RANCANG BANGUN SENSOR MONITORING PADA JARINGAN WI-FI (HOTSPOT) DI W-P CAFE SUMBERSARI MALANG BERBASIS SNORT

SKRIPSI

Disusun oleh:

IMAM IZZAT MUTTAQIN
NIM. 04.12.617

JURUSAN TEKNIK ELEKTRO S-1
KONSENTRASI TEKNIK KOMPUTER & INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

2011

LEMBAR PERSETUJUAN

RANCANG BANGUN SENSOR MONITORING PADA JARINGAN WI–FI (HOTSPOT) DI W–P CAFE SUMBERSARI MALANG BERBASIS SNORT

SKRIPSI

Disusun dan diajukan untuk melengkapi dan memenuhi persyaratan
guna mencapai gelar Sarjana Teknik

Disusun Oleh :
Imam Izzat Muttaqin
NIM : 04.12.617

Mengetahui,
Ketua Program Studi Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y. 1018800189

Diperiksa dan Disetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Joseph Dedy Irawan, ST, MT	**Irmalia Suryani Faradisa, ST, MT**
NIP. 1974041620011002	**NIP.P. 1030100365**

JURUSAN TEKNIK ELEKTRO S-1
KONSENTRASI TEKNIK KOMPUTER DAN INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2011

ABSTRAK

RANCANG BANGUN SENSOR MONITORING PADA JARINGAN WI-FI (HOTSPOT) DI W-P CAFE SUMBERSARI MALANG BERBASIS SNORT

Imam Izzat Muttaqin, NIM 04.12.617
Dosen Pembimbing I : Joseph Dedy Irawan, ST, MT
Dosen Pembimbing II : Irmalia Suryani Faradisa, ST, MT

Penerapan Jaringan nirkabel selain memberikan kemudahan dalam berkomunikasi atau tranksaksi data, ternyata terdapat pula beberapa kelemahan pada segi keamanannya. Jaringan nirkabel tidak memiliki jalur pertahanan yang jelas sehingga setiap komputer pengguna harus siap terhadap gangguan ataupun serangan yang mungkin terjadi.

Penerapan sensor monitoring diusulkan salah satu solusi yang dapat digunakan untuk membantu pengaturan jaringan dalam memantau kondisi jaringan dan menganalisa paket – paket berbahaya yang terdapat dalam jaringan tersebut.

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan.

Sensor monitoring ini menggunakan sistem *rule base*. Dimana sensor ini mendeteksi suatu paket-paket berdasarkan aturan-aturan yang sudah didefinisikan pada kumpulan data aturan.

Kata Kunci : Paket data, Sensor Monitoring, Snort.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Dengan mengucap syukur kehadirat Allah SWT yang maha pengasih dan maha penyayang yang dengan segala Kasih dan Anugerah – Nya, telah memberikan kekuatan, kesabaran, bimbingan dan perlindungan sehingga penulis dapat menyelesaikan laporan skripsi dengan judul :

" RANCANG BANGUN SENSOR MONITORING PADA JARINGAN WI-FI (HOTSPOT) DI W-P CAFE SUMBERSARI MALANG BERBASIS SNORT "

Pembuatan skripsi ini disusun guna memenuhi syarat akhir kelulusan pendidikan jenjang Strata I di Institut Teknologi Nasional Malang. Dalam penyusunan skripsi ini penulis banyak mendapat bantuan baik moril maupun materiil, saran dan dorongan semangat dari berbagai pihak, untuk itu penulis mengucapkan terima kasih kepada :

1. Bapak Ir. Soeparno Djiwo, MT selaku rektor ITN Malang.
2. Bapak Ir. H. Sidik Noertjahjono, MT selaku Dekan Fakultas Teknologi Industri.
3. Bapak Ir. Yusuf Ismail Nakhoda, MT selaku Ketua Jurusan Teknik Elektro S-1 ITN Malang.
4. Bapak Joseph Dedy Irawan, ST, MT. selaku Dosen Pembimbing I.
5. Ibu Irmalia Suryani Faradisa, ST, MT. selaku Dosen Pembimbing II.
6. Ayah dan Ibuku yang selalu memberikan semangat, dorongan dan do'a serta seluruh keluarga yang telah banyak memberikan bantuan baik moril maupun materi.
7. Rekan - rekan dan semua pihak yang tidak dapat penulis sebutkan satu per satu, yang telah membantu dalam penyelesaian skripsi ini.

Penulis menyadari bahwa laporan ini masih banyak yang perlu disempurnakan. Oleh sebab itu kritik dan saran yang membangun sangat diharapkan.

Akhir kata, penulis mohon maaf kepada semua pihak bilamana selama penyusunan skripsi ini penyusun membuat kesalahan secara tidak sengaja dan semoga skripsi ini dapat bermanfaat bagi kita semua.

Malang, 2011

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Penerapan Jaringan nirkabel selain memberikan kemudahan dalam berkomunikasi atau tranksaksi data, ternyata terdapat pula beberapa kelemahan pada segi keamanannya. Jaringan nirkabel tidak memiliki jalur pertahanan yang jelas sehingga setiap komputer pengguna harus siap terhadap gangguan ataupun serangan yang mungkin terjadi.

Keamanan jaringan bergantung pada kecepatan pengatur jaringan dalam menindak lanjuti sistem saat terjadi gangguan. Penerapan sensor monitoring diusulkan salah satu solusi yang dapat digunakan untuk membantu pengaturan jaringan dalam memantau kondisi jaringan dan menganalisa paket - paket berbahaya yang terdapat dalam jaringan tersebut.

Sensor monitoring ini menggunakan sistem rule base. Dimana sensor ini mendeteksi suatu paket - paket berdasarkan aturan-aturan yang sudah didefinisikan pada kumpulan data aturan.

Oleh karena itu sensor monitoring diterapkan karena sistem ini mampu mendeteksi paket - paket berbahaya pada jaringan dan langsung memberikan peringatan kepada pengatur jaringan tentang kondisi jaringan saat itu.

1.2 Rumusan Masalah

Berdasarkan hal diatas maka timbul permasalahan yaitu bagaimana merancang sistem sensor monitoring dengan menggunakan tampilan *web base*.

1.3 Tujuan

Adapun tujuan dari penulisan skripsi ini yaitu untuk menghasilkan sensor monitoring pada jaringan *wifi* dengan tampilan yang mudah dikendalikan atau dioperasikan tanpa mengurangi kinerja dari jaringan yang akan di monitoring.

1.4 Batasan Masalah

Agar permasalahan mengarah sesuai dengan tujuan yang diharapkan, maka pembahasan dibatasi oleh hal - hal sebagai berikut :

1. Sensor monitoring ini hanya diimplementasikan pada *operating system Ubuntu Server* 10.04 LTS.
2. *Web server* yang digunakan adalah *Apache*.
3. *Database* yang digunakan *Mysql*.
4. Sensor menggunakan *snort rule base*.
5. Hanya diimplementasikan pada jaringan *wifi / hotspot*.

1.5 Metode Penelitian

Adapun metode penelitian yang digunakan adalah sebagai berikut:

1. Studi literature

   Pengumpulan data yang dilakukan dengan mencari bahan-bahan kepustakaan dan referensi dari berbagai sumber sebagai landasan teori yang ada hubunganya dengan permasalahan yang dijadikan objek penelitian.

2. Analisa Kebutuhan Sistem

   Data dan informasi yang telah diperoleh akan dianalisa agar didapatkan kerangka global yang bertujuan untuk mendefinisikan kebutuhan sistem di mana nantinya akan digunakan sebagai acuan perancangan sistem.

3. Perancangan dan Implementasi

   Berdasarkan data dan informasi yang telah diperoleh serta analisa kebutuhan untuk membangun sistem ini, akan dibuat rancangan kerangka global yang menggambarkan mekanisme dari sistem yang akan dibuat dan diimplementasikan kedalam system.

4. Eksperimen dan Evaluasi

   Pada tahap ini, sistem yang telah selesai dibuat akan diuji coba, yaitu pengujian berdasarkan fungsionalitas program, dan akan dilakukan koreksi dan penyempurnaan program jika diperlukan.

1.6 Sistematika Penulisan

Untuk mempermudah dan memahami pembahasan penulisan skripsi ini, maka sistematika penulisan disusun sebagai berikut :

Bab I : Pendahuluan

Berisi Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Pembatasan Permasalahan, Metode Penelitian dan Sistematika Penulisan.

Bab II : Tinjauan Pustaka

Berisi tentang landasan teori mengenai permasalahan yang berhubungan dengan penelitian yang dilakukan.

Bab III : Perancangan dan Analisa Sistem

Dalam bab ini berisi mengenai analisa kebutuhan sistem baik *software* maupun *hardware* yang diperlukan untuk membuat kerangka global yang menggambarkan mekanisme dari sistem yang akan dibuat.

Bab IV : Pembuatan dan Pengujian Sistem

Berisi tentang implementasi dari perancangan sistem yang telah dibuat serta pengujian terhadap sistem tersebut.

Bab V : Penutup

Merupakan bab terakhir yang memuat intisari dari hasil pembahasan yang berisikan kesimpulan dan saran yang dapat digunakan sebagai pertimbangan untuk pengembangan penulisan selanjutnya.

BAB II

DASAR TEORI

2.1 Jaringan Komputer

Jaringan komputer adalah dua atau lebih komputer yang saling terhubung melalui kabel atau dengan koneksi nirkabel sehingga mereka dapat saling bertukar informasi.

Komputer – komputer tersebut saling terhubung dengan *Network Interface Card* (NIC) di tiap komputer dengan menggunakan media kabel ataupun nirkabel tergantung dari jenis NIC yang digunakan.

Menurut jangkauannya, jaringan komputer dibagi menjadi 3 yaitu :

1. *Local Area Network* (LAN)
   LAN merupakan jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 Km.

2. *Metropolitan Area Network* (MAN)
   MAN merupakan jaringan komputer yang saling terkoneksi dalam satu kawasan kota yang jaraknya bisa lebih dari 1 Km.

3. *Wide Area Network* (WAN)
   WAN merupakan jaringan komputer yang menghubungkan banyak LAN ke dalam suatu jaringan terpadu. Antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan oleh letak geografi dengan menggunakan metode komunikasi tertentu.

2.1.1 Arsitektur Jaringan

Standar yang paling populer untuk menggambarkan arsitektur jaringan adalah model referensi *Open System Interconnect* (OSI) yang dikembangkan oleh *International Organization for Standarization* (ISO) pada tahun 1977 dan diperkenalkan pada tahun 1984. Pada model referensi OSI terdapat 7 buah lapisan yang setiap lapisnya mengilustrasikan fungsi – fungsi jaringan ini antara lain :

a. *Lapisan ke - 7 - Application*

   Lapisan yang paling dekat dengan pengguna dan memiliki fungsi untuk menyediakan sebuah layanan jaringan kepada pengguna aplikasi, berisi protokol – protokol yang umum digunakan oleh pengguna. Lapisan ini berbeda dengan lapisan lainnya yang dapat menyediakan layanan kepada lapisan lain.

   Contoh : *Simple Mail Transfer Protocol* (SMTP), *Hypertext Transfer Protocol* (HTTP), dan *File Transfer Protocol* (FTP).

b. *Lapisan ke - 6 – Presentations*

   Lapisan ini menentukan format data yang dipindahkan di antara aplikasi dan mengelola informasi yang disediakan oleh lapisan application supaya informasi yang dikirimkan dapat dibaca oleh lapisan Application pada sistem lain. Lapisan ini menyediakan layanan berupa tranformasi format data, enskripsi dan kompresi.

c. *Lapisan ke - 5 – Session*

   Lapisan ini berfungsi untuk menyelenggarakan, mengatur dan memutuskan sesi komunikasi. Lapisan session menyediakan layanan kepada lapisan Presentation dan juga mensinkronisasi dialog di antara dua komputer lapisan Presentation dan mengatur pertukaran data.

d. *Lapisan ke - 4 Transport*

Lapisan ini berfungsi sebagai pemecah informasi menjadi paket – paket data yang akan dikirim dan menyusun kembali paket – paket data menjadi sebuah informasi yang dapat diterima. Dua protokol umum pada lapisan ini adalah *Transfer Control Protocol* (TCP) yang berorientasi koneksi dan *User Datagram Protocol* (UDP) yang tidak berorientasi koneksi.

e. *Lapisan ke - 3 – Network*

Lapisan ini menyediakan transfer informasi di antara ujung sistem melewati beberapa jaringan komunikasi berurutan. Lapisan ini melakukan pemilihan jalur terbaik dalam komunikasi jaringan yang terpisah secara geografis.

f. *Lapisan ke - 2 - Data Link*

Lapisan ini berfungsi mengubah paket – paket data menjadi frame, menghasilkan alamat fisik, pesan – pesan kesalahan, pemesanan pengiriman data. Lapisan Data Link mengupayakan agar lapisan Physical dapat bekerja dengan baik dengan menyediakan layanan untuk mengaktifkan, mempertahankan dan menonaktifkan hubungan.

g. *Lapisan ke - 1 – Physical*

Lapisan ini bertugas menangani transmisi data dalam bentuk bit melalui jalur komunikasi. Lapisan ini menjamin transmisi data berjalan dengan baik dengan cara mengatur karakteristik tinggi tegangan, periode perubahan tegangan, lebar jalur komunikasi, jarak maksimum komunikasi dan koneksi.

