บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

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 คือสามารถแยกร่างได้ เปรียบเสมือนเครื่องมือที่อยู่ใน 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

1.2 วัตถุประสงค์ของโครงงาน

พัฒนาเครื่องมือ ISAN Security Gizmo Box ที่ประกอบไปด้วยเครื่องมือการตรวจสอบความมั่งคงปลอดภัยเบื้องต้นและอยู่ในรูปแบบของ Graphical User Interface (GUI) โดย ISAN Security Gizmo Box แบ่งประเภทผู้ใช้งานออกเป็น 2 ประเภท ได้แก่ Advanced User ประกอบด้วยเครื่องมือ Password Evaluation, Malware Scanning, Message Digest Generator และ Network Engineer ประกอบด้วยเครื่องมือ Vulnerability Scanning, HTTPS Testing Digest Generator

1.3 ขอบเขตของโครงงาน

1.3.1 ISAN Security Gizmo Box อยู่ในรูปแบบ Virtual Appliance ของ 2 Virtual Machines คือ Oracle VM VirtualBox และ VMware Workstation Player

1.3.2 ISAN Security Gizmo Box ผู้ใช้งานประเภท Advanced User ประกอบไปด้วย Password Evaluation, Malware Scanning, Message Digest Generator

1.3.3 ISAN Security Gizmo Box ผู้ใช้งานประเภท Network Engineer ประกอบไปด้วย Vulnerability Scanning, HTTPS Testing

1.3.4 เครื่องมือประเมินรหัสผ่าน (Password Evaluation) มีคุณสมบัติ ดังนี้

1) วัดค่าความต้านทานในการถูกโจมตีด้วยเทคนิค Brute-force attack ได้ดีหรือไม่โดยการคำนวณออกมาเป็นข้อมูลเชิงปริมาณ คือ Bits of entropy และข้อมูลเชิงคุณภาพ คือ ข้อมูลที่ประเมินจากค่า entropy

2) Special Warning การแจ้งเตือนความเสี่ยงของรหัสผ่าน เช่น มีเฉพาะตัวเลข มีเฉพาะตัวอักษร ไม่มีตัวพิมพ์เล็ก ไม่มีตัวพิมพ์ใหญ่ ไม่ผสมอักขระพิเศษ อ้างอิงตามค่ามาตรฐาน NIST Special Publication 800-63B [1]

3) คำนวณหาค่า Estimated time to crack

4) เปรียบเทียบรหัสผ่านที่ผู้ใช้งานป้อนเข้ามาว่าถูกบันทึกไว้ใน NordPass common Passwords หรือไม่

5) ใช้เทคนิค Dictionary attack [3] เพื่อตรวจสอบว่ารหัสผ่านถูกค้นพบหรือถูกบันทึกไว้ใน Wordlist ของ Hacker หรือไม่โดยใช้ Dictionary จากหลายแหล่งได้แก่ CrackStation [12], Rockyou.txt โดยแบ่งรูปแบบการดำเนินการเป็น 2 รูปแบบ

- Straightforward Dictionary attack
- Skipping attack โดยแบ่งออกเป็น 2 รูปแบบได้แก่ Combinator attack และ Hybrid attack ซึ่งใช้ Hashcat เข้ามาช่วยในการทดสอบเพื่อขยายขอบเขตของ Dictionary ให้กว้างมากขึ้น และเพิ่มโอกาสในการค้นหามากขึ้น

6) การเลือกใช้ Multi-wordlist โดยสามารถเลือกใช้ wordlist ได้หลายไฟล์สำหรับการทำ Dictionary attack

1.3.5 เครื่องมือตรวจสอบ Malware (Malware Scanning) มีคุณสมบัติ ดังนี้

1) ตรวจสอบ Malware จากไฟล์ที่ผู้ใช้งานเพิ่มเข้ามาเพื่อตรวจสอบ

2) ตรวจสอบ Malware จาก URL ของเว็บไซต์ที่ผู้ใช้งานเพิ่มเข้ามาเพื่อตรวจสอบ

3) สามารถเรียกใช้งานบริการ Antivirus ได้หลายบริษัทมาช่วยสแกนผ่าน VirusTotal API

1.3.6 แสดงผลการทดสอบในรูปแบบของรายงาน โดยรายละเอียดของรายงานประกอบด้วย ชื่อไฟล์หรือ URL ของเว็บไซต์ วันและเวลา ชื่อบริษัทที่ใช้ในการสแกน

