COLLEGE OF COMPUTING
KHON KAEN UNIVERSITY

Network Project
Threat Monitor

CP422011 Introduction to Computer Networking
อาจารย์ผู้สอน ศ. ดร.จักรชัย โสอินทร์ และ ผศ. ดร.เพชร อิ่มทองคำ

หลักการและเหตุผล

โครงการพัฒนาระบบเฝ้าระวังภัยไซเบอร์แบบ Real-time มีแดชบอร์ดรวมข้อมูลช่วยลดเวลาวิเคราะห์ คุ้มค่ากว่าสำหรับองค์กรงบจำกัด แต่ยังมีฟังก์ชันหลักครบ และยังมีกราฟและสถิติช่วยเห็นแนวโน้มและวางแผนป้องกันล่วงหน้า

เครื่องมือที่ใช้

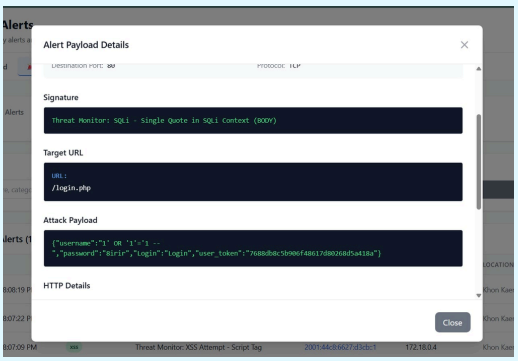
วิธีการใช้งาน

run ip link show แล้วจะได้ interface มาแล้วก็นำ inteface ที่ได้ไปแก้ใน compose.yml, suricata.yaml

```
command: ["-c", "/etc/suricata/suricata.yaml", "-i", "<yourinterface>", "-i",
```

```
entrypoint: ["zeek"]
command: ["-C", "-i", "<yourinterface>", "local"]
```

```
af-packet:
  - interface: <yourinterface>
    cluster-id: 99
```



วัตถุประสงค์

- ศึกษาการเก็บรวบรวม วิเคราะห์ และนำเสนอข้อมูลเหตุการณ์ความปลอดภัยไซเบอร์อย่างเป็นระบบ
- พัฒนาระบบดักจับ จัดเก็บ วิเคราะห์ และนำเสนอข้อมูลการโจมตี ผ่านแดชบอร์ดและกราฟสถิติแบบเรียลไทม์
- ปรับแต่งระบบให้เหมาะกับองค์กรงบและทรัพยากรจำกัด โดยคงฟังก์ชันสำคัญของ IDS ไว้อย่างครบถ้วน

ขอบเขตการทำงาน

ตรวจจับภัยคุกคามได้แบบ real time ในการโจมตีหลายๆรูปแบบ เช่น XXS SQL Injection เป็นต้น

ข้อจำกัด

- รันได้บนหลายระบบก็จริง แต่ประสิทธิภาพสู้ Linux แบบเนทีฟซึ่งเหมาะกับ Docker ไม่ได้
- โปรเจกต์นี้เน้นแจ้งเตือนเหตุโจมตีเท่านั้น ยังไม่ระบุแนวทางป้องกันจากเหตุการณ์นั้นได้
- ระบบตรวจจับได้เฉพาะเครื่องเซิร์ฟเวอร์ที่รันคอนเทนเนอร์ ยังไม่ครอบคลุมเครื่องอื่นในเครือข่าย
- IP ที่เห็นบนแดชบอร์ดอาจเป็น Public IP ของเราเตอร์ หรือ IP จาก VPN/Tor (exit node) ไม่ใช่ IP ภายในเครื่องจริง

สรุปผล

ระบบเฝ้าระวังแบบเรียลไทม์ แสดงผลบนแดชบอร์ด/กราฟ ปรับให้เหมาะองค์กรทรัพยากรจำกัดและคงฟังก์ชันหลักของ IDS เพื่อแจ้งเตือนเหตุโจมตี โดยจำกัดที่โฮสต์ที่รันคอนเทนเนอร์ ประสิทธิภาพดีที่สุดบน Linux เนทีฟ ยังไม่แนะนำวิธีป้องกัน และ IP ที่เห็นอาจจะเป็น Public/VPN/Tor ไม่ใช่ต้นทางจริง

สมาชิก Group5 Sec1
นายกฤษกร แสนสกุล 673380144-0
นายคำภีร์ดารา ภูกิ่งเงิน 673380152-1
นายนันทภัทร เพรชสังหาร 673380166-0
นางสาวศุภาพิชญ์ เพ็ชรสุรักษ์ 673380190-3