Abstract

Cyber attacks such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) often threaten the operations of academic institutions. Conventional security systems are often ineffective in detecting and mitigating large-scale attacks. Therefore, improving the ability to detect and prevent cyber attacks is a top priority, especially in academic environments that store sensitive data.

This research applies Suricata as an Intrusion Prevention System (IPS) to detect and prevent anomalous attacks on Telkom University Surabaya servers. Suricata monitors network traffic in real-time and uses rules to identify and automatically block suspicious traffic. Integration with Telegram allows for quick notifications to network administrators, so they can take additional action immediately.

The results showed Suricata IPS was effective in detecting and blocking TCP, UDP, and ICMP packets with 99% accuracy, although accuracy on the HTTP protocol decreased to 90%. The Telegram notification system successfully provided real-time notifications with a delay of 1 to 2 seconds, despite using higher resources. Overall, the combination of Suricata and Telegram notifications proved effective in improving server security and reducing the risk of cyberattacks.

Keywords: suricata, intrusion prevention system (IPS), server security, cyber attack, anomaly