1) เพื่อแสดงผลลัพธ์บนหน้าจอ GUI ให้ผู้ใช้งานสามารถดูรายละเอียดของผลลัพธ์ที่ได้จากการสแกน โดยผลลัพธ์ที่ได้จากการสแกนจะแบ่งออกเป็น 3 กลุ่ม ดังนี้

- Malicious คือ พบ Malware
- Suspicious คือ สงสัยว่าอาจจะมี Malware
- Undetected คือ ไม่สามารถตรวจสอบได้

2) เพื่อบันทึกผลลัพธ์หรือแชร์ให้กับผู้อื่น ด้วยการส่งรายงานจากการสแกน โดยการระบุ Email address ปลายทางที่ต้องการส่งไปซึ่งจะอยู่ในรูปแบบของ PDF ไฟล์

1.3.7 เครื่องมือคำนวณค่า Message Digest Generator มีคุณสมบัติ ดังนี้

1) Function การคำนวณ Message Digest ที่รองรับได้แก่ MD5, SHA-1, SHA-2 และ SHA-3

2) สามารถนำเข้าข้อมูลได้ 2 รูปแบบ คือ ข้อความและ ไฟล์เพื่อนำไปคำนวณหาค่าแฮช

3) การแสดงผลลัพธ์จากการคำนวณ Message Digesting แสดงได้ 2 รูปแบบ คือ แสดง Message Digest ที่คำนวณได้ในรูปแบบข้อความและ นำ Message digest ที่ได้จากข้อความโดยแปลงให้อยู่ในรูปของ QR Code เพื่อให้ง่ายต่อการนำไปใช้งาน

4) เปรียบเทียบค่าแฮชที่ได้กับค่าแฮชที่ผู้ใช้งานป้อนเข้ามา

5) สามารถส่งผลลัพธ์ไปยัง Line Notify ได้

1.3.8 เครื่องมือตรวจสอบหาช่องโหว่ (Vulnerability Scanning) และตรวจสอบ Port และ Service ที่เปิดของเครื่องปลายทางมีคุณสมบัติ ดังนี้

1) ใช้คำสั่ง Nmap เพื่อตรวจสอบ Port และ Service ที่เปิดอยู่ของเครื่องปลายทางโดยใช้ฐานข้อมูลจาก Well-Know Port แบ่งเป็น 4 ประเภท ดังนี้

- Quick scan โดยใช้ Option Timing Template 4 หรือ -T4 และ Fast Mode หรือ -F
- Stealth Scan โดยใช้ Option TCP SYN scan หรือ -sS
- Aggressive Scan โดยใช้ Option OS detection หรือ -O และ Version detection หรือ -sV
- ใช้ Vulners.NSE โดยใช้ Option --script vulners ร่วมกับ Nmap

2) แสดงผลการทดสอบในรูปแบบของรายงาน โดยรายละเอียดของรายงานประกอบด้วย เครื่องมือที่ใช้ วันและเวลา เครื่องปลายทาง Port สถานะ Service Version Operating System และ CVE โดยแบ่งการแสดงผลเป็น 2 รูปแบบ คือ

- แสดงผลลัพธ์บนหน้าจอ GUI ให้ผู้ใช้งานสามารถดูรายละเอียดของผลลัพธ์จากการทดสอบด้วย Testssl.sh โดยมีรายละเอียดดังข้อ 4)

- สามารถบันทึกผลลัพธ์หรือแชร์ให้กับผู้ใช้งานอื่น ด้วยการส่งรายงานจากการสแกนโดยการระบุ Email address ปลายทางที่ต้องการส่งไปซึ่งจะอยู่ในรูปแบบของ PDF ไฟล์

