บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 งานวิจัยและทฤษฎีที่เกี่ยวข้อง

2.1.1 Bit of Entropy

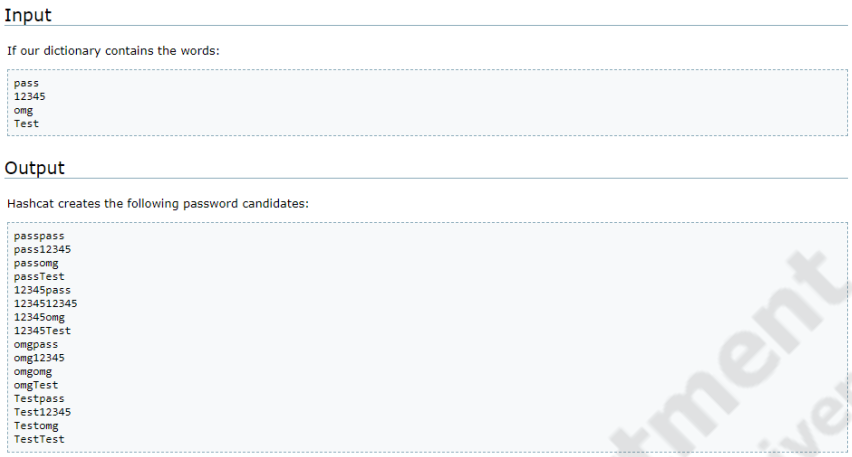
Bit of entropy คือ หน่วยวัดความแข็งแกร่งของรหัสผ่าน ซึ่ง Entropy [2] คำนวณได้จากสูตร E = L*log2(P) ซึ่ง L คือ ความยาวของรหัสผ่าน (Length) และ P คือ ขนาดของกลุ่มอักษรเฉพาะ (Pool of Characters) ที่ใช้สร้างรหัสผ่านจำนวนของค่าได้จะมีความแปรปรวนเป็นอย่างมากจนไม่สามารถคาดเดาได้และเป็นหนึ่งในมาตรการที่ใช้กันโดยทั่วไป

2.1.2 Dictionary attack

Dictionary Attack [3] คือการโจมตีความมั่นคงปลอดภัยทางไซเบอร์ประเภทหนึ่งที่เกี่ยวข้องกับการใช้รายการคำ วลี หรือสตริงอักขระอื่นๆ ที่กำหนดไว้ล่วงหน้าเป็นพื้นฐานในการพยายามเดารหัสผ่าน การโจมตีทำงานโดยลองใช้แต่ละคำในรายการทีละคำจนกว่าจะพบรหัสผ่านที่ถูกต้อง การโจมตีด้วย Dictionary มักใช้ร่วมกับการโจมตีประเภทอื่นๆ เช่น Brute-force attack เพื่อเพิ่มโอกาสในการประสบความสำเร็จลักษณะสำคัญอย่างหนึ่งของ Dictionary attack คือรายการคำที่ใช้มักจะปรับให้เหมาะกับเป้าหมายเฉพาะที่ถูกโจมตี Burt-force attack

2.1.3 Combinator attack

Combinator attack เป็นอีกหนึ่งในวิธีย่อยของ Skipping attack โดย Combinator มีการสร้าง Dictionary เพิ่มโดยเป็นการผสมหรือนำรหัสผ่านมาต่อกันเป็นรหัสผ่านใหม่เพื่อเพิ่มความเป็นไปได้ที่จะโจมตีสำเร็จโดยการใช้ Dictionary attack ในรูปแบบ Combination wordlist



Input

If our dictionary contains the words:

```
pass
12345
omg
Test
```

Output

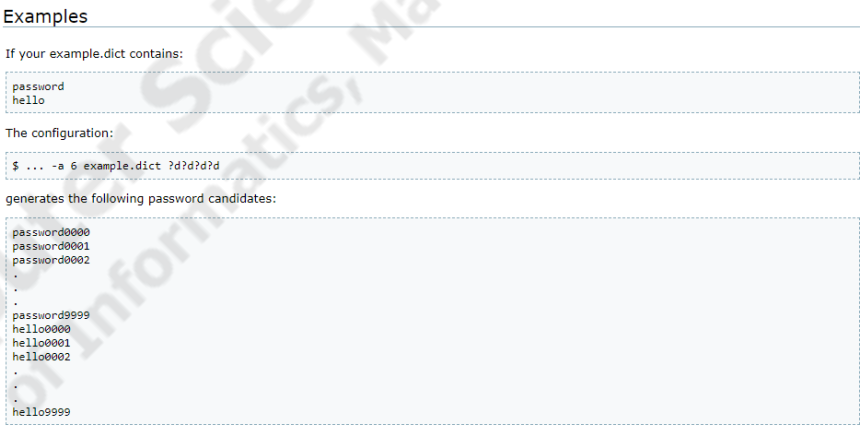
Hashcat creates the following password candidates:

```
passpass
pass12345
passomg
passTest
12345pass
1234512345
12345omg
12345Test
omgpass
omg12345
omgomg
omgTest
Testpass
Test12345
Testomg
TestTest
```

