กรณีศึกษาความปลอดภัยในระบบจำลองการควบคุมและรักษาความปลอดภัย

A CASE STUDY ON SIMULATED SECURITY CONTROL SYSTEMS

ภัทรชัย สุภาควัฒน์

สหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2565

A CASE STUDY ON SIMULATED SECURITY CONTROL SYSTEMS

PHATTHARACHAI SUPAKAWAT

A COOPERATIVE EDUCATION SUBMITTED IN
PARTIAL FULFILLMENT OF THE REQUIREMENT FOR
THE DEGREE OF BACHELOR OF SCIENCE (COMPUTER SCIENCE)
DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2022

สหกิจศึกษา	กรณีศึกษาความปลอดภัยในระบบจำลองการควบคุมและรักษาความปลอดภัย A CASE STUDY ON SIMULATED SECURITY CONTROL SYSTEMS
ชื่อนักศึกษา	นายภัทรชัย สุภาควัฒน์ รหัสนักศึกษา 62050206
ปริญญา	วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
ภาควิชา	วิทยาการคอมพิวเตอร์
ปีการศึกษา	2565
อาจารย์ที่ปรึกษา	ผศ.ดร.วรางคณา กิ้มปาน

คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง (สจล.) อนุมัติให้สหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ ประจำปีการศึกษา 2565

คณะกรรมการสอบ	ลายมือชื่อ
ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ ประธานกรรมการ	
ผศ.ดร.วรางคณา กิ้มปาน กรรมการและอาจารย์ที่ปรึกษา	

สหกิจศึกษา กรณีศึกษาความปลอดภัยในระบบจำลองการควบคุมและรักษาความปลอดภัย
ชื่อนักศึกษา นายภัทรชัย สุภาควัฒน์ รหัสนักศึกษา 62050206
ปริญญา วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
ภาควิชา วิทยาการคอมพิวเตอร์
ปีการศึกษา 2565
อาจารย์ที่ปรึกษา ผศ.ดร.วรางคณา กิ้มปาน

บทคัดย่อ

ในปัจจุบัน มีการใช้งานอุปกรณ์ IoT เป็นที่นิยมเพิ่มมากขึ้นเมื่อเทียบกับสมัยก่อนด้วยอินเทอร์เน็ตที่เข้าถึงมากยิ่งขึ้น ทำให้การประยุกต์ใช้อุปกรณ์ IoT ในชีวิตประจำวันช่วยให้ผู้คนมีความสะดวกสบาย และดำเนินการใช้ชีวิตได้ง่ายขึ้นเป็นอย่างมาก ในขณะเดียวกัน ผู้ที่ไม่หวังดีก็มีเป้าหมายในการโจมตีอุปกรณ์ IoT เพิ่มมากขึ้นแปรผันตรงจากผู้ใช้ที่มีจำนวนมากขึ้น จึงทำให้เห็นการโจมตีประเภทต่าง ๆ เกิดขึ้นกับอุปกรณ์ IoT เกิดได้ง่ายขึ้นกว่าสมัยก่อน ตัวอย่างเช่น การโจมตีแบบทำซ้ำ การโจมตีโดยการปฏิเสธการให้บริการ เป็นต้น ผู้ใช้งานหลายคนอาจตกเป็นเหยื่อในการโจมตีได้โดยไม่รู้ตัว จากการใช้อุปกรณ์ที่ไม่มีการป้องกัน การใช้ซอฟต์แวร์ที่ล้าสมัย ทางผู้จัดทำได้เล็งเห็นถึงปัญหาว่ายังไม่ค่อยมีผู้คนให้ความตระหนักในด้านความปลอดภัยของอุปกรณ์ IoT จึงได้จัดทำกรณีศึกษาความปลอดภัยในระบบควบคุมจำลองโดยมีอุปกรณ์ IoT ที่สื่อสารผ่านโปรโตคอล Radio Frequency ขึ้น เพื่อให้ผู้ใช้งานได้ตระหนักถึงความปลอดภัยบนโลกดิจิทัลเพิ่มมากขึ้น จากผลการดำเนินการพบว่าการโจมตีแบบทำซ้ำนั้นสามารถเกิดขึ้นได้ง่ายกับอุปกรณ์ IoT ที่มีการใช้โปรโตคอล Radio Frequency ส่งผลให้ผู้ใช้งานอาจโดนเข้าถึง ทำลาย หรือแก้ไขโดยไม่ได้รับอนุญาตได้ แต่มีวิธีป้องกัน คือผู้ใช้งานควรใช้อุปกรณ์ที่มีการทำ Rolling code transmitter เพื่อป้องกันเทคนิคในการโจมตีแบบทำซ้ำ

คำสำคัญ: การโจมตีแบบทำซ้ำ-อุปกรณ์ IoT-การป้องกันเทคนิคการโจมตีแบบทำซ้ำ

Title	A Case Study on Simulate Security Control Systems
Students	Mr. Phattharachai Supakawat Student ID 62050206
Degree	Bachelor of Science (Computer Science)
Department	Computer Science
School	Science
University	King Mongkut's Institute of Technology Ladkrabang (KMITL)
Academic Year	2565
Advisor	Asst.Prof.Dr. Warangkhana Kimpan

Abstract

In the recent years, the use of IoT devices is becoming increasingly popular compared to the past with more accessible internet. This has made the use of IoT devices in everyday life more convenient and has made life easier. At the same time, due to the increasing of users, attackers are increasingly targeting IoT devices. This has led to various types of attacks on IoT devices becoming more common, such as replay attacks or denial of service attacks. Many users may be victims of an attack without realizing it due to the use of unprotected devices, outdated software, and a lack of awareness about the security of IoT (IoT) devices. Therefore, we proposed "A CASE STUDY ON SIMULATE SECURITY CONTROL SYSTEMS" project to increase awareness about digital security. The results of the study found that replay attacks can easily occur on IoT devices using the Radio Frequency protocol, allowing attacker to be accessed, destroyed, or modified without authentication. However, one way to prevent this is for users to use devices with Rolling code transmitters in order to protect against replay attack techniques.

Keywords: Replay attack, IoT devices, Preventing replay attack techniques

กิตติกรรมประกาศ

ในการจัดทำกรณีศึกษาความปลอดภัยในระบบจำลองการควบคุมและรักษาความปลอดภัย (A Case Study On Simulate Security Control Systems) นี้สำเร็จลุล่วงไปได้ด้วยดีเนื่องจากได้รับการสนับสนุน ความช่วยเหลือและความกรุณาต่าง ๆ จากบุคคลหลายท่าน ซึ่งผู้จัดทำขอกราบขอบพระคุณบุคคลดังต่อไปนี้

ขอขอบพระคุณ อาจารย์วรางคณา กิ้มปาน อาจารย์ที่ปรึกษาที่คอยช่วยเหลือและให้การสนับสนุนในการทำสหกิจศึกษา ซึ่งเป็นผู้ที่เสียสละเวลาและแนะนำชี้แนวทางของปัญหา รวมไปถึงการตรวจสอบความเรียบร้อยและความสมบูรณ์ของงานมาโดยตลอด

ขอขอบพระคุณ นายณัฐกรณ์ ธีระประยุติ และบุคลากรทุกท่านจากบริษัท อินค็อกนิโตแล็บ จำกัด ที่ให้โอกาสพร้อมกับคำปรึกษาและคำแนะนำ รวมถึงความรู้ ทักษะ และประสบการณ์ที่มีค่าและได้รับการต้อนรับ การดูแลที่ดีมาโดยตลอดช่วงระยะเวลาสหกิจศึกษา

ขอขอบพระคุณ คณาจารย์ของภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ให้ความรู้และทักษะต่าง ๆ ตลอดระยะเวลาการศึกษาที่ผ่านมา

สุดท้ายนี้ขอขอบพระคุณบิดา มารดา รวมถึงสมาชิกในครอบครัวที่คอยให้การสนับสนุนโอกาสในการศึกษาเล่าเรียน และคอยเป็นกำลังใจในการทำสหกิจศึกษา จนสามารถฝ่าอุปสรรคต่าง ๆ ไปได้ทำให้สหกิจศึกษาในครั้งนี้สมบูรณ์ได้ ทางผู้จัดทำขอขอบพระคุณอย่างสูงไว้ ณ ที่นี้ด้วย

ภัทรชัย สุภาควัฒน์

สารบัญ

หน้า

สารบัญรูป

รูปที่ **หน้า**

สารบัญรูป (ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องจากการควบคุมการสื่อสารและการส่งข้อมูลของอุปกรณ์ IoT มักใช้อินเทอร์เน็ตในการเชื่อมต่อซึ่งกันและกัน โดยการเชื่อมต่อกันของอุปกรณ์ IoT ในปัจจุบันนั้นง่ายจนทำให้ผู้ใช้งานสามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ตในระยะไกลได้ แต่ทว่าความเสี่ยงที่จะก่อให้เกิดการโจมตีบนอุปกรณ์ IoT ก็มีจำนวนเพิ่มมากขึ้นเช่นเดียวกัน ทำให้ผู้ที่เลือกใช้งานอุปกรณ์ IoT ต่าง ๆ ต้องคำนึงถึงเรื่องความปลอดภัยบนโลกดิจิทัลว่าจะนำมาใช้อย่างไรให้เกิดความเสี่ยงน้อยที่สุดทั้งในด้านกายภาพและด้านดิจิทัล ทางผู้จัดทำได้เล็งเห็นถึงปัญหาว่ายังไม่ค่อยมีผู้คนให้ความตระหนักในด้านความปลอดภัยของอุปกรณ์ IoT จึงได้จัดทำกรณีศึกษาความปลอดภัยในระบบควบคุมจำลองโดยมีอุปกรณ์ IoT ที่สื่อสารผ่านโปรโตคอล Radio frequency ขึ้น เพื่อให้ผู้ใช้งานได้ตระหนักถึงความปลอดภัยบนโลกดิจิทัลเพิ่มมากขึ้น

1.2 วัตถุประสงค์ของงานวิจัย

1) ศึกษาความปลอดภัยของอุปกรณ์ IoT ที่มีการสื่อสารด้วยโปรโตคอล Radio frequency
2) จำลองระบบที่มีการใช้งานอุปกรณ์ IoT ที่สื่อสารผ่านโปรโตคอล Radio frequency และจำลองการโจมตีระบบ
3) ให้ความรู้ทางด้านเทคนิคในการโจมตีอุปกรณ์ IoT และแนะนำแนวทางการป้องกันการโจมตีสำหรับอุปกรณ์ IoT

1.3 ขอบเขตของงานวิจัย

1) จำลองระบบที่มีการใช้อุปกรณ์ IoT ที่มีการสื่อสารด้วยโปรโตคอล Radio frequency
2) พัฒนา source code ที่ใช้ในการโจมตีระบบควบคุมจำลอง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1) ผู้ใช้งานสามารถเรียนรู้เกี่ยวกับการโจมตีของโปรโตคอล Radio frequency
2) สร้างความตระหนักรู้ให้กับผู้ใช้งานอุปกรณ์ IoT เพิ่มมากขึ้น

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of things: IoT)

IoT หรืออินเทอร์เน็ตประสานสรรพสิ่ง [1] [2] เป็นระบบของอุปกรณ์คอมพิวเตอร์ที่สัมพันธ์หรือเชื่อมต่อกันผ่านอินเทอร์เน็ต โดยมีความสามารถในการประมวลผล มีเทคโนโลยีอื่น ๆ ที่เชื่อมต่อและแลกเปลี่ยนข้อมูลกับอุปกรณ์และระบบอื่น ๆ ผ่านทางอินเทอร์เน็ต และสามารถควบคุมหรือสั่งการให้อุปกรณ์ต่าง ๆ ทำงานตามที่ต้องการได้ผ่านทางเครือข่ายอินเทอร์เน็ต อุปกรณ์เหล่านี้สามารถเป็นได้ทั้งวัตถุในบ้านทั่วไปไปจนถึงเครื่องมืออุตสาหกรรมที่มีความซับซ้อนมากขึ้น ในโลกยุคปัจจุบันมีความนิยมในการใช้งาน IoT มากสูงถึง 7 พันล้านเครื่อง และมีแนวโน้มที่จะมากขึ้นเรื่อย ๆ ในปีถัด ๆ ไปอย่างมีนัยสำคัญ และในช่วงไม่กี่ปีที่ผ่านมา IoT ช่วยให้โลกมีการพัฒนาขึ้นอย่างมาก เพราะสามารถเชื่อมต่อวัตถุต่าง ๆ เข้าด้วยกันผ่านอินเทอร์เน็ต ทำให้การสื่อสารมีความต่อเนื่องมากยิ่งขึ้น จากทั้งคนสู่คน คนกับสิ่งของ หรือแม้แต่สิ่งของกับสิ่งของเองก็ตาม ซึ่งทำให้โลกทางกายภาพพบกับโลกดิจิทัลทำงานร่วมกันได้ง่ายและสะดวกมากยิ่งขึ้น

2.2 ชื่อโดเมน (Domain name)

ทางเว็บไซต์ Cloudflare [3] [4] ได้ให้นิยามสำหรับ Domain name ไว้ว่าเป็นสตริงข้อความที่จับคู่กับ ที่อยู่ IP ที่เป็นตัวเลข ซึ่งสามารถนำไปใช้ในการเข้าถึงเว็บไซต์ได้ เพื่อให้ผู้ใช้งานมีความสะดวกสบาย เพียงพิมพ์ข้อความลงในช่องค้นหาของเบราว์เซอร์ต่าง ๆ ก็สามารถเข้าถึงเว็บไซต์ใดเว็บไซต์หนึ่งได้ทันที ซึ่ง domain name ยังสามารถแบ่งย่อยออกได้เป็น 2 ส่วนได้แก่ 1) Top-level domain (TLD) และ 2) Second-level domain (SLD) โดย TLD จะเป็นส่วนสำหรับ extension ของ Domain เช่น .com .org เป็นต้น และ SLD จะเป็นส่วนชื่อเฉพาะของ Domain ซึ่งส่วนใหญ่มักจะตั้งตามชื่อธุรกิจหรือหน่วยงานต่าง ๆ โดยตัวอย่างของ Domain name เช่น kmitl.ac.th แบ่งได้เป็น TLD คือ .ac.th และ SLD คือ kmitl และ thaigov.go.th แบ่งได้เป็น TLD คือ .go.th และ SLD คือ thaigov ซึ่งเป็นเว็บสำหรับหน่วยงานรัฐบาลของประเทศไทย

2.3 โดเมนย่อย (Subdomain)

เป็นชื่อย่อยของโดเมน [4] หรือเรียกได้ว่าเป็นชื่อเว็บไซต์ย่อย ๆ ของเว็บไซต์หลัก เกิดจากการที่ ทำการแบ่งชื่อภายในเว็บไซต์ออกเป็นหลาย ๆ อัน เพื่อทำให้ผู้ใช้งานสามารถจดจำได้ง่าย หรือสามารถประยุกต์ใช้ในการแบ่งเป็นหมวดหมู่ต่าง ๆ ของเว็บไซต์ได้ โดยทั่วไปแล้วชื่อของ subdomain มักจะอยู่ก่อนหน้าของชื่อ domain ตัวอย่างเช่น mail.google.com จะเห็นได้ว่าชื่อของ subdomain นั้นคือ mail ในส่วนของชื่อโดเมนคือ google และในส่วนท้ายที่สุดของ URL จะมีชื่อเรียกว่า Top-level domain โดยจากในตัวอย่างคือ .com

2.4 แม่ข่ายเสมือน (Virtual Host)

ทางเว็บไซต์ IBM [5] ได้กล่าวไว้ว่าแนวคิดของแม่ข่ายเสมือนเป็นการอนุญาตให้มีเว็บไซต์มากกว่าหนึ่งเว็บไซต์บนเซิร์ฟเวอร์เดียวกัน โดยแต่ละเว็บไซต์จะมีความแตกต่างกันตามชื่อแม่ข่าย ซึ่งการทำแม่ข่ายจำลองถือเป็นวิธีในการใช้ทรัพยากรของ Server ให้เกิดประโยชน์และมีประสิทธิภาพสูงที่สุด ซึ่ง Virtual Host สามารถใช้ IP-based หรือ name-based ได้ โดย IP-based หมายความว่ามีที่อยู่ IP ที่แตกต่างกันสำหรับแต่ละเว็บไซต์ และ name-based หมายความว่ามีชื่อหลายชื่อที่ทำงานร่วมกันอยู่บนแต่ละที่อยู่ IP ตัวอย่างของการใช้ Virtual Host ในการทำเว็บไซต์ สามารถสังเกตได้จาก URL เช่น company1.example.com กับ company2.example.com เป็นต้น

2.5 Open-Source Intelligence (OSINT)

เป็นขั้นตอนการค้นหาและวิเคราะห์ข้อมูลของเป้าหมายจากแหล่งข้อมูลที่เปิดเผยและเป็นสาธารณะที่สามารถเข้าถึงได้ [7] เช่น สื่อสารสังคมออนไลน์ เว็บไซต์ แหล่งข่าวสารออนไลน์ เป็นต้น เพื่อให้ได้ข้อมูลที่เป็นประโยชน์ และใช้ได้กับวัตถุประสงค์ตามต้องการ เช่น การทำนายเหตุการณ์ในอนาคต เรื่องความปลอดภัย การค้าขาย การวางแผนการตลาด เป็นต้น โดยการทำ OSINT นั้นสามารถใช้เครื่องมือหรือเทคนิคต่าง ๆ เข้ามาร่วมด้วยได้เพื่อช่วยในการประหยัดเวลาในการทำ ตัวอย่างเครื่องมือในการทำ OSINT ได้แก่ Whois SpiderFoot เป็นต้น

2.6 การแจงนับโดเมนย่อย (Subdomain Enumeration)

เป็นเทคนิคในการค้นหาโดเมนย่อยสำหรับเซิร์ฟเวอร์ที่มีโดเมนตั้งแต่หนึ่งโดเมนขึ้นไป เพื่อช่วยในการค้นหาโดเมนย่อยที่ถูกซ่อนอยู่ และอาจนำไปสู่การขยายผลการโจมตีได้ โดยแบ่งออกได้เป็น 2 ประเภทหลัก ๆ ได้แก่ Passive Enumeration เป็นการค้นหาโดเมนย่อยที่ไม่ได้กระทำกับเป้าหมาย

