บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศที่คนรู้จักและใช้งานมากที่สุดคืออินเทอร์เน็ต(Internet) เนื่องจากสามารถค้นคว้าหาความรู้ได้มากมายจากทั่วทุกมุมโลก มหาวิทยาลัยราชภัฏเชียงรายเป็นสถาบันการศึกษาระดับอุดมศึกษา ดำเนินการสอนในระดับปริญญาตรีและปริญญาโทในหลายสาขา มีนักศึกษารวมทั้งสิ้นประมาณ 17,000 คน ในการดำเนินการเรียนการสอนนั้นได้อาศัยเทคโนโลยีสารสนเทศเข้ามาเป็นส่วนหนึ่งเพื่อเพิ่มทักษะและพัฒนาศักยภาพในการศึกษาของนักศึกษา รวมถึงการค้นคว้าหาข้อมูลของคณาจารย์และเจ้าหน้าที่ต่างๆ ที่เกี่ยวข้อง ในด้านการบริหารงานทั่วไปนั้นมีระบบสารสนเทศสำหรับการบริหารงาน ซึ่งนำมาช่วยในการทำงานหลายด้านของมหาวิทยาลัย เนื่องจากมีนักศึกษาเพิ่มจำนวนขึ้นมากทุกปี ดังนั้นจำนวนเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ในเครือข่ายของมหาวิทยาลัยนั้นได้เพิ่มจำนวนขึ้นเพื่อรองรับความต้องการที่เพิ่มมากขึ้น

ด้านเครือข่ายภายในมหาวิทยาลัยนั้นโครงสร้างหลักเป็นระบบบกิกะบิตอีเธอร์เน็ต (Gigabit Ethernet) ซึ่งสามารถรองรับปริมาณงานที่มีมากในเครือข่ายได้อย่างไม่มีปัญหา และในด้านการเชื่อมต่อกับอินเทอร์เน็ต มีการเชื่อมต่อกับผู้ให้บริการอินเทอร์เน็ต 3 รายเพื่อเพิ่มประสิทธิภาพและรองรับปริมาณความต้องการในการใช้งานที่เพิ่มมากขึ้น

เนื่องจากโครงสร้างหลักของเครือข่ายมีขนาดใหญ่ ปัญหาที่พบมากที่สุดคือการแพร่ระบาดของไวรัสอย่างรวดเร็วและการโดนผู้ไม่ประสงค์ดีทำการโจมตีระบบเพื่อให้หยุดการทำงานอยู่เสมอ เนื่องจากเจ้าหน้าที่รับผิดชอบมีน้อย ประกอบกับจำนวนเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ในเครือข่ายมีเป็นจำนวนมาก ทำให้การจัดการกับปัญหาเป็นไปด้วยความลำบากอย่างยิ่ง

จากการศึกษาข้อมูลเพิ่มเติมพบว่าองค์กรขนาดใหญ่มักมีระบบ ป้องกันและตรวจจับการบุกรุกเครือข่ายโดยมากจะเป็นฮาร์ดแวร์ที่มีราคาแพงมาก ซึ่งทางมหาวิทยาลัยราชภัฏเชียงรายไม่มีงบประมาณเพียงพอในการจัดซื้อ ดังนั้นจึงได้เกิดแนวคิดในการสร้างระบบตรวจจับการบุกรุกเครือข่ายของมหาวิทยาลัยโดยใช้ซอฟต์แวร์เสรี (Free Software) ที่ไม่ได้มีการเรียกเก็บค่าลิขสิทธิ์ซึ่งน่าจะมีความเหมาะสมกับทางมหาวิทยาลัยมากที่สุด

1.2 วัตถุประสงค์ของการศึกษา

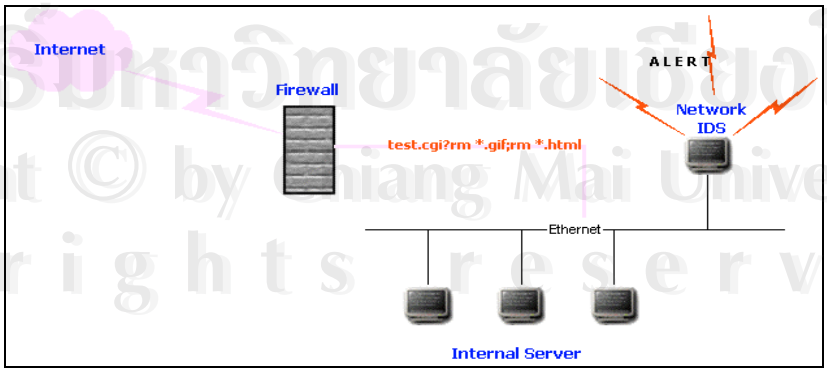
เพื่อสร้างระบบตรวจจับการบุกรุกเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏเชียงราย

