BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan Sistem informasi sangat dibutuhkan pada saat perkembangan (IT) yang cukup pesat, terutama dengan adanya jaringan *internet* yang dapat memudahkan dalam melakukan komunikasi dengan pihak yang lain. Dengan mudahnya pengaksesan terhadap informasi tersebut menyebabkan timbulnya masalah baru yaitu informasi atau data-data penting dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan sendiri. Sehingga suatu system keamanan jaringan menjadi salah satu aspek yang penting.

Seorang pengelola *server* jaringan dan internet *(System administrator)* memiliki tanggung jawab terhadap keamanan system dari waktu ke waktu, memastikan bahwa system dan jaringan yang dikelola terjaga dari berbagai peluang ancaman. Politeknik Negeri Sriwijaya merupakan salah satu tempat dimana penggunaan jaringan internet terbuka terhadap pemakainya. Penggunaan tersebut bisa dipergunakan dengan benar dan tidak pula disalahgunakan pemakainannya. Hal ini mengakibatkan suatu system jaringan yang seharusnya digunakan sebagai pembelajaran akan tetapi disalahgunakan penggunaannya untuk aktifitas lain seperti mengakses jejaring sosial. Selain itu administrator harus mengetahui sesuatu *log* yang mengidentifikasi adanya serangan atau penyalahgunaan jaringan.

Oleh karena itu, dibutuhkan suatu sistem dalam menangani penyalahgunaan jaringan atau ancaman yang akan terjadi yaitu dengan menggunakan aplikasi *Intrusion Detection System* (IDS) yaitu *Snort* dan PfSense (Router OS) sebagai penindak lanjut terhadap alert *snort* yang dihasilkan.

Dengan permasalahan tersebut, penulis akan membuat proposal akhir yang berjudul "**IMPLEMENTASI INTRUSION DETECTION**

SYSTEM (IDS) DI JARINGAN POLITEKNIK NEGERI SRIWIJAYA".

1.2 Rumusan Masalah

Adapun rumusan masalahnya adalah bagaimana mengimplementasi *Intrusion Detection System* dari serangan pada jaringan yang ada di Politeknik Negeri Sriwijaya.

1.3 Batasan Masalah

Penerapan *Firewall* tidak dapat melakukan pemblokiran terhadap jenis serangan ini, karena *administrator* system telah melakukan konfigurasi terhadap firewall untuk membuka kedua *port.*

1.4 Tujuan

Tujuan dari pembuatan laporan akhir ini sebagai berikut:

1. Untuk mengetahui sebuah system *Intrusion Detection System* (IDS) snort dapat mendeteksi adanya serangan penyalahgunaan jaringan
2. Untuk mengetahui penganalisaan *log* yang dihasilkan sebagai peringatan kepada administrator.

1.5 Manfaat

1. Dapat memahami cara kerja dari beberapa IDS
2. Mengetahui jalur mana saja yang sering digunakan penyusup agar nantinya dapat dilakukan pemblokiran sehingga tidak dapat dimanfaatkan Kembali
3. Mengetahui IDS mana yang bekerja lebih optimal dan efektif.