2.1.2 Jaringan LAN Nirkabel (WLAN)

WLAN menggunakan dua macam teknik modulasi, yaitu *Orthogonal Frequency Division Multiplexing* (OFDM) dan *Direct Sequence Spread Spectrum* (DSSS). OFDM akan menyebabkan kecepatan pengiriman data lebih tinggi dibandingkan dengan DSSS, tetapi DSSS lebih sederhana daripada OFDM sehingga akan lebih murah dalam implementasinya. Standar yang lazim digunakan untuk WLAN adalah 802.11 yang ditetapkan oleh IEEE pada akhir tahun 1990. Standar 802.11 kemudian terbagi lagi menjadi beberapa jenis, yakni :

- 802.11

  Menggunakan teknik modulasi OFDM dan berjalan pada frekuensi 5 GHz dengan kecepatan pengirian data mencapai 54 Mbps. Kecepatan pengiriman data lebih tinggi sehingga potensi terjadinya gangguan dari perangkat nirkabel lainnya lebih kecil karena frekuensi ini jarang digunakan. Ada beberapa kelemahan antara lain membutuhkan biaya yang lebih besar, jarak jangkauan lebih pendek karena frekuensi tinggi dan juga dapat menyebabkan sinyal mudah diserap oleh benda penghalang seperti tembok.

- 802.11b

  Menggunakan teknik modulasi DSSS dan berjalan pada frekuensi 2,4 GHz dengan kecepatan pengiriman data mencapai 11 Mbps. Kelebihan dari standar ini adalah biaya implementasi lebih kecil dan jarak jangkau lebih luas. Kelemahannya adalah kecepatan pengiriman data lebih lambat dan rentan terhadap gangguan karena frekuensi 2,4 GHz banyak digunakan oleh perangkat lainnya.

- 802.11g

  Menggunakan teknik modulasi OFDM dan DSSS sehingga memiliki karakteristik dari kedua standar di atas. Standar ini bekerja pada frekuensi 2,4 GHz dengan kecepatan pengiriman data mencapai 54 Mbps tergantung dari jenis modulasi yang digunakan. Kecepatan pengiriman data tinggi (menyamai standar 802.11a), jarak jangkauan cukup luas dan lebih tahan terhadap penyerapan oleh material tertentu karena bekerja pada frekuensi 2,4 GHz, namun rentan terhadap gangguan dari perangkat nirkabel lainnya.

2.2 Pengertian Sensor Monitoring

2.2.1 Intrusion Detection System (IDS)

IDS adalah sebuah aplikasi perangkat lunak atau perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan menganalisis masalah keamanan jaringan. Terdapat 2 jenis IDS, yaitu :

1. Network – based IDS (NIDS)

   NIDS akan melakukan pemantauan terhadap seluruh bagian pada jaringan dengan mengumpulkan paket – paket data yang terdapat pada jaringan tersebut serta melakukan analisa dan menentukan apakah paket – paket tersebut merupakan paket normal atau paket serangan.

2. Host – based IDS (HIDS)

HIDS hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan. HIDS biasanya akan memantau kejadian seperti kesalahan login berkali – kali dan melakukan pengecekan pada file.

Hal yang perlu diperhatikan pada implementasi IDS adalah perihal *false positive* dan *false negative*. *False positive* adalah peringatan serangan yang dihasilkan oleh IDS akan sebuah paket normal pada sistem yang dimonitor. *False negative* adalah sebuah serangan yang benar – benar terjadi namun terlewatkan oleh IDS sehingga IDS tidak akan menghasilkan peringatan apapun atas serangan tersebut. IDS dapat melewatkan serangan karena serangan tersebut tidak dikenali oleh IDS atau karena penyerang berhasil menggunakan sebuah metode serangan yang dapat menghindari IDS.

2.2.2 Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort merupakan sebuah produk terbuka yang dikembangkan oleh Marty Roesch dan tersedia gratis di www.snort.org. Snort bisa digunakan pada sistem operasi linux, Windows, BSD, solaris dan sistem operai lainnya. Snort merupakan IDS berbasis jaringan yang menggunakan metode deteksi rule based, menganalisa paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya.

Gambar 2.1 Logo Snort
Sumber : http://www.snort.org/

Snort digunakan karena memiliki beberapa kelebihan sebagai berikut

- Mudah dalam konfigurasi dan penambahan aturan – aturan.
- Gratis
- Dapat berjalan pada sistem operasi yang berbeda – beda.
- Pembaharuan pola serangan secara berkala.

Snort memanfaatkan perangkat tcpdump untuk mengambil dan menganalisa paket data terhadap sekumpulan jenis serangan yang sudah terdefinisi. Snort dapat berjalan dalam tiga mode antara lain :

- Paket *sniffer*, melihat paket yang lewat di jaringan.
- Paket *logger*, mencatat semua paket yang lewat di jaringan untuk di analisis.
- NIDS, mendeteksi serangan yang dilakukan melalui jaringan komputer dengan konfigurasi dari berbagai aturan yang akan membedakan sebuah paket normal dengan paket serangan.

Pendekatan yang sering digunakan untuk mengenali serangan, antara lain :

a) *Rule Base Detection*

Analisis dilakukan terhadap aktifitas sistem, mencari kejadian yang cocok dengan pola perilaku yang dikenali sebagai serangan.

Ada empat tahap proses analisis pada sistem deteksi ini :

- *Preprocessing*

  Mengumpulkan data tentang pola dari serangan dan meletakkannya pada skema klasifikasi. Kemudian suatu model akan dibangun dan dimasukkan ke dalam bentuk format yang umum seperti nama pola serangan, nomor identitas pola serangan dan penjelasan pola serangan.

- *Analysis*

  Data dan formatnya akan dibandingkan dengan pola serangan yang sudah dikenali.

- *Response*

  Jika ada yang cocok dengan pola serangan, mesin analisis akan mengirimkan peringatan ke server.

- *Refinement*

  Perbaikan dari analisis pencocokan pola yang diturunkan untuk memperbarui pola serangan. Banyak IDS mengijinkan pembaharuan pola serangan secara *manual* sehingga tidak mudah untuk diserang dengan menggunakan pola serangan terbaru.

2.2.3 Komponen Snort

Snort terdiri dari komponen – komponen yang mempunyai tugas dan fungsinya sendiri – sendiri yaitu :

1) *Packet Capture Library*

Packet capture library adalah sebuah perangkat lunak yang terpisah yang mengambil paket data dari NIC. Paket – paket itu adalah paket data *Lapisan Data Link* (OSI model) yang biasanya disebut frame yang masih belum diproses. Pada sistem Linux dan UNIX, Snort menggunakan libpcap, sedangkan pada sistem Windows, Snort menggunakan winpcap.

2) *Packet decoder*

Packet decoder mengambil frame lapisan 2 (Data Link) yang dikirimkan oleh *packet capture library* dan kemudian memecahnya. Pertama – tama komponen ini membaca kode sandi terhadap frame lapisan 2, kemudian paket lapisan 3 (*protocol IP*), lalu kemudian paket lapisan 4 (paket TCP atau UDP). Setelah proses selesai dilakukan, snort mempunyai semua informasi masing – masing protokol untuk pemrosesan lebih lanjut.

3) *Preprocessor*

Preprocessor pada snort memiliki beberapa fitur tambahan yang dapat dimatikan atau dinyalakan. *Preprocessor* bekerja pada paket yang sudah dibaca kode sandinya dan kemudian melakukan transformasi pada data itu supaya lebih mudah untuk diproses oleh Snort.

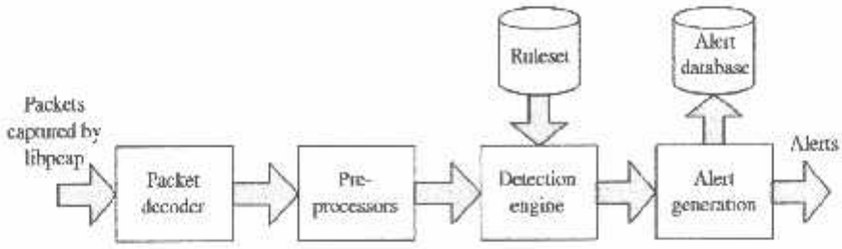
4) *Detection Engine*

Komponen ini mengambil informasi dari packet decoder dan preprocessor yang kemudian memproses data itu pada lapisan Transport dan Application, membandingkan data yang terkandung dalam paket dengan aturan – aturan yang juga merupakan fitur tambahan dari komponen ini.

5) *Output*

Ketika preprocessor terpancing karena adanya data yang cocok dengan definisi jenis jaringan, Snort kemudian menghasilkan peringatan dan kemudian melakukan pencatatan. Snort mendukung beberapa macam keluaran, seperti keluaran dalam format teks atau biner. Pencatatan juga bisa dilakukan ke dalam penyimpanan data ataupun syslog.

Seperti pada gambar 2.2 di bawah ini menjelaskan cara kerja sistem dari snort untuk mengenali serangan.



Gambar 2.2 cara kerja sistem snort

2.3 Apache Web Server

Server HTTP Apache atau *WWW Apache* adalah server web yang dapat dijalankan di banyak sistem operasi (Unix, BSD, Linux, Microsoft Windows dan Novell Netware serta platform lainnya) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

Apache menyediakan fasilitas yang kaya, yang sangat dibutuhkan suatu server serius, seperti otentikasi, pengaturan akses direktori, virtual host, kemampuan URL rewriting, dan juga alias. Kemampuan melakukan content negotiation membuat Apache mampu melayani beragam client secara otomatis, baik untuk berbagai browser yang memiliki kemampuan berbeda ataupun untuk device akses yang berbeda. Fungsi log yang dimiliki oleh Apache dapat dikirim melalui proses piping, sehingga dapat dilakukan rotasi log, filter log, serta melakukan pemisahan log secara langsung.

Awalnya Apache dikembangkan berdasakan keinginan untuk memperbaiki Web server yang saat itu populer (*NCSA web server*). Tetapi akhirnya mengalami perombakan dan penulisan ulang dan menjadi Web server yang berdiri sendiri dan berbeda dengan NCSA. Kini malah mengalahkan kepopuleran NCSA Web server.

Pada tahun 1999 dibentuk Apache Software Foundation untuk mengurus perkembangan Apache ini. Apache telah membuktikan sebagai web server yang cepat, stabil dengan fitur yang paling kaya di antara web server lainnya. Saat ini proyek Apache telah berkembang dan tidak hanya sekedar Web server.

Gambar 2.3 Logo Apache Web Server
Sumber : http://www.apache.org/

2.4 MySql

MySQL adalah sebuah perangkat lunak sistem manajemen basis data SQL (bahasa Inggris: database management system) atau DBMS yang multithread, multi-user, dengan sekitar 6 juta instalasi di seluruh dunia. MySQL AB membuat MySQL tersedia sebagai perangkat lunak gratis dibawah lisensi GNU General Public License (GPL), tetapi mereka juga menjual dibawah lisensi komersial untuk kasus-kasus dimana penggunaannya tidak cocok dengan penggunaan GPL.

2.5 Ubuntu Server

Ubuntu adalah Sistem Operasi yang bersifat open source termasuk dalam salah distribusi Linux berbasiskan Debian. Proyek Ubuntu resmi disponsori oleh Canonical Ltd yang merupakan perusahaan milik seorang kosmonot asal Afrika Selatan Mark Shuttleworth. Nama Ubuntu diambil dari nama sebuah konsep idiologi di Afrika Selatan , "Ubuntu" berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusian terhadap sesama manusia". Setiap rilis mempunyai nama kode dan nomor versi. Nomor versi berdasarkan tahun dan bulan dari rilis. Sebagai contoh, rilis Ubuntu yang pertama, 4.10, dirilis tanggal 20 Oktober 2004. Rilis ubuntu keluar setiap 6 bulan sekali tiap bulan April dan Oktober. Rilis ubuntu

biasanya terdiri dari berbagai edisi, yaitu edisi Desktop, Server, dan Netbook. Khusus untuk LTS (*Long Term Support*) edisi ini di support dari developer sampai tiga tahun berbeda dengan edisi biasa yang hanya satu tahun. Berikut adalah tabel Release Ubuntu seperti pada Tabel 2.1

Tabel 2.1 Tabel Release Ubuntu

Version	Code name	Release date	Supported until	
			Desktop	Server
4.10	Warty Warthog	2004-10-20	2006-04-30	
5.04	Hoary Hedgehog	2005-04-08	2006-10-31	
5.10	Breezy Badger	2005-10-13	2007-04-13	
6.06 LTS	Dapper Drake	2006-06-01	2009-07-14	2011-06
6.10	Edgy Eft	2006-10-26	2008-04-25	
7.04	Feisty Fawn	2007-04-19	2008-10-19	
7.10	Gutsy Gibbon	2007-10-18	2009-04-18	
8.04 LTS	Hardy Heron	2008-04-24	2011-04	2013-04
8.10	Intrepid Ibex	2008-10-30	2010-04-30	
9.04	Jaunty Jackalope	2009-04-23	2010-10-23	
9.10	Karmic Koala	2009-10-29	2011-04	
10.04 LTS	Lucid Lynx	2010-04-29	2013-04	2015-04
10.10	Maverick Meerkat	2010-10-10	2012-04	
11.04	Natty Narwhal	2011-04-28	2012-10	

Colour	*Meaning*
Red	*Release no longer supported*
Green	*Release still supported*
Blue	*Future release*

2.5.1 Konvensi Penamaan

Ubuntu rilis juga diberi nama kode, menggunakan kata sifat dan hewan dengan huruf pertama yang sama (misalnya Dapper Drake). *Dengan pengecualian dari dua rilis, nama kode dalam urutan abjad,* sehingga penentuan cepat adalah rilis yang lebih baru. Umumnya, Ubuntu release yang sering disebut hanya menggunakan kata sifat kode bagian nama (misalnya Dapper).

