ABSTRAK

Banyaknya organisasi maupun individu yang belum paham terhadap keamanan jaringan sehingga mendapatkan potensi serangan dan mengalami kerusakan sistem. Untuk melakukan pecegahan potensi serangan dikembangkan yaitu *Intrusion Detection System* (IDS). Dari beberapa metode *non-machine learning* yang digunakan belum akurat, sehingga memerlukan metode dengan *machine learning* yang lebih akurat untuk mendeteksi serangan. Untuk mengatasi permasalahan, dalam penelitian melakukan perbandingan menggunakan metode *K-Nearest Neighbor* dan *Naïve Bayes* untuk mendeteksi serangan jaringan komputer dengan optimal. Dalam penelitian ini, implementasi menggunakan metode *K-Nearest Neighbor* dan *Naïve Bayes* dalam mendeteksi serangan HTTPDoS dengan menggunakan dataset ISCX testbed 14 Juni 2012 yang terdiri dari 157.867 paket dan sebanyak 19 fitur. Penelitian ini menganalisis perbandingan metode yang akan dihasilkan dari proses klasifikasi dengan confusion matrix dan kurva ROC. Pada hasil akhir penelitian yang diperoleh adalah metode KNN menghasilkan persentase akurasi sebesar 99,994% dan memiliki kualitas klasifikasi data yang sangat baik dibandingkan persentase akurasi *Naïve Bayes* 39,885%.

Kata kunci— KNN, IDS, Naïve Bayes, Klasifikasi, Serangan