

กล่องเครื่องมือความมั่นคงไอสานกิซโม่

ISAN Security Gizmo Box

โครงงานปริญญานิพนธ์

ของ

**กาญจนา พินิจ**

**พีรธัช บุตรโท**

เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

ปีการศึกษา

ลิขสิทธิ์เป็นของมหาวิทยาลัยมหาสารคาม

คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

กล่องเครื่องมือความมั่นคงไอสานกิซโม่

ISAN Security Gizmo Box

โครงงานปริญญานิพนธ์

ของ

**กาญจนา พินิจ**

**พีรธัช บุตรโท**

Text, letter

Description automatically generated

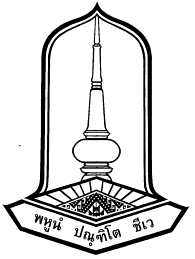
เสนอต่อมหาวิทยาลัยมหาสารคาม เพื่อเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์

ปีการศึกษา

ลิขสิทธิ์เป็นของมหาวิทยาลัยมหาสารคาม

คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม



คณะกรรมการสอบโครงงานปริญญานิพนธ์ ได้พิจารณาปริญญานิพนธ์ของ นางสาวกาญจนา พินิจ และนายพีรธัช บุตรโท แล้วเห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ ของมหาวิทยาลัยมหาสารคาม

คณะกรรมการสอบโครงงานปริญญานิพนธ์

|  |  |
| --- | --- |
| ………………………………………..……  (..................................................) | ประธานสอบ |
| ………………………………………..……  (...................................................) | กรรมการ |
| ………………………………………..……  (ผู้ช่วยศาสตราจารย์ ดร.สมนึก พ่วงพรพิทักษ์) | ที่ปรึกษาโครงงานปริญญานิพนธ์หลัก |

หลักสูตรวิทยาการคอมพิวเตอร์อนุมัติให้รับโครงงานปริญญานิพนธ์ฉบับนี้ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

|  |  |
| --- | --- |
| …………………………….……………….…………  (อาจารย์พชระ พฤกษะศรี) | …………………………….……………….…………  (ผู้ช่วยศาสตราจารย์พิมลรัตน์ อ้วนศรีเมือง) |
| อาจารย์ผู้ประสานงานวิชาโครงงานปริญญานิพนธ์  วันที่ เดือน พ.ศ. | |

บทคัดย่อ

ชื่อโครงงาน กล่องเครื่องมือความมั่นคงไอสานกิซโม่

ผู้จัดทำ 63011212069 นางสาวกาญจนา พินิจ

63011212098 นายพีรธัช บุตรโท

อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.สมนึก พ่วงพรพิทักษ์

หลักสูตร วิทยาศาสตรบัณฑิต (สาขาวิชาวิทยาการคอมพิวเตอร์)

คณะ วิทยาการสารสนเทศ

มหาวิทยาลัย มหาวิทยาลัยมหาสารคาม

ปีที่พิมพ์

ISAN Security Gizmo Box รวบรวมการตรวจสอบความมั่นคงปลอดภัยเบื้องต้นประกอบไปด้วย Password Evaluation, Malware Scanning, Vulnerability Scanning, HTTPS Testing และ Message Digest Generator ไว้ในเครื่องมือเดียวกันและอยู่ในรูปแบบ ของ Graphical User Interface (GUI) อีกทั้งยังอยู่ในรูปแบบ Virtual Machine (VM) Image ของ Hypervisor 2 ชนิด คือ Oracle VM VirtualBox และ VMware Workstation Player

**คำสำคัญ:** Virtual Machine, Entropy, Brute-force attack, Vulnerability, Security, HTTPS, GUI, Malware, Digest

กิตติกรรมประกาศ

โครงงานปริญญานิพนธ์ฉบับนี้สำเร็จสมบูรณ์ได้ด้วยความกรุณาและความช่วยเหลืออย่างสูงยิ่งจาก ผู้ช่วยศาสตราจารย์ ดร.สมนึก พ่วงพรพิทักษ์ อาจารย์ที่ปรึกษาโครงงานปริญญานิพนธ์ และ กรรมการควบคุมโครงงานปริญญานิพนธ์ ประธานกรรมการสอบ และ กรรมการสอบ

ขอขอบพระคุณ (ขอบคุณผู้เชี่ยวชาญที่ช่วยตรวจ หรือช่วยให้คำแนะนำ ถ้ามี)

ขอขอบพระคุณ (ขอบคุณผู้ให้การช่วยเหลือสนับสนุนอื่นๆ ถ้ามี)

กาญจนา พินิจ

พีรธัช บุตรโท

สารบัญ

**หน้า**

บทคัดย่อภาษาไทย…………………………………………………………………………………………………………...........ก

กิตติกรรมประกาศ……………………………………………………………………………………………………………………ข

สารบัญตาราง…………………………………………………………………………………………………………....................ง

สารบัญภาพ………………………………………………………………………………………………………..……............. …..ฉ

[บทที่ 1 บทนำ 1](#_Toc130505811)

[1.1 หลักการและเหตุผล 1](#_Toc130505812)

[1.2 วัตถุประสงค์ของโครงงาน 1](#_Toc130505813)

[1.3 ขอบเขตของโครงงาน 2](#_Toc130505814)

[1.4 ภาพรวมของระบบ 6](#_Toc130505815)

[1.5 ตัวอย่างเครื่องมือ 8](#_Toc130505816)

[1.6 ประโยชน์ที่คาดว่าจะได้รับ 11](#_Toc130505817)

[1.7 อุปกรณ์และเครื่องมือที่ใช้ในการดำเนินงาน 11](#_Toc130505818)

[1.8 แผนการดำเนินงาน 12](#_Toc130505819)

[บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 11](#_Toc130505820)

[2.1 งานวิจัยและทฤษฎีที่เกี่ยวข้อง 11](#_Toc130505821)

[2.2 Software ที่เกี่ยวข้อง 17](#_Toc130505822)

[บทที่ 3 ขั้นตอนการดำเนินงาน 22](#_Toc130505823)

[3.1 กรอบการดำเนินงาน 22](#_Toc130505824)

[3.2 การพัฒนาระบบด้วย Qt Designer 23](#_Toc130505825)

[3.3 Password Evaluation 24](#_Toc130505826)

[3.4 Message Digest 29](#_Toc130505827)

[3.5 Malware Scanning 30](#_Toc130505828)

[3.6 Vulnerability Scanning 33](#_Toc130505829)

[3.7 HTTPS Testing 36](#_Toc130505830)

เอกสารอ้างอิง……………………………………………………………………….………………………………....................40

สารบัญตาราง

**หน้า**

[ตารางที่ 1.1 แผนการดำเนินงาน 12](#_Toc130504617)

[ตารางที่ 2.1 ตารางเปรียบเทียบการทำงานของระบบงานที่เกี่ยวข้อง…………………………………………….21](#_Toc122655653)

สารบัญภาพประกอบ

**หน้า**

[ภาพประกอบที่ 1.1 ภาพรวมระบบทั้งหมด 6](#_Toc130505205)

[ภาพประกอบที่ 1.2 โครงสร้างสถาปัยตกรรมภายในของระบบ 7](#_Toc130505206)

[ภาพประกอบที่ 1.3 ตัวอย่างหน้าแรกของเครื่องมือ ISAN Security Gizmo Box 8](#_Toc130505207)

[ภาพประกอบที่ 1.4 ตัวอย่างหน้าเครื่องมือ Password Evaluation 8](#_Toc130505208)

[ภาพประกอบที่ 1.5 ตัวอย่างหน้าเครื่องมือ Malware Scanning 9](#_Toc130505209)

[ภาพประกอบที่ 1.6 ตัวอย่างหน้าเครื่องมือ Vulnerability Scanning 9](#_Toc130505210)

[ภาพประกอบที่ 1.7 ตัวอย่างหน้าเครื่องมือ HTTPS Testing 10](#_Toc130505211)

[ภาพประกอบที่ 1.8 ตัวอย่างหน้าเครื่องมือ Message Digest Generator 10](#_Toc130505212)

ภาพประกอบที่ 2.1 Pool of Characters………………………………………………………………………………….11

ภาพประกอบที่ 2.2 ตัวอย่างการคำนวณ Bit of Entropy 12

ภาพประกอบที่ 2.3 ตัวอย่าง Input/Output Combinator attack 12

ภาพประกอบที่ 2.4 ตัวอย่างโปรแกรม Kali Linux 18

ภาพประกอบที่ 2.5 ตัวอย่างโปรแกรม PenTBox 19

ภาพประกอบที่ 2.6 ตัวอย่างเว็บไซต์ Pentestbox……………………………………………………………………. 20

[ภาพประกอบที่ 3.1 ภาพรวมของโครงงานปริญญานิพนธ์ 22](#_Toc130505730)

[ภาพประกอบที่ 3.2 การพัฒนา Interface ด้วย Qt Designer 23](#_Toc130505731)

[ภาพประกอบที่ 3.3 Code การเรียกใช้ Qt Designer 24](#_Toc130505732)

[ภาพประกอบที่ 3.4 เครื่องมือประเมินรหัสผ่าน (Password Evaluation) 24](#_Toc130505733)

[ภาพประกอบที่ 3.5 เงื่อนไขการแสดงข้อมูลเชิงคุณภาพ 25](#_Toc130505734)

[ภาพประกอบที่ 3.6 เทคนิคการทำ Combinator attack ด้วย python และ Hashcat 26](#_Toc130505735)

[ภาพประกอบที่ 3.7 เทคนิคการทำ Hybrid attack ด้วย Python และ Hashcat 26](#_Toc130505736)

[ภาพประกอบที่ 3.8 ตัวอย่างการทดสอบ Straight forward attack บน kali 27](#_Toc130505737)

[ภาพประกอบที่ 3.9 ตัวอย่างการทดสอบ Combinator attack บน kali Linux 27](#_Toc130505738)

[ภาพประกอบที่ 3.10 ตัวอย่างการทดสอบ Hybrid attack บน kali Linux 28](#_Toc130505739)

[ภาพประกอบที่ 3.11 เครื่องมือคำนวณค่า (Message Digest) 29](#_Toc130505740)

[ภาพประกอบที่ 3.12 เครื่องมือตรวจสอบ Malware (Malware Scanning) 30](#_Toc130505741)

[ภาพประกอบที่ 3.13 แสดงการไหลของข้อมูลเมื่อเรียกใช้ VirusTotal API-URL Scan 31](#_Toc130505742)

[ภาพประกอบที่ 3.14 ทดลองการเรียกใช้ VirusTotal API-URL Scan 31](#_Toc130505743)

[ภาพประกอบที่ 3.15 แสดงการไหลของข้อมูลเมื่อเรียกใช้ VirusTotal API-File Scan 32](#_Toc130505744)

[ภาพประกอบที่ 3.16 ทดลองการเรียกใช้ VirusTotal API-File Scan 32](#_Toc130505745)

[ภาพประกอบที่ 3.17 เครื่องมือตรวจสอบหาช่องโหว่ (Vulnerability Scanning) 33](#_Toc130505746)

[ภาพประกอบที่ 3.18 TCP Port Scanning 34](#_Toc130505747)

[ภาพประกอบที่ 3.19 Syn Scanning 34](#_Toc130505748)

[ภาพประกอบที่ 3.20 ทดสอบ Vulner.NSE กับ https://reg.msu.ac.th 35](#_Toc130505749)

[ภาพประกอบที่ 3.21 ทดสอบ Vulner.NSE กับ https://isanmsu.com 36](#_Toc130505750)

[ภาพประกอบที่ 3.22 เครื่องมือตรวจสอบความปลอดภัย HTTPS 36](#_Toc130505751)

[ภาพประกอบที่ 3.23 การตรวจสอบ URL 37](#_Toc130505752)

[ภาพประกอบที่ 3.24 การตรวจสอบ HSTS Preload 37](#_Toc130505753)

[ภาพประกอบที่ 3.25 การทดสอบ vulnerabilities ด้วย tests.sh กับ https://reg.msu.ac.th 38](#_Toc130505754)

[ภาพประกอบที่ 3.26 การทดสอบ vulnerabilities ด้วย tests.sh กับ https://isanmsu.com 38](#_Toc130505755)

[ภาพประกอบที่ 3.27 การทดสอบ vulnerabilities ด้วย tests.sh กับ https://it.msu.ac.th 38](#_Toc130505756)

# บทนำ

## หลักการและเหตุผล

ปัจจุบันการทำงานบนเครือข่ายคอมพิวเตอร์มีอัตราเพิ่มสูงขึ้นอย่างต่อเนื่องเช่นเดียวกับภัยคุกคามทางไซเบอร์  (Cyber Threat) เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) เป็นต้น การโจมตีแต่ละครั้งล้วนสร้างความเสียหายอย่างมหาศาล ทั้งต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ การใช้งาน บนเครือข่ายคอมพิวเตอร์ล้วนมีช่องโหว่และความเสี่ยงต่างๆ ส่งผลให้ภัยคุกคามทางไซเบอร์ สามารถเกิดขึ้นได้ตลอดเวลา

แม้ว่าจะมีเครื่องมือทางด้าน Security อยู่หลายตัวแต่เครื่องมือเหล่านั้นก็มักจะมีปัญหาในการติดตั้ง และเครื่องมือส่วนใหญ่อยู่ในรูปแบบ Command line ทำให้ผู้ใช้งานต้องมีความรู้เกี่ยวกับคำสั่งต่างๆซึ่งยากต่อการใช้งานสำหรับผู้ใช้คอมพิวเตอร์ทั่วไปหรือผู้ใช้มือใหม่การจะใช้เครื่องมือแต่ละประเภทจะต้องใช้เวลาในการศึกษาคำสั่งและการอ่านผลลัพธ์ที่ซับซ้อนทำให้ผู้ใช้งานต้องศึกษาอย่างละเอียดเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

