Integrasi IDS Heterogen dengan SIEM untuk Deteksi Serangan DDoS di Lingkungan Multi-Organisasi Jaringan Komputer

M. Akmal Maliki[1], Parman Sukarno[2], Aulia Arif Wardana[3]
[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]akmalm@student.telkomuniversity.ac.id,
[2]psukarno@telkomuniversity.ac.id,
[3]aulia.wardana@pwr.edu.pl,

Abstrak

Meningkatnya ketergantungan pada jaringan komputer untuk operasional bisnis telah menyebabkan peningkatan serangan *Distributed Denial of Service* (DDoS). Serangan-serangan ini menimbulkan ancaman signifikan terhadap keamanan jaringan, stabilitas ekonomi, dan operasi organisasi. Organisasi yang terhubung melalui jaringan yang sama dengan organisasi yang lain dapat berisiko juga terkena serangan DDoS. Dalam menanggapi ancaman yang berkembang saat ini, didapatkan solusi untuk mengembangkan sistem deteksi yang mengintegrasikan *Intrusion Detection System* (IDS) yang heterogen dengan *Security Information and Event Management* (SIEM). Integrasi ini dikembangkan untuk mendeteksi serangan DDoS dalam jaringan komputer di lingkungan multi-organisasi. Sistem ini menggunakan *Opensearch Dashboard*, menyediakan antarmuka terpusat dan efisien untuk *Security Operations Center*. Pengujian sistem dilakukan melalui simulasi serangan DDoS yang terkoordinasi oleh tiga penyerang dengan durasi 7-8 menit. Snort menunjukkan tingkat deteksi rata-rata sebesar 95,4%, dengan mekanisme *alert correlation* yang secara efisiensi mampu mendeteksi dengan rata-rata sebesar 84,6%. Di antara sistem IDS yang diuji, Zeek IDS mengonsumsi sumber daya paling banyak, dengan rata-rata penggunaan CPU sebesar 24,6% dan penggunaan memori sebesar 86,5%. Sebaliknya, Dasbor Wazuh menunjukkan konsumsi sumber daya yang lebih rendah, dengan rata-rata penggunaan CPU sebesar 0,6% dan penggunaan memori sebesar 5,2%.

Kata kunci: DDoS, IDS, SIEM, Multi-Organisasi, Jaringan Komputer