**Abstrak**

*Denial of Service* (DoS) adalah serangan dimana penyerang menghabiskan sumber daya jaringan komputer. Dampak dari serangan DoS menyebabkan komputer tidak dapat berfungsi dengan normal. *Intrusion Detection System* (IDS) berperan sebagai pendeteksi berbagai jenis serangan pada jaringan komputer termasuk DoS. IDS mengidentifikasi serangan berdasarkan klasifikasi data jaringan. Metode *Intrusion Detection System* (IDS) *non-machine learning* saat ini tidak terlalu akurat, sehingga diperlukan metode IDS dengan *machine learning* yang lebih akurat dalam mendeteksi serangan. Untuk mengatasi permasalahan ini, penelitian ini membandingkan metode *Naïve Bayes* dan *Probabilistic Neural Network* (PNN) untuk mendeteksi serangan DoS secara optimal. Pada penelitian ini, implementasi menggunakan metode *Naïve Bayes* dan PNN dalam mendeteksi serangan DoS menggunakan NSL-KDD dataset dengan 13 fitur dari 41 fitur. Hasil dari penelitian ini yaitu *Naïve Bayes* memiliki akurasi lebih tinggi dengan nilai akurasi 100% daripada PNN yang hanya mempunyai nilai akurasi sebesar 91,93% dalam mendeteksi serangan DoS.

**Kata kunci : Keamanan Jaringan Komputer, *Naïve Bayes*, *Probabilistic Neural Network* (PNN), *Denial of Service*.**