**บทที่ 4**

**การทดสอบระบบ**

ในบทนี้จะกล่าวถึงการทดสอบเครื่องมือ ISAN Security Gizmo Box ทั้ง 5 เครื่องมือ ได้แก่ Password Evaluation Malware Scanning Message Digest Vulnerability Scanning และ HTTPS Testing เพื่อทดสอบการทำงานของเครื่องมือต่างๆ ว่าเครื่องมือมีการทำงานที่ถูกต้องหรือไม่ ดังนี้

* ทดสอบป้อนรหัสผ่านเพื่อตรวจสอบผลลัพธ์การคำนวณข้อมูลเชิงปริมาณและข้อมูลเชิงคุณภาพ
* ทดสอบป้อนรหัสผ่านตรวจสอบผลลัพธ์การคำนวณระยะเวลาที่คาดว่าจะใช้ในการถอดรหัสผ่านและ Special Warning การแจ้งเตือนความเสี่ยงของรหัสผ่าน
* ทดสอบป้อนรหัสผ่านทดสอบการตรงกันของรหัสผ่านที่ป้อนเข้ามากับ NordPass common passwords
* ทดสอบป้อนรหัสผ่านเพื่อทดสอบการโจมตีด้วยเทคนิค Dictionary attack โดยใช้การโจมตีรูปแบบ Straightforward Dictionary attack
* ทดสอบป้อนรหัสผ่านเพื่อทดสอบการโจมตีด้วยเทคนิค Dictionary attack โดยใช้การโจมตีรูปแบบ Skipping attack
* ทดสอบเพิ่มไฟล์และ URL ของเว็บไซต์เพื่อตรวจสอบการนำเข้าข้อมูล
* ทดสอบความถูกต้องของผลลัพธ์ที่ได้ว่ามีการแสดงผลข้อมูลครบถ้วน
* ทดสอบสร้างรายงาน Malware Scanning
* ทดสอบเพิ่มไฟล์และข้อความเพื่อตรวจสอบความถูกต้องในการนำเข้าข้อมูล
* ทดสอบการทำงานของ hash functions กับข้อมูลที่นำเข้ามา
* ทดสอบความถูกต้องของผลลัพธ์ที่ได้ทั้งรูปแบบข้อความและ QR code
* ทดสอบป้อน Line API Token ส่งผลลัพธ์ผ่าน Line Notify
* ทดสอบป้อน IP address และโดเมนเนมของเว็บไซต์เพื่อตรวจสอบการนำเข้าข้อมูล
* ทดสอบการใช้งาน Nmap กับ Options ต่างๆ
* ทดสอบสร้างรายงาน Vulnerability Scanning
* ทดสอบบันทึกรายงานส่งรายงาน Vulnerability Scanning ผ่าน Email address
* ทดสอบการป้อน URL ของเว็บไซต์เพื่อตรวจสอบการนำเข้าข้อมูล
* ทดสอบความถูกต้องของผลลัพธ์ที่ได้จากการตรวจสอบความปลอดภัยของ Protocol
* ทดสอบความถูกต้องของผลลัพธ์ที่ได้จากการตรวจสอบ HSTS Configuration และ HSTS Preload
* ทดสอบสร้างรายงาน HTTPS Testing
* ทดสอบบันทึกรายงานส่งรายงานผ่าน Email address
  1. **เครื่องมือ Password Evaluation**
     1. ทดสอบป้อนรหัสผ่านเพื่อตรวจสอบผลลัพธ์การคำนวณข้อมูลเชิงปริมาณและข้อมูลเชิงคุณภาพ

ตารางที่ 4.1 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **ข้อมูลเชิงปริมาณ** | **ข้อมูลเชิงคุณภาพ** | **ผลการทดสอบ** |
| gizmo | สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |
| Isangizmo113\* | สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |
| ไอสาน กิซโม่ | ไม่สามารถประมวลผลได้ | ไม่สามารถประมวลผลได้ | ผ่าน |
|  |  |  |  |

* + 1. ทดสอบป้อนรหัสผ่านตรวจสอบผลลัพธ์การคำนวณระยะเวลาที่คาดว่าจะใช้ในการถอดรหัสผ่านและ Special Warning การแจ้งเตือนความเสี่ยงของรหัสผ่าน

ตารางที่ 4.2 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **ระยะเวลาที่คาดว่าจะใช้ในการถอดรหัส** | **การแจ้งเตือนความเสี่ยงของรหัสผ่าน** | **ผลการทดสอบ** |
| gizmo | สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |
| Isangizmo113\* | สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |
| ไอสาน กิซโม่ | ไม่สามารถประมวลผลได้ | ไม่สามารถประมวลผลได้ | ผ่าน |

* + 1. ทดสอบป้อนรหัสผ่านทดสอบการตรงกันของรหัสผ่านที่ป้อนเข้ามากับ NordPass common passwords

ตารางที่ 4.3 [ชื่อตาราง]

|  |  |  |
| --- | --- | --- |
| **ข้อมูลนำเข้า** | **NordPass common passwords** | **ผลการทดสอบ** |
| gizmo | สามารถประมวลผลได้ | ผ่าน |
| Isangizmo113\* | สามารถประมวลผลได้ | ผ่าน |
| ไอสาน กิซโม่ | ไม่สามารถประมวลผลได้ | ผ่าน |