โครงการปริญญานิพนธ์นี้จึงเสนอเครื่องมือที่รวบรวมการตรวจสอบความมั่นคงปลอดภัยเบื้องต้นประกอบไปด้วย Password Evaluation, Malware Scanning, Vulnerability Scanning, HTTPS Testing  และ Message Digest Generator  ไว้ในเครื่องมือเดียวและอยู่ในรูปแบบ ของ Graphical User Interface (GUI) เป็นรูปแบบที่นิยมในปัจจุบันและเหมาะกับผู้ใช้งานทั่วๆไปและจะแสดงผลลัพธ์การทดสอบที่มีความเหมาะสมเข้าใจง่าย และมีรายงานผลลัพธ์ที่ได้ผ่านทาง E-mail ปลายทางที่ต้องการ อีกทั้งยังอยู่ในรูปแบบ Virtual Machine (VM) Image ของ Hypervisor 2 ชนิด คือ Oracle VM VirtualBox และ VMware Workstation Player

## วัตถุประสงค์ของโครงงาน

พัฒนาเครื่องมือ ISAN Security Gizmo Box ที่ประกอบไปด้วยเครื่องมือทางด้าน Cyber Security ซึ่งจะอำนวยความสะดวกแก่ผู้ใช้งานทั่วไปเนื่องจากเป็นรูปแบบของ Graphical User Interface (GUI) โดย ISAN Security Gizmo Box จะแยกเป็น Modules ย่อย ๆ ประกอบไปด้วย Password Evaluation, Malware Scanning, Vulnerability Scanning, HTTPS Testing  และ Message Digest Generator

## ขอบเขตของโครงงาน

### ISAN Security Gizmo Box อยู่ในรูปแบบ Virtual Machine (VM) Image ที่สามารถรันบน Hypervisor 2 ชนิด คือ Oracle VM VirtualBox และ VMware Workstation Player

1. ISAN Security Gizmo Box แบ่งกลุ่มเครื่องมือเป็น Advance User Group ประกอบไปด้วย Password Evaluation, Malware Scanning Message Digest และ Network Engineer Group ประกอบไปด้วย Vulnerability Scanning, HTTPS Testing โดยแต่ละเครื่องมือมีรายละเอียด ดังนี้

### เครื่องมือประเมินรหัสผ่าน (Password Evaluation) มีคุณสมบัติ ดังนี้

#### วัดค่าความต้านทานในการถูกโจมตีด้วยเทคนิค Brute-force attack ได้ดีหรือไม่ โดยการคำนวณออกมาเป็นข้อมูลเชิงปริมาณและข้อมูลเชิงคุณภาพ

#### 1.1) ข้อมูลเชิงปริมาณคือ Bit of Entropy ซึ่งถูกคิดค้นโดย Claude E.

#### Shannon [[2]](#Entropy)

#### 1.2) ข้อมูลเชิงคุณภาพประเมินจาก Bit of Entropy ออกมาในรูปแบบระบุ

#### คุณลักษณะว่าดีหรือไม่

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

#### 3) ใช้เทคนิค Dictionary attack [[3]](#Dictionary) เพื่อตรวจสอบว่ารหัสผ่านถูกค้นพบหรือถูกบันทึกไว้ใน Wordlist ของ Hacker หรือไม่โดยใช้ Dictionary จากหลายแหล่ง ได้แก่ CrackStation [[12]](#CrackStation), Rockyou.txt โดยแบ่งรูปแบบการดำเนินการเป็น 2 รูปแบบ

#### 3.1) Straightforward Dictionary attack เป็นการค้นหาจาก Dictionary

#### โดยตรงพร้อมแจ้งเตือนผู้ใช้ว่าพบรหัสใน Dictionary ใด

#### 3.2) Skipping attack เป็นการค้นหาจากการรวม Dictionary เข้าด้วยกัน

#### โดยแบ่งออกเป็น 2 รูปแบบได้แก่ Combinator attack และ Hybrid

#### attack ซึ่งใช้ Hashcat เข้ามาช่วยในการทดสอบ เพื่อขยายขอบเขต

#### ของ Dictionary ให้กว้างมากขึ้น และเพิ่มโอกาสในการค้นหามากขึ้น

### เครื่องมือตรวจสอบ Malware (Malware Scanning) มีคุณสมบัติ ดังนี้

* 1. ตรวจสอบ Malware จากไฟล์ที่ผู้ใช้เพิ่มเข้ามาเพื่อตรวจสอบ
  2. ตรวจสอบ Malware จาก URL ที่สงสัยจากผู้ใช้เพิ่มเข้ามาเพื่อตรวจสอบ
  3. สามารถเรียกใช้งานบริการ Antivirus จากหลายบริษัทมาช่วยสแกน เช่น Avira, Bitdefender, Kaspersky เป็นต้น ด้วย VirusTotal API
  4. แสดงผลการทดสอบในรูปแบบของรายงาน โดยรายละเอียดของรายงานประกอบด้วย ชื่อไฟล์หรือURL วันและเวลา ชื่อบริษัทที่ใช้ในการสแกน ผลลัพธ์ที่ได้จากการสแกนจะแบ่งออกเป็น 3 รูปแบบ ดังนี้

4.1) Not Found คือ ไม่พบ Malware

4.2) Suspicious คือ สงสัยว่าอาจจะมี Malware

4.3) Malware คือ พบว่ามี Malware โดยระบุชื่อบริษัทที่ตรวจพบและชนิด

ของ Malware เช่น Ransomware, Trojan

### เครื่องมือตรวจสอบหาช่องโหว่ (Vulnerability Scanning) และตรวจสอบ Port และ Service ที่เปิดของเครื่องปลายทาง มีคุณสมบัติ ดังนี้

### ใช้คำสั่ง Nmap เพื่อตรวจสอบ Port และ Service ที่เปิดอยู่ของเครื่องปลายทางโดยใช้ฐานข้อมูลจาก Well-Know Port แบ่งเป็น 3 ประเภท ดังนี้

* 1. Stealth Scan ในกรณีที่ต้องการข้อมูลที่อาจถูก Block จาก Firewall โดยใช้ Option TCP SYN scan หรือ -sS และ TCP FIN Scan หรือ -sF
  2. Aggressive Scan ในกรณีที่ต้องการข้อมูล Operating System และ Version ของเครื่องปลายทาง โดยใช้ Option OS Detection หรือ -O และ Version Detection หรือ -sV
  3. Adaptive Scan เพื่อปรับ Option เพื่อการสแกนที่เหมาะกับสถานการณ์ เช่น การใช้ SYN Scan ร่วมกับ -O เพื่อสแกนหา Operating System และหลีกเลี่ยงการถูก Block จาก Firewall หรือการเพิ่ม option -T4 เข้ามาเพื่อลดระยะเวลาในการสแกน

### ใช้ Vulners.NSE โดยใช้ Option --script vulners ร่วมกับ Nmap อ้างอิงฐานข้อมูลของช่องโหว่จาก OpenVAS เพื่อตรวจสอบหาช่องโหว่ของเครื่องปลายทาง

### แสดงผลการทดสอบในรูปแบบของรายงาน โดยรายละเอียดของรายงานประกอบด้วย เครื่องมือที่ใช้ วันและเวลา เครื่องปลายทาง Port สถานะ Service Version Operating System และ CVE โดยแบ่งการแสดงผลเป็น 2 รูปแบบคือ

### 3.1) เพื่อแสดงผลลัพธ์บนหน้าจอ GUI ให้ผู้ใช้สามารถดูรายละเอียดของผลลัพธ์ที่ได้จาการสแกน

3.2) เพื่อบันทึกผลลัพธ์หรือแชร์ให้กับผู้อื่น ด้วยการส่งรายงานจากการสแกน โดยการระบุ Email Address ปลายทางที่ต้องการส่งไปซึ่งจะอยู่ในรูปแบบของ PDF File

### 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 Configuration และ HSTS Preload

### 4) แสดงผลการทดสอบในรูปแบบของรายงานโดยรายละเอียดของรายงานประกอบด้วย ข้อมูลเกี่ยวกับ Domain Name, Certificate, Certificate Authority ที่ออก Digital Certificate ให้กับเว็บไซต์ ข้อมูลเกี่ยวกับอัลกอริทึมที่ใช้เข้ารหัส, Digital Signature และ Hashing functions ที่ใช้ พร้อมบอกจำนวนบิตที่ใช้ และแจ้งเตือนผู้ใช้งานหากพบว่าไม่เหมาะสม ข้อมูลเกี่ยวกับจุดอ่อน หรือโอกาสที่จะถูก Downgrade Attack เช่น POODLE, DROWN, ORACLE Attacks ว่าเป็นไปได้หรือไม่ และ ข้อมูลเกี่ยวกับการ HSTS Configuration และ HSTS Preload ว่าเหมาะสมหรือไม่

### 5) ผลลัพธ์ที่ได้จากการทดสอบสามารถแสดงผลลัพธ์ได้ 2 รูปแบบ ได้แก่

### 5.1) แสดงผลลัพธ์บนหน้าจอ GUI ให้ผู้ใช้สามารถดูรายละเอียดของผลลัพธ์จากการทดสอบด้วย testssl.sh โดยมีรายละเอียดดังข้อ 4)

5.2) สามารถบันทึกผลลัพธ์หรือแชร์ให้กับผู้ใช้อื่น ด้วยการส่งรายงานจากการสแกนด้วย Open Source Testssl.sh โดยการระบุ Email Address ปลายทางที่ต้องการส่งไป จะอยู่ในรูปแบบของ PDF File

### เครื่องมือคำนวณค่า Message Digest (Message Digest Generator) มีคุณสมบัติ ดังนี้

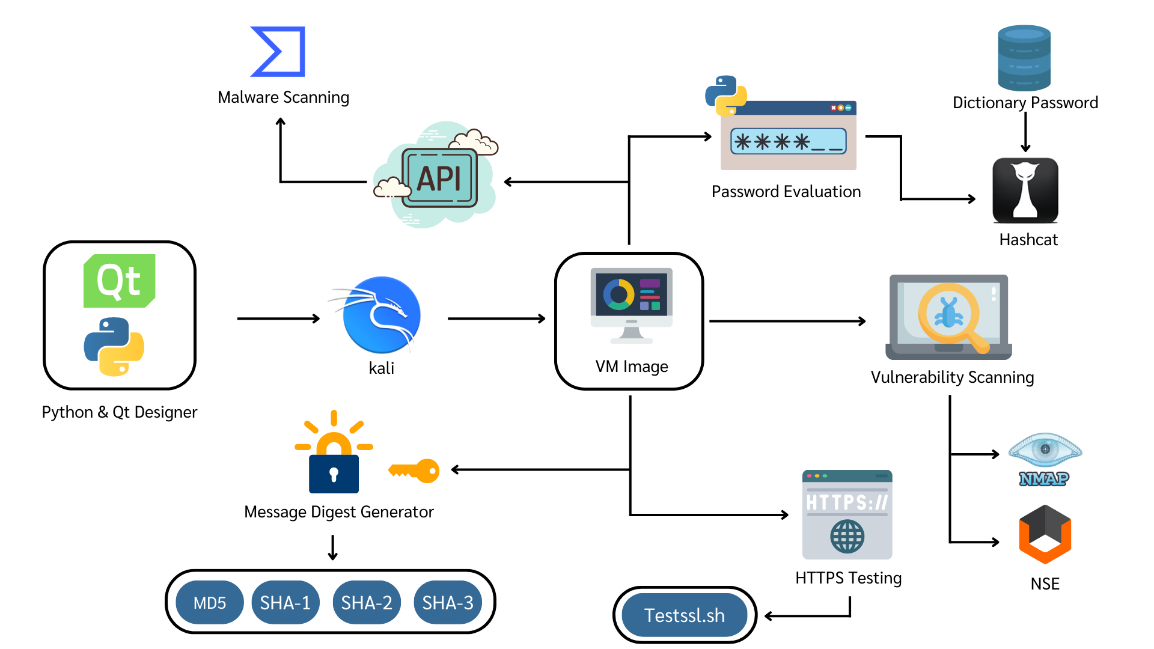
### Algorithms การคำนวณ Message Digest ที่รองรับได้แก่ MD5, SHA-1, SHA-2, SHA3

### การคำนวณ Message Digest โดยสามารถ Input ข้อมูลได้ 2 แบบคือ ข้อความ

### และ File เพื่อนำไปคำนวณหาค่า Message Digest

### การแสดงผลลัพธ์จากการคำนวณ Message digesting โดยแสดงได้ 2 รูปแบบ คือ แสดง Message Digest ที่คำนวณได้ในรูปแบบข้อความ และ นำ Message Digest ที่ได้จากข้อความโดยแปลงให้อยู่ในรูปของ QR Code เพื่อให้ง่ายต่อการนำไปใช้

