ABSTRAK

YUSUF LAURENTSIUS HAREFA. 2025. Analisis dan Implementasi *Intrusion Detection System* (IDS) pada Sistem Monitoring Kamera Berbasis IoT. Dibimbing oleh HENDRA KURNIAWAN dan NOLAN EFRANDA.

Keamanan pada ekosistem *Internet of Things* (IoT) menjadi tantangan krusial seiring dengan meningkatnya ancaman serangan siber yang dapat mengganggu fungsionalitas perangkat. Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis performa Snort sebagai *Intrusion Detection System* (IDS) pada *Virtual Private Server* (VPS) untuk memantau trafik dari perangkat NodeMCU ESP32-CAM. Metodologi yang digunakan adalah simulasi serangan *Distributed Denial of Service* (DDoS) meliputi *TCP SYN Flood*, *UDP Flood*, dan *ICMP Flood* guna mengevaluasi kemampuan deteksi serta dampaknya terhadap transmisi data gambar secara real-time melalui notifikasi bot Telegram. Hasil penelitian menunjukkan bahwa Snort IDS berhasil mendeteksi seluruh aktivitas serangan dengan tingkat akurasi 100% berdasarkan log alert yang dihasilkan. Namun, pengujian performa mengindikasikan adanya penurunan kualitas layanan (*Quality of Service*) yang signifikan saat terjadi serangan. Rata-rata waktu transmisi gambar meningkat dari 5,66 detik pada kondisi normal menjadi 9,11 detik saat terjadi serangan *UDP Flood*. Secara keseluruhan, serangan DDoS menyebabkan kenaikan latensi dalam rentang 21,91% hingga 60,95%. Meskipun terjadi peningkatan latensi, sistem menunjukkan ketangguhan (*resilience*) yang baik karena integritas data tetap terjaga tanpa adanya *packet loss*. Integrasi IDS dengan Telegram efektif memberikan peringatan dini bagi administrator untuk meningkatkan respons keamanan pada jaringan IoT.

Kata kunci: *Snort IDS, IoT, ESP32-CAM, DDoS, Latensi, Telegram Bot.*

ABSTRACT

YUSUF LAURENTSIUS HAREFA. 2025. Analysis and Implementation of Intrusion Detection System (IDS) in IoT-Based Camera Monitoring System. Supervised by HENDRA KURNIAWAN and NOLAN EFRANDA.

Security in the Internet of Things (IoT) ecosystem is becoming a crucial challenge as cyber threats that can disrupt device functionality increase. This study aims to implement and analyze the performance of Snort as an Intrusion Detection System (IDS) on a Virtual Private Server (VPS) to monitor traffic from NodeMCU ESP32-CAM devices. The methodology used was a Distributed Denial of Service (DDoS) attack simulation, including TCP SYN Flood, UDP Flood, and ICMP Flood, to evaluate detection capabilities and their impact on real-time image data transmission via Telegram bot notifications. The results showed that Snort IDS successfully detected all attack activities with 100% accuracy based on the generated alert logs. However, performance testing indicated a significant decrease in Quality of Service (QoS) during attacks. The average image transmission time increased from 5.66 seconds under normal conditions to 9.11 seconds during a UDP Flood attack. Overall, DDoS attacks caused latency increases ranging from 21.91% to 60.95%. Despite the increase in latency, the system demonstrated good resilience as data integrity was maintained without any packet loss. The integration of IDS with Telegram effectively provided early warnings to administrators to improve security responses on the IoT network.

Keywords: *Snort IDS, IoT, ESP32-CAM, DDoS, Latency, Telegram Bot.*