1.3.9 เครื่องมือตรวจสอบความมั่นคง Hypertext Transfer Protocol Secure (HTTPS Testing) มีคุณสมบัติ ดังนี้

1) ตรวจสอบ HTTPS Header โดยใช้ Open-Source Testssl.sh

2) ตรวจสอบความปลอดภัยของ Protocol ที่ให้บริการ SSL/TLS

3) ตรวจสอบ HSTS Preload

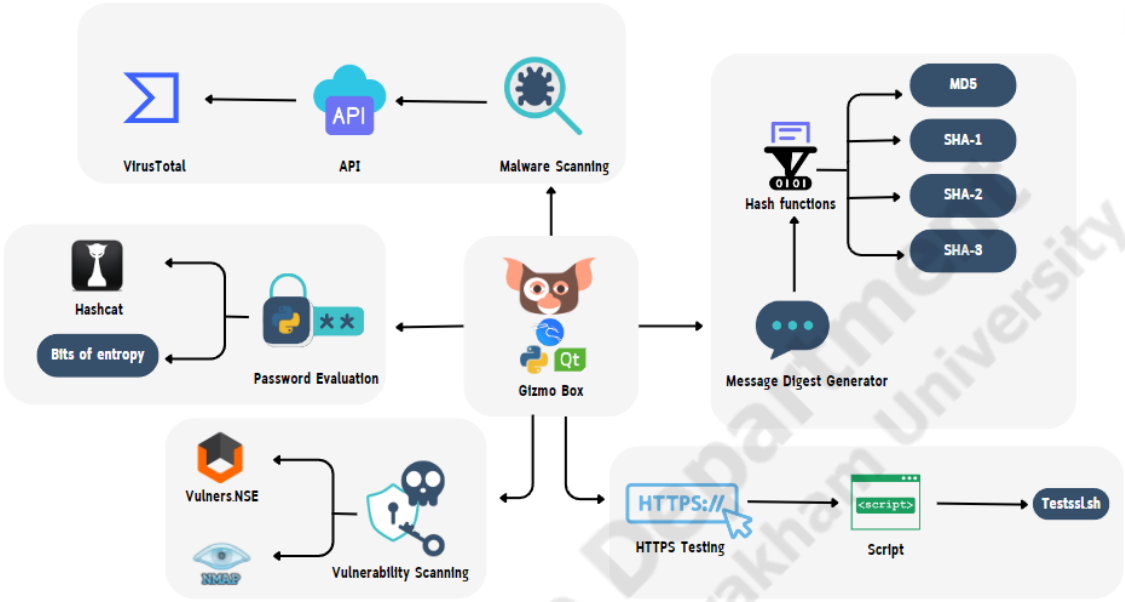
4) แสดงผลการทดสอบในรูปแบบของรายงานโดยรายละเอียดของรายงานประกอบด้วยข้อมูลเกี่ยวกับ Domain Name, Certificate, Certificate Expiration, Offensive Security Certified Professional ข้อมูลเกี่ยวกับ Algorithm ที่ใช้เข้ารหัส, Digital Signature และ hashing functions ที่ใช้ พร้อมบอกจำนวนบิตที่ใช้ และแจ้งเตือนผู้ใช้งานหากพบว่าไม่เหมาะสม ข้อมูลเกี่ยวกับจุดอ่อน หรือโอกาสที่จะถูก Downgrade Attack เช่น POODLE, DROWN, BEAST, SWEET32, LUCK13, Heartbleed ว่าเป็นไปได้หรือไม่ และข้อมูลเกี่ยวกับการ HSTS Preload

5) ผลลัพธ์ที่ได้จากการทดสอบสามารถแสดงผลลัพธ์ได้ 2 รูปแบบ ได้แก่

- แสดงผลลัพธ์บนหน้าจอ GUI ให้ผู้ใช้งานสามารถดูรายละเอียดของผลลัพธ์จากการทดสอบด้วย Testssl.sh โดยมีรายละเอียดดังข้อ 4)

