BAB I
PENDAHULUAN

1.1 Latar Belakang

Faktor keamanan merupakan hal mutlak yang harus diperhatikan dalam membangun suatu jaringan. Sistem keamanan yang dimiliki oleh sistem operasi tidaklah cukup untuk digunakan dalam pengamanan dari serangan *cracker*. Administrator merupakan salah satu hal yang dapat mempengaruhi kehandalan suatu aspek keamanan pada jaringan. Peran seorang administrator sangat dibutuhkan dalam mengatur sistem agar serangan *cracker* bisa diminimalisir. Satu hal yang tidak bisa terlepas dari seorang administrator dalam menjaga keamanan suatu jaringan adalah dengan melakukan audit log. Pada umumnya seorang administrator membutuhkan waktu yang cukup lama untuk mengaudit log sistem untuk mengetahui suatu kejanggalan pada jaringan atau terjadi serangan dari *cracker*.

Untuk mengatasi masalah diatas perlu diterapkan suatu tindakan pengamanan jaringan yang dapat mendeteksi serangan *cracker* dan mengamankan sistem. IPS merupakan suatu sistem perpaduan antara IDS dan *firewall* yang dapat digunakan mengamankan suatu sistem dengan mendeteksi serangan secara dini disertai dengan tindakan pengamanan lebih lanjut. Pada proyek akhir ini digunakan Snort IDS sebagai pendeteksi serangan dan IPTables *firewall* untuk melakukan *blocking* IP penyerang sebagai tindakan pengamanan.

Pada umumnya seorang administator harus mengkonfigurasi IPS secara manual melalui *console*. Untuk itu diperlukan sebuah media antarmuka yang bisa membantu seorang administator dalam melakukan konfigurasi IPS. Pada proyek akhir ini penulis akan merancang dan mengimplementasikan IPS berbasis web sehingga diharapkan proses konfigurasi-konfigurasi penting bisa dilakukan secara cepat dan efektif melalui web.

1.2 Perumusan Masalah

Rumusan masalah yang akan dibahas dalam Proyek Akhir ini adalah sebagai berikut

1. Bagaimana melindungi sistem dari serangan oleh pihak yang tidak memiliki otoritas?
2. Bagaimana membangun suatu aplikasi web yang dapat membantu admin dalam melakukan konfigurasi sistem dan *update rule* Snort serta menampilkan *alert* dan data serangan dalam bentuk aplikasi web?

1.3 Tujuan

Proyek akhir ini bertujuan untuk membuat aplikasi yang dapat membantu admin dalam mengkonfigurasi sistem dengan rincian sebagai berikut.

1. Merancang dan membangun IPS(*Intrusion Prevention System*) yang mampu melindungi sistem dan mendeteksi serangan dengan melakukan *blocking* terhadap IP penyerang.
2. Merancang dan membangun aplikasi berbasis web yang mampu membantu admin dalam mengkonfigurasi IPS(*Intrusion Prevention System*), yaitu konfigurasi Snort, dan *update rule* Snort serta menampilkan *alert* dan data serangan melalui aplikasi web.

1.4 Batasan Masalah

Proyek akhir ini memiliki beberapa batasan masalah agar pembahasan tidak meluas dari topik, yaitu

1. Sistem Operasi yang digunakan dalam membangun IPS ini adalah Ubuntu 10.04.
2. Perangkat lunak IDS yang digunakan dalam membangun IPS ini adalah Snort 2.8.5.2.
3. Perangkat lunak *firewall* yang digunakan dalam membangun sistem adalah IPTables v1.4.4.
4. Perangkat lunak middleware yang digunakan untuk pembacaan log *alert* snort adalah BlockIT 1.4.3a.
5. Sistem dibangun menggunakan PHP 5.2.6 dan MySQL 5.0.51b.

6. Serangan yang digunakan dalam pengujian adalah Akses Dashboard IPS, *SQL injection, port scanning, DoS attack.*
7. Pengujian tidak dilakukan untuk jenis serangan yang memanipulasi *mac address.*
8. Pengujian menggunakan metode *false positive.*

1.5 Metodologi Penyelesaian

Metoda yang digunakan dalam memecahkan permasalahan-permasalahan dalam Proyek Akhir ini, yaitu :

1. Studi Literatur

   Pada tahap ini dilakukan pengumpulan data dan informasi yang digunakan untuk mendukung proses perancangan sistem.

2. Analisis dan Perancangan Sistem

   Analisis kebutuhan serta perancangan dilakukan untuk menunjang pembangunan sistem yang akan dibuat untuk menjawab tujuan yang terpapar pada bab 1. Analisis dilakukan mulai dari analisis *hardware* sampai analisis *software* yang dibutuhkan dalam pembangunan sistem ini. Selain itu perancangan sistem dilakukan untuk memberikan gambaran umum terhadap sistem yang akan dibangun atau dibuat.

3. Pembangunan Sistem

   Pembangunan sistem beracuan pada hasil analisis dan perancangan desain. Selain itu pembangunan sistem ini juga beracuan pada metodologi dan parameter yang digunakan untuk membangun sistem yang berguna untuk memenuhi tujuan dari sistem tersebut.

4. Pengujian Sistem

   Pada tahap pengujian, sistem yang sudah dibangun akan diuji dengan cara melakukan tes *blackbox*, yaitu menguji fungsionalitas menu yang ada pada aplikasi web terhadap user-user yang ada. Selain itu juga dilakukan simulasi pengetesan IPS terhadap jenis-jenis serangan yang sudah ditentukan, yaitu Akses Dashboard IPS, *SQL injection, port scanning,* dan *DoS attack.*

1.6 Sistematika Penulisan

Adapun sistematika penulisan proyek akhir sebagai berikut.

1. BAB I PENDAHULUAN

   Berisi latar belakang masalah, tujuan penulisan, rumusan masalah dan batasannya, metodologi penyelesaian masalah yang digunakan serta sistematika penulisan yang memuat susunan penulisan proyek akhir ini.

2. BAB II LANDASAN TEORI

   Pada bab ini menguraikan tentang landasan teori yang mendukung dan mendasari dalam penulisan proyek akhir ini, yaitu mengenai pembuatan aplikasi berbasis web untuk mendukung IPS.

3. BAB III PERANCANGAN SISTEM

   Bab ini berisi tentang perancangan dari aplikasi berbasis web untuk IPS.

4. BAB IV IMPLEMENTASI DAN PENGUJIAN

   Bab ini berisi tentang implementasi dari sistem serta pengujian terhadap sistem.

5. BAB V SIMPULAN DAN SARAN

   Berisi mengenai simpulan dari penulisan proyek akhir serta saran untuk pengembangan lebih lanjut.

1.7 Jadwal Kegiatan

Tabel 1.1 Jadwal Kegiatan

Kegiatan	Juni 2011				Juli 2011				Agustus 2011			
	1	2	3	4	1	2	3	4	1	2	3	4
Studi Literatur												
Analisis & Perancangan Sistem												
Pembangunan Sistem												
Pengujian Sistem												
Pembuatan Laporan												