

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 PuledPork 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

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN.....	ii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN.....	iii
PRAKATA.....	iv
ABSTRAK.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xiii
DAFTAR TABEL.....	xv
DAFTAR KODE PROGRAM.....	xvi
DAFTAR NOTASI/ LAMBANG.....	xvii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Pembahasan	2
1.4 Ruang Lingkup.....	2
1.5 Sumber Data.....	3
1.6 Sistematika Penyajian	3
BAB 2 KAJIAN TEORI	4
2.1 <i>Intrusion Detection System</i>	4
2.1.1 <i>Host-Based IDS</i>	4
2.1.2 <i>Network-Based IDS</i>	5
2.1.3 <i>Alerts dan Logs</i>	5
2.2 <i>Detection Philosophies</i>	6

2.2.1 <i>Signature-Based IDS</i>	6
2.2.2 <i>Anomaly-Based IDS</i>	7
2.3 <i>Snort</i>	7
2.3.1 <i>Tabel Basis Data Snort</i>	8
2.3.2 <i>Skema Basis Data Snort</i>	8
2.4 <i>Barnyard2</i>	9
2.5 <i>PulledPork</i>	10
2.6 <i>PHP IDS Analyzer</i>	10
2.6.1 <i>BASE</i>	10
2.6.2 <i>ACID</i>	10
2.7 <i>UML</i>	11
2.7.1 <i>Use Case</i>	11
2.7.2 <i>Activity Diagram</i>	12
2.7.3 <i>Class Diagram</i>	12
2.8 <i>PHP</i>	12
2.9 <i>HTML</i>	13
2.10 <i>CSS</i>	13
2.11 <i>Javascript</i>	13
2.12 <i>MySQL</i>	13
BAB 3 ANALISIS DAN RANCANGAN SISTEM	15
3.1 <i>Analisis</i>	15
3.2 <i>Topologi</i>	16
3.3 <i>Pemodelan Perangkat Lunak</i>	17
3.3.1 <i>Use Case IDS Log Viewer System</i>	17
3.3.2 <i>Activity Diagram</i>	18
3.3.2.1 <i>Activity Diagram Login</i>	18

3.3.2.2	<i>Activity Diagram</i> Konfigurasi Basis Data.....	18
3.3.2.3	<i>Activity Diagram</i> Lihat Rangkuman <i>Event</i>	19
3.3.2.4	<i>Activity Diagram</i> Lihat <i>Event</i> Berdasarkan Tingkat Ancaman.....	20
3.3.2.5	<i>Activity Diagram</i> Lihat <i>Event</i> Berdasarkan Grafik	21
3.3.2.6	<i>Activity Diagram</i> Lihat <i>Event</i>	21
3.3.2.7	<i>Activity Diagram</i> <i>Sorting Event</i>	22
3.3.2.8	<i>Activity Diagram</i> Cari <i>Event</i>	23
3.3.2.9	<i>Activity Diagram</i> Lihat Detil <i>Event</i>	23
3.3.2.10	<i>Activity Diagram</i> Buat Report.....	24
3.3.2.11	<i>Activity Diagram</i> Ekspor <i>Event</i>	25
3.3.2.12	<i>Activity Diagram</i> Lihat <i>Signature</i>	25
3.3.2.13	<i>Activity Diagram</i> Tambah Rekomendasi	26
3.3.2.14	<i>Activity Diagram</i> Ubah Rekomendasi.....	27
3.3.2.15	<i>Activity Diagram</i> Ubah <i>User</i>	28
3.3.3	<i>Class Diagram</i>	29
3.3.3.1	<i>Class</i> Sensor	29
3.3.3.2	<i>Class</i> <i>Signature</i>	30
3.3.3.3	<i>Class</i> <i>User</i>	31
3.3.3.4	<i>Class</i> <i>Recommendation</i>	31
3.3.3.5	<i>Class</i> <i>Reference</i>	31
3.3.3.6	<i>Class</i> <i>Events</i>	32
3.3.3.7	<i>Class</i> <i>Iphdr</i>	33
3.3.3.8	<i>Class</i> <i>Tcphdr</i>	33
3.3.3.9	<i>Class</i> <i>MainView</i>	34
3.3.3.10	<i>Class</i> <i>Event</i> DAO	35
3.3.3.11	<i>Class</i> <i>Recommendation</i> DAO	36

