ENTERPRISE NETWORK INSPECTOR

ระบบเพิ่มทัศนวิสัยเครือข่ายท้องถิ่นและป้องกันการบุกรุกระดับโฮสต์

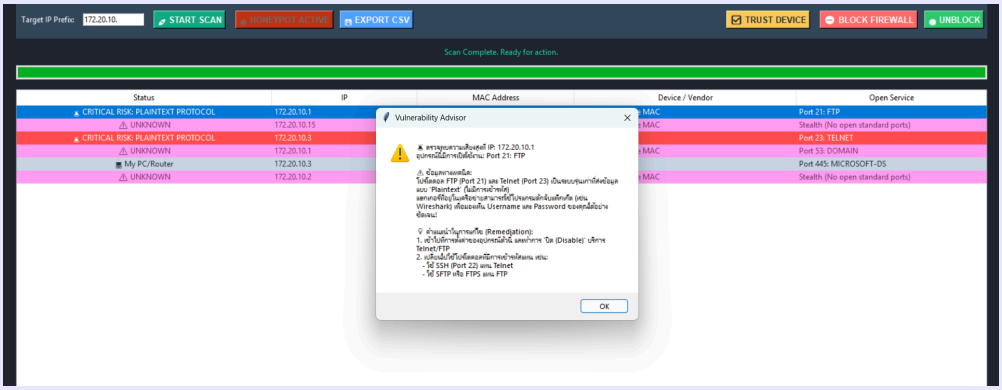
ผู้จัดทำ (Group 5):
นายสิทธิชัย ไพโรจน์ 673380566-4 (Network Architect)
นายกันตภูมิ เดาขุนทด 673380364-6 (Lead Programmer)
นายณัฐนนท์ เนาวรัตน์ 673380369-6 (Concurrency Specialist)
นายสกลเกียรติ จันทร์วงษา 673380565-6 (API Integrator)
นายกฤษณพงษ์ วีระชาติ 673380363-8 (Performance Tester)
นายสุกฤษ อารีป้อม 673380385-8 (System Documentation)
อาจารย์ที่ปรึกษา: ศ.ดร.จักรชัย โสอินทร์
อาจารย์ที่ปรึกษา: นายชาติชาย ปุณริบูรณ์

PROBLEM STATEMENT

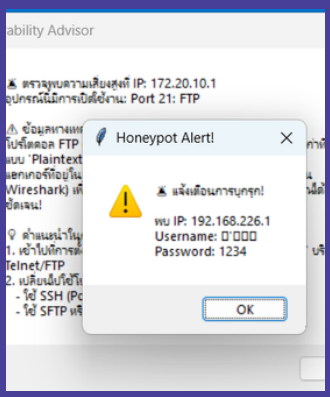
- **Lack of Network Visibility:** แอดมินมักไม่ทราบว่ามีอุปกรณ์แปลกปลอม (Rogue Devices) เชื่อมต่อในวง LAN ซึ่งอาจเป็นช่องโหว่ให้ถูกแฮก
- **Plaintext Protocol Risks:** อุปกรณ์เก่า (Router/IoT) มักเปิดพอร์ต Telnet (23) หรือ FTP (21) ทิ้งไว้ ส่งข้อมูลแบบไม่เข้ารหัส เสี่ยงต่อการถูกดักจับรหัสผ่าน
- **Lack of Proactive Defense:** โปรแกรมสแกนทั่วไปทำได้แค่ค้นหา แต่ไม่สามารถบล็อกผู้บุกรุก หรือไม่มีระบบแจ้งเตือนแบบทันที (Early Warning)

RELATED WORK COMPARISON

- **Nmap:** สแกนละเอียดแต่ใช้งานยาก (Command Line) สั่งบล็อก IP ไม่ได้
- **Angry IP Scanner:** ใช้ง่าย แต่ไม่มีระบบแจ้งเตือนความเสี่ยง (Vulnerability Alert)
- **Our System:** ผสมผสานการทำงานแบบ All-in-One มี GUI ใช้งานง่าย ตรวจจับความเสี่ยงวิกฤต พร้อมระบบสั่งบล็อก Firewall และมี Honeypot ในตัว



TOOLS



ARCHITECTURE & METHODOLOGY

- **Data Flow:**

โยน IP (254 IPs) ลง Queue ➔ สร้าง 70 Threads ขนานกัน ➔ เช็คสถานะ (Ping) ➔ ดึง MAC Address (ARP) ➔ สแกนพอร์ต (Socket TCP) ➔ แสดงผลบน GUI

3. สถาปัตยกรรมและการทำงาน (System Architecture)

- **High-Speed Concurrency:** ใช้ threading และตั้งค่า Socket Timeout ที่ 0.2 วินาที ทำให้สแกนอุปกรณ์ทั้งวง LAN เสร็จอย่างรวดเร็ว
- **OS Firewall Integration:** ใช้ subprocess ส่งคำสั่ง netsh advfirewall เพื่อบล็อก IP ผ่านระบบปฏิบัติการโดยตรง
- **Honeypot Decoy:** จำลอง Socket Server บน Port 23 ทำหน้าที่เป็น "โถน้ำผึ้ง" ดักจับการบุกรุก

References:
- Nmap Project Guide (Network Discovery Methods)
- NIST SP 800-61 Rev. 2 (Incident Response Framework)
- OWASP Top 10 - Cryptographic Failures (Plaintext Protocols)
- Spitzner's Honeypot Architecture (Active Defense)
- Python Network Programming & Concurrency