KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

SKRIPSI

DESAIN DAN IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) UNTUK PENGAMANAN JARINGAN KOMPUTER LOKAL PADA YAYASAN IBA PALEMBANG

Oleh :

SASTRO WIJAYA

012090270

Untuk Memenuhi Sebagian dari Syarat-Syarat

Guna Mencapai Gelar Sarjana Komputer

PALEMBANG

2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

SKRIPSI

DESAIN DAN IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) UNTUK PENGAMANAN JARINGAN KOMPUTER LOKAL PADA YAYASAN IBA PALEMBANG

Oleh :

SASTRO WIJAYA

012090270

Untuk Memenuhi Sebagian dari Syarat-Syarat

Guna Mencapai Gelar Sarjana Komputer

PALEMBANG

2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PEMBIMBING

NAMA	**: Sastro Wijaya**
NOMOR POKOK	**: 012090270**
PROGRAM STUDI	**: Teknik Informatika**
JENJANG PENDIDIKAN	**: Strata Satu (SI)**
KONSENTRASI	**: Jaringan**
JUDUL LAPORAN	**: Desain dan Implementasi *Intrusion Detection System* (IDS) untuk Pengamanan Jaringan Komputer Lokal pada Yayasan IBA Palembang**

Tanggal : 17 September 2012 **Mengetahui,**

Pembimbing : **Ketua,**

Pria Winardi, S.T.
NIDN : 0203077902

Rudi Sutomo, S.Kom., M.Si.
NIP : 028.PCT.08

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PENGUJI

NAMA	**: Sastro Wijaya**
NOMOR POKOK	**: 012090270**
PROGRAM STUDI	**: Teknik Informatika**
JENJANG PENDIDIKAN	**: Strata Satu (SI)**
KONSENTRASI	**: Jaringan**
JUDUL LAPORAN	**: Desain dan Implementasi *Intrusion Detection System* (IDS) untuk Pengamanan Jaringan Komputer Lokal pada Yayasan IBA Palembang**

Tanggal : 17 September 2012	**Tanggal : 17 September 2012**
Penguji 1 :	**Penguji II :**
Rudi Sutomo, S.Kom., M.Si	**Molavi Arman, S.Kom.**
NIDN : 0222057501	**NIDN: 0205058003**

Menyetujui,

Ketua,

Rudi Sutomo, S.Kom., M.Si.
NIP : 028.PCT.08

MOTTO DAN PERSEMBAHAN

MOTTO

Kamu tak bisa kembali ke masa lalu dan mengubah sebuah awal yang buruk, namun kamu bisa membuat akhir yang indah, mulai saat ini.

Jangan pernah katakan umurlah telah bertambah, tapi katakanlah umur mu selalu berkurang karena dosa lah yang selalu bertambah

PERSEMBAHAN

1. Allah Subhanahu Wata'ala
2. Orang tua saya
3. Kakak, ayuk, keluarga saya
4. Teman-teman seperjuangan
5. Almamaterku

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa yang telah memberikan rahmat dan hidayah-Nya kepada penulis, sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan baik dan tepat pada waktunya.

Penulisan skripsi ini merupakan untuk memenuhi sebagian dari syarat-syarat guna menyelesaikan program strata satu, STMIK Palcomtech Palembang. Skripsi ini berjudul "**Desain dan Implementasi *Intrusion detection system* (IDS) untuk pengamanan jaringan komputer lokal pada Yayasan IBA Palembang ".**

Dalam Penulisan skripsi ini Penulis menyadari sepenuhnya bahwa Penulis telah banyak mendapat bantuan untuk menyelesaikan skripsi ini dari berbagai pihak, baik dari pihak Akademik, Keluarga, maupun Sahabat-sahabat seperjuangan. Oleh karena itu, penulis ucapkan rasa terima kasih yang tulus serta do'a dan harapan agar semua bantuan yang telah diberikan kepada penulis dapat bermanfaat bagi kita semua dan diberkahi Tuhan Yang Maha Esa.

Ucapan terima kasih yang tulus juga ditujukan kepada pihak Pembimbing yang telah membantu dan membimbing penulis dalam menyusun skripsi ini, semoga skripsi ini bermanfaat bagi semua pihak yang menggunakannya.

Palembang, 17 September 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL i

HALAMAN PERSETUJUAN PEMBIMBING ii

HALAMAN PENGESAHAN PENGUJI iii

HALAMAN MOTTO DAN PERSEMBAHAN iv

HALAMAN KATA PENGANTAR..... v

HALAMAN DAFTAR ISI..... vi

HALAMAN DAFTAR GAMBAR..... x

HALAMAN DAFTAR TABEL xiii

ABSTRAK xiv

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Perumusan Masalah 3

1.3 Batasan Masalah..... 3

1.4 Tujuan Penelitian 3

1.5 Manfaat Penelitian 4

1.6 Sistematika Penulisan 5

BAB II GAMBARAN UMUM PERUSAHAAN

2.1 Profil Perusahaan 7

2.1.1 Sejarah Perusahaan 7

2.1.2 Visi dan Misi 8

2.2 Struktur Organisasi 10

2.3 Tugas wewenang 12

BAB III TINJAUAN PUSTAKA

3.1 Landasan Teori 14

3.1.1 Jaringan Komputer 14

3.1.2 Jangkauan Area Jaringan 14

3.1.3 Topologi Jaringan 18

3.1.4 Model Osi..... 23

3.1.5 Media Transmisi Komputer 27

3.1.6 Protokol Jaringan 30

3.1.7 Open Source 37

3.1.8 Linux 37

3.1.9 Debian 38

3.1.10 Server 38

3.1.11 Http..... 39

3.1.12 Mysql 40

3.1.13 *Intrusion Detection System (IDS)* 41

3.1.14 *Intrusion Prevention System (IPS)*..... 43

3.1.15 Suricata 46

3.1.16 *Basic Analysis and Security Engine (BASE)*..... 47

3.1.17 *Iptables*..... 50

3.2 Hasil Penelitian Terdahulu..... 51

BAB IV METODE PENELITIAN

4.1 Lokasi dan Waktu Penelitian 55

4.1.1 Lokasi 55

4.1.2 Waktu Penelitian 55

4.2 Jenis Data 55

4.2.1 Data Primer 55

4.2.2 Data Skunder 56

4.3 Teknik Pengumpulan Data 56

4.4 Jenis Penelitian 57

4.4.1 Penelitian Terapan..... 57

4.5 Teknik Pengembangan Sistem 58

BAB V HASIL DAN PEMBAHASAN

5.1 Analisa 63

5.2 Desain..... 64

5.3 *Simulation Prototype*..... 65

5.4 Implementasi..... 66

5.4.1 Instalasi server..... 68

5.4.2 Konfigurasi IP Address..... 68

5.4.3 Instalasi dan Konfigurasi DNS 70

5.4.4 Instalasi perangkat tambahan Suricata..... 74

5.4.5 Instalasi dan konfigurasi Suricata beserta IDS 75

5.4.6 Instalasi BASE dan Adodb 81

5.4.7 Konfigurasi awal sebelum malakukan serangan..... 87

5.4.8 Proses yang akan dilakukan penyerangan..... 88

5.4.9 keluaran/hasil yang didapat 89

5.4.10 Pengujian Serangan 89

5.4.11 Tindakan Pencegahan 93

5.5 Monitoring 95

5.6 Management 95

BAB VI PENUTUP

6.1 Simpulan 97

6.2 Saran 97

DAFTAR PUSTAKA 99

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1 Bagan Organisasi Perusahaan 11

Gambar 3.1 Topologi Bus 18

Gambar 3.2 Topologi Token *RING*..... 19

Gambar 3.3 Topologi *STAR* 20

Gambar 3.4 Topologi *tree* 21

Gambar 3.5 Topologi *Mash* *22*

Gambar 3.6 Model OSI 24

Gambar 3.7 Kabel *Unshielded Twisted Pair* 28

Gambar 3.8 Kabel *Shillded Twisted Pair*..... 29

Gambar 3.9 Kabel *Koaksial* 30

Gambar 3.10 Kabel *Fiber Optik*..... 31

Gambar 3.11 Aliran Paket Data 50

Gambar 4.1 NDLC 57

Gambar 5.1 Topologi Jaringan Yayasan IBA Palembang 64

Gambar 5.2 Topologi Jaringan komputer yang akan diimplementasi ... 65

Gambar 5.4 Konfigurasi IP address 68

Gambar 5.5 file */etc/network/interface* 68

Gambar 5.6 Perintah *restart* kartu jaringan 69

Gambar 5.7 file *Ifconfig* 69

Gambar 5.8 Tes Ping Client 70

Gambar 5.9 Konfigurasi *file /etc/bind/named.conf.local* 70

Gambar 5.10 *Named.conf.local* 71

Gambar 5.11 *cp db.local db.iba.com*a 71

Gambar 5.12 *cp db.127 db.202.45.67* 71

Gambar 5.13 perintah */bind/db.iba.com* 72

Gambar 5.14 file *bind /db.iba.com*..... 72

Gambar 5.15 perintah */bind/db.202.45.67* 72

Gambar 5.16 *file bind/db.202.45.67*..... 73

Gambar 5.17 *restart* aplikasi *bind9*..... 73

Gambar 5.18 *nslookup suricata.iba.com*..... 74

Gambar 5.19 *nslookup* 202.45.67.9 74

Gambar 5.20 *install* Perangkat tambahan 75

Gambar 5.21 *Install suricata dan IDS* 75

Gambar 5.22 *copy suricata rule*..... 76

Gambar 5.23 *Rule-rule Suricata dan Snort* 78

Gambar 5.24 *instalasi libpcap dan barnyard2* 79

Gambar 5.25 membuat *database Suricata* 79

Gambar 5.26 i*mpor table database*..... 79

Gambar 5.27 Menampilkan *Databases*..... 80

Gambar 5.28 *ekstarak file Base dan Adodb* dan install LAMP 81

Gambar 5.29 *Install all mail* 82

Gambar 5.30 konfigurasi file apache2/php.ini..... 82

Gambar 5.31 Mengubah hak akses *Base*..... 83

Gambar 5.32 *Settings BASE step* awal 83

Gambar 5.33 *Settings* BASE *step* 1..... 84

Gambar 5.34 *Settings BASE step 2* 84

Gambar 5.35 *Setting* BASE *step 3* 85

Gambar 5.36 *Settings BASE Create BASE AG* 85

Gambar 5.37 *Settings BASE step 4* 86

Gambar 5.38 Halaman awal pada saat *login* 86

Gambar 5.39 Penghilangan hak akses Base 86

Gambar 5.40 Hasil konfigurasi Suricata dan BASE 87

Gambar 5.41 *Port Scaner* 90

Gambar 5.42 Tampilan BASE setalah dilakukan *Port Scaning* 90

Gambar 5.43 klasifikasi serangan setelah dilakukan *Port Scaning* 91

Gambar 5.44 Percobaan *Ping Of Death* 92

Gambar 5.45 Tampilan *Home* pada BASE 92

Gambar 5.46 Menjalankan IpTableas 93

Gambar 5.47 Percobaan *Port scanner* yang gagal 94

Gambar 5.48 *Ping Attack* yang gagal 94

Gambar 5.49 Monotoring 95

DAFTAR TABEL

Table 3.1 Perbandingan Antar Topologi Jaringan 23

Table 3.2 Pembagian Kelas Ip 33

Table 3.3 Subnet Mask Kelas Ip 36

Table 3.4 Hasil Penelitian Pertama 50

Table 3.5 Hasil Penelitian Kedua 52

ABSTRAK

DESAIN DAN IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) UNTUK PENGAMANAN JARINGAN KOMPUTER LOKAL PADA YAYASAN IBA PALEMBANG

Laporan skripsi ini penulis selesaikan dengan tujuan meninjak lanjuti dari masalah-masalah yang dihadapi selama melakukan riset, di Yayasan IBA Palembang ini belum ada nya keamanan jaringan lokal yang lebih optimal, oleh karena itu penulis memberikan solusi dari masalah tersebut dengan membuat keamanan jaringan lokal yang lebih optimal, yang penulis kembangkan adalah dengan memberikan layanan kemananan jaringan lokal sehinga server lebih mudah di dilihat kalau adanya penyusupan dari luar sehinga permasalhan dari yaysan sedikit demi saedikit terkendali..

Penulis mengumpulkan data guna menyelesaikan skripsi ini dengan menggunakan teknik pengamatan dan wawancara, teknik ini bertujuan agar apa yang diperoleh penulis selama melakukan riset tidak melenceng dari keadaan perusahaan. Oleh karena itu penulis mengamati jaringan lokal perusahaan ini dan melakukan wawancara untuk menemukan apa kekurangan dari sistem yang sedang berjalan pada Yayasan ini sehingga penulis bisa menyimpulkan dan membantu memecahkan masalah perusahaan ini agar sistem kerja lebih optimal.

Apa yang dibangun atau dikembangkan pada jaringan Yayasan ini semoga bermanfaat dan berguna bagi kelangsungan sistem kerja Yayasan ini, sehingga penulis merasa bangga telah membantu sistem kerja Yayasan ini lebih optimal.

Kata kunci : Lokal, Suricata,Base.

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Di era yang moderen pada saat ini keamanan jaringan komputer memang faktor yang sangat penting untuk diperhatikan saat ini. Jika pada zaman terdahulunya kemanan jaringan masih ditempatkan pada urutan prioritas yang rendah, namun pada saat sekarang perilaku tersebut harus segera di atasi. Hal ini disebabkan, kejahatan dengan menggunakan bantuan komputer, media komunikasi, dan perangkat elektronik lainnya meningkat sangat tajam. Dalam hal ini sangat kontras perkembangan kebutuhan perangkat komputer untuk kehidupan sehari-hari yang juga semakin meninggi, tidak hanya di dalam kegiatan perkuliahan saja, kehidupan rumah tangga pun sudah perlu dilengkapi dengan sebuah komputer. Keamanan jaringan sendiri sudah seharusnya menjadi hal yang sangat diperhatikan seperti mengontrol siapa yang mengakses *resources* jaringan, pengontrolan akses ini juga harus mengatur bagaimana subjek yang berupa *user, program, file,* komputer dan lainnya berinteraksi dengan objek-objek berupa sebuah *file, database,* komputer dan lainnya atau lebih tepatnya infrastruktur jaringan.

Oleh karena itulah, mengapa keamanan jaringan komputer menjadi begitu penting untuk diperhatikan saat ini. Apalagi jika kebutuhannya sudah berhubungan dengan kegiatan perkuliyahan, dan kegiatan perkuliyahan tersebut sangat banyak berhubungan dengan server yang diakases oleh *user*.

Server yayasan IBA sekarang masi tergolong kurang aman akibat nya server tersebut banyak mengalami kendala seperti sering terjadinya penyusupan, dan menyebabkan server mengalami lamban dalam memproses user yang masuk kedalam server dan juga sering terjadinya server tersebut mati dengan sendirinya.

Tindakan pencegahan yang harus dilakukan penulis agar hal tersebut tidak terjadi maka diperlukan suatu pengamanan jaringan komputer dengan melakukan deteksi terhadap suatu jaringan dan melakukan suatu tindakan terhadap jenis serangan yang ditemukan agar masalah-masalah seperti penyusupan data, perusakan data dan hal-hal yang mengenai kemanan jaringan yang dihadapi dapat diatasi dengan mudah.

Dengan adanya kemungkinan masalah-masalah mengenai keamanan jaringan rasanya cukup penting untuk menerapkan suatu teknologi yang mampu melakukan deteksi terhadap serangan pada jaringan dan melakukan tindakan terhadap serangan tersebut. Semua proses ini bisa dilakukan dengan mengandalkan sebuah teknologi khusus yang disebut dengan istilah *Intrution Detection System (IDS)* dimana teknologi ini merupakan gabungan dari sistem *Intrution Prevention System (IPS)* dengan sistem *firewall.*

Oleh karena itu penulis tertarik mengambil judul "*Desain* dan *Implementasi Intrusion detection system (IDS)* untuk pengamanan jaringan komputer lokal pada Yayasan IBA Palembang"

1.2 Perumusan Masalah

Didalam melakukan penelitian penulis menyimpulkan 2 (dua) rumusan masalah yaitu :

1. Bagaimana desain dan implementasi *Intrusion Detection System (IDS)* pada jaringan komputer lokal Yayasan IBA Palembang?
2. Apakah penggunaan *tools IDS suricata.* yang merupakan pengembangan dari *tools IDS snort* pada jaringan Komputer Yayasan IBA Palembang dapat mencegah dan mendeteksi serangan ?

1.3 Batasan Masalah

Dalam penulisan laporan ini penulis membatasi permasalahan agar penelitian ini tidak menyimpang serta tidak terlalu luas, yakni mencakup desain arsitektur jaringan dan penerepan *tools IDS suricata,* yang dijalankan pada sistem operasi debian sebagai *Intrusion Detection System (IDS)* dan tindakan pencegahan serangan yang dimaksud disini adalah tindakan pencegahan awal yang dilakukan dengan berdasarkan data-data yang dihasilkan oleh *tools IDS BASE.*

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

1. Mendesain dan mengimplementasi *Intrusion Detection System (IDS).* Guna untuk meningkatkan kinerja dan keamanan jaringan Komputer *local* pada Yayasan IBA Palembang.

2. Untuk mengetahui apakah *tools IDS suricata*. Pada jaringan Komputer local pada Yayasan IBA Palembang dapat mencegah dan mendeteksi serangan.

1.5 Manfaat Penelitian

1.5.1 Manfat Penelitian

1. Bagi Penulis

   Penelitian ini diharapkan dapat menambah ilmu pengetahuan serta dapat menerapkan dan mengembangkan ilmu yang didapat selama menjadi mahasiswa di STMIK PalComTech Palembang, khususnya pada mata kuliah Praktek Jaringan Komputer.

2. Bagi Perusahaan Yayasan IBA Palembang Agar dapat meningkatan keamanan jaringan komputer lokal terhadap penggunaan dan memantau lalu lintas jaringan dengan menerapkan *tools IDS suricata.*

3. Bagi Akademik

   Sebagai referensi bagi penulis lainnya untuk dijadikan sebagai bahan perbandingan dalam menyusun penelitian di masa yang akan datang dan memjadi bahan bacaan pada umunya dan khususnya bagi mahasiswa palcomtech palembang.

1.6 Sistem Penelitian

Sistematika penulisan skripsi ini dibagi menjadi 6 bab yang diuraikan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, dan sistematika penulisan.

BAB II GAMBARAN UMUM PERUSAHAAN

Bab ini akan menjelaskan tentang gambaran umum yayasan seperti frofil yayasan, sejarah yayasan, visi dan misi yayasan, struktur organisasi yayasan dan tugas wewenang yayasan.

BAB III TINJAUAN PUSTAKA

Bab ini akan menjelaskan teori-teori pendukung yang nantinya digunakan dalam pembuatan sebuah *intrution detection system(IDS)* yang akan dibuat, seperti landasan teori dan pengertian-pengertian yang dibutuhkan.

BAB IV METODE PENELITIAN

Bab ini menguraikan tentang lokasi dan waktu penelitian, jenis data, teknik pengumpulan data dan jenis penelitian.

BAB V ANALISA DAN PEMBAHASAN

Bab ini menguraikan tentang hasil yang telah dicapai dan pembahasan meliputi tentang cara instalasi dan konfigurasi suricata, instalasi dan konfigurasi *Blockit*, serta konfigurasi *iptables* di sistem operasi debian sebagai *server.*

BAB VI SIMPULAN DAN SARAN

Bab ini penulis menguraikan beberapa simpulan dari pembahasan masalah dari bab-bab sebelimnya serta memberikan saran yang bermanfaat bagi Yayasan IBA Palembang.

