UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISA SECURITY INFORMATION MANAGEMENT MENGGUNAKAN OSSIM PADA SEBUAH PERUSAHAAN

SKRIPSI

OLEH

MOEHAMAD RIHAL

06 06 07 8411

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK KOMPUTER

UNIVERSITAS INDONESIA

JUNI 2010

UNIVERSITAS INDONESIA

IMPLEMENTASI DAN ANALISA SECURITY INFORMATION MANAGEMENT MENGGUNAKAN OSSIM PADA SEBUAH PERUSAHAAN

SKRIPSI

DIAJUKAN SEBAGAI SALAH SATU SYARAT UNTUK MEMPEROLEH GELAR SARJANA TEKNIK

OLEH

MOEHAMAD RIHAL

06 06 07 8411

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK KOMPUTER

UNIVERSITAS INDONESIA

JUNI 2010

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	**: Moehamad Rihal**
NPM	**: 0606078411**
Tanda Tangan	**:** 
Tanggal	**: 12 Juni 2010**

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh

Nama	: Moehamad Rihal
NPM	: 06078411
Program Studi	: Teknik Komputer
Judul Skripsi	: Implementasi dan Analisa *Security Information Management* Dengan Menggunakan OSSIM Pada Sebuah Perusahaan

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer, Fakultas Teknik Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Prima Dewi Purnamasari ST, MT, MSc	( )
Penguji	: Muhammad Salman S.T, MIT	( )
Penguji	: Ir. Endang Sriningsih MT,Si	( )

Ditetapkan di : Depok

Tanggal : 8 Juli 2010

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kehadirat Allah SWT, karena atas segala rahmat dan hidayat-Nya saya dapat menyelesaikan skripsi ini. Saya menyadari bahwa skripsi ini tidak akan terselesaikan tanpa bantuan dari berbagai pihak. Oleh karena itu, saya mengucapkan terima kasih kepada :

1. Ibu Prima Dewi Purnamasari ST, MT, MSc selaku pembimbing skripsi ini, yang telah meluangkan waktunya, serta masukan-masukan selama bimbingan;
2. Bapak Sudiro, Bapak Paryono Yuniarto, Bapak Susanto, Bapak Kusni dan karyawan lainnya selaku pihak Perusahaan yang telah banyak membantu dalam usaha memperoleh data;
3. Orang tua dan keluarga terutama Ayah saya yang selalu memberi nasehat dan memotivasi saya untuk selalu berusaha keras dan semangat dalam setiap pekerjaan yang dilakukan;
4. Teman – teman terima kasih atas bantuan, dan motivasi yang diberikan pada saya dalam menyelesaikan skripsi ini;
5. Dan seluruh Sivitas Akademik Departemen Teknik Elektro yang tidak dapat saya sebutkan satu persatu.

Akhir kata, semoga Allah SWT berkenan membalas kebaikan semua pihak yang telah membantu. Semoga skripsi ini bermanfaat bagi perkembangan ilmu pengetahuan.

Depok, 12 Juni 2010

Moehamad Rihal

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Moehamad Rihal
NPM : 0606078411
Program Studi : Teknik Komputer
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

IMPLEMENTASI DAN ANALISA SECURITY INFORMATION MANAGEMENT MENGGUNAKAN OSSIM PADA SEBUAH PERUSAHAAN

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 12 Juni 2010
Yang menyatakan

(Moehamad Rihal)

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

ABSTRAK

Nama : Moehamad Rihal

Program Studi : Teknik Komputer

Judul : IMPLEMENTASI DAN ANALISA SECURITY INFORMATION MANAGEMENT MENGGUNAKAN OSSIM PADA SEBUAH PERUSAHAAN

Semakin banyak peralatan keamanan jaringan yang diimplementasikan, maka semakin banyak pula peralatan yang perlu dikelola dan dipantau. Semakin banyak peralatan yang dipasang maka semakin banyak *log-log* yang dihasilkan. *Security Information Management* (SIM) berfungsi menyediakan informasi yang terkait dengan keamanan jaringan secara terpusat.

Pada skripsi ini dimplementasikan sistem aplikasi *security information management* menggunakan OSSIM pada sebuah perusahaan dengan mengintegrasikan OSSIM dengan perangkat keamanan jaringan seperti IDP dan *firewall*. Pada skripsi ini juga dilakukan pemantauan terhadap trafik TCP, UDP dan ICMP selama satu pekan, dan melakukan skenario serangan ICMP *flooding* ke server OSSIM selama beberapa menit kemudian dianalisis kondisi jaringan pada hari tersebut.

Rata-rata trafik protokol baik TCP, UDP dan ICMP selama satu minggu menunjukkan bahwa pada saat jam kerja lebih tinggi dibandingkan pada saat bukan jam kerja. Rata-rata trafik TCP pada jam kerja lebih besar 74,85 kb (12,1 %), rata-rata trafik UDP lebih besar 50,6 kb/s (54,1 %) dan rata-rata trafik ICMP pada jam kerja lebih besar 19,1 b/s (7,6 %). Melalui skenario serangan Ping *flooding* ICMP ke server OSSIM menunjukkan bahwa OSSIM dapat mendeteksi serangan secara real-time melalui pengamatan trafik jaringan dan laporan SIEM *event*.

Kata Kunci : *Log*, *Security Information Management (SIM)*, OSSIM Pemantauan, ICMP *flooding*

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

ABSTRACT

Name : Moehamad Rihal

Study Program : Computer Engineering

Title : IMPLEMENTATION AND ANALYSIS OF SECURITY INFORMATION MANAGEMENT IN A COMPANY USING OSSIM

The more devices implemented in network security, the more devices are needed to be managed and monitored. Security Information Management (SIM) provides information which is related to centered security network.

In this final project, it has been implemented a SIM application system in a company by integrating OSSIM with security network devices such as IDP and firewall. Traffic monitoring for TCP, UDP and ICMP has been conducted for a week. An attacking scenario with ICMP flooding to OSSIM server has also been conducted for a few minutes and then the network condition for that day are analyzed.

The average of the traffic protocol of TCP, UDP and ICMP in a week are higher in the working hour than non-working hour. The average of TCP traffic at the working hour greater than 74.85 kb/s (12.1 %), UDP greater than 50.6 kb/s (54.1 %) and for ICMP greater than 19.1 b/s (7.6 %). From the flooding attack scenario, OSSIM can detect the attacking in real-time through the traffic monitoring and SIEM event report.

Keywords: Log, Security Information Management (SIM), OSSIM, Monitoring, ICMP flooding

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

DAFTAR ISI

HALAMAN JUDUL i
PERNYATAAN ORISINALITAS ii
LEMBAR PENGESAHAN iii
KATA PENGANTAR iv
LEMBAR PERSETUJUAN PUBLIKASI v
ABSTRAK vi
ABSTRACT vii
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xiii
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Tujuan 3
1.3 Batasan Masalah 4
1.4 Metode Penelitian 4
1.5 Sistematika Penulisan 4
BAB 2 OSSIM (Open Source Security Information Management) 6
2.1 Manajemen Jaringan 6
2.1.1 Network Intrusion Detection 10
2.1.2 Risk Management 11
2.1.2.1 Risk Assesment 11
2.1.2.2 Threat Identification 12
2.1.2.3 Risk Mitigation 12

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2.1.2.4 Evaluation dan Assessment 12
2.1.3 ISMS (Information Security Management System) 13
2.2 OSSIM 14
2.2.1 Sekilas Tentang OSSIM 14
2.2.2 Arsitektur OSSIM 15
2.2.2.1 Sensor 16
2.2.2.2 Manajemen Server 17
2.2.2.3 Database 17
2.2.2.4 Frontend 17
2.2.3 Kegunaan OSSIM 18
2.2.3.1 Detektor 18
2.2.3.2 Monitor 20
2.2.3.3 Vulnerability Scanners 21
2.2.3.4 Automatic Inventory 22
2.2.3.5 Collector System 22
2.2.4 Correlation 22
2.2.4.1 Logical Correlation 22
2.2.4.2 Cross Correlation 23
2.2.4.3 Inventory Correlation 23
2.3 Firewall dan NSM 23
BAB 3 PERANCANGAN IMPLEMENTASI OSSIM PADA JARINGAN 25
3.1 Identifikasi Masalah Pada Perusahaan 25
3.2 Perancangan Implementasi OSSIM Pada Perusahaan 26
3.2.1 Arsitektur Umum 27

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

3.2.2 Deskripsi dari Sistem 28
3.3 Rancangan Skenario Penelitian 30
BAB 4 IMPLEMENTASI DAN UJI COBA SISTEM PADA JARINGAN 32
4.1 Implementasi 32
4.1.1 Spesifikasi Perangkat Server OSSIM 32
4.1.2 Konfigurasi 33
4.1.2.1Konfigurasi Host 33
4.1.2.2 Konfigurasi Jaringan 34
4.1.2.3 Konfigurasi Policy 35
4.1.2.4 Konfigurasi Directive Rule 35
4.1.2.5 Konfigurasi Korelasi antar Detektor 38
4.1.2.6 Konfigurasi Perangkat IDP dan Firewall 38
4.2 Pengambilan Data dan Analisis 40
4.2.1 Trafik Jaringan 40
4.2.2 Data dan Analisis Pengamatan SIEM *event* Untuk Skenario Serangan 46
BAB 5 KESIMPULAN 52
DAFTAR REFERENSI 53
Lampiran 1 54
Lampiran 2 55

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

DAFTAR GAMBAR

Gambar 1.1 Faktor-faktor penyebab network down 2

Gambar 2.1 *Enterprise Design* Infrastruktur Jaringan 6

Gambar 2.2 Kabel-kabel dan peralatan pada jaringan 8

Gambar 2.3 Management Life Cycle 9

Gambar 2.4 Elemen-elemen keamanan informasi 14

Gambar 2.5 Ilustrasi kontrol manajemen jaringan secara terpusat 15

Gambar 2.6 Sensor pada OSSIM untuk monitor jaringan 16

Gambar 2.7 Interaksi dari komponen-komponen pada OSSIM 18

Gambar 2.8 Pemantauan jaringan 20

Gambar 2.9 Pemantauan Ketersediaan 21

Gambar 3.1 Topologi Jaringan 27

Gambar 3.2 Arsitektur Diagram OSSIM 28

Gambar 3.3 Diagram Alir Data Dari Sistem 30

Gambar 3.4 Topologi Skenario Ping *flooding* ICMP 31

Gambar 4.1 Server OSSIM 32

Gambar 4.2 Tampilan Dalam Melakukan Pengaturan Host 33

Gambar 4.3 Konfigurasi Jaringan yang Dikelola 34

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Gambar 4.4 Pengaturan Policy Jaringan 35

Gambar 4.5 Rule yang Ditambahkan 36

Gambar 4.6 Plugin SID Snort untuk Directive DOS 37

Gambar 4.7 Korelasi Antar Detektor 38

Gambar 4.8 Konfigurasi Firewall 39

Gambar 4.9 Grafik Pengamatan TCP 41

Gambar 4.10 Grafik Pengamatan UDP 42

Gambar 4.11 Grafik Pengamatan ICMP 42

Gambar 4.12 Pengamatan Top 10 *Source* IP protokol TCP 43

Gambar 4.13 Pengamatan Top 10 *Destination* IP protokol TCP 44

Gambar 4.14 Pengamatan Top *Source port* yang menggunakan Protokol TCP 44

Gambar 4.15 Grafik Pemantauan Trafik Jaringan 45

Gambar 4.16 Laporan SIEM *event* Top 10 *Attacker* Pada Tanggal 10 Juni 2010 47

Gambar 4.17 Laporan SIEM *event* Top 10 *Attacked* Pada Tanggal 10 Juni 2010 47

Gambar 4.18 Laporan SIEM *event* Top 15 *Events* Pada Tanggal 10 Juni 2010 48

Gambar 4.19 Grafik Pemantauan Trafik ICMP Saat Skenario Serangan 49

Gambar 4.20 Pemantauan Trafik ICMP Top *Source* IP Saat Skenario Serangan 49

Gambar 4.21 Pemantauan Trafik ICMP Top *Destination* IP Skenario Serangan 50

Gambar 4.22 *Alarm* yang Dihasilkan dari Skenario Serangan 50

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

DAFTAR TABEL

Tabel 2.1 Evalusi Perbandingan fitur Pemantauan OSSIM, NSM dan Firewall..... 24

Tabel 4.1 Trafik TCP 40

Tabel 4.2 Trafik UDP 40

Tabel 4.3 Trafik ICMP 40

Tabel 4.4 Rata-rata Trafik Protokol..... 41

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

BAB 1

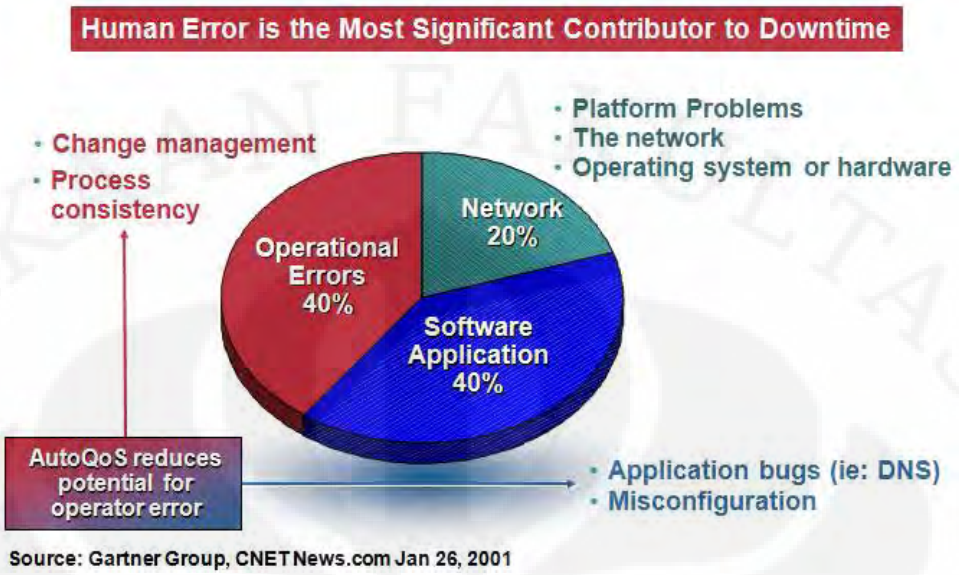
PENDAHULUAN

1.1 LATAR BELAKANG

Era globalisasi seperti saat ini, adalah saat di mana proses peradaban manusia mulai berubah, di mana saat ini interaksi manusia membutuhkan kecepatan dan ketepatan proses yang tersistem sehingga manusia dapat dengan mudah dan efektif meningkatkan kualitas hidup dan kehidupannya. *Information Technology* (IT)/Teknologi Informasi merupakan gaya hidup baru yang tidak dapat dipisahkan dalam bermasyarakat, mulai dari segi sosial, pendidikan, hiburan, militer dan lain-lain. Penggunaan telepon seluler, komputer dan Internet bukan menjadi hal yang asing lagi bagi kita yang hidup di era globalisasi ini. Dan bukan tidak mungkin kebutuhan tersebut menjadi hal yang pokok dan mendasar bagi kita untuk dapat bertahan hidup di maraknya teknologi modern saat ini.

Dengan semakin berkembangnya teknologi Internet, sehingga mengakibatkan pengguna teknologi tersebut semakin meluas dan begitu juga dengan ancaman yang timbul dari proses kegiatan tersebut. Pada sebuah perusahaan atau organisasi, keamanan jaringan komputer merupakan bagian yang tidak terpisahkan dari keamanan sistem informasi. Berbagai teknik atau mekanisme pertahanan dalam suatu jaringan bergantung pada seorang *administrator (admin)* jaringan yang mengelolanya. Seorang *admin* harus mengetahui betul kondisi jaringan. Usaha untuk mengamankan suatu jaringan harus dipandang secara keseluruhan, tidak bisa secara parsial, setiap lapisan dalam jaringan harus dapat melakukan fungsinya secara aman. Pemilihan teknologi perangkat untuk keamanan jaringan harus tepat sesuai dengan kebutuhan dan kondisi jaringan. Pemilihan teknologi yang tidak tepat, selain akan mengeluarkan biaya yang besar juga dapat mengurangi tingkat keamanan dalam sebuah jaringan. Gambar 1.1 menunjukkan beberapa faktor penyebab *network down,* yaitu dari gambar tersebut dapat terlihat bahwa peran seorang admin sangat berpengaruh terhadap kondisi jaringan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 1.1 Faktor-faktor penyebab *network down* [1]

Dalam usaha untuk meningkatkan keamanan jaringan, sebuah organisasi atau perusahaan mungkin akan mengimplementasikan beberapa perangkat teknologi kemanan jaringan komputer, seperti *firewall*, *Intrusion Detecion System* (IDS) dan *Intrusion Prevention System* (IPS). Bahkan untuk sebuah organisasi atau jaringan yang besar, penggunaan perangkat tersebut bukan hanya satu atau dua saja yang diimplementasikan, karena semua bergantung dengan tingkat dan kondisi yang diperlukan untuk pengamanan. Dengan banyaknya peralatan jaringan komputer yang diimplementasikan maka semakin banyak pula peralatan yang perlu dikelola. Setiap peralatan yang dipasang perlu dikonfigurasi sesuai dengan kebutuhan jaringan, setiap peralatan jaringan yang dipasang juga perlu dipantau, dan setiap peralatan yang dipasang perlu dianalisa apakah berfungsi sesuai dengan rancangan awal.

Salah satu cara memantau peralatan adalah dengan memantau *log-log* dan *alert* yang dihasilkan oleh peralatan. Semakin banyak peralatan yang dipasang akan semakin banyak pula *log-log* yang dihasilkan. Maka dengan begitu akan memerlukan banyak waktu dan kesulitan untuk menganalisa seluruh *log* dan *alert* yang ada. Salah satu penyebab utama kegagalan sistem kemanan jaringan komputer adalah kesalahan pengelolaan dalam melakukan analisa seluruh *log* dan *alert* yang ada, termasuk pada saat seorang admin jaringan melakukan pencarian

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

log-log dan *alert* yang tersimpan dalam jumlah yang banyak. Kesalahan analisa dapat menjadikan pengelolaan yang lambat sehingga tidak tepatnya dalam menanggapi dan melakukan tindakan pada saat terjadi serangan. Oleh karena itu diperlukan mekanisme pertahanan dalam melakukan pengelolaan jaringan yang disebut *Security Information Management* (SIM).

Security Information Management (SIM) berfungsi menyediakan informasi yang terkait dengan keamanan jaringan secara terpusat dan juga berfungsi untuk mengumpulkan *log-log* dan *alert* yang dihasilkan oleh peralatan keamanan ke dalam satu database. SIM juga dapat melakukan analisa dengan teknik korelasi, sehingga seorang admin dapat dengan mudah dan mengetahui lebih cepat keadaan dan kondisi jaringan sehingga dapat melakukan penanganan yang lebih terarah. Salah satu aplikasi SIM adalah OSSIM (*Open Source Security Information Management*). Pada skripsi ini, penulis mengimplementasikan salah satu bentuk mekanisme pertahanan pada sebuah jaringan dengan menggunakan aplikasi OSSIM pada sebuah perusahaan.

1.2 TUJUAN

Tujuan skripsi ini adalah menerapkan atau mengimplementasikan sistem aplikasi *security information management* dengan menggunakan OSSIM pada sebuah perusahaan yang mempunyai jaringan yang besar dan mempunyai perangkat keamanan jaringan yang banyak. Melalui OSSIM akan dilakukan pemantauan terhadap trafik jaringan dan pemantauan terhadap serangan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

1.3 BATASAN MASALAH

Penulisan Skripsi ini dibatasi oleh hal-hal berikut:

1. Implementasi dilakukan pada jaringan komputer di sebuah gedung suatu perusahaan dengan mengintegrasikan OSSIM dengan perangkat-perangkat keamanan jaringan lainnya yaitu IDP dan Firewall.
2. Parameter yang akan dilihat adalah trafik jaringan yang dihasilkan OSSIM selama satu pekan dengan dibatasi oleh waktu jam kerja dan bukan jam kerja.
3. Trafik jaringan yang dilihat adalah untuk protokol TCP, UDP dan ICMP.
4. Akan dilakukan skenario serangan ping ke server OSSIM selama 10 menit dengan besar paket 1000 bytes. Dan akan dilakukan analisis jaringan saat terjadi serangan pada hari tersebut.

1.4 METODE PENETILIAN

Metode yang digunakan dalam penelitian ini adalah**:**

a) Studi literatur dengan mempelajari informasi dari berbagai sumber literatur, seperti buku, jurnal dan artikel-artikel yang berkaitan dengan sistem yang akan dibuat.
b) Implementasi aplikasi OSSIM pada jaringan perusahaan.
c) Pengambilan data:
    1. Trafik protokol TCP, UDP dan ICMP
    2. Pengambilan data Skenario serangan
d) Menganalisa berdasarkan hasil pengambilan data.

1.5 SISTEMATIKA PENULISAN

Sistematika penulisan pada skripsi ini ialah sebagai berikut:

BAB 1 Pendahuluan

Terdiri dari latar belakang, tujuan, batasan masalah, metode penelitian dan sistematika penulisan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

BAB 2 OSSIM

Membahas mengenai *Network Management* dan OSSIM (Open Source Security Information Management).

BAB 3 Perancangan Implementasi OSSIM Pada Jaringan

Membahas mengenai masalah yang ada pada perusahaan, implementasi OSSIM pada perusahaan dan rancangan skenario dari penelitian.

BAB 4 Implementasi dan Uji Coba Sistem Pada Jaringan

Membahas mengenai proses implementasi dan konfigurasi, pengambilan data dan analisis hasil pengambilan data.

BAB 5 Kesimpulan

Merupakan penutup yaitu kesimpulan dari penulisan skripsi ini.

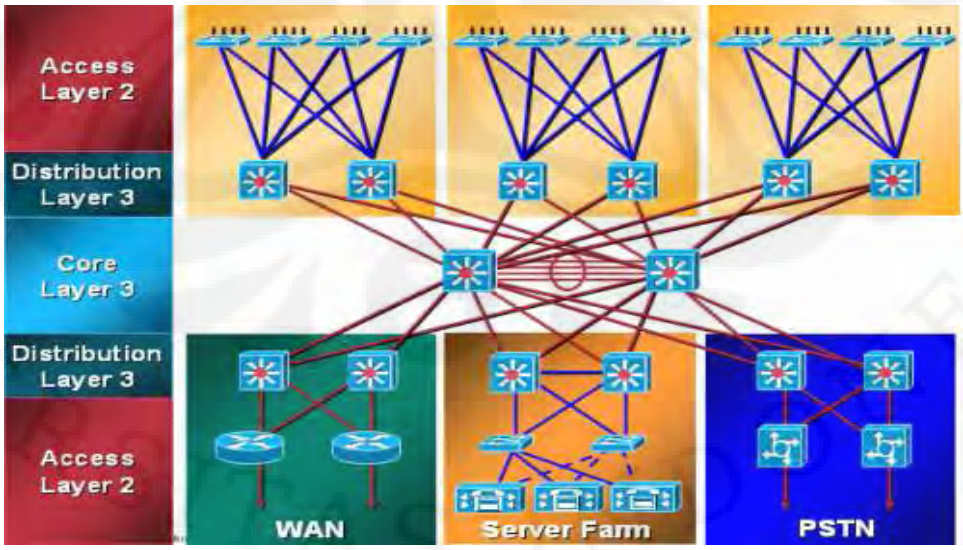
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

BAB 2

OSSIM (*OPEN SOURCE SECURITY INFORMATION MANAGEMENT*)

2.1 Manajemen Jaringan

Kebutuhan data dan informasi yang cepat, tepat, dan akurat saat ini sangatlah pokok bagi semua lapisan pengguna teknologi infomasi. Pada setiap organisasi atau sebuah perusahaan, kebutuhan teknologi informasi menjadi suatu bagian dari kegiatan atau aktivitas yang membantu proses produksinya, misalnya kebutuhan akan komunikasi data dimana dapat terhubung dengan kantor cabang, para pegawai dan rekan bisnis lainnya. Untuk mencapai itu semua diperlukan faktor-faktor pengelolaan infrastruktur *internetworking* yang baik agar komunikasi jaringan dapat berjalan lancar. Agar *internetworking* berjalan dengan baik diperlukan manajemen jaringan yang baik pula. Pada sebuah organisasi dengan infrastuktur jaringan yang besar akan mengalami kesulitan dalam pengelolaan apabila tidak diterapkan manajemen jaringan yang benar. Apabila pengelolaan manajemen sistem jaringan salah atau tidak tepat maka akan berdampak pada terganggunya kegiatan operasional perusahaan. Gambar 2.1 dibawah ini adalah salah satu contoh desain infrastruktur jaringan pada sebuah perusahaan dimana diperlukan sebuah manajemen jaringan yang baik.



