Sistem Deteksi dan Prevensi pada Computer Network untuk Menangani Serangan Distributed Denial of Service (DDoS) secara Realtime dan Multi-Agent

Johanes Raphael Nandaputra[1], Parman Sukarno[2], Aulia Arif Wardana[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]johanesraphael@students.telkomuniversity.ac.id, [2]psukarno@telkomuniversity.ac.id,
[3]auliawardan@telkomuniversity.ac.id,

Abstrak

Penelitian ini membangun sebuah sistem *realtime* dan *multi-agent* untuk menangani serangan *Distributed Denial of Service* (DDoS). Integrasi *Intrusion Detection System* (IDS), *Security Information and Event Management* (SIEM), dan *Security Orchestration, Automation, and Response* (SOAR) membentuk mekanisme pertahanan yang kuat, memanfaatkan Discord untuk mengirimkan notifikasi peringatan ke *Security Operations Center* (SOC). Diuji dengan mengirimkan 10 serangan DDoS melalui SYN *flooding*, sistem ini menghasilkan ketepatan sebesar 89%, yang menunjukkan kemampuannya untuk meminimalkan *false positive* dan mengidentifikasi ancaman yang sebenarnya. Sistem ini juga menunjukkan bahwa Wazuh Indexer mengkonsumsi sumber daya paling banyak dengan penggunaan CPU rata-rata 22,94% dan penggunaan memori 58,04%, sementara Shuffle Frontend menunjukkan konsumsi sumber daya yang lebih rendah, dengan penggunaan CPU rata-rata 0,0% dan penggunaan memori 0,14%. Konsumsi sumber daya yang bervariasi ini menyoroti kemampuan adaptasi dan skalabilitas sistem di berbagai skenario operasional.

Kata kunci : DDoS, *real-time, multi-agent,* IDS, SIEM, SOAR, SOC