BAB II

GAMBARAN UMUM YAYASAN

2.1 Profil Yayasan

2.1.1 Sejarah Yayasan

Kesempatan memperoleh pendidikan, sebelum revolusi dan pada awal kemerdekaan, sangatlah terbatas. Banyak anak-anak yang tidak dapat sekolah. Keprihatinan ini membangkitkan kehendak Almarhum Bapak Bajumi Wahab, yang didukung isterinya yaitu almarhum Ibu Sajidah, untuk menyelenggarakan pendidikan bagi masyarakat. Sehingga ada generasi penerus yang mampu menciptakan dan membangun dunia usaha. Gedung Yayasan IBA sebuah gedung yang cukup tua di Palembang didirikan oleh H. Bajumi Wahab dan mendapat dukungan dari istrinya. Selaku donatur tunggal, H. Bajumi Wahab mendirikan yayasan yang namanya merupakan kesatuan dari nama Ida dan Bajumi sendiri, yaitu Yayasan IBA sebagai langkah kongkrit dalam menumbuhkan pendidikan agar dapat dicapai masyarakat luas, yang untuk pertama kalinya dibantu oleh dr. M. Isa (Alm.), Nasaruddin Nuch (Alm.) serta Dentjik Wahab (Alm.). Yayasan ini didirikan pada tanggal 01 September 1959 disahkan dengan Akte Notaris Tan Thong Kie Nomor 48 tambahan Nomor 61 tanggal 29 Juli 1960 serta dimuat dalam lebaran Negara Nomor 60 tahun 1960. Bangunan ini dirancang oleh arsitek

lulusan Amerika, Oen Poo Haw. Gedung tersebut diresmikan pemakaiannya oleh Nyonya H. Bajumi Wahab pada tanggal 06 Nopember 1960.

Sampai dengan saat ini dengan areal seluas 12.5 hektar di pusat kota Palembang tepatnya di jalan Mayor Ruslan Palembang, maka lembaga pendidikan IBA merupakan Lembaga Pendidikan swasta terluas di kota Palembang. Saat ini Yayasan Pendidikan IBA mengelola pendidikan:

- Taman Kanak - Kanak IBA
- Sekolah Dasar IBA
- Sekolah Menengah Pertama IBA
- Sekolah Menengah Atas IBA
- Universitas IBA

2.1.2 Visi dan MISI

b.Visi

Sebagai Pusat Unggulan (Center of Excellence) dalam Pengembangan Ilmu Pengetahuan, Teknologi dan Seni, serta Sumber Daya Manusia berdasarkan Nilai-nilai Religius dan Kebangsaan guna memenuhi tuntutan zaman serta dapat memberi arah perubahan khususnya di Sumatera Selatan.

b.Misi

Memajukan Ilmu Pengetahuan, Teknologi, dan Seni berdasarkan Nilai-nilai Religius dan Kebangsaan guna memenuhi

tuntutan zaman dalam rangka membangun masyarakat Indonesia, khususnya masyarakat Sumatera Selatan.

Mengembangkan Sumber Daya Manusia berdasarkan Nilai-nilai Religius dan Kebangsaan yang merupakan tuntutan zaman serta memberi arah perubahan dalam rangka membangun masyarakat Indonesia sebagai masyarakat yang sejahtera, makmur dan adil.

Melakukan penelitian dan pengabdian kepada masyarakat berdasarkan Nilai-nilai Religius dan Kebangsaan yang merupakan tuntutan zaman serta memberi arah perubahan dalam rangka membangun masyarakat Indonesia sebagai masyarakat yang sejahtera, makmur dan adil.

Menjalin kerjasama dan mengembangkan jaringan kerjasama dengan berbagai pihak, baik swasta maupun pemerintah di tingkat lokal/regional maupun nasional untuk memperkuat daya saing lembaga.

Kampus Universitas IBA (UIBA), jalan Mayor Ruslan, terletak ditengah kota Palembang. Dilalui rute kenderaan angkutan umum dan tidak jauh dari rute bus Trans Musi.

Kampus UIBA berada dalam lahan seluas 12 hektar, milik Yayasan IBA, terdiri dari gedung berlantai 3 yang dipergunakan oleh Fakultas Ekonomi dan Fakultas Hukum. Dua gedung terpisah berlantai 3, ditempati masing-masing oleh Fakultas Teknik dan

Fakultas Pertanian. Ditambah gedung berlantai 3 lainnya untuk kantor rektorat dan perpustakaan.

Berdampingan dengan gedung tersebut diatas, terdapat lapangan sepak bola, dua lapangan bola basket, lapangan upacara dan areal terbuka hijau.

2.2 Stuktur Organisasi

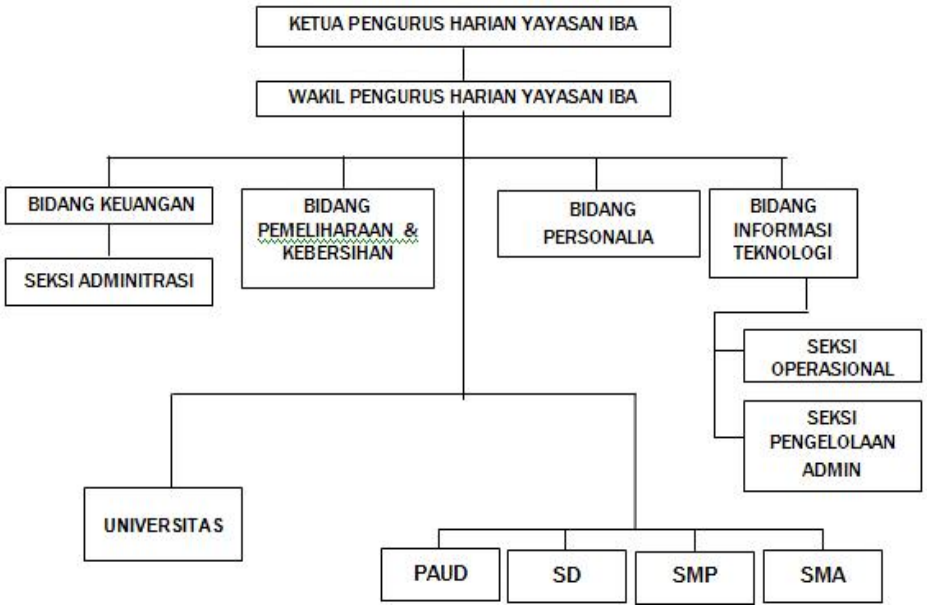
2.2.1 Bagian/Unit Kerja

Organisasi akan dapat mencapai tujuannya apabila orang didalamnya melakukan kerjasama yang baik, dimana kerjasama hanya dapat terjadi apabila hubungan diantara orang yang satu dengan yang lainnya dapat berjalan sebagaimana mestinya. Hubungan orang yang satu dengan yang lainnya akan semakin lancar ditentukan oleh struktur organisasi sekolah yang jelas, serta wewenang dan tanggung jawab masing-masing bagian. Setiap anggota organisasi akan mengetahui dari mana ia menerima perintah dan kepada siapa ia harus melapor. Dengan demikian berarti pula bahwa struktur organisasi merupakan bentuk komunikasi antara anggota-anggota organisasi itu.

Dalam perkembangan semakin maju dan semakin besar suatu sekolah, maka persoalan mengenai organisasi semakin banyak dan rumit. Organisasi dibutuhkan karena adanya suatu kerjasama yang baik dalam melaksanakan aktivitas di perusahaan. Suatu organisasi

untuk mencapai target yang diinginkan perlu membentuk suatu badan organisasi yang disesuaikan dengan tugas dan tanggung jawab masing-masing jawaban. Hal ini bertujuan agar tindakan yang dilakukan serta cara pengaturannya memang berdasarkan atas kewajiban karena tugas yang dibebankan oleh seorang pimpinan kepada bawahan. Struktur organisasi ini sangat erat hubungannya dengan tindakan yang dilakukan. Berikut adalah struktur organisasi pada Yayasan IBA Palembang.

Struktur Organisasi Yayasan IBA Palembang



(Sumber: Yayasan IBA Palembang)

Gambar 2.1 Bagan Struktur Organisasi

2.3 Tugas Wewenang

Berikut ini adalah pembagian tugas dari struktur organisasi pada Yayasan IBA Palembang.

a. Ketua Pegurus Harian Yayasan IBA

Mengangkat dan memberhentikan pelaksana kegiatan Yayasan, yaitu semua pegawai pelaksana di lingkungan Sekretariat Yayasan maupun di lingkungan kampus Universitas Yayasan IBA Palembang, serta Memahami dan menjabarkan dalam bentuk kegiatan kebijaksanaan yang berkaitan dengan Yayasan.

b. Wakil Pegurus Harian Yayasan IBA

Mewakili atau membantu Ketua Yayasan apabila Ketua Yayasan berhalangan sesuai dengan kebijaksanaan yang telah ditetapkan oleh Pengurus Yayasan. Serta melaksanakan dan mengkoordinasikan pelaksanaan tugas-tugas sesuai dengan bidang/urusan yang ditugaskan oleh Ketua Yayasan.

c. Bidang Pemeliharaan & Kebersihan

Melaksanakan sebagian tugas yang meliputi pengelolaan kebersihan, pembangunan, pemeliharaan, instalasi listrik dan air dalam lingkungan Yayasan IBA Palembang.

d. Bidang Keuangan

Bagian yang menjalankan fungsi akuntansi yang bertanggung jawab mencatat transaksi keuangan dan menyusun laporan keuangan.

e. Bidang Personalia

Bidang yang berhubungan dengan tenaga kerja, seperti penempatan, penggajian, pelatihan, pendidikan, mutasi dan promosi, kompensasi dan pemberhentian langsung menjadi tanggung jawab personalia.

f. Bidang Informasi Teknologi

Melakukan kegiatan yang berhubungan dengan dunia IT, seperti mengatur dan mengawasi jaringan komunikasi yang ada pada kawasan Yayasan IBA Palembng. Serta seorang IT memperbaiki segala kerusakan IT yang ada pada Yayasan IBA Palembang.

g. Seksi Administrasi

1. Mencatat dan bertanggung jawab terhadap laporan keluar masuknya uang.
2. Melayani dan membuat nota transaksi pembayaran yang dilengkapi dengan nota-nota pembayaran berdasarkan transaksi.
3. Menyusun nota dan faktur sebagai arsip administrasi.

h. Seksi Operasional

Melayani segala kebutuhan akdemik dan non akedemik pada Yayasan IBA Palembang

i. Seksi penglolahan Admin

Menyediakan informasi untuk masyarakat melalui internet, mengembangkan jasa inpormasi dan jaringan komunikasi sesuai kebutuhan parah penguna.

BAB III

TINJAUAN PUSTAKA

3.1 Landasan Teori

3.1.1 Jaringan Komputer

Menurut Sofana (2011:4) jaringan komputer (*computer network*) adalah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada *printer* yang sama dan bersama-sama menggunakan *hardware*/*software* yang terhubung dengan jaringan.

3.1.2 Jangkauan Area Jaringan

Menurut Sufriyanto (2005:300), berdasarkan luas wilayahnya atau letak geografisnya, jaringan komputer dibedakan menjadi:

a. Local Area Network (LAN)

Lan menggambarkan suatu jaringan yang menjangkau area yang terbatas, miasalnya suatu kantor atau gedung, di mana komputer yang mempunyai jaringan secara fisik berdekatan suatu lainnya. LAN yang besar misalnya pada kantor ataupun perusahaan yang kompleks, dapat dipisahkan menjadi beberapa *workgroup* untuk memudahkan

manajemennya. Dalam hal ini, suatu *workgroup* terdiri dari *user* yangmelakukan *share resource* yang sama,seperti file, printer, dan program aplikasi. Jarak maksimum yang di jangkau LAN kurang lebih 10 km.

Keuntungan jaringan LAN adalah:

- Pertukaran file dapat dilakukan dengan mudah (*file sharing*).
- Pemakain printer dapat dilakukan oleh semua klien (*printer sharing*).
- File-file data dapat disimpan pada server, sehinga data dapat diakses dari semua klien menurut otoriasi sekuritas dari semua karyawan, yang dapat dibuat berdasarkan struktur organisasi perusahaan sehinga keamanan data terjamin.
- File data yang keluar atau masuk dari atau ke server dapat dikendalikan.
- Proses *back up* data dapat lebih mudah dan cepat.
- Risiko kehilangan data oelh virus komputer menjadi sangat kecil.
- Komunikasi antar karyawan dapat dilakukan dengan mengunakan *e-mail* dan *chat*.

b. *Metropolitan Area Network* (MAN)

MAN merupakan jaringan dengan area lebih luas dari LAN, yang bisa terdiri dua atau lebih LAN yang dihubungkan bersama-sama dalam batas-batas kira-kira suatu kawasan metropolitan atau satu kota. MAN bertipikal *publik* dengan kinerja tinggi. Istila MAN lebih jarang digunakan untuk mendefinisikan jaringan dari pada istilah LAN dan WAN, karena ia kurang sering dipergunakan. Kebanyakan jaringan yang terdapat dalam gedung atau kampus masuk dalam kategori LAN, atau mencakup jarak yang lebih jauh lagi,dengan *node* di kota-kota, negara yang berbeda, dan ini memenuhi syarat sebagi WAN.jarak yang maksimum yang di jangkau MAN kira-kira 80 kilometer.

c. *Wide Area Network* (MAN)

WAN adalah yang jangkauan *area* geografik paling luas, bisa antar pulau, negara, benua bahkan bisa ke luar angkasa. Contoh terbaik dan sangat terkenal adalah *internet.* Tetapi, WAN dapat juga menjadi jaringan pribadi. Sebagi contoh, seatu perusahaan dengan kantor-kantor diberbagai negara dapat memiliki WAN yang menghubungkan berbagai lokasi melalui hubungan telpon, satelit, dan teknologi-teknologi lainya. Biasanya WAN terdiri dari banyak LAN yang diinterkoneksikan.

WAN dapat mengunakan transport pribadi atau *publik* dan dapat terdiri dari keneksi permanen atau *di-dial* bila perlu. *Link* WAN biasanya lambat bila dibangdingkan dengan *link* LAN. WAN dikategorikan baik sebagai yang didistribusikan atau sentral. WAN yang didistribusikan, seperti *Internet*, tidak mempunyai titik pusat pengendalian.Sebaliknya, WAN sentral didasarkan pada *server* sentral atau tempat yang dipusatkan(seperti kantor pusat perusahaan) dimana semua komputer di hubungkan.

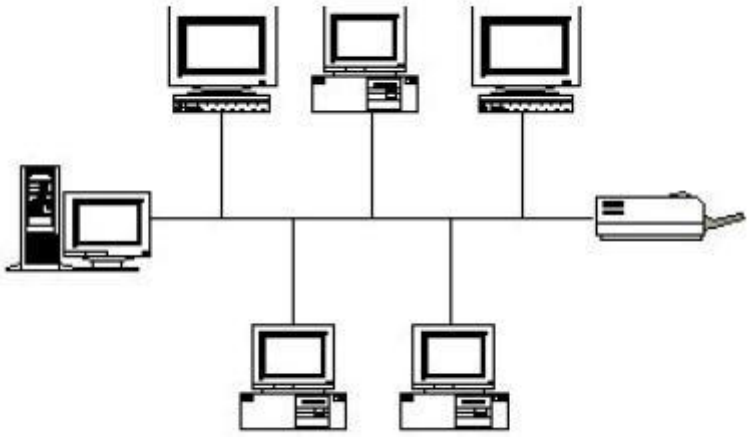
Keuntungan jaringan WAN adalah:

- Server kantor pusat dapat berfungsi sabagia bank data daru kantor cabng.
- Komunikasi antar kantor dapat mengunakan *e-mail* dan *chat.*
- Dokumen atau file yang biasanya dikirimkan melalui *faks* ataupun paket pos, dapat dikirm melalui *e-mail* dan transfer file dari kantor pusat dan kantor cabang dengan biaya yang relatif murah dan dalam jangka waktu yang sangat cepat.
- *Pooling data* dan *ipdating data* antar kantor dapat dilakukan setiap hari pada waktu yang ditentukan.

3.1.3 Topologi Jaringan

Sebuah LAN dapat diimplementasikan dengan berbagai macam topologi. Topologi yang dimaksud di sini merupakan struktur jaringan fisik yang digunakan untuk mengimplementasikan LAN tersebut. Topologi dasar yang bisa digunakan dalam jaringan komputer adalah

a. Topologi *Bus (liner)*



Gambar 3.1 Topologi *Bus*

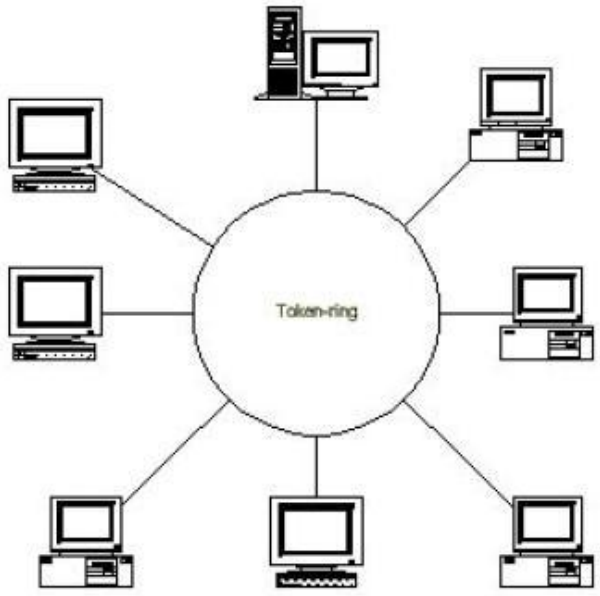
Keuntungan dari topologi Bus adalah:

- Mudah atau sederhana untuk menambahkan komputer kejaringan ini, hanya perlu memasang konektor baru
- Tidak terlalu banyak mengunakan kabel dibandingakn dengan topologi star(bintang).

Kekurangan dari topologi bus(*liner*)

- Seluruh jaringan akan mati jika ada kerusakan pada kabel utama.
- Membutuhkan terminator pada kedua sisi dari kabel utamanya.
- Sangat sulit mengidentifikasi permasalahan jika jaringan sedang jatuh atau mati.
- Sangat tidak didasrkan dipakai sebagai salah satu solusi pada pengunaan jaringan di gedung besar.

