MEMBANGUN INTRUSION DETECTION SYSTEM PADA WINDOWS 2003 SERVER

Dony Ariyus[1]dan Jazi Eko Istiyanto[2]
[1] STMIK AMIKOM YOGYAKARTA
[2]FMIPA UGM Yogyakarta

Abstract

This paper presents How to build intrusion detection system in windows 2003 server that aim to detect intruder in computer's network. Building intrusion detection system wants many components to support one to another, that:
Winpcap, Snort Php, Microsoft Sql 2000, Base, Adodb, Phplot, Jpgraph, Apahce

System that build can capture the packet from network and done decode, normalization, detection engine for pattern's identifications and give output in the form of alert or file's log to user. Detection's process that done by using anomaly detection and misuse detection so that possibility from not detection a packet be slimmer

Keywords*: Intrusion Detection System, Snort, Anomaly detection, Misuse detection*

1. Pendahuuan

Faktor keamanan merupakan suatu hal yang mutlak dalam membangun suatu jaringan. Pada dasarnya sistem keamanan yang dimiliki oleh sistem operasi tidaklah cukup untuk mengamankan suatu jaringan komputer.

Peran utama untuk mencegah terjadinya kejahatan komputer perlu dilakukan pengamanan yang berlapis-lapis pada suatu jaringan komputer, seperti firewall yang berfungsi mengatur TCP/IP dan port-port yang mana diizinkan atau tidak untuk melewati jaringan. Keamanan yang terdapat di sistem operasi juga berfungsi untuk menghalangi dan memperlambat suatu serangan untuk mendapatkan akses layaknya sebagai super user.

System keamanan tersebut tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator tidak bisa mengetahui dengan pasti apa yang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk mengaudit sistem guna mencari permasalahan yang telah terjadi.

Untuk mengatasi masalah tersebut dibutuhkan suatu tool yang mampu mendeteksi lebih awal terjadinya intruder atau kegiatan yang merugikan suatu jaringan. *Intrusion Detection System* merupakan suatu solusi yang sangat tepat untuk keperluan tersebut.

Salah satu IDS (*Intrusion Detection System*) yang sangat populer dalam keamanan IT adalah snort. Snort dibuat dan dikembangkan pertama kali oleh Martin Roesh pada bulan November 1998, lalu menjadi sebuah open source project. Bahkan di situs resminya *www.snort.org* mereka berani mengklaim sebagai standar "intrusion detection/prevention". Snort merupakan IDS yang sangat populer dan cukup ampuh digunakan para hacker dan admin di seluruh dunia.

Untuk membangun Intrusion Detection System dengan menggunakan snort sebagai alat deteksi bukanlah hal yang mudah, karena banyak permasalahan yang terdapat pada sistem snort itu sendiri. Hal ini disebabkan snort masih dalam tahap pengembangan lebih lanjut. Menbangun Intusion Detection system pada sistem operasi windows 2003 server dibutuhkan beberapa komponen tambahan supaya alert dan log bisa tersimpan dengan database.

2. Pembahasan

Penelitian yang dilakukan merupakan penelitian pustaka yang akan didukung oleh penelitian eksperimentasi dengan membangun suatu intrusion detection system pada windows 2003 server

2.1 Intrusion Detection System

Intrusion detection system (IDS) merupakan detector serangan yang akan menganggu sebuah jaringan, kemampuan dari IDS memberikan peringatan kepada administrator saat terjadi sebuah aktifitas tertentu yang tidak diinginkan. Selain memberikan peringatan, IDS juga mampu melacak source IP sebuah system attacker. Suatu IDS akan melakukan pengamatan (monitoring) terhadap paket-paket yang melewati jaringan dan berusaha menemukan apakah terdapat paket-paket yang berisi aktifitas mencurigakan dengan mengacu pada pola serangan yang terdapat pada signature dan rule yand disimpan di dalam database sehingga administrator bisa melakukan tindakan pencegahan dari apa yang pernah terjadi.