2.5.1.1 Ubuntu 4.10 (Warty Warthog)

Ubuntu 4.10 (Warty Warthog), dirilis pada tanggal 20 Oktober 2004, adalah Canonical rilis pertama Ubuntu, bangunan pada Debian GNU / Linux dengan rencana untuk rilis baru setiap enam bulan dan delapan belas bulan dukungan setelahnya. Ubuntu 4.10 's dukungan yang berakhir pada tanggal 30 April 2006. Ubuntu 4.10 adalah versi pertama dari ShipIt Ubuntu untuk menawarkan layanan, memungkinkan pengguna untuk memesan CD instalasi gratis. Yang versi desktop termasuk, antara lain program-program desktop, Gaim 1.0, GIMP 2.0, GNOME 2,08, Mozilla Firefox 0.9, dan OpenOffice.org 1.1. versi server dikirim dengan MySQL 4.0, PHP 4.3, dan Python 2.3. Ubuntu 4.10 digunakan Linux kernel 2.6.8 dengan XFree86 4.3.

2.5.1.2 Ubuntu 5.04 (Hoary Hedgehog)

Ubuntu 5.04 (Hoary Hedgehog), dirilis pada tanggal 8 April 2005, adalah kedua Canonical rilis Ubuntu. Ubuntu 5.04 's dukungan berakhir pada tanggal 31 Oktober 2006.

Ubuntu 5.04 menambahkan banyak fitur baru termasuk update manager, upgrade notifier, readahead dan grepmap, suspend, hibernate dan siaga dukungan, dinamis penskalaan

frekuensi untuk prosesor, ubuntu hardware database, Kickstart instalasi, dan APT otentikasi. Ubuntu 5.04 diperbolehkan instalasi dari perangkat USB. Ubuntu 5.04 digunakan UTF-8 secara default.

Instalasi desktop Ubuntu 5,04 termasuk, antara program-program lain, Gaim 1.1, GIMP 2.2, GNOME 2.10, Mozilla Firefox 1.0, dan OpenOffice.org 1.1. Termasuk instalasi server MySQL 4.0, PHP 4.3, dan Python 2.4. Ubuntu 5.04 menggunakan Linux 2.6.10 dan X. Org 6.8.

2.5.1.3 Ubuntu 5.10 (Breezy Badger)

Ubuntu 5.10 (Breezy Badger), dirilis pada 12 Oktober 2005, adalah ketiga Canonical rilis Ubuntu. Ubuntu 5.10 's dukungan yang berakhir pada tanggal 13 April 2007. Ubuntu 5.10 menambahkan beberapa fitur baru termasuk grafis bootloader (Usplash), sebuah Tambah / Hapus Aplikasi alat ini, sebuah menu editor (Alacarte), language selector yang mudah, manajemen volume logis dukungan, penuh Hewlett-Packard printer yang mendukung, OEM installer dukungan, dan Launchpad integrasi untuk bug pelaporan dan pengembangan piranti lunak.

Instalasi desktop Ubuntu 5.10 mencakup, antara program-program lain, Gaim 1.5,GIMP 2.2, GNOME 2.12, Mozilla Firefox 1.0, dan OpenOffice.org 2.0 beta. termasuk instalasi server MySQL 4.1, PHP 5.0, dan Python 2.4. Ubuntu 5.10 menggunakan Linux 2.6.12 dan X. Org 6.8.

2.5.1.4 Ubuntu 6.06 LTS (Dapper Drake)

Ubuntu 6.06 (Dapper Drake), dirilis pada tanggal 1 Juni 2006, adalah keempat Canonical rilis, dan yang pertama Long

Term Support (LTS) release. Ubuntu 6.06 dirilis di belakang jadwal, karena telah dimaksudkan sebagai 6.04. Pembangunan belum selesai pada bulan April 2006 dan Mark Shuttleworth disetujui menyelipkan tanggal rilis hingga Juni, sehingga bukan 6,06.

Ubuntu 6.06 's dukungan yang berakhir pada tanggal 14 Juli 2009 untuk desktop dan akan berakhir pada 1 Juni 2011 untuk server. Ubuntu 6.06 mencakup beberapa fitur baru, termasuk mempunyai Live CD dan Install CD bergabung ke salah satu disk, sebuah installer grafis di Live CD (Ubiquity), Usplash saat shutdown serta startup, manajer jaringan mudah beralih dari beberapa kabel dan koneksi nirkabel, tema Humanlooks diimplementasikan menggunakan Tango pedoman, berdasarkan Clearlooks dan menampilkan warna-warna jingga, bukan coklat, dan GDebi installer grafis untuk berkas paket. Ubuntu 6.06 tidak termasuk cara untuk menginstal dari sebuah perangkat USB, tapi untuk pertama kalinya mengizinkan instalasi dilepas langsung ke perangkat USB.

Instalasi desktop Ubuntu 6.06 mencakup, antara program-program lain, Gaim 1.5, GIMP 2.2, GNOME 2.14, Mozilla Firefox 1.5, dan OpenOffice.org 2.0. Termasuk instalasi server MySQL 5.0, PHP 5.1, dan Python 2.4, serta pilihan untuk menginstal LAMP. Ubuntu 6.06 menggunakan Linux 2.6.15 dan X. Org 7.0.

2.5.1.5 Ubuntu 6.10 (Edgy Eft)

Ubuntu 6.10 (Edgy Eft), dirilis pada tanggal 26 Oktober 2006, adalah kelima Canonical rilis Ubuntu. Ubuntu 6.10 's dukungan yang berakhir pada tanggal 25 April 2008. Ubuntu

6.10 menambahkan beberapa fitur baru termasuk banyak dimodifikasi tema Manusia, Upstart init daemon, otomatis laporan kerusakan (Apport), Tomboy aplikasi pencatatan, dan F-spot foto manager. Easy Ubuntu, pihak ketiga program yang dirancang untuk membuat Ubuntu lebih mudah digunakan, termasuk dalam Ubuntu 6.10 sebagai meta-paket.

Instalasi desktop Ubuntu 6.10 mencakup, antara program-program lain, Gaim 2.0, GIMP 2.2, GNOME 2.16, Mozilla Firefox 2.0, dan OpenOffice.org 2.0. termasuk instalasi server MySQL 5.0, PHP 5.1, dan Python 2,4 . Ubuntu 6.10 menggunakan Linux 2.6.17 dan X. Org 7.1.

2.5.1.6 Ubuntu 7.04 (Feisty Fawn)

Ubuntu 7.04 (Feisty Fawn), dirilis pada tanggal 19 April 2007, adalah keenam Canonical rilis Ubuntu. Ubuntu 7.04 's dukungan yang berakhir pada tanggal 19 Oktober 2008. Ubuntu 7.04 mencakup beberapa fitur baru, di antara mereka migrasi asisten untuk membantu mantan Microsoft Windows pengguna transisi ke Ubuntu, dukungan untuk Kernel-based Virtual Machine, dibantu codec dan driver Pembatasan instalasi termasuk Adobe Flash, Java, MP3 dukungan, instalasi lebih mudah Nvidiadan ATI driver, Compiz desktop effects, dukungan untuk Wi-Fi Protected Access, penambahan Sudoku dan catur, penggunaan disk analyzer (Baobab), GNOME Control Center, dan Zeroconf dukungan untuk berbagai perangkat. Ubuntu 7.04 menjatuhkan dukungan untuk Power PC arsitektur.

Instalasi desktop Ubuntu 7.04 mencakup, antara program-program lain, Gaim 2.0, GIMP 2.2, GNOME 2.18, Mozilla Firefox 2.0, dan OpenOffice.org 2.2. Termasuk instalasi

server MySQL 5.0, PHP 5.2, dan Python 2.5. Ubuntu 7.04 menggunakan Linux 2.6.20 dan X. Org 7.2.

2.5.1.7 Ubuntu 7.10 (Gutsy Gibbon)

Ubuntu 7.10 (Gutsy Gibbon), dirilis pada tanggal 18 Oktober 2007, adalah yang ketujuh Canonical rilis Ubuntu. Ubuntu 7.10 's dukungan yang berakhir pada 18 April 2009. Ubuntu 7.10 mencakup beberapa fitur baru, di antaranya *AppArmorkerangka keamanan, cepat pencarian desktop*, seorang firefox plug-in manager (Ubufox), alat konfigurasi grafis untuk X.org penuh NTFS support (baca / tulis) melalui NTFS-3G, dan sistem pencetakan yang dirubah dengan PDF pencetakan secara default. Compiz Fusion ini diaktifkan sebagai default dalam Ubuntu 7.10 dan Perpindahan pengguna telah ditambahkan.

Instalasi desktop Ubuntu 7.10 mencakup, antara program-program lain, GIMP 2.4, GNOME 2.20, Mozilla Firefox 2.0, OpenOffice.org 2.3, dan Pidgin 2,2 . Termasuk instalasi server MySQL 5.0, PHP 5.2 dan Python 2.5. Ubuntu 7.10 *menggunakan Linux 2.6.22 dan X. Org 7.2.*

2.5.1.8 Ubuntu 8.04 LTS (Hardy Heron)

Ubuntu 8.04 (Hardy Heron), dirilis pada tanggal 24 April 2008, adalah kedelapan Canonical rilis Ubuntu. Ini kedua Long Term Support (LTS) release. Ubuntu 8.04 's dukungan akan berakhir pada April 2011 untuk desktop dan April 2013 untuk server. Ubuntu 8.04 mencakup beberapa fitur baru, di antaranya Tracker pencarian desktop integrasi, Brasero disk burner, Transmission BitTorrent client, Fitur: VNC client, sistem suara melalui PulseAudio, dan Active

Directoryotentikasi dan login menggunakan Terbuka Demikian pula. Di samping Ubuntu 8.04 termasuk update untuk lebih baik Tango kepatuhan, berbagai kegunaan Compiz perbaikan, otomatis meraih dan melepaskan dari kursor mouse ketika berjalan pada VMware mesin virtual, dan metode yang lebih mudah untuk menghapus ubuntu. Ubuntu 8.04 merupakan versi pertama Ubuntu untuk menyertakan Wubi installer di Live CD yang mengizinkan Ubuntu untuk diinstal sebagai satu file pada Windows hard drive tanpa perlu repartition disk.

Instalasi desktop Ubuntu 8.04 mencakup, antara program-program lain, GIMP 2.4, GNOME 2.22, Mozilla Firefox 3.0 beta,OpenOffice.org 2.4, dan Pidgin 2.4. termasuk instalasi server MySQL 5.0, PHP 5.2 dan Python 2,5 . Ubuntu 8.04 menggunakan Linux 2.6.24 dan X. Org 7.3.

2.5.1.9 Ubuntu 8.10 (Intrepid Ibex)

Ubuntu 8.10 (Intrepid Ibex), dirilis pada 30 Oktober 2008, adalah Canonical rilis kesembilan Ubuntu. Akan didukung sampai April 2010. Ubuntu 8.10 memiliki beberapa fitur baru termasuk perbaikan komputer mobile dan desktop skalabilitas, meningkatkan fleksibilitas untuk konektivitas internet, sebuah Ubuntu Live USB pencipta dan rekening tamu, yang memungkinkan orang lain untuk menggunakan komputer Anda dan dengan hak-hak pengguna sangat terbatas (misalnya mengakses Internet, dengan menggunakan perangkat lunak dan memeriksa e-mail). guest account yang memiliki folder Home dan tidak ada yang dilakukan pada akan disimpan secara permanen di hard disk komputer. Intrepid Ibex juga berisi direktori yang dienkripsi untuk

pengguna pribadi , dimasukkannya Dynamic Kernel Module Support, alat yang memungkinkan driver kernel yang akan dibangun kembali secara otomatis ketika kernel yang baru dirilis dan dukungan untuk membuat USB flash drive gambar.

Instalasi desktop Ubuntu 8.10 mencakup, antara program-program lain, GIMP 2.6, GNOME 2,24, Mozilla Firefox 3.0, OpenOffice.org 2.4, dan Pidgin 2.5. termasuk instalasi server MySQL 5.0, PHP 5.2 dan python 2.5. Ubuntu 8.10 menggunakan Linux 2.6.27 dan X. Org 7.4. Cepat-user-switch-applet mengalami perubahan besar dan menggantikan tombol logout. Hal ini dapat digunakan untuk mengubah Pidgin atau empati status.

