ABSTRAK

Dengan peningkatan serangan *Bruteforce* secara global, termasuk yang terjadi di Indonesia, serta kerentanan SQL *Injection* yang cukup signifikan pada aplikasi *web*, serta rekor serangan DoS yang tercatat pada kuartal pertama 2023, menjadi jelas bahwa keamanan *webserver* perlu ditingkatkan guna memastikan integritas, validitas data, dan ketersediaan layanan bagi pengguna. Dalam menghadapi tantangan ini, *Intrusion Prevention System* (IPS) telah menjadi pendekatan umum. IPS memiliki fungsi mendeteksi dan mencegah serangan siber dengan menganalisis lalu lintas jaringan secara *realtime*, menjadi solusi perlindungan yang efektif. IPS dapat melindungi dari serangan *Bruteforce*, SQL *Injection*, dan serangan DoS, termasuk ICMP *flood* yang memberikan beban berlebih pada sumber daya server. Pengujian evaluasi IPS menunjukkan hasil memuaskan, dimana terjadi penurunan penggunaan CPU dari 15,8% menjadi 7,7%, penggunaan *memory* meningkat dari 47,8% menjadi 61,7%. Pada serangan SQL *Injection*, penggunaan CPU menurun dari 7,1% menjadi 5,5%, *memory* tetap 48,4%. Serangan DoS mengalami penurunan penggunaan CPU drastis dari 47,7% menjadi 7,1%, dengan penggunaan *memory* stabil pada 60,8%. IPS berhasil mempertahankan *response time* 2,6 ms. Selain itu, penelitian berhasil mengaplikasikan Telegram *bot* untuk memberi informasi pada *administrator* jaringan mengenai ancaman serangan dengan batasan penggunaan CPU lebih dari 70%. Mekanisme ini memungkinkan *administrator* memungkinkan tindakan mitigasi dengan tepat waktu. Kesimpulannya, IPS efektif dalam melindungi sistem dari serangan *Bruteforce*, SQL *Injection*, dan DoS. Diperlukan perhatian khusus pada penggunaan sumber daya saat serangan DoS untuk efisiensi yang lebih baik. Data pengujian menunjukkan bahwa IPS efektif dalam menghadapi serangan *Bruteforce*, SQL *Injection* dan DoS dengan performa yang baik.

Kata Kunci: *Intrusion Prevention System* (IPS), *Bruteforce*, SQL *Injection*, DoS, Telegram