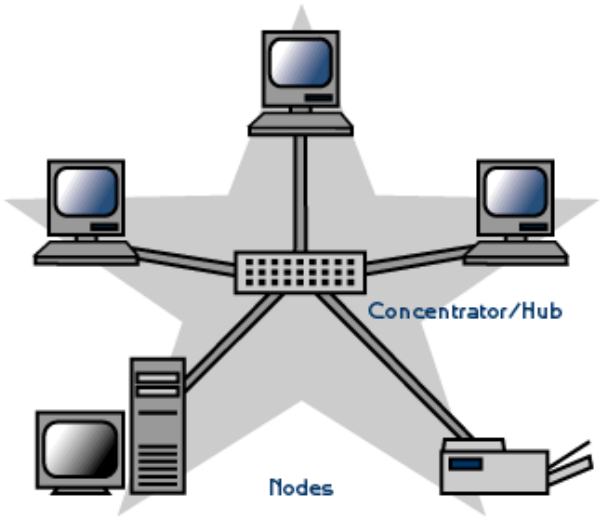
b. Topologi Ring (cincin)



Gambar 3.2 Topologi *Ring*

keuntungan mengunakan topologi Ring ini adalah kemungkinan terjadinya bentrokan dalam transfer data ditiadakan. Kelemahan pengunaan topologi ini adalah harga implementasinya yang relatip mahal. Selain itu tingkat kesulitan untuk menjaga jaringan kembali juga susah. Topologi Ring kurang begitu banyak diimplementasi karena membutuhkan peralatan yang khusus.

c. Topologi *star* (bintang)



Gambar 3.3 Topologi *Star*

Keuntungan topologi jaringan model bintang:

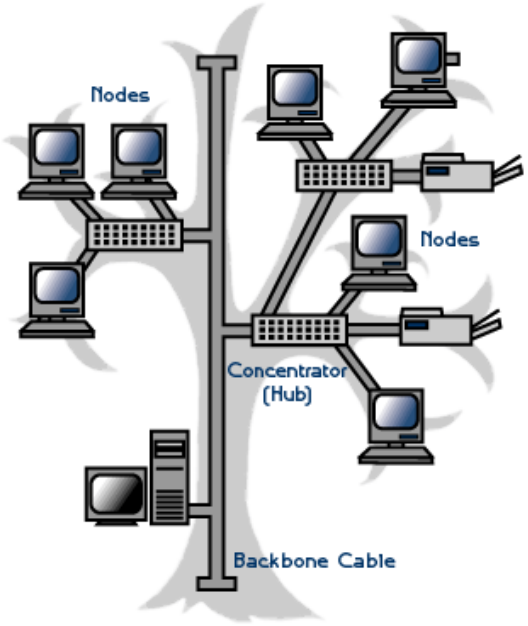
- Mudah dipasng dan mudah dalam pengkabelan.
- Tidak mengakibatkan ganguan pada jaringan ketika akan memasang atau memindahkan prangkat jaringan lain.

- Mudah untuk mendeteksi kesalahan dan memindahkan perangkat-perangkat lain.

Kekurangan topologi jaringan model bintang:

- Membutuhkan banyak kabel dari pada topologi jaringan *bus*.
- Membutuhkan *hub* atau konsentrator, dan bilamana *hub* atau konsentrator tersebut atau rusak *node-node* yang terkoneksi tidak tersedia.
- Lebih mahal dari pada topologi *Bus* (Linear), karena biaya untuk pengandaan *hub* dan konsentrator.

d. Topologi *tree* (pohon)



Gambar 3.4 Topologi *Tree*

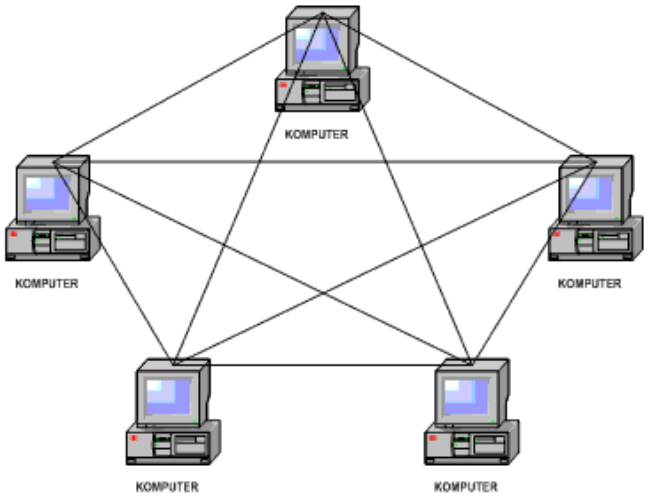
Keuntungan topologi jaringan model pohon:

- Instalasi jaringan dari titik ketitik pada masing-massing segmen.
- Didukung oleh banyak prangkat keras dan prangkat lunak.

Kekurangan topologi jaringan model pohon:

- Keselurahan panjang kabel pada tiap-tiap segmen dibatasi oleh tipe kabel yang digunakan.
- Jika jaringan utama atau *backbone* rusak, keseluruan segmen ikut jatuh juga.
- Sangat sulit untuk dikonfigurasi dan juga untuk pengkabelannya dabandingakan topologi jaringan model lain.

e. Topologi *Mash* (web)



Gambar 3.5 Topologi *Mash*

dibawah ini diperlihatkan tabel yang memuat perbandingan pengunaan media transmisi kabel dan protokol dalam sebuah LAN.

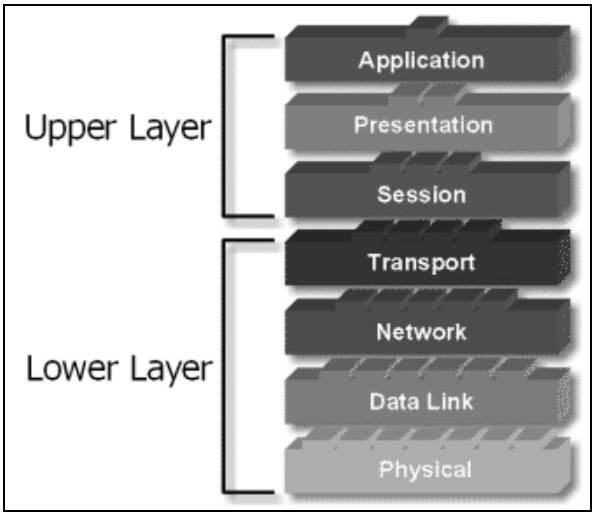
Tabel 3.1 Perbandingan Antar Topologi Jaringan

Topologi Fisik	Kabel yang bisa digunakan	Protokol yang umumnya digunakan
Bus	Kabel *twisted pair* Kabel koaksial Kabel fiber optic	Ethernet Local Talk
Star	Kabel *twisted pair* Kabel fiber optic	Ethernet Local Talk
Tree	Kabel *twisted pair* Kabel koaksial Kabel fiber optic	Ethernet
Ring	Kabel *twisted pair*	Token ring

3.1.4 Model OSI

Menurut Sofana (2011:105) OSI (O*pen System Intercinnection*) Reference Model OSI adalah sebuah model untuk jaringan komputer yang dikembangkan oleh *International Organization For Standardization* (OSI) di Eropa pada tahun 1977. Model OSI ini disebut juga model OSI tujuh lapis atau OSI *seven layer.*

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap *layer* yang berhubungan dengan aliran komuikasi data, termasuk jenis-jenis protokol jaringan dan metode transmisi. Model dibagi menjadi 7 *layer*, dengan karakteristik dan fungsinya masing-masing. Tiap *layer* harus dapat berkomunikasi dengan *layer* diatasnya maupun dibawahnya secara langsung melalui serentetan protokol dan standar.



Gambar 3.6 OSI MODEL

Penjelasan dari masing-masing layer tersebut adalah sebagai berikut.

1. Layer 7: *Application Layer*

Lapisan paling tinggi ini mengatur interaksi pengguna komputer dengan program aplikasi yang dipakai. Lapisan ini juga mengatur bagaimana aplikasi dapat menggakses jaaringan, dan kemudian

membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP, dan NFS.s

2. Layer 6 : *Presentation Layer*

Pada lapisan ini dilakukan konversi data agar data yang dikirim dapat dimengerti oleh penerima, kompresi teks dan penyadian data.

Protokol yang berada dalam level ini adalah perangkat lunak redirector (*redirector software*), seperti layanan *workstation* (dalam Windows NT) dan juga *Network shell* (semacam *Virtual Network Computing (VNC)* atau *Remote Desktop Protokol* (*RDP*)).

3. Layer 5 : *Session Layer*

Lapisan ini menyiapkan saluran komunikasi dan terminal dalam hubungan antar terminal, mengoodinasikan proses pengiriman dan penerimaan serta mengatur pertukaran data.

4. Layer 4 : *Transport Layer*

Lapisan ini mengatur keutuhan data, menerima data dari lapisan *session* dan meneruskannya ke lapisan *network*. Lapisan ini berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadap paket-paket

yang hilang di tengah jalan.

5. Layer 3: *Network Layer*

Lapisan ini menetukan rutte pengiriman dan mengendalikan kemacetan (mendefinisikan alamat-alamat IP), membuat *header* untuk paket-paket, dan kemudian melakukan *routing* melalui *internet working* dengan menggunakan *router* dan *switch layer*-3. Agar data sampai ditempat tujuan dengan benar.

6. Layer 2 : *Data Link Layer*

Pada lapisan ini data diubah dalam bentuk paket, sinkronisasi paket yang dikirim maupun yang diterima menjadi format yang disebut *frame*. Selain itu, pada level ini terjadi koreksi kesalahan, *flow control*, pengalamatan perangkat keras (seperti halnya *Media Access Control Address (MAC Address)*), dan menetukan bagaimana perangkat-perangkat jaringan seperti *hub, Brige, reapeter*, dan *switch layer* 2 beroprasi. Spesifikasi IEEE 802, membagi leve ini menjadi dua level anak, yaitu lapisan *Logical Link Control* (LLC), dan lapisan *Media Access Control* (MAC).

7. Layer 1 : *Physical Layer*

Lapisan terendah ini mengatur sinkronisasi pengiriman dan penerimaan data, spesifikasi meknik, elektrik dan *interface* antar terminal, seperti besar tegangan, frekuensi, impedansi, koneksi *pin* dan jenis kabel. Layer ini juga untuk mendefinisikan media transmisi

jaringan, arsistektur jaringan (serperti.halnya *Ethernet* atau *Token Ring*), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network Interface Card* (NIC) dapat berinteraksi dengan media kabel atau radio.

3.1.5 Media Transmisi Komputer

Menurut Supriyanto (2005:307), media transmisi adalah media atau perangkat yang berfungsi untuk menghubungkan secara fisik untuk komunikasi data antara komputer satu dengan komputer yang lainnya. Secara garis besar media transmisi pada jaringan komputer dibedakan menjadi tiga media, yaitu.

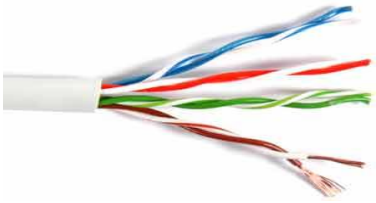
a. Kabel

Ada beberapa macam tipe kabel yang umumnya digunakan dalam LAN. Pada beberapa kasus, sebuah jaringan hanya menggunkan satu macam tipe kabel, di jaringan yang lain menggunakan kabel yang berbeda pula. Kabel yang dipilih adalah berdasarkan dengan topologi jaringan, protokol jaringan, dan ukurannya. Ini sangat penting untuk diketahui karena kesuksesan jaringan tergantung dari semua aspek tersebut. Tipe-tipe kabel yang digunakan di dalam jaringan adalah sebagai berikut.

1. Kabel *Unshielded Twisted Pair* (UTP)

Kabel *twisted pair* ada dua tipe yaitu *shielded* dan *unsheilded. unshielded twisted pair* (UTP) adalah yang paling populer dan umumnya merupakan pilihan yang terbaik untuk jaringan sederhana. Kualitas kabel UTP berbeda dengan telepon. Kabel ini cocok untuk topologi *star* (bintang). Spesifikasi teknis dari *twisted pair* adalah.

- Jarak terjauh 100 meter.
- Dihubungkan dengan konektor RJ-45.
- Memiliki beberapa kategori, yaitu kategori 1, 2, 3, 4, dan 5.
- Masalah yang dihadapi adalah *crosstalk.*



Gambar 3.7 Kabel *Unshielded Twisted Pair*

2. Kabel *Shielded Twisted Pair* (STP)

Kabel *shielded twisted pair* (STP) mirip dengan kabel UTP, kekurangan kabel ini adalah sangat sensitif terhadap sinyal radio dan listrik. Kabel ini sangat baik digunakan di mana

lingkungan pengaruh listrik kurang. Kabel ini biasanya digunakan pada jaringan yang menggunkan topologi ring.

Gambar 3.8 Kabel *Shielded Twisted Pair*

3. Kabel Koaksial

Kabel koaksial adalah kabel yang memiliki satu konduktor tembaga di tengahnya. Sebuah lapisan plastik menutupi di antara konduktor dan lapisan pengaman serat besi, lapisan serat besi tersebut membantu menutupi gangguan dari lampu listrik, kendaraan, dan komputer. Selain instalasi sangat sulit kabel ini juga sangat tidak tahan terhadap serangan dari sinyal-sinyal tertentu. Tapi kabel ini mempunyai keuntungan karena dapat mendukung penggunaan kabel yang panjang diantara jaringan daripada kabel *twisted pair*. Jenis kabel ini biasanya digunakan untuk topologi bus.

Gambar 3.9 Kabel *Koaksial*

4. Kabel Fiber Optik

Kabel serat optik (*fiber optic)* mempunyai kemampuan mentransmisi sinyal melewati jarak yang lebih jauh dibandingkan kabel koaksial maupun kabel *twisted*, juga mempunyai kecepatan yang baik. Hal ini sangat baik digunakan ketika digunakan untuk fasilitas konferensi Radio atau layanan interaktif. 10 BaseF adalah merujuk ke spesifikasi untuk kabel fiber optikdengan membawa sinyal Ethernet.

Gambar 3.10 Kabel Fiber Optik

3.1.6 Protokol Jaringan

Menurut Supriyanto (2005:318), protokol adalah aturan yang harus ditaati atau diikuti oleh komputer yang dihubungkan untuk menghasilkan dan mengatur komunikasi melalui jaringan. Jadi untuk

memungkinkan terjadinya komunikasi antar komputer pada jaringan komputer diperlukan sebuah protokol, yang mendefinisikan aturan-aturan transfer data sehingga komunikasi bisa berjalan dengan baik.

a. TCP/IP

Protokol TCP/IP merupakan protokol yang paling populer dan paling banyak digunakan saat ini, alasannya adalah TCP/IP menggunakan skema pengalamatan fleksibel yang dapat sekali di-*route*, bahkan untuk jaringan yang paling besar, hampir semua sistem operasi dan platform dapat menggunakan TCP/IP, sejumlah besar untilitas dan *tool* dapat dipergunakan, sebagian digabungkan dengan rangkaian protokol dan sebagian ditambahkan dalam program untuk mengawasi dan mengatur TCP/IP, TCP/IP merupakan protokol internet global, kebanyakan jaringan tingkat *enterprise* menjalankan TCP/IP, dan yang penting bahwa administrator jaringan akrab dengan protokolny. Inti dari protokol ini terdiri dari dua bagian besar, yaitu TCP dan IP.

TCP (*transmission control protocol*) digunakan untuk aplikasiyang membutuhkan koneksi dengan pembangunanjalur virtual sementara UDP tidak. Cara kerja protokol TCP adalah seperti cara kerja komunikasi telepon. Sebelum dapat berkomunikasi dengan lewat telepon, maka dibangun jalur virtual antara penghubung dan yang dihubungi. Setelah jalur dibangun barulah kominikasi bisa berlangsung. Setelah komunikasi ini selesai, jalur virtual ini akan dihacurkan kembali.

IP (*internet protocol*) mengatur pengalamtan jaringan TCP/IP, dimana sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda antara yang satu dengan yang lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data. Komputer mengidentifikasi alamat setiap komputer menggunakan sekumpulan angka sebanyak 32 bit yang dikenal sebagai alamat IP (IP *address*).

Alamat IP terdiri dari bilanagan biner sepanjang 32 bit yang dibagi atas 4 segmen. Tiap segmen terdiri atas 8 bit yang bearti memiliki nilai desimal 0-255 (2^8). Range alamat (*address*) yang bisa digunakan harus dalam bentuk kode biner, yang dimulai dari 00000000.00000000.00000000.00000000 – 11111111.11111111. 11111111. 11111111. Jadi, jaringan TCP/IP dengan 32 bit *address* ini mampu menampung sebanyak 2^{32}, ini bearti ada lebih dari 4 miliar host tepatnya 4.294.467.296 alamat yang dapat terhubung dengan alamat ini. Untuk memudahkan pembacaan dan penulisan, alamat IP biasanya direpresentasikan dalam bilangan desimal. Jadi *range address* di atas dapat diubah menjadi *address* 0.0.0.0 sampai *address* 255.255.255.255. nilai desimal dari alamat IP inilah yang dikenal dalam pemakaian sehari-hari.

1. Kelas Alamat IP

Bit jaringan berperan dalam identifikasi suatu jaringan dari jaringan yang lain, sedangkan bit *host* berperan dalam identifikasi host dalam suatu jaringan. Jadi, seluruh *host* yang tersambung dalam jaringan yang sama memiliki bit jaringan yang sama. Sebagian dari bit-bit bagian awal dari alamat IP merupakan *network bit* atau *network number*, sedangkan sisanya untuk host. Garis pemisah antara bagian jaringan dan host tidak tetap, bergantung pada kelas jaringan. Ada 3 kelas alamat (address) yang utama dalam TCP/IP, yakni kelas A, kelas B, dan kelas C. Software internet protocol menentukan pembagian jenis kelas ini dengan menguji beberapa bit pertama dari alamat IP. Selain ketiga kelas tersebut, masih ada 2 kelas lagi yang ditunjuk untuk pemakaian khusus, yakni kelas D yang digunakan untuk *multicast address* dan kelas E yang digunakan untuk cadangan kegiatan eksperimental.

Tabel 3.2 Pembagian Kelas Ip

Kelas	**Range**	**Subnet mask**	**Komputer**	**Range IP**
A	**1 – 126**	255.0.0.0	255^3 = 16,7 jt	1.0.0.0 – 126.255.255.254
B	**128 – 191**	255.255.0.0	255^2 = 65.024	128.0.0.0– 191.255.255.254

C	**192 - 223**	255.255.255.0	255 = 254	192.0.0.0 – 233.255.255.0
D	**224 – 239**	Multicast IP Address		
E	**240 - 250**	Dicadangkan untuk eksperimen		

2. Alamat Khusus

Selain alamat yang dipergunakan untuk pengenalan *host*, ada beberapa jenis alamat yang digunakan untuk keperluan khusus dan tidak boleh digunakan untuk pengenal *host*. Alamat tersebut adalah *network address, broadcast address,* dan *netmask*.

a. *Network address*

Alamat (*address*) ini digunakan untuk mengenali suatu *network* pada jaringan *internet*. Tujuannya adalah untuk menyederhanakan informasi *routing* pada *internet*. *Router* cukup untuk melihat *network address* untuk menetukan kemana paket tersebut harus dikirimkan.

b. *Broadcast Address*

Alamat (*address*) ini digunakan untuk mengirim atau menerima informasi yang harus diketahui oleh seluruh host yang ada pada suatu jaringan. Seperti diketahui, setiap paket IP memiliki *header* alamat tujuan berupa alamat IP dari *host* yang akan dituju oleh paket tersebut. Dengan adanya alamat ini, maka hanya *host*

tujuan saja yang memproses paket tersebut, sedangkan *host* lain akan mengabaikannya. Dengan adanya *broadcast address* suatu host dapat mengirim paket ke alamat *broadcast* kemudian seluruh host yang ada di jaringan tersebut mendapatkan data yang sama.

c. *Netmask*

Adalah alamat yang digunakan untuk melakukan masking atau filter pada proses pembentukan routing supaya kita cukup memerhatikan beberapa bit saja dari total 32 bit alamat IP. Artinya dengan menggunakan netmask tidak perlu memerhatikan seluruh 32 bit alamat IP untuik menentukan routing, akan tetapi cukup beberapa buah saja dari alamat IP yang kita perlu perhatikan untuk menentukan ke mana paket tersebut dikirim.

