บทที่ 5

สรุปผลและข้อเสนอแนะ

ผลจากการทดสอบระบบตรวจจับแบะตอบโต้การทำงานด้วยเทคนิคแฝดนรก และ เว็บไซต์สำหหรับลงทะเบียน Access Point สามารถสรุปผลการดำเนินงานได้ดังนี้

5.1 สรุปผลและอภิปรายผล

ในปัจจุบันการติดต่อสื่อสารต่างๆ ภายในองค์กรนิยมใช้งานเครือข่ายไร้สาย เนื่องจากมีความสะดวกสบายในการใช้งาน แต่หากพูดถึงความปลอดภัยในการใช้งานเครือข่ายไร้สายแล้วนั้น ด้านความปลอดภัยของเครือข่ายไร้สายถือว่าเสี่ยงต่อการถูกโจมตีจากผู้ไม่ประสงค์ดีเป็นอย่างมากถึงแม้ว่ามาตรฐานความปลอดภัยในปัจจุบันของเครือข่ายไร้สายจะถูกพัฒนามาเป็น WPA3 แล้วก็ตาม แต่ก็ยังสามารถถูกโจมตีได้ด้วยเทคนิค Evil Twin Attack ดังนั้นโครงการปริญญานิพนธ์นี้จึงได้พัฒนา ระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก โดยแบ่งออกเป็น 2 ส่วนหลักคือ เว็บไซต์สำหรับลงทะเบียน Access Point และ ระบบตรวจจับและตอบโต้การโจมตี โดยระบบตรวจจับและตอบโต้การโจมตีนั้นสามารถใช้ได้โดย การติดตั้งในบริเวณที่อาจเกิดการโจมตี หรือ ใช้เพื่อเดินตรวจสอบในบริเวณต่างๆที่อาจเกิดการโจมตี เพื่อทำการตรวจจับการโจมตีในบริเวณดังกล่าว เมื่อตรวจพบการโจมตีระบบจะแจ้งเตือนไปยัง Line Group และ Email ที่ลงทะเบียนไว้กับเว็บไซต์ และ ระบบสามารถตอบโต้การโจมตีเบื้องต้นได้โดยการส่ง De-authentication Packet ไปยังเป้าหมายเพื่อทำให้ Access Point ของเป้าหมายไม่สามารถใช้งานได้ชั่วคราวเพื่อรอการลงพื้นที่ตรวจสอบจากผู้ดูแลรับผิดชอบ จากผลการทดสอบ ระบบสามารถตรวจจับและจำแนกประเภทการโจมตีออกเป็น 3 ประเภท ดังนี้

1) Rogue Access Point คือ Access Point ที่ไม่ได้ลงทะเบียนไว้
2) WiFi phishing คือ Access Point ปลอมที่มีชื่อเหมือนกับ Access Point ที่ลงทะเบียนไว้
3) Evil Twin Attack คือ Access Point ปลอมที่มีชื่อ และ MAC Address เหมือนกับ Access Point ที่ลงทะเบียนไว้แต่มี Channel ไม่ตรงกัน

เมื่อตรวจพบการโจมตีระบบจะแจ้งเตือนข้อมูลการโจมตีไปยัง Line Group และ Email ที่ลงทะเบียนไว้กับเว็บไซต์ได้

5.2 ผลสัมฤทธิ์ของโครงการ

1) ได้ต้นแบบระบบตรวจจับและตอบโต้การโจมตีเครือข่ายไร้สายภายในองค์กรเพื่อใช้ในการตรวจการโจมตีเครือข่ายไร้สายที่เกิดขึ้นภายในองค์กรทำให้เกิดความปลอดภัยในการใช้งานเครือข่ายไร้สายมากยิ่งขึ้น

2) ได้เรียนรู้เทคนิควิธีการโจมตีเครือข่ายไร้สาย เพื่อศึกษาหาแนวทางป้องกันและตอบโต้การโจมตี

5.3 ข้อเสนอแนะ

เนื่องจากระบบตรวจจับและตอบโต้การโจมตีด้วยเทคนิคแฝดนรก ถูกพัฒนาขึ้นเพื่อใช้ภายในองค์กรโดยมีจุดประสงค์เพื่อความปลอยภัยในการใช้งานเครือข่ายไร้สายภายในองค์กร สามารถนำไปต่อยอดได้หลายส่วนดังนี้

1) Software ในส่วนของระบบตรวจจับและตอบโต้การโจมตี สามรถนำมาพัฒนาต่อยอดให้สามารถทำงานอยู่ในอุปกรณ์ขนาดเล็ก เช่น Raspberry Pi เพื่อให้สะดวกต่อการติดตั้งใช้งานมากยิ่งขึ้น
2) Software ในส่วนของระบบตรวจจับและตอบโต้การโจมตี สามารถนำไปพัฒนาต่อยอดให้สามารถทำงานใน Unix Virtual Machine ที่ทำงานอยู่บน Smartphone ได้โดยใช้ Andronix หรือ Termux
3) พัฒนาในส่วนของ ระบบตรวจจับและตอบโต้การโจมตี มี Interface GUI ให้สวยงามมากยิ่งขึ้น
4) พัฒนาในส่วนของ ระบบตรวจจับและตอบโต้การโจมตี ให้สามารถตรวจจับการโจมตีเครือข่ายไร้สายในรูปแบบอื่นๆเพิ่มมากขึ้น
5) พัฒนาในส่วนของ ระบบตรวจจับและตอบโต้การโจมตีให้สามารถตรวจจับและรายงานคุณภาพของสัญญาณและการทำงานของ Access Points
6) พัฒนาในส่วนของ เว็บไซต์สำหรับลงทะเบียน Access Point ให้สามารถตรวจสอบความถูกต้องของ Access Point ที่ลงทะเบียน ในกรณีผู้ใช้ลงทะเบียนข้อมูล Access Point ผิด
7) พัฒนาในส่วนของ ระบบตรวจจับและตอบโต้การโจมตี ให้สามารถตอบโต้อัตโนมัติทันทีเมื่อมีเกิดการโจมตี
8) พัฒนาในส่วนของ ระบบตรวจจับและตอบโต้การโจมตี ให้สามารถตรวจจับและแยกแยะ การโจมตีประเภท Rogue Access Point ว่าเป็นการโจมตีเพื่อระบบการการทำงานของเครือข่ายหลัก หรือ เป็นเพียง Mobile Hotspot ที่ถูกเปิดใช้งานเพื่อความสะดวกของผู้ใช้งานเอง