BAB 1. PENDAHULUAN

1.1. Latar Belakang

Pada era perkembangan dunia teknologi saat ini, sudah dapat membuat jaringan dengan mudah. Dengan terbentuknya sebuah jaringan yang memungkinkan berinteraksi maupun bertukar data dengan lebih efisien dan praktis. Akses yang mudah terhadap informasi tersebut menyebabkan timbulnya masalah baru yaitu informasi atau data-data penting dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri, sehingga suatu sistem keamanan jaringan menjadi salah satu aspek yang penting. Tidak semua informasi dapat diakses untuk umum. Internet merupakan jaringan luas dan bersifat publik, oleh karena itu diperlukan suatu usaha untuk menjamin keamanan informasi terhadap data atau layanan yang menggunakan internet (Cahyanto, 2015). Internet merupakan salah satu bentuk jaringan yang mana dapat menghubungkan perangkat-perangkat di seluruh dunia. pada tahun 2019 jumlah pengguna internet di Indonesia sudah mencapai 196,7 juta jiwa. Angka ini setara dengan 73,7% dari total penduduk Indonesia yaitu 266,9 juta jiwa. Dengan begitu pentingnya keberadaan suatu jaringan, tentu tidak boleh mengesampingkan dari sisi keamanannya (APJII, 2020).

Direktorat Tindak Pidana Kejahatan Siber (Dittipidsiber) Bareskrim Polri sepanjang tahun 2019, yakni bulan Januari-Agustus menangani 3.429 kasus kejahatan siber. Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan (Ariyus, Intrusion Detection System, 2007).

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang tersebut, maka dapat diambil rumusan masalah sebagai berikut :

1. Bagaimana merancang sistem keamanan jaringan berbasis IDS.
2. Bagaimana mendeteksi gangguan atau aktivitas ilegal pada server secara otomatis.
3. Bagaimana melakukan tindakan lebih lanjut secara cepat dan efektif.

1.3. Tujuan

Sesuai dengan rumusan masalah yang telah dikemukakan, tujuan dari pembuatan sistem ini adalah untuk merancang system keamanan jaringan berupa pencegahan penyusupan dengan menggunakan *IDS* dan *snort alert* yang dipadukan dengan *bot* pada telegram. Sehingga dapat mendeteksi gangguan secara otomatis walaupun administrator tidak sedang berada pada system.

1.4. Manfaat

Sistem yang akan penulis bangun ini akan memberikan kontribusi kepada sistem keamanan jaringan pada *server*, juga membuat suatu jaringan yang *secure* dan dapat dengan cepat melakukan tindakan jika terdapat aktivitas yang mencurigakan.

1.5. Batasan Masalah

Dengan mengidentifikasi masalah-masalah yang ada,agar lebih terarah dan dapat dipahami dengan mudah, maka perlu dilakukan pembatasan masalah. Pembatasan terhadap masalah yang ada pada pembuatan sistem ini antara lain :

1. Server yang digunakan berupa Virtual Server menggunakan VirtualBox.
2. IDS berfungsi sebagai pendeteksi aktivitas yang mencurigakan pada sistem.
3. Menggunakan Bot pada Telegram sebagai pengirim pesan saat terdapat aktivitas mencurugakan pada sistem.