที่จะตรวจจับแบบการบุกรุกแบบใหม่ๆ ที่ไม่เคยมีมาก่อน และความเกี่ยวโยงกับระบบปฏิบัติการค่อนข้างต่ำ รวมทั้งยังสามารถที่จะตรวจจับการบุกรุกที่ไม่ได้โจมตีช่องโหว่ เช่นการโจมตีจากภายใน

ข้อเสีย ที่สำคัญที่สุดคือการแจ้งเตือนที่ผิดพลาดจะค่อนข้างสูงในช่วงของการศึกษาพฤติกรรมของระบบ และเนื่องจากพฤติกรรมของที่ระบบที่จะเปลี่ยนแปลงอยู่ตลอดเวลา IDS ก็ต้องใช้เวลาในการศึกษาและเป็นเหตุให้ IDS ขัดข้องหรืออาจทำให้เกิดการแจ้งเตือนที่ผิดพลาดมากขึ้น

4.6 IP Security (IPSec)

ในสังคมอินเตอร์เน็ต ได้มีความตระหนักในเรื่องของความปลอดภัยและความเป็นส่วนตัวมานานแล้ว ดังจะเห็นได้จากความพยายามในการสร้างความปลอดภัยสำหรับงานต่างๆ ขึ้นมา เช่น แอพพลิเคชันสำหรับการพิสูจน์ตน(Kerberos), การดูแลความปลอดภัยทางเว็บ (SSL : Secure Socket Layer) และระบบอื่น ๆ

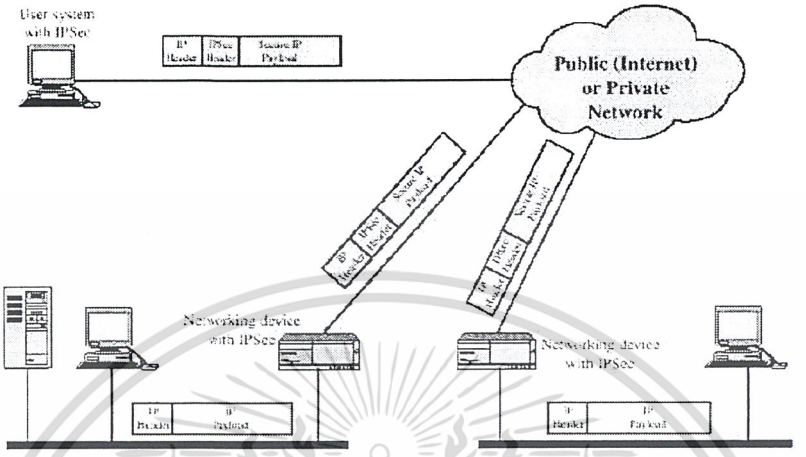
อย่างไรก็ตามในการเชื่อมต่อระหว่างคอมพิวเตอร์ คงไม่ได้มีเพียงแอพพลิเคชันดังที่ได้กล่าวมาเท่านั้น และการสร้างความปลอดภัยให้กับแต่ละแอพพลิเคชันก็เป็นเรื่องที่ไม่ง่าย เพราะจะเกี่ยวข้องกับการกำหนดมาตรฐานใหม่ขึ้นเป็นจำนวนมาก จึงมีการนำความปลอดภัยใส่เข้าไปในระดับไอพี (Internet Protocol) เสียเลย ทำให้แอพพลิเคชันอะไรก็ตามที่ทำงานอยู่บนระดับไอพี,ก็จะได้อานิสงค์แห่งความปลอดภัยนั้นไปด้วย

การรักษาความปลอดภัยระดับไอพีหรือเรียกย่อๆ ว่า IPSec นั้น มีหน้าที่ในการให้บริการอยู่ 3 อย่างด้วยกันคือระบบการพิสูจน์ตน (Authentication) การรักษาความลับ (Confidential) และการบริหารคีย์ (Key Management)

4.6.1 รูปแบบการใช้งาน

เราอาจใช้ IPSec ในการเชื่อมต่อระหว่างสำนักงานสาขา(Branch Office) โดยผ่านเครือข่ายอินเตอร์เน็ตหรือใช้ในการเชื่อมต่อระยะไกล (Remote Access) ผ่านเครือข่ายอินเตอร์เน็ต หรือใช้ในการเชื่อมต่อระหว่างเครือข่ายแบบอินทราเน็ต (Intranet)และเอ็กซ์ทราเน็ต (Extranet)ระหว่างองค์กร

นอกจากนี้ยังใช้ในการสื่อสารแบบอี-คอมเมิร์ซ (Electronics Commerce) ทั้งนี้เนื่องจาก IPSec นั้นสามารถทั้งด้านการพิสูจน์ตน และการเข้ารหัสในทุก ๆ การสื่อสารที่มีพื้นฐานบนระดับ IP



รูปที่ 4-19 รูปแบบการใช้งานปกติของ IPSec

ในรูปที่ 4-19 ได้แสดงรูปแบบการใช้งานปกติของ IPSec โดยการสื่อสารภายในวงแลน(Local Area Network) แต่ละวงจะเป็นการสื่อสารตามปกติ แต่เมื่อการสื่อสารได้ก้าวข้ามออกไปข้างนอกจะมีการใช้ IPSec โดยการนำ IPSec มาใช้นี้จะเริ่มที่เราท์เตอร์ (Router) และไฟร์วอลล์ (Firewall) หรือเกตเวย์ (Gateway) ของเครือข่าย โดยจะมีการเข้ารหัสข้อมูลแล้วจึงส่งออกไป และเมื่อถึงปลายทางก็จะถอดรหัสออกมา ซึ่งการทำงานทั้งหมดนี้จะเกิดขึ้นโดยที่เครื่องคอมพิวเตอร์ไม่มีส่วนรับทราบเลย นอกจากนั้นIPSec ยังสามารถใช้งานในกรณีที่ผู้ใช้การเชื่อมต่อแบบไดอัล-อัพได้อีกด้วย สามารถใช้ในการเชื่อมต่อเข้ามาที่หน่วยงานนั้น ๆ โดยตรง

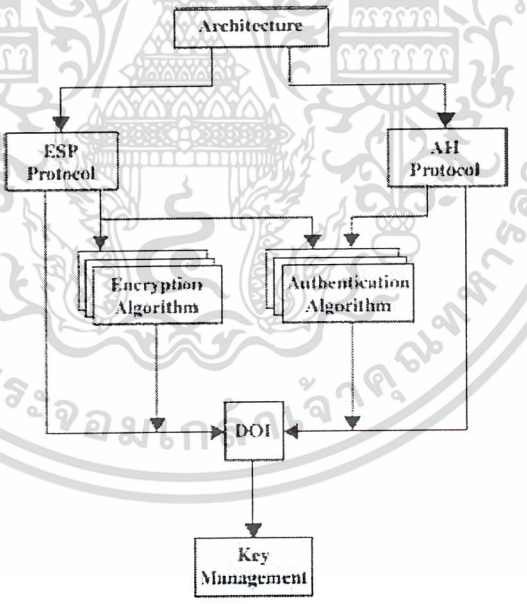
4.6.2 ประโยชน์ของ IPSec

- เมื่อมีการนำ IPSec มาใช้ที่ไฟร์วอลล์หรือเราท์เตอร์ จะทำให้มีระบบความปลอดภัยที่แข็งแกร่งที่สามารถใช้ได้กับทุกการสื่อสาร โดยการสื่อสารภายในจะไม่มีความสิ้นเปลือง (overhead) ของ IPSec
- เมื่อมีการใช้ IPSec กับไฟร์วอลล์ ทุกการสื่อสารภายนอกจะไม่สามารถข้าม IPSecได้ เนื่องจากไฟร์วอลล์เป็นเพียงจุดเดียวที่เชื่อมต่อกับภายนอก ดังนั้นการติดต่อระหว่างภายในและภายนอกก็จะต้องทำโดยผ่าน IPSec เท่านั้น
- เนื่องจาก IPSec ทำงานอยู่ภายใต้TCPและUDP ดังนั้นแอพพลิเคชันที่ทำงานบน TCP และ UDP จึงต้องทำงานผ่าน IPSec ไปด้วย ดังนั้นโปรแกรมต่างๆ ก็ไม่ต้องเขียนขึ้นมาใหม่

- การทำงานของ IPSec ไม่กระทบกับผู้ใช้ โดยผู้ใช้จะไม่รับรู้ถึงการมีอยู่ของIPSec เลย ดังนั้นจึงไม่ต้องเสียค่าใช้จ่ายในการสอนผู้ใช้
- IPSec สามารถจะสร้างความปลอดภัยในระดับผู้ใช้ได้ ซึ่งเป็นผลดีที่ทำให้สามารถจะระบุถึงผู้ใช้แต่ละคนที่เข้ามาใช้งานจากระยะไกลได้
- IPSec ช่วยให้การทำงานของโพรโตคอลในการจัดหาเส้นทาง (Routing Protocol) มีความปลอดภัยมากยิ่งขึ้น เพราะช่วยให้การทำงานสามารถใช้ความสามารถของIPSec ในการเข้ารหัสข้อมูลและพิสูจน์ถึงเราท์เตอร์จริง ๆ ได้

4.6.3 การทำงานของ IPSec

IPSec สร้างการทำงานให้เกิดความปลอดภัยที่ไอพีเลเยอร์ (IP layer) โดยให้ระบบสามารถเลือกโพรโตคอลที่ต้องการได้ และสามารถพิจารณาอัลกอริทึมที่จะใช้สำหรับบริการต่างๆ (services) โดย 2 โพรโตคอลที่ถูกใช้ในการสร้างความปลอดภัยก็คือ โพรโตคอลในการพิสูจน์ตน (Authentication protocol) และโพรโตคอลที่รวมทั้งการเข้ารหัสและการพิสูจน์ตน (Encryption and Authentication protocol) ดังแสดงในรูป 4-20



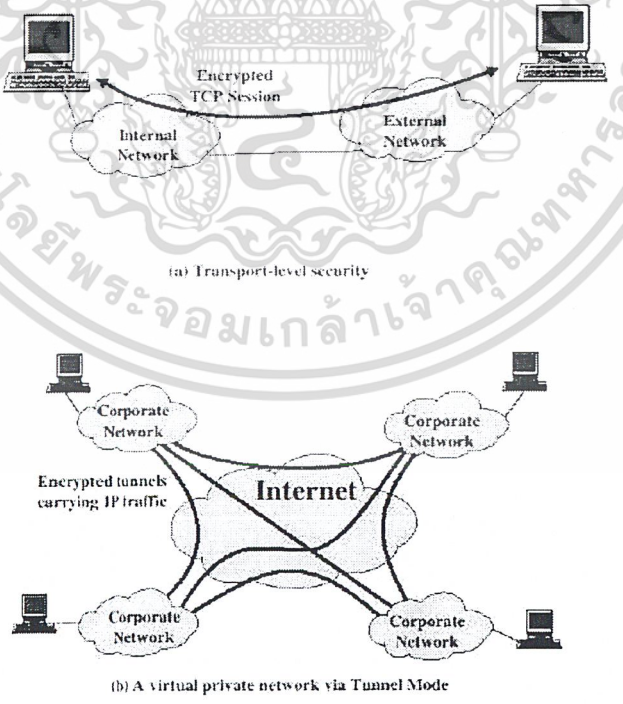
รูปที่ 4-20สถาปัตยกรรมของ IPSec

สำหรับตารางที่ 4-2 จะแสดงถึงบริการต่างๆ ที่สามารถใช้ได้จากโพรโตคอล AHและ โพรโตคอล ESP ให้เห็นว่า โดยสำหรับโพรโตคอล ESP จะแยกออกเป็น 2 กรณีได้อีกคือ การเข้ารหัสอย่างเดียว (encryption only) และการเข้ารหัสรวมถึงการพิสูจน์ตนด้วย(encryption plus authentication)

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access Control	Y	Y	Y
Connectionless Integrity	Y		Y
Data Origin Authentication	Y		Y
Rejection of Replayed Packets	Y	Y	Y
Confidentiality		Y	Y
Limited Traffic Flow Confidentiality		Y	Y

ตารางที่ 4-2บริการต่าง ๆที่สามารถใช้ได้จากโพรโตคอล AH และ โพรโตคอลESP

สำหรับโหมดการทำงานของ IPSec จะแบ่งเป็น 2 โหมด แสดงในรูป 4-21 คือ Transport-level security และ A virtual private network via tunnel mode



รูปที่ 4-21 แสดงโหมดการทำงานของ IPSec

4.6.4 ปัญหาของ IPSec

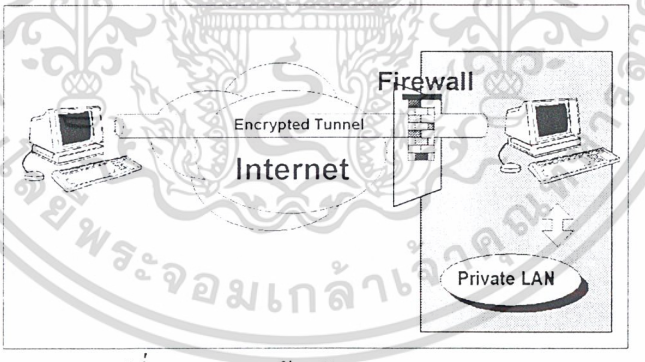
1. ไม่สามารถเลือกแบบในการส่งได้ เช่น ในกรณีที่นำมาใช้กับเว็บเอพพลิเคชัน หากจะเข้ารหัสก็จะต้องเข้ารหัสทุกหน้าซึ่งบางทีอาจเกินความจำเป็น
2. หากจะใช้งาน IPSec จากเครื่องต้นทางไปเครื่องปลายทางโดยไม่ผ่านเราท์เตอร์หรือไฟร์วอลล์ ระบบปฏิบัติการของเครื่องต้นทางและเครื่องปลายทางจะต้องสนับสนุน IPSec

4.7 VPN (Virtual Private Network)

VPN เป็นการจำลองเครือข่ายภายในบนเครือภายภายนอกอย่างเช่นอินเตอร์เน็ต ที่เรียกว่า "virtual"ก็เพราะมันขึ้นอยู่กับการใช้การเชื่อมต่อเสมือน (virtual connections) ซึ่งเป็นคอนเน็กชันชั่วคราว ไม่ได้เป็นการติดต่อทางกายภาพ แต่มันประกอบด้วยแพ็กเก็ตที่ถูกเราท์ไปมาโดยผ่านเครื่องหลากหลายบนอินเตอร์เน็ต การเชื่อมต่อเสมือนที่มีความปลอดภัยนี้อาจถูกสร้างขึ้นระหว่างเครื่องสู่เครื่อง หรือเป็นแบบเครื่องสู่เครือข่าย หรือระหว่างเครือข่ายก็ได้

4.7.1 ความจำเป็นของ VPN

VPN จำเป็น เพราะว่าการติดต่อกันระหว่างหน่วยงานที่มีการใช้เครือข่ายภายนอกอย่างเช่นอินเตอร์เน็ตนั้นมีช่องโหว่(Vulnerability) เอื้ออำนวยต่อการถูกโจมตี ความเสี่ยงที่จะถูกโจมตีนี้ขึ้นอยู่กับความสำคัญของข้อมูลที่ถูกส่งและความสำคัญของผู้รับ ผู้ส่งด้วย



รูปที่ 4 –22 การสร้างทันเนล (Tunneling)

จากรูปที่ 4-22 จะแสดงให้เห็นว่าการติดต่อระหว่างภายนอกและภายในจะต้องผ่านไฟร์วอลล์ก่อน ซึ่งไฟร์วอลล์จะทำหน้าที่กรองข้อมูลที่วิ่งผ่านตัวมันเอง ดังนั้นจะเห็นว่าระบบความปลอดภัยนั้นจะป้องกันเฉพาะเครือข่ายภายในเท่านั้น ส่วนผู้ที่ต้องใช้เครือข่ายโทรศัพท์โทรเข้ามาหา ISP นั้นยังไม่มีการป้องกันใดๆ ข้อมูลที่อยู่ในรูปแพ็กเก็ตจะวิ่งผ่านไฟร์วอลล์มาจากเครือข่ายภายนอก ซึ่งในระบบที่เปิดกว้างอย่างอินเตอร์เน็ตนั้น การดักข้อมูลสามารถทำได้ง่าย จึงเป็นที่มาของการพัฒนาระบบ VPN นี้เอง เพื่อให้ VPN ที่

ถูกพัฒนาขึ้นมาใหม่นี้สามารถใช้งานได้อย่างสมบูรณ์แบบ ระบบ VPN จะต้องมีคุณสมบัติต่อไปนี้ควบคู่ไปด้วย

- ไว้ใจได้ : ระบบ VPN จะต้องให้ความรู้สึกมั่นใจว่าข้อมูลที่เป็นความลับและเป็นส่วนตัวของแต่ละผู้ใช้ จะไม่ถูกดักหรือเปิดใช้งานโดยผู้อื่นที่ไม่ได้รับอนุญาติ
- รัดกุม : ระบบ VPN จะต้องมีระบบการตรวจสอบผู้ใช้งานอย่างละเอียดรัดกุม ผู้ที่จะมีสิทธ์ใช้งานในระบบต้องเป็นสมาชิกที่ผ่านการตรวจสอบแล้วเท่านั้น นอกจากนี้ VPN จะต้องสร้างความมั่นใจให้กับระบบข้อมูลว่าข้อมูลและแหล่งข้อมูลที่ส่งผ่านข้อมาปะปนกับข้อมูลภายในนั้นถูกต้องมาจากผู้ที่เชื่อถือได้
- มั่นคง : ข้อมูลที่ผู้ส่งส่งออกมานั้น จะต้องเหมือนกับข้อมูลที่ผู้รับได้รับ หมายความว่าข้อมูลที่ส่งเข้าออกระบบเครือข่าย จะต้องไม่มีการสูญหาย บิดเบือน หรือ ติดค้าง ข้อมูลจะต้องมีระบบการตรวจสอบเพื่อยืนยันการรับส่งที่ถูกต้อง
- รองรับได้หลายโพรโตคอล : ในระบบเครือข่ายแต่ละที่นั้นมีการใช้โพรโตคอลแตกต่างกันออกไป แต่การที่จะให้สามารถรับส่งข้อมูลข้ามเครือข่ายได้นั้น ระบบจะต้องรองรับโพรโตคอลที่แตกต่างกันนั้นได้ ไม่สิ้นเปลืองแบนด์วิดธ์ (Bandwidth) มากกว่าการรับส่งข้อมูลแบบธรรมดามากนัก สามารถปรับเข้าสู่ระบบที่มีอยู่แล้วได้ง่าย และง่ายต่อการขยายระบบ VPN ในอนาคต

4.7.2 VPN ทำงานอย่างไร

เมื่อเครื่องคอมพิวเตอร์ 2 เครื่องที่อยู่ต่างเครือข่ายกัน เช่น เครื่องหนึ่งโทรเข้ามาที่ ISP เพื่อใช้งานอินเตอร์เน็ตแต่ต้องการส่งข้อมูลให้กับอีกเครื่องหนึ่งที่อยู่ในครือข่ายภายของบริษัท เครื่องคอมพิวเตอร์ 2 เครื่องนี้จะมีการสร้างทันเนล (Tunneling) เพื่อเชื่อมระหว่างกัน โดยทันเนลนี้จะเปรียบเสมือนอุโมงค์เชื่อมระหว่างปลายทาง 2 ข้าง ซึ่งท่อนี้จะปิดกั้นไม่ให้บุคคลที่อยู่ภายนอกท่อสามารถดักหรือเก็บข้อมูลไปได้ การสร้างทันเนล จะเป็นดังรูปที่ 4 –22

การการสร้างทันเนลใน VPN

การการสร้างทันเนลคือการเอ็นแคบซูเลท (encapsulate) ข้อมูลแล้วจัดรูปแบบให้เป็นแพ็กเก็ตของข้อมูลปกติเพื่อส่งไปภายนอกเครื่อง ซึ่งรูปแบบของแพ็กเก็ตนั้นก็ขึ้นอยู่กับโพรโตคอลที่จะใช้ในการสื่อสาร ดังนั้นเมื่อนำเอาการสร้างทันเนลมาใช้ในการทำ VPN เราจึงเพิ่มความปลอดภัยด้วยการเข้ารหัส โดยเอาข้อมูลที่จะส่งในรูป ไอพีแพ็กเก็ตปกติมาเข้ารหัส ซึ่งโดยทั่ว ๆไปจะใช้ IPSec, SSL เป็นต้น (เนื่องจากโพรโตคอล IP นี้เป็นโพรโตคอลที่ใช้ในระบบอินเตอร์เน็ต) จากนั้นก็จะเอ็นแคบซูเลทให้เป็นที่ใช้ในระบบ VPN ซึ่งโพรโตคอลสำหรับ VPN ที่นิยมใช้ทั่วไป ได้แก่

- Point to Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Layer 2 Forwarding (L2F)
- IP Security (IPSec)
- SSL/SSH
- SOCKETS Protocol (SOCKS v5)

ซึ่งผู้ผลิตซอฟต์แวร์และฮาร์ดแวร์สำหรับ VPN จะนำโพรโตคอลเหล่านี้มาใช้ในการส่งข้อมูลข้ามเครือข่าย ดังนั้นข้อมูลที่ถูกส่งข้ามเครือข่ายจึงเป็นข้อมูลที่ไม่สามารถอ่านได้ตามปกติ ฝั่งผู้รับเท่านั้นที่จะมีกลไกในการอ่านรูปแบบของ โพรโตคอลสำหรับ VPN และกลไกสำหรับการถอดรหัส อีกทั้งยังมีการพิสูจน์ตนเพื่อยืนยันให้แน่ใจได้ว่าทั้งสองฝั่งที่ทำการเชื่อมต่อกันนี้เป็นตัวจริงทั้งคู่ ซึ่งก็จะใช้เทคโนโลยีอาทิเช่น PKI (X.509 certificates), RADIUS เป็นต้น สิ่งนี้เองที่ทำให้ VPN มีความปลอดภัย

PPTP (Point-to-Point Tunneling Protocol)

เป็นโพรโตคอลที่เอ็นแคปซูเลทโพรโตคอลอื่นๆ เพื่อการส่งข้ามเครือข่ายไอพียกตัวอย่างเช่น ใช้ส่ง Netware IPX packets ข้ามอินเตอร์เน็ตตามการเข้ารหัส แบบ RSA PPTP จะถูกใช้สร้าง VPN ภายใน เครือข่ายสาธารณะ ซึ่งผู้ใช้ภายนอกสามารถเข้าสู่เน็ตเวิร์กได้ทาง ISP ใด ๆ ที่สนับสนุน PPTP บนเซิร์ฟเวอร์ ของเขา

L2TP (Layer 2 Tunneling Protocol)

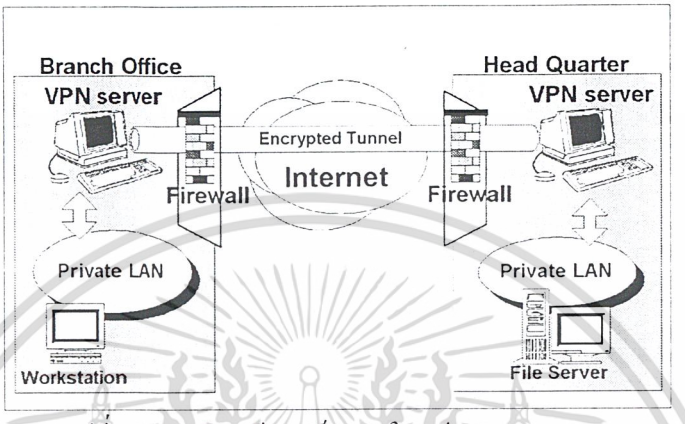
เป็นโพรโตคอล จาก IETF เพื่อการสร้าง VPN บนอินเตอร์เน็ต มันจะสนับสนุนโพรโตคอลอื่นๆเช่น Apple Talk และ IPX ด้วย และเช่นเดียวกับ IPSec L2TP เป็นการรวมตัวระหว่าง Point-to-Point Tunneling protocol ของ Microsoftกับ Layer 2 Forwarding (L2F)technology ของCisco

L2F (Layer 2 Forwarding)

เป็นโพรโตคอล จาก Ciscoเพื่อสร้างการติดต่อแบบ VPN บนอินเตอร์เน็ต ซึ่งมันถูกรวมกับ PPTP ใน L2TP protocol