2.5.1.10 Ubuntu 9.04 (Intrepid Ibex)

Ubuntu 9.04 (Intrepid Ibex), dirilis pada tanggal 23 April 2009 adalah Canonical's kesepuluh rilis dari distribusi. Akan didukung sampai Oktober 2010. Fitur baru termasuk cepat boot waktu , integrasi layanan web dan aplikasi ke dalam *desktop antarmuka. Ini memiliki baru usplash layar, baru* layar login dan juga dukungan untuk kedua Wacom (hotplugging) dan netbook. Ini juga mencakup sistem pemberitahuan yang baru, Beritahu OSD , dan tema. Ini menandai pertama kalinya bahwa semua inti pengembangan Ubuntu pindah ke Bazar terdistribusi kontrol revisi sistem.

Instalasi desktop Ubuntu 9.04 mencakup, antara program-program lain, GIMP 2.6, GNOME 2,26, Mozilla Firefox 3.0, OpenOffice.org 3.0, dan Pidgin 2.5. Ubuntu 9.04 menggunakan Linux 2.6.28 dan X. Org 7.4. Default sistem berkas ext3 denganext4 tersedia di instalasi sebagai pilihan.

2.5.1.11 Ubuntu 9.10 (Karmic Koala)

Ubuntu 9,10 (Karmic Koala), dirilis pada tanggal 29 Oktober 2009 dan adalah Canonical's kesebelas rilis distribusi dan akan didukung sampai April 2011.

Dalam pengumuman kepada masyarakat di 20 Febnuari 2009, Mark Shuttleworth menjelaskan bahwa 9,10 akan berfokus pada perbaikan dalam komputasi awan di server menggunakan Eucalyptus, perbaikan lebih lanjut dalam kecepatan boot serta pembangunan di Netbook Remix.

Instalasi desktop Ubuntu 9,10 mencakup, antara program-program lain, GIMP 2.6, GNOME 2,28, Mozilla Firefox 3.5,OpenOffice.org 3.1, Linux 2.6.31, dan Empati Instant Messenger, bukan Pidgin. The default filesystem ext4, danUbuntu Satu klien, yang interface dengan Canonical penyimpanan online baru sistem, diinstal secara default. Hal ini juga debut aplikasi baru yang disebut Ubuntu Software Center yang menyatukan manajemen paket. Kanonik berniat untuk aplikasi ini untuk menggantikan Add / Remove Programs (gnome-app-install) di 9.10 dan kemungkinan Synaptic, Software Sources, GDebi dan Update Manager di Ubuntu 10,04. Karmic Koala juga mencakup tayangan slide selama proses instalasi (melalui mana-mana-slide) yang menyoroti dan fitur aplikasi dalam Ubuntu.

2.5.1.12 Ubuntu 10.04 LTS (Lucid Lynx)

Ubuntu 10,04 (Lucid Lynx) ini pertama kali diumumkan di Atlanta Linux Fest oleh Shuttleworth di 19 September 2009, dan direncanakan untuk rilis pada tanggal 29 April 2010.

Rilis baru berisi kernel Linux 2.6.32 dan meningkatkan dukungan untuk nVidia driver proprietary grafis, sementara beralih ke open source driver grafis nVidia, nouveau, secara default.

Pada tanggal 4 Maret 2010 diumumkan bahwa Lucid Lynx akan menampilkan tema baru, termasuk logo baru.

2.6 Php

PHP (Hypertext Prepocessor) adalah bahasa pemrograman script yang paling banyak dipakai saat ini. PHP banyak dipakai untuk memrogram situs web dinamis, walaupun tidak tertutup kemungkinan digunakan untuk pemakaian lain. Contoh terkenal dari aplikasi PHP adalah phpBB dan MediaWiki (software di belakang Wikipedia). PHP juga dapat dipakai sebagai pilihan lain dari ASP.NET/C#/VB.NET Microsoft, ColdFusion Macromedia, JSP/Java Sun Microsystems, dan CGI/Perl. Contoh aplikasi lain yang lebih kompleks berupa CMS yang dibangun menggunakan PHP adalah Mambo, Joomla!, Postnuke, Xaraya, dan lain-lain.

PHP mempunyai banyak kelebihan di banding bahasa pemrograman yang lainnya, yaitu :

- ✓ Bahasa pemrograman PHP adalah sebuah bahasa script yang tidak melakukan sebuah kompilasi dalam penggunaanya.
- ✓ Web Server yang mendukung PHP dapat ditemukan dimana - mana dari mulai apache, IIS, Lighttpd, hingga Xitami dengan konfigurasi yang relatif mudah.

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisa Sistem

Pemahaman konsep dasar sistem operasi Ubuntu 10.04 dan snort merupakan hal yang utama untuk dipahami dalam pembuatan sensor monitoring. Maka dari itu diperlukan semacam referensi untuk menghasilkan suatu sistem yang handal.

3.1.1 Deskripsi Umum Sistem

Sistem yang dikembangkan dalam tugas akhir ini adalah sensor monitoring dimana sistem ini memiliki fungsi dasar yaitu, melakukan fungsi rekam paket (*packet record*) yaitu perangkat lunak yang terpisah yang mengambil paket data dari NIC. Analisa Packet (*analyze packet*) yaitu menganalisa packet yang sudah ditangkap dan dicocokkan kedalam rule database yang sudah dipersiapkan. Output yaitu hasil keluaran setelah data diolah dan dicocokan kedalam tampilan *web base*.

3.1.2 Fitur Sistem Sensor Monitoring

Dalam pembuatan sistem sensor monitoring disamping fitur utama adalah menganalisa paket data yang lewat dalam jaringan. Sistem ini mempunyai fitur lain guna mempermudah pelaporan kondisi jaringan yang termonitoring Dalam pembuatan sistem sensor monitoring disamping fitur utama adalah menganalisa paket data yang lewat dalam jaringan. Sistem ini mempunyai fitur lain guna mempermudah pelaporan kondisi jaringan yang termonitoring :

1. Report berupa graphic yang dapat digenerate per hari, minggu, bulan dan tahun.
2. Report perhari akan dikirimkan ke email administrator yang didaftarkan.

3.1.3 Analisa Kebutuhan Sistem

Sistem Sensor Monitoring yang akan di implementasikan secara keseluruhan memiliki kebutuhan teknis minimal sebagai berikut :

1. Komputer tower Intel(R) Pentium 4
2. RAM DDR2 2 Gigabyte (GB).
3. Hardisk sata 80 Gigabyte.

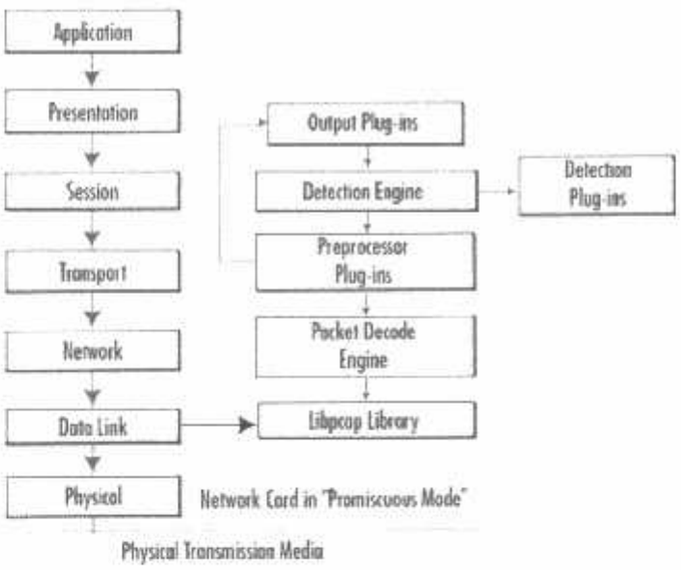
Selain perangkat keras Sensor Monitoring yang akan dibangunkan juga membutuhkan spesifikasi perangkat-perangkat lunak minimum sebagai berikut :

1. *Operating System* Ubuntu 10.04 LTS - 64 bits.
2. Apache Webserver / 2.2.14.
3. PHP 5 - pemrograman *Web base* Sensor Monitoring.
4. Mysql Server 5 – Sebagai *Database Server*.
5. Snort sebagai *base engine* sistem monitoring

3.1.4 Analisa Sensor Monitoring

3.1.4.1 Jenis Sensor

Jenis Sensor yang digunakan adalah snort Network base, dimana melakukan pemantauan terhadap seluruh bagian pada jaringan dengan mengumpulkan paket-paket data yang terdapat pada jaringan. Ilustrasi Sensor Monitoring dengan snort dalam protokol jaringan pada Gambar 3.1



Gambar 3.1 Snort Pada Jaringan OSI Layer

3.2 Perancangan Sistem

Perancangan sistem merupakan langkah awal yang harus dilakukan dalam proses pembangunan sebuah sistem sensor monitoring berbasis snort, khusunya untuk Ubuntu 10.04 server. Sebagai media interaksi yang dapat mempermudah administrator jaringan dalam menganalisa jaringannya aplikasi ini dilengkapi tampilan GUI (*Graphical Unit Interface*) berbasis Web atau *Web Base*.

Dalam perancangan sistem, ada beberapa tahapan yang dilakukan, yaitu:

1. Desain Sistem Sensor Monitoring

   Desain Sensor Monitoring yang akan dibangun adalah sebuah sistem sensor monitoring berbasis snort yang bebas lisensi tapi tetap berkualitas dan handal dalam menangani lalu lintas data dalam suatu jaringan wifi dengan menggunakan software Ubuntu Server 10.04 LTS.

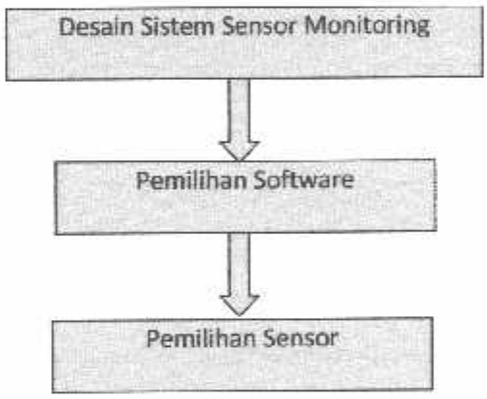
2. Pemilihan Software

Pembangunan sensor monitoring memanfaatkan software Ubuntu 10.04 LTS karena sudah terbukti software ini mempunyai stabilitas yang tinggi dan tidak menghabiskan memori yang banyak dalam PC.

3. Pemilihan Sensor

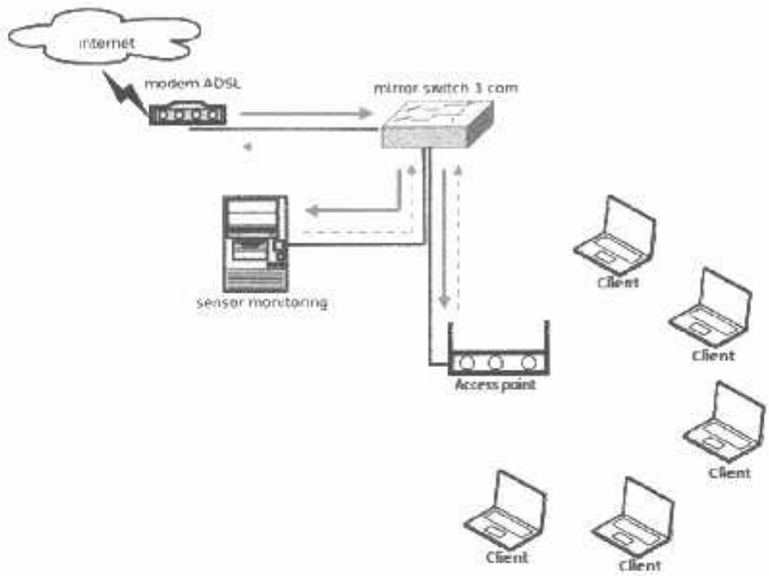
Memakai snort untuk melakukan monitoring pada sebuah jaringan wifi adalah pemilihan yang tepat dikarenakan perangkat lunak snort merupakan tipe network base dalam melakukan pemantauan aktifitas jaringan.

