บทความวิจัย

กล่องเครื่องมือความมั่นคงไอสานกิซโม่

ISAN Security Gizmo Box

สมนึก พ่วงพรพิทักษ์, กาญจนา พินิจ, พีรธัช บุตรโท

สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

บทคัดย่อ

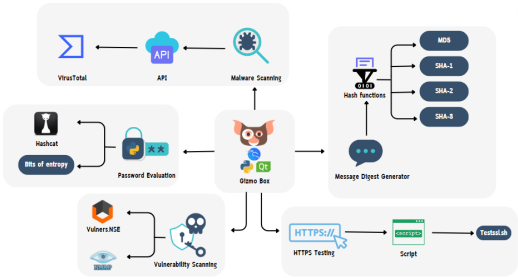
ISAN Security Gizmo Box เป็นเครื่องมือที่รวบรวมเครื่องมือเกี่ยวกับการตรวจสอบความมั่นคงปลอดภัยเบื้องต้นโดยแบ่งประเภทผู้ใช้งานงานออกเป็น 2 ประเภท ได้แก่ Advanced User ประกอบด้วยเครื่องมือ Password Evaluation, Malware Scanning, Message Digest Generator และ Network Engineer ประกอบด้วยเครื่องมือ Vulnerability Scanning, HTTPS Testing ไว้ในเครื่องมือเดียวกันและอยู่ในรูปแบบของ Graphical User Interface (GUI) ที่พัฒนาด้วย Qt Designer และเรียกใช้งานด้วยภาษา Python อีกทั้งยังนำเสนอในรูปแบบ Virtual Appliance ของ 2 Virtual Machines คือ Oracle VM VirtualBox และ VMware Workstation Player

บทนำ

ปัจจุบันการทำงานบนเครือข่ายคอมพิวเตอร์มีอัตราเพิ่มสูงขึ้นอย่างต่อเนื่องเช่นเดียวกับภัยคุกคามทางไซเบอร์ (Cyber Threat) เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์ (Snooping) การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) เป็นต้น การใช้งานบนเครือข่ายคอมพิวเตอร์ล้วนมีช่องโหว่และความเสี่ยงต่าง ๆ ส่งผลให้ภัยคุกคามทางไซเบอร์ สามารถเกิดขึ้นได้ตลอดเวลา แม้ว่าจะมีเครื่องมือตรวจสอบด้านความมั่นคงปลอดภัยอยู่หลายตัวแต่เครื่องมือเหล่านั้นมักมีปัญหาในการติดตั้งและการใช้งานอีกทั้งเครื่องมือส่วนใหญ่อยู่ในรูปแบบ Command Line Interface (CLI) ทำให้ผู้ใช้งานต้องมีความรู้เกี่ยวกับคำสั่งต่าง ๆ ซึ่งยากต่อการใช้งานสำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไปหรือผู้ใช้งานมือใหม่การที่จะใช้เครื่องมือแต่ละประเภทจะต้องใช้เวลาในการศึกษาคำสั่งและการอ่านผลลัพธ์ที่ซับซ้อนทำให้ผู้ใช้งานต้องศึกษาอย่างละเอียดเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

โครงงานปริญญานิพนธ์นี้จึงนำเสนอเครื่องมือที่รวบรวมการตรวจสอบความมั่นคงปลอดภัยเบื้องต้นที่ชื่อว่า ISAN Security Gizmo Box โดย Gizmo เป็นตัวละครหนึ่งในภาพยนตร์แฟนตาซีและคอมเมดี้เรื่อง "Gremlins" ที่ออกฉายครั้งแรกในปี 1984 จุดเด่นของ Gizmo คือสามารถแยกร่างได้เปรียบเสมือนเครื่องมือที่อยู่ใน Gizmo Box ซึ่งประกอบไปด้วย Password Evaluation, Malware Scanning, Message Digest Generator, Vulnerability Scanning และ HTTPS Testing ไว้ในเครื่องมือเดียวและอยู่ในรูปแบบของ Graphical User Interface

(GUI) เป็นรูปแบบที่นิยมในปัจจุบันและเหมาะสำหรับผู้ใช้งานทั่วไปซึ่งจะแสดงผลลัพธ์การทดสอบในรูปแบบที่มีความเหมาะสมเข้าใจง่ายและสามารถส่งรายงานผลลัพธ์ผ่านทางอีเมลอีกทั้งยังอยู่ในรูปแบบ Virtual Appliance ของ 2 Virtual Machines คือ Oracle VM VirtualBox และ VMware Workstation Player



