BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Di era digital yang semakin maju, keamanan jaringan menjadi hal yang sangat penting diperhatikan bagi perorangan, organisasi, dan juga perusahaan. Hal ini dikarenakan jaringan yang bersifat publik sehingga dapat diakses dengan mudah dan bebas oleh orang di seluruh dunia. Hal inilah yang membuat jaringan sangat rentan dari segi keamanannya dan menyebabkan terjadinya kejahatan di dunia maya atau lebih dikenal dengan kejahatan *cyber*. Kejahatan *cyber* ini dapat menyerang jaringan komputer, menyusup kedalam jaringan mengambil data-data rahasia dan melumpuhkan sistem jaringan komputer [1]. Dari tahun ke tahun, jumlah serangan *cyber* di Indonesia terus meningkat. Berdasarkan data Badan Siber dan Sandi Negara (BSSN) periode Januari-Mei 2021, jumlah kasus serangan siber di Indonesia mencapai 448 juta kasus [2].

Serangan siber sendiri memiliki beberapa jenis, antara lain *port scanning, SSH, brute force, MiTM, dan DDoS.* Dari semua jenis serangan siber ini, serangan yang paling sering digunakan adalah *DDoS* [3]. Serangan *DDoS* ini dapat melumpuhkan *client-server* agar tidak bisa terhubung pada jaringan atau jaringan menjadi *down,* eksploitasi *password* dan *username* pada *microtik router* dan menginjeksi *database* pada aplikasi *web* untuk bisa mendapatkan *password* dan *username* sehingga dapat *login* sebagai *admin* [4]. Di Indonesia sendiri, ada terjadi percobaan *DDoS* pada penyelenggaraan PON XX, tercatat terdapat sekitar 112.762.000 akses ke domain-domain yang berkaitan dengan PON 2021 [5]. Untuk meminimalkan serangan *DDoS* ini, *firewall* saja tidak cukup untuk dapat memblokir jaringan dan juga tidak bisa mengetahui taktik dari penyerang tersebut.

Penggunaan *firewall* sendiri masih kurang efektif dikarenakan menutup semua akses tanpa memperdulikan siapapun yang sedang terkoneksi dalam jaringan [6]. Untuk itu, diperlukan sistem yang memiliki keamanan jaringan yang dapat mendeteksi, mencegah, dan mencatat dari aktivitas serangan *port scanning*, *SSH, brute force, MiTM, dan DDoS* [7]. Keamanan secara berlapis dapat membantu keamanan jaringan dengan mengintegrasikan *IPS*[8]. Sebenarnya masih banyak metode yang dapat dilakukan untuk mengamankan sebuah sistem jaringan. Salah satunya adalah menggunakan *IDS* dan *IPS.* Metode ini lebih dikenal dengan metode *IDPS.*

Metode *IDPS* ini dapat mendeteksi dan juga mencegah serangan siber. Metode ini digunakan sebagai solusi untuk mengamankan jaringan dari kejahatan siber selain menggunakan *firewall* saja. Dengan menggunakan metode ini, akan lebih mudah untuk mendeteksi serangan *DDoS.* Metode *IDPS* ini akan bekerja seperti *firewall* yang dapat mengizinkan dan kemudian memblokir paket data tapi metode ini mempunyai pengamanan yang lebih kuat daripada *firewall.* Metode *IDPS* ini adalah penggabungan dua buah metode, yaitu metode *IDS* dan *IPS.*

Untuk metode *IDS* ini sebuah *software* yang ditujukan menjadi pemantau aktivitas yang berbahaya [9]. *IDS* ini dapat mencegah resiko keamanan sistem jaringan yang melanggar keamanan sistem jaringan [10]. Terdapat beberapa *software IDS* yang sering digunakan didunia jaringan antara lain Snort, Suricata, OSSEC, Sagan, Bro, Solarwinds Logs & Event Manager [11]. Sedangkan, metode *IPS* ini sebuah perangkat lunak atau perangkat keras yang bekerja untuk monitoring trafik jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak sebagaimana mestinya [12]. Pada penelitian ini, untuk dapat menyelesaikan permasalahan keamanan jaringan dengan mengintegrasikan *IDPS* menggunakan *tools* OSSEC dan Snort.