ภาพประกอบที่ 2.1 ตัวอย่าง Input/Output Combinator attack

2.1.4 Hybrid attack

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



Examples

If your example.dict contains:

```
password
hello
```

The configuration:

```
$ ... -a 6 example.dict ?d?d?d?d
```

generates the following password candidates:

```
password0000
password0001
password0002
.
.
.
password9999
hello0000
hello0001
hello0002
.
.
.
hello9999
```

ภาพประกอบที่ 2.2 ตัวอย่าง Create Dictionary เพื่อโจมตีด้วย Hybrid Attack

2.1.5 Rockyou.txt

Rockyou.txt คือไฟล์ที่รวบรวมรหัสผ่านมากกว่า 14 ล้านรหัสที่รวบรวมมาจากแหล่งต่าง ๆ เช่น การละเมิดข้อมูล การรวบรวมรหัสผ่านที่รั่วไหล และฐานข้อมูลรหัสผ่านสาธารณะ ไฟล์นี้ถูกรวมอยู่ใน Kali Linux ซึ่งเป็นระบบปฏิบัติการแบบ open source ที่ออกแบบมาเพื่อความปลอดภัยคอมพิวเตอร์ ไฟล์นี้มักใช้เพื่อวัตถุประสงค์ด้านความปลอดภัย เช่น การทดสอบการเจาะและการจำลองการโจมตี

2.1.6 Malware

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

1) Virus มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว

2) Worm สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

3) Trojan หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัยแต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง

4) Backdoor เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์โดยไม่รู้ตัว

5) Rootkit เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

6) Spyware แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น

7) Ransomware ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้

2.1.7 VirusTotal

VirusTotal [14] 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 เข้ากับระบบรักษาความปลอดภัยที่ใหญ่ขึ้นซึ่งจะช่วยป้องกันอันตรายที่เกี่ยวข้องกับไฟล์และเว็บไซต์อย่างมีประสิทธิภาพ

2.1.8 Message Digest algorithm 5 (MD5)

Message Digest algorithm 5 [11] (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

2.1.9 Secure Hash Algorithm (SHA)

Secure Hash Algorithm (SHA) [15] 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)

2.1.10 Vulnerability

Vulnerability คือ จุดอ่อนหรือช่องโหว่ หมายถึง สภาพแวดล้อมหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์และหากถูกใช้ให้เป็นประโยชน์โดยภัยคุกคามก็อาจทำให้ทรัพย์สินหรือข้อมูลต่าง ๆ ขององค์กรได้รับความเสียหาย นับได้ว่าความเสี่ยงของช่องโหว่ในระบบคอมพิวเตอร์ทั้งซอฟแวร์หรือฮาร์ดแวร์ เป็นสิ่งที่มีผลกระทบความสำคัญต่อความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กรหรือบริษัท การค้นพบช่องโหว่ใหม่ มักจะนำไปสู่การสร้างโปรแกรมเจาะระบบ (Exploit Code), ไวรัสหรือมัลแวร์จากผู้บุกรุก เช่น SQL Injection เกิดขึ้นเมื่อแอปพลิเคชันเว็บหรือโปรแกรมไม่ตรวจสอบหรือกรอกข้อมูลผู้ใช้อย่างไม่ระมัดระวังในคำสั่ง SQL ที่ส่งถึงฐานข้อมูล หากผู้ดูแลระบบสามารถรับมราบข่าวสารของช่องโหว่ และติดตั้งโปรแกรมซ่อมแซมของช่องโหว่ไม่ทัน Cross-Site Scripting (XSS) จะเป็นช่องโหว่ที่เริ่มต้นจากข้อมูลไม่น่าเชื่อถือที่มาจากผู้ใช้หรือแหล่งอื่น ๆ ะได้รับผลกระทบจากความเสี่ยงเหล่านี้แน่นอน โดยทั่วไปข่าวสารเกี่ยวกับช่องโหว่ มักจะได้มาจาก เจ้าของผลิตภัณฑ์ หรือเว็บไซต์ทางด้านความมั่นคงปลอดภัย

