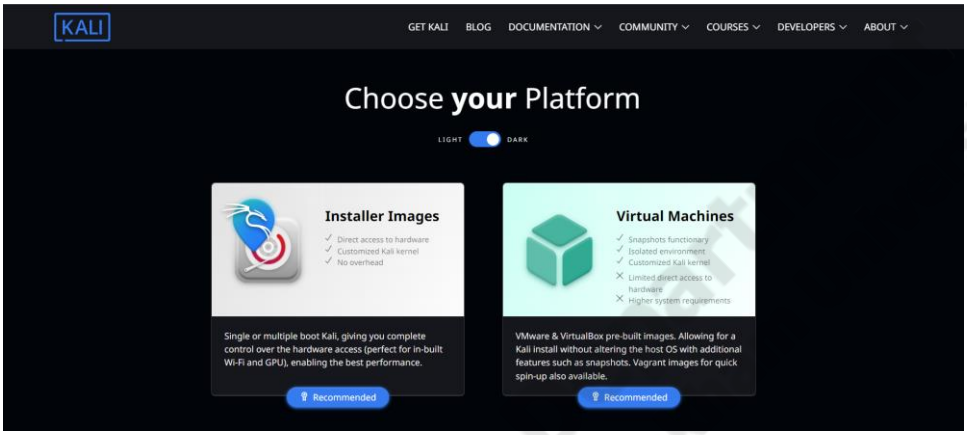
ภาคผนวก

ภาคผนวก ก

คู่มือการติดตั้งเครื่องมือ ISAN Security Gizmo Box

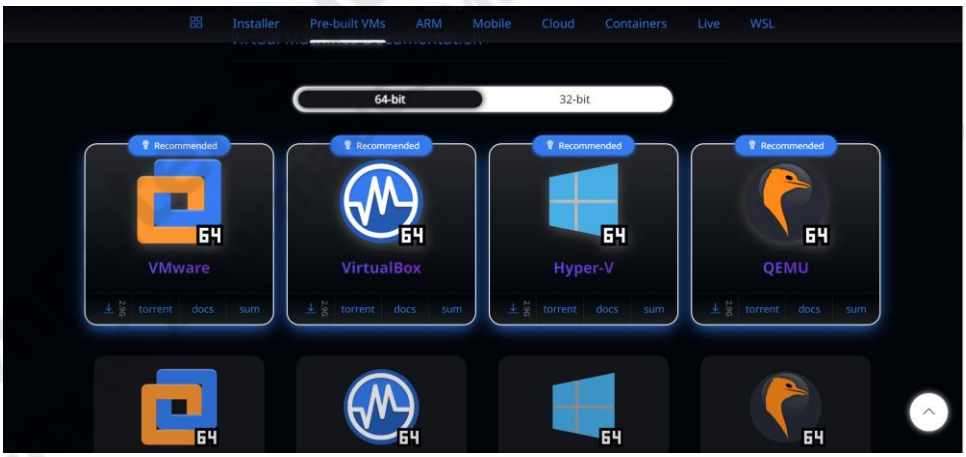
คู่มือการติดตั้งเครื่องมือ ISAN Security Gizmo Box

1) วิธีการติดตั้งแบบ Manual Installation



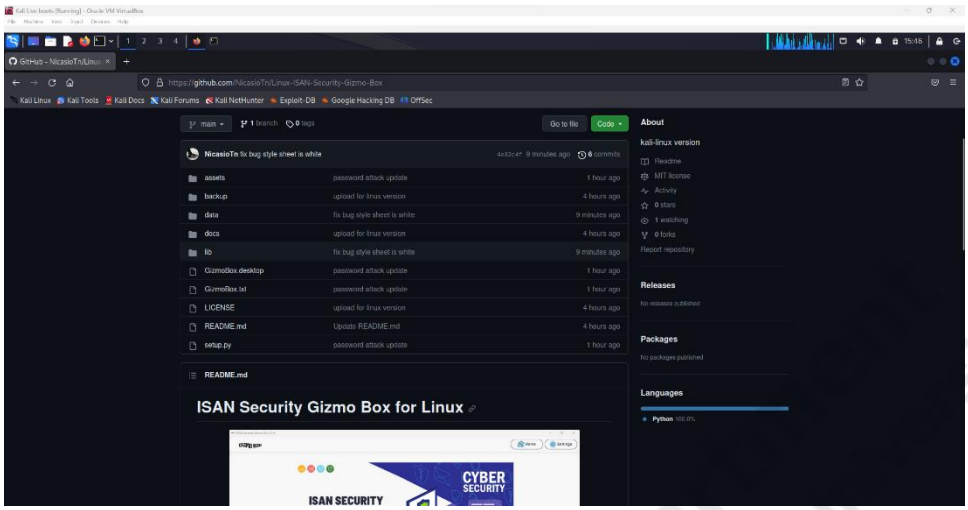
ภาพประกอบที่ ก-1 หน้าเว็บไซต์ของ Kali Linux

เข้าไปที่ https://kali.org/ เพื่อทำการติดตั้ง Kali Linux โดยเลือกเป็น Virtual Machines



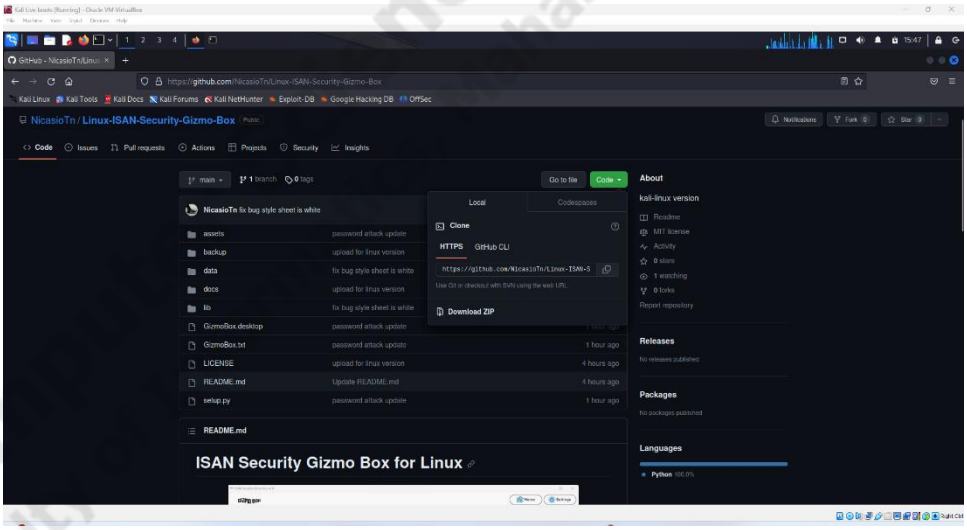
ภาพประกอบที่ ก-2 หน้าดาวน์โหลด Kali Linux

ผู้ใช้งานต้อง Download VM image โดยเครื่องมือ ISAN Security Gizmo Box รูปแบบ Virtual Appliance ของ 2 Virtual Machines คือ Oracle VM VirtualBox และ VMware Workstation Player



ภาพประกอบที่ ก-3 หน้า GitHub Linux-ISAN-Security-Gizmo-Box

เข้าไปที่ https://github.com/NicasioTn/Linux-ISAN-Security-Gizmo-Box/ เพื่อนำ URL สำหรับการติดตั้งเครื่องมือ ISAN Security Gizmo Box

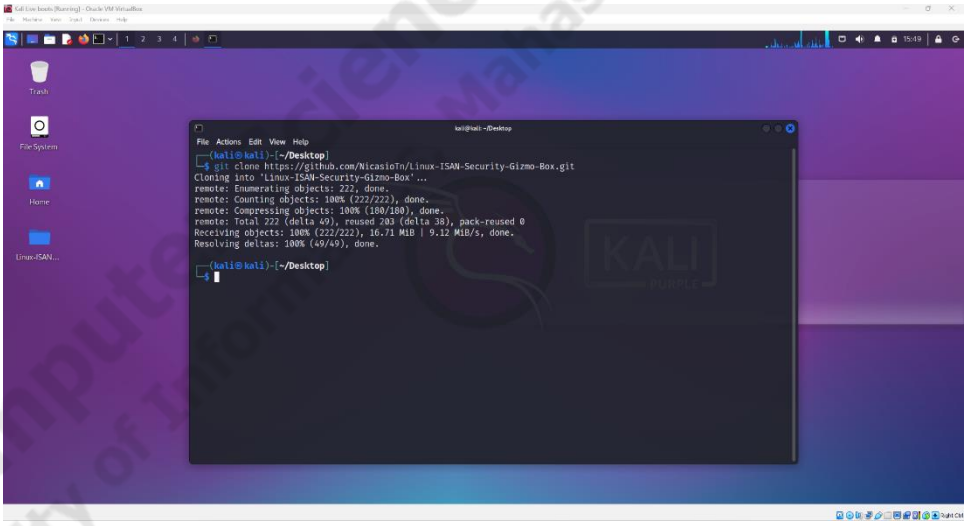


ภาพประกอบที่ ก-4 คัดลอก URL ของ Linux-ISAN-Security-Gizmo-Box

ทำการคัดลอก URL ของ Linux-ISAN-Security-Gizmo-Box ดังภาพ เพื่อนำ URL สำหรับการติดตั้งเครื่องมือ ISAN Security Gizmo Box

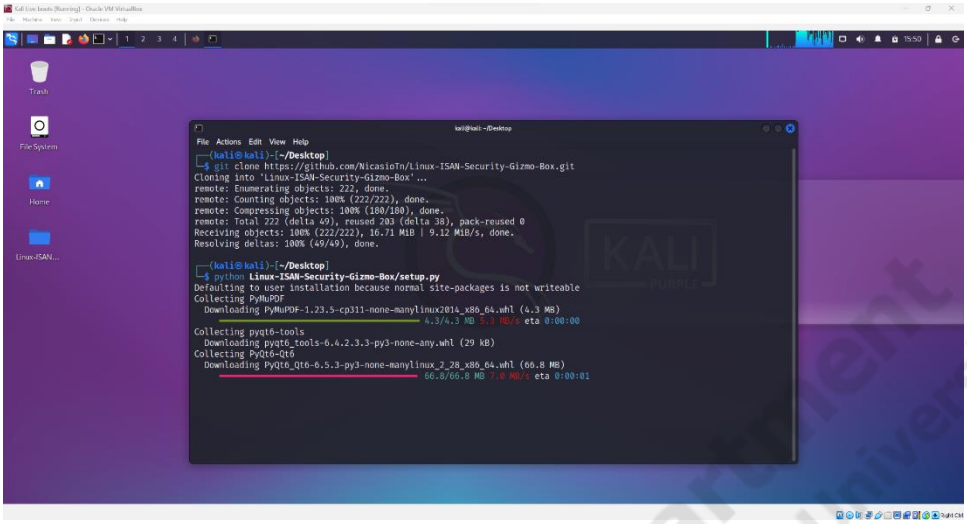
ภาพประกอบที่ ก-5 เปิด Terminal บน Kali Linux