- สามารถบันทึกผลลัพธ์หรือแชร์ให้กับผู้ใช้งานอื่น ด้วยการส่งรายงานจากการสแกนโดยการระบุ Email address ปลายทางที่ต้องการส่งไปซึ่งจะอยู่ในรูปแบบของ PDF ไฟล์

1.4 ภาพรวมของระบบ



ภาพประกอบที่ 1.1 ภาพรวมของระบบ

ภาพรวมทั้งหมดของระบบ ISAN Security Gizmo Box จะแยกเป็น Modules ย่อย ๆ ประกอบไปด้วย Password Evaluation, Malware Scanning, Vulnerability Scanning, HTTPS Testing และ Message Digest Generator โดยเครื่องมือที่ได้อยู่ในรูปแบบ Virtual Appliance ของ 2 Virtual Machines แบบใหญ่ๆ คือ Oracle VM VirtualBox และ VMware Workstation Player โดยทั่วไปใน Kali Linux มีเครื่องมือด้านความมั่นคงปลอดภัยที่หลากหลายแต่เนื่องด้วยเครื่องมือแต่ละประเภทต้องเรียกใช้โดย Command Line Interface (CLI) ซึ่งยากต่อการใช้งานสำหรับผู้ใช้งานคอมพิวเตอร์ทั่วไปหรือผู้ใช้งานมือใหม่การจะใช้แต่ละเครื่องมือแต่ละประเภทจะต้องใช้เวลาในการศึกษาคำสั่งและการอ่านผลลัพธ์ที่ซับซ้อนทำให้ผู้ใช้งานต้องศึกษาอย่างละเอียดเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

ภาพประกอบที่ 1.2 โครงสร้างสถาปัตยกรรมภายใน

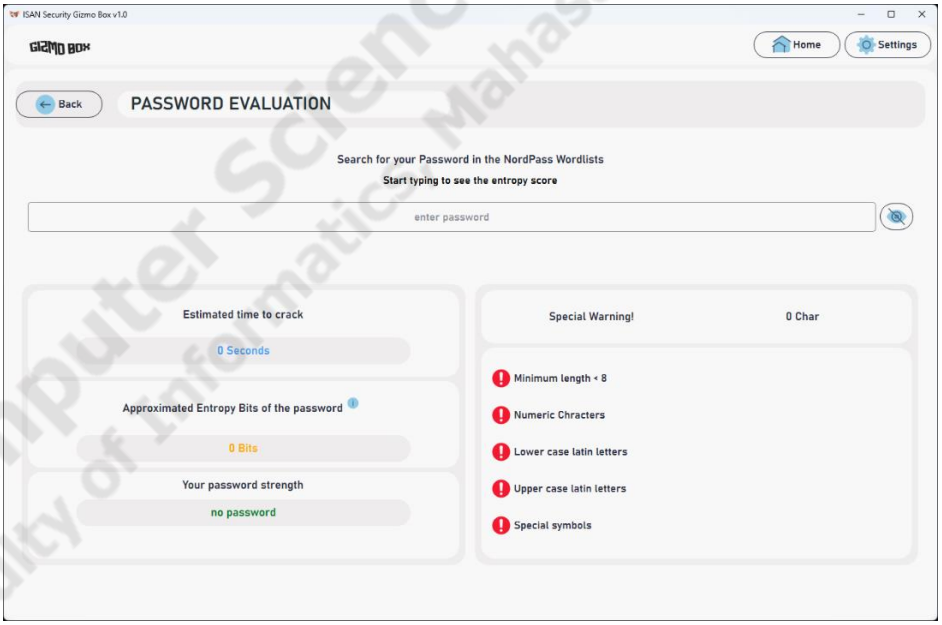
โครงสร้างสถาปัตยกรรมภายในของระบบ ISAN Security Gizmo Box มีดังนี้ คือติดตั้ง Kali Linux เป็นฐานของเครื่องมือและมีการติดตั้งเครื่องมือเพิ่มเติม เช่น Vulners.NSE, Testssl.sh เป็นต้น และมีการเขียนโปรแกรมเพิ่มเติมด้วยภาษา Python ร่วมกับ Qt Designer เพื่อให้อยู่ในรูปแบบของ Graphic User Interface (GUI) ที่เป็นมิตรต่อผู้ใช้งาน