2.1.11 Common Vulnerabilities and Exposures (CVE)

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

2.1.12 Vulners.NSE

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

2.1.13 Hypertext Transfer Protocol (HTTP)

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

2.1.14 Secure Socket Layer (SSL)

Secure Socket Layer (SSL) คือ Protocol ด้านความปลอดภัยที่ถูกพัฒนาขึ้นเพื่อป้องกันการส่งข้อมูลผ่านอินเทอร์เน็ตและได้มีการกำหนดเป็นมาตราฐานความปลอดภัยที่มีความน่าเชื่อถือที่สุด โดยบริษัท Netscape เป็นผู้ที่คิดค้นขึ้นมาและส่งต่อไปให้กับ Internet Engineering Task Force (IETF) เป็นกลุ่มนานาชาติของผู้ที่มีส่วนร่วม ในการพัฒนาโครงสร้างของอินเทอร์เน็ต ให้มีการพัฒนา SSL เป็น TLS (Transport Layer Security) และใช้ในการป้องกันความปลอดภัยของการสื่อสารทางอินเทอร์เน็ตในปัจจุบันโดย TLS และ SSL ถูกใช้ในการเข้ารหัสข้อมูลและสร้างการเชื่อมต่อความปลอดภัยระหว่างเว็บเบราวเซอร์และเซิร์ฟเวอร์ที่ใช้งาน Hypertext Transfer Protocol Secure

2.1.15 Testssl.sh

Testssl.sh [18] เป็นเครื่องมือบรรทัดคำสั่งที่มีคุณลักษณะหลากหลายและเป็น open source ซึ่งใช้สำหรับตรวจสอบบริการที่เปิดใช้งานการเข้ารหัส TLS/SSL สำหรับการเข้ารหัสโพรโทคอล และการเข้ารหัสบางอย่างที่รองรับ ข้อบกพร่องบนเซิร์ฟเวอร์ Linux/BSD สามารถทำงานบน macOS X และ Windows โดยใช้ MSYS2 หรือ Cygwin

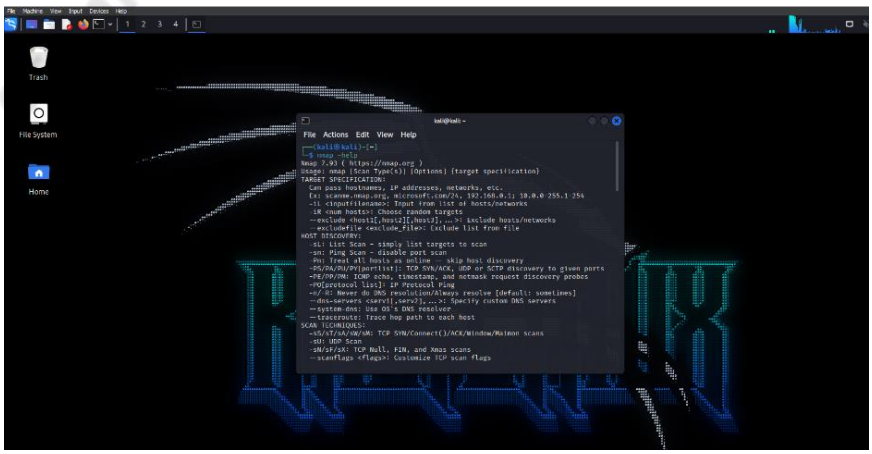
2.1.16 Transport Layer Security (TLS)

Transport Layer Security (TLS) ถูกพัฒนามาจาก SSL Protocol และการทำงานของ Protocol จะทำการเข้ารหัสให้กับข้อมูลก่อนที่จะส่งไปยังผู้รับข้อมูลปลายทาง เพื่อเพิ่มความปลอดภัยให้กับข้อมูลในขณะที่กำลังส่งข้อมูลเหล่านั้นจากเครื่องแม่ข่ายไปยังเครื่องลูกข่าย

2.2 Software ที่เกี่ยวข้อง

2.2.1 Virtual Machine (VM)

Virtual Machine [8] (VM) เป็นซอฟต์แวร์ที่ใช้ทรัพยากรของเครื่องคอมพิวเตอร์ไม่ว่าจะเป็น RAM, Hard disk, CPU ในการจำลองเครื่องคอมพิวเตอร์เสมือน ซึ่งจะเรียกเครื่องที่ถูกใช้ทรัพยากรว่า Host และเรียกเครื่องเสมือนว่า Guest โดยในเครื่อง Guest สามารถติดตั้งและใช้งานระบบปฏิบัติการได้เสมือนกับเป็นซอฟต์แวร์หนึ่งของเครื่องคอมพิวเตอร์ ดังนั้นจึงสามารถติดตั้งระบบปฏิบัติการอื่นที่แตกต่างจากระบบปฏิบัติการหลักของเครื่อง Host ได้