คลิกขวาเพื่อเปิด Terminal โดยคลิกที่ Open Terminal Here สำหรับรันคำสั่งติดตั้งเครื่องมือ ISAN Security Gizmo Box



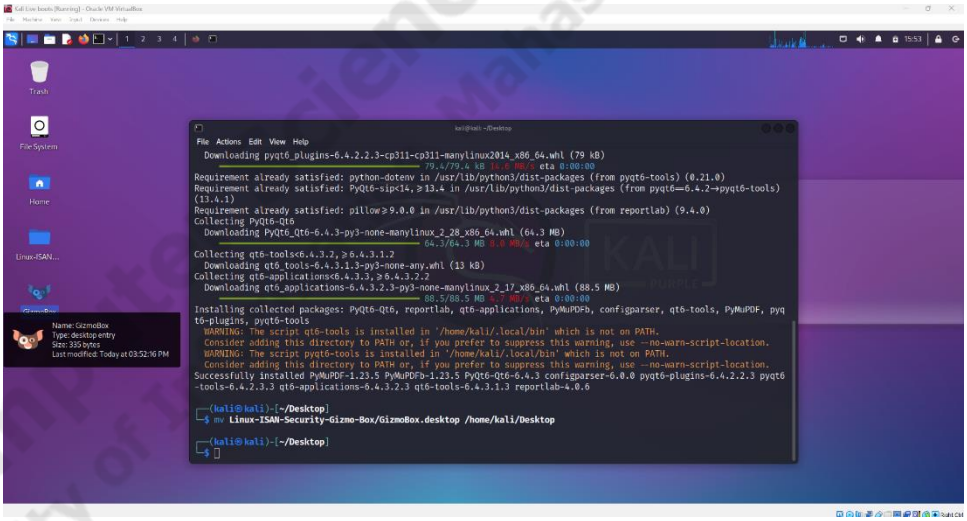
ภาพประกอบที่ ก-6 Git clone Linux-ISAN-Security-Gizmo-Box.git

รันคำสั่ง git clone https://github.com/NicasioTn/Linux-ISAN-Security-Gizmo-Box.git บน Terminal ซึ่งเป็นการดึง source code ตัวล่าสุดจากเซิร์ฟเวอร์มาไว้ในเครื่องของผู้ใช้งาน



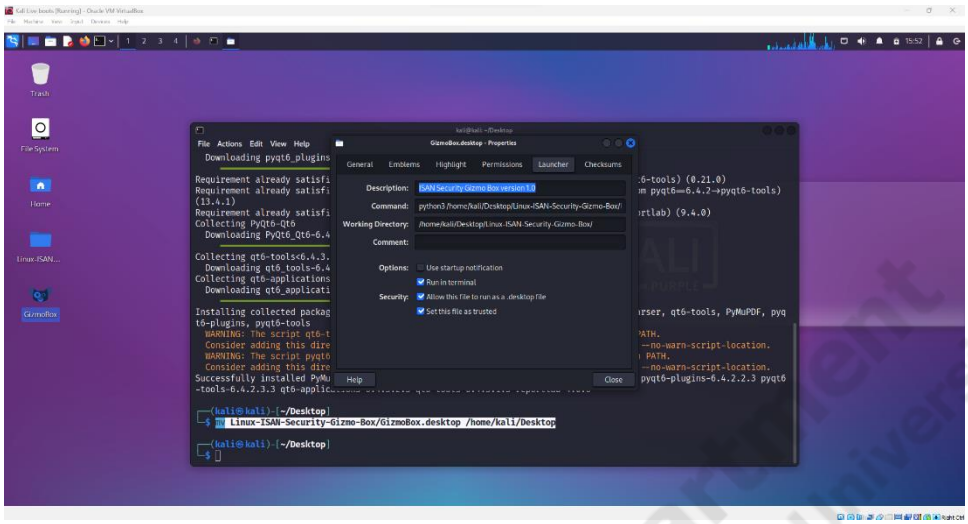
ภาพประกอบที่ ก-7 รันคำสั่ง setup

รันคำสั่ง python Linux-ISAN-Security-Gizmo-Box/setup.py เพื่อลง library ที่จำเป็นต้องใช้ เช่น PyQt6-Qt6, pyqrcode, pyqt6-tools



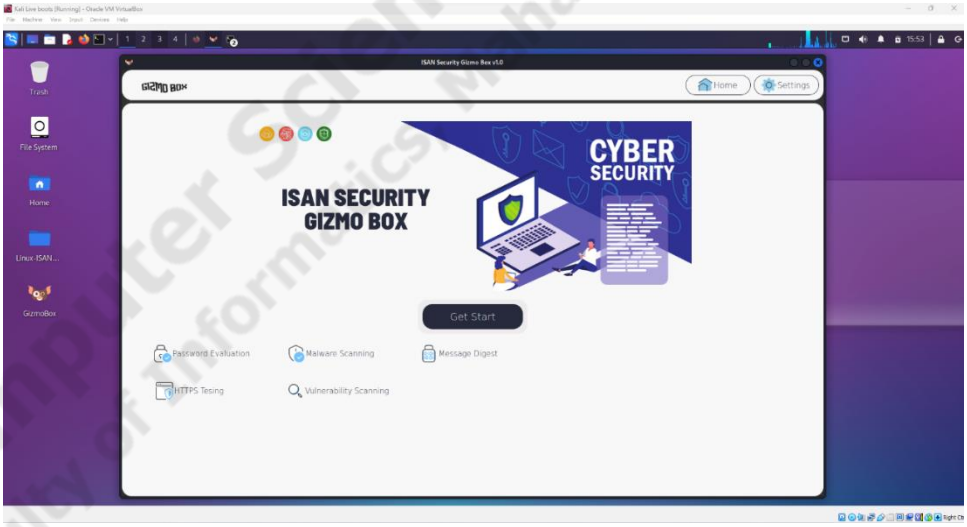
ภาพประกอบที่ ก-8 ย้ายไฟล์ Linux-ISAN-Security-Gizmo-Box

รันคำสั่ง mv Linux-ISAN-Security-Gizmo-Box/setup.py /home/kali/Desktop เพื่อย้ายไฟล์ไปไว้ที่ Desktop ซึ่งจะช่วยให้สะดวกมากขึ้นเมื่อเรียกใช้งานเครื่องมือ ISAN Security Gizmo Box



ภาพประกอบที่ ก-9 ตั้งค่า Security

คลิกขวาที่ไอคอน Gizmo Box เลือกเมนู Properties จากนั้นไปที่หน้า Launcher เลือกที่ช่อง Set This file as trust เพื่อให้ระบบเชื่อถือไฟล์เครื่องมือ ISAN Security Gizmo Box

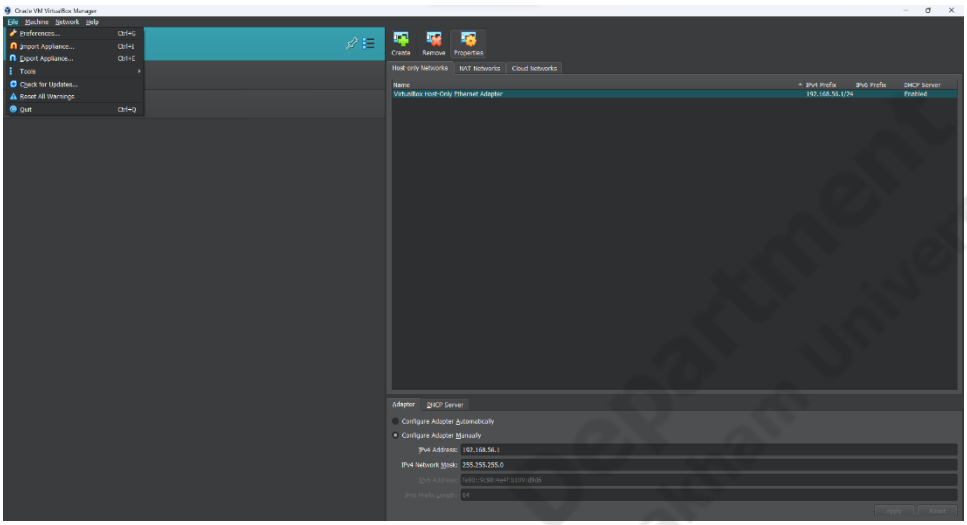


ภาพประกอบที่ ก-10 หน้า ISAN Security Gixmo Box

เสร็จสิ้นการติดตั้งเมื่อเปิดเครื่องมือ ISAN Securtity Gizmo Box จะสามารถใช้งานเครื่องมือได้โดยเลือกตามกลุ่มผู้ใช้งานที่ต้องการ

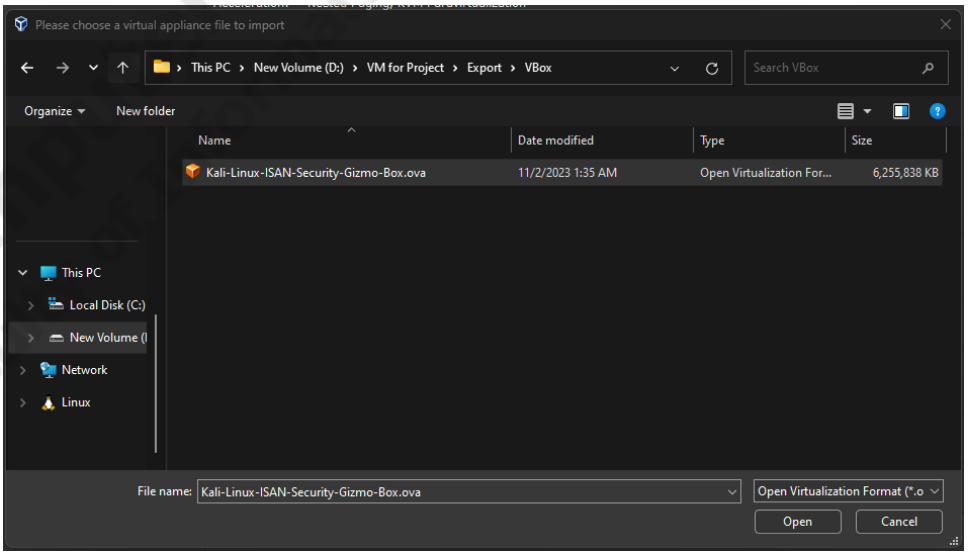
2) วิธีการติดตั้งแบบ Import Virtual Appliances