Gambar 2.1 *Enterprise Design* Infrastruktur Jaringan [5]

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

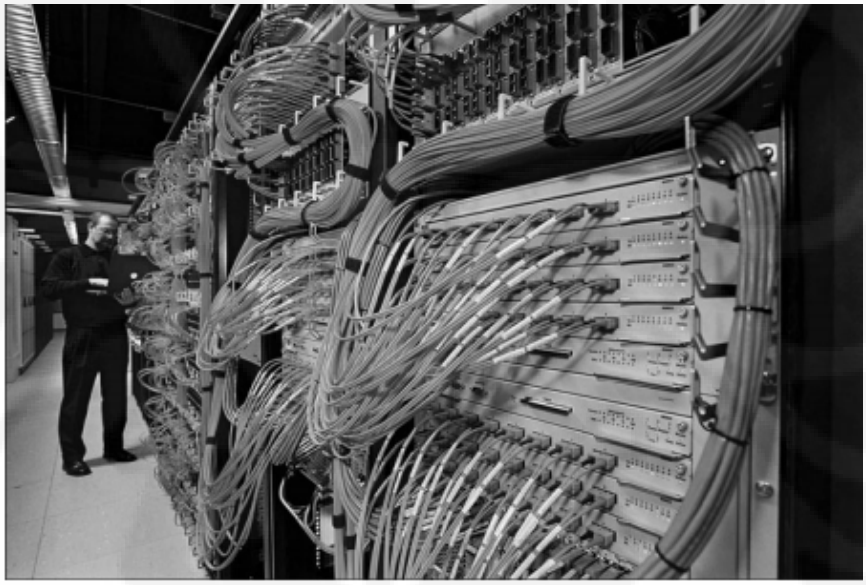
Pengelolaan jaringan adalah sesuatu hal yang penting untuk suksesnya operasional jaringan perusahaan, perusahaan sangat bergantung pada *service* dari jaringan. Menjaga *service* dari sistem jaringan sama dengan menjaga keberlangsungan bisnis perusahaan [9]. Yang dimaksud dengan manajemen jaringan adalah aktivitas, metode, prosedur, dan peralatan yang berkaitan dengan operasional, administrasi, pemeliharaan, dan *provisioning* dari sistem jaringan [9].

- Operasional adalah menjaga jaringan (*service* dari jaringan yang tersedia) agar tetap hidup dan berjalan dengan baik. Operasional juga termasuk memantau jaringan dari masalah yang mungkin terjadi.
- Administrasi menjaga sumber daya pada jaringan dan bagaimana peralatan tersebut bekerja, dimana semuanya dapat dikontrol.
- Pemeliharaan bertujuan untuk perbaikan dan peningkatan. Contohnya pada saat router membutuhkan *patch* terbaru dari operating sistemnya, atau ketika switch baru ditambahkan pada sebuah jaringan. Sebagai tujuan untuk membuat manajemen jaringan berjalan dengan baik.
- *Provisoning* berkonsentrasi bagaimana mengkonfigurasi peralatan-peralatan pada jaringan untuk mensupport pelayanananya.

Pentingnya manajemen jaringan adalah sebagai alasan untuk menjaga dan merawat keberlangsungan jaringan. Sebuah jaringan adalah suatu struktur yang kompleks yang memerlukan perlakuan atau perhatian yang harus benar-benar di rencanakan [9]. Konfigurasi peralatan jaringan seperti *router, firewall, switch* dan peralatan lainnya harus dikelola dan disesuaikan dengan kebutuhan jaringan yang kita bangun. Sebagai contoh pada sebuah perusahaan dengan jaringan yang besar dimana didalamnya terdapat ratusan bahkan ribuan user pada jaringan yang terhubung satu dengan yang lainnya menjadi sebuah masalah yang kompleks, sehingga perlu pengelolaan untuk user-user pada sebuah kantor cabang yang didalamnya terdapat divisi-divisi, dimana satu dengan divisi lainnya berinterkoneksi untuk keperluan komunikasi mereka dan dimana pula antar divisi tersebut tidak perlu saling berkomunikasi misalnya pada sebuah divisi keuangan pada perusahaan yang sifatnya *private*. Kondisi tersebut sangat diperlukan

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

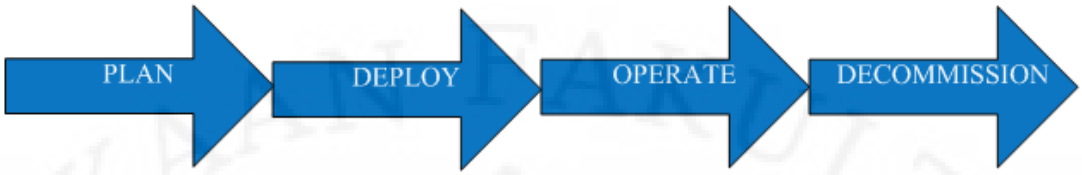
pengelolaan jaringan yang baik pada saat semua user-user tersebut terhubung pada jaringan. Bagaimana jadinya apabila seorang administrator jaringan mengelola ratusan user yang terhubung jaringan yang didalamnya juga terdapat peralatan dan perlengkapan jaringan yang saling terhubung untuk kinerja dan fungsi dari peralatan tersebut pada suatu jaringan. Gambar 2.2 di bawah ini adalah contoh gambar yang mana terdapat kabel-kabel yang tersusun oleh rak-rak yang sangat banyak.



Gambar 2.2 Kabel-kabel dan peralatan pada jaringan [3]

Dalam mengelola jaringan terdiri dari berbagai aspek, satu diantaranya yaitu bagaimana proses dari *management life cycle* tersebut. *Management life cycle* adalah istilah bagaimana mengelola jaringan dari lahir hingga mati (*from cradle to grave)*.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 2.3 *Management Life Cycle*

Adapun langkah-langkah dari *management life cycle* adalah sebagai berikut [3]:

1. *Planning*

   Sebelum operasional berjalan, suatu sistem jaringan harus direncanakan sesuai dengan kebutuhan user, peralatan-peralatan jaringan dan penentuan lokasi sistem jaringan tersebut. Topologi jaringan harus sesuai dengan apa yang direncanakan, sehingga perfomasi sistem jaringan yang dihasilkan akan bekerja dengan maksimal. Penentuan *cost* dan *budget* juga termasuk dalam perencanaan sistem jaringan ini.

2. *Deployment*

   Setelah proses perencanaan telah selesai, sebuah sistem jaringan sudah dapat dibangun, hal ini berarti semua peralatan-peralatan sistem jaringan yang dibutuhkan harus diimplementasikan, termasuk didalamnya yaitu proses instalasi dan konfigurasi peralatan sistem jaringan.

3. *Operation*

   Setelah proses instalasi dan konfigurasi dan sistem jaringan berjalan, maka selanjutnya adalah bagaimana mengoperasikan sistem jaringan tersebut. Pengoperasian disini meliputi pemantauan jaringan, perbaikan jaringan dan pemeliharaan sistem jaringan.

4. *Decommision*

   Decommision adalah proses dimana menon-aktifkan peralatan-peralatan sistem jaringan dimana peralatan tersebut sudah tidak lagi dibutuhkan atau kinerjanya sudah tidak lagi maksimal dengan kebutuhan sistem jaringan yang semakin tinggi. Misalnya yaitu adanya teknologi baru, sebagai contoh penggunaan Internet *dial up* diganti dengan adanya teknologi DSL (*Digital Subscriber Line*).

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2.1.1 *Network Intrusion Detection*

Sebelum mengetahui apa yang dimaksud dengan *network intrusion detection* terlebih dahulu kita perlu mengetahui apa *itu Intrusion Detection System* (IDS). IDS dapat didefinisikan sebagai suatu tools, metode dan perangkat sistem yang bertugas untuk membantu mengidentifikasi, mendeteksi dan melaporkan adanya aktifitas yang mencurigakan yang biasa terjadi pada suatu sistem jaringan komputer [2]. IDS dapat berupa perangkat *hardware* ataupun *software.* IDS dapat melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan). Ditinjau dari aspek lokasi dimana IDS diimplementasikan, IDS dapat terbagi menjadi dua jenis, yaitu *Network-Based Intrusion Detection System* (NIDS) dan *Host-Based Intrusion Detection System* (HIDS). Adapun pada bagian ini hanya akan dijelaskan tentang NIDS.

Network-Based Intrusion Detection System adalah IDS yang diimplementasikan pada sebuah sistem jaringan komputer dimana semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk dicari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS biasanya terdapat pada "pintu masuk" sebuah sistem jaringan [2].

Ada 2 cara bagaimana NIDS bekerja.

1. *Signature-based* IDS yaitu IDS yang menggunakan pendeteksian berbasis *signature*. *Signature* adalah tipe sebuah serangan yang sudah dikenali atau ditandai. Seperti halnya yang dilakukan oleh beberapa antivirus, dimana melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.
2. *Anomaly-based* IDS yaitu IDS yang mendeteksi adanya anomalitas pada sebuah jaringan. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. *Anomaly-based* IDS menggunakan teknik statistik untuk membandingkan lalu lintas

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini bersifat *false positive* yang berarti menduga adanya serangan meskipun belum tentu benar bahwa hal tersebut adalah sebuah serangan. Metode ini menjadikan tugas administrator menjadi lebih rumit, dimana harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan *false positive* yang muncul.

IDS umumnya bersifat pendeteksi pasif dimana tugasnya hanya mendeteksi adanya intrusi yang muncul, kemudian memberikan peringatan kepada administrator bahwa terjadi serangan atau gangguan pada sistem jaringan, namun saat ini ada perangkat IDS yang bersifat aktif deteksi yang biasa disebut IPS (*Intrusion Prevention System*). IPS dapat bekerja bukan hanya melakukan pendeteksian *intrusion* namun juga dapat melakukan tindakan-tindakan pencegahan serangan seperti menutup beberapa *port* dan melakukan pemblokiran alamat IP dari hasil pendeteksian serangan.

2.1.2 *Risk Management*

Risk Management Process merupakan suatu program, strategi, taktik, dan operasional resiko yang bertujuan untuk meminimalisasi dampak buruk dari sebuah perusahaan atau suatu organisasi dalam pengambilan keputusan [9]. Adapun tahapan dari *Risk Management Process* secara umum yaitu *risk assestment, threat identification, risk mitigation, evaluation* dan *assessment* [9].

2.1.2.1 *Risk Assesment*

Risk Assessment merupakan tahap mengidentifikasi resiko dalam *Risk Management Process*. Sebuah organisasi atau perusahaan menggunakan *risk assessment* untuk menentukan bahaya apa saja yang berpotensi dan resiko-resiko yang akan ditimbulkan terhadap sistem IT. Keluaran yang diharapkan dari proses ini adalah dapat membantu mengidentifikasikan kontrol yang sesuai untuk mengurangi atau menghilangkan resiko-resiko tersebut selama proses pengurangan resiko (*risk mitigation)*.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Resiko adalah fungsi dari kemungkinan celah yang dikerjakan oleh suatu sumber ancaman dan hasil dari dampak yang ditimbulkannya terhadap suatu perusahaan. Untuk menentukan kemungkinan dari kerugian yang akan ditimbulkan di masa depan. Ancaman tersebut harus dianalisis dan dibandingkan dengan kemungkinan celah yang ditimbulkan dan kontrol yang harus diberikan terhadap sistem IT. Level dari ancaman tersebut kemudian ditentukan dari pengaruhnya terhadap dampak yang ditimbulkan terhadap asset dan sumber daya IT perusahaan.

2.1.2.2 *Threat Identification*

Threat (ancaman) adalah potensi - potensi yang berbahaya yang dihasilkan oleh suatu sumber (*threat source*) yang dapat menyerang celah yang dimiliki suatu sistem. Suatu sumber ancaman tidak dapat menghasilkan ancaman ketika tidak ada celah.

2.1.2.3 *Risk Mitigation*

Pada tahap *risk mitigation*, meliputi tahap pemberian prioritas, evaluasi dan implementasi kontrol pengurangan resiko yang direkomendasikan dan diperoleh dari tahap *risk assessment*. Karena proses menghilangkan semua resiko yang mungkin terjadi merupakan hal yang sangat tidak praktis dan mendekati mustahil, maka merupakan kewajiban dari *senior management/business managers* untuk menggunakan pendekatan *least-cost* dan mengimplementasikan kontrol yang paling penting untuk mengurangi level resiko ke level yang lebih dapat diterima, dengan mengedepankan dampak yang minimal pada sumber daya dan misi organisasi.

2..1.2.4 *Evaluation* dan *Assessment*

Pada sebagian besar perusahaan, jaringan yang dimiliki biasanya akan terus-menerus mengalami perkembangan, meliputi sistem yang dimiliki, komponen-komponen yang dimiliki serta *software* atau aplikasi yang akan diganti atau mengalami *update* dengan versi terbaru. Selain itu, perubahan juga akan meliputi pergantian serta perubahan aturan keamanan yang dimiliki. Setiap perubahan tersebut menimbulkan permasalahan karena resiko-resiko baru akan

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

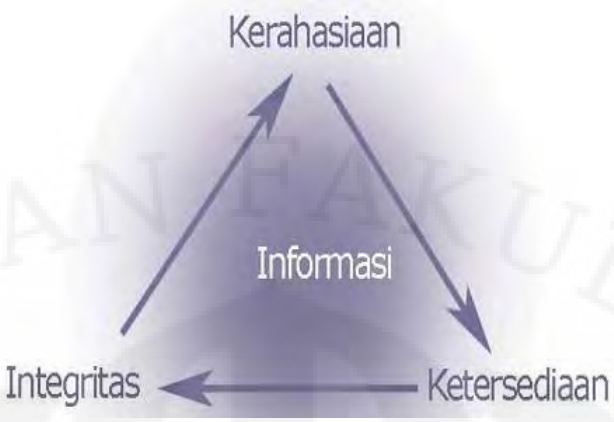
muncul serta resiko yang sebelumnya telah dapat diatasi akan muncul kembali. Oleh karena itu, proses *risk management* harus terus berjalan dan mengalami perkembangan.

2.1.3 ISMS (*Information Security Management System*)

Information Security Management System adalah suatu sistem manajemen keamanan informasi pada sebuah organisasi yang berfokus menginisiatif untuk menginformasikan managemen resiko dari mana saja resiko tersebut berasal [9]. Sistem manajemen ini menyediakan pendekatan sistematik dalam mengatur informasi yang sensitif agar dapat memproteksinya. Ini meliputi data pegawai, proses-proses dan sistem informasi pada organisasi tersebut. Istilah ISMS ini muncul berdasarkan pada standar ISO/IEC 2001 dan ISO/IEC 27002 [4]. Yaitu merujuk pada suatu sistem manajemen yang berhubungan dengan keamanan informasi. Konsep utama ISMS adalah merancang, menerapkan, dan memelihara suatu rangkaian terpadu baik proses dan sistem untuk secara efektif mengelola keamanan informasi dan menjamin kerahasiaan, integritas, serta ketersediaan aset-aset informasi serta meminimalkan risiko keamanan informasi. Terdapat 3 aspek penting dari Information Security yang semuanya merupakan gambaran dari ISMS yaitu *confidentiality, integrity* dan *availability* [4].

1. *Confidentiality* (kerahasiaan) yaitu suatu aspek yang menjamin kerahasiaan data atau informasi, memastikan suatu informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* (integritas) yaitu suatu aspek yang menjamin data tidak dirubah tanpa ada ijin pihak yang berwenang, menjaga keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas ini.
3. *Availability* (ketersediaan) yaitu suatu aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 2.4 Elemen-elemen keamanan informasi [4]

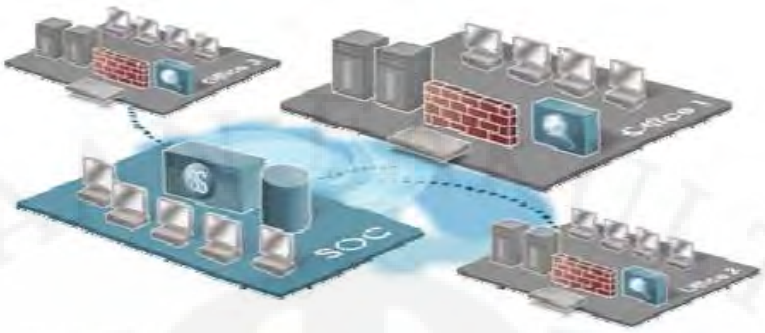
Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

2.2 OSSIM

2.2.1 Sekilas Tentang OSSIM

OSSIM atau *Open Source Security Information Management* adalah sebuah *Platform Security Information Management* yang berbasiskan open source dan merupakan kumpulan lebih dari 15 *open source security* program yang semuanya terkandung didalam teknologi atau sistem ini untuk menghasilkan kontrol manajemen keamanan pada sebuah jaringan [8]. Pada dasarnya OSSIM ini berupaya mengintegrasikan beberapa perangkat lunak dan *existing tools* lainnya untuk bekerjasama melakukan suatu penyimpanan, melakukan korelasi dan manajemen perangkat. Sehingga dapat menghasilkan kumpulan *event, log* dan informasi kondisi keamanan jaringan dari sebuah *single console*. Dengan adanya kerjasama beberapa aplikasi dan perangkat keamanan jaringan, memungkinkan untuk dapat mengontrol jaringan dengan mengurangi waktu yang diperlukan dan mengelola informasi secara terpusat pada sebuah jaringan suatu perusahaan yang besar. Pada gambar 2.5 menunjukkan ilustrasi manajemen jaringan secara terpusat pada sebuah organisasi dengan beberapa kantor cabang.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 2.5 Ilustrasi kontrol manajemen jaringan secara terpusat [8]

OSSIM terdiri dari kumpulan beberapa *tools* atau program-program *security* menjadi sebuah *server single console* untuk menghasilkan informasi keamanan pada sebuah jaringan. *Tools* tersebut diantaranya adalah [10]:

1. Snort sebagai IDS
2. Nessus sebagai Vulnerability Scanner
3. Ntop adalah tools untuk monitor jaringan
4. Nagios digunakan untuk *availability monitor*
5. Osiris dan snare sebagai *host* IDS
6. Arpwatch dan Pads sebagai anomaly detector
7. Pof dan Fprobe sebagai detektor pasif
8. Nmap sebagai *network scanner*
9. Acid/Base sebagai forensinc analyzer
10. Oinkmaster, PHPAcl, fw1logcheck, scanMap3D
11. OSVDB sebagai vulnerability database

2.2.2 Arsitektur OSSIM

OSSIM terdiri dari 4 elemen bagian yaitu [8]:

1. Sensors
2. Manajemen Server
3. Database
4. Frontend

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2.2.2.1 Sensor

Sensor dipakai atau disebarkan pada sebuah jaringan untuk memantau aktivitas-aktivitas suatu sistem jaringan. Segala peristiwa-peristiwa atau kejadian pada suatu jaringan dapat diterima oleh server OSSIM ini melalui sensor, dalam hal ini sensor dapat disebut sebagai pendetektor.

Gambar 2.6 Sensor pada OSSIM untuk monitor jaringan [8]

Suatu hal yang sangat penting bahwa OSSIM juga dapat menerima kejadian pada jaringan dari peralatan-peralatan komersial atau suatu aplikasi yang dikostumisasi sebagai sensor yang ditanam, sehingga dapat berkolaborasi dengan OSSIM. Sensor-sensor tersebut pada umumnya sebagai suatu host dan mempunyai tingkatan konfigurasi yang berbeda.

1. Untuk level konfigurasi tingkat paling bawah, sensor atau detektor OSSIM ini bersifat pasif monitor hanya menerima atau mengkoleksi data dari suatu jaringan.
2. Sensor pada OSSIM dapat pula dikonfigurasi sebagai suatu *host scanners* yang mana bersifat aktif sensor dimana sensor ini dapat melakukan scanning pada jaringan untuk melihat dan mengetahui celah pada suatu jaringan.
3. Untuk level yang paling atas dalam melakukan konfigurasi sensor OSSIM, dapat menambahkan OSSIM *Agent* sebagai detektor sehingga dapat menerima

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

data dari host yang ditunjuk sebagai agent OSSIM tersebut untuk melakukan pendeteksian pada jaringan sepeti router atau firewall, detektor tersebut dapat berkomunkasi untuk mengirimkan data mereka kepada manajemen server OSSIM.

2.2.2.2 Manajemen Server

Suatu manajemen server atau server pada umumnya terdiri dari beberapa komponen bagian yaitu:

1. Frameworkd adalah suatu kontrol *daemon* atau proses yang berjalan dibelakang, yang mengikat bagian-bagian untuk bekerjasama.
2. OSSIM server adalah pusat dari segala informasi yang diterima dari sensor-sensor OSSIM.

Adapun fungsi dari Manajemen Server ini adalah:

1. Server utama yang mempunyai tugas untuk menormalisasi, memberikan prioritas, mengkoleksi, melakukan *risk assesment* dan mengkorelasi perangkat-perangkat lainnya.
2. Melakukan perawatan dan tugas-tugas eksternal seperti *backup data, backup scheduled, inventory* secara *online*, dan melakukan atau mengajukan penscanan.

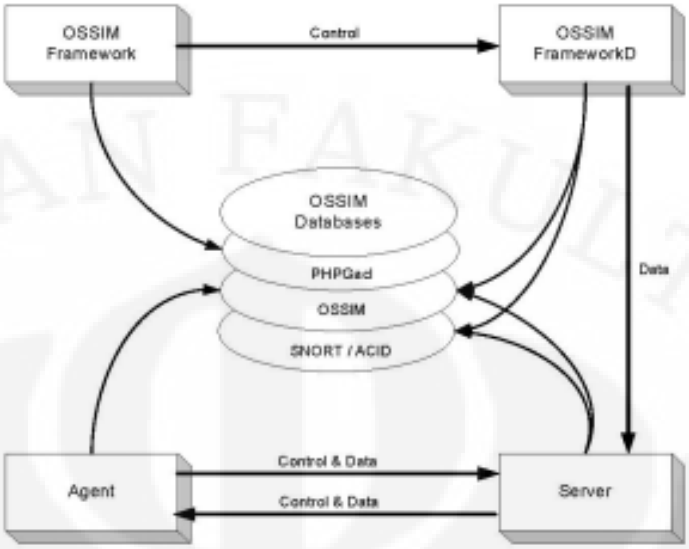
2.2.2.3 *Database*

Database pada OSSIM berfungsi untuk melakukan penyimpanan data dari semua kejadian pada suatu jaringan yang berguna sebagai informasi untuk manajemen sistem. Database pada OSSIM adalah SQL database.

2.2.2.4 *Frontend*

Frontend adalah suatu konsole yang memberikan visualisasi informasi secara *web base system* pada layar komputer.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 2.7 Interaksi dari Komponen-Komponen pada OSSIM [1]

Adapun Interaksi komponen pada OSSIM ditunjukkan pada Gambar 2.7 dimana penjelasan interaksinya adalah sebagai berikut:

1. *Agent* atau sebuah sensor OSSIM mengirimkan data ke database OSSIM, dan juga melakukan kontrol atau komunikasi data tersebut dengan server untuk dilakukan prioritas dan korelasi
2. *Server* bertugas menerima data dan melakukan prioritas, korelasi dan risk assesment dan mengirimkan hasil data tersebut ke database OSSIM.
3. *User* atau admin melakukan pengecekan, konfigurasi terhadap server melalui Frameworkd
4. OSSIM framework adalah sebuah panel yang memberikan informasi pada admin

Semua komponen yang ada pada OSSIM berdiri sendiri dan dapat dikonfigurasi sesuai kebutuhan admin jaringan. Semua komponennya dapat terpisah atau dapat pula diintegrasikan dalam satu mesin.

2.2.3 Kegunaan OSSIM

2.2.3.1 Detektor

OSSIM berfungsi sebagai pendeteksi adanya ancaman-ancaman yang ada pada suatu sistem pada jaringan atau yang disebut sebagai detektor. Bedasarkan

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

prinsip kerjanya terdapat 2 tipe detektor pada OSSIM yaitu *Pattern Detectors* dan *Anomaly Detectors*.

