ABSTRACT

Cyberattacks on government websites in Indonesia have steadily increased, with over 109 million incidents recorded in 2023 by the National Cyber Security Operations Center of BSSN. Netcraft surveys indicate that over one billion websites globally face similar threats, underscoring the urgent need for enhanced security measures, especially given infrastructure limitations and inadequate security implementation. Around 51% of Micro, Small, and Medium Enterprises (MSMEs) in Indonesia reported experiencing web attacks, with 95% noting these attacks as severely disruptive to operations. This research implements a Suricata-based Intrusion Prevention System (IPS) to defend web servers against attacks like SQL Injection, XSS, and command injection. Suricata functions as a primary security layer, monitoring network traffic and blocking threats in real-time. Detection logs in JSON format are managed via Filebeat, processed by Logstash, stored in Elasticsearch, and visualized through Kibana. All components are operated within a single Docker container, streamlining the setup process. Testing confirmed that the configured rules achieved 100% effectiveness in detecting and blocking attack payloads. Suricata logs integrated seamlessly with Elasticsearch, with Kibana enabling insightful visualizations for detailed attack analysis. The novelty of this research lies in implementing the entire real-time threat detection security system on a low-end and resource-limited computer, demonstrating effective threat management by enhancing Suricata rules and firewall rules (NFQueue) to block SQL injection, XSS, and command injection.

Keywords: Cyberattacks, Elasticsearch, Intrusion prevention system, Suricata, Web attack.