Ilustrasi diagram perancangan sistem sensor monitoring dapat dilihat pada Gambar 3.2



Gambar 3.2 Diagram Perancangan Sensor Monitoring

3.3 Desain Sistem



Keterangan :

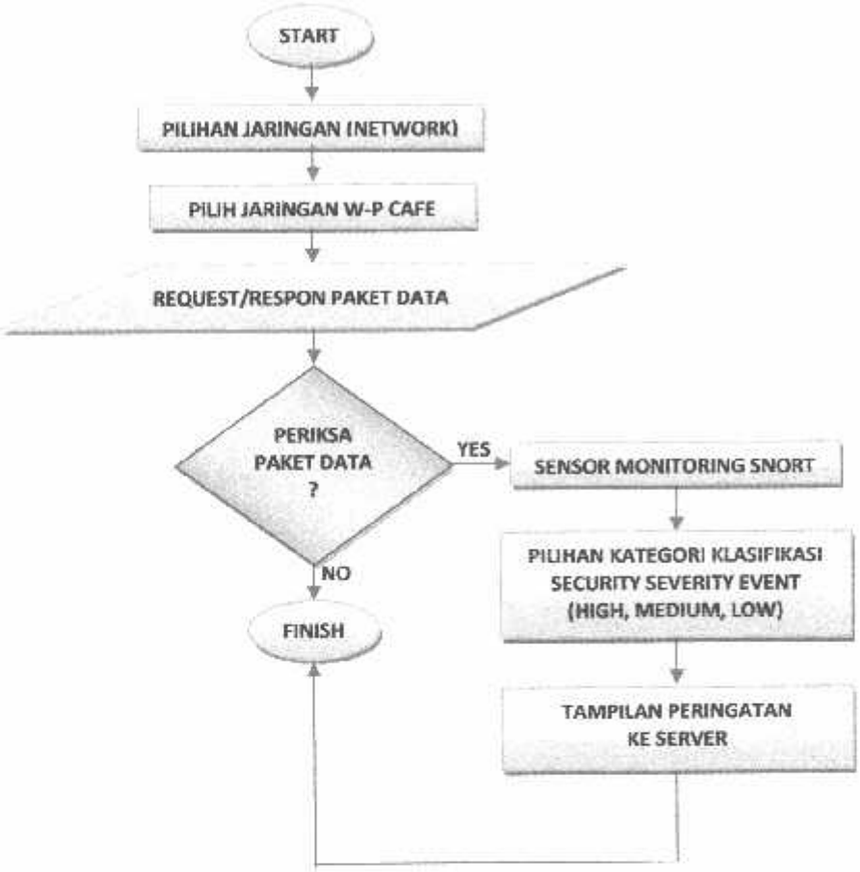
⟶ = aliran data masuk

⇢ = aliran data keluar

Gambar 3.3 Desain Sistem Sensor Monitoring

Dari Gambar 3.3 tampak bahwa Aliran data yang masuk dari *router* dikirim melalui *mirror Switch* kemudian paket data tersebut di copy oleh server sensor monitoring dan diteruskan ke *Access Point* dan disebar pada masing – masing client. Fungsi dari server sensor monitoring ini hanya mengcopy paket data yang lewat tanpa menghalangi aliran paket data yang melintas melalui mirror switch maupun Access Point.

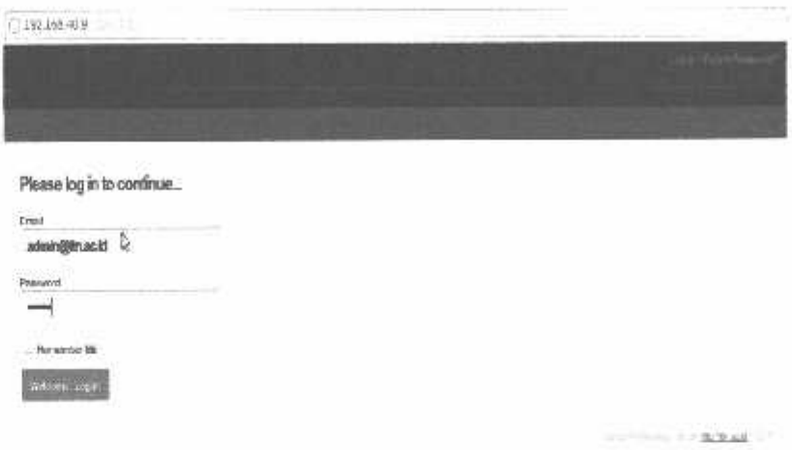
3.3.1 Flowchart Sistem Sensor Monitoring



Gambar 3.4 Flowchart Sistem Sensor Monitoring

3.4 Tampilan Halaman Administrator Sensor Monitoring

Pada bagian ini akan dijelaskan mengenai tampilan dari Halaman Administrator Sensor Monitoring.



Gambar 3.4 Tampilan Halaman login

Gambar 3.5 Halaman Menu Dashboard

Gambar 3.6 Halaman Menu Account

Dari Gambar 3.4 dan 3.5 menunjukkan proses umum secara keseluruhan berupa hasil kerja sistem monitoring berupa tampilan menu severity event dan sub menu severity, yang menunjukkan aktifitas sensor monitoring yang bekerja secara otomatis memantau lalu lintas data yang lewat di jaringan dengan dikategorikan dalam 3 klasifikasi security (*High Severity*, *Medium Severity* dan *Low Severity*).

Pada Gambar 3.6 adalah halaman menu administrator setelah login. Dimana terdapat submenu diantaranya : *Dashboard*, *Report*, *Sensor*, *Sources*, *Signatures*, *Account*.

Fungsi Masing – Masing Menu adalah :

Dashboard : Menu utama yang digunakan untuk melihat kinerja sensor.

Report : Digunakan sebagai laporan paket data yang di sensor.

Sensor : Digunakan untuk menunjukkan NIC yang dibuat oleh sensor.

Sources : Alamat IP yang tercatat dalam sensor snort.

Signatures : Daftar rule yang digunakan sensor.

Account : Pengaturan – pengaturan yang digunakan untuk fungsi administrator.

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem

4.1.1 Instalasi dan Konfigurasi Ubuntu 10.04 LTS

Ubuntu 10.04 LTS merupakan salah satu distro Linux yang ditujukan untuk keperluan server sama halnya dengan beberapa distro Linux yang lain. Pada beberapa administrator server Linux, pengguna atau administrator tidak memerlukan tampilan grafis, schingga instalasi hanya dilakukan pada *base sistem* dan paket-paket instalasi tertentu yang sudah tersedia di dalam CD/DVD instalasinya. Mengenai tahapan-tahapan Instalasi Ubuntu 10.04 LTS secara lengkap dilampirkan.

Instalasi dan Konfigurasi Snort di Server Ubuntu 10.04 LTS

Tahap persiapan untuk server install sudo apt-get install nmap

```
sudo apt-get install libpcre3 libpcre3-dev libpcrecpp0 libpcap0.8
libpcap0.8-dev \
mysql-server libmysqlclient15-dev libphp-adodb libgd2-xpm libgd2-
xpm-dev php5-mysql \
php5-gd php-pear apache2 php5 php5-xmlrpc php5-mysql php5-gd php5-
cli php5-curl \
mysql-client libdumbnet1 libdumbnet-dev
```

```
pear install Numbers_Roman-1.0.2
pear install Numbers_Words-0.16.2
pear install Image_Canvas-0.3.2
pear install Image_Graph-0.7.2
pear install --alldeps mail
```

4.1.2 Instalasi dan Konfigurasi Snort

*Untuk melakukan instalasi **Snort**, lakukan perintah sebagai berikut :*

```
sudo tar zxvf snort-2.8.6.tar.gz
cd snort-2.8.6
sudo ./configure --prefix=/usr/local/snort
sudo make
sudo make install
sudo mkdir /var/log/snort
sudo groupadd snort
sudo useradd -g snort snort
sudo chown snort:snort /var/log/snort
sudo vi /usr/local/snort/etc/snort.conf
dynamicpreprocessor
directory/usr/local/snort/lib/snort dynamicpreprocessor/
dynamicengine/usr/local/snort/lib/snort dynamicengine/libsf_engine.
so
dynamicdetection directory /usr/local/snort/lib/snort_dynamicrules
```

4.1.3 Konfigurasi Database Snort

```
echo "create database snort;" | mysql -u root -p
mysql -u root -p -D snort < ./schemas/create_mysql
echo "grant create, insert, select, delete, update on snort.* to
snort@localhost identified by 'YOURPASSWORD'" | mysql --u root -p
```

4.1.4 Konfigurasi Server Ubuntu Untuk Tuning Performance Snort

```
sudo tar zxvf barnyard2-1.8.tar.gz
cd barnyard2-1.8
sudo ./configure --with-mysql
sudo make
sudo make install
sudo cp etc/barnyard2.conf /usr/local/snort/etc
sudo mkdir /var/log/barnyard2
sudo vi /usr/local/snort/etc/barnyard2.conf
```

```
config reference_file: /usr/local/snort/etc/reference.config
config classification file:
/usr/local/snort/etc/classification.config
config gen_file: /usr/local/snort/etc/gen-msg.map
config sid_file: /usr/local/snort/etc/sid-msg.map
config hostname: localhost
config interface: eth0  //penempatan sensor pada nic eth0
```

```
output database: log, mysql, user=snort password=YOURPASSWORD
dbname snort
 host=localhost
```

Modifikasi file /usr/local/etc/snort/snort.conf:

```
var HOME_NET any
var EXTERNAL_NET any
var DNS_SERVERS [1.1.1.1/32,2.2.2.2/32]
var SMTP_SERVERS $HOME_NET
var RULE_PATH //snort/
preprocessor frag2
preprocessor stream4: detect_scans detect_state_problems
preprocessor stream4_reassemble: ports all
preprocessor unidecode: 80 8080
preprocessor rpc_decode: 111
preprocessor bo: -nobrute
preprocessor telnet_decode
preprocessor portscan: 0.0.0.0/0 6 3 /var/log/snort/portscan.log
preprocessor portscan-ignorehosts: $DNS_SERVERS

output a ert syslog: LOG_AUTH LOG_ALERT LOG_PID
output database: log, mysql, user=snort password=new_password
dbname=snort host=localhost
```

Script Preprocessor berfungsi sebagai triggers peringatan.

Kemudian tambahkan file rules yang diinginkan pada *file /usr/local/etc/snort/snort.conf.* Semua file rules snort disimpan di direktori */etc/snort.*

```
# Include classification & priority settings
include /usr/local/snort/classification.config
include /usr/local/snort/exploit.rules
include /usr/local/snort/scan.rules
include /usr/local/snort/finger.rules
include /usr/local/snort/ftp.rules
include /usr/local/snort/telnet.rules
include /usr/local/snort/smtp.rules
include /usr/local/snort/rpc.rules
include /usr/local/snort/rservices.rules
include /usr/local/snort/backdoor.rules
include /usr/local/snort/dos.rules
include /usr/local/snort/ddos.rules
include /usr/local/snort/dns.rules
include /usr/local/snort/netbios.rules
include /usr/local/snort/web-cgi.rules
include /usr/local/snort/web-coldfusion.rules
include /usr/local/snort/web-frontpage.rules
include /usr/local/snort/web-iis.rules
include /usr/local/snort/web-misc.rules
include /usr/local/snort/sql.rules
include /usr/local/snort/x11.rules
include /usr/local/snort/icmp.rules
include /usr/local/snort/shellcode.rules
include /usr/local/snort/misc.rules
include /usr/local/snort/policy.rules
include /usr/local/snort/info.rules
#include /usr/local/snort/icmp-info.rules
include /usr/local/snort/virus.rules
include /usr/local/snort/local.rules
# vision.rules will be catched by arachnids_upd
include /etc/snort/vision.rules
```

File yang berkaitan dengan tools snort adalah:

/etc/snort/classification.config

```
#
# config classification:shortname,short description,priority
#
#config classification: not-suspicious,Not Suspicious Traffic,0
config classification: unknown,Unknown Traffic,1
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,3
config classification: successful-recon-limited,Information Leak,4
config classification: successful-recon-largescale,Large Scale
Information Leak,5
config classification: attempted-dos,Attempted Denial of Service,6
config classification: successful-dos,Denial of Service,7
config classification: attempted-user,Attempted User Privilege
Gain,8
config classification: unsuccessful-user,Unsuccessful User
Privilege
Gain,7
config classification: successful-user,Successful User Privilege
Gain,9
config classification: attempted-admin,Attempted Administrator
Privilege
Gain,10
config classification: successful-admin,Successful Administrator
Privilege Gain,11
```

```
# added from vision18.conf
# classification for use with a management interface
# low risk
config classification: not suspicious,policy traffic that is not
suspicious,0
config classification: suspicious,suspicious miscellaneous
traffic,
config classification: info-failed,failed information gathering
attempt,2
config classification: relay-failed,failed relay attempt,3
config classification: data-failed,failed data integrity attempt,4
config classification: system-failed,failed system integrity
attempt,5
config classification: client-failed,failed client integrity
attempt,6
```

```
# med risk
config classification: denialofservice,denial of service,7
config classification: info-attempt,information gathering attempt,8
config classification: relay-attempt,relay attempt,9
config classification: data-attempt,data integrity attempt,10
config classification: system-attempt,system integrity attempt,11
config classification: client-attempt,client integrity attempt,12
config classification: data-or-info-attempt,data integrity or
information
gathering attempt,config classification: system-or-info-
attempt,system
integrity or information gathering attempt,config classification:
relay-
or-info-attempt,relay of information gathering attempt,15
# high risk
config classification: info-success,successful information
gathering
attempt,16
config classification: relay-success,successful relay attempt,17
config classification: data-success,successful data integrity
attempt,18
config classification: system-success,successful system integrity
attempt,19
config classification: client-success,successful client integrity
attempt,20
```

File ini berfungsi untuk mendefinisikan rules.

Jalankan snort dengan perintah:

```
# /etc/init.d/snortd start
```

Set snort untuk dijalankan pada saat boot time.

Gunakan *script* yang terdapat pada *contrib directory*, *S99snort*.