1.5 ตัวอย่างเครื่องมือ ISAN Security Gizmo Box

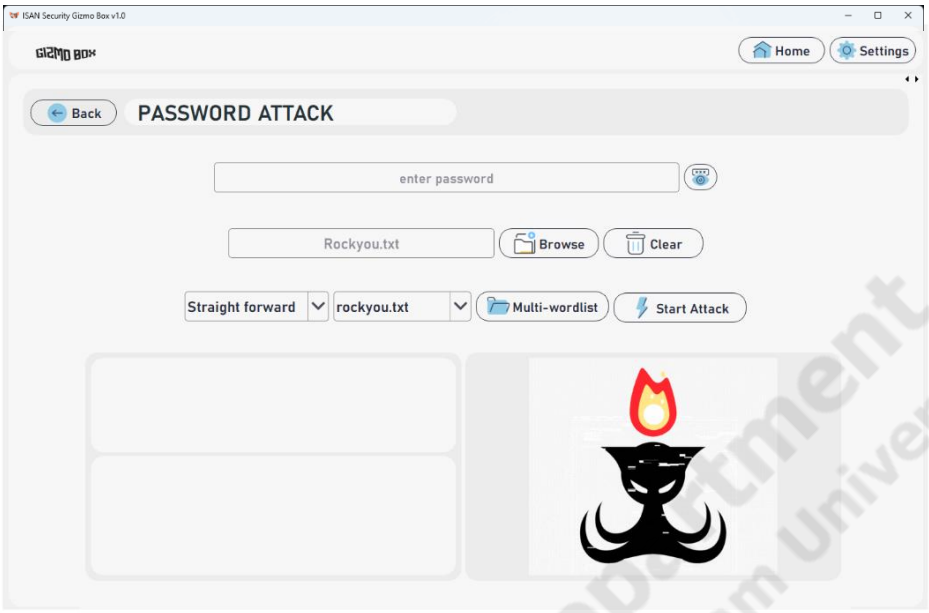
ภาพประกอบที่ 1.3 หน้าแรกของเครื่องมือ ISAN Security Gizmo Box

