Abstract

Detection of threats on the network system is very important for attacks on the network can be detected and carried out protection of information quickly and precisely. The application to detect intrusions has been popular now is IDS. However, IDS systems that are generally available today are signatures based that are unable to detect unknown theft. To solve problem, in this journal will discuss about the best algorithm of some selected algorithms so as to solve the problem of false positive and accuracy. The algorithms used are Decision Tree, K-Nearest Neighbor and Naïve Bayes. Based on the tests conducted naïve bayes is the best algorithm with 95% accuracy and false positive 0.5815133%, K-Nearest Neighbor with an accuracy of 81.192% and false positive 0.681%, Decision Tree with an accuracy of 74.388% and false positive 22.658%.

Keyword : Snort, IDS, Intrusion Detection System, Naïve Bayes, KNN, Decision Tree, NSL KDD, False Postive, Accuracy.