บทที่ 5

สรุปผลและข้อเสนอแนะ

จากการทดสอบระบบเครื่องมือ ISAN Security Gizmo Box ทั้ง 5 เครื่องมือ ได้แก่ Password Evaluation, Malware Scanning, Message Digest Generator, Vulnerability Scanning, HTTPS Testing สามารถสรุปผลและข้อเสนอแนะการทดสอบได้ดังนี้

5.1 สรุปผลและอภิปรายผล

การทำงานบนเครือข่ายคอมพิวเตอร์มีอัตราเพิ่มสูงขึ้นอย่างต่อเนื่องเช่นเดียวกับภัยคุกคามทางไซเบอร์ (Cyber Threat) การใช้งานบนเครือข่ายคอมพิวเตอร์ล้วนมีช่องโหว่และความเสี่ยงต่าง ๆ ส่งผลให้ภัยคุกคามทางไซเบอร์สามารถเกิดขึ้นได้ตลอดเวลา

แม้ว่าจะมีเครื่องมือตรวจสอบด้านความมั่นคงปลอดภัยอยู่หลายตัวแต่เครื่องมือเหล่านั้นมักมีปัญหาในการติดตั้งและการใช้งานอีกทั้งเครื่องมือส่วนใหญ่อยู่ในรูปแบบ Command Line Interface (CLI) ซึ่งยากต่อการใช้งานสำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไปหรือผู้ใช้งานมือใหม่ เนื่องจากต้องใช้เวลาในการศึกษาคำสั่งและการอ่านผลลัพธ์ที่ซับซ้อนทำให้ผู้ใช้งานต้องศึกษาอย่างละเอียดเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

โครงงานปริญญานิพนธ์นี้จึงนำเสนอเครื่องมือที่รวบรวมการตรวจสอบความมั่นคงปลอดภัยเบื้องต้นโดยพัฒนาเครื่องมือให้อยู่ในรูปแบบของ Graphical User Interface (GUI) ซึ่งจะช่วยอำนวยความสะดวกให้กับผู้ใช้งานเครื่องมือ ISAN Security Gizmo Box มีทั้งหมด 5 เครื่องมือและมีการทำงานดังนี้

5.1.1 เครื่องมือ Password Evaluation เป็นเครื่องมือสำหรับประเมินความมั่นคงปลอดภัยของรหัสผ่านซึ่งในปัจจุบันรหัสผ่านคือวิธีพื้นฐานที่ใช้กันอย่างกว้างขวางในการพิสูจน์ตัวตนในระบบออนไลน์และระบบอื่น ๆ แต่รหัสผ่านมีข้อจำกัดในด้านความปลอดภัยจึงได้มีการพัฒนาเครื่องมือนี้ขึ้นมาโดยผู้ใช้งานจะต้องป้อนรหัสผ่านเพื่อใช้ในการคำนวณผลลัพธ์ซึ่งรหัสผ่านที่ถูกป้อนเข้ามาจะนำไปคำนวณหา Bits of entropy, Estimated time to crack, Special warning อ้างอิงตามค่ามาตรฐาน NIST Special Publication 800-63B และเปรียบเทียบรหัสผ่านกับ NordPass common passwords นอกจากนี้ยังมีการทดสอบ Dictionary attack กับรหัสผ่านเพื่อวัดระดับความแข็งแกร่งของรหัสผ่านโดยจะเป็นแนวทางในการปรับปรุงรหัสผ่านเพื่อให้ผู้ใช้งานสามารถปรับปรุงรหัสผ่านของตนเองให้มีความปลอดภัยและแข็งแกร่งมากขึ้น

5.1.2 เครื่องมือ Malware Scanning เป็นเครื่องมือที่สำคัญในการตรวจสอบความปลอดภัยของระบบข้อมูลและเครือข่ายเนื่องจากมัลแวร์มักสร้างความเสียหายให้กับข้อมูลหรือระบบ จึงพัฒนา

เครื่องมือเพื่อให้ผู้ใช้งานสามารถตรวจสอบไฟล์หรือ URL ของเว็บไซต์ว่ามีมัลแวร์แฝงอยู่หรือไม่โดยเรียกใช้งาน VirusTotal API ซึ่งมีความสามารถในการตรวจสอบมัลแวร์โดยผู้ใช้งานจะต้องเพิ่มไฟล์หรือป้อน URL ของเว็บไซต์ที่ต้องการตรวจสอบหลังจากนั้นเครื่องมือ Malware scanning จะทำการเรียกใช้งาน VirusTotal API เพื่อทำการตรวจสอบหามัลแวร์และแสดงผลลัพธ์บน Graphical User Interface (GUI) นอกจากนี้ยังสามารถสร้างรายงานผลลัพธ์ดังกลาวและส่งรายงานไปยังอีเมลที่ต้องการได้

5.1.3 เครื่องมือ Message Digest Generator เป็นเครื่องมือสำคัญในความปลอดภัยข้อมูลและความสามารถในการตรวจสอบความครบถ้วนของข้อมูลโดยเครื่องมือจะทำการใช้ฟังก์ชันทางคณิตศาสตร์ได้แก่ MD5, SHA-1, SHA-2, SHA-3 หากข้อมูลถูกเปลี่ยนแปลงผลลัพธ์ที่ได้จะต่างออกไปทำให้สามารถใช้ในการตรวจสอบความปลอดภัยของข้อมูลได้ผู้ใช้งานสามารถเพิ่มไฟล์หรือข้อความเพื่อสร้าง Message digest โดยผลลัพธ์จะมีทั้งข้อความที่ถูกแฮชแล้วและนำค่าที่ได้ไปสร้าง QR code นอกจากนี้ยังสามารถส่งข้อความและ QR code ดังกล่าวไปยังกลุ่มแชทโดยได้ใช้ Line Notify

