BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Seiring dengan perkembangan teknologi pada era sekarang internet merupakan hal yang sangat dibutuhkan oleh semua aspek kehidupan manusia, karena dengan internet kita bisa mudah berkomunikasi jarak jauh melalui jaringan dan internet juga dapat digunakan sebagai media untuk menyimpan data-data yang penting [1].

Pengguna internet baik di dunia maupun di Indonesia setiap tahunnya semakin meningkat, tentunya ada sisi positif dari jaringan internet yang tinggi, namun dari sisi negatif tentunya internet atau teknologi informasi ini menjadi *tools* baru yang digunakan oleh pelaku kejahatan untuk merugikan orang lain [2]. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), sepanjang bulan Januari hingga Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibanding periode yang sama tahun lalu yang tercatat di kisaran 39 juta [3]. Hal ini tentunya menjadi ancaman bagi pengguna internet di Indonesia.

Saat ini informasi merupakan sebuah aset yang sangat penting. Kemampuan komunikasi data dalam mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah instansi atau perusahaan. Disisi lain, dengan adanya kemudahan tersebut ternyata menyimpan permasalahan keamanan yang sangat krusial, yang meliputi *Confidentality, Aunthenticity, Integrity, Availability* [4]. Sehingga sistem keamanan jaringan komputer saat ini menjadi sangat penting dalam menjaga kerahasiaan dan integritas data untuk menjaga dari penyusup yang berusaha mengubah atau bahkan merusak data yang dimiliki oleh suatu jaringan.

Semakin canggih dan beragam serangan dalam suatu server yang dilakukan oleh *hacker*, tentunya bertujuan untuk menghalangi sebuah perusahaan ataupun seseorang dalam memberikan layanan terbaik dan optimal. Hal ini dapat terjadi, apabila jaringan *local* telah terhubung dengan internet sehingga dikatakan kurang aman dan menjadi ancaman keamanan suatu jaringan. Adapun serangan yang

paling sering terjadi seperti *port scanning*, *sniffing*, DoS (*Denial of Service*), DDoS (*Distributed Denial Of Service*), *malware*, UDP *flooding*, SYN *flooding* dll.

Oleh karena itu, diperlukan suatu sistem keamanan jaringan yang aman dari serangan *hacker*. Dalam keamanan jaringan, terdapat beberapa metode serta *tools* yang dapat digunakan. Metode yang sering digunakan yaitu IDS yang dapat mendeteksi suatu serangan sedangkan IPS yang melakukan pemblokiran serangan. Sehingga, untuk mengatasi serangan pada sebuah jaringan diperlukan sistem yang dapat mendeteksi serta memblokir serangan yang ingin dikirim kepada web server. Hal tersebut dapat dilakukan dengan menggunakan metode yaitu *Intrusion Detection and Prevention System* (IDPS). Penerapan *Intrusion Detection and Prevention System* (IDPS) digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu administrator dalam memantau dan menganalisa paket-paket berbahaya yang terdapat dalam sebuah jaringan [5]. Dalam penerapan metode IDPS ini, dapat digunakan *tools open source* salah satunya yaitu Snort, dimana *tools* ini digunakan untuk menjalankan fungsi *Intrusion Detection and Prevention System* (IDPS) untuk memonitoring paket-paket data yang masuk ke dalam suatu jaringan. Jadi, setiap aktifitas lalu lintas paket yang terjadi dalam sebuah jaringan akan dipantau serta dicocokan dengan *rules* snort yang terus diupdate untuk mencegah adanya celah keamanan yang dapat dilakukan oleh penyusup.

Berdasarkan latar belakang di atas, maka penulis melakukan penelitian berfokus pada dua serangan DDoS yaitu UDP *flooding* dan SYN *flooding* dengan judul **"ANALISIS KINERJA SISTEM KEAMANAN JARINGAN DENGAN METODE *INTRUSION DETECTION AND PREVENTION SYSTEM* (IDPS) MENGGUNAKAN SNORT TERHADAP SERANGAN UDP FLOODING & SYN FLOODING".**

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1) Bagaimana perancangan konfigurasi dalam penerapan sistem keamanan jaringan menggunakan *Intrusion Detection and Prevention System* (IDPS) dengan Snort?

2) Bagaimana kinerja *tools* Snort sebagai IDPS terhadap serangan UDP *flooding* dan SYN *flooding*?
3) Bagaimana kinerja IDPS dengan Snort berdasarkan parameter *Quality of Service* (QoS)?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1) Sistem keamanan jaringan dengan menggunakan jaringan *Local Area Network* (LAN).
2) Penerapan *Intrusion Detection and Prevention System* (IDPS) untuk mendeteksi serta memblokir serangan UDP *flooding* dan SYN *flooding*
3) Penggunaan *tools* Snort dalam penerapan metode *Intrusion Detection and Prevention System* (IDPS)
4) Tool yang digunakan untuk serangan UDP flooding yaitu LOIC.
5) Tool yang digunakan untuk serangan SYN flooding adalah Hping3
6) Menggunakan Linux Ubuntu 18.04
7) Parameter *Quality of Service* yang diamati yaitu *throughput*, *delay*, dan *Jitter* untuk mengetahui kinerja Intrusion Detection and Prevention System (IDPS)

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1) Untuk mengetahui penerapan sistem keamanan jaringan menggunakan *Intrusion Detection and Prevention System* (IDPS) dengan Snort.
2) Untuk mengetahui kinerja tools Snort sebagai IDPS terhadap serangan UDP flooding dan SYN flooding.
3) Untuk mengetahui kinerja IDPS dengan Snort berdasarkan parameter *Quality of Service* (QoS).

1.5 MANFAAT

Penelitian ini diharapkan dapat memperoleh manfaat, yaitu:

1) Mampu merancang konfigurasi sistem keamanan jaringan menggunakan metode *Intrusion Detection and Prevention System* (IDPS) dengan Snort
2) Mampu meningkatkan keamanan jaringan dalam web server karena serangan yang masuk akan dapat dideteksi dan diblokir oleh Snort dalam menjalankan fungsi IDPS.
3) Mampu menganalisis hasil kinerja *Intrusion Detection and Prevention System* (IDPS) dengan Snort yang akurat sesuai dengan parameter *Quality of Service* (QoS).

1.6 SISTEMATIKA PENULISAN

Penelitian ini terbagi menjadi beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, manfaat dan tujuan penelitian, batasan masalah dan sistematika penulisan. Bab 2 membahas tentang studi pustaka, penjelasan jaringan komputer, keamanan jaringan, *firewall*, pengertian dan penjelasan mengenai sistem IDPS, *tools* Snort, serangan jaringan, serta serangan UDP *flooding* dan SYN *flooding*. Pada bab 3 membahas mengenai rancangan alur penelitian, konfigurasi jaringan serta pengujian. Bab 4 membahas mengenai analisa dan pembahasan berdasarkan penelitian yang dilakukan. Bab 5 membahas mengenai kesimpulan dan saran untuk penelitian yang akan dilaksanakan selanjutnya.