4.7.3 การเอา VPN ไปใช้ในชีวิตจริง

การพัฒนาเอาเทคโนโลยี VPN ไปใช้ในองค์กรเพื่อช่วยอำนวยความสะดวกและปลอดภัย สามารถจำแนกได้เป็น 2 รูปแบบ คือ



รูปที่ 4-23การอิมพลีเมนท์ VPN ในรูปแบบ site-to-site

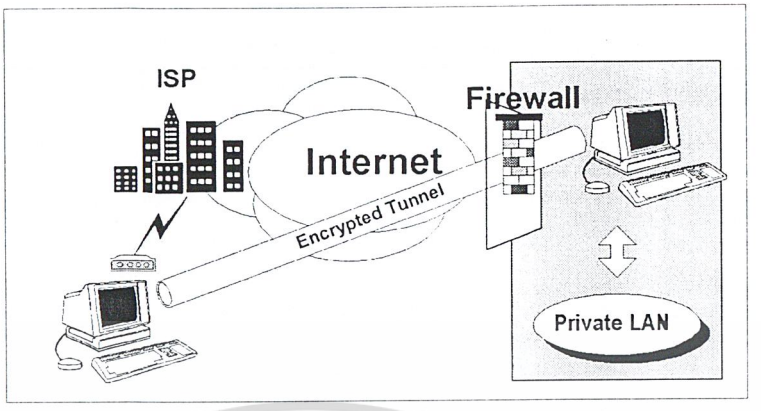
4.7.3.1 Site-to-Site

เมื่อองค์กรใดๆต้องการติดต่อกับระบบเครือข่ายของสาขาขององค์กรตนข้ามเครือข่ายอินเตอร์เน็ต และใช้ VPN ในการควบคุมความปลอดภัยข้ามเครือข่าย สิ่งที่ทุกองค์กรจะต้องมีในการทำระบบ VPN คือ VPN เซิร์ฟเวอร์ เพื่อตรวจสอบและทำการเข้ารหัส-ถอดรหัสแพ็กเกจต่างๆที่ส่งเข้าออกระหว่างภายในและภายนอกเครือข่าย ถ้าหากไม่มี VPN เซิร์ฟเวอร์ในด้านใดด้านหนึ่ง การติดต่อจะเป็นไปไม่ได้เลย ดังรูปที่4-23 สมมติว่าบริษัทหนึ่งติดตั้ง VPN เซิร์ฟเวอร์ ที่สำนักงานของตน และให้สาขาที่อยู่ห่างไกลต่อผ่านเครือข่ายอินเตอร์เน็ตเข้ามาเพื่อติดต่อส่งข้อมูลภายในกัน สาขานั้นก็จะต้องมี VPN เซิร์ฟเวอร์ เพื่อเป็นตัวควบคุมแพ็กเก็ตเข้าออกระบบเครือข่ายของสาขานั้นด้วย โดยที่ VPN เซิร์ฟเวอร์ ทั้งสองข้างจะต้องเป็น เซิร์ฟเวอร์ชนิดเดียวกัน คือ คุยกันได้ มีระบบการเข้าและถอดรหัสเดียวกัน ซึ่งส่วนใหญ่จะใช้ VPN เซิร์ฟเวอร์ยี่ห้อเดียวกัน VPN เซิร์ฟเวอร์ ของทั้งสองฝั่งจะสร้างทันเนลต่อตรงระหว่างกัน ดังนั้นเครื่องลูกข่ายที่อยู่หลังเซิร์ฟเวอร์นี้ จะส่งข้อมูลออกระบบเครือข่ายอีกฝั่งหนึ่งผ่านทางทันเนลนี้ด้วย

4.7.3.2 PC-to-site

เนื่องจากทุกวันนี้มีความต้องการที่จะให้ผู้ที่ออกไปปฏิบัติงานนอกสำนักงาน ไม่ว่าจะเป็นที่ต่างจังหวัด, ต่างประเทศ หรือร้านค้าขายปลีกสามารถติดต่อและส่งผ่านข้อมูลกับสำนักงานใหญ่ได้อย่างสะดวก, รวดเร็ว และประหยัด ไม่ว่าจะอยู่ที่ไหน หรือติดต่อเมื่อไหร่ จากที่เราได้อธิบายไปในตอนต้นแล้วว่า เมื่อสำนักงานใหญ่ต่อเข้าระบบอินเตอร์เน็ตที่มีเครือข่ายเชื่อมต่อกันทั่วโลก และเปิดให้ผู้ใช้งานจากภายนอกติดต่อผ่าน ISP ได้ การเชื่อมต่อที่เกิดขึ้นจะถูกควบคุมโดยระบบ VPN ระบบ VPN ในรูปแบบนี้ ทำได้ 2 ลักษณะ คือ

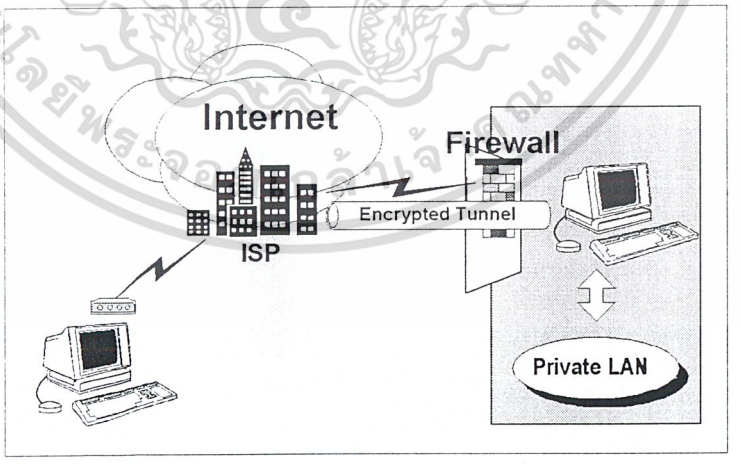
1. Client- initiated คือลักษณะการเชื่อมต่อดังรูปที่ 4-24



รูปที่ 4-24 Client- initiated

ผู้ใช้งานที่ต้องการติดต่อกับเครือข่ายภายในของบริษัทจะโทรเข้าหา ISP หลังจากที่ผ่านการตรวจสอบชื่อและรหัสผ่านที่ ISP จะต้องตรวจสอบเพื่อดูว่าผู้ที่โทรเข้ามานั้นเป็นสมาชิกของตนหรือไม่ ถ้าใช่ISP นั้นก็จะอนุญาติให้ผู้ใช้นั้นสามารถผ่านเข้าสู่ระบบอินเตอร์เน็ตได้ หลังจากนั้นผู้ใช้งานก็จะสร้างทันเนลจากเครื่องเวิร์กสเตชันของตนไปสู่เครื่อง VPN เซิร์ฟเวอร์ เพื่อส่งข้อมูลกัน ทันเนลนั้นจะถูกสร้างโดย ซอฟต์แวร์ที่ติดตั้งที่เครื่องเวิร์คสเตชันนั้น ดังนั้นถ้าเครื่องเวิร์คสเตชันนั้นต้องการดึงข้อมูลจากไฟล์เซิร์ฟเวอร์ภายในระบบเครือข่ายของบริษัท ก็จะสามารถทำได้โดยผ่านทันเนลนี้

2. Network access server บริษัทที่ต้องการให้ผู้ใช้งานสามารถโทรเข้า ISP และติดต่อมาที่ระบบเครือข่ายของบริษัท จะต้องทำการติดต่อกับ ISP ที่บริษัทตนเชื่อมสายเข้ามา ดังในรูปที่ 4-25



รูปที่ 4-25 Network access server

บริษัทเดินสายวงจรเช่ามายัง ISP และให ISP นั้นทราบว่าทางบริษัทต้องการให้นิสาติดต่อผ่านระบบ VPN มายังบริษัทของตนได้ เมื่อนิสาล็อกเข้าสู่ระบบอินเตอร์เน็ตที่ISP แล้ว ISP จะตรวจสอบดูว่าผู้ใช้งานนั้นเป็นสมาชิกของเครือข่ายบริษัทใด ซึ่งเมื่อตรวจสอบพบแล้ว ISP นั้นก็จะสร้างทันเนลจาก ISP ถึงที่บริษัทนั้น และให้นิสาส่งผ่านข้อมูลไปยังบริษัทของตนเองผ่านทันเนลที่มีความปลอดภัย

ทั้ง 2 ลักษณะนี้มีข้อดีข้อเสียแตกต่างกันไป แบบ Client-initiated มีความยืดหยุ่นในการต่อเข้า ISP ใดๆก็ได้ เนื่องจากทันเนลสร้างขึ้นที่ตัวผู้ใช้เองโดยตรงโดยไม่ต้องพึ่ง ISP ในขณะที่แบบ Network access server ต้องใช้ ISP หรือกลุ่มของ ISP เดียวกับที่บริษัทต่อระบบเครือข่าย ทำให้มีข้อจำกัดในการใช้งานจากที่ต่างๆ แต่แบบ Network access server นี้ ผู้ใช้งานภายนอกสามารถใช้งานได้ทันทีไม่ว่าจะเป็นเครื่องโน้ตบุ๊กหรือพีซีใดๆ ในขณะที่แบบ Client-initiated ก่อนการใช้งาน ผู้ใช้ต้องติดตั้งโปรแกรมซึ่งเป็นVPN ไคลเอ็นต์ ลงที่เครื่องก่อน จึงจะติดต่อเข้าไปยังเซิร์ฟเวอร์ของตนได้

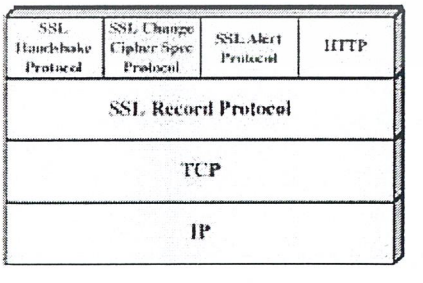
จะเห็นได้ว่าระบบ VPN ที่เพิ่มความปลอดภัยสำหรับการส่งต่อข้อมูลนั้น สามารถประยุกต์ใช้เพื่อให้องค์กรของท่านมีประสิทธิภาพการทำงานสูงสุด ภายใต้การควบคุมที่เข้มงวด เนื่องการความเสียหายในการโจรกรรมทางคอมพิวเตอร์นั้น มีค่ามากเกินกว่าจะประเมินได้ องค์กรของท่านเริ่มมองหาแนวทางการนำ VPN มาประยุกต์ใช้แล้วหรือยัง

4.7 Secure Sockets Layer (SSL)

เดิมที SSL ถูกพัฒนาโดยเน็ตสเคป ต่อมาได้กลายเป็นข้อตกลงที่แพร่หลายบนเว็บแอพพลิเคชัน เพื่อใช้สำหรับการติดต่อที่มีการพิสูจน์ตนและเข้ารหัสระหว่างเซิร์ฟเวอร์กับไคลเอ็นต์

4.7.1 โพรโตคอล SSL (The SSL Protocol)

SSL เป็นบริการที่ทำงานในระดับปลายทางถึงปลายทาง โดยในระหว่างการส่งจะอาศัยการทำงานของโพรโตคอลTCP โดยมีบริการต่าง ๆ ดังนี้



รูปที่ 4-26 แสดงถึงโพรโตคอล SSL

การพิสูจน์ตนของเซิร์ฟเวอร์ (SSL server authentication)

อนุญาตให้ผู้ใช้ตรวจสอบว่าติดต่อกับเซิร์ฟเวอร์ที่ถูกต้อง โดยจะใช้เทคนิคการเข้ารหัสแบบพับลิคคีย์เพื่อตรวจสอบการรับรองความถูกต้องของเซิร์ฟเวอร์ ตรวจสอบว่า public ID ถูกต้องและได้รับรับรอง โดย CA ทั้งนี้ความมั่นใจเป็นสิ่งที่สำคัญสำหรับผู้ใช้ ตัวอย่างเช่น การส่งหมายเลขบัตรเครดิตเข้าไปในระบบเครือข่าย ผู้ใช้ต้องมั่นใจว่าเซิร์ฟเวอร์ที่ติดต่อด้วยเป็นเซิร์ฟเวอร์ที่เราต้องการติดต่อด้วยจริง ๆ (ไม่ใช่เซิร์ฟเวอร์อื่นที่ปลอมตัวมา)

การพิสูจน์ตนของไคลเอ็นต์ (SSL client authentication)

อนุญาติให้เซิร์ฟเวอร์ตรวจสอบว่าติดต่อกับผู้ใช้ที่ถูกต้อง โดยจะใช้เทคนิคเดียวกับการพิสูจน์ตนของเซิร์ฟเวอร์ เพื่อตรวจสอบการรับรองความถูกต้องของผู้ใช้ และตรวจสอบว่า public ID ถูกต้องและได้รับรับรองโดย CA ทั้งนี้ความมั่นใจเป็นสิ่งที่สำคัญสำหรับเซิร์ฟเวอร์ ตัวอย่างเช่น การส่งความลับทางการเงินของธนาคารไปให้กับลูกค้า จะต้องทำการตรวจสอบว่า คนที่เราส่งข้อมูลให้เป็นลูกค้าจริง ๆ (ไม่ใช่คนอื่น ๆปลอมตัวมา)

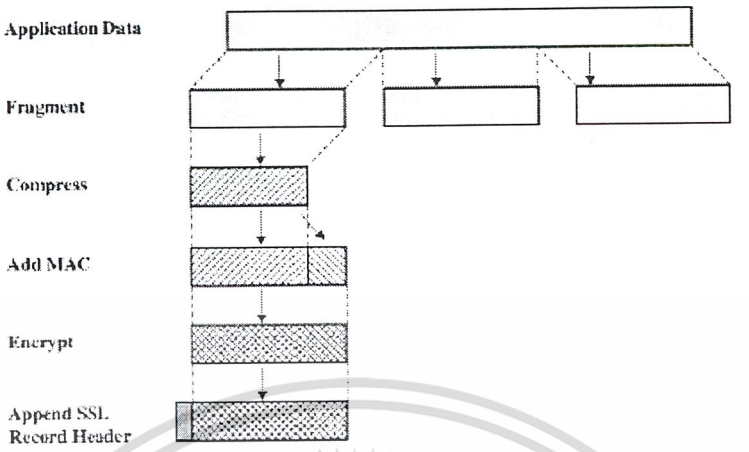
การเข้ารหัสในการเชื่อมต่อ (An encrypted SSL connection)

กำหนดให้ข้อมูลที่ส่งไปมาระหว่างไคลเอ็นต์กับเซิร์ฟเวอร์ ต้องผ่านกระบวนการเข้ารหัสและถอดรหัส ดังนั้นจะทำให้เพิ่มการรักษาความลับระหว่างผู้รับและผู้ส่งเพราะความลับเป็นสิ่งที่สำคัญสำหรับการติดต่อ ทั้งนี้ข้อมูลที่ส่งผ่าน SSL ที่มีการเข้ารหัส จะถูกป้องกันจากการดักจับได้ในแง่ที่ว่า ผู้ดักจับจะอ่านไม่รู้เรื่องเพราะผ่านการเข้ารหัสแล้ว

4.7.2 การทำงานของ SSL

SSL จะมีการแบ่งออกเป็น 2 ชั้นการทำงานย่อยคือ บริการ SSL และส่วนที่ทำหน้าที่ประสานงานระหว่าง 2 ฝั่ง คือ SSL Handshake Protocol, SSL Change Cipher Spec Protocol และSSL Alert Protocol

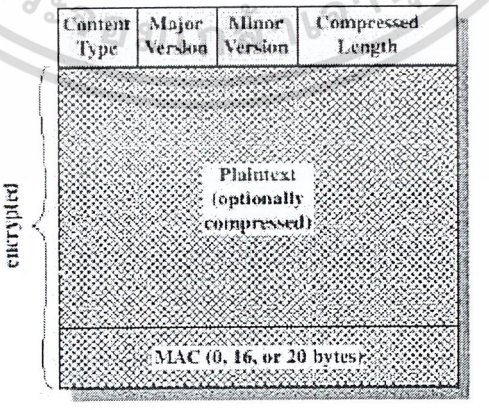
ในการทำงานของ SSL จะมีการสร้างเซสชันขึ้นมาก่อน โดยHandshake Protocol โดยเซสชันหนึ่งจะใช้สำหรับเครื่องหนึ่งไปเครื่องหนึ่งเท่านั้น และในเซสชันจะมีการกำหนดการทำงานและพารามิเตอร์ที่ใช้รับส่งระหว่างเครื่องเอาไว้ จากนั้นจึงมีการสร้างการเชื่อมต่อบนเซสชันอีกที



รูปที่ 4-27การทำงานทั้งหมดของ SSL Record Protocol

การทำงานของ SSL Record Protocol จะมีการบริการพื้นฐาน 2 ชนิดคือการเข้ารหัสโดยจะมีการใช้ซีเคร็ตคีย์ระหว่าง 2 ฝั่ง และรับรองการส่งโดยจะมีการสร้าง MAC (Message Authentication Code) ขึ้นมา โดย รูปที่ 4-27 แสดงการทำงานทั้งหมดของ SSL Record Protocol กล่าวคือ

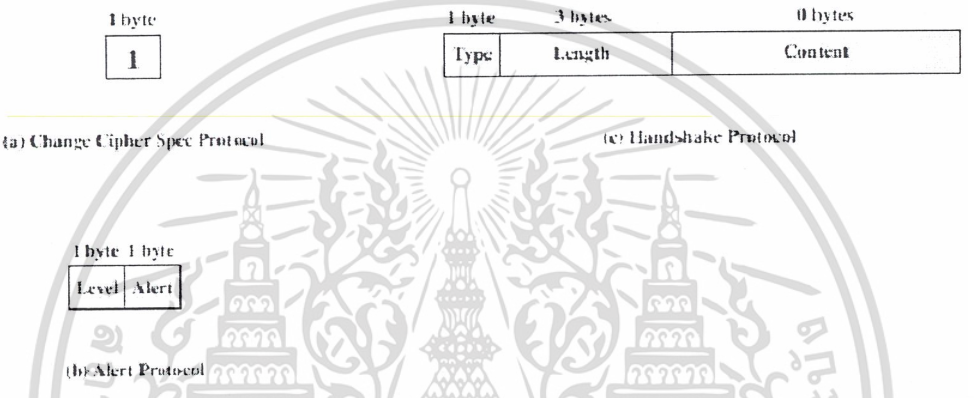
1. จะแบ่งข้อมูลออกเป็นบล็อกละ 16 KB หรือน้อยกว่าเพื่อที่จัดการได้ง่าย
2. นำข้อมูลมาบีบให้เล็กลง (เป็นออปชัน)
3. ใส่ข้อมูล MAC (Message Authentication Code) เพื่อทำการพิสูจน์ตน
4. เข้ารหัส
5. ใส่เฮดเดอร์ ซึ่งประกอบด้วย Content type ใช้บอกโพรโตคอลที่เรียกใช้,Major Versionและ Minor Version บอกเวอร์ชันของ SSL และ Compressed Length บอกความยาวของข้อมูลในแพ็กเก็ต ดังแสดงในรูป 4-28



รูปที่ 4-28 SSL Record Format

Change Cipher Spec Protocol จะประกอบด้วยฟิลด์เดียว และมีความยาวเพียงไบต์เดียว โดยมีค่าข้อมูลเท่ากับ 1 (ดูจากรูป 4-29 a) โดยข้อมูลนี้จะทำให้การทำงานของ SSL มีการก็อปปี้ข้อมูลจาก Pending State ไปยัง Current State ซึ่งทำให้มีการปรับปรุงข้อมูลเกี่ยวกับการเข้ารหัสที่ใช้ในคอนเน็กชัน

Alert Protocol จะประกอบด้วยข้อมูล 2 ไบต์ (ดูจากรูป 4-29 b) โดยไบต์แรกบอกระดับโดย 1 หมายถึง เตือน และ 2 หมายถึงร้ายแรง โดยหากระดับเป็นแบบร้ายแรง จะมีการยุติการเชื่อมต่อทัน และไบต์ที่ 2 เป็นรหัสที่บอกข้อมูลว่าเป็นการแจ้งข่าวสารอะไร



รูปที่ 4-29 SSL Protocol Payload

Handshake Protocol ทำให้ส่วนของเซิร์ฟเวอร์และบราวเซอร์สามารถทำการพิสูจน์ตนซึ่งกันและกันได้ และมีการกำหนดพารามิเตอร์ที่ใช้ในการเข้ารหัสและ MAC ระหว่างกัน โพรโตคอลนี้มีโครงสร้างดังรูปที่ 4-29c โดยจะประกอบด้วย 3 ฟิลด์ด้วยกันคือ

Type บอกชนิดของข้อมูล

Length บอกความยาวทั้งหมด

Content เป็นพารามิเตอร์ของข้อมูลแต่ละข้อมูล

บทที่ 5
ทฤษฎีการทดสอบไฟร์วอลล์

5.1 หลักการทดสอบ Firewall

จุดประสงค์ของการทดสอบก็เพื่อตรวจสอบว่าไฟร์วอลล์ทำงานได้อย่างที่เราต้องการหรือไม่ ทำงานอย่างมีประสิทธิภาพเพียงไร โดยควรจะต้องทำสิ่งเหล่านี้

วัดความสามารถของไฟร์วอลล์ในด้านต่าง ๆ คือ

- ด้านความปลอดภัย (Security)
- ด้านการจัดการ (Management)
- ด้านประสิทธิภาพ (Performance)
- ฟังก์ชันของไฟร์วอลล์ เช่น
  - การกรองแพ็กเก็ต (packet filtering)
  - การเก็บล็อก (logging)
  - ความสามารถในการแจ้งเตือน (alert capability) เมื่อเกิดเหตุการณ์ผิดปกติ

จากนั้น นำข้อมูลที่ได้ไปทำการเปรียบเทียบข้อเด่นข้อด้อยของไฟร์วอลล์แต่ละตัว

5.1.1 ด้านความปลอดภัย (Security)

เป็นด้านที่มีความสำคัญที่สุดในการทดสอบไฟร์วอลล์ เพราะจุดประสงค์ของไฟร์วอลล์ก็คือ การรักษาความปลอดภัย ซึ่งการทดสอบด้านนี้จะเป็นการตรวจสอบหาจุดบกพร่องในการรักษาความปลอดภัยของไฟร์วอลล์

ในการทดสอบความปลอดภัยของผลิตภัณฑ์ไฟร์วอลล์นี้ จะทำการทดสอบ 2 ส่วนด้วยกันคือ

- **การทดสอบการโจมตีโดยใช้ Denial of Services (DoS)** ซึ่งเป็นการโจมตีที่ทำให้โฮสต์ที่ถูกโจมตีไม่สามารถทำงานได้ตามปกติ แล้วดูว่าไฟร์วอลล์สามารถรับมือกับการโจมตีได้หรือไม่ โดยจะทำการโจมตีไปยังโฮสต์ที่อยู่หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ แล้วพิจารณาว่า ไฟร์วอลล์มีปฏิกิริยาต่อการโจมตีอย่างไร แจ้งเตือนหรือไม่ เป็นต้น รายละเอียดของ DoS แต่ละตัวจะแสดงอยู่ในบทที่ 6 Denial of Servic (DoS) ต่อไป

- **การทดสอบความปลอดภัยโดยใช้การสแกนเพื่อตรวจสอบ (Scanning)** ซึ่งเป็นการใช้โปรแกรมจำพวกพอร์ตสแกนเนอร์(Port Scanner), โปรแกรมสำรวจช่องโหว่ (Vulnerability Scanner) ที่จะนำมาใช้ในการทดสอบมีทั้งที่รันบนวินโดว์(Windows-based Scanner) และ ที่รันบนยูนิกซ์(Unix-based Scanner) ซึ่งรายละเอียดของแต่ละโปรแกรมนั้น จะได้แสดงในบทที่ 7 การสแกนเพื่อตรวจสอบ ต่อไป โดยเราจะพิจารณาว่าเมื่อทำการสแกนโฮสต์ที่ติดตั้งไฟร์วอลล์ หรือโฮสต์หลังไฟร์วอลล์แล้ว

ไฟร์วอลล์มีผลอย่างไรกับการสแกนนั้นๆ เช่น ทำให้สแกนไม่ได้คือไม่มีข้อมูลใดๆ ตอบสนองกลับกลับไปเลย หรืออาจมีข้อมูลตอบสนองเพียงบางส่วน หรืออาจได้รับข้อมูลตามปกติเหมือนไม่มีไฟร์วอลล์ป้องกัน ก็เป็นได้

