ABSTRACT

The server is the center of service providers and data processing in a network, requests sent by clients will be processed by the server. Security is needed so that the server is in good condition and can protect information on the network and minimize the occurrence of anomalous activities such as DoS attacks. Based on these problems, a research on network security was conducted using the Snort application as a Host-based Intrusion Prevention System (HIPS) with anomaly-based detection techniques to protect the services provided by the server from attackers. From the research that has been done HIPS can detect and block 72550 of 72600 ICMP Flood attacks, 98418 of 98718 UDP Flood attacks, 25950 of 26950 SYN Flood attacks, 141 151 FTP Bruteforce attacks. In addition, an analysis of the Quality of Service value was carried out before and during the attack. The CPU value has increased because the CPU has to work to answer incoming requests, the throughput value has increased due to the amount of data received is more than the time required. The delay and jitter have decreased because the total delay and jitter have a small value compared to the number of packets received, besides the packet loss value in all experiments is zero percent or can be said to be perfect, this is because the packets that go to the server have been filtered by IPS.

Keywords: *Host-based Intrusion Prevention System* (HIPS), DoS, Snort, *Quality of Service*