BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dalam berbagai bidang dewasa ini sangatlah signifikan, baik dalam bidang pendidikan, bisnis, keamanan, dan lain sebagainya. Salah satu teknologi yang berkembang saat ini adalah teknologi *Wifi* (*Wireless Fidelity)*. Dalam kehidupan modernisasi saat ini internet merupakan salah satu kebutuhan pokok manusia, baik untuk pekerjaan, pendidikan maupun untuk hiburan. Untuk itu tak sedikit layanan publik yang dipasang teknologi *wireless* seperti taman, *café*, terminal, bandara, stasiun, perpustakaan dan lain sebagainya, akan tetapi sebagian dari tempat tersebut tidak mempedulikan keamanan layanan yang diberikan. Sehingga layanan yang mereka berikan biasanya mudah *down* atau diserang oleh pengunjung yang jahil dan hasilnya pun tidak hanya merugikan pengunjung lain tapi juga merugikan pengelola tersebut. Untuk itu dibutuhkan sebuah sistem yang dapat memberikan informasi mengenai layanan yang sedang dikelola sehingga kerusakan jaringan dapat diminimalisir.

Fitur *IPS* dan *IDS* ini dapat meningkatkan keamanan dalam *server* sehingga dapat mempersulit serangan yang dilakukan terhadap *server*. *IPS* dapat mencegah serangan yang berlangsung, dan *IDS* dapat memberikan notifikasi kepada *admin* dan mencatat informasi si penyerang dan memasukkan ke dalam *log files.*

Salah satu aplikasi keamanan yang mendukung *IPS* dan *IDS* ini adalah *BRO-IDS* (*Intrusion Detection System*). Aplikasi ini merupakan aplikasi *open source* sehingga dapat dikembangkan dengan bebas oleh para penggunanya. Kelebihan dari aplikasi ini, dapat me*monitoring* jaringan secara *real-time* dan memberikan notifikasi kepada *admin* pengelola jaringan tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka rumusan masalahnya adalah :

1. Bagaimana cara menerapkan *IPS* dan *IDS* pada jaringan atau *server* dengan aplikasi *Bro* ?
2. Bagaimana cara mengintegrasikan *IPS* dan *IDS* menggunakan aplikasi *Bro* dengan *sms gateway* ?
3. Bagaimana memberikan notifikasi ke *admin* mengenai jaringan yang dikelola?

1.3 Tujuan

Tujuan dari penelitian ini adalah :

1. Mengkonfigurasi *IPS* dan *IDS* pada *server* menggunakan aplikasi *Bro* pada *linux CentOS 7*
2. Mengintegrasikan *sms gateway* pada *IPS* dan *IDS* yang telah dikonfigurasi dengan aplikasi *Bro*
3. Memberikan notifikasi kepada *admin* mengenai jaringan yang dikelola saat terjadi serangan maupun saat tidak terjadi serangan.

1.4 Batasan Masalah

Permasalahan yang akan diteliti dibatasi agar penelitian terfokus pada tujuan yang ingin dicapai. Batasan permasalahan dalam penelitian ini adalah :

1. Perangkat lunak yang digunakan dalam membuat sistem ini adalah *Bro*, sedangkan untuk *sms gateway*-nya menggunakan aplikasi *third-party* atau *sms gateway open source* lainnya
2. Sistem Operasi yang digunakan *server Linux CentOS 7 64 bit*

3. Jumlah perangkat yang digunakan sebanyak 3 *PC* (1 sebagai *server* dan 2 sebagai *client*)
4. *Access point* menggunakan *handphone admin*
5. Menggunakan *IP dynamic*
6. Menggunakan aplikasi *Bro-ids* 2.4.1
7. Fitur *Bro-ids* yang digunakan mendeteksi serangan yang berlangsung
8. Fitur *Bro-ids* yang digunakan me*monitoring* jaringan
9. Fitur *Bro-ids* yang digunakan mengirim notifikasi serangan ke *email* lalu diteruskan ke *hanpdhone admin*
10. Pada proyek akhir ini lebih fokus terhadap fungsi *Bro-ids* sebagai *IDS*
11. Menggunakan serangan *DOS* (*Distribute of Service*)
12. Menggunakan serangan *Port Scanner*
13. Menggunakan serangan *FTP Brute-force*
14. Mengirim notifikasi ke *email admin*
15. Mengirim notifikasi ke *handphone admin* saat terjadi serangan
16. Waktu masuknya notifikasi ke *Handphone admin* tergantung dari jaringan yang digunakan.