OSSEC dan Snort ini merupakan *tools* yang akan digunakan untuk mendeteksi serangan *DDoS* nantinya. OSSEC ini sebuah aplikasi *opensource* yang dapat digunakan untuk melakukan monitoring *log server* [14]. Sedangkan Snort telah diakui sebagai *tools IPS open source* terbaik dan telah banyak diunduh dan digunakan pada tahun 2015 [5]. Setelah penggunaan *tools IDPS* ini, akan dilakukan penghitungan QoS.

Metode yang digunakan dalam penelitian ini adalah *Quality of Service (*QoS*)* yang membandingkan *throughput, delay, jitter,* dan *Packet loss.* Berdasarkan penelitian ini, peneliti bertujuan untuk melakukan perbandingan kinerja *tools* OSSEC dan Snort.

Penelitian ini akan melakukan pengujian dan analisis tingkat akurasi *tools* OSSEC dan Snort saat dikonfigurasi dengan sistem perlindungan *Intrusion Detection and Prevention System (IDPS)* saat terdeteksi adanya serangan. Dan setelah itu, hasil akhir dari ketiga *tools* tersebut akan dihitung menggunakan parameter QoS. Tujuannya adalah untuk mengetahui kinerja dari OSSEC dan Snort dalam mendeteksi serta melakukan pencegahan terhadap serangan *DDoS.*

1.2 Perumusan Masalah

Berdasarkan latar belakang yang ada, dapat dilihat bahwa permasalahan dari penelitian ini antara lain sebagai berikut:

1. Implementasi dari OSSEC dan Snort saat diimplementasikan dengan konfigurasi *IDPS.*
2. Perbandingan performansi dari *tools IDPS,* yaitu OSSEC dan Snort dengan menggunakan QoS.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah diatas, pertanyaan penelitian ini antara lain sebagai berikut:

1. Bagaimana cara mengimplementasikan *tools* OSSEC dan Snort pada konfigurasi *Intrusion Detection and Prevention System (IDPS)*?

2. Bagaimana perbandingan performansi dari *tools IDPS,* yaitu OSSEC dan Snort dengan menggunakan QoS?

1.4 Batasan Masalah

Berdasarkan latar belakang masalah dan tujuan penelitian, agar penelitian dapat dilakukan dengan baik maka ditetapkan batasan masalah penelitian sebagai berikut:

1. Berfokus pada perbandingan performansi kinerja dari *tools* OSSEC dan Snort saat dilakukan pengujian serangan
2. Menerapkan sistem *Intrusion Detection and Prevention System (IDPS)*
3. Penelitian ini tidak mencakup analisis serangan atau metode keamanan jaringan lainnya selain *DDoS*
4. Pengujian serangan menggunakan tipe serangan *DDoS (ICMP Flood, TCP Flood,* dan *UDP Flood)*
5. Komparasi OSSEC dan Snort hanya berfokus dalam mendeteksi dan mencegah serangan
6. Parameter performansi yang digunakan adalah *Quality of Service (*QoS*).*

1.5 Tujuan Penelitian

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

1. Untuk menerapkan konfigurasi *IDPS* pada *tools* OSSEC dan Snort
2. Untuk mengetahui perbandingan performansi dari *tools IDPS,* yaitu OSSEC dan Snort dengan menggunakan QoS.

1.6 Manfaat Penelitian

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

1. Dapat mengetahui kemampuan masing-masing *tools* OSSEC dan Snort pada konfigurasi *IDPS.*

2. Dapat mengetahui perbandingan performansi dari *tools IDPS*, yaitu OSSEC dan Snort dengan menggunakan QoS.