Kaitan antara *host address*, *network address*, *broadcast address*, dan *network mask* sangat erat, semua dapat dihitung dengan mudah jika kita cukup paham mengenai bilangan biner. Jika kita ingin secara serius mengoperasikan sebuah jaringan komputer menggunakan teknologi TCP/IP dan *internet*, adalah mutlak bagi kita untuk menguasi konsep alamat IP tersebut.

a. Subnet Mask

Subnet mask digunakan untuk menentukan alokasi IP bagi komputer-komputer pada suatu jaringan lokal. *Subnet mask* merupakan angka biner yang digunakan untuk membedakan *network*

ID dengan *host* ID, dan menunjukan lokasi suatu *host*, apakah ia berada pada jaringan atau tidak.

Tabel 3.3 Subnet Mask Kelas Ip

Kelas IP	Subnet Mask	Dalam Desimal
A	11111111.00000000. 00000000.00000000	255.0.0.0
B	11111111.11111111. 00000000.00000000	255.255.0.0
C	11111111.11111111. 11111111.00000000	255.255.255.0

b. Wacana Ipv6

Pengembangan IPv6, IP generasi berikut atau Ipng (IP *next generation*) yang direkomendasikan pada pertemuan IETF di Toronto tanggal 25 Juli 1994 dilatarbelakangi oleh kekurangan alamat IP yang saat ini memiliki panjang 32 bit, akibat ledakan pertumbuhan jaringan. IPv6 merupakan versi baru dari IP yang merupakan pengembangan dari IPv4. Perbaikan utama pada IPv6 perluasan ruang alamat IP, penyederhanaan *header* dari paker, *Plug* dan *Play*, serta fungsi keamanan. Masing-masing perbaikan tersebut dimaksudkan

agar dapat merespon pertumbuhan internet, meningkatkan reliabilitas, maupun kemudahan pemakaian.

Perkembangan internet yang demikian pesat beberapa tahun terakhir ini tel;ah mengakibatkan kelangkaan alamat IP address. Perubahan terbessar pada IPv6 adalah perluassan alamat IP dari 32 bit pada IPv4 menjadi 128 bit. 128 bit ini adalah ruang alamat yang berkelanjutan dengan menghilangkan konsep kelas. Selain itu juga dilakukan perubahan pada cara penulisan alamat IP. Pada IPv6, 128 bit tersebut dipisahkan menjadi masing-masing 16 bit yang tiap bagian dipisahkan dengan ":" dan dituliskan dengan heksadesimal.

3.1.7 *Open Source*

Menurut Schmidt (2003 : 475) Open source adalah suatu metode pengembangan software yang memanfaatkan kekuatan didistribusikan peer review dan transparansi proses.

3.1.8 *Linux*

Linux menurut supriyato (2005:97) merupaka sistem operasi bebas dan terbuka (*ope source*) berlesesi *General Public lisence* (GPL) yang mana pendistribusia dan pengembanganya bisa dilakukan secara bebas dengan mengikukan kode program asal sebagai turunannya. Pengembangan *software* bebas memiliki tujuan agar setiap orang dapat mendapatkan manfaat dari *software* secara bebas sehinga setiap orang

dapat menjalankan, mengandakan, menyebarluaskan, mempelajari, mengubah, dan meningkatka kinerja *software*.

Perkembangan LINUX sagat pesat karena didukung oleh pengembang *sorces* yang bebas bagi pengunaya dan relatif sudah sempurna untuk dioperasika. Sistem operasi LINUX saat ini sudah berpenampilan grafis dan semudah pemakaiyan pada windows. Dengan konsep *open source* (kode program bisa dilihat dan di kembangkan oleh siapa saja) dan gratis,banyak pemakai, terutama di lingkungan kampus, yang tertarik mengelutinya. Dukungan aplikasi yang kian meluas, dari aplikasi perkantoran, multimedia, hingga *database,* yang kebanyakan bersipat gratis, membuat kalangan pemakai linuk tumbuh lebih cepat.

3.1.9 Debian

Debian menurut supriyanto (2005:97) adalah distribusi yang mengutamakan kestabilan dan keandalan, meskipun mengorbankan aspek kemudahan dan kemutakhiran program. Debian mengunakan .*deb* dalam paket instalasi programnya.

3.1.10 Server

Server menurut supriyanto (2005:105) adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Server didukung dengan prosesor yang bersifat

scalable dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut sebagai sistem operasi jaringan atau network operating system. Server juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pencetak (printer), dan memberikan akses kepada workstation anggota jaringan. Umumnya, di atas sistem operasi server terdapat aplikasi-aplikasi yang menggunakan arsitektur klien/server.

3.1.11 Http

Menurut Sukarno (2006:15) Pengertian HTTP atau definisi HTTP (HyperText Transfer Protocol) adalah sebuah protokol untuk meminta dan menjawab antara client dan server. Sebuh client HTTP seperti web browser, biasanya memulai permintaan dengan membuat hubungan TCP/IP ke port tertentu di tempat yang jauh (biasanya port 80). Sebuah server HTTP yang mendengarkan di port tersebut menunggu client mengirim kode permintaan (request) yang akan meminta halaman yang sudah ditentukan, diikuti dengan pesan MIME yang memiliki beberapa informasi kode kepala yang menjelaskan aspek dari permintaan tersebut, diikut dengan badan dari data tertentu.

3.1.12 Mysql

Menurut Sukarno (2006:3) MySQL merupakan salah satu RDBMS (*Relational Database Management System*) di bawah lisensi GPL yang bersifat sumber terbuka dan bebas untuk didistribusikan[8]. MySQL menggunakan bahasa SQL (*Structured Query Language*) yang merupakan bahasa query standar yang digunakan luas. MySQL umum digunakan dalam aplikasi berbasis web karena sifatnya yang gratis, stabil dan cepat, kemudahan penggunaan, *cross-platform* berjalan baik di UNIX maupun *platform* Windows, serta dukungan yang luas. Dalam penggunaannya dengan *server* RADIUS, PHP dipergunakan untuk membangun logika dan antarmuka aplikasi, sedangkan MySQL untuk menyimpan data autentikasi yang berisi data login para pengguna, data autorisasi yang berisi hak akses dari pengguna, dan data-data akuntansi yang mencatat penggunaan setiap *user*. Data ini kemudian akan dipergunakan oleh modul SQL FreeRadius untuk mengatur pembatasan akses pengguna.

MySQL merupakan salah satu SQL database *open source* yang sangat popular saat ini dan menawarkan fitur dan fungsi yang sangat berguna, termasuk aspek keamanan.

Berikut fitur-fitur yang mendukung MySQL, yaitu ;

a. Multi – threading, mendukung query *multiple simultaneous.*

b. Mendukung penggunaan *password* pada system dan kepemilikan yang fleksibel.
c. Dapat mencapai 16 keys per tabel. Setiap key dapat dipakai samapail 15 field.
d. Mendukung *field primery key, field-field key* dan unik pada *create.*

Dukungan terhadap satu sampai empat *bit int, fload, double, fixed* dan panjang *string variable, time stamps,*

3.1.13 *Intrusion Detection System (IDS)*

Rafiudin (2010:121) *Intrusion Detection System* (IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Intrusion Detection System (IDS) dapat dikembangkan di berbagai tempat pada jaringan untuk meningkatkan keamanan dan proteksi sebuah perusahaan. Pada umumnya, ada dua bentuk dasar *Intrusion Detection System (IDS)* yang digunakan saat ini: *Intrusion Detection System* (*IDS)* berbasis jaringan dan *Intrusion Detection System* (*IDS)* berbasis host. Kedua tipe sensor ini menawarkan teknik yang berbeda untuk mendeteksi dan menangguhkan

kegiatan yang jahat, dan keduanya harus dikembangkan untuk menyediakan peningkatan yang paling efektif pada strategi pertahanan berlapis :

1. *Host-Based Intrusion Detection System (HIDS)* merupakan aplikasi perangkat lunak khusus yang diinstal pada komputer (biasanya server) untuk melihat semua aliran komunikasi masuk dan keluar ke dan dari server tersebut dan untuk memonitor system file jika ada perubahan. *HIDS* sangat efektif untuk *server* aplikasi Internet-accessible, seperti web atau e-mail server karena mereka dapat melihat aplikasi pada source-nya untuk melindungi mereka. Sebagai contoh, berkas-berkas yang sensitif (seperti program untuk melakukan login, authetikasi) dimonitor dengan ketat. Jika terjadi perubahan yang tidak direncanakan maka ada kemungkinan penerobos sudah masuk dan mengganti (mengubah) berkas tersebut. Demikian pula berkas log dimonitor untuk mengetahui adanya penerobosan.
2. *Network-Based Intrusion Detection System (NIDS)* menempati secara langsung pada jaringan dan melihat semua aliran yang melewati jaringan. *NIDS* merupakan strategi yang efektif untuk melihat traffic masuk/keluar maupun traffic di antara host ataupun di antara segmen jaringan lokal. *NIDS* biasanya dikembangkan di depan dan di belakang firewall dan *VPN gateway*

untuk mengukur ke efektifan peranti-peranti keamanan tersebut dan berinteraksi dengan mereka untuk mernperkuat keamanan jaringan.

NIDS dan *HIDS* harus dikembangkan bersama-sama untuk menyediakan pertahanan lapisan yang benar-benar efektif dengan melihat dan mengontrol komunikasi perusahaan. IDS juga menyediakan perusahaan dengan check-and-balance pada keefektifan sistem keamanan dan keseluruhan keefektifan biaya keamanan mereka. Bagian selanjutnya mendiskusikan keseluruhan kapabilitas IDS.

3.1.14 *Intrusion Prevention System (IPS)*

Rafiudin (2010:145) *IPS (Intrusion Prevention System)* merupakan jenis metode pengamanan jaringan baik software atau hardware yang dapat memonitor aktivitas yang tidak diinginkan atau *intrusion* dan dapat langsung bereaksi untuk untuk mencegah aktivitas tersebut. *IPS (Intrusion Prevention System)* merupakan pengembangan dari dari *IDS (Intrusion Detection System)* .Sebagai pengembangann dari teknologi firewall, IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau pattern, tidak hanya berdasarkan *ports* atau *IP address* seperti *firewall* umumnya. . *Intrusion Detection System* Selain dapat memantau dan *monitoring, IPS (Intrusion Prevention*

System) dapat juga mengambil kebijakan dengan memblock paket yang lewat dengan cara melapor ke *firewall*.

Ada beberapa metode *IPS (Intrusion Prevention System)* melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut.

- *Signature-based Intrusion Detection System*

Pada metode ini, telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data signature yang ada harus tetap ter-update.

- *Anomaly-based Intrusion Detection System*

Pada metode *Anomaly-based Intrusion Detection System* harus melakukan konfigurasi terhadap *IDS (Intrusion Detection System)* dan *IPS (Intrusion Prevention System),* sehingga *IDS (Intrusion Detection System)* dan *IPS (Intrusion Prevention System)* dapat mengatahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila *IDS (Intrusion Detection System)* dan IPS *(Intrusion Prevention System)* menemukan ada anomali

pada paket yang diterima atau dikirimkan, maka *IDS (Intrusion Detection System)* dan *IPS (Intrusion Prevention System)* akan memberikan peringatan pada pengelola jaringan atau akan menolak paket tersebut untuk diteruskan. Untuk metode ini, pengelola jaringan harus terus-menerus memberi tahu *IDS (Intrusion Detection System)* dan *IPS (Intrusion Prevention System)* bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian oleh *IDS (Intrusion Detection System)* atau *IPS (Intrusion Prevention System).*

Intrussion prevenstion system mengkombinasikan kemampuan *network based IDS* dengan kemampuan *firewall*, sehingga selain mendeteksi adanya penyusup juga bisa menindak lanjuti dengan melakukan blok terhadap IP address yang melakukan serangan. Beberapa *Intrusion Prevention System* (IPS) opensource yang dikenal.

- *Portsentry*

Portsentry digunakan untuk melakukan pemblokiran *IP address* yang melakukan *scanning port* dengan menggunakan fasilitas dari *firewall* atau teknik *null route*.

- *Sshdfilter*

sshdfilter digunakan untuk melakukan blocking *IP address* yang melakukan *ssh brute forcing*.

- *Snort*

Snort di gabungkan dengan *blockit* dan *firewall* merupakan *Nework Intrusion Prevention System* yang mampu melakukan blocking *IP address* terhadap beragam serangan yang di definisi di signature snort.

3.1.15 *Suricata*

Meneurt Thomas (2005*) Suricata* adalah perangkat lunak pendeteksi dan pecegah intrusi (Intrusion Detection and Prevention System) open source yang merupakan generasi berikutnya dari perangkat IDS/IPS yang ada saat ini yang tidak sekedar dimaksudkan untuk hanya menggantikan atau meniru perangkat-perangkat yang ada di industry, tetapi akan membawa ide-ide dan teknologi baru. Suricata dirilis oleh OISF. Suricata dapat menggunakan rule rule yang biasa digunakan oleh perangkat lunak snort IDS.

Suricata memiliki kemampuan untuk mendeteksi serangan berdasarkan signature dari aturan sama seperti kemampuan yang dimiliki oleh snort. Suricata memiliki beberapa fitur yang belum dimiliki oleh Snort, misalnya akselerator memiliki dukungan multi-threading, namun beberapa aturan yang berlaku di Snort tidak bisa dilakukan di Suricata hal tersebut dikarenakan tidak kompetibel.

Di sisi lain, Snort lebih baik dari Suricata. Snort tetap merupakan IDS yang sangat kuat / IPS, sangat baik didokumentasikan melalui

Internet dan yang benar mendeteksi sebagian besar malwares dan teknik penggelapan. Preprosesor yang sangat berguna untuk merakit kembali paket terfragmentasi.

Perbandingan fitur inspeksi stateful menunjukkan bahwa Snort dan Suricata memiliki pendekatan yang berbeda. Snort basis deteksi pada aturan dan ambang batas untuk melacak jumlah waktu aturan dipicu sedangkan Suricata memperkenalkan variabel sesi (misalnya melalui flowint) memungkinkan untuk membuat counter. Variabel ini kemudian dapat digunakan oleh aturan manual (local.rules file) untuk memicu peristiwa. Satu keuntungan Suricata memiliki adalah kemampuannya untuk memahami tingkat 7 dari model OSI, yang meningkatkan kemampuannya mendeteksi malwares. Suricata telah menunjukkan bahwa hal itu jauh lebih efisien daripada Snort untuk mendeteksi, virus malwares dan shellcodes.

Sebagai kesimpulan, Snort tetap standar de facto untuk *IDS / IPS* dalam lingkungan produksi. Hal ini stabil, mudah dikonfigurasi dan sangat baik didokumentasikan. Namun demikian, Suricata adalah sebuah *IDS/IPS* baru sebagai sebuah pengembangan untuk *IDS/IPS*

3.1.16 *Basic Analysis and Security Engine (BASE)*

Meneurt Thomas (2005*) Basic Analysis and Security Engine (Base)* merupakan suatu layanan web query front-end untuk melakukan

anilisis alert. Dengan menggunakan *BASE* akan mempermudah untuk mengoordinasi semua alert dan log yang ada pada database, sehingga alert dan log akan lebih mudah untuk dianalisa. *BASE* ditulis dengan menggunakan bahasa pemrograman PHP dan menampilkan informasi dari database pada halaman web dengan baik. *Basic Analysis and Security Engine (Base)* dapat membaca *log tcpdump binary* dan alert dalam format Snort, meskipun data tersebut sudah di proses. *Basic Analysis and Security Engine (Base)* dapat menampilkan paket informasi pada laye-3 dan laye-4 dalam bentuk grafik. Informasi tersebut akan terus berubah berdasarkan waktu, sensor, signature, protocol, IP address, port TCP/UDP ataupun berdasarkan bentuk spesifik. *BASE* interface search berdasarkan query dari alert meta informasi seperti sensor. Grup alert, signanature, klasifikasi dan watu deteksi, dengan baik seperti sumber dan tujuan alamat paket, port, paket payload, ataupun paket flag.

Basic Analysis and Security Engine (Base) mempermudah dalam memanajemen data alert, Administrator dapat mengelompokan data alert berdasrkan kategori, menghapus kesalahan dan mengendalikan alert, melakukan pengarsipan dan melakukan pengiriman data ke alamat email untuk dilakukan proses selanjutnya. *Basic Analysis and Security Engine (Base)* dapat diimplementasikan pada system operasi lainnya. *Basic Analysis and Security Engine (Base)* mempunyai bagian-bagian

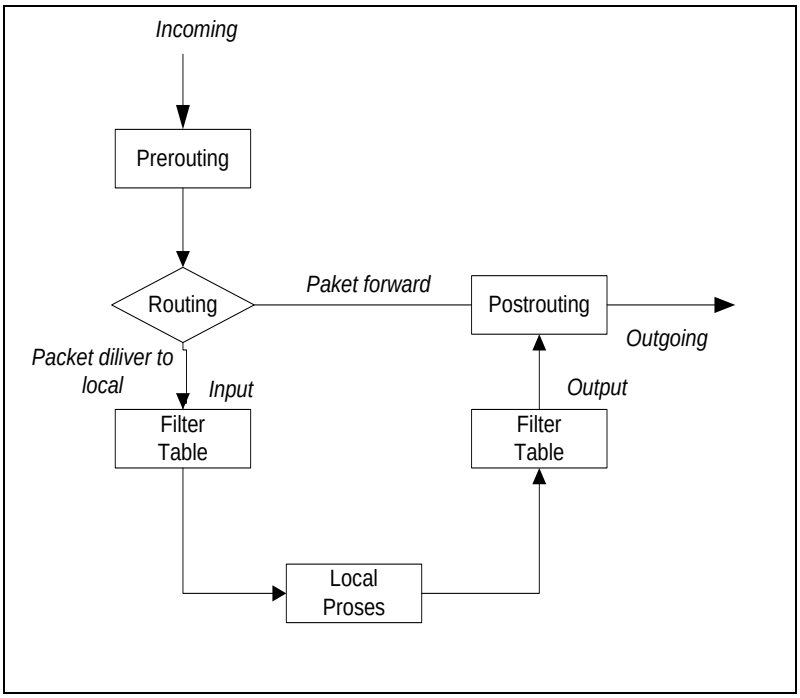
yaitu :

a. *Searc* berfungsi untuk mencari *alert* yang sesuai dengan alert meta informasi (seperti sensor, *signature*, *detection tim*e)
b. *Graph alert* data berfungsi untuk membuat chart dan statistic berdasarkan waktu, sensor, *signature*, *protocol*, *ip address*, TCP/UDP port, klasifikasi.
c. *Graph/alert detection time* berfungsi untuk membuat statistic berdasarkan waktu.
d. *Unique alert* berfungsi untuk menampikan instrusi yang terdeteksi pada sensor.
e. Sensor/total berfungsi untuk menampilkan jumlah sensor da nip *address* sensor.
f. *Categories* berfungsi untuk membuat grup *alert*, mendukung alert yang dianggap semu atau palsu, mengirimkan *alert* ke email serta mendukung pengarsipan *alert* dapat dipindahkan antar database.
g. *Traffic profile by protocol* berfungsi untuk men-*display* grafik informasi *alert* layer 3 (transfort, TCP, UDP)
h. *Total number of alert* berfungsi untuk menampilkan detail informasi intrusi.

