ABSTRACT

The development of network security is needed along with the development of today's technology. The increase in increasingly sophisticated technology has led to various crimes. The number of irresponsible attackers such as damaging the system, committing data theft and falsifying data that can harm the owner. With this, network security requires a system that can detect and prevent attacks such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). Based on these problems, in this study security is carried out with the Snort3 application as NIPS to secure the PC Server. In this case, the IPS on the PC Router is also equipped with a Demilitarized Zone (DMZ) which is used as a data packet communication line. The design was carried out to be tested using brute force, Man-in-The-Middle (MiTM) and Distributed Denial of Service (DDoS) attacks. The tests carried out are in the form of detecting and preventing attacks that have been registered in the rules as well as attacks that are not registered or can be referred to as anomalies. In addition, it compares the use of resources during attacks without security and after security. The results of this study are that the Snort3 application can prevent attacks with an accuracy of 100%, and can detect and prevent anomalous attacks using checksum monitoring of malicious packet filters.

Keyword**:** *Network-based Intrusion Prevention System* (NIPS), Snort3, *Demilitarized Zone* (DMZ), *brute force*, *Man-in-The-Middle* (MiTM), *Distributed Denial of Service* (DDoS).