

ABSTRAK

Ancaman siber terhadap infrastruktur server tidak lagi sekadar potensi, melainkan realitas yang terbukti mampu melumpuhkan sistem layanan digital secara masif. Serangan *Distributed Denial of Service (DDoS)* dan *Brute Force* terus meningkat secara eksponensial, namun sistem notifikasi konvensional berbasis surel yang digunakan mayoritas administrator jaringan terbukti gagal memberikan respons yang memadai karena latensi pengiriman pesan yang tidak bersifat instan. Penelitian ini bertujuan mengimplementasikan sistem monitoring keamanan server secara real-time yang mengintegrasikan *SNORT* sebagai *Intrusion Detection System (IDS)* dengan *WhatsApp API* berbasis bahasa pemrograman Go sebagai media notifikasi peringatan dini (*early warning system*). Metodologi penelitian menerapkan kerangka kerja *TAARA (Trigger, Acquire, Analyze, Report, and Action)* yang mencakup tahapan identifikasi serangan sebagai pemicu, akuisisi data log, analisis pola serangan, pelaporan otomatis ke perangkat seluler administrator, serta otentikasi integritas log menggunakan nilai hash untuk keperluan forensik digital. Sistem diuji terhadap tiga skenario serangan, yaitu *TCP Flood*, *UDP Flood*, dan *ICMP Flood*, yang disimulasikan menggunakan *LOIC (Low Orbit Ion Cannon)* dalam lingkungan laboratorium terkontrol. Hasil pengujian membuktikan bahwa sistem mampu mendeteksi dan meneruskan informasi serangan secara real-time dengan rata-rata latensi notifikasi *WhatsApp* sebesar 1,5 hingga 3 detik pasca-deteksi, yang secara signifikan lebih unggul dibandingkan sistem notifikasi berbasis surel. Temuan ini menegaskan bahwa integrasi *SNORT IDS* dengan *WhatsApp API* berbasis Go merupakan solusi yang tidak hanya responsif, tetapi juga ringan secara sumber daya dan dapat diadopsi secara mandiri oleh organisasi dengan infrastruktur terbatas.

Kata Kunci: *Monitoring Server, Snort IDS, WhatsApp API, go-whatsapp-web-multidevice, Metode TAARA, Keamanan Jaringan.*

ABSTRACT

Cyber threats against server infrastructure are no longer a distant risk but a proven reality capable of crippling digital service systems on a massive scale. Distributed Denial of Service (DDoS) and Brute Force attacks continue to escalate exponentially; however, conventional email-based notification systems used by most network administrators have demonstrably failed to provide adequate response due to inherent message delivery latency. This research aims to implement a real-time server security monitoring system that integrates Snort as an Intrusion Detection System (IDS) with a Go-based WhatsApp API as an early warning notification medium. The research methodology employs the TAARA framework (Trigger, Acquire, Analyze, Report, and Action), encompassing attack identification as a trigger, log data acquisition, attack pattern analysis, automated reporting to the administrator's mobile device, and log integrity authentication using hash values for digital forensic purposes. The system was tested against three attack scenarios — TCP Flood, UDP Flood, and ICMP Flood — simulated using LOIC (Low Orbit Ion Cannon) in a controlled laboratory environment. Test results demonstrate that the system can detect and relay attack information in real-time with an average WhatsApp notification latency of 1.5 to 3 seconds post-detection, significantly outperforming email-based notification systems. These findings affirm that the integration of Snort IDS with a Go-based WhatsApp API is a solution that is not only highly responsive but also resource-efficient and independently deployable by organizations with limited infrastructure.

Keywords: Server Monitoring, Snort IDS, WhatsApp API, go-whatsapp-web-multidevice, TAARA Method, Network Security.