## ภาพรวมของระบบ



ภาพประกอบที่ 1.1 ภาพรวมระบบทั้งหมด

1) ภาพรวมทั้งหมดของระบบ ISAN Security Gizmo Box จะแยกเป็น Modules ย่อย ๆ ประกอบไปด้วย Password Evaluation, Malware Scanning, Vulnerability Scanning, HTTPS Testing และ Message Digest Generator โดยเครื่องมือที่ได้อยู่ในรูปแบบ Virtual Machine (VM) Image ที่สามารถรันบน Hypervisor 2 แบบใหญ่ๆ คือ Oracle VM VirtualBox และ VMware Workstation Player VM Image โดยทั่วไปใน Kali Linux มีเครื่องมือ Security ที่หลากหลายอยู่ในตัว Image นั้นพร้อมอยู่แล้วแต่เนื่องด้วยเครื่องมือแต่ละประเภทต้องเรียกใช้โดย Command line ซึ่งยากต่อการใช้งานสำหรับผู้ใช้คอมพิวเตอร์ทั่วไปหรือผู้ใช้มือใหม่การจะใช้แต่ละเครื่องมือแต่ละประเภทจะต้องใช้เวลาในการศึกษาคำสั่งและการอ่านผลลัพธ์ที่ซับซ้อนทำให้ผู้ใช้งานต้องศึกษาอย่างละเอียดเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

Graphical user interface, application

Description automatically generated

ภาพประกอบที่ 1.2 โครงสร้างสถาปัยตกรรมภายในของระบบ

2) โครงสร้างสถาปัตยกรรมภายในของระบบ ISAN Security Gizmo Box มีดังนี้ Virtual Machine (VM) Image โดยติดตั้ง Kali Linux เป็นฐานของเครื่องมือ ซึ่ง Kali Linux มีเครื่องมือ Security พื้นฐานอยู่แล้ว แต่มีการติดตั้งเครื่องมือเพิ่มเติม เช่น Vulner.NSE, Testssl เป็นต้น และมีการเขียนโปรแกรมเพิ่มเติมด้วยภาษา Python ร่วมกับ Qt Designer เพื่อให้อยู่ในรูปแบบของ Graphic User Interface (GUI) ที่เป็นมิตรต่อผู้ใช้งาน

## ตัวอย่างเครื่องมือ

เครื่องมือ ISAN Security Gizmo Box ที่จะพัฒนามีลักษณะโดยประมาณดังภาพประกอบต่อไปนี้

Text

Description automatically generated

ภาพประกอบที่ 1.3 ตัวอย่างหน้าแรกของเครื่องมือ ISAN Security Gizmo Box

Graphical user interface, text, application, chat or text message

Description automatically generated

ภาพประกอบที่ 1.4 ตัวอย่างหน้าเครื่องมือ Password Evaluation

Graphical user interface, application

Description automatically generated

ภาพประกอบที่ 1.5 ตัวอย่างหน้าเครื่องมือ Malware Scanning

A screenshot of a computer

Description automatically generated with medium confidence

ภาพประกอบที่ 1.6 ตัวอย่างหน้าเครื่องมือ Vulnerability Scanning

**Graphical user interface, text, application, chat or text message

Description automatically generated**

ภาพประกอบที่ 1.7 ตัวอย่างหน้าเครื่องมือ HTTPS Testing

Qr code

Description automatically generated

ภาพประกอบที่ 1.8 ตัวอย่างหน้าเครื่องมือ Message Digest Generator

## ประโยชน์ที่คาดว่าจะได้รับ

ISAN Security Gizmo Box จะช่วยอำนวยความสะดวกแก่ผู้ใช้งานทั่วไปให้สามารถใช้งานเครื่องมือด้าน Security โดยไม่ต้องมีความรู้ในการใช้ Command line และช่วยประหยัดเวลาในการศึกษาวิธีการใช้งานเครื่องมือประเภท เนื่องจาก ISAN Security Gizmo Box อยู่ในรูปแบบของ Graphical User Interface (GUI) และมีเครื่องมือหลากหลาย Modules ให้เลือกใช้งาน

## อุปกรณ์และเครื่องมือที่ใช้ในการดำเนินงาน

1. Hardware

1.1) เครื่องคอมพิวเตอร์ที่ 1 มีคุณสมบัติ ดังนี้

1. ระบปฏิบัติการ Windows 11 Home 64 bit

2. หน่วยประมวลผล AMD Ryzen 5 3550H CPU 2.10 GHz

3. หน่วยความจำเครื่อง Ram 24 GB

1.2) เครื่องคอมพิวเตอร์ที่ 2 มีคุณสมบัติ ดังนี้

1. ระบปฏิบัติการ Windows 11 Home 64 bit

2. หน่วยประมวลผล AMD Ryzen 7 4700U CPU 2.00 GHz

3. หน่วยความจำเครื่อง Ram 8 GB

1. Software

2.1) Visual Studio Code ใช้เขียนโปรแกรม

2.2) Qt Designer ใช้สร้าง Graphical User Interface (GUI)

2.3) Kali Linux ใช้เป็นฐานเครื่องมือ Security

2.4) Virtual Machine (VM) Image ใช้รันบน Hypervisor 2 แบบได้แก่

1. Oracle VM VirtualBox

2. VMware Workstation Player

2.5) เครื่องมือที่ใช้เพิ่มเติม

1. Nmap

2. Testssl.sh

3. Vulner.NSE

     4. Hashcat

## แผนการดำเนินงาน

โครงงานปริญญานิพนธ์ฉบับนี้ ดำเนินงาน ณ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคามระหว่างเดือน ตุลาคม 2565 ถึง กันยายน 2566

ตารางที่ 1.1 แผนการดำเนินงาน

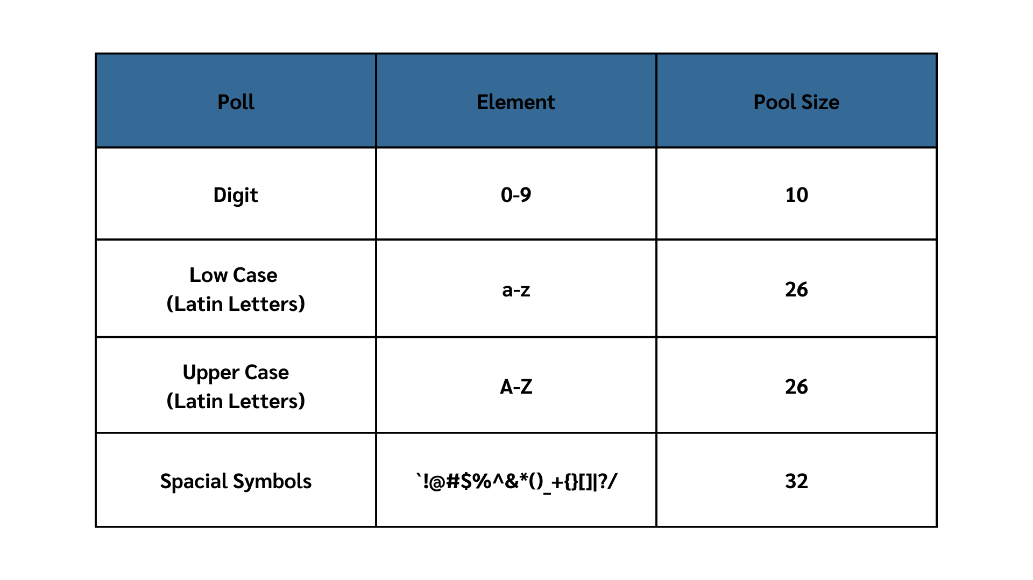
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **กิจกรรม** | **เดือน** | | | | | | | | | | | |
| **ต.ค.** | **พ.ย.** | **ธ.ค.** | **ม.ค.** | **ก.พ.** | **มี.ค.** | **เม.ย.** | **พ.ค.** | **มิ.ย.** | **ก.ค.** | **ส.ค.** | **ก.ย.**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

# ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

## งานวิจัยและทฤษฎีที่เกี่ยวข้อง

### Bit of Entropy

Bit of entropy คือ หน่วยวัดความแข็งแกร่งของรหัสผ่าน ซึ่ง Entropy [[2]](#Entropy) คำนวณได้จากสูตร E = L\*log2(P) ซึ่ง L คือ ความยาวของรหัสผ่าน (Length) และ P คือ ขนาดของกลุ่มอักษรเฉพาะ (Pool of Characters) ที่ใช้สร้างรหัสผ่าน จำนวนของค่าได้จะมีความแปรปรวนเป็นอย่างมากจนไม่สามารถคาดเดาได้และเป็นหนึ่งในมาตรการที่ใช้กันโดยทั่วไป



ภาพประกอบที่ 2.1 **Pool**of Characters

Graphical user interface, text

Description automatically generated

ภาพประกอบที่ 2.2 ตัวอย่างการคำนวณ Bit of Entropy

### Dictionary attack

Dictionary Attack [[3]](#Dictionary) คือการโจมตีความมั่นคงปลอดภัยทางไซเบอร์ประเภทหนึ่งที่เกี่ยวข้องกับการใช้รายการคำ วลี หรือสตริงอักขระอื่นๆ ที่กำหนดไว้ล่วงหน้าเป็นพื้นฐานในการพยายามเดารหัสผ่านหรือคีย์ การโจมตีทำงานโดยลองใช้แต่ละคำในรายการ ทีละคำ จนกว่าจะพบรหัสผ่านที่ถูกต้อง การโจมตีด้วย Dictionary มักใช้ร่วมกับการโจมตีประเภทอื่นๆ เช่น Brute-force attack เพื่อเพิ่มโอกาสในการประสบความสำเร็จลักษณะสำคัญอย่างหนึ่งของ Dictionary Attack คือรายการคำที่ใช้มักจะปรับให้เหมาะกับเป้าหมายเฉพาะที่ถูกโจมตี Burt-force attack

### Combinator attack

Combinator attack เป็นอีกหนึ่งในวิธีย่อยของ Skipping Attack โดย Combinator มีการสร้าง Dictionary เพิ่มโดยเป็นการผสมหรือนำรหัสผ่านมาต่อกันเป็นรหัสผ่านใหม่เพื่อเพิ่มความเป็นไปได้ที่จะโจมตีสำเร็จโดยการใช้ Dictionary attack ในรูปแบบ Combination Wordlist

Graphical user interface, text, application, email

Description automatically generatedภาพประกอบที่ 2.3 ตัวอย่าง Input/Output Combinator attack

### Hybrid attack

Hybrid attack เป็นการโจมตีแบบ Combinator ซึ่งเป็นการใช้เทคนิค Dictionary attack ผสมกับการโจมตีแบบ Brute-force attack เช่น นําหน้าด้วยคําแต่ละคําจาก Dictionary หรือต่อท้ายคำแต่ละคำ และยังมาการแทนทีอักษร ที่เรียกเทคนิคนี้ว่า Mask เพื่อกำหนดจุดที่จะ Brute-force

Graphical user interface, text, application, email

Description automatically generated

ภาพประกอบที่ 2.4 ตัวอย่าง Create Dictionary เพื่อโจมตีด้วย Hybrid Attack

### Malware

Malicious [[6]](#Malware) Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์หรือทำให้สูญเสีย CIA เป็น ส่วนประกอบหนึ่งของ INFOSEC [[4]](#INFOSEC) (Information Security) ซึ่งมาจากคำว่า Confidentiality (การรักษาความลับของข้อมูล) Integrity (ความแท้จริงของข้อมูล) และ Availability (การใช้งานได้ของระบบ) ซึ่งเป็นส่งที่ Security Professional ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท ตัวอย่างเช่น

­ Virus: มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว

­ Worm: สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

­ Trojan: หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง

­ Backdoor: เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์โดยไม่รู้ตัว

­ Rootkit: เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

­ Spyware: แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น

­ Ransomware: ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้

จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

### VirusTotal

VirusTotal [[14]](#VirusTotal) เป็น free online service ที่วิเคราะห์ไฟล์หรือ URL เพื่อหามัลแวร์และภัยคุกคามอื่นๆ ดำเนินการโดย Google และใช้งานโดยผู้คน ธุรกิจ และองค์กร ใช้เพื่อสแกนไฟล์และ URL เพื่อหาไวรัส เวิร์ม โทรจัน และมัลแวร์ประเภทอื่นๆ VirusTotal ยังมี API (Application Programming Interface) ที่ช่วยให้นักพัฒนาสามารถรวมความสามารถในการสแกนของ VirusTotal เข้ากับแอปพลิเคชันหรือบริการของตนเองได้ เมื่อใช้ API นักพัฒนาสามารถส่งไฟล์หรือ URL เพื่อสแกนและรับผลลัพธ์ทางโปรแกรม สิ่งนี้มีประโยชน์สำหรับงานตรวจจับและวิเคราะห์มัลแวร์โดยอัตโนมัติ หรือสำหรับการรวมความสามารถของ VirusTotal เข้ากับระบบรักษาความปลอดภัยที่ใหญ่ขึ้น

### Vulnerability

Vulnerability คือ จุดอ่อนหรือช่องโหว่ หมายถึง สภาพแวดหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์ และหากถูกใช้ให้เป็นประโยชน์โดยภัยคุกคามก็อาจทำให้ทรัพย์สินหรือข้อมูลต่างๆขององค์กรได้รับความเสียหาย นับได้ว่าความเสี่ยงของช่องโหว่ (Vulnerability) ในระบบคอมพิวเตอร์ทั้งซอฟแวร์ หรือฮาร์ดแวร์ เป็นสิ่งที่มีผลกระทบความสำคัญต่อความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร หรือบริษัท การค้นพบช่องโหว่ใหม่ มักขะนำไปสู่การสร้างโปรแกรมเจาะระบบ (Exploit Code), ไวรัส หรือมัลแวร์จากผู้บุกรุก หากผู้ดูแลระบบสามารถรับมราบข่าวสารของช่องโหว่ และติดตั้งโปรแกรมซ่อมแซมของช่องโหว่ไม่ทัน จะได้รับผลกระทบจากความเสี่ยงเหล่านี้แน่นอน โดยทั่วไปข่าวสารเกี่ยวกับช่องโหว่ มักจะได้มาจาก เจ้าของผลิตภัณฑ์ หรือ เว็บไซต์ทางด้านความมั่นคงปลอดภัย

