BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Seiring dengan perkembangan teknologi di era internet saat ini merupakan sesuatu yang sangat dibutuhkan dalam segala aspek kehidupan manusia karena dengan bantuan internet kita dapat dengan mudah berkomunikasi melalui jaringan jarak jauh dan internet juga dapat digunakan untuk menyimpan informasi penting [1]. Jumlah pengguna internet terus bertambah dari tahun ke tahun, tentunya internet yang tinggi juga memiliki sisi positif, namun sisi negatifnya tentunya internet atau teknologi informasi merupakan alat baru yang digunakan para penjahat untuk merugikan orang lain.

Keamanan jaringan komputer penting karena mengontrol akses ke jaringan dan mencegah serangan atau penyalahgunaan di Internet. Tidak dapat dipungkiri bahwa banyak virus dan serangan terjadi di internet itu sendiri, sehingga banyak pengguna, perusahaan, dan pemerintah yang menjadi korban serangan dan menderita kerugian. [2].

Saat ini ada banyak cara untuk menyerang jaringan komputer. Sebenarnya melakukan penyerangan atau penyusupan tidak membutuhkan keahlian atau pemahaman konsep IT yang mendalam, karena sudah banyak aplikasi dan metode pendukung yang memungkinkan untuk dengan mudah melakukan penyerangan atau penyusupan jaringan. Serangan umum termasuk penolakan layanan (DOS), mengendus, pemindaian *port*, pengintaian, injeksi SQL, malware, dll.

Oleh karena itu, diperlukan solusi untuk menjaga perlindungan jaringan terhadap serangan atau penyusup. Sistem Anti-intrusi "IPS" adalah solusi untuk mendeteksi dan mencegah aktivitas mencurigakan di Internet. IPS menawarkan berbagai alat *open source* seperti Snort, Suricata dan Zeek. [3].

Snort diakui sebagai alat dan standar terbaik untuk alat IPS *open source*, telah diunduh empat juta kali dan diharapkan menjadi alat IPS *open source* yang paling banyak digunakan pada tahun 2015. [4] Suricata merupakan *tools open source* yang memiliki performa yang lebih unggul karena suricata

mendukung *multithread*, selain itu suricata juga kompatibel dengan *rule* Snort sehingga dapat menggunakan *rule* Snort yang tersedia untuk digunakan pada suricata. Dan Zeek merupakan *tools open source* yang memiliki kemampuan dalam menganalisis aktifitas jaringan secara terperinci karena bekerja pada *application layer* dan dapat digunakan dalam skala yang besar.

Metode yang digunakan dalam penelitian ini adalah QOS (*Quality of Service*), yaitu membandingkan dari segi pengukuran QOS, yaitu *throughput*, *delay*, *jitter* dan *packet loss*. Berdasarkan penelitian hingga saat ini dan pernyataan yang dijelaskan di atas, peneliti bermaksud untuk melakukan pembandingan kompetitif kinerja tiga *tools* Snort, Suricata dan Zeek.

Benchmarking dalam penelitian ini melibatkan beberapa hal, yang pertama adalah menguji dan menganalisis tingkat akurasi ketiga *tools* tersebut saat dikonfigurasi dengan sistem perlindungan intrusi IPS. setelah upaya serangan telah terdeteksi. Lainnya adalah pengetahuan tentang pengujian QOS (*Quality Of Service*).

1.2 RUMUSAN MASALAH

Berdasarkan pada latar belakang masalah diatas, maka rumusan dalam penelitian ini adalah:

1. Implementasi dari Snort, Suricata dan Zeek saat diimplementasikan pada konfigurasi IPS.
2. Bagaimana perbandingan performansi dari keempat aplikasi *Intrusion Prevention System* (IPS) yaitu Snort, Suricata dan Zeek dengan menggunakan QOS.

1.3 PERTANYAAN PENELITIAN

Berdasarkan uraian di atas, penulis merumuskan beberapa pertanyaan penelitian yang akan dibahas dalam penelitian ini, antara lain:

1. Bagaimana mengimplementasikan *tools* Snort, Suricata dan Zeek pada konfigurasi *Intrusion Prevention System* (IPS)?
2. Bagaimana perbandingan performansi dari 4 aplikasi *Intrusion Prevention System* (IPS) yaitu Snort, Suricata dan Zeek dengan menggunakan QOS?

1.4 BATASAN MASALAH

Berdasarkan rumusan masalah dan tujuan penelitian untuk melakukan penelitian sebagai permasalahan yang ada, maka beberapa ruang lingkup masalah penelitian ini adalah sebagai berikut:

1. Menggunakan Linux Ubuntu versi 22.04 sebagai system operasi
2. Penerapan *sistem Intrusion Prevention System* (IPS).
3. Komparasi Snort, Suricata dan Zeek hanya berfokus dalam mendeteksi dan mencegah serangan ICMP *Flood* dan SYN *Flood*.
4. *Tool* yang digunakan untuk serangan ICMP *Flood* adalah Hping3.
5. *Tool* yang digunakan untuk serangan SYN *Flood* adalah Hping3.
6. Berfokus terhadap perbandingan Performansi dari segi kinerja dari keempat *tools* Snort, Suricata dan Zeek saat dilakukan pengujian serangan ICMP *Flood* dan SYN *Flood*
7. Parameter performansi yang digunakan pada penelitian ini menggunakan parameter *Quality of Service* (QOS).

1.5 TUJUAN PENELITIAN

Berdasarkan rumusan permasalahan yang ada, dapat diketahui bahwa tujuan dari penelitian ini adalah:

1. Menerapkan konfigurasi IPS pada Snort, Suricata dan Zeek.
2. Mengetahui perbandingan performansi dari 4 aplikasi *Intrusion Prevention System* (IPS) yaitu Snort, Suricata dan Zeek dengan menggunakan QOS.

1.6 MANFAAT PENELITIAN

Dari hasil penelitian yang dilakukan, diharapkan dapat memberi manfaat sebagai berikut:

1. Dapat mengetahui kemampuan dari *tools* Snort, Suricata dan Zeek pada konfigurasi IPS.
2. Dapat mengetahui perbandingan performansi dari 3 *tool* (IPS) yaitu Snort, Suricata dan Zeek dengan menggunakan QOS.