โดยตรง เช่น การทำ Google Hacking [8] เป็นต้น และ Active Enumeration เป็นการค้นหาโดเมนย่อยที่กระทำกับเป้าหมายโดยตรง เช่น การทำ Brute-force เป็นต้น

2.7 เครื่องเสมือน (Virtual Machine)

ทางเว็บไซต์ IBM [9] ได้กล่าวว่า Virtual Machine เป็นเทคโนโลยีหนึ่งที่ใช้ในการจำลองคอมพิวเตอร์ผ่านซอฟต์แวร์ โดยเป็นการจำลองการทำงานของระบบปฏิบัติการซึ่งใน VM จะถูกเรียกว่า “guest OS” แต่ละเครื่องจำลองจะประกอบไปด้วยไฟล์สำหรับการตั้งค่า (Configuration file) ที่เก็บข้อมูลการตั้งค่าทั้งหมดของเครื่องจำลอง ไฟล์ดิสก์เสมือน (Virtual disk file) ซึ่งเป็นดิสก์ในเวอร์ชั่นซอฟต์แวร์ที่มีการใช้ในการเก็บข้อมูลภายในเครื่องเสมือน และไฟล์บันทึกเหตุการณ์ (log file) ที่บันทึกกิจกรรมที่เกิดขึ้นทั้งหมดภายในเครื่องเสมือน เช่น ความผิดพลาดของระบบ สถานะของเครื่อง เป็นต้น [10] ซึ่งเครื่องเสมือนดังกล่าวนี้มีการทำขึ้นเพื่อลดการใช้พลังงานจากการใช้คอมพิวเตอร์หลาย ๆ เครื่อง อีกทั้งยังช่วยแบ่งเบาภาระการทำงานของคอมพิวเตอร์ได้อีกด้วย ช่วยให้การจัดสรรทรัพยากรภายในเครื่องเป็นไปอย่างคุ้มค่า และอนุญาตให้มีสภาพแวดล้อมระบบปฏิบัติการหลายระบบพร้อมกันบนเครื่องเดียวกันได้

2.8 Python

Python [11] เป็นภาษาโปรแกรมแบบ Object-Oriented ระดับสูงตัวหนึ่งที่ถูกใช้งานอย่างแพร่หลาย มีการออกแบบให้เข้าใจง่าย เรียนรู้ง่าย โดยมีการตัดความซับซ้อนของโครงสร้างและไวยากรณ์ของภาษาออกไป ซึ่งทำให้การบำรุงรักษาโปรแกรมง่ายขึ้นและสามารถลดค่าใช้จ่ายได้มากขึ้น และสามารถทำงานบนแพลตฟอร์มต่าง ๆ ได้มากมาย เช่น เว็บแอปพลิเคชัน เป็นต้น โดย Python เป็นภาษาโปรแกรมที่ใช้ Interpreter ในการแปลง Source code เป็นโปรแกรมที่สามารถใช้งานได้ ซึ่งภาษา Python ไม่มีขั้นตอนการคอมไพล์ (Compilation) เหมือนกับภาษาโปรแกรมอื่น ๆ ทำให้ผู้พัฒนาโปรแกรมสามารถแก้ไข ทดสอบ เมื่อเจอปัญหากับโปรแกรมได้อย่างรวดเร็ว

2.9 GitHub

เป็นแพลตฟอร์มออนไลน์ที่ให้บริการสำหรับผู้พัฒนาซอฟต์แวร์แบบทำงานร่วมกัน โดยที่ผู้ใช้งานสามารถสร้างพื้นที่เก็บโค้ด (Repository) ขึ้นมาได้โดยไม่มีค่าใช้จ่าย และสามารถเปิดเผยได้แบบสาธารณะหรือเป็นเอกสารเฉพาะกลุ่มได้ ซึ่งทำให้ผู้ใช้งานสามารถแชร์และทำงานร่วมกันได้อย่างสะดวกและรวดเร็ว นอกจากนี้ยังมีเครื่องมืออื่น ๆ ภายในแพลตฟอร์ม เช่น ระบบควบคุมเวอร์ชัน (Version control) ซึ่งช่วยให้ผู้ใช้งานสามารถติดตามการเปลี่ยนแปลงของ Source code ได้อย่างชัดเจน และการจัดการโค้ดร่วมกันในทีมสามารถดำเนินการได้อย่างมีประสิทธิภาพและมีความ

ต่อเนื่อง นับว่า GitHub เป็นแพลตฟอร์มที่มีความสำคัญสำหรับนักพัฒนาทั่วโลกที่ต้องการแชร์และเรียนรู้เทคนิคการพัฒนาซอฟต์แวร์ อีกทั้งยังส่งผลต่อการเติบโตของชุมชนนักพัฒนาและนักเขียนโค้ดในทั่วโลก

2.10 git-dumper

เป็นเครื่องมือแบบ Open-source ที่มีการเปิดเผยอยู่บนแพลตฟอร์ม Github [12] ที่ใช้สำหรับดึงโค้ดจาก Git โดยไม่ต้องมีสิทธิ์เข้าถึงโดยตรง โดย git-dumper จะใช้เทคนิคการโจมตีโดยการใช้ git-bundle และ git-archive เพื่อดึงข้อมูลโค้ดจาก Git repository ของเป้าหมายโดยที่ไม่ต้องดึงโค้ดโดยตรงจาก Repository นั้น ๆ ด้วยวิธีการเข้าถึงที่ไม่ได้รับอนุญาต ทำให้ git-dumper เป็นเครื่องมือที่มีประสิทธิภาพสำหรับการดึงโค้ดจาก Repository ที่ไม่สามารถเข้าถึงได้โดยตรงหรือ Repository ที่ถูกป้องกันไม่ให้มีการเข้าถึงโดยไม่มีสิทธิ

2.11 Directory brute-force

เป็นเทคนิคที่ใช้ในการค้นหาและระบุ directory ที่ถูกซ่อนอยู่ในเว็บไซต์ [13] ซึ่งอาจนำไปสู่การขยายผลการโจมตีได้หรืออาจพบเจอจุดที่เป็นความเสี่ยงต่อความปลอดภัยของเว็บไซต์ได้ ซึ่งสามารถดำเนินการได้โดยการใช้โปรแกรมหรือสคริปต์ที่ออกแบบมาเพื่อเป้าหมายในการค้นหาไฟล์หรือ directory ที่ซ่อนอยู่ในเว็บไซต์ด้วยวิธีการลองค้นหาด้วยรูปแบบและตัวอักษรที่เปลี่ยนแปลงไปเรื่อย ๆ จนกว่าจะพบไฟล์หรือโฟลเดอร์ที่ต้องการหรือไม่พบเลยก็จะหยุดการทำงานตามที่กำหนด

2.12 Nmap

ทางเว็บไซต์ ETDA [14] ได้ให้นิยามของ Nmap เอาไว้ว่าเป็นซอฟต์แวร์ที่มีความเกี่ยวข้องกับ Network ซึ่งถือเป็นซอฟต์แวร์ที่มีความนิยมในการใช้งานสูง โดยในตอนเริ่มต้น Nmap ถูกพัฒนาขึ้นให้ใช้ได้ในระบบปฏิบัติการ Linux เท่านั้น เพื่อใช้ในการค้นหาระบบเครือข่ายหรือใช้ในการค้นหาบริการที่เปิดใช้งานอยู่บนระบบเครือข่ายอินเทอร์เน็ต และต่อมา Nmap ได้ถูกพัฒนาให้ใช้ได้แทบทุกระบบปฏิบัติการ เช่น Windows, Mac OS และพัฒนาให้มีความสามารถในด้านอื่น ๆ อีกด้วย เช่น Operating System Version Detection เป็นต้น

2.13 gobuster

เป็นเครื่องมืออัตโนมัติที่ช่วยในการโจมตี Brute-force [15] ซึ่งถูกพัฒนาขึ้นโดยใช้ภาษาโปรแกรมที่ มีชื่อว่า Golang ถือเป็นเครื่องมือที่มีความสามารถหลากหลายในการโจมตี เช่น directory brute-force, subdomain enumeration เป็นต้น โดย gobuster ถือเป็นเครื่องมือที่มีความสมบูรณ์และเป็นที่นิยมในการทดสอบช่องโหว่ของเว็บไซต์และการทำการเจาะเข้าระบบ (Penetration testing) สามารถใช้งานได้ง่าย และสามารถรองรับการทำงานแบบพร้อมกันหลาย ๆ คำขอได้ (Concurrency) อีกทั้งยังมีความสามารถในการประมวลผลที่มีความเร็วสูง ข้อเสียเดียวของ gobuster คือ การสแกน directory แบบ Recursive ซึ่งต้องทำการสแกนอีกครั้งเมื่อเจอโฟลเดอร์ที่ลึกกว่าหนึ่งระดับ แต่การสแกนด้วย gobuster จะทำงานได้รวดเร็วเมื่อเทียบกับเครื่องมือสแกนอื่น ๆ ที่สแกนโฟลเดอร์แบบ recursive ได้เช่นเดียวกัน ที่เหลือนั้นสามารถใช้เครื่องมือสแกนอื่น ๆ เพื่อช่วยเติมความสมบูรณ์ได้ โดยเครื่องมือ gobuster จะทำการส่งคำร้องขอ (Request) ไปยังเว็บไซต์โดยใช้ Wordlist หรือ Word dictionary เพื่อค้นหาคำที่กำหนดภายในเป้าหมาย

2.14 Universal Radio Hacker (URH)

เป็นเครื่องมือแบบ Open-source ที่มีการเปิดเผยอยู่บนแพลตฟอร์ม Github [16] [17] ถือเป็นชุดเครื่องมือที่สมบูรณ์พร้อมสำหรับการตรวจสอบโปรโตคอลไร้สายต่าง ๆ เช่น Radio Frequency (RF) เป็นต้น ซึ่งถือเป็นชุดเครื่องมือที่สนับสนุนการทำงานคู่กับ Software Defined Radios หลายตัวในท้องตลาด มีความสามารถในการทำ fuzzing สำหรับโปรโตคอลแบบ stateless มีการถอดรหัสที่สามารถกำหนดได้โดยผู้ใช้งาน และอื่น ๆ อีกมากมายภายในชุดเครื่องมือ เช่น การวิเคราะห์โปรโตคอลสำหรับการสื่อสารของอุปกรณ์ IoT ที่มีเพิ่มมากขึ้นทุกวันบนโลก โปรโตคอลดังกล่าวมักจะปรากฏขึ้นอย่างแพร่หลายและมีการนิยมใช้เพิ่มมากขึ้น อุปกรณ์ IoT ส่วนมากทำงานบนความถี่ 433.92 MHz หรือ 868.3 MHz และใช้โปรโตคอลที่เป็นกรรมสิทธิ์สำหรับการสื่อสาร และมักจะมีการเข้ารหัสในการสื่อสารเอาไว้แล้ว แต่เมื่อ Universal Radio Hacker ดักจับสัญญาณมาได้ก็สามารถถอดรหัสข้อความดังกล่าวออกมาเป็นข้อความที่มนุษย์สามารถเข้าใจได้อย่างง่ายดาย

2.15 ความถี่วิทยุ (Radio Frequency: RF)

เว็บไซต์ techtarget [18] ได้กล่าวไว้ว่า Radio Frequency (RF) หรือความถี่วิทยุ คืออัตราการสั่นของกระแสไฟฟ้าสลับ หรือของสนามแม่เหล็กไฟฟ้ามักใช้ในการสื่อสารไร้สาย เช่น การส่งสัญญาณวิทยุ สัญญาณโทรทัศน์ สัญญาณไวไฟ (Wi-Fi) สัญญาณโทรศัพท์มือถือ เป็นต้น มีช่วงความถี่อยู่ตั้งแต่ประมาณ 3 kHz ถึงประมาณ 300 GHz ซึ่งค่านี้อยู่ระหว่างขีดจำกัดของความถี่เสียง

กับความถี่อินฟราเรด โดย RF สามารถถูกส่งผ่านอากาศได้โดยไม่ต้องมีสายสื่อสารเชื่อมต่อ ทำให้มีความสะดวกสบายและมีความยืดหยุ่นในการใช้งานมากขึ้น

2.16 วงจรแปลงผันแบบเพิ่มระดับ (Boost Converter)

Boost Converter หรือวงจรเพิ่มแรงดันไฟฟ้า เรียกได้อีกชื่อหนึ่งว่าวงจรทบระดับ เป็นวงจรคอนเวอร์เตอร์ประเภทหนึ่งที่สามารถนำไปใช้งานได้กว้างขวาง ซึ่งสามารถนำมาใช้ปรับค่าแรงดันไฟฟ้าขาออกได้ซึ่งขึ้นอยู่กับกระแสไฟฟ้าขาเข้าตามที่ระบุ มีหลักการทำงานคือการนำกระแสไฟฟ้าขาเข้าไปแลกเป็นแรงดันไฟฟ้าในขาออกแทน ดังนั้นยิ่งเพิ่มแรงดันไฟฟ้าให้มีค่าสูงขึ้นมากกระแสไฟฟ้าก็จะลดลงเป็นความสัมพันธ์แบบผกผันกัน

2.17 Docker

ทางเว็บไซต์ IBM [20] ได้กล่าวไว้ว่า Docker เป็นซอฟต์แวร์ที่ออกแบบและพัฒนาขึ้นมาเพื่อช่วยเหล่านักพัฒนาโปรแกรมในการสร้าง แชร์ และเรียกใช้งานแอปพลิเคชันที่สร้างขึ้นให้ง่ายขึ้น โดยเมื่อมีการใช้งานมักจะมีการใช้หลักการการแยกตัว และจะเกิดการจำลองสภาพแวดล้อมที่เรียกว่าคอนเทนเนอร์ (Container) ที่เป็นพื้นที่ที่แยกจากกันและมีความเป็นอิสระต่อกัน หรือเรียกได้ว่าเป็นเทคโนโลยี Containerization นำมาเพื่อใช้ในการสร้างหรือใช้งานแอปพลิเคชันหรือ service ต่าง ๆ โดยสามารถเลือกใช้ได้เฉพาะในส่วนที่จำเป็นเท่านั้นเพื่อเป็นการประหยัดพื้นที่ในการพัฒนา และยังช่วยให้ผู้พัฒนาสามารถรวมเอาแอปพลิเคชันทั้งหมดพร้อมกับสิ่งที่เกี่ยวข้องรวมไว้ใน Container ที่เรียกว่า Docker Image ซึ่งถือเป็นแบบจำลองของ Container โดยที่มีโปรแกรมและส่วนขยายต่าง ๆ ที่ต้องใช้งานอยู่ภายใน Image และเมื่อมีการสร้าง Container จาก Docker Image นั้น โปรแกรมและส่วนขยายที่อยู่ภายใน Image ก็จะถูกเรียกใช้งานโดยอัตโนมัติ จากนั้นสามารถสร้างและเรียกใช้งาน Container ต่าง ๆ ได้โดยง่าย ไม่ต้องกังวลเกี่ยวกับการติดตั้งหรือการจัดการสภาพแวดล้อม อีกทั้งยังช่วยให้ลดการติดตั้งและกำหนดสภาพแวดล้อมสำหรับแอปพลิเคชันได้ง่ายขึ้น โดยที่ไม่ต้องกังวลเกี่ยวกับโปรแกรมและส่วนขยายที่ต้องติดตั้งเพิ่มเติม หรือปัญหาการสร้างสภาพแวดล้อมที่แตกต่างกันไปในแต่ละเครื่อง และช่วยให้ผู้ใช้งานสามารถติดตั้งและรันแอปพลิเคชันบนเครื่อง Server หรือ Cloud ได้อย่างยืดหยุ่นและสะดวกสบายมากยิ่งขึ้น นอกจากนั้นทุกวันนี้ผู้พัฒนาซอฟต์แวร์ก็มักจะนิยมใช้ Docker เป็นส่วนมาก มักจะเห็น DockerFile ประกอบอยู่ในโปรเจคใหญ่หลาย ๆ ตัวในปัจจุบัน ซึ่ง DockerFile ถือเป็นไฟล์ที่มีคำสั่งสำหรับสร้าง Docker container image อยู่ภายใน DockerFile เป็นเครื่องมือที่ช่วยอัตโนมัติในการสร้าง Docker image โดยจะประกอบด้วยคำสั่งต่างๆ ที่เป็น Command Line Interface (CLI) ที่ Docker Engine จะทำงานตามลำดับเพื่อสร้าง Docker image โดยอัตโนมัติ

2.18 Dnsmasq

เป็นซอฟต์แวร์ที่ให้บริการเกี่ยวกับ Network service ต่าง ๆ [21] ที่จะเน้นไปทางด้าน DNS เช่น DNS Server, DNS Forwarder เป็นต้น ซึ่งเป็นซอฟต์แวร์ที่มีความเหมาะสมในการนำมาใช้งานกับอุปกรณ์ IoT หรืออุปกรณ์ Embedded ต่าง ๆ โดย Dnsmasq ถูกออกแบบมาให้ง่ายต่อการกำหนดค่าได้หลากหลาย เช่น การกำหนดที่อยู่ IP แบบคงที่ (Static IP) การกำหนดการส่งต่อ DNS เป็นต้น และสามารถใช้เป็น Local DNS cache เพื่อเพิ่มความเร็วในการเรียกดูเว็บไซต์บนเครือข่ายได้ อีกทั้งยังสามารถใช้ให้บริการ DNS โดยแปลงชื่อโดเมนเป็นที่อยู่ IP สำหรับเครื่องลูกข่ายบนเครือข่ายได้ โดยจะสามารถทำหน้าที่เป็น DHCP server เพื่อกำหนดที่อยู่ IP และการกำหนดค่าเครือข่ายอื่น ๆ ให้กับเครื่องลูกข่ายได้ นอกจากนี้ Dnsmasq ยังสามารถใช้งานบนหลายแพลตฟอร์ม เช่น Linux macOS และ Windows และสามารถผสานกับบริการเครือข่ายอื่น ๆ เพื่อให้ได้เป็นเครือข่ายที่ครบวงจร