5.1.2 ด้านการจัดการ (Management)

การจัดการและการคอนฟิกก็เป็นปัจจัยสำคัญอย่างหนึ่งที่จะต้องคำนึงถึง เพราะการมีระบบไฟร์วอลล์ที่สามารถจัดการ และตั้งค่าได้ง่ายจะทำให้สะดวกสำหรับผู้ดูแลระบบ และยังทำให้เกิดความผิดพลาดน้อยลงในการเซ็ตค่าต่าง ๆ ด้วย ในทางตรงข้าม ถ้ามีความซับซ้อนมากในการจัดการ ก็อาจจะทำให้เกิดความผิดพลาดในการปรับตั้งค่าให้กับไฟร์วอลล์ ซึ่งจะนำไปสู่ช่องโหว่ในการโจมตี

ในการทดสอบด้านการจัดการของผลิตภัณฑ์ไฟร์วอลล์นี้ จะทำการทดสอบ

1. ความยากง่ายในการติดตั้ง มี GUI ช่วยสำหรับการติดตั้งหรือไม่
2. ความยากง่ายในการคอนฟิก มี GUI สำหรับการปรับตั้งค่าหรือไม่

5.1.3 ด้านประสิทธิภาพ (Performance)

การวัดประสิทธิภาพของไฟร์วอลล์ ก็เพื่อที่จะทำให้มั่นใจได้ว่า ตัวไฟร์วอลล์จะไม่ไปถ่วงการส่งข้อมูลผ่านทางสายอินเทอร์เน็ตที่ค่อนข้างช้าอยู่แล้วให้ช้าลงไปอีกก่อนจะเริ่มทำการวัดประสิทธิภาพจะต้องทำการ ping ไปที่เครื่องเป้าหมาย (ที่มีไฟร์วอลล์) ก่อน เพื่อให้ CPU มีการทำงานอย่างเต็มประสิทธิภาพก่อน เราจะส่งแพ็กเก็ตไปเรื่อย ๆ จนกระทั่ง CPU utilization เท่ากับ 100 เปอร์เซ็นต์ แล้วเราสามารถพิจารณาประสิทธิภาพของไฟร์วอลล์จากจำนวนแพ็กเก็ตที่ไฟร์วอลล์รองรับได้เมื่อ CPU utilization เท่ากับ 100 เปอร์เซ็นต์

ไฟร์วอลล์ที่มีประสิทธิภาพดี ควรส่งถ่ายข้อมูลได้อย่างรวดเร็ว ไม่ควรเกิดปัญหาคอขวดของเครือข่าย อาจจะวัดโดยใช้ FTP หรือ ping

5.1.4 ทดสอบฟังก์ชันของไฟร์วอลล์

- **การกรองแพ็กเก็ต (packet filtering)**

  เพื่อทำการทดสอบว่าไฟร์วอลล์ทำงานได้ถูกต้องตามที่ต้องการหรือไม่ เป็นไปตามการปรับตั้งค่าของเราหรือเปล่า โดยขั้นตอนแรกต้องตั้งกฎที่จะให้ไฟร์วอลล์ทำตามขึ้นมาก่อน และสำหรับแต่ละกฎจะต้องระบุขอบเขตภายในกฎ

  ตัวอย่างกฎเช่น " อนุญาตให้แพ็กเก็ตที่เป็นทีซีพีผ่านจากโฮสต์ใด ๆ ไปยังเว็บเซิร์ฟเวอร์ผ่านพอร์ต 80 " เราก็จะแบ่งการทดสอบเป็น 3 ขอบเขตคือ

  1. การส่งแพ็กเก็ตที่เป็นทีซีพีไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ตน้อยกว่า 80
  2. การส่งแพ็กเก็ตที่เป็นทีซีพีไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ต 80
  3. การส่งแพ็กเก็ตที่เป็นทีซีพีไปยังเว็บเซิร์ฟเวอร์ ผ่านพอร์ตมากกว่า 80

จากนั้นสำหรับแต่ละขอบเขต ก็ให้สร้างการทดสอบที่อยู่ภายในขอบเขตนั้น ๆ โดยจะต้องทำการตรวจสอบว่าไฟร์วอลล์จะปฏิเสธหรือส่งต่อทุก ๆ แพ็กเก็ตสำหรับแต่ละขอบเขต

โดยทั้งนี้ในฟังก์ชัน

- **การเก็บล็อก (logging)**

  ทำการตรวจสอบถึงความยากง่ายในการจัดการล็อกไฟล์ เพราะกฎข้อหนึ่งของการบริการความปลอดภัยของระบบก็คือ การจัดให้มีล็อกไฟล์ของระบบ และต้องจัดให้มีการใช้งานข้อมูลที่บันทึกไว้อย่างสม่ำเสมอ และนอกจากนี้ยังต้องมีการจัดการใช้ข้อมูลล็อกไฟล์ได้อย่างมีประสิทธิภาพ เนื่องจากล็อกไฟล์ส่วนมากจะเป็นเท็กซ์ไฟล์ขนาดใหญ่ ซึ่งการหาแนวโน้มสำคัญ ๆ จากข้อมูลเหล่านี้เป็นเรื่องที่ยาก ดังนั้นจึงควรจะมีเครื่องมือที่จะอ่านข้อมูลภายในล็อกไฟล์เหล่านี้ และสรุปข้อมูลต่าง ๆ ออกมาแสดงในรูปแบบของกราฟหรือตาราง เพื่อให้สามารถทำความเข้าใจได้ง่ายขึ้น โดยในส่วนนี้ เราจะพิจารณาว่า ไฟร์วอลล์แต่ละตัวมีเครื่องมือที่จะอ่านข้อมูลจากล็อกไฟล์ และทำการสรุปออกมาในรูปกราฟิกหรือไม่

- **ความสามารถในการแจ้งเตือน (alert capability) เมื่อเกิดเหตุการณ์ผิดปกติ**

  โดยตรวจดูว่า ไฟร์วอลล์สามารถเตือนผู้ดูแลระบบ เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น ได้หรือไม่ โดยจะตรวจสอบว่า สามารถแจ้งเตือนผ่านสื่อดังนี้คือ

  - อีเมลล์
  - เพจเจอร์
  - SMS Message
  - ICQ

  โดยพิจารณาว่าไฟร์วอลล์ตัวนั้น ๆ มีความสามารถนี้หรือไม่ และถ้ามี ก็จะทำการพิจารณาระยะเวลาที่ใช้ในการแจ้งเตือนนั้น สามารถแจ้งเตือนได้รวดเร็วแค่ไหน

หมายเหตุ โปรเจ็คของเรามุ่งเน้นไปที่การทดสอบความปลอดภัย และอยู่ได้บนอินเตอร์เน็ตที่มีแต่ภัยคุกคาม เนื่องจากสองด้านนี้เป็นด้านที่สำคัญอย่างยิ่ง ผลิตภัณฑ์ไฟร์วอลล์ใดๆที่เราจะนำมาใช้ หากไม่สามารถรักษาความปลอดภัย หรือแจ้งเตือนการคุกคาม และไม่สามารถทนต่อภาวะถูกโจมตีได้แล้ว ไฟร์วอลล์นั้นก็ไม่สามารถทำงานได้จริงในโลกแห่งอินเตอร์เน็ต สำหรับในด้านอื่นๆ นั้นเราจะไม่ทำการทดสอบในชั้นนี้ เนื่องด้วย ด้านอื่นๆ อาทิ ด้านการจัดการ จะขึ้นอยู่กับความพึงพอใจและความเหมาะสมกับแต่ละองค์กร บรรทัดที่จะนำมาพิจารณาจึงแตกต่างกันไปในแต่ละบุคคล

5.2 การโจมตีโฮสต์หลังไฟร์วอลล์ด้วย DoS

โดยทั่วไปแล้ว การโจมตีเป้าหมายด้วย DoS จะมีจุดประสงค์เพื่อให้เซิร์ฟเวอร์ผู้ให้บริการต่างๆ (เช่น เว็บเซิร์ฟเวอร์ (Web Server)) หยุดทำงาน หรือทำงานได้ช้าลง ซึ่งผู้ดำเนินการเซิร์ฟเวอร์เหล่านี้จะติดตั้งไฟร์วอลล์เอาไว้ และจะให้เซิร์ฟเวอร์ผู้ให้บริการอยู่ในส่วนของ DMZ นั่นหมายความว่าเซิร์ฟเวอร์เหล่านี้เป็นโฮสต์ที่อยู่หลังไฟร์วอลล์

ในการโจมตีเมื่อยิง DoS มาที่เซิร์ฟเวอร์แล้ว เราจะพิจารณาผลที่เกิดขึ้นดังนี้

- อาการของโฮสต์หลังไฟร์วอลล์ที่ถูกยิง (เซิร์ฟเวอร์ผู้ให้บริการ) ซึ่งอาการที่อาจเกิดได้มีดังนี้
  - เครื่องแฮงก์ ต้องบูตเครื่องใหม่
  - เครื่องช้าลงมาก ทำอะไรไม่ได้
  - มีการใช้ซีพียู (CPU Usage) เป็น 100% อยู่ชั่วขณะหนึ่งแล้วกลับสู่สภาพเดิม
  - ไม่มีอาการใดๆเกิดขึ้น
- การแจ้งเตือนของไฟร์วอลล์โฮสต์

5.3 การโจมตีไฟร์วอลล์โฮสต์ด้วย DoS

ในบางครั้งผู้บุกรุกมุ่งโจมตีไปที่เครื่องไฟร์วอลล์ เพื่อทำให้ไฟร์วอลล์หยุดทำงานหรืออ่อนแอลง แล้วจะสามารถเข้าไปหาประโยชน์หรือเข้าไปสร้างความเสียหายที่เน็ตเวิร์ก และโฮสต์ภายในต่อไปได้ ซึ่งประเด็นนี้น่าสนใจที่ว่า ไฟร์วอลล์ที่เราใช้มีการจัดการอย่างไรกับปัญหานี้ ไฟร์วอลล์จะปฏิบัติตนอย่างไร เมื่ออยู่ในภาวะถูกโจมตีด้วย DoS

ในการโจมตีเมื่อเรายิง DoS ไปที่ไฟร์วอลล์โฮสต์แล้ว เราจะพิจารณาผลที่เกิดขึ้นดังนี้

- ปฏิกิริยาของไฟร์วอลล์โฮสต์ที่ถูกยิง ดังนี้
  - ไฟร์วอลล์คงอยู่ได้และปฏิบัติหน้าที่ได้ตามปกติ
  - ไฟร์วอลล์หยุดการทำงาน แต่ก่อนหยุดไม่สามารถปฏิบัติตามนโยบายป้องกันเน็ตเวิร์กภายในเมื่อพบสิ่งผิดปกติ (เช่น ปิด/เปิดเซอร์วิส)
  - ไฟร์วอลล์หยุดการทำงาน แต่ก่อนหยุดยังสามารถปฏิบัติตามนโยบายป้องกันเน็ตเวิร์กภายในเมื่อพบสิ่งผิดปกติ ไฟร์วอลล์ทำงานได้ช้าลง
- การแจ้งเตือนของไฟร์วอลล์โฮสต์
  - ไฟร์วอลล์โฮสต์มีการแจ้งเตือนว่าถูกโจมตีหรือไม่

บทที่ 6

Denial of Service (DoS)

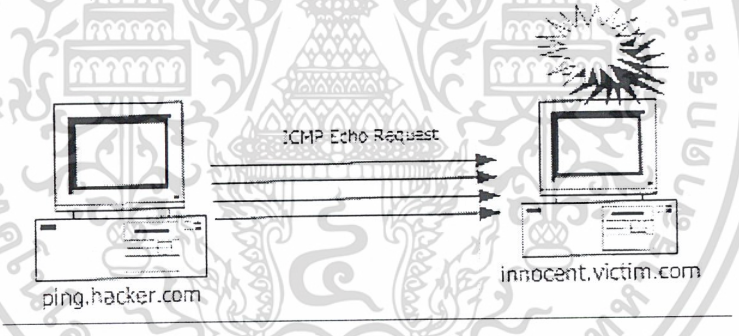
ในบทนี้ เราจะศึกษาเกี่ยวกับ DoS อย่างละเอียด โดยจะนำเสนอเป็นประเภทต่างๆของ DoS พร้อมทั้งเจาะลึกไปยัง DoS ที่ใช้แครชระบบปฏิบัติการวินโดว์ทั้งหลาย (Win32) โดยจะทำการทดสอบโจมตีระบบปฏิบัติการ Windows NT, XP, 2000 Professional และ 2000 Advanced Server ด้วยDoSที่เหมาะสม

6.1 DoSประเภทต่างๆ

6.1.1 Pingflood (ไฟล์ pingflood.c)

Ping Flood Attack เป็นการโจมตีที่ใช้ในยุคแรกๆ ของ DoS มิได้อาศัยเทคนิคซับซ้อน แต่อาศัยปริมาณแพ็กเก็ตมากๆ อย่างเดียว แต่ก็สร้างความเสียหายได้ไม่น้อย

- หลักการโจมตีแบบPing Flood



รูปที่ 6-1 แสดงการโจมตีแบบ Ping Flood

คือส่ง ICMP Echo Request ปริมาณมากๆไปยังเป้าหมายอย่างรวดเร็ว ทำให้ โฮสต์ที่ถูกโจมตีต้องคอยตอบ ICMP Echo Reply ตลอดเวลาจนแทบไม่มีเวลาทำงานอื่น อีกทั้งมีผลกับเน็ตเวิร์กที่เครื่องเป้าหมายตั้งอยู่ด้วย เนื่องจากจะเต็มไปด้วยแพ็กเก็ตเหล่านี้ โดยจะมีผลกระทบมากในเน็ตเวิร์กที่มีการใช้การสื่อสารเลเยอร์ต่ำร่วมกัน เช่น 10Base-5, 10Base-T ที่ใช้ฮับเป็นตัวกระจายสัญญาณ และปัจจัยสำคัญที่ทำให้การโจมตีสัมฤทธิ์ผลคือ แบนด์วิดธ์ของแฮกเกอร์ คือความเร็วของการส่ง ICMP แพ็กเก็ตเป็นหลัก

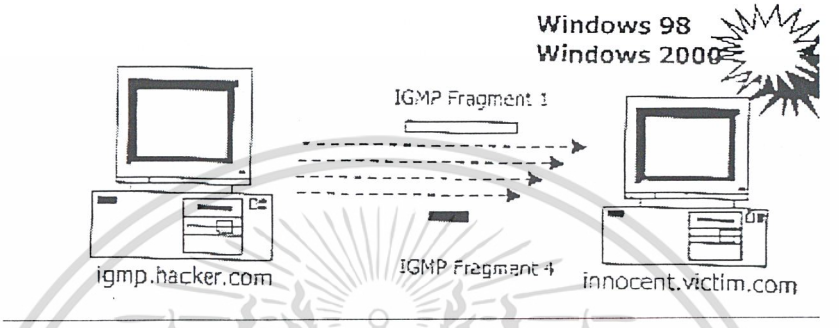
- คุณสมบัติของไฟล์

เมื่อทำการรัน มันจะส่ง ICMP Echo Request ออกไปทุกๆ วินาที การจะทำสำเร็จได้ โดยจะใช้ Alarm System call และการรอสัญญาณ SIGALRM จากเคอร์เนล (Kernel) Pingflood จะส่งสัญญาณ

SIGALRM จำนวนมากอย่างง่ายดายไปยัง Ping Process มันสามารถทำอย่างนี้ได้เนื่องจาก Ping Process นั้นเป็นเพียงUser ธรรมดาก็สั่งงานได้แล้ว

6.1.2 Fragmented IGMP (fawx.c, fawx2.c)

- **หลักการโจมตีแบบ Fragmented IGMP**



รูปที่ 6-2 การโจมตีแบบ Fragmented IGMP

วิธีนี้เป็นผลพวงจากข้อผิดพลาดภายในระบบปฏิบัติการของไมโครซอฟท์วินโดว์เอง ทั้ง 98 และ 2000 โดยการส่งชุดของแฟรกเมนต์ของแพ็กเก็ตของไอจีเอ็มพี (IGMP) ที่ใหญ่เกินไป และทำการส่งหลายๆครั้ง จะทำให้ระบบปฏิบัติการหยุดทำงานและปรากฏจอสีฟ้า ทำให้เป้าหมายเข้าใจว่าเกิดการผิดปกติของฮาร์แวร์ ซึ่งไฟร์วอลล์ บนWin32 ส่วนมากยังไม่สนับสนุนไอจีเอ็มพี ทำให้ประสบผลสำเร็จในการโจมตีมากกว่าที่จะใช้การโจมตีที่ไอซีเอ็มพี (ICMP) ซึ่งมักจะถูกกรองเอาไว้ได้โดยไฟร์วอลล์ (ระบบปฏิบัติการต้องได้รับการแพตซ์ (Patch) ที่ทางไมโครซอฟท์ได้ออกมาเพิ่มเติมแล้ว จะทำให้เซิร์ฟเวอร์เป้าหมายสามารถเปิดให้บริการได้อย่างมีเสถียรภาพต่อไป)

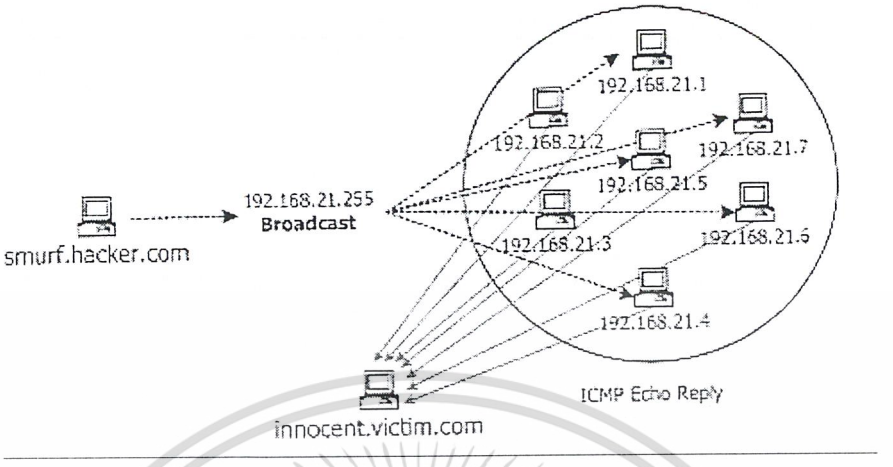
- **คุณสมบัติของไฟล์**

คอมไพล์บนลีนุกซ์ แต่ใช้โจมตีเป้าหมายที่ใช้ระบบปฏิบัติการของ ไมโครซอฟท์วินโดว์โดยเฉพาะ

6.1.3 Smurf

Smurf Attack เป็นการปรับปรุงเทคนิคของการ Flood เน็ตเวิร์กให้ฉลาดกว่าเดิม แทนที่จะอาศัยแบนด์วิดธ์ เพื่อโจมตีเป้าหมายอย่างเดียวแบบ Ping Flood Smurf ได้ค้นพบเทคนิคขยายการโจมตีทำให้แฮกเกอร์มีเครื่องทุ่นแรงและเปิดโอกาสให้ผู้ที่มีแบนด์วิดธ์ต่ำสามารถทำการ Flood ไปยังเป้าหมายได้รุนแรงทีเดียว

- **หลักการโจมตีแบบ Smurf Attack**



รูปที่ 6-3 การโจมตีแบบ Smurf Attack

Smurf Attack จะใช้ ICMP Echo Reply เป็นกลไกในการโจมตี, ใช้ร่วมกับเทคนิคของการปลอมหมายเลขไอพี และ จะส่ง ICMP Echo Request ไปยัง Broadcast Address

จากโปรโตคอลไอซีเอ็มพี เมื่อได้รับ ICMP Echo Request แล้ว จะต้องส่ง ICMP Echo Reply กลับไปยังหมายเลขไอพีของผู้ที่ส่ง Request มา อย่างไรก็ตามในข้อกำหนดของไอพีจะมีไอพีแอดเดรส ที่เป็นของบรอดคาสต์สำหรับเน็ตเวิร์กนั้น ซึ่งมีไว้เพื่อใช้ในกรณีที่ต้องการส่งข่าวสารถึงทุกๆโฮสต์ในเน็ตเวิร์ก นั่นคือ เมื่อส่งแพ็กเก็ตใดไปยังบรอดคาสต์แอดเดรส จะทำให้ทุกโฮสต์ได้รับแพ็กเก็ตนั้นอย่างทั่วถึง ดังนั้นเมื่อมีโฮสต์ใดที่ส่ง ICMP Echo Request มายังบรอดคาสต์ก็จะทำให้ทุกๆโฮสต์ทั้งหมดที่อยู่ในเน็ตเวิร์กนั้นจะได้รับ ICMP Echo พร้อมกัน และจะตอบกลับด้วย ICMP Echo Reply ไปยังผู้ส่งเสมอ และตอบกลับเท่ากับจำนวนเครื่องที่อยู่ในเน็ตเวิร์กนั้นในขณะนั้นเลยที่เดียว ซึ่งปรากฏการณ์เช่นนี้เรียกว่าการขยายสัญญาณ (Amplification) อัตราการขยายขึ้นอยู่กับปริมาณโฮสต์ที่อยู่ในเน็ตเวิร์กขณะนั้น

การโจมตีเริ่มด้วยการที่แฮกเกอร์จะส่ง ICMP Echo Request ไปยังบรอดคาสต์แอดเดรสทำให้โฮสต์ทั้งหมดในเน็ตเวิร์กขณะนั้นทำการตอบกลับมายังไอพีแอดเดรสที่ระบุว่าเป็นของผู้ส่ง ดังนั้นวิธีการโจมตีก็ต้องใช้ควบคู่ไปกับการปลอมไอพีแอดเดรส โดยให้ไอพีแอดเดรสต้นทางของ ICMP Echo Request ที่ส่งไปนั้นเป็นไอพีแอดเดรส ของเป้าหมายที่เราจะโจมตี ทำให้เป้าหมายได้รับ ICMP Echo Reply จำนวนมากจนไม่สามารถสื่อสารกับผู้อื่นบนเน็ตเวิร์กได้หรือถึงกับหยุดทำงานไปเลย

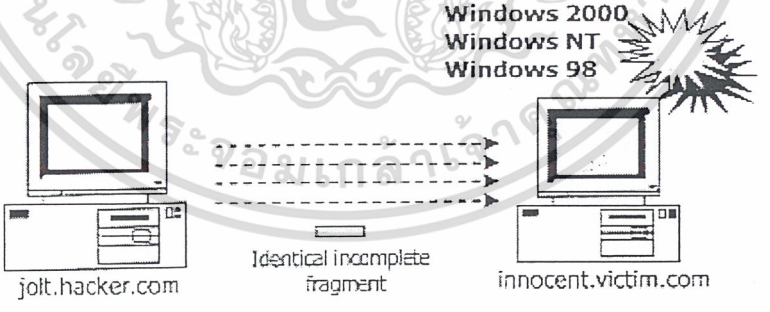
ทั้งนี้ เทคนิคของ Smurf ซึ่งอาศัยการบรอดคาสต์ไปยังทุกโฮสต์ ดังนั้นอาจใช้ได้ผลไม่ดีนักกับเน็ตเวิร์กที่ใช้เราเตอร์ เพราะสามารถจำกัดขอบเขตการบรอดคาสต์ได้โดยกำหนดที่ Access Control List (ACL) ของเราเตอร์

6.1.4 Jolt (jolt3.c)

เป็นDoS ที่อาศัยช่องโหว่ของการ "รีแอสเซมเบิลแฟรกเมนต์" (IP Fragment Reassembly) โดยมีรายละเอียดคือ

