1. Pendahuluan

Latar Belakang

Intrusion Detection System (IDS) merupakan salah satu komponen yang tugasnya memantau arus lalu lintas jaringan pada suatu jaringan [1]. Dengan banyaknya jenis serangan siber, IDS akan kesulitan untuk mendeteksinya. Jadi, ada IDS yang dibuat menggunakan teknik deteksi anomali. Deteksi Anomali adalah metode yang menggunakan teknik pembelajaran mesin yang dapat mendeteksi jika sebuah paket dalam jaringan memiliki perilaku mencurigakan yang hampir mirip dengan serangan siber [2]. Deteksi Anomali adalah cabang dari tipe IDS yang menggunakan algoritma pembelajaran mesin untuk mendeteksi pola serangan dari aktivitas jaringan.

Pada jaringan skala besar, penerapan IDS pada jaringan dengan banyak aset akan sangat mempengaruhi keamanan jaringan karena akan banyak log yang dihasilkan dari setiap aset, yang di sisi lain proses monitoring akan sulit untuk dikelola [3]. Oleh karena itu, IDS harus digabungkan dengan SIEM untuk memudahkan pemantauan jaringan. System Information & Event Management (SIEM) merupakan sistem yang dapat mengelola log yang dihasilkan oleh beberapa sumber data, salah satunya adalah IDS [4]. SIEM juga dapat digunakan sebagai pemantauan analisis langsung untuk memantau dan menganalisis lalu lintas aliran jaringan secara real-time untuk bertindak cepat jika terdeteksi anomali pada paket tertentu.

Batasan Masalah

Dalam jurnal ini hanya membatasi masalah yaitu sistem akan diuji coba menggunakan skenario DoS pada jaringan lokal selama 1 jam untuk melihat performansi dari sistem yang dibuat dan melihat penggunaan CPU dan RAM oleh sistem tersebut, tetapi dalam tes performansi, hanya akan ada 4 komponen yang di uji yaitu ELK Stack (Elasticsearch, Logstash, Kibana), dan Zeek (IDS).

Tujuan

Tujuan dari penulisan jurnal dan pembuatan sistem pada jurnal ini yaitu untuk mengintegrasikan IDS berbasis machine learning menggunakan SIEM untuk dilakukan *live analysis* dan ingin mengetahui bagaimana performansi SIEM jika diintegrasikan dengan IDS berbasis *machine learning* dari segi *Overhead Analysis*

Organisasi Tulisan

Pada penulisan jurnal ini ada lima bagian, yaitu: pendahuluan, studi terkait, sistem yang dibangun, evaluasi, dan kesimpulan. Pada bagian pendahuluan akan dijelaskan terlebih dahulu permasalahan yang sedang dihadapi beserta batasan masalah dan tujuan. Bagian studi terkait akan menjelaskan beberapa studi dari jurnal- jurnal internaisonal yang akan digunakan pada jurnal ini untuk memilih beberapa sistem sesuai studi yang telah dilakukan yang memiliki kapabilitas untuk diwujudkannya sistem yang ingin dibangun pada jurnal ini. Pada bagian evaluasi akan melakukan skenario pengujian dan juga akan mengevaluasi hasil dari pengujian tersebut. Pada bagian yang terakhir yaitu kesimpulan, akan dijelaskan kesimpulan yang dapat diambil dari hasil pengujian di bagian evaluasi dan merangkum nya pada bagian kesimpulan, dan juga terdapat pengembangan selanjutnya di akhir bagian kesimpulan.