3.1.17 *IPtables*

IP*Table* merupakan suatu program yang digunakan untuk memasukkan dan menghapus isi tabel tersebut filter paket kernel. Dengan demikian, apapun yang dituliskan dalam tabel tersebut akan hilang ketika dilakukan reboot terhadap system. Supaya system dapat selalu mempunyai kemampuan filter paket yang diinginkan, aturan-aturan yang diberikan dapat ditulis dalam skrip inisialisasi. Dapat juga digunakan perintah iptables-save untuk menyimpan aturan yang diberikan dan perintah *iptables-restore* untuk menjalankan semua aturan yang sudah ditulis. (Wagito,2007:146)

Sebenarnya IPTable tidak hanya bisa digunakan untuk membangun Firewall, tetapi juga dapat dionfigurasikan menjadi sebuah router unuk menghubungkan subnet network yang berbeda. (Wagito, 2007:109).



(Sumber : Wagito, 2007:109)

Gamabar 3.11 Aliran Paket Data

3.2 Hasil Penelitian Terdahulu

a. Hasil penenlitian Pertama

Tabel 3.4 Hasil Penelitian Pertama

Judul Penelitian	Nama Penelitian	Variabel
1.DESAIN DAN IMPLEMENTASI *NETWORK INTRUSION DETECTION SYSTEM*	Mahmud	Hasil yang didapat dalam penelitian ini adalah *intrusion Detection System*(IDS) yang berfungsi sebagai level keamanan di tingkat aplikasi setelah suatu paket

(NIDS) DENGAN *SNOR T* PADA JARINGAN KOMPUTER STIMIK PALCOMTECH PALEMBANG		melewati sebuah *firewall* dan yang mempunyai tugas untuk mendeteksi dan mengatur penyusup yang menyerang suatu jaringan. Salah satu masalah keamanan yang cukup signifikan pada jaringan adalah masuknya user dan program(misalnya: *worm,trojanhorse,virus,*dan lain-lain) yang diangap merusak system. *Snort* merupakan suatu prangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintas jaringan secara *real time traffic* dan *logging* kedalam *database* serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan

b. Hasil Penelitian Kedua

Tabel 3.5 Hasil Penelitian Kedua

Judul Penelitian	Nama Penelitian	Variabel
DESAIN DAN IMPLEMENTASI *NETWORK INTRU SION DETECTION SYSTEM* (IDS) UNTUK PENGAMANAN JARINGAN KOMPUTER LOKAL PADA CV.HONDA UNION MOTOR	Azwarnas	Hasil yang didapat dalam penelitian ini adalah *intrusion Detection System* (IDS) teknik-teknik pencegahan terhadap serangan sistem informasi terus dikembangkan sehingga integritas, pada sebuah sistem informasi menjadi lebih terjamin. Salah satunya adalah dengan sistem pendeteksian penyusup. Dalam tulisan ini penulis membangun sebuah sistem pendektesian penyusup dengan mengunakan Snort IDS dan Iptables firewall. Sistem ini bekerja dengan membangun sebuah mesin yang membaca prameter IP asal penyerang pada alert yang kemudian memerintahkan firewall untuk memblok akses dari IP penyerang tersebut. Untuk memudah membaca pola serangan yang terjadi penulis mengunakan BASE(*Basic Analysis Security*

		Enginet) hasil pengujian memberikan hasil yang memuaskan sesuai dengan yang diharapkan, yakni dengan mempunyai sistem untuk memblok (menutup) akses terhadap usaha-usaha penyerangan.

BAB IV

METODE PENELITIAN

4.1 Lokasi Dan Waktu Penelitian

4.1.1 Lokasi

Lokasi penelitian ini dilaksanakan pada Yayasan IBA Palembang yang beralamat Jl. Mayor Ruslan Palembnag.

4.1.2 Waktu Penelitian

Waktu penelitian berjalan dari tanggal 7 Maret sampai dengan 7 April 2012.

4.2 Jenis Data

Data merupakan susuatu bentuk informasi yang sangat penting dalam melakukan penelitian. Dalam penulisan skripsi ini Penulis menggunakan beberapa jenis data dalam pengumpulan data, yang terdiri dari:

4.2.1 Data Primer

Menurut Umar (2007:42), Data primer merupakan data yang didapat dari sumber pertama baik secara individu atau perseorangan seperti hasil dari wawancara atau hasil pengisian kuesioner yang biasa dilakukan oleh peneliti.

Data primer tersebut didapat Penulis secara langsung dari Pegawai Pengadilan Tinggi Palembang khususnya pada bagian umum, yang menjelaskan jalannya program, topologi yang dipakai serta

permasalahan yang sering terjadi khususnya dalam jaringan di Pengadilan Tinggi Palembang.

4.2.2 Data Sekunder

Menurut Umar (2007:42), data sekunder merupakan data primer yang telah diolah lebih lanjut dan disajikan baik oleh pihak pengumpulan data primer atau oleh pihak lain, biasanya berupa sejarah instansi, visi dan misi, aktivitas oraganisasi dan struktur organisasinya serta topologi yang digunakan pada Yayasan IBA Palembang.

4.3 Teknik Pengumpulan Data

1. Pengamatan (*Observasi*)

   Menurur Hasan (2008:17), observasi adalah cara pengumpulan data dengan terjun dan melihat langsung ke lapangan, terhadap objek yang diteliti. Dengan metode observasi ini penulis mendapatkan data-data yang jelas tentang penelitian ini, maka penulis meninjau langsung kelokasi objek yang di teliti dalam hal ini penulis melakukan observasi langsung di Yayasan IBA Palembang.

2. Wawancara (*Interview*)

   Menurut Hasan (2008:17), wawancara adalah cara pengumpulan data dengan langsung mengadakan tanya jawab kepada objek yang diteliti atau kepada perantara yang mengetahui persoalan dari objek yang

sedang diteliti. Penulis melakukan wawancara langsung dengan Kepala IT Yayasan IBA Palembang yaitu Bapak Erwan.

4.4 Jenis Penelitian

4.4.1 Penelitian Terapan

Menurut Kuncoro (2009:07), penelitian terapan, sering disebut *applied research*, merupakan penelitian yang menyangkut aplikasi teori untuk memecahkan permasalahan tertentu. Ada tiga contoh dari penelitian terapan, yaitu: (1) **Penelitian Evaluasi**, yaitu penelitian yang diharapkan dapat memberikan masukan atau pengambilan keputusan tentang nilai relatif dari dari dua atau lebih alternatif tindakan; (2) **Penelitian dan Pengembangan**, yaitu: penelitian yang bertujuan untuk mengembangkan produk sehingga produk tersebut mempunyai kualitas yang lebih tinggi; (3) **Penelitian Tindakan**, yaitu: penelitian yang dilakukan untuk segera dipergunakan sebagai dasar tindakan pemecahan masalah yang ada.

Penelitian yang di ambil penulis adalah penelitian dan pengembangan.

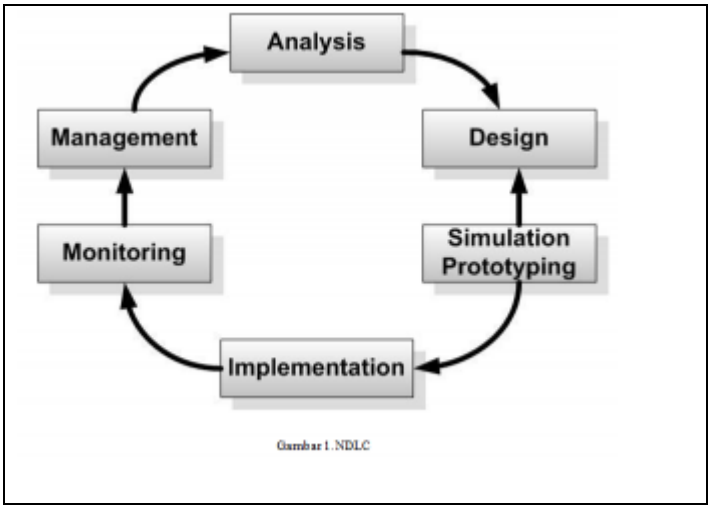
Penelitian dan pengembangan, Tujuan utama dari penelitian dan pengembangan bukan untuk formulasi dan uji hipotesis, melainkan untuk mendapatkan produk baru atau proses baru. Melalui penelitian dan pengembangan produk, perusahaan akan menghasilkan produk baru dengan kualitas yang lebih tinggi, sehingga dapat memenuhi selera konsumen. Sehubungan dengan

penelitian dan pengembangan produk, perusahaan dapat menerapkan pengendalian kualitas total yang prinsip utamanya adalah *kaizen* atau selalu mengadakan perbaikan secara berkesinambungan.

4.5 Teknik Pengembang Sistem

Menurut James E. Goldman, Philips T. Rawles, (2001:470) Dalam pengembangan aplikasi ini digunakan metode pengembangan *Network Development Life Cycle Model* (

Model) atau juga dikenal dengan metodelogi *Classic Life Cycle Model* (CLCM)/ *Linear Sequential Model* (LSM)/*Waterfall Method*. Pada metode ini terdapat enam tahap untuk mengembangkan suatu perangkat lunak. Keenam tahapan itu tersusun dari atas kebawah, diantaranya : *Analysis, Design, Simulation prototyping, Implementation, Monitoring, Managemen.*



Gambar 4.1 Model NDLC

1. Analysis

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya ;

a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah / operator agar mendapatkan data yang konkrit dan lengkap. pada kasus di Computer Engineering biasanya juga melakukan brainstorming juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda
b. survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap design, survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan.
c. membaca manual atau blueprint dokumentasi, pada analysis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan suatu sistem dokumentasi menjadi

pendukung akhir dari pengembangan tersebut, begitu juga pada project network, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

2. Design

Dari data-data yang didapatkan sebelumnya, tahap Design ini akan membuat gambar design topology jaringan interkoneksi yang akan dibangun. Design bisa berupa design struktur topology, design akses data, design tata layout perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang project yang akan dibangun Biasanya hasil dari design berupa ;

a. Gambar-gambar topology (server farm, firewall, datacenter, storages, lastmiles, perkabelan, titik akses dan sebagainya)
b. Gambar-gambar detailed estimasi kebutuhan yang ada

3. Simulation Prototype

Beberapa networker akan membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network seperti BOSON, PACKET TRACERT, NETSIM, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para networker’s yang hanya menggunakan alat Bantu tools VISIO untuk membangun topology yang akan didesign.

4. Implementation

Di tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi networker's akan menerapkan semua yang telah direncanakan dan didesign sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya project yang akan dibangun dan ditahap inilah Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

5. Monitoring

merupakan tahapan yang penting agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan monitoring. Monitoring bisa berupa melakukan pengamatan pada ;

a. Infrastruktur hardware : dengan mengamati kondisi reliability / kehandalan system yang telah dibangun (reliability = performance + availability + security),
b. Memperhatikan jalannya packet data di jaringan (pewaktuan, latency, peektime, troughput)
c. Metode yang digunakan untuk mengamati "kesehatan" jaringan dan komunikasi secara umum secara terpusat atau tersebar Pendekatan yang paling sering dilakukan adalah pendekatan Network Management, dengan pendekatan ini banyak

perangkat baik yang lokal dan tersebar dapat di monitor secara utuh.

6. Management,

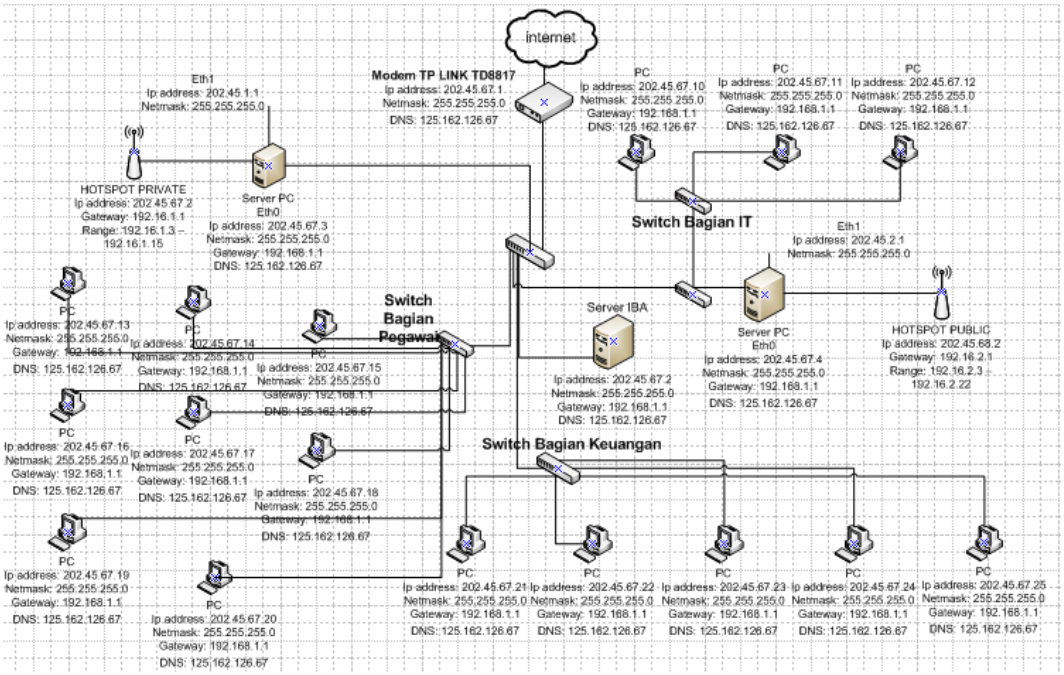
Merupakan manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah Policy, kebijakan perlu dibuat untuk membuat / mengatur agar sisem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur Reliability terjaga. Policy akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan.

BAB V

ANALISA DAN PEMBAHASAN

5.1 Analisa

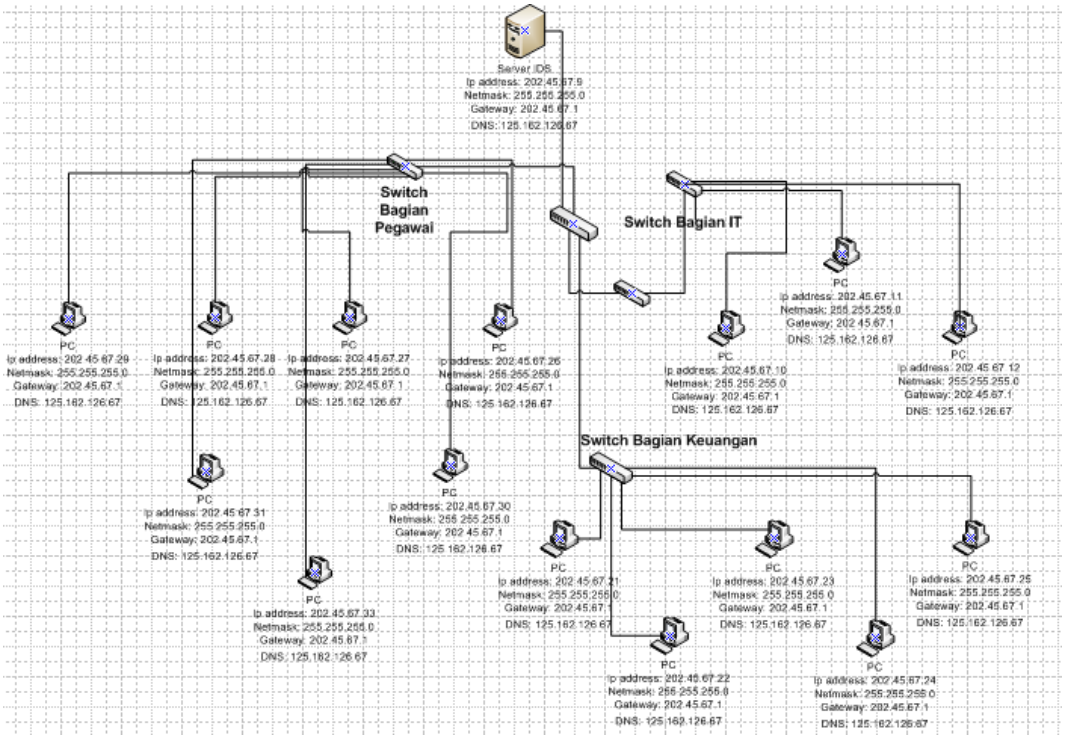
Desain jaringan komputer pada Yayasan IBA palembang mengunakan topologi *star*. Masing-masing workstation dihubungkan secara langsung ke server melalui switch. Menurut pengamatan penulis Yayasan IBA palembang memilih menggunakan topologi star yang bertujuan agar mudah untuk pengimplementasiannya dan memang cocok untuk diterapkan pada Yayasan IBA palembang, selain itu topologi star memiliki keunggulan dari topologi yang lain. Keunggulan dari topologi tipe star ini adalah bahwa dengan adanya kabel tersendiri untuk setiap workstation ke server, maka *bandwidth* atau lebar jalur komunikasi dalam kabel akan semakin lebar sehingga akan meningkatkan kinerja jaringan secara keseluruhan dan juga bila terdapat gangguan di suatu jalur kabel maka gangguan hanya akan terjadi dalam komunikasi antara workstation yang bersangkutan dengan server sehingga jaringan secara keseluruhan tidak mengalami gangguan. Yayasan IBA palembang belum pernah sebelumnya menggunakan IDS ataupun tool pengamanan jaringan lainnya sehingga pihak Yayasan IBA palembang tidak pernah menggetahui ada atau tidaknya penyusup yang mengganggu jaringan komputer pada Yayasan IBA palembang Palembang.



Gambar 5.1 Topologi Jaringan Yayasan IBA Palembang

5.2 Desain

Tahap desain ini akan membuat gambar topologi jaringan yang sudah dimodifikasi berdasarkan pada topologi jaringan yang sudah ada pada Yayasan IBA Palembang. Dari hasil pengamatan penulis yang telah dilakukan, maka topologi jarongan pada Yayasan IBA Palembang dapat digambarkan secara sederhana seperti gambar dibawah ini



(Sumber: Pengolah Sendiri)

Gambar 5.2 Topologi jaringan komputer yang akan diimplementasikan

Dari gambar topologi jaringan yang akan diimplementasikan penulis tidak banyak melakukan perubahan pada topologi sebelumnya hanya penambahan satu unit *server* yang terletak didalam jaringan komputer Yayasan IBA palembang yang bertugas untuk memantau pergerakan data dalam jaringan tersebut. IDS sendiri mempunyai tugas memonitorinng jaringan pada satu segmen dengan *server* IDS itu sendiri.