2.1 Oracle VM VirtualBox



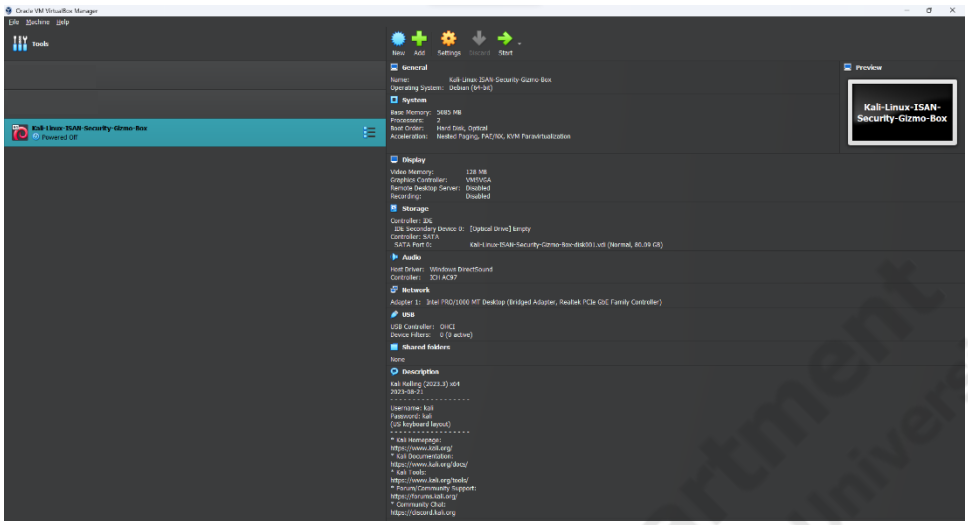
ภาพประกอบที่ ก-11 Import Virtual Appliance สำหรับ Oracle VM VirtualBox

ผู้ใช้งานต้องทำการดาวน์โหลดไฟล์ที่ใช้สำหรับการติดตั้งเครื่องมือ ISAN Security Gizmo Box ที่ ISAN-Security-Gizmo-Box-VBox.zip เมื่อ Unzip จะได้ไฟล์นามสกุล .ova จากนั้นคลิก Import Appliance



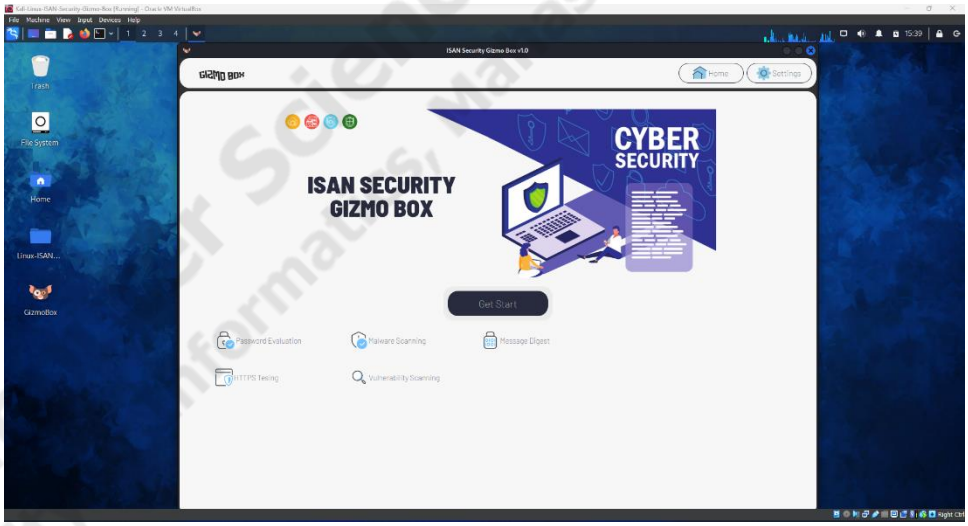
ภาพประกอบที่ ก-12 เลือกไฟล์นามสกุล.ova

เลือกไฟล์ Kali-Linux-ISAN-Security-Gizmo-Box.ova เพื่อใช้ในการ Import เข้ามายัง Oracle VM VirtualBox



ภาพประกอบที่ ก-13 ผลลัพธ์จากการ Import Virtual Appliance

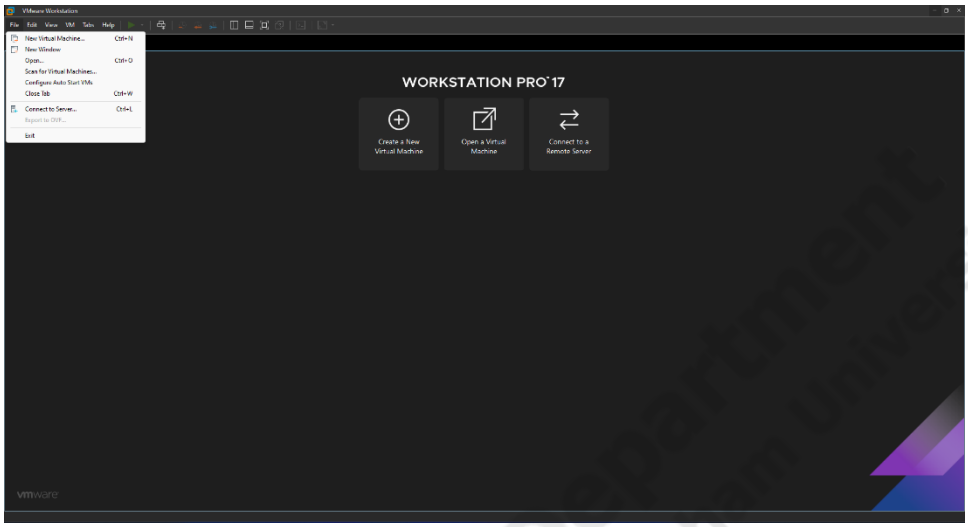
หลังจาก Import สำเร็จจะได้ Kali-Linux-ISAN-Security-Gizmo-Box ที่ Setup เครื่องมือ ISAN Security Gizmo Box ไว้แล้ว



ภาพประกอบที่ ก-14 เครื่องมือ ISAN Security Gizmo Box บน Oracle VM VirtualBox

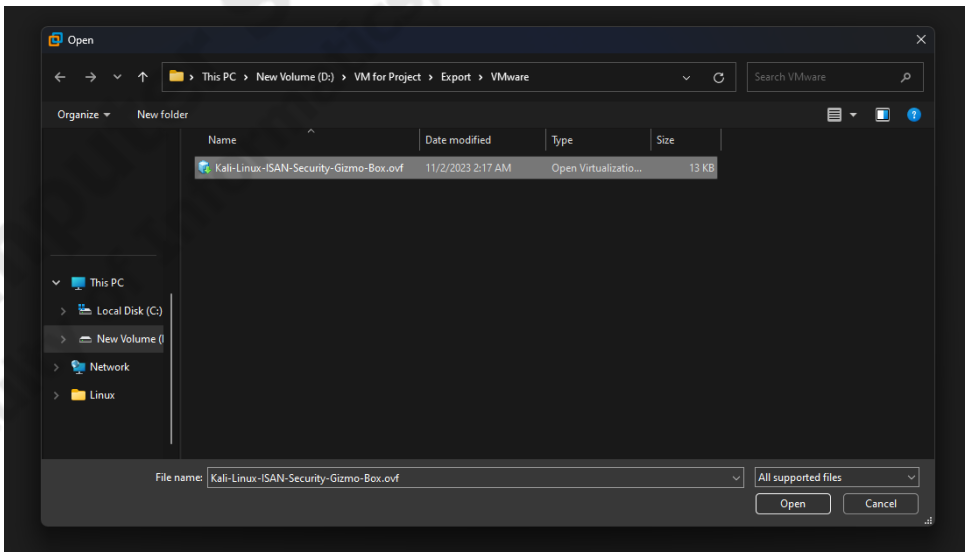
เมื่อเปิด Kali-Linux-ISAN-Security-Gizmo-Box จะเห็นว่ามีเครื่องมือ ISAN Security Gizmo Box และสามารถคลิกที่ไอคอนเพื่อใช้งานเครื่องมือ

2.2) VMware Workstation Player



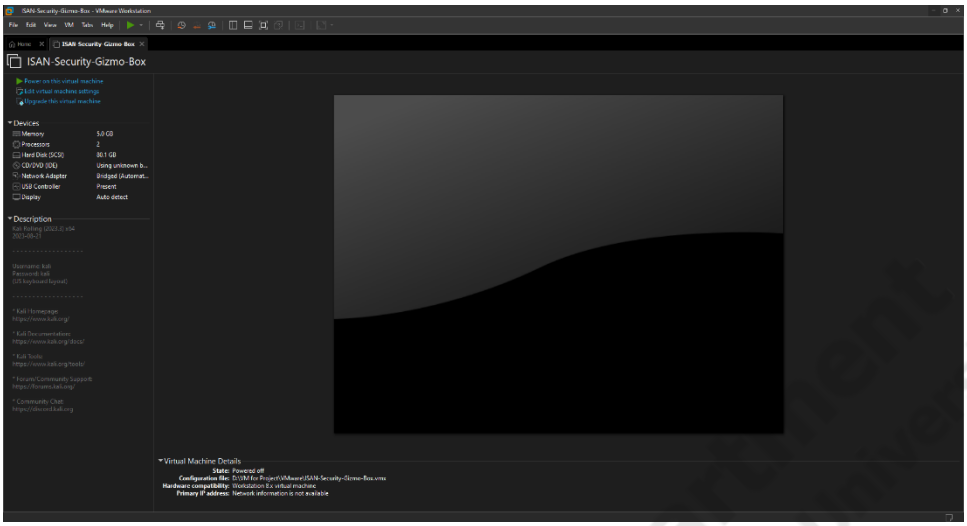
ภาพประกอบที่ ก-15 Import Virtual Appliance สำหรับ VMware Workstation Player