2.2 Perancangan Sistem Intrusion Detection System

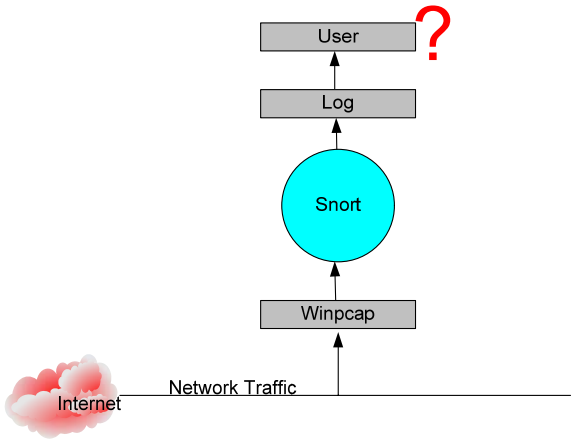
Perancangan sistem yang akan digunakan untuk membangun *Intrusion Detection System*, terlebih dahulu yang dilakukan adalah mengumpulkan komponen yang akan digunakan sebagai IDS. Pada dasarnya snort dan winpcap sudah bisa untuk medeteksi paket yang melintasi jaringan komputer tapi tidak hal seperti ini yang akan dibangun. IDS yang akan dibangun adalah IDS yang bisa menyimpan alert dalam database dan setup otomatis jika komputer di hidupkan. Untuk mendapatkan IDS yang seperti itu dalam penelitian ini menggunakan beberapa komponen tambahan yang memudahkan user dalam menggunakan IDS. Komponen-komponen yang digunakan adalah:

a) Snort http://www.snort.org/
b) Winpcap http://www.winpcap.org/
c) SQL Server 2000 http://www.microsoft.com/sql
d) BASE http://secureideas.sourceforge.net/
e) PHP http://www.php.net/
f) Apache http:// Apache.net
g) ADODB http://adodb.sourceforge.net/
h) PHPlot http://sourceforge.net/projects/phplot/
i) Jpgraph http://www.aditus.nu/jpgraph/jpdownload.php

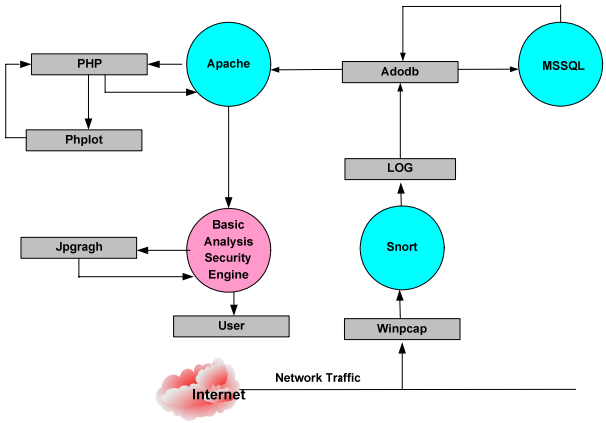
Umumnya IDS dibangun hanya dibutuhkan 2 (dua) komponen tambahan yaitu snort dan winpcap kedua komponen tersebut berfungsi sebagai driver capture paket dan detektor engine, jika IDS hanya

menggunakan winpcap dan snort, sulit bagi administrator untuk menganalisis alert atau log, walaupun itu disimpan di dalam hardisk. Hubungan snort dan winpcap seperti digambarkan pada gambar 1

Pengembang lebih lanjut dari sistem *Intrusion Detection System*, memerlukan berbagai tool tambahan, sehingga IDS lebih user friendly sehingga alert lebih terorganisir dan mudah untuk dimengerti seperti digambarkan pada gambar 2.



Gambar 1 Snort dengan Winpcap



Gambar 2 Architecture Intrusion Detection System

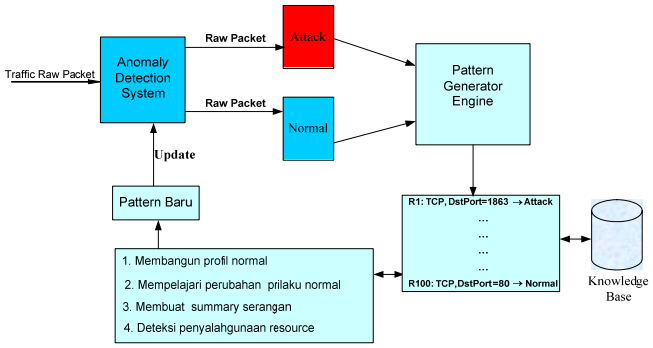
Winpcap mengirim packet capture ke snort untuk dianalisis oleh system engine, output plugin snort akan mengirim alert ke database yang mana variable dari database telah didefinisikan pada snort config. File log dan alert akan disimpan di dalam database pengimplementasian menggunakan BASE, tapi terlebih dahulu harus ada penghubung antara database dengan web server yaitu Adodb. Untuk melihat alert pada base console dibutuhkan php sebagai penghubung ke Basic Analysis Security Engine (BASE).