5.3 *Simulation Prototype*

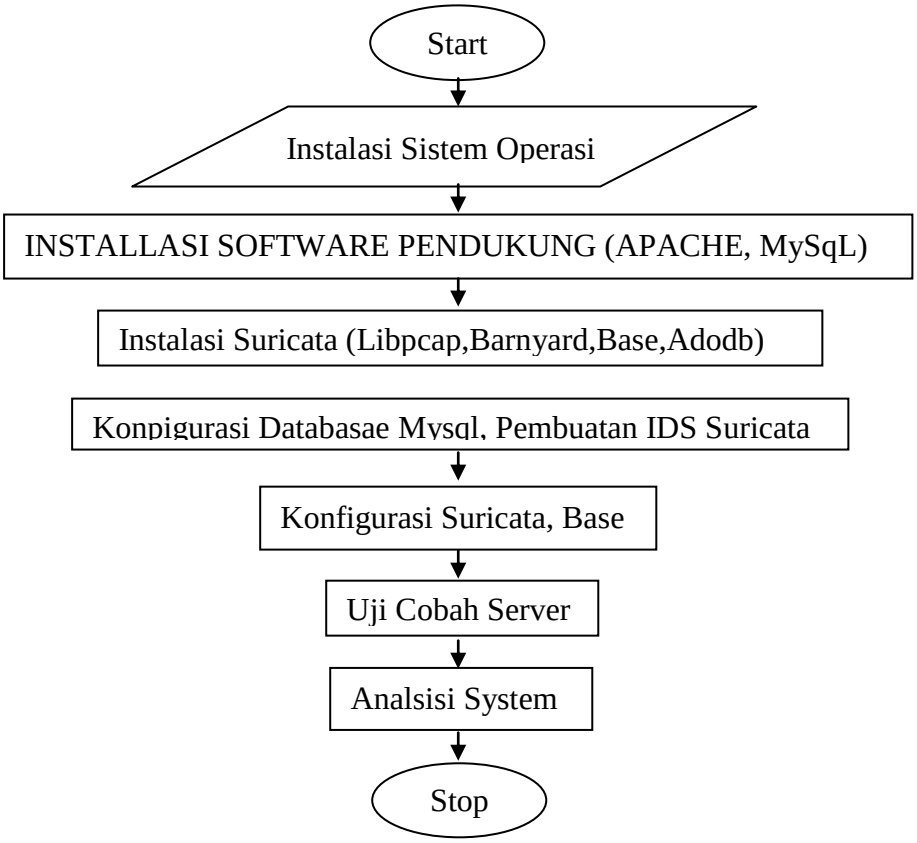
Komputer karyawan atau *client* yang ada saat ini di Yayasan IBA Palembang, semuahnya mengunakan sistem operasi windows xp, dengan

procesor pentium IV 1,6 Ghz, *hardisk* 80 Gb dan memori RAM 512 Mb, monitor LCD Acer 16`' dan mengunakan aplikasi pendukung *microsoft office*.

Spesifikasi komputer *server* yaitu *procesor* pentium IV 1,6 Gh, *hardisk* 80 Gb dan memori DDR1 512 Mb, DVDRW, *mainboard* MSI, monitor 16`', *keyboard* dan *mouse optik.*

5.4 Implementasi

Dalam membangun sebuah IDS dibutuhkan langkah-langkah sistematis mulai dari instalasi sistem operasi yang digunakan, instalasi *software*, konfigurasi *software- software*, konfigurasi database dan uji coba sistem. Adapun langkah-langkah dalam membuat IDS mengunakan aplikasi suricata dapat dilihat pada gambar dibawah ini:



Gambar 5.3 Pembuatan IDS suricata

Berdasarkan hasil pengamatan yang didapat pada Yayasan IBA palembang, penulis mencoba mengkonfigurasikan IDS Suricata serta BASE menggunakan Debian 6. Adapun langkah-langkah selanjutnya yang harus dilakukan yaitu : Instalasi Server, Konfigurasi IP Address, Intalasi Perangkat Suricata, Instalasi dan konfigurasi Suricata, Instalasi dan Konfigurasi Base.

5.4.1 Instalasi Server

Langkah awal yang harus dilakukan adalah install server, pada saat penginstanlan berlangsung, install pula LAMP dan Open SSH. Pengimplementasian ini penulis menggunakan Debian 6.

5.4.2 Konfigurasi IP Address

Langkah selanjutnya yang harus dilakukan adalah konfigurasi IP Address server yaitu dengan perintah :

```
root@debian:/home/server#nano /etc/network/interfaces
```

Gambar 5.4 Konfigurasi IP *address*

Setelah masuk dalam file etc/network/interfaces masukkan ip address pada konfigurasinya sebagai berikut :

```
# This file describes the network interfaces
available on your system
# and how to activate them. For more information,
see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 202.45.67.9
netmask 255.255.255.0
gateway 202.45.67.1
```

(Sumber: dilolah sendiri)

Gambar 5.5 file */etc/network/interface*

Simpanlah file yang telah diedit tekan Ctrl + O, enter, serta Ctrl+X. Setelah melakukan konfigurasi IP Address, restart kartu jaringan dengan perintah :

```
root@debian:/home/server#/etc/init.d/networking
restart
```

(Sumber penglolah sendiri)

Gambar 5.6 Perintah *restart* kartu jaringan

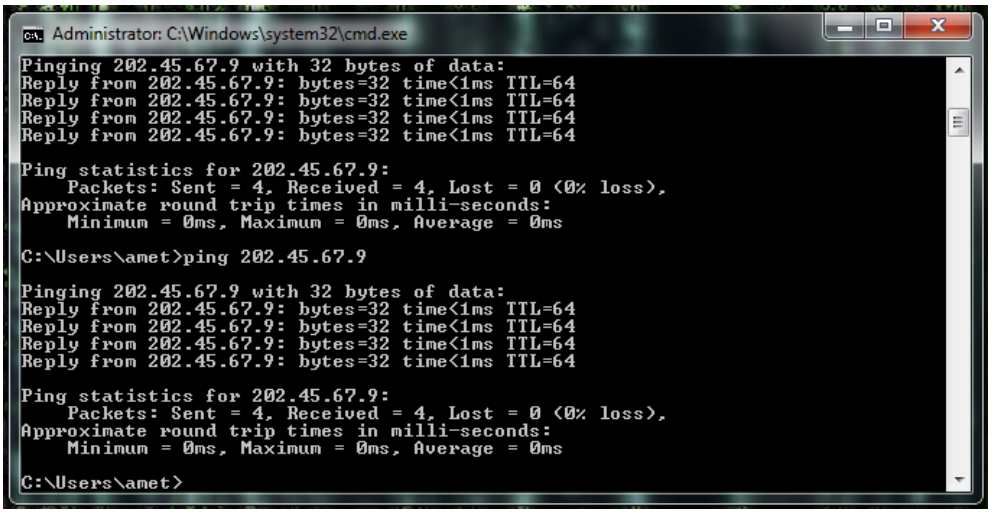
Pastikanlah file konfigurasi telah terpasang dengan cara mengetikan perintah :

```
root@debian:/home/server#ifconfig

eth0   Link encap:Ethernet  HWaddr 00:26:2d:59:f8:ee
       inet addr:202.45.67.9   Bcast:202.45.67.255  Mask:255.255.255.0
       inet6 addr: fe80::226:2dff:fe59:f8ee/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:106 errors:0 dropped:0 overruns:0 frame:0
       TX packets:220 errors:0 dropped:0 overruns:0 carrier:1
       collisions:0 txqueuelen:1000
       RX bytes:24694 (24.1 KiB)  TX bytes:35940 (35.0 KiB)
       Interrupt:28


lo     Link encap:Local Loopback
       inet addr:127.0.0.1  Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING  MTU:16436  Metric:1
       RX packets:118 errors:0 dropped:0 overruns:0 frame:0
       TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:22543 (22.0 KiB)  TX bytes:22543 (22.0 KiB)
```

(Sumber: Pengolah Sendiri)

Gambar 5.7 File *Ifconfig*

Kemudian lakukanlah test *Ping* dari klien untuk memastikan konfigurasi telah berhasil :



Gambar 5.8 Tes *Ping Clien*

5.4.3 Instalasi dan Konfigurasi DNS

DNS menjadi salah satu bagian yang penting didalam jaringan, ketika seorang mengunjung situs mengetik suatu alamat misalkan http://www.sunanruber.com pada aplikasi browser, DNS akan mengambil alamat tersebut dan mentranslasikannya ke alamat IP. Tanpa adanya DNS, pengunjung tetap akan dapat mengakses alamat tersebut, akan tetapi sungguh sulit menghapal alamat IP sebuah server, jika dibandingkan dengan nama host atau domain.

Selanjutnya menginstall bind9 dan langsung Buatlah nama domain dengan perintah dibawah ini :

```
root@debian:/home/server#apt-get install bind9
root@debian:/etc/bind#nano named.conf.local
```

(Sumber: Pengolah Sendiri)

Gambar 5.9 Konfigurasi *file /etc/bind/named.conf.local*

Setelah mengetik perintah diatas, selanjutnya editlah file /etc/bind/named.conf.local yang merupakan konfigurasi pendukung untuk nama domain seperti pada gambar dibawah ini :

```
zone "iba.com" {
type master;
file "/etc/bind/db.iba.com";
};
zone "67.45.202.in-addr.arpa" {
type master;
file "/etc/bind/db.202.45.67";
};
```

(Sumber: Pengolah Sendiri)

Gambar 5.10 *Named.conf.local*

Langkah selanjutnya yang harus dilakukan adalah meng *copy* file *copy db.local ke db.iba.com*

```
root@debian:/etc/bind#cp db.local db.iba.com
```

(Sumber: Pengolah Sendiri)

Gambar 5.11 *cp db.local db.iba.com*

Langkah selanjutnya yang harus dilakukan adalah meng *copi file copy db.127 ke db.202.45.67.*

```
root@debian:/etc/bind#cp db.127 db.202.45.67
```

(Sumber: Pengolah Sendiri)

Gambar 5.12 *cp db.127 db.202.45.67*

Langkah selanjutnya yang harus dilakukan adalah *konfigurasi file nano db.iba.com*

```
root@debian:/etc/bind#nano db.iba.com
```

(Sumber: Pengolah Sendiri)

Gambar 5.13 perintah */bind/db.iba.com*

Setelah mengetik perintah diatas, langkah selanjutnya mengedit file *file/bind/db.iba.com.*

```
;
; BIND data file for local loopback interface
;
$TTL    604800
iba.com.            IN         SOA        ns.iba.com.
root.iba.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )         ; Negative
Cache TTL

;

iba.com.            IN      NS      ns.iba.com.
ns.iba.com.         IN      A       202.45.67.9
suricata.iba.com.   IN      A       202.45.67.9
```

(Sumber: Pengolah Sendiri)

Gambar 5.14 file *bind/db.iba.com*

Selanjutnya simpan serta keluar dari *file konfigurasi* tersebut dengan cara *Ctrl*+o dan *Ctrl*+x.

Langkah selanjutnya yang harus dilakukan adalah *konfigurasi file nano db.202.45.67.*

```
root@debian:/etc/bind#nano db.202.45.67
```

(Sumber: Pengolah Sendiri)

Gambar 5.15 perintah */bind/db.202.45.67*

Setelah mengetik perintah diatas, langkah selanjutnya mengedit *file/bind/db.202.45.67*

```
; BIND data file for local loopback interface
;
$TTL    604800
67.45.202.in-addr.arpa.                IN          SOA
ns.iba.com. root.iba.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )         ; Negative
Cache TTL
;
67.45.202.in-addr.arpa.              IN            NS
ns.iba.com.
9.67.45.202.in-addr.arpa.             IN           PTR
suricata.iba.com.
9.67.45.202.in-addr.arpa.             IN           PTR
iba.com.
```

(Sumber: Pengolah Sendiri)

Gambar 5.16 *file bind/db.202.45.67*

Selanjutnya simpan serta keluar dari file konfigurasi tersebut dengan cara Ctrl+O dan Ctrl+x. Selanjutnya lakukan *restart* pada aplikasi *bind9* dengan perintah dibawah ini :

```
root@debian:/etc/bind#/etc/init.d/bind9 restart

Stopping domain name service...: bind9 waiting for
pid 1360 to die.

Starting domain name service...: bind9.
```

(Sumber: Pengolah Sendiri)

Gambar 5.17 *restart* aplikasi *bind9*

Langkah selanjutnya tes DNS servernya dengan mengetik nslookup suricata.iba.com, seperti gambar dibawah ini :

```
root@debian:/etc/bind#nslookup suricata.iba.com

Server:         202.45.67.9
Address:  202.45.67.9#53

Name:     suricata.iba.com
Address: 202.45.67.9
```

(Sumber: Pengolah Sendiri)

Gambar 5.18 *nslookup suricata.iba.com*

Langkah selanjutnya tes DNS servernya dengan mengetik nslookup 202.45.67.9, seperti gambar dibawah ini *:*

```
root@debian:/etc/bind#nslookup 202.45.67.9

Server:         202.45.67.9

Address:  202.45.67.9#53

9.67.45.202.in-addr.arpa name = suricata.iba.com.
9.67.45.202.in-addr.arpa name = iba.com.
```

(Sumber: Pengolah Sendiri)

Gambar 5.19 *nslookup* 202.45.67.9

5.4.4 Instalasi perangkat tambahan Suricata

Untuk penginstallan suricata dan base dibutuhkan beberapa perangkat tambahan seperti *Libpcre3-dev, libtool mysql-client, mysql server, libmysqlclient-dev checkinstall libpcre3-dev libpcap-dev libyaml-dev zlib1g-dev libcap-ng-dev libhtp1 libnetfilter-queue-dev*

libnetfilter-queue1 libnfnetlink-dev libnfnetlink0. Untuk penginstalan perangkat tambahan tersebut ketikan perintah :

```
root@debian:/home/server#apt-get install libpcre3
libpcre3-dev build-essential autoconf automake
libtool mysql-client mysql-server libmysqlclient-
dev checkinstall libpcre3-dev libpcap-dev libyaml-
dev zlib1g-dev libcap-ng-dev libhtp1 libnetfilter-
queue-dev libnetfilter-queue1 libnfnetlink-dev
libnfnetlink0 libnet1 libnet1-dev
```

(Sumber: Pengolah Sendiri)

Gambar 5.20 *install* Perangkat tambahan

5.4.5 Instalasi dan konfigurasi Suricata beserta IDS

Setelah IP address terpasang dan terkoneksi ke jaringan,serta perangat tambahan telah tersinstal dengan baik. maka kita dapat melakukan instalasi Suricata.

```
root@debian:/opt# tar xzvf yaml-0.1.3.tar.gz
root@debian:/opt/yaml-0.1.3# ./configure && make
&& make install
root@debian:/opt# tar -xvf libnfnetlink-
1.0.0.tar.bz2
root@debian:/opt/libnfnetlink-1.0.0# ./configure
&& make && make install
root@debian:/opt# tar -xvf libnetfilter_queue-
1.0.0.tar.bz2
root@debian:/opt# tar xzvf suricata-
1.1beta1.tar.gz
root@debian:/opt/suricata-1.1beta1# mkdir
/var/log/suricata
root@debian:/opt/suricata-1.1beta1# ./configure
--enable-nfqueue --enable-debug
root@debian:/opt/suricata-1.1beta1# make && make
install
```

(Sumber: Pengolah Sendiri)

Gambar 5.21 *Install suricata dan IDS*

Setelah selesai penginstalan suricata buat folder suricata dan download rule-rule suricata, kemudian salin rule-rule snort sehingga rule-rule menjadi lebih lengkap, rule-rule suricata dapat didownload pada

http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz.

```
root@debian:/home/suricata# mkdir /etc/suricata
root@debian:/etc/suricata# wget
http://rules.emergingthreats.net/open/suricata/
emerging.rules.tar.gz
root@debian:/etc/suricata# tar xzvf
emerging.rules.tar.gz
root@debian:/opt/suricata-1.1beta1# cp
suricata.yaml /etc/suricata/
root@debian:/opt/suricata-1.1beta1# cp
classification.config /etc/suricata/
root@debian:/opt/suricata-1.1beta1# cp
reference.config /etc/suricata/
```

(Sumber: Pengolah Sendiri)

Gambar 5.22 *copy suricata rule*

Untuk melihat rule-rule snort yang telah disalin kepada rule-rule suricata ketikkan perintah berikut ini :

```
root@debian:/etc/suricata#gedit suricata.yaml

default-rule-path: /etc/suricata/rules/
rule-files:
 - attack-responses.rules
 - backdoor.rules
 - bad-traffic.rules
 - chat.rules
 - ddos.rules
 - deleted.rules
 - dns.rules
 - dos.rules
```

```
- experimental.rules
- exploit.rules
- finger.rules
- ftp.rules
- icmp-info.rules
- icmp.rules
- imap.rules
- info.rules
- local.rules
- misc.rules
- mysql.rules
- netbios.rules
- nntp.rules
- oracle.rules
- other-ids.rules
- p2p.rules
- policy.rules
- pop2.rules
- pop3.rules
- porn.rules
- rpc.rules
- rservices.rules
- scada.rules
- scan.rules
- shellcode.rules
- smtp.rules
- snmp.rules
- specific-threats.rules
- spyware-put.rules
- sql.rules
- telnet.rules
- tftp.rules
- virus.rules
- voip.rules
- web-activex.rules
- web-attacks.rules
- web-cgi.rules
- web-client.rules
- web-coldfusion.rules
- web-frontpage.rules
- web-iis.rules
```

```
 - web-misc.rules
 - web-php.rules
 - x11.rules
 - emerging-attack_response.rules
 - emerging-dos.rules
 - emerging-exploit.rules
 - emerging-game.rules
 - emerging-inappropriate.rules
 - emerging-malware.rules
 - emerging-p2p.rules
 - emerging-policy.rules
 - emerging-scan.rules
 - emerging-virus.rules
 - emerging-voip.rules
 - emerging-web.rules
 - emerging-web_client.rules
 - emerging-web_server.rules
 - emerging-web_specific_apps.rules
 - emerging-user_agents.rules
 - emerging-current_events.rules

HOME_NET: "[202.45.67.0/24]
```

(Sumber: Pengolah Sendiri)

Gambar 5.23 *Rule-rule Suricata dan Snort*

Setelah itu lakukan instalasi dan konfigurasi libpcap dan barnyard2 Yang berfungsi untuk koneksi database antara suricata dan MySql, instalasi barnyard dapat dilakukan dengan mengetikkan perintah berikut:

```
root@debian:/opt# tar xzvf libpcap-1.0.0.tar.gz
root@debian:/opt/libpcap-1.0.0# ./configure && make
&& make install
root@debian:/opt# tar xzvf barnyard2-1.9.tar.gz
root@debian:/opt/barnyard2-1.9# ./configure -with-
mysql  && make && make install
root@debian:/home/server# mkdir /var/log/barnyard2
root@debian:/opt/barnyard2-1.9/etc#cp  barnyard2.conf
/etc/suricata/root@debian:/opt/barnyard2-1.9/etc#
```

```
gedit barnyard2.conf
config reference_file:
/etc/suricata/reference.config
config classification_file:
/etc/suricata/classification.config
config gen_file: /etc/suricata/rules/gen-
msg.mapconfig sid_file:
/etc/suricata/rules/sid-msg.map
output    database:    log,    mysql,    usersuricata
password=12345 dbname=suricatadb
host=localhost sensor_name=sensor
```

(Sumber: Pengolah Sendiri)

Gambar 5.24 *instalasi libpcap dan barnyard2*

Setelah selesai installasi *libpcap dan barnyard2* maka buat database suricata dengan mengetikkan perintah :

```
mysql> create database suricatadb;
Query OK, 1 row affected (0.00 sec)
mysql> grant create, insert, select, delete, update
on suricatadb.* to suricata@localhost;
Query OK, 0 rows affected (0.00 sec)
mysql> set password for
suricata@localhost=password('12345');
Query OK, 0 rows affected (0.00 sec)
mysql>exit;
```

(Sumber: Pengolah Sendiri)

Gambar 5.25 membuat *database Suricata*

Setalah membuat database suricatadb lakukan perintah berikut :

```
root@debian:/ barnyard2-1.9#
/usr/bin/mysql –u root -p suricatadb <
schemas/create_mysql
```

(Sumber: Pengolah Sendiri)