3.3.3.12 <i>Class Reference</i> DAO	37
3.3.3.13 <i>Class Sensor</i> DAO	37
3.3.3.14 <i>Class Signature</i> DAO.....	37
3.3.3.15 <i>Class User</i> DAO	38
3.3.4 <i>Entity Relationship Diagram</i>	38
3.4 Rancangan Antarmuka	40
3.4.1 Rancangan Antarmuka <i>Form Login</i>	40
3.4.2 Rancangan Antarmuka <i>Form Configure Database</i>	40
3.4.3 Rancangan Antarmuka <i>Dashboard</i>	41
3.4.4 Rancangan Antarmuka <i>Tabel Event</i>	42
3.4.5 Rancangan Antarmuka <i>Detil Event</i>	43
3.4.6 Rancangan Antarmuka <i>Form Advanced Search</i>	44
3.4.7 Rancangan Antarmuka <i>Report</i>	44
3.4.8 Rancangan Antarmuka <i>Setting</i>	45
3.4.9 Rancangan Antarmuka <i>Tabel Signature</i>	46
3.4.10 Rancangan Antarmuka <i>Form Tambah Recommendation</i>	46
3.4.11 Rancangan Antarmuka <i>Form Update Recommendation</i>	47
BAB 4 IMPLEMENTASI.....	48
4.1 Tampilan Aplikasi.....	48
4.1.1 Tampilan <i>Form Login</i>	48
4.1.2 Tampilan <i>Form Configure Database</i>	49
4.1.3 Tampilan Antarmuka <i>Dashboard</i>	51
4.1.4 Tampilan <i>Tabel Event</i>	53
4.1.5 Tampilan Antarmuka <i>Detil Event</i>	54
4.1.6 Tampilan <i>Form Advanced Search</i>	55
4.1.7 Tampilan Antarmuka <i>Report</i>	56

4.1.8 Tampilan Antarmuka <i>Setting</i>	57
4.1.9 Tampilan Tabel <i>Signature</i>	59
4.1.10 Tampilan <i>Form</i> Tambah Rekomendasi.....	60
4.1.11 Tampilan <i>Form Update</i> Rekomendasi	62
4.2 Implementasi <i>Entity Relationship Diagram</i>	63
BAB 5 PENGUJIAN.....	64
5.1 Pengujian <i>Login</i>	64
5.2 Pengujian Konfigurasi Basis Data	64
5.3 Pengujian Menu <i>Dashboard</i>	65
5.4 Pengujian Menu <i>Event</i>	66
5.5 Pengujian Menu <i>Advanced Search</i>	67
5.6 Pengujian <i>Update User</i>	67
5.7 Pengujian Tambah Rekomendasi.....	68
5.8 Pengujian <i>Update</i> Rekomendasi	69
5.9 Hasil Angket.....	69
BAB 6 SIMPULAN DAN SARAN	73
6.1 Simpulan	73
6.2 Saran.....	73
DAFTAR PUSTAKA	A-0

DAFTAR GAMBAR

Gambar 2.1 Contoh Penulisan <i>Signature</i>	6
Gambar 2.2 Alur Kerja Komponen <i>Snort</i>	7
Gambar 2.3 Skema Basis Data <i>Snort</i>	9
Gambar 2.4 Contoh Penggunaan <i>Barnyard2</i>	10
Gambar 3.1 Topologi Penelitian	16
Gambar 3.2 <i>Use Case IDS Log Analysis System</i>	17
Gambar 3.3 <i>Activity Diagram Login</i>	18
Gambar 3.4 <i>Activity Diagram</i> Konfigurasi Basis Data	19
Gambar 3.5 <i>Activity Diagram</i> Lihat Rangkuman <i>Event</i>	20
Gambar 3.6 <i>Activity Diagram</i> Lihat <i>Event</i> Berdasarkan Tingkat Ancaman	20
Gambar 3.7 <i>Activity Diagram</i> Lihat <i>Event</i> Berdasarkan Grafik	21
Gambar 3.8 <i>Activity Diagram</i> Lihat <i>Event</i>	22
Gambar 3.9 <i>Activity Diagram</i> <i>Sorting Event</i>	22
Gambar 3.10 <i>Activity Diagram</i> Cari <i>Event</i>	23
Gambar 3.11 <i>Activity Diagram</i> Lihat Detil <i>Event</i>	24
Gambar 3.12 <i>Activity Diagram</i> Buat <i>Report</i>	24
Gambar 3.13 <i>Activity Diagram</i> Ekspor <i>Event</i>	25
Gambar 3.14 <i>Activity Diagram</i> Lihat <i>Signature</i>	26
Gambar 3.15 <i>Activity Diagram</i> Tambah Rekomendasi	26
Gambar 3.16 <i>Activity Diagram</i> Ubah Rekomendasi	27
Gambar 3.17 <i>Activity Diagram</i> Ubah <i>User</i>	28
Gambar 3.18 Kelas Diagram Aplikasi	29
Gambar 3.19 Kelas <i>Sensor</i>	30
Gambar 3.20 Kelas <i>Signature</i>	30
Gambar 3.21 Kelas <i>User</i>	31
Gambar 3.22 Kelas <i>Recommendation</i>	31
Gambar 3.23 Kelas <i>Reference</i>	32
Gambar 3.24 Kelas <i>Events</i>	32
Gambar 3.25 Kelas <i>Iphdr</i>	33
Gambar 3.26 Kelas <i>Tcphdr</i>	34

