Detection and Prevention System on Computer Network to Handle Distributed Denial of Service (DDoS) Attacks in Realtime and 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,

Abstract

This research builds a realtime and multi-agent system to handle Distributed Denial of Service (DDoS) attacks. The integration of an Intrusion Detection System (IDS), Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) establishes a robust defense mechanism, utilizing Discord for sending alert notifications to the Security Operations Center (SOC). Tested with sending 10 DDoS attacks by SYN flooding, the system resulted in a precision of 89%, showcased its capability to minimize false positives and identify true threats. The system also shows that Wazuh Indexer consumed the most resources with an average CPU usage of 22.94% and memory usage of 58.04%, while Shuffle Frontend exhibited lower resource consumption, with an average CPU usage of 0.0% and memory usage of 0.14%. These varied resource consumptions highlight the system's adaptability and scalability across diverse operational scenarios.

Keywords: DDoS, real-time, multi-agent, IDS, SIEM, SOAR, SOC