บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ปัจจุบันอินเทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินกิจกรรมต่างๆ เป็นอย่างมาก ไม่ว่าจะเป็นด้านการติดต่อสื่อสาร ธุรกิจ การศึกษา หรือว่าเพื่อความบันเทิง องค์กรต่างๆทั้งภาครัฐและเอกชนต่างก็นำเอาเน็ตเวิร์กของตนเชื่อมต่อเข้ากับอินเทอร์เน็ตเพื่อที่จะได้รับประโยชน์เหล่านี้ แต่เราต้องไม่ลืมว่าการนำเอาเน็ตเวิร์กไปเชื่อมต่อกับอินเทอร์เน็ตนั้น ทำให้ใครก็ได้บนอินเทอร์เน็ตสามารถเข้ามายังเน็ตเวิร์กนั้นๆได้ ปัญหาที่ตามมาก็คือความปลอดภัยของระบบเน็ตเวิร์ก เช่น ทำให้เกิดความเสี่ยงต่อการถูกเจาะระบบ และ ขโมยข้อมูล เป็นต้น

เมื่อคำนึงถึงเรื่องความปลอดภัยของคอมพิวเตอร์มักเป็นการยากในการมองภาพที่ชัดเจนว่า อะไรที่จะบ่งบอกได้ว่าการใช้งานคอมพิวเตอร์มีความปลอดภัย เนื่องจากความปลอดภัยของคอมพิวเตอร์เป็นสิ่งที่จับต้องไม่ได้และยากต่อการวัด แต่อย่างไรก็ตามเราสามารถเปรียบเทียบความปลอดภัยของคอมพิวเตอร์กับการรักษาความปลอดภัยสถานที่ ในการรักษาความปลอดภัย สถานที่นั้นนอกจากการจัดบริเวณที่ต้องรักษาความปลอดภัยให้มีรั้วรอบขอบชิด มีกุญแจที่ใช้ล็อกประตูหรือทางเข้าออก สิ่งหนึ่งที่จะขาดไม่ได้คือการจัดให้มีบุคคลหรืออุปกรณ์ที่คอยตรวจสอบการละเมิดต่ออุปกรณ์หรือเครื่องกีดขวางที่จัดตั้งเพื่อความปลอดภัย ทั้งนี้เนื่องจากอาจมีผู้ไม่หวังดีพยายามบุกรุกโดยทำลายอุปกรณ์หรือเครื่องกีดขวางดังกล่าวดังนั้นเราจึงต้องอาศัยระบบที่ใช้ตรวจสอบเมื่อมีการทำลายหรือล่วงล้ำต่ออุปกรณ์หรือเครื่องกีดขวางที่ได้ติดตั้งไว้อีกชั้นหนึ่ง ตัวอย่างอุปกรณ์ที่ใช้ตรวจสอบเช่น ระบบสัญญาณเตือนขโมยที่ใช้ควบคู่กับรั้วที่แข็งแรง

ระบบเครือข่ายคอมพิวเตอร์ก็เช่นเดียวกัน บุคคลทั่วไปมักคิดว่าการติดตั้งระบบรักษาความปลอดภัยหรือไฟร์วอลล์ ตามลำพังก็สามารถทำให้เครือข่ายคอมพิวเตอร์มีความปลอดภัย แต่อย่างไรก็ตาม การติดตั้งระบบรักษาความปลอดภัย ให้กับระบบเครือข่ายคอมพิวเตอร์ก็เปรียบเสมือน การสร้างรั้วหรือกำแพงที่มียามคอยเฝ้าประตูเพื่อตรวจสอบบุคคลที่จะเข้าออกสถานที่ แต่หากมีบุคคลไม่หวังดีสามารถปีนรั้วหรือสามารถหลอกระบบรักษาความปลอดภัยเข้ามาได้ การรักษาความปลอดภัยโดยใช้รั้วก็หมดความหมาย ดังนั้นในการเพิ่มความปลอดภัยอีกประการหนึ่งคือการใช้ระบบตรวจสอบการบุกรุก ซึ่งมีคุณลักษณะเหมือนยามที่คอยตรวจตราภายในระบบเครือข่ายของเราอีกที มีหน้าที่ในการตรวจจับ การใช้งานและความพยายามในการใช้

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright © by Chiang Mai University
All rights reserved

งาน คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ซึ่งขัดกับข้อบังคับ เจตุจำนงค์การใช้งาน และอาจส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ได้

ดังนั้นการผสมผสานระบบตรวจสอบผู้บุกรุกร่วมกับระบบรักษาความปลอดภัยระบบเครือข่าย จึงเป็นการทำให้ระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์และระบบเครือข่ายขององค์กรทั้งการดูแล ตรวจสอบ และมาตรการป้องกันมีประสิทธิภาพมากขึ้น

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อตรวจสอบ เก็บข้อมูลและวิเคราะห์การบุกรุกระบบเครือข่ายได้ ณ เวลาที่เกิดขึ้นจริง

1.2.2 พัฒนาประสิทธิภาพของระบบเตือนภัยและป้องกันการบุกรุกระบบเครือข่ายขนาดกลางและเล็กให้ดีขึ้น

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 ป้องกันระบบเครือข่ายจากการบุกรุกได้ดีขึ้น

1.3.2 ช่วยให้ผู้ดูแลระบบตรวจสอบและวิเคราะห์การบุกรุกระบบเครือข่ายได้ถูกต้องและเร็วขึ้น