ผู้ใช้งานต้องทำการดาวน์โหลดไฟล์ที่ใช้สำหรับการติดตั้งเครื่องมือ ISAN Security Gizmo Box ที่ ISAN-Security-Gizmo-Box-VMware.zip เมื่อ Unzip จะได้ไฟล์นามสกุล .ova จากนั้นคลิก Open



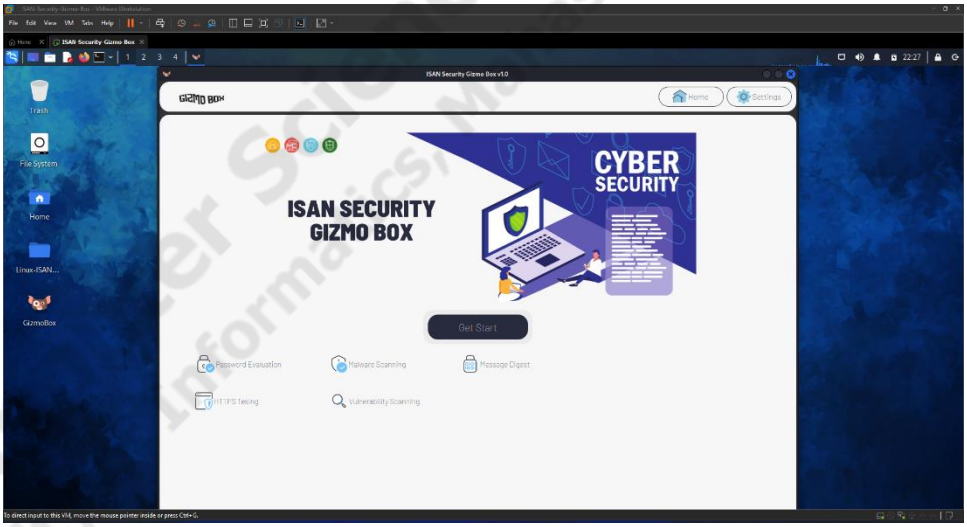
ภาพประกอบที่ ก-16 เลือกไฟล์นามสกุล.ovf

เลือกไฟล์ Kali-Linux-ISAN-Security-Gizmo-Box.ovf เพื่อใช้ในการ Import เข้ามายัง VMware Workstation Player



ภาพประกอบที่ ก-17 ผลลัพธ์จากการ Import Virtual Appliance

หลังจาก Import สำเร็จจะได้ Kali-Linux-ISAN-Security-Gizmo-Box ที่ Setup เครื่องมือ ISAN Security Gizmo Box ไว้แล้ว



ภาพประกอบที่ ก-18 เครื่องมือ ISAN Security Gizmo Box บน VMware Workstation

เมื่อเปิด Kali-Linux-ISAN-Security-Gizmo-Box จะเห็นว่ามีเครื่องมือ ISAN Security Gizmo Box และสามารถคลิกที่ไอคอนเพื่อใช้งานเครื่องมือ

ภาคผนวก ข

คู่มือการใช้งานเครื่องมือ ISAN Security Gizmo Box

คู่มือการใช้งานเครื่องมือ ISAN Security Gizmo Box

ภาพประกอบที่ ข-1 หน้าแรกของเครื่องมือ ISAN Security Gizmo Box

คลิกที่ Get Start เพื่อเริ่มใช้งานเครื่องมือ ISAN Security Gizmo Box โดยแบ่งกลุ่มเครื่องมือออกเป็น 2 กลุ่ม และแต่ละกลุ่มผู้ใช้งานมีเครื่องมือที่แตกต่างกันออกไป

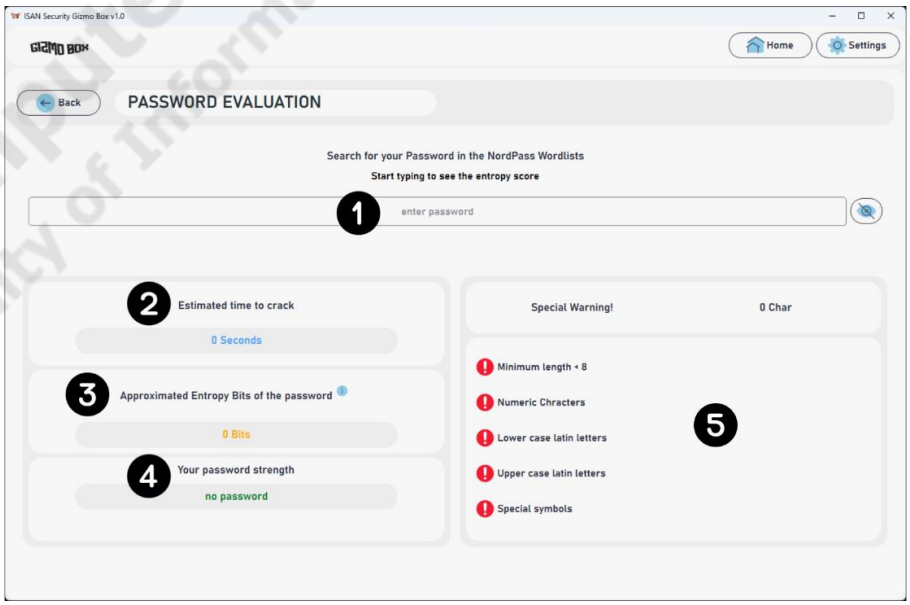
1) เครื่องมือ Password Evaluation

ภาพประกอบที่ ข-2 หน้าเลือกประเภทผู้ใช้งาน

เครื่องมือ Password Evaluation จัดอยู่ในกลุ่มของ Advanced User ดังนั้นคลิกที่ Advanced User เพื่อเข้าใช้งานเครื่องมือ Password Evaluation, Malware Scanning, Message Digest Generator

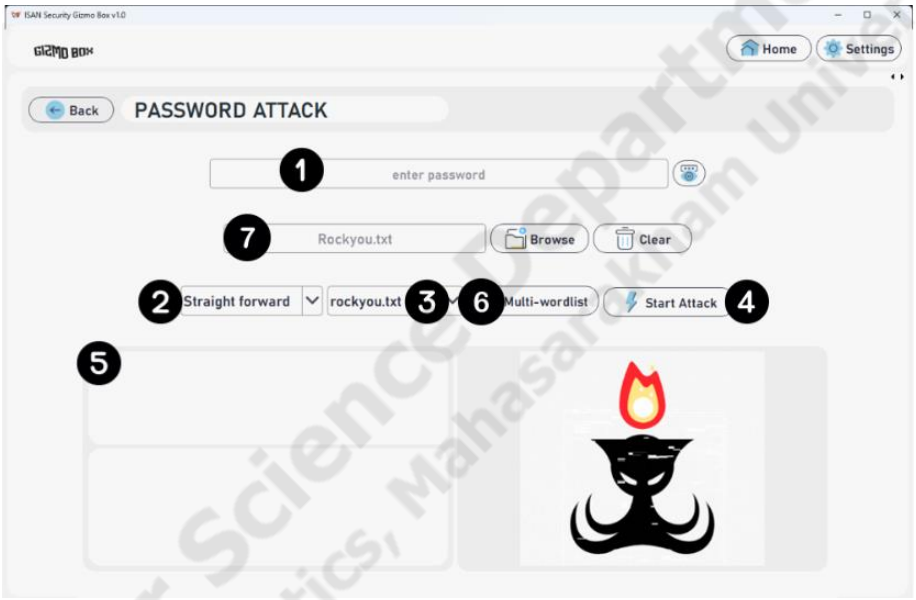
ภาพประกอบที่ ข-3 หน้าเครื่องมือของ Advanced User

คลิกที่ Password Evaluation เพื่อเข้าใช้งานเครื่องมือ โดยเครื่องมือสามารถคำนวณความปลอดภัยและความแข็งแกร่งของรหัสผ่านได้



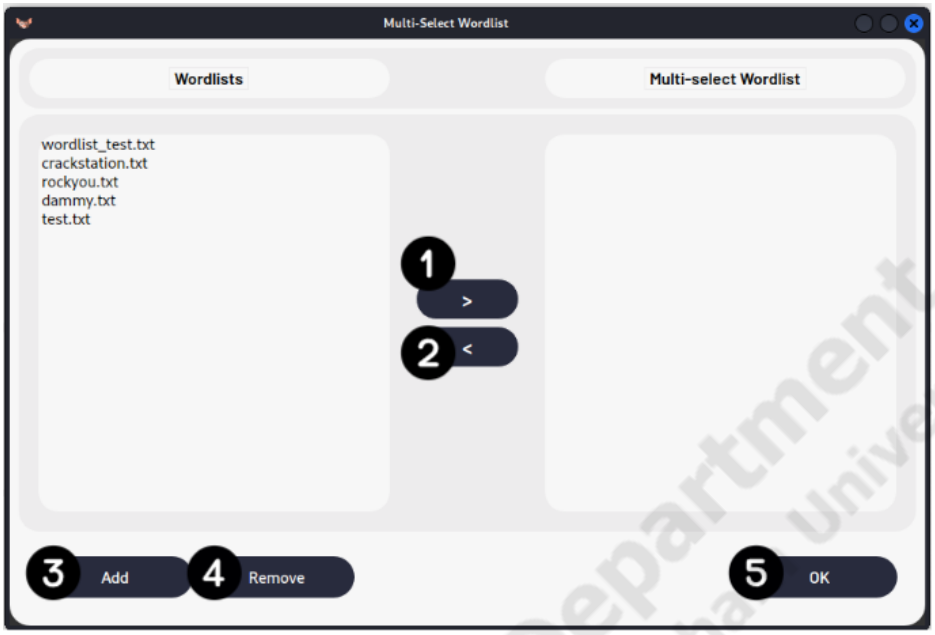
ภาพประกอบที่ ข-4 หน้าเครื่องมือ Password Evaluation

