BAB 1
PENDAHULUAN

1.1 Latar Belakang

Pada era teknologi informasi ini keamanan menjadi salah satu faktor penting dalam pengelolaan dan penggunaan aplikasi. Faktor keamanan menjadi sangat penting dalam pengelolaan jaringan. Ancaman serangan seperti *DOS, malware,* dan serangan yang bertujuan meretas lainnya membuat keamanan jaringan perlu ditingkatkan. Dalam upaya mencegah serangan tersebut dan meningkatkan keamanan jaringan digunakan IDS atau *Intrusion Detection System.*

Snort merupakan salah satu aplikasi IDS yang umum digunakan dalam memonitor aktivitas dari jaringan. *Snort* mendokumentasikan setiap aktivitas yang terjadi pada jaringan, sehingga serangan atau aktivitas yang mencurigakan pada jaringan dapat diketahui oleh aplikasi ini. Namun, dokumentasi atau *log* dari *snort* tidak mudah dibaca bagi orang awam, sehingga menyulitkan pengelola jaringan dalam melakukan analisis, *maintenance*, dan perbaikan jaringan.

Pembacaan data *alert* atau *log* dari *snort* yang manual membuat perbaikan dan *maintenance* jaringan tidak efektif. Aktivitas mencurigakan atau serangan yang tercatat dalam *log* yang berjenis teks masih perlu dianalisis dikarenakan tidak disebutkan jenis serangan, tingkat ancaman pada jaringan, dan solusi perbaikan jaringan. Hal tersebut dapat menyebabkan kebingungan pada pengelola dan ancaman pada jaringan yang perlu diperbaiki atau ditingkatkan keamanannya dengan segera.

Solusi, klasifikasi jenis, dan tingkat ancaman dari permasalahan yang tercatat dalam *log* sangat penting, hal tersebut diperlukan dalam proses meningkatkan keamanan jaringan untuk mencegah dan minimalisir serangan atau ancaman yang akan datang. Pengelolaan jaringan pun akan jadi lebih mudah dan cepat.

Berdasarkan permasalahan tersebut, akan dibuat sebuah aplikasi berbasis *web* untuk membantu pembacaan data *log* IDS, sehingga ancaman atau serangan yang tercatat dalam *log* dapat dikategorikan dan diberikan solusinya. Selain itu, proses analisis dan pengelolaan jaringan menjadi lebih cepat. Sehingga

selanjutnya ancaman dan serangan dapat dicegah dan tingkat keamanan jaringan dapat meningkat.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam tugas akhir ini adalah sebagai berikut:

1. Bagaimana cara aplikasi membantu administrator untuk mengetahui tingkat ancaman dan jenis serangan aktivitas jaringan yang tercatat?
2. Bagaimana cara aplikasi membantu administrator dalam menangani aktivitas jaringan yang tercatat dengan tingkat ancaman serius?

1.3 Tujuan Pembahasan

Berdasarkan rumusan masalah, maka tujuan dari tugas akhir ini adalah sebagai berikut:

1. Membuat aplikasi berbasis *web* yang menampilkan data *log* ke dalam bentuk kategorial dan klasifikasi kelompok untuk meningkatkan kemudahan pengguna dalam membaca data *log Snort*.
2. Membuat aplikasi berbasis *web* yang memberikan saran perbaikan untuk meningkatkan pengetahuan pengguna dalam menyelesaikan masalah yang ada.

1.4 Ruang Lingkup

Perangkat lunak yang dibutuhkan dalam membuat aplikasi ini adalah sebagai berikut:

a. Snort 2.9.8.2
b. Barnyard2 2.1.14
c. PulledPork
d. Bahasa pemrograman PHP 5.6
e. MySQL 5.6.14
f. PHPMyAdmin
g. Eclipse PHP Mars 2.0

1.5 Sumber Data

1. Data Primer

Data yang didapat dari dokumentasi atau *log* alat IDS dalam studi kasus ini yaitu *Snort*.

2. Data Sekunder

Data yang diperoleh dari *e-book, literature*, tutorial, dan internet sebagai pendukung dari data primer.

1.6 Sistematika Penyajian

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang masalah, rumusan masalah, tujuan pembahasan, ruang lingkup kajian dan sistematika pembahasan dari penelitian yang dilakukan.

BAB II KAJIAN TEORI

Bab ini membahas mengenai teori-teori yang melandasi dan mendukung terhadap penelitian yang dilakukan.

BAB III ANALISIS DAN RANCANGAN SISTEM

Bab ini membahas mengenai perancangan aplikasi dan desain sistem dalam tugas akhir ini.

BAB IV HASIL PENELITIAN

Bab ini berisi kumpulan *screenshot* dari aplikasi yang telah dibuat dan penjelasan dari setiap gambar.

BAB V PEMBAHASAN

Bab ini berisi laporan dan hasil uji aplikasi yang dilakukan dengan menggunakan metode *Blackbox Testing*.

BAB VI PENUTUP

Bab ini berisi simpulan dari hasil penelitian yang penulis dapat, dan saran yang penulis usulkan untuk lebih mengembangkan penelitian ini di masa yang akan datang.