ABSTRACT

There are many organizations and individuals who do not understand network security so that they get potential attacks and experience system damage. To prevent potential attacks, an Intrusion Detection System (IDS) was developed. Some of the non-machine learning methods used are not yet accurate, so they require methods with more accurate machine learning to detect attacks. To overcome the problem, the study conducted a comparison using the K-Nearest Neighbor and Naïve Bayes methods to optimally detect computer network attacks. In this study, the implementation used the K-Nearest Neighbor and Naïve Bayes methods in detecting HTTPDoS attacks using the ISCX testbed dataset of June 14, 2012 consisting of 157,867 packages and as many as 19 features. This study analyzes the comparison of methods that will result from the classification process with the confusion matrix and the ROC curve. In the final results of the study obtained, the KNN method produced an accuracy percentage of 99.994% and had an excellent data classification quality compared to the naïve Bayes accuracy percentage of 39.885%.

Keywords*— KNN, IDS, *Naïve Bayes, Classification, Attacks