Copy file tersebut ke direktori */etc/init.d* dang anti nama file menjadi snort.

```
# cp contrib/S99snort /etc/irit.d/snort
```

Ganti baris berikut:

```
CONFIG /etc/snort/snort.conf
SNORT_GID=snort
```

Kemudian masuk ke *direktori /etc/init.d* dan ketikan perintah:

```
# chmod 755 snort
# cd /etc/rc3.d
# ln -s ../init.d/snort S99snort
# ln -s ../init.d/snort K99snort
# cd /etc/rc5.d
# ln -s ../in_t.d/snort S99snort
# ln -s ../init.d/snort K99snort
```

Setting up database pada MySQL :

Untuk membuat *database* snort pada mysql, lakukan langkah berikut:

```
# /usr/local/mysql/bin/mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR snort@localhost=PASSWORD('new_password');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort@loca_host;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

Dari Snort 2.0.2 source directory jalankan perintah berikut:

```
# /usr/local/mysql/bin/mysql -u root -p < ./contrib/create_mysql
  snort
Enter password:
```

Kemudian install *extra DB* tables menggunakan perintah pada *contrib directory* (masuk terlebih dahulu ke *contrib. directory*) :

```
# zcat snortdb-extra.gz |/usr/local/mysql/bin/mysql -p snort
Enter password:
```

```
# /usr/local/mysql/bin/mysql -p
>Enter password:
mysql> SHOW DATABASES;
(You should see the following)
+------------+
| Database
+-------------
| mysql
| snort
| test
+------------+
3 rows in set (0.00 sec)
mysql> use snort
>Database changed
```