2.3 Intrusion Detection System Mengenali Adanya Intruder

Penyusupan (intrusion) didefinisikan sebagai kegiatan yang bersifat anomaly, incorrect atau inappropriate yang terjadi di jaringan atau di host. Pada Intrusion Detection System, pengenalan terhadap intruder dibagi menjadi dua bagian:

1. Knowledgebased atau misuse detection : mengenali adanya penyusup dengan cara menyadap paket data kemudian membandingkannya dengan database rule (berisi signature-signature serangan) jika paket data mempunyai pola yang sama atau setidaknya salah satu pola terdapat di database rule, maka di anggap adanya serangan
2. Behavior based atau anomaly based : Mengenali adanya penyusup dengan mengamati adanya kejanggalan-kejanggalan pada system, atau adanya penyimpangan–penyimpangan dari kondisi normal, sebagai contoh ada penggunaan memori yang melonjak secara terus menerus atau koneksi parallel dari 1 (satu) port IP dalam jumlah yang banyak dan dalam waktu yang bersamaan.

Rule dan signature hanya berisi pola serangan yang selalu di update secara rutin, karena ada serangan baru setiap hari. Proses deteksi anomaly tidak menggunakan rule dan signature , hanya mengamati kondisi normal dari sistem jaringan, jika suatu waktu kondisi dari jaringan tidak normal, hal seperti ini dianggap sebagai suatu serangan. Keunggulan dari sistem deteksi ini bisa mengenali serangan baru yang polanya tidak ada pada rule dan signature hasil dari pembelajaran sistem deteksi itu sendiri. Pembelajaran sistem anomaly Seperti gambar 3 dibawah ini:



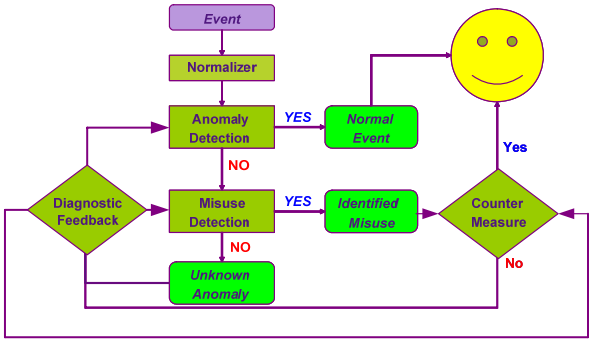
Gambar 3 Proses Pembelajaran System Deteksi Anomaly

Kekurangan dari system deteksi anomaly ini adalah banyaknya alert false positive yang yang dikirim ke user. Contoh jika suatu waktu server menerima banyak request dari true client internal dan kinerja system meningkat dengan cepat (memory, prosesor), maka system deteksi akan melaporkan sebagai serangan.

IDS yang dibangun menggunakan dua system deteksi ini untuik mengatasi masalah serangan yang terjadi, jika suatu pola serangan tidak ada pada rule dan signature, maka system deteksi anomaly berfungsi untuk mencari pola serangan baru.

