1 PENDAHULUAN

1.1 Latar Belakang

Dinas Komunikasi dan Infomatika (Diskominfo) Kota Bogor merupakan organisasi pelayanan publik yang bertanggung jawab menangani bidang data dan jaringan komunikasi yang menghubungkan semua lembaga pemerintahan seperti kelurahan, kecamatan dan dinas-dinas yang terhubung ke *Server* Diskominfo Kota Bogor. Tugas *server* yaitu melayani semua perangkat yang terhubung ke jaringannya, *server* sendiri merupakan perangkat utama dalam sistem komunikasi jaringan yang berfungsi sebagai penyedia layanan dan memiliki *log* yang sangat banyak (Sholihah *et al.* 2020).

Semua jaringan yang terhubung ke Diskominfo Kota Bogor telah terhubung dengan menggunakan Fiber Optik. Fiber Optik adalah kabel berbahan serat optik yang menggunakan cahaya sebagai media transmisinya untuk mengirim data (Hanif dan Arnaldy 2017). Diskominfo memiliki sebuah ruangan *Network Operation Center* (NOC) dimana semua jaringan yang terhubung ke *Server* Diskominfo dapat dikontrol dan dimonitor secara *real-time*. Untuk keamanan jaringan, *Server* Diskominfo hanya menggunakan *firewall* saja. Walaupun telah menggunakan *firewall*, *server* Diskominfo pernah mengalami permasalahan seperti *server down* atau *server* diretas yang disebabkan serangan dari peretas.

Untuk mengatasi hal tersebut dibutuhkan suatu sistem keamanan jaringan tambahan salah satunya yaitu dengan menggunakan *Intrusion Detection System* (IDS). IDS atau sistem deteksi intrusi merupakan sebuah metode yang dapat digunakan untuk memonitor lalu lintas jaringan secara *real-time*, mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan dan memberi notifikasi pada administrator jaringan. Salah satu perangkat lunak yang dapat menerapkan IDS adalah Snort.

Berdasarkan hal tersebut, maka dilakukan Implementasi *Intrusion Detection System* (IDS) Sebagai Keamanan Sistem dan *Server* di Diskominfo Kota Bogor dengan menggunakan Snort sebagai salah satu pilihan untuk menjaga kemanan jaringan.

1.2 Rumusan Masalah

Rumusan masalah dari Implementasi *Intrusion Detection System* (IDS) Sebagai Keamanan Sistem dan *Server* di Diskominfo Kota Bogor apakah sistem deteksi intrusi Snort dapat mendeteksi aktivitas mencurigakan dalam sebuah sistem atau jaringan.

1.3 Tujuan

Tujuan dari Implementasi *Intrusion Detection System* (IDS) Sebagai Keamanan Sistem dan *Server* di Diskominfo Kota Bogor adalah sebagai berikut :

1. Sistem dapat mendeteksi jika terjadi serangan atau adanya penyusup.
2. Memberi notifikasi kepada administrator jaringan bila terjadi serangan.

3. Membuat sistem keamanan jaringan dengan menggunakan Snort sebagai IDS.

1.4 Manfaat

Manfaat dari Implementasi *Intrusion Detection System* (IDS) Sebagai Keamanan Sistem dan *Server* di Diskominfo Kota Bogor adalah sebagai berikut :

1. Membuat sistem keamanan yang dapat mendeteksi alur serangan seperti *Port Scanning*, FTP *Login*, dan DDoS UDP *Flooding*.
2. Membantu administrator jaringan memantau keamanan jaringan dari serangan peretas.

1.5 Ruang Lingkup

Ruang Lingkup dari Implementasi *Intrusion Detection System* (IDS) Sebagai Keamanan Sistem dan *Server* di Diskominfo Kota Bogor adalah sebagai berikut :

1. Sistem yang dibuat bersifat virtual dengan menggunakan Virtualbox.
2. Sistem operasi yang digunakan adalah Linux Ubuntu 16.04 sebagai *server*.
3. Perangkat lunak IDS yang digunakan adalah Snort.
4. Hanya dapat mendeteksi aktivitas serangan seperti yang ada pada *rule* Snort seperti *Port Scanning*, FTP *Login*, dan DDoS UDP *Flooding*.