```
mysql> SHOW TABLES;
+------------------+
| Tables in snort
+------------------+
| data
| detail
| encoding
| event
| flags
| icmphdr
| iphdr
| opt
| protocols
| reference
| reference_system
| schema
| sensor
| services
| sig_class
| sig_reference
| signature
```

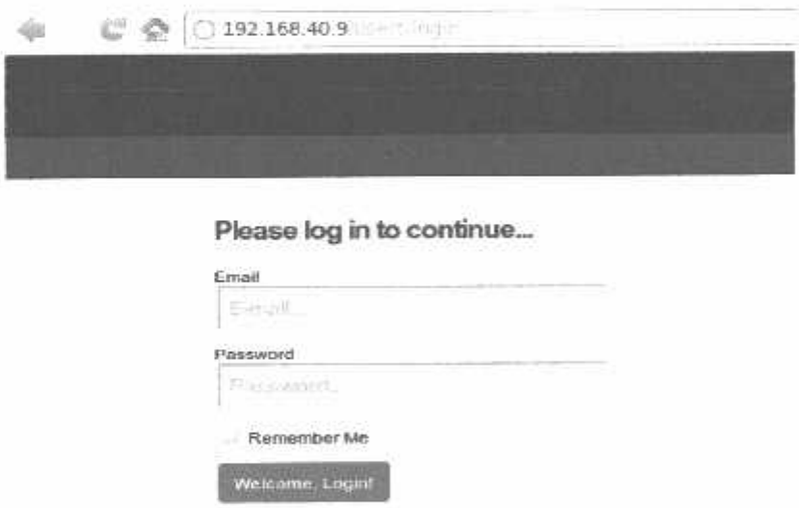
```
| tcphdr
| udphdr
+-------------------+
19 rows in set (0.00 sec)>Bye
```

4.2 Pengujian Sistem

Setelah berhasil di implementasikan langkah selanjutnya adalah melakukan serangkaian ujicoba sistem. Pengujian Sistem dilakukan untuk mengetahui kinerja *Sensor*.

4.2.1 Penerapan Aplikasi Sensor Monitoring

Penerapan aplikasi Sensor Monitoring dengan menggunakan aplikasi *snort* dan bahasa pemrograman *Php* yang dikonfigurasi dengan aplikasi lainnya seperti *server ubuntu 10.04 LTS, apache, Sql server*. Penerapan dapat di uji dengan melakukan proses *login*. Pengujian dilakukan dengan mengirimkan *email* dan *password*, Halaman *login* seperti pada Gambar 4.1.



Gambar 4.1 Tampilan Halaman Login

Email dan *password* berfungsi sebagai pengendali hak penuh atas kinerja sensor monitoring, dalam hal ini yaitu admin.

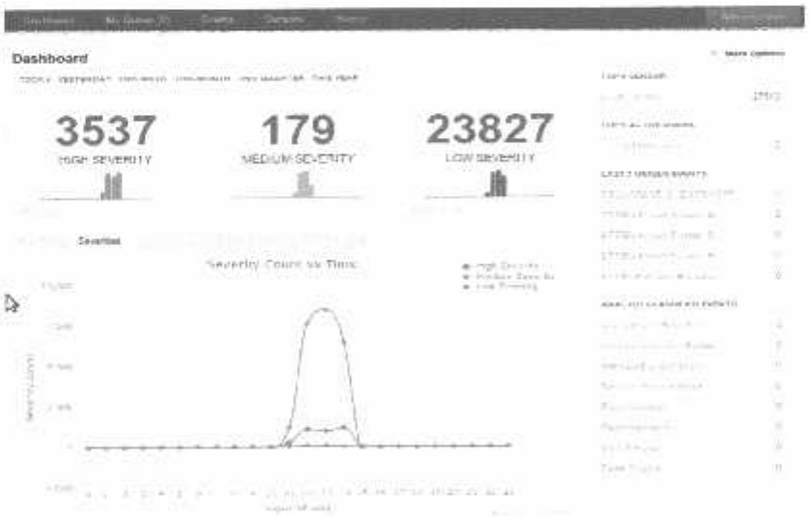
4.2.2 Menu Utama (Dashboard)

Setelah proses di atas berhasil maka akan keluar tampilan menu dashboard. *dashboard* merupakan tampilan *interface webbase* atau menu utama untuk melihat kinerja sensor monitoring secara keseluruhan berdasarkan jumlah event dan waktu selama si admin memantau kondisi jaringan pada saat itu. Seperti pada Gambar 4.2.

Gambar 4.2 Tampilan Menu Dashboard

4.2.3 Menu Severity Count

Pada severity count menunjukkan hasil analisa paket data yang melintasi jaringan yang berdasarkan 3 kategori tingkatan klasifikasi security (high severity, medium severity, low security), dan dalam hitungan per waktu.



Gambar 4.3 Tampilan Menu Severities

4.2.4 Menu protocols

Pada menu protokol menunjukkan beberapa jumlah event berdasarkan protokol count dan waktu. Seperti layanan pada protokol *TCP* berupa Koneksi dari client ke server, dan kemudian banyak data dapat dikirimkan melalui koneksi tersebut.

Protokol *UDP* merupakan Koumikasi yang dicapai dengan mengirimkan informasi satu arah, dari source ke destination tanpa mengecek untuk melihat apakah tujuan masih ada, atau apakah koneksi disiapkan untuk menerima informasi. Paket UDP melewati jaringan dalam unit-unit yang berdiri sendiri.

Protokol *ICMP* messages yang digunakan client untuk mendeteksi host tersebut online pada jaringan atau tidak. Contoh: PING command.

Gambar 4.4 Tampilan Menu Protocols

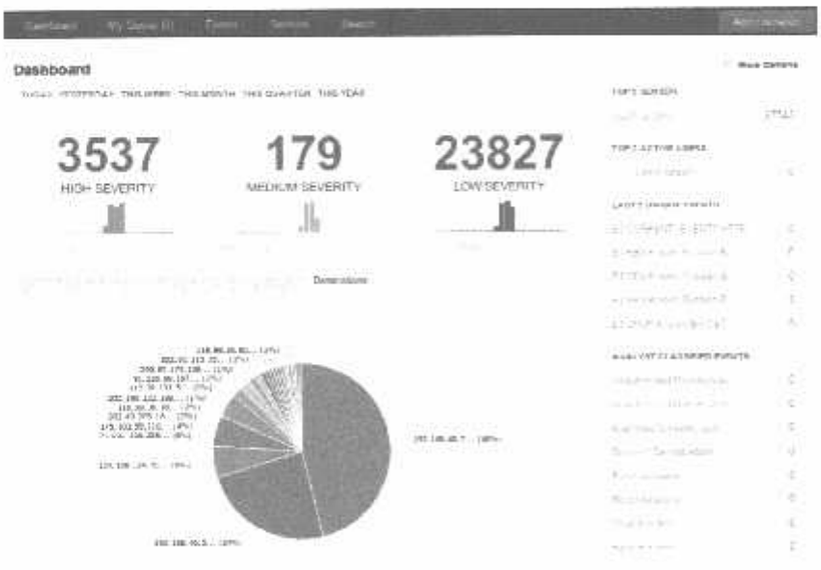
4.2.5 Menu Signature

Berupa tampilan grafik yang termonitor dimana terdapat sejumlah daftar nama event yang terdaftar dalam *rule snort*. Misalnya dalam *rule base* snort terdapat paket data berupa http_inspect:LONG HEADER dan sebanyak 13424 paket data selama ada transaksi dari si clien yang meminta layanan terhadap host tujuan. jika paket data tersebut terdapat dalam *rule base* snort, maka akan terpantau oleh sensor monitoring seperti Gambar 4.5.

Gambar 4.5 Tampilan Menu Signatures

4.2.6 Menu Destinations

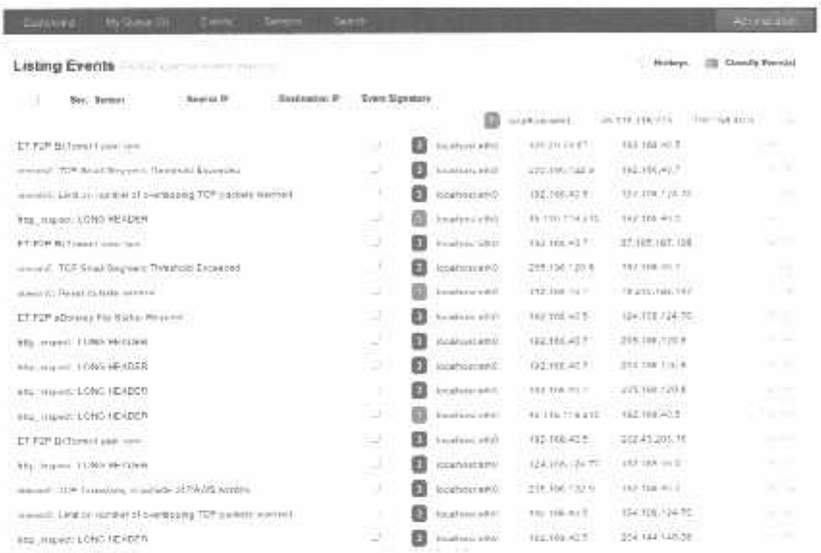
Bentuk pola sejumlah event alamat asal yang berada dalam jaringan yang terpantau dalam sensor monitoring dengan melakukan aktifitas transaksi paket data, dalam hal ini client meminta layanan terhadap IP tujuan. IP tujuan tersebut berupa host name yang memberikan layanan yang diminta oleh si client seperti dalam Gambar 4.6.



Gambar 4.6 Tampilan Menu Destinations

4.2.7 Menu Listing Events

Tampilan Daftar event atau paket data yang ditangkap oleh sensor. Event tersebut berupa kode warna tertentu yang menunjukkan tingkat paket data yang normal, paket data normal ataupun yang membahayakan, dalam hal ini tingkat abnormal ditandai dengan warna merah, namun selama pengujian paket data tersebut dikategorikan normal dikarenakan admin bertindak sebagai client.



Gambar 4.7 Tampilan Menu Listing Events

4.2.8 Menu Listing Sensor

Gambar 4.8 menunjukkan *interface* atau alamat *NIC* yang digunakan untuk sensor. Pada hal ini memakai *eth0* dengan sejumlah event yang terpantau oleh sensor. Dalam hal ini sebagai pengujian digunakan nama sensor menggunakan nama *imam*, host name berupa *local host* dengan *interface eth0*, event count 27543 event.

Gambar 4.8 Tampilan Menu Listing Sensors

4.2.9 Menu Search

Pencarian tentang suatu jenis signature event secara singkat dari beberapa jenis signature event dalam rule base snort yang ada seperti nama *signature, source address, destination address, timestamp, source port, destination port, select sensor, select classification, select severity.*

Gambar 4.9 Tampilan Menu Search

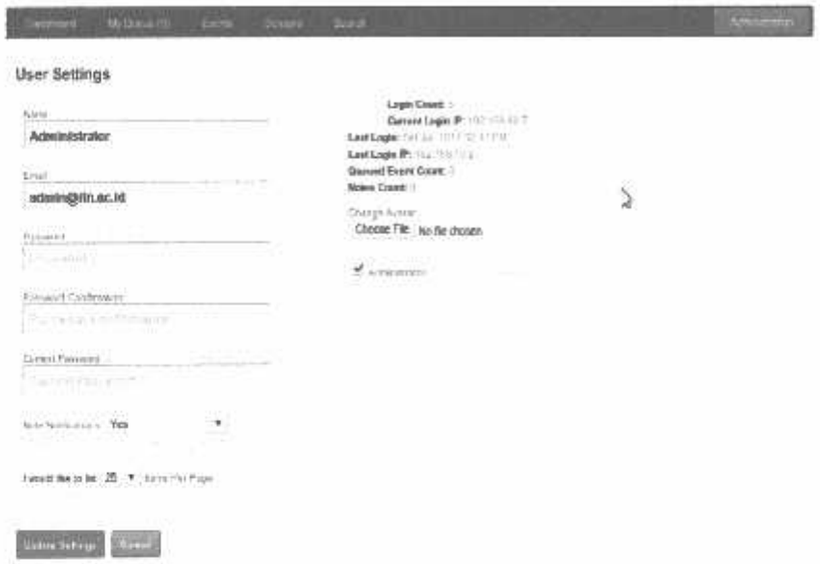
4.2.10 Menu General Setting

Berfungsi sebagai pengaturan umum bagi fungsi admin seperti nama pengguna sensor, *company email* yang disesuaikan dengan email yang didaftarkan.

Gambar 4.10 Tampilan Menu General setting

4.2.11 Menu User Setting

Berfungsi sebagai pengaturan akses login bagi pengguna aplikasi seperti perubahan *email*, *password* lama dengan *password* baru. Jumlah daftar *list* signature dalam tabel signature name yang belum diklasifikasi sesuai dengan rule base sensor monitoring dalam hal ini berupa aplikasi snort.

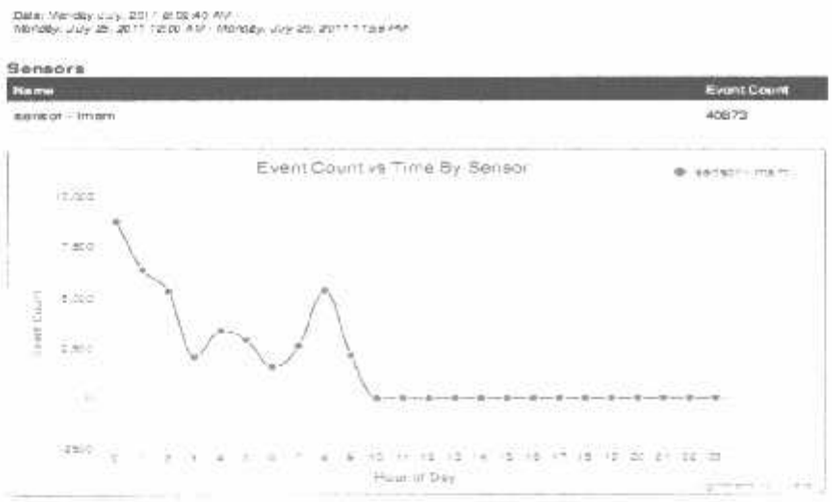


Gambar 4.11 Tampilan Menu User Setting

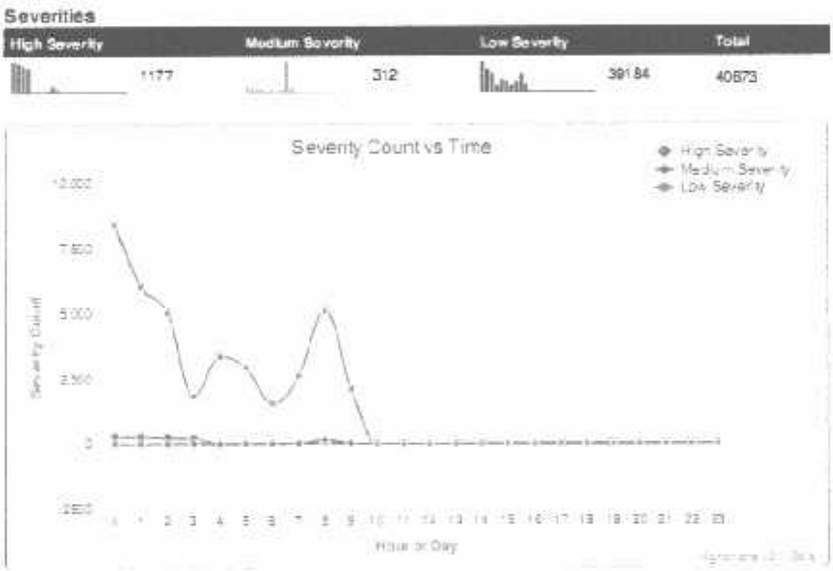
4.3 Hasil Pelaporan Sistem

Kinerja Sensor akan dipantau terus oleh pengelola atau admin dan hasilnya dari sistem sensor monitoring akan dilaporkan ke server dengan digenerate berupa *PDF*. Gambar 4.11 merupakan halaman user yang berfungsi sebagai pengendali sensor, user di atas merupakan administrator sebagai name, email berupa *admin@itn.ac.id*, serta password lama dan baru jika menginginkan perubahan dalam hal keamanan sistem. Report yang dikirimkan kepada email si admin berupa isi laporan menyangkut jumlah total event dan real time. Berdasarkan kategori dalam severity paket normal ataupun paket – paket yang mencurigakan.

Tujuan dari report atau pelaporan sistem yaitu sebagai *output* dari tindak lanjut peringatan oleh sistem sensor terhadap server dengan hasil laporan tersebut bisa mengurangi kecurangan oleh si client terhadap penghubung penyedia layanan internet dalam hal ini yaitu ITN Malang.



Gambar 4.12 Gafik Sensor Event Count

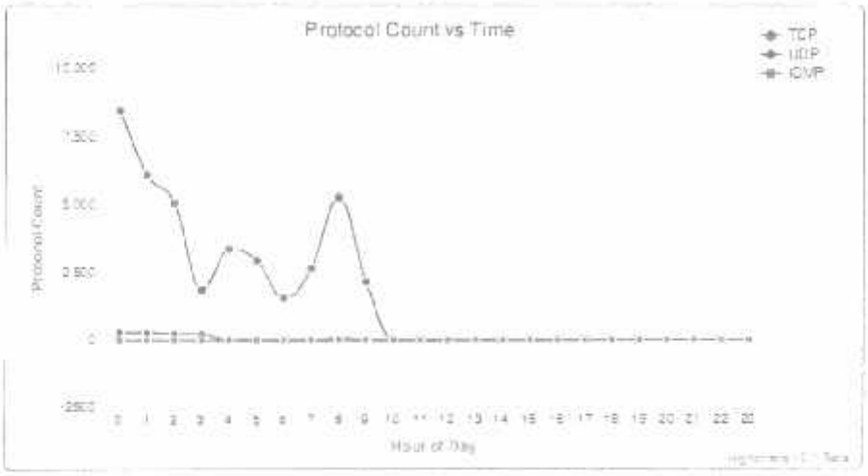


Gambar 4.13 Gafik Severity Event Count

Pada gambar 4.13 menunjukkan laporan severity count per hari berdasarkan tiga kategori angka dan tampilan skala grafik (high severity, medium severity, dan low severity). Analisa pengujian dilakukan mulai pukul 12 hingga pukul 10 dengan total mencapai 40673 severity count dan sejauh itu tingkat security event yang didominasi oleh paket data normal.

Protocols

TCP Count	UDP Count	ICMP Count	Total
39522	1151	0	40673



Gambar 4.14 Gafik Protocol Count

Pada gambar 4.14 menampilkan jumlah laporan keseluruhan paket data berdasarkan *protocol event*. Protokol – protokol tersebut adalah *TCP*, *UDP*, dan *ICMP*.

Top 15 Signatures

Signature Name	Percentage	Event Count
http_inspect: LONG HEADER	33.18%	13424
stream5: Reset outside window	29.03%	11745
http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP R...	13.27%	5368
stream5: Limit on number of overlapping TCP packets reached	10.02%	4055
stream5: Bad segment, overlap adjusted size less than/equal 0	4.41%	1784
ET P2P BitTorrent DHT nodes reply	2.56%	1036
stream5: TCP Small Segment Threshold Exceeded	2.28%	921
stream5: FIN number is greater than prior FIN	1.82%	737
ET SCAN Behavioral Unusual Port 445 traffic, Potential Scan or...	1.32%	535
stream5: TCP Timestamp is missing	0.9%	366
ET RBN Known Russian Business Network IP TCP (296)	0.26%	104
stream5: TCP window closed before receiving data	0.2%	80
ET CURRENT_EVENTS HTTP contacting a suspicious *.co.cc domain	0.15%	62
ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)	0.15%	62
http_inspect: NON-RFC DEFINED CHAR	0.15%	61
http_inspect: OVERSIZE REQUEST-URI DIRECTORY	0.1%	39
smtp: Attempted data header buffer overflow	0.06%	25
ET P2P BitTorrent DHT ping request	0.05%	24
stream5: Data sent on stream not accepting data	0.04%	18
stream5: TCP Timestamp is outside of PAWS window	0.04%	15

Gambar 4.15 Report Signature Name

Menunjukkan laporan jumlah aktifitas nama event teratas dalam *persentage* dan event count yang terdaftar dalam rule base (aturan snort yang telah terdefinisi berupa paket – paket data di dalam aplikasi snort, seperti contoh laporan tersebut berupa http_inspect:LONG HEADER dengan persentasi 33.18% dan jumlah event sebanyak 13424 paket data.

Top 10 Source Addresses

Source IP Address	Percentage	Event Count
192.168.40.5	78.57%	27089
192.168.40.7	7.97%	2747
174.122.138.170	1.89%	653
174.121.62.122	1.67%	577
209.90.137.220	1.39%	479
184.73.216.187	1.16%	399
184.73.160.184	1.13%	391
184.73.213.48	1.02%	350
173.194.49.81	0.79%	272
173.194.49.74	0.73%	251

Gambar 4.16 Report Source IP Address

Top 10 Destination Addresses

Destination IP Address	Percentage	Event Count
192.168.40.5	25.05%	8635
192.168.40.7	6.41%	2209
118.98.36.22	5.53%	1907
118.98.36.21	2.63%	906
184.73.160.184	2.05%	705
184.73.216.187	1.94%	667
184.73.213.48	1.88%	652
118.98.36.156	1.98%	641
118.98.36.32	1.76%	606
74.125.96.147	1.62%	559

Gambar 4.17 Report Destination IP Address

Pada Gambar 4.16 dan Gambar 4.17 menunjukkan laporan jumlah event 10 teratas alamat IP asal terhadap tujuan. Sebagai contoh client meminta layanan internet terhadap *host name* berupa IP tujuan 192.168.40.5 dengan perbandingan layanan sebanyak 25.05% dan total client melakukan transaksi layanan internet sebanyak 8635 paket data.

BAB V

PENUTUP

5.1. Kesimpulan

1. Setiap aliran paket data yang mengalir dari *router* yang akan menuju *mirror switch* dan *access point*, maka dari sinilah fungsi dari cara kerja sistem sensor monitoring pada komputer server yaitu mengcopi atau menggandakan paket data yang melalui *swith 3 com*.
2. Setiap paket data baru yang masuk pada sensor maka perubahan jumlah event pada sensor monitoring akan berubah atau *update* otomatis sesuai pengaturan pada admin, dan hasil laporan sensor monitoring bisa *digenerate* setiap waktu, per minggu ataupun per bulan berupa file dengan ekstensi dot PDF (.PDF).
3. Dalam klasifikasi sensor hanya terdapat 3 jenis kategori yaitu *high severity*, *medium severity*, dan *low severity*.
4. Semakin banyak data yang melewati sensor, maka mempengaruhi kinerja dari *server*, ditunjukkan dengan *loading web server* yang lama.

5.2. Saran

