

การมองเห็นเครือข่ายด้วย Security Onion

โดย นายนิภัทร์ ดวงคู่สัน

นายภัทรธร สุภาพ

บทคัดย่อ

โครงการนี้มีวัตถุประสงค์เพื่อศึกษาและประยุกต์ใช้ Security Onion ซึ่งเป็นแพลตฟอร์มโอเพนซอร์ส (Open-source Platform) สำหรับการเฝ้าระวังความปลอดภัยเครือข่าย (Network Security Monitoring, NSM) และเป็นระบบตรวจจับการบุกรุก (Intrusion Detection System, IDS) เพื่อเพิ่มความสามารถในการมองเห็นกิจกรรมในเครือข่ายและตรวจจับภัยคุกคามทางไซเบอร์ ภายใน Security Onion ประกอบด้วยเครื่องมือสำคัญ เช่น ระบบตรวจจับการบุกรุกระดับเครื่องคอมพิวเตอร์ (Host-based Intrusion Detection System, HIDS) ระบบตรวจจับการบุกรุกระดับเครือข่าย (Network-based Intrusion Detection System, NIDS) และชุดเครื่องมือ ELK Stack ที่ช่วยรวบรวมและนำเสนอข้อมูลการแจ้งเตือน ในการดำเนินโครงการ ได้ติดตั้งระบบแบบจำลองและกำหนดค่าการดักจับข้อมูล (Traffic Mirroring) บนสวิตช์หลัก (Core Switch) จากนั้นทดสอบโดยจำลองการโจมตีด้วย Nmap Script Engine ผลการทดสอบพบว่า ระบบสามารถตรวจจับและแจ้งเตือนการโจมตีได้หลากหลายรูปแบบ ทั้งการโจมตีข้ามเครือข่ายจาก (Wireless Local Area Network, WLAN) ไปยัง (Virtual Local Area Network, VLAN) การโจมตีภายใน VLAN เดียวกันและการโจมตีจากภายนอกเครือข่ายได้สำเร็จ แสดงให้เห็นว่า Security Onion เป็นทางเลือกที่มีประสิทธิภาพในการยกระดับความปลอดภัยเครือข่ายและสอดคล้องกับวัตถุประสงค์ของโครงการ

Network Visibility with Security Onion

By Mr. Niphat DuangDusan

Mr. Patraratorn Supap

ABSTRACT

This project aims to study and implement Security Onion, an open-source platform for Network Security Monitoring (NSM) and Intrusion Detection System (IDS), to enhance network visibility and detect cyber threats. Security Onion integrates essential tools including Host-based Intrusion Detection System (HIDS), Network-based Intrusion Detection System (NIDS), and the ELK Stack for collecting and presenting alert data. The implementation involved deploying a cluster configuration and setting up traffic mirroring on the core switch. Testing was conducted by simulating attacks using Nmap Script Engine. The results demonstrated that the system successfully detected and alerted various attack patterns, including cross-network attacks from Wireless Local Area Network (WLAN) to Virtual Local Area Network (VLAN), attacks within the same VLAN, and attacks from outside the network. This shows that Security Onion is an effective solution for enhancing network security and aligns with the project objectives.