# บทที่ 5

# สรุปผลและข้อเสนอแนะ

ผลการทดสอบระบบการเชื่อมต่อแอคเซสพอยต์ที่ไม่ถูกต้องและเว็บไซต์สำหรับลงทะเบียนแอคเซสพอยต์ สามารถสรุปผลการดำเนินการทำงานได้ดังนี้

## 5.1 สรุปผลและอภิปรายผล

เทคโนโลยี Wi-Fi จะยังคงเป็นส่วนสำคัญของการเชื่อมต่ออินเทอร์เน็ตในอนาคต ดังนั้นการพัฒนาและปรับปรุงเทคโนโลยี Wi-Fi เป็นสิ่งสำคัญเพื่อตอบสนองความต้องการของผู้ใช้และการเชื่อมต่ออุปกรณ์ในอนาคต ความปลอดภัยของเครือข่าย Wi-Fi จะเป็นหัวใจสำคัญ เพื่อป้องกันการแอบขโมยข้อมูลและการบุกรุก มีการคิดค้นมาตรการความปลอดภัยที่ขึ้นใหม่ในระบบ Wi-Fi การใช้ระบบแจ้งเตือนช่วยในการจัดการความปลอดภัยของเครือข่าย Wi-Fi โดยให้ผู้ใช้รายงานและระบบจับความผิดปกติเพื่อเพิ่มความปลอดภัยและความเชื่อถือในระบบ ระบบการแจ้งเตือนการเชื่อมต่อแอคเซสพอยต์ที่ไม่ถูกต้องแบ่งประเภทการตรวจพบ Wi-Fi แบ่งออกเป็น 2 ประเภทได้แก่

1. Aircrack-ng คือ Access Point ปลอมที่มี ESSID เหมือนกับ Access Point ที่ลงทะเบียนไว้ แต่ BSSID ไม่ตรงกัน

2. Rouge Access Point คือ Access Point ที่ไม่มี ESSID และ BSSID ไม่ได้ลงทะเบียน เมื่อตรวจพบ Wi-Fi จะขึ้นแทบสีบนชื่อของ Wi-Fi และแจ้งเตือน แบ่งออกเป็น 3 สี

(1) แทบสีแดง โดยหากตรวจพบว่าเป็น Evil-Twin ซึ่งมี ESSID ที่ลงทะเบียนในระบบแต่ BSSID ไม่ได้ถูกลงทะเบียน

(2) แทบสีเหลือง โดยหากตรวจพบว่าเป็น Rouge Access Point ซึ่งมี ESSID และ BSSID ที่ไม่ได้ลงทะเบียนในระบบ

(3) แทบสีเขียว คือ Access Point ที่ลงทะเบียนหรือบันทึกข้อมูลลงในระบบแล้วโดย ESSID และ BSSID ตรงกับที่ลงทะเบียน

## 5.2 ผลสัมฤทธิ์ของโครงการ

1. ความปลอดภัยของระบบ โครงการนี้เป็นการเพิ่มความปลอดภัยในระบบการเชื่อมต่อ Wi-Fi โดยการป้องกันการเชื่อมต่อไม่ถูกต้อง อาจทำให้ระบบมีความปลอดภัยมากขึ้น

2. การปรับปรุงกระบวนการบริหารจัดการในองค์กร เพื่อให้ระบบการแจ้งเตือนมีประสิทธิภาพมากขึ้น

3. เรียนรู้ศึกษาเทคนิคการโจมตีใหม่ๆ หรือช่องโหว่ เพื่อความปลอดภัยสำหรับการใช้งานโทรศัพท์มือถือ

**5.3 ข้อเสนอแนะ**

1. ใช้ทรัพยากรของระบบเพื่อปรับปรุงประสิทธิภาพของระบบและเว็บไซต์ในการลงทะเบียน Access Point และการแจ้งเตือน การตอบสนองของระบบหรือความเร็วในการดำเนินการ

2. พิจารณาการปรับปรุงอินเตอร์เฟซและส่วนติดต่อของเว็บไซต์ลงทะเบียนเพื่อทำให้มันเป็นไปตามความสะดวกและง่ายต่อผู้ใช้

3. การเพิ่มมาตรการความปลอดภัยและการป้องกันการโจมตีที่อาจเกิดขึ้นต่อระบบแจ้งเตือนแอคเซสพอยต์

4. อัปเดตและดูแลรักษาระบบอย่างต่อเนื่องเพื่อป้องกันช่องโหว่และข้อบกพร่องที่อาจเกิดขึ้น

5. พัฒนาในส่วนของโมไบล์แอปพลิเคชันอินเตอร์เฟซให้สวยงามและง่ายต่อการใช้งานสำหรับผู้ใช้

6. พัฒนาระบบเพื่อทำการแจ้งเตือนแก่ผู้ใช้หรือผู้ดูแลระบบเมื่อเกิดการโจมตี และให้คำแนะนำเกี่ยวกับขั้นตอนการแก้ไข

7. รวบรวมข้อมูลเกี่ยวกับเชื่อมต่อแอคเซสพอยต์ไม่ถูกต้องจากหลายแหล่ง เพื่อเสริมความเชื่อถือและประสิทธิภาพของระบบ

8. พัฒนาให้ระบบสามารถป้องกันและแจ้งเตือนเมื่อถูกโจมตีเทคนิค Mac Spoofing หรือเทคนิคต่างๆ