* + 1. ทดสอบป้อนรหัสผ่านเพื่อทดสอบการโจมตีด้วยเทคนิค Dictionary attack โดยใช้การโจมตีรูปแบบ Straightforward Dictionary attack

ตารางที่ 4.4 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **Rock you** | **Crack station** | **ผลการทดสอบ** |
| gizmo |  |  |  |
| Isangizmo113\* |  |  |  |
| ไอสาน กิซโม่ |  |  |  |

* + 1. ทดสอบป้อนรหัสผ่านเพื่อทดสอบการโจมตีด้วยเทคนิค Dictionary attack โดยใช้การโจมตีรูปแบบ Skipping attack

ตารางที่ 4.4 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **Combinator** | **Hybrid** | **ผลการทดสอบ** |
| gizmo |  |  |  |
| Isangizmo113\* |  |  |  |
| ไอสาน กิซโม่ |  |  |  |

* 1. **เครื่องมือ Malware Scanning**
     1. ทดสอบเพิ่มไฟล์และ URL ของเว็บไซต์เพื่อตรวจสอบการนำเข้าข้อมูล

ตารางที่ 4.5 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **การวิเคราะห์ไฟล์** | **การวิเคราะห์ URL**  **ของเว็บไซต์** | **ผลการทดสอบ** |
| ไฟล์ | สามารถประมวลผลได้ | ไม่สามารถประมวลผลได้ | ผ่าน |
| URL | ไม่สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |

* + 1. ทดสอบความถูกต้องของผลลัพธ์ที่ได้ว่ามีการแสดงผลข้อมูลครบถ้วน

ตารางที่ 4.6 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **ผลลัพธ์ที่ได้** | **รายละเอียดของข้อมูล**  **ที่นำเข้า** | **ผลการทดสอบ** |
| ไฟล์ | ข้อมูลครบถ้วน | ข้อมูลครบถ้วน | ผ่าน |
| URL | ข้อมูลครบถ้วน | ข้อมูลครบถ้วน | ผ่าน |

* + 1. ทดสอบสร้างรายงาน Malware Scanning

-------- ทดสอบรายงาน -------

* 1. **เครื่องมือ Message Digest Generator**
     1. ทดสอบเพิ่มไฟล์และข้อความเพื่อตรวจสอบความถูกต้องในการนำเข้าข้อมูล

ตารางที่ 4.7 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **การวิเคราะห์ไฟล์** | **การวิเคราะห์ข้อความ** | **ผลการทดสอบ** |
| ไฟล์ | สามารถประมวลผลได้ | ไม่สามารถประมวลผลได้ | ผ่าน |
| ข้อความ | ไม่สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |

* + 1. ทดสอบการทำงานของ hash functions กับข้อมูลที่นำเข้ามา

ตารางที่ 4.8 [ชื่อตาราง]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **MD5** | **SHA-1** | **SHA-2** | **SHA-3** | **ผลการทดสอบ** |
| ไฟล์ | สามารถประมวลผลได้ | สามารถประมวลผลได้ | สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |
| ข้อความ | สามารถประมวลผลได้ | สามารถประมวลผลได้ | สามารถประมวลผลได้ | สามารถประมวลผลได้ | ผ่าน |

* + 1. ทดสอบความถูกต้องของผลลัพธ์ที่ได้ทั้งรูปแบบข้อความและ QR code

ตารางที่ 4.9 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **ข้อความ** | **QR code** | **ผลการทดสอบ** |
| ไฟล์ | ข้อมูลครบถ้วน | ข้อมูลครบถ้วน | ผ่าน |
| ข้อความ | ข้อมูลครบถ้วนได้ | ข้อมูลครบถ้วน | ผ่าน |

* + 1. ทดสอบป้อน Line API Token ส่งผลลัพธ์ผ่าน Line Notify

ตารางที่ 4.9 [ชื่อตาราง]

|  |  |  |  |
| --- | --- | --- | --- |
| **ข้อมูลนำเข้า** | **Line API Token** | **Line Notify** | **ผลการทดสอบ** |
| Line API Token | สามารถประมวลผลได้ | สามารถส่งข้อมูลได้ | ผ่าน |
| ไม่ใช่ Line API Token | ไม่สามารถประมวลผลได้ | ไม่สามารถส่งข้อมูลได้ | ผ่าน |

* 1. **เครื่องมือ Vulnerability Scanning**
     1. ทดสอบป้อน IP address และโดเมนเนมของเว็บไซต์เพื่อตรวจสอบการนำเข้าข้อมูล
     2. ทดสอบการใช้งาน Nmap กับ Options ต่างๆ
     3. ทดสอบสร้างรายงาน Vulnerability Scanning
     4. ทดสอบบันทึกรายงานส่งรายงานผ่าน Email address
  2. **เครื่องมือ HTTPS Testing**
     1. ทดสอบการป้อน URL ของเว็บไซต์เพื่อตรวจสอบการนำเข้าข้อมูล
     2. ทดสอบความถูกต้องของผลลัพธ์ที่ได้จากการตรวจสอบความปลอดภัยของ Protocol
     3. ทดสอบความถูกต้องของผลลัพธ์ที่ได้จากการตรวจสอบHSTS Configuration และ HSTS Preload
     4. ทดสอบสร้างรายงาน HTTPS Testing
     5. ทดสอบบันทึกรายงานส่งรายงานผ่าน Email address
  3. **สรุปผลการทดสอบ**

จากการทดสอบระบบ ISAN Security Gizmo Box พบว่า