BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Teknologi informasi dalam berbagai bidang kehidupan memberikan kesempatan untuk dapat dimanfaatkan secara tepat dan efektif, termasuk salah satunya dalam bidang jaringan komputer. Jaringan Komputer dengan sangat pesat terus berkembang dan orang-orang sekarang banyak yang membutuhkan akses internet. Jurusan teknik komputer politeknik negeri sriwijaya saat ini sedang berencana untuk melakukan pembuatan server baru didalam gedung itu sendiri. Server yang akan di bangun didalam gedung itu sendiri bertujuan agar laboratorium jaringan komputer pada jurusan teknik komputer dapat mengakses jaringan pada server sendiri dan juga sebagai pembelajaran baru kepada mahasiswa baru yang akan belajar di jurusan teknik komputer. lalu saat ini server yang akan dibangun tersebut membutuhkan keamanan jaringan yang dapat membantu mengatasi masalah kepada seseorang yang berniat jahat untuk mengganggu kelancaran pada saat penggunaan server. Dengan alasan tertentu mereka melakukan penyerangan yang dapat merugikan pemilik serta pengguna server dan jaringan komputer.

Berbagai macam serangan mereka gunakan untuk menyerang jaringan komputer dengan *tools* yang dibuat secara mandiri ataupun yang telah ada. IDS diterapkan karena hanya mampu mendeteksi serangan pada jaringan dan memberikan peringatan kepada administrator yang sedang memantau kondisi jaringan. Snort yang merupakan *software open source* IDS yang digunakan dalam penelitian untuk mendeteksi serangan kepada server laboratorium jaringan teknik komputer. Oleh karena itu pada server baru ini diusulkan untuk membuat sistem IDS yang diharapkan dapat membantu administrator dalam memantau kondisi jaringan pada server tersebut.

Pada penelitian sebelumnya yang dilakukan oleh Arpenta L.T. Ginting, Junika Napitupulu, dan Jamaluddin Jamaluddin (2015). Diperlukan adanya sistem pendeteksian untuk mengetahui adanya aktivitas-aktivitas yang mencurigakan. pendeteksian tehadap aktivitas-aktivitas mencurigakan yang ada dilakukan secara manual oleh administrator. Penelitian yang dilakukan oleh Randy et al., (2015).

Melakukan penerapan pada sistem operasi linux menggunakan snort sebagai mesin sensor dan *Iptables* sebagai penanganan serangan pada keamanan jaringan nirkabel dari serangan yang dapat mengancam. Penelitian yang dilakukan Rishabh Gupta, Soumya Singh, Shubham Verma,dan Swasti Singhal (2017). Ada banyak upaya oleh *Black Hat Hackers* untuk membobol keamanan jaringan perusahaan dan beberapa dari mereka bahkan berhasil tanpa terdeteksi. Seiring dengan kegiatan berbahaya ini semakin populer di kalangan *Black Hat Hackers*. Setiap hari sejumlah besar data dihasilkan dan diteruskan dan banyak dari data ini menyimpan informasi sensitif tentang perusahaan dan karyawannya. Penelitian yang dilakukan oleh A.Gupta dan L.Sharma (2019) Penyerang DoS yang bertujuan melelahkan sumber daya server seperti kapasitas tautan internet, ruang penyimpanan dalam jaringan, dll. Sehingga server tidak dapat memberikan layanan kepada pengguna asli. dan penyerang *port scanning* digunakan oleh penyerang untuk menemukan layanan yang dapat dieksploitasi pada sistem target atau untuk menerobosnya. Sistem server memiliki layanan tertentu yang berjalan di dalamnya yang diikat ke nomor *port* tertentu. Penelitian yang dilakukan oleh Parningotan (2018) adanya *Log Bug* yang didapatkan pada komputer server yang diindikasikan adanya serangan *Denial of Service* (DoS) pada jaringan komputer Dinas Lingkungan Hidup kota Batam.

Dengan permasalahan yang ada diatas penulis akan membuat sebuah sistem monitoring jaringan permasalahan yang ada tersebut menggunakan IDS pada server laboratorium jaringan komputer di jurusan teknik komputer dengan judul "**IMPLEMENTASI NETWORK INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT DI LABORATORIUM JARINGAN TEKNIK KOMPUTER GEDUNG KULIAH VI**".

1.2 RUMUSAN MASALAH

Berdasarkan uraian diatas, maka penulis merumuskan permasalahan yang ada yaitu bagaimana menerapkan sistem keamanan jaringan menggunakan snort yang hanya mendeteksi dan serangan *Port Scanning* dan serangan DoS dan mencatat IP si penyerang tersebut ke *database* pada server jaringan komputer.

1.3 BATASAN MASALAH

Untuk menghindari kekompleksitasan dalam pembahasan masalah penulisan tugas akhir ini, maka penulis membatasi masalah dengan menggunakan IDS snort yg hanya mendeteksi serangan *Port Scanning* dan serangan DoS dan mencatat IP penyerang dan IP yang diserang serta waktu dan tanggal penyerangan terjadi ke *database*, yang diharapkan dapat dengan mudah bisa dimengerti dan diimplementasikan.

1.4 TUJUAN

Tujuan dari Tugas Akhir ini adalah memudahkan admin untuk mengawasi jaringan pada server laboratorium jaringan komputer di jurusan teknik komputer menggunakan snort.

1.5 MANFAAT

Adapun manfaat dari pembuatan laporan akhir ini yaitu:

1. Membantu admin mengetahui IP orang yang melakukan serangan ke server.
2. Memudahkan admin dalam pengawasan serangan.
3. Dapat mengetahui aktivitas yang mencurigakan dalam jaringan.