บทที่ 5
บทสรุป

5.1 สรุปผล

ระบบป้องกันและตรวจสอบผู้บุกรุกเครือข่าย บนระบบปฏิบัติการลีนุกซ์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ เป็นการค้นว้าแบบอิสระเชิงวิทยานิพนธ์ ที่มีวัตถุประสงค์เพื่อจัดทำระบบที่สามารถตรวจสอบและป้องกันผู้บุกรุกบนระบบเครือข่ายได้เองแบบอัตโนมัติ มุ่งเน้นทำให้การตรวจสอบและป้องกันการบุกรุกบนระบบเครือข่ายโดยรวมดีขึ้น อีกทั้งศึกษาอุปสรรค ปัญหา และข้อจำกัดต่างๆ ในการพัฒนาระบบ เพื่อเป็นแนวทางในการพัฒนาระบบตรวจสอบและป้องกันผู้บุกรุกเครือข่ายอื่น ๆ ต่อไปในอนาคต

การจัดทำระบบฯ ในครั้งนี้ ได้เริ่มจากการศึกษาและวิเคราะห์เทคโนโลยีที่ใช้ในการบุกรุก การป้องกันการบุกรุก ตลอดจนลักษณะระบบเครือข่ายและรูปแบบการบุกรุกที่เกิดขึ้นจริงบนเครือข่ายของคณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ เพื่อนำมาใช้ในการออกแบบและพัฒนาระบบ โดยผู้พัฒนาได้เลือกใช้เครื่องมือในการพัฒนา ดังนี้คือจัดทำระบบตรวจสอบผู้บุกรุกด้วยโปรแกรม Snort เวอร์ชัน 2.0 ระบบป้องกันการบุกรุกด้วยโปรแกรม Iptables บนระบบปฏิบัติการลีนุกซ์ Redhat เวอร์ชัน 9 ส่วนที่ประสานการทำงานระบบตรวจสอบและระบบป้องกันการบุกรุกด้วยโปรแกรมปลั๊กอิน Snortsam เวอร์ชัน 2.21 และส่วนติดต่อกับผู้ใช้แบบกราฟิก (Graphic User Interface) ด้วยโปรแกรม ACID เวอร์ชัน 0.9.6b23

ในส่วนของการทดสอบระบบได้ทำการทดสอบความถูกต้องในการตรวจสอบการบุกรุกที่เกิดขึ้น ตลอดจนการทำงานร่วมกันกับระบบป้องกันการบุกรุก ทำให้การตรวจสอบและป้องกันการบุกรุกมีประสิทธิภาพดีขึ้น และช่วยแบ่งเบาภาระของผู้ดูแลระบบได้จริง

5.2 ปัญหาและอุปสรรค

ปัญหาและอุปสรรคในการค้นคว้าแบบอิสระเชิงวิทยานิพนธ์ ระบบป้องกันและตรวจสอบผู้บุกรุกเครือข่าย บนระบบปฏิบัติการลีนุกซ์ คณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ มีดังนี้

1. เนื่องจากเครือข่ายคณะวิทยาศาสตร์ที่ใช้เป็นกรณีศึกษา ได้รับการป้องกันจากระบบรักษาความปลอดภัยทั้งจากไฟร์วอลล์ของมหาวิทยาลัย และแอนตี้ไวรัส-ไฟร์วอลล์ของคณะวิทยาศาสตร์เอง ทำให้การบุกรุกที่เกิดขึ้นจากภายนอกมหาวิทยาลัยและทั้งที่เกิดขึ้นจากภายในมหาวิทยาลัยเอง ถูกกรองให้ลดไปอย่างมาก เป็นผลให้ไม่สามารถวัดประสิทธิภาพของระบบฯได้อย่างเต็มที่

2. เครือข่ายที่เป็นกรณีศึกษาใช้หมายเลขไอพีแอดเดรสปลอม (Private IP) ซึ่งทำให้การอัฟเดตข้อมูลการบุกรุกค่อนข้างลำบาก ตลอดจนการแจ้งเตือนการบุกรุกในรูปแบบของอีเมล์ไม่สามารถแจ้งเตือนไปยังระบบภายนอกที่ใช้หมายเลขไอพีแอดเดรสจริง (Public IP) ได้

3. ผู้ดูแลระบบต้องมีทักษะความรู้ในเทคโนโลยีทางด้านระบบเครือข่าย การบุกรุก และการป้องกันการบุกรุกค่อนข้างสูง ซึ่งจำเป็นในการวิเคราะห์ทำความเข้าใจต่อข้อมูลการบุกรุกต่างๆ การหาสาเหตุการบุกรุก ตลอดจนการหาทางป้องกันที่เหมาะสมต่อไป

5.3 ข้อจำกัดของระบบ

1. ซอร์ฟแวร์ที่ใช้พัฒนาระบบฯทั้งหมดเป็นโอเพนซอร์ส (Open Source) ทำให้มีอาจมีปัญหาด้านความปลอดภัยเนื่องจากมีโอกาสถูกตรวจสอบโดยบรรดาผู้บุกรุกเพื่อหารูโหว่ของระบบ

2. ประสิทธิภาพของระบบฯขึ้นอยู่กับหลายองค์ประกอบเช่น เชื่อมต่อและสื่อสารข้อมูลบนเครือข่าย อุปกรณ์เครือข่าย และฮาร์ดแวร์ของเครื่องที่ตัวระบบฯทำงานเอง

3. การจัดวางตำแหน่งของระบบตรวจสอบผู้บุกรุกและระบบป้องกันผู้บุกรุก เนื่องจากข้อจำกัดทางด้านฮาร์ดแวร์และรูปแบบการเชื่อมต่อเครือข่ายระหว่างภาควิชาต่างๆ ภายในคณะฯ ทำให้เป็นการยากต่อการวางระบบฯให้ครอบคลุมการทำงานได้ทั้งหมด

4. ระบบฯไม่สามารถกำจัดต้นเหตุของการบุกรุกได้ ทำได้เพียงป้องกันการบุกรุกที่ตรวจเจอเท่านั้น

5. ข้อมูลรูปแบบการบุกรุกในส่วนของไวรัสและหนอนไม่ครอบคลุมเท่าข้อมูลในโปรแกรมประเภทแอนตี้ไวรัสโดยเฉพาะ (ผู้ดูแลระบบต้องกำหนดเพิ่มเข้าไปในฐานข้อมูลการบุกรุกของระบบฯเอง)

5.4 ข้อเสนอแนะ

1. ปรับปรุงการแสดงผลให้ดูง่ายขึ้นสำหรับผู้บริหาร
2. พัฒนาการอัฟเดรตข้อมูลรูปแบบการบุกรุกให้มีความทันสมัยอยู่เสมอและเป็นไปอย่างอัตโนมัติ
3. นำเทคโนโลยีทางด้านป้องกันการบุกรุกอื่นๆเข้ามาประยุกต์ใช้ร่วมกันอีก เช่น Honey Pot[1] , IPS (Intrusion Prevention System)[2]

[1] Honey Pot เทคโนโลยีในการล่อหลอกให้ผู้บุกรุกเข้ามาทำการโจมตีเครื่องที่แกล้งเป็นเหยื่อล่อ เพื่อศึกษาข้อมูลและวิธีการบุกรุกที่เกิดขึ้น

[2] Intrusion Prevention Syetem เป็นระบบป้องกันการบุกรุกที่ประกอบด้วยไฟร์วอลล์ ระบบตรวจสอบผู้บุกรุก นโยบายในการบังคับใช้ และส่วนประเมินรูโหว่ที่มีอยู่ รวมกันในหนึ่งระบบ