### Open Vulnerability Assessment System (OpenVAS)

Open Vulnerability Assessment System [[9]](#OpenVAS) (OpenVAS) เป็นแพลตฟอร์มสำหรับสแกนช่องโหว่บนระบบเครือข่ายฟรี โดยองค์ประกอบหลักเป็นแพ็คเกจ Linux หรือสามารถดาวน์โหลดมาใช้งานได้ในรูปแบบ Virtual Appliance สำหรับทดสอบและประเมินผลระบบ OpenVAS มีการอัพเดทฐานข้อมูลการค้นหาช่องโหว่ทุกวันจาก Network Vulnerability Tests (NVT) ซึ่งปัจจุบันมีฐานข้อมูลช่องโหว่มากกว่า 33,000 รูปแบบ

### Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures [[10]](#CVE) (CVE) เป็นโครงการรักษาความปลอดภัย ที่มีเป้าหมายสำคัญในการดูแลซอฟต์แวร์ที่เผยแพร่แบบสาธารณะโดยโครงการนี้ได้รับเงินทุนสนับสนุนจากกระทรวงความมั่นคงแห่งมาตุภูมิของรัฐบาลกลางแห่งประเทศสหรัฐอเมริกา และกำกับดูแลโดยองค์กรไม่แสวงหาผลกำไร MITRE Corporation CVE เป็นเสมือนอภิธานศัพท์ของช่องโหว่ต่าง ๆ ใช้ระบบ Security Content Automation Protocol

### Hypertext Transfer Protocol (HTTP)

Hypertext Transfer Protocol (HTTP) คือ โพรโทคอลสื่อสารสำหรับการแลกเปลี่ยนสารสนเทศผ่านอินเทอร์เน็ต 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

### Secure Socket Layer (SSL)

Secure Socket Layer (SSL) คือโพรโทคอลทางด้านความปลอดภัย และได้มีการกำหนดเป็นมาตราฐานความปลอดภัยที่มีความน่าเชื่อถือที่สุด โดยบริษัท Netscape เป็นผู้ที่คิดค้นขึ้นมาและส่งต่อไปให้กับ IETF (Internet Engineering Task Force) เป็นกลุ่มนานาชาติของผู้ที่มีส่วนร่วม ในการพัฒนาโครงสร้างของอินเทอร์เน็ต ให้มีการพัฒนา SSL ต่อเพื่อให้มีมาตราฐานและเป็นที่ยอมรับมากยิ่งขึ้น

### Transport Layer Security (TLS)

Transport Layer Security (TLS) ถูกพัฒนามาจาก SSL โพรโทคอล และการทำงานของโพรโทคอลจะทำการเข้ารหัสให้กับข้อมูลก่อนที่จะส่งไปยังผู้รับข้อมูลปลายทาง เพื่อเพิ่มความปลอดภัยให้กับข้อมูลในขณะที่กำลังส่งข้อมูลเหล่านั้นจากเครื่องแม่ข่ายไปยังเครื่องลูกข่าย

### Message Digest algorithm 5 (MD5)

Message Digest algorithm 5 [[11]](#MD5) (MD5) คือ รูปแบบการเข้ารหัสแบบ Hash ชนิดหนึ่งการเข้ารหัสแบบ Hash  (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)

Secure Hash Algorithm (SHA) [[15]](#SHA) 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]](#SHA2) และ SHA-3 [[17]](#SHA3) เวอร์ชันที่ใช้กันอย่างแพร่หลายคือ SHA-2 ซึ่งประกอบด้วยฟังก์ชันแฮชที่แตกต่างกันหลายฟังก์ชัน โดยมีขนาดบล็อกและขนาดเอาต์พุตที่แตกต่างกัน ฟังก์ชัน SHA-2 ที่พบบ่อยที่สุดคือ SHA-256 (ซึ่งสร้างเอาต์พุต 256 บิต) และ SHA-512 (ซึ่งสร้างเอาต์พุต 512 บิต)

### Vulners.NSE

Vulners.NSE [[13]](#NSE) ทำให้ความสามารถในการทำงานของ Nmap นั้นถูกขยายขอบเขตออกไปขึ้นอยู่กับฟังก์ชันการทำงานของสคริปต์ที่ถูกเรียกใช้ ในปัจจุบันสามารถทำให้ Nmap สแกนหาช่องโหว่ตาม CVE ตามจำนวนของช่องโหว่ที่ Vulners มีอยู่ในฐานข้อมูลกว่า 1,000,000 ช่องโหว่

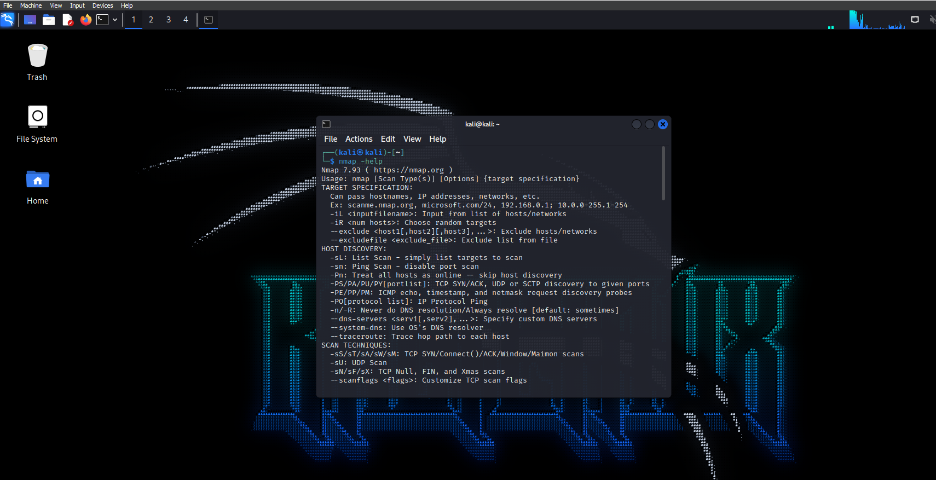
## Software ที่เกี่ยวข้อง

### Virtual Machine (VM)

Virtual Machine [[8]](#VM) (VM) เป็นซอฟต์แวร์ที่ใช้ทรัพยากรของเครื่องคอมพิวเตอร์ไม่ว่าจะเป็น RAM, Hard disk, CPU ในการจำลองเครื่องคอมพิวเตอร์เสมือน ซึ่งจะเรียกเครื่องที่ถูกใช้ทรัพยากรว่า Host และเรียกเครื่องเสมือนว่า Guest โดยในเครื่อง Guest สามารถติดตั้งและใช้งานระบบปฏิบัติการได้เสมือนกับเป็น Software หนึ่งของเครื่องคอมพิวเตอร์ ดังนั้นจึงสามารถติดตั้งระบบปฏิบัติการอื่นที่แตกต่างจากระบบปฏิบัติการหลักของเครื่อง Host ได้ เช่น เครื่อง Host ใช้งาน Microsoft Windows แต่เครื่อง Guest ติดตั้ง Linux เป็นต้น นอกจากนี้ยังสามารถสร้าง Guest ได้มากกว่า 1 Guest ในเครื่อง Host เดียวกัน

### Kali

Kali เป็นระบบปฏิบัติการณ์ลินุกซ์ (Linux) ตัวหนึ่งของคอมพิวเตอร์ซึ่งมีพื้นฐานบน Linux distribution [[5]](#Linux) ที่พัฒนาต่อมาจาก Debian ชื่อเล่นไทยว่า “ลีนุกซ์มังกรไฟ” ถูกเขียนขึ้นมาเหมือนกับ ระบบอื่นๆ เช่น Ubuntu ความสามารถที่แตกต่างจาก Linux ตัวอื่นๆ คือการติดตั้งและใส่ Feature หลักๆ และสำคัญ เกี่ยวกับ IT security (งานด้านความปลอดภัยระบบไอที) ไว้ให้ โดยที่ไม่ต้องติดตั้ง หรือถ้ายังไม่ได้ติดตั้งก็สามารถติดตั้งได้ง่าย ผ่านระบบติดตั้งภายในที่มีให้เรียกว่า software repository ของ Kali



ภาพประกอบที่ 2.5 ตัวอย่างโปรแกรม Kali Linux

### Visual Studio Code (VS Code)

Visual Studio Code (VS Code) เป็นโปรแกรม Code Editor ที่ใช้ในการแก้ไขและปรับแต่งโค้ด จากค่าย Microsoft มีการพัฒนาออกมาในรูปแบบของ Open Source จึงสามารถนำมาใช้งานได้แบบฟรี ซึ่ง Visual Studio Code นั้น เหมาะสำหรับนักพัฒนาโปรแกรมที่ต้องการใช้งานข้ามแพลตฟอร์ม รองรับการใช้งานทั้งบน Windows, macOS และ Linux สนับสนุนทั้งภาษา JavaScript, TypeScript และ Node.js สามารถเชื่อมต่อกับ Git ได้ นำมาใช้งานได้ง่ายไม่ซับซ้อน มีเครื่องมือส่วนขยายต่าง ๆ ให้เลือกใช้อย่างมากมาย

### Qt Designer

Qt Designer เป็นเครื่องมือในการสร้างแอปพลิเคชั่น และ GUI ด้วย PySide ซึ่งสามารถทำงานบน Desktop PC, Smart Phone และ Embedded System สามารถทำงานได้หลายระบบปฏิบัติการ (OS) หรือ เรียกว่า Cross-platform การเขียน GUI โดย Qt จะมี API และ Library ต่าง ๆ อีกทั้งยังสนับสนุนการพัฒนาทั้ง C++, Java, Python, Perl, Pascal และ PHP

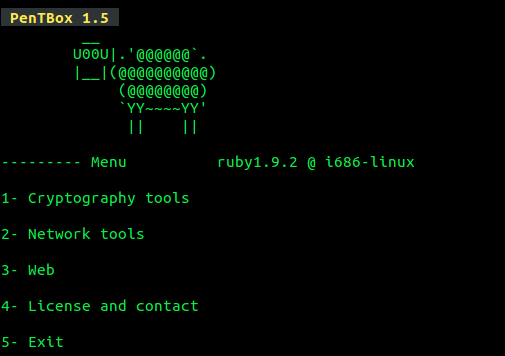
### Hashcat

Hashcat [[7]](#Hashcat) เป็น Open-Source Password Recovery หรือ Password Cracking โดยสามารถใช้ถอดรหัส Hash Algorithm ได้หลายอย่าง ไม่ว่าจะเป็น MD5, SHA1, SHA256, HMAC, WPA, JWT รวมถึง Bitcoin, Ethereum และยังรองรับทั้ง CPU และ GPU

### PenTBox

PenTBox เป็นชุดรักษาความปลอดภัยที่ออกแบบมาเพื่อทดสอบความปลอดภัย ความเสถียรของเครือข่าย โปรแกรมเขียนขึ้นด้วยภาษา Ruby และมุ่งเน้นไปที่ระบบ GNU/Linux แต่เข้ากันได้กับ Windows, MacOS และอื่นๆ มีคุณสมบัติ ดังนี้

* Password Crackers
* Denial of Service testing tools (DoS and DDoS)
* Secure Password Generators
* Honeypots

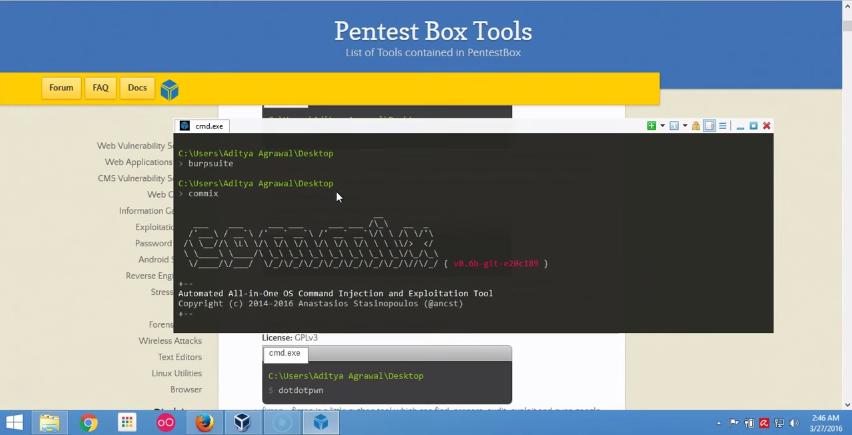


ภาพประกอบที่ 2.6 ตัวอย่างโปรแกรม PenTBox

### Pentestbox

Pentestbox เป็น Software ที่รวบรวมเครื่องมือทางด้าน Security ไว้หลายเครื่องมือ โดย Pentestbox สามารถรันบนระบบปฏิบัติการ Windows, Linux ได้ ไม่จำเป็นต้องอาศัยเครื่องเสมือน เช่น Virtual Machine (VM) Pentestbox มีคุณสมบัติ ดังนี้