1. *Pattern Detectors*

Detektor tipe ini biasa disebut sebagai program yang berjalan dengan cara mendengarkan aktivitas-aktivitas pada sistem jaringan, prinsip kerjanya yaitu mencari pola-pola dari log, dan menghasilkan suatu kejadian kondisi keamanan. Ketika *log-log* tersebut sesuai dengan pola yang ada yang dimiliki detektor sebagai suatu ancaman (*matched patterns*) maka akan dianggap sebagai suatu serangan. *Pattern Detectors* yang terdapat pada OSSIM dapat dikonfigurasi berdasarkan letak detektor atau sensor berada, yaitu *Pattern Detectors* yang sudah ada didalam (*included*) OSSIM atau detektor diluar (*external detectors)*.

- *Pattern Detector* didalam OSSIM

Didalam OSSIM sudah terdapat beberapa aplikasi program yang diinstall sebagai *pattern detectors*. Adapun aplikasi yang telah terinstall yaitu *Snort* sebagai NIDS (*Network Intrusion Detector System*), *Snare* dan *Osiris* sebagai HIDS (*Host Intrusion Detector System*).

- *External Detector*

OSSIM mempunyai suatu koleksi sistem yang mengijinkan data dikumpulkan dari beberapa peralatan jaringan. Suatu koleksi sistem pada OSSIM mengambil data dari peralatan lain seperti sistem Windows, Linux, Unix, firewall, IDP dan server lainnya.

2. Anomaly Detectors

Kemampuan mendeteksi anomaly melebihi kemampuan dari *pattern matching*. Cara kerja dari *anomaly detectors* yaitu mendeteksi sistem dengan cara mempelajari statistik kebiasaan dari sistem jaringan atau kebiasaan normal pada jaringan, saat suatu jaringan beraktivitas tidak seperti biasaanya, detektor ini menduka bahwa terdapat ancaman pada jaringan. Pada dasarnya pendeteksiaan *anomaly* tidak dapat mengatakan bahwa suatu yang terdeteksi adalah suatu serangan atau bukan. *Anomaly detector* bekerja saat *signature* pada *pattern*

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

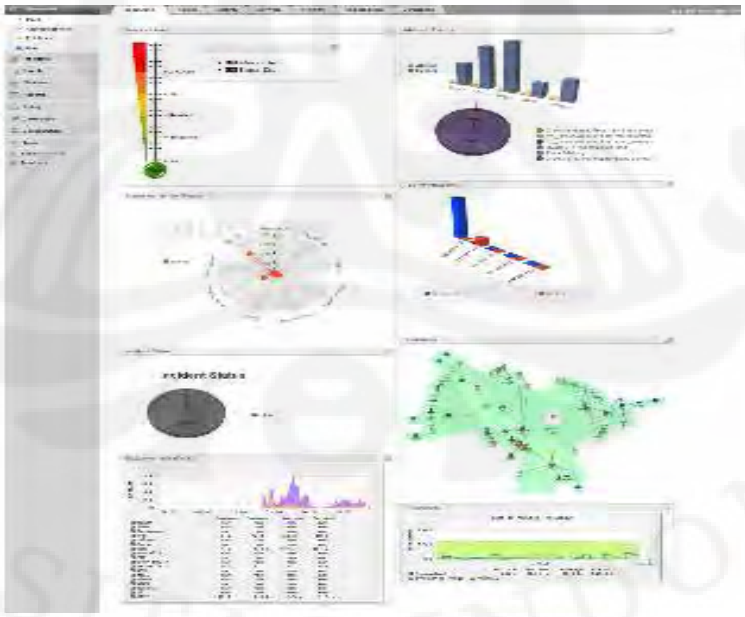
detector tidak ditemui (*matching* dengan data berbagai ancaman) atau belum *terupdate*.

2.2.3.2 Monitor

Tujuan utama diimplementasikan SIM oleh admin adalah menghasilkan informasi mengenai keadaan keamanan dari jaringan dan dapat dipantau oleh admin jaringan tersebut. Pemantauan yang bisa dilakukan OSSIM ini terbagi menjadi dua bagian yaitu pemantauan jaringan dan pemantauan ketersediaan.

1. Pemantauan jaringan

Pemantauan jaringan adalah proses pemantauan aktivitas keseluruhan dari sistem jaringan, yaitu aktivitas yang normal dan tidak normal, trafik dari jaringan, protokol-protokol yang dilewati kesistem jaringan dan berbagai aktivitas kondisi jaringan lainnya. Pada pemantauan ini memberikan informasi mengenai keadaan dari sistem jaringan yang direpresentasikan dalam bentuk grafik, statistik, dan data – data yang dibutuhkan dalam proses pemantauan. Gambar 2.8 adalah tampilan dalam pemantauan jaringan.



Gambar 2.8 Pemantauan Jaringan [8]

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2. Pemantauan Ketersediaan

Pemantauan Ketersediaan adalah proses pemantauan untuk mendapatkan informasi keadaan mati hidupnya peralatan dalam jaringan. Informasi tersebut sangat penting untuk mengetahui adanya pendeteksian dari serangan DoS (*Denial of Service*). Dalam melakukan pamantau ini OSSIM menggunakan *tools* Nagios yang mempunyai kemampuan untuk mengecek, menampilkan dan melaporkan host dan jaringan yang dalam keadaan *down* (mati). Gambar 2.9 adalah bentuk tampilan dalam melakukan pemantauan ketersediaan.

Gambar 2.9 Pemantauan Ketersediaan [8]

2.2.3.3 *Vulnerability Scanners*

Vulnerability Scanners adalah proses pemeriksaan sistem jaringan dari celah yang dapat masuknya serangan dan ancaman-ancaman. Proses pemeriksaannya dengan mencari kelemahan-kelemahan dari peralatan jaringan, melakukan pengetesan atau mensimulasikan serangan untuk mengecek suatu sistem jaringan jika terdapat service atau aplikasi yang lemah. Proses ini dilakukan oleh Nessus yang merupakan tools yang ada pada OSSIM ini. Proses pemeriksaan celah bisa dilakukan secara terjadwal atau *terschedule*.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2.2.3.4 *Automatic Inventory*

OSSIM dapat melakukan otomatisasi penyimpanan segala informasi dan data dari sistem jaringan seperti tipe sistem operasi dan versinya, tipe service dan versinya, Mac dan IP *address* dari perangkat-perangkat dalam sistem jaringan. Proses *automatic inventory* ini dilakukan oleh sensor yang bekerja secara pasif detektor maupun secara aktif detektor yang mencari dan menemukan host yang terintegrasi dalam sistem jaringan. Proses automatic inventory ini dilakukan oleh program atau tools yaitu *Nmap, Pof, Pads, Arpwatch,* dan *OCS.*

2.2.3.5 *Collector System*

OSSIM juga dapat sebagai *collector* yaitu mengumpulkan dan mempersatukan semua kejadian dari seluruh sensor atau agent yang berhubungan dengan OSSIM, baik itu kejadian yang tingkat tinggi (*critical)* atau bukan dan ditampilkan dalam layar komputer. Dengan mempersatukan semua kejadian, maka dapat mengamati status dari keamanan setiap waktu kejadian.

2.2.4 *Correlation*

Korelasi adalah salah satu keunggulan dari cara kerja OSSIM ini, seluruh event-event yang diterima oleh OSSIM dilakukan dengan teknik korelasi yaitu teknik dimana menghubungkan atau mengkorelasikan fungsi-fungsi dari setiap tools atau sistem yang ada di OSSIM atau tidak ditanam di OSSIM sehingga event-event yang diterima dapat menghasilkan informasi yang dibutuhkan oleh seorang adminitrator dalam melakukan pemantauan jaringan. Teknik korelasi pada OSSIM terbagi menjadi 3 bagian yaitu *Logical Correlation, Cross Correlation, dan Inventory Correlation* [8].

2.2.4.1 *Logical Correlation*

Logical Correlation adalah korelasi antar event yang diterima oleh sistem OSSIM berarti korelasinya antara detektor dengan detektor yang lainnya. *Logical correlation* dimaksudkan untuk mengetahui fakta-fakta dan mengecek jika seluruh kejadian tersebut adalah kejadian yang murni serangan atau hanya dugaan serangan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2.2.4.2 *Cross Correlation*

Cross Correlation adalah korelasi antara kejadian dan adanya celah atau antara detektor dan *vulnerability scanner*. Cross Correlation dimaksudkan untuk memprioritaskan atau tidak memprioritaskan event-event yang diketahui atau tidak diketahui sebagai celah kelemahan dari sistem. *Cross Corelation* ini bergantung pada spesifik *vulnerability database* dan *Detector Cross Correlation tables* untuk setiap detektor. OSSIM menggunakan OSVDB sebagai *vulnerability database*.

2.2.4.3 *Inventory Correlation*

Inventory Correlation adalah korelasi antara *events* dan *service* dari sistem operasi. Setiap serangan targetnya adalah sebuah sistem operasi komputer atau *service* yang diberikan oleh sistem operasi tersebut. *Inventory Correlation* melakukan pengecekan jika mesin penyerang digunakan pada sistem operasi yang digunakan untuk melakukan penyerangan. Jika itu benar dilakukan maka hal itu benar merupakan suatu serangan tapi jika bukan maka akan memberikan konfirmasi bahwa event tersebut adalah hanya dugaan serangan yang bukan suatu serangan. Korelasi ini bergantung pada keakurasiaan dari Inventory, OSSIM dapat melakukan manual atau otomatis penyimpanan.

2.3 Firewall dan NSM

Firewall adalah sebuah sistem atau sebuah perangkat yang mengizinkan paket atau data dalam sebuah lalu lintas jaringan yang dianggap aman untuk dilaluinya dan juga sebaliknya yaitu mencegah Paket atau data yang tidak aman pada sebuah lalu lintas jaringan. Umumnya, sebuah Firewall diterapkan dalam sebuah mesin terintegrasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya.

NSM (*Netscreen Security Manager*) adalah sebuah server khusus untuk me-*maintanance* dan *monitoring* perangkat IDP dari *platform* Juniper, dimana berfungsi melakukan pengontrolan dan pemusatan log dan alert yang ada pada

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

perangkat IDP, sehingga dengan adanya NSM *server* seorang *administrator* dapat melakukan pengelolaan dan pemantauan terhadap banyaknya IDP yang diimplementasikan pada sebuah jaringan.

Pada tabel 2.1 adalah data hasil perbandingan Antara OSSIM, NSM dan *firewall* dengan membandingkan fitur yang biasa dilakukan *admin* dalam melakukan pemantauan.

Tabel 2.1 Evalusi Perbandingan fitur Pemantauan OSSIM, NSM dan Firewall

No.	Fitur	OSSIM	NSM	Firewall
1.	Grafik			
	➢ Trafik Protokol	√	-	-
	➢ *Top attacker*	√	√	-
	➢ *Top attacked*	√	√	-
2.	Log			
	➢ *User*	√	√	√
	➢ *Event* berdasarkan *risk*	√	√	√
3.	Laporan log			
	➢ *Web interface*	√	√	√
	➢ Pdf	√	-	-
	➢ *Office document*	√	-	-
4.	Pencarian Log berdasarkan kriteria (waktu, *signature*, Ip *Address*)	√	-	-

Dalam membandingkan fitur yang ada pada masing-masing perangkat pada saat melakukan pemantauan baik itu pemantauan log, event dan pemantauan yang lainnya sesuai pada Tabel 2.1, dari data tersebut diketahui bahwa OSSIM lebih banyak memiliki fitur dalam melakukan pemantauan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

BAB 3
PERANCANGAN IMPLEMENTASI OSSIM PADA JARINGAN

Pada bab ini penulis akan menjelaskan mengenai rancangan dari implementasi OSSIM pada sebuah perusahaan, sebelumnya juga akan dijelaskan masalah-masalah yang dihadapi oleh perusahaan sehingga dengan adanya implementasi ini menjadi suatu solusi dari permasalahan yang ada. Disamping itu, juga akan dijelaskan mengenai skenario dalam pengambilan data setelah proses implementasi dilakukan.

3.1 Identifikasi Masalah Pada Perusahaan

Pada proses identifikasi ini penulis melakukan wawancara dengan seorang administrator jaringan khususnya bagian *network security* pada perusahaan tersebut. Yang kemudian dirangkum menjadi sebuah permasalahan yang ada pada perusahaan.

Kasus permasalahan yang ada pada perusahaan adalah:

1. Saat ini, sistem pengaturan dan penyimpanan terhadap log alat pengaman jaringan tidak terpusat, sehingga mempersulit pemantauan dan pengolahan log dari beberapa alat pengamanan jaringan dalam satu antar muka.
2. Sistem yang sedang berjalan tidak dapat menampilkan laporan log dari beberapa firewall dalam satu interface.
3. Perangkat firewall yang digunakan saat ini tidak dapat menampilkan grafik dari log firewall, sedangkan NSM (*Netscreen Security Manager*) yaitu server manajemen IDP (*Intrusion Detection Prevention*) tidak dapat menampilkan lebih dari satu grafik dalam satu halaman.
4. Kesulitan dalam melakukan pemantauan keamanan keseluruhan jaringan.
5. Tidak tersedianya *alert* keamanan dari sistem jaringan secara *real time* dilaporkan kepada administrator apabila terjadi permasalahan krusial pada sistem jaringan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

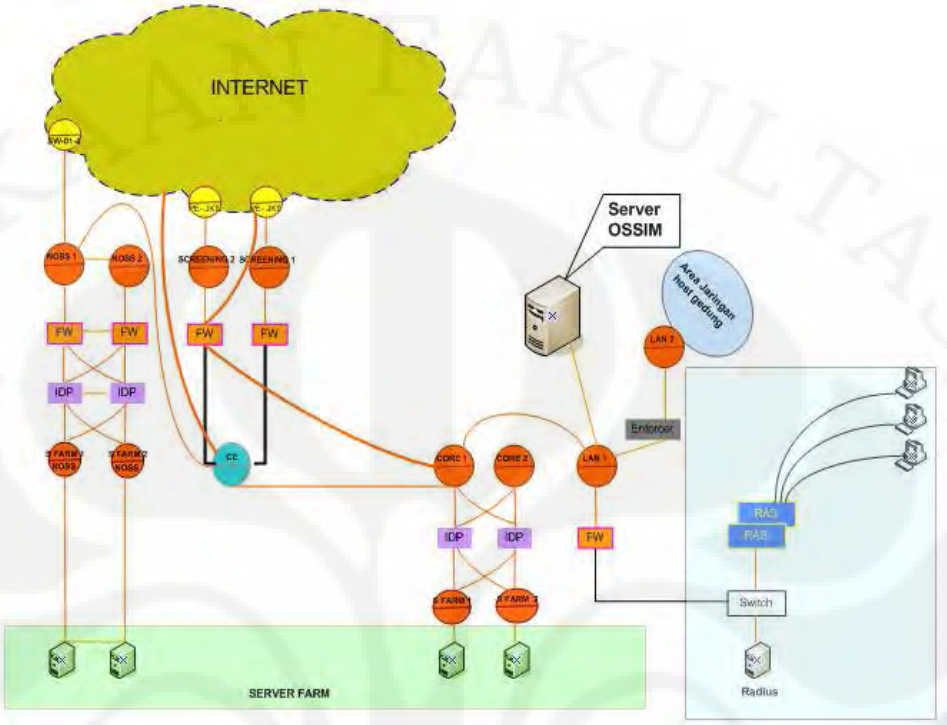
Yang diharapkan dari adanya OSSIM adalah:

1. Dengan adaanya OSSIM seluruh alat pengaman jaringan dikorelasi menghasilkan informasi dengan waktu yang sama.
2. Mengetahui lebih jelas tentang *bandwidth* yang sedang digunakan dan juga dapat mengetahui *port* yang digunakan pada suatu sistem jaringan.
3. Bisa menampilkan *source* dan *destination IP address* yang dianggap serangan.
4. Bisa melihat kondisi jaringan secara luas mengenai utilitas jaringan, me-*review log* jaringan, dan *alert* yang muncul pada suatu waktu dalam satu antar muka.
5. Mudah dalam melakukan pemantauan sistem jaringan setiap waktunya.

3.2 Perancangan Implementasi OSSIM Pada Perusahaan

Setelah proses identifikasi masalah telah dilakukan, yang kemudian dengan adanya proses identifikasi masalah tersebut, penulis memberikan solusi yaitu menerapkan dan mengimplementasikan OSSIM sebagai sistem manajemen informasi keamanan pada perusahaan. Sistem manajemen informasi keamanan ini adalah sebuah sistem dimana penulis melakukan konfigurasi dengan membangun OSSIM server dan mengintegrasikannya dengan beberapa perangkat keamanan jaringan perusahaan yaitu IDP (*Intrusion Detection Prevention*) dan Firewall. IDP dan Firewall akan dijadikan sebagai detektor dari OSSIM ini yang fungsinya untuk menjaga dan melakukan pencegahan pertama apabila terdapat serangan dari luar sistem jaringan, peralatan tersebut mempunyai log-log berupa data pada saat terjadinya serangan. Log-log atau event yang dihasilkan oleh perangkat tersebut akan dikirimkan ke server OSSIM untuk dijadikan inputan sebagai informasi dari serangan. Meskipun OSSIM mempunyai sensor sendiri yaitu Snort yang fungsinya juga mendeteksi serangan, namun dengan mengintegrasikan perangkat tersebut ke OSSIM server, data yang didapatkan akan dikorelasikan oleh OSSIM ini, sehingga menghasilkan informasi kejadian kondisi keamanan jaringan secara lebih cepat. Pada Gambar 3.1 dapat dilihat topologi jaringan dari rancangan implementasi OSSIM server pada jaringan perusahaan tempat implementasi OSSIM akan dilakukan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 3.1 Topologi Jaringan

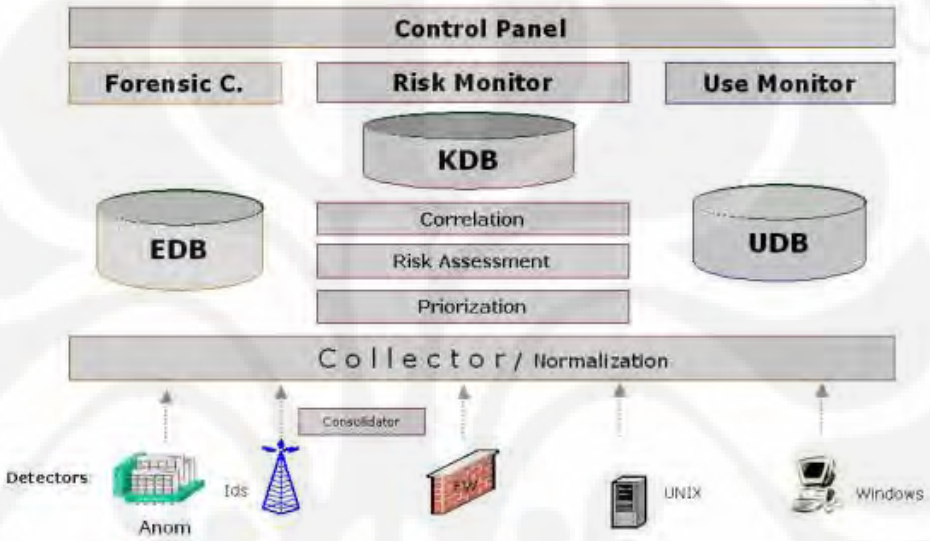
Pada implementasi perangkat yang akan dikelola terdiri dari perangkat-perangkat keamanan jaringan komputer yaitu IDP dan Firewall. IDP yang ada pada perusahaan berjumlah 4 perangkat dan keempatnya dikelola oleh 1 buah NSM server, *log* atau *event* yang dihasilkan IDP diterima oleh NSM server. Sehingga OSSIM server hanya perlu mengambil *log* yang dihasilkan oleh NSM server. Firewall yang ada pada perusahaan berjumlah 5 buah, Firewall tersebut akan dikelola oleh OSSIM server sebagai sebuah detektor OSSIM. Log yang dihasilkan oleh Firewall akan dikirimkan ke server OSSIM sehingga menghasilkan informasi log firewall untuk ditampilkan pada control *panel* pada OSSIM. Selain IDP dan *firewall* OSSIM juga akan mengkonfigurasi perangkat yang ada pada jaringan seperti perangkat *router* dan *switch*. Hal tersebut berfungsi untuk pengelolaan dan informasi dari kondisi perangkat pada jaringan, sehingga dapat diketahui oleh admin melalui pemantauan pada server OSSIM.

3.2.1 Arsitektur Umum

Sistem informasi keamanan ini mempunyai dua dasar pendekatan yaitu, yang pertama adalah bagian proses pendahuluan dimana dilaksanakan oleh

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

detektor atau sensor yang menghasilkan respon terhadap serangan pada sistem jaringan dan yang kedua adalah bagian proses pengumpulan data secara sentral sehingga dihasilkan informasi data keamanan dari sistem jaringan secara terpusat. Gambar dibawah ini adalah bagian-bagian setiap layer yang merepresentasikan arsitektural layer dari *sensor, server*, dan *console*. Setiap bagian layer menjelaskan proses dari sistem ini.



Gambar 3.2 Arsitektur Diagram OSSIM [7]

Terdapat 3 dasar sistem database yang ditunjukkan dalam sistem diagram implementasi ini yaitu EDB (*Event Database),* yaitu merupakan database tempat penyimpanan event-event yang dihasilkan oleh *detektor* atau *sensor*. KDB (*Knowledge Database*), adalah database yang berisi informasi parameter sistem jaringan yang mendefinisikan policy dari kemanan jaringan. UDB atau *Profile database*, yaitu database yang menyimpan informasi sebagai profile dari pemantauan.

3.2.2 Deskripsi dari Sistem

Pada implementasi OSSIM server diintegrasikan dengan perangkat keamanan yang ada pada perusahaan, yaitu IDP dan Firewall sebagai *sensor* atau detektor dari sistem ini. Setiap kejadian yang dihasilkan oleh detektor tersebut

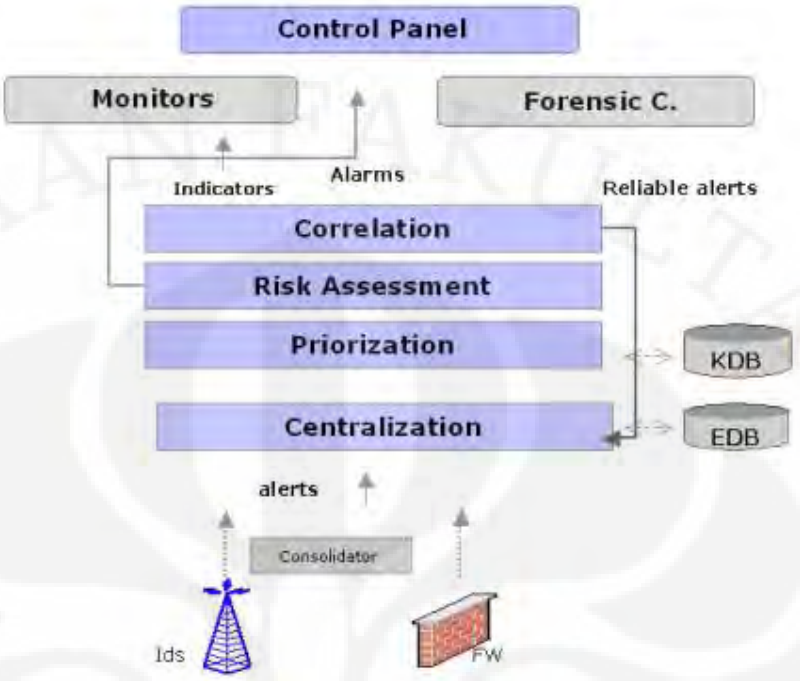
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

berupa *log*, kemudian dari *log* tersebut akan dikirimkan ke server OSSIM dan diidentifikasikan oleh OSSIM server sebagai *pattern* dan *anomaly* detektor *(alerts)*. Adapun langkah-langkah deskripsi dari sistem yang diimplementasikan, atau proses aliran data yang berjalan pada sistem sehingga menghasilkan informasi keamanan jaringan adalah sebagai berikut:

1. Sistem kolektor pada OSSIM menerima *log* tersebut menggunakan beberapa tipe protokol komunikasi.
2. Kolektor tersebut menormalisasi dan melakukan penyimpanan data secara tersentralisasi ke dalam *event database*.
3. Kemudian dilakukan prioritas dari beberapa *log* yang diterima untuk mendefinisikan *security policy* pada sistem penyimpanan KDB.
4. Setelah dilakukan prioritas kemudian dilakukan penganalisaan atau *risk assessment* yang direpresentasikan berupa *alarm* menuju control panel.
5. Untuk prioritas *alerts* yang didefinisikan melakukan korelasi akan dikirim kesetiap proses korelasi untuk menghasilkan informasi yang dapat dipercaya dalam hal terdapat sebuah serangan.
6. Risk monitor secara periodik menampilkan bagian-bagian informasi dari keadaaan kemananan sistem jaringan.
7. Control panel menampilkan semua alarms dan kejadian yang baru saja diterima, informasi-informasi dari sistem keamanan jaringan.
8. Dari Control Panel administrator dapat memantau semua kejadian dari setiap waktu menggunakan *forensic console*.
9. Administrator juga dapat mengecek dan mengkonfigurasi sistem sesuai dengan yang diinginkan dalam melakukan pangamanan dan pemantauan.

