BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Pada tahun 2019, kasus *cybercrime* di Indonesia semakin tinggi, sejalan dengan perkembangan internet dan teknologi yang ada. Beberapa serangan yang masuk diantaranya, virus *ransomware wannacry*, OWASP, *Automated Threat* dan DDoS. Serangan DDoS, merupakan serangan yang banyak dialami oleh pengguna [1]. Jenis serangan TCP dan UDP *flood* merupakan salah jenis serangan DDoS yang bertujuan untuk menghabiskan sumber daya server, seperti penggunaan CPU [2] karakteristik serangan *Distributed Denial of Service* (DDoS) sulit di bedakan dari arus lalu lintas jaringan normal, sehingga untuk mengidentifikasi serangan ini diperlukan sistem yang dapat mengklasifikasi serangan DDoS [3]. Penelitian ini akan menguji dua *tools* dengan menggunakan metode IDS yang dapat mendeteksi serangan DDoS.

Intrusion Detection System (IDS) merupakan sebuah metode yang dapat mendeteksi serangan DDoS yang masuk kedalam lalu lintas jaringan dengan cara membaca log dari *traffic* serangan yang dicurigai, dan menolak lalu lintas yang terdeteksi sebagai ancaman dalam jaringan [4].

Oleh karena itu, peneliti menggunakan metode IPS pada dua *tools* yang dapat mendeteksi dan memblokir serangan yang masuk.

Berdasarkan latar belakang diatas, penelitian ini akan membandingkan dua *tools* yaitu zeek dan suricata dengan metode IDS untuk mendeteksi dan memblokir serangan DDoS yang masuk kedalam lalu lintas jaringan serta *Opensearch-dashboards* untuk mengontrol lalu lintas jaringan. Dengan judul **“ANALISIS PERBANDINGAN KEAMANAN JARINGAN DENGAN METODE IDS MENGGUNAKAN ZEEK DAN SURICATA”**. Skenario yang akan dilakukan Terdapat dua skenario yang akan dilakukan yaitu, pada saat IPS

tidak aktif dan pada saat IPS diaktifkan. Penelitian ini menggunakan parameter *confusion matrix* untuk mengukur tingkat akurasi dari serangan yang masuk.

1.2 RUMUSAN MASALAH

Yang menjadi rumusan masalah dari penelitian ini:

1. Bagaimana IDS pada zeek dan suricata dapat mendeteksi terjadinya serangan DDoS?
2. Bagaimana pengaruh penerapan metode IDS pada zeek dan suricata dalam mengatasi serangan DDoS terhadap lalu lintas jaringan?
3. Bagaimana perbandingan kinerja IDS pada zeek dan suricata terhadap serangan DDoS?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini:

1. Metode yang digunakan *Intrusion Detection System* (IDS).
2. Penggunaan *tools* zeek dan suricata dalam penerapan *Intrusion Detection System* (IDS).
3. Paremeter yang di uji *confusion matrix.*

1.4 TUJUAN

Tujuan dari penelitian:

1. Untuk merancang bagaimana IDS dapat mendeteksi terjadinya serangan DDoS.
2. Untuk menganalisis pengaruh penerapan metode IDS dalam mengatasi serangan DDoS.
3. Untuk menganalisis perbandingan kinerja *Intrusion Detection System* (IDS) terhadap serangan DDoS.

1.5 MANFAAT

Manfaat penelitian ini adalah:

1. Mengetahui sistem kerja dari metode yang digunakan.
2. Mengetahui metode yang digunakan dapat mengatasi serangan DDoS.

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan ini dibagi menjadi beberapa bab. Bab 1 berisi latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan. Bab 2 berisi kajian pustaka, dasar teori, keamanan jaringan, serangan jaringan DDoS, IDS, suricata, *Tool* DDoS, *Opensearch-dashboards,* dan *confusion matrix*. Bab 3 membahas mengenai tahapan yang akan dilakukan terdiri dari alur penelitian, perangkat keras maupun perangkat lunak yang akan digunakan, skenario penelitian, topologi jaringan, alat, dan konfigurasi *tools*. Bab 4 membahas mengenai hasil pengujian, dan analisis hasil pengujian. Bab 5 membahas mengenai kesimpulan yang didapatkan dari pengujian dan saran yang diajukan sebagai pertimbangan penelitian selanjutnya.