บทที่ 5
บทสรุป

5.1 สรุปผล

ในการสร้างระบบตรวจสอบผู้บุกรุกเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏเชียงราย เป็นการค้นคว้าอิสระเชิงวิทยานิพนธ์ที่มุ่งเน้นในการสร้างระบบในการตรวจสอบเพื่อหาทางป้องกันการบุกรุกเครือข่ายของมหาวิทยาลัยฯ โดยใช้เครื่องมือในการพัฒนาที่ไม่มีการเรียกเก็บค่าลิขสิทธิ์ในการใช้งาน เพื่อเป็นแนวทางสำหรับองค์กรหรือหน่วยงานอื่นที่ขาดทุนทรัพย์ในการสร้างระบบ และเพื่อทำให้การทำงานของเครือข่ายคอมพิวเตอร์ของหน่วยงานสามารถใช้งานได้อย่างมีประสิทธิภาพมากขึ้น

ในการสร้างระบบตรวจสอบการบุกรุกเครือข่ายนี้ได้เริ่มจากการศึกษาเครื่องมือที่นำมาใช้และการออกแบบระบบ โดยมีการพัฒนาระบบเพิ่มเติมขึ้นมาใช้งานเองเพื่อทำให้การทำงานมีความสะดวกมากยิ่งขึ้น ผู้พัฒนาได้ใช้ซอฟต์แวร์ Snort เวอร์ชัน 2.3.2ในการตรวจสอบผู้บุกรุกเครือข่ายบนระบบปฏิบัติการ Fedora Core 3 และ FreeBSD 5.2.1 โดยทำการพัฒนาส่วนจัดการเรื่องกฎในการตรวจสอบของโปรแกรม Snort ด้วยภาษา พีเอชพี (PHP) สำหรับส่วนที่ใช้แสดงข้อมูลสถิตินั้นได้เลือกใช้โปรแกรม ACID เวอร์ชัน 0.9.6b23 ซึ่งพัฒนาให้สามารถแสดงผลเป็นภาษาไทยเพื่อสะดวกในการใช้งาน

ผลจากการสร้างระบบตรวจสอบผู้บุกรุกภายในเครือข่ายมหาวิทยาลัยราชภัฏเชียงรายทำให้ทราบว่าเครือข่ายภายในมีการใช้งานที่ผิดกฎเกณฑ์ที่กำหนดไว้อยู่มากนั่นจึงเป็นสาเหตุที่ทำให้ทราบว่าทำไมเครือข่ายที่ใช้งานอยู่จึงไม่มีเสถียรภาพ ทำให้สามารถหาแนวทางในการจัดการกับปัญหาที่เกิดขึ้นได้ในอนาคต

5.2 ปัญหาและอุปสรรค

ปัญหาและอุปสรรคในการค้นคว้าแบบอิสระเชิงวิทยานิพนธ์ ระบบตรวจสอบผู้บุกรุกเครือข่ายมหาวิทยาลัยราชภัฏเชียงราย มีดังนี้

1. ผู้ดูแลระบบต้องมีความมีความเข้าใจในเรื่องของเทคโนโลยีในการบุกรุกหรือโจมตีเครือข่ายซึ่งพัฒนารูปแบบใหม่ๆ ขึ้นมามาก
2. เนื่องจากซอฟต์แวร์ที่ใช้เป็นแบบไม่เก็บค่าใช้จ่ายจึงขาดการสนับสนุนด้านเทคนิค ทำให้ผู้ที่ใช้งานต้องทำการศึกษาค้นคว้าแบบลองผิดลองถูกเอง

3. ซอฟต์แวร์ที่ใช้สร้างระบบมีมากกว่า 1 โปรแกรมทำให้ต้องใช้เวลาในการติดตั้งและศึกษาทดลองเป็นระยะเวลานาน และมีโอกาสที่จะประสบปัญหาเรื่องความปลอดภัยจากตัวซอฟต์แวร์ที่ใช้นั้นเอง
4. การติดตั้งระบบตรวจจับการบุกรุกในเครือข่ายที่ใช้โปรโตคอล DHCP จะไม่สามารถระบุตำแหน่งของเครื่องที่ทำการละเมิดกฎเกณฑ์ได้อย่างถูกต้อง เนื่องจากมีการเปลี่ยนแปลงของหมายเลขอ้างอิงตลอดเวลา