ในกระบวนการจัดการแฟรกเมนต์ทั่วๆไปที่มีอยู่ในระบบปฏิบัติการคือ การนำข้อมูลในแฟรกเมนต์มาเติมลงในหน่วยความจำที่จัดสรรเพื่อรีแอสเซมเบิลทั่วไป ซึ่งในเมื่อระบบปฏิบัติการไม่สามารถที่จะทราบได้ว่าชุดของแฟรกเมนต์ที่ส่งเข้ามาเช่นนี้เป็นแฟรกเมนต์ที่ผิดปกติจึงพยายามจะรีแอสเซมเบิลแฟรกเมนต์เหล่านี้ให้กลับมาเป็นดาต้าแกรมตามปกติให้ได้ แต่เมื่อแฟรกเมนต์เหล่านี้ล้วนแต่เป็นแฟรกเมนต์ที่ไม่สมบูรณ์การทำงานของระบบปฏิบัติการจึงเสียเวลาเปล่า ประกอบกับหมายเลขของแฟรกเมนต์ (Fragment ID) นั้นเป็นหมายเลขซ้ำเดิมตลอดทำให้ระบบปฏิบัติการต้องนำข้อมูลของแฟรกเมนต์เดิมลงไปยังหน่วยความจำตำแหน่งที่ได้จัดสรรไว้เดิมตลอด ซึ่งกระบวนการดังกล่าวจะใช้เวลาของซีพียู มากกว่าการรีแอสเซมเบิลทั่วไป ทำให้เมื่อได้รับแฟรกเมนต์เข้ามาในปริมาณที่สูงมากๆ ระบบปฏิบัติการจึงต้องใช้เวลาการประมวลผลของซีพียูมากขึ้นเป็นลำดับ ประกอบกับโปรแกรมส่วนที่จัดการเกี่ยวกับการสื่อสารข้อมูลในเน็ตเวิร์กนั้นจะเป็นโปรแกรมที่ทำงานในระดับต่ำและทำงานที่ลำดับความสำคัญสูง เมื่อโปรแกรมในส่วนของทีซีพี/ไอพี ที่จัดการเกี่ยวกับแฟรกเมนต์ต้องการใช้ซีพียู ระบบปฏิบัติการก็จะอนุญาตให้เข้าใช้ได้ก่อนโปรแกรมอื่นๆที่มีความสำคัญต่ำกว่า จนเมื่อโฮสต์ถูกโจมตีจากแฟรกเมนต์มากทำให้ซีพียูไม่มีเวลาเหลือพอที่จะไปประมวลผลงานอื่นๆได้เลยแม้แต่อินพุตและเอาท์พุต ทำให้โฮสต์ไม่ตอบสนองใดๆกับผู้ใช้เลยจนกว่าแพ็กเก็ตของการโจมตีจะยุติลง หรือผู้ใช้ทำการปิดเครื่องไป

- **หลักการโจมตีแบบ Jolt**



รูปที่ 6-4 การโจมตีแบบ Jolt

Jolt เป็นการโจมตีโดยอาศัยแฟรกเมนต์ทั่วไป โดยจะส่งแฟรกเมนต์แพ็กเก็ตซ้ำๆ จำนวนมากอย่างต่อเนื่องมาที่เซิร์ฟเวอร์เป้าหมาย หากข้อมูลมีความเร็วมาก และ ปริมาณมาก ก็จะทำให้เครื่องทำงานช้าลง แต่หากสามารถเพิ่มความเร็ว และปริมาณในการส่งข้อมูลมากพอก็จะทำให้หยุดทำงานไปเลย สังเกตได้จากการใช้ซีพียูของ เซิร์ฟเวอร์ได้ ซึ่งจะขึ้นสูงถึง100% นั่นคือซีพียูถูกใช้ไปในการจัดการกับ Fragment หมดนั่นเอง จึงไม่ตอบสนองกับผู้ใช้

จากการสังเกต ระบบปฏิบัติการของไมโครซอฟท์ จะอ่อนไหวต่อแฟรกเมนต์แพ็กเก็ตเป็นพิเศษ การ DoS สำหรับวินโดว์ส่วนใหญ่สามารถกระทำได้โดยง่าย โดยอาศัย Fragment และ จะส่งผลเสียต่อเป้าหมายอย่างมาก อาการที่เกิดขึ้นกับเซิร์ฟเวอร์เมื่อถูกโจมตีด้วยแฟรกเมนต์ คือ หยุดทำงานและแสดงหน้าจอสีฟ้า ซึ่งต้องทำการบูตใหม่, หยุดทำงานชั่วขณะ ไม่ตอบสนองใดๆคล้ายจะแฮงค์ ไม่สามารถควบคุมเครื่องได้ ก็ต้องรีเซ็ตหรือบูตใหม่ และ อีกอาการหนึ่งคือ ทำงานช้าลงมาก ตอบสนองช้า เพราะซีพียูใช้ในการจัดการกับแฟรกเมนต์ที่เข้ามา

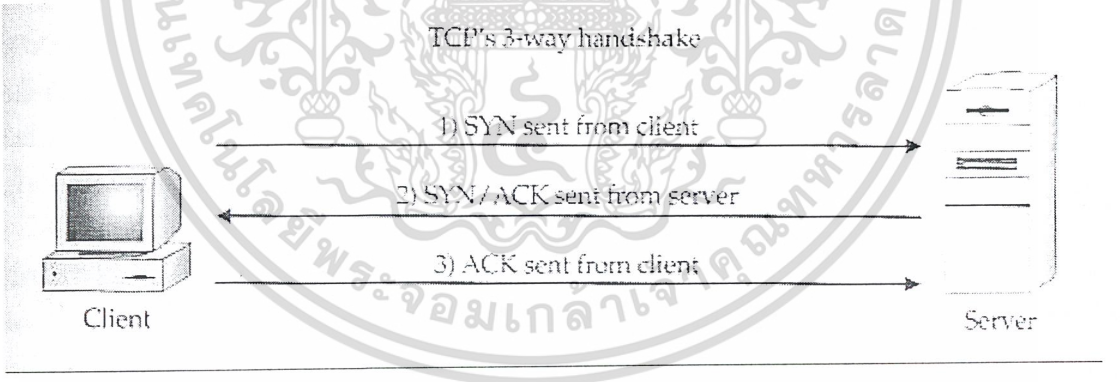
- คุณสมบัติของไฟล์

นี้จะทำให้การใช้ซีพียูของเครื่องเป้าหมายที่ใช้ Windows 98, NT4/SP5,6 และ Win2k เป็น 100% และต้องทำการคอมไพล์บนลีนุกซ์

6.1.5 Synflood (synflood.c)

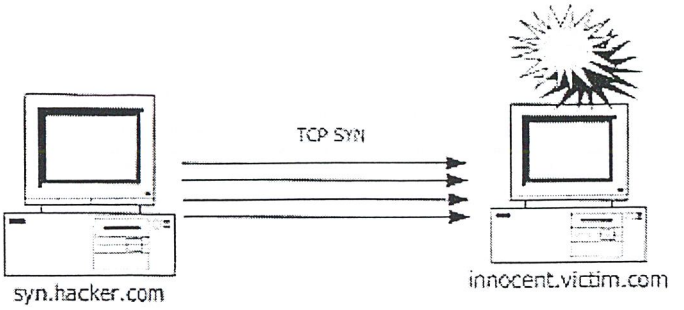
SYN Flood Attack เป็นการโจมตีที่ใช้การหาช่องโหว่จากของโพรโตคอลทีซีพี (TCP: Transmission Control Protocol) ในส่วนของการทำ 3-way Handshake

- **หลักการโจมตีแบบ SYN Flood**



รูปที่ 6-5 การทำ 3-way Handshake

เป็นการโจมตีโดยการส่ง SYN จำนวนมาก ทำให้เซิร์ฟเวอร์ต้องคอยตอบด้วย SYN,ACK ตลอดเวลาดังรูปบน ทำให้เซิร์ฟเวอร์ไม่มีเวลาไปทำอย่างอื่น ผลกระทบอย่างน้อยที่สุดก็คือเซิร์ฟเวอร์ที่ถูกโจมตีจะทำงานช้าลงกว่าเดิมแน่นอน โดยถ้าหากระบบปฏิบัติการของเซิร์ฟเวอร์เป้าหมายจัดการหน่วยความจำได้ไม่มีประสิทธิภาพพอ เซิร์ฟเวอร์ก็อาจจะหยุดทำงานได้ ปัจจัยสำคัญที่ทำให้การโจมตีสัมฤทธิ์ผลคือความเร็วสูงสุดที่แฮกเกอร์สามารถส่ง SYN ได้



รูปที่ 6-6 การโจมตีแบบ SYN Flood

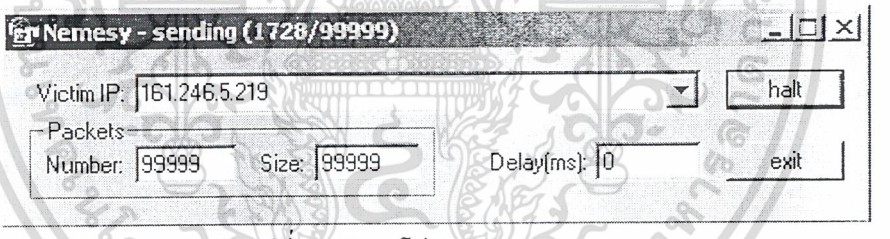
- คุณสมบัติของไฟล์

  คอมไพล์บนลีนุกซ์ และสามารถใช้โจมตีได้กับทุกระบบปฏิบัติการ

หมายเหตุ ประเภทของDoS ที่ยกขึ้นมากล่าวนี้เป็นเพียงส่วนหนึ่งเท่านั้น โดยที่ได้นำมานี่ส่วนใหญ่จะเป็นประเภทที่ใช้ได้ผลหรือสร้างมาเพื่อโจมตีระบบปฏิบัติการวินโดว์ (Win32)

6.2 DoS ที่หยิบยกมาใช้ในการทดสอบ

6.2.1 โปรแกรม Nemesy



รูปที่ 6-7 แสดงโปรแกรม Nemesy

- หลักการโจมตี
  - ส่ง IGMP Fragment แพ็กเก็ต และ ทำ IP Fragement Reassemblyไปยังเครื่องเป้าหมายได้โดยกำหนดขนาดและจำนวนแพ็กเก็ตเองได้ ดังภาพ
  - ทำ IP Spoofing คือ ปลอม IP ของเครื่องต้นทางที่รันโปรแกรมได้
- ระบบปฏิบัติการที่โจมตีได้ผล
  - ตระกูลวินโดว์ทั้งหลาย (Win32)
- คอมไพล์และรันบนระบบปฏิบัติการ
  - วินโดว์ (Win32)

6.2.2 Jolt2.c

- หลักการโจมตี
  - เป็นDoS แบบที่ใช้ช่องโหว่ของการทำรีแอสเซมเบิลแฟรกเมนต์ของวินโดว์ โดยจะส่งแฟรกเมนต์แพ็กเก็ตซ้ำๆ จำนวนมากอย่างต่อเนื่องมาที่เซิร์ฟเวอร์เป้า

หมาย หากข้อมูลมีความเร็วมาก และ ปริมาณมาก ก็จะทำให้เครื่องทำงานช้าลง แต่หากสามารถเพิ่มความเร็ว และปริมาณในการส่งข้อมูลมากพอก็จะทำให้หยุดทำงานไปเลย สังเกตได้จากการใช้ซีพียูของ เซิร์ฟเวอร์ได้ ซึ่งจะขึ้นสูงถึง 100% นั่นคือ CPU ถูกใช้ไปในการจัดการกับ Fragment หมดนั่นเอง จึงไม่ตอบสนองกับผู้ใช้

- ระบบปฏิบัติการที่โจมตีได้ผล
  - ตระกูลวินโดว์ทั้งหลาย (Win32)
- คอมไพล์และรันบนระบบปฏิบัติการ
  - ลีนุกซ์ (Linux)

  การใช้คำสั่ง : jolt2 [-s แอดเดรสต้นทาง] [-p พอร์ต] แอดเดรสปลายทาง

6.2.3 Jolt3.c

- หลักการโจมตี
  - เหมือนกับ jolt2 ต่างกันที่ jolt3 นี้สามารถเพิ่มรอบการโจมตีได้ โดยใส่เป็นจำนวนครั้งที่จะทำการส่งแพ็กเก็ตไปได้
- ระบบปฏิบัติการที่โจมตีได้ผล
  - ตระกูลวินโดว์ทั้งหลาย (Win32)
- คอมไพล์และรันบนระบบปฏิบัติการ
  - ลีนุกซ์ (Linux)

  การใช้คำสั่ง : jolt2 [-s src_addr] [-p port] [-n number] des_addr

6.2.5 Killwin.c

- หลักการโจมตี
  - เป็นการปรับปรุงเทคนิคของ Winnuke ซึ่งเป็นDoSที่จะส่งแพ็กเก็ตที่ "Out of Band" มายังพอร์ต 139 (พอร์ตNetBios) ซึ่งเป็นพอร์ต TCP ของเครื่องเป้าหมาย เมื่อเครื่องได้รับก็จะแครช กลายเป็นจอสีฟ้า
- ระบบปฏิบัติการที่โจมตีได้ผล
  - วินโดว์ 95, 98
- คอมไพล์และรันบนระบบปฏิบัติการ
  - ลีนุกซ์ (Linux)

  การใช้คำสั่ง : killwin <target> [-p port (Default 139)] [-t hits (Default 1)]

6.2.6 Synflood.c

- หลักการโจมตี
  - แบบ Synflood ดังที่อธิบายไว้ในหัวข้อ 6.1 DoSประเภทต่างๆ
- ระบบปฏิบัติการที่โจมตีได้ผล

- ทุกระบบปฏิบัติการ

- คอมไพล์และรันบนระบบปฏิบัติการ
  - ลีนุกซ์ (Linux)

การใช้คำสั่ง : synflood <src_addr> <des_addr> <port> <num>

6.3 ผลการทดสอบโจมตีระบบปฏิบัติการWindowsด้วย DoS

	WinNT	WinXP	Win2k Professional	Win2k Advanved Server
Nemesy	A	A	A	A
Jolt2.c	A	A	A	A
Jolt3.c	A	A	A	A
Killwin.c	B	B	B	B
Synflood.c	C	C	C	C

ตารางที่ 6-1 แสดงผลการโจมตีด้วย DoS ชนิดต่างๆ ไปยังระบบปฏิบัติการวินโดว์วอร์ชันต่างๆ

ผลกระทบที่อาจเกิดขึ้นกับโฮสต์ที่ถูกโจมตี

A : เป็นปกติตามเดิม

B : ตอบสนองช้ามากๆ ทำงานไม่ได้เลยจนต้องบูตเครื่องใหม่

C : หยุดทำงานไม่ตอบสนองใดๆ ต้องบูตเครื่องใหม่

E : หยุดทำงาน และวินโดว์ปรากฏจอสีฟ้า (Blue Screen) จำเป็นต้องบูตเครื่องใหม่

หมายเหตุ การโจมตีด้วย DoS นี้ใช้ความเร็วของการ์ดแลนด์เป็น 100.0 เมกะบิตต่อวินาที (Mbps)

จากการทดลอง จะเห็นได้ว่า DoS ที่มีผลต่อระบบปฏิบัติการวินโดว์มากที่สุด คือ killwin และ synflood ดังนั้น ในการทดสอบไฟร์วอลล์ในบทที่ 9 เราจะใช้ DoS 2 ไฟล์นี้ในการโจมตี

บทที่ 7
การสแกนเพื่อตรวจสอบ

7.1 ความสำคัญของการสแกนพอร์ต

เมื่อพอร์ตเป็นสิ่งสำคัญ การสแกนพอร์ตก็ถือเป็นขั้นตอนที่สำคัญเช่นเดียวกัน สิ่งที่ทำให้การสแกนพอร์ตเป็นการกระทำที่ถือได้ว่ามุ่งร้ายต่อระบบคือ ผลลัพธ์ของการสแกนพอร์ตจะทำให้แฮกเกอร์สามารถล่วงรู้ได้ว่ามีแอพพลิเคชันใดบ้างที่ทำงานอยู่บนโฮสต์ โดยปกติทั่วไปแล้วแอพพลิเคชันแต่ละชนิดที่เปิดให้บริการอยู่จะได้หมายเลขพอร์ตที่ตายตัวและรู้จักกันโดยทั่วไป เมื่อผลการสแกนปรากฏว่ามีพอร์ตใดที่เปิดให้บริการอยู่ก็สามารถนำข้อมูลที่ได้มาเทียบกับบริการมาตรฐาน ก็จะทราบได้ว่ามีแอพพลิเคชันใดที่ให้บริการอยู่ และข้อมูลเหล่านี้ก็จะเป็นประโยชน์ต่อการเลือกเทคนิคในการโจมตีต่อไป

การสแกนพอร์ตนี้จะเป็นการสำรวจแต่ละโฮสต์ โดยผลลัพธ์ที่ได้จะทำให้ทราบว่าพอร์ตเป้าหมายเปิดให้บริการอยู่หรือไม่ แต่เนื่องจากการสแกนพอร์ตนี้เป็นการกระทำที่ส่อเจตนามุ่งร้ายอย่างชัดเจน เพราะในการปฏิบัติงานทั่วไปมีการสแกนพอร์ตน้อยมาก การสแกนพอร์ตจึงเข้าข่ายการบุกรุกเครือข่าย ดังนั้นเทคนิคในการสแกนจึงมีวิธีการที่ซับซ้อนขึ้นเรื่อย ๆ เพื่อมิให้เป้าหมายรู้ตัว และไม่สามารถตรวจพบได้โดยง่าย

ทั้งนี้เราจะนำการสแกนพอร์ตมาใช้ในการตรวจสอบว่า ไฟร์วอลล์ที่ทำมาทดสอบนั้น สามารถป้องกันการสแกนพอร์ตได้หรือไม่

7.2 เทคนิคในการสแกนพอร์ต

7.2.1 TCP connect scanning

เทคนิคนี้เป็นการทำทีเสมือนว่าต้องการติดต่อไปยังแอพพลิเคชันที่ทำงานอยู่บนเซิร์ฟเวอร์นั้น โดยส่งสัญญาณไปขอเริ่มสื่อสารบนพอร์ตเป้าหมายบนเซิร์ฟเวอร์ จากนั้นก็รอผลตอบกลับจากพอร์ตนั้น ๆ ว่าจะตอบรับคำขอหรือไม่ หากมีแอพพลิเคชันอยู่ที่พอร์ตดังกล่าว ก็ย่อมจะต้องตอบรับและส่งสัญญาณมาเพื่อเริ่มการเชื่อมต่อในลำดับถัดไป

7.2.2 TCP SYN (half open) scanning

การสแกนพอร์ตแบบนี้ หากพิจารณาดูแล้วจะใกล้เคียงกับวิธี TCP connect scanning แต่สิ่งที่แตกต่างกันคือ วิธีนี้ผู้สแกนจะทำการส่ง SYN แพ็กเก็ตมาเพื่อทำการติดต่อเองโดยตรงกับเป้าหมายโดยไม่ผ่านระบบปฏิบัติการ และรอผลการตอบรับของเป้าหมายกลับมาด้วย SYN ACK หรือหากไม่มีแอพพลิเคชันทำงานอยู่ก็จะตอบกลับมาด้วย RST

7.2.3 TCP FIN (stealth) scanning

เมื่อ TCP SYN scanning นั้นสามารถทำได้โดยง่ายก็ย่อมสามารถถูกตรวจจับได้โดยง่ายเช่นกัน แต่อีกวิธีหนึ่งคือ TCP FIN scanning เป็นการสแกนที่สังเกตได้ค่อนข้างยาก โดยเฉพาะหากลำดับของพอร์ตของการสแกนเป็นแบบสุ่มและเว้นระยะพอสมควร ซึ่งจะทำให้แพ็กเก็ตที่ใช้สแกนสามารถเล็ดรอดเข้ามาได้โดยไร้ร่องรอย

โดยปกติ FIN แพ็กเก็ตจะเป็นแพ็กเก็ตของ TCP ที่จะส่งเมื่อยุติการติดต่อ นั่นหมายถึงจะต้องมีการสื่อสารกันมาก่อนแล้ว แต่ TCP FIN scanning จะเป็นการส่ง FIN แพ็กเก็ตไปยังเป้าหมายโดยไม่มีการสื่อสารใด ๆ มาก่อน และเป็นที่แน่นอนว่าเป้าหมายที่ได้รับจะต้องทราบอย่างแน่นอนว่า ไม่เคยได้รับการติดต่อจากไอพีแอดเดรสและพอร์ตต้นทางนั้นมาก่อนเลย แต่อย่างไรโฮสต์เป้าหมายก็ยังคงตอบ FIN แพ็กเก็ตนั้นกลับไปอยู่ดี

จุดสำคัญก็คือโดยปกติการตอบ FIN แพ็กเก็ตกลับไปของพอร์ตที่เปิดไว้และพอร์ตที่ไม่ได้เปิดให้บริการก็ไม่เหมือนกัน หากเป็นพอร์ตที่ไม่ได้เปิดอยู่โฮสต์ก็จะตอบด้วย RST FLAG และหากเป็นพอร์ตที่เปิดให้บริการอยู่ก็จะต้องด้วย FIN ACK กลับไป

7.2.4 TCP SYN/FIN scanning

วิธีการนี้จะใช้ TCP Flag ทั้ง SYN และ FIN พร้อมกัน ซึ่งการส่งทั้ง SYN และ FIN พร้อมกัน นั้นไม่มีกำหนดอยู่ในโปรโตคอล ดังนั้นการตอบรับของโฮสต์แต่ละประเภทในกรณีที่เปิดพอร์ตนั้นอยู่จะแตกต่างกันออกไป อาจจะตอบรับเป็น SYN ACK หรือ FIN ACK ส่วนการตอบรับในกรณีที่พอร์ตปิดจะตอบเหมือนกันคือ RST

7.2.5 TCP Xmas scanning

TCP Xmas scanning จะไม่ใช้ TCP Flag ทั้ง 3 ตัวซึ่งเป็นที่สังเกตได้ง่าย คือ SYN-ACK-RST ในการสแกน ทั้งนี้เพื่อหลีกเลี่ยงการตรวจจับให้มากที่สุด แต่จะใช้ FIN Push URGENT ไปยังพอร์ตเป้าหมายที่เครื่องปลายทาง ในกรณีที่พอร์ตปิดเครื่องปลายทางจะส่งแพ็กเก็ต TCP RST ของทุก ๆ พอร์ตที่ปิดอยู่กลับมาให้

7.2.6 TCP FTP bounce scanning

เป็นเทคนิคการสแกนโดยอาศัยวิธีการอย่างลับ ๆ ในการเปิดคอนเน็กชันติดต่อไปยัง FTP Server โดยอาศัยประโยชน์จากการที่ FTP Server สนับสนุนการติดต่อแบบพร็อกซี นอกจากนี้ FTP bounce scanning ยังสามารถถูกใช้เพื่อส่งเมล์ปลอมที่ไม่สามารถติดตามได้ว่ามาจากไหน ใช้เพื่อการโจมตี FTP Server, ทำให้ฮาร์ดดิสก์เต็ม, หลบหลีกการตรวจจับของไฟร์วอลล์ และยังสร้างการรบกวนให้เกิดขึ้นกับระบบปลายทางด้วย

ยิ่งไปกว่านั้น เรายังสามารถคอนเน็กเข้าไปที่ FTP Server ก่อนแล้วค่อนสแกนเครื่องเป้าหมายเพื่อให้ดูเหมือนว่า คอนเน็กชันที่เปิดเข้าไปเพื่อสแกนนั้นเป็นคอนเน็กชันที่วิ่งมาจาก FTP Server วิธีนี้จะช่วยป้องกันการติดตามกลับว่าแฮกเกอร์มาจากไหน อีกทั้งยังช่วยให้สามารถผ่านเข้าไปในระบบได้ ถึงแม้ว่าระบบจะมีการเซ็ตฟิลเตอร์แอดเดรสเอาไว้ก็ตาม

ถึงแม้เทคนิคนี้จะมีข้อดีดังกล่าวที่กล่าวมาก็ตาม แต่มันทำงานได้ค่อนข้างช้า นอกจากนั้น FTP Server เวอร์ชันใหม่ ๆ ก็มักไม่ยอมให้การกระทำดังกล่าวเกิดขึ้นได้

7.2.7 UDP raw ICMP port unreachable scanning

UDP raw ICMP port unreachable scanning เปรียบเสมือน TCP SYN scanning เพราะเป็นการส่งแพ็กเก็ตไปทดสอบการตอบรับของยูดีพีพอร์ตนั้น ๆ โดยการพยายามจะติดต่อกับแอพพลิเคชันที่ทำงานบนพอร์ตนั้น ๆ ตามปกติแล้วให้โฮสต์นั้นตอบรับกลับมาอย่างใดอย่างหนึ่ง เพียงแต่ยูดีพีไม่มี Flag จึงไม่สามารถใช้เทคนิคอื่นมาหลบหลีกหรืออำพรางตนเองได้