2.19 Engine-X (Nginx)

เป็นซอฟต์แวร์แบบ open-source ที่ใช้สำหรับการให้บริการเว็บ [22] หรือเรียกว่าเว็บเซิร์ฟเวอร์ ซึ่งนิยมใช้กันในปัจจุบัน นอกจากนี้ยังมีโมดูลเสริมให้ใช้บริการ เช่น การทำ proxy, caching ใช้ในการทำโปรแกรมรับส่งข้อมูลระหว่างเครือข่าย (Reverse proxy) เป็นต้น ซึ่ง Nginx ถือเป็นเว็บเซิร์ฟเวอร์ตัวหนึ่งที่ออกแบบมาเพื่อประสิทธิภาพและมีความเสถียรที่ค่อนข้างสูง โดย nginx รองรับการทำงานในระบบแบบ Concurrent connections หรือการเชื่อมต่อพร้อมกันจำนวนมาก โดย nginx เหมาะสำหรับเว็บไซต์ที่มีการให้บริการแบบสม่ำเสมอ อีกทั้งยังสามารถใช้เป็น load balancer หรือตัวกลางในการจัดการเว็บเซิร์ฟเวอร์หลายเครื่องได้อีกด้วย ในปัจจุบันมีการใช้งาน Nginx เป็นเว็บเซิร์ฟเวอร์มากถึง 350 ล้านแห่งทั่วโลก รวมไปถึงบริษัทไอทียักษ์ใหญ่ เช่น Dropbox Netflix ก็มีการใช้งานในการส่งเนื้อหาของเว็บไซต์อย่างรวดเร็ว เชื่อถือได้ และปลอดภัยด้วยบริการของ Nginx ด้วยเช่นเดียวกัน

2.20 เครือข่ายส่วนบุคคลเสมือน (Virtual Private Network: VPN)

การจำลองช่องทางการสื่อสารทางอินเทอร์เน็ตแบบส่วนตัวระหว่างอุปกรณ์และระบบเครือข่ายภายใต้ช่องทางการสื่อสารของผู้ให้บริการอินเทอร์เน็ต (ISP) ซึ่ง VPN มีบทบาทสำคัญอย่างมากในด้านการทำงานและการปิดกั้นเนื้อหาต่าง ๆ เพราะจะช่วยในการปกปิด IP Address และเข้ารหัสข้อมูลต่าง ๆ ที่มีการสื่อสารในระหว่างการใช้งาน VPN ของผู้ใช้งาน

2.21 Lock picking

เป็นเทคนิคในการปลดล็อคแม่กุญแจ โดยจัดการกับส่วนของอุปกรณ์แม่กุญแจโดยไม่พึ่งกุญแจ ซึ่งเทคนิคนี้หากนำไปใช้ในทางที่ผิดจะมีความผิดฐานอาญา ซึ่งควรได้รับอนุญาตก่อนการกระทำ แต่ก็ถือเป็นทักษะที่สำคัญสำหรับช่างกุญแจเพื่อเข้าถึงสถานที่ที่ล็อคโดยไม่มีกุญแจ หรือใช้เพื่อเปิดแม่กุญแจที่ได้รับความเสียหาย/ใช้งานไม่ได้ ในขณะเดียวกันผู้ไม่หวังดีสามารถนำเทคนิคนี้ไปใช้ในการเข้าถึงสถานที่ต่าง ๆ โดยไม่ได้รับอนุญาตได้เช่นเดียวกัน

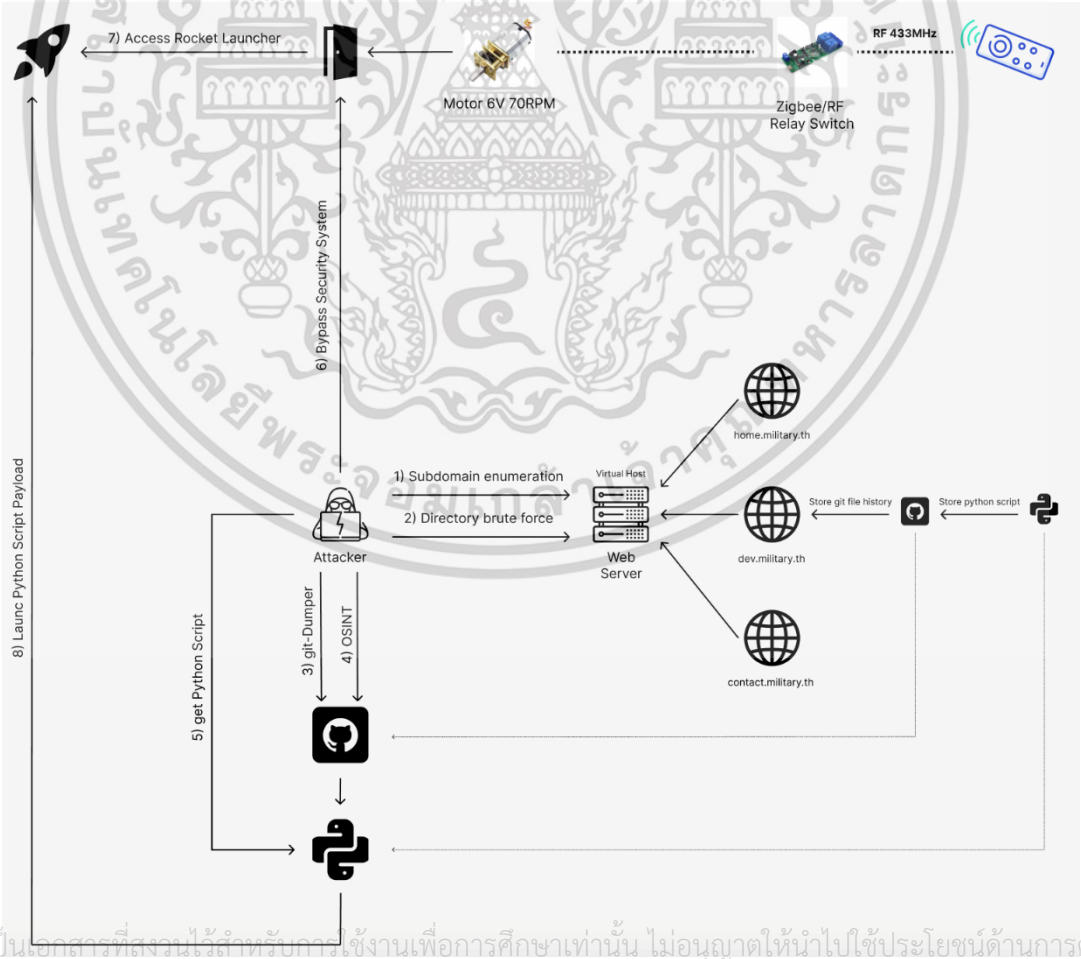
2.22 Replay attack

การโจมตีแบบทำซ้ำเป็นรูปแบบการโจมตีประเภทหนึ่งที่ผู้โจมตีสามารถทำการดักจับข้อมูลเอาไว้ [23] ด้วยวิธีการต่าง ๆ ตัวอย่างเช่น ข้อมูลถูกส่งในเครือข่ายที่ไม่มีความปลอดภัย และนำข้อมูลดังกล่าวกลับมาใช้งานใหม่ เพื่อทำการเข้าถึงหรือกระทำสิ่งต่าง ๆ กับระบบโดยไม่ได้รับอนุญาต

บทที่ 3
วิธีการดำเนินงานวิจัย

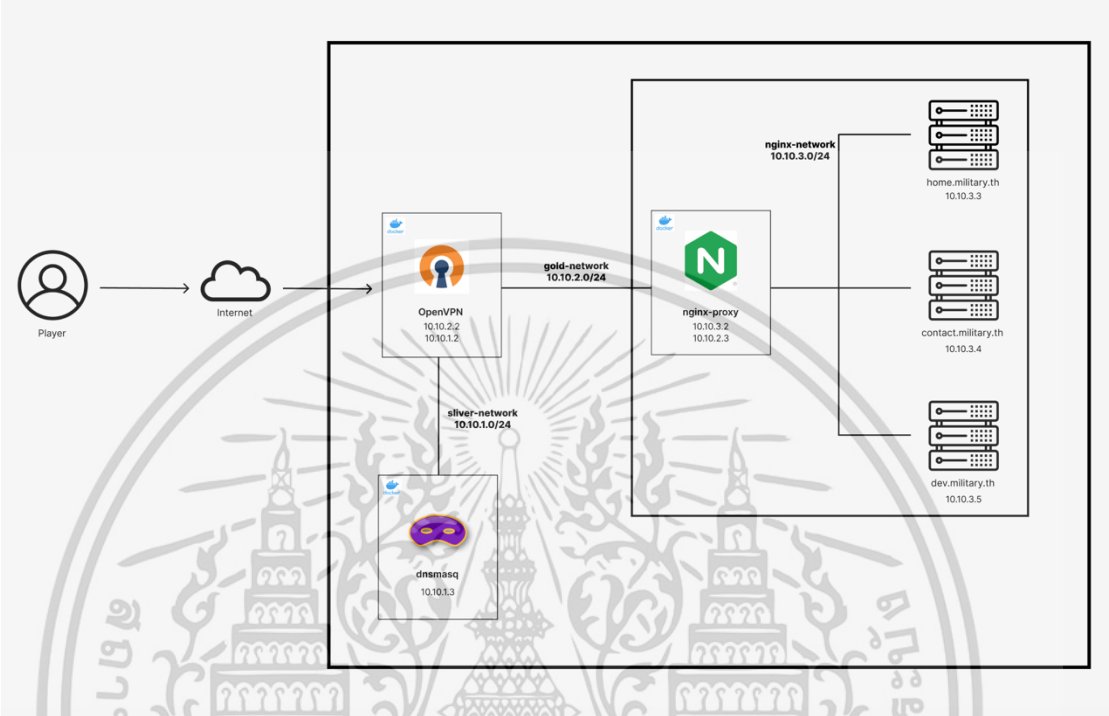
3.1 ขั้นตอนการจัดเตรียมระบบ

ทำการจำลองระบบโดยใช้อุปกรณ์ IoT ที่มีการสื่อสารผ่านโปรโตคอล Radio Frequency (RF) จำนวน 1 ตัว ได้แก่ RF Relay Switch ถือเป็นอุปกรณ์ที่รับสัญญาณคลื่นวิทยุจากรีโมทบังคับเพื่อควบคุมมอเตอร์ มาใช้ในการจำลองระบบควบคุมการเปิด-ปิดของประตูรั้วในสถานที่หวงห้าม ภายในกระทรวงกลาโหมที่มีการเก็บเครื่องยิงจรวดเอาไว้ ซึ่งภายในระบบจำลองจะมีเว็บเซิร์ฟเวอร์ให้ผู้โจมตีสามารถโจมตีเข้ามาได้จากอินเทอร์เน็ตเพื่อหาข้อมูลเกี่ยวกับชุดคำสั่งในการควบคุมเครื่องยิงจรวด เพื่อที่จะสามารถนำไปควบคุมการทำงานของเครื่องยิงจรวดภายในสถานที่หวงห้ามดังกล่าวภายในกระทรวงกลาโหมได้ ผ่านการโจมตีด้วยเทคนิค Replay attack ในระบบจำลองการควบคุมการเปิด-ปิดของประตูรั้วไฟฟ้า โดยใช้การดักจับสัญญาณรีโมทที่มีการสื่อสารผ่านโปรโตคอล Radio Frequency บนคลื่นความถี่ 433 MHz และทำการใช้สัญญาณดังกล่าวซ้ำ ๆ เพื่อทำการข้ามขั้นตอนการรักษาความปลอดภัยของพื้นที่หวงห้ามภายในกระทรวงกลาโหม เป็นไปตามภาพรวมของระบบแสดงดังรูปที่ 3.1



รูปที่ 3.1 แผนภาพแสดงภาพรวมของระบบ

การสร้างเครือข่ายและเครื่องเป้าหมายจำลองจะมีการใช้ docker ในการสร้าง โดยภายในเครือข่ายจำลองที่สร้างขึ้น ผู้ใช้งานสามารถเชื่อมต่อเข้าไปภายในเครือข่ายผ่านโปรแกรม OpenVPN เพื่อทำให้ใช้งานระบบรวมไปถึงเครื่องเป้าหมายภายในเครือข่ายจำลองได้ ซึ่งจะมีรายชื่อเครื่องต่าง ๆ และหมายเลข IP Address ที่ผู้จัดทำกำหนดในแต่ละเครื่องแตกต่างกันออกไปดังที่แสดงในรูปที่ 3.2



รูปที่ 3.2 แผนภาพแสดงเครือข่ายจำลองที่สร้างขึ้นโดย docker

3.1.1 การจัดเตรียมเว็บเซิร์ฟเวอร์

สำหรับเว็บไซต์ที่ใช้ภายในระบบจำลอง จะเป็นการนำรูปแบบเว็บไซต์มาจากเว็บไซต์ที่ใช้ในการออกแบบที่ชื่อว่า teleporthq โดยเซิร์ฟเวอร์ที่ใช้ในการรันเว็บไซต์จะมีระบบปฏิบัติการเป็น Debian GNU/Linux version 11.0 ที่ได้มีการติดตั้ง nginx version 1.23.2 ไว้ภายใน โดยที่ทั้งหมดจะรันอยู่บน Docker Container

ในการติดตั้งเว็บไซต์เอาไว้ภายใน Docker Container จะมีการสร้าง Docker Image โดยใช้ไฟล์ Dockerfile เนื่องจากโครงสร้างของเว็บเป้าหมายจะต้องสร้าง 1 Docker Container ต่อ 1 Web page ทำให้มีการใช้งาน Dockerfile ในจำนวนที่เท่ากับจำนวนหน้าของเว็บไซต์ (ซึ่งในที่นี้คือ 4 ไฟล์ นับรวมไฟล์ Dockerfile ของ nginx-proxy ด้วย) ผู้จัดทำจึงได้เขียนไฟล์ docker-compose.yml ให้มีการเรียกใช้ไฟล์ Dockerfile ไว้ให้เรียบร้อย เพื่อให้ง่ายต่อการใช้คำสั่งในการสร้าง โดยภายในจะมีการระบุว่าจะตั้งค่า Docker Container อย่างไร และให้ใช้ networks ตัวใดในการสื่อสาร ดังที่แสดงในรูป 3.3

docker-compose.yml

web > docker-compose.yml

```yaml
version: '3.5'

services:
    nginx-proxy:
        cap_add:
            - NET_ADMIN
        # image: nginxproxy/nginx-proxy
        build:
            context: ./
            dockerfile: dockerfile.nginx
        ports:
            - '80:80'
        volumes:
            - /var/run/docker.sock:/tmp/docker.sock:ro
        networks:
            nginx-network:
                ipv4_address: 10.10.3.2

            gold-network:
                ipv4_address: 10.10.2.3

    site-home:
        container_name: front-home
        restart: unless-stopped
        build:
            context: ./
            dockerfile: dockerfile.home
        environment:
            - VIRTUAL_HOST=home.military.th
            - VIRTUAL_PORT=80
        networks:
            nginx-network:
                ipv4_address: 10.10.3.3

    site-contact:
        container_name: front-contact
        restart: unless-stopped
        build:
            context: ./
            dockerfile: dockerfile.contact
        environment:
            - VIRTUAL_HOST=contact.military.th
            - VIRTUAL_PORT=80
        networks:
            nginx-network:
                ipv4_address: 10.10.3.4

    site-dev:
        container_name: front-dev
        restart: unless-stopped
        build:
            context: ./
            dockerfile: dockerfile.dev
        environment:
            - VIRTUAL_HOST=dev.military.th
            - VIRTUAL_PORT=80
        networks:
            nginx-network:
                ipv4_address: 10.10.3.5

networks:
    nginx-network:
        name: nginx
        driver: bridge
        ipam:
            config:
                - subnet: 10.10.3.0/24
                  gateway: 10.10.3.1

    gold-network:
        name: gold
        driver: bridge
        ipam:
            config:
                - subnet: 10.10.2.0/24
                  gateway: 10.10.2.1
```

รูปที่ 3.3 docker-compose.yml ของเว็บไซต์เป้าหมาย

จากไฟล์ docker-compose.yml ที่ผู้จัดทำได้สร้างขึ้น ทำให้สามารถทำการสร้าง Docker Image และทำการรัน Docker Container ได้ง่ายจากคำสั่งเพียงคำสั่งเดียว ได้แก่

```
$ docker-compose up –build -d
```

3.1.2 การจัดเตรียมเซิร์ฟเวอร์ DNS

สำหรับเซิร์ฟเวอร์ DNS ถูกนำมาใช้ในการกำหนดชื่อโดเมนและหมายเลข IP Address ให้กับเว็บไซต์เป้าหมายภายในเครือข่ายจำลอง โดยมีการดึง Docker Image ที่มีชื่อว่า jpillora/dnsmasq จาก Docker hub มาใช้งาน ซึ่งผู้จัดทำได้สร้างไฟล์ docker-compose.yml แสดงดังรูปที่ 3.4 ให้มีการสร้าง container ตามไฟล์ Dockerfile ที่มีการระบุไว้ดังรูปที่ 3.5 โดยภายในไฟล์ Dockerfile ได้มีการเรียกใช้ Shell script ไฟล์ที่มีชื่อว่า start ที่ผู้จัดทำได้สร้างชุดคำสั่งในการทำ Network routing เอาไว้ดังรูปที่ 3.6

docker-compose.yml

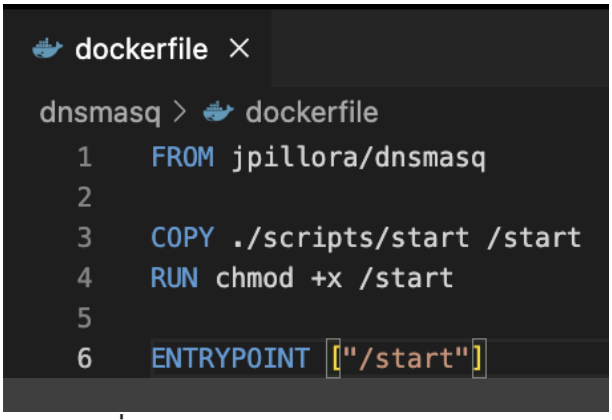
dnsmasq > docker-compose.yml

```yaml
version: '3'

services:
  dnsmasq-multiarch:
    cap_add:
      - NET_ADMIN
    container_name: dnsmasq
    # image: outlyernet/dnsmasq-multiarch
    build:
      context: ./
      dockerfile: dockerfile
    # ports:
      # - '53/udp'
      # - '80/tcp'
    volumes:
      - './dnsmasq.conf:/etc/dnsmasq.conf'
    logging:
      options:
        max-size: 100m
    environment:
      - HTTP_USER=admin_system_dnsmasq_project
      - HTTP_PASS=admin_system_dnsmasq_AsKTsvUspOsxa1sWtsaXplm24XTsaePflag
    restart: unless-stopped
    networks:
      sliver-network:
        ipv4_address: 10.10.1.3

networks:
  sliver-network:
    external:
      name: sliver
```

