หมายเลขโครงงาน	

แบบฟอร์มขอบเขตโครงงาน TEAM-PROJECT 3

ชื่อภาษาไทย ระบบตรวจจับการโจมตี Distributed Denial of Service (DDoS) แบบเรียลไทม์

ชื่อภาษาอังกฤษ Realtime Distributed Denial of Service (DDoS) Detection

โดย

นาย นายเมธาสิทธิ์ อมรวุฒิพงศ์ รหัสนักศึกษา 66010670

นาย วิศรุต สิริโสภาพร รหัสนักศึกษา 66010773

อาจารย์ที่ปรึกษาหลัก _____

(ผศ.ดร.นภัทร สระเอี่ยม) ลงนามวันที่ _____/_____/_____

อาจารย์ที่ปรึกษาร่วม _____

(ผศ.ดร.สมปอง วิเศษพานิชกิจ) ลงนามวันที่ _____/_____/_____

วัตถุประสงค์โดยคร่าวของการนำเสนอโครงงาน TEAM-PROJECT 3

1. เพื่อศึกษากระบวนการโจมตีแบบ DDoS รวมถึงรูปแบบการโจมตี โปรโตคอลที่เกี่ยวข้อง และผลกระทบที่เกิดขึ้นกับระบบเครือข่ายและบริการต่าง ๆ
2. เพื่อศึกษาการใช้งาน Zeek Network Security Monitor สำหรับเก็บข้อมูลทราฟฟิกในเครือข่าย และวิเคราะห์พฤติกรรมที่ผิดปกติซึ่งอาจสัมพันธ์กับการโจมตีแบบ DDoS
3. เพื่อสร้างระบบการแจ้งเตือนผ่าน Line Application สำหรับแสดงผลการตรวจจับ แจ้งเตือนสถานะการโจมตี และควบคุมการทำงานของระบบได้แบบเรียลไทม์

ขอบเขตของโครงงาน TEAM-PROJECT 3

1. สร้างระบบตรวจจับการโจมตี Distributed Denial of Service (DDoS) แบบเรียลไทม์
2. สร้างระบบแจ้งเตือนผ่าน Line Application

หมายเลขโครงงาน	

บล็อกไดอะแกรมของโครงงานที่นำเสนอ

แผนการปฏิบัติงานตลอดภาคการศึกษา

ช่วงการดำเนินงาน	แผนงานที่จะดำเนินการ	
เดือนที่ 1 (ธ.ค. 2568)	สัปดาห์ที่ 1	ศึกษาแนวคิดการโจมตีแบบ DDoS รวมถึงประเภทต่าง ๆ และลักษณะของทราฟฟิกที่ผิดปกติ พร้อมศึกษาวิธีทำงานของ Zeek ที่ใช้สำหรับเก็บ log เครือข่าย โดยวิเคราะห์ว่าฟีเจอร์ใดสามารถนำไปตรวจจับการโจมตีได้จริง
	สัปดาห์ที่ 2	ดำเนินการติดตั้งและตั้งค่า Zeek บนระบบที่เหมาะสม เช่น WSL2 หรือ Linux Server เพื่อเริ่มต้นเก็บข้อมูลทราฟฟิกแบบปกติและทดสอบการทำงานของไฟล์ log เบื้องต้น
	สัปดาห์ที่ 3	ทำการสร้างทราฟฟิกจำลองในเครือข่าย ทั้งแบบปกติและแบบ DDoS เพื่อรวบรวมข้อมูลจริงจาก Zeek และนำไปวิเคราะห์ในสัปดาห์ต่อ ๆ ไป
	สัปดาห์ที่ 4	จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 1
เดือนที่ 2 (ม.ค. 2569)	สัปดาห์ที่ 1	วิเคราะห์ฟีเจอร์จาก log ของ Zeek อย่างละเอียด เพื่อเลือกคุณลักษณะที่เหมาะสมต่อการฝึกโมเดล AI
	สัปดาห์ที่ 2	นำข้อมูลที่เตรียมไว้มาใช้สอนโมเดล AI แล้วลองปรับค่าการตั้งต่าง ๆ เพื่อดูว่าแบบไหนทำงานได้ดีที่สุดในการตรวจจับการโจมตี
	สัปดาห์ที่ 3	นำโมเดลที่ฝึกแล้วมาทดสอบกับชุดข้อมูลใหม่เพื่อประเมินประสิทธิภาพ
	สัปดาห์ที่ 4	จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 2

หมายเลขโครงงาน	

แผนการปฏิบัติงานตลอดภาคการศึกษา (ต่อ)

ช่วงการดำเนินงาน	แผนงานที่จะดำเนินการ	
เดือนที่ 3 (ก.พ. 2569)	สัปดาห์ที่ 1	ออกแบบระบบสำหรับการใช้งานจริง เช่น การส่ง log จาก Zeek ⟶ ระบบประมวลผล ⟶ โมเดล AI ⟶ alert รวมถึงร่าง API หรือ Workflow
	สัปดาห์ที่ 2	ดำเนินการพัฒนาสำหรับแสดงผลการแจ้งเตือน โดยเชื่อมต่อกับโมเดลตรวจจับ DDoS ที่พัฒนาไว้ พร้อมทดสอบการแสดงผลเบื้องต้น
	สัปดาห์ที่ 3	เริ่มทดสอบระบบแบบ End-to-End โดยจำลองการโจมตีจริง แล้วตรวจสอบว่าการแจ้งเตือน Line ทำงานแบบเรียลไทม์
	สัปดาห์ที่ 4	จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 3
เดือนที่ 4 (มี.ค. 2569)	สัปดาห์ที่ 1	ปรับปรุงระบบแจ้งเตือนให้แม่นยำและตอบสนองได้รวดเร็วขึ้น
	สัปดาห์ที่ 2	จัดเตรียมรายงานฉบับสมบูรณ์ โดยรวมเนื้อหาทั้งหมด
	สัปดาห์ที่ 3	จัดทำและส่งรายงานฉบับสมบูรณ์

หมายเหตุ

รายงานความก้าวหน้าที่จะมีกำหนดส่งของทุกๆเดือน ตามประกาศของภาควิชาฯ โดยในรายงานจะต้องมีหลักฐานผลการดำเนินงานเชิงประจักษ์ เช่น ผลการทดลอง ผลการทดสอบ และความสอดคล้องตามแผนการปฏิบัติงานที่ได้แสดงไว้

หมายเลขโครงงาน	

บทคัดย่อโครงงาน TEAM-PROJECT 3

ชื่อภาษาไทย ระบบตรวจจับการโจมตี Distributed Denial of Service (DDoS) แบบเรียลไทม์

ชื่อภาษาอังกฤษ REALTIME DISTRIBUTED DENIAL OF SERVICE (DDoS) DETECTION

บทคัดย่อ

โครงงานนี้นำเสนอระบบตรวจจับการโจมตีแบบ DDoS แบบเรียลไทม์ โดยมีวัตถุประสงค์เพื่อช่วยให้สามารถเฝ้าระวังความผิดปกติในเครือข่ายได้อย่างรวดเร็วและแม่นยำ ระบบประกอบด้วยส่วนการเก็บข้อมูลทราฟฟิกด้วย Zeek การประมวลผลและจำแนกพฤติกรรมด้วยโมเดล AI รวมถึงระบบแจ้งเตือนผ่าน Line Notify เมื่อพบรูปแบบทราฟฟิกที่มีลักษณะคล้ายการโจมตี โดยระบบทั้งหมดทำงานร่วมกันแบบอัตโนมัติ ตั้งแต่การรับข้อมูล วิเคราะห์ จนถึงแจ้งเตือนผู้ดูแลเครือข่ายเพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้ทันเวลา

Abstract

This project presents the development of a real-time DDoS attack detection system designed to help network administrators identify unusual traffic patterns quickly and accurately. The system consists of three main components: traffic capture using Zeek, behavior analysis through a machine learning model, and instant alert notifications delivered via Line Notify whenever suspicious activity is detected. These components work together automatically, starting from collecting network data, analyzing it for potential threats, and finally notifying the administrator so that appropriate action can be taken without delay.