1. Pendahuluan

1.1.Latar Belakang

Perkembangan teknologi pada perangkat lunak, perangkat keras dan jaringan saat ini yang begitu pesat membuat teknologi pada jaringan komputer juga ikut serta dalam perkembangan tersebut. Hal ini ditunjukkan dengan semakin banyaknya penggunaan teknologi sebagai sarana transaksi dan pengaksesan data secara online. Seiring dengan perkembangan tersebut, banyak bermunculan penyalahgunaan teknologi yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab atas perbuatannya yang merusak atau mengakses data secara illegal dengan memanfaatkan celah yang ada.

Untuk mengetahui data tersebut merupakan ancaman atau tidak, dapat dilakukan dengan pendeteksian intrusi pada jaringan. Intrusion Detection System (IDS) merupakan suatu sistem yang dapat mendeteksi adanya serangan atau gangguan yang terjadi pada suatu jaringan berdasarkan network-based atau host-based. Dalam tugas akhir ini, penulis menggunakan Intrusion Detection System dan algortima klasifikasi.

IDS menggunakan dua teknik untuk mendeteksi suatu intrusi yang terjadi pada jaringan, yaitu teknik Signature-based dan Anomaly-based. Teknik signature-based adalah teknik yang mencocokan lalu lintas jaringan dengan basis data yang berisi signature serangan dan penyusupan yang telah didenisikan. Teknik anomaly-based adalah Teknik yang memperhatikan pola lalu lintas pada jaringan yang normal (Sagita, 2011). Penggunaan IDS dengan deteksi anomaly-based menggunakan teknik membandingkan pola normal pada jaringan. Teknik anomali sangat rentan terhadap tingginya false-postive alarm yang terdeteksi dan akan mempengaruhi akurasi pendeteksian menurun (Singh and Gupta, 2012).

IDS telah banyak diimplementasikan menggunakan algoritma machine learning AI pada Snort dengan akurasi yang didapatkan masih terbilang rendah. Pada penilitian yang dilakukan (George, Poornachandran and Kaimal, 2011) adalah dengan cara mengimplementasikan algoritma SVM sebagai klasikasi pada pre-processor snort dan mendapatkan akurasi yang rendah dan false-alarm rate yang terbilang masih cukup tinggi. Algoritma Bayesian sebagai metode klasikasi ditawarkan oleh (Singh and Gupta, 2012). Penggunaan algoritma ADS yang merupakan extension dari Snort sebagai preprocessor untuk mendeteksi anomali data yang dilakukan oleh (Saganowski, Goncerzewicz and Andrysiak, 2013) mendapatkan deteksi rate yang tinggi namun false-positive alarm yang juga tinggi. Naïve Bayes telah banyak diimplementasikan pada snort untuk mendeteksi serangan mendapatkan deteksi akurasi yang terbilang cukup tinggi tetapi mendapatkan false-alarm rate yang juga tinggi. Dimana dalam graf yang ditampilkan pada penelitian sebelumnya membuktikan algoritma graft j48 tidak mendeteksi adanya false-alarm yang terjadi tetapi dalam detection rate masih rendah dari algoritma naive bayes (Hussein, Ali and Kasiran, 2012).

Untuk mengatasi masalah tersebut dalam tugas akhir ini akan diusulkan untuk melakukan studi pemilihan algoritma terbaik pada IDS untuk mengatasi masalah tingginya false-positive yang terjadi pada IDS sehingga mendapatkan nilai akurasi yang tinggi seperti yang diharapkan.

1.2.Topik dan Batasannya

Berdasarkan latar belakang yang telah diuraikan, dapat dirumuskan permasalahan pada studi ini adalah cara membangun sebuah intrusi deteksi sistem menggunakan algortima classifier untuk mengurangi false positive dan meningkatkan hasil akurasi menggunakan serangan yang terdapat pada NSL KDD.

Adapun batasan masalah pada studi ini adalah studi dilakukan pada linux jenis ubuntu 14.04, penggunaan bahasa pemograman python sebagai implementasi algoritma dan NSL KDD sebagai data serangan yang akan dilakukan intrusi.

1.3.Tujuan

Tujuan dari studi ini adalah untuk melakukan pembelajaran tentang algoritma terbaik yang akan melakukan deteksi pada sebuah data serangan untuk mengurangi false positive dan meningkatkan nilai akurasi pada intrusi deteksi serangan.

1.4. Organisasi Penulisan

Penulisan tugas akhir ini disusun dalam beberapa bagian yang setiap bagian, berisi data-data berikut : Bagian 1 - Pendahuluan, Bagian 2 - Studi Terkait, Bagian 3 - Sistem yang dibangun, Bagian 4 - Evaluasi, dan Bagian 5 – Kesimpulan.