บทที่ 5
บทวิจารณ์และสรุป

5.1 วิเคราะห์และสรุปผลการทดสอบ

วิเคราะห์ผลการทดลอง

จากการทดลองที่ได้ทดสอบมาได้ผลเป็นที่น่าพอใจ เนื่องจากระบบที่เตรียมเอาไว้สามารถทำการเก็บข้อมูลหลักฐานได้อย่างครบถ้วน และแสดงผลออกมาได้ถูกต้องตามที่ออกแบบไว้ และสามารถป้องกันการโจมตีรูปแบบที่ต้องการได้ทั้งหมด ทั้งการโจมตีผ่านทางครือข่าย และการโจมตี ส่วนการฟื้นฟูระบบเมื่อเกิดความผิดปกติที่หลุดรอดจากการป้องกันของระบบนั้นนอกจากเราจะฟื้นฟูข้อมูลให้กลับมาเหมือนเก่าแล้ว ก็ควรจะนำข้อมูลหลักฐานที่เกี่ยวข้องต่างๆมาตัดสินใจเพื่อหาสาเหตุของความผิดปกติ และคิดค้นวิธีป้องกันเพื่อพัฒนาระบบของเราต่อไป

5.2 ปัญหาและอุปสรรค

ในช่วงระหว่างการพัฒนาชุดโปรแกรมตอบสนองเมื่อเกิดการละเมิดความปลอดภัยนั้นได้ประสบปัญหาต่างๆ หลายประการ ซึ่งได้รวบรวมมาและสรุปเป็นข้อๆ ดังนี้

1. เนื่องจากโครงงานนี้เป็นโครงงานต่อเนื่องจากปีการศึกษาที่แล้วดังนั้นจึงค่อนข้างเสียเวลาค่อนข้างมากในการที่จะศึกษาโครงงานเดิม และประกอบกับ log book เดิมที่มีข้อมูลไม่ครบถ้วน ทำให้ค่อนข้างที่จะกินเวลามากขึ้น

2 การใช้ระบบปฏิบัติการลีนุกซ์เป็นระบบปฏิบัติการหลักที่ใช้ในการทำโครงงานนั้นบ่อยครั้งที่มีปัญหากับเวอร์ชั่นของเคอร์นัล และปัญหาต่างๆ ที่เกิดจากตัวเคอร์นัล เอง ซึ่งส่งผลให้ต้องใช้เวลาในการศึกษาและเข้าใจว่าการพัฒนาควรจะใช้ เคอร์นัล เวอร์ชั่นอะไรให้มีความเสถียรมากที่สุด และเนื่องจากระบบที่พัฒนานั้นจะมีปัญหาเรื่อง environment ของระบบของ linux นั้นค่อนข้างจะหลากหลาย ทำให้ประสบปัญหาว่า environment ของระบบไม่ค่อยจะตรงกับ แหล่งอ้างอิงที่ใช้ในการพัฒนาโปรแกรม ซึ่งส่งผลให้ใช้เวลาแก้ปัญหาส่วนนี้เป็นอย่างมาก

3. ในการพัฒนาโปรแกรมนั้นจะมีการทำงานสอดคล้องกันระหว่างหลายภาษาทำให้ format ของ variable ต่างๆนั้นไม่ค่อยจะตรงกัน เช่น ตัวแปรเวลาที่ได้มาจากการทำงานของโปรแกรมที่พัฒนาจากภาษา C นั้น จะต้องมีการแก้ไขก่อนที่จะทำการบันทึกหรือติดต่อข้อมูลกับฐานข้อมูลก่อน มิฉะนั้นตัว Web Application จะไม่สามารถเรียกดูข้อมูลในส่วนนั้นได้ วิธีแก้ไขคือพัฒนาให้ตัวแปรต่างๆอยู่ในรูป variable ซึ่งขึ้นอยู่กับการทำงานของ application ใด application หนึ่ง ซึ่งหากมีการติดต่อมาจาก application อื่น ก็ให้มีการปรับเปลี่ยนจากส่วนของ application นั้น ให้สอดคล้องกับอีกส่วนหนึ่งแทน

