บทที่ 8
สรุปผลและวิจารณ์

8.1 สรุปผลการทดสอบ

จากการพัฒนาโปรแกรมป้องกันการบุกรุกแบบไดเรกทรอรีเบส ทำให้สามารถ เข้าใช้งานแอ็คทีฟไดเร็คทอรี (Active Directory) เพื่อทำการ เพิ่ม ลด แก้ไข เปลี่ยนแปลง กฎการป้องกันการบุกรุกของไฟร์วอลที่อยู่ใน ไดเรกทอรีดาต้าเบสได้ ทำให้สามารถป้องกันการโจมตีได้ตามการกำหนดกฎการป้องกัน ที่มีอยู่ในไดเรกทอรีดาต้าเบส และสามารถนำข้อมูลการโจมตีที่ตรวจจับได้จากเครื่องลูกข่ายมาเก็บลงฐานข้อมูลโดยล็อกมินิเตอร์ โดยสามารถนำข้อมูลที่ได้มาแสดงผลและวิเคราะห์เพื่อกำหนดกฎการป้องกันได้ตามการโจมตีที่เกิดขึ้นได้จริง

แต่การทำงานที่อยู่ในระบบวินโดว์2000 จะมีปัญหาพัฒนาเนื่องการโปรแกรมป้องกันที่พัฒนาขึ้นมาทดลองนั้นต้องทำงานอยู่ในระดับเคอร์เนลโหมด (Kernel mode) จึงต้องมีการเขียนโปรแกรมแบบ System Service เพื่อให้สามารถทำงานได้กับผู้ใช้ทุกกลุ่มโดยไม่มีปัญหา

การพัฒนาในขณะนี้ จะมุ่งเน้นไปที่การเข้าถึงการทำงานของไดเรกทอรีเซอร์วิส เพื่อนำมาใช้งาน และการจัดการกฎการป้องกันการโจมตีที่เครื่องเพอร์ซันนอลไฟร์วอลเพื่อใช้ป้องกันการโจมตีในเครือข่าย

8.2 ปัญหาและอุปสรรคในการพัฒนา

- การศึกษาโครงงานเดิมที่มีอยู่แล้ว ซึ่งจำเป็นที่จะต้องศึกษาโดยละเอียดเพื่อที่จะให้สามารถนำมาพัฒนาต่อได้อย่างถูกต้อง และมีประสิทธิภาพ แต่เนื่องจากโครงงานเดิมนั้นมีข้อความอธิบายโปรแกรม (Comment) น้อยมากทำให้การศึกษาโค้ดโปรแกรม และ โครงสร้างการทำงานของโปรแกรมทำได้ยาก และ ช้าซึ่งจะต้องเสียเวลานาน
- ปัญหาการรวมโครงงานแต่ละส่วนเข้าด้วยกันเพื่อที่จะให้ทำงานร่วมกันได้อย่างถูกต้องนั้นจะต้องมีการทำความเข้าใจหลักการทำงาน ของโปรแกรมแต่ละส่วนเป็นอย่างดีเพื่อที่จะให้สามารถนำมารวมเข้าด้วยกันแล้ว มีประสิทธิภาพมากที่สุด
- ในการคอมไพล์ (Compile) โค้ดโปรแกรมในบางครั้งถ้าหาก คอมไพเลอร์ (Complier) ที่ใช้หรือ รุ่นของเซอร์วิสแพ็ค (Service Pack) ไม่ตรงกันอาจจะคอมไพล์โค้ดโปรแกรมแล้วเกิดข้อผิดพลาดเกิดขึ้น ดังนั้นจึงควรตรวจสอบรุ่น และ เซอร์วิสแพ็คของโค้ดโปรแกรมที่เขียนขึ้นว่าพัฒนามาจากเวอร์ชันได

8.3 การพัฒนาต่อ

การพัฒนาต่อในขั้นต่อไปจะแบ่งออกเป็น 2 ส่วนดังนี้

8.2.1 การพัฒนาเพิ่มความสามารถพื้นฐาน

1. เพิ่มความสามารถในการทำงานโปรแกรมภายใต้สิทธิของผู้ใช้ได้ทุกกลุ่ม
2. การจัดการกฎการป้องกัน ให้มีความถูกต้องมากขึ้นเนื่องจากการเก็บข้อมูลของ ไดเรกทอรีจะไม่ค่อยแน่นอน

8.2.2 การพัฒนาเพิ่มความสามารถให้ใช้งานได้หลากหลายมากยิ่งขึ้น

1. การนำไดเรกทอรีมาใช้ในการเก็บข้อมูลได้มากขึ้น เช่น อ็อฟชันในการป้องกันการโจมตีที่มีการโจมตีบ่อยๆ เป็นต้น
2. พัฒนาโปรแกรมป้องกันการบุกรุกในรูปแบบอื่นๆ เช่น เกตเวย์ไฟร์วอล หรือโปรแกรมป้องกันเฉพาะด้าน เป็นต้น
3. ในการพัฒนาระบบตรวจจับผู้บุกรุกทางเครือข่ายคอมพิวเตอร์ควรใช้ระบบตรวจจับผู้บุกรุกที่เป็นแบบเปิดเผยโค้ด (Open source) ที่มีการปรับปรุงและพัฒนารูปแบบการในการตรวจจับผู้บุกรุกตลอดเวลา เพื่อที่จะให้สามารถตรวจจับการโจมตีรูปแบบใหม่ ๆ ได้อย่างมีประสิทธิภาพ