

ABSTRACT

Network security has become very important along with the increasing cyber threats, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which can disrupt network operations. To face this challenge, Dinkominfo Banyumas Regency implemented a Suricata-based Intrusion Detection System (IDS) system. Suricata was chosen for its ability to detect cyber threats in real-time and provide early warning to network administrators. This research focuses on the installation, configuration, and testing of the Suricata system against simulated threats. The results show that Suricata is effective in detecting attacks, with high accuracy and speed. The resulting early warnings enable a quick response to prevent further network disruptions. The implementation also improved the preparedness of Dinkominfo's IT team in managing and maintaining the network security system on an ongoing basis. Suricata proved to be a reliable IDS solution to maintain Dinkominfo's network stability.

Keywords: *Information Technology, IDS, Dinkominfo, Suricata, Network Security*