1. Untuk pengembangan selanjutnya disarankan untuk administrasi sebagai pengendali *server* bisa menindaklanjuti dan menangani sendiri dengan melakukan *bloking source* IP ataupun membatasi akses terhadap pelaku gangguan pada jaringan *nirkabel*, tidak hanya sebatas *wifi* saja, tetapi juga diharapkan bisa diterapkan di beberapa bentuk jaringan lainnya seperti LAN, MAN ataupun WAN, ataupun konfigurasi antar jaringan. Diperlukan juga penambahan *model security* lain yang lebih kompleks, supaya keamanan jaringan menjadi lebih baik.

DAFTAR PUSTAKA

OpenSource.telkomspeedy.com/wiki/index.php/snort. Diakses tanggal 06 Juli 2011.

http://jogjalinux.or.id/berita/arsip/2010/01/14/kustumisasi-konfigurasi-IDS-snort.
Diakses tanggal 06 Juli 2011.

Abraham NethanelSetawan Junior, Agus H, Alexander 2009 " *Perancangan dan Implementasi Intrusion Detection System pada Jaringan Nirkabel.* Diakses tanggal 06 Juli 2011.

SnortTMUsers Manual The Snort Project, 2006. Diakses tanggal 06 Juli 2011.

http://blog.snort.org/2011/02/ubuntu-1004-install-guide-for-snort.html.
Diakses tanggal 10 Juli 2011.

Puji Hartono, "*Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall*", Bandung, 2006. Diakses tanggal 10 Juli 2011.

http://belajarkomputersekarang.wordpress.com/2011/03/15/snort/. Diakses tangal 10 Juli 2011.

Ryan Russel, "Snort Intrusion 2.0 Intrusion Detection", Syngress, 2003. Diakses tanggal 13 Juli 2011.

Michael Rush, Angela Aurobaugh, Graham Clark, Becky Pinkard, Jake Babbin, "*Intrusion Prevention And Active Response deploying Network And Host IPS*", Syngress, 2005. Diakses tanggal 13 Juli 2011.

http://www.howtoforge.com/intrusion-detection-with-snort-mysql-apache2-on-ubuntu.
Diakses tanggal 19 Juli 2011.

Sourcefire, Inc, "*Snort User Manual*, www.snort.org, 2006. Diases tanggal 20 Juli 2011.

http://mauren.doscom.org/2011/04/instalasi-snort-linux-ubuntu.html. Diakses tanggal 25 Juli 2011.

http://blog.snort.org/2011/02/ubuntu-1004-install-guide-for-snort.html. Diakses tanggal 25 Juli 2011.

LAMPIRAN

Lampiran 1. Istilah Dalam Kamus IT

Port	Protokol	Servis
7	TCP	echo
9	TCP	discard
13	TCP	daytime
19	TCP	chargen
20	TCP	ftp-control
21	TCP	ftp-data
23	TCP	telnet
25	TCP	smtp
37	UDP	time
43	TCP	whois
53	TCP/UDP	dns
67	UDP	bootps
68	UDP	bootpc
69	UDP	tftp
70	TCP	gopher
79	TCP	finger
80	TCP	http
110	TCP	pop3
111	TCP	sunrpc
119	TCP	nntp
123	UDP	ntp
137	UDP	netbios-ns

Port	Protokol	Servis
138	UDP	netbios-dgm
139	TCP	netbios-ssn
143	TCP	imap
161	UDP	snmp
162	UDP	snmp-trap
179	TCP	bgp
443	TCP	https (http/ssl)
520	UDP	rip
1080	TCP	socks
33434	UDP	traceroute

LAMPIRAN

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

NAMA : IMAM IZZAT MUTTAQIN
NIM : 04.12.617
JURUSAN : Teknik Komputer dan Informatika S-1
JUDUL : **RANCANG BANGUN SENSOR MONITORING PADA JARINGAN WI-FI (HOTSPOT) DI W-P CAFE SUMBERSARI MALANG BERBASIS SNORT**

Dipertahankan dihadapan Tim Penguji Skripsi Jenjang Program Strata Satu (S-1)

Pada Hari : Sabtu
Tanggal : 13 Agustus 2011
Dengan Nilai : 78,45 (B+)

PANITIA UJIAN SKRIPSI

KETUA

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y.1018800189

SEKRETARIS

Dr. Aryuanto S, ST. MT
NIP.P.1030800417

ANGGOTA PENGUJI

PENGUJI I

M. Ibrahim Ashari, ST, MT
NIP.P. 1030100358

PENGUJI II

Ahmad Faisol, ST
NIP.P. 1031000431

INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
JURUSAN TEKNIK ELEKTRO S-1
Jl. Karanglo KM.2 Malang

FORMULIR PERBAIKAN SKRIPSI

Dalam pelaksanaan ujian skripsi jenjang Strata 1 Jurusan Teknik Elektro Konsentrasi Teknik Komputer dan Informatika, maka perlu adanya perbaikan skripsi untuk mahasiswa :

NAMA : IMAM IZZAT MUTTAQIN
NIM : 04.12.617
JURUSAN : Teknik Komputer dan Informatika S-1
JUDUL : **RANCANG BANGUN SENSOR MONITORING PADA JARINGAN WI-FI (HOTSPOT) DI W-P CAFE SUMBERSARI MALANG BERBASIS SNORT**

No	Penguji	Tanggal	Uraian	Paraf
1.	Penguji I	13 Agustus 2011	1. Tambahkan Keterangan Gambar dan Tabel.	
2.	Penguji II	13 Agustus 2011	1. Tambahkan Flowchart.	

Disetujui :

Dosen Penguji I

M. Ibrahim Ashari, ST, MT
NIP.P. 1030100358

Dosen Penguji II

Ahmad Faisol, ST
NIP.P. 1031000431

Mengetahui :

Dosen Pembimbing I

Joseph Dedy Irawan, ST, MT
NIP. 1974041620011002

Dosen Pembimbing II

Irmalia Suryani Faradisa, ST, MT
NIP.P. 1030100365

INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
JURUSAN TEKNIK ELEKTRO

Formulir Perbaikan Ujian Skripsi

Dalam pelaksanaan Ujian Skripsi Janjang Strata 1 Jurusan Teknik Elektro Konsentrasi T. Energi Listrik / T. Elektronika / T.Infokom, maka perlu adanya perbaikan skripsi untuk mahasiswa :

NAMA : Imam Izzat M.
N I M : 0412617
Perbaikan meliputi :

tambahkan keterangan pd gbr dan tabel

Malang, 12 agust 2011

(M. Ibrahim Ashari, ST, MT)

Institut Teknologi Nasional Malang
Fakultas Teknologi Industri
Jurusan Teknik Elektro S-1

LEMBAR PENGAJUAN JUDUL SKRIPSI
JURUSAN TEKNIK ELEKTRO S-1

Konsentrasi : Teknik Energi Listrik / Teknik Elektronika /Teknik Komputer & Informatika /Teknik Komputer / Teknik Telekomunikasi*)

1.	Nama Mahasiswa: IMAM IZZAT M			Nim: 04.12.617
2.	Waktu Pengajuan	Tanggal: 14	Bulan: 06	Tahun: 2011
3.	Spesifikasi Judul (berilah tanda silang)**) a. Sistem Tenaga Elektrik b. Energi & Konversi Energi c. Tegangan Tinggi & Pengukuran d. Sistem Kendali Industri e. Elektronika & Komponen (f) Elektronika Digital & Komputer g. Elektronika Komunikasi h. lainnya			
4.	Konsultasikan judul sesuai materi bidang ilmu kepada Dosen*) Dr. Aryanto, ST, MT	Ketua Jurusan Ir. Yusuf Ismail Nakhoda, MT NIP. Y. 1018800189		
5.	Judul yang diajukan mahasiswa:	RANCANG BANGUN APLIKASI BILLING PADA JARINGAN WIFI (HOTSPOT) DENGAN MENGGUNAKAN BORLAN DELPHI DI W-P KAFE SUMBER SARI MALANG		
6.	Perubahan judul yang disetujui Dosen sesuai materi bidang ilmu	Rancang Bangun Aplikasi Manajemen Jaringan Wifi pada Cafe W-P sumber Sari Malang		
7.	Catatan: Judul yg sebelumnya sudah ada dilakukan oleh mahasiswa lainnya (lulus 2009). Persetujuan Judul skripsi yang dikonsultasikan kepada Dosen materi bidang ilmu	Disetujui 1/7/ 2011 Dosen		

Perhatian:
1. Formulir pengajuan ini harap dikembalikan kepada jurusan paling lambat satu minggu setelah disetujui kelompok dosen keahlian dengan dilampirkan proposal skripsi beserta persyaratan skripsi sesuai form S-1
2. Keterangan: *) Coret yang tidak perlu
   **) dilingkari a, b, c, ... atau g sesuai bidang keahlian

Form S-2

INSTITUT TEKNOLOGI NASIONAL
JL. Raya Karanglo,Km 2
MALANG

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak / ~~Ibu~~, JOSEPH DEDY IRAWAN, ST, MT.
Dosen Institut Teknologi Nasional
Malang

Yang bertanda tangan di bawah ini :

Nama : IMAM IZZAT M
Nim : 04.18.417
Jurusan : Teknik Elektro S-1
Konsentrasi : Teknik Elektronika/Energi Listrik /Komputer & Informatika

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing Utama / Pendamping *), untuk penyusunan Skripsi dengan judul (Proposl terlampir) :

RANCANG BANGUN APLIKASI MANAJEMEN JARINGAN WIFI PADA CAFE W-P SUMBERSARI MALANG

Adapun tugas tersebut sebagai salah satu syarat untuk menempuh Ujian Akhir Sarjana Teknik.
Demikian permohonan kami dan atas kesediaan Bapak/Ibu kami ucapkan terima kasih.

Mengetahui
Ketua Jurusan T. Elektro S-1

Ir. Yusuf Ismail Nakhoda,MT
NIP. Y. 1018800189

Malang,

Hormat kami

IMAM IZZAT M

*) coret yang tidak perlu

Form S-3a

INSTITUT TEKNOLOGI NASIONAL
JL. Raya Karanglo,Km 2
MALANG

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. ~~Bapak~~ / Ibu, IRMALIA SURYANI FARADISA, ST, MT.
Dosen Institut Teknologi Nasional
Malang

Yang bertanda tangan di bawah ini :

Nama	: IMAM IZZAT M
Niin	: 04.12.617
Jurusan	: Teknik Elektro S-1
Konsentrasi	: Teknik Elektronika/Energi Listrik /Komputer & Informatika

Dengan ini mengajukan permohonan, kiranya Bapak/Ibu bersedia menjadi Dosen Pembimbing Utama / Pendamping *), untuk penyusunan Skripsi dengan judul (Proposl terlampir) :

RANCANG BANGUN APLIKASI MANAJEMEN JARINGAN WIFI PADA CAFE W-P SUMBERSARI MALANG.

Adapun tugas tersebut sebagai salah satu syarat untuk menempuh Ujian Akhir Sarjana Teknik.
Demikian permohonan kami dan atas kesediaan Bapak/Ibu kami ucapkan terima kasih.

Mengetahui
Ketua Jurusan T. Elektro S-1

Ir. Yusuf Ismail Nakhoda,MT
NIP. Y. 1018800189

Malang,

Hormat kami

IMAM IZZAT M

*) coret yang tidak perlu

Form S-3a

INSTITUT TEKNOLOGI NASIONAL
JL. BENDUNGAN SIGURA-GURA 2
MALANG

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai permohonan dari mahasiswa/i :

Nama : IMAM IZZAT M

Nim : 04 12 617

Semester : 14

Jurusan : Teknik Elektro S-1

Konsentrasi : Teknik Elektronika/Teknik Energi Listrik/Komputer & Informatika

Dengan ini menyatakan bersedia/~~tidak bersedia~~ *) membimbing skripsi dari mahasiswa tersebut, dengan judul :

RANCANG BANGUN APLIKASI MANAJEMEN JARINGAN WIFI PADA CAFE W-P SUMBERSARI MALANG

Demikian surat pernyataan ini kami buat agar dapat digunakan seperlunya.

Malang,

Hormat kami

NIP.

Catatan:
Setelah disetujui agar formulir ini
Diserahkan mahasiswa/I yang bersangkutan
Kepada jurusan untuk diproses lebih lanjut
*) Coret yang tidak perlu

Form S-3b

INSTITUT TEKNOLOGI NASIONAL
JL. BENDUNGAN SIGURA-GURA 2
MALANG

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai permohonan dari mahasiswa/i :

Nama : IMAM IZZAT M

Nim : 0412617

Semester : 14

Jurusan : Teknik Elektro S-1

Konsentrasi : Teknik Elektronika/Teknik Energi Listrik/Komputer & Informatika

Dengan ini menyatakan bersedia/tidak bersedia *) membimbing skripsi dari mahasiswa tersebut, dengan judul :

RANCANG BANGUN APLIKASI MANAJEMEN JARINGAN WIFI PADA CAFE W-P SUMBERSARI MALANG

Demikian surat pernyataan ini kami buat agar dapat digunakan seperlunya.

Malang,

Hormat kami

NIP.

Catatan:
Setelah disetujui agar formulir ini
Diserahkan mahasiswa/I yang bersangkutan
Kepada jurusan untuk diproses lebih lanjut
*) Coret yang tidak perlu

Form S-3b

INSTITUT TEKNOLOGI NASIONAL
Jl. Bendungan Sigura – gura No.2
MALANG

FORMULIR BIMBINGAN SKRIPSI

Nama : Imam Izzat M.
Nim : 04.12.617
Masa Bimbingan : 09 Juli 2011 s/d 09 Desember 2011
Judul Skripsi : Rancang bangun sensor monitoring pada jaringan wi-fi (Hotspot) di W-P Cafe Sumber Sari Malang Berbasis Snort

No	Tanggal	Uraian	Paraf Pembimbing
1	15-07-2011	Konsultasi bab I, II, III	
2	20-07-2011	Bimbingan bab I, II, III	
3	25-07-2011	Konsultasi bab I, II, III, IV	
4	26-07-2011	Bimbingan bab I, II, III, IV	
5		ACC SEMINAR	
6		ACC LAMPIRAN	
7			
8			
9			
10			

Malang, Juli 2011
Dosen pembimbing I

Joseph Dedy Irawan, ST, MT
NIP.Y. 1974041620011002

Form S-4b

INSTITUT TEKNOLOGI NASIONAL
Jl. Bendungan Sigura – gura No.2
MALANG

FORMULIR BIMBINGAN SKRIPSI

Nama : Imam Izzat M.
Nim : 04.12.617
Masa Bimbingan : 09 Juli 2011 s/d 09 Desember 2011
Judul Skripsi : Rancang bangun sensor monitoring pada jaringan wi-fi (Hotspot) di W-P Cafe Sumber Sari Malang Berbasis Snort

No	Tanggal	Uraian	Paraf Pembimbing
1	13-07-2011	Konsultasi bab I, II, III	
2	19-07-2011	Bimbingan bab I, II, III - Revisi	
3	29-07-2011	Konsultasi bab I, II, III, IV	
4			
5			
6			
7			
8			
9			
10			

Malang,

Dosen pembimbing II

Irmalia Suryani Faradisa, ST, MT.
NIP.P.1030100365

Form S-4b