Langkah-langkah diatas diilustrasikan pada Gambar 3.3.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 3.3 Diagram Alir Data Dari Sistem [7]

3.3 Rancangan Skenario Penelitian

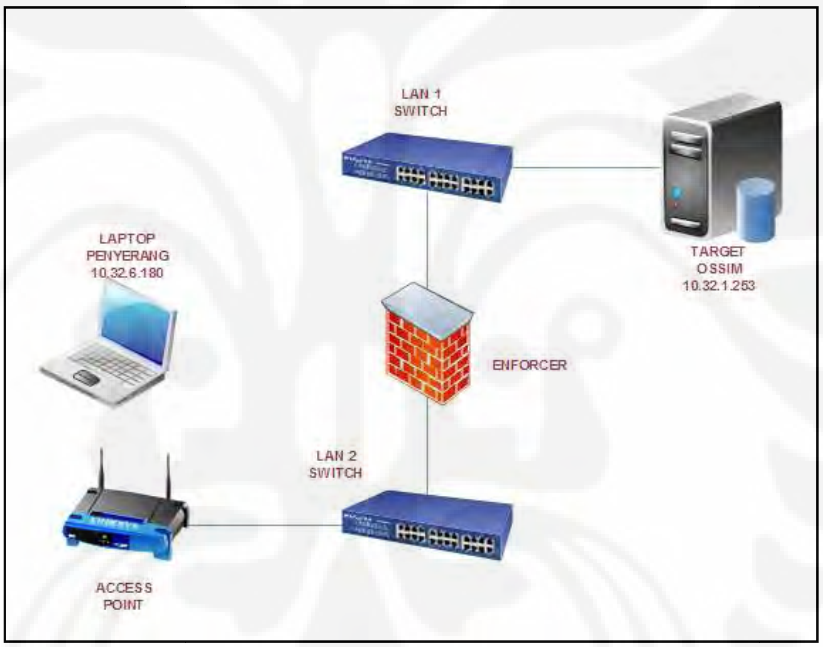
Pada penelitian selanjutnya penulis akan melakukan pengamatan dan analisa terhadap sistem yang telah diimplementasikan dengan membatasi pada beberapa parameter yang dihasilkan oleh sistem tersebut berupa hasil laporan dan pemantauan dari beberapa serangan yang dideteksi oleh sistem. Parameter-parameter yang dibatasi dari pemantauan adalah berupa parameter dari kondisi jaringan selama beberapa pengamatan, untuk waktu pengambilan data yang disesuaikan sejak sistem diimplementasikan. Adapun proses dan parameter pengambilan data yaitu:

1. Proses pengambilan data berupa pengamatan trafik jaringan berupa nilai rata-rata trafik paket protokol yang dideteksi oleh sistem setiap harinya, selama satu pekan berdasarkan waktu yang ditentukan yaitu saat jam kerja dan bukan jam kerja.
2. Parameter data yang diambil yaitu, untuk pengamatan trafik jaringan berupa banyaknya aktivitas protokol yang digunakan pada sistem jaringan yaitu TCP,

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

UDP, dan ICMP. Dari trafik tersebut nantinya akan dianalisa kondisi trafik yang memungkinkan terdapat serangan pada jaringan.

3. Pada Skripsi ini juga akan dilakukan rancangan skenario pengujian sistem yang telah diimplementasikan untuk membuktikan performa dari sistem terhadap adanya serangan. Pengujian hanya dilakukan sekali yaitu pengujian serangan dengan melakukan serangan Ping ICMP *flooding* ke server OSSIM selama beberapa menit dengan besar paket 1000 bytes. Dari proses pengujian tersebut akan dilakukan analisa data berupa kejadian yang dilaporkan sistem dalam menanggapi adanya serangan pada waktu dan hari pengujian. Adapun rancangan skenario serangan dapat dlihat pada Gambar 3.4.



Gambar 3.4 Topologi Skenario Ping *flooding* ICMP

Dari skenario pengambilan data diatas nantinya didapatkan analisa data mengenai performa dari server OSSIM untuk mendeteksi berbagai jenis macam serangan yang ada pada sistem jaringan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

BAB 4

IMPLEMENTASI DAN UJI COBA SISTEM PADA JARINGAN

4.1 Implementasi

4.1.1 Spesifikasi Perangkat Server OSSIM

Adapun spesifikasi perangkat yang digunakan dalam membangun server OSSIM ini adalah sebuah komputer rak server dari *Platform* Dell PowerEdge 750, seperti terlihat pada Gambar 4.1, dimana spesifikasi *hardware*-nya adalah:

1. *Processor* Intel Pentium 4 3,2Ghz.
2. *Memory* 1.00 Gb.
3. *Hard disk* 32 Gb.
4. 1 *port network interface*
5. 1 buah *CD-Room Drive*
6. 1 buah *Keyboard*
7. 1 buah *Monitor*

Gambar 4.1 Server OSSIM

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

4.1.2 Konfigurasi

Langkah pertama dalam melakukan konfigurasi OSSIM adalah mengetahui bagian mana saja dari jaringan yang akan dipantau dan dikelola, baik itu hostnya, perangkat keamanan dan sistem jaringan.

4.1.2.1 Konfigurasi Host

Pada penelitian ini penulis melakukan konfigurasi sesuai dengan deskripsi sistem pada bab sebelumnya. *Host* yang akan dipantau atau dikelola terdiri dari 6 buah firewall, 4 buah IDP, 2 router, 4 switch, dan sebuah NSM (*Netscreen Security Manager*). *Host* tersebut akan didaftarkan OSSIM supaya memudahkan *administrator* dalam melakukan pemantauan dan pengelolaan, sebagai contoh yaitu pemantauan *availability host*. Pada saat mendaftarkan *host,* perlu mendefinisikan nilai *asset* dari host tersebut, karena nilai *asset* akan menentukan nilai resiko dari sistem. Penulis mengklasifikasikan nilai *asset* berdasarkan tingkat keamanan masing-masing *host*. Semakin rentannya *host* tersebut terhadap serangan maka semakin tinggi nilai *asset*-nya. Nilai *asset* dari *firewall* dan IDP diberi nilai 5, *router* diberi nilai 3, *switch* diberi nilai 2 dan untuk NSM server dan OSSIM diberi nilai 1. Contoh proses pendaftaran *host* dan penentuan *asset* dapat dilihat pada Gambar 4.2.

Gambar 4.2 Tampilan Dalam Melakukan Pengaturan Host

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

4.1.2.2 Konfigurasi Jaringan

Konfigurasi jaringan bertujuan untuk mendefinisikan jaringan mana saja yang akan dikelola. Pada penelitian skripsi ini, jaringan yang dimonitor adalah jaringan yang menuju server, yaitu jaringan yang berada dibelakang IDP. Terdapat 5 segmen jaringan server dibelakang IDP dan 1 segmen jaringan *host* karyawan perusahaan. Seperti pada proses konfigurasi *host*, proses konfigurasi jaringan juga perlu pendefinisian nilai *asset* dari jaringan, yang nantinya juga menentukan nilai resiko dari jaringan tersebut. Nilai asset pada jaringan ditentukan berdasarkan seberapa besar jaringan tersebut berharga, artinya seberapa besar keinginan untuk mengamankan host-host tersebut. Jaringan server adalah jaringan yang perlu dijaga dari serangan sehingga nilai asset yang didefinisikan juga tinggi. Klasifikasi nilai yang ditentukan adalah:

1. Asset jaringan server = 5
2. Asset jaringan host karyawan = 2

Gambar 4.3 adalah jaringan yang akan dikelola oleh OSSIM.

Gambar 4.3 Konfigurasi Jaringan yang Dikelola

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

4.1.2.3 Konfigurasi *Policy*

Policy di buat untuk mengatur bagian mana saja yang akan di monitor dan dikelola terhadap serangan yang ada. Pada saat pengaturan *policy* perlu didefinisikan nilai prioritas dari setiap policy yang dibuat untuk menentukan nilai resiko terhadap sistem jaringan. Dalam penentuan prioritas *policy* yang dianggap penting untuk dikelola dan diamankan jaringannya diberi nilai yang lebih tinggi yaitu nilai 5. Sebagai contoh penentuan *policy* yang akan menuju ke server diberi nilai 5. Gambar 4.4 adalah salah satu pengaturan policy yang menuju jaringan server.

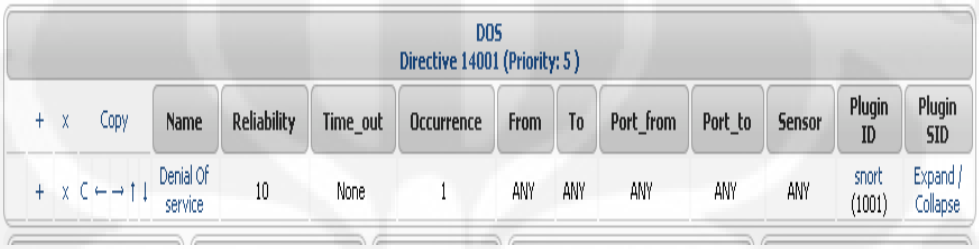
Gambar 4.4 Pengaturan *Policy* Jaringan

4.1.2.4 Konfigurasi *Directive Rule*

Pada bagian ini dilakukan pengkoreksian/pengubahan *default rule corelation directive* OSSIM. *Directive rule* berfungsi untuk mendefinisikan macam-macam serangan terhadap detektor yang menanganinya. Pada bagian ini terdapat bagian dimana perlu melakukan perubahan nilai *reliability* dari sensor saat dia mendeteksi serangan, misalnya Snort mendeteksi adanya *intrusion* dengan

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

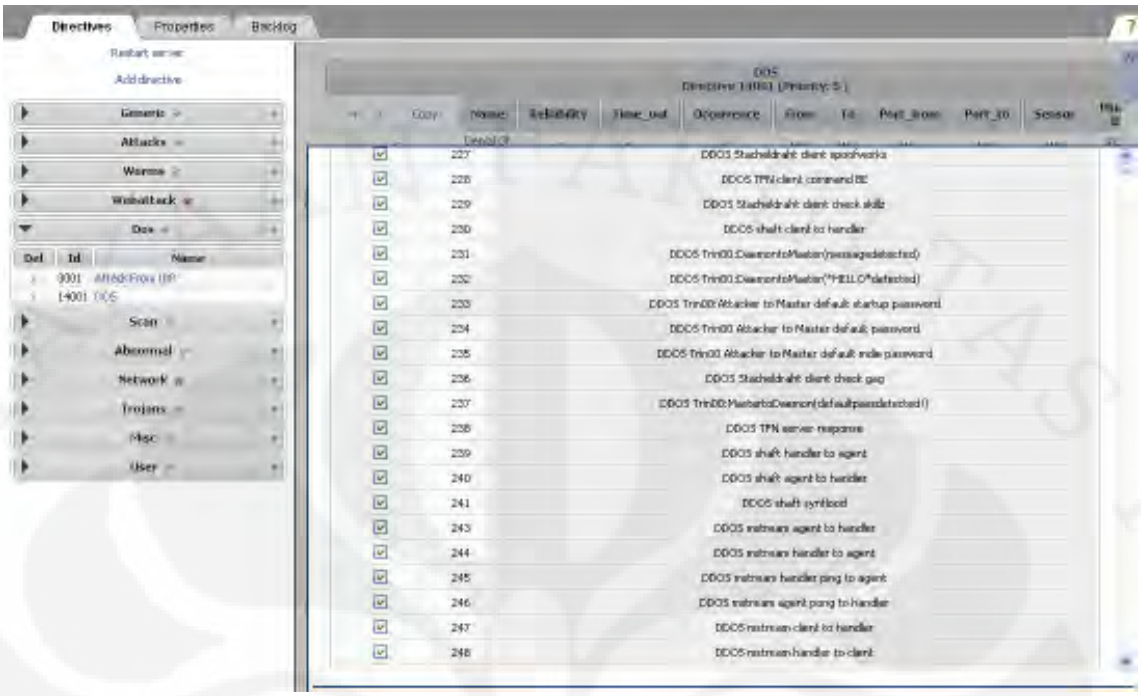
tingkat kepercayaan yang ditentukan, semakin tinggi tingkat kepercayaannya maka akan mempengaruhi nilai resiko yang akan dihasilkan. Pada bagian ini penulis juga menambahkan perintah rule seperti mendefinisikan *ping anomaly* dan DOS, *ping anomaly* didefinisikan dengan prioritas 3 dan nilai *reliability* 10 sedangkan DOS didefinisikan dengan prioritas 5 dan nilai *reliabity* 10. Semua itu ditangani oleh detektor Snort. Gambar 4.5 adalah perintah yang ditambahkan pada rule di OSSIM.



Gambar 4.5 Rule yang Ditambahkan

Rule ditambahkan untuk menspesifikasikan serangan yang muncul supaya nilai resiko dapat diklasifikasikan, yaitu resiko yang sifatnya kecil, menengah dan tinggi. Agar *rule* yang ditambahkan dapat menangani serangan secara tepat, maka perlu juga mengedit plugin SID, plugin SID adalah macam-macam tipe serangan yang ditangani oleh detektor, sebagai contoh *directive* DOS *plugin* SID-nya ditunjukkan pada Gambar 4.6.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 4.6 Plugin SID Snort untuk Directive DOS

Penentuan nilai resiko yang ditampilkan OSSIM adalah hasil dari *event* yang dihasilkan oleh beberapa *tools* OSSIM. Dibawah ini akan dijelaskan bagaimana OSSIM melakukan kalkulasi terhadap resiko yang muncul. Adapun parameter nilai resiko yang dihasilkan ditentukan oleh nilai *asset*, prioritas, dan *reliability*. Formula dalam melakukan kalkulasi resiko adalah sebagai berikut:

$$\text{Resiko} = \frac{\text{asset x priority x reliability}}{25} \quad \text{.....[6]}$$

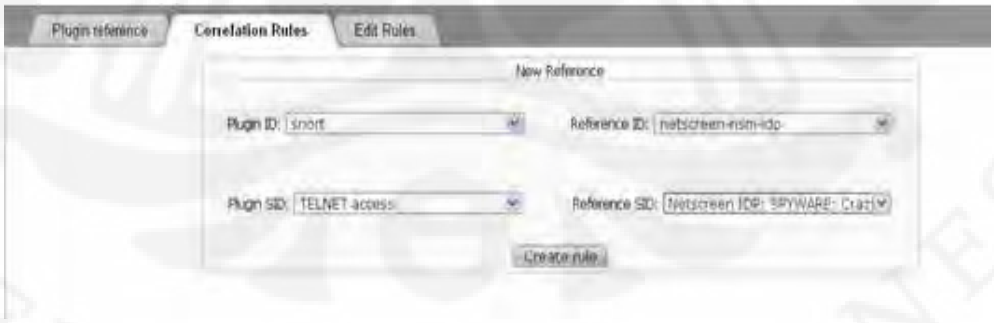
Seperti pada pengaturan *host* dan jaringan perlu mendefinisikan nilai *asset* dari *host* dan jaringan yang akan kita kelola. Nilai *asset* berkisar antara 1-5 dimana semakin tinggi nilai *host* dan jaringan didefinisikan, maka akan semakin tinggi nilai kepentingan dari *host* dan jaringan tersebut, artinya semakin dijagalah *asset host* dan jaringan tersebut. Sedangkan nilai *reliability* adalah nilai yang didefinisikan ketika kita mengkonfigurasi rule korelasi OSSIM. Nilai *reliability* berkisar antara 1-10, semakin tinggi nilai *reliability* maka akan semakin tinggi nilai yang dapat dipercaya terhadap *rule* tersebut. Nilai yang dipercaya disini adalah tingkat kepercayaan atau nilai dari serangan yang muncul. Apabila kita

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

anggap sebuah serangan tertentu memilki nilai yang tinggi dalam merusak sistem jaringan maka nilai *reliability* juga harus tinggi. Sedangkan penentuan nilai prioritas didefinisikan pada saat melakukan konfigurasi *rule* pada detektor, OSSIM adalah manajemen *tools* dimana mengatur detektor-detektor yang ada untuk saling berkolaborasi dalam mendeteksi serangan, sehingga penentuan prioritas adalah penentuan dari detektor yang ditunjuk untuk lebih dahulu dipercaya dalam menagani serangan, disamping itu penentuan prioritas juga digunakan ketika mendefinisikan *policy*.

4.1.2.5 Konfigurasi Korelasi antar Detektor

Salah satu keunggulan OSSIM adalah adanya teknik korelasi antar detektor. Korelasi antar detektor dimaksudkan untuk menilai kebenaran dari adanya serangan yang muncul, karena *log-log* yang dihasilkan oleh setiap detektor berbeda-beda dan masing-masing juga mendeteksi serangan yang berbeda-beda, sehingga teknik korelasi antar detektor menjadi sebuah nilai dari OSSIM untuk melakukan analisis terhadap adanya serangan yang dideteksi oleh detektor yang dihubungkan ke server OSSIM. Pada penelitian ini penulis menambahkan *rule* korelasi antar detektor yang dimiliki perusahaan yaitu detektor *netscreen-nsm-idp* dan *firewall*. Kemudian juga menambahkan *rule* korelasi antara detektor OSSIM yaitu *Snort* dengan *netscreen-nsm-idp*. Gambar 4.7 adalah korelasi antar detektor yang didefinisikan oleh penulis dalam penelitian.



Gambar 4.7 Korelasi Antar Detektor

4.1.2.6 Konfigurasi Perangkat IDP dan Firewall

Konfigurasi ini ditujukan untuk mengambil *log* yang ada pada perangkat keamanan untuk dikirimkan ke server OSSIM sehingga Informasi *event* atau *log*

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

dari perangkat dikumpulkan ke server OSSIM untuk dijadikan informasi yang terpadu terhadap kondisi keamanan dari jaringan yang dikelola. Pada penelitian ini hanya mengambil informasi *event log* dari 2 perangkat security yaitu IDP sebagai informasi dari serangan yang dideteksi dan *firewall* yang berisi informasi trafik dan event dari log yang dihasilkan firewall tersebut. IDP yang ada pada perusahaan berjumlah 4 perangkat dan keempatnya dikelola oleh 1 buah NSM server, *log dan event* yang dihasilkan IDP diterima oleh NSM server. Sehingga OSSIM server hanya perlu mengambil log yang dihasilkan Oleh NSM server. Adapun Pengaturan untuk mengirimkan *log* dari NSM server yaitu masuk ke menu konfigurasi NSM server dengan memilih menu Action Manager, kemudian memilih sub menu Action Parameter dan masukan alamat IP OSSIM pada pilihan *syslog server* IP

Firewall yang ada pada perusahaan berjumlah 5 buah, *firewall* tersebut akan dikelola oleh OSSIM server sebagai sebuah detektor OSSIM, log yang dihasilkan oleh *firewall* akan dikirimkan ke OSSIM server sehingga menghasilkan informasi log *firewall* untuk ditampilkan pada control panel OSSIM. Beda halnya dengan perangkat IDP, *firewall* tidak memilki server khusus yang mengelola mereka, sehingga untuk mengirimkan log *firewall* ke OSSIM server harus mengkonfigurasi semua perangkat firewall yang ada. Gambar 4.8 adalah salah satu contoh konfigurasi *firewall* untuk mengirimkan log dan eventnya ke OSSIM.

Gambar 4.8 Konfigurasi *Firewall*

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Dari gambar 4.8 dapat dilihat bahwa *log* yang dikirimkan ke alamat IP server OSSIM adalah *log* yang berupa *trafik log* dan *event log*.

4.2 Pengambilan Data dan Analisis

4.2.1 Trafik Jaringan

Biasanya suatu lalu lintas jaringan menggunakan beberapa tipe protokol. Protokol digunakan untuk berhubungan antar komputer. Agar dua buah komputer dapat berkomunikasi dan saling bertukar informasi maka diperlukan suatu protokol yang sama. Sehingga banyaknya lalu-lintas yang ada pada sebuah jaringan adalah banyaknya trafik protokol yang ada pada jaringan tersebut. OSSIM server memiliki *feature* untuk melakukan pengamatan trafik jaringan, pengamatan trafik jaringan kali ini adalah pengamatan trafik protokol yang dideteksi oleh server OSSIM. Pada skripsi ini penulis melakukan pengamatan dan pengambilan data trafik protokol pada sistem jaringan kemudian melakukan analisis kondisi trafik jaringan dengan beberapa waktu pengamatan yaitu saat jam kerja (pukul 08.00-17.00) dan bukan jam kerja (pukul 17.00-08.00) selama kurun waktu seminggu yaitu dari tanggal 1 Juni 2010 sampai 7 Juni 2010. Adapun data yang diambil adalah data nilai rata-rata dari protocol TCP, UDP dan ICMP. Data hasil pengamatan trafik TCP selama seminggu dapat dilihat pada Tabel 4.1, sedangkan trafik UDP dapat dilihat pada Tabel 4.2 dan trafik ICMP dapat dilihat pada Tabel 4.3.

Tabel 4.1 Trafik TCP

Hari ke	Jam Kerja	Bukan Jam Kerja
1	410,5 kb/s	159,3 kb/s
2	865,2 kb/s	1,4 Mb/s
3	677,5 kb/s	142,0 kb/s
4	448,2 kb/s	337,9 kb/s
5	387,9 kb/s	472,6 kb/s
6	208,0 kb/s	633,4 kb/s
7	1,3 Mb/s	626,8 kb/s

Tabel 4.2 Trafik UDP

Hari ke	Jam Kerja	Bukan Jam Kerja
1	267 kb/s	70,5 kb/s
2	88,0 kb/s	67,0 kb/s
3	78,5 kb/s	1,9 kb/s
4	64,8 kb/s	9,6 kb/s
5	46,6 kb/s	65,7 kb/s
6	76,1 kb/s	83,3 kb/s
7	35,1 kb/s	3,7 kb/s

Tabel 4.3 Trafik ICMP

Hari ke	Jam Kerja	Bukan Jam Kerja
1	138,2 b/s	70,5 kb/s
2	119,9 b/s	67,0 kb/s
3	224 b/s	421,8 b/s
4	610,2 b/s	398,1 b/s
5	223,7 b/s	111,0 b/s
6	112,2 b/s	118,4 b/s
7	319,0 b/s	426,9 b/s

Keterangan:

Hari Sabtu dan Minggu
Trafik Terbesar
Trafik Terkecil

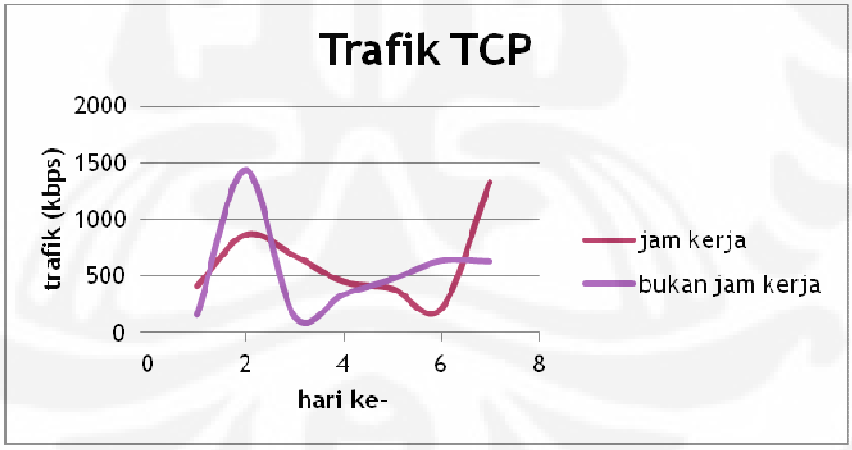
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Tujuan pengambilan data ini adalah untuk menganalisis kondisi keamanan dari jaringan, dengan cara mengamati perubahan trafik jaringan. Dari data pengamatan sepekan didapatkan bahwa kondisi rata-rata trafik jaringan dari ketiga protokol, saat jam kerja lebih besar dibandingkan dengan data yang diambil saat bukan jam kerja. Data tersebut dapat dilihat pada tabel 4.4.

