ABSTRAK

Keamanan menjadi salah satu faktor penting di era teknologi informasi ini. Maraknya serangan pada jaringan membuat data yang berupa informasi penting dapat dieksploitasi dan kelancaran jaringan dapat terganggu. Penggunaan IDS atau *Intrusion Detection System* mampu mendeteksi serangan yang mengancam jaringan, sehingga tingkat keamanan pada jaringan dapat meningkat. *Snort* merupakan salah satu IDS yang umum digunakan, namun pembacaan data *log* dengan menggunakan *console* akan menyulitkan pengguna jika data *log* yang tersimpan sangat banyak. Oleh karena itu, penelitian ini dilakukan agar pembacaan dan analisis data *log* pada *Snort* menjadi lebih mudah. Aplikasi dibuat dengan menggunakan bahasa pemrograman PHP dan basis data MySQL. Aplikasi bergantung pada *Barnyard2* sebagai aplikasi untuk menyimpan data *log* ke dalam MySQL dan *PulledPork* sebagai aplikasi untuk menambahkan *rule* pada *Snort* secara otomatis. Hasil penelitian menunjukkan bahwa aplikasi mampu membantu pengguna dalam membaca data *log Snort* dan juga membantu pengguna dalam memahami serangan yang ditemukan dan cara menyelesaikan masalah yang ada.

Kata kunci: IDS, jaringan, PHP, sekuritas, *Snort*, *website*.

ABSTRACT

Security becomes one of the main factor in this information technology era. A lot of attacks toward networks cause data exploitation and network traffic disturbance. The use of IDS or Intrusion Detection System helps detect attacks that endanger the security of a network, so that the security level can be increased. Snort is one of the example of IDS that is commonly used, but reading its log data via console can become a hardship for some users if the data is too large. So, the purpose of this research is to make Snort's log reading and analyzing becomes easier. This application created with the use of PHP programming language and MySQL database. This application needs Barnyard2 as log saving to MySQL database and PulledPork as rule automatic updating. The result of this research shows that the application can helps users reading the log and understanding the attacks and how to resolve it.

Keywords: IDS, networking, PHP, network security, Snort, website.

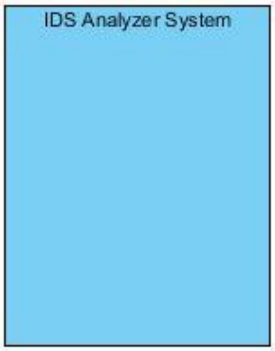
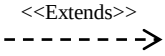
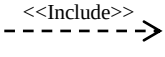
DAFTAR ISI

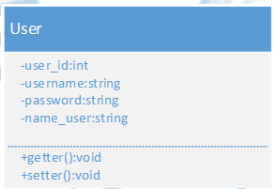
DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE PROGRAM

DAFTAR NOTASI/ LAMBANG

Jenis	Notasi/Lambang	Nama Gambar	Arti
Use Case		*System Boundary*	Untuk menggambarkan jangkauan sistem dan memberikan alternatif pilihan sistem
Use Case		*Actor*	*Actor* mempresentasikan seseorang atau sesuatu yang berinteraksi dengan sistem
Use Case		*Communication*	Tujuan komunikasi adalah untuk memperlihatkan bahwa sebuah *actor* terlibat dalam *usecase*
Use Case		*Generalization*	Relasi antara dua *actor* atau dua *usecase* dimana salah satunya menurunkan, menambahkan atau *override* sifat dari yang lainnya
Use Case		*Extend*	Ekstensi *use case* tambahan dari *use case* utama
Use Case		*Include*	Perilaku yang sama dari satu atau banyak *use case* dengan merujuk sebagai instansi yang berbeda

Jenis	Notasi/Lambang	Nama Gambar	Arti
Use Case		*Usecase*	Gambaran fungsionalitas dari satu sistem, sehingga pengguna dapat memahami guna dari sistem
Activity Diagram		*Start/Initial State*	Titik awal
Activity Diagram		*End/Final State*	Titik akhir
Activity Diagram		*Activity/Action State*	Menunjukkan satu proses
Activity Diagram		*Decision*	Pemilihan keputusan
Activity Diagram		*Control Flow*	Perpindahan dari proses yang satu ke proses lainnya
Class Diagram		*Class*	Kelas mendeskripsikan berbagai jenis objek yang dapat dimiliki oleh sistem
Class Diagram		*Aggregation*	Menunjukkan bahwa kelas dapat memiliki koleksi dari kelas lainnya

Referensi:

Notasi/ Lambang dari *Learning UML 2.0* [1]