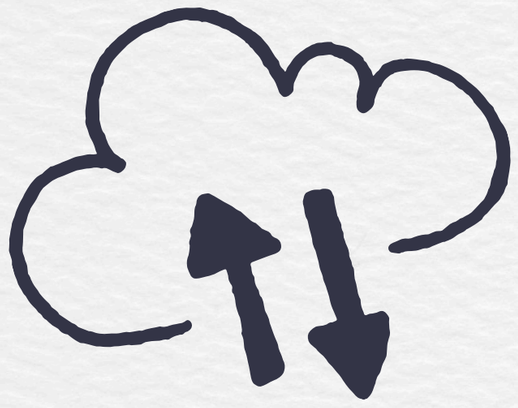
NETWORK INTRUSION DETECTION

หลักการและเหตุผล

ระบบตรวจจับการบุกรุก (IDS) มีความสำคัญในการเฝ้าระวังพฤติกรรมผิดปกติภายในเครือข่าย
จึงพัฒนาระบบต้นแบบ Mini IDS Dashboard ที่ใช้งานง่ายและแจ้งเตือนแบบเรียลไทม์



วัตถุประสงค์

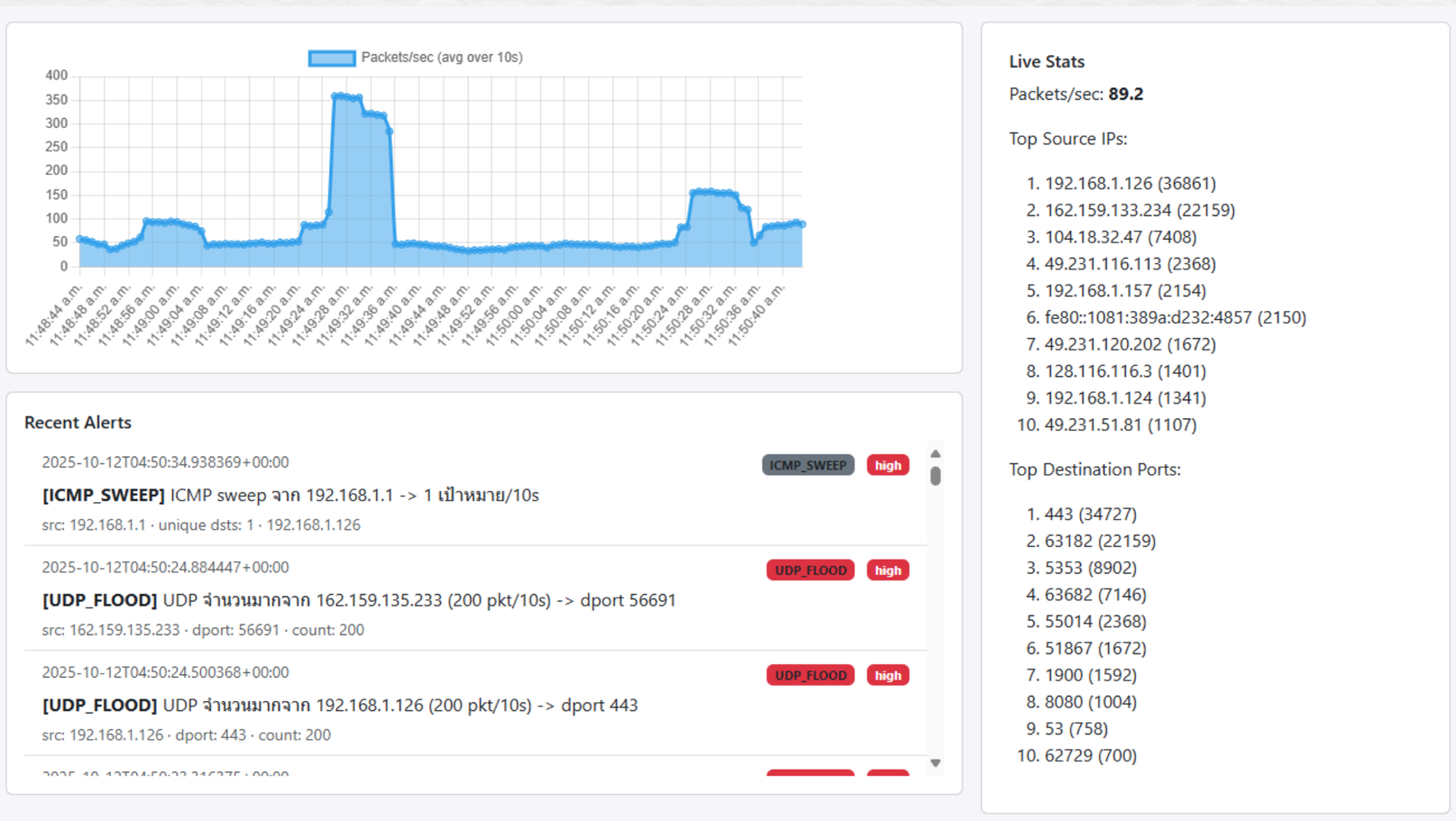
1. เพื่อศึกษาการทำงานของระบบตรวจจับการบุกรุกเครือข่าย
2. เพื่อพัฒนา Dashboard แสดงผลและแจ้งเตือนผ่าน Telegram แบบเรียลไทม์

อุปกรณ์ที่ใช้

- Python 3 – ภาษาหลักของระบบ
- Flask – ใช้สร้างเว็บเซิร์ฟเวอร์และหน้า Dashboard
- Flask-SocketIO – ส่งข้อมูลเรียลไทม์ระหว่าง Server กับ Client
- Scapy – ดักจับและวิเคราะห์แพ็กเก็ตเครือข่าย
- Telegram Bot API – สำหรับแจ้งเตือนอัตโนมัติ
- Visual Studio Code (VS Code) – เครื่องมือพัฒนาโปรแกรม

วิธีการทำงาน

- Python (Flask) ทำหน้าที่เป็น Web Server สำหรับรับ-ส่งข้อมูลและแสดง Dashboard แบบเรียลไทม์
- โดยใช้ Socket.IO ในการสื่อสารแบบสองทาง (WebSocket Protocol)
- ระหว่าง Client (หน้าเว็บ) และ Server (ระบบตรวจจับ) พร้อมทั้งใช้ Scapy ในการดักจับและวิเคราะห์แพ็กเก็ตเครือข่าย



สมาชิก

นายจิรวัฒน์ อาจหาญยิ่ง 673380209-8
นายฐิตินัส ดวงท้าวเศษ 673380213-7
นายสุริยะ ชาวบุรี 673380250-1
นายกษิดิศ วิลัยปาน 673380496-9
นายปวริศ คลองสนั่น 673380501-2