5.1.4 เครื่องมือ Vulnerability scanning เป็นเครื่องมือที่มีความสำคัญในความปลอดภัยของระบบข้อมูลโดยเครื่องมือนี้จะช่วยค้นหาช่องโหว่ของระบบเพื่อให้ผู้ใช้งานสามารถหาแนวทางในการป้องกันไม่ให้ตกเป็นเหยื่อของผู้ไม่ประสงค์ดีได้ซึ่งผู้ใช้งานสามารถป้อน IP address หรือโดเมนเนมของเว็บไซต์เพื่อใช้ทำการทดสอบได้และเครื่องมือจะไปเรียกใช้งาน Nmap ซึ่งเป็นโปรมแกรมที่ใช้ตรวจสอบ Port ที่เปิดใช้งานหรือข้อมูลที่อาจจะมีความเสี่ยงทำให้ระบบโดยโจมตีได้และแสดงผลลัพธ์บน Graphical User Interface (GUI) นอกจากนี้ยังสามารถสร้างรายงานผลลัพธ์ดังกลาวและส่งรายงานไปยังอีเมลที่ต้องการได้

5.1.5 เครื่องมือ Hypertext Transfer Protocol Secure (HTTPS Testing) เป็นเครื่องมือที่ตรวจสอบความปลอดภัยของการสื่อสารด้วย Protocol และสร้างความเชื่อมั่นให้กับผู้ที่เข้ามาใช้งานเว็บไซต์ว่าข้อมูลที่ส่งและรับถูกเข้ารหัสอย่างปลอดภัยซึ่งเครื่องมือนี้จะช่วยสร้างความน่าเชื่อถือให้กับเว็บไซต์นั้น ๆ ผู้ใช้งานสามารถป้อน URL เว็บไซต์ที่ต้องการทดสอบเครื่องมือจะทำการใช้ Testssl.sh เป็นเครื่องมือในรูปแบบสคริปต์สำหรับการทดสอบความปลอดภัยและการประเมินความเสี่ยงของเว็บไซต์และแสดงผลลัพธ์บน Graphical User Interface (GUI) นอกจากนี้ยังสามารถสร้างรายงานผลลัพธ์ดังกลาวและส่งรายงานไปยังอีเมลที่ต้องการได้

5.2 ปัญหาที่พบและข้อเสนอแนะ

ปัญหาที่พบในขณะดำเนินงาน คือ การนำเครื่องมือไปรันบนระบบปฏิบัติการ Linux หน้าของ Graphical User Interface (GUI) มีข้อผิดพลาดในการแสดงผลในส่วนของสีและฟอนต์จึงได้ทำการแก้ไขโดยติดตั้งฟอนต์ที่ใช้บนระบบปฏิบัติการ Linux และการสร้างรายงานอัตโนมัติด้วยภาษา Python ไม่มีความยืดหยุ่นเพียงพอทำให้การนำเสนอผลลัพธ์ที่แตกต่างกันไม่มีความสวยงามเท่าที่ควรในท้ายที่สุด

เครื่องมือ ISAN Security Gizmo Box สามารถทำงานได้ตามวัตถุประสงค์และทั้ง 5 เครื่องมือยังสามารถนำไปพัฒนาต่อได้ ดังนี้

5.2.1 เครื่องมือ Password Evaluation รองรับเฉพาะรหัสผ่านที่เป็นภาษาอังกฤษเมื่อผู้ใช้งานป้อนรหัสผ่านที่เป็นภาษาอื่นทำเครื่องมือไม่ทำการประมวลผลจึงอาจจะเพิ่มการรองรับภาษาอื่น ๆ เช่น ภาษาไทยหรือภาษาจีน เป็นต้น

5.2.2 เครื่องมือ Malware Scanning ใช้เฉพาะ VirusTotal API เพียงแหล่งเดียวสามารถเพิ่มฐานข้อมูลอื่นเข้ามาช่วยในการตรวจสอบมัลแวร์

5.2.3 เครื่องมือ Message Digest Generator ใช้แฮชฟังก์ชันเพียง 4 ชนิด คือ MD5, SHA-1, SHA-2, SHA-3 สามารถเพิ่มแฮชฟังก์ชันชนิดอื่นเพื่อเพิ่มความหลากหลายได้ เช่น CRC16 หรือ CRC32

5.2.4 เครื่องมือ Vulnerability Scanning ใช้ Nmap ในการสแกนบางครั้งอาจเกิดปัญหา segmentation fault ส่งผลให้เกิดการถูกปฏิเสธการเชื่อมต่อ (connection refused) ซึ่งสาเหตุอาจเกิดจาก การตั้งค่าไฟร์วอลล์หรือการควบคุมการเข้าถึง และหากในอนาคตมีช่องโหว่รูปแบบอื่น ๆ เกิดขึ้นควรปรับปรุงให้เครื่องมือสามารถทำการตรวจสอบช่องโหว่เหล่านั้นหรือนำ AI เข้ามาช่วยในการประมวลผลลัพธ์

5.2.5 เครื่องมือ Hypertext Transfer Protocol Secure (HTTPS Testing) ใช้ Testssl.sh ในการตรวจสอบความปลอดภัยของเว็บไซต์ในอนาคตหากเทคโนโลยีมีการเปลี่ยนแปลงไปควรปรับปรุงสคริปต์ให้สามารถทำการตรวจสอบเว็บไซต์เหล่านั้นหรือนำ AI เข้ามาช่วยในการประมวลผลลัพธ์