ภาพประกอบที่ 1 ภาพรวมของระบบ

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

Bit of entropy คือ หน่วยวัดความแข็งแกร่งของรหัสผ่าน ซึ่ง Entropy [1] คำนวณได้จากสูตร E = L*log2(P) ซึ่ง L คือ ความยาวของรหัสผ่าน (Length) และ P คือ ขนาดของกลุ่มอักษรเฉพาะ (Pool of Characters) ที่ใช้สร้างรหัสผ่านจำนวนของค่าได้จะมีความแปรปรวนเป็นอย่างมากจนไม่สามารถคาดเดาได้และเป็นหนึ่งในมาตรการที่ใช้กันโดยทั่วไป

Dictionary Attack [2] คือการโจมตีความมั่นคงปลอดภัยทางไซเบอร์ประเภทหนึ่งที่เกี่ยวข้องกับการใช้รายการคำ วลี หรือสตริงอักขระอื่นๆ ที่กำหนดไว้ล่วงหน้าเป็นพื้นฐานในการพยายามเดารหัสผ่าน การโจมตีทำงานโดยลองใช้แต่ละคำในรายการทีละคำจนกว่าจะพบรหัสผ่านที่ถูกต้อง การโจมตีด้วย Dictionary มักใช้ร่วมกับการโจมตีประเภทอื่นๆ เช่น Brute-force attack เพื่อเพิ่มโอกาสในการประสบความสำเร็จลักษณะสำคัญอย่างหนึ่งของ Dictionary attack คือรายการคำที่ใช้มักจะปรับให้เหมาะกับเป้าหมายเฉพาะที่ถูกโจมตี Burt-force attack

Malicious [3] Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์หรือทำให้สูญเสีย CIA เป็น ส่วนประกอบหนึ่งของ INFOSEC [4] (Information Security) ซึ่งมาจากคำว่า Confidentiality (การรักษาความลับของข้อมูล) Integrity (ความแท้จริงของข้อมูล) และ Availability (การใช้งานได้ของระบบ) ซึ่งเป็นส่งที่ Security Professional

VirusTotal [5] เป็น free online service ที่วิเคราะห์ไฟล์หรือ URL เพื่อหามัลแวร์และภัยคุกคามอื่น ๆ ดำเนินการโดย Google และใช้งานโดยผู้คน ธุรกิจ และองค์กร ใช้เพื่อสแกนไฟล์และ URL เพื่อหาไวรัส เวิร์ม โทรจัน และมัลแวร์ประเภทอื่น ๆ VirusTotal ยังมี Application Programming Interface (API) ที่ช่วยให้นักพัฒนาสามารถรวมความสามารถในการสแกนของ VirusTotal เข้ากับแอปพลิเคชันหรือบริการของตนเองได้ เมื่อใช้ API นักพัฒนาสามารถส่งไฟล์หรือ URL เพื่อสแกนและรับผลลัพธ์ทางโปรแกรม สิ่งนี้มีประโยชน์สำหรับงานตรวจจับและวิเคราะห์มัลแวร์โดยอัตโนมัติ หรือสำหรับการรวมความสามารถของ

VirusTotal เข้ากับระบบรักษาความปลอดภัยที่ใหญ่ขึ้น

Message Digest algorithm 5 [4] (MD5) คือ รูปแบบการเข้ารหัสแบบแฮชชนิดหนึ่งการเข้ารหัสแบบแฮช (Cryptographic hash) คือ การแปลงรูปแบบของข้อมูลที่รับเข้ามาไม่ว่าขนาดเท่าใดก็ตาม ให้อยู่ในอีกรูปแบบหนึ่งที่มีขนาดคงที่ เพราะฉะนั้น จะไม่สามารถเรียกดูข้อมูลต้นฉบับได้ (Decrypt) ทำได้เพียงตรวจสอบว่าข้อมูลที่ให้มาแต่ละครั้งเหมือนกันหรือไม่ ความปลอดภัยจึงค่อนข้างสูง ในที่นี้ MD5 เป็นการเข้ารหัสแบบ 128-bit ให้ค่าเป็นตัวเลขฐาน 16 (0123456789abcd) ขนาด 32 ตัวอักษร แต่ก็มีบางประเภทที่ให้ค่าเป็น binary และ base64