* Web Vulnerability Scanners
* Sniffing
* Reverse Engineering
* Wireless Attacks



ภาพประกอบที่ 2.7 ตัวอย่างเว็บไซต์ Pentestbox

ตารางที่ 2.1 ตารางเปรียบเทียบการทำงานของระบบงานที่เกี่ยวข้อง

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Comparison Criteria** | **Kali Linux** | **PentestBox** | **PenTBox** | **ISAN Security Gizmo Box** |
| การติดตั้ง | เป็น OS Image ที่ Boots  ได้ และมี VM Images ที่เปิดด้วย Hypervisor ได้หลากหลาย | ต้องติดตั้งบน Windows OS | ต้องติดตั้งบน Linux | เป็น Kali Linux OS Image  โดยออกแบบให้เป็น VM Images บน Oracle Virtual box หรือ VM Ware Player |
| User Friendliness | ใช้ค่อนข้างยาก  ต้องรู้คำสั่งและ command line parameters | interface เป็น console commands | มี user interface เป็น menu & choices ลักษณะ interface เป็น Text User Interface (TUI) | User interface หลักเป็น GUI  สำหรับ features หลักๆ ที่นำเสนอใน Project นี้ และมี command line mode สำหรับใช้ Kali Linux Functions |
| ความหลากหลายของ features & functions | เป็น Security & Penetration testing tools จำนวนมาก | มี functions หลายอย่างที่สร้างขึ้นเพื่อเลียนแบบ Kali Linux และ Linux Utilities ต้องยังน้อยกว่า Kali Linux อยู่มาก | มี features/functions ค่อนข้างน้อย เป็น version แรกๆ ในอนาคตจะมีการเพิ่ม functions ต่อไป | คุณสมบัติเบื้องต้นบน GUI สำหรับบน version แรกที่นำเสนอ ยังเริ่มต้นแค่บาง functions แต่สามารถใช้ functions อื่นๆ ของ Kali Linux  ผ่าน command line ได้ และยังสามารถใช้ functions เพิ่มเติมที่ติดตั้ง เพิ่มเข้าไปใน Kali Linux อีกด้วย (โดยใช้ command line) |

Kali Linux มีให้เลือกใช้งานทั้งแบบ Graphic User Interface และ Command Line Interface แต่ส่วนใหญ่ยังอยู่ในรูปแบบ Command Line Interface ซึ่ง PentestBox และ PenTBox จะมีเพียง Command Line Interface เท่านั้นส่วน ISAN Security Gizmo Box จะอยู่ในรูปแบบ Graphic User Interface ที่ผู้ใช้งานสามารถใช้งานโดยไม่ต้องใช้คำสั่งเพียงกรอกข้อมูล เช่น หมายเลข IP address สำหรับ สแกน Port หรือ กรอก Domain name Server สำหรับสแกนเว็บไซต์ และสามารถกดปุ่ม Scan เพื่อประมวลผลซึ่งเป็นการใช้งานโดย User ไม่ต้องพิมพ์คำสั่งบน Command Line Interface

# ขั้นตอนการดำเนินงาน

ในบทนี้จะกล่าวถึงการสร้าง GUI และทดสอบเครื่องมือ Password Evaluation, Malware Scanning, Message Digest Generator, Vulnerability Scanning, HTTPS Testing แสดงขั้นตอนการดำเนินงานในส่วนที่จะพัฒนาเป็นโปรแกรม ISAN Security Gizmo Box โดยสร้างจาก PyQT6 และ Python โดยเป็นโปรแกรมที่รวบรวมเครื่องมือที่กล่าวมาข้างต้นโดยจะมีกรอบการดำเนินงานดังนี้

## กรอบการดำเนินงาน

Diagram

Description automatically generated

ภาพประกอบที่ 3.1 ภาพรวมของโครงงานปริญญานิพนธ์

จากภาพประกอบที่ 3.1 ภาพรวมของโครงงานปริญญานิพนธ์ แสดงให้เห็นถึงกรอบการดำเนินงาน ดังนี้

1. ศึกษาการคำนวณ Bit of entropy และนำผลลัพธ์ที่ได้มาคำนวณหาข้อมูลเชิงปริมาณ คือ ค่าของ Bit of entropy ละข้อมูลเชิงคุณภาพ คือระดับของความต้านทานโดยคำนวณจาก Special Warning โดยอ้างอิงตามค่ามาตรฐาน NIST Special Publication 800-63B ความยาวของรหัสผ่านและช่วงของ Bit of entropy
2. ศึกษาเทคนิคการทำ Dictionary Attack โดยแบ่งเป็น 2 รูปแบบ คือ Straightforward Dictionary attack และ Skipping attack
3. ศึกษาและทดสอบการเรียกใช้งาน VirusTotal API เพื่อนำมาใช้ในการตรวจสอบ Malware
4. ศึกษาและทดสอบการทำ Vulnerability Scanning โดยใช้คำสั่ง Nmap และทำการทดสอบ Vulner.NES
5. ทดสอบ Open-Source testssl.sh เพื่อใช้ในการตรวจสอบ HTTPS Header และตรวจสอบ HSTS Configuration และ HSTS Preload
6. ศึกษา Algorithms การคํานวณ Message Digest ได้แก่ MD5, SHA-1, SHA-2(224, 256, 384, 512) , SHA-3(224, 256, 384, 512)

## การพัฒนาระบบด้วย Qt Designer

A screenshot of a computer

Description automatically generated with medium confidence

ภาพประกอบที่ 3.2 การพัฒนา Interface ด้วย Qt Designer

จากภาพประกอบที่ 3.2 การพัฒนา Interface ด้วย Qt Designer เพื่อเป็นตัวกลางในการสื่อสารระหว่างผู้ใช้และเครื่องมือการทำงานต่าง ๆ โดยด้านซ้ายจะเป็น Widget Box หรือ Components ที่ประกอบไปด้วย Layouts, Spacers, Buttons, item View, Containers, Input Widgets และ Display Widgets ที่สามารถใช้งานได้ใน Qt Designer และ ด้านขวาคือ Properties ที่เกี่ยวข้องกับการตกแต่งหรือปรับเปลี่ยน Style Sheet ให้กับแต่ละ Object ของ Qt Designer โดยประกอบไปด้วย Object Inspector จะแสดง Object ที่มีใน Frame และส่วนของ Property Editor เช่น font, geometry, window Title

Text

Description automatically generated

ภาพประกอบที่ 3.3 Code การเรียกใช้ Qt Designer

ภาพที่ 3.3 Code การเรียกใช้ Qt Designer File หรือ .ui ด้วย Python Language และ VS Code เพื่อโหลดไฟล์ UI ด้วย Library ของ PyQt6.uic Function LoadUi()

## Password Evaluation

### การประเมินรหัสผ่านด้วยเครื่องมือ Password Evaluation

Graphical user interface

Description automatically generated

ภาพประกอบที่ 3.4 เครื่องมือประเมินรหัสผ่าน (Password Evaluation)

สำหรับเครื่องมือประเมินรหัสผ่านผู้ใช้งานสามารถป้อนรหัสผ่านที่ต้องการเพื่อใช้ในการคำนวณ Entropy โดยใช้สูตรการคำนวณ E = Length \* Log2(Pool\_of\_Chars) และจะแสดงผลลัพธ์เป็นข้อมูลเชิงปริมาณและข้อมูลเชิงคุณภาพ

จากการศึกษาข้อมูลพบว่าเว็บไซต์ keepass.info ระบุข้อมูลเชิงคุณภาพของรหัสผ่านที่มีความแข็งแกร่งนั้นมีขนาดของเอนโทรปีอยู่ที่ 112-128 บิต ส่วนเว็บไซต์ barldung.com ระบบว่าข้อมูลเชิงคุณภาพของรหัสผ่านที่มีความแข็งแกร่งมีขนาดของเอนโทรปี อยู่ที่ 75-100 บิต จากข้อมูลดังกล่าว กล่าวโดยสรุปคือ keepass.info เป็นเว็บไซต์ Password Manager มีจุดประสงค์ให้คอมพิวเตอร์ตั้งรหัสผ่านให้ ทำให้เอนโทรปีของรหัสผ่านมีค่าที่สูงแต่รหัสผ่านที่ได้นั้นมีความยาวและยากเกินกว่ามีมนุษย์จะจดจำได้

### การวิเคราะห์ข้อมูลเชิงปริมาณ

Diagram

Description automatically generated

ภาพประกอบที่ 3.5 เงื่อนไขการแสดงข้อมูลเชิงคุณภาพ

จากภาพประกอบที่ 3.5 เงื่อนไขการแสดงข้อมูลเชิงคุณภาพ แสดงให้เห็นว่ารหัสผ่านที่มีความยาว 8 หลัก และเมื่อนำไปคำนวณจะได้ E = 8 \* 7 โดย 7 บิต มาจาก log2(128) แสดงให้เห็นว่ามีความหลากหลายของรูปแบบอักขระถึง 128 รูปแบบ ซึ่งเมื่อเทียบกับ pool of characters แล้วชี้ให้เห็นว่า รหัสผ่านที่มีค่าเอนโทรปีตั้งแต่ 50 บิต ขึ้นไปก็เพียงพอแล้วจึงสรุปได้ว่าหากรหัสผ่านที่มีค่าเอนโทรปีตั้งแต่ 50 บิต ขึ้นไปถือว่าเป็นรหัสผ่านระดับกลาง แต่หาก Entropy Bits ตั้งแต่ 80 บิต ขึ้นไปโดยคำนวณได้จากสูตร E = 12 \* 7 ซึ่งจะมีค่าเท่ากับ 84 บิต จะถือว่าเป็นรหัสผ่านที่มีความแข็งแกร่งหรือเป็นรหัสผ่านที่ดีต่อการใช้งาน โดยยังไม่ได้เปรียบเทียบกับรหัสผ่านใน wordlist ของ attacker จึงสรุปได้ว่าค่าเอนโทรปีต่ำสุดที่จะยอมรับได้คือ 50 บิต และค่าเอนโทรปีที่ 80 บิต ขึ้นไปจะถือว่ามีความปลอดภัยโดยถ้าหากอยู่ระหว่าง 51-79 บิต หมายความว่ารหัสผ่านนั้นพอใช้ได้และอาจจะต้องทำให้ได้ถึง 80 บิต หลังจากนั้นจะมีการนำรหัสผ่านที่ป้อนเข้ามาไปตรวจสอบกับ Top 200 most common password of the years ย้อนหลัง 3 ปี ที่จัดโดย Nordpass.com

นอกจากนี้เครื่องมือประเมินรหัสผ่านจะทำการนำรหัสผ่านที่ป้อนเข้ามาไปตรวจสอบกับ Dictionary ว่าเป็นรหัสผ่านที่ตรงกับ wordlist หรือไม่ โดยใช้วิธี Dictionary attack แบ่งเป็น 2 รูปแบบ คือ Straightforward Dictionary attack และ Skipping attack ซึ่ง Skipping attack มีรายละเอียด ดังนี้

Diagram

Description automatically generated

ภาพประกอบที่ 3.6 เทคนิคการทำ Combinator attack ด้วย python และ Hashcat

Combinator attack คือ วิธีการโจมตีระบบความปลอดภัยของรหัสผ่านโดยใช้การสร้างรายการคำนวณที่เป็นไปได้ทั้งหมดของคำผสมกันระหว่างคำที่อาจเป็นรหัสผ่านได้ โดยการสร้างรายการคำนวณที่เป็นไปได้ทั้งหมดนี้จะเป็นการนำเอาคำที่อาจจะเป็นรหัสผ่านได้มาผสมกันจนกว่าจะได้รหัสผ่านที่ถูกต้อง วิธีการนี้อาจใช้เวลานานและยังขึ้นอยู่กับความยากง่ายของรหัสผ่านและจำนวนคำในรายการคำนวณที่สร้างขึ้น การใช้ Combinator attack จึงเป็นเครื่องมือที่ใช้ในการทดสอบความปลอดภัยของรหัสผ่าน

Diagram

Description automatically generated

ภาพประกอบที่ 3.7 เทคนิคการทำ Hybrid attack ด้วย Python และ Hashcat

Hybrid attack คือ วิธีการโจมตีระบบความปลอดภัยของรหัสผ่านโดยใช้การสร้างรายการคำนวณที่เป็นไปได้โดยใช้เป็นแบบระบุ Mask คือในกรณีที่ทราบว่ารหัสผ่านลงท้ายด้วยตัวเลข สามารถระบุให้ทำการ Brute-force attack ตัวสุดท้ายเป็นตัวเลขได้ ซึ่งจะช่วยเพิ่มโอกาสในการค้นหารหัสผ่านมากขึ้น

### ทดลองการใช้เทคนิค Dictionary attack

A screenshot of a computer

Description automatically generated with medium confidence

ภาพประกอบที่ 3.8 ตัวอย่างการทดสอบ Straight forward attack บน kali Linux

โดยเครื่องที่ทำการทดสอบมีคุณสมบัติ ดังนี้ AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx และใช้ Hashcat โดยมี option ในการทดสอบ ดังนี้ -a คือ attack mode 0 คือ Straight Dictionary attack และ -m 0 คือ md5 ใช้การระบุรูปแบบของ hash Algorithm ที่ใช้ในการเข้ารหัสของรหัสผ่าน Dictionary ที่ใช้ทำการทดสอบคือ rockyou.txt ซึ่งเป็น Password Dictionary ที่ Hacker หรือ Security Professional เลือกใช้โดยมีรหัสผ่านทั้งหมด 14,344,392 รหัสผ่าน

Graphical user interface, text

Description automatically generated

ภาพประกอบที่ 3.9 ตัวอย่างการทดสอบ Combinator attack บน kali Linux

จากภาพประกอบที่ 3.10 ตัวอย่างการทดสอบ Combinator attack บน kali โดยมี option ในการทดสอบ ดังนี้ -a คือ attack mode 1 คือ combinator attack และ -m 0 คือ md5 ใช้การระบุรูปแบบของ hash algorithm ที่ใช้ในการเข้ารหัสของรหัสผ่าน