5.3 ข้อจำกัดของระบบ

ข้อจำกัดของระบบตรวจจับผู้บุกรุกเครือข่ายมีดังนี้

1. การแจ้งเตือนผู้ดูแลระบบไม่เป็นแบบทันทีทันใด (Real – Time) ทำให้บางครั้งไม่สามารถระงับเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที
2. ส่วนที่ทำการจัดการเรื่องกฎของการตรวจสอบไม่สามารถตรวจสอบความถูกต้องของการเขียนกฎเกณฑ์ ทำให้บางครั้งกฎที่เขียนไปใช้ไม่สามารถทำงานได้จริง
3. ระบบไม่สามารถแก้ปัญหาที่ต้นเหตุของการณ์บุกรุกได้ ทำได้เพียงบันทึกรับทราบเป็นเหตุการณ์เพื่อรอให้ผู้ดูแลที่เกี่ยวข้องนำข้อมูลไปจัดการต่อไป
4. การจัดการเรื่องกฎของเครื่องเซ็นเซอร์ยังไม่สามารถกระทำโดยอัตโนมัติทำให้ประสบความยุ่งยากในการใช้งานสำหรับผู้ที่ได้มีความรู้ในการใช้งานเรื่องการเขียนกฎของโปรแกรมสนอร์ท
5. ผู้ที่ใช้งานระบบนี้ต้องมีความรู้ในเรื่องของเครือข่ายคอมพิวเตอร์ และที่สำคัญอย่างยิ่งคือมีความรู้ความเข้าใจในเรื่องโปรแกรมสนอร์ท
6. ยังไม่มีส่วนในการจัดการฐานข้อมูลที่ใช้จัดเก็บข้อมูลการบุกรุก

5.4 ข้อเสนอแนะ

1. พัฒนาส่วนการแจ้งเตือนเหตุการณ์ให้เป็นแบบทันทีทันใด (Real-Time)
2. ทำการรวบรวมซอฟต์แวร์เพื่อสร้างเป็นแพคเกจ (Package) สำหรับการติดตั้งระบบได้อย่างรวดเร็ว
3. พิจารณานำเทคโนโลยีอื่นมาประยุกต์ใช้ร่วมด้วย เพื่อทำให้มีประสิทธิภาพในการทำงานของเครือข่ายมีเพิ่มมากขึ้น
4. ประสิทธิภาพการทำงานในส่วนนี้จะขึ้นอยู่กับองค์ประกอบดังต่อไปนี้
   1.) สมรรถนะของเครื่องที่โปรแกรม Snort ทำงานอยู่

2.) จำนวนของกฎที่ใช้ในการเปรียบเทียบข้อมูลการบุกรุก

3.) ความเร็วของช่องทางที่เชื่อมต่อระบบเครือข่ายของเครื่องที่โปรแกรม Snort ทำงานอยู่

4.) ความหนาแน่นของข้อมูลบนเครือข่าย

5. เนื่องกฎเกณฑ์ที่ใช้ในการตรวจสอบมีรูปแบบการเขียนที่ยากควรมีการพัฒนารูปแบบมาตรฐาน (Template) เพื่ออำนวยความสะดวกต่อผู้ใช้งาน
6. ควรมีการบริหารจัดการกับฐานข้อมูลที่ใช้จัดเก็บเนื่องจากเซ็นเซอร์จะรายงานข้อมูลเข้ามาเป็นจำนวนมาก ในกรณีที่เกิดเหตุการณ์หลายๆ จุดในเครือข่ายขึ้นพร้อมๆ กันทำให้ขนาดของข้อมูลที่จัดเก็บมีขนาดใหญ่อย่างรวดเร็ว ผู้ดูแลระบบควรมีควรความรู้ในการบริหารจัดการกับฐานข้อมูล MySQL ด้วยจะเป็นประโยชน์อย่างยิ่ง