ABSTRACT

As cyber threats such as Denial of Service (DoS) attacks continue to rise, the implementation of an Intrusion Detection System (IDS) has become a strategic step in maintaining network stability and security. This study explores the performance comparison between two signature-based IDS tools, Snort and Suricata, in detecting SYN Flood attacks within a simulated network environment. The research adopts the PPDIOO methodology, which includes phases from planning to system operation. The testing environment was built using GNS3 and Virtual Machines running Ubuntu and Kali Linux operating systems. Both IDS tools were configured with specific rules to detect SYN packets from the TCP protocol, and testing was conducted five times with each session lasting 30 seconds. Evaluation results show that Snort achieved an average accuracy rate of 72%, while Suricata recorded 65%. Snort outperformed Suricata in four out of five tests and reached the highest accuracy of 83%. This performance difference indicates that Snort is superior in terms of consistency and detection accuracy compared to Suricata. This study is expected to serve as a reference in selecting the appropriate IDS for organizational network needs..

Keywords*: Network Security, IDS, LAN, GNS3, Suricata, Sno*