7.3 พอร์ตสแกนเนอร์ที่นำมาทดสอบ

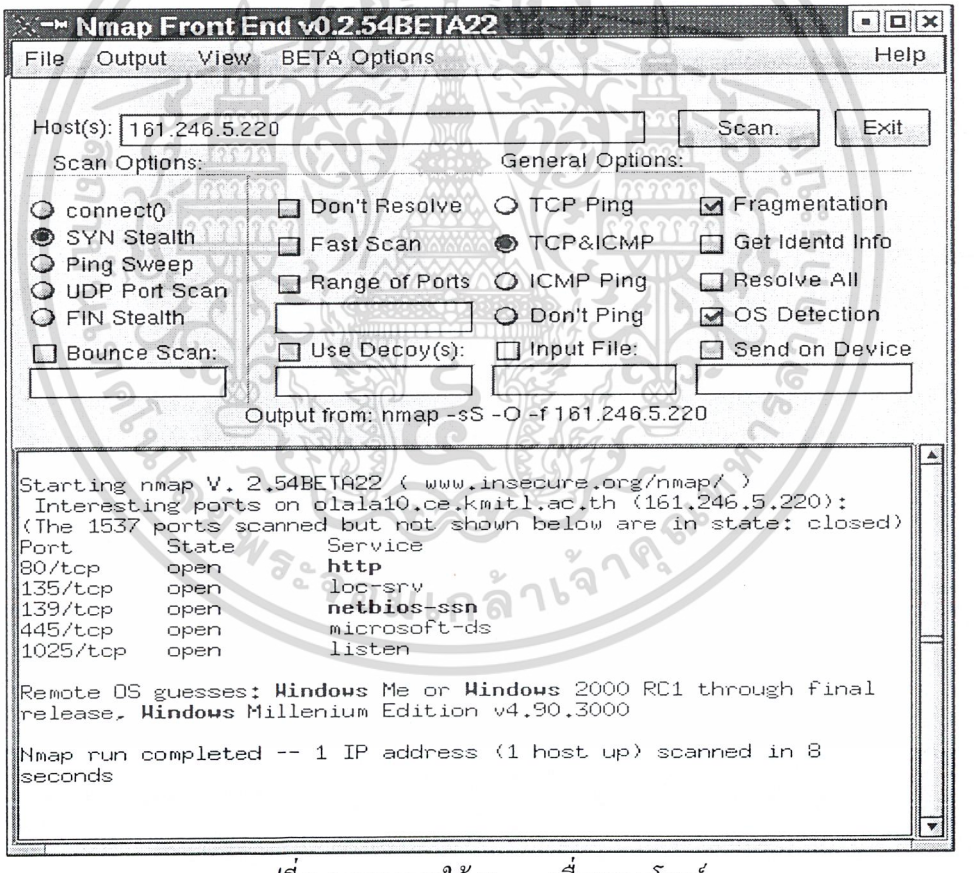
7.3.1 เครื่องมือสแกนพอร์ตที่งานอยู่บนยูนิกซ์

- **Nmap (Network Mapper)**

Nmap สามารถสแกนได้ทั้งพอร์ตทีซีพี และยูดีพีที่ให้เราระบุหมายเลขไอพีแอดเดรส โดยได้รวมเอาเทคนิคการสแกนต่าง ๆ ที่กล่าวไปข้างต้นทั้งหมด ซึ่งค่อนข้างหายากสำหรับเครื่องมือตัวเดียวแต่ให้ได้ครบทุกเทคนิค

Nmap มีฟีเจอร์หลายอย่างที่ใช้ในการเข้าไปสำรวจ รูปแบบการใช้คำสั่งของ Nmap นั้นมีทั้งที่ให้เราใช้สแกนเครื่องปลายทางเพียงเครื่องเดียว หรือสแกนเครื่องทั้งหมดในเน็ตเวิร์กก็ได้

การใช้งาน Nmap สามารถใช้งานได้ทั้งแบบที่เป็นคอมมานไลน์(command line) และยังมีแบบที่มียูสเซอร์อินเตอร์เฟซสวยงามให้ใช้งานด้วย สำหรับตัวอย่างการใช้งาน **Nmap** เป็นดังรูปที่ 7-1



รูปที่ 7-1 แสดงการใช้ Nmap เพื่อสแกนโฮสต์

ในฝั่งของ Scan Options ผู้ใช้สามารถเลือกได้ว่าจะใช้เทคนิคในการสแกนพอร์ตแบบใด สำหรับออปชันที่มีให้เลือกคือ connect(), SYN Stealth, Ping Sweep, UDP Port Scan, FIN Stealth และBounce Scan

สำหรับ Bounce Scan จะทำงานได้เฉพาะภายใต้เงื่อนไขบางอย่างเท่านั้น เงื่อนไขแรกคือ FTP Server จำเป็นต้องมีไดเร็กทอรีที่เปิดให้สามารถอ่านและเขียนข้อมูลได้ อย่างเช่น /incoming เงื่อนไขที่สองคือ FTP Server จะต้องยินยอมให้ Nmap ป้อนหมายเลขพอร์ตปลอมเข้าไปด้วยคำสั่ง PORT

ในฝั่งของ General Options ผู้ใช้สามารถเลือกออปชั่นในการสแกนได้เพิ่มเติม คือ

Fast Scan	สแกนเฉพาะพอร์ตที่ระบุในพอร์ตลิสต์ของ Nmap
Range of Ports	เพื่อใส่ช่วงของพอร์ตที่จะให้Nmap ทำการสแกน
Use Decoy(s)	เพื่อใช้ในการลวงไฟร์วอลล์ที่ไซต์ปลายทางโดยการส่งแพ็กเก็ตปลอมจำนวนมากที่ไม่เกี่ยวข้องกับการสแกนเข้าไปในระบบในขณะเดียวกับที่ทำการสแกนจริงไปด้วยพร้อม ๆ กัน และเพื่อให้ยากต่อการติดตาม Nmap จึงได้มีการปลอมหมายเลขไอพีแอดเดรสของเซิร์ฟเวอร์อื่นที่มีตัวตนอยู่จริง ออปชั่นนี้อาจทำให้เครื่องปลายทางตอบสนองแพ็กเก็ตปลอมดังกล่าว พร้อมๆ กับตอบสนองต่อแพ็กเก็ตที่เราส่งเข้าไปสแกนด้วย ยิ่งไปกว่านั้นยังช่วยสร้างภาระให้กับไฟร์วอลล์หรือเครื่องปลายทางด้วยในการตรวจสอบว่าแพ็กเก็ตไหนถูกส่งมาจากเซิร์ฟเวอร์ที่ถูกต้องหรือแพ็กเก็ตไหนถูกส่งมาเพื่อการสแกน แต่ขอให้จำไว้ว่าไอพีแอดเดรสปลอมดังกล่าวต้องเป็นไอพีแอดเดรสของเซิร์ฟเวอร์ที่มีอยู่จริง มิฉะนั้นแล้วการสแกนจะกลายเป็นการทำ SYN Flood
Fragmentation	เพื่อแฟรกเมนต์หรือหั่นซอยแพ็กเก็ตออกเป็นแพ็กเก็ตย่อยๆ ทั้งนี้เพื่อให้ยากต่อการตรวจจับของไฟร์วอลล์ อย่างไรก็ดีออปชั่นนี้มักใช้ได้กับไฟร์วอลล์ที่ไม่ฉลาดมากนักใช้ไม่ได้ผลกับไฟร์วอลล์สมัยใหม่
Get Identd Info	เป็นวิธีการคอนเน็กเข้าไปที่พอร์ต 113เพื่อค้นหาชื่อผู้ใช้ที่เปิดคอนเน็กชันแบบ TCP (TCP connection) กับเครื่องปลายทางอยู่ ส่วนใหญ่แล้วผลลัพธ์ที่ได้มักเป็นชื่อเจ้าของ (owner) ของโปรเซสที่ทำงานอยู่บนพอร์ตใดพอร์ตหนึ่ง ซึ่งผลลัพธ์ตรงนี้มักมีประโยชน์สำหรับการโจมตียูนิกซ์
OS Detection	ใช้ TCP/IP fingerprint เพื่อตรวจสอบระบบปฏิบัติการ

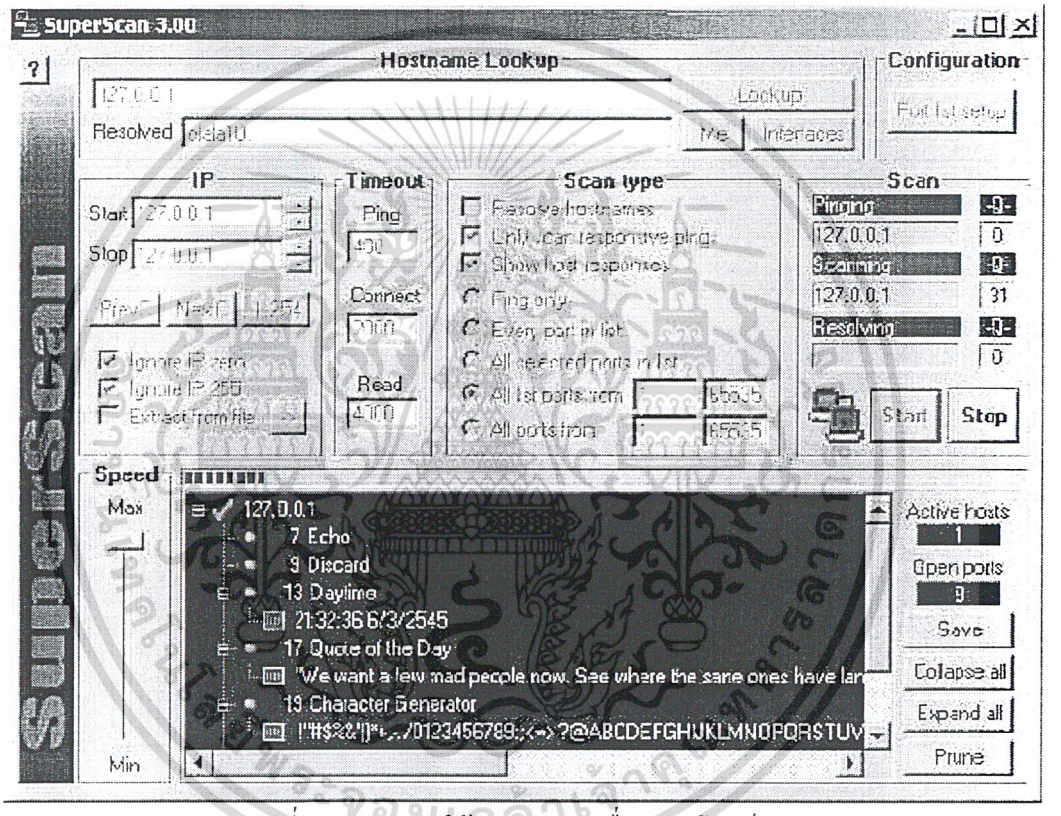
7.3.2 เครื่องมือสแกนพอร์ตที่งานอยู่บนวินโดวส์

- **SuperScan**

SuperScan ใช้สำหรับสแกนพอร์ตทีซีพี ที่ให้เราระบุหมายเลขไอพีแอดเดรส (IP Address) และหมายเลขพอร์ตที่เราต้องการ ส่วนปุ่ม Extract From File ก็ช่วยอำนวยความสะดวกคือ เราสามารถอ่านเท็กซ์ไฟล์ใด ๆ เพื่อดึงเอาเฉพาะหมายเลขไอพีแอดเดรสและชื่อโฮสต์ออกมา ปุ่มนี้ฉลาดพอที่จะค้นหาไอพีแอดเดรสและชื่อโฮสต์เองโดยที่คุณไม่ต้องเซ็ตอะไรเป็นพิเศษ ขอเพียงแต่ให้ลบข้อความและคำต่าง ๆ ที่ไม่จำเป็นออกจากเท็กซ์ไฟล์

SuperScan จะอนุญาตให้คลิกปุ่ม Browse และ Extract as ได้หลายครั้งตามต้องการในกรณีที่เราต้องการถึงเอาไอพีแอดเดรสและชื่อโฮสต์มาจากหลาย ๆ ไฟล์ เมื่อชื่อโฮสต์ถูกโหลดเข้ามา ก็สามารถคลิกปุ่ม Resolve เพื่อแปลงชื่อโฮสต์เป็นไอพีแอดเดรสได้ด้วย

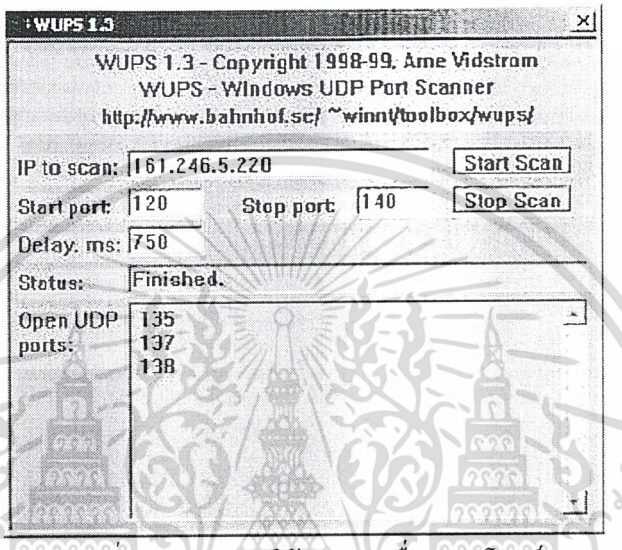
นอกจากนี้ SuperScan ยังได้ให้ไฟล์ที่รวบรวมหมายเลขพอร์ตที่สมบูรณ์ที่สุดด้วย โดยหลังจากที่โหลดไฟล์ดังกล่าวแล้ว ก็จะสามารถเลือกหรือไม่เลือกพอร์ตต่าง ๆ ได้ด้วยตนเอง รูปที่ 7-2 จะแสดงตัวอย่างการใช้งาน SuperScan



รูปที่ 7-2 แสดงการใช้ Superscan เพื่อสแกนโฮสต์

- **WUPS (Windows UDP Port Scanner)**

WUPS ใช้สำหรับสแกนพอร์ตยูดีพี ที่ให้เราระบุหมายเลขไอพีแอดเดรส (IP Address) และช่วงของพอร์ตที่เราต้องการ โดยมีข้อเสียคือ สามารถทำการสแกนได้ทีละโฮสต์เท่านั้น สำหรับตัวอย่างการใช้งาน WUPS จะแสดงในรูปที่ 7-3



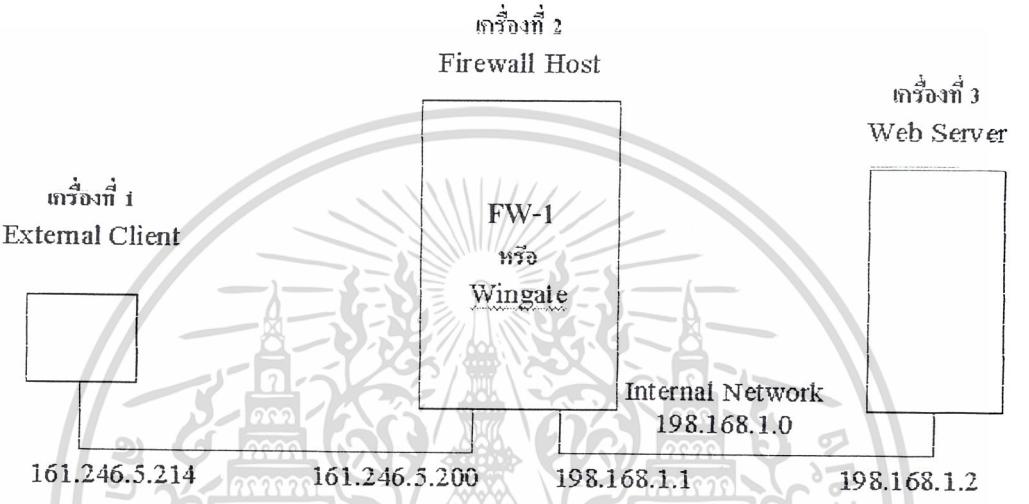
รูปที่ 7-3 แสดงการใช้ WUPS เพื่อสแกนโฮสต์

บทที่ 8

คุณลักษณะของผลิตภัณฑ์ไฟร์วอลล์ที่นำมาทดสอบ และการคอนฟิก

8.1 เน็ตเวิร์กโทโพโลยี ของเรา (Network Topology)

8.1.1 เน็ตเวิร์กโทโพโลยีสำหรับทดสอบเอนเตอร์ไพรส์ไฟร์วอลล์



รูปที่ 8-1 แสดงเน็ตเวิร์กโทโพโลยี สำหรับทดสอบเอนเตอร์ไพรส์ไฟร์วอลล์

สำหรับเน็ตเวิร์กโทโพโลยีที่วางขึ้นมาเพื่อทำการทดสอบนั้น ประกอบด้วยเครื่อง 3 เครื่อง คือ

1. ไคลเอ็นต์ภายนอก (External Client)

เป็นไคลเอ็นต์ที่ไม่ได้อยู่ในเครือข่ายภายใน (internal network) โดยจุดประสงค์หลักของเครื่องนี้คือ ใช้เพื่อทำการโจมตีไฟร์วอลล์โฮสต์ และโฮสต์หลังไฟร์วอลล์ โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู : AMD Thunderbird
- หน่วยความจำ : 256 เมกกะไบต์
- การ์ดแลนความเร็ว : 10/100 เมกกะบิตต่อวินาที (Mbps) 1 ใบ
- ระบบปฏิบัติการ : Mandrake 8.1

2. ไฟร์วอลล์โฮสต์ (Firewall Host)

เป็นเครื่องเซิร์ฟเวอร์ที่เป็นไฟร์วอลล์โฮสต์ โดยจุดประสงค์หลักของเครื่องนี้คือ ใช้เพื่อเป็นไฟร์วอลล์ในการป้องกันเครือข่ายภายใน โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู : AMD K6-2 350 MHz
- หน่วยความจำ : 384 เมกกะไบต์
- การ์ดแลนความเร็ว : 10/100 เมกกะบิตต่อวินาที 2 ใบ
- ระบบปฏิบัติการ : Window 2000 Server

3. ไคลเอ็นต์ภายใน (Internal Client)

เป็นไคลเอ็นต์ที่อยู่ในเครือข่ายภายใน โดยจุดประสงค์หลักของเครื่องนี้คือ ใช้เป็นเว็บเซิร์ฟเวอร์ (Web Server) เพื่อให้บริการ โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู : Pentium3 450 MHz
- หน่วยความจำ : 384 เมกกะไบต์
- การ์ดแลนความเร็ว : 10/100 เมกกะบิตต่อวินาที 1 ใบ
- ระบบปฏิบัติการ : Window 2000 Server

วิธีการเชื่อมต่อ

ใช้สายครอส (cross) 2 สายเพื่อทำการเชื่อมต่อดังนี้

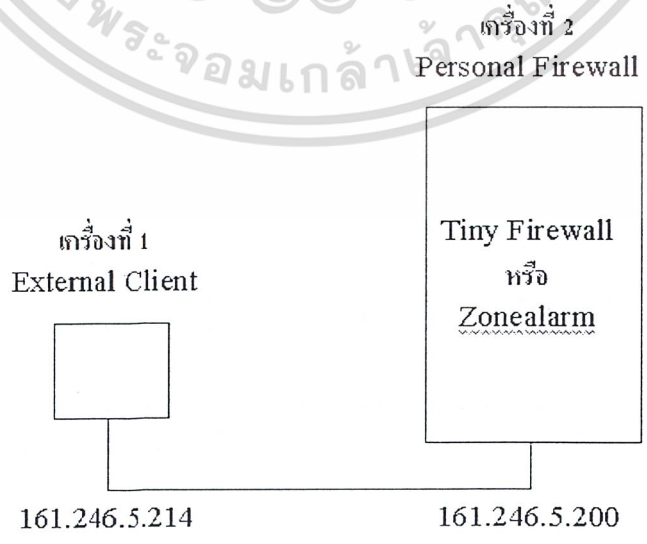
1. สายที่ 1 ต่อระหว่างไคลเอ็นต์ภายนอกกับไฟร์วอลล์โฮสต์ สำหรับเหตุที่เชื่อมต่อกันด้วยสายครอสก็เพื่อจะทำให้ความเร็วที่ใช้โฉมตีเป็น 100 MHz หรืออาจมีทางเลือกอีกวิธีหนึ่งก็คือเชื่อมต่อกันด้วยอับความเร็ว 100 MHz ก็ได้ โดยระบุไอพีแอดเดรสของการ์ดแลนดังนี้

- ไคล์เอ็นต์ภายนอก : 161.246.5.214
- ไฟร์วอลล์โฮสต์ : 161.246.5.220

2. สายที่ 2 ต่อระหว่างไฟร์วอลล์โฮสต์กับไคลเอ็นต์ภายใน โดยระบุไอพีแอดเดรสของการ์ดแลนดังนี้

- ไฟร์วอลล์โฮสต์ : 198.168.1.2
- ไคลเอ็นต์ภายใน : 198.168.1.2

8.1.2 เน็ตเวิร์กโทโพโลยีสำหรับทดสอบเพอร์ซันนอลไฟร์วอลล์



รูปที่ 8-2 แสดงเน็ตเวิร์กโทโพโลยีสำหรับเพอร์ซันนอลไฟร์วอลล์

สำหรับเน็ตเวิร์กโทโพโลยีที่วางขึ้นมาเพื่อทำการทดสอบนั้น ประกอบด้วยเครื่อง 2 เครื่อง คือ

1. ไคลเอ็นต์ภายนอก (External Client)

เป็นไคลเอ็นต์ที่ไม่ได้อยู่ในเครือข่ายภายใน (internal network) โดยจุดประสงค์หลักของเครื่องนี้คือ ใช้เพื่อทำการโจมตีไฟร์วอลล์โฮสต์ โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู : AMD Thunderbird
- หน่วยความจำ : 256 เมกกะไบต์
- การ์ดแลนความเร็ว : 10/100 เมกกะบิตต่อวินาที 1 ใบ
- ระบบปฏิบัติการ : Mandrake 8.1

2. เพอร์ซันนอลไฟร์วอลล์ (Personal Firewall)

เป็นเครื่องเซิร์ฟเวอร์ที่เป็นไฟร์วอลล์โฮสต์ โดยจุดประสงค์หลักของเครื่องนี้คือ ใช้เพื่อเป็นไฟร์วอลล์ในการป้องกันเครื่องคอมพิวเตอร์ส่วนบุคคล (personel computer) โดยมีสเป็กของเครื่องเป็นดังนี้

- ซีพียู : AMD K6-2 350 MHz
- หน่วยความจำ : 384 เมกกะไบต์
- การ์ดแลนความเร็ว : 10/100 เมกกะบิตต่อวินาที 1 ใบ
- ระบบปฏิบัติการ : Window 2000 Server

วิธีการเชื่อมต่อ

ต่อการ์ดแลนของทั้ง 2 เครื่องเข้ากับเน็ตเวิร์ก 161.246.5.0 โดยระบุไอพีแอดเดรสของการ์ดแลนดังนี้