Gambar 3.27 Kelas <i>Main View</i>	35
Gambar 3.28 Kelas <i>Event Dao</i>	36
Gambar 3.29 Kelas <i>Recommendation Dao</i>	36
Gambar 3.30 Kelas <i>Reference Dao</i>	37
Gambar 3.31 Kelas <i>Sensor Dao</i>	37
Gambar 3.32 Kelas <i>Signature Dao</i>	38
Gambar 3.33 Kelas <i>User Dao</i>	38
Gambar 3.34 <i>Entity Relationship Diagram</i> Aplikasi	39
Gambar 3.35 Rancangan Antarmuka <i>Form Login</i>	40
Gambar 3.36 Rancangan Antarmuka <i>Form Configure Database</i>	41
Gambar 3.37 Rancangan Antarmuka <i>Dashboard</i>	42
Gambar 3.38 Rancangan Antarmuka Tabel <i>Event</i>	42
Gambar 3.39 Rancangan Antarmuka Detil <i>Event</i>	43
Gambar 3.40 Rancangan Antarmuka <i>Form Advanced Search</i>	44
Gambar 3.41 Rancangan Antarmuka <i>Report</i>	45
Gambar 3.42 Rancangan Antarmuka <i>Setting</i>	45
Gambar 3.43 Rancangan Antarmuka Tabel <i>Signature</i>	46
Gambar 3.44 Rancangan Antarmuka <i>Add Recommendation</i>	47
Gambar 3.45 Rancangan Antarmuka <i>Update Recommendation</i>	47
Gambar 4.1 Tampilan <i>Form Login</i>	48
Gambar 4.2 Tampilan <i>Form Configure Database</i>	50
Gambar 4.3 Tampilan Antarmuka <i>Dashboard</i>	51
Gambar 4.4 Tampilan Tabel <i>Event</i>	53
Gambar 4.5 Tampilan Antarmuka Detil <i>Event</i>	55
Gambar 4.6 Tampilan <i>Form Advanced Search</i>	56
Gambar 4.7 Tampilan Antarmuka <i>Report</i>	57
Gambar 4.8 Tampilan Antarmuka <i>Setting</i>	58
Gambar 4.9 Tampilan Tabel <i>Signature</i>	60
Gambar 4.10 Tampilan <i>Form Tambah Rekomendasi</i>	61
Gambar 4.11 Tampilan <i>Form Update Rekomendasi</i>	62
Gambar 4.12 Implementasi <i>Entity Relationship Diagram</i>	63

DAFTAR TABEL





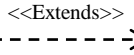
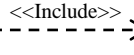
Tabel 2.1 Deskripsi Basis Data <i>Snort</i>	8
Tabel 5.1 Pengujian <i>Login</i>	64
Tabel 5.2 Pengujian Konfigurasi Basis Data	65
Tabel 5.3 Pengujian Menu <i>Dashboard</i>	65
Tabel 5.4 Pengujian Menu <i>Event</i>	66
Tabel 5.5 Pengujian Menu <i>Advanced Search</i>	67
Tabel 5.6 Pengujian <i>Update User</i>	68
Tabel 5.7 Pengujian Tambah Rekomendasi	68
Tabel 5.8 Pengujian <i>Update</i> Rekomendasi	69
Tabel 5.9 Hasil Angket Kategori Kemudahan	70
Tabel 5.10 Hasil Angket Kategori Solusi	71







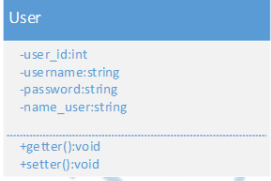



DAFTAR KODE PROGRAM

Kode Program 4.1 <i>Login</i>	49
Kode Program 4.2 Konfigurasi Basis Data	50
Kode Program 4.3 Lihat Rangkuman <i>Event</i>	52
Kode Program 4.4 Lihat <i>Event</i> Berdasarkan Tingkat Ancaman	52
Kode Program 4.5 Lihat <i>Event</i> Berdasarkan Grafik	52
Kode Program 4.6 Lihat <i>Event</i>	54
Kode Program 4.7 <i>Sorting Event</i>	54
Kode Program 4.8 Lihat Detil <i>Event</i>	55
Kode Program 4.9 <i>Search Event</i>	56
Kode Program 4.10 Buat Report.....	57
Kode Program 4.11 Ubah <i>User</i>	58
Kode Program 4.12 Ekspor <i>Event</i>	59
Kode Program 4.13 Lihat <i>Signature</i>	59
Kode Program 4.14 Tambah Rekomendasi	61
Kode Program 4.15 Ubah Rekomendasi.....	62

DAFTAR NOTASI/ LAMBANG

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

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

Referensi:

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