Secure Hash Algorithm (SHA) [6] ได้รับการพัฒนาโดย National Institute of Standards and Technology (NIST) ในสหรัฐอเมริกา เผยแพร่ครั้งแรกเป็นมาตรฐานในปี 1993 โดยมีเป้าหมายในการจัดหาวิธีการที่ปลอดภัยและเชื่อถือได้สำหรับการสร้างค่าแฮชจากข้อมูลดิจิทัล SHA เวอร์ชันดั้งเดิมที่เรียกว่า SHA-0 พบว่ามีช่องโหว่บางอย่างและถูกแทนที่ด้วยเวอร์ชันแก้ไขที่เรียกว่า SHA-1 ในปี 1995 SHA มีหลายเวอร์ชัน ได้แก่ SHA-1, SHA-2 [16] และ SHA-3 [17] เวอร์ชันที่ใช้กันอย่างแพร่หลายคือ SHA-2 ซึ่งประกอบด้วยฟังก์ชันแฮชที่แตกต่างกันหลายฟังก์ชัน โดยมีขนาดบล็อกและขนาดเอาต์พุตที่แตกต่างกัน ฟังก์ชัน SHA-2 ที่พบบ่อยที่สุดคือ SHA-256 (ซึ่งสร้างเอาต์พุต 256 บิต) และ SHA-512 (ซึ่งสร้างเอาต์พุต 512 บิต)

Vulnerability คือ จุดอ่อนหรือช่องโหว่ หมายถึง สภาพแวดล้อมหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ และหากถูกใช้ให้เป็นประโยชน์โดยภัยคุกคามก็อาจทำให้ทรัพย์สินหรือข้อมูลต่าง ๆ ขององค์กรได้รับความเสียหาย นับได้ว่าความเสี่ยงของช่องโหว่ในระบบคอมพิวเตอร์ทั้งซอฟแวร์ หรือฮาร์ดแวร์ เป็นสิ่งที่มีผลกระทบความสำคัญต่อความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร หรือบริษัท การค้นพบช่องโหว่ใหม่มักจะนำไปสู่การสร้างโปรแกรมเจาะระบบ (Exploit Code), ไวรัส หรือมัลแวร์จากผู้บุกรุก หากผู้ดูแลระบบสามารถรับมราบข่าวสารของช่องโหว่ และติดตั้งโปรแกรมซ่อมแซมของช่องโหว่ไม่ทัน จะได้รับผลกระทบจากความเสี่ยงเหล่านี้แน่นอน โดยทั่วไปข่าวสารเกี่ยวกับช่องโหว่ มักจะได้มาจาก เจ้าของผลิตภัณฑ์ หรือเว็บไซต์ทางด้านความมั่นคงปลอดภัย

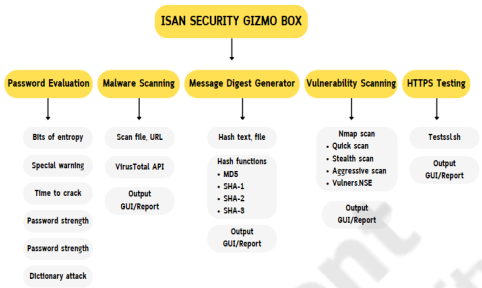
Hypertext Transfer Protocol (HTTP) คือ Protocol สื่อสารสำหรับการแลกเปลี่ยนสารสนเทศผ่านอินเทอร์เน็ต โดยหลักแล้วใช้ในการรับเอกสารข้อความหลายมิติที่นำไปสู่การเชื่อมต่อกับ World Wide Web (WWW) จะใช้เมื่อเรียกโปรแกรม web browser เช่น Firefox, Google Chrome, Safari, Opera และ IE Microsoft Internet Explorer เรียกดูข้อมูลหรือเว็บเพจ โปรแกรมบราวเซอร์ดังกล่าวจะใช้โพรโทคอล HTTP ซึ่งโพรโทคอลนี้ทำให้ Server ส่งข้อมูลมาให้บราวเซอร์ตามต้องการ

และบราวเซอร์จะนำข้อมูลมาแสดงผลบนจอภาพได้อย่างถูกต้อง ในการแลกเปลี่ยนข้อมูลกันระหว่าง Server และ Client ของ World Wide Web (Server) โดยส่งข้อมูลแบบ Clear text คือ ข้อมูลที่ทำการส่งไปนั้น ไม่ได้ทำการเข้ารหัส ทำให้สามารถถูกดักจับและอ่านข้อมูลได้ง่าย

