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,

Abstract

The increasing reliance on computer networks for business operations has led to a rise in Distributed Denial of Service (DDoS) attacks. These attacks pose significant threats to network security, economic stability, and organizational operations. Organizations connected through the same network are particularly vulnerable. Organizations that are connected via the same network as other organizations may also be at risk of DDoS attacks. In response to currently developing threats, a solution was found to develop a detection system that integrates a heterogeneous Intrusion Detection System (IDS) with Security Information and Event Management (SIEM). This integration was developed to detect DDoS attacks in computer networks in multi-organization environments. The system employs the Opensearch dashboard, providing a centralized and efficient interface for the Security Operations Center. System testing was conducted through coordinated DDoS attack simulations by three attackers over a duration of 7-8 minutes. The Snort IDS demonstrated an average detection rate of 95.4%, with an alert correlation mechanism efficiency of 84.6%. Among the IDS systems tested, Zeek IDS consumed the most resources, with an average CPU usage of 24.6% and memory usage of 86.5%. In contrast, the Wazuh Dashboard exhibited lower resource consumption, with an average CPU usage of 0.6% and memory usage of 5.2%.

Keywords: DDoS, IDS, SIEM, Multi-Organizations, Computer Network