4. ในการพัฒนาระบบที่ได้ออกแบบไว้นั้น ในช่วงแรกประสบปัญหากับเทคนิค และ วิธีการในการพัฒนาระบบซึ่งมีหลากหลายวิธี ส่งผลให้ค่อนข้างจะเสียเวลาในการเลือกวิธีการและเทคนิคต่างๆ ว่าเหมาะสมหรือไม่อย่างไรในการนำมาพัฒนาระบบ

5. ในการเขียนส่วนของ Web Application นั้นจะพัฒนาบนภาษา php ซึ่งจะต้องมีการติดต่อกับไฟล์ต่างๆใน system ซึ่งถือว่าจะต้องใช้คำสั่งที่นอกเหนือจากการพัฒนาของตัว Web Application ทั่วๆไป ทำให้เมื่อพัฒนาจะต้องหาแหล่งอ้างอิง หรือแหล่งความรู้ต่างๆ มาเพิ่มเติม

6. การหาหลักฐานเพื่อเตรียมให้ผู้ดูและระบบสืบหาหลักฐานนั้น จำเป็นจะต้องรู้ถึงรูปแบบการโจมตีในรูปแบบต่างๆ และเทคนิคต่างๆ ที่ผู้บุกรุกจะใช้เพื่อหลบหลีกการตามรอย และต้องรู้ว่าเหตุการณ์แบบใดที่ผิดปกติ และเหตุการณ์ใด เป็นเหตุการณ์ปกติ

7. ในการเก็บ Snapshot หากมีการสั่งให้ระบบทำการเก็บ Snapshot พร้อมๆ กันในหลายๆ Directory อาจทำให้ซีพียูทำงานหนักจนไม่สามารถประมวลผลงานอย่างอื่นได้ ซึ่งเป็นปัญหาตกค้างจากการทำงานของปีที่แล้ว แต่ได้ปีการศึกษานี้ได้แก้ไขดดยแยกการทำงานของทำ Snapshot ไปอีก Server หนึ่ง จึงพอที่จะลดทอนปัญหาส่วนนี้ได้ส่วนหนึ่งแต่ก็ยังไม่เพียงพอเนื่องจากเครื่องที่ใช้นั้นมีทรัพยากรไม่เพียงพอ

5.3 แนวทางการประยุกต์และพัฒนา

1. พัฒนาระบบให้สามารถรองรับตัว Server ที่ให้บริการได้เยอะขึ้น ในพื้นฐานของตัวระบบที่เท่าเดิม ซึ่งสามารถทำได้หากมีการแก้ไข Code ของระบบที่ถูกต้องและมีเครื่องคอมพิวเตอร์ที่มีศักยภาพพอในการพัฒนา
2. ทำการปรับปรุง Source Code ที่ได้เขียนให้มีประสิทธิภาพและรัดกุมมากขึ้น รวมทั้งเพิ่มการดัก error หรือ exception บางส่วนด้วย
3. ผู้บุกรุกที่มีความสามารถอาจทำการตัดการเชื่อมต่อระหว่างเครื่อง Server ที่ทำการดูแลและส่งข้อมูลจึงต้องเพิ่มส่วนที่ทำหน้าที่ตรวจสอบการเชื่อมต่อดังกล่าว
4. พัฒนาให้ระบบมีกระบวนการเคลียร์ค่า log file ต่างๆ ที่เก่า ซึ่งอาจจะแยกไว้ Backup ต่างๆ เพื่อให้ประสิทธิภาพในการ Query ข้อมูล เพื่อดู log ต่างๆ นั้นมีมากขึ้น
5. พัฒนาให้ระบบมีส่วนของป้องกันการ Exploit Code ที่มากขึ้น นอกเหนือจากการป้องกันบัฟเฟอร์โอเวอร์โฟลว์ ที่เกิดจากการเรียกใช้ ไลบรารี ภาษา C เท่านั้น
6. พัฒนาให้ระบบสามารถ alert การตรวจจับสิงผิดปกติที่เกิดขึ้นการทำงาน ซึ่งอาจมีผลกระทบขั้นร้ายแรงต่อระบบ หรือ เซิฟเวอร์ที่ให้บริการ โดยอาจจะให้มีการแจ้งเตือนผ่านเมลล์ หรือ sms หาก ผู้ดูแลหรือ Administrator ของระบบ หากไม่ได้ดูผลการทำงานของระบบอยู่ เช่น อาจติดธุระสำคัญๆ เป็นต้น
7. ทำการ Harden ระบบให้มีความปลอดภัยมากขึ้น