รูปที่ 3.4 docker-compose.yml ของเซิร์ฟเวอร์ DNS



รูปที่ 3.5 Dockerfile ของเซิร์ฟเวอร์ DNS

รูปที่ 3.6 Shell script ในการทำ Network Routing ของเซิร์ฟเวอร์ DNS

จากไฟล์ docker-compose.yml ที่ผู้จัดทำได้สร้างขึ้น ทำให้สามารถทำการสร้าง Docker Image และทำการรัน Docker Container ได้ง่ายจากคำสั่งเพียงคำสั่งเดียว ได้แก่

```
$ docker-compose up –build -d
```

3.1.3 การจัดเตรียมเซิร์ฟเวอร์ OpenVPN

เซิร์ฟเวอร์ OpenVPN ถูกนำมาใช้เพื่อให้ผู้ใช้งานสามารถเชื่อมต่อเข้าไปยังเครือข่ายจำลองที่สร้างขึ้นได้ โดยมีการดึง Docker Image ที่มีชื่อว่า kylemanna/openvpn จาก Docker hub มาใช้งาน ซึ่งผู้จัดทำได้สร้างไฟล์ docker-compose.yml เพื่อให้ง่ายต่อการใช้งานในการสร้าง Docker image ผู้ใช้งานสามารถติดตั้งและตั้งค่าเซิร์ฟเวอร์ OpenVPN ได้ตามชุดคำสั่งด้านล่าง โดยชุดคำสั่งจะดำเนินการสร้าง Docker Container ขึ้นมาใช้งาน ไปจนถึงขั้นตอนในการกำหนดให้เซิร์ฟเวอร์ OpenVPN นั้นรันอยู่ภายใต้หมายเลข IP Address ของเครือข่ายจำลองตามที่ผู้จัดทำกำหนดคือ 34.143.229.118 และให้ทำการสร้างโฟลเดอร์ openvpn-data ขึ้นมาซึ่งเป็นที่สำหรับจัดเก็บ Configuration file ของเซิร์ฟเวอร์

```
# Initialize and generate OpenVPN config file
$ docker-compose run --rm openvpn ovpn_genconfig -u udp://34.143.229.118:1194

# Fix ownership
$ sudo chown -R $(whoami): ./openvpn-data

# Start OpenVPN server
$ docker-compose up --build -d openvpn
```

เมื่อทำการสร้างและเปลี่ยนแปลงสิทธิในการเข้าถึง Configuration file ภายในโฟลเดอร์ openvpn-data ตามคำสั่งด้านบนเรียบร้อยแล้ว ให้ทำการแก้ไข Configuration file โดยทำการเพิ่มเซิร์ฟเวอร์ DNS เข้าไปภายในเพื่อให้เซิร์ฟเวอร์ OpenVPN สามารถรู้จักและรับช่องทางการสื่อสารซึ่งกันและกันได้ และทำการ comment บรรทัดสำหรับ DNS ที่เป็นเลข 8.8.4.4 ออก สามารถดูตัวอย่างในการแก้ไขได้ดังนี้

```
...
push “block-outside-dns”

### Add this line
push “dhcp-option DNS 10.10.1.3”
=============================
push “dhcp-option DNS 8.8.8.8”

### Comment this line
# push “dhcp-option DNS 8.8.4.4”
=============================

push "comp-lzo no"
...
```

จากนั้นจะต้องทำ Network routing ให้กับ Docker container ของ OpenVPN เพื่อให้สามารถสื่อสารกับ container อื่น ๆ ได้โดยไม่ติดปัญหา หลังจากตั้งค่าทุกอย่างเสร็จเรียบร้อยให้ทำการ restart OpenVPN server container เพื่อให้ container นำค่าการตั้งค่าไปใช้งาน โดยชุดคำสั่งในการทำ Network routing มีดังนี้

```
$ docker exec -it <OPENVPN_SERVER_CONTAINER> bash
$ route add -net 10.10.2.0 netmask 255.255.255.0 gw 10.10.2.1

# restart OpenVPN server container
$ docker-compose restart <OPENVPN_SERVER_CONTAINER>
```

เมื่อมีการตั้งค่าทุกอย่างเสร็จเรียบร้อย ต่อไปจะเป็นขั้นตอนในการสร้างไฟล์ OpenVPN สำหรับ Client ที่จะนำไปใช้ในการเชื่อมต่อเข้ามายังเครือข่ายจำลอง ซึ่งเมื่อทำการสร้างเสร็จเรียบร้อยแล้วจะได้ไฟล์สกุล .ovpn สำหรับนำไปใช้งานกับซอฟต์แวร์ OpenVPN Connect โดยสามารถทำการสร้างตามชุดคำสั่งต่อไปนี้

```
# Generate a client certificate
$ export CLIENTNAME="your_client_name"
$ docker-compose run --rm openvpn easyrsa build-client-full $CLIENTNAME nopass

$ docker-compose run --rm openvpn ovpn_getclient
  $CLIENTNAME > $CLIENTNAME.ovpn
```

เพื่อความสะดวกสบายในการใช้งานในครั้งต่อ ๆ ไปหลังจากมีการตั้งค่าเซิร์ฟเวอร์ OpenVPN เสร็จเรียบร้อยตามกระบวนการข้างต้นแล้ว ผู้ใช้งานสามารถสร้างและรัน Docker container สำหรับ OpenVPN ด้วยคำสั่งดังนี้

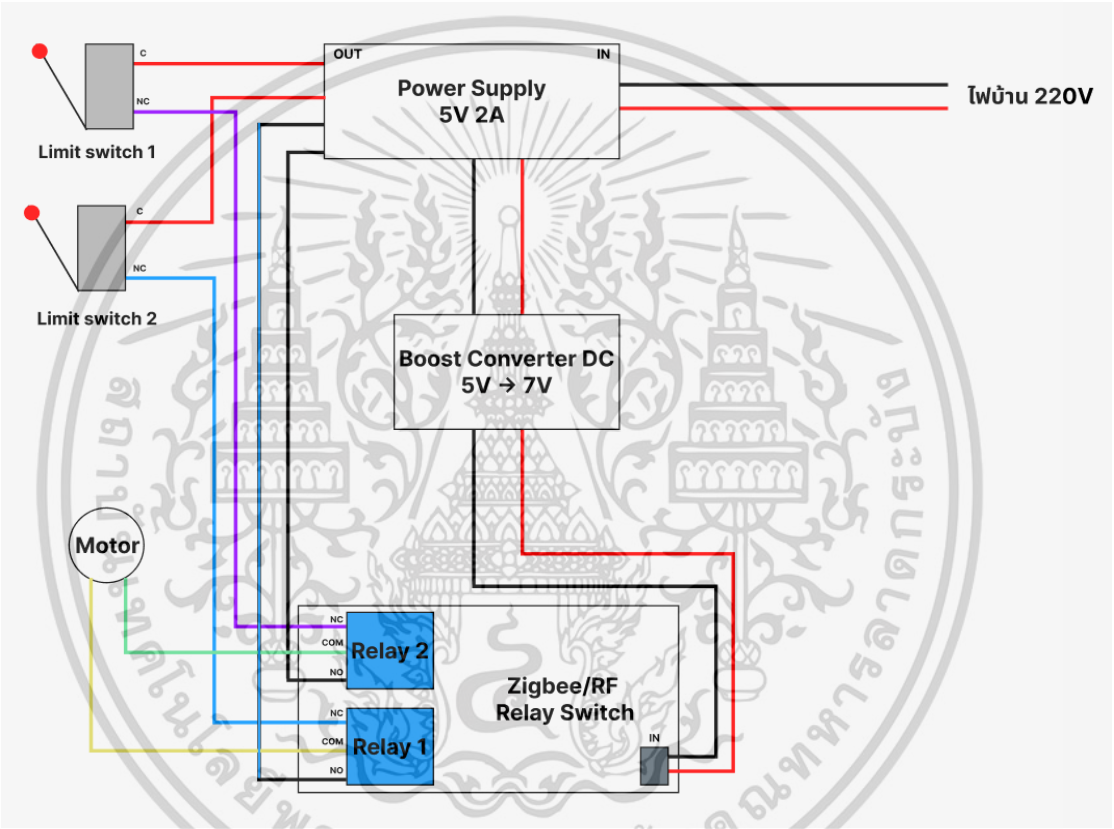
```
docker-compose up --build -d
```

3.1.4 การจัดเตรียมอุปกรณ์ Hardware

สำหรับอุปกรณ์ Hardware ที่นำมาใช้ในการจำลองระบบประตูรั้วไฟฟ้าที่มีการสื่อสารและสั่งการผ่านรีโมท RF ในความถี่ 433 MHz ประกอบไปด้วยอุปกรณ์ต่าง ๆ ดังนี้

1. RF Relay Switch ขนาด 2 Relay จำนวน 1 ตัว
2. Boost Converter DC จำนวน 1 ตัว
3. Power Supply 5V 2A จำนวน 1 ตัว
4. Gear Motor 6V 70RPM จำนวน 1 ตัว
5. Limit Switch จำนวน 2 ตัว

โดยนำอุปกรณ์ทั้งหมดมาทำการเชื่อมต่อกันด้วยสายไฟ และทำการบัดกรีเข้าด้วยกันเพื่อให้สามารถใช้งานเป็นระบบประตูรั้วไฟฟ้าได้ตามเป้าหมาย ตามแผนภาพ Boxology Circuit แสดงดังรูปที่ 3.7

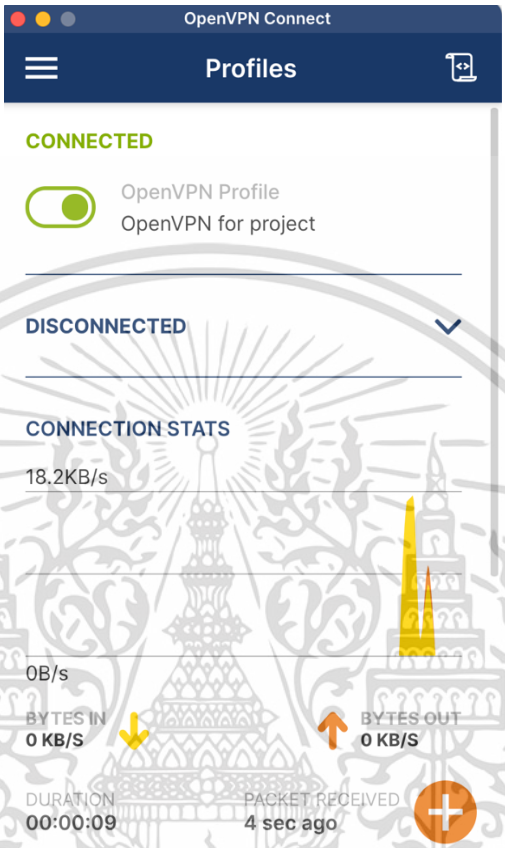


รูปที่ 3.7 แผนภาพ Boxology Circuit

3.2 ขั้นตอนการโจมตีระบบ

การโจมตีจะเป็นการโจมตีเป็นส่วน ๆ เพื่อค้นหาข้อมูลและเบาะแสต่าง ๆ ในการขยายผลการโจมตี ซึ่งจากระบบจำลองที่ได้จัดเตรียมขึ้นจะต้องโจมตีเข้ามาจากเว็บเซิร์ฟเวอร์ก่อนจากนั้นจึงค่อยขยายผลการโจมตีไปยังส่วนอื่น เพื่อที่จะเข้าควบคุมเครื่องยิงจรวดที่ตั้งอยู่ในพื้นที่หวงห้ามภายในกระทรวงกลาโหม โดยมีขั้นตอนในการโจมตีทั้งหมด ดังนี้

ก่อนที่จะเข้าสู่กระบวนการโจมตีเว็บเซิร์ฟเวอร์ ผู้โจมตีจะต้องทำการเชื่อมต่อ OpenVPN ตามไฟล์ client ที่มีการจัดเตรียมไว้ก่อน เพื่อให้สามารถเข้าถึงเครือข่ายและระบบจำลองที่สร้างขึ้นมาได้ โดยการเชื่อมต่อสามารถเชื่อมต่อได้ผ่านซอฟต์แวร์ OpenVPN Connect แสดงดังรูป 3.8

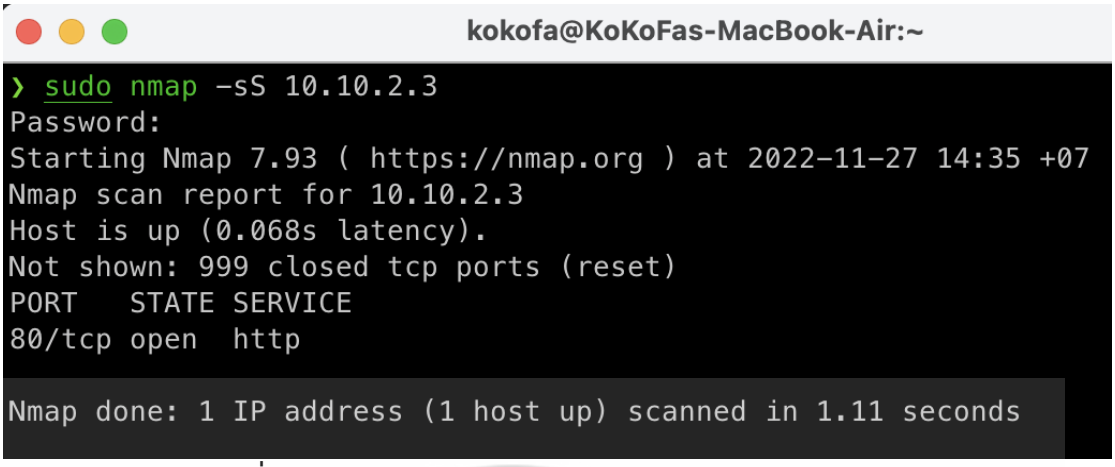


รูปที่ 3.8 การเชื่อมต่อ OpenVPN ผ่านซอฟต์แวร์ OpenVPN Connect

3.2.1 การโจมตีเว็บเซิร์ฟเวอร์

เริ่มต้นจากการทำการสแกนหาพอร์ตที่ระบบเปิดอยู่ด้วยโปรแกรมในการสแกนหาพอร์ต เช่น nmap เป็นต้น โดยในการจำลองนี้เว็บไซต์เป้าหมายจะมีหมายเลข IP address คือ 10.10.2.3 พบว่ามีพอร์ต 80 เปิดอยู่ซึ่งเป็นพอร์ตสำหรับ Hypertext Transfer Protocol (HTTP) แสดงดังรูปที่ 3.9 โดยสามารถทำได้โดยใช้คำสั่งต่อไปนี้

```
$ sudo nmap -sS <IP_ADDRESS>
```



รูปที่ 3.9 ผลลัพธ์จากการสแกนหาพอร์ตของระบบด้วย nmap

จากนั้นให้ทำการเข้าถึงเว็บไซต์ผ่านเว็บเบราว์เซอร์ จะพบกับหน้า home ของเว็บไซต์กระทรวงกลาโหมที่จำลองขึ้น แสดงดังรูปที่ 3.10 ซึ่งมีฟังก์ชันที่สามารถใช้งานได้อยู่บน navigation bar ที่ลิงก์ไปยังหน้าช่องทางการติดต่อ

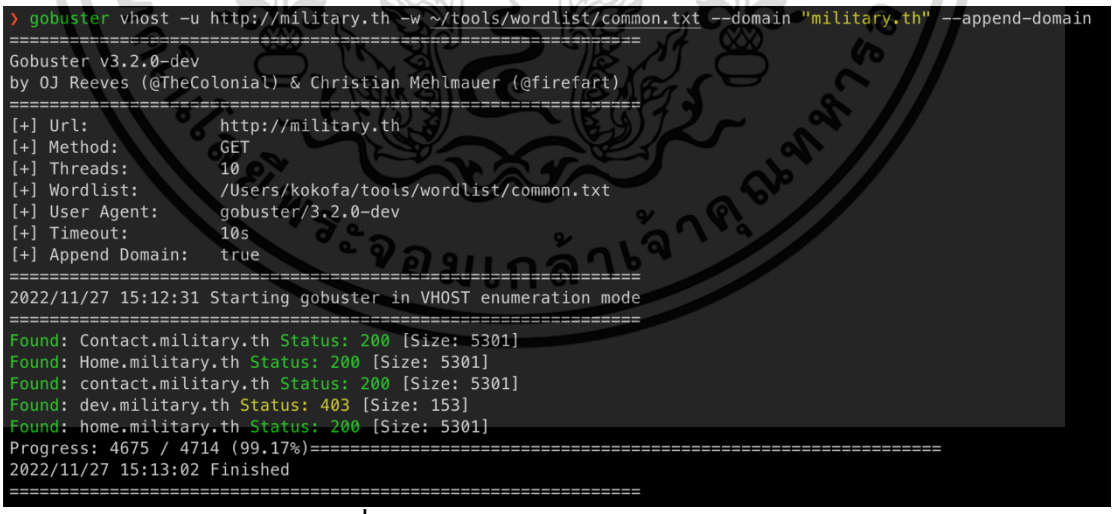
รูปที่ 3.10 เว็บไซต์หน้า Home

เมื่อเข้าถึงหน้าช่องทางการติดต่อ ผู้โจมตีสามารถสังเกตได้จาก Address bar จะพบกับโดเมน (Domain) ที่ใช้ชื่อว่า military.th และมีโดเมนย่อย (Subdomain) ที่ใช้ชื่อว่า contact แสดงดังรูปที่ 3.11 ซึ่งเป็นข้อมูลที่บ่งชี้ว่าเว็บไซต์อาจจะมีการเปิดใช้งานโดเมนย่อย จึงนำไปสู่การโจมตีเพื่อค้นหาโดเมนย่อย (Subdomain enumeration) เพื่อใช้ในการขยายผลการโจมตีได้