- ไคล์เอ็นต์ภายนอก : 161.246.5.214
- ไฟร์วอลล์โฮสต์ : 161.246.5.220

8.2 ผลิตภัณฑ์ไฟร์วอลล์ที่นำมาศึกษา

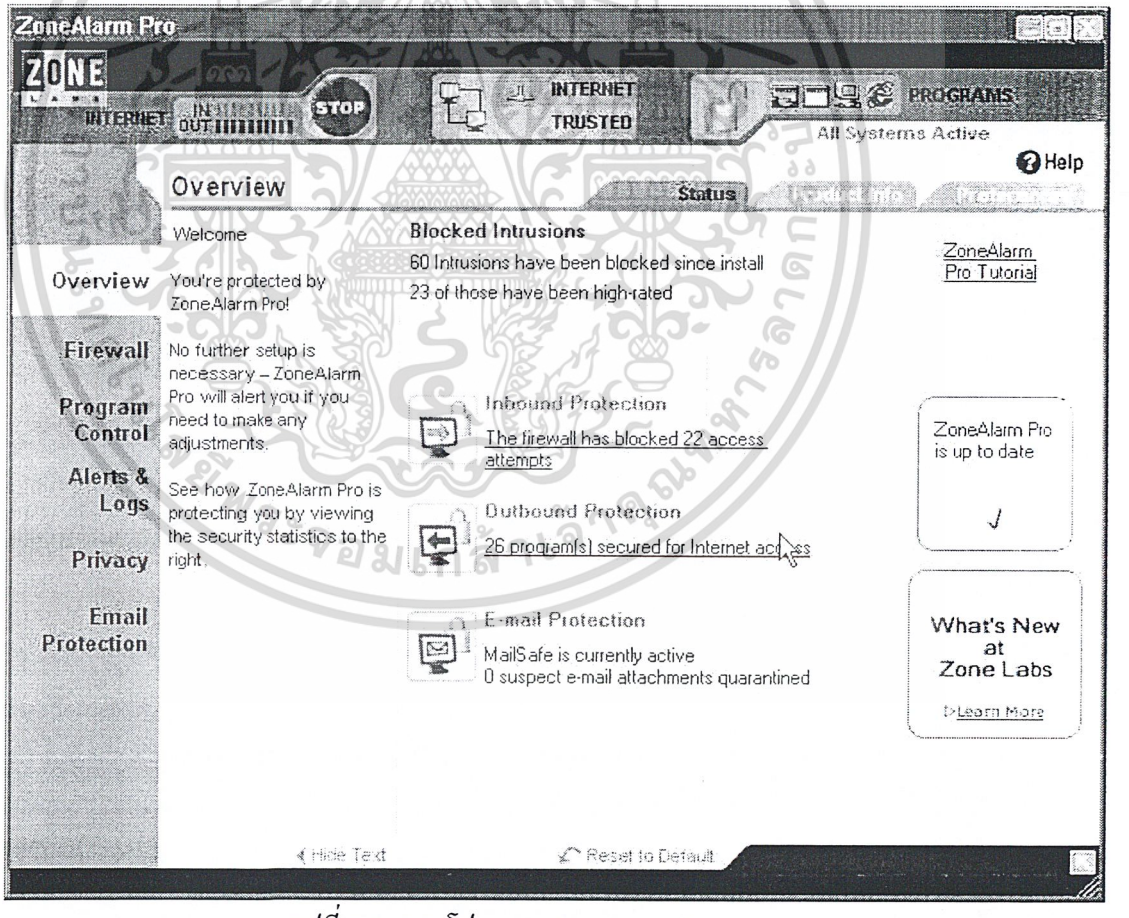
ไฟร์วอลล์ที่เรานำมาทดสอบมีทั้งประเภทแอพพลิเคชันพรอกซี (Application Proxy) และประเภทสเตตฟูลอินสเป็กชัน (Stateful Instpection) และมีทั้งเอนเตอร์ไพรส์ไฟร์วอลล์ (Enterprise Firewall) และเพอร์ซันนอลไฟร์วอลล์ (Personal Firewall)

8.2.1 ZoneAlarm Pro V.3.0

8.2.1.1 คุณลักษณะของ ZoneAlarm Pro

- **ความต้องการของระบบ (System Requirement)**
  - ไอบีเอ็ม พีซี หรือเทียบเท่า
  - ระบบโปรเซสเซอร์ 486 ขึ้นไป
  - ระบบปฏิบัติการวินโดว์ 98/ME/NT/2000/XP
  - RAM 8 เมกะไบต์ (MB)
  - เนื้อที่ว่างฮาร์ดดิส 10 เมกะไบต์

- เป็นผลิตภัณฑ์เชิงการค้า (Commercial product) ซึ่งที่เรามาใช้นี้ เป็นการดาวน์โหลดมาทดลองใช้เท่านั้น
- ZoneAlarm Pro มี 4 ส่วนหลักๆที่ใช้ต่อสู้กับการคุกคามบนอินเตอร์เน็ต ดังนี้
  - **ไฟร์วอลล์**
  - **ส่วนควบคุมโปรแกรม** จะป้องกันโปรแกรมจำพวกโทรจันไม่ให้เข้ามาฝังตัวและติดตั้งอยู่ในเครื่องคอมพิวเตอร์ได้
  - **การรักษาความเป็นส่วนตัว** คือจะป้องกันเครื่องจากความวุ่นวายของ cookie และการป๊อปอัพ (Pop up) โฆษณาต่างๆ และยังป้องกันเครื่องจากสคริปต์ และวัตถุฝังตัวต่างๆ จากเว็บเพจ
  - **การป้องกันอีเมล์** ปกป้องเครื่องจากหนอนอินเตอร์เน็ต และไวรัส ทั้งที่รู้จักแล้วและยังไม่รู้จักซึ่งจะมากับอีเมล์ได้
- ใช้งานง่าย พร้อมทั้งมี Wizard ช่วยในการคอนฟิก อีกทั้งในการปรับแต่งค่าต่างๆ ก็ทำได้ง่ายดาย และเข้าใจง่าย

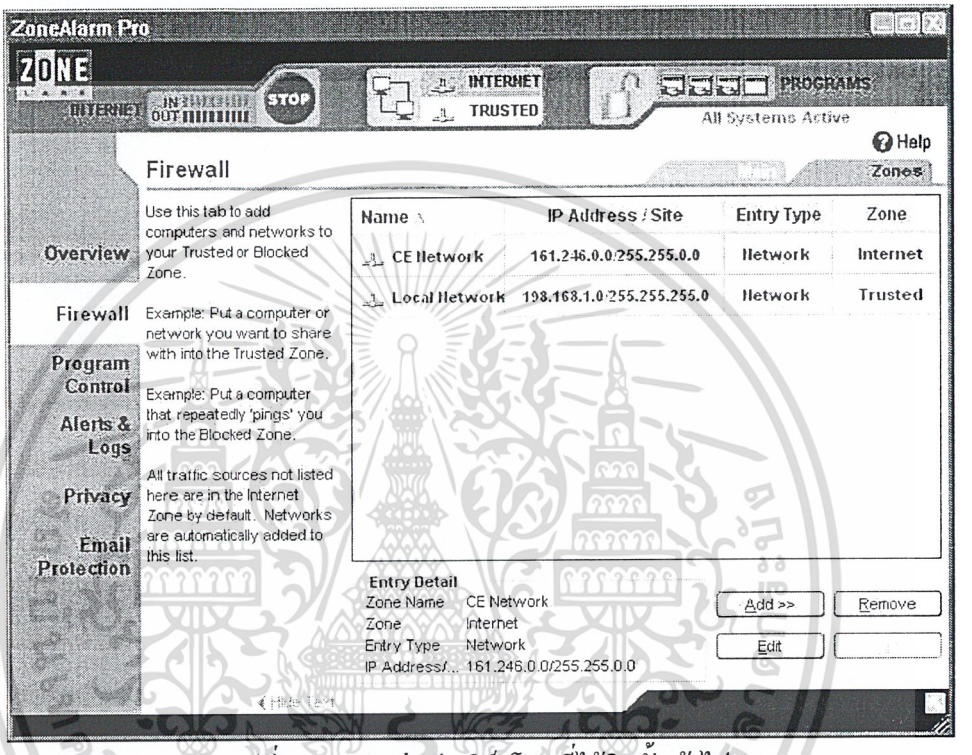


รูปที่ 8-3 แสดงโปรแกรมZoneAlarm Pro

8.2.1.2 การคอนฟิก ZoneAlarm Pro

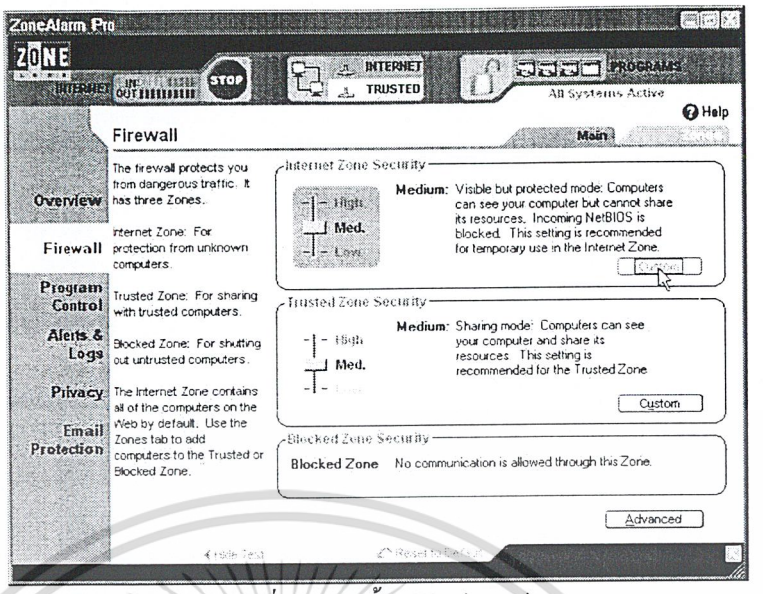
ในการปรับแต่งค่าต่างๆ ในโปรแกรม จะอธิบายตามจุดต่างๆ ที่เราให้ความสนใจ นั่นคือทางด้านความปลอดภัย ดังนี้

- เซ็ตค่าเน็ตเวิร์กของเราตามเน็ตเวิร์กโทโพโลยี โดยให้เน็ตเวิร์กภายนอกคือเน็ตเวิร์กของภาควิชา และ เน็ตเวิร์กภายในคือเน็ตเวิร์กที่เราสร้างขึ้นใหม่ตามโทโพโลยี พร้อมทั้งเชื่อถือเน็ตเวิร์กภายในไว้ด้วย

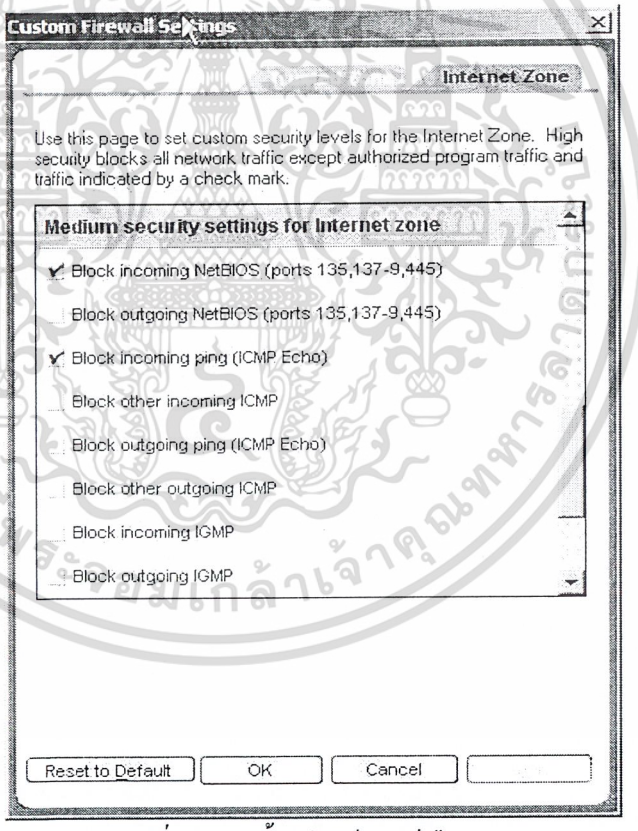


รูปที่ 8-4 แสดงค่าเน็ตเวิร์กโซนที่ได้ติดตั้งเข้าไป

- ทำการตั้งค่าการรักษาความปลอดภัยของไฟร์วอลล์ สำหรับความปลอดภัยจากอินเตอร์เน็ต เน็ตเวิร์ก เลือกแบบกลาง (Medium) และยังเข้าไปปรับแต่งเพิ่มเติมได้อีก โดยการกดปุ่ม Custom เพื่อเลือกตั้งค่าเพิ่มเติมเอง แล้วเลือกเช็คดังรูปที่ 8-6 เพื่อบล็อกพอร์ตเกี่ยวกับ NetBios ซึ่งเป็นจุดอ่อนที่เป็นเป้าหมายของผู้บุกรุกในการโจมตีด้วย DoS ส่วนมาก ส่วนเช็คที่สองนั้นเป็นการบล็อกการ Ping เข้ามากจากภายนอก



รูปที่ 8-5 การตั้งค่าไฟร์วอลล์



รูปที่ 8-6 การตั้งค่าไฟร์วอลล์เลือกเอง

8.2.2 Tiny Personal Firewall V.2

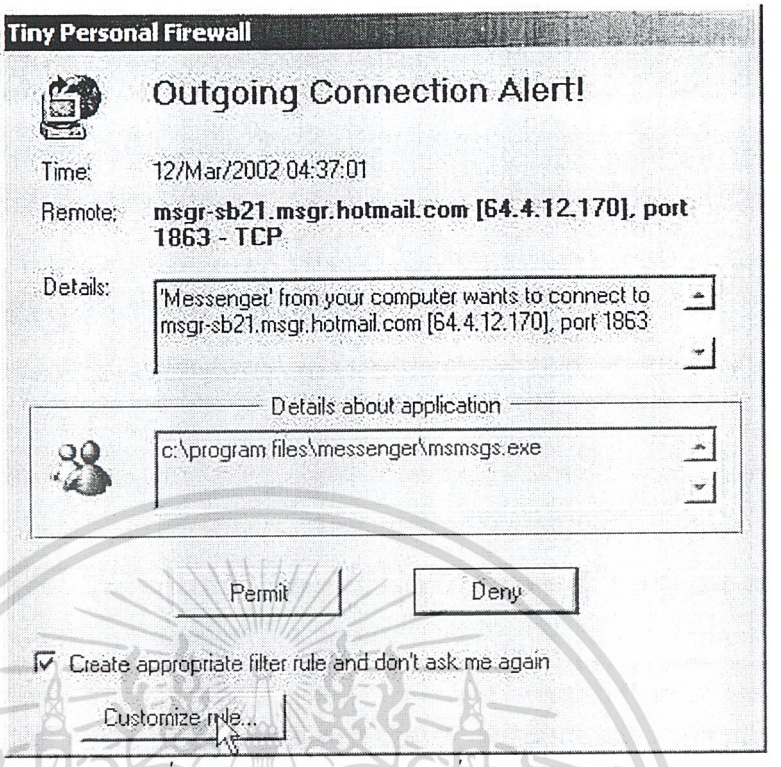
8.2.2.1 คุณลักษณะของTiny Personal Firewall

เป็นเทคโนโลยีด้านความปลอดภัยแบบส่วนตัวที่ใช้งานง่าย ซึ่งป้องกันพีซีจากผู้บุกรุกได้อย่างเต็มรูปแบบ ใช้ได้ดีทั้งเครื่องที่ต่ออยู่ในระบบเน็ตเวิร์กขององค์กรและเครื่องแสตนอโลน (Stand Alone) ซึ่งติดต่อกับอินเตอร์เน็ตด้วยการใช้บริการจากISP ต่างๆ Tiny Personal Firewall มีคุณสมบัติที่สำคัญดังนี้

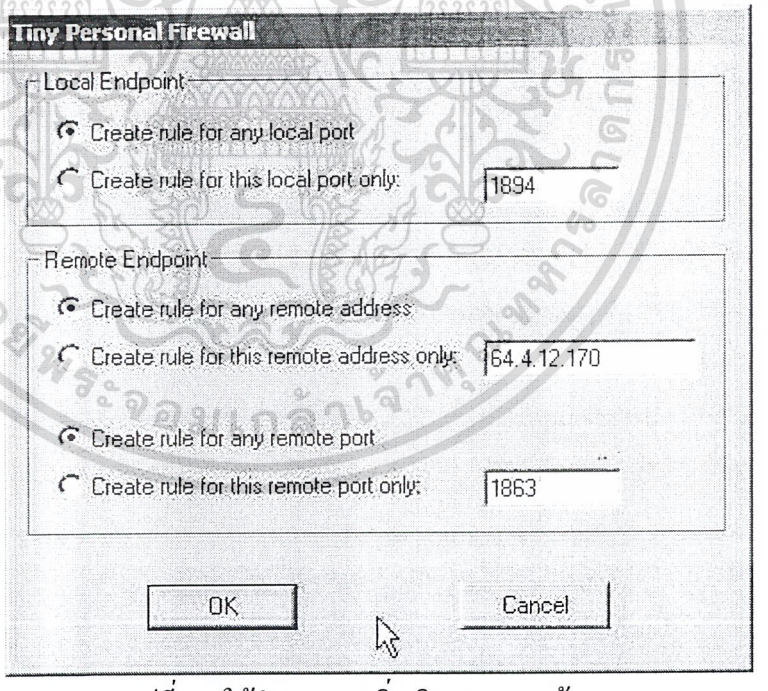
- **ความต้องการของระบบ**
  - 586 Pentium Class
  - RAM 16 เมกะไบต์
  - เนื้อที่ว่างบนฮาร์ดดิสต์ 1 เมกะไบต์
  - ระบบปฏิบัติการวินโดว์ 9x/2000/ME/NT
- **การตรวจจับการบุกรุก (Intrustion Detection)**

  ประกอบด้วย wizard ที่ใช้งานง่ายซึ่งจะคอยตรวจจับกิจกรรมที่ไม่เคยรู้จักมาก่อน และเตรียมพร้อมให้ผู้ใช้ติดตั้งข้อมูลเข้าไป หลังจากติดตั้งข้อมูลใหม่เรียบร้อยกฎที่ออกมาใหม่นี้จะประยุกต์ใช้ในรายการกฎการกรอง (Filter Rules) เลย ซึ่งในส่วนนี้ก็สามารถงดใช้งานได้ด้วย (Disable)

  ดังรูปที่ 8- 7 ทำการทดสอบส่ง ICMP แพ็กเก็ตเข้ามา ในการใช้งานครั้งแรก Tiny Personal Firewall จะยังไม่รู้จักกิจกรรมนี้จึงทำการแจ้งเตือน และทางด้านล่างของรูปก็จะให้ติดตั้งข้อมูลใหม่เข้าไปได้ โดยติ๊กเครื่องหมายถูกที่ Create appropriate filter rule and don't ask me again และเราก็สามารถกดปุ่ม customize rule เพื่อกำหนดกฎต่างๆ ตามต้องการดังแสดงในรูป 8-8

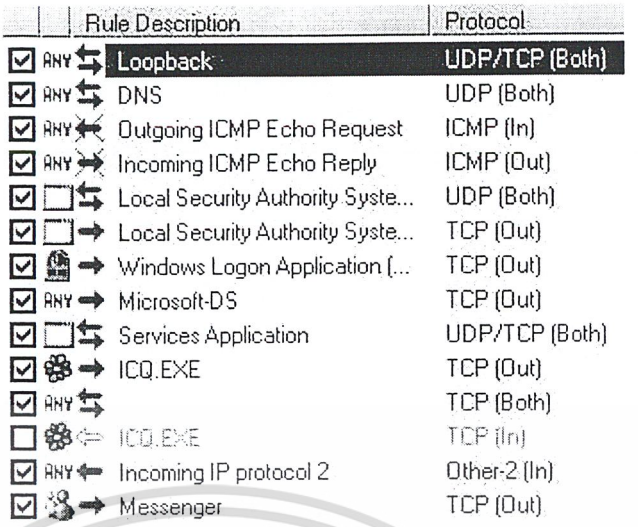


รูปที่ 8-7 การตรวจจับกิจกรรมที่ไม่เคยรู้จักมาก่อน



รูปที่ 8-8 ให้กำหนดกฎเพิ่มเติมตามความต้องการ

และเมื่อกำหนดกฎการกรองไปแล้วก็สามารถงดใช้งานได้ดังแสดงในรูปที่ 8-9



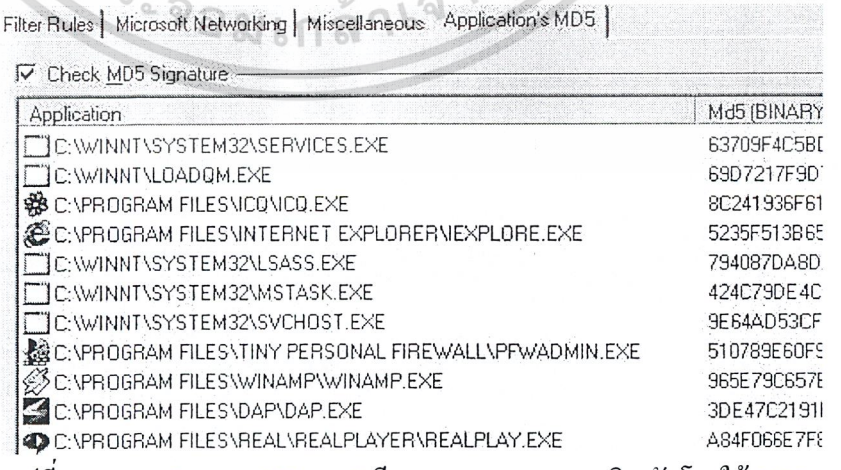
รูปที่ 8-9 แสดงถึงกฎการกรอง โดยสามารถกำหนดการใช้งานได้

- การกรองแอพพลิเคชัน (**Application Filter**)

  เพื่อที่จะป้องกันม้าโทรจันและแอพพลิเคชันที่พิสูจน์ความถูกต้องไม่ได้ Tiny Personal Firewall จึงมีการกรองแอพพลิเคชัน ซึ่งจะมีwizard ที่จะตรวจจับเมื่อมีแอพพลิเคชันพยายาม bind พอร์ตเพื่อการติดต่อสื่อสาร มันจะสร้างกฎการกรอง ที่ขึ้นอยู่กับอินพุตของผู้ใช้ด้วย คือผู้ใช้สามารถอนุญาตแอพพลิเคชันนั้นจากกฎการกรองได้ และจะมีการเก็บดาต้าเบสของแอพพลิเคชันทั่วๆไปว่าใช้พอร์ตไหนเป็นปกติไว้ด้วย

- **MD5 Signature**

  เพื่อให้แน่ใจได้ว่าม้าโทรจันทั้งหลายจะไม่สามารถปลอมตัวเป็นแอพพลิเคชันที่เชื่อถือ จึงใช้การตรวจสอบโดยใช้ลายเซ็นดิจิตอล MD5 ดังแสดงใน รูปที่ 8-10



รูปที่ 8-10 Tiny Personal Firewall มีการตรวจสอบแอพพลิเคชันโดยใช้ MD5

- **แอดเดรสที่เชื่อถือได้ (Trusted Address)**

  ผู้ใช้สามารถกำหนดกฎการกรองได้เอง โดยอาจกำหนดแอดเดรสที่เชื่อถือได้เป็น IP เดียว หรือ เป็นช่วงของ IP หรือจะเชื่อถือทั้งเน็ตเวิร์กใดๆได้เลย

