ABSTRACT

Network security issues are increasingly a concern due to the rapid development of information technology. This makes someone illegally enter the system and paralyze the system. In addition, there are loopholes and no security system that protects the system making the system vulnerable to attack.

Therefore, in this final project a security system is made by using Suricata as a Network Intrusion Detection System (NIDS) and Ntopng as a tool to monitor the network up to layer 7. With a focus on Denial of Services (DoS) attacks, it will be seen a comparison between the two applications in dealing with DoS attacks.

In this research, based on the rules of Suricata that the author made, the author managed to detect all attacks that were tested. While the default rule on Ntopng, the author is only able to identify the type of DoS attack in the form of SYN flood. For DoS attacks with the purpose of a website server, the accuracy of the Suricata rule created by the author is superior to the default rule on Ntopng for LOIC applications at 52.70%, while for Hping3 applications at 48.80%, and GoldenEye applications at 52.84% . Whereas for DoS attacks with the aim of FTP server, the accuracy of the Suricata rule that I made was also superior to the default rule on Ntopng for LOIC applications by 52.30%, while for Hping3 applications it was 59.97%. So there is a big difference between the percentage of accuracy, precision rate, and recall rate of Suricata and Ntopng, where Suricata is superior in the accuracy of its rules in detecting DoS attacks.

Keywords : *suricata, ntopng, rule, DoS.*