ผู้ใช้งานจะต้องทำการป้อนรหัสผ่าน (หมายเลข 1) เพื่อใช้สำหรับการคำนวณความปลอดภัยและความแข็งแกร่งของรหัสผ่าน ซึ่งผลลัพธ์ที่จะแสดงมีดังนี้ (หมายเลข 2) คือ ผลลัพธ์ Estimated time to crack ระยะเวลาที่คาดว่าจะใช้ในการถอดรหัส (หมายเลข 3) คือ ผลลัพธ์ Bits of entropy หน่วยวัดความแข็งแกร่งของรหัสผ่าน (หมายเลข 4) คือ ผลลัพธ์ข้อมูลเชิงคุณภาพที่คำนวณจาก Bits of entropy (หมายเลข 5) คือ ผลลัพธ์จำนวนอักขระของรหัสผ่านที่ผู้ใช้งานป้อนเข้ามา (หมายเลข 6) คือ ผลลัพธ์องค์ประกอบของรหัสผ่าน



ภาพประกอบที่ ข-5 หน้า Dictionary attack

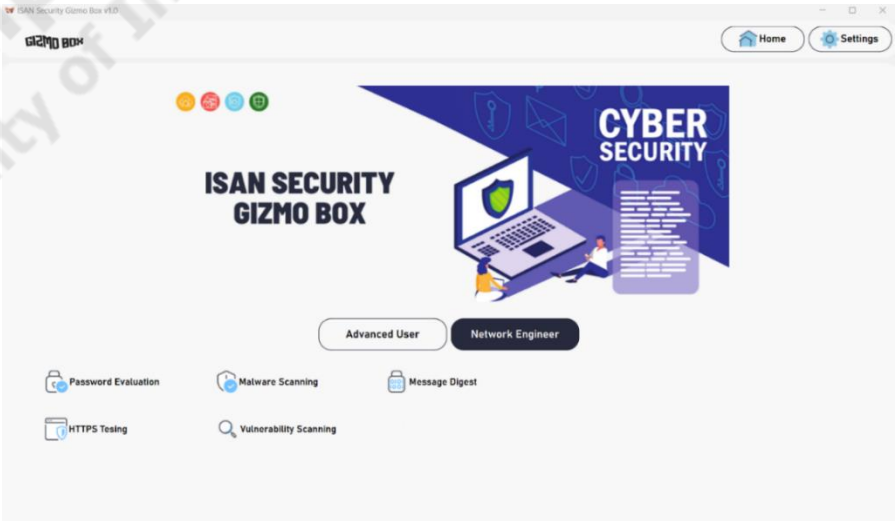
รหัสผ่านที่ผู้ใช้งานป้อนมาก่อนหน้านี้ (หมายเลข 1) ซึ่งในหน้า Password attack จะไม่ทำการแก้ไขรหัสผ่านได้เนื่องจากมีการตรวจสอบความปลอดภัยเบื้องต้นในหน้า Password Evaluation เรียบร้อยแล้ว จากนั้นผู้ใช้งานจะต้องทำการเลือก Mode (หมายเลข 2) และเลือก wordlist (หมายเลข 3) หากผู้ใช้งานไม่ได้เลือกเครื่องมือจะมี Default Mode และ Default wordlist ให้ คลิก Start Attack (หมายเลข 4) เพื่อเริ่มการโจมตีและผลลัพธ์ที่ได้จากการดำเนินการจะแสดงผลที่ (หมายเลข 5) หากผู้ใช้งานต้องการโจมตีมากกว่า 1 wordlist สามารถเลือก (หมายเลข 6) หรือผู้ใช้งานมี wordlist สามารถเพิ่มเข้ามาในเครื่องมือได้ (หมายเลข 7)



ภาพประกอบที่ ข-6 หน้า Multi-wordlist

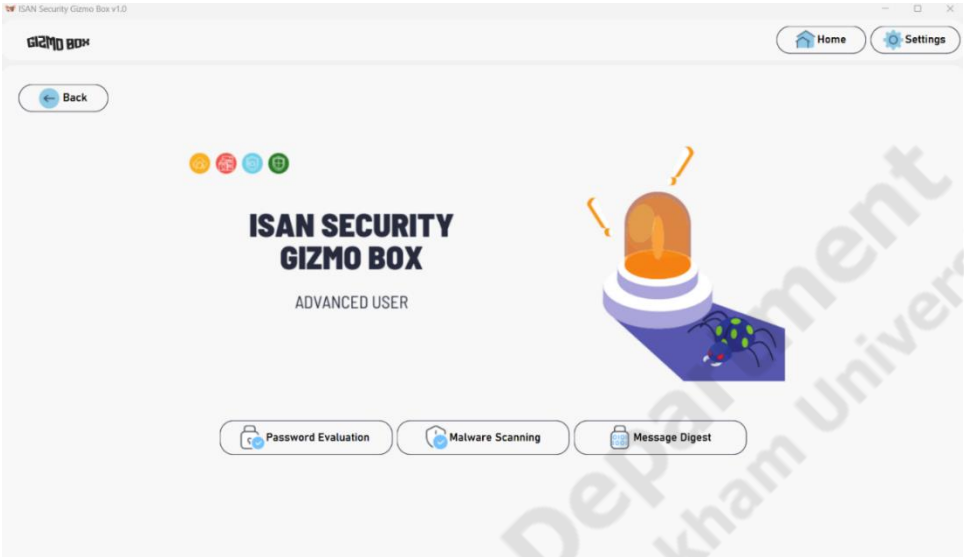
เมื่อเลือก Multi-wordlist ในหน้า Password attack จะเปิดหน้านี้ขึ้นมา Default wordlist จะอยู่ด้านซ้ายมือ คลิกที่ชื่อ wordlist ที่ต้องการแล้วคลิก (หมายเลข 1) เพื่อเพิ่ม wordlist ไปไว้ด้านขวามือหากไม่ต้องการ wordlist ใด ๆ คลิกที่ (หมายเลข 2) เพื่อเอา wordlist ออก นอกจากนี้ผู้ใช้งานสามารถเพิ่ม wordlist ได้โดยคลิก (หมายเลข 3) และลบออกได้เมื่อคลิก (หมายเลข 4) แต่จะไม่สามารถลบ Default wordlist ได้หลังจากนั้นคลิก OK (หมายเลข 5) เพื่อทำการยืนยันการตั้งค่าดังกล่าว

2) เครื่องมือ Malware Scanning



ภาพประกอบที่ ข-7 หน้าเลือกประเภทผู้ใช้งาน

เครื่องมือ Malware Scanning จัดอยู่ในกลุ่มของ Advanced User ดังนั้นคลิกที่ Advanced User



ภาพประกอบที่ ข-8 หน้าเครื่องมือของ Advanced User

คลิกที่ Malware Scanning เพื่อเข้าใช้งานเครื่องมือโดยเครื่องมือสามารถตรวจสอบไฟล์และ URL ของเว็บไซต์เพื่อหามัลแวร์ได้

ภาพประกอบที่ ข-9 เครื่องมือ Malware Scanning

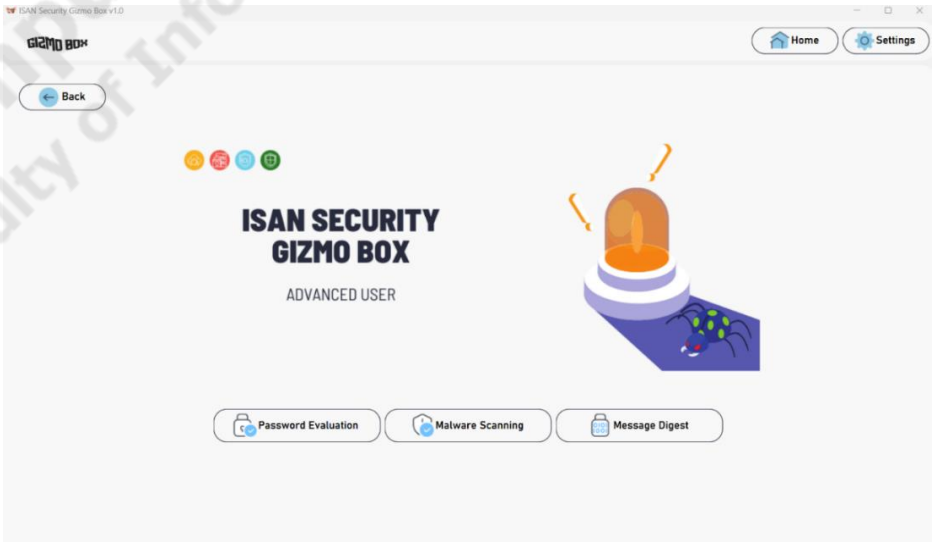
ผู้ใช้งานจะต้องทำการป้อนไฟล์หรือ URL ของเว็บไซต์ (หมายเลข 1) เพื่อใช้สำหรับการสแกนหามัลแวร์ จากนั้นกดที่ (หมายเลข 2) เพื่อทำการสแกน โดยผลลัพธ์ที่ได้ (หมายเลข 3) แสดงภาพกราฟิก

(หมายเลข 4) แสดงภาพรวมของผลลัพธ์ที่ได้จากการสแกน (หมายเลข 5) แสดงรายละเอียดของไฟลหรือ URL ของเว็บไซต์ที่ผู้ใช้งานป้อนเข้ามา และ (หมายเลข 6) สร้างรายงานผลลัพธ์ในรูปแบบไฟล์ PDF

3) เครื่องมือ Message Digest Generator

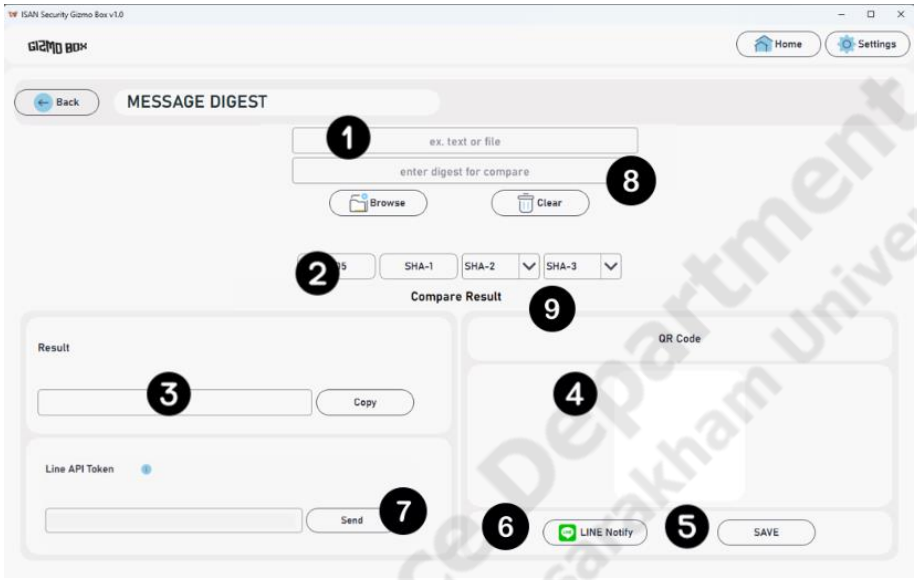
ภาพประกอบที่ ข-10 หน้าเลือกประเภทผู้ใช้งาน