ภาพประกอบที่ 2.3 ตัวอย่างโปรแกรม Kali Linux

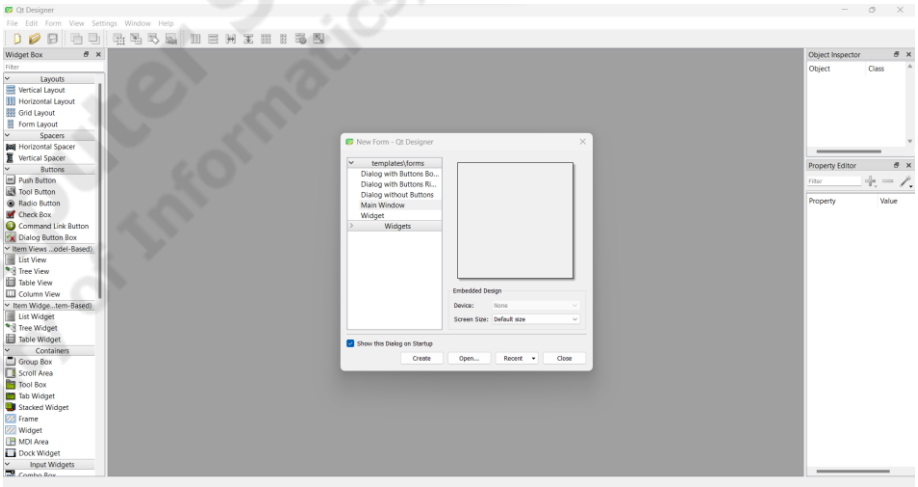
2.2.2 Kali Linux

Kali Linux เป็นระบบปฏิบัติการณ์ลินุกซ์ (Linux) ตัวหนึ่งของคอมพิวเตอร์ซึ่งมีพื้นฐานบน Linux distribution [5] ที่พัฒนาต่อมาจาก Debian ถูกเขียนขึ้นมาเหมือนกับ ระบบอื่นๆ เช่น Ubuntu ความสามารถที่แตกต่างจาก Linux ตัวอื่นๆ คือการติดตั้งและใส่ Feature หลักๆ และสำคัญเกี่ยวกับงานด้านความปลอดภัยระบบไอทีไว้ให้ โดยที่ไม่ต้องติดตั้ง หรือถ้ายังไม่ได้ติดตั้งก็สามารถติดตั้งได้ง่ายผ่านระบบติดตั้งภายในที่มีให้เรียกว่า software repository ของ Kali

2.2.3 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

2.2.4 Qt Designer



ภาพประกอบที่ 2.4 ตัวอย่างโปรแกรม Qt Designer

Qt Designer เป็นเครื่องมือในการสร้างแอปพลิเคชัน และ GUI ด้วย PySide ซึ่งสามารถทำงานได้หลายระบบปฏิบัติการ (OS) หรือ เรียกว่า Cross-platform การเขียน GUI โดย Qt จะมี API และ Library ต่าง ๆ ที่สร้างขึ้นเพื่อช่วยในการสร้างและจัดการกับ GUI components อีกทั้งยังสนับสนุนการพัฒนาทั้ง C++, Java, Python, Perl, Pascal และ PHP

2.2.5 Hashcat

Hashcat [7] 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

2.2.6 PenTBox

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

1) Password Crackers
2) Denial of Service testing tools (DoS and DDoS)

2.2.7 PentestBox

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

1) Web Vulnerability Scanners
2) Sniffing
3) Reverse Engineering

ตารางที่ 2.1 การเปรียบเทียบการทำงานของเครื่องมือที่เกี่ยวข้อง

Comparison Criteria	PenTBox	PentestBox	Gizmo Box
การติดตั้ง	Linux, Windows	Windows	Linux
User Friendliness	Command Line	Command Line	Graphic User Interface
ความหลากหลายของ features & functions	- Port Scanner - Exploitation Tools - Password Cracking - Password Sniffing	- Port Scanner - Exploitation Tools - Password Cracking - Password Sniffing	- Password Evaluation - Malware Scanning - Message Digest - Vulnerability Scanning - HTTPS Testing

จากตารางเปรียบเทียบการทำงานของเครื่องมือที่เกี่ยวข้องพบว่า เครื่องมือ PenTBox และ PentestBox มีฟังก์ชันการทำงานที่คล้ายกันและส่วนใหญ่จะเป็นฟังก์ชันเกี่ยว กับรหัสผ่าน เช่น Password Cracking และ Password Sniffing ซึ่งเครื่องมือ ISAN Security Gizmo Box จะประกิบไปด้วยเครื่องมือที่หลายหลายได้แก่ Password Evaluation, Malware Scanning, Message Digest Generator, Vulnerability Scanning และ HTTPS Testing เป็นต้น