Tabel 4.4 Rata-rata Trafik Protokol

Protokol	**Jam kerja**	**Bukan Jam kerja**
TCP	613,7 kb/s	538,85 kb/s
UDP	93,7 kb/s	43,1 kb/s
ICMP	249,6 b/s	230,5 b/s

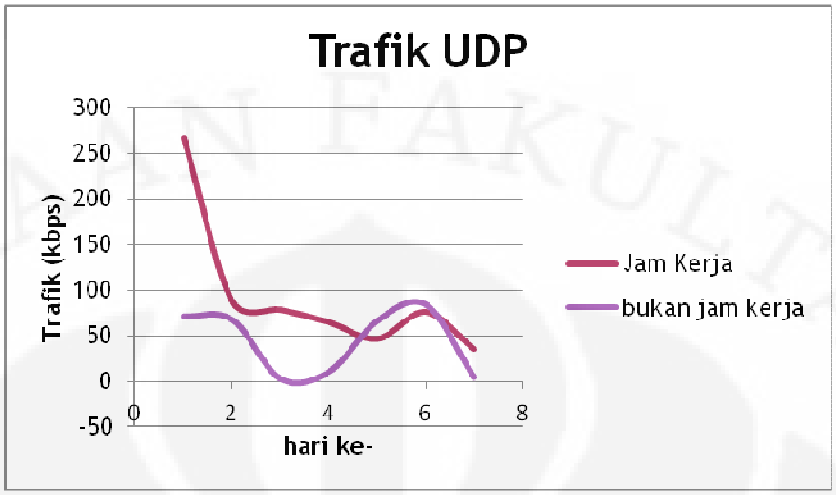
Dari data tersebut dapat diambil kesimpulan bahwa saat jam kerja aktivitas pada jaringan memiliki trafik yang tinggi. Rata-rata trafik TCP pada jam kerja lebih besar 74,85 kb/s, rata-rata trafik UDP pada jam kerja lebih besar 50,6 kb/s dan rata-rata trafik ICMP pada jam kerja lebih besar 19,1 b/s.



Gambar 4.9 Grafik pengamatan TCP

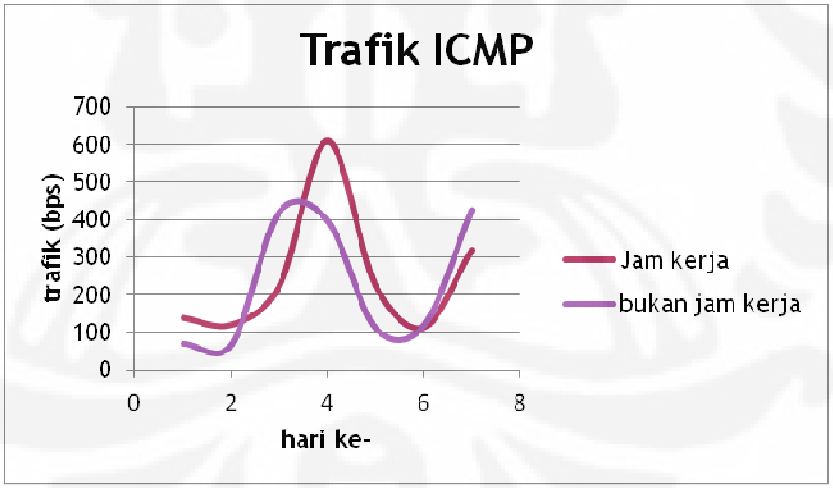
Dari Pengamatan trafik protokol TCP selama sepekan seperti yang ditunjukkan pada grafik Gambar 4.9, dapat diketahui bahwa pemakaian protokol tersebut setiap harinya bersifat *fluktuatif* dimana kondisi setiap harinya tidak dapat diprediksi nilai yang pasti terhadap pemakaian protokol TCP.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 4.10 Grafik pengamatan UDP

Sementara untuk pengamatan trafik protokol UDP selama sepekan seperti yang ditunjukan pada Gambar 4.10. Pemakaian protokol tersebut setiap harinya juga bersifat *fluktuatif* dimana kondisi setiap harinya tidak dapat diprediksi nilai yang pasti, namun dari grafik masih bersifat normal untuk pemakaian trafik protokol tersebut, karena kondisi antara jam kerja memang lebih tinggi dibandingkan dengan kondisi trafik pada saat bukan jam kerja.



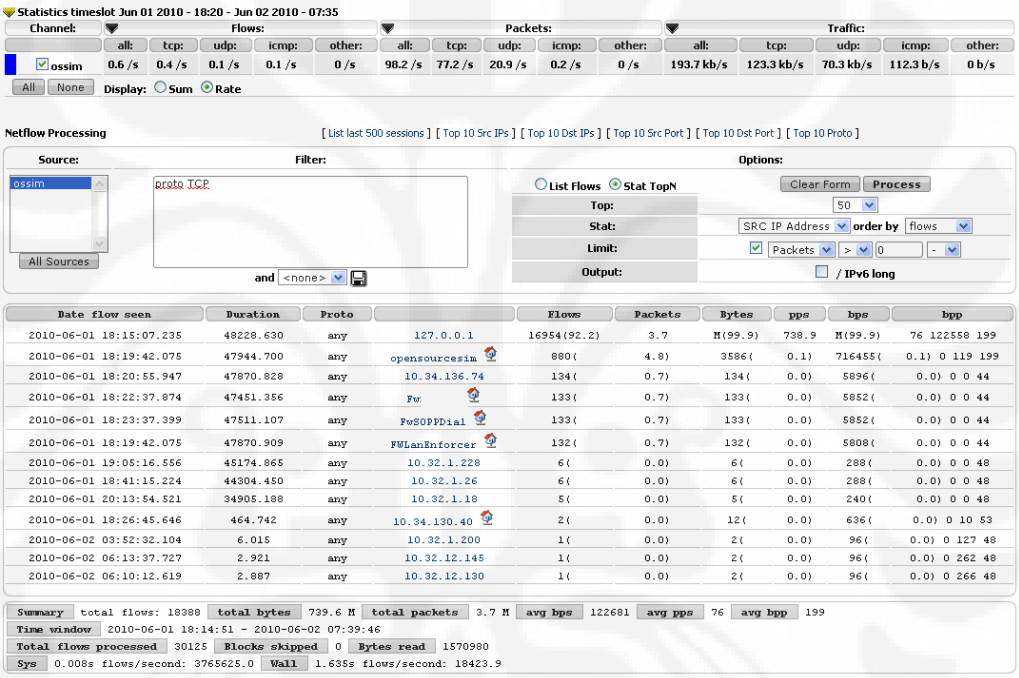
Gambar 4.11 Grafik pengamatan ICMP

Sementara untuk pengamatan grafik ICMP yang ditunjukkan pada Gambar 4.11 juga masih bersifat normal untuk kondisi saat jam kerja dan bukan jam kerja, tetapi pada hari ketujuh pengamatan, diketahui bahwa kondisi pada saat bukan jam kerja lebih tinggi dibandingkan kondisi pada saat jam kerja. Namun selisih dari rata-rata pada hari tersebut masih terlalu kecil.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Dalam melakukan pengamatan trafik jaringan perlu juga mengetahui aktivitas yang terjadi dalam jaringan tersebut, setiap trafik yang digunakan pada suatu waktu dengan menunjukkan trafik yang tinggi, maka perlu diduga sebagai suatu anomali dari jaringan. Untuk melakukan pengecekan apakah pada waktu tertentu diduga adanya serangan maka diperlukan pengecekan Top IP yang menggunakan protokol tersebut dan *service port* yang digunakan oleh IP tersebut.

Pada Gambar 4.12 adalah data pengamatan Top 10 *Source* IP yang menggunakan protokol TCP pada tanggal 1-2 Juni 2010 (bukan jam kerja).

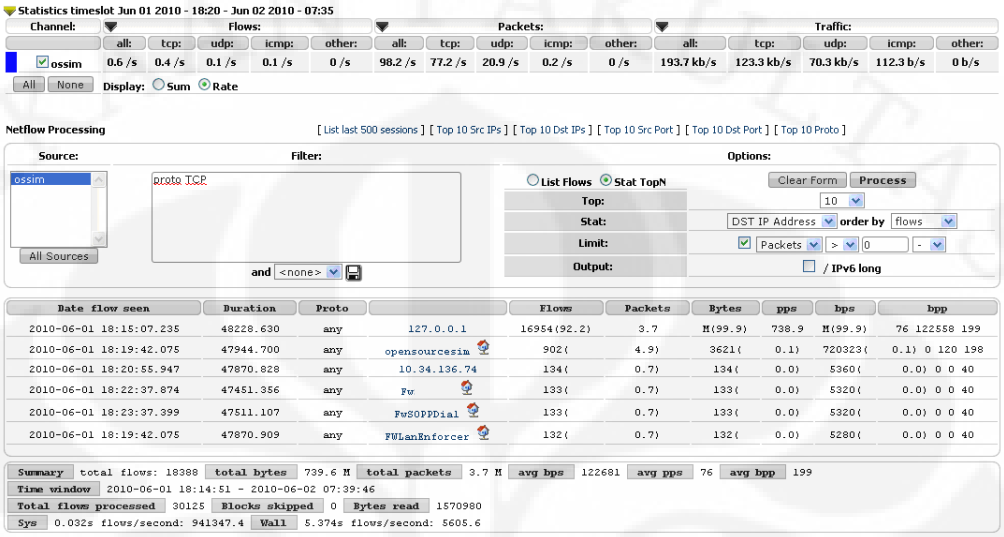


Gambar 4.12 Pengamatan Top 10 *Source* IP protokol TCP

Setiap sumber IP yang menggunakan protokol dengan besarnya trafik, paket dan flow yang tinggi pada suatu waktu, maka bisa diduga sebagai suatu IP penyerang, terlebih jika IP tersebut adalah IP yang tidak dikenali oleh *administrator* atau bukan IP yang biasa menggunakan protokol dengan trafik yang tinggi. Karena pada saat suatu IP sumber yang melakukan aktivitas yang tinggi, seperti melakukan *flooding* atau membanjiri suatu paket protokol sehingga dapat mengancam sebuah sistem jaringan. Dengan membajiri suatu paket protokol pada jaringan dapat mengakibatkan *denial of service* (DOS) pada sistem jaringan. Apabila memang terbukti ada ancaman *denial of service* (DOS) maka juga perlu

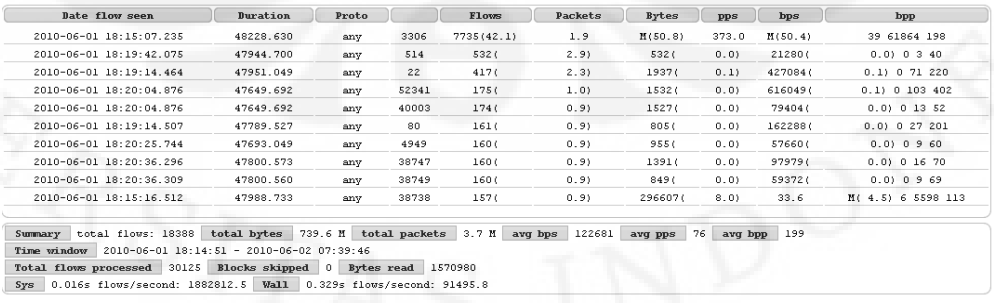
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

mengamati Top destination IP yang menggunakan banyaknya protokol tersebut. Salah satu bentuk pengamatan Top destination IP dapat dilihat pada Gambar 4.13.



Gambar 4.13 Pengamatan Top 10 *Destination* IP protokol TCP

Dengan mengamati tujuan IP yang banyak menggunakan protokol tersebut maka bisa melakukan tindakan pengamanan IP tersebut. Pengamatan dari trafik jaringan adalah pengamatan aktivitas dari paket protokol yang digunakan dalam sistem jaringan. Parameter – parameter yang diperlukan dalam pengamatan aktivitas trafik jaringan adalah sumber dan tujuan IP *address* tersebut dan besarnya protokol yang digunakan oleh IP tersebut. Selain itu untuk lebih mengetahui aktivitas dan dugaan serangan pada sistem jaringan juga diperlukan pengamatan *service port* yang digunakan oleh IP *address* tersebut. Pada Gambar 4.14 adalah pengamatan Top 10 source port yang digunakan dalam sistem jaringan.

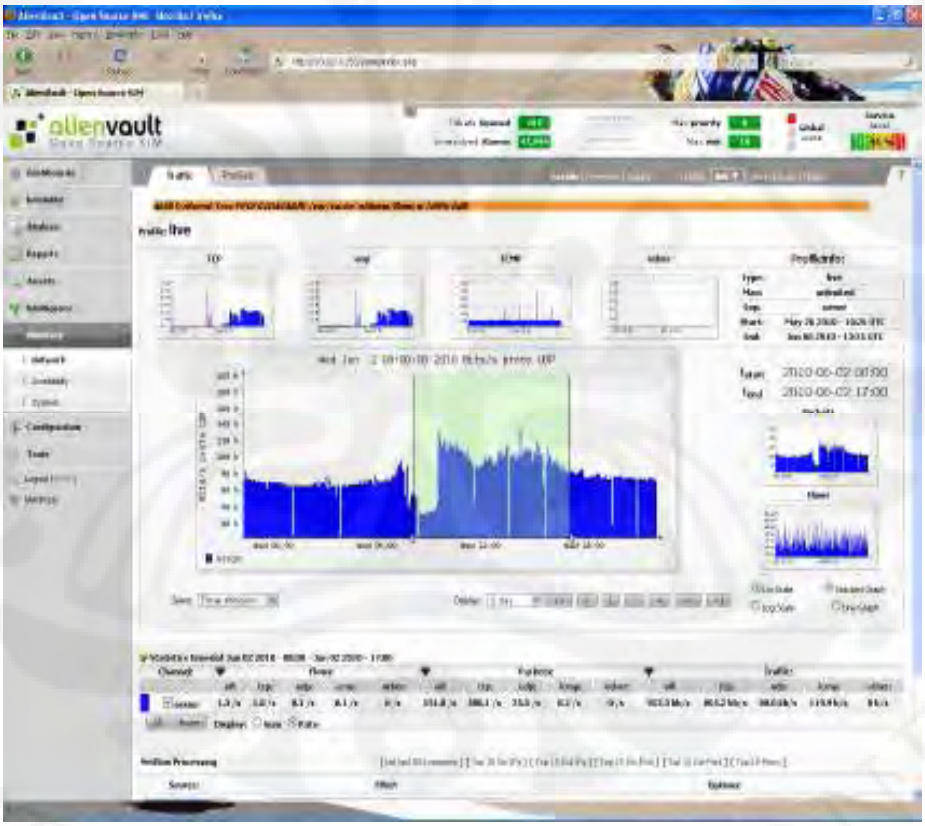


Gambar 4.14 Top *Source port* yang menggunakan Protokol TCP

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Setiap port digunakan pada lalu lintas sistem jaringan seperti sebuah *service* yang dilakukan melalui port tersebut, maka perlu dilakukan tindakan dalam melakukan pengamanan, terlebih untuk *service port* yang *vulnerable*. Karena *service port* yang *vulnerable* dapat mengancam kondisi keamanan dari jaringan. Tindakan yang dapat dilakukan *administrator* terhadap *service port* yang *vulnerable* yaitu melakukan *monitoring* atau melakukan pemutusan (blok) port, tergantung seberapa besar ancaman terhadap aktivitas port yang dilakukan pada sistem jaringan tersebut.

Salah satu data grafik yang dihasilkan oleh server OSSIM pada tanggal 2 Juni 2010 saat jam kerja dapat dilihat pada Gambar 4.15 dan data grafik keseluruhan selama seminggu pengamatan dapat dilihat pada Lampiran 2.



Gambar 4.15 Grafik Pemantauan Trafik Jaringan

Untuk lebih jelasnya dalam memantau kondisi keamanan jaringan, selain mengamati aktivitas trafik jaringan diperlukan juga analisis terhadap *top source* IP dan *top destination* IP yang menggunakan protokol tersebut dan laporan SIEM

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

event yang dihasilkan oleh OSSIM. Untuk dapat membuktikan hal tersebut maka akan dilakukan pengamatan dan skenario serangan ICMP *flooding* pada sub bab berikutnya.

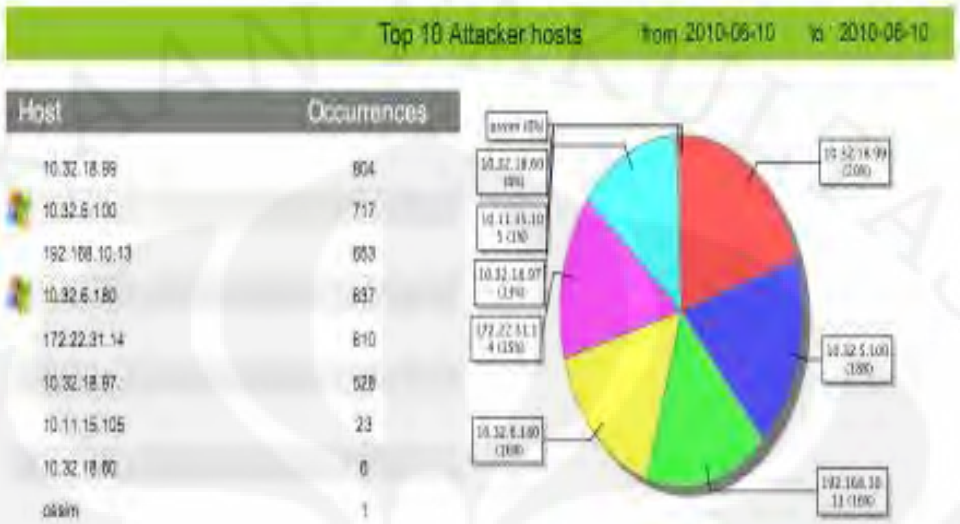
4.2.2 Data dan Analisis Pengamatan SIEM *event* Untuk Skenario Serangan

Salah satu laporan yang dihasilkan oleh server OSSIM adalah data *Security Information Event Management* (SIEM *event*). Laporan tersebut merupakan hasil korelasi dan informasi kejadian dari semua detektor yang dijadikan sebagai *agent* dari ossim yaitu NSM, Firewall, Snort dan detektor lainnya. Adapun laporan yang dihasilkan oleh SIEM *event* ini berisi Top 10 *attacker hosts*, Top 10 *attacked hosts*, dan Top 15 *events*.

1. Top 10 *attacker hosts* adalah informasi yang berisi peringkat 10 besar penyerang dari sistem jaringan yang dikelola, parameter dalam penentuan Top 10 attacker adalah banyaknya kejadian atau *event* yang dideteksi Oleh sistem yaitu *log event* yang dihasilkan oleh detektor-detektor OSSIM.
2. Top 10 *attacked hosts* adalah informasi yang berisi peringkat 10 besar host yang diserang, parameter penentuan dari Top *attacked* ini juga berasal dari banyaknya kejadian atau event yang dideteksi oleh sistem.
3. Top 15 events adalah informasi yang berisi 15 besar peringkat dari banyaknya suatu kejadian yang dideteksi oleh OSSIM.

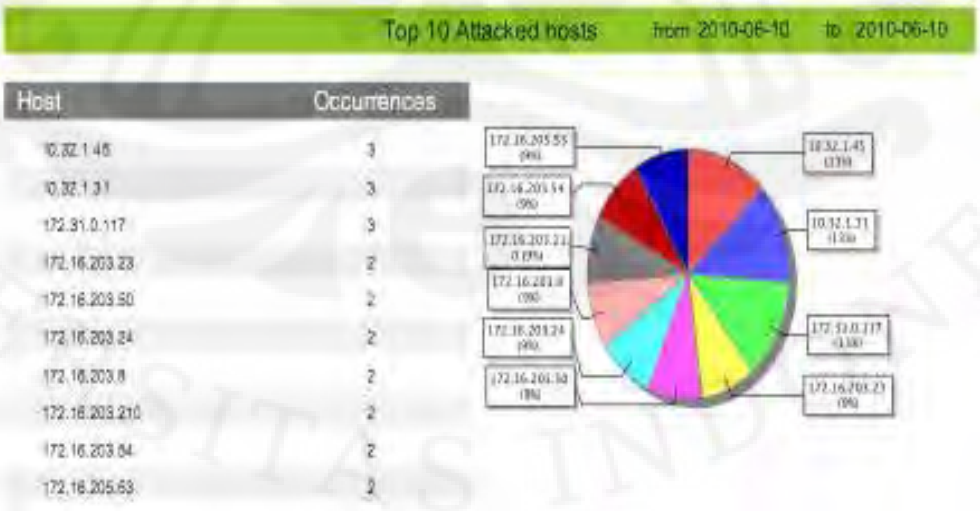
Dari data akan dianalisa mengenai hasil informasi yang diberikan oleh OSSIM terhadap kejadian yang ada pada sistem jaringan pada perusahaan, data SIEM *event* ini akan diambil dalam waktu satu hari pengamatan yaitu pada tanggal 10 Juni 2010. Dimana pada saat itu akan di lakukan skenario penyerangan terhadap sistem jaringan yaitu melakukan *flooding* ICMP terhadap server OSSIM dengan parameter ping selama 10 menit dan diberikan beban paket ICMP sebesar 1000 bytes. Data laporan SIEM event dalam melakukan skenario penyerangan dapat dilihat pada Gambar 4.16 dan data tersebut adalah data kondisi kejadian pada tanggal 10 Juni 2010.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 4.16 Laporan SIEM *event* Top 10 *Attacker* Pada Tanggal 10 Juni 2010

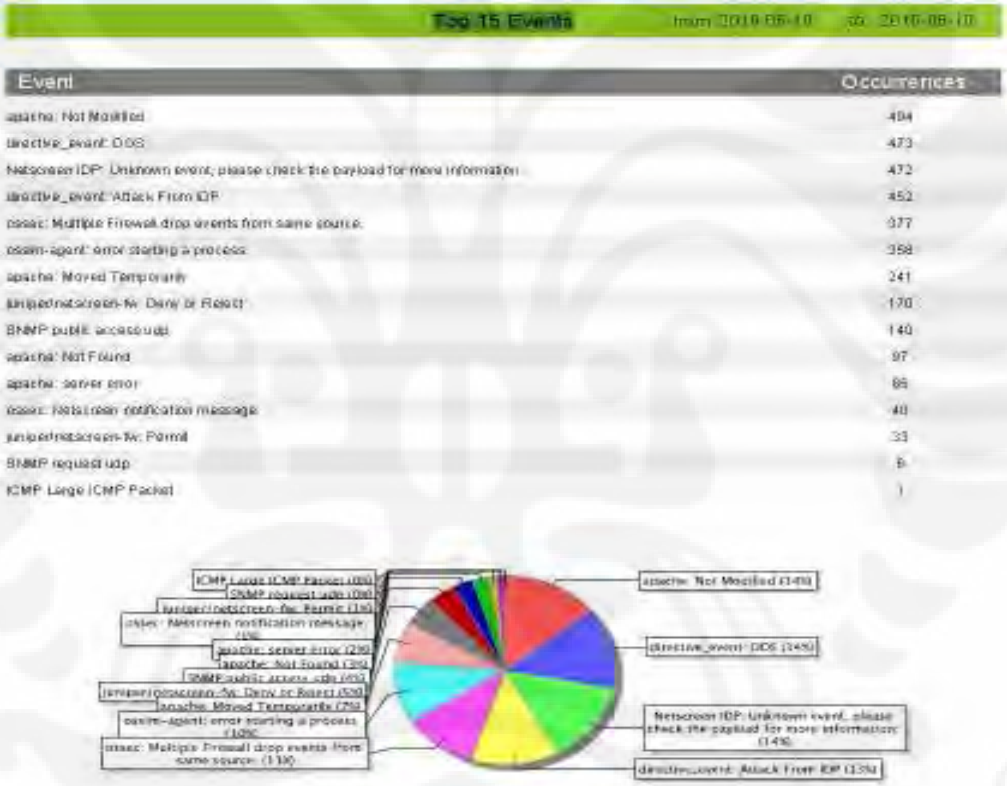
Pada Gambar 4.16 dapat dilihat IP 10.32.6.180 (IP yang digunakan penulis dalam melakukan serangan) dideteksi OSSIM sebagai IP penyerang. Pada data tersebut IP 10.32.6.180 ada pada urutan ke 4 *top attacker* dalam 1 hari dengan banyaknya kejadian yang dilaporkan OSSIM sebanyak 637. Namun jika dilihat pada pengamatan trafik jaringan dalam selang waktu saat penyerangan seperti terlihat pada Gambar 4.20 dapat dilihat bahwa IP tersebut merupakan *top attacker*.