เครื่องมือ Message digest Generator จัดอยู่ในกลุ่มของ Advanced User ดังนั้นคลิกที่ Advanced User



ภาพประกอบที่ ข-11 หน้าเครื่องมือของ Advanced User

คลิกที่ Message Digest Generator เพื่อเข้าใช้งานเครื่องมือ โดยเครื่องมือ Message Digest Generator แฮชข้อความหรือไฟล์



ภาพประกอบที่ ข-12 หน้าเครื่องมือ Message digest Generator

ผู้ใช้งานจะต้องการการป้อนข้อความหรือไฟล์ (หมายเลข 1) เพื่อทำการแฮช จากนั้นทำการเลือกฟังก์ชันที่การใช้ในการแฮช (หมายเลข 2) โดยผลลัพธ์ที่ได้จะแสดงในรูปแบบข้อความ (หมายเลข 3) และ QR Code (หมายเลข 4) หากผู้ใช้งานต้องการบันทึกรูปภาพ QR Code สามารถคลิกที่ (หมายเลข 5) และหากต้องการส่ง Line Notify สามารถคลิกที่ (หมายเลข 6) โดยจะต้องมี Line API Token จึงจะสามารถคลิก (หมายเลข 7) เพื่อส่งผลลัพธ์ได้ นอกจากนี้ผู้ใช้งานยังสามารถเพิ่มค่าแอชเพื่อทำการปรียบเทียบกับผลลัพธ์ได้ว่าตรงกันหรือไม่ (หมายเลข 8) โดยผลลัพธ์จะแสดงที่ (หมายเลข 9)

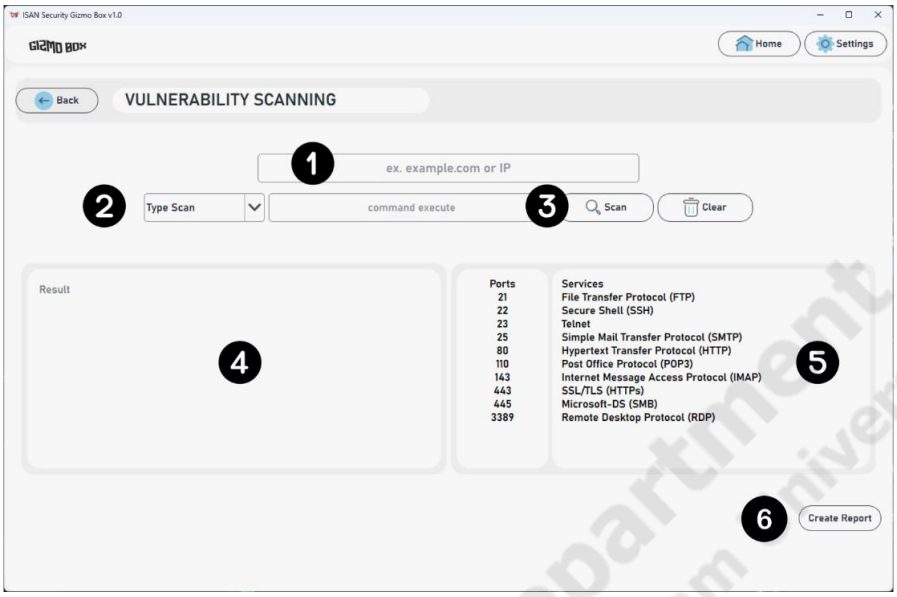
4) เครื่องมือ Vulnerability Scanning

ภาพประกอบที่ ข-13 หน้าเลือกประเภทผู้ใช้งาน

เครื่องมือ Vulnerability Scanning จัดอยู่ในกลุ่มของ Advanced User ดังนั้นคลิกที่ Advanced User

ภาพประกอบที่ ข-14 หน้าเครื่องมือของ Network Engineer

คลิกที่ Vulnerability Scanning เพื่อเข้าใช้งานเครื่องมือเพื่อใช้ในการสแกนหาข้อมูลช่องโหว่



ภาพประกอบที่ ข-15 หน้าเครื่องมือ Vulnerability Scanning

ผู้ใช้งานจะต้องป้อนโดเมนเนมหรือ IP address (หมายเลข 1) เพื่อทำการสแกนหาช่องโหว่ โดยผู้ใช้งานสามารถเลือกประเภทการสแกนได้ที่ (หมายเลข 2) จากนั้นคลิกที่ (หมายเลข 3) เพื่อทำการสแกน ผลลัพธ์ที่ได้จะแสดงที่ (หมายเลข 4) ในส่วนของ (หมายเลข 5) จะแสดงพอร์ตพื้นฐานที่ไม่ควรเปิด และ (หมายเลข 6) สร้างรายงานผลลัพธ์ในรูปแบบไฟล์ PDF

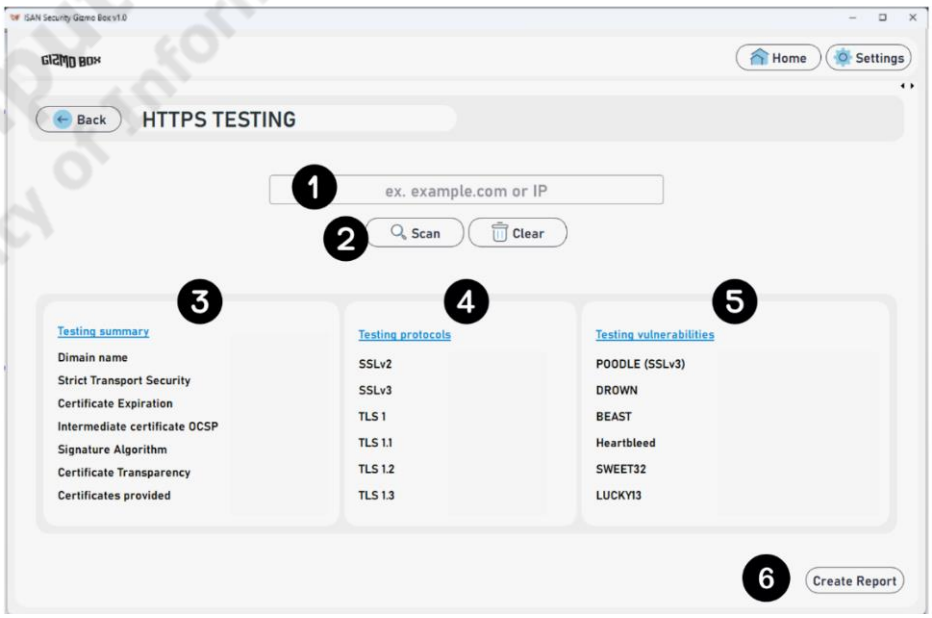
5) เครื่องมือ HTTPS Testing

ภาพประกอบที่ ข-16 หน้าเลือกประเภทผู้ใช้งาน

เครื่องมือ HTTPS Testing จัดอยู่ในกลุ่มของ Network Engineer ดังนั้นคลิกที่ Network Engineer

ภาพประกอบที่ ข-17 หน้าเครื่องมือของ Network Engineer

คลิกที่ HTTPS Testing เพื่อเข้าใช้งานเครื่องมือโดยสามารถใช้สำหรับการตรวจสอบความปลอดภัยและการตั้งค่า Preload



ภาพประกอบที่ ข-18 หน้าเครื่องมือ HTTPS Testing

ผู้ใช้งานจะต้องทำการป้อนโดเมนเนมหรือ IP address (หมายเลข 1) เพื่อทำการตรวจสอบ HTTPS Testing จากนั้นคลิกที่ (หมายเลข 2) เพื่อทำการสแกนโดยผลลัพธ์ Testing summary จะแสดงที่ (หมายเลข 3) ผลลัพธ์ Testing protocols จะแสดงที่ (หมายเลข 4) ผลลัพธ์ Testing vulnerabilities จะแสดงที่ (หมายเลข 5) และ (หมายเลข 6) สร้างรายงานผลลัพธ์ในรูปแบบไฟล์ PDF

ภาพประกอบที่ ข-19 หน้าสร้างรายงานและส่งอีเมล

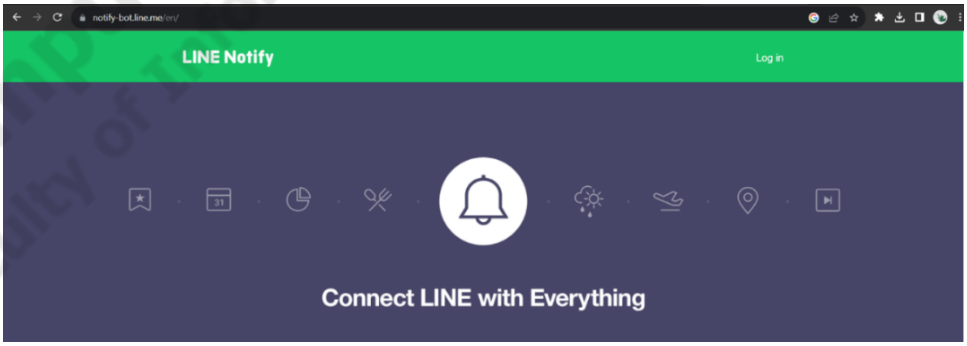
รายละเอียดรายงานผลลัพธ์ที่อยู่ในรูปแบบของ PDF (หมายเลข 1) หากผู้ใช้งานต้องการส่งรายงานผลลัพธ์ที่อยู่ในรูปแบบ PDF ไปยังอีเมลต้องทำการกรอกที่อยู่อีเมล (หมายเลข 2) หัวข้ออีเมล (หมายเลข 3) เนื้อหาของอีเมล (หมายเลข 4) ไฟล์รายงาน (หมายเลข 5) โดยแต่ละเครื่องมือจะแนบไฟล์ผลลัพธ์มาให้แล้วไม่สามารถแก้ไขได้ จากนั้นสามารถคลิกส่งอีเมลได้ (หมายเลข 6)