รูปที่ 3.11 เว็บไซต์หน้า Contact

การโจมตีเพื่อค้นหาโดเมนย่อยสามารถใช้โปรแกรมโจมตีแบบอัตโนมัติได้ ตัวอย่างเช่น FFUF, gobuster เป็นต้น โดยในที่นี้จะใช้การส่งคำสั่งผ่านโปรแกรม gobuster ในการโจมตีเพื่อค้นหาโดเมนย่อยบนเว็บไซต์ พบว่ามีโดเมนย่อยอื่น ๆ ที่สามารถเข้าถึงได้ เช่น dev.cybercity.com โดยมีผลลัพธ์ของการใช้โปรแกรม gobuster แสดงดังรูปที่ 3.12

```
$ gobuster vhost -u http://military.th -w ~/tools/wordlist/common.txt
--domain "military.th" --append-domain
```

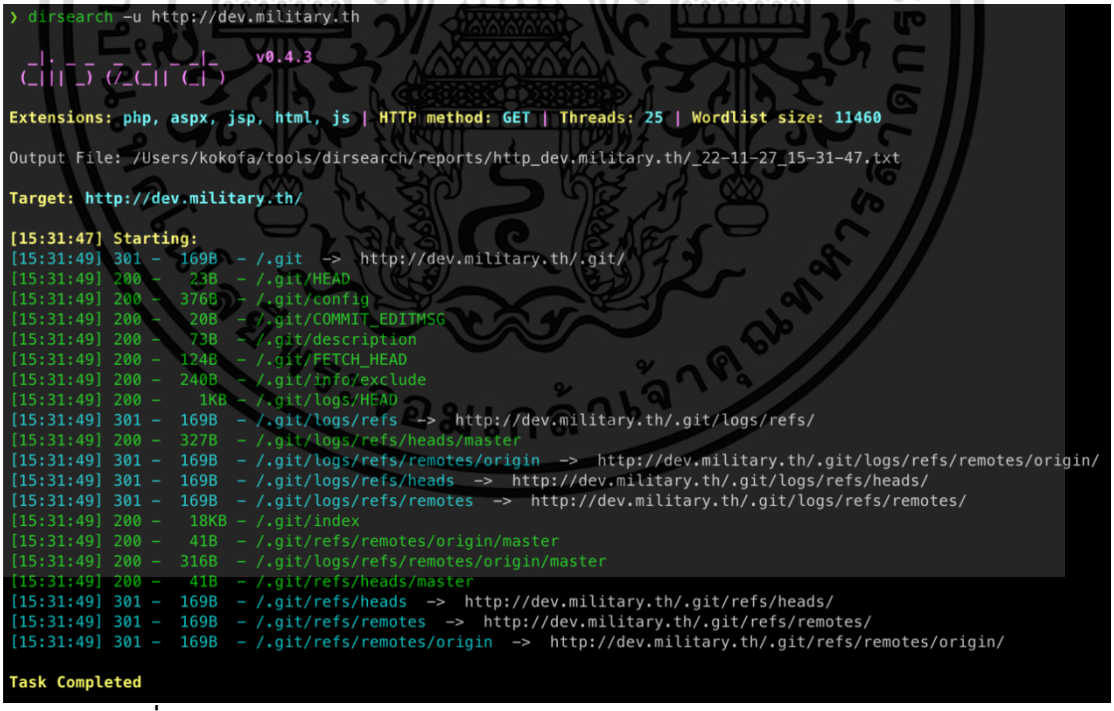


รูปที่ 3.12 ผลลัพธ์จากโปรแกรม gobuster

ไปที่ dev.cybercity.com พบว่าระบบมีการตอบกลับ HTTP Status เป็น 403 Forbidden แสดงดังรูปที่ 3.13 โดยที่ผู้โจมตีสามารถทำ directory brute-force ที่ dev.military.th โดยใช้โปรแกรมโจมตีแบบอัตโนมัติ ตัวอย่างเช่น dirsearch, FUFF เป็นต้น เพื่อหาว่ามี directory ใดบ้างที่สามารถเชื่อมต่อได้ แสดงดังรูปที่ 3.14

```
$ dirsearch -u http://dev.military.th
```

รูปที่ 3.13 เว็บไซต์ที่มีการแสดง Error ในหน้า dev



รูปที่ 3.14 ผลลัพธ์จากการทำ directory brute-force ของระบบด้วย dirsearch

ผลลัพธ์จากการทำ Directory brute-force พบว่าสามารถเข้าถึงโฟลเดอร์ /.git ได้ ซึ่งเป็นโฟลเดอร์ที่มีข้อมูลสำคัญต่าง ๆ ของโครงการที่ถูกเก็บไว้ใน git repository เพื่อควบคุมเวอร์ชัน ดังนั้นผู้โจมตีสามารถใช้เครื่องมือ git-dumper ในการดึงไฟล์สำคัญดังกล่าวออกมาได้ แสดงดังรูปที่ 3.15 พบว่าได้ไฟล์ rocket_port3.py ซึ่งคาดเดาได้จากชื่อไฟล์ว่าเป็นไฟล์ที่ใช้ในการควบคุมเครื่องยิงจรวดที่เป็นเป้าหมายในการโจมตี แสดงดังรูปที่ 3.16

```
$ ./git-dumper http://dev.military.th ~/tools/dump
```

```
❯ ./git_dumper.py http://dev.military.th ~/tools/dump
[-] Testing http://dev.military.th/.git/HEAD [200]
[-] Testing http://dev.military.th/.git/ [403]
[-] Fetching common files
[-] Fetching http://dev.military.th/.git/description [200]
[-] Fetching http://dev.military.th/.git/hooks/applypatch-msg.sample [200]
[-] Fetching http://dev.military.th/.git/COMMIT_EDITMSG [200]
[-] Fetching http://dev.military.th/.gitignore [500]
[-] http://dev.military.th/.gitignore responded with status code 500
[-] Fetching http://dev.military.th/.git/hooks/post-commit.sample [500]
[-] http://dev.military.th/.git/hooks/post-commit.sample responded with status code 500
[-] Fetching http://dev.military.th/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/commit-msg.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/post-receive.sample [500]
[-] http://dev.military.th/.git/hooks/post-receive.sample responded with status code 500
[-] Fetching http://dev.military.th/.git/hooks/post-update.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/pre-commit.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/prepare-commit-msg.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/pre-rebase.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/pre-receive.sample [200]
[-] Fetching http://dev.military.th/.git/objects/info/packs [500]
[-] Fetching http://dev.military.th/.git/info/exclude [200]
[-] http://dev.military.th/.git/objects/info/packs responded with status code 500
[-] Fetching http://dev.military.th/.git/hooks/pre-push.sample [200]
[-] Fetching http://dev.military.th/.git/hooks/update.sample [200]
[-] Fetching http://dev.military.th/.git/index [200]
[-] Finding refs/
[-] Fetching http://dev.military.th/.git/FETCH_HEAD [200]
[-] Fetching http://dev.military.th/.git/HEAD [200]
```

รูปที่ 3.15 ผลลัพธ์ของเครื่องมือ git-dumper

รูปที่ 3.16 ไฟล์ python ที่ได้จากการใช้เครื่องมือ git-dumper

ทำการเปิดและตรวจสอบเนื้อหาไฟล์ rocket_port3.py ด้วยโปรแกรม Visual Studio Code พบข้อมูลสำคัญว่าจะต้องมีไฟล์อีกหนึ่งไฟล์ในการติดต่อ port 10 ให้ได้ก่อนเนื่องจากการกำหนดของอุปกรณ์ถึงจะควบคุมเครื่องยิงจรวดได้สำเร็จ และพบคำใบ้เพิ่มเติมถูกบันทึกอยู่ภายในว่าชุดคำสั่งที่ได้รับอยู่ใน version 1.2 และอาจจะมีการอัพเดท version ใหม่ ๆ โดยการ commit ขึ้นมาบน git ที่ได้รับ แสดงดังรูปที่ 3.17

รูปที่ 3.17 ภายในไฟล์ rocket_port3.py มีการบันทึกข้อมูลสำคัญ

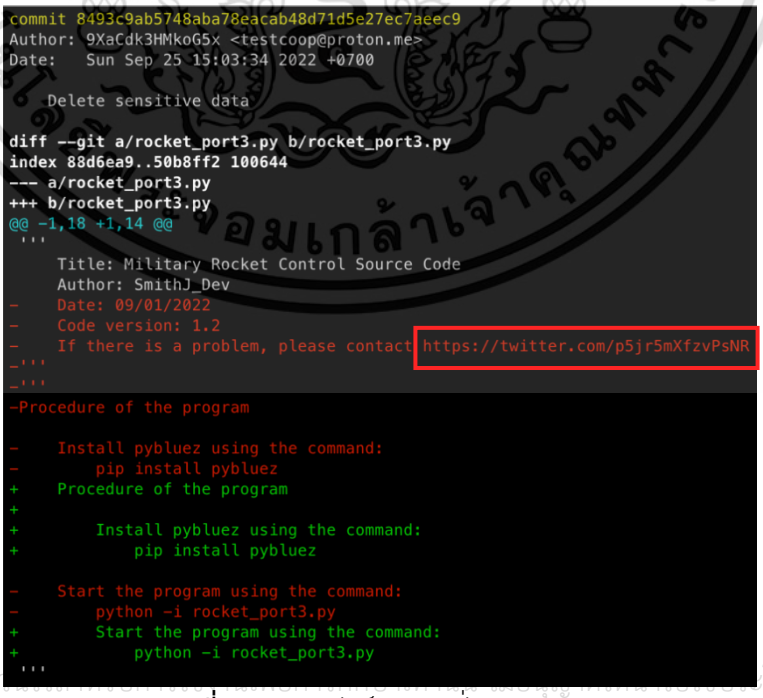
เมื่อผู้โจมตีเห็นข้อมูลที่พอจะเดาได้ว่าอาจมีข้อมูลสำคัญอื่น ๆ อยู่ภายใน git commit ผู้โจมตีจึงได้เข้าถึงประวัติการ commit ของ git โดยใช้คำสั่ง git log แสดงดังรูปที่ 3.18 พบว่ามีการ commit ที่บ่งชี้ถึงการลบข้อมูลสำคัญบางอย่างออกจากไฟล์ดังกล่าว

```
$ git log
```

รูปที่ 3.18 ผลลัพธ์ของคำสั่ง git log

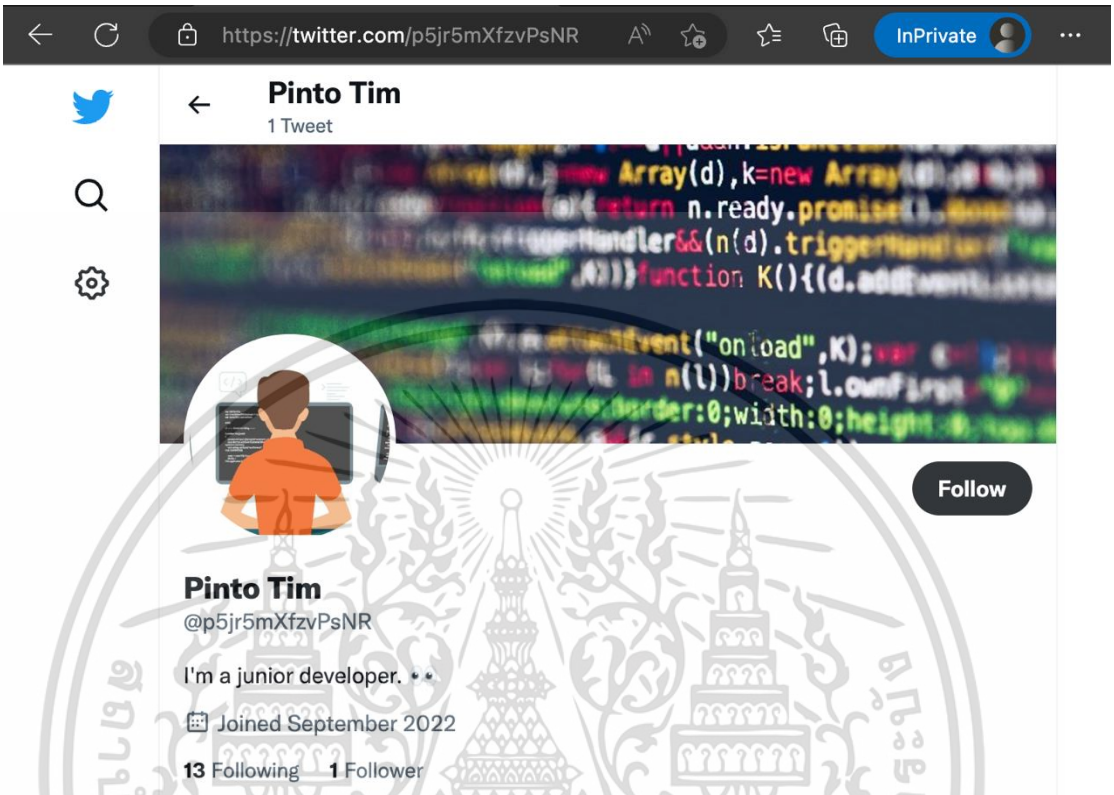
ผู้โจมตีสามารถใช้คำสั่ง git show ในการแสดงประวัติการแก้ไขของไฟล์ตามรหัสของ commit ที่สนใจ พบว่ามีลิงก์ในการเข้าถึงหน้า Twitter ของผู้พัฒนาโปรแกรม แสดงดังรูปที่ 3.19

```
$ git show <COMMIT_ID>
```



รูปที่ 3.19 ผลลัพธ์ของคำสั่ง git show

เมื่อผู้โจมตีได้ทำการค้นหาบัญชี Twitter ของผู้พัฒนาจากข้อมูลที่รั่วไหลจากการทำ git commit ของ source code มาเรียบร้อยดังแสดงในรูปที่ 3.20 ผู้โจมตีจึงได้ทำการ OSINT จนพบบัญชี Twitter อีกหนึ่งบัญชีจากการติดตามบัญชีของผู้พัฒนาคนดังกล่าวไว้ แสดงดังรูปที่ 3.21

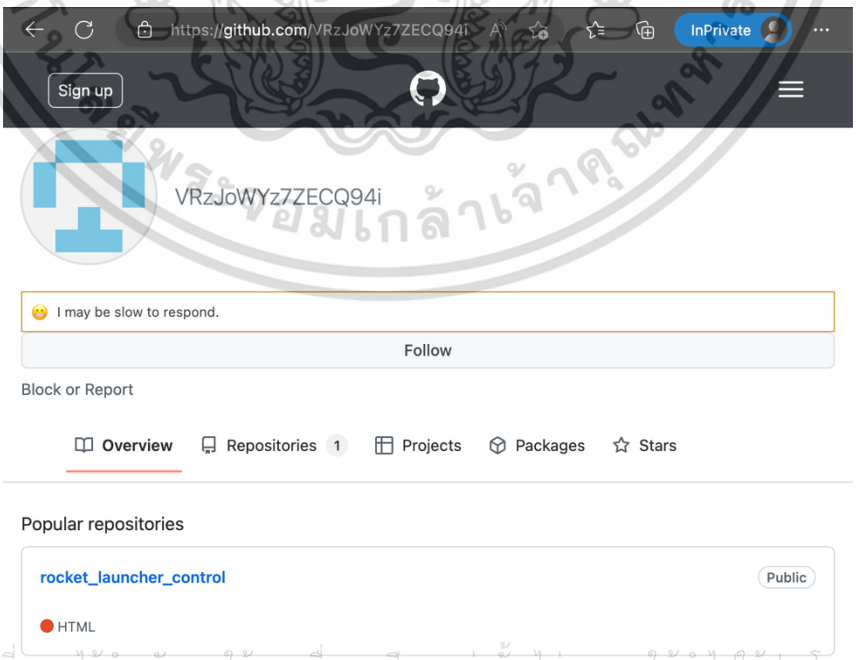


รูปที่ 3.20 บัญชี Twitter ของผู้พัฒนา

รูปที่ 3.21 บัญชี Twitter ที่มีการติดตามบัญชีของผู้พัฒนา

ซึ่งภายในบัญชีของ Smith James มีการระบุ github ไว้ที่หน้าโปรไฟล์แสดงดังรูปที่ 3.22 และภายใน github ดังกล่าวมี repository ที่มีการเก็บไฟล์ควบคุมจรวดอีกไฟล์หนึ่งเอาไว้ดังรูปที่ 3.23 ซึ่งถือเป็นข้อมูลที่ผู้โจมตีต้องการเพื่อใช้ยึดเครื่องยิงจรวดตามเป้าหมาย

รูปที่ 3.22 Github ที่ระบุในหน้าบัญชี Twitter



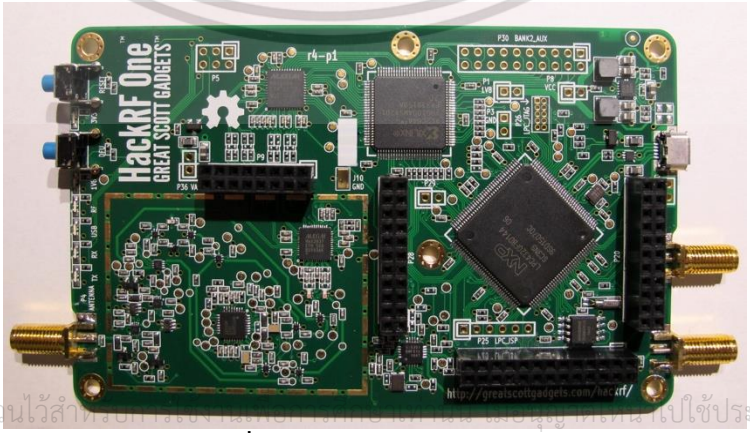
รูปที่ 3.23 หน้า github ที่มี repository ที่มีการเก็บไฟล์ควบคุมจรวด

เมื่อผู้โจมตีได้ข้อมูลต่าง ๆ จนครบถ้วนพร้อมที่จะทำการยึดเครื่องยิงจรวดที่ตั้งอยู่ในพื้นที่หวงห้ามของกระทรวงกลาโหมแล้ว ผู้โจมตีได้ออกเดินทางไปยังพื้นที่ดังกล่าวและพบกับระบบรักษาความปลอดภัยที่ประตูทั้งสองชั้น โดยประตูรั้วด้านนอกเป็นประตูอัตโนมัติที่ควบคุมผ่านรีโมทสัญญาณ RF 433 MHz และเมื่อผ่านเข้าไปได้จะพบกับประตูที่มีการรักษาความปลอดภัยด้วยแม่กุญแจอีกชั้นหนึ่ง ซึ่งผู้โจมตีสามารถโจมตีเพื่อข้ามขั้นตอนรักษาความปลอดภัยของประตูได้ ดังนี้

