

ABSTRACT

Network security is the main thing needed to secure data. Because of the evolution of information technology, attacks methods are various. To prevent the risk of attacked, a first step is needed with a system to secure the network so that the data held by the target is not misused by the attacker. One system that can be used to prevent the risk of attacked is Intrusion Detection System (IDS) which can detect suspicious activity in a network.

Anomaly-Based detection method is chosen to be able to detect suspicious and abnormal activities for the system that cannot be done by Signed-based methods. In this study, attack testing using three DoS tools, namely LOIC, Torshammer and Xerxes tools with the testing scenario of using IDS and without IDS.

From the results of testing that has been done, IDS has successfully detected the attack, for sending the most consecutive attack packages, namely Torshammer, Xerxes and LOIC. In the detection of tools, Torshammer's attack on the FTP Server target was 9525 packages, for Xerxes tools, there were 10777 packages and LOIC tools as many as 6166 packages. While attacks on the target Web Server for torshammer tools as many as 320 packages, for Xerxes tools as many as 473 packages and for LOIC tools as many as 60 packages. The accuracy of the IDS performance results is 88.66%, precision is 88.58% and the false positive rate is 63.17%.

Keywords: Network Security, Intrusion Detection System, Anomaly-Based, Denial of Service