6) หน้าตั้งค่าระบบ

ภาพประกอบที่ ข-20 หน้าตั้งค่าระบบ

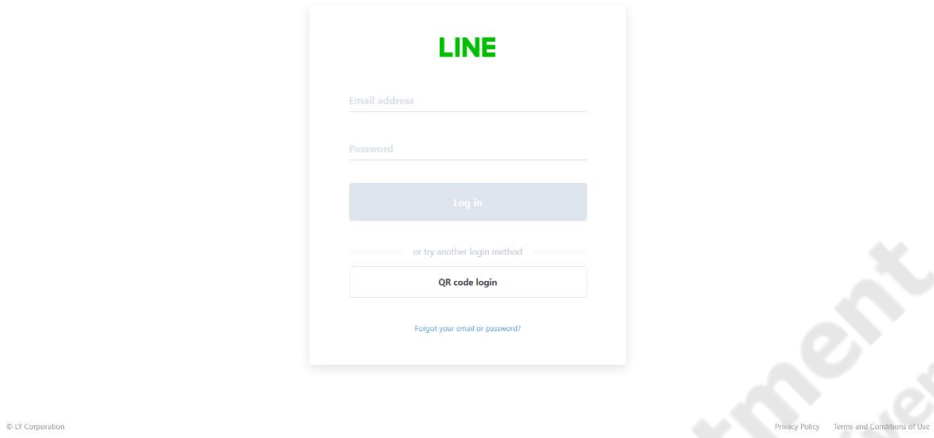
ตั้งค่าการแจ้งเตือน (หมายเลข 1) ตั้งค่าภาษา (หมายเลข 2) ตั้งค่าเสียง (หมายเลข 3) ตั้งค่า Line API Token (หมายเลข 4) ตั้งค่า VirusTotal API (หมายเลข 5) ตั้งค่าธีม (หมายเลข 6) บันทึกการเปลี่ยนแปลงการตั้งค่า (หมายเลข 7)

7) การขอ LINE API Token



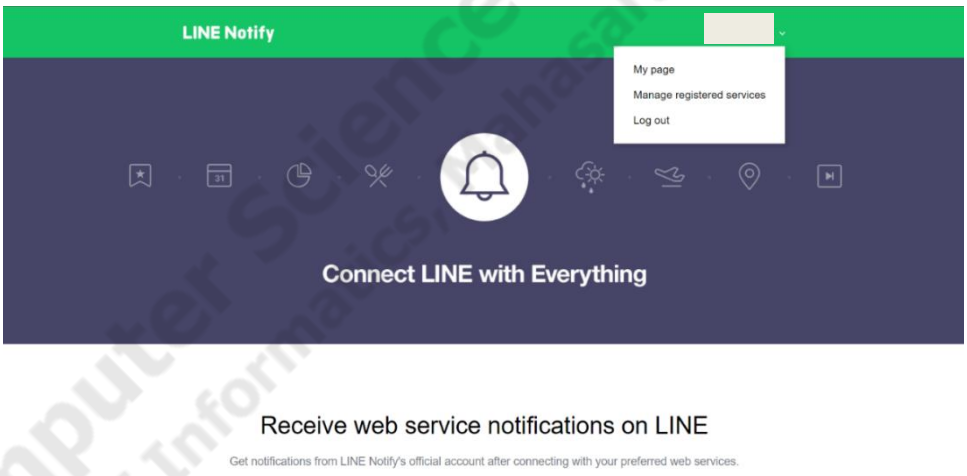
ภาพประกอบที่ ข-21 หน้าแรกของ Line Notify

ไปที่หน้า LINE Notify https://notify-bot.line.me/en/ เพื่อทำการขอ Line API Token สำหรับ Line Notify



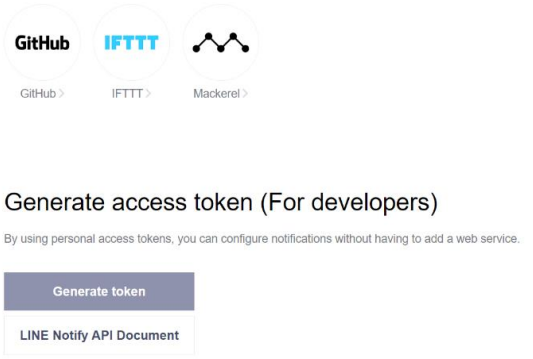
ภาพประกอบที่ ข-22 หน้าเข้าสู่ระบบ

คลิก Log in เพื่อเข้าสู่ระบบสำหรับดำเนินการของ Line API Token โดยผู้ใช้งานที่มีบัญชี Line อยู่แล้วสามารถเข้าสู่ระบบโดยมี 2 วิธี คือ เข้าสูทระบบผ่านอีเมลหรือเข้าสู่ระบบผ่าน QR Code



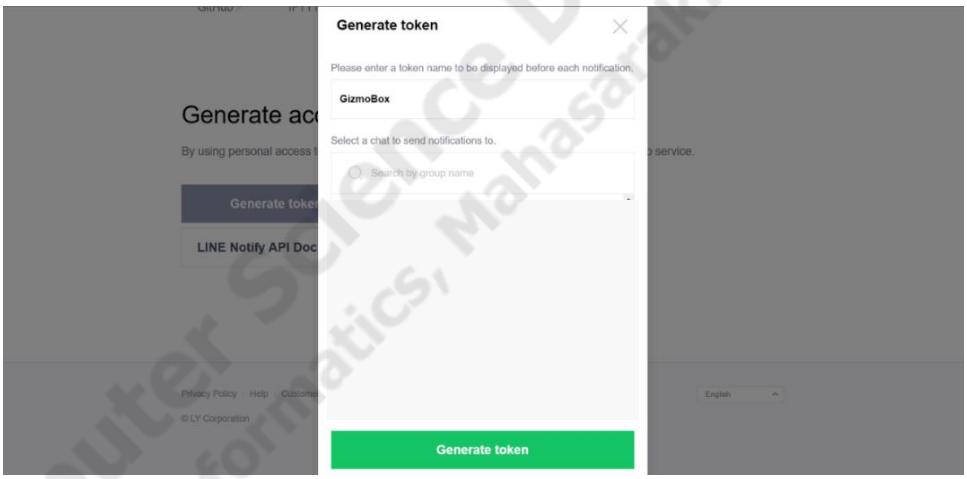
ภาพประกอบที่ ข-23 หน้าหลัง Line Notify

เมื่อเข้าสู่ระบบแล้วคลิกที่ My Page ด้านบนขวา เพื่อเข้าไปยังหน้าที่ใช้สำหรับสร้าง Line API Token ที่จะนำไปใช้กับเครื่องมือ ISAN Security Gizmo Box



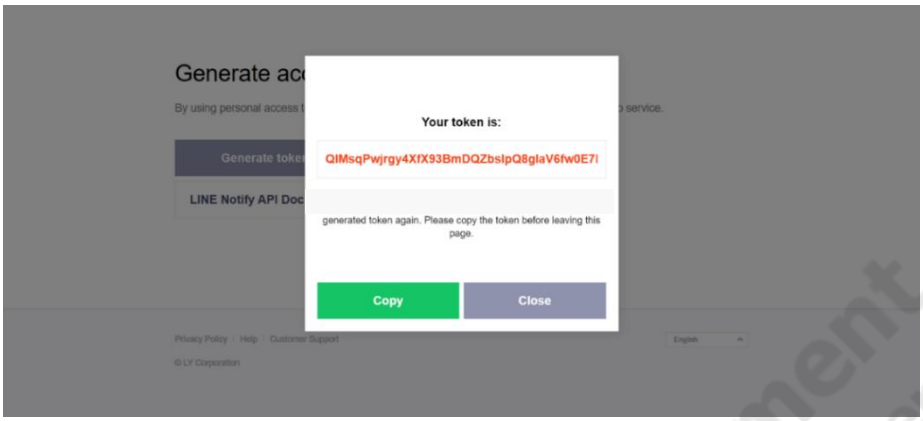
ภาพประกอบที่ ข-24 หน้า Generate Token

ในหน้า My Page คลิกที่ Generate Token เพื่อทำการสร้าง Line API Token ที่จะนำไปใช้กับเครื่องมือ ISAN Security Gizmo Box



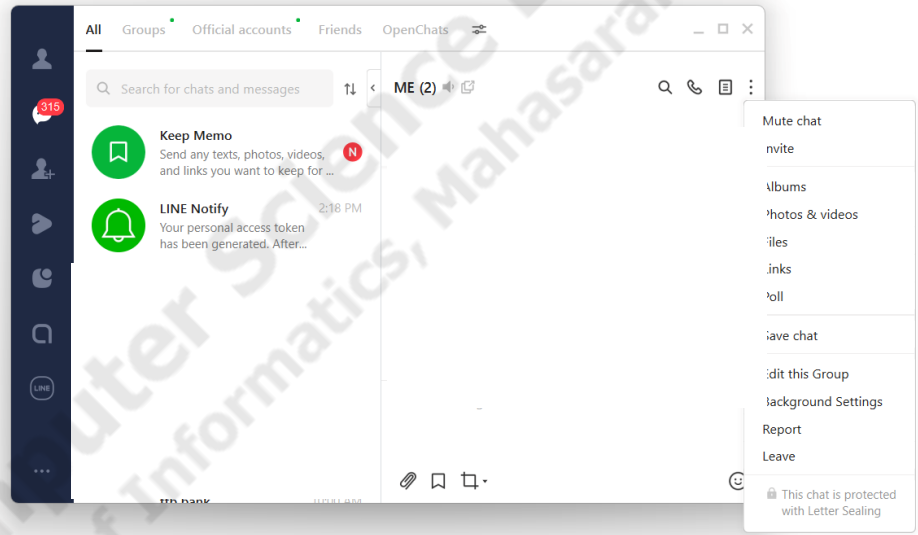
ภาพประกอบที่ ข-25 หน้าตั้งชื่อ Token

ในหน้า Generate Token จะต้องตั้งชื่อ Token และคลิก Generate Token เพื่อที่จะนำไปใช้กับเครื่องมือ ISAN Security Gizmo Box