3.2.2 การโจมตีระบบประตูรั้วไฟฟ้า

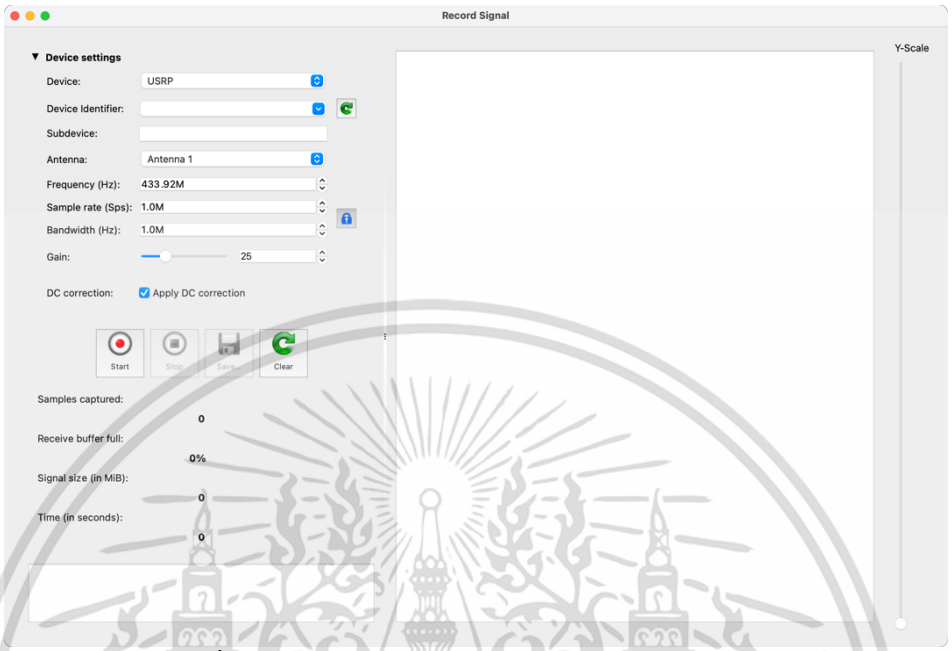
ผู้โจมตีจะต้องใช้เครื่องมือที่ชื่อว่า Universal Radio Hacker (URH) (GitHub: https://github.com/jopohl/urh) พร้อมทั้ง Hardware ที่มีชื่อว่า HackRF แสดงดังรูปที่ 3.24 และ 3.25 ตามลำดับ เพื่อช่วยในการดักจับสัญญาณ Radio Frequency และทำการโจมตีด้วยเทคนิค Replay attack เพื่อทำการข้ามขั้นตอนการรักษาความปลอดภัยของประตูภายในพื้นที่หวงห้ามในกระทรวงกลาโหม

รูปที่ 3.24 Github ของเครื่องมือ Universal Radio Hacker (UAH)



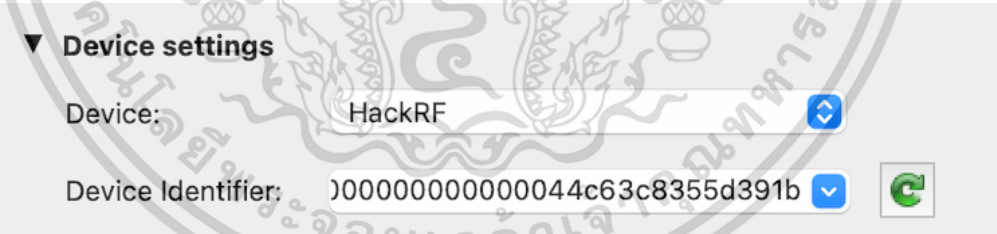
รูปที่ 3.25 HackRF hardware

เมื่อทำการติดตั้งเครื่องมือเรียบร้อยแล้ว ให้ทำการเปิดโปรแกรมพร้อมทั้งต่ออุปกรณ์ Hardware ที่ใช้สำหรับการโจมตีเข้ากับเครื่องคอมพิวเตอร์ที่จะใช้ในการโจมตี จากนั้นไปที่เมนู File >> Record signal เพื่อทำการดักจับสัญญาณรีโมทของผู้ใช้งาน แสดงดังรูปที่ 3.26



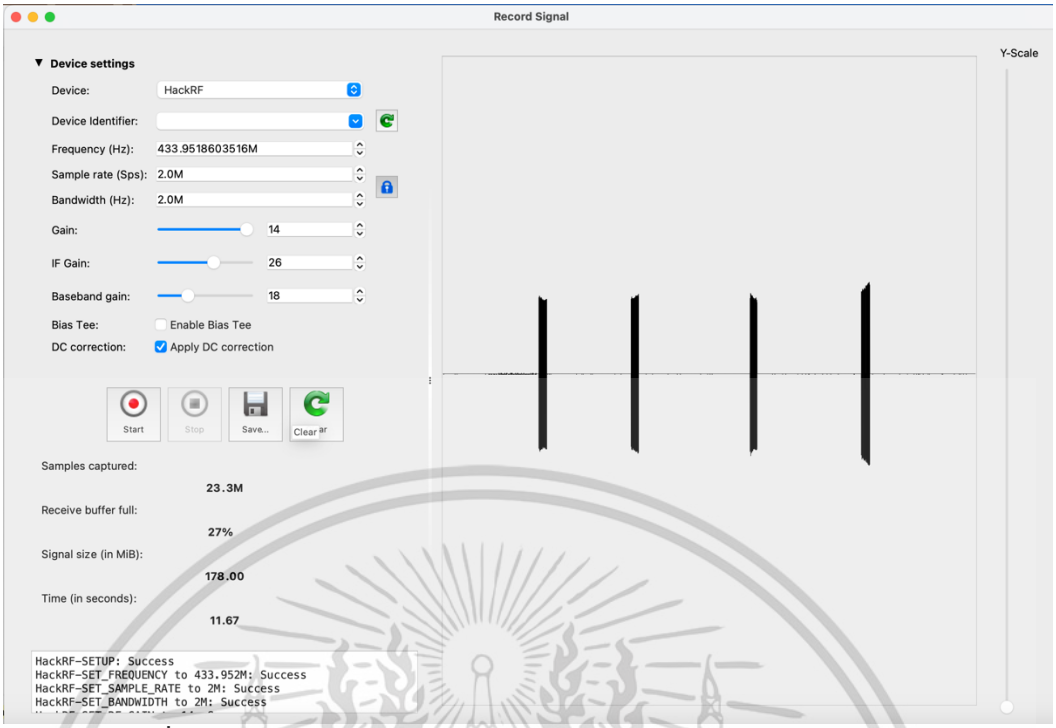
รูปที่ 3.26 เมนู Record Signal ภายในโปรแกรม UAH

จากนั้นทำการตั้งค่าโปรแกรมโดยเลือก Device ให้เป็น HackRF และ Device Identifier ให้เป็นอุปกรณ์ Hardware ที่ต่อกับเครื่องคอมพิวเตอร์ในการโจมตี แสดงดังรูปที่ 3.27 หรือสามารถกดปุ่มลูกศรสีเขียวเพื่อให้โปรแกรมทำการ Identify ให้อัตโนมัติ



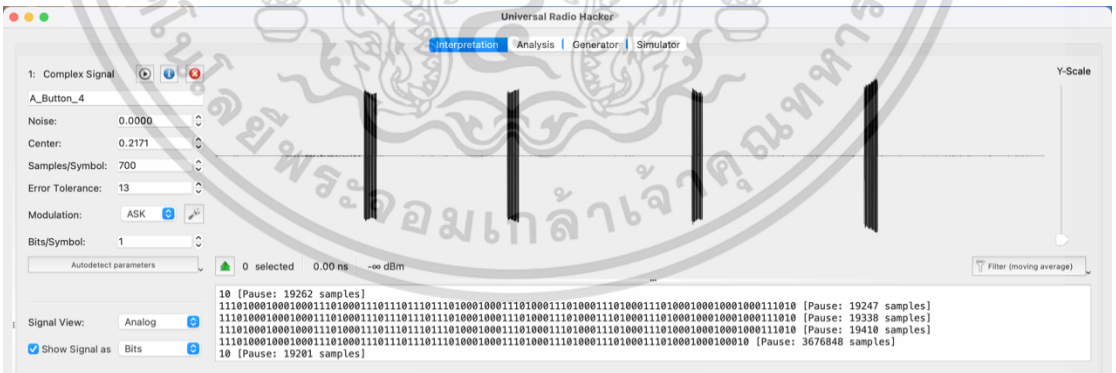
รูปที่ 3.27 การตั้งค่าอุปกรณ์บนโปรแกรม UAH

เมื่อทำการตั้งค่าโปรแกรมเสร็จเรียบร้อยแล้ว ผู้โจมตีสามารถนำชุดอุปกรณ์ในการโจมตีนี้ไปทำการดักจับสัญญาณการเปิด-ปิดประตูรั้วไฟฟ้าที่สื่อสารผ่านโปรโตคอล Radio Frequency บนคลื่นความถี่ 433 MHz ได้ โดยทำการกดปุ่ม Start เพื่อทำการ record signal เมื่อทำการดักจับสัญญาณได้แล้วจะปรากฏรูปคลื่นสัญญาณในด้านขวาของโปรแกรม แสดงดังรูป 3.28



รูปที่ 3.28 การดักจับสัญญาณ Radio Frequency ภายในโปรแกรม UAH

เมื่อผู้โจมตีสามารถดักจับสัญญาณได้แล้ว ให้ทำการปิดหน้าต่างเมนู Record Signal และให้ไปยังเมนู Interpretation ภายในโปรแกรม แสดงดังรูปที่ 3.29 เพื่อทำการวิเคราะห์สัญญาณและเตรียมทำการโจมตีด้วยเทคนิค Replay attack ซึ่งภายในเมนูดังกล่าวจะปรากฏรูปคลื่นสัญญาณที่ทำการดักจับมาได้



รูปที่ 3.29 เมนู Interpretation ภายในโปรแกรม UAH

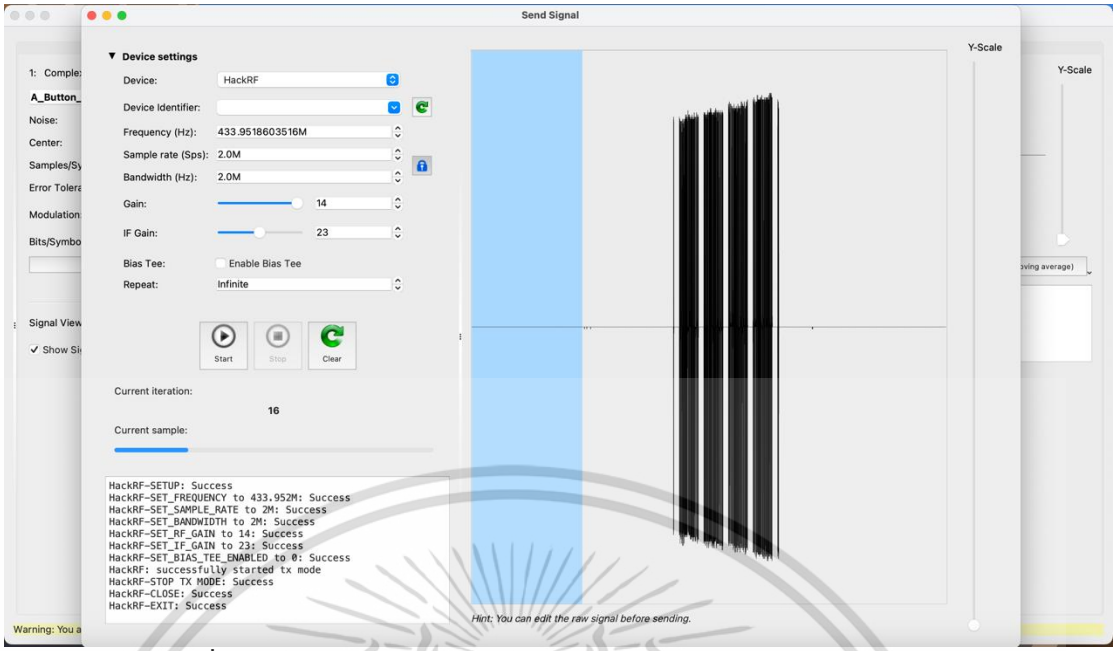
จากนั้นผู้โจมตีสามารถเลือกรูปคลื่นสัญญาณที่เหมาะสมในช่วงใดช่วงหนึ่งได้ โดยการลากเมาส์คลุมคลื่นสัญญาณที่ต้องการ จากนั้นทำการคลิกเมาส์ขวาเพื่อเลือกฟังก์ชัน Crop to selection ในการตัดออกมาเฉพาะคลื่นสัญญาณที่ต้องการ แสดงดังรูปที่ 3.30

รูปที่ 3.30 การเลือกช่วงสัญญาณที่ต้องการภายในโปรแกรม UAH

เมื่อผู้โจมตีทำการเลือกช่วงคลื่นสัญญาณเสร็จเรียบร้อยแล้ว บริเวณ preview ที่ปรากฏรูปคลื่นสัญญาณจะเปลี่ยนแปลงไป จากนั้นให้ผู้โจมตีทำการกดปุ่ม Replay signal บริเวณซ้ายมือของรูปคลื่นสัญญาณ เพื่อทำการโจมตีด้วยเทคนิค Replay attack แสดงดังรูปที่ 3.31

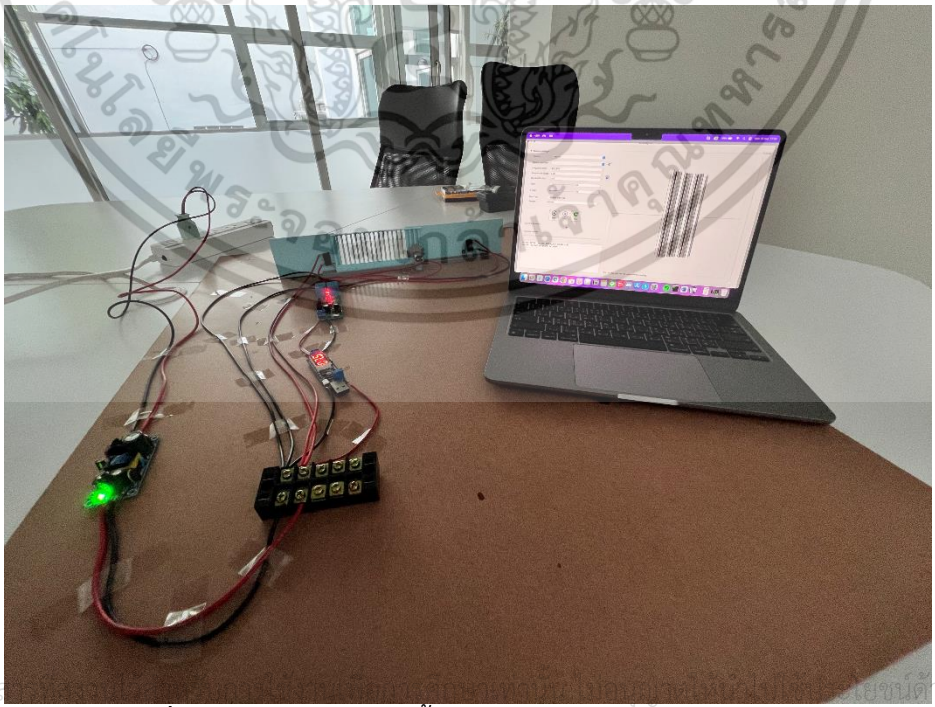
รูปที่ 3.31 การเตรียมพร้อมในการโจมตีด้วยเทคนิค Replay attack

เมื่อทำการกดปุ่ม Replay signal แล้ว ผู้โจมตีจะพบกับหน้าต่าง Send Signal ปรากฏขึ้นมา ให้ทำการตั้งค่าอุปกรณ์เช่นเดียวกันกับรูปที่ 3.27 และสามารถตั้งค่าจำนวนครั้งในการส่งสัญญาณซ้ำได้ที่ช่อง Repeat โดยค่า default จะอยู่ที่ Infinite เมื่อทำการตั้งค่าเสร็จเรียบร้อยแล้วผู้โจมตีจะสามารถโจมตีด้วยเทคนิค Replay attack ได้ทันทีด้วยการกดปุ่ม Start แสดงดังรูปที่ 3.32



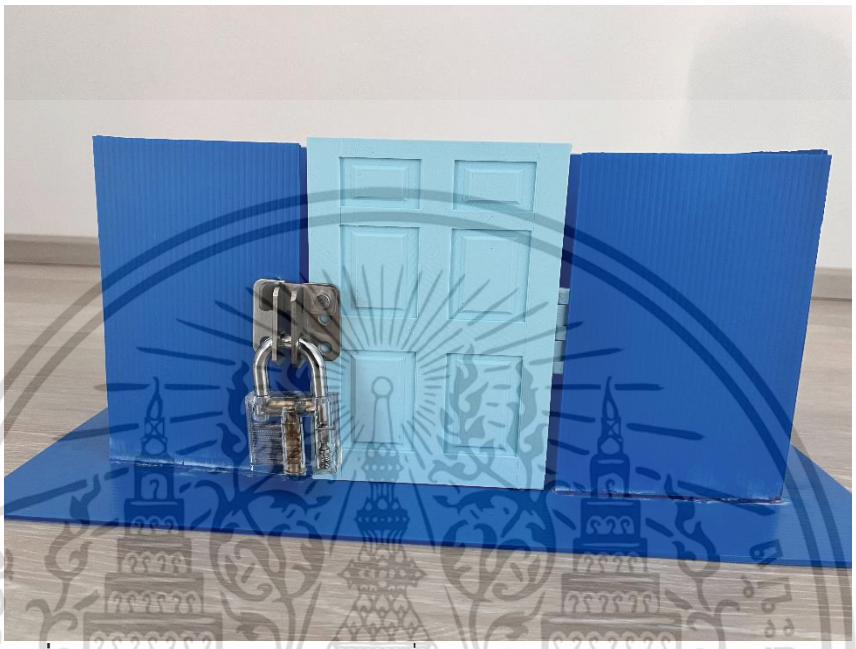
รูปที่ 3.32 การโจมตีด้วยเทคนิค Replay attack โดยใช้โปรแกรม UAH