ภาพประกอบที่ 1.4 หน้าเลือกประเภทผู้ใช้งาน

ภาพประกอบที่ 1.5 หน้าเลือกเครื่องมือของ Advanced User

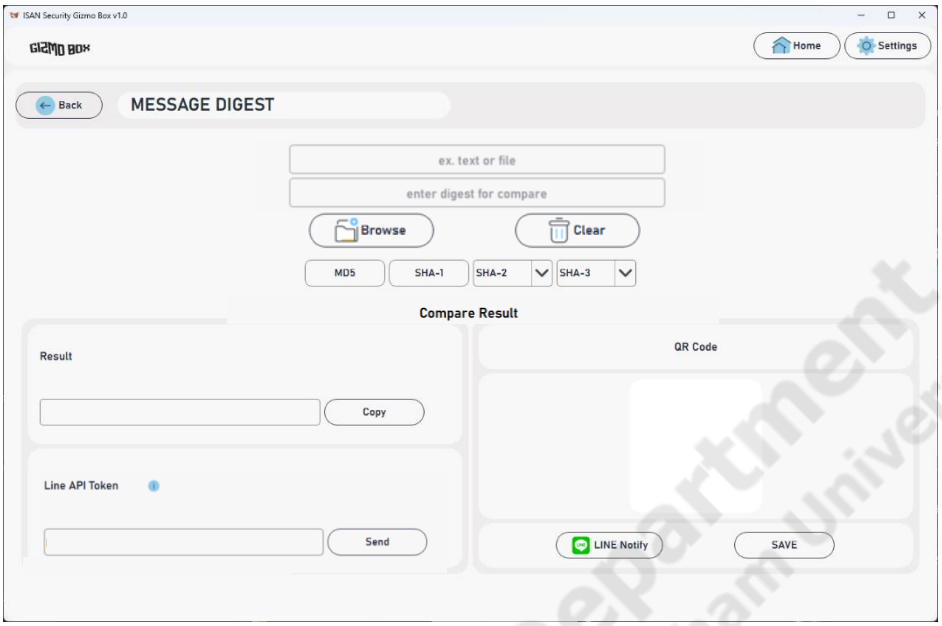


ภาพประกอบที่ 1.6 หน้าเครื่องมือ Password Evaluation



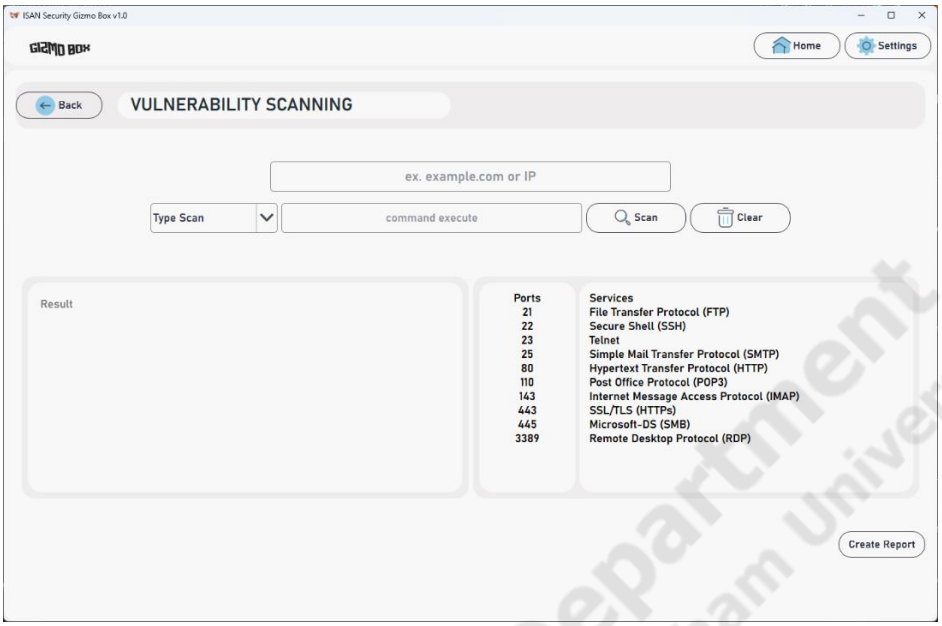
ภาพประกอบที่ 1.7 หน้าเครื่องมือ Password attack