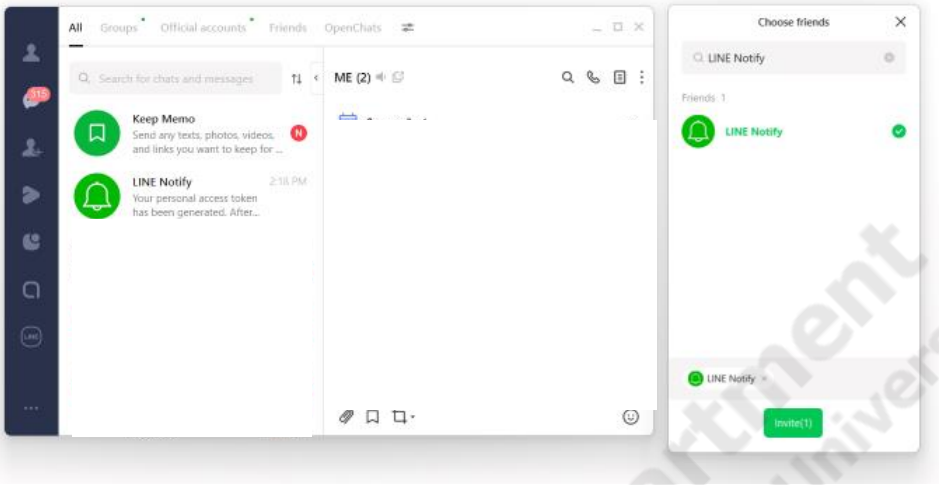
ภาพประกอบที่ ข-26 หน้า Token

หลังจากการสร้าง Token เสร็จสิ้นจะได้รับ Token ใหม่ที่สามารถใช้ในการส่งข้อความแจ้งเตือนผ่าน Line Notify



ภาพประกอบที่ ข-27 หน้ากลุ่ม Line

คลิกไอคอนสามจุดด้านบนขวาเพื่อเพิ่ม Line Notify เข้ากลุ่มโดยผู้ใช้งานเลือกกลุ่มที่ตนเองต้องการเพิ่ม Line Notify เข้าไป



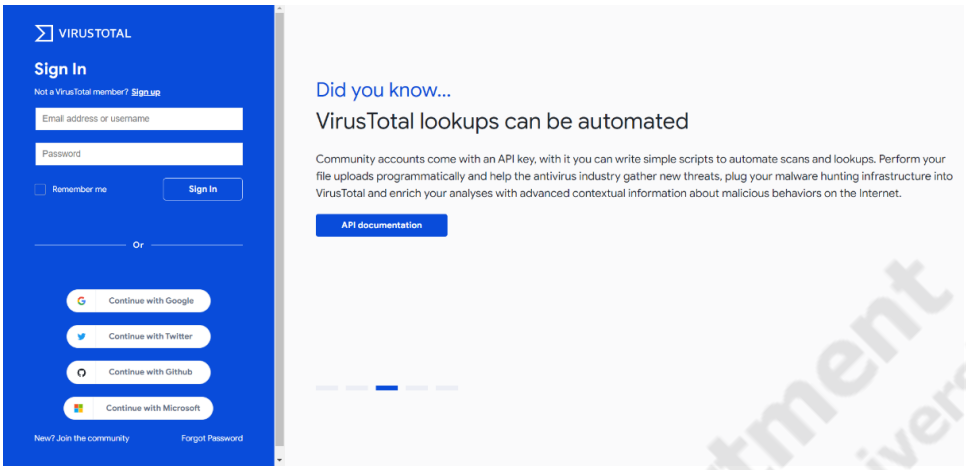
ภาพประกอบที่ ข-28 หน้าเพิ่ม Line Notify เข้ากลุ่ม

เลือก LINE Notify จากนั้นคลิก Invite เพื่อเพิ่ม Line Notify เข้ากลุ่ม และเมื่อใช้งานเครื่องมือ Message Digest Generator จะสามารถใช้งานฟังก์ชัน Line Notify ได้

8) การขอ VirusTotal API

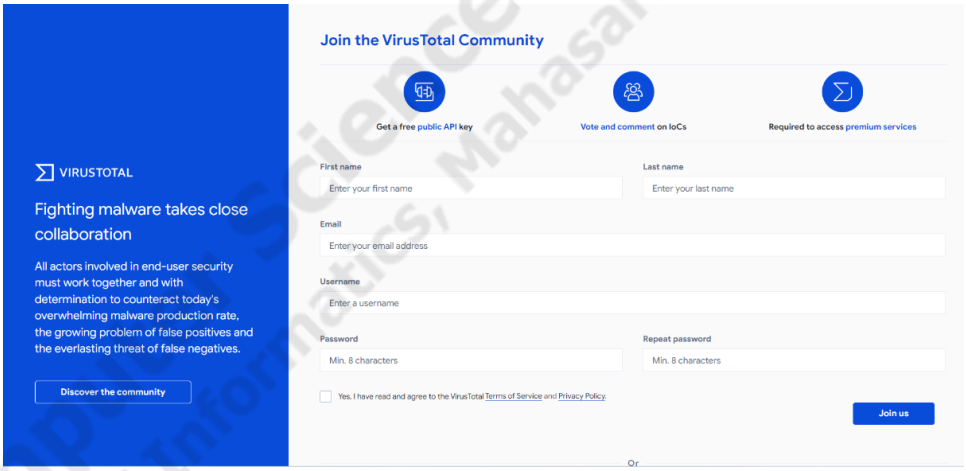
ภาพประกอบที่ ข-29 หน้าเว็บไซต์ VirusTotal

ไปที่เว็บไซต์ของ VirusTotal https://www.virustotal.com/ เพื่อทำการขอ VirusTotal API Token สำหรับนำมาใช้เครื่องมือ Malware Scanning



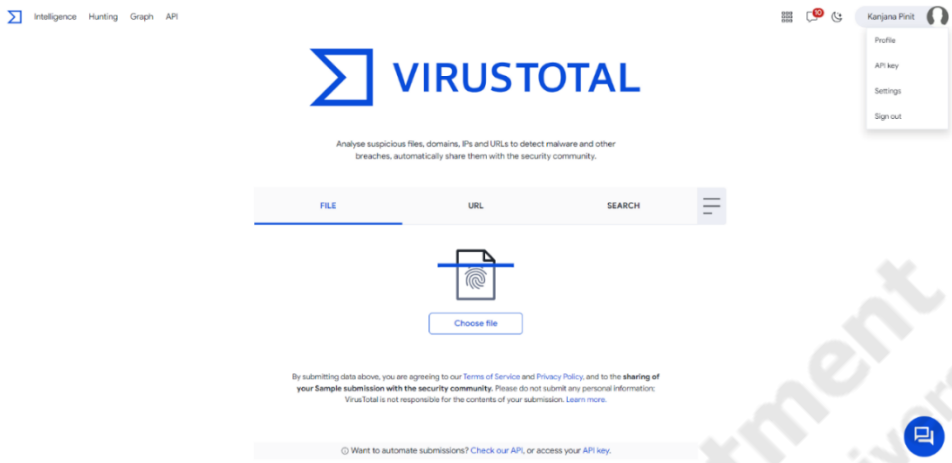
ภาพประกอบที่ ข-30 หน้าเข้าสู่ระบบของ VirusTotal

คลิกที่ Sign in หรือ Sign up เพื่อสร้างบัญชีหรือเข้าสู่ระบบเพื่อไปคัดลอกเอา VirusTotal API Token



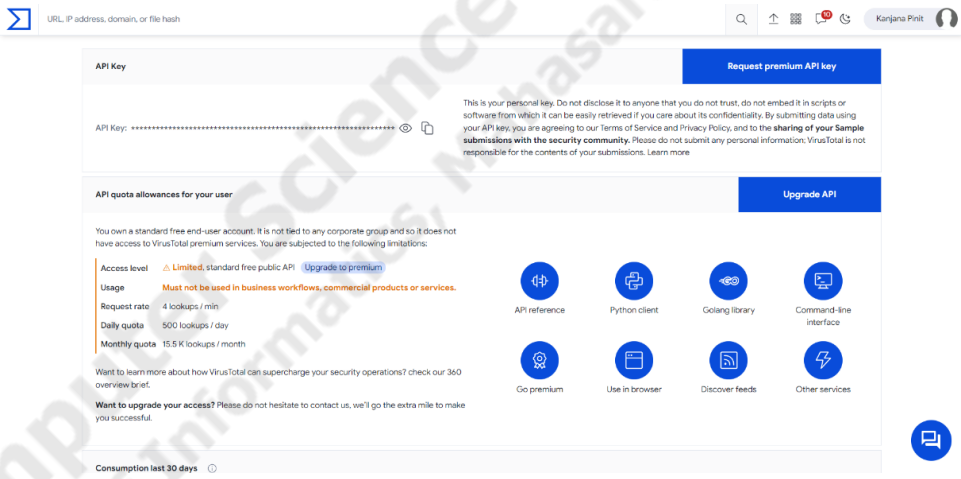
ภาพประกอบที่ ข-31 หน้าสมัครสมาชิกของ VirusTotal

(กรณียังไม่มีบัญชี VirusTotal) ในหน้าลงทะเบียน กรอกข้อมูลที่จำเป็นและ คลิกที่ "I accept the VirusTotal terms of service and privacy policy" เพื่อยอมรับข้อกำหนดและนโยบายความเป็นส่วนตัวของ VirusTotal หลังจากลงทะเบียนสำเร็จสามารถเข้าสู่ระบบด้วยชื่อผู้ใช้และรหัสผ่านที่สร้างขึ้น



ภาพประกอบที่ ข-32 หน้าขอ API VirusTotal

เมื่อเข้าสู่ระบบหรือสร้างบัญชีเสร็จแล้วจะเห็นเมนูด้านบนของหน้าเว็บ VirusTotal คลิกที่ My API key หรือ API Key (ขึ้นอยู่กับเวอร์ชันปัจจุบันของ VirusTotal)



ภาพประกอบที่ ข-33 หน้า API VirusTotal

จะได้รับ API key และข้อมูลอื่น ๆ ในหน้า API Key ซึ่งสามารถใช้ในการเชื่อมต่อกับ API ของ VirusTotal ได้