การพัฒนาระบบตรวจจับพฤติกรรมที่น่าสงสัยในเครือข่าย

Information and Communication Technology Security SC362006

หลักการและเหตุผล

ปัจจุบันการโจมตีทางไซเบอร์เพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะในองค์กรที่มีเครือข่ายขนาดใหญ่ เช่น การโจมตีแบบ DDoS, การเจาะช่องโหว่ผ่านพอร์ต, และการแพร่กระจายมัลแวร์ในเครือข่าย

หาทางองค์กรไม่สามารถตรวจจับพฤติกรรมที่ผิดปกติในเครือข่ายได้ทันเวลา อาจทำให้เกิดความเสียหายทางข้อมูล หรือการสูญเสียทรัพย์สินอย่างมาก

เนื่องจากเป็นสิ่งที่สามารถใช้ได้จริงและมีการเข้าถึงได้ง่ายและง่ายต่อการเข้าใจ เพื่อลดความเสี่ยงของผลลัพธ์ที่ไม่สมควรจะเกิดขึ้นจากความประมาทของผู้ใช้เอง

วัตถุประสงค์

- เพื่อสร้างระบบตรวจจับและแจ้งเตือนเมื่อพบพฤติกรรมที่น่าสงสัย

ขอบเขตของการศึกษา

- รูปแบบพฤติกรรมที่ผิดปกติในเครือข่าย
  เช่น การสแกนพอร์ตหรือการส่งข้อมูลที่เกินปกติ

เครื่องมือที่ใช้พัฒนา

ภาษาที่ใช้เขียน

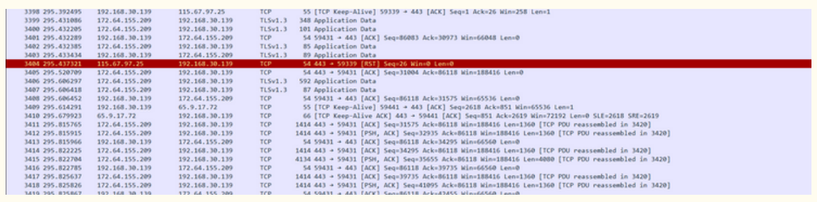
ภาษา Python

ฟังก์ชั่นการทำงาน

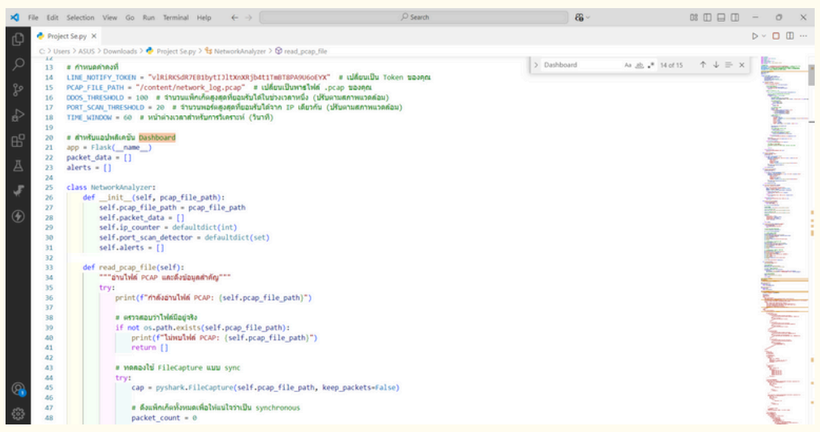
- ฟังก์ชันตรวจสอบความผิดปกติ จาก Logs
  - เช่น DDos , การสแกนพอร์ต หรือการส่งข้อมูลที่เกินปกติ
- แจ้งเตือนเมื่อพบความผิดปกติ ผ่าน LINE Notify

วิธีใช้งาน

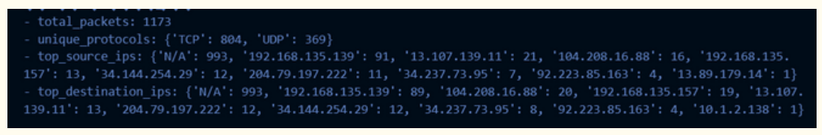
1.ดาวน์โหลดไฟล์ Logs ที่ต้องการมา



2.เลือกไฟล์ที่ต้องการตรวจสอบ ผ่านชื่อไฟล์ และกดรันโค้ด



3.แสดงข้อความบอกผลการตรวจสอบ เมื่อเจอความผิดปกติ แจ้งเตือนผ่าน LINE Notify



สมาชิก Group 2 Section 1

1. นางสาวฐิติมา บุญพรมมา รหัสประจำตัวนักศึกษา 663380154-6
2. นางสาวพิธิดา คำชารี รหัสประจำตัวนักศึกษา 663380175-8
3. นายภานุวัฒน์ ลครราช รหัสประจำตัวนักศึกษา 663380179-0
4. นายภูริณัฐ บุญมาถึง รหัสประจำตัวนักศึกษา 663380180-5
5. นายนายปกรณ์ รอดปรีชา รหัสประจำตัวนักศึกษา 663380489-5

เสนอ

ศาสตราจารย์ดร. จักรชัย โสอินทร์

อ้างอิง

https://cybersecurityventures.com/

https://www.cyfence.com/article/2023-threat-statistics-summary-from-csoc-by-nt-cyfence/

https://today.line.me/th/v2/article/vXjMJEo