ABSTRAK

Aplikasi web sebagai salah satu media digital yang sering menjadi sasaran serangan siber mengalami sekitar 75% dari total serangan siber. Pada tahun 2023, sebanyak 30.000 situs web diretas setiap hari, hal ini menunjukkan betapa rentannya aplikasi web karena ketersediaannya yang harus konstan bagi pengguna. Salah satu jenis ancaman keamanan aplikasi web adalah adanya permintaan yang berisi *payload* berbahaya seperti SQLi dan XSS ke aplikasi web. Jenis ancaman keamanan aplikasi web lainnya adalah DDoS. Serangan DDoS ini dapat membuat situs web tidak berfungsi atau tidak dapat diakses.

Untuk mengatasi permasalahan tersebut maka dirancang solusi berupa perancangan dan implementasi WAF, *rate limiting* serta IDS pada keamanan aplikasi web. Pada solusi, WAF diimplementasikan untuk memfilter *payload* berbahaya berupa SQLi dan XSS. Sedangkan *rate limiting* diimplementasikan untuk memfilter serangan DDoS berdasarkan *threshold* yang ditentukan. Selain itu, diimplementasikan Snort untuk mengirimkan pesan ke aplikasi Telegram sebagai *alert* ketika terjadi ketiga serangan tersebut.

Berdasarkan hasil pengujian, WAF memperoleh skor *security quality* sebesar 99,6% dan *detection quality* sebesar 92,3%. Rata-rata *throughput* tanpa *rate limiting* adalah 13382.389916 kbits/s, sedangkan rata-rata *throughput* dengan *rate limiting* adalah 8004.082379 kbits/s. Rata-rata *packet loss* tanpa *rate limiting* adalah 0.191928% sedangkan rata-rata *packet loss* dengan *rate limiting* adalah 0.011805%. Rata-rata *delay* tanpa *rate limiting* sebesar 0.000355 s, sedangkan rata-rata *delay* dengan *rate limiting* sebesar 0.000284 s. Rata-rata jitter tanpa *rate limiting* sebesar 0.000012 s, sedangkan rata-rata *jitter* dengan *rate limiting* sebesar 0.000020 s. Pada IDS, Snort berhasil mengirimkan pesan peringatan sesuai dengan jenis serangan yang terjadi.

Kata kunci: ***web application firewall, rate limiting, intrusion detection system, cyber defense***