Proses logika pengenalan paket dengan sistem anomaly detection dan misuse detection dapat di ilustrasikan pada gambar 4 dibawah ini

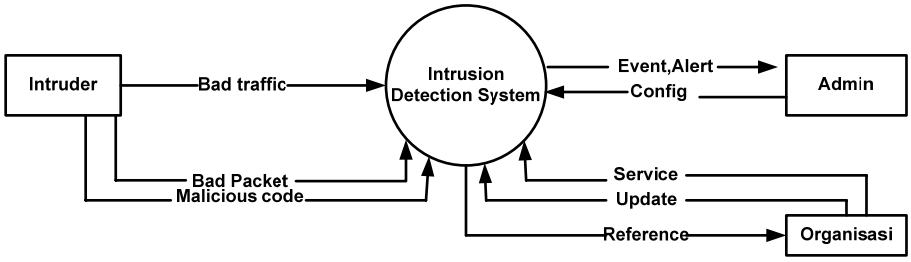
Arsitektur dari kedua system ini dalam mendeteksi suatu paket atau event mempunyai tiga proses yaitu: detection anomaly, misuse detection, dan diagnosis feedback, hal ini memungkin snort bisa mengenali jenis serangan yang baru, seperti dijelaskan pada gambar 5 dibawah ini



Gambar 5 Architecture Proses Anomaly Detection dan Misuse Detection

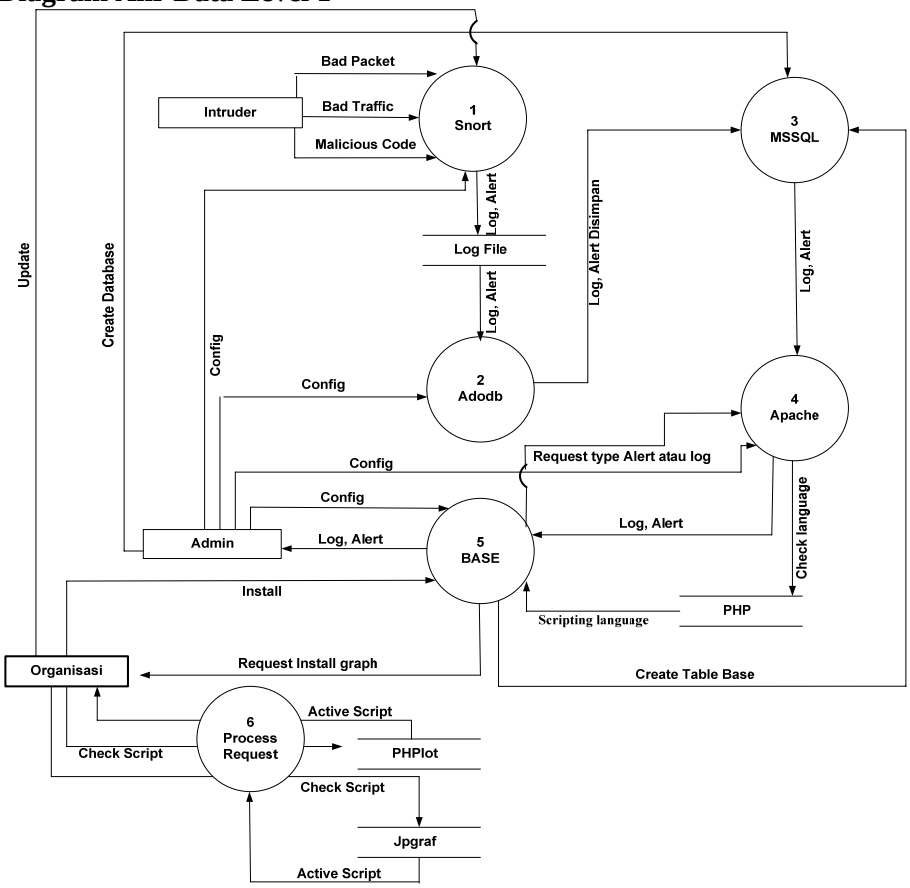
2.4 Data Flow Diagram

Diagram konteks dari intrusion detection system, mengambarkan secara umum proses dari intrusion detection system, semua data yang berasal dari luar jaringan akan diproses di intrusion detection system, dengan output alert ke user (administrator),



