BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada era global saat ini, teknologi informasi telah berkembang dengan pesat, terutama dengan adanya jaringan *Internet* yang dapat memudahkan dalam melakukan komunikasi dengan pihak yang lain. Selain itu, para pengguna atau *user* dapat mengakses hampir seluruh informasi yang dibutuhkan baik itu informasi yang bersifat publik maupun bersifat pribadi. Namun dengan mudahnya pengaksesan 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.

Berdasarkan data Kementerian Komunikasi dan Informatika (Kominfo) Republik Indonesia per tanggal 5 juni 2019, menyatakan rata-rata serangan *Distributed Denial of Service (DdoS)* meningkat sebesar 14 persen dari jumlah serangan pada kuartal ketiga 2014, dan meningkat 245 persen dari tahun sebelumnya. Seperti yang dijabarkan pada *blog iDefense's 2015 Cyber Threats and Trends*, perpaduan dari gerakan protes secara *online* dan nyata berkontribusi terhadap meningkatnya serangan *DDoS* sebagai strategi melawan organisasi-organisasi, termasuk sektor publik, selama 2014. Menurut informasi yang didapat dalam situs infokomputer sepanjang 2017 terdapat lima kasus *cyber security*. Lima kasus di antaranya yaitu pada bulan November 2017, publik dikejutkan dengan pengakuan dari *CEO Uber* yang baru, *Dara Khosrowshahi*, bahwa data pengguna maupun mitra pengemudi *Uber* telah dibobol oleh peretas. Data yang berhasil dibobol peretas tersebut berupa nama, alamat *email*, serta nomor telepon sekitar 50 juta pengguna dan 7 juta mitra pengemudi dari seluruh dunia. Sehingga dalam hal ini masalah keamanan merupakan salah satu aspek terpenting pada suatu sistem informasi. Aspek tersebut cukup vital dalam pengembangan infrastruktur suatu perusahaan yang memiliki ketergantungan akan dunia IT. Khususnya pengembangan sistem informasi itu sendiri. Banyak hal untuk melakukan pengamanan, yaitu diperlukan perangkat yang mendukung serta sumber daya manusia yang mampu dalam menyelesaikan setiap masalah keamanan dari sistem informasi. Pencegahaan yang paling sering dilakukan untuk masalah ini adalah

dengan menempatkan seorang *administrator*, yang bertugas untuk mengawasi dan melakukan tindakan *preventif* ketika terjadi aksi penyusupan dan serangan. Masalah akan timbul ketika *administrator* sedang tidak berada pada kondisi yang memungkinkan untuk memantau lalu lintas jaringan. Apabila jaringan mengalami gangguan yang menyebabkan jaringan tidak berfungsi maka *administrator* juga tidak dapat lagi mengkases sistem bahkan *administrator* tidak dapat memperbaiki atau memulihkan sistem dengan cepat. Oleh karena itu dibutuhkan suatu sistem dalam menangani dan *monitoring* jaringan dari ancaman yang akan terjadi secara optimal dan otomatis. Bahkan kemanan jaringan harus terus mendapatkan perhatian dari para pemakai jaringan yang membuat semakin banyak *tools* yang digunakan untuk mendeteksi bahkan mengambil tindakan apabila terjadi serangan yang masuk ke dalam jaringan.

Berdasarkan permasalahan tersebut *administrator* membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan, dan mengambil tindakan tepat untuk pencegahan yang akan membantu mengautomatisasi fungsi kerja dasar *administrator. Intrusion Detection and Prevention System* (IDPS) merupakan salah satu pilihan untuk meningkatkan keamanan jaringan dalam sebuah jaringan baik *Intranet* maupun *Internet*. Penerapan *Intrusion Detection and Prevention System* (IDPS) digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu *administrator* dalam memantau dan menganalisa paket-paket berbahaya yang terdapat dalam sebuah jaringan. IDPS diterapkan karena mampu mendeteksi penyusup atau paket-paket berbahaya dalam jaringan dan memberikan laporan berupa *log* kepada *administrator* tentang aktivitas dan kondisi jaringan secara *real-time* sekaligus melakukan *drop packet* terhadap penyusup. Sehingga segera dapat diambil tindakan terhadap gangguan atau serangan yang terjadi. *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. *Intrusion Prevention System* (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan

komputer, IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik.