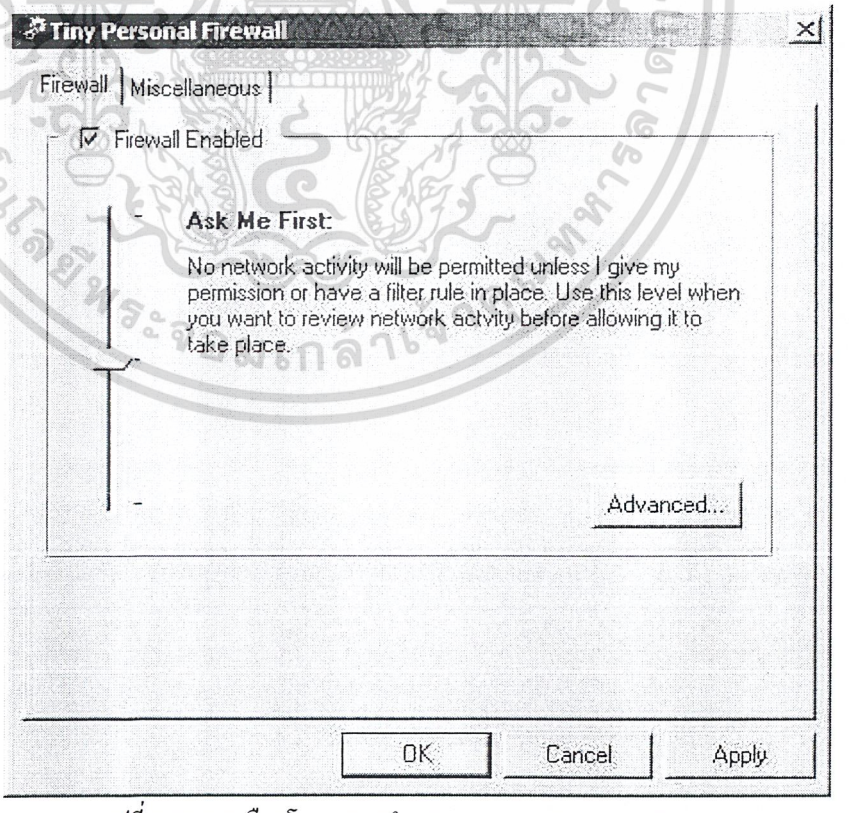
- **การบริหารจัดการทางไกล**

  สามารถทำการคอนฟิกนโยบายความปลอดภัยต่างๆได้จากระยะไกล

8.2.2.2 การคอนฟิก Tiny Personal Firewall

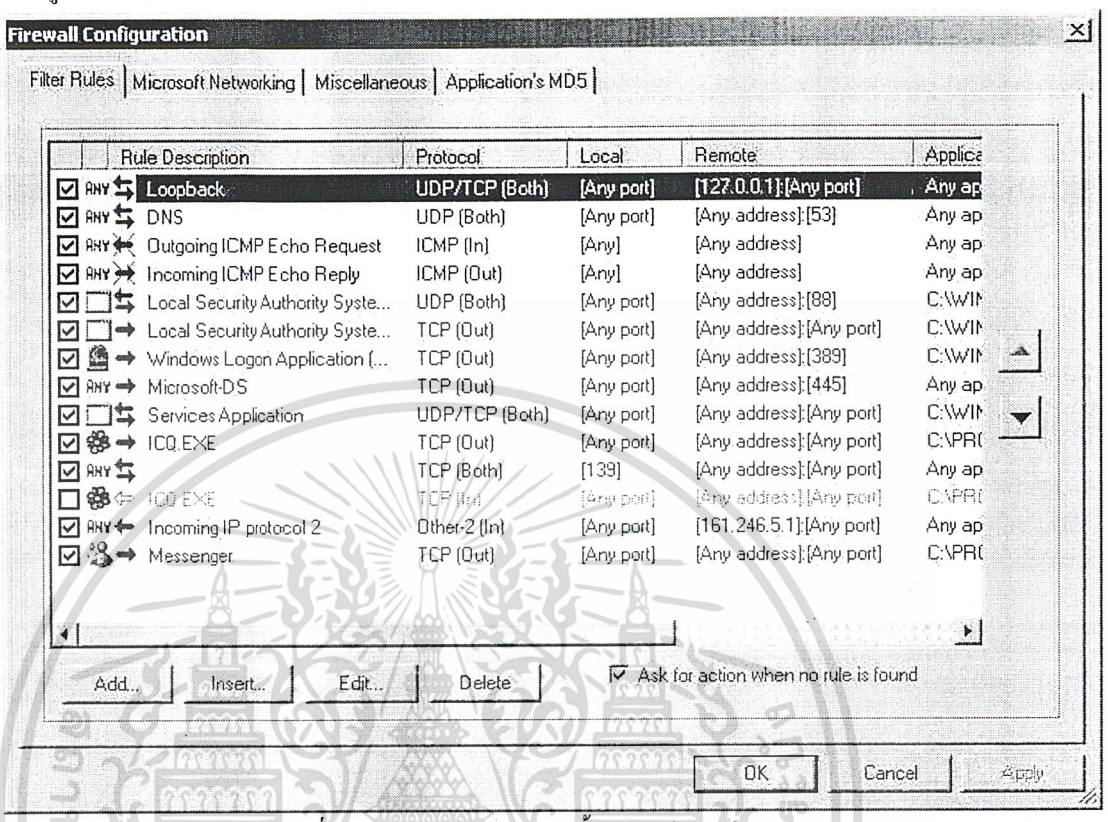
ในการปรับแต่งค่าต่างๆ ในโปรแกรม จะอธิบายตามจุดต่างๆ ที่เราให้ความสนใจ นั่นคือทางด้านความปลอดภัย ดังนี้

- ทำการตั้งค่าการรักษาความปลอดภัยของไฟร์วอลล์ โดยสามารถเลือกโหมดการทำงานได้ 3 โหมดดังรูปที่ 8-11 คือ
  - Don't Bother Me คือถ้าพฤติกรรมที่เข้ามาไม่ตรงกับกฎที่ระบุไว้ Tiny Personal Firewall ก็จะไม่ขึ้นหน้าจอให้สร้างกฎใหม่
  - Ask Me First คือถ้าพฤติกรรมที่เข้ามาไม่ตรงกับกฎที่ระบุไว้ Tiny Personal Firewall ก็จะขึ้นหน้าจอให้ผู้ใช้งานตัดสินใจ
  - Cut Me Off คืองดการใช้งานเน็ตเวิร์ก จะใช้ออปชั่นนี้ก็ต่อเมื่อไม่ต้องการใช้งานเน็ตเวิร์ก เพื่อเพิ่มความปลอดภัยให้มากที่สุด



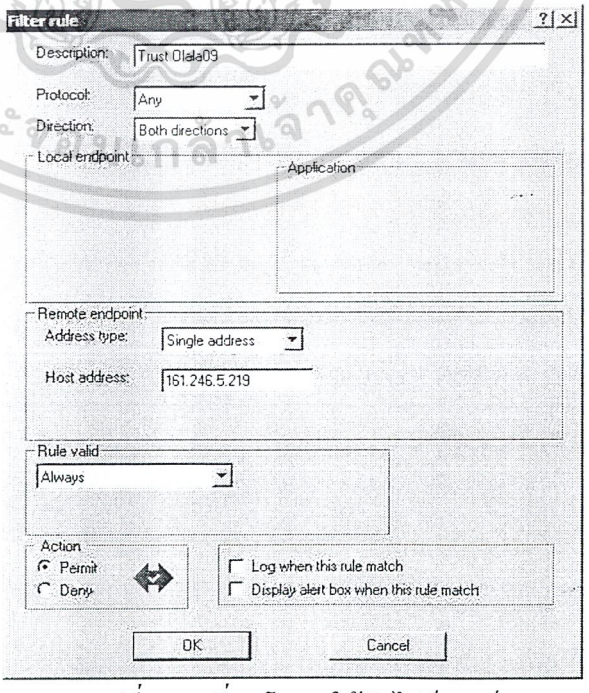
รูปที่ 8-11 การเลือกโหมดการทำงานของ Tiny Personal Firewall

- ต่อไปจะเป็นการสร้างกฎการใช้งาน โดยสามารถเพิ่ม, แทรก, แก้ไข หรือลบกฎใดๆ ได้ ดังรูปที่ 8-12



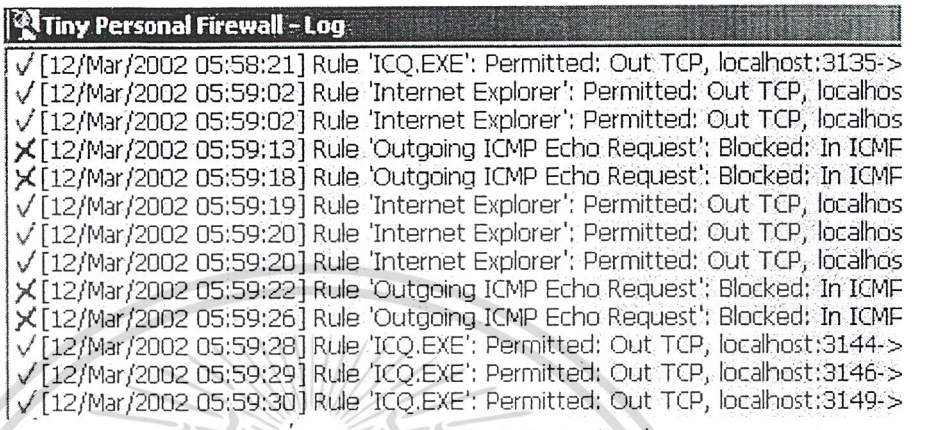
รูปที่ 8-12 แสดงหน้าจอปรับตั้งค่าไฟร์วอลล์

- ถ้าจะทำการเพิ่มนโยบายใดๆ ก็กดปุ่ม Add โดยเมื่อ Add แล้วจะแสดงหน้าจอในรูป 8-13



รูปที่ 8-13 เพิ่มนโยบายให้กับไฟร์วอลล์

- Tiny Personal Firewall จะทำการสร้างล็อกไฟล์ ถ้าหากว่าตรงกับกฎที่เราวางเอาไว้ดังแสดงในรูปที่ 8-14



รูปที่ 8-14 แสดงการจัดเก็บในล็อกไฟล์

8.2.3 WinGate

8.2.3.1 คุณลักษณะของ WinGate

- เป็นโปรแกรมสำหรับการแชร์อินเตอร์เน็ต
- ไฟร์วอลล์
- NAT (Network Address Translator)
- สามารถจัดการจากทางไกลได้ (Remote Administration)
- มีการจัดเก็บลงล็อกไฟล์

8.2.4 Checkpoint Firewall-1

8.2.4.1 คุณลักษณะของ Checkpoint Firewall-1

- เป็นไฟร์วอลล์เต็มรูปแบบ
- ประกอบด้วยเทคโนโลยีทางความปลอดภัยมากมาย ทั้ง NAT, VPNs, เพอร์ซันนอลไฟร์วอลล์
- สามารถจัดการจากทางไกลได้ (Remote Administration)
- มี security policy ที่จัดการง่าย
- มีการจัดเก็บลงล็อกไฟล์
- มีการแจ้งเตือน

บทที่ 9
การทดสอบไฟร์วอลล์

9.1 การทดสอบเพอร์ซันนอลไฟร์วอลล์ ZoneAlarm Pro

ระบบปฏิบัติการที่ทำการทดสอบ : วินโดว์2000 เซิร์ฟเวอร์

9.1.1 การโจมตีเพอร์ซันนอลไฟร์วอลล์ ZoneAlarm Pro ด้วย DoS

9.1.1.1 การป้องกันตัวของ ZoneAlarm Pro จากการโจมตีด้วย DoS

จากการคอนฟิกให้ไฟล์วอลล์สำหรับโซนอินเตอร์เน็ตมีค่าเป็น Med ตามที่กล่าวไว้ในหัวข้อ 8.2.1.2 โปรแกรมจะทำการบล็อกพอร์ต NetBios ขาเข้า (135,137-139,445) เอาไว้โดยอัตโนมัติ พร้อมกับตั้งค่าให้บล็อกพอร์ตTCPหมายเลข 10 เอาไว้แล้ว (หากเลือกค่าเป็น Low นั่นคือไฟร์วอลล์ไม่ทำงาน จะไม่มีการบล็อกพอร์ตใดๆ)

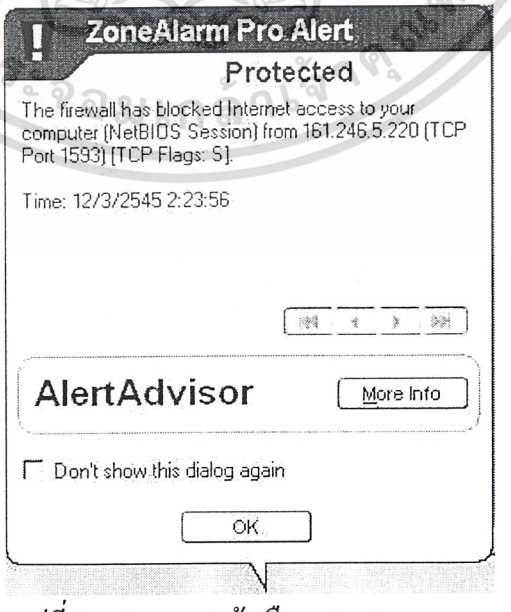
9.1.1.2 โจมตีด้วย killwin.c

DoS ไฟล์นี้โดยดีฟอลท์จะโจมตีไปที่พอร์ต NetBios Session นั่นคือพอร์ต 139 ซึ่งระบบปฏิบัติการวินโดว์ทั่วไป จะเปิดพอร์ตนี้เอาไว้

ผลการโจมตี

- ZoneAlarm ทำการบล็อกเอาไว้ได้ โดยจะแจ้งเตือนขึ้นมาดังรูปที่ 9-1 แล้วเก็บเป็นล็อกไว้ดังรูปที่ 9-2
- ไฟร์วอลล์โฮสต์ทำงานได้ตามปกติ

☐ ฝ่ายผู้โจมตี เชลล์ (Shell)ของลีนุกซ์ที่ทำการรัน killwin จะไม่มีการตอบสนองใดๆ



รูปที่ 9-1 แสดงการแจ้งเตือนของ ZoneAlarm

Rating	Date / Time /	Type	Protocol	Program	Source IP	Destination IP	Direction	Action Taken	Count	Sc
High	2002/03/11 09:41	Repeat Program		TCP IP Serv			(data)	Allowed (once)	1	
Medium	2002/03/11 09:19	Firewall	ICMP		161.246.5.241	161.246.5.219	Incoming	Blocked	1	OLAI
Medium	2002/03/11 09:12	Firewall	UDP	TCP IP Serv	161.246.5.219:68	255.255.255.255:67	Outgoing	Blocked	1	olala
Medium	2002/03/11 09:05	Firewall	IGMP (type:1		161.246.5.1	224.0.0.1	Incoming	Blocked	6	eme
Medium	2002/03/11 09:05	Firewall	UDP	TCP IP Serv		255.255.255.255:67	Incoming	Blocked	353	
Medium	2002/03/11 09:05	Firewall	UDP		161.246.5.1:520	255.255.255.255:520	Incoming	Blocked	3	eme
High	2002/03/11 08:44	Firewall	TCP (flags:S)		161.246.5.214:3283	161.246.5.219:139	Incoming	Blocked	1	
Medium	2002/03/11 08:39	Firewall	ICMP		161.246.5.214	161.246.5.219	Incoming	Blocked	1	
High	2002/03/11 08:36	Firewall	TCP (flags:S)		161.246.5.214:3282	161.246.5.219:80	Incoming	Blocked	1	
High	2002/03/11 08:35	Firewall	TCP (flags:S)		161.246.5.214:3282	161.246.5.219:80	Incoming	Blocked	1	
High	2002/03/11 08:34	Firewall	TCP (flags:S)		161.246.5.214:3282	161.246.5.219:80	Incoming	Blocked	1	
High	2002/03/11 08:32	Firewall	TCP (flags:S)		161.246.5.214:3282	161.246.5.219:137	Incoming	Blocked	1	
High	2002/03/11 08:31	Firewall	TCP (flags:S)		161.246.5.214:3282	161.246.5.219:139	Incoming	Blocked	1	
High	2002/03/11 08:29	Firewall	TCP (flags:S)		161.246.5.214:3282	161.246.5.219:139	Incoming	Blocked	1	

รูปที่ 9-2 รายละเอียดการเก็บล็อกกิ้ง (Logging) ที่ได้แจ้งเตือนไว้

9.1.1.3 โจมตีด้วย synflood.c

จะสั่งให้โจมตีไปที่พอร์ต 10

<u>ผลการโจมตี</u>

- เครื่องไม่ตอบสนองใดๆ หยุดการทำงานไป จนกว่าจะหยุดโจมตี
- ถ้าพอร์ตที่ถูกโจมตีนั้นถูกสั่งบล็อกเอาไว้ก่อนหน้านี้แล้ว เมื่อการโจมตีหยุดลง ZoneAlarm จึงแจ้งเตือนขึ้นมาดังรูป9-3 ว่ามีการโจมตีที่พอร์ตหมายเลข 10 แต่ถ้าไม่ได้บล็อกเอาไว้ก่อน จะไม่มีการแจ้งเตือนใดๆ

รูปที่ 9-3 แสดงการแจ้งเตือนของ ZoneAlarm

9.1.2 การสแกนเพอร์ซันนอลไฟร์วอลล์ ZoneAlarm

ทำการคอนฟิกให้เพอร์ซันนอลไฟร์วอลล์ ZoneAlarmทำงานในโหมด Med หลังจากนั้นใช้ Nmap เพื่อสแกนพอร์ต ได้ผลลัพธ์ของการสแกตพอร์ตออกมาคือ

- Port 23,80 ปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap ไม่สามารถตรวจหาระบบปฏิบัติการได้

9.2 การทดสอบ Tiny Personal Firewall

ระบบปฏิบัติการที่ทำการทดสอบ : วินโดว์2000

9.2.1 การโจมตี Tiny Personal Firewall ด้วย DoS

9.2.1.1 การป้องกันตัวของ Tiny Personal Firewall จากการโจมตีด้วย DoS

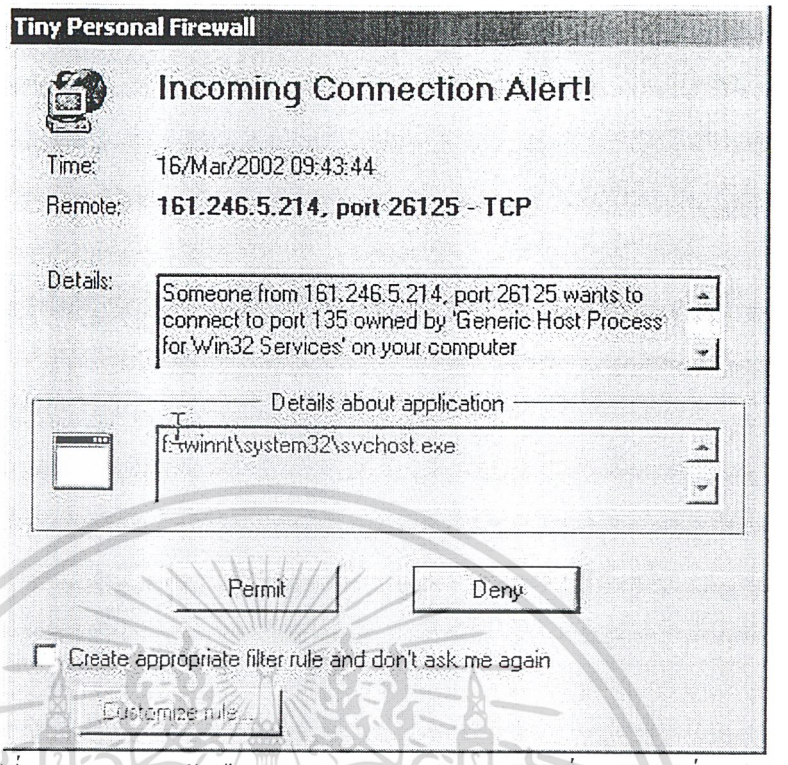
โดยดีฟอลต์ โปรแกรมจะทำการบล็อกพอร์ต NetBios ขาเข้า (135,137-139,445) เอาไว้โดยอัตโนมัติ หากเลือกให้ไฟร์วอลล์ทำงานอยู่ และไม่สามารถเปิดปิดพอร์ตเกี่ยวกับ NetBios เองได้ โดยเราจะเลือกโหมดการทำงานของไฟร์วอลล์ ตามหัวข้อ 8.2.2.2 (เลือก Ask me first) คือให้แจ้ง และให้ผู้ใช้ตัดสินใจว่าจะปฏิเสธ (Deny) หรืออนุญาต (Permit) และทำการบล็อกพอร์ต TCP หมายเลข 10

9.2.1.2 โจมตีด้วย killwin.c

DoS ไฟล์นี้โดยดีฟอลท์จะโจมตีไปที่พอร์ต NetBios Session นั่นคือพอร์ต 139 ซึ่งระบบปฏิบัติการวินโดว์ทั่วไป จะเปิดพอร์ตนี้เอาไว้

ผลการโจมตี

- มีการแจ้งถามเช่นในรูป 9-5 ให้ผู้ใช้ตัดสินใจ แต่ถึงแม้จะอนุญาตก็จะไม่เกิดผลเสียอะไร เนื่องจากแพ็กเก็ตที่มานั้นหมดอายุไปก่อนแล้ว
- ไฟร์วอลล์โฮสต์ทำงานได้ตามปกติ
- ฝ่ายผู้โจมตี เชลล์ (Shell)ของลีนุกซ์ที่ทำการรัน killwin จะไม่มีการตอบสนองใดๆ



รูปที่ 9-4 แสดงการแจ้งเตือน และถามความเห็นของผู้ใช้เมื่อถูกโจมตีที่พอร์ต135

9.2.1.3 โจมตีด้วย Synflood.c

สั่งให้ทำการโจมตีไปที่พอร์ต TCP หมายเลข 10

ผลการโจมตี

- เครื่องไม่ตอบสนองใดๆ จนกว่าจะหยุดโจมตี
- แจ้งเตือนขึ้นทันทีที่เครื่องกลับมาทำงานอีกครั้ง ดังรูป 9-5 แต่จะแจ้งเป็นพอร์ตหมายเลข 10 แทน

☐ ไม่ว่าพอร์ตที่ถูกโจมตีนั้น จะเปิดหรือปิดอยู่ ถ้า ไม่ได้รับการอนุญาตหรือบล็อกเอาไว้ในกฎการกรอง Tiny จะแจ้งเตือนทันทีที่กลับมาทำงานใหม่ได้อีกครั้ง

9.2.2 การสแกน Tiny Personal Firewall

ทำการคอนฟิกให้ Tiny Personal Firewall ทำงานในโหมด Ask Me First หลังจากนั้นใช้ Nmap เพื่อสแกนพอร์ต ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 139 เปิดอยู่
- Port 23,80 ปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap สามารถตรวจหาระบบปฏิบัติการได้

9.3 สรุปผลการทดสอบผลิตภัณฑ์ไฟร์วอลล์ชนิดเพอร์ซันนอลไฟร์วอลล์

9.3.1 สรุปผลการโจมตีด้วย DoS

จากการทดลองโจมตีไฟร์วอลล์ทั้งสองตัวด้วย Killwin.c ปรากฏว่าไฟร์วอลล์ทั้งสองตัวสามารถต้านทานได้ เนื่องจาก

- สำหรับ ZoneAlarm นั้นได้มีการตั้งค่าเอาไว้ให้บล็อกพอร์ตเกี่ยวกับ NetBios ซึ่งหากไม่ตั้งค่าเช่นนี้ ไฟร์วอลล์โฮสต์ก็จะแครชทันทีเนื่องจากถูกโจมตีด้วย Killwin
- สำหรับ Tiny Personal Firewall นั้น บล็อกพอร์ตเกี่ยวกับNetBios เป็นดีฟอลต์โดยผู้ใช้ไม่สามารถปรับเปลี่ยนได้เลย

ส่วนผลจากการโจมตีด้วย Synflood.c นั้นทั้งสองผลิตภัณฑ์ไม่สามารถต้านทานได้ทั้งคู่ และมีลักษณะที่เหมือนกัน จึงไม่นำมาเป็นนัยสำคัญในการตัดสินใจ

ดังนั้น จากผลที่ได้ถือว่า ZoneAlarm มีความยืดหยุ่นต่อการตั้งค่านโยบายความปลอดภัยต่างๆ เป็นข้อได้เปรียบกว่าในแง่ของการใช้งาน แต่หากผู้ใช้ไม่มีความรู้มากพอแล้ว Tiny จะปลอดภัยกว่า

	ZoneAlarm	TINY
Killwin.c	A	A
Synflood.c	C	C

ตารางที่ 9-1 สรุปการโจมตี DoS ไปยังเพอร์ซันนอลไฟร์วอลล์

A : ปกติ

B : ตอบสนองช้ามากๆ

C : หยุดทำงานไม่ตอบสนองใดๆ

หมายเหตุ จากตาราง การทดลองได้ทำการคอนฟิกให้บล็อกพอร์ต TCP หมายเลข 10 และ 139 และโจมตี killwin และ Synflood ไปยังพอร์ต 139 และ 10 ตามลำดับ

9.3.2 สรุปผลการโจมตีด้วยการสแกนพอร์ต

จากการทดลองในการสแกนพอร์ตโฮสต์ที่ทำการติดตั้งเพอร์ซันนอลไฟร์วอลล์ ZoneAlarm และ Tiny Personal Firewall โดยใช้ Nmap จะทำการสรุปผลการทดลองดังนี้

ทั้ง เพอร์ซันนอลไฟร์วอลล์ ZoneAlarm และ Tiny Personal Firewall ให้ผลการสแกนพอร์ตที่ไม่ตรงกับความเป็นจริงโดยสิ้นเชิง กล่าวคือ

- สำหรับ ZoneAlarm

  พอร์ต 23,80 ที่เปิดอยู่, Nmap ตรวจสอบพบว่าพอร์ตนี้ปิด

  ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตถูกฟิลเตอร์

  (ไม่รู้ว่าเปิดหรือปิด)

