Analisis Implementasi Security Information and Event Management System (SIEM) Berbasis Wazuh pada Serangan Denial of Service (DoS) = Implementation Analysis of Wazuh Based Security Information and Event Management (SIEM) for Denial of Service (DoS) Attack

Muhammad Taqiy Nur Furqon, author

Abstrak

Serangan Denial of Service adalah salah satu ancaman serius bagi keamanan jaringan yang dapat menyebabkan gangguan dan tidak tersedianya suatu layanan. Security Information and Event Management (SIEM) Wazuh merupakan sebuah solusi open-source yang dirancang untuk memberikan visibilitas, analisis, dan respons terhadap ancaman keamanan dalam jaringan. Penelitian ini bertujuan untuk menganalisis implementasi SIEM Wazuh dalam mendeteksi serangan DoS dengan mengintegrasikan SIEM Wazuh dengan Intrusion Detection System (IDS) Suricata sebagai pengumpul log paket jaringan. Penelitian dilakukan dalam lingkungan mesin virtual dengan tiga skenario serangan, SYN flood, UDP flood, serta ICMP flood yang dilakukan dengan Hping. Dari hasil penelitian didapatkan bahwa Wazuh dapat mendeteksi semua serangan berdasarkan rule kustom yang telah dibuat dengan waktu rerata deteksi tiap serangan secara berurut 13,99 detik, 45,083 detik, dan 1,2 detik. Penelitian ini menunjukkan bahwa Wazuh mendeteksi serangan berdasarkan rule dan fitur seperti pemantauan log real-time, analisis rule-based serta integrasi dengan sistem keamanan lainnya berkontribusi terhadap efektivitas Wazuh dalam mendeteksi serangan DoS. .....Denial of Service attacks pose a serious threat to network security, causing disruption and service unavailability. Security Information and Event Management (SIEM) Wazuh is an open-source solution designed to provide visibility, analysis, and response to security threats within networks. This research aims to analyze the implementation of SIEM Wazuh in detecting DoS attacks by integrating it with the Intrusion Detection System (IDS) Suricata as the network packet logging collector. The study was conducted in a virtual machine environment with three attack scenarios: SYN flood, UDP flood, and ICMP flood simulated using Hping3. The research findings indicate that Wazuh can detect all attacks based on custom rules created, with average detection times for each attack scenario sequentially being 13.99 seconds, 45.083 seconds, and 1.2 seconds. The study demonstrates that Wazuh detects attacks through rules and features such as real-time log monitoring, rule-based analysis, and integration with other security systems contributing to its effectiveness in detecting DoS attacks.