A screenshot of a computer

Description automatically generated

ภาพประกอบที่ 3.10 ตัวอย่างการทดสอบ Hybrid attack บน kali Linux

จากภาพประกอบที่ 3.10 ตัวอย่างการทดสอบ Hybrid attack บน kali Linux โดยมี option ในการทดสอบ ดังนี้ -a คือ attack mode 6 คือ Hybrid attack โดย Hybrid attack แบ่งออกเป็น 2 รูปแบบ คือ 6 – 7 โดยที่ใช้คือ -a 6 รูปแบบจะเป็น Wordlist + Mark และ -m 0 คือ md5 ใช้การระบุรูปแบบของ hash Algorithm ที่ใช้ในการเข้ารหัสของรหัสผ่าน

## Message Digest

Graphical user interface, application

Description automatically generated

ภาพประกอบที่ 3.11 เครื่องมือคำนวณค่า (Message Digest)

จากภาพประกอบที่ 3.11 เครื่องมือคำนวณค่า (Message Digest) ผู้ใช้สามารถป้อนข้อมูลได้ 2 รูปแบบ คือไฟล์และข้อความ และแสดงผลลัพธ์ออกมาในรูปแบบข้อความที่ถูกแฮชแล้ว และ QR Code ที่ผู้ใช้สามารถบันทึกรูปภาพได้ โดย Algorithms มีดังนี้

MD5 (Message Digest Algorithm 5) เป็นอัลกอริทึมการเข้ารหัสที่ใช้กับข้อมูลขนาดเล็ก โดยมีข้อจำกัดคือมีโอกาสที่จะเกิดการชนของข้อมูล (collision) ได้ง่าย ซึ่งอาจจะทำให้เกิดการเข้ารหัสซ้ำกันได้

SHA-1: เป็นฟังก์ชันการแฮชที่มีขนาดการแฮชเป็น 160 บิต และถูกพัฒนาโดย NSA (National Security Agency) ในปี 1995 ซึ่งถือว่าเป็นฟังก์ชันการแฮชที่เก่าและมีช่องโหว่ในการเข้ารหัส จึงไม่ควรนำมาใช้งานในปัจจุบัน

SHA-2: เป็นฟังก์ชันการแฮชที่มีขนาดการแฮชเป็น 224, 256, 384 หรือ 512 บิต และถูกพัฒนาโดย NIST (National Institute of Standards and Technology) เพื่อเป็นตัวแทนของ SHA-1 ที่มีความปลอดภัยต่ำ โดย SHA-2 ถือว่ามีความปลอดภัยสูงกว่า SHA-1 และยังสามารถใช้งานได้ในปัจจุบัน

SHA-3: เป็นฟังก์ชันการแฮชที่มีขนาดการแฮชเป็น 224, 256, 384 หรือ 512 บิต และถูกพัฒนาโดย NIST โดยใช้วิธีการแฮชแบบ Keccak ซึ่งเป็นวิธีการแฮชแบบเร็วและปลอดภัย โดย SHA-3 ถือว่ามีความปลอดภัยสูงกว่า SHA-2 และมีการใช้งานกันอย่างแพร่หลายในการรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์

## Malware Scanning

A screenshot of a computer

Description automatically generated with medium confidence

ภาพประกอบที่ 3.12 เครื่องมือตรวจสอบ Malware (Malware Scanning)

เครื่องมือเครื่องมือตรวจสอบ Malware (Malware Scanning) ผู้ใช้สามารถสามารถป้อนข้อมูลได้ 2 รูปแบบคือ ไฟล์หรือ URL หลังจากนั้นเครื่องมือจะทำเรียกใช้งาน VirusTotal API ซึ่งเป็น API ที่ให้บริการตรวจสอบไฟล์หรือ URL ว่ามีความเสี่ยงต่อความปลอดภัยหรือไม่ โดยมีการรวบรวมข้อมูลจากหลายๆ เครื่องมือตรวจสอบไวรัสและมัลแวร์ ซึ่งอาจจะรวมถึงโปรแกรมแอนติไวรัส และอื่นๆ อีกมากมาย เพื่อทำการวิเคราะห์ไฟล์หรือ URL นั้นๆ ว่ามีความเสี่ยงต่อความปลอดภัยหรือไม่ การเรียกใช้งาน VirusTotal API โดยเป็น Public API เป็น API ที่ให้บริการฟรี สามารถใช้งานได้ โดยไม่จำเป็นต้องมีบัญชีผู้ใช้งาน แต่จะมีจำกัดในการใช้งาน โดยสามารถใช้งานได้ไม่เกิน 500 คำขอต่อวัน และจำกัดคำขอต่อวินาที 4 คำร้องขอ

Diagram

Description automatically generated

ภาพประกอบที่ 3.13 แสดงการไหลของข้อมูลเมื่อเรียกใช้ VirusTotal API-URL Scan

เมื่อผู้ใช้ต้องการตรวจสอบเกี่ยวกับ Web Site หรือปลายทางที่จะต้องเข้าถึงผู้ใช้สามารถนำ URL ของปลายทางหรือ Web Site ที่ต้องการตรวจสอบส่งไปให้เครื่องมือสแกนไวรัสหลากหลายเครื่องมือช่วยกันสแกนหาเพื่อตรวจสอบ fishing ของ Web Site โดยผ่านตัวกลาง API VirusTotal ที่รวบรวมเครื่องมือการตรวจสอบไวรัสหรือ Malware ที่ไม่หวังดีโดย VirusTotal API จะตอบกลับหรือคืนค่ากลับมาเป็น Json Data โดยรายละเอียดประกอบไปด้วย วันและเวลา, ชื่อเครื่องมือที่ใช้สแกน , ผลลัพธ์การสแกน

Text

Description automatically generated

ภาพประกอบที่ 3.14 ทดลองการเรียกใช้ VirusTotal API-URL Scan

ใช้ API : https://www.virustotal.com/vtapi/v2/url/scan ด้วย แบบ Post โดยมี Parameters ที่ต้องส่งไปคือ API-key ที่ได้จากการสมัครสมาชิกและ URL ที่ต้องการตรวจสอบและการคืนค่ากลับมาจะเป็น Json Data จากนั้นต้องร้องขอผลลัพธ์จากการสแกนด้วย API:https : //www.virustotal.com/vtapi/v2/url/report แบบ Get โดยมี Parameters คือ API-key และ resource หรือ URL ที่ส่งไปสแกนในครั้งแรกนั้นค่าที่ได้ประกอบไปด้วย ชื่อเครื่องมือในการสแกน ผลลัพธ์จากการสแกนซึ่งอยู่ในรูปแบบของ Json Data

Diagram

Description automatically generated

ภาพประกอบที่ 3.15 แสดงการไหลของข้อมูลเมื่อเรียกใช้ VirusTotal API-File Scan

เมื่อผู้ใช้ต้องการตรวจสอบเกี่ยวกับ Malware หรือ Malicious File โดนนำ File ที่ต้องการตรวจสอบส่งไปให้เครื่องมือสแกนไวรัสหลากหลายเครื่องมือช่วยกันสแกนหาเพื่อตรวจสอบ Malicious Software ในรูปแบบต่าง ๆ เช่น Malware, Trojan, Spyware เป็นต้น โดยผ่านตัวกลาง API VirusTotal ที่รวบรวมเครื่องมือการตรวจสอบไวรัสหรือ Malware ที่ไม่หวังดีโดย VirusTotal API จะตอบกลับหรือคืนค่ากลับมาเป็น Json Data โดยรายละเอียดประกอบไปด้วย วันและเวลา, ชื่อเครื่องมือที่ใช้สแกน , ผลลัพธ์การสแกน, เวอร์ชันของเครื่องมือ,

Text

Description automatically generated

ภาพประกอบที่ 3.16 ทดลองการเรียกใช้ VirusTotal API-File Scan

ใช้ API : https://www.virustotal.com/vtapi/v2/file/scan แบบ Post เพื่ออัพโหลดไฟล์ผ่าน API โดยมี Parameters ที่ต้องส่งไปคือ API-key ที่ได้จากการสมัครสมาชิกและ File หรือ Path File ที่ต้องการนำไปตรวจสอบจะต้องใช้ resource ที่ได้จากการสแกนครั้งแรกเพื่อนำไปเป็น parameter ในการดึงข้อมูล Report จาก API: https : //www.virustotal.com/vtapi/v2/url/report จะได้ค่ากลับมาจะเป็น Json Data

## Vulnerability Scanning

A screenshot of a computer

Description automatically generated

ภาพประกอบที่ 3.17 เครื่องมือตรวจสอบหาช่องโหว่ (Vulnerability Scanning)

เครื่องมือตรวจสอบหาช่องโหว่ (Vulnerability Scanning) ผู้ใช้สามารถป้อนข้อมูลในรูปแบบ URL, IP address หรือ hostname เพื่อทำการสแกนหาช่องโหว่และรายงานผลการสแกนในรูปแบบของ Table View พร้อมกับแจ้งเตือนผู้ใช้หากมี port ที่น่าสงสัยเปิดอยู่และ สรุป Report ออกมาในรูปแบบของ PDF File โดยมีรูปแบบที่ใช้ในการสแกน ดังนี้

Diagram

Description automatically generated

ภาพประกอบที่ 3.18 TCP Port Scanning

TCP SYN Scan เป็นเทคนิคหนึ่งในการสแกนพอร์ต (port scanning) บนเครือข่ายคอมพิวเตอร์ โดยใช้โปรโตคอล TCP ในการส่งข้อมูลไปยังเครื่องหมายเลขพอร์ตต่างๆ เพื่อหาพอร์ตที่เปิดใช้งานอยู่บนเครื่องนั้นๆ

การทำงานของ TCP SYN Scan จะเริ่มต้นด้วยการส่งสัญญาณ SYN (Synchronize) packet ไปยังเครื่องหมายเลขพอร์ตที่ต้องการสแกน ถ้าเครื่องหมายเลขพอร์ตนั้น ๆ มีการตอบสนองกลับมาด้วยสัญญาณ SYN-ACK (Synchronize-Acknowledgment) packet แสดงว่าพอร์ตนั้น ๆ เปิดใช้งานอยู่ แต่ถ้าไม่มีการตอบสนองกลับมา แสดงว่าพอร์ตนั้น ๆ ปิดอยู่หรือถูกบล็อกไว้ TCP SYN Scan เป็นเทคนิคที่มีประสิทธิภาพสูงและเป็นที่นิยมใช้ในการทดสอบความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์ แต่ก็สามารถถูกตรวจจับและบล็อกได้โดยระบบป้องกันการโจมตีต่าง ๆ ที่มีอยู่ในเครือข่าย

Diagram

Description automatically generated

ภาพประกอบที่ 3.19 Syn Scanning

Nmap Stealth Scan เป็นการสแกนเครื่องคอมพิวเตอร์แบบไม่เปิดเผยตัวเอง โดยการสแกนนี้จะทำการสแกนพอร์ตบนเครื่องคอมพิวเตอร์โดยไม่ส่ง packet ชนิด SYN ไปยังเครื่องที่ต้องการสแกน ซึ่งวิธีการเชื่อมต่อแบบนี้จะไม่เปิดเผยตัวเองต่อเครื่องคอมพิวเตอร์ที่เรากำลังสแกนอยู่ การใช้งาน Nmap Stealth Scan สามารถทำได้โดยใช้คำสั่ง nmap -sS <target> โดยที่ <target> คือ IP address หรือชื่อโดเมนของเครื่องคอมพิวเตอร์ทีต้องการสแกน ซึ่งสามารถช่วยป้องกันการโจมตีจากผู้ไม่หวังดีได้ในบางกรณี

Aggressive scan ใน nmap เป็นการสแกนพอร์ตโดยใช้เทคนิคการสแกนที่เร็วและเจาะจงมากขึ้น โดยการสแกนแบบ Aggressive จะเป็นการสแกนทุกรูปแบบที่เป็นไปได้และใช้เทคนิคการสแกนที่หลากหลาย เพื่อหาข้อมูลเพิ่มเติมเกี่ยวกับระบบเครือข่ายที่กำลังถูกสแกน การสแกนแบบ Aggressive อาจทำให้ระบบเครือข่ายที่ถูกสแกนเกิดความเสี่ยงต่อการโจมตีได้ง่ายขึ้น โดนใช้คำสั่ง nmap -A การใช้งานคำสั่งดังกล่าวจะทำการสแกนพอร์ตของเครื่องเป้าหมายโดยใช้เทคนิคการสแกนที่หลากหลาย เช่น การสแกนด้วย OS detection, version detection, script scanning, traceroute และอื่นๆ ซึ่งจะช่วยให้ผู้ใช้ได้ข้อมูลเพิ่มเติมเกี่ยวกับระบบเครือข่ายที่ถูกสแกนได้มากขึ้น

**ตัวอย่างการทำการทดสอบ Vulner.NSE**

Vulner.NSE เป็น script สำหรับเครื่องมือสแกน network โดย Nmap ช่วยให้ผู้ใช้สามารถสแกนหาช่องโหว่ในระบบเป้าหมายได้ โดยการสอบถามฐานข้อมูลช่องโหว่และเปรียบเทียบผลลัพธ์กับพอร์ตและบริการที่เปิดใช้งานบนระบบเป้าหมาย script นี้สามารถใช้งานได้กับ Nmap ทุกเวอร์ชัน และสามารถทำงานกับระบบปฏิบัติการที่แตกต่างกันได้