Gambar 4.17 Laporan SIEM *event* Top 10 *Attacked* Pada Tanggal 10 Juni 2010

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

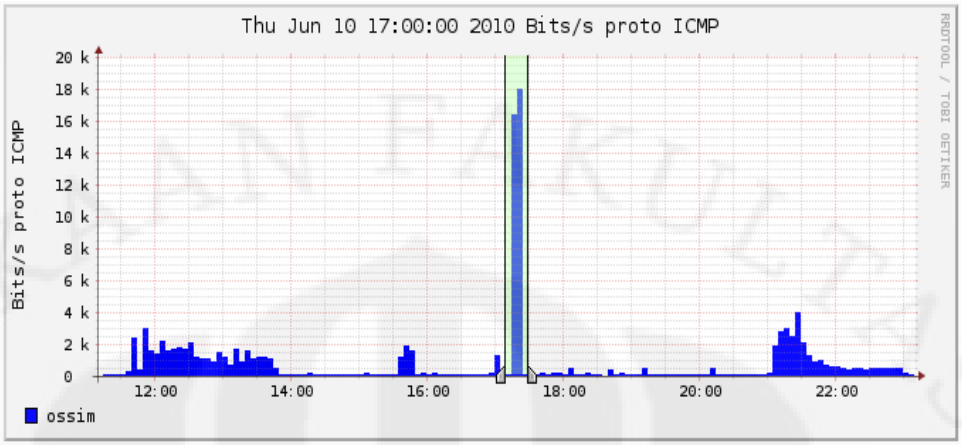
Pada bagian *Top attacked host* pada Gambar 4.17, server OSSIM tidak dideteksi sebagai host yang diserang karena memang skenario dilakukan hanya sekali dan hanya beberapa menit, sedangkan data SIEM event adalah data yang diambil selama satu hari. Sehingga *host* OSSIM tidak masuk dalam Top 10 *attacked*. Kemudian pada bagian Top 15 *event* yang ditunjukkan pada Gambar 4.18, terdapat satu kejadian event yaitu *ICMP Large ICMP packet*, karena paket yang dikirim besar jadi OSSIM mendeteksi ada paket ICMP yang tidak normal dikirimkan.



Gambar 4.18 Laporan SIEM *event* Top 15 *Events* Pada Tanggal 10 Juni 2010

Untuk mengetahui bukti selanjutnya dilakukan pengecekan dengan melakukan pemantauan trafik jaringan sesuai waktu saat melakukan serangan. Dengan mengamati grafik dari trafik jaringan menjadi sebuah referensi akan adanya serangan. Grafik pemantauan trafik jaringan dapat dilihat pada Gambar 4.19

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Gambar 4.19 Grafik Pemantauan Trafik ICMP Saat Skenario Serangan

Dari grafik pada Gambar 4.19 pada selang dimana saat skenario serangan menunjukkan tingginya sebuah trafik pada jaringan dengan menggunakan protokol ICMP. Grafik tersebut terlihat lebih tinggi dibandingkan sebelum dan sesudah skenario serangan hal ini membuktikan terdapatnya anomali dari trafik jaringan.

Setelah diketahui dari grafik terdapat anomali dari jaringan, kemudian dilakukan pengecekan terhadap Top *Source* dan Top *Destination* IP yang menggunakan protokol tersebut. Dari data *Host* dengan IP 10.32.6.180 terdaftar sebagai IP terbanyak kedua yang menggunakan packet ICMP. Data tersebut dapat dilihat dari Gambar 4.20 ketika melakukan pemantauan trafik jaringan protocol ICMP pada waktu serangan.

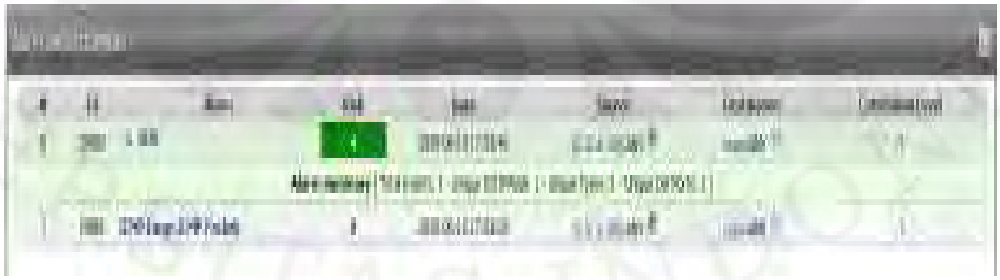
Gambar 4.20 Pemantauan Trafik ICMP Top *source* IP Saat Skenario Serangan

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Pada pemantauan dengan selang waktu saat terjadinya serangan yaitu pada Gambar 4.21 dapat dilihat bahwa IP tersebut juga sebagai *Top destination* IP. Hal ini dikarenakan bahwa sifat dari Ping yaitu mengirimkan paket *reques*t informasi ke IP yang dituju dan kemudian IP yang dituju tersebut me-*reply* kembali paket informasinya.

Gambar 4.21 Pemantauan Trafik ICMP Top *Destination IP* Skenario Serangan

Dari data tersebut membuktikan bahwa OSSIM mendeteksi adanya skenario serangan yang dibuat oleh penulis dan OSSIM dapat menampilkan laporan kejadian serangan secara *real time*. Selain itu melalui skenario serangan yang dilakukan penulis, OSSIM juga mendeteksi adanya *alarm* berupa nilai resiko dari sistem jaringan. Nilai resiko ini sesuai dengan perhitungan nilai kalkulasi yang ditentukan berdasarkan pemberian nilai asset, priority dan realibility. Informasi berupa *alarm* dapat dilihat pada Gambar 4.22.



Gambar 4.22 *Alarm* yang Dihasilkan dari Skenario Serangan

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

Alarm yang dihasilkan dari gambar 4.22 adalah hasil korelasi dari detektor yang ada pada OSSIM, dan sesuai dengan kalkulasi perhitungan resiko yaitu penentuan nilai asset, prioritas dan nilai realibility bahwa nilai resiko dari directive DOS pada saat serangan adalah 4. Directive DOS adalah directive yang ditambahkan pada saat melakukan konfigurasi merupakan sebuah alarm yang menunjukkan nilai resiko yang ada pada suatu serangan, karena serangan Ping *flooding* ini berpotensi terhadap *Denial Of service* (DOS), sehingga muncul alarm yang dihasilkan oleh detektor dan diinformasikan oleh OSSIM. Nilai 4 didapat dari perhitungan kalkulasi dimana nilai asset source dan sumber = 2, prioritas *directive* DOS = 5 dan *realibility* = 10. sehingga perhitungan kalkulasi adalah:

(10 x 5 x 2) : 25 = 4

Sedangkan nilai resiko dari alarm *ICMP Large ICMP Packet* mempunyai nilai resiko 0 karena memang berdasarkan kalkulasi bahwa nilai Priority dan Realibilty secara defauth adalah 1 sehingga

(1 x 1 x 2) : 25 = 0

Dan sesuai dengan data pada Lampiran 1, OSSIM dapat menampilkan *log* dan *event* yang diterima oleh perangkat keamanan jaringan yaitu *firewall* dan IDP. Sehingga disini penulis dapat mengambil kesimpulan bahwa OSSIM lebih efektif dalam melakukan pemantauan kondisi keamanan keseluruhan jaringan.

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

BAB 5

KESIMPULAN

Dari hasil Implementasi dan Analisis data baik pengamatan trafik dan uji coba sistem dapat diambil kesimpulan bahwa:

1. Rata-rata trafik protokol baik TCP, UDP dan ICMP selama satu minggu menunjukkan bahwa, rata-rata trafik jaringan pada saat jam kerja lebih tinggi dibandingkan pada bukan jam kerja.
2. Rata-rata trafik TCP pada jam kerja lebih besar 74,85 kb/s atau 12,1 %.
3. Rata-rata trafik UDP pada jam kerja lebih besar 50,6 kb/s atau 54,1 %.
4. Rata-rata trafik ICMP pada jam kerja lebih besar 19,1 b/s atau 7,6 %.
5. Melalui skenario serangan Ping *flooding* ICMP ke server OSSIM menunjukan bahwa OSSIM dapat mendeteksi serangan secara *real-time*, yaitu melalui pengamatan trafik jaringan dan laporan SIEM *event.*

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

DAFTAR REFERENSI

[1] Anwar, M.M., Zafar, M.F., & Ahmed, Z. A Proposed Preventive Information Security System. Journal IEEE.

[2] Carl Endorf,Eugene Schultz,Jim Mellander. Intrusion Detection & Prevention. Osborne.2004

[3] Clemm, A . (2007). *Network Management Fundamentals*. Cisco Press. Indiana Polish : USA.

[4] ISO 17799: Standar Sistem Manajemen Keamanan Informasi Penulis: Melwin Syafrizal, S.Kom

[5] Krishnamoorthy, V. Cisco AutoQOS: A New Paradigm for Automating the Delivery of Network Quality of Service. 2002

[6] Lavender, B.E. Open Source Security Information Management. Final Project 2008. CSC 250.

[7] Milne, Kelvin. 2 September 2004. Open Source Security Information Manager. User manual.

[8] Team AlientVault.OSSIM General description.

[9] Tipton, H.F., & Krause, M. (2007). *Information Security Management Hand Book.* (6th ed.). New York: Auerbach Publications Taylor & Francis Group.

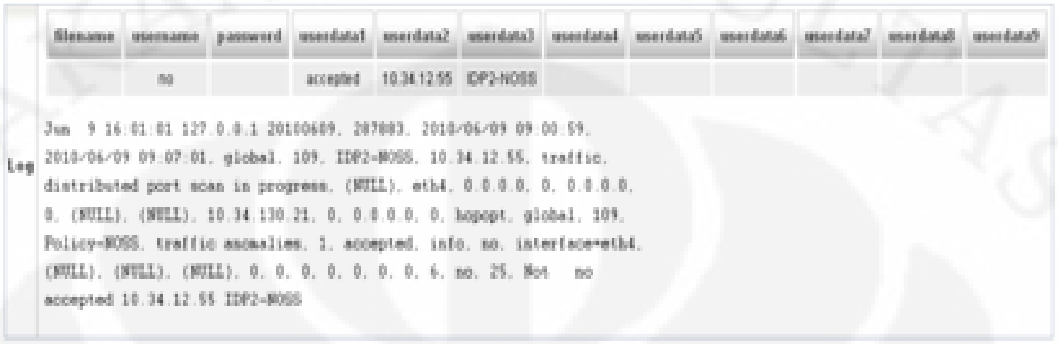
[10] "http://www.alienvault.com/community.php?section=Home".[Diakses tanggal 24 Maret 2010]

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

LAMPIRAN 1

Log yang dihasilkan dari Perangkat yang dibaca OSSIM

1. Log IDP



filename	username	password	userdata1	userdata2	userdata3	userdata4	userdata5	userdata6	userdata7	userdata8	userdata9
	no		accepted	10.34.12.55	IDP2-NOSS						

Log

```
Jun  9 16:01:01 127.0.0.1 20100609, 207003, 2010/06/09 09:00:59,
2010/06/09 09:07:01, global, 109, IDP2-NOSS, 10.34.12.55, traffic,
distributed port scan in progress, (NULL), eth4, 0.0.0.0, 0, 0.0.0.0,
0, (NULL), (NULL), 10.34.130.21, 0, 0.0.0.0, 0, logopt, global, 109,
Policy-NOSS, traffic anomalies, 1, accepted, info, no, interface=eth4,
(NULL), (NULL), (NULL), 0, 0, 0, 0, 0, 0, 0, 6, no, 25, Not   no
accepted 10.34.12.55 IDP2-NOSS
```

2. Log Firewall

filename	username	password	userdata1	userdata2	userdata3	userdata4	userdata5	userdata6	userdata7	userdata8	userdata9

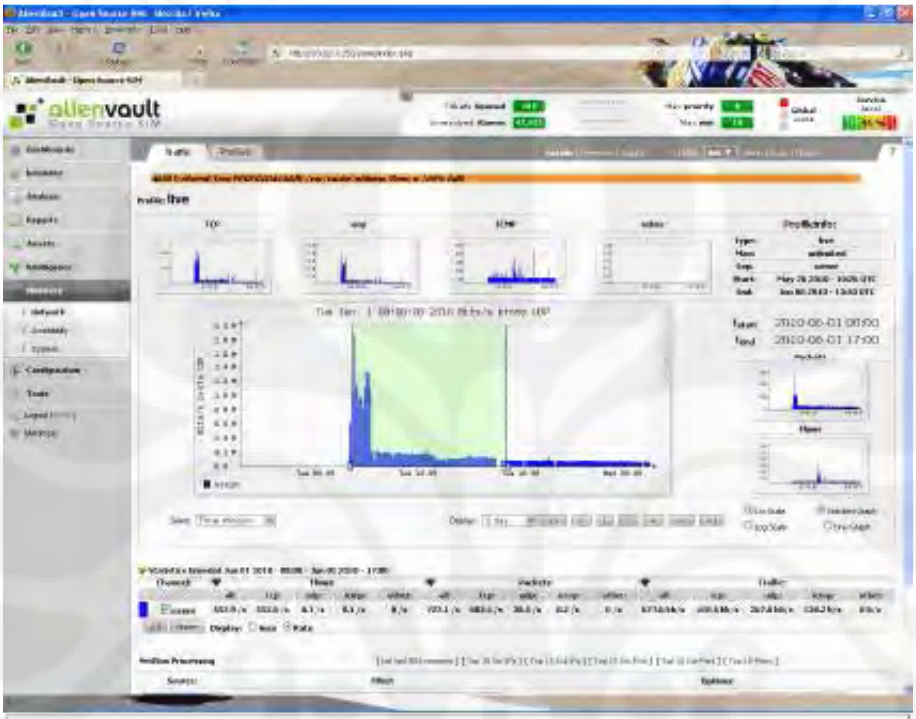
Log

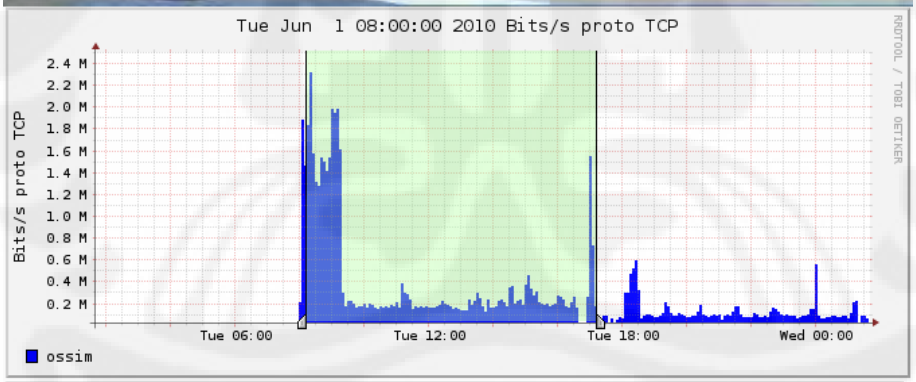
```
Jun 10 16:55:19 10.1.14.35 FW-SYNERGI-TELKOM-GROUP  NetScreen
device_id=FW-SYNERGI-TELKOM-GROUP
[Root]system-notification-00257(traffic): start_time="2010-06-10
17:23:06" duration=0 policy_id=320001 service=http proto=6 src
zone=Null dst zone=null action=Deny sent=0 rcvd=40 src=10.32.1.251
dst=10.1.14.35 src_port=61402 dst_port=80 session_id=0
```

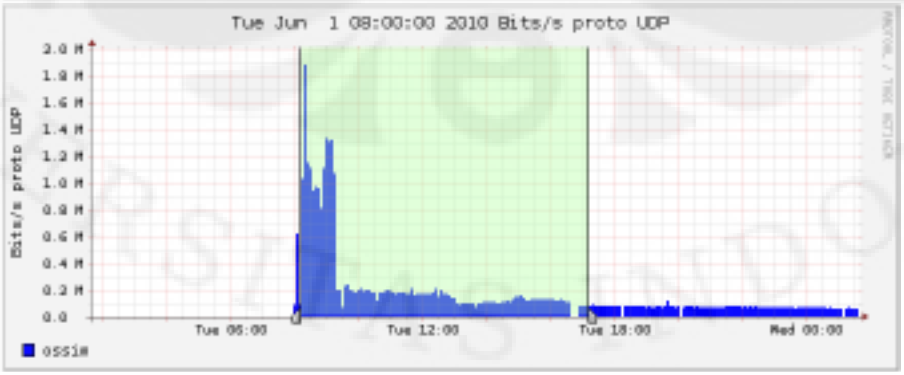

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

LAMPIRAN 2

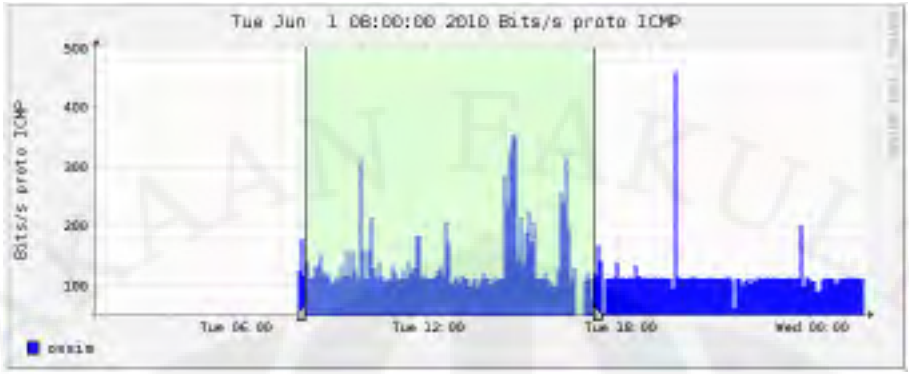
Pengamatan Grafik Trafik TCP,UDP dan ICMP selama Seminggu 1 Juni 2010 (Jam Kerja 08.00-17.00)



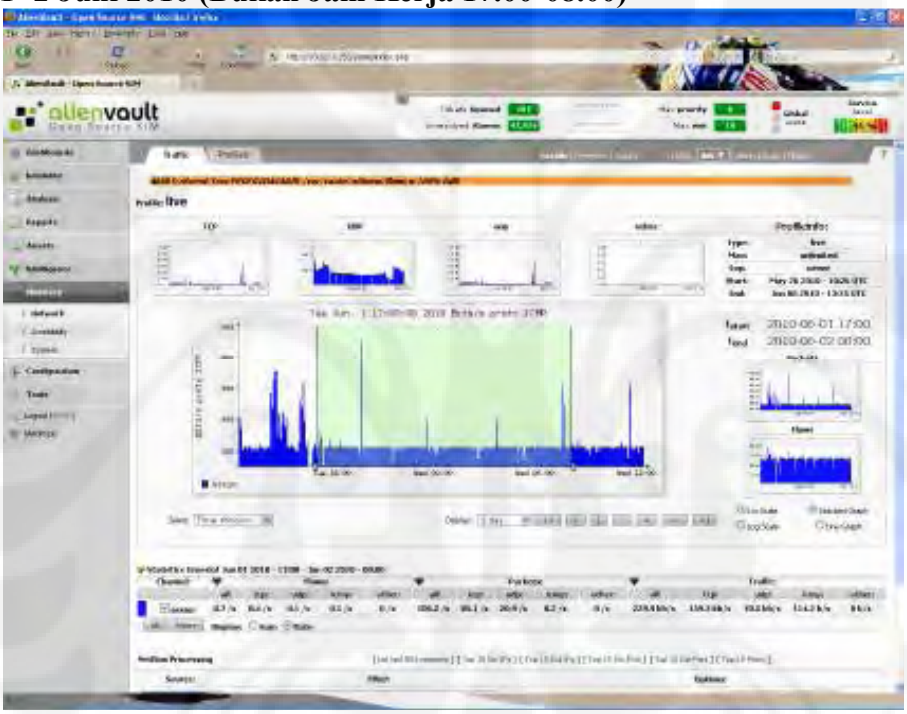




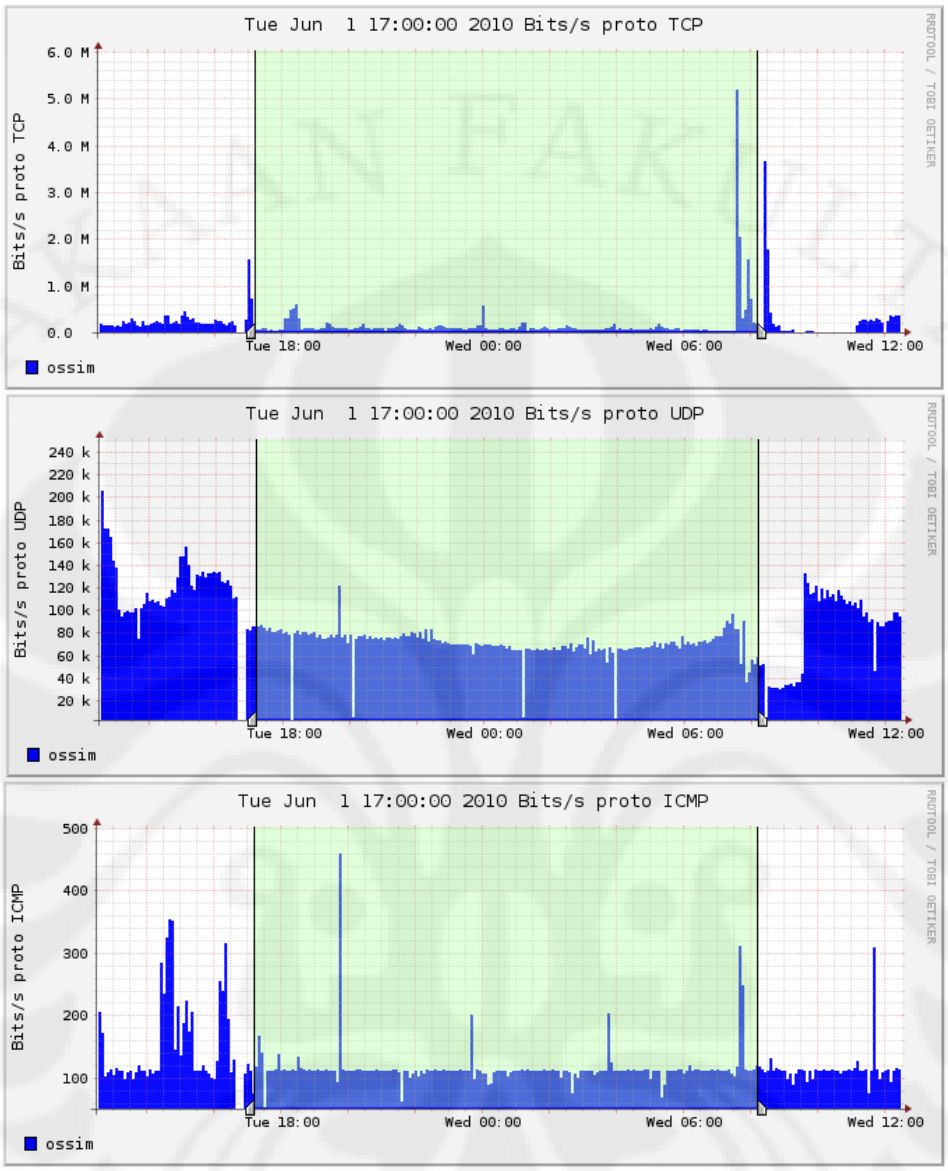
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



1 -2 Juni 2010 (Bukan Jam Kerja 17.00-08.00)