1.5 Definisi Operasional

Bro Network Monitor Security adalah sebuah aplikasi *open source* yang dikembangkan untuk melindungi *server* ataupun jaringan berbasis *IDS*, aplikasi ini tidak hanya mampu melindungi, tetapi dapat juga menganalisis trafik jaringan. Karena aplikasi ini bersifat *open source*, maka pengguna secara bebas dapat mengembangkan aplikasi ini.

Aplikasi *third-party* adalah : sebuah program perangkat lunak atau perangkat keras yang dikembangkan oleh pihak ketiga yang mengacu pada sistem operasi atau program tertentu untuk mendukung kinerja dari sitem operasi atau program tersebut. Biasanya aplikasi *third party* ini adalah *plugin* atau perangkat lunak untuk aplikasi tertentu.[6]

IFTTT (IF THIS THEN THAT) adalah sebuah aplikasi yang memungkinkan kita untuk menghubungkan 2 aplikasi *web* menjadi satu. Secara sederhana, setiap aktivitas yang kita lakukan secara *online* dapat diatur untuk memiliki reaksi otomatis pada sebuah aplikasi *web* tertentu. *IFTTT* adalah rantai yang dapat menggabungkan aplikasi tersebut dan dapat saling mendukung satu sama lainnya. Cara kerja *IFTTT* ini pada dasarnya membutuhkan 2 hal yaitu pemicu **(*trigger)*** dan reaksi ***(resulting action)*.** [7]

SMS Gateway adalah sebuah sistem aplikasi yang digunakan untuk mengirim atau menerima pesan dari pihak tertentu, aplikasi ini biasanya digunakan untuk melakukan *broadcast* atau promosi kepada kalangan terkait. Untuk *sms gateway* ini dapat berupa jaringan *GSM* atau *CDMA* tergantung dari pemilik sistem tersebut.

1.6 Metode Pengerjaan

Metodologi yang dilakukan untuk menyelesaikan implementasi *IPS* dan *IDS* menggunakan *BRO-IDS* yang terintegrasi dengan *sms gateway* adalah :

a. Studi Pustaka

   Studi pustaka dilakukan dengan cara mencari dan pegumpulan data – data, teori dan informasi yang diambil dari buku – buku yang ada hubungannya dengan masalah yang akan dibahas dalam pengerjaan.

b. Perancangan Sistem

   Pada tahap ini dilakukan perancangan dan pemodelan pada sistem yang akan diuji serta perangkat keras (*hardware*) dan perangkat lunak (*software*) dan kemungkinannya untuk diimplementasikan.

c. Implementasi

Implementasi sistem yang dilakukan sesuai dengan hasil analisa dan perancangan desain sistem. Mengumpulkan data – data parameter yang telah ditentukan dari pengujian implementasi.

d. Pengujian

Melakukan pengujian terhadap sistem yang dibuat apakah sistem sudah berjalan seperti yang diinginkan pada topologi yang telah direncanakan.

e. Analisis pengujian dan penarikan kesimpulan

Melakukan analisis pengujian yang telah didapatkan dari hasil pengujian

f. Penyusunan Laporan

Mendokumentasikan secara keseluruhan atas kegiatan yang telah dilakukan dalam pengerjaan proyek akhir.

1.7 Jadwal Pengerjaan

Tabel 1- 1 Jadwal pengerjaan

Kegiatan	2016															
	April				Mei				Juli				Juli			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Studi Pustaka																
Perancangan Sistem																
Implementasi																
Pengujian																
Analisis Pengujian dan Penarikan Kesimpulan																
Penyusunan Laporan																