Text

Description automatically generated

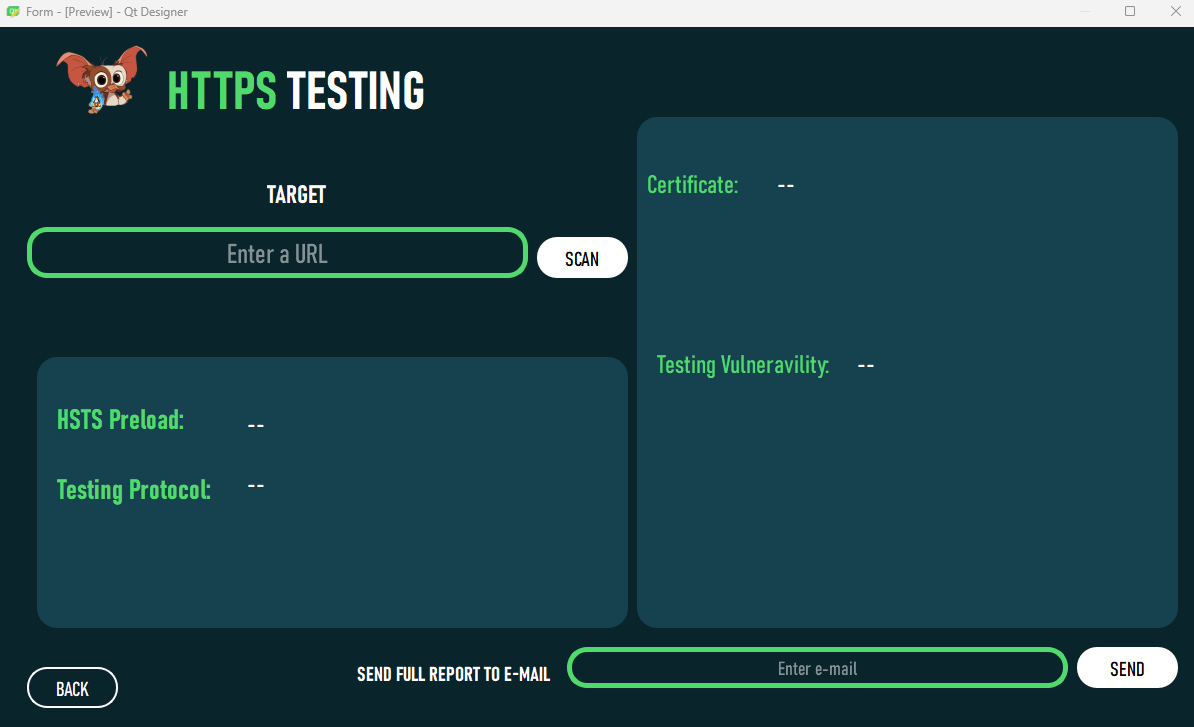
ภาพประกอบที่ 3.20 ทดสอบ Vulner.NSE กับ <https://reg.msu.ac.th>

Text

Description automatically generated

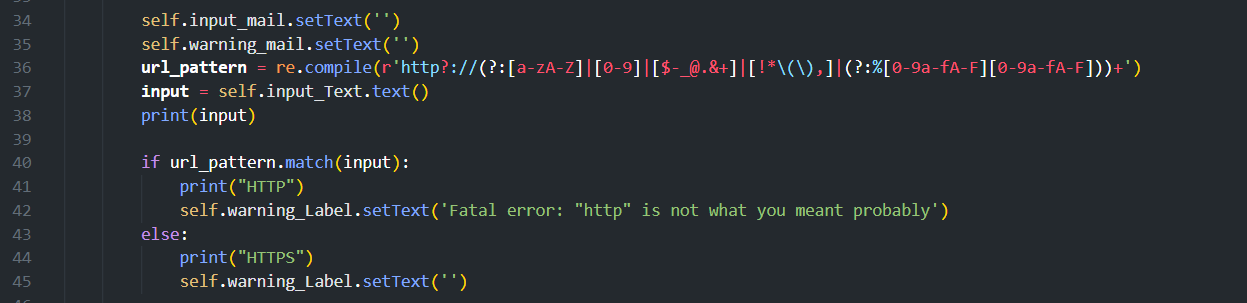
ภาพประกอบที่ 3.21 ทดสอบ Vulner.NSE กับ <https://isanmsu.com>

## HTTPS Testing



ภาพประกอบที่ 3.22 เครื่องมือตรวจสอบความปลอดภัย HTTPS

เครื่องมือตรวจสอบความปลอดภัย HTTPS เพื่อทำการตรวจสอบ HTTPS (Hypertext Transfer Protocol over Secure Socket Layer หรือ Http over SSL) ได้ผลการทดสอบที่ได้แสดงข้อมูลทั่วไป เช่น Certificate Protocol ที่ใช้งาน นอกจากนี้ยังแสดงข้อมูลเกี่ยวกับ Vulnerabilities ต่างๆ ผู้ใช้สามารถกรอก URL และสามารถส่งผลลัพธ์ที่เป็นไฟล์ PDF ไปยัง Email ได้



ภาพประกอบที่ 3.23 การตรวจสอบ URL

เมื่อผู้ใช้งานทำการกรอก URL เข้ามาจะทำการตรวจสอบว่าเป็น HTTP (Hypertext Transfer Protocol) หรือ HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) ในกรณีที่เป็น HTTPS ครื่องมือจะไม่ทำการสแกนและจะทำการแจ้ง error ไปยังผู้ใช้งาน แต่หากเป็น https เครื่องมือจะทำการสแกนและแสดงผลลัพธ์ออกมา นอกจากนี้ยังมีการตรวจสอบ HSTS Preload

HSTS Preload เป็นการเพิ่มเติมความปลอดภัยในการเชื่อมต่อแบบ HTTPS โดยใช้ HSTS (HTTP Strict Transport Security) ซึ่งเป็นการส่ง header ในการติดต่อกับเว็บไซต์เพื่อบอกว่าเว็บไซต์นี้จะใช้ HTTPS เท่านั้น และบอกผู้ใช้งานว่าหากมีการเชื่อมต่อไม่ปลอดภัยจะไม่อนุญาตให้เชื่อมต่อกับเว็บไซต์

Text

Description automatically generated

ภาพประกอบที่ 3.24 การตรวจสอบ HSTS Preload

จากภาพประกอบที่ 3.24 เป็นการตรวจสอบ HSTS Preload โดยใช้ library HSTS preload ซึ่งเป็น library ที่เขียนขึ้นมาเพื่อช่วยตรวจสอบว่าโดเมนนั้นสามารถใช้งาน HSTS preloading ได้หรือไม่ HSTS preloading เป็นการเพิ่มโดเมนเข้าสู่รายการที่เก็บไว้ในเบราว์เซอร์ เพื่อให้เว็บไซต์ใช้ HTTPS อย่างเดียวเมื่อเข้าถึงโดเมนดังกล่าว โดยไม่ต้องทำการ redirect จาก HTTP ไปยัง HTTPS ก่อน ซึ่งจะช่วยป้องกันการโจมตีแบบ Man-in-the-middle ได้

### ตัวอย่างผลการทดสอบ Vulnerabilities ด้วย testssl.sh บน kali Linux

มีช่องโหว่หลายประเภทที่อาจเกิดขึ้นใน SSL/TLS ทำให้ผู้ไม่หวังดีสามารถโจมตีและเข้าถึงข้อมูลที่ถูกส่งผ่านได้ ตัวอย่างเช่นการโจมตี Man-in-the-middle ที่ผู้ไม่หวังดีสามารถแทรกตัวเองเข้าไประหว่างการสื่อสารของผู้ใช้งานสองคน และสามารถดักจับและอ่านข้อมูลที่ถูกส่งผ่านได้

A picture containing graphical user interface

Description automatically generated

ภาพประกอบที่ 3.25 การทดสอบ vulnerabilities ด้วย tests.sh กับ <https://reg.msu.ac.th>

Graphical user interface, text

Description automatically generated

ภาพประกอบที่ 3.26 การทดสอบ vulnerabilities ด้วย tests.sh กับ <https://isanmsu.com>

A screenshot of a computer

Description automatically generated with medium confidence

ภาพประกอบที่ 3.27 การทดสอบ vulnerabilities ด้วย tests.sh กับ <https://it.msu.ac.th>

จากผลการทดสอบที่ได้ พบช่องโหว่เกี่ยวกับ SSL/TLS ที่น่าสนใจ ดังนี้

POODLE (Padding Oracle On Downgraded Legacy Encryption) เป็นช่องโหว่ที่เกี่ยวกับการ downgrade การเชื่อมต่อ SSL/TLS จากเวอร์ชันที่ปลอดภัยลงเป็นเวอร์ชันที่ไม่ปลอดภัย เพื่อให้ผู้โจมตีสามารถแฝงตัวเข้าไปและดักจับข้อมูลที่ถูกส่งผ่าน SSL/TLS ได้

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) เป็นช่องโหว่ที่เกี่ยวข้องกับการใช้งาน SSLv2 ซึ่งเป็นโปรโตคอล SSL/TLS เก่าแก่และไม่ปลอดภัย ช่องโหว่นี้ทำให้ผู้โจมตีสามารถถอดรหัสข้อมูลที่ถูกส่งผ่าน SSL/TLS ได้

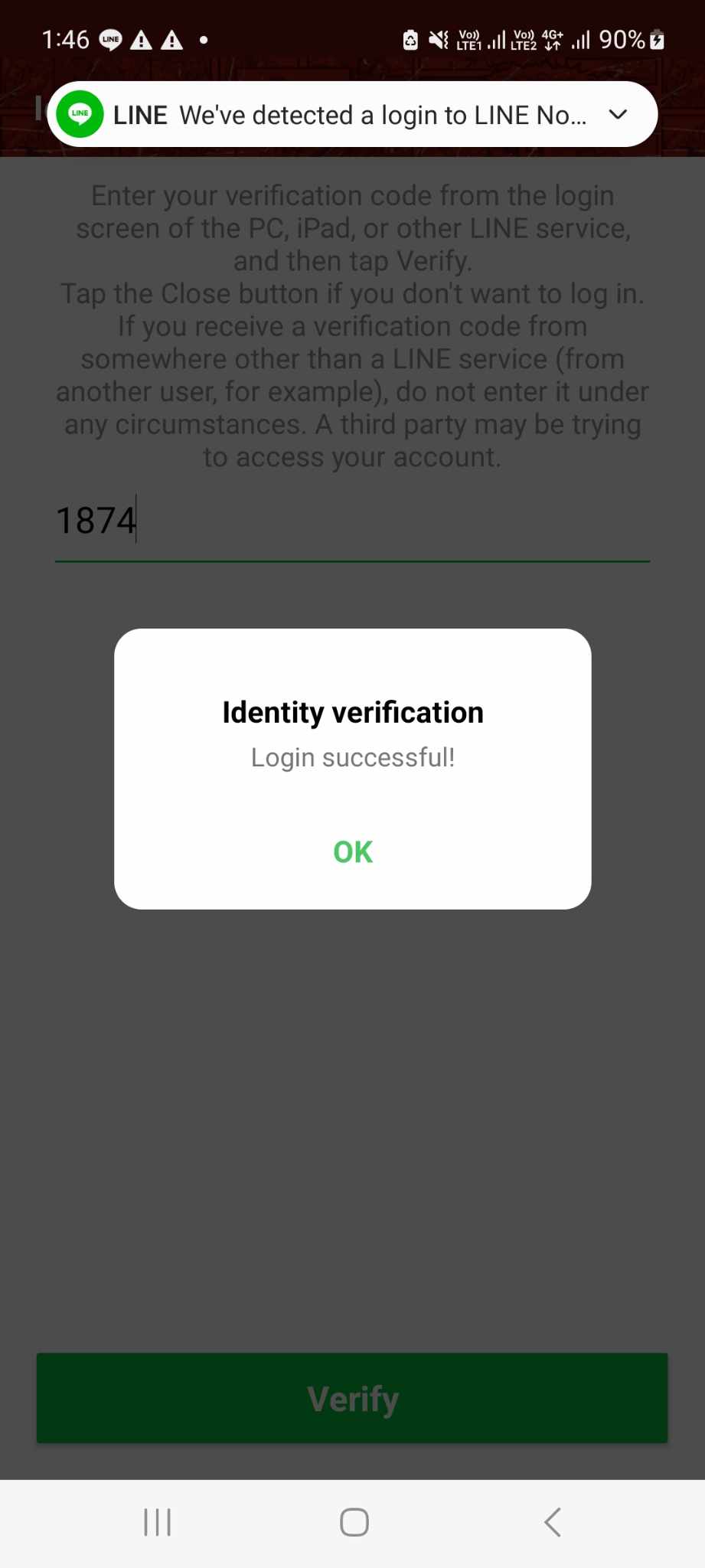
BEAST (Browser Exploit Against SSL/TLS) เป็นช่องโหว่ที่เกี่ยวข้องกับการโจมตี SSL/TLS ด้วยวิธีการใช้เครื่องมือที่ชื่อว่า BEAST ซึ่งสามารถไปอ่านข้อมูลที่ถูกเข้ารหัสที่ผ่าน SSL/TLS ได้ โดยช่องโหว่นี้เกิดจากการใช้งานโปรโตคอล CBC (Cipher Block Chaining) ที่ไม่ปลอดภัยใน SSL/TLS รุ่นเก่า

