# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Seiring berkembangnya teknologi Informasi dan pemanfaatan komputer untuk kehidupan sehari-hari, hal tersebut dengan sendirinya menimbulkan sebuah permasalahan tersembunyi salah satunya keamanan jaringan. Inti dari keamanan jaringan komputer adalah untuk melindungi sumber daya informasi, perlindungan terhadap media penyimpanan dan aliran sumber informasi agar tidak terjadi kebocoran atau kerusakan informasi.

Masalah pada jaringan ataupun gangguan pada dasarnya dapat dibagi menjadi dua bagian, pertama adalah gangguan internal dan kedua adalah gangguan eksternal. Gangguan internal merupakan gangguan yang berasal dari dalam jaringan itu sendiri, baik dari infrasruktur jaringan internal tersebut, dalam hal ini adalah adanya pihak pihak yang mengetahui kondisi keamanan dan kelemahan dari jaringan tersebut. Gangguan eksternal adalah gangguan yang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin mengganggu keamanan yang ada pada jaringan tersebut. Proses ini bisa terjadi melalui jaringan yang diakses oleh pihak luar yang ingin melakukan gangguan ataupun pengrusakan terhadap jaringan tersebut.

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, walaupun terkadang ada beberapa organisasi yang menempatkannya pada urutan yang ke sekian setelah hal lain. Namun ketika jaringan mendapat serangan dan terjadi kerusakan sistem, investasi yang dikeluarkan cukup besar untuk melakukan perbaikan sistem. Untuk itu sudah selayaknya investasi di bidang keamanan jaringan lebih diperhatikan, untuk mencegah kerusakan dari ancaman serangan yang saat ini semakin beragam serta semakin canggih. Terlebih lagi ketika jaringan lokal sudah terhubung ke internet maka ancaman serangan terhadap keamanan jaringan seiring semakin meningkat. Oleh karena itu, dibutuhkan suatu sistem untuk menganalisa gangguan atau

ancaman yang akan terjadi secara optimal dalam waktu cepat dan otomatis yang hasil keluaran dari serangan tersebut dapat pula menampilkan dalam bentuk informasi. Bahkan keamanan jaringan yang membuat semakin banyaknya *tools* yang akan digunakan untuk mendeteksi bahkan dapat mengambil keputusan apabila terjadi serangan yang masuk ke dalam jaringan. **Snort** bisa digunakan sebagai *tools* untuk membantu dalam mengenali ***Intrusion Detection System* (IDS).** Dan kombinasi *Intrusion Detection System* dengan ***Demilitarized Zone* ( DMZ)** bisa mejadi salah satu solusi karena dengan topologi DMZ, posisi DMZ sendiri terletak diantara suatu jaringan *privat* dan jaringan publik (internet).

## 1.2. Rumusan Masalah

Apakah *Intrusion Detection System* mampu mendeteksi serangan terhadap *Demilitarized Zone* jaringan yang ada dan berapa tingkat akurasinya?

## 1.3. Batasan Masalah

Agar dalam perancangan ini dapat dicapai sesuai dengan sasaran dan tujuan yang diharapkan, maka permasalahan yang ada dibatasi yaitu Indikator serangan:

1. Port Scaning
2. DoS

## 1.4. Tujuan Penelitian

Berdasarkan rumusan masalah di atas penelitian ini bertujuan untuk membuktikan dan mengimplementasikan *Intrusion Detection System* yang mampu mendeteksi secara aktif kemungkinan adanya serangan dan mengukur tingkat akurasi jika di terapkan dengan topologi *Demilitarized Zone.*

## 1.5. Manfaat

Sebagai alternatif untuk mendeteksi adanya serangan dan mengetahui tingkat akurasi *Intrusion Detection System* dalam mengenali sebuah paket data tersebut merupakan serangan atau bukan.