Kali Linux เป็นระบบปฏิบัติการณ์ลินุกซ์ (Linux) ตัวหนึ่งของคอมพิวเตอร์ซึ่งมีพื้นฐานบน Linux distribution [5] ที่พัฒนาต่อมาจาก Debian ถูกเขียนขึ้นมาเหมือนกับ ระบบอื่นๆ เช่น Ubuntu ความสามารถที่แตกต่างจาก Linux ตัวอื่นๆ คือการติดตั้งและใส่ Feature หลักๆ และสำคัญเกี่ยวกับ งานด้านความปลอดภัยระบบไอทีไว้ให้โดยที่ไม่ต้องติดตั้ง หรือถ้ายังไม่ได้ติดตั้งก็สามารถติดตั้งได้ง่าย ผ่านระบบติดตั้งภายในที่มีให้เรียกว่า software repository ของ Kali

ขั้นตอนการดำเนินงาน

ในการพัฒนาเครื่องมือ ISAN Security Gizmo Box จะใช้ PyQt6 ร่วมกับภาษา Python เพื่อพัฒนา Graphical User Interface (GUI) ด้วย Qt Designer เพื่อเป็นตัวกลางในการสื่อสารระหว่างผู้ใช้งานและเครื่องมือต่าง ๆ ของเครื่องมือ ISAN Security Gizmo Box และขั้นตอนการดำเนินงานในการสร้างทั้ง 5 เครื่องมือ ได้แก่ Password Evaluation, Malware Scanning, Message Digest Generator, Vulnerability Scanning, HTTPS Testing โดยจะมีกรอบการดำเนินงานดังนี้



ภาพประกอบที่ 2 กรอบการดำเนินงาน

การทดสอบระบบ

จากการทดสอบระบบ ISAN Security Gizmo Box พบว่าเครื่องมือทั้ง 5 เครื่องมือ ประกอบด้วย ด้วย Password Evaluation, Malware Scanning, Message Digest Generator, Vulnerability Scanning และ HTTPS Testing สามารถทำงานได้ตามปกติทั้งการนำเข้าข้อมูล การประมวลผลข้อมูลการแสดงผลลัพธ์ต่าง ๆ และการนำไปใช้งานบน Virtual Machines และสามารถนำเข้าข้อมูลประมวลผลข้อมูลและแสดงผลลัพธ์ได้เช่นเดียวกันนอกจากนี้ Graphical User Interface (GUI) ยังอยู่ในรูปแบบที่เป็นมิตรกับผู้ใช้งาน

สรุปผลและข้อเสนอแนะ

การทำงานบนเครือข่ายคอมพิวเตอร์มีอัตราเพิ่มสูงขึ้นอย่างต่อเนื่องเช่นเดียวกับภัยคุกคามทางไซเบอร์ (Cyber Threat) การใช้งานบนเครือข่ายคอมพิวเตอร์ล้วนมีช่องโหว่และความเสี่ยงต่าง ๆ ส่งผลให้ภัยคุกคามทางไซเบอร์สามารถเกิดขึ้นได้ตลอดเวลา

แม้ว่าจะมีเครื่องมือตรวจสอบด้านความมั่นคงปลอดภัยอยู่หลายตัวแต่เครื่องมือเหล่านั้นมักมีปัญหาในการติดตั้งและการใช้งานอีกทั้ง

เครื่องมือส่วนใหญ่อยู่ในรูปแบบ Command Line Interface (CLI) ซึ่งยากต่อการใช้งานสำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไปหรือผู้ใช้งานมือใหม่เนื่องจากต้องใช้เวลาในการศึกษาคำสั่งและการอ่านผลลัพธ์ที่ซับซ้อนทำให้ผู้ใช้งานต้องศึกษาอย่างละเอียดเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

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

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

2) เครื่องมือ Malware Scanning เป็นเครื่องมือที่สำคัญในการตรวจสอบความปลอดภัยของระบบข้อมูลและเครือข่ายเนื่องจากมัลแวร์มักสร้างความเสียหายให้กับข้อมูลหรือระบบจึงพัฒนาเครื่องมือเพื่อให้ผู้ใช้งานสามารถตรวจสอบไฟล์หรือ URL ของเว็บไซต์ว่ามีมัลแวร์แฝงอยู่หรือไม่โดยเรียกใช้งาน VirusTotal API ซึ่งมีความสามารถในการตรวจสอบมัลแวร์โดยผู้ใช้งานจะต้องเพิ่มไฟล์หรือป้อน URL ของเว็บไซต์ที่ต้องการตรวจสอบหลังจากนั้นเครื่องมือ Malware scanning จะทำการเรียกใช้งาน VirusTotal API เพื่อทำการตรวจสอบหามัลแวร์และแสดงผลลัพธ์บน Graphical User Interface (GUI) นอกจากนี้ยังสามารถสร้างรายงานผลลัพธ์ดังกลาวและส่งรายงานไปยังอีเมลที่ต้องการได้

