Automated Vulnerability Assessment & Incident Response System

ระบบประเมินความเปราะบางและแจ้งเตือนภัยคุกคามทางไซเบอร์อัตโนมัติ

อาจารย์ที่ปรึกษา: ศ.ดร.จักรชัย โสอินทร์

อาจารย์ที่ปรึกษา: อ. ดร.ชาติชาย ปุณริบูรณ์

GROUP 5

ปัญหาและที่มา (Background)

การโจมตีทางไซเบอร์ส่วนใหญ่เกิดจากการเปิดพอร์ตและบริการที่มีช่องโหว่ทิ้งไว้ (Unpatched) ประกอบกับเครื่องมือป้องกันเดิมมักเป็นแบบตั้งรับ (Passive) ตรวจสอบยาก และไม่มีการแจ้งเตือนทันทีเมื่อเกิดเหตุ

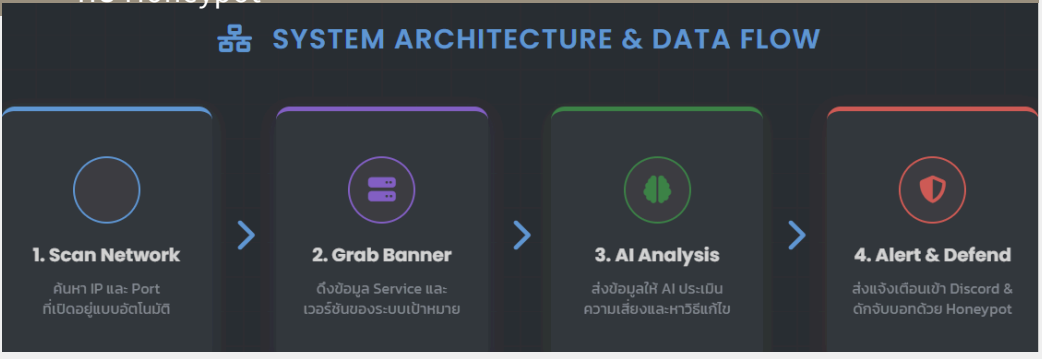
วัตถุประสงค์ (Objectives)

1. **Automated Scanner:** สร้างระบบสแกนเครือข่ายและหาช่องโหว่อัตโนมัติที่ทำงานไวและใช้งานง่าย
2. **Real-Time Alert:** แจ้งเตือนภัยคุกคามระดับอันตรายผ่าน Discord แบบทันที
3. **Active Defense:** ยกระดับการป้องกันด้วยระบบลวง (Honeypot) เพื่อดักจับผู้บุกรุก

ฟีเจอร์เด่น (Key Features)

- **SOC Dashboard:** หน้าจอ GUI สรุปผล IP, พอร์ต, และความเสี่ยง จบในหน้าเดียว
- **AI Analyst:** ใช้ AI ช่วยแปลผลช่องโหว่ทางเทคนิคและแนะนำวิธีแก้ไขให้เข้าใจง่าย
- **Honeypot Trap:** พอร์ตจำลองเพื่อหลอกล่อแฮกเกอร์ พร้อมแจ้งเตือนทันทีที่ถูกโจมตี
- **Smart Network:** ระบบแยกแยะ IP ตัวเองอัตโนมัติ ป้องกันการสแกนชนกับ Honeypot

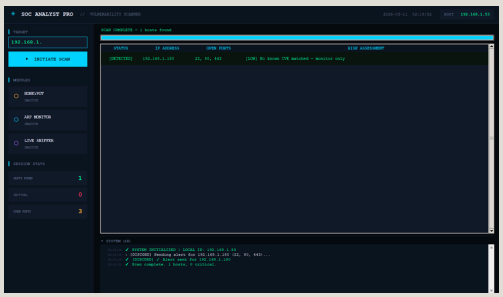
SYSTEM ARCHITECTURE & DATA FLOW



เครื่องมือที่ใช้ (Tools)

ผลการดำเนินงาน (Conclusion)

ระบบสามารถสแกนเป้าหมาย ระบุพอร์ต/ช่องโหว่ และประเมินความเสี่ยงได้อย่างแม่นยำ การแจ้งเตือนผ่าน Discord ช่วยลดเวลาตอบสนองต่อเหตุการณ์ (Incident Response Time) ได้จริง พร้อมมีระบบ Honeypot ที่สกัดกั้นการโจมตีเชิงรุกได้อย่างมีประสิทธิภาพ



ผู้จัดทำ (Group 5):

นายสิทธิชัย ไพโรจน์ 673380566-4

นายกันตภูมิ เดาขุนทด 673380364-6

นายณัฐนนท์ เนาวรัตน์ 673380369-6

นายสกลเกียรติ จันทร์วงษา 673380565-6

นายกฤษณพงษ์ วีระชาติ 673380363-8

นายสุกฤษ อารีป้อม 673380385-8