ภาพประกอบที่ 1.8 หน้าเครื่องมือ Malware Scanning

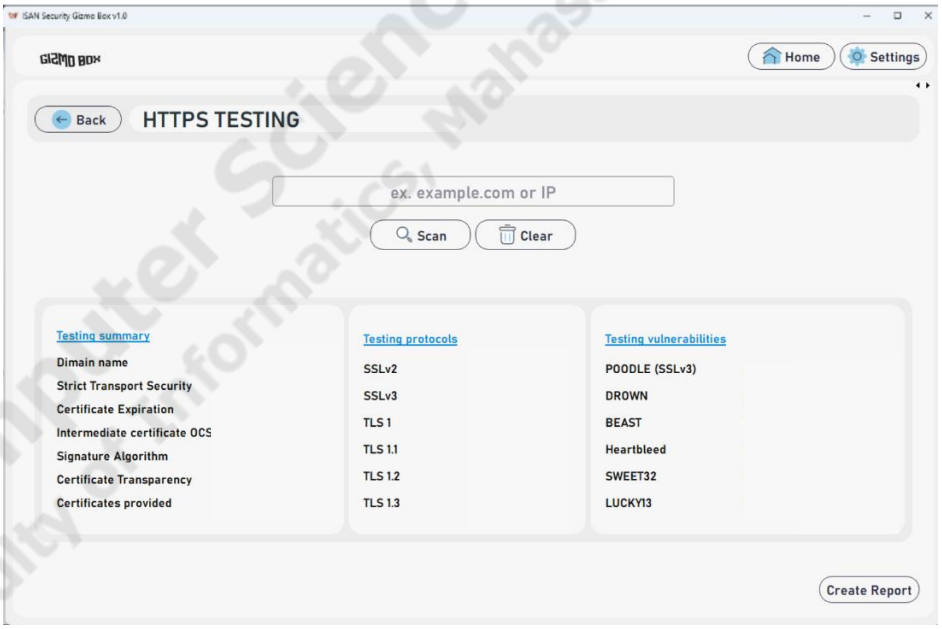


ภาพประกอบที่ 1.9 หน้าเครื่องมือ Message Digest Generator

ภาพประกอบที่ 1.10 หน้าเลือกเครื่องมือของ Network Engineer

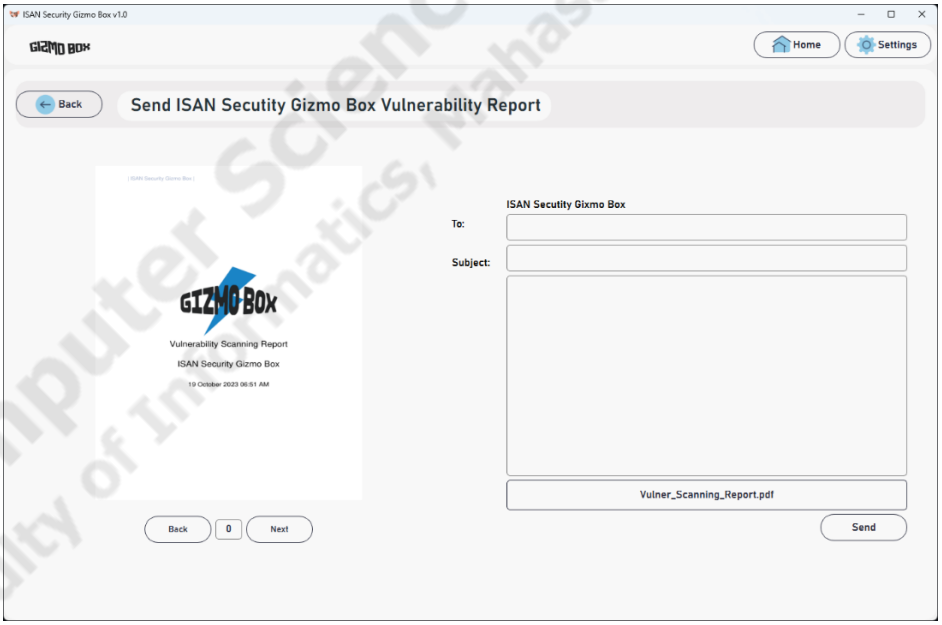


ภาพประกอบที่ 1.11 หน้าเครื่องมือ Vulnerability Scanning



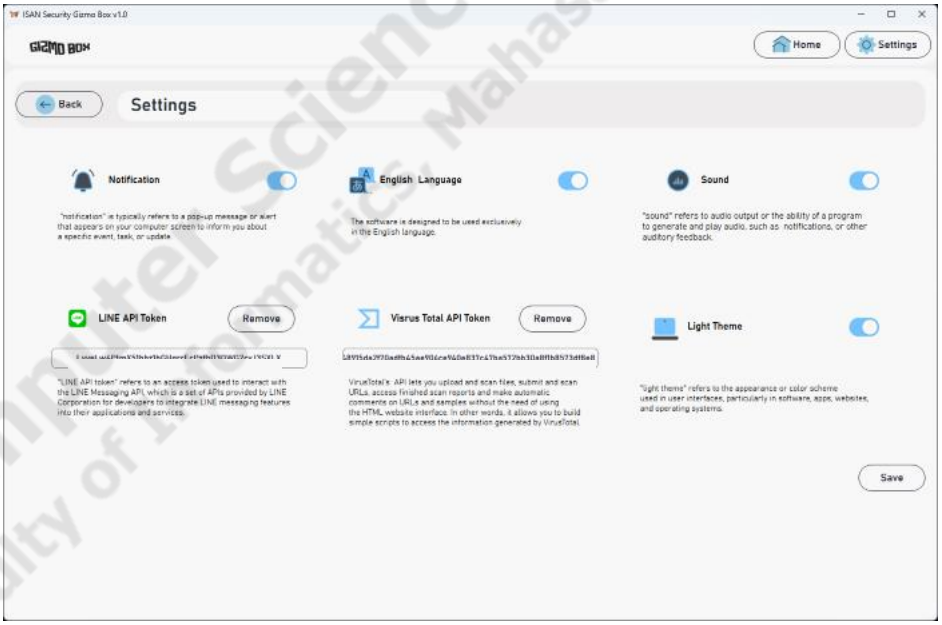
ภาพประกอบที่ 1.12 หน้าเครื่องมือ HTTPS Testing