1.3.3 สามารถทำรายงานสรุปการบุกรุกระบบเครือข่ายได้

1.4 ขอบเขตและวิธีการศึกษา

ศึกษาเทคนิควิธี ออกแบบและจัดทำระบบตรวจสอบผู้บุกรุกระบบเครือข่ายร่วมกับระบบรักษาความปลอดภัย บนระบบปฏิบัติการลีนุกซ์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ ซึ่งมีรายละเอียดของขอบเขตและวิธีการศึกษา ดังนี้

1.4.1 แผนการดำเนินการ

1.4.1.1 ศึกษาค้นคว้าและเก็บรวบรวมข้อมูล

1.4.1.2 ระบุความต้องการของระบบ

1.4.1.3 พัฒนาระบบต้นแบบ

1.4.1.4 ติดตั้งและทดลองใช้งาน

1.4.1.5 ปรับแต่งต้นแบบและแก้ไขข้อผิดพลาด

1.4.1.6 จัดทำเอกสารประกอบ

1.4.1.7 นำเสนองานการวิจัยค้นคว้าแบบอิสระ

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright © by Chiang Mai University
All rights reserved

1.4.2 ขอบเขต

1.4.2.1 การจัดเก็บข้อมูล

ส่วนที่ 1 รูปแบบของการบุกรุก

ส่วนที่ 2 ข้อมูลการบุกรุกบนระบบเครือข่ายที่ตรวจสอบพบ

1.4.2.2 การจัดการและบริหารข้อมูล

1.4.2.3 การสืบค้นและรายงานผลข้อมูล ในรูปแบบต่างๆ

1.4.2.4 การทำงานร่วมกับระบบรักษาความปลอดภัยบนระบบปฏิบัติการลีนุกซ์

1.4.3 วิธีศึกษา

1.4.3.1 ศึกษาและให้คำจำกัดความของระบบ (System Definition)

ทำการศึกษาถึงระบบป้องกันการบุกรุก ระบบตรวจสอบผู้บุกรุกเครือข่าย ลักษณะเครือข่าย ขั้นตอนการตรวจสอบการบุกรุกบนระบบเครือข่าย คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ และกำหนดขอบเขตการศึกษา

1.4.3.2 วิเคราะห์ระบบ (System Analysis)

- ทำการศึกษาเทคโนโลยีระบบเครือข่าย การติดต่อสื่อสารบนระบบเครือข่าย จุดบกพร่องที่ทำให้เกิดการบุกรุก เทคโนโลยีที่ใช้ป้องกันและตรวจสอบการบุกรุก
- ทำการจำแนกพฤติกรรมและประเภทข้อมูลต่างๆบนระบบเครือข่าย และจำแนกระดับความรุนแรงของการบุกรุก เพื่อกำหนดนโยบายการป้องกัน

1.4.3.3 ประยุกต์การใช้งานระบบ (System Implementation)

ทำการประยุกต์ใช้งานระบบตรวจสอบผู้บุกรุกระบบเครือข่ายร่วมกับระบบรักษาความปลอดภัยบนระบบปฏิบัติการลีนุกซ์

1.4.4 เครื่องมือที่ใช้ในการศึกษา

1.4.4.1 ซอฟต์แวร์

(1) ระบบตรวจสอบผู้บุกรุกเครือข่าย

โปรแกรม Snort เวอร์ชัน 2.0 เป็นเครื่องมือที่ใช้ตรวจจับการบุกรุกทางเครือข่าย (Network Intrusion Detection)

(2) ฐานข้อมูล

โปรแกรม Mysql เวอร์ชัน 3.23.54a-11 เป็นฐานข้อมูลเก็บข้อมูลการบุกรุกระบบ

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright © by Chiang Mai University
All rights reserved

(3) ส่วนติดต่อกับผู้ใช้

โปรแกรม ACID เวอร์ชัน 0.9.6b23 เป็นส่วนติดต่อกับผู้ใช้แบบกราฟิก ผ่านทางเว็บเพ็จ โดยพัฒนาจากภาษา PHP

(4) เว็บเซิร์ฟเวอร์

โปรแกรม Apache เวอร์ชัน 2.0.40-21 เป็นเว็บเซิร์ฟเวอร์

(5) ระบบป้องกันความปลอดภัยไฟร์วอลล์

โปรแกรม Iptables เวอร์ชัน 1.2.7a-2

(6) ส่วนประสานการทำงานระบบตรวจสอบและระบบป้องกันผู้บุกรุก

โปรแกรมปลั๊กอิน Snortsam เวอร์ชัน 2.21

(7) ระบบปฏิบัติการ

Redhat Linux เวอร์ชัน 9.0

1.4.4.2 ฮาร์ดแวร์

(1) เครื่องคอมพิวเตอร์ส่วนบุคคล 2 เครื่อง แบ่งเป็น

- ระบบป้องกันการบุกรุก (Pentium III 550 MHz. Ram 256 MB.)
- ระบบตรวจสอบผู้บุกรุก (Celeron 450 MHz. Ram 256 MB.)

(2) Hub 10/100 Mbps. 1 ตัว

1.5 สถานที่ที่ใช้ในการศึกษาและรวบรวมข้อมูล

1.5.1 คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่

1.5.2 บัณฑิตศึกษาสถาน มหาวิทยาลัยเชียงใหม่

ลิขสิทธิ์มหาวิทยาลัยเชียงใหม่
Copyright © by Chiang Mai University
All rights reserved