Gambar 5.26 i*mpor table database*

Untuk menampilkan database yang telah dibuat maka ketikan perintah :

```
root@debian:/home/server#mysql -u root -p
Enter password:12345
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| suricatadb         |
+--------------------+
   3 rows in set (0.00 sec)
  mysql> use suricatadb
  >Database changed
mysql> SHOW TABLES;
+----------------------+
| Tables_in_suricatadb |
+----------------------+
| data                 |
| detail               |
| encoding             |
| event                |
| icmphdr              |
| iphdr                |
| opt                  |
| reference            |
| reference_system     |
| schema               |
| sensor               |
| sig_class            |
| sig_reference        |
| signature            |
| tcphdr               |
| udphdr               |
+----------------------+
  mysql>exit
```

(Sumber: Pengolah Sendiri)

Gambar 5.27 Menampilkan *Databases*

Setelah membuat dtabase suricata dan melakukan intalasi libpcap dan barnyard2, salin directori barnyard2 ke etc/suricata kemudian buka barnyard.conf lalu salin config gen_file: /etc/suricata/rules/gen-msg.map dan config sid_file:/etc/suricata/rules/sid-msg.map kedalam barnyard2.conf

5.4.6 Instalasi BASE dan Adodb

Base merupakan analisis dasar sebagai keamanan suatu mesin yang berfungsi untuk mencari dan mengolah database dari alert network security yang dibangkitkan oleh perangkat lunak pendeteksi serangan yaitu Intrusion Detection System (IDS). Base terintergrasi dengan Adodb sebagai penghubung ke database suricata. ekstrak file base-1.4.5.tar.gz dan file adodb4991.tgz ke file /var/www

```
root@debian:/var/www# tar xzvf base-1.4.5.tar.gz
root@debian:/var/www# mv base-1.4.5 base
root@debian:/var/www# tar xzvf adodb4991.tgz
root@debian:/home/server#apt-get install apache2
php5 php5-mysql php5-gd php-pear libmysqlclient15-
dev
```

(Sumber: Pengolah Sendiri)

Gambar 5.28 *ekstarak file Base dan Adodb* dan install LAMP

Kemudian instal *alldeps mail, alldeps mail-mime, alldeps image_canvas-0.3.2, image_graph-0.7.1* untuk paket pendukung *base dan adobe.*

```
root@debian:/home/server#pear install --alldeps mail
root@debian:/home/server#pear install --alldeps
mail_mime
root@debian:/home/server#pear install --alldeps
image_canvas-0.3.2
root@debian:/home/server#pear install --alldeps
image_graph-0.7.1
```

(Sumber: Pengolah Sendiri)

Gambar 5.29 *Install all mail*

Kemudian edit file /etc/php5/apache2/php.ini dengan menambahkan extension=mysql.so extension=gd.so.

```
root@debian:/home/server#gedit

/etc/php5/apache2/php.ini

;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;

; If you wish to have an extension loaded
automatically, use the following
; syntax:
;
;   extension=modulename.extension
;
; For example, on Windows:
;
;   extension=msql.dll
;
; ... or under UNIX:
;
   extension=mysql.so
   extension=gd.so
```

(Sumber: Pengolah Sendiri)

Gambar 5.30 konfigurasi file apache2/php.ini

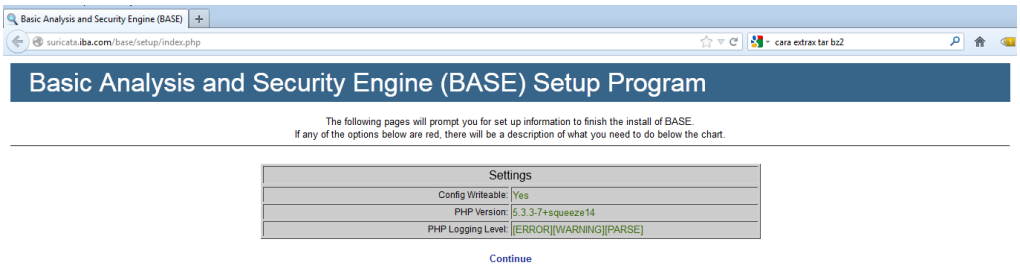
Kemudian beri izin akses untuk menulis pada folder /var/www dengan mengetikan :

```
root@debian:/var/www#cd /var/www
root@debian:/var/www#chmod a+w base
```

(Sumber: Pengolah Sendiri)

Gambar 5.31 Mengubah hak akses *Base*

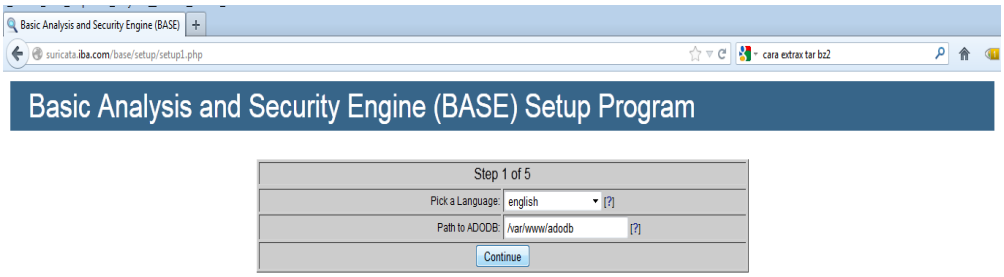
Kemudian buka browser ketikkan perintah Http://suricata.iba.com/setup/index.php maka akan tampil seperti dibawah ini :



(Sumber: Pengolah Sendiri)

Gambar 5.32 *Settings BASE step* awal

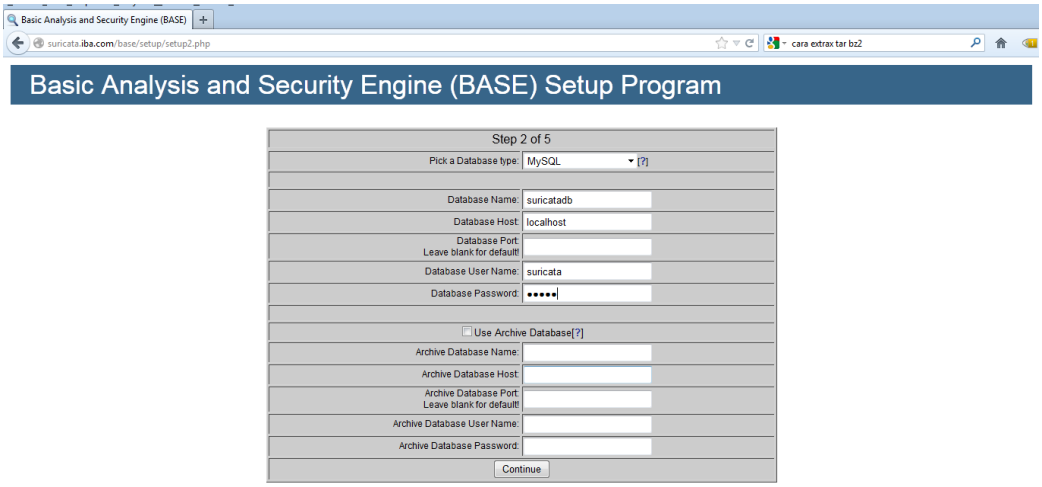
Klik *continue* untuk melanjutkan penginstallan base, kemudian pada step pertama isi *path to adodb* dengan /var/www/adodb.



(Sumber: Pengolah Sendiri)

Gambar 5.33 *Settings* BASE *step* 1

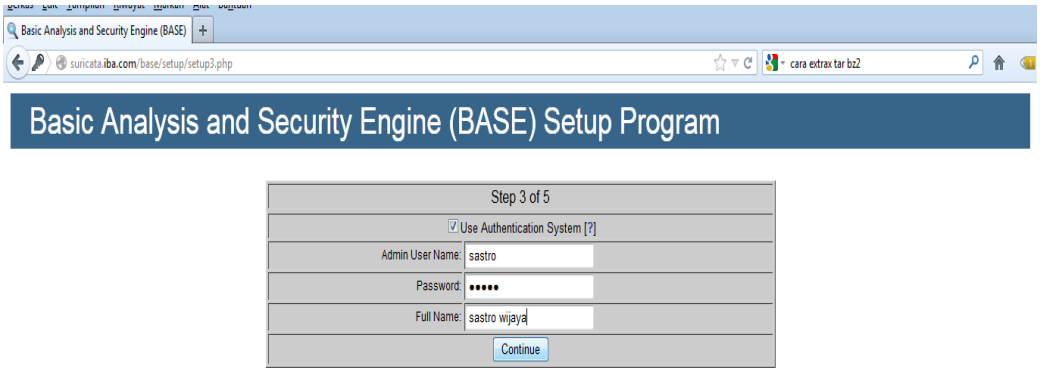
Step kedua isilah kolom yang kosong pada BASE seperti dibawah ini:



(Sumber: Pengolah Sendiri)

Gambar 4.34 *Settings BASE step 2*

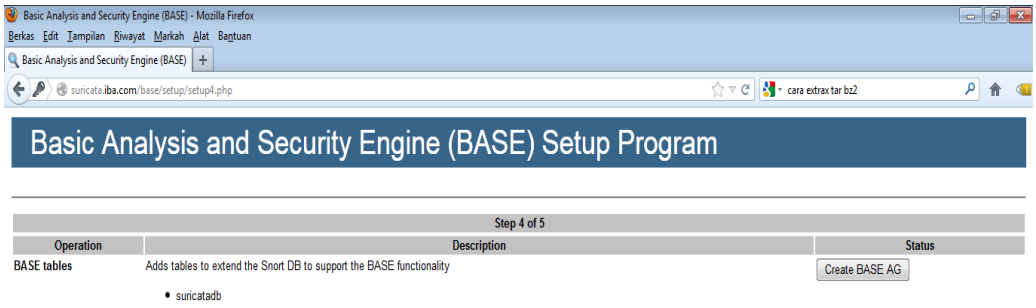
Step ketiga kita diminta menggunakan *autentication system*. Bila kita ingin mengunakan *authentication system* maka tandai *use authentication system*, isi *username* dan *Password*.



(Sumber: Pengolah Sendiri)

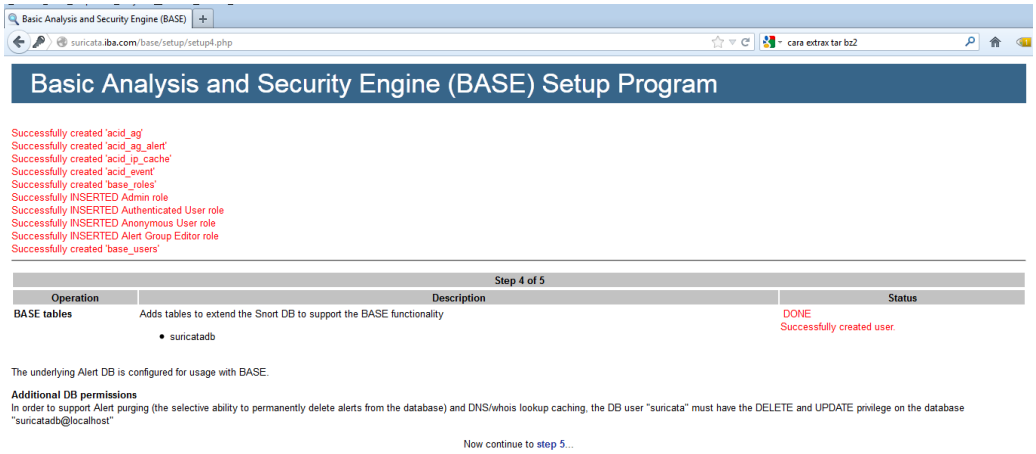
Gambar 5.35 *Setting* BASE *step 3*

setelah itu pilih *Create BASE AG* yang akan diproses kemudian klik *continue step 5*



(Sumber: Pengolah Sendiri)

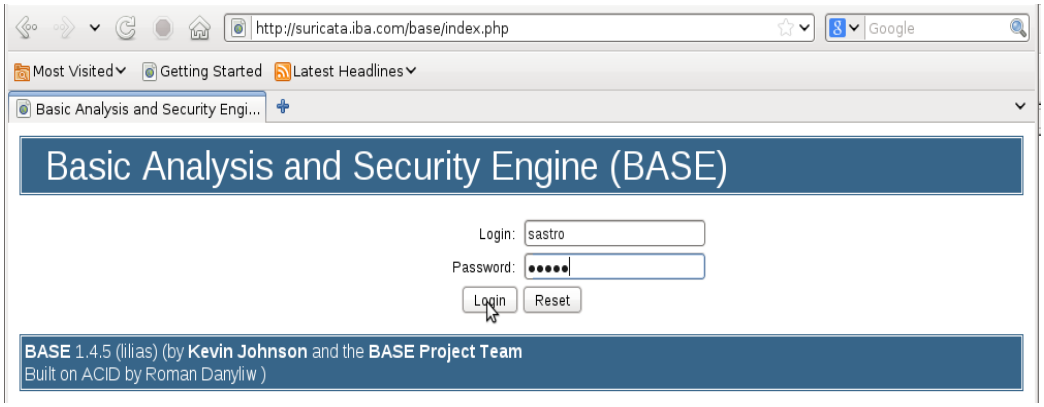
Gambar 5.36 *Settings BASE Create BASE AG*



(Sumber: Pengolah Sendiri)

Gambar 5.37 *Settings BASE step 4*

Setelah sukses men-*setting* maka akan tampil jendela login. Isi Login dan Password yang telah dibuat sebelumnya.



(Sumber: Pengolah Sendiri)

Gambar 5.38 Halaman awal pada saat *login*

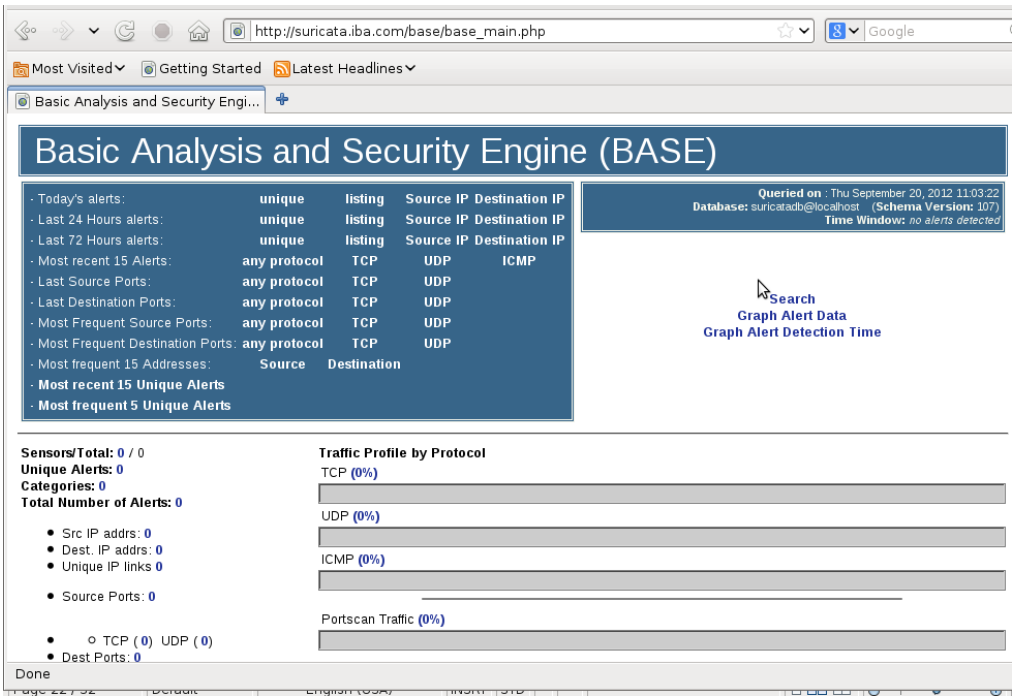
Dalam rangka mengamanan BASE sebaiknya ubahlah kembali hak akses di komputer server. Dengan mengetikan perintah :

```
root@debian:/home/server#chmod og-w base
```

(Sumber: Pengolah Sendiri)

Gambar 5.39 Penghilangan hak akses Base

Bila semua berjalan dengan baik maka akan tampil seperti dibawah ini:



(Sumber: Pengolah Sendiri)

Gambar 5.40 Hasil konfigurasi Suricata dan BASE

5.4.7 Konfigurasi awal sebelum melakukan serangan

Terdapat satu buah komputer *server* yang menjalankan sistem operasional Debian 6 yang akan memantau lalu lintas jaringan yang masuk dan keluar.

Terdapat pula dua buah komputer yang menjalankan sistem operasi windows xp. Komputer pertama sebagai klien monitoring yang berupa tampilan web gui dan komputer kedua sebagai *intruder* yang akan melakukan berbagai cara eksploitasi terhadap server.

5.4.8 Proses yang akan dilakukan penyerangan

Intruder digunakan untuk mengetes sistem, hal yang akan dilakukan *intruder* antara lain:

1. ***Scanner***

   Dengan melakukan *Port Scaning* yang bertujuan mencari informasi *port* yang terbuka mengunakan aplikasi NetTool sebagai awal dari bentuk serangan.

2. ***Denial of service (DOS)***

   a. *Ping Attack*, dengan tujuan meningkatkan kinerja sistem sampai batas maksimal *traffic* pada jaringan tersebut menjadi penuh dengan mengirimkan sebuah paket IP yang ukurannya lebih besar dari yang diizinkan oleh *protocol* IP yaitu 65.536 byte..

   b. TCP dan Udp *flooding*, serangan selanjutnya *intruder* melancarkan serangan terhadap *protocol* TCP dan UDP dengan

      mengunakan *tools hacking* Digiblast dengan mem-*flooding* TCP dan UDP tersebut, tujuannya membuat server *hang* atau *crash*.

5.4.9 Keluaran/hasil yang didapatkan

A. *Port scaning*, serangan berhasil jika penyerang berhasil mengdapatkan informasi tentang *port-port* yang terbuka pada server.

B. *Ping Attack*, serangan berhasil jika penyerang berhasil membanjiri *traffic* dan meningatkan kinerja sistem sampai batas maksimal sehingga sistem menjadi *hang* atau *crash*.

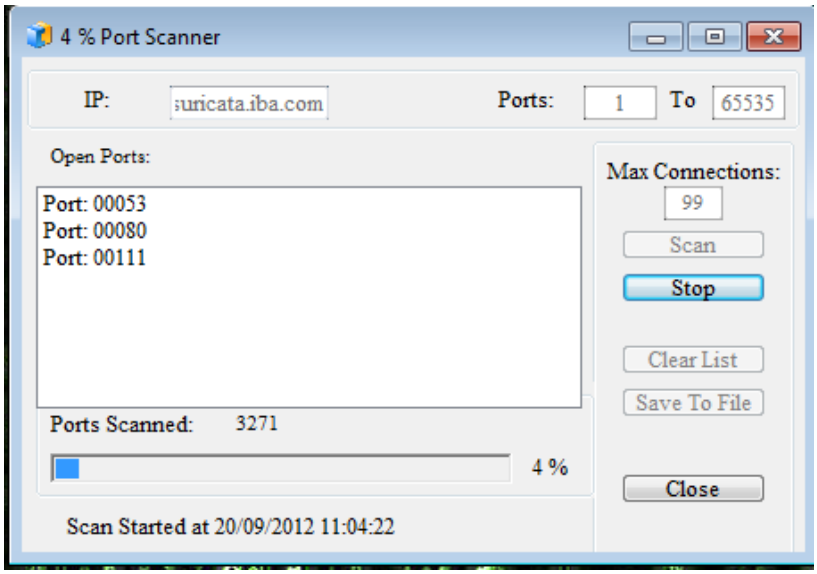
C. TCP dan UDP *Attack*, serangan berhasil jika penyerang berhasil mem-*flooding protocol* TCP dan UDP sehingga *server* menjadi *Hang*.