ผลลัพธ์ของการโจมตีขั้นตอนการรักษาความปลอดภัยของประตูรั้วไฟฟ้าภายในพื้นที่หวงห้ามในกระทรวงกลาโหม พบว่าระบบจำลองที่สร้างขึ้นจะมีการรับสัญญาณที่ผู้โจมตีทำการส่งไปยังชุดควบคุมการทำงานของประตูรั้วไฟฟ้า ทำให้เกิดการทำงานเปิด-ปิดของประตูรั้วไฟฟ้าตามที่ผู้โจมตีต้องการ โดยที่ผู้โจมตีไม่จำเป็นต้องมีรีโมทที่แท้จริงในการควบคุมการทำงานของประตูรั้วไฟฟ้า ซึ่งทำให้ผู้โจมตีสามารถบุกรุกเข้าไปยังสถานที่หวงห้ามแห่งนี้ได้ โดยได้มีการทำชิ้นงานในการจำลองระบบประตูรั้วไฟฟ้าขึ้นแสดงดังรูปที่ 3.33



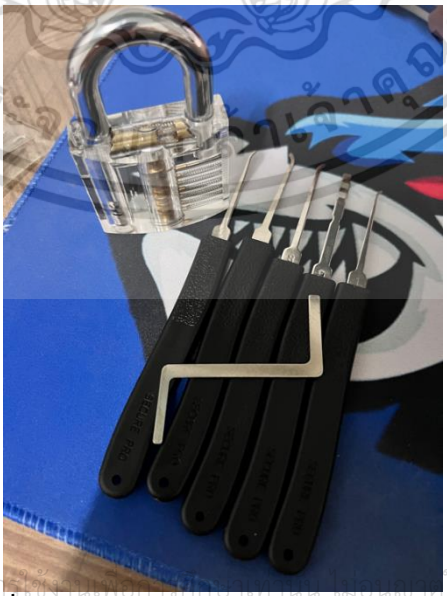
รูปที่ 3.33 การโจมตีประตูรั้วไฟฟ้าด้วยเทคนิค Replay attack

เมื่อผู้โจมตีสามารถข้ามขั้นตอนรักษาความปลอดภัยของประตูรั้วไฟฟ้าในด่านแรกมาได้แล้ว จะต้องมาพบกับประตูอีกชั้นหนึ่งที่มีการรักษาความปลอดภัยเอาไว้ด้วยแม่กุญแจ ทำให้ผู้โจมตีจะต้องใช้การโจมตีทางกายภาพ (Physical attack) ด้วยเทคนิคที่เรียกว่า Lock picking เพื่อทำการเข้ายึดเครื่องยิงจรวดที่เป็นเป้าหมายในการโจมตีให้ได้ โดยได้มีการทำโมเดลจำลองของระบบประตูที่มีการรักษาความปลอดภัยด้วยแม่กุญแจแสดงดังรูปที่ 3.34



รูปที่ 3.34 โมเดลจำลองระบบประตูที่มีการรักษาความปลอดภัยด้วยแม่กุญแจ

โดยผู้โจมตีสามารถใช้ชุดอุปกรณ์เฉพาะในการทำ Lock picking แสดงดังรูปที่ 3.35 เพื่อทำการปลดล็อคแม่กุญแจที่ถือเป็น access control ของประตูชั้นใน ในการโจมตีเพื่อข้ามขั้นตอนรักษาความปลอดภัยได้



รูปที่ 3.35 ชุดอุปกรณ์ในการทำ Lock picking

โดยหลักการของการทำ Lock picking คือการจัดการกับส่วนประกอบของแม่กุญแจเพื่อทำการปลดล็อคโดยที่ไม่ต้องพึ่งพาการใช้กุญแจ โดยทั่วไปแล้วคนจะใช้กุญแจเสียบเข้าไปในแม่กุญแจและใช้แรงกดและบิดเพื่อทำการปลดล็อค ดังนั้นชุดอุปกรณ์เฉพาะในการทำ Lock picking จะแบ่งเป็น 2 ส่วน เรียกว่า pick และ tension แสดงดังรูปที่ 3.36 โดยที่ pick เปรียบเสมือนรอยหยักบนกุญแจ ใช้สำหรับทำหน้าที่ในการยก pin ภายในแม่กุญแจให้เข้าที่ตามกำหนด ส่วน tension เป็นแท่งหมุนที่คอยส่งแรงบิดไปที่กระบอกล็อคภายในแม่กุญแจเพื่อให้หมุนได้เสมือนการบิดกุญแจ

รูปที่ 3.36 ลักษณะของ pick (ซ้าย) และ tension (ขวา) ในการทำ Lock picking

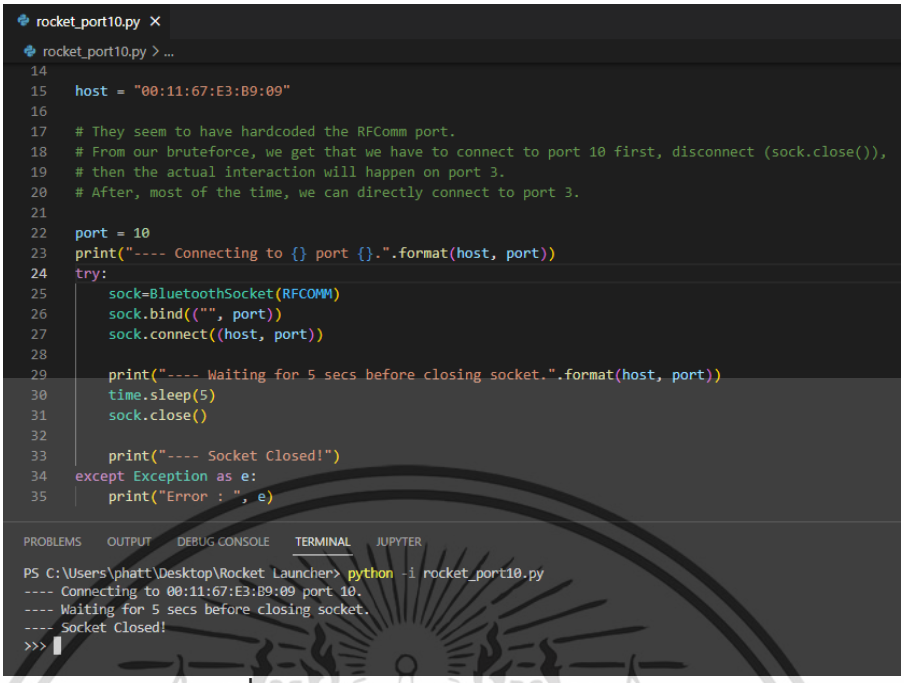
เมื่อผู้โจมตีสามารถโจมตีเพื่อข้ามขั้นตอนรักษาความปลอดภัยของประตูทั้งสองมาเพื่อทำการเข้าถึงเครื่องยิงจรวดได้เรียบร้อยแล้ว ผู้โจมตีสามารถที่จะรันไฟล์ที่ได้รับจากช่วงการโจมตีเว็บเซิร์ฟเวอร์ก่อนจะมาถึงพื้นที่หวงห้าม ที่เขียนด้วยภาษา Python เพื่อเข้าควบคุมเครื่องยิงจรวด

โดยเริ่มต้นจากการติดตั้งทรัพยากรที่ Python scripts ต้องการ นั่นคือโมดูลตัวหนึ่งที่ชื่อว่า pybluez ซึ่งเป็นโมดูลที่อนุญาตให้ Python เข้าถึง Bluetooth ของเครื่องได้ โดยสามารถติดตั้งได้โดยใช้โปรแกรม pip ที่มาพร้อมกับ Python ด้วยคำสั่งต่อไปนี้

```
pip install pybluez
```

เมื่อทำการติดตั้งเรียบร้อยแล้ว ให้เข้าไปยังไฟล์ rocket_port10.py เพื่อทำการรัน scripts ในการติดต่อ socket ของเครื่องยิงจรวดก่อนทำการควบคุมด้วยคำสั่งของภาษา Python แสดงดังรูปที่ 3.37

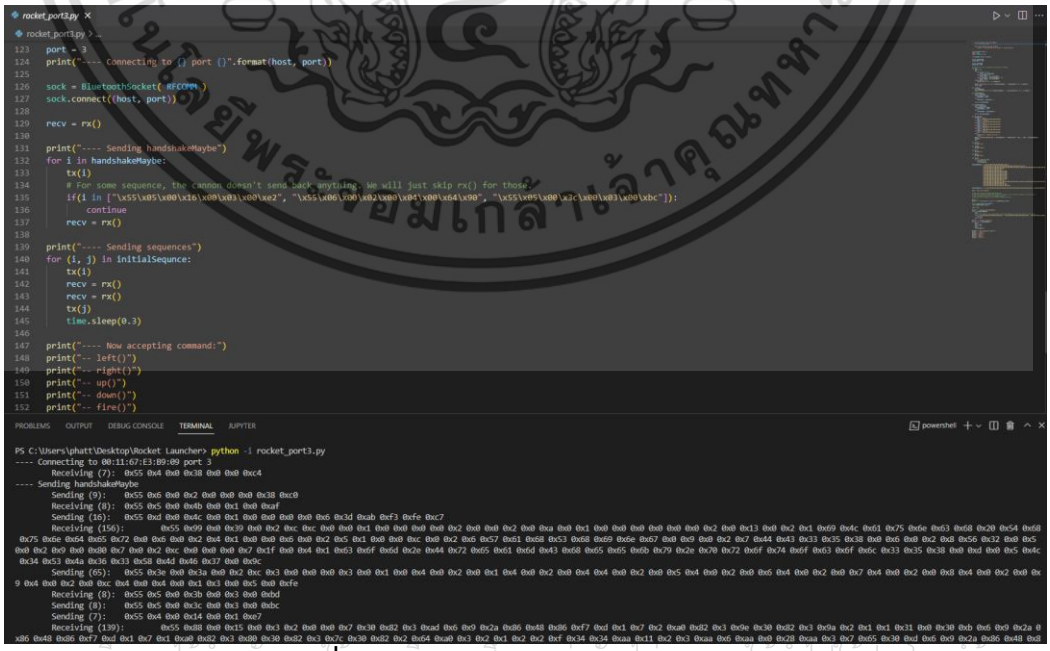
```
python -i rocket_port10.py
```



รูปที่ 3.37 รัน scripts ในการติดต่อ port 10

เมื่อทำการรัน Python script เพื่อทำการติดต่อ port10 เรียบร้อยแล้ว ให้เข้าไปยังไฟล์ rocket_port3.py เพื่อทำการรัน Python script อีกชุดหนึ่งเพื่อเข้าควบคุมเครื่องยิงจรวด ด้วยคำสั่งของภาษา Python และเมื่อทำการรันเสร็จเรียบร้อยโปรแกรมจะรอรับคำสั่งในการควบคุมเครื่องยิงจรวดจากผู้โจมตี แสดงดังรูปที่ 3.38 และรูปที่ 3.39

```
python -i rocket_port3.py
```