Berdasarkan uraian latar belakang diatas, maka Tugas Akhir mengambil topik implementasi keamanan jaringan menggunakan *Intrusion detection Prevention System* (IDPS) dalam judul **" SISTEM KEAMANAN JARINGAN BERBASIS INTRUSION DETECTION PREVENTION SYSTEM (IDPS) MENGGUNAKAN NOTIFIKASI MEDIA SOSIAL "**

1.2 Identifikasi Masalah

Berdasarkan uraian yang sudah dijelaskan diatas, maka identifikasi masalah dalam penyusunan Tugas Akhir ini adalah sebagai berikut :

1. Bagaimana mengimplementasikan sistem keamanan jaringan berbasis *Intrusion Detection and Prevention System* (IDPS)
2. Bagaimana mengkonfigurasi IDPS ke dalam jaringan agar dapat terintegrasi dengan media sosial sehingga mempermudah dalam melakukan monitoring jaringan.

1.3 Tujuan Tugas Akhir

Adapun tujuan dari penelitian ini adalah :

1. Dapat melakukan implementasi keamanan jaringan berbasis *Intrusion Detection Prevention system* (IDPS)
2. Dapat melakukan konfigurasi *Intrusion Detection Prevention system* (IDPS) dengan media sosial sebagai notifikasi.

1.4 Manfaat Tugas Akhir

Adapun manfaat yang ingin diberikan dari hasil penelitian tugas akhir ini adalah sebagai berikut:

1. Bagi Penulis :

a. Memahami cara memperkuat sistem keamanan jaringan dengan mengimplementasikan keamanan jaringan menggunakan *Intrusion Detection Prevention system* (IDPS)

b. Untuk memperluas wawasan dan memperdalam pengalaman penulis mengenai konsep dan bentuk penerapan *Intrusion Detection*

Prevention system (IDPS) dalam meningkatkan kualitas aspek keamanan jaringan dengan mendeteksi sekaligus mencegah terjadinya *intrusi* (penyusupan) penyerangan terhadap sistem jaringan.

2. Bagi Masyarakat Umum

Penelitian ini dapat menjadi acuan dan masukan terutama bagi masyarakat umum yang memiliki bidang minat pada keamanan jaringan komputer. terutama dalam kegunaannya untuk mengamankan jaringan komputer yang dimilikinya di jaringan komputer atau *server*, khususnya bagi masyarakat umum yang berprofesi sebagai *administrator* jaringan komputer.

1.5 Lingkup Tugas Akhir

1. Penelitian dilakukan untuk mengimplementasikan *Intrusion Detection Prevention System* (IDPS) dalam penelitian ini menggunakan *SNORT* dengan sistem *monitoring* serta menggunakan *API Telegram* untuk mendukung pengiriman notifikasi ke media sosial yaitu telegram.
2. Penelitian ini dilakukan pada jaringan lokal Pengukuran keberhasilan terimplementasinya *Intrusion Detection Prevention System* (IDPS) yang dapat mengirimkan notifikasi jika ada penyusupan, ke media sosial dengan menggunakan pengujian simulasi penyerangan dengan 5 serangan pada jaringan yaitu *ping of death, nmap (port scan), Telnet,* dan *Ftp*.

1.6 Sistematika Penulisan Tugas Akhir

Untuk mempermudah penyusunan dan pembahasan Tugas Akhir ini akan diuraikan secara garis besarnya dalam beberapa bab penulisan dengan rincian sebagai berikut :

BAB 1 PENDAHULUAN

Pada bab ini berisi latarbelakang masalah, identifikasi masalah, tujuan dan manfaat penelitian, lingkup penelitian, serta sistematika penulisan.

BAB 2 TIJAUAN PUSTAKA

Pada bab ini membahas definisi-definisi dan konsep-konsep dasar yang digunakan dalam penelitian ini, meliputi IDS, IPS, *snort* dan hal lain yang dianggap perlu sebagai rujukan masalah.

BAB 3 METODE

Pada bab ini dijelaskan mengenai hasil dari metodologi yang digunakan

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang analisa dan pengujian dari sistem IDPS tersebut yang hasil dari *alert*-nya dan *log*-nya dapat tampil memalui media sosial

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan yang di dapat dari hasil penelitian yang dilakukan serta saran untuk pengembangan lebih lanjut.