

Abstrak

Deteksi ancaman pada sistem jaringan sangat penting agar serangan pada jaringan dapat dideteksi dan dilakukan perlindungan informasi secara cepat dan tepat. Aplikasi untuk mendeteksi intrusi yang populer sekarang adalah IDS. Namun, sistem IDS yang tersedia secara komersial saat ini adalah signaturebased yang tidak mampu mendeteksi serangan yang tidak diketahui. Untuk memecahkan masalah tersebut, tugas akhir ini akan membahas mengenai algoritma terbaik dari beberapa algoritma yang telah dipilih sehingga dapat menyelesaikan permasalahan false positive dan akurasi. Algoritma yang digunakan yaitu Decision Tree, K-Nearest Neighbour dan Naïve Bayes. Berdasarkan pengujian yang dilakukan naïve bayes merupakan algoritma terbaik dengan akurasi 95% dan false positive 0.5815133%, K-Nearest Neighbour dengan akurasi 81.192% dan false positive 0.681%, Decision Tree dengan akurasi 74.388% dan false positive 22.658%.

Kata Kunci : Snort, IDS, Intrusi Deteksi Sistem, Naïve Bayes, KNN, Decision Tree, NSL KDD, False Positive, Akurasi.