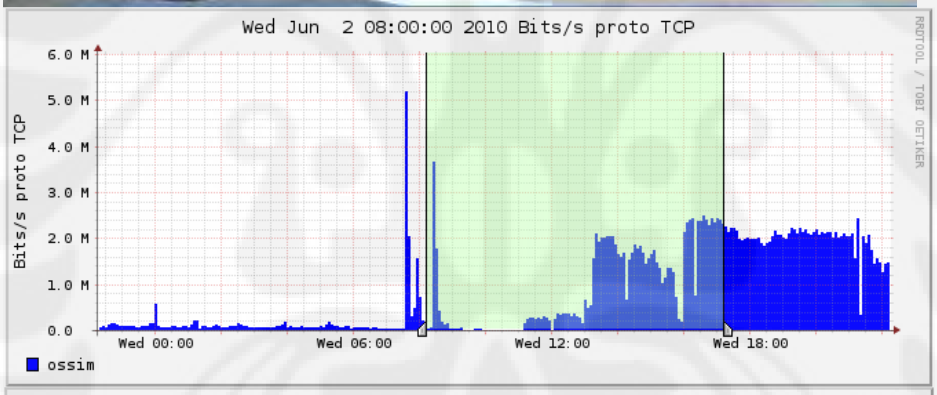


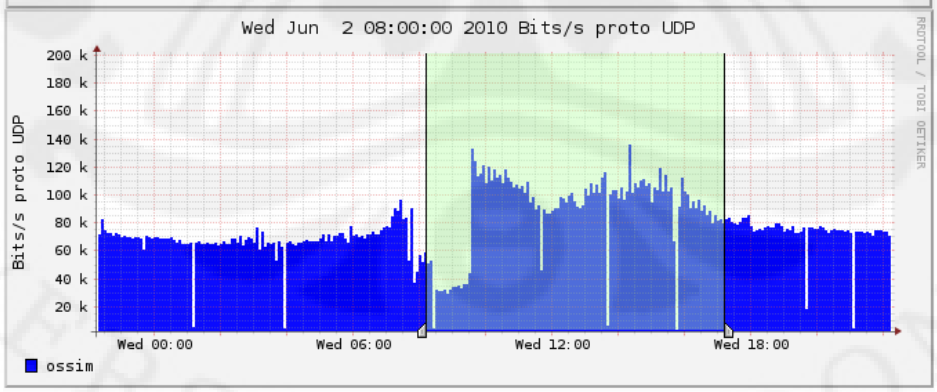
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



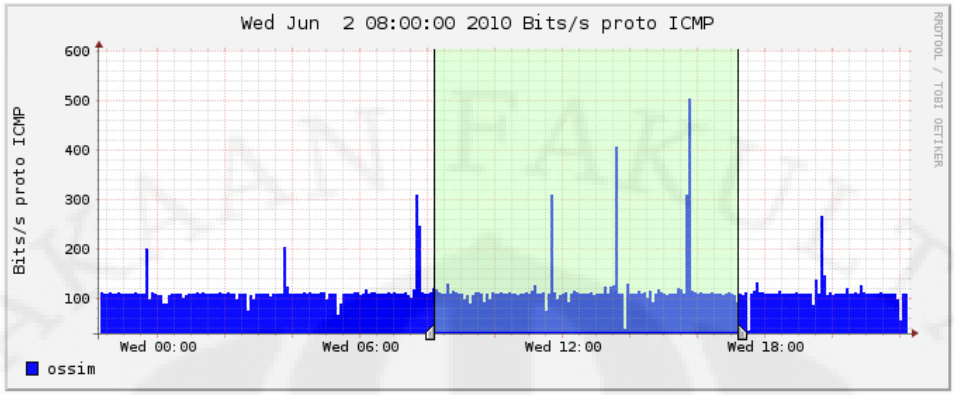
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

2 Juni 2010 (Jam Kerja 08.00-17.00)

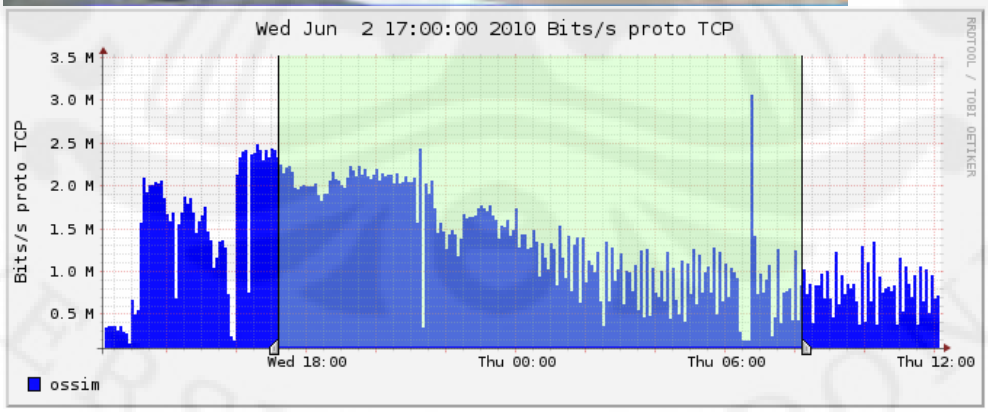




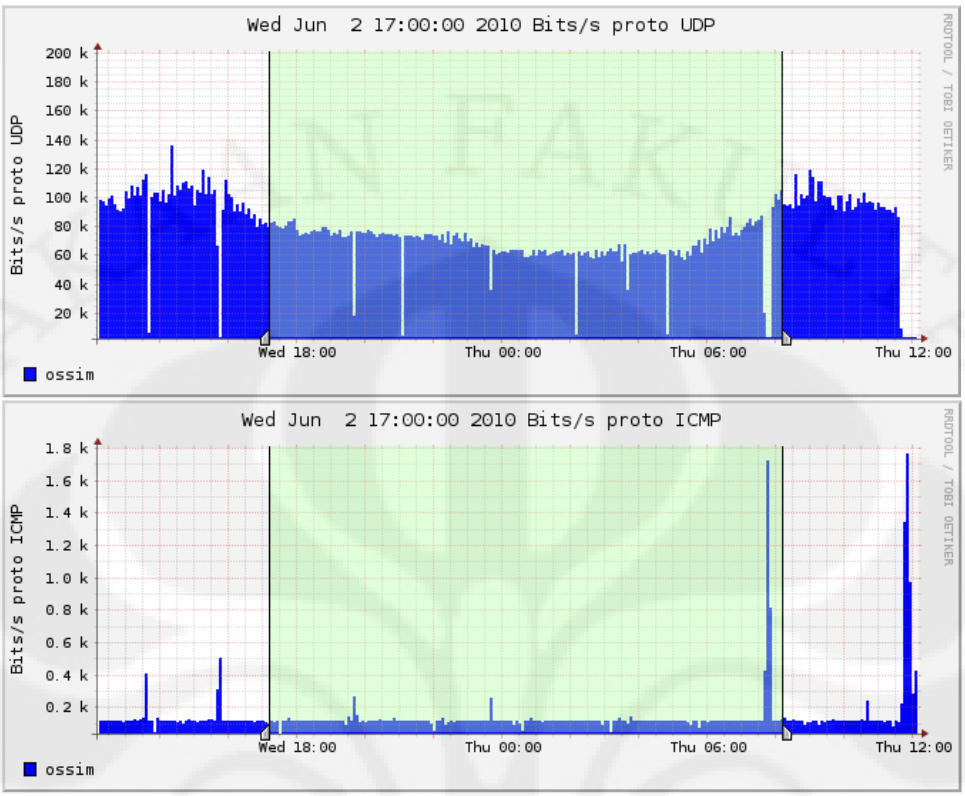
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



2 -3 Juni 2010 (Bukan Jam Kerja 17.00-08.00)

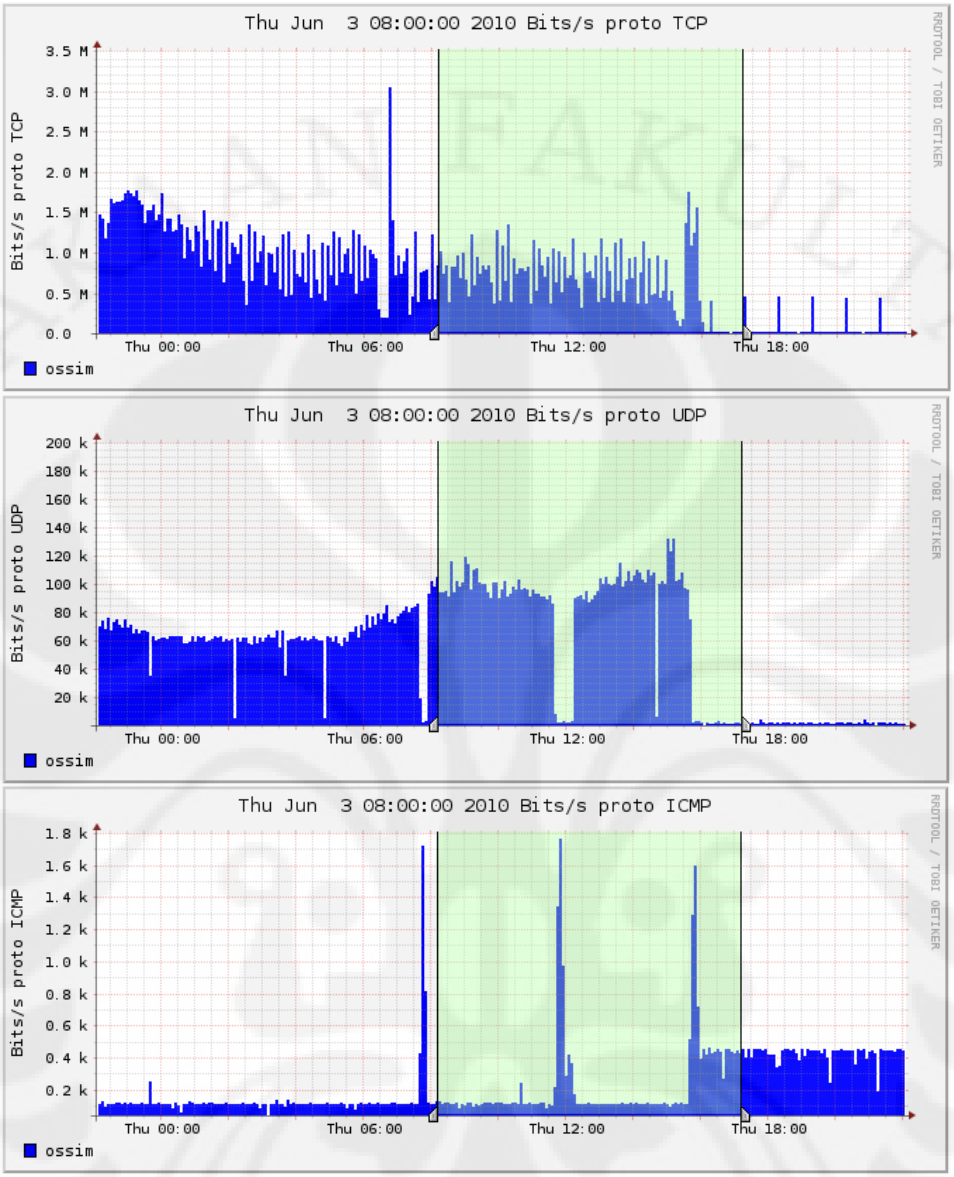


Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



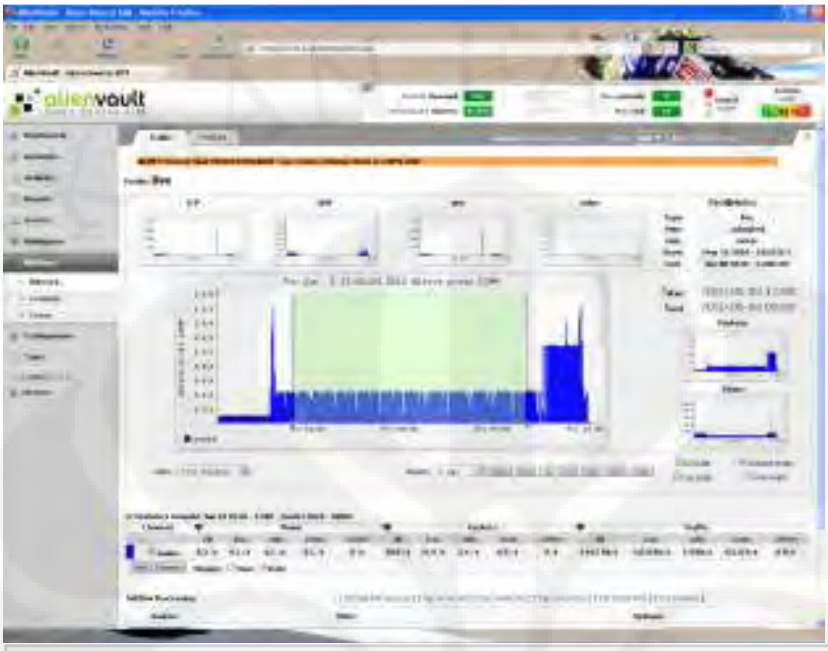
3 Juni 2010 (Jam Kerja 08.00-17.00)

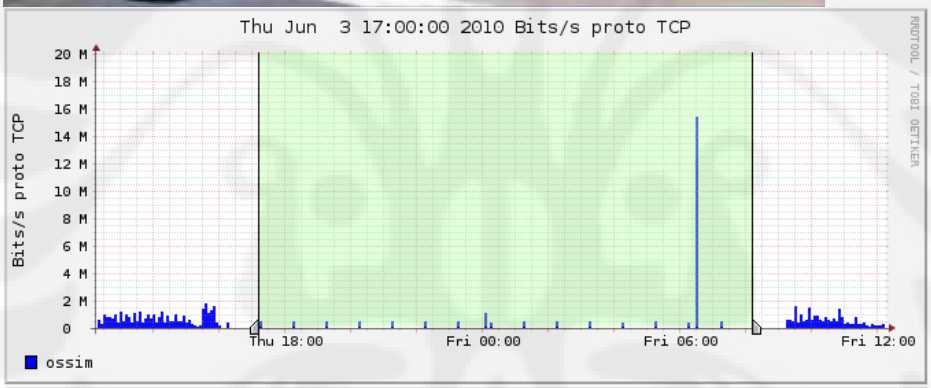
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

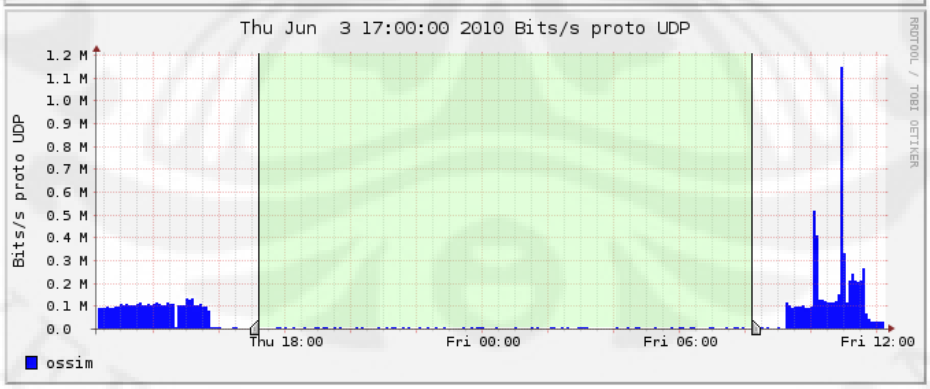


Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

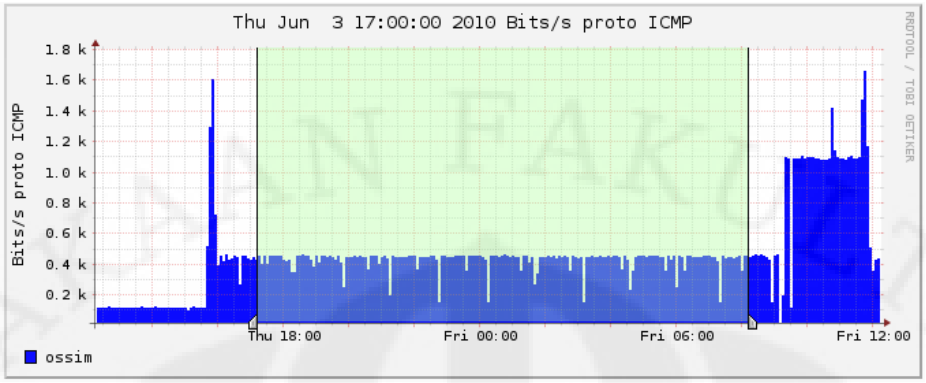
3-4 Juni 2010 (Bukan Jam Kerja 17.00-08.00)



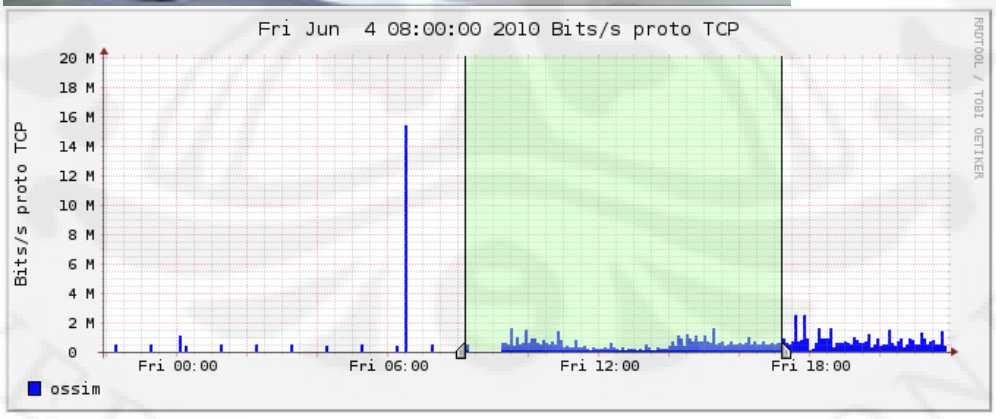




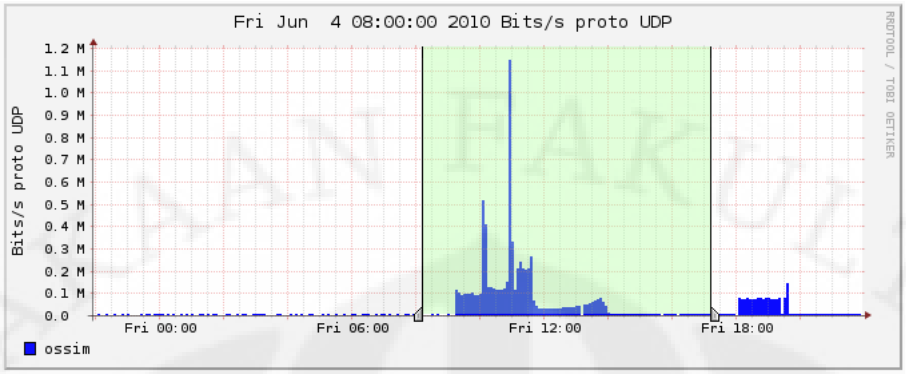
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

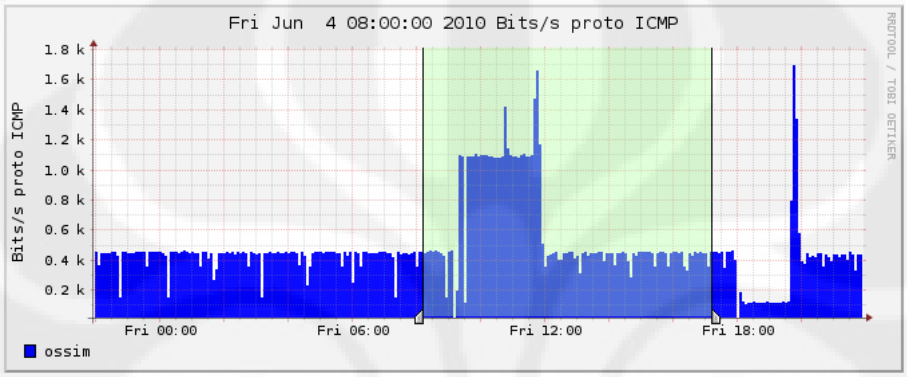


4 Juni 2010 (Jam Kerja 08.00-17.00)



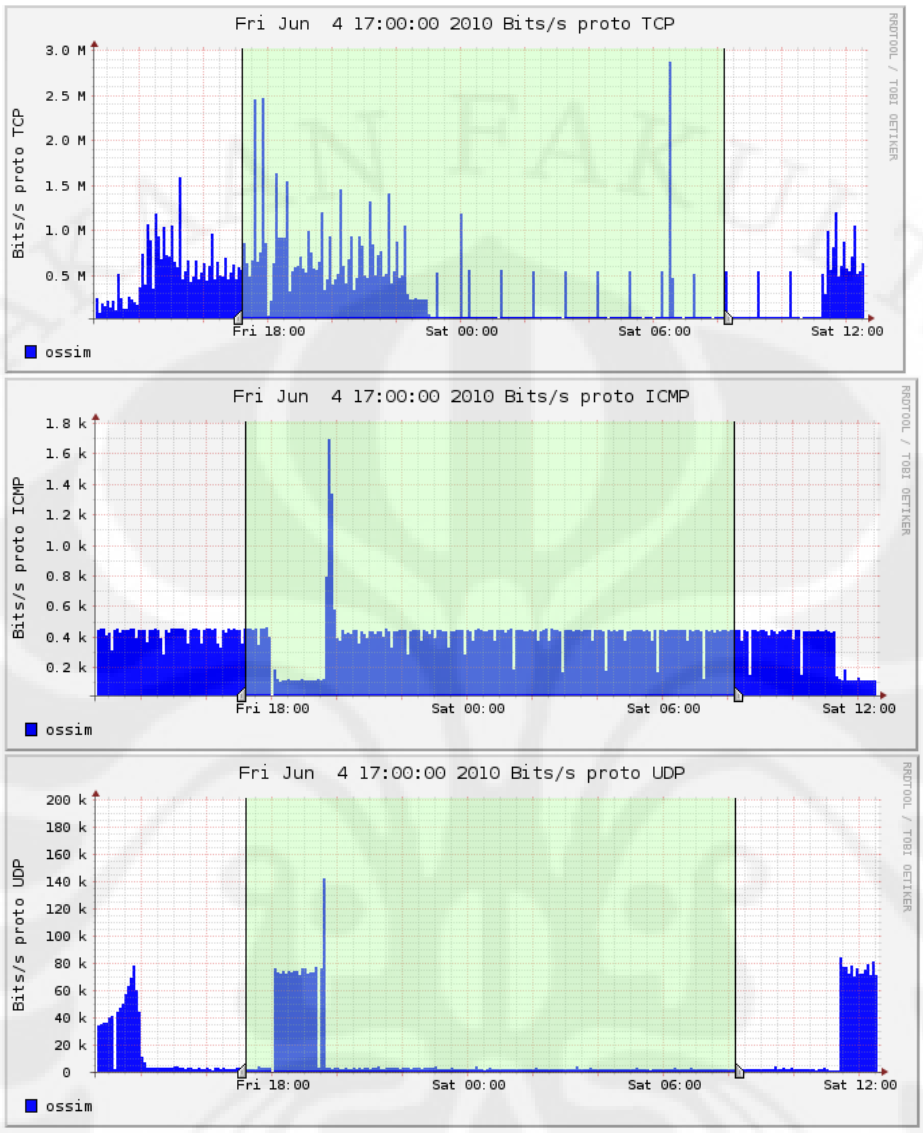
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010





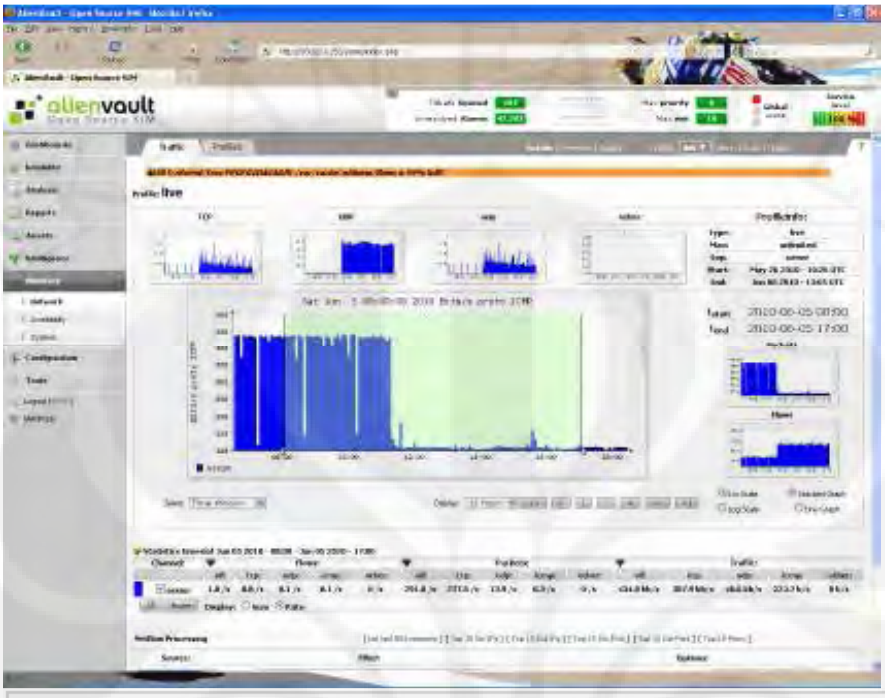
4-5 Juni 2010 (Bukan Jam Kerja 17.00-08.00)