5.4.10 Pengujian Serangan

1.*Scanner*

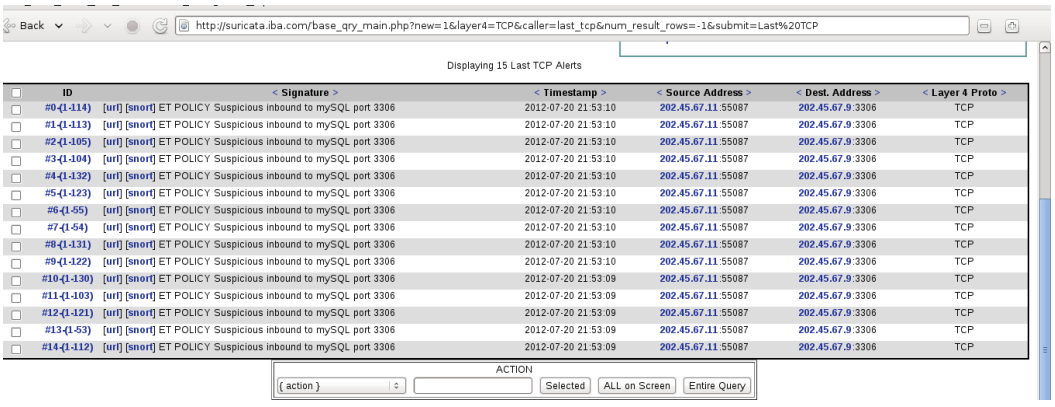
Scaner merupakan utillitas bantu untuk mendeteksi celah-celah keamanan.bertujuan memperoleh informasi mengenai *port* yang terbuka pada *server* teknis serangan yaitu dengan menjalankan aplikasi NetTool pilih *Port scanner*, sebelumnya dibutuhkan informasi alamat IP *server* sebelum menyerang. Setelah mengetahui alamat IP *server* kemudian ketikan alamat IP server pada *tools port scanning* dalam hal ini 202.45.67.21 kemudian lakukan *Scanning Port*, informasi mengenai *port-port* yang terbuka di *server*. Lakukan Pengujiannya yaitu *Intruder* mendapatkan

informasi mengenai informasi mengenai *port* yang terbuka antara lain : 80 ,53,111, .



(Sumber: Pengolah Sendiri)

Gambar 5.41 *Port Scaner*

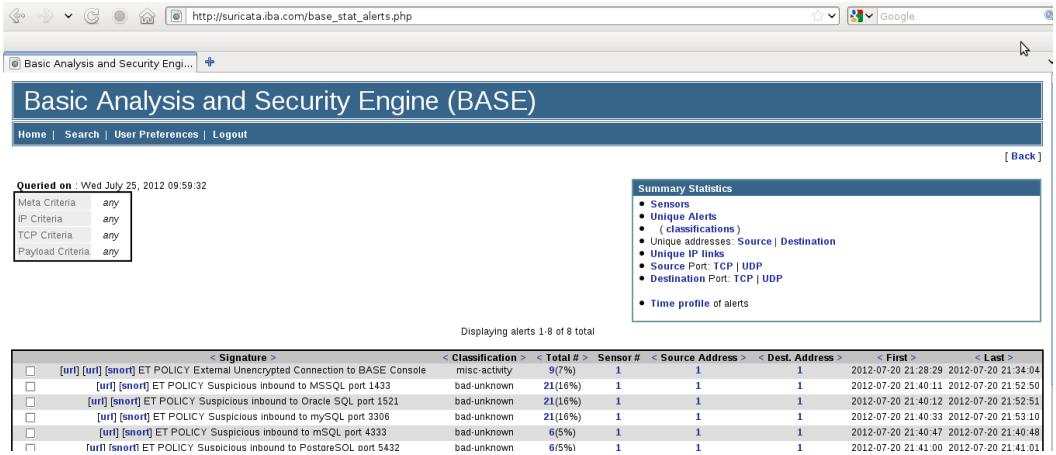


(Sumber: Pengolah Sendiri)

Gambar 5.42 Tampilan BASE setalah dilakukan *Port Scaning*

Tampak *alert/signature* diatas ada usaha untuk men-*scan* *port* yang terbuka pada server suricata.iba.com dari workstation

(intruder) suricata.iba.com dan diklasifasikan sebagai *unclassified* seperti terlihat dibawah ini :



(Sumber: Pengolah Sendiri)

Gambar 5.43 klasifikasi serangan setelah dilakukan *Port Scaning*

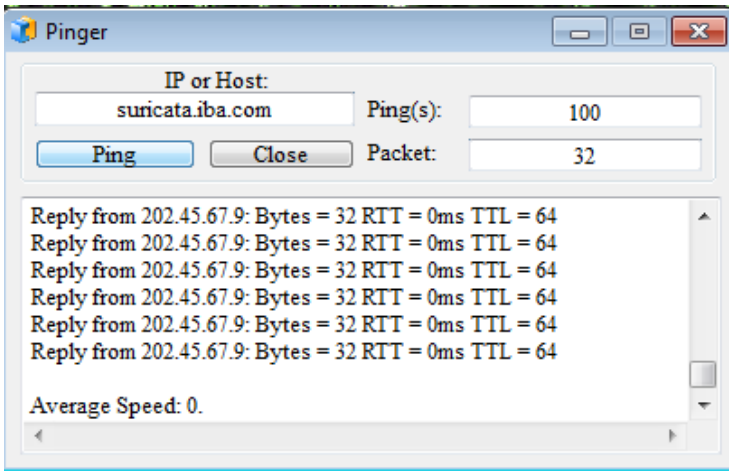
1. Denial of Service Attack (DOS)

Deskripsi singkat : DOS merupakan serangan yang dilancarkan melalui paket-paket tertentu, biasanya paket-paket sederhana dengan jumlah yang sangat banyak/besar dengan maksud mengacaukan keadaan jaringan target. Bentuk serangan yang akan dilancarkan yang di kategorikan DOS antara lain *Ping Attack, Syn Attcak* dan *TCP/UDP flooding.*

A. Ping Attack/Ping Of death

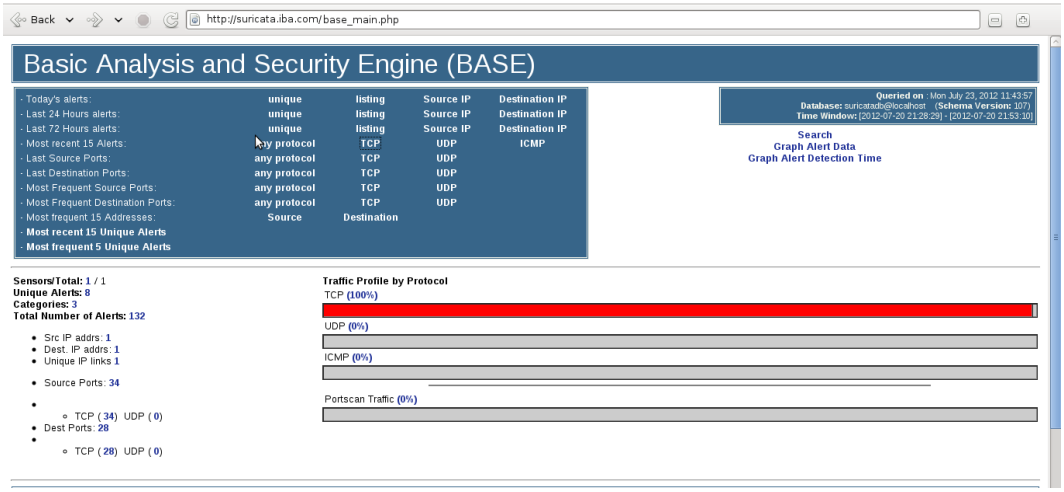
Eksploitasi program ping dengan memberikan paket yang ukuran besar ke sistem yang dituju, lebih besar dari yang diijinkan oleh protocol IP yaitu 65.536 byte bertujuan membuat sistem menjadi *crash atau hang*. Teknis serangannya dengan

cara masuk ke *command promt/cmd* kemudian lakukan *ping* IP alamat *server* dengan mengirimkan paket dengan ukuran besar dengan cara mengetikan perintah **Ping 202.45.67.9 –l 64000 –t** atau dengan cara dengan *Software* Net Tool pilih PING



(Sumber: Pengolah Sendiri)

Gambar 5.44 Percobaan *Ping Of Death*



(Sumber: Pengolah Sendiri)

Gambar 5.45 Tampilan *Home* pada BASE

B. TCP dan UDP Attack

TCP dan UDP Attack adalah suatu serangan dengan membanjiri *protocol* TCP dan UDP dengan permintaan pengiriman paket data, TCP dan UDP adalah dasar dari koneksi hal ini berarti koneksi langsung antara dua komputer untuk melakukan *transfer* data antara ke dua host bertujuan membuat sistem menjadi *crash* atau *hang*. Teknis serangan yaitu dengan menjalankan aplikasi Digiblast, setelah melakukan pencarian *port* yang terbuka dengan memasukan alamat IP target kemudian ketikan data yang akan dikirim untuk membanjiri *protocol*, kemudian pilih *protocol* yang akan di-*flooding* apakah TCP atau UDP saja atau keduanya.

5.4.11 Tindakan Pencegahan

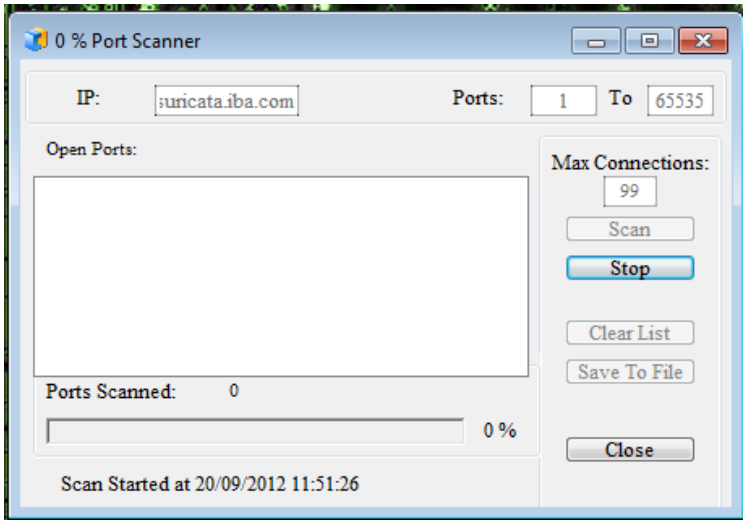
Setelah mendapatkan informasi mengenai ada usaha *port scanning, Ping Of death, Syn Attack, dan TCP/UDP Flooding* maka saya sebagai penulis melakukan tindakan pencegahan yaitu mengaktifan *iptable* yang berguna mencegah serangan-serangan dari *intruder* yaitu dengan cara mengetikkan *root@suricata:/home/febri# iptables -I INPUT -j NFQUEU*

```
root@debian:/home/server# iptables -I INPUT -j
NFQUEUE
```

(Sumber: Pengolah Sendiri)

Gambar 5.46 Menjalankan *IPTables*

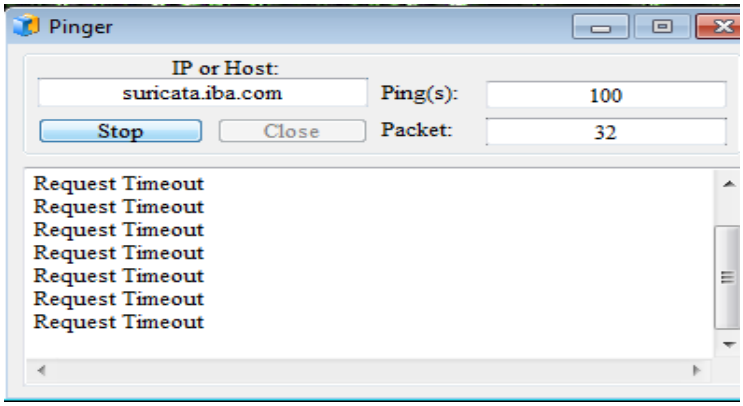
Rule diatas menerangkan tentang pencegahan menggunakan *IpTable*, penulis mencoba kembali melakukan Port Scaning dan hasilnya *Port scanner* tidak bisa mendapatkan informasi *port-port* yang terbuka.



(Sumber: Pengolah Sendiri)

Gambar 5.47 Percobaan *Port scanner* yang gagal

Kemudian kembali melakukan *Ping Of death*. gambar dibawah ini menunjukkan penolakan *ping attack* yang dilakukan PC klien.

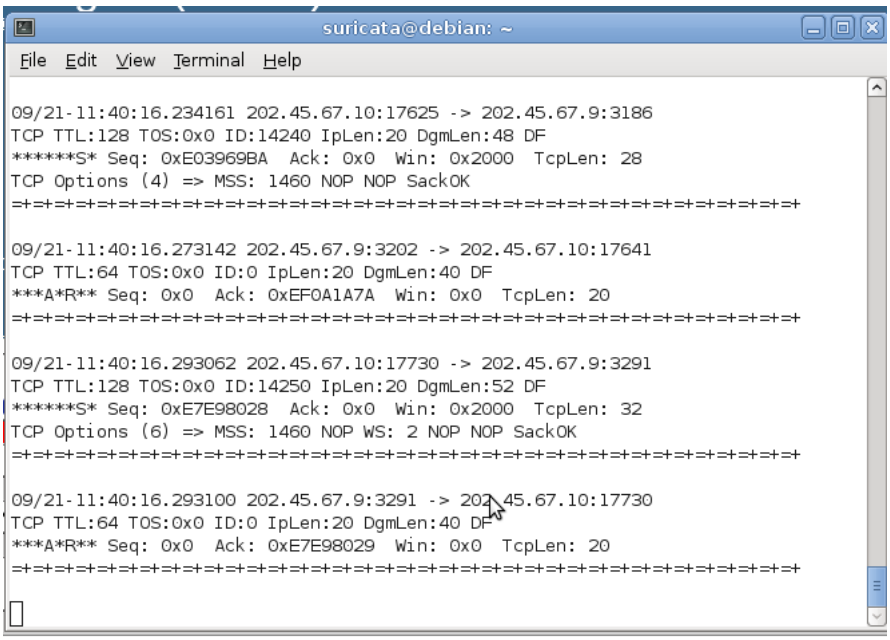


(Sumber: Pengolah Sendiri)

Gambar 5.48 *Ping Attack* yang gagal

5.5 Monitoring

Setelah implementasi tahapan monitoring merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengankeinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*. Dan kegiatan monitorng dapat dilihat pada gambar dibawah ini.



Gambar 5.49 Monitoring

5.6 Management

Tahap keenam dari NDLC adalah *management*. Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. *Policy* akan

sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau *alignment* dengan strategi bisnis perusahaan.

Dalam menjaga kualitas kemanan jaringan local pada Yayasan IBA palembang, penulis membuat *Intrusion detection system* (IDS) yang memadia guna meningkatkan kinerja karyawan dalam mengimplementasikan suricata yang telah di desian sedemikian rupa, dan agar dapat di jaga dan selalu di update rules-rulesnya.

BAB VI

SIMPULAN DAN SARAN

5.1 Simpulan

Setelah pnulis melakukan pembahasan tentang IDS, maka Penulis dapat menyimpulkan bahwa penggunaan *suricata* sebagai IDS dapat diimplementasikan pada jaringan komputer Yayasan IBA Palembang yang menggunakan topologi *star* dan *suricata* mampu untuk memantau pergerakan antara LAN. Adapun aplikasi *suricata* sebagai IDS pada Jaringan Komputer Yayasan IBA Palembang juga dapat mempermudah bagi *admin network* untuk mendapatkan data-data yang dapat meningkatkan kinerja dan mengamankan dari serangan-serangan pada jaringan lokal komputer Yayasan IBA Palembang. Sehingga *admin network* dapat mengambil kebijakan-kebijakan untuk memperbaikinya dengan berdasarkan data-data yang dihasilkan oleh *suricata* sebagai IDS (*Instrusion Detection System*).

5.2 Saran

Adapun Penulis juga memberikan saran yang kiranya dapat bermanfaat dalam meningkatkan kinerja dan keamanan pada jaringan komputer Yayasan IBA Palembang, yaitu:

1. Saran agar daftar *rule suricata* yang digunakan penulis selalu di-*update* menyesuaikan dengan kondisi, karena pola serangan-serangan baru memiliki *signature* yang baru.

2. Saran untuk pengembangan *server* ini, yaitu dengan mengembangkan fungsinya yaitu tidak hanya sebagai IDS (*Instrusion Detection System*), tetapi juga dapat sebagai IPS (*Instrusion Prevention System*) yang dapat bertugas sebagai aplikasi yang dapat bereaksi *secara real time* untuk mencegah kegiatan tersebut dengan berdasarkan data yang didapatkan oleh IDS.
3. Dan juga Penulis menyarankan agar dapat dilakukan perbaikan pada infrastruktur jaringan komputernya, mengingat adanya beberapa intrusi mengenai kegagalan komunikasi pada komputer pengguna.

DAFTAR PUSTAKA

Azwarnas. Desain Dan Implementasi *Network Intrusion Detection System* (IDS) Untuk Pengamanan Jaringan Komputer Lokal Pada Cv.Honda Union Motor. Skripsi sarjana, Program Studi Teknik Informatika STMIK PalComTech, Palembang, 2010.

Hasan, Iqbal. 2008. *Metode Penelitian dan Apliaksinya*. Bogor : Ghalia Indonesia.

James E. Goldman, Philips T. Rawles, Third Edition, 2001, *Applied Data Communications, A business-Oriented Approach,* , John Wiley & Sons

Kuncoro, mudrid. 2009. *Metode riset untuk bisnis dan ekonom*i. Edisi 3. Jakarta: Erlanga

Mahmud. Desain Dan Implementasi *Network Intrusion Detection System* (NIDS) Dengan *Snort* Pada Jaringan Komputer Stimik Palcomtech Palembang. Skripsi sarjana, Program Studi Teknik Informatika STMIK PalComTech, Palembang, 2010.

Nugroho, Adi.Analisa dan Perancangan Sistem Informasi dengan metologi Berorientasi Objek, Penerbit Informatika, Bandung.

Rafiudin, Rahmat. 2010. *Menggayang Hacker Dengan Snort.* Jakarta: Andi Publisher.

Schmidt, KM, 2003, *Public subsidies for open source?* - Harvard Journal of Law & Technology, 2003 - lecg.com

Sukarno, Edy. 2002. *Sistem Pengendalian Manajemen: Suatu Pendekatan Praktis*. Jakarta: PT. Gramedia Pustaka Utama

Supriyanto, Aji. 2007. *Pengantar Teknologi Informasi*. Jakarta: Salemba Infotek.

Sofana, Iwan. 2011. *Tiori dan Module Pratikum Jaringan Komputer***.** Bandung Module.

Thomas, Tom. 2005. Network Security First step. Penerbit Andi, Yogyakarta.

Thomas, Tom. 2005. Computer Networking First-step, Computer Networking First-step.Penerbit Andi, Yogyakarta.

Umar. 2007, *Metode untuk Skripsi dan Tesis Bisnis*. Jakarta: Raja Garfindo Persada.

Wagito. 2007. *Jaringan Komputer Teori dan Implementasi Berbasis Linux.* Jakarta: Gava Media.