# BAB I
# PENDAHULUAN

## 1.1 LATAR BELAKANG

*Server* merupakan salah satu komponen penting dalam jaringan, dikarenakan *server* menyimpan data berharga seperti informasi pengguna yang bersifat pribadi, dan menyediakan layanan untuk pengguna[1]. Keamanan jaringan dibutuhkan *server* untuk menjaga performansi yang diberikan untuk pengguna, suatu serangan dapat terjadi kapan saja dan dimana saja. Serangan yang sering ditemui yaitu *Denial of Service* (DoS), serangan ini bertujuan untuk mengganggu ketersediaan layanan dengan cara membanjiri *server* atau jaringan dengan lalu lintas yang berlebihan. Serangan DoS dapat mengganggu layanan yang disediakan *server*, menghambat kinerja, gangguan jaringan, mengurangi kinerja *server*, dan merusak reputasi perusahaan[2]. Metode *Intrusion Detection Prevention System* (IDPS) dapat dimplementasikan untuk mendeteksi dan mencegah serangan Dos yang tertuju ke *server*. Apabila terdapat lalu lintas yang mencurigakan maka IDPS dapat mengenali dan memberikan tindakan lebih lanjut seperti *drop* atau *reject*[3].

Penelitian yang dilakukan oleh Hendri Alamsyah, Riska, dan Abdussalam Al Abar pada tahun 2020 dengan judul "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System"[3]. Penelitian ini mengimplementasikan metode IDPS Suricata untuk mendeteksi dan mencegah lalu lintas yang mencurigakan, hasil dari penelitian ini yaitu IDPS Suricata dapat mendeteksi dan mencegah serangan *port scanning*, akses telnet dan ftp yang telah diujikan. Terdapat beberapa penelitian yang mengimplementasikan IDS Snort dalam mendeteksi serangan[1][4][5], pada penelitian tersebut Snort dapat mendeteksi berbagai serangan yang diujikan.

Penelitian ini akan mengimplementasikan metode IDPS menggunakan *tools Snort* dalam mendeteksi serangan ICMP *Flood*, UDP *Flood*, dan SYN *Flood* yang tertuju ke server. Penelitian ini mengukur performansi IDPS Snort berdasarkan parameter *Quality of Service* (QoS) yang diberikan *server* kepada pengguna. Diharapkan dengan adanya *Snort* sebagai IDPS dapat meningkatkan kualitas QoS yang diberikan *server* saat serangan terjadi dibandingkan pada saat belum mengimplementasikan metode IDPS Snort.

## 1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1. Bagaimana perancangan sistem keamanan dengan impelemtasi IDPS *Snort*?
2. Bagaimana performansi IDPS *Snort* berdasarkan parameter *Quality Of Service*?
3. Bagaimana dampak serangan *Denial of Service* (DoS) dari sisi *client*?

## 1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Penelitian dilakukan secara virtual menggunakan *Virtual Machine*.
2. Penelitian hanya berfokus pada *Snort* dalam mendeteksi dan mencegah serangan yang masuk.
3. Serangan yang digunakan yaitu ICMP *flood,* SYN *flood,* dan UDP *flood.*
4. Skenario pengujian pada penelitian ini yaitu saat *server* dalam keadaan normal, server dalam keadaan diserang namun *Snort* belum aktif, dan pada saat server dalam keadaan diserang dan *Snort* aktif.
5. Parameter performansi yang digunakan yaitu parameter QoS

## 1.4 TUJUAN

Adapun tujuan penulisan skripsi ini adalah:

1. Menganalisa proses perancangan sebuah sistem keamanan dengan menerapkan *Snort* sebagai IDPS.
2. Menganalisa kinerja *Snort* berdasarkan parameter *Quality Of Service* (QoS)
3. Menganalisa dampak dari serangan *Denial of Service* (DoS) dari sisi pengguna atau *client*

## 1.5 MANFAAT

Penelitian ini diharapkan dapat memberikan pengetahuan terhadap proses perancangan sistem keamanan jaringan dengan menerapkan *Snort* sebagai IDPS, dapat menentukan dan menganalisa *rules* untuk mendeteksi dan mencegah serangan yang masuk, serta mengetahui performansi kinerja *Snort* berdasarkan parameter *Quality Of Service* yang hasilkan *server*.

## 1.6 SISTEMATIKA PENULISAN

Penelitian ini dibagi menjadi lima bab. Bab pertama berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan. Bab dua membahas tentang tinjauan pustaka dan dasar teori yang menjadi pendukung penulis dalam penyusunan proposal. Bab tiga berisi tentang prosedur penelitian meliputi perancangan sistem, alat yang digunakan, konfigurasi jaringan dan penjabaran skenario pengujian yang telah dilakukan. Bab empat berisi hasil dan analisis berdasarkan pengujian yang telah dilakukan. Bab lima berisi kesimpulan dan saran pengembangan bersadarkan pengujian yang telah dilakukan serta menjadi masukan untuk penelitian selanjutnya.