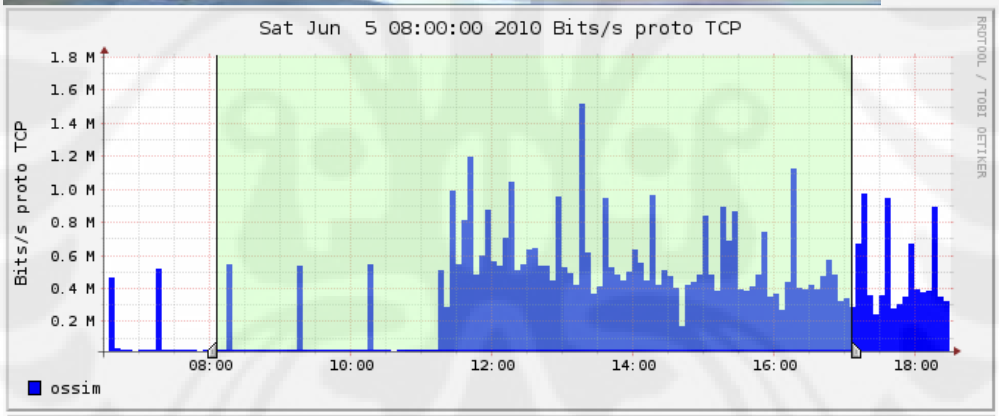
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

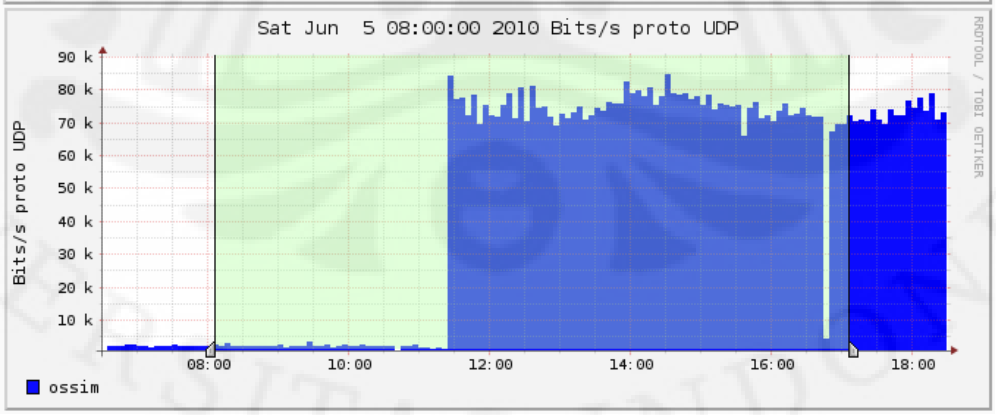


Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

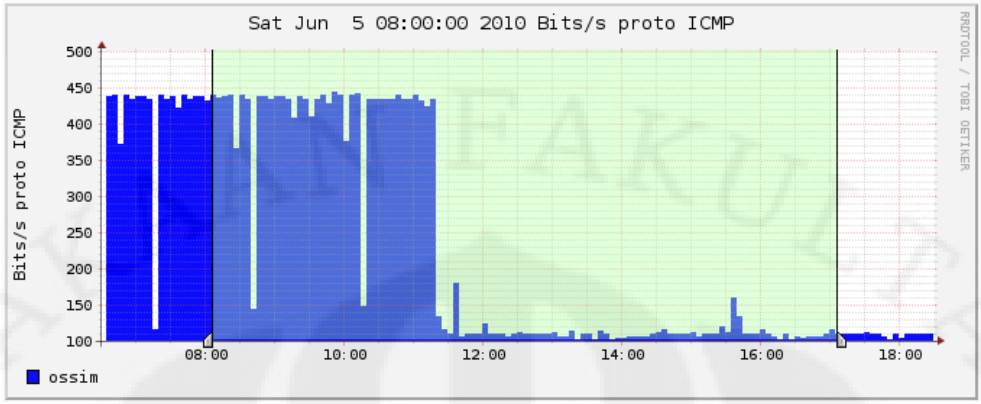
5 Juni 2010 (Jam Kerja 08.00-17.00)



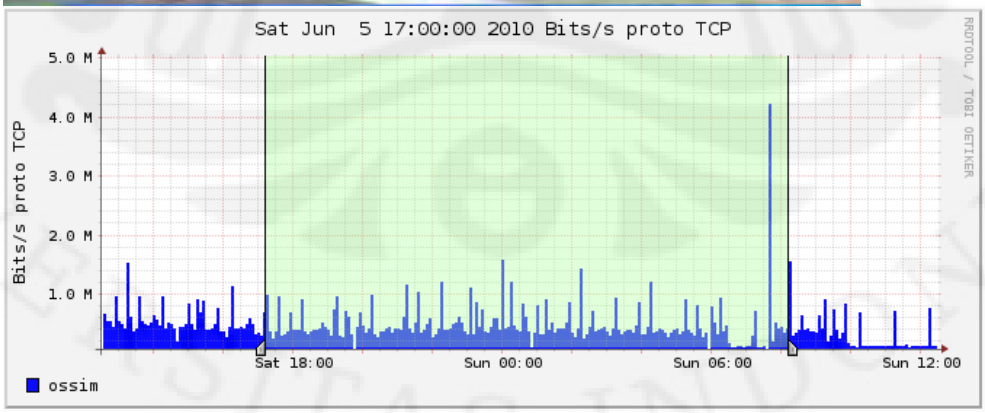




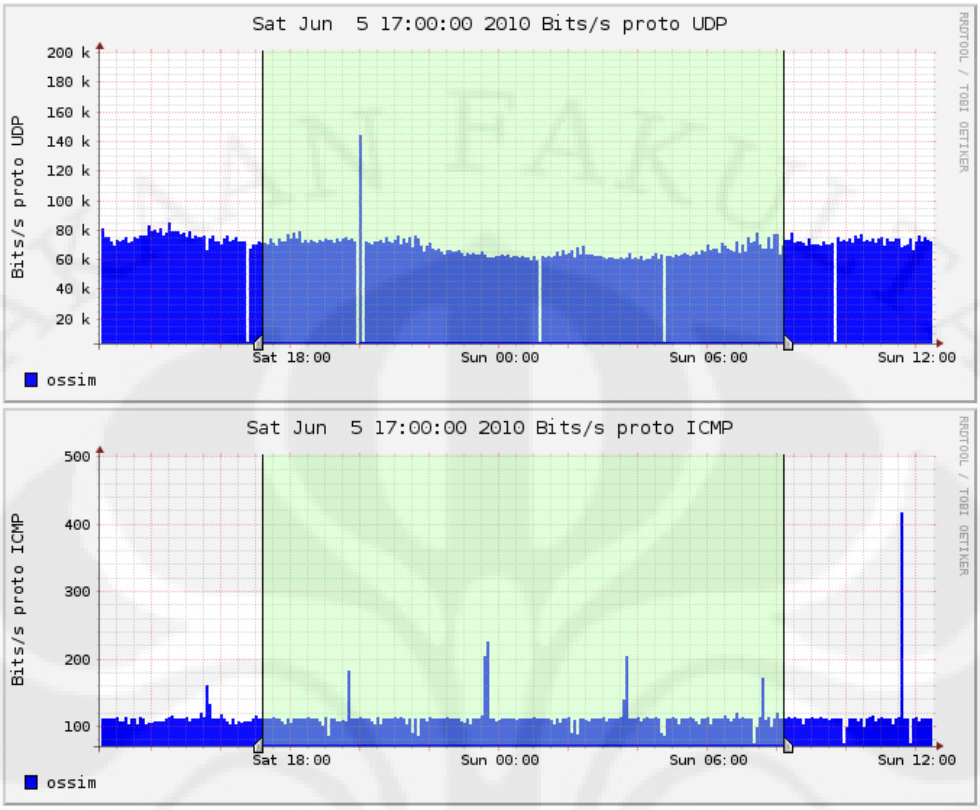
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



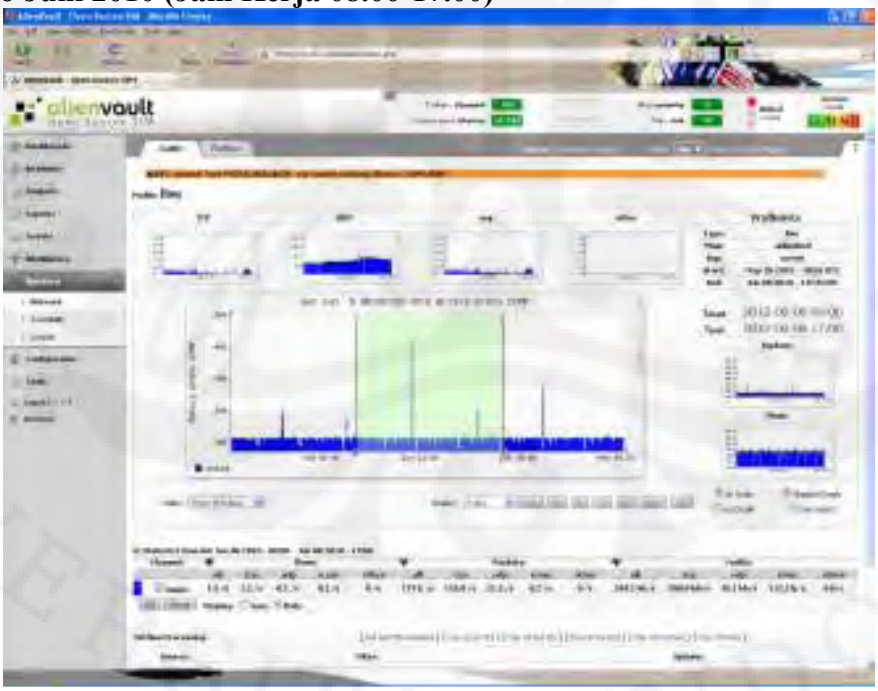
5-6 Juni 2010 (Bukan Jam Kerja 17.00-08.00)



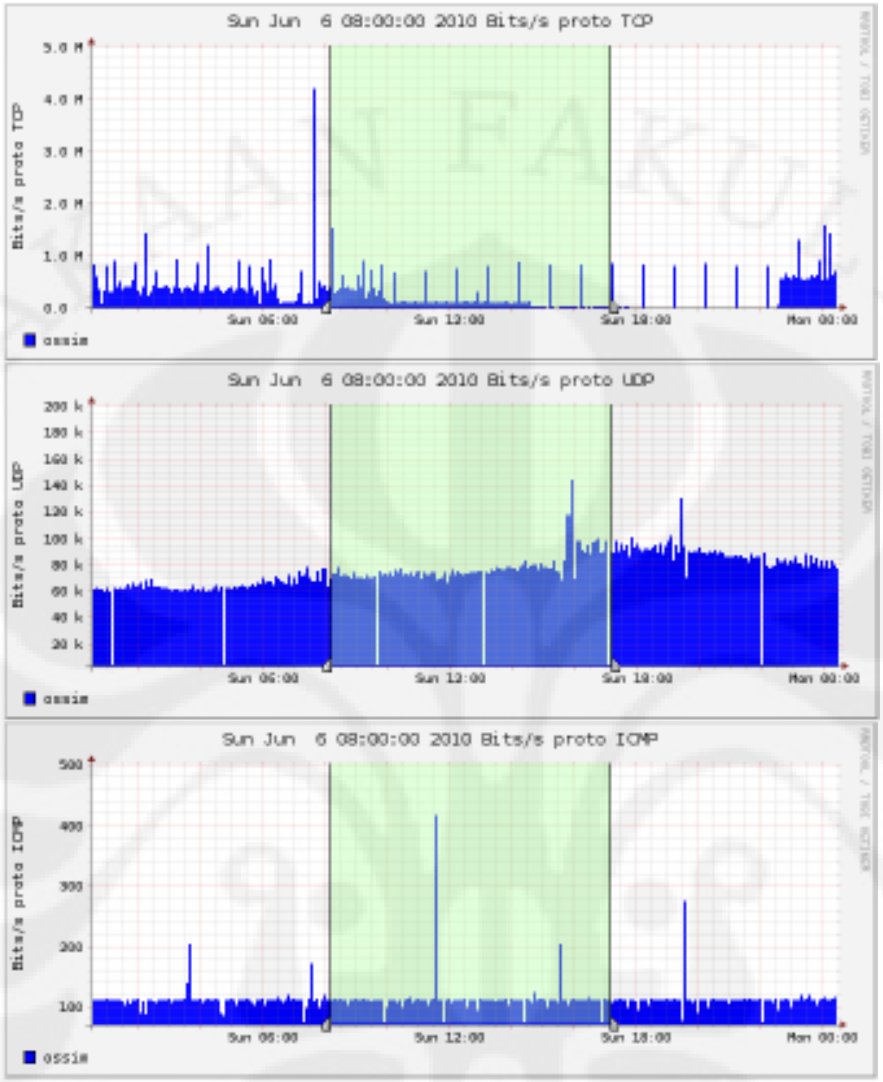
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



6 Juni 2010 (Jam Kerja 08.00-17.00)

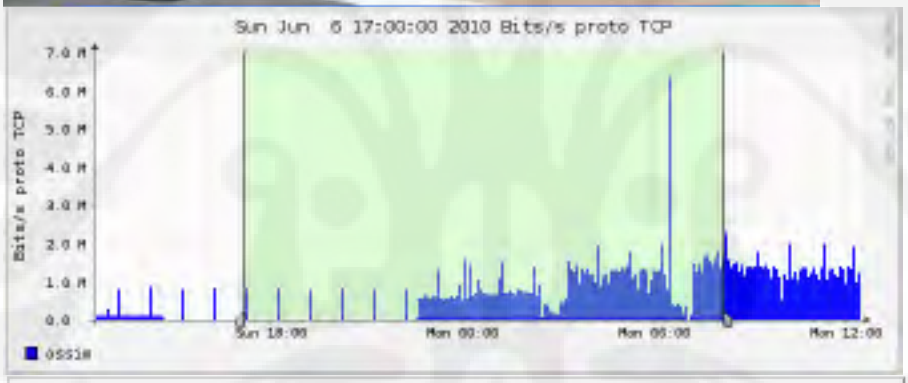


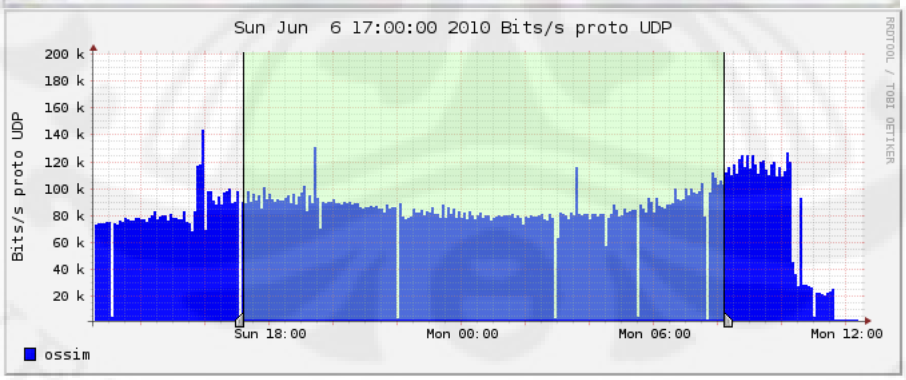
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



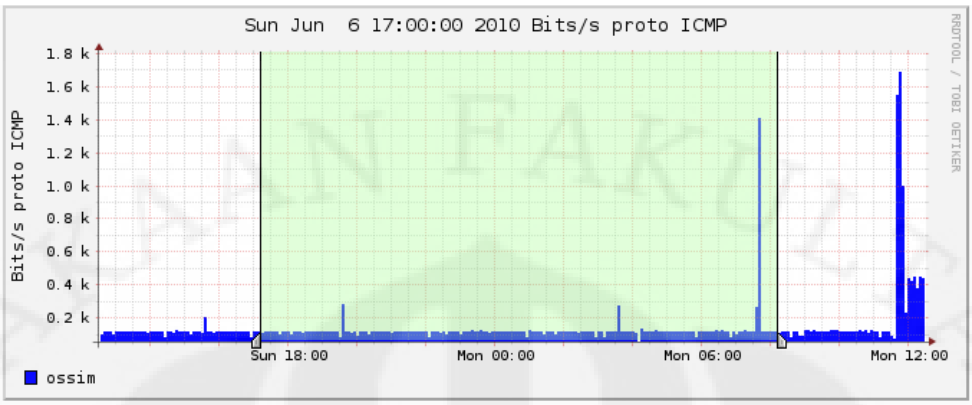
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010

6-7 Juni 2010 (Bukan Jam Kerja 17.00-08.00)

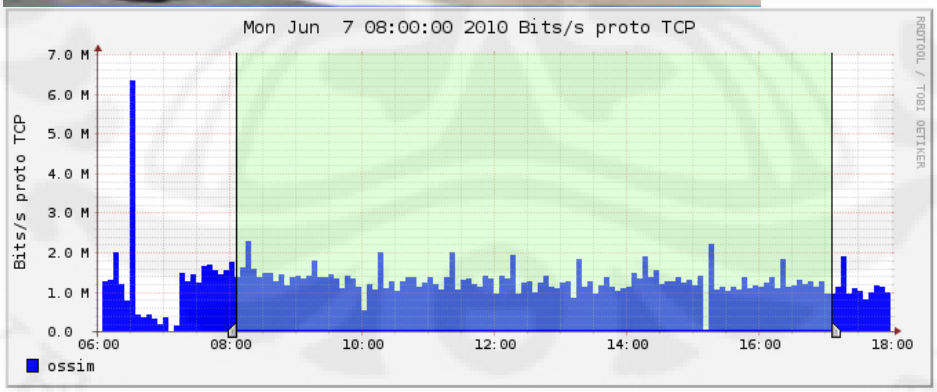




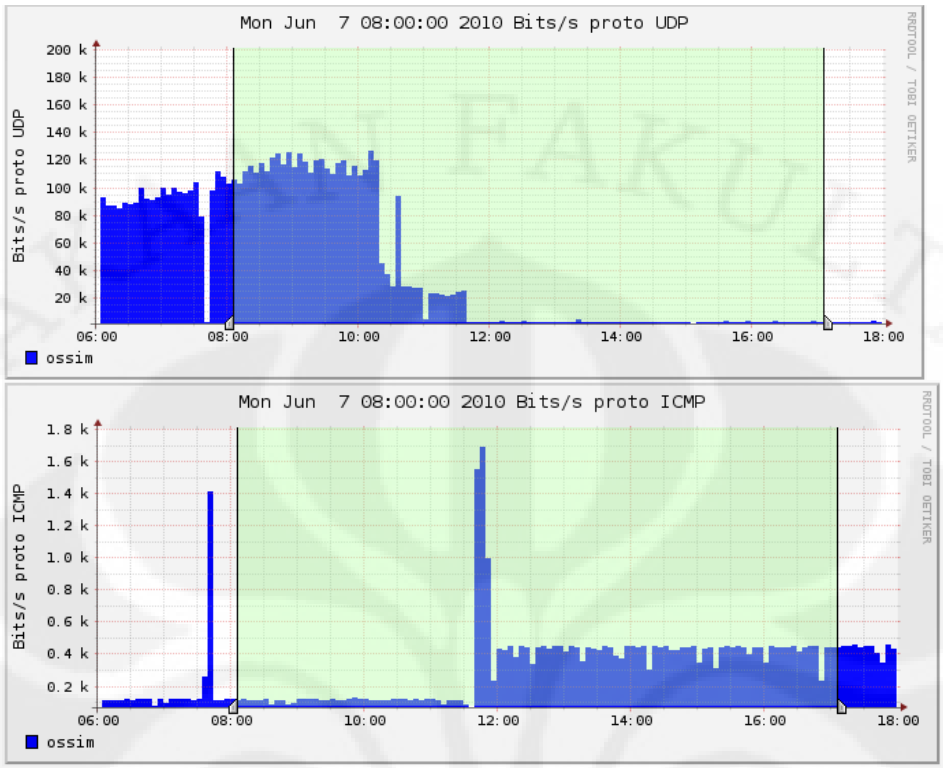
Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



7Juni 2010 (Jam Kerja 08.00-17.00)

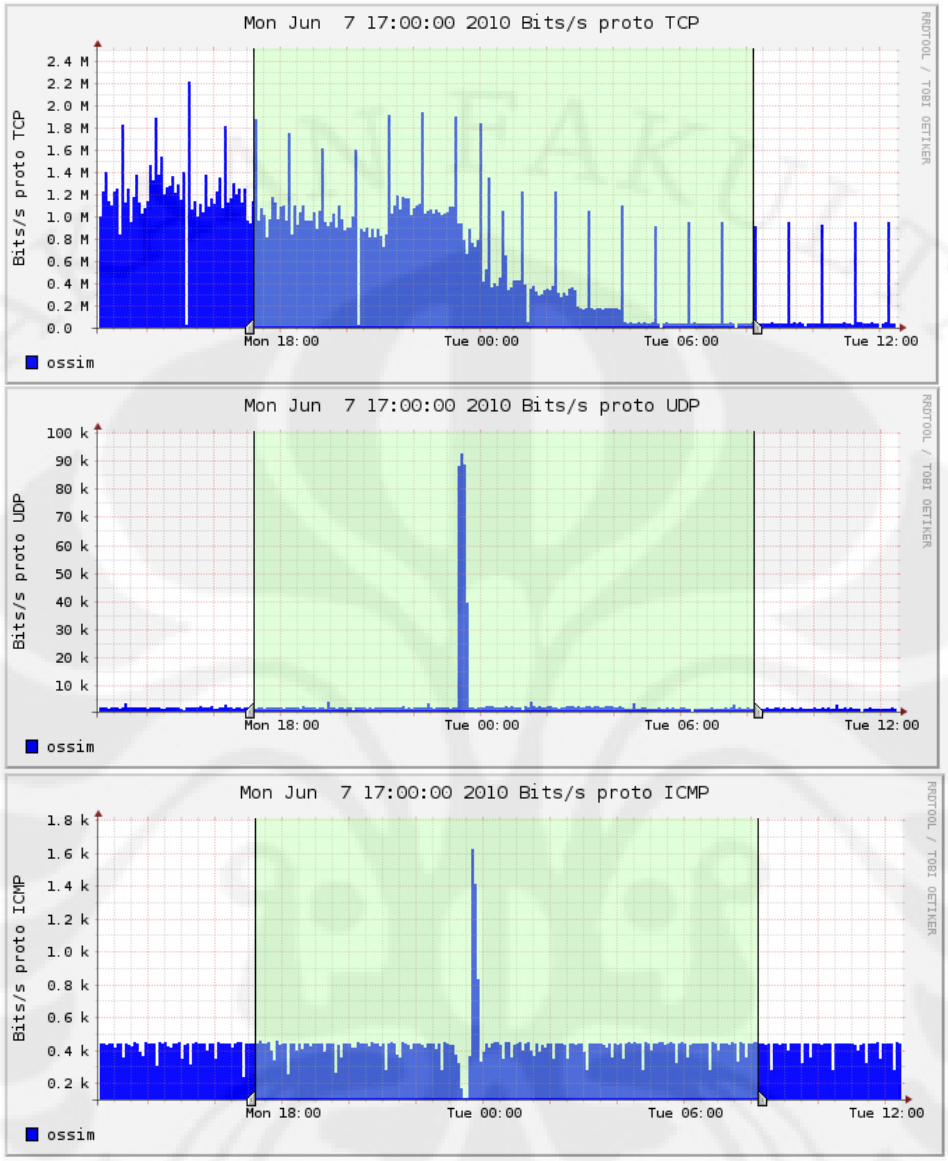


Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



6-7 Juni 2010 (Bukan Jam Kerja 17.00-08.00)

Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010



Implementasi dan analisa..., Moehamad Rihal, FT UI, 2010