Gambar 6 Diagram Konteks

Diagram Alir Data Level 1

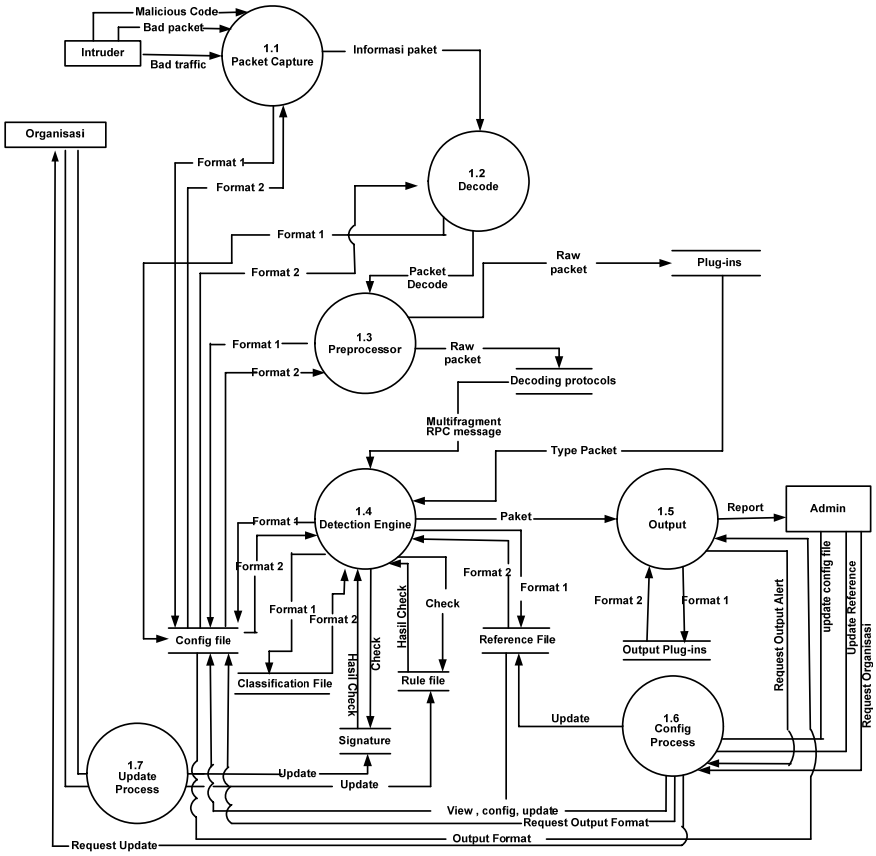


Gambar 7 Diagram Alir Data Level 1

DAD Level 1 merupakan perluasan dari DAD level 0 yang terdapat 5 proses yaitu Snort, Adodb, MSSQL, Apache, dan Base. Kelima proses tersebut di configurasi oleh admin. Log dan alert yang telah di deteksi di simpan pada file log yang kemudian akan disimpan pada MSSQL dengan perantara Adodb sebagai Database Abstraction Library. Log dan alert di

analisis pada BASE dengan menggunakan perantara Apache sebagai web server dengan menggunakan bahasa script PHP. BASE merupakan berfungsi sebagai interface untuk menganalisis log dan alert.

Diagram Alir Data Level 2



Gambar 8 Diagram Alir Data Level 2 Proses 1

DAD level 2 seperti yang diperlihatkan pada gambar 8 merupakan perluasan dari DAD level 0. pada gambar tersebut proses dibagi menjadi 5

bagian, masing-masing adalah proses capture, decode, preprosesor, detection engine, output.

Packet dari internet yang dikirim kejaringan di capture oleh packet capture dan kemudian dilakukan pencodean seperti binary, ASCII, Hex, hasil dari pencodean akan diproses di preprocessor untuk disaring kembali protocol dari paket tersebut. Hasil Dari proses preprocessor akan dideteksi untuk mengenali pola-pola serangan yang terdapat pada signature dan rule, jika paket memiliki pola yang sama dengan signature dan rule, informasi tersebut akan dikirim ke admin dengan menggunakan output plugin

2.5 Implementasi

Implementasi dari IDS adalah mendeteksi kemungkinan bad traffic yang melintasi suatu jaringan komputer.Fungsi dasar dari IDS itu sendiri mengumpulkan kode-kode dari suatu paket yang polanya dikenali dari rule dan signature yang disimpan di dalam suatu forder dalam bentuk file log kemudian di transfer ke database dengan menggunakan fasilitas adodb.

File log yang disimpan bisa dipelajari untuk melakukan antisipasi pada kemudian hari, supaya yang telah terjadi tidak terulang lagi.