3) เครื่องมือ Message Digest Generator เป็นเครื่องมือสำคัญในความปลอดภัยข้อมูลและความสามารถในการตรวจสอบความครบถ้วนของข้อมูลโดยเครื่องมือจะทำการใช้ฟังก์ชันทางคณิตศาสตร์ได้แก่ MD5, SHA-1, SHA-2, SHA-3 หากข้อมูลถูกเปลี่ยนแปลงผลลัพธ์ที่ได้จะต่างออกไปทำให้สามารถใช้ในการตรวจสอบความปลอดภัยของข้อมูลได้ ผู้ใช้งานสามารถเพิ่มไฟล์หรือข้อความเพื่อสร้าง Message digest โดยผลลัพธ์จะมีทั้งข้อความที่ถูกแฮชแล้วและนำค่าที่ได้ไปสร้าง QR code นอกจากนี้ยังสามารถส่งข้อความและ QR

code ดังกล่าวไปยังกลุ่มแชทโดยได้ใช้ Line Notify

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

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

ปัญหาที่พบและข้อเสนอแนะ

ปัญหาที่พบในขณะดำเนินงาน คือ การนำเครื่องมือไปรันบนระบบปฏิบัติการ Linux หน้าของ Graphical User Interface (GUI) มีข้อผิดพลาดในการแสดงผลในส่วนของสีและฟอนต์จึงได้ทำการแก้ไขโดยติดตั้งฟอนต์ที่ใช้บนระบบปฏิบัติการ Linux และการสร้างรายงานอัตโนมัติด้วยภาษา Python ไม่มีความยืดหยุ่นเพียงพอทำให้การนำเสนอผลลัพธ์ที่แตกต่างกันไม่มีความสวยงามเท่าที่ควรในท้ายที่สุดเครื่องมือ ISAN Security Gizmo Box สามารถทำงานได้ตามวัตถุประสงค์และทั้ง 5 เครื่องมือยังสามารถนำไปพัฒนาต่อได้ ดังนี้

1) เครื่องมือ Password Evaluation รองรับเฉพาะรหัสผ่านที่เป็นภาษาอังกฤษเมื่อผู้ใช้งานป้อนรหัสผ่านที่เป็นภาษาอื่นทำเครื่องมือไม่ทำการประมวลผลจึงอาจจะเพิ่มการรองรับภาษาอื่น ๆ เช่น ภาษาไทยหรือภาษาจีน เป็นต้น

2) เครื่องมือ Malware Scanning ใช้เฉพาะ VirusTotal API เพียงแหล่งเดียวสามารถเพิ่มฐานข้อมูลอื่นเข้ามาช่วยในการตรวจสอบมัลแวร์

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

4) เครื่องมือ Vulnerability Scanning ใช้ Nmap ในการสแกนบางครั้งอาจเกิดปัญหา segmentation fault ส่งผลให้เกิดการถูก

ปฏิเสธการเชื่อมต่อ (connection refused) ซึ่งสาเหตุอาจเกิดจาก การตั้งค่าไฟร์วอลล์หรือการควบคุมการเข้าถึง และหากในอนาคตมีช่องโหว่รูปแบบอื่น ๆ เกิดขึ้นควรปรับปรุงให้เครื่องมือสามารถทำการตรวจสอบช่องโหว่เหล่านั้นหรือนำ AI เข้ามาช่วยในการประมวลผลลัพธ์

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

เอกสารอ้างอิง

1. C.Shannon. "A Mathematical Theory of Communication".1948

2. J. Atwood. “Dictionary attack 101”. January 2009.

3. "Malware Etymology". Online Etymology Dictionary. Retrieved 17, November 2022.

4. R. Rivest. “MD5 message-digest”. April 1992.

5. Hispasec Sistemas. “VirusTotal”. June 2004

6. National Security Agency. "Secure Hash Algorithm 1". 1995