Heartbleed เป็นช่องโหว่ที่เกิดขึ้นในไลบรารี OpenSSL ทำให้ผู้ไม่หวังดีสามารถอ่านข้อมูลที่อยู่ในหน่วยความจำของเซิร์ฟเวอร์ได้ รวมถึงข้อมูลที่เป็นความลับ เช่น รหัสผ่าน หรือข้อมูลบัตรเครดิต ช่องโหว่นี้ได้รับความสนใจจากสื่อและชุมชนไอทีในช่วงปี 2014

SWEET32 เป็นช่องโหว่ที่เกิดขึ้นในการเข้ารหัสด้วยวิธีการ Triple-DES ทำให้ผู้ไม่หวังดีสามารถอ่านข้อมูลที่ถูกเข้ารหัสได้ ช่องโหว่นี้ได้รับการเผยแพร่ในปี 2016

LUCKY13 เป็นช่องโหว่ที่เกิดขึ้นในการเข้ารหัสด้วยวิธีการ CBC-mode ทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสได้ ช่องโหว่นี้ได้รับการเผยแพร่ในปี 2013

## A white square with green text Description automatically generatedคู่มือการติดตั้ง Line API KEY to Group Chat



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a phone

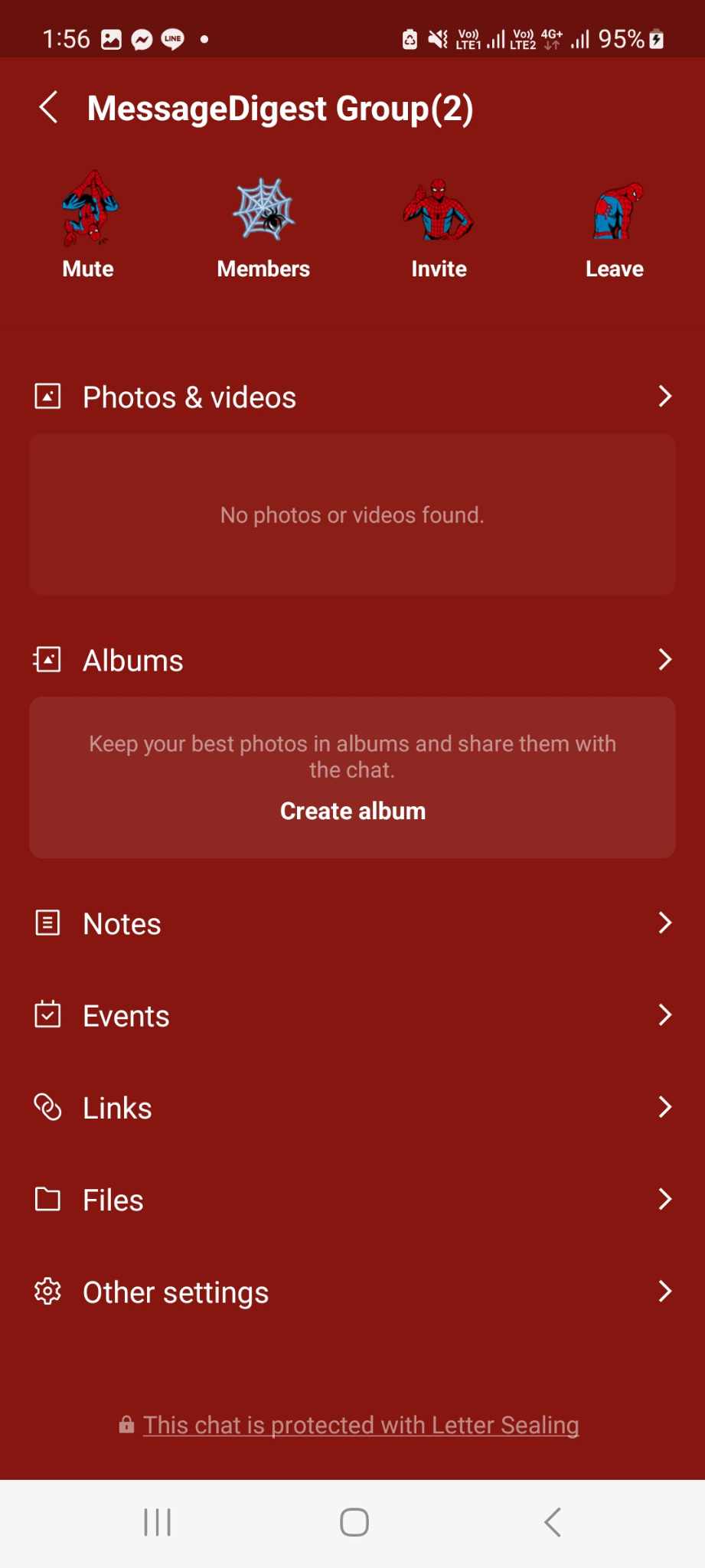
Description automatically generated

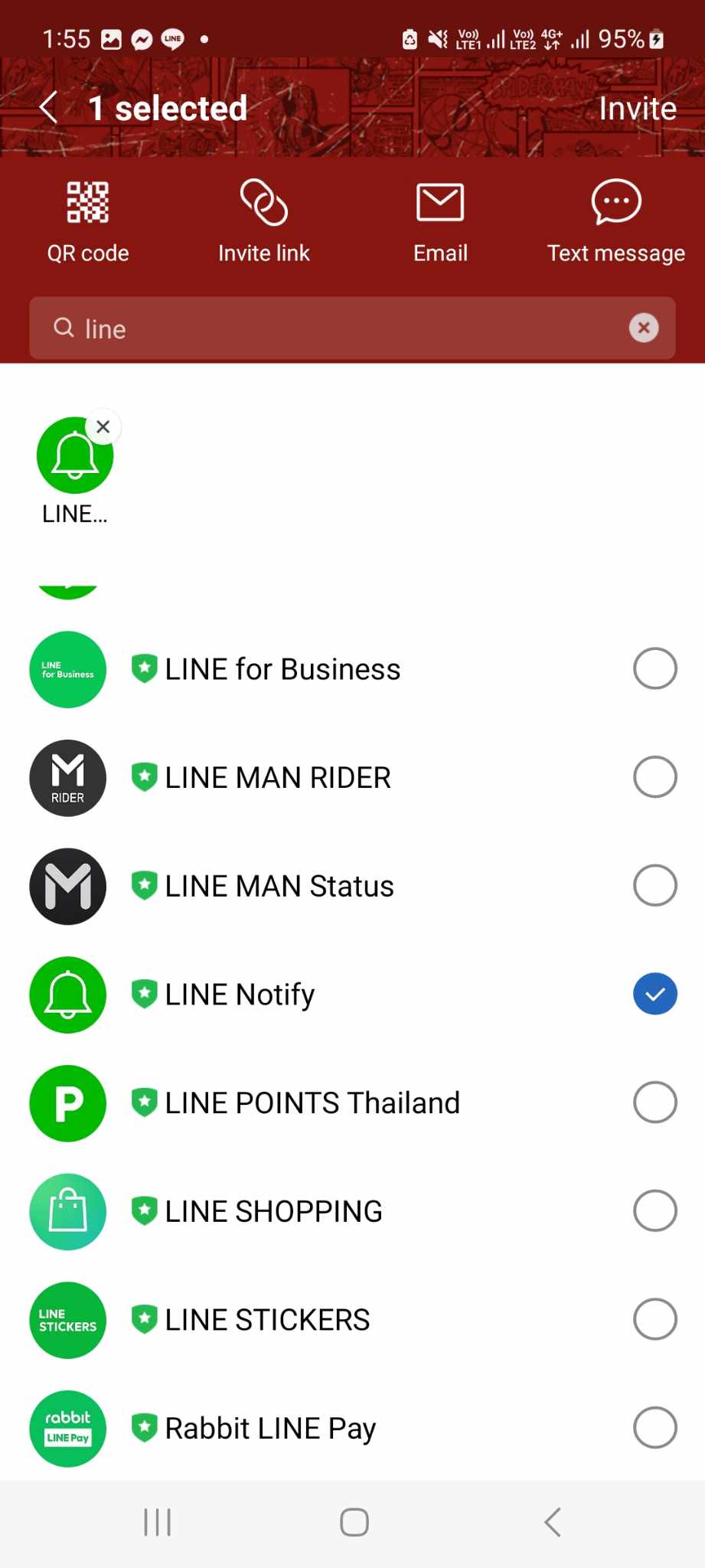
A screenshot of a computer

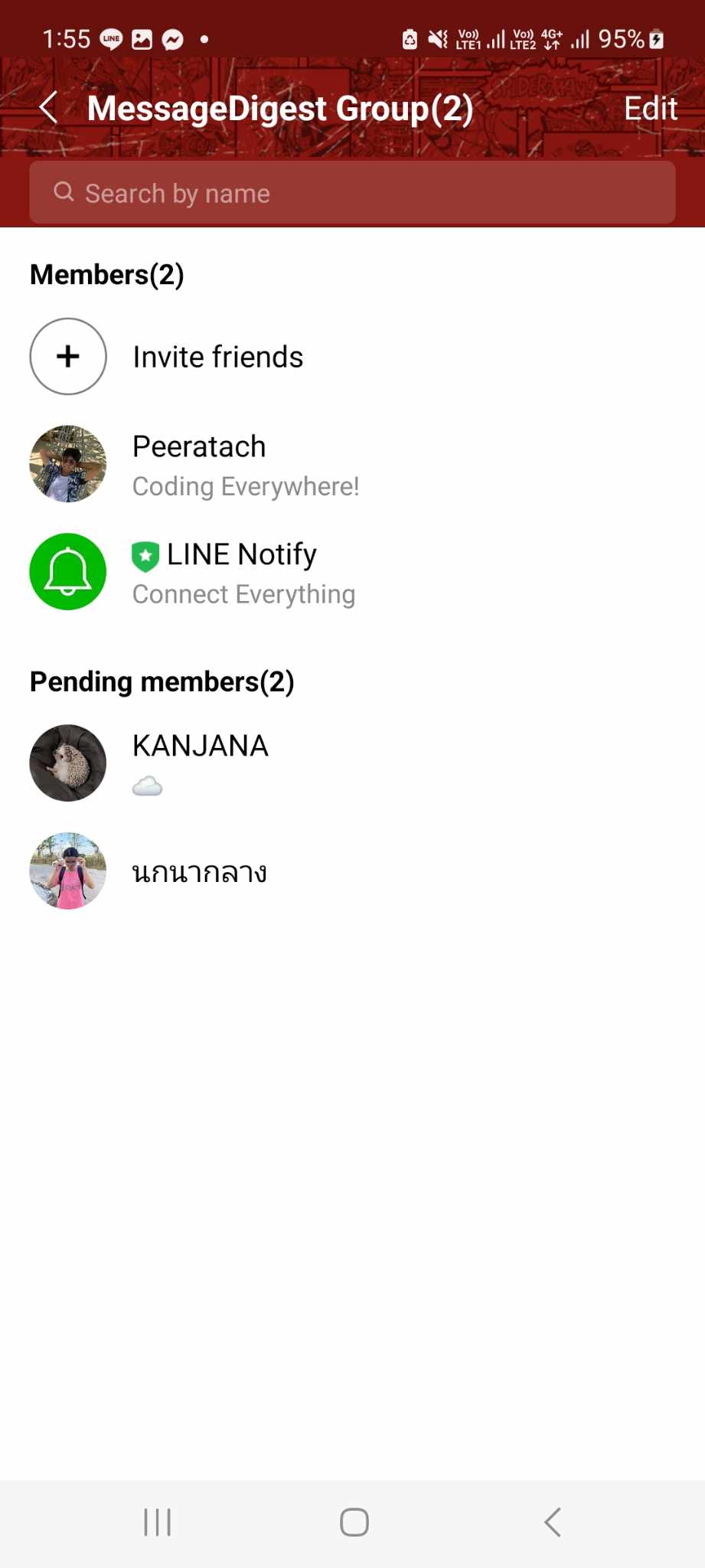
Description automatically generated

A screenshot of a computer

Description automatically generated









เอกสารอ้างอิง

[1] P. Grassi, M. Garcia, J. Fenton. “Digital Identity Guidelines” NIST Special Publication 800-63 Revision 3, June 2017.

[2] C. Shannon. "A Mathematical Theory of Communication".1948

[3] J. Atwood. “Dictionary attack 101”. January 2009.

[4] M. Curry, B. Marshall, R. Crossler, E. Robert, J. Correia. “InfoSec Process Action Model (IPAM): Systematically Addressing Individual Security Behavior”. April 2018.

[5] "Linux Operating Systems: Distributions". swift.siphos.be. 27, November 2014. Archived from the original on 3, October 2018.

[6] "Malware Etymology". Online Etymology Dictionary. Retrieved 17, November 2022.

[7] J. Steube, G. Gristina. “Hashcat”. 21, November 2021.

[8] Oliphant, Patrick. "Virtual Machines". VirtualComputing. Archived from the original on 2016-07-29. Retrieved 23, September 2016.

[9] Greenbone Networks GmbH. “OpenVAS”. 18, June 2022.

[10] M. Corporation. "CVE – Common Vulnerabilities and Exposures". Retrieved 18, June 2009.

[11] R. Rivest. “MD5 message-digest”. April 1992.

[12] Defuse Security. “CrackStation”. 26, May 2019.

[13] M. Ruef. “Vulner NSE”.2018

[14] Hispasec Sistemas. “VirusTotal”. June 2004

[15] National Security Agency. "Secure Hash Algorithm 1". 1995

[16] National Security Agency. "Secure Hash Algorithm 2". 2001

[17] G. Bertoni, J. Daemen, M. Peeters, G. van Assche. "Secure Hash Algorithm 3". 2016