1.3 ประโยชน์ที่ได้รับ

มหาวิทยาลัยราชภัฏเชียงรายมีระบบตรวจจับการบุกรุกเครือข่ายที่ไม่ต้องเสียเงินค่าลิขสิทธิ์ในการจัดซื้ออุปกรณ์ฮาร์ดแวร์ (Hardware) ราคาแพง

1.4 นิยามศัพท์เฉพาะ

Network Intrusion Detection System หมายถึง ระบบการตรวจจับการบุกรุกแบบ network-based นั้นจะทำการเฝ้าดูข้อมูลบนเครือข่ายโดยที่ระบบดังกล่าวจะทำการรับข้อมูลทั้งหมดที่อยู่บนส่วนของเครือข่ายที่รับผิดชอบ นอกเหนือจากส่วนของเครือข่ายที่รับผิดชอบ และชนิดของการสื่อสารอื่นๆ แล้วระบบดังกล่าวก็ไม่สามารถทำการตรวจจับได้



รูปที่ 1.1 แสดงหลักการทำงานของ ระบบการตรวจจับการบุกรุกแบบเครือข่าย

1.5 เครื่องมือที่ใช้ในการศึกษา

1.5.1 ด้านฮาร์ดแวร์

1. เครื่องไมโครคอมพิวเตอร์ มีคุณสมบัติดังนี้
   1) หน่วยประมวลผลกลาง (CPU) Intel Pentium 4 ความเร็ว 2.4 กิกกะเฮิรต์
   2) หน่วยความจำ (Memory) ขนาด 512 เมกกะไบต์
   3) จอภาพ (Monitor) 15 นิ้ว แบบเอสวีจีเอ (SVGA)
   4) หน่วยความจำสำรอง (Hard disk) 40 กิกกะไบต์
   5) การ์ดแสดงผลมีหน่วยความจำ 32 เมกกะไบต์
2. อุปกรณ์ Switch 4 ตัว

1.5.2 ด้านซอฟต์แวร์

1. ระบบปฏิบัติการ
   1) ระบบปฏิบัติการ Linux Fedora Core3 Kernel 2.6.9-1.667
   2) ระบบปฏิบัติการ FreeBSD 5.2.1
2. ฐานข้อมูล MySQL 4.0
3. โปรแกรมภาษาที่ใช้ในการพัฒนาระบบ
   1) ภาษาพีเอชพี(PHP Language) 4.3.10
   2) ภาษาเอชทีเอมแอล (HTML)
4. โปรแกรมประยุกต์สำหรับการช่วยสร้างระบบตรวจสอบการบุกรุก
   1) โปรแกรมสนอท (Snort) 2.2.0
   2) โปรแกรม ทีซีพีดัมพ์ (tcpdump) 3.8.3
   3) โปรแกรม อาร์ปาเช่ เวบเซอร์ฟเวอร์ (Apache web Server) 2.0.53
   4) โปรแกรม เอซิด (ACID) 0.9.6b23
   5) โปรแกรม เอนแมพ (NMap) 3.75
   6) โปรแกรม Plug-ins อื่นๆ ของโปรแกรม Snort

1.6 ขอบเขต และวิธีศึกษา

ศึกษา ออกแบบ และพัฒนาระบบตรวจสอบผู้บุกรุกเครือข่ายของมหาวิทยาลัยราชภัฏเชียงรายซึ่งมีขอบเขตและรายละเอียดดังต่อไปนี้

1.6.1 ขอบเขต

1. การจัดเก็บรูปแบบและตำแหน่งการบุกรุก
2. การรายงานผลเป็นภาษาไทย
3. การแสดงรายงานเชิงสถิติ
4. การจัดการเกี่ยวกับกฎเพื่อปรับแต่งเงื่อนไขในการตรวจสอบการบุกรุก

1.6.2 วิธีการศึกษา

1. ศึกษาหลักการทำงานของโปรโตคอล (Protocol) ทีซีพี/ไอพี (TCP/IP)
2. ศึกษาหลักการทำงานของระบบการตรวจจับการบุกรุกแบบเครือข่าย (Network Intrusion Detection System)
3. ศึกษาโครงสร้างของระบบเครือข่ายภายในของมหาวิทยาลัยราชภัฏเชียงราย
4. ออกแบบแผนผังระบบตรวจจับการบุกรุก ภายในเครือข่ายมหาวิทยาลัยราชภัฏเชียงราย
5. ทำการสร้าง ออกแบบ และทดสอบรูปแบบการโจมตีเครือข่ายจากภายในและภายนอกมหาวิทยาลัย
6. ทำการพัฒนาส่วนจัดการเรื่องกฎการตรวจสอบ
7. ทำการติดตั้งระบบตามที่ได้ออกแบบไว้
8. ทดสอบและปรับปรุงระบบ