BAB 1
PENDAHULUAN

1.1 Latar Belakang

Saat ini penggunaan teknologi informasi di segala bidang sangatlah penting. Namun, penggunaan ini terkadang tidak diimbangi dengan keamanan yang baik yang dapat menyebabkan beberapa kerugian seperti kehilangan data, kerentanan pada sistem dan kerusakan pada sistem (Alviana & Sumitra, 2018). Keamanan informasi menjadi faktor yang sangat penting untuk melindungi kerahasiaan data *(confidentiality)*, integritas data *(integrity)* dan ketersediaan data maupun layanan (*availability)* bagi pengguna dan penyedia sebuah layanan yang memanfaatkan teknologi informasi. Sebuah organisasi, perusahaan maupun individu yang memanfaatkan teknologi informasi harus dapat melindungi sistem mereka dari berbagai ancaman yang beresiko dapat merusak sistem.

Banyak sekali ancaman dan serangan yang dapat menjadi resiko terhadap keamanan sebuah sistem jaringan salah satunya adalah serangan *Denial of Service (DoS)*. Serangan *Denial of Service (DoS)* terus menjadi ancaman sampai saat ini, bahkan dalam bentuk yang jauh lebih besar dan merusak seperti *Distributed Denial of Service (DDoS)*. Target utama dari serangan *Denial of Service (DoS)* adalah membuat sumber informasi menjadi tidak tersedia atau sederhananya target utama dari serangan tersebut adalah *availability* (Qadir & Quadri, 2016). *Flooding Attack* adalah salah satu metode serangan yang menargetkan jaringan komputer yang termasuk kedalam tipe serangan *Denial of Service (DoS)*. Serangan *flooding* bertujuan untuk membanjiri trafik data pada jaringan agar dapat menyebabkan jaringan menjadi lumpuh diakibatkan beban data yang berlebihan (Pradhana et al., 2021).

Dalam menjaga sistem jaringan komputer dari risiko keamanan, dibutuhkan adanya sistem yang bisa mengawasi setiap kejadian pada lalu lintas jaringan komputer agar risiko keamanan yang ditimbulkan dapat diminimalisir serta dapat membantu untuk mendeteksi adanya penyusupan atau intrusi di dalam jaringan tersebut. Salah satu metode yang dapat digunakan adalah dengan menerapkan *Intrusion Detection System (IDS)*, IDS dapat bekerja berdasarkan analisis yang

dilakukan terhadap lalu lintas paket data pada suatu jaringan (Gozali & Setiaji, 2013).

Snort dan *Suricata* merupakan tipe IDS *open-source* yang menjadi pilihan bagus untuk penerapan sistem pendeteksi intrusi dikarenakan popularitas serta kualitasnya. Namun, diantara kedua IDS ini terkadang pengguna sulit untuk menentukan mana IDS yang baik dan cocok untuk sistemnya dikarenakan kedua IDS tersebut mempunyai kelebihannya masing-masing. *Suricata* mempunyai fitur *multithread* yang dapat menjalankan banyak *thread* dari semua CPU yang tersedia di mesin, menurut *Open Information Security Foundation (OISF) Suricata* seharusnya mampu menangani lalu lintas mulai dari 100 hingga 200 *Mbps* (Bada et al., 2020). Maka dari itu *Suricata* diharapkan menjadi sistem deteksi intrusi generasi berikutnya (Albin & Rowe, 2012). Walaupun dengan hadirnya *Suricata*, *Snort* juga masih tetap digunakan secara luas di jaringan di seluruh dunia karena desainnya yang ringan dan opsi penerapannya yang fleksibel, basis pengguna *Snort* berkembang pesat di tahun-tahun berikutnya (hingga 400.000 pada tahun 2021) (Siemons, 2021).

Walaupun kedua IDS tersebut sudah banyak diterapkan, namun masih sedikit yang menganalisa kinerja dari sistem tersebut, baik dari sisi kinerja deteksi maupun kinerja penggunaan sumber daya pada komputer (Alviana & Sumitra, 2018). *Suricata* terlihat lebih unggul dari sisi performa daripada *Snort* dikarenakan fitur *multithreading* yang ada pada *Suricata* membuat prosessor dapat menjalankan beberapa *thread* secara bersamaan. Tetapi sekarang *Snort* juga sudah memiliki fitur *multithreading* pada versi terbarunya yaitu *Snort* 3.

Oleh karena itu berdasarkan fakta dan permasalahan diatas, penulis bertujuan untuk menganalisa terhadap kinerja *Snort* dan *Suricata* yang diharapkan dapat membantu untuk menentukan IDS yang terbaik untuk mendeteksi serangan *Flooding* dari segi kinerja kecepatan deteksi serangan, jumlah serangan yang terdeteksi dan konsumsi terhadap sumber daya komputer. Kecepatan deteksi serangan dan banyaknya serangan yang terdeteksi akan digunakan sebagai acuan seberapa baik kinerja IDS dalam mendeteksi serangan, semakin cepat serangan terdeteksi maka semakin cepat juga serangan tersebut dapat ditangani, lalu semakin

banyak serangan yang terdeteksi maka semakin kecil resiko serangan yang dapat mempengaruhi sistem. Parameter konsumsi sumber daya akan digunakan sebagai acuan seberapa baik IDS dalam mengelola sumber daya, semakin sedikit sumber daya yang digunakan maka semakin baik karena sistem tidak perlu memakai terlalu banyak sumberdaya yang ada.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas dapat dirumuskan masalah pada penelitian ini sebagai berikut:

1. Bagaimana kinerja kecepatan deteksi, jumlah serangan terdeteksi dan penggunaan sumber daya pada *Intrusion Detection System (IDS) Snort* dan *Suricata* dalam mendeteksi serangan *Flooding*?
2. Adakah perbedaan kinerja pada kecepatan deteksi, jumlah serangan terdeteksi dan penggunaan sumber daya pada *Intrusion Detection System (IDS) Snort* dan *Suricata* sehingga dapat disimpulkan IDS mana yang terbaik dan terstabil untuk mendeteksi serangan *Flooding*?

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas batasan masalah pada penelitian ini sebagai berikut:

1. IDS yang digunakan adalah *Snort* dan *Suricata*.
2. Parameter pengukuran kinerja adalah kecepatan deteksi, jumlah serangan terdeteksi dan penggunaan sumberdaya (RAM & CPU) komputer.
3. Serangan yang dilakukan untuk pengujian kinerja IDS adalah *SYN Flooding, UDP Flooding* dan *HTTP GET & POST Flooding*.
4. *Snort* akan diuji saat menggunakan mode *singlethread* dan *multithread* untuk melihat perbedaan kinerja pada versi terbarunya dan *Suricata* akan diuji menggunakan mode *multithread.*

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

1. Membandingkan kinerja *Snort* dan *Suricata* saat menjadi target beberapa macam serangan *Flooding.*
2. Membandingkan *Snort* dan *Suricata* untuk menentukan mana yang lebih unggul dan lebih stabil dalam mendeteksi serangan *Flooding*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Dapat menentukan IDS mana yang lebih baik dan cocok diantara *Snort* dan *Suricata* untuk diterapkan pada sistem.
2. Dapat meningkatkan kinerja *Snort* dan *Suricata* dalam mendeteksi serangan *Flooding* berdasarkan *rule* yang digunakan.