

Adam Darmasaputra. 2025. Implementasi Sistem Keamanan Jaringan Berbasis IDS/IPS Suricata dan ELK Stack Pada Linux Di SMKN 1 Dlanggu. Skripsi, Program Studi Pendidikan Informatika, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Trunojoyo Madura. Pembimbing Nuru Aini.

ABSTRAK

Jaringan komputer di SMKN 1 Dlanggu belum memiliki sistem keamanan yang mampu mendeteksi dan mencegah serangan secara real-time, sehingga rentan terhadap serangan DDoS. Untuk mengatasi hal tersebut, dikembangkan sistem IDS/IPS berbasis Suricata yang terintegrasi dengan Filebeat, Elasticsearch, dan Kibana menggunakan metode Security Development Life Cycle (SDLC) dengan model Waterfall. Metode ini dipilih karena alurnya terstruktur dan mendukung pengembangan sistem keamanan secara menyeluruh. Pengujian dilakukan menggunakan serangan *Syn Flood*, *Ping of Death*, *ICMP Flood*, dan *HTTP Flood*. Sebelum implementasi, lalu lintas jaringan menunjukkan lonjakan signifikan akibat permintaan palsu yang menurunkan kinerja layanan. Setelah implementasi, serangan berhasil dideteksi dan diblokir secara real-time, sehingga layanan tetap tersedia. Hasil menunjukkan sistem bekerja efektif dan stabil. Rata-rata keberhasilan sistem berdasarkan hasil validasi mencapai 92,45% sebelum implementasi dan 89,00% sesudah implementasi. Implementasi ini dinilai layak untuk diterapkan dalam meningkatkan keamanan jaringan di SMKN 1 Dlanggu.

Kata Kunci : DDOS, *Intrusion Detection and Prevention System (IDPS)*, Keamanan jaringan, *Security Development Life Cycle (SDLC)*, *Waterfall*.

Adam Darmasaputra. 2025. *Implementation of Network Security System Based on IDS/IPS Suricata and ELK Stack on Linux at SMKN 1 Dlanggu*. Skripsi, Informatics Education Study Program, Faculty of Teacher Training and Education, Trunojoyo Madura University. Supervisor: Nuru Aini.

ABSTRACT

The computer network at SMKN 1 Dlanggu currently lacks a security system capable of detecting and preventing attacks in real time, making it vulnerable to DDoS attacks. To address this issue, an IDS/IPS system based on Suricata was developed and integrated with Filebeat, Elasticsearch, and Kibana using the Security Development Life Cycle (SDLC) method with the Waterfall model. This method was chosen because of its structured flow and comprehensive support for secure system development. Testing was conducted using SYN Flood, Ping of Death, ICMP Flood, and HTTP Flood attacks. Before implementation, network traffic showed significant spikes caused by fake requests that degraded service performance. After implementation, the attacks were successfully detected and blocked in real time, ensuring service availability. The results showed that the system functioned effectively and remained stable. The average success rate based on validation results reached 92.45% before implementation and 89,00% after implementation. This implementation is considered feasible to improve network security at SMKN 1 Dlanggu.

Keywords: *DDOS, Intrusion Detection and Prevention System (IDPS), Network security, Security Development Life Cycle (SDLC), Waterfall.*