- สำหรับ Tiny Personal Firewall

  พอร์ต 23,80 ที่เปิดอยู่, Nmap ตรวจสอบพบว่าพอร์ตนี้ปิด

  พอร์ต 139 ที่ deny ไว้, Nmap ตรวจสอบพบว่าพอร์ตนี้เปิด

  ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตถูกฟิลเตอร์

ส่วนการตรวจจับระบบปฏิบัติการ พบว่า

- ZoneAlarm สามารถปิดบังระบบปฏิบัติการได้
- Tiny Personal Firewall ไม่สามารถปิดบังระบบปฏิบัติการได้

เพราะฉะนั้นโดยภาพรวมแล้ว การปิดบังร่องรอยของโฮสต์ที่ทำการติดตั้งเพอร์ซันนอลไฟร์วอลล์ ZoneAlarm ได้ผลลัพธ์เป็นที่น่าพอใจกว่าโฮสต์ที่ทำการติดตั้ง Tiny Personal Firewall เนื่องจากผลลัพธ์ของการสแกนพอร์ตพบว่าทั้ง ZoneAlarm และ Tiny Personal Firewall ทำให้ผลการสแกนพอร์ตไม่ตรงกับความเป็นจริงโดยสิ้นเชิง แต่สำหรับการตรวจจับระบบปฏิบัติการพบว่า ZoneAlarm สามารถปิดบังระบบปฏิบัติการได้ แต่ Tiny Personal Firewall ทำไม่ได้ อันนี้เป็นข้อดีที่ ZoneAlarm มีเหนือ Tiny Personal Firewall นั่นเอง

9.4 การทดสอบ WinGate

ระบบปฏิบัติการที่ทำการทดสอบ : วินโดว์2000 เซิร์ฟเวอร์

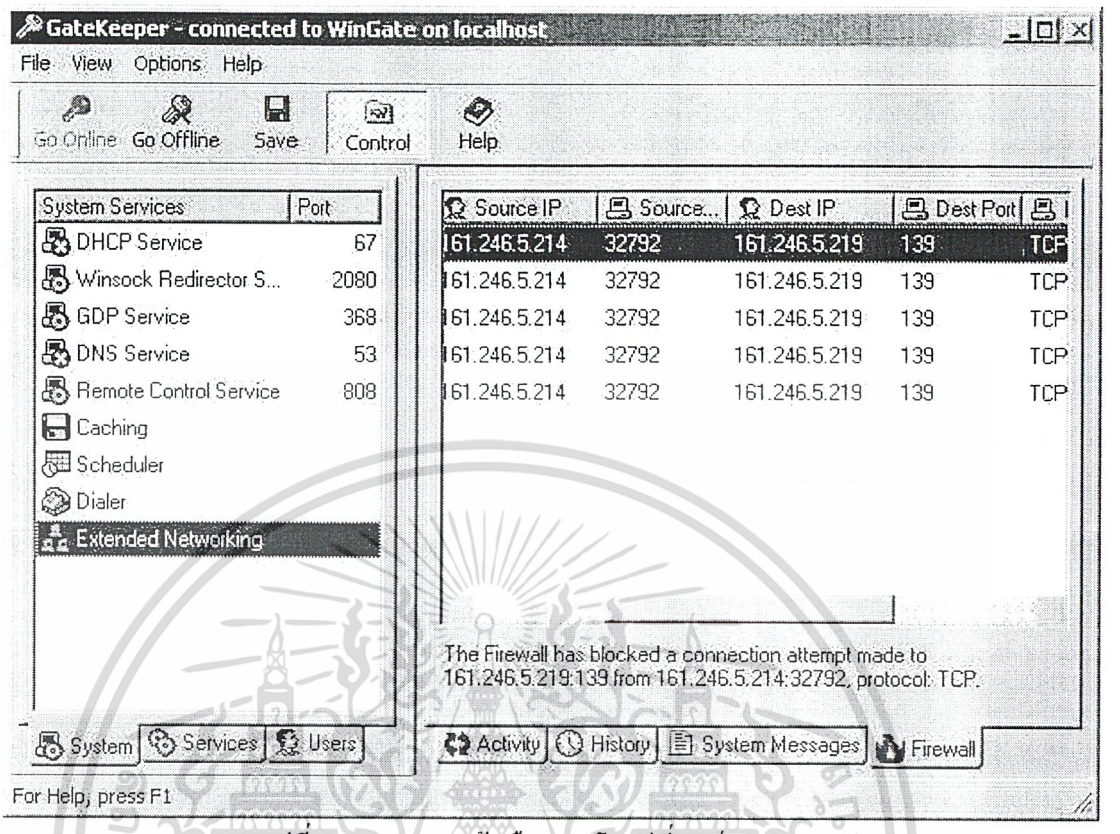
9.4.1 การโจมตี WinGate ด้วย DoS

9.4.1.1 โจมตีด้วย killwin.c

โจมตีไปที่พอร์ต 139

<u>ผลการโจมตี</u>

- ถ้าบล็อกพอร์ต 139 เอาไว้แล้ว (หรือไม่ได้อนุญาตพอร์ตนี้) จะเครื่องจะทำงานปกติ พร้อมแจ้งเตือนดังรูปที่ 9-7
- ถ้าอนุญาตพอร์ต 139 เอาไว้ เมื่อถูกโจมตี เครื่องจะตอบสนองช้ามาก จนต้องบูตใหม่



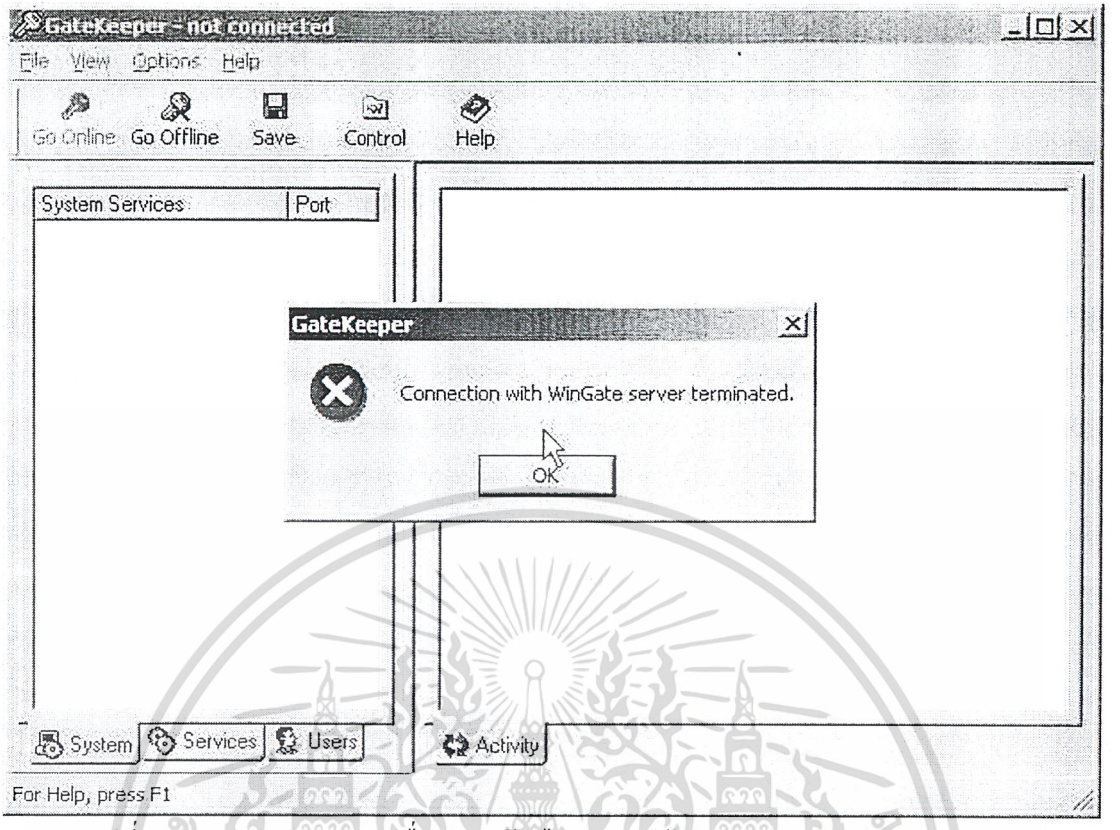
รูปที่ 9-5 แสดงการแจ้งเตือนการโจมตีที่พอร์ต 139 ของ WinGate

9.4.1.2 โจมตีด้วย synflood.c

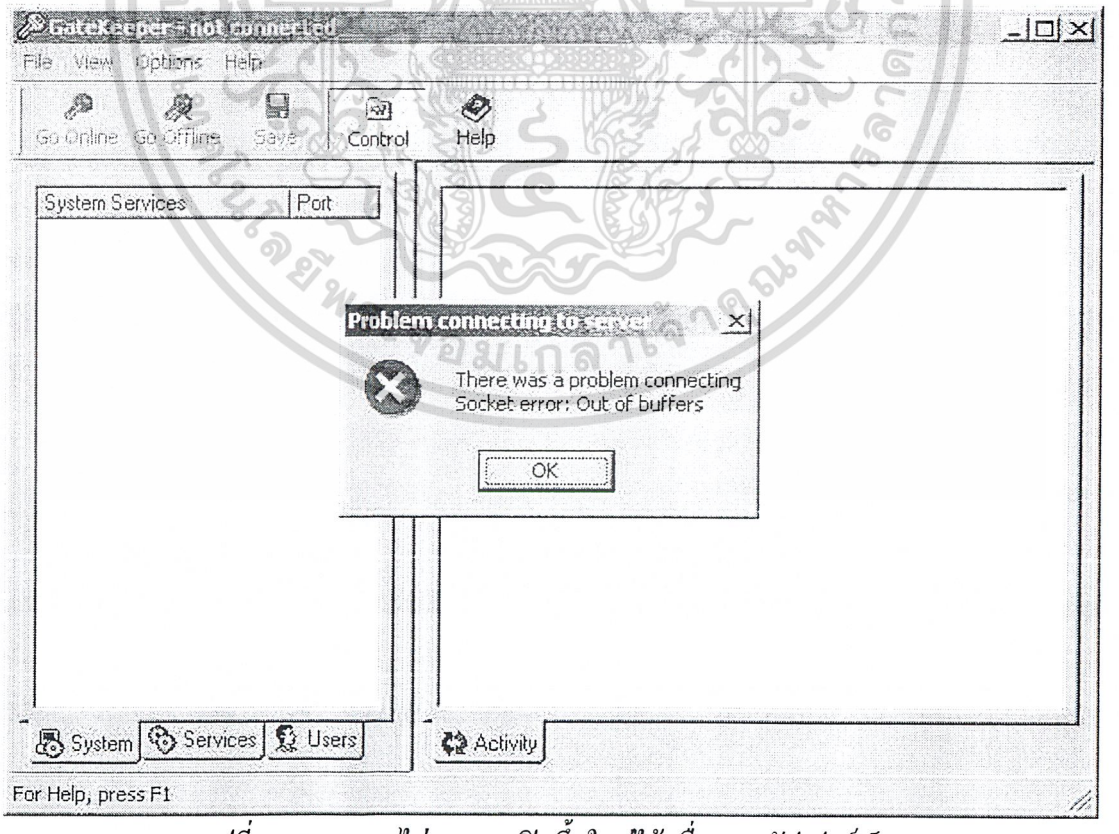
โจมตีไปที่พอร์ต 10

ผลการโจมตี

- ถ้าอนุญาตพอร์ต 10 เอาไว้ เมื่อถูกโจมตี เครื่องจะไม่ตอบสนองใดๆ หยุดทำงาน
- ถ้าบล็อกพอร์ต 10 เอาไว้ (หรือไม่ได้อนุญาต) เครื่องจะเป็นปกติ ก็ต่อเมื่อปริมาณแพ็กเก็ตที่ยิงมามีไม่มากนัก (ไม่เกิน 1 แสนแพ็กเก็ต) หากปริมาณแพ็กเก็ตที่ยิงมามีจำนวนมากๆ จะทำให้ WinGate ซึ่งจะทำการแจ้งเตือนสำหรับทุกๆ แพ็กเก็ตที่เข้ามานั้นทำงานหนักจนดึงซีพียูมาใช้งาน 100 % เครื่องจะตอบสนองช้ามากๆ จนต้องปิดWinGate ทิ้งไป หรือWinGate ปิดตัวเองไปดังรูปที่ 9-8 และเมื่อเปิดขึ้นมาใหม่ก็ยังเกิดปัญหาบัฟเฟอร์เต็ม ไม่สามารถเข้า WinGate ได้ ดังรูปที่ 9-9 อีกทั้งขณะที่ WinGate กำลังแจ้งเตือนมากเกินไป(Over Alert)อยู่นั้น จะไม่ป้องกันพอร์ตที่บล็อกเอาไว้
- แม้ว่า WinGate จะมีปัญหาปิดตัวเองไป แต่ยังคงรักษาค่าเซอร์วิสหรือพอร์ตต่างๆ ที่ตั้งเอาไว้ได้



รูปที่ 9-6 WinGate ปิดตัวเองเนื่องจากแจ้งเตือนมากเกินไป เพราะการโจมตีด้วย Synflood



รูปที่ 9-7 WinGate ไม่สามารถเปิดขึ้นใหม่ได้ เนื่องจากบัฟเฟอร์เต็ม

9.4.2 การสแกน WinGate

ใช้ Nmapเพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง WinGate ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 80 เปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap ไม่สามารถตรวจหาระบบปฏิบัติการได้

9.5 การทดสอบ Checkpoint Firewall-1

ระบบปฏิบัติการที่ทำการทดสอบไฟร์วอลล์โฮสต์ : วินโดว์ NT

ระบบปฏิบัติการที่ทำการทดสอบโฮสต์หลังไฟร์วอลล์ : วินโดว์2000 เซิร์ฟเวอร์

9.5.1 การโจมตี Checkpoint Firewall-1 ด้วย DoS

9.5.1.1 โจมตี killwin.c

- **กรณีทดสอบโฮสต์หลังไฟร์วอลล์**

  โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- โฮสต์หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ ทำงานตามปกติ
- ไม่มีการแจ้งเตือน เนื่องจากเป็นพอร์ตที่อนุญาตเอาไว้
- เครื่องที่ทำการโจมตี จะมีข้อความปรากฏบอกว่า "การเชื่อมต่อถูกปฏิเสธ" (Connection Refused)
- แม้จะโจมตีที่พอร์ตอื่นๆ ที่ไม่ได้อนุญาต ก็ยังคงทำงานปกติ

- **กรณีทดสอบไฟร์วอลล์โฮสต์**

  โจมตีไปที่พอร์ต 139

ผลการโจมตี

- ไฟร์วอลล์โฮสต์ทำงานตามปกติ
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 139
- เครื่องที่ทำการโจมตี จะมีข้อความปรากฏบอกว่า "การเชื่อมต่อถูกปฏิเสธ" (Connection Refused)

9.5.1.2 โจมตี synflood.c

- **กรณีทดสอบโฮสต์หลังไฟร์วอลล์**

  โจมตีไปที่พอร์ต 80 (เปิดพอร์ต 80 สำหรับโปรโตคอล http ที่โฮสต์หลังไฟร์วอลล์)

ผลการโจมตี

- โฮสต์หลังไฟร์วอลล์ และไฟร์วอลล์โฮสต์ ไม่ตอบสนองใดๆ หยุดการทำงาน
- ไม่มีการแจ้งเตือน เนื่องจากเป็นพอร์ตที่อนุญาตเอาไว้

- ถ้าโจมตีไปพอร์ตที่ไม่ได้อนุญาตไว้ โฮสต์หลังไฟร์วอลล์จะปลอดภัย แต่เครื่องไฟร์วอลล์ จะหยุดการทำงาน

- **กรณีทดสอบไฟร์วอลล์โฮสต์**

  โจมตีไปที่พอร์ต 80

<u>ผลการโจมตี</u>

- ไฟร์วอลล์โฮสต์หยุดทำงาน ไม่ตอบสนอง
- มีการแจ้งเตือนการบุกรุกเครื่องไฟร์วอลล์ที่พอร์ต 80 หลังจากกลับมาทำงานอีกครั้ง
- ไม่ว่าจะโจมตีไปที่พอร์ตใดๆ ก็หยุดทำงานทุกครั้ง แม้จะไม่อนุญาตให้ใครเข้าถึงเครื่องไฟร์วอลล์ได้เลย

9.5.2 การสแกน Checkpoint Firewall-1

9.5.3 ใช้ Nmapเพื่อสแกนพอร์ตโฮสต์ที่ติดตั้ง Checkpoint Firewall-1 ได้ผลลัพธ์ของการสแกนพอร์ตออกมาคือ

- Port 264,265 เปิดอยู่
- Port อื่นๆ ที่เหลือถูกฟิลเตอร์
- Nmap สามารถตรวจหาระบบปฏิบัติการได้

9.6 สรุปผลการทดสอบผลิตภัณฑ์ไฟร์วอลล์ชนิดเอนเตอร์ไพรส์ไฟร์วอลล์

9.6.1 สรุปผลการโจมตีด้วย DoS

Check Point Firewall -1 ดีกว่า เนื่องจาก WinGate มีปัญหาเรื่องการแจ้งเตือนมากเกินไปเมื่อถูกโจมตีด้วย Synflood และช่วงเวลานั้นก็เป็นช่องโหว่ให้โจมตีที่พอร์ตอื่นๆ ซึ่งถูกบล็อกเอาไว้ได้ ส่วนFirewall-1 แม้จะหยุดทำงานไป แต่ยังคงป้องกันพอร์ตอื่นๆ และเครื่องภายในไว้ได้และเมื่อกลับมาทำงานใหม่ก็ทำงานต่อได้อย่างปกติ ผิดกับ WinGate ที่กลับมาทำงานใหม่ไม่ได้เพราะบัฟเฟอร์หมด ต้องบูตเครื่องใหม่เท่านั้น

	FW-1	WinGate
Killwin.c	**A**	**A**
Synflood.c	**C**	**D**

ตารางที่ 9-2สรุปการโจมตี DoS ไปยังเอนเตอร์ไพร์สไฟร์วอลล์

A : ปกติ

B : ตอบสนองช้ามากๆ

C : หยุดทำงานไม่ตอบสนองใดๆ

D : แจ้งเตือนมากเกินไป จนทำงานต่อไม่ได้

หมายเหตุ จากตาราง การทดลองได้ทำการคอนฟิกให้บล็อกพอร์ต TCP หมายเลข 10 และ 139 และโจมตี killwin และ Synflood ไปยังพอร์ต 139 และ 10 ตามลำดับ

9.7.2 สรุปผลการโจมตีด้วยการสแกนพอร์ต

จากการทดลองในการสแกนพอร์ตโฮสต์ที่ทำการติดตั้ง WinGate และ Checkpoint Firewall-1 โดยใช้ Nmap จะทำการสรุปผลการทดลองดังนี้

- สำหรับ WinGate

  พอร์ต 23,80 ที่เปิดอยู่, Nmap ตรวจสอบพบว่าพอร์ต 23 ปิด แต่พอร์ต 80 เปิด

  ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตเหล่านั้นถูกฟิลเตอร์

- สำหรับ Checkpoint Firewall-1

  มีพอร์ต 264,265 ที่เปิดอยู่

  ส่วนพอร์ตอื่นๆ ที่เหลือ, Nmap ตรวจสอบพบว่าพอร์ตเหล่านั้นปิดอยู่

ส่วนการตรวจจับระบบปฏิบัติการ พบว่า

- WinGate สามารถปิดบังระบบปฏิบัติการได้
- Checkpoint Firewall-1 ไม่สามารถปิดบังระบบปฏิบัติการได้

เพราะฉะนั้นโดยภาพรวมแล้ว ไม่สามารถสรุปว่าผลิตภัณฑ์ไหนดีกว่าโดยอาศัยผลลัพธ์จากการสแกนเท่านั้น

เนื่องจากผลลัพธ์ของการสแกนพอร์ตพบว่า WinGate สามารถปิดบังการสแกนได้เป็นส่วนใหญ่ แต่ไม่ทั้งหมด ส่วน Checkpoint Firewall-1 ทำให้ผลการสแกนพอร์ตออกมาไม่ตรงกับความเป็นจริงโดยสิ้นเชิง

แต่สำหรับการตรวจจับระบบปฏิบัติการพบว่า WinGate สามารถปิดบังระบบปฏิบัติการได้ แต่ Checkpoint Firewall-1ทำไม่ได้

ดังนั้นในการพิจารณาว่าผลิตภัณฑ์ไหนดีกว่ากัน จะต้องพิจารณาปัจจัยอื่นๆ ประกอบด้วย

หมายเหตุ การโจมตีด้วย DoS ทั้งสองประเภทและการสแกนพอร์ต เป็นการโจมตีไปยังพอร์ต TCP อย่างเดียว พอร์ตที่กล่าวถึงในบทนี้ จึงเป็นพอร์ต TCP ทั้งหมด

บทที่ 10
สรุปการทำงาน

วัตถุประสงค์ของวิทยานิพนธ์ฉบับนี้คือการศึกษาเทคโนโลยีในการรักษาความปลอดภัยให้กับระบบเครือข่ายขององค์กรที่เชื่อมต่อกับอินเตอร์เน็ต โดยมุ่งเน้นไปที่ไฟร์วอลล์ ซึ่งจะเป็นการประยุกต์ใช้ระบบไฟร์วอลล์สำหรับเครือข่าย พร้อมทั้งทำการทดสอบในด้านความปลอดภัย อีกทั้งยังศึกษาการโจมตีที่เรียกว่า DoS (Denial of Service) และศึกษาการสำรวจเครือข่ายด้วยการสแกน และนำทั้งหมดนี้มาใช้ในการทดสอบไฟร์วอลล์ และเครือข่าย ในด้านความปลอดภัย
ซึ่งก็ได้ผลตามวัตถุประสงค์ที่ตั้งใจไว้ โดยดำเนินการดังนี้

- ศึกษาและหา DoS ที่เหมาะสมในการโจมตี
- ศึกษาและหาสแกนเนอร์ที่เหมาะสมในการทดสอบ
- ติดตั้งระบบเครือข่ายขึ้นมา
- ศึกษาผลิตภัณฑ์แต่ละตัวที่จะนำมาทดสอบ
- ติดตั้งผลิตภัณฑ์แต่ละตัว แล้วทำการคอนฟิก ปรับแต่งค่าให้เหมาะสม
- ตั้งค่านโยบายความปลอดภัยให้สอดคล้องกับการใช้งานปกติ
- สำรวจระบบด้วยสแกนเนอร์
- โจมตีด้วย DoS ที่หามาได้
- สังเกตผลที่เกิดขึ้นกับไฟร์วอลล์โฮสต์หรือเครือข่าย

จากผลการทดสอบที่ได้ ดังกล่าวมาแล้วในบทที่9 นั้น เราสามารถสรุปการทำงาทั้งหมดของเราได้ว่า

“ ในการจะเลือกผลิตภัณฑ์ไฟร์วอลล์ใดๆ สำคัญที่สุดนั่นคือ ผู้บุกรุกจะทำการโจมตีเครือข่าย หรือไฟร์วอลล์โฮสต์ของเราได้หรือไม่ ขึ้นอยู่กับการคอนฟิกหรือการปรับแต่งค่าของไฟร์วอลล์ โดยเฉพาะอย่างยิ่งนโยบายความปลอดภัย (Security Policy) ที่เหมาะสมกับองค์กรและการใช้งานนั่นเอง“

บรรณานุกรม

หนังสือ

[1] D.Brent Chapman and Elizabeth D.Zwicky, "Building Internet Firewalls", O'Reilly&Associates, Inc., 1995

[2] Joel Scambray, Stuart McClure and George Kurtz, "Hacking Exposed: Network Security Secrets & Solutions", Se-education Public Company, 2001

[3] Eric Maiwald, "Network Security a Beginner's guide", Osborne McGraw Hill, 2001

[4] เรืองไกร รังสิพล, "เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน", Provision, 2544

เวปไซต์

[1] http://www.sans.org/

[2] http://packetstorm.widexs.nl/

[3] http://www.itsecurity.com/

[4] http://www.insecure.org

[5] http://www.wingate.net

[6] http://www.zonelabs.com

[7] http://www.tinysoftware.com/

[8] http://www.microsoft.com/isaserver/

[9] http://thaicert.nectec.or.th/

[10] http://www.topsecure.net/