BAB I

PENDAHULUAN

1.1. Latar Belakang

Saat ini layanan informasi yang banyak diakses oleh pengguna internet di seluruh dunia adalah melalui sebuah *website*. Sebagai salah satu layanan informasi, *web server* akan menerima banyak permintaan yang dikirim dari *browser* pengguna kemudian akan memberikan respon atau tanggapan dengan menampilkan sebuah halaman *website*. *Web Server* seringkali menjadi target utama dalam berbagai penyerangan yang berakibat ringan sampai yang dapat berakibat fatal. Hal tersebut terjadi karena kurangnya penerapan yang optimal dari aspek keamanan pada jaringan *server*, sehingga terjadinya resiko yang cukup signifikan (Lukman & Suci, 2020). Berdasarkan daftar serangan *Denial of Service* terbaru menurut (Blair Felter, 2020) yang terjadi pada bulan Februari 2018 pada *GitHub*, terjadi serangan yang membanjiri *server* dengan mengirimkan ukuran paket data sebesar 1,3 *Tbps* dan sebanyak 126,9 juta paket data yang membuat sistem pada github menjadi *down*.

Salahsatu serangan yang umum terjadi menurut (Infocyte, 2021) pada posisi keempat adalah *Denial of Service.* Serangan *Denial of Service* merupakan serangan yang bertujuan untuk menghambat atau memutus ketersediaan informasi (Hermawan, 2013). *Syn Flood* merupakan salah satu jenis serangan yang umum dari DOS (Infocyte, 2021), yang bekerja dengan cara membanjiri server dengan permintaan SYN sehingga server akan mengembalikan paket SYN-ACK secara terus menerus (Suartana, 2020).

Dalam upaya mencegah pengguna layanan yang tidak sah, maka *Intrusion Detection System* merupakan pilihan terbaik dalam mengidentifikasi atau pemantau jika terjadinya aktifitas-aktifitas yang mencurigakan dalam sebuah infrastruktur jaringan dan akan mengirimkan sebuah peringatan jika hal tersebut terjadi kepada *administrator system* (Suartana, 2020). Terdapat berbagai aplikasi IDS yang dapat digunakan diantaranya *snort* dan *suricata* yang merupakan salahsatu dari sepuluh aplikasi terbaik menurut (Vijay et al., 2021).

Beberapa percobaan untuk membandingkan kinerja aplikasi IDS sudah dilakukan pada penelitian sebelumnya, diantaranya : Analisis Perbandingan *Quality of Service* (QoS) Penerapan *Snort* IDS dan *Bro* IDS Dalam Arsitektur *Software Define Network* (SDN) (Sukarno & Nugroho, 2018), *Performance Comparison of Intrusion Detection Systems and Application of Machine Learning to Snort System* (Shah & Issac, 2018), dan Analisis Perbandingan Kinerja *Snort* Dan *Suricata* Sebagai *Intrusion Detection System* Dalam Mendeteksi Serangan *Syn Flood* Pada *Web Server Apache* (Lukman & Suci, 2020).

Penelitian yang akan dilakukan berdasarkan potensi keterbaruan yang didapatkan pada penelitian sebelumnya yang mencoba untuk membandingkan kinerja dari aplikasi IDS. Berdasarkan potensi tersebut menghasilkan keterbaruan : penambahan jenis serangan dari *denial of service* yaitu *XMAS flood* dan *slowloris* untuk perbandingan kinerja deteksi aplikasi *snort* dan *suricata* terhadap beberapa serangan yang berbeda. Penambahan serangan tersebut disertai dengan penambahan parameter pengujian *load average* yang digunakan untuk mengukur

beban sistem yang menjalankan aplikasi *snort* dan *suricata* ketika mendeteksi sebuah serangan.

Snort dan *suricata* ini menarik di teliti dikarenakan sifatnya *opensource* dan merupakan peringkat empat dan lima dari sepuluh aplikasi IDS yang paling baik (Vijay et al., 2021). Pada penelitian ini akan dilakukan perbandingan kinerja aplikasi IDS dengan parameter: deteksi, penggunaan CPU, penggunaan memori, dan *load average* dari masing-masing aplikasi. Serangan DoS dipilih untuk dijalankan pada percobaan terhadap IDS. Setiap hasil percobaan dicatat dalam tabel serta disajikan dalam bentuk grafik.

1.2. Rumusan Masalah

Berdasarkan latar belakang penelitian, masalah yang akan di selesaikan adalah sebagai berikut :

1. Bagaimana pengaruh serangan *Syn Flooding* terhadap performa deteksi dari aplikasi *snort* dan *suricata* ?
2. Bagaimana pengaruh serangan *XMAS Flood* terhadap performa deteksi dari aplikasi *snort* dan *suricata* ?
3. Bagaimana pengaruh serangan *Slowloris* terhadap performa deteksi dari aplikasi *snort* dan *suricata* ?
4. Bagaimana rata-rata beban atau *load average* pada setiap sistem yang menjalankan aplikasi *snort* dan *suricata* ketika terjadinya serangan *denial of service* ?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini berdasarkan latar belakang penelitian adalah sebagai berikut :.

1. Mengukur kinerja deteksi, penggunaan memori, dan penggunaan CPU setiap aplikasi dengan menggunakan serangan TCP *Syn Flooding.*
2. Mengukur kinerja deteksi, penggunaan memori, dan penggunaan CPU setiap aplikasi dengan menggunakan serangan TCP *XMAS Flood.*
3. Mengukur kinerja deteksi, penggunaan memori, dan penggunaan CPU setiap aplikasi dengan menggunakan serangan *Slowloris.*
4. Mengukur rata-rata beban atau *load average* sistem ketika menerima serangan *denial of service* dengan menjalankan aplikasi *snort* dan *suricata*.

1.4. Manfaat Penelitian

Manfaat dari penelitian ini dapat dilihat sebagai berikut :

1. Dapat mengimplementasikan IDS kedalam sebuah jaringan *web server* guna untuk meningkatkan keamanan.
2. Dapat mengetahui hasil dari proses pengujian kinerja aplikasi *Intrusion Detection System*.
3. Dapat mengetahui perbandingan kinerja aplikasi *snort* dan *suricata* dalam mengidentifikasi jenis serangan dari *Denial of Service*.

1.5. Ruang Lingkup Penelitian

Penelitian ini difokuskan kepada perbandingan kinerja aplikasi *Intrusion Detecting System Snort* dan *Suricata* dalam mengidentifikasi jenis serangan DoS.

1.6. Struktur Penulisan Penelitian

Penulisan pada penelitian ini terbagi menjadi lima BAB, masing-masing BAB diuraikan sebagai berikut :

BAB I PENDAHULUAN

Bab ini membahas latar belakang, permasalahan pada penelitian, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian, serta struktur penulisan yang akan dilakukan untuk penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini menguraikan teori-teori yang berhubungan dengan *Intrusion Detecting System*, dan *Denial of Service* sebagai fokus utama penelitian serta *state of the art* dari penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan alur penelitian, dan juga apa saja yang akan dilakukan pada penelitian yang akan dilakukan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini memuat analisis dari perancangan atau alur pada bab sebelumnya, yaitu perancangan yang sesuai metodologi dan implementasi IDS untuk mendapatkan hasil yang akan di analisis.

BAB V KESIMPULAN DAN SARAN

Bab ini memuat kesimpulan dari hasil analisis penelitian, serta garis besar apa saja yang telah dilakukan ketika penelitian. Dan juga saran berisi tentang rekomendasi sesuai dengan batasan yang terdapat dalam penelitian.