ภาพประกอบที่ 1.13 หน้าแสดงรายงานและส่งอีเมลของเครื่องมือ Malware Scanning



ภาพประกอบที่ 1.14 หน้าแสดงรายงานและส่งอีเมลของเครื่องมือ Vulnerability Scanning

ภาพประกอบที่ 1.15 หน้าแสดงรายงานและส่งอีเมลของเครื่องมือ HTTPS Testing



ภาพประกอบที่ 1.16 หน้าตั้งค่าเครื่องมือ ISAN Security Gizmo Box

1.6 ประโยชน์ที่คาดว่าจะได้รับ

ISAN Security Gizmo Box จะช่วยอำนวยความสะดวกแก่ผู้ใช้งานทั่วไปให้สามารถใช้งานเครื่องมือด้านความมั่นคงปลอดภัย และช่วยประหยัดเวลาเนื่องจาก ISAN Security Gizmo Box อยู่ในรูปแบบของ Graphical User Interface (GUI) และมีเครื่องมือหลากหลาย Modules ให้เลือกใช้งาน

1.7 อุปกรณ์ที่ใช้ดำเนินการ

1.7.1 Hardware

1) เครื่องคอมพิวเตอร์ที่ 1 มีคุณสมบัติ ดังนี้

- ระบบปฏิบัติการ Windows 11 Home 64 bit
- หน่วยประมวลผล AMD Ryzen 5 3550H CPU 2.10 GHz
- หน่วยความจำเครื่อง Ram 24 GB

2) เครื่องคอมพิวเตอร์ที่ 2 มีคุณสมบัติ ดังนี้

- ระบบปฏิบัติการ Windows 11 Home 64 bit
- หน่วยประมวลผล AMD Ryzen 7 4700U CPU 2.00 GHz
- หน่วยความจำเครื่อง Ram 8 GB

1.7.2 Software

1) Visual Studio Code ใช้เขียนโปรแกรม
2) Qt Designer ใช้สร้าง Graphical User Interface (GUI)
3) Kali Linux ใช้เป็นฐานเครื่องมือความมั่นคลปลอดภัย
4) Virtual Appliance ของ 2 Virtual Machines ดังนี้

- Oracle VM VirtualBox
- VMware Workstation Player

5) เครื่องมือที่ใช้เพิ่มเติม

- Nmap
- Testssl.sh
- Vulners.NSE
- Hashcat

1.8 แผนการดำเนินการ

โครงงานปริญญานิพนธ์ฉบับนี้ ดำเนินงาน ณ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม ระหว่างเดือน ตุลาคม 2565 ถึง กันยายน 2566

ตารางที่ 1.1 แผนการดำเนินงาน

กิจกรรม	เดือน											
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
1. ศึกษาและรวบรวมข้อมูล												
2. วิเคราะห์และกำหนดขอบเขต												
3. ออกแบบระบบ												
4. พัฒนาโปรแกรม												
5. ทดสอบระบบ												
6. ทำรายงานสรุป												
7. นำเสนอโครงงาน												