

## **BAB I**

### **PENDAHULUAN**

#### **1. 1 Latar Belakang**

Di era digital ini, jaringan adalah bagian dari kehidupan kita. Mereka adalah anugerah bagi dunia. Mereka membawa dunia lebih dekat kepada kita. Dengan jaringan, ancaman penyusupan menjadi sangat umum. Dunia maya tidak pernah lepas dari hacker. Dipraktiknya, tidak mungkin membangun sistem yang sepenuhnya aman. Dengan demikian, ada berbagai perangkat keras dan perangkat lunak yang diciptakan untuk mencegah jaringan dari lalu lintas data yang berbahaya. Mulanya firewall dianggap penting untuk memberikan keamanan bagi jaringan tetapi sekarang sistem IDS dan IPS adalah yang utama perangkat bersama dengan firewall.[1]

Deteksi intrusi saat ini dan pencegahan diperlukan untuk keamanan jaringan apa pun. Untuk melindungi organisasi dari serangan cyber, intrusi sistem deteksi (IDS) memainkan peran penting. Sumber terbuka alat untuk sistem deteksi intrusi dapat melakukan protocol analisis untuk mendeteksi serangan dengan menggunakan aturan dan tanda tangan. Setiap alat IDS open source memiliki perbedaan kemampuan untuk mendeteksi berbagai jenis serangan. Banyak peneliti mempelajari kinerja deteksi opensource IDS. Setiap IDS memiliki keunggulan yang berbeda dan kerugian seperti tingkat deteksi spesifik jenis serangan, false positive, dll. Banyak juga yang buka perpustakaan perangkat lunak sumber untuk pembelajaran mendalam suatu jaringan komputer memerlukan suatu sistem pengawasan dan pengamanan data untuk menjaga agar informasi penting yang ada dalam jaringan tersebut tetap aman. [2]

Merujuk kepada data statistic APJII (Asosiasi Penyelenggaraan Jasa Internet Indonesia), Survei APJII tahun 2019 – Q2 2020 menyebutkan bahwa pengguna internet di Indonesia mencapai 196,7 juta pengguna populasi RI 266,9 juta penduduk. naik 8.9 % menjadi 73.7 % artinya, transformasi digital bisa terjadi lebih cepat, apalagi dalam keadaan pandemic. dalam hal ini maka sistem keamanan berupa monitoring keamanan jaringan adalah hal yang paling tepat jika dipadukan dengan ids snort untuk mengawasi packet packet yang berada pada jaringan yang digunakan oleh client.[3]

## **1.2 Perumusan masalah**

Untuk memperjelas dan mengarahkan penelitian ini agar hasil yang di dapat sesuai dengan yang diharapkan, maka masalah yang ada dapat dirumuskan adalah

- a. Mengapa menggunakan Snort dengan IDS disambungkan dengan telegram sebagai media monitoring jaringan?
- b. Berapa tingkat keberhasilan yang didapatkan setelah menggunakan ids snort dan media telegram sebagai notifikasi?

## **1.3 Tujuan Penelitian**

Tujuan dari penelitian ini adalah mengimplementasikan snort sebagai Network Intrusion Detection system dengan notifikasi alert dikirimkan melalui media telegram

## **1.4 Batasan Masalah**

- a. Deteksi serangan dengan menggunakan *Intrusion Detection System*
- b. Penelitian ini menggunakan *Snort* sebagai *Network Intrusion Detection System*
- c. Notifikasi serangan dikirimkan dengan media telegram
- d. Penelitian ini hanya berfokus pada serangan DDoS, SQL Injection dan Port Scan

### **1.5 Manfaat Penelitian**

Untuk mengetahui tingkat keamanan yang ada pada sistem komputer menggunakan IDS snort dengan media monitoring telegram

