BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan jaringan komputer dikategorikan dalam dua bagian, yaitu keamanan secara fisik dan juga keamanan secara non-fisik. Keamanan secara fisik merupakan keamanan yang lebih memfokuskan segala sesuatunya berdasarkan sifat fisiknya (*hardware*). Dalam hal ini misalnya pengamanan komputer agar terhindar dari pencurian dengan mengikatkan *hardware* tersebut ke rantai yang kokoh sehingga fisik komputer tersebut tetap pada tempatnya. Sedangkan keamanan non-fisik adalah keamanan dimana suatu kondisi keamanan yang menitikberatkan pada kepentingan sistem yang berada didalam komputer (*software*). Sebagai contoh yaitu pengamanan data keuangan pada sebuah perusahaan.

Keamanan fisik ataupun non-fisik kedua-duanya sangat penting namun yang terpenting adalah bagaimana cara agar jaringan komputer tersebut terhindar dari gangguan. Gangguan tersebut dapat berupa gangguan dari dalam (internal) ataupun gangguan dari luar (eksternal). Gangguan internal merupakan gangguan yang berasal dari lingkup dalam jaringan infrastruktur tersebut. Gangguan atau serangan internal biasanya lebih sering terjadi pada jaringan sebuah institusi dan menyerang server, data, atau service yang ada, melalui telnet, SSH, DOS, keylogger dan lain-lain. Gangguan eksternal adalah gangguan yang

memang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada.

Maka dari itu, penulis mendesain dan mengimplementasikan bagaimana membuat sebuah sistem keamanan server untuk mencegah penyusup (*intruder*), kemudian melakukan *auto capture* untuk mengetahui terjadinya serangan pada server.

1.2 Rumusan Masalah

Adapun rumusan masalah yang akan dibahas yaitu, bagaimana membuat sebuah sistem keamanan server untuk mencegah penyusup (*intruder*) dan serangan yang dilakukan oleh *attacker*, kemudian melakukan *auto capture* untuk mengetahui terjadinya serangan pada server.

1.3 Batasan Masalah

Desain dan implementasi *auto capture* file log pada *Intrusion Prevention System (IPS)* mempunyai batasan masalah dengan tujuan agar pembahasan tidak melebar dan lebih terperinci. Adapun ruang lingkup permasalahannya antara lain :

1. Konfigurasi Snort dan *packages* tambahan lain agar serangan yang terjadi dapat langsung di *auto capture* oleh sistem yang dibuat.
2. Sistem mengambil contoh jenis gangguan dan pencegahan dari serangan *Ping of Death*.

3. Menggunakan 2 PC/laptop sebagai simulasi, 1 PC menggunakan sistem operasi Ubuntu 13.04 sebagai server yang sudah dikonfigurasi IPS, dan 1 PC menggunakan sistem operasi windows 7 sebagai attacker.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini antara lain :

1. Membangun sistem pencegahan penyusupan atau serangan pada server sekaligus mendokumentasikan hasil serangan kedalam bentuk file yang berekstensi (.txt)
2. Dokumentasi bahwa telah terjadi serangan, kemudian *administrator* bisa menutup celah yang sering diserang oleh *attacker*
3. Mengerti dan memahami jenis-jenis serangan yang dilakukan oleh *attacker*

1.5 Manfaat Penelitian

Manfaat dari penelitian ini agar dicapai dalam pelaksanaannya adalah :

1. *Administrator* tidak perlu membuka file log yang berisi *history* dari serangan-serangan yang telah terjadi
2. Untuk dokumentasi bahwa telah terjadi serangan pada server
3. Meminimalisir terjadinya aktifitas-aktifitas yang merugikan bagi server

1.6 Metode Penelitian

Langkah-langkah dalam melakukan penelitian yang berjudul "*Auto Capture* File Log pada *Intrusion Prevention System* (IPS) saat terjadi serangan pada Jaringan Komputer" ini sebagai berikut:

1.6.1 Metode Pengumpulan data

1.6.1.1 Metode Pustaka

Studi kepustakaan dilakukan melalui informasi dari berbagai media kepustakaan meliputi buku-buku, artikel-artikel, jurnal ilmiah, dan informasi lain dari internet yang berkaitan dengan *auto capture* file log pada *Intrusion Prevention System.*

1.6.2 Metode Pengembangan Sistem

1.6.2.1 Metode Analisis

Metode analisis yang digunakan untuk mengidentifikasi masalah yang terjadi dengan menggunakan analisis kelemahan sistem, setelah mengidentifikasi masalah, selanjutnya adalah solusi penyelesaiannya. Selain itu dibutuhkan juga analisis kebutuan sistem, serta analisis kelayakan sistem.

1.6.2.2 Metode Perancangan

Metode perancangan yang dilakukan menggunakan konsep permodelan sistem seperti, perancangan topology yang dipakai, perancangan *Intrusion Prevention System* dan antar muka *auto capture* file log.

1.6.2.3 Evaluasi Sistem

Evaluasi sistem dilakukan untuk mengetahui apakah sistem yang telah dirancang dan diimplementasikan sudah lebih baik dari sistem sebelumnya

1.7 Sistematika Penelitian

Sistematika penulisan Skripsi ini akan membantu mengarahkan penulisan laporan agar tidak menyimpang dari batasan masalah yang dijadikan sebagai kerangka penulisan dalam mencapai tujuan penulisan laporan Skripsi sesuai dengan apa yang diharapkan. Laporan Penelitian ini disusun secara sistematik kedalam 5 bab, yaitu:

BAB I PENDAHULUAN

Bab ini berisi mengenai gambaran umum tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, manfaat dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas mengenai dasar-dasar teori proses perangkat lunak yang digunakan untuk pembuatan *auto capture* file log pada *intrusion prevention system* (IPS) saat terjadi serangan pada jaringan komputer.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi penjelasan tentang analisis sistem yang terdiri dari mendifinisikan masalah, analisis kebutuhan sistem, analisis kelayakan sistem, skema alur sistem, serta perancangan sistem yang meliputi perancangan aplikasi atau interface.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas tentang uji coba sistem, manual program, manual installasi, implementasi dan pengujian sistem, analisis mengenai hasil dari pengujian koneksi jaringan, serta pengujian *auto capture* file log.

BAB V PENUTUP

Bab ini berisi tentang hasil dan uraian pembahasan aplikasi yang telah dibuat berupa kesimpulan dan saran.

DAFTAR PUSTAKA

Bab ini berisi tentang pustaka yang digunakan penulis sebagai pedoman dan bahan dalam pembuatan skripsi.

LAMPIRAN

Berisi tentang keseluruhan yang digunakan dan listing program dalam desain dan perancangan sistem.

1.8 Rencana Kegiatan Penelitian

Tabel 1.1 Rencana Penelitian

No	Kegiatan	Waktu Pelaksanaan																			
		Oktober				November				Desember				Januari				Februari			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
I	Masa Persiapan																				
	1. Pemilihan Topik																				
	2. Pengumpulan Data																				
II	Masa Penyusunan																				
	3. Analisa Sistem																				
	4. Proses Simulasi																				
	5. Proses Pengujian																				
III	Penulisan Skripsi																				
IV	Pendadaran																				