รูปที่ 3.38 รัน scripts ในการติดต่อ port3

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPYTER

        Sending (9):    0x55 0x6 0x0 0x2 0x0 0x4 0x0 0x64 0x90
        Sending (10):   0x55 0x7 0x0 0x3f 0x0 0x2 0x0 0x1 0x1 0xb6
        Receiving (9):  0x55 0x6 0x0 0x41 0x0 0x2 0x0 0x3f 0x78
---- Sending sequences
        Sending (18):   0x55 0xf 0x0 0x43 0x0 0x3 0x0 0x1 0xa 0x30 0x30 0x30 0x30 0x30 0x46 0x30 0xd 0x2d
        Receiving (9):  0x55 0x6 0x0 0x41 0x0 0x3 0x0 0x43 0x73
        Receiving (33): 0x55 0x1e 0x0 0x42 0x0 0x5 0x0 0x1 0xa 0x30 0x30 0x30 0x30 0x37 0x46 0x37 0xd 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0xf
        Sending (9):    0x55 0x6 0x0 0x2 0x0 0x5 0x0 0x42 0xb1
---- Now accepting command:
-- left()
-- right()
-- up()
-- down()
-- fire()
>>> left()
        Sending (18):   0x55 0xf 0x0 0x43 0x0 0x4 0x0 0x1 0xa 0x30 0x38 0x30 0x30 0x30 0x46 0x38 0xd 0x2c
        Receiving (9):  0x55 0x6 0x0 0x41 0x0 0x4 0x0 0x43 0x72
>>>
```

รูปที่ 3.39 โปรแกรมรอรับคำสั่งในการควบคุมเครื่องยิงจรวดจากผู้โจมตี

บทที่ 4
ผลการวิจัยและการอภิปรายผล

การโจมตีทุกรูปแบบที่ได้มีการจำลองผ่านมานั้น มีทั้งการอาศัยช่องโหว่ที่เกิดขึ้นบนระบบหรืออุปกรณ์ รวมถึงการตั้งค่าที่ไม่เหมาะสมจากผู้พัฒนา เนื่องจากผู้พัฒนาไม่มีความตระหนักรู้ถึงความปลอดภัยทางไซเบอร์ โดยการโจมตีทุกรูปแบบสามารถเป็นหนทางให้ผู้โจมตีสามารถขยายผลการโจมตีเป็นวงกว้างต่อระบบได้

4.1 สาเหตุและความเสียหายที่เกิดขึ้นจากการโจมตี

4.1.1 สาเหตุของการโจมตี

ในช่วงไม่กี่ปีหลังที่ผ่านมานี้ จะเห็นได้ว่าโลกมักจะเกิด Cyber attack อยู่บ่อยครั้ง ทำให้เราสามารถพบเห็นการโจมตีในหลายรูปแบบมากขึ้นตามข่าวต่าง ๆ รวมไปถึง Cyberwarfare ซึ่งก็คือ Cyber attack ที่มีเป้าหมายทางการทหารหรือสงครามระหว่างประเทศทางด้านไซเบอร์ก็มีเพิ่มขึ้นอยู่เป็นประจำในทุกวัน ตัวอย่างเช่น สงครามรัสเซีย-ยูเครนก็มีการโจมตี Cyberwarfare ด้วยเช่นกัน ก่อนที่จะมีการกล่าวถึงผลกระทบและวิธีการแก้ไขของช่องโหว่ต่าง ๆ ที่เกิดขึ้น เว็บไซต์ CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (CSIS) ได้มีการจัดทำ Significant Cyber Incidents ที่เกี่ยวกับกลาโหมหรือทางการทหารของประเทศต่าง ๆ บนโลก โดยได้มีการระบุรูปแบบที่พบในการโจมตีทาง Cyberwarfare ได้ดังนี้

1. การโจรกรรมทางไซเบอร์ (Espionage)

เป็นการใช้เทคนิคต่าง ๆ ในการสอดส่องประเทศอื่น ๆ เพื่อขโมยความลับหรือข้อมูลที่มีความละเอียดอ่อนของประเทศออกไปเพื่อกระทำในสิ่งที่ไม่สมควร โดยอาจใช้เทคนิคต่าง ๆ เช่น การทำ spear phishing attacks เป็นต้น

2. การโจมตีแบบการปฏิเสธบริการ (Denial-of-service: DOS)

เป็นการโจมตีที่ทำให้ไม่สามารถเข้าถึงเว็บไซต์หรือบริการใด ๆ ที่ตกเป็นเป้าหมายเพื่อขัดขวาง ถ่วงเวลา การปฏิบัติการและระบบที่สำคัญของประเทศอื่น ๆ โดยใช้การส่งคำขอปลอมเข้าไปจำนวนมากทำให้ระบบไม่สามารถให้บริการได้ตามปกติ

3. การโฆษณาชวนเชื่อ (Propaganda Attacks)

เป็นการโจมตีที่เล่นกับจิตวิทยาของคนในการหลงเชื่อโฆษณาชวนเชื่อ หรือการประชาสัมพันธ์ในทางที่ผิดที่นำข้อมูลที่น่าอับอายมาเปิดเผย ทำให้ผู้คนสูญเสียความไว้วางใจในประเทศของตนเองและในที่สุดก็เข้าข้างฝ่ายศัตรู

4. การโจมตีทางเศรษฐกิจ (Economic Disruption)

ระบบเศรษฐกิจสมัยใหม่ในปัจจุบันมักใช้คอมพิวเตอร์เพื่อช่วยในการทำงาน โดยการโจมตีรูปแบบนี้จะโจมตีที่เครือข่ายของคอมพิวเตอร์ที่อำนวยความสะดวกทางธุรกิจ เช่น ตลาดหุ้น ระบบการชำระเงิน ระบบธนาคาร เป็นต้น ทำให้ผู้โจมตีอาจเข้าถึงเงินทุนหรือนำเงินไปใช้ประโยชน์ในทางที่ผิดได้ หรือเป็นการที่ทำให้เป้าหมายไม่ได้รับเงินที่ควรจะได้รับ

4.1.2 ผลกระทบของการโจมตี

จุดประสงค์ในการทำ Cyberwarfare นั้นก็เพื่อการทำสงครามระหว่างประเทศในรูปแบบใหม่ ๆ โดยผลกระทบของการโจมตีหรือการเกิด Cyberwarfare นั้นมีหลากหลาย ยกตัวอย่างได้ดังนี้

1. ข้อมูลที่สำคัญถูกโจรกรรม

ในแต่ละประเทศมักจะมีข้อมูลที่สำคัญในชั้นความลับเก็บเอาไว้ หากเกิดการโจมตีทางไซเบอร์เกิดขึ้นข้อมูลเหล่านั้นอาจถูกเป็นเป้าหมายในการโจรกรรมออกไป เพื่อทำการเปิดเผยหรือทำลายจุดอ่อนของประเทศต่าง ๆ ได้

2. สูญเสียรายได้ที่อาจจะเกิดขึ้น

ในระยะเวลาที่โดยโจมตีทางไซเบอร์ ทำให้ประเทศที่ตกเป็นเป้าหมายอาจไม่ได้รับความเชื่อมั่นจากประเทศอื่น ๆ บนโลกได้ ก่อให้เกิดการสูญเสียรายได้ให้กับประเทศในเชิงเศรษฐกิจ หรือแม้กระทั่งสูญเสียรายได้ภายในประเทศเองจากการที่ระบบการเงินภายในประเทศไม่สามารถใช้งานได้ ทั้งนี้จะกระทบมากหรือน้อยก็ขึ้นอยู่กับการโดนโจมตีของประเทศนั้น ๆ

3. ความน่าเชื่อถือลดลง

ในระยะเวลาที่โดยโจมตีทางไซเบอร์ ทำให้ประเทศที่ตกเป็นเป้าหมายไม่ได้รับความน่าเชื่อถือจากประเทศอื่นทั้งในระยะสั้นและระยะยาว ซึ่งอาจส่งผลกระทบเป็นวงกว้างต่อประเทศที่ตกเป็นเป้าหมาย เช่น ด้านเศรษฐกิจ ด้านความมั่นคง เป็นต้น

4.2 แนวทางการป้องกัน

การป้องกันช่องโหว่ต่าง ๆ ที่เกิดขึ้นในระบบจำลองที่ได้กล่าวถึงในข้างต้น สามารถใช้เครื่องมือและวิธีการดำเนินการต่าง ๆ ในการจัดการระบบเพื่อปรับปรุงระบบให้มีความปลอดภัยและมีประสิทธิภาพมากยิ่งขึ้นได้ด้วยแนวทางต่าง ๆ ดังนี้

4.2.1 Web Application Firewall (WAF)

Web Application Firewall เป็นเครื่องมือหนึ่งที่ช่วยในการรักษาความปลอดภัยของเว็บไซต์ของได้ให้ปลอดภัยจากการโจมตีในรูปแบบต่าง ๆ ได้อย่างหลากหลาย เช่น การโจมตี

subdomain enumeration การโจมตี directory brute-force เป็นต้น โดย WAF จะเป็นเครื่องมือที่ลดความรุนแรงใน Application Layer ได้ เมื่อเว็บไซต์มีการใช้งานจะทำให้เกิด traffic ต่างๆ โดยที่ traffic เหล่านั้นก็จะส่งมายัง WAF และ WAF ก็จะทำการกรองและตรวจสอบ traffic เหล่านั้น หากพบว่าเป็น traffic ที่ผิดปกติหรือสุ่มเสี่ยงก็จะป้องกันไม่ให้ traffic เหล่านั้นสามารถโจมตีเว็บไซต์ได้

4.2.2 วิธีป้องกันการรั่วไหลของข้อมูล

การรั่วไหลของข้อมูลหรือ Sensitive data exposure ถือเป็นช่องโหว่ที่ติดอันดับของ OWASP Top10 ในปี 2017 โดยในปัจจุบันได้มีการจัดอันดับใหม่และได้นำมารวมกันอยู่ภายในหัวข้อ OWASP Top10 A02:2021 Cryptographic Failures ซึ่งตามนิยามของ OWASP ได้กล่าวไว้ว่าเป็นช่องโหว่ที่ไม่ได้มีการป้องกัน หรือป้องกันได้ไม่ดีพอ เกี่ยวกับข้อมูลที่มีความสำคัญของระบบ ซึ่งส่งผลให้ผู้โจมตีสามารถนำหรือแก้ไขข้อมูลภายในระบบได้ สามารถป้องกันได้โดยการกำหนด Access control ให้เหมาะสม มีการยืนยันสิทธิการเข้าถึงก่อนที่ระบบจะอนุญาตให้เข้าถึงไฟล์หรือข้อมูลดังกล่าว หรือหากเป็นข้อมูลที่ไม่ได้มีความสำคัญหรือไม่ได้ใช้งานแล้วควรเอาออกจากระบบในทันที

4.2.3 Rolling code transmitter

การทำ Rolling code หรือเรียกอีกชื่อหนึ่งว่า Hopping code เป็นหนึ่งในวิธีที่ใช้ในการป้องกันการโจมตีรูปแบบ replay attack หรือการถูกดักฟังและบันทึกสัญญาณเพื่อนำไปใช้ในภายหลังของระบบไร้กุญแจ (Keyless) ที่นิยมใช้กันในปัจจุบัน เช่น ประตูรั้วไฟฟ้า ประตูรถยนต์ เป็นต้น ซึ่งถือเป็นวิธีการเข้ารหัสที่มีความปลอดภัยที่สูง โดยใช้ Chip Hardware รหัส HCS301 มาช่วยในการทำให้ข้อมูลที่ส่งออกเปลี่ยนไปเรื่อย ๆ โดยไม่มีการซ้ำกัน และเมื่อตัวรับสัญญาณได้รับค่าจะทำการคำนวณค่าที่ได้รับ หากค่าถูกต้องอุปกรณ์ถึงจะทำงาน และค่าดังกล่าวที่ถูกใช้งานไปแล้วจะไม่สามารถนำกลับมาใช้ได้อีก

4.2.4 อัปเดตระบบและซอฟต์แวร์เป็นประจำ

ผู้ดูแลระบบควรหมั่นตรวจสอบและอัปเดตระบบหรือบริการที่ใช้ภายในระบบอยู่เป็นประจำเพื่อป้องกันการใช้งานอุปกรณ์หรือซอฟต์แวร์ต่าง ๆ ที่ล้าสมัยซึ่งก่อให้เกิดช่องโหว่ที่ทำให้ผู้โจมตีสามารถเข้ายึดครองอุปกรณ์หรือระบบได้

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

จากการศึกษากรณีศึกษาความปลอดภัยในระบบจำลองการควบคุมและรักษาความปลอดภัย ได้ทำตามวัตถุประสงค์คือ ทำการสร้างระบบจำลองที่มีการใช้งานอุปกรณ์ IoT ที่มีการสื่อสารผ่านโปรโตคอล Radio frequency และจำลองการโจมตีระบบ เพื่อเรียนรู้ในด้านความปลอดภัยของอุปกรณ์ รวมทั้งด้านเทคนิคในการโจมตี จากนั้นทำการสรุปผลกระทบที่เกิดขึ้นและวิธีการป้องกันของช่องโหว่ต่าง ๆ ภายในระบบ จากผลลัพธ์ที่ได้พบว่าถึงแม้โปรโตคอล Radio frequency ที่มีการใช้งานอย่างแพร่หลายมาเป็นระยะเวลายาวนาน แต่ก็ไม่ได้มีการเปลี่ยนแปลงในด้านความปลอดภัยมากยิ่งขึ้นสักเท่าใด ซึ่งสามารถส่งคำสั่งเดิมโดยตรงเพื่อทำเทคนิคการโจมตีแบบทำซ้ำได้ทันที ในปัจจุบันโปรโตคอล Radio frequency ได้ใช้อยู่ในอุตสาหกรรมต่าง ๆ ที่หลากหลายในชีวิต ตัวอย่างเช่น อุตสาหกรรมยานยนต์ อุตสาหกรรมการก่อสร้าง เป็นต้น ดังนั้นอุตสาหกรรมที่มีการใช้งานโปรโตคอล Radio frequency ก็มีโอกาสถูกเป็นเป้าหมายในการโจมตีได้ และมีโอกาสก่อให้เกิดความเสียหายที่ไม่สามารถประเมินค่าได้อีกด้วย

5.2 ข้อเสนอแนะ

1. ควรใช้อุปกรณ์ที่มีการรองรับรูปแบบการส่งรหัสแบบ Rolling Code เพื่อป้องกันเทคนิคการโจมตีแบบทำซ้ำ (Replay Attack)
2. ควรมีการนำ Web Application Firewall (WAF) มาประยุกต์ในการใช้งาน เพื่อตรวจสอบภัยคุกคามที่โจมตีเว็บเซิร์ฟเวอร์
3. ทำการอัพเดทซอฟต์แวร์ และ security patch ของอุปกรณ์ที่ใช้งานภายในระบบอยู่เสมอ
4. ควรมีการติดตามข่าวสารด้านการโจมตีทางไซเบอร์ หรือภัยทางไซเบอร์อยู่เสมอ

เอกสารอ้างอิง

[1] What is IoT?. [Online]. Avaliable: https://www.oracle.com/th/internet-of-things/what-is-iot/. เข้าถึงเมื่อวันที่ 18 กันยายน 2565

[2] IoT - Wikipedia. [Online]. Avaliable: https://en.wikipedia.org/wiki/Internet_of_things. เข้าถึงเมื่อวันที่ 18 กันยายน 2565

[3] What is a domain name? | Domain name vs. URL. [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name/. เข้าถึงเมื่อวันที่ 20 กันยายน 2565

[4] What's a Subdomain & How Is It Used?. [Online]. Available: https://blog.hubspot.com/website/what-is-a-subdomain. เข้าถึงเมื่อวันที่ 20 กันยายน 2565

[5] Virtual hosts. [Online]. Available: https://www.ibm.com/docs/en/was-nd/8.5.5?topic=hosts-virtual. เข้าถึงเมื่อวันที่ 20 กันยายน 2565

[6] Apache Virtual Host documentation. [Online]. Available: https://httpd.apache.org/docs/2.4/vhosts/. เข้าถึงเมื่อวันที่ 20 กันยายน 2565

[7] OPEN SOURCE INTELLIGENCE (OSINT). [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/. เข้าถึงเมื่อวันที่ 20 กันยายน 2565

[8] Google Hacking: What is a Google Hack?. [Online]. Available: https://www.acunetix.com/websitesecurity/google-hacking/. เข้าถึงเมื่อวันที่ 20 กันยายน 2565

[9] What is a virtual machine?. [Online]. Available: https://www.vmware.com/topics/glossary/content/virtual-machine.html. เข้าถึงเมื่อวันที่ 22 กันยายน 2565

[10] VMware: An Essential Guide. [Online]. Available: https://www.ibm.com/th-en/topics/virtual-machines. เข้าถึงเมื่อวันที่ 22 กันยายน 2565

[11] What is Python? Executive Summary. [Online]. Available: https://www.python.org/doc/essays/blurb/. เข้าถึงเมื่อวันที่ 22 กันยายน 2565

[12] git-dumper. [Online]. Available: https://github.com/arthaud/git-dumper. เข้าถึงเมื่อวันที่ 22 กันยายน 2565

[13] What Is Directory Bursting and How Does It Work?. [Online]. Available: https://www.makeuseof.com/what-is-directory-bursting/. เข้าถึงเมื่อวันที่ 22 ตุลาคม 2565

[14] Nmap. [Online]. Available: https://www.etda.or.th/th/Our-Service/ThaiCERT/Incident-Coordination/Information/Published-documents/Technical/papers-technical/Nmap.aspx. เข้าถึงเมื่อวันที่ 23 กันยายน 2565

[15] Gobuster – Penetration Testing Tools in Kali Tools. [Online]. Available: https://www.geeksforgeeks.org/gobuster-penetration-testing-tools-in-kali-tools/. เข้าถึงเมื่อวันที่ 23 ตุลาคม 2565

[16] Universal Radio Hacker. [Online]. Available: https://github.com/jopohl/urh. เข้าถึงเมื่อวันที่ 23 ตุลาคม 2565

[17] Universal Radio Hacker: Investigate Wireless Protocols like a Boss. [Online]. Available: https://hakin9.org/universal-radio-hacker-investigate-wireless-protocols-like-a-boss/ เข้าถึงเมื่อวันที่ 23 ตุลาคม 2565

[18] radio frequency (RF, rf). [Online]. Available: https://www.techtarget.com/searchnetworking/definition/radio-frequency. เข้าถึงเมื่อวันที่ 23 ตุลาคม 2565

[19] Radio frequency. [Online]. Available: https://en.wikipedia.org/wiki/Radio_frequency. เข้าถึงเมื่อวันที่ 23 ตุลาคม 2565

[20] What is Docker?. [Online]. Available: https://www.ibm.com/th-en/topics/docker เข้าถึงเมื่อวันที่ 24 ตุลาคม 2565

[21] Dnsmasq. [Online]. Available: https://thekelleys.org.uk/dnsmasq/doc.html เข้าถึงเมื่อวันที่ 24 ตุลาคม 2565

[22] What is NGINX?. [Online]. Available: https://www.nginx.com/resources/glossary/nginx/ เข้าถึงเมื่อวันที่ 24 ตุลาคม 2565

[23] What Is a Replay Attack?. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/replay-attack. เข้าถึงเมื่อวันที่ 24 ตุลาคม 2565

[24] Deploy your app. [Online]. Available: https://docs.docker.com/language/java/deploy/. เข้าถึงเมื่อวันที่ 3 ตุลาคม 2565

[25] How to Deploy App Using Docker. [Online]. Available: https://medium.com/@habibridho/docker-as-deployment-tools-5a6de294a5ff. เข้าถึงเมื่อวันที่ 3 ตุลาคม 2565

[26] Top Cloud Deploy Features – 2022 | Medium. [Online]. Available: https://medium.com/google-cloud/top-cloud-deploy-features-2022-eeb4721513a3. เข้าถึงเมื่อวันที่ 22 ตุลาคม 2565

[27] ทำการ deploy Function บน Google Cloud Platform. [Online]. Available: https://www.somkiat.cc/deploy-function-on-google-cloud-platform/. เข้าถึงเมื่อวันที่ 22 ตุลาคม 2565

[28] GitHub - kylemanna/docker-openvpn: OpenVPN server in a Docker container complete with an EasyRSA PKI CA. [Online]. Available: https://github.com/kylemanna/docker-openvpn. เข้าถึงเมื่อวันที่ 24 ตุลาคม 2565

[29] Install Docker Engine on Debian | Docker Documentation. [Online]. Available: https://docs.docker.com/engine/install/debian. เข้าถึงเมื่อวันที่ 18 ธันวาคม 2565

[30] HOWTO – OpenVPN Community. [Online]. Available: https://community.openvpn.net/openvpn/wiki/HOWTO#ExpandingthescopeoftheVPN56toincludeadditionalmachinesoneithertheclientorserversubnet. เข้าถึงเมื่อวันที่ 18 ธันวาคม 2565

[31] HackRF One. [Online]. Available: https://en.wikipedia.org/wiki/HackRF_One เข้าถึงเมื่อวันที่ 18 ธันวาคม 2565

[32] Incident Response: The Steps to a Root Cause Analysis for State Government. [Online]. Available: https://statetechmagazine.com/article/2021/10/incident-response-steps-root-cause-analysis-state-government-perfcon. เข้าถึงเมื่อวันที่ 19 ธันวาคม 2565

[33] Cyber Warfare. [Online]. Available: https://www.imperva.com/learn/application-security/cyber-warfare/. เข้าถึงเมื่อวันที่ 19 ธันวาคม 2565

ภาคผนวก

ภาคผนวก ก

ขั้นตอนการติดตั้งโปรแกรม Docker บนระบบปฏิบัติการ Debian

1. การติดตั้ง Docker บนระบบปฏิบัติการ Debian จะมีการอ้างอิงมาจากเอกสารทางการของ Docker โดยจะต้องทำการติดตั้งโปรแกรมที่จำเป็นสำหรับ Docker ด้วยคำสั่งดังต่อไปนี้

```
$ sudo apt-get update

$ sudo apt-get install \
    ca-certificates \
    curl \
    gnupg \
    lsb-release \
```

2. จากนั้นจะต้องทำการเพิ่ม Docker repository ก่อนจึงจะติดตั้ง Docker ได้ ด้วยคำสั่งดังต่อไปนี้

```
$ sudo mkdir -p /etc/apt/keyrings

$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg

$ echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu \
  $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
```

3. หลังจากที่ติดตั้งโปรแกรมที่จำเป็นและเพิ่ม Docker repository แล้ว ให้ทำการอัปเดตครั้งหนึ่งก่อนที่จะทำการติดตั้ง Docker

```
$ sudo apt-get update
$ sudo apt-get install -y docker-ce docker-ce-cli containerd.io docker-compose-plugin
```

4. ทำการทดสอบใช้งาน Docker โดยการสร้าง Docker Container จาก Docker Image ที่มีชื่อว่า hello-world ด้วยคำสั่งต่อไปนี้

```
$ sudo docker run hello-world
```

5. เมื่อติดตั้งและทดสอบการใช้งาน Docker เรียบร้อยแล้ว หากพบปัญหาในการปฏิเสธสิทธิในการใช้งาน (Permission Denial) ให้ทำการเพิ่มผู้ใช้งานลงไปยัง group docker ซึ่งทำได้โดยคำสั่งดังต่อไปนี้

```
$ sudo groupadd docker
$ sudo gpasswd -a $USER docker
$ sudo service docker restart
```

งานทะเบียนคณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

คำรับรองเล่มโครงงานพิเศษ/ปัญหาพิเศษ/สหกิจศึกษา

วันที่ 18 เดือน พฤษภาคม พ.ศ. 2566

ข้าพเจ้า นาย/นาง/นางสาว ภัทรชัย สุภาควัฒน์ รหัสประจำตัว 62050206

นักศึกษาหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชา วิทยาการคอมพิวเตอร์ ภาควิชา วิทยาการคอมพิวเตอร์

ขอรับรองว่าโครงงานพิเศษ/ปัญหาพิเศษ/สหกิจศึกษา เรื่อง

ชื่อภาษาไทย กรณีศึกษาความปลอดภัยในระบบจำลองการควบคุม และรักษาความปลอดภัย

ชื่อภาษาอังกฤษ A Case Study on Simulate Security Control Systems

ปีการศึกษา 2565

เป็นผลงานวิจัยที่มิได้คัดลอกหรือละเมิดลิขสิทธิ์ของผู้อื่นและได้ผ่านการตรวจสอบความซ้ำซ้อนเรียบร้อยแล้ว และได้แนบเอกสารการตรวจสอบการลอกเลียนงานวรรณกรรมที่ตรวจสอบจากเล่มโครงงานพิเศษ/ปัญหาพิเศษ/สหกิจศึกษาฉบับสมบูรณ์แล้ว

โปรแกรมอักขราวิสุทธิ์ 0.4 % หรือโปรแกรม Turnitin .....%

ลงชื่อ ภัทรชัย สุภาควัฒน์

(นายภัทรชัย สุภาควัฒน์)

นักศึกษา

ข้าพเจ้า ศ. / รศ. / ผศ. / ดร. / อ. กรองทอง กิ้มฟ้า อาจารย์ที่ปรึกษาโครงงานพิเศษ/ปัญหาพิเศษ/สหกิจศึกษา ได้ตรวจสอบโครงงานพิเศษ/ปัญหาพิเศษ/สหกิจศึกษาของนักศึกษาข้างต้น แล้ว ขอรับรองว่าเป็นผลงานวิจัยของนักศึกษาจริงและมีเนื้อหาสมบูรณ์ จึงลงชื่อไว้เป็นหลักฐาน

ลงชื่อ .....

อาจารย์ที่ปรึกษา