ABSTRACT

COMPARISON ANALYSIS OF THE PERFORMANCE OF OSSEC AND SNORT *INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) USING QUALITY OF SERVICE (*QOS*)*

By
Arifah Ramadhan
20102270

A public network will be easily accessed by everyone from various countries, this is what makes this network vulnerable to attack. Even though every network already uses a firewall, it can be easily attacked by attackers. In solving this problem, a system that is stronger than a firewall is needed, namely the Intrusion Detection and Prevention System or better known as IDPS. Securing the system can be done by integrating OSSEC and Snort *where this system will provide logs to record activities carried out by attackers. OSSEC will act like a firewall that can allow and block. While* Snort *will analyze all network traffic to intercept and look for several types of intrusions in a network. In this research, a Distributed Denial of Service (DDoS) attack is tested on a network server that has been installed with OSSEC and* Snort*. After testing the attack, network quality measurements will be made using Quality of Service (*QoS*) to determine the state of the network before the attack and after the attack. In the performance comparison between* Snort *and OSSEC in detecting attacks, for ICMP Flood attacks,* Snort *is superior in terms of throughput and Packet loss, while OSSEC is better in delay and jitter. In detecting TCP Flood attacks,* Snort *showed superior performance in throughput, delay, and Packet loss, while OSSEC excelled in jitter. For UDP Flood attacks,* Snort *is better in throughput and delay, while OSSEC has better performance in jitter and Packet loss.*

Keywords*: *Intrusion Detection and Prevention System, OSSEC,* Snort*, Quality of Service