หมายเลขโครงงาน	

แบบฟอร์มขอบเขตโครงงาน TEAM-PROJECT 3

ชื่อภาษาไทย แพลตฟอร์มรวมระบบรักษาความปลอดภัยเครือข่ายแบบหลายโมดูลสำหรับการตรวจจับและป้องกันภัยคุกคามเบื้องต้น

ชื่อภาษาอังกฤษ A MODULAR UNIFIED NETWORK SECURITY PLATFORM FOR BASIC THREAT DETECTION AND PROTECTION

โดย

นาย ณัฐศักดิ์ คูหล้า รหัสนักศึกษา 66010272

นาย ปราบดา ศรีพิชัย รหัสนักศึกษา 66010462

อาจารย์ที่ปรึกษาหลัก _____

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

อาจารย์ที่ปรึกษาร่วม _____

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

วัตถุประสงค์โดยคร่าวของการนำเสนอโครงงาน TEAM-PROJECT 3

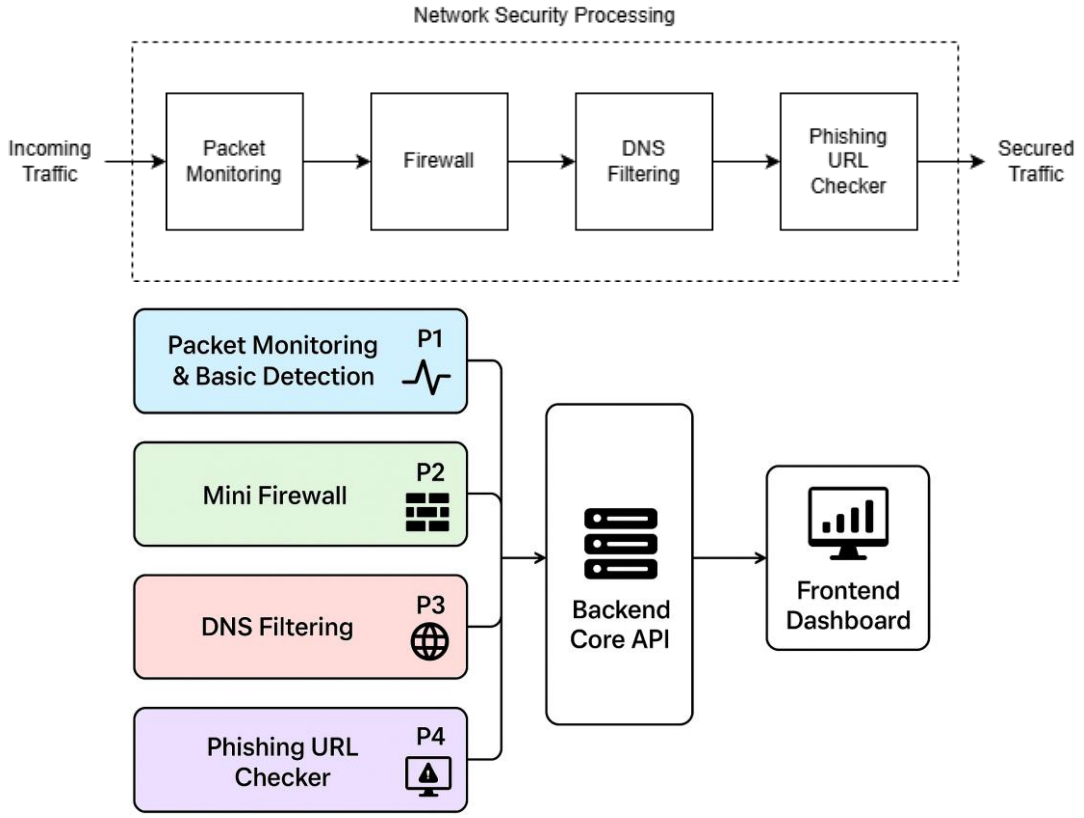
1. เพื่อศึกษาวิธีการตรวจจับและวิเคราะห์แพ็กเก็ตเครือข่ายพื้นฐาน โดยใช้เทคนิคการมอนิเตอร์ทราฟฟิกเพื่อระบุพฤติกรรมผิดปกติ เช่น ARP Spoofing และ Port Scanning
2. เพื่อศึกษาการทำงานของระบบควบคุมการเข้าถึงเครือข่าย (Firewall / Access Control) และพัฒนาเครื่องมือสำหรับกำหนดกฎการอนุญาตหรือปฏิเสธการเชื่อมต่อในระดับเบื้องต้น
3. เพื่อศึกษากระบวนการกรองและบล็อกโดเมนที่เป็นอันตรายผ่านระบบ DNS Filtering เพื่อลดความเสี่ยงจากเว็บไซต์ประเภทมัลแวร์ โฆษณา และฟิชชิ่ง
4. เพื่อศึกษารูปแบบและคุณลักษณะของ URL ที่ใช้ในการโจมตีแบบฟิชชิ่ง และพัฒนาเครื่องมือตรวจสอบ URL แบบ rule-based สำหรับช่วยระบุความเสี่ยงของลิงก์ก่อนเข้าถึง

หมายเลขโครงงาน	

ขอบเขตของโครงงาน TEAM-PROJECT 3

1. พัฒนาเครื่องมือสำหรับตรวจจับและวิเคราะห์ทราฟฟิกเครือข่ายเบื้องต้น (Packet Monitoring Tool) โดยประยุกต์ใช้การดักจับแพ็กเก็ตและการตรวจสอบพฤติกรรมผิดปกติ เพื่อใช้เป็นพื้นฐานของระบบรักษาความปลอดภัยในระดับสูงต่อไป
2. พัฒนาระบบควบคุมการเข้าถึงเครือข่าย (Mini Firewall) โดยสร้างกฎ Allow/Deny และแสดงสถานะหรือบันทึกข้อมูลทราฟฟิกที่ถูกบล็อก
3. พัฒนาระบบกรองโดเมนอันตรายด้วยวิธี DNS Filtering โดยรวบรวมรายการโดเมนเสี่ยง วิเคราะห์การร้องขอ DNS และบล็อกโดเมนที่ไม่ปลอดภัย
4. พัฒนาเครื่องมือตรวจสอบฟิชชิ่ง URL แบบ rule-based โดยออกแบบเงื่อนไขตรวจจับ เช่น ลักษณะโดเมนปลอม ชื่อคล้ายเว็บจริง การเข้ารหัสตัวอักษรผิดปกติ ฯลฯ
5. ทดสอบและประเมินประสิทธิภาพของเครื่องมือทั้ง 4 ส่วน โดยทดลองในเครือข่ายจำลอง วิเคราะห์ผลการตรวจจับ บันทึกสถานะ และสรุปจุดแข็งหรือข้อจำกัดของแต่ละโมดูล

บล็อกไดอะแกรมของโครงงานที่นำเสนอ



หมายเลขโครงงาน	

แผนการปฏิบัติงานตลอดภาคการศึกษา

ช่วงการดำเนินงาน	แผนงานที่จะดำเนินการ	
เดือนที่ 1 (ธ.ค. 2568)	สัปดาห์ที่ 1	ศึกษาข้อมูล บทความ และงานวิจัยที่เกี่ยวข้องกับ Packet Monitoring & Basic Detection
	สัปดาห์ที่ 2	ลงมือสร้างระบบป้องกัน Packet Monitoring & Basic Detection security โดยใช้ Python + Scapy หรือ TShark CLI ทำ packet capture และทดสอบระบบ
	สัปดาห์ที่ 3	ศึกษาข้อมูล บทความ และงานวิจัยที่เกี่ยวข้องกับ Mini Firewall
	สัปดาห์ที่ 4	จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 1
เดือนที่ 2 (ม.ค. 2569)	สัปดาห์ที่ 1	ลงมือสร้างระบบป้องกัน Mini Firewall security โดยใช้ iptables/nftables ผ่าน Python หรือ REST API และทดสอบระบบ
	สัปดาห์ที่ 2	ศึกษาข้อมูล บทความ และงานวิจัยที่เกี่ยวข้องกับ DNS Filtering
	สัปดาห์ที่ 3	ลงมือสร้างระบบป้องกัน DNS Filtering security โดยทำ “DNS Proxy” ด้วย Python ใช้ lib dnslib เพื่อรับ query ⟶ ตรวจ domain ⟶ forward หรือ block, ทำ blacklist / whitelist จาก Database และทดสอบระบบ
	สัปดาห์ที่ 4	จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 2
เดือนที่ 3 (ก.พ. 2569)	สัปดาห์ที่ 1	ศึกษาข้อมูล บทความ และงานวิจัยที่เกี่ยวข้องกับ Phishing URL Checker
	สัปดาห์ที่ 2	ลงมือสร้างระบบป้องกัน Phishing URL Checker security โดยใช้ Rule-based URL Inspection + Regex + Simple Heuristics และทดสอบระบบ
	สัปดาห์ที่ 3	ออกแบบระบบรวมโมดูลให้อยู่ในระบบเดียว แบบ แยกแต่สื่อสารกันผ่าน API / Log โดยใช้วิธี Backend Core API + Modular Services + Dashboard เดียว และทดสอบระบบ
	สัปดาห์ที่ 4	จัดทำและส่งรายงานความก้าวหน้าครั้งที่ 3

หมายเลขโครงงาน	

แผนการปฏิบัติงานตลอดภาคการศึกษา (ต่อ)

ช่วงการดำเนินงาน	แผนงานที่จะดำเนินการ	
เดือนที่ 4 (มี.ค. 2569)	สัปดาห์ที่ 1	เชื่อมต่อระบบรวม ทดสอบความถูกต้อง และประเมินประสิทธิภาพในการใช้งานระบบ
	สัปดาห์ที่ 2	ปรับแก้ไขให้เหมาะสมเพื่อความเสถียร
	สัปดาห์ที่ 3	จัดทำเล่มและรายงานฉบับสมบูรณ์

หมายเหตุ

รายงานความก้าวหน้าที่จะมีกำหนดส่งของทุกๆเดือน ตามประกาศของภาควิชาฯ โดยในรายงานจะต้องมีหลักฐานผลการดำเนินงานเชิงประจักษ์ เช่น ผลการทดลอง ผลการทดสอบ และสอดคล้องตามแผนการปฏิบัติงานที่ได้แสดงไว้

หมายเลขโครงงาน	

บทคัดย่อโครงงาน TEAM-PROJECT 3

ชื่อภาษาไทย แพลตฟอร์มรวมระบบรักษาความปลอดภัยเครือข่ายแบบหลายโมดูลสำหรับการตรวจจับและป้องกันภัยคุกคามเบื้องต้น

ชื่อภาษาอังกฤษ A MODULAR UNIFIED NETWORK SECURITY PLATFORM FOR BASIC THREAT DETECTION AND PROTECTION

บทคัดย่อ

โครงงานนี้นำเสนอการพัฒนา “แพลตฟอร์มรักษาความปลอดภัยเครือข่ายแบบรวมศูนย์” ที่ออกแบบให้สามารถตรวจจับภัยคุกคามและควบคุมระบบได้จากอินเทอร์เฟซเดียว โดยแพลตฟอร์มประกอบด้วยสี่โมดูลหลัก ได้แก่ (1) ระบบตรวจสอบแพ็กเก็ตและการโจมตีพื้นฐาน (Packet Monitoring & Basic Detection) สำหรับเฝ้าระวังพฤติกรรมผิดปกติ เช่น ARP Spoofing และการสแกนพอร์ต (2) ระบบไฟร์วอลล์ขนาดเล็ก (Mini Firewall) ที่ผู้ใช้สามารถกำหนดกฎการป้องกันได้ผ่านหน้าจอควบคุม (3) ระบบกรองโดเมนผ่าน DNS (DNS Filtering) สำหรับบล็อกเว็บไซต์ที่เป็นอันตราย และ (4) ระบบตรวจสอบลิงก์ฟิชชิงแบบกฎเงื่อนไข (Phishing URL Checker) เพื่อวิเคราะห์ความเสี่ยงจาก URL ที่น่าสงสัย

ทั้งสี่โมดูลถูกออกแบบให้ทำงานร่วมกันผ่าน Backend Core API ซึ่งทำหน้าที่เป็นศูนย์กลางในการรับข้อมูล ประมวลผล และส่งต่อผลการตรวจจับไปยังแดชบอร์ดแบบรวมศูนย์ (Unified Dashboard) ที่ผู้ใช้สามารถตรวจสอบสถานะความปลอดภัยได้แบบเรียลไทม์ โครงสร้างแบบโมดูลาร์ (Modular Architecture) นี้ช่วยให้ระบบมีความยืดหยุ่น สามารถเพิ่มหรือปรับปรุงฟังก์ชันในอนาคตได้ง่าย ผลลัพธ์ของโครงงานแสดงให้เห็นว่าการรวมหลายเครื่องมือด้านความปลอดภัยไว้ในแพลตฟอร์มเดียวสามารถเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามและลดความซับซ้อนในการบริหารจัดการระบบได้อย่างชัดเจน และ โครงงานนี้คาดหวังว่าจะช่วยลดปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ได้

หมายเลขโครงงาน	

Abstract

This project presents the development of a unified network security platform designed to enhance threat detection and simplify security management through a centralized interface. The platform integrates four core modules: (1) a Packet Monitoring & Basic Detection module for identifying abnormal network behaviors such as ARP spoofing and port scanning, (2) a Mini Firewall module that allows users to create and manage basic security rules, (3) a DNS Filtering module for blocking malicious or unwanted domains, and (4) a rule-based Phishing URL Checker that analyzes suspicious URLs to detect potential phishing threats.

All modules operate collaboratively through a Backend Core API, which serves as the central processing layer responsible for receiving, analyzing, and distributing security data. The results are visualized through a unified dashboard that provides real-time monitoring and system control. The modular architecture allows for flexibility, scalability, and the ability to integrate additional security features in the future. The outcomes of this project demonstrate that consolidating multiple security functions into a single platform significantly improves threat visibility, operational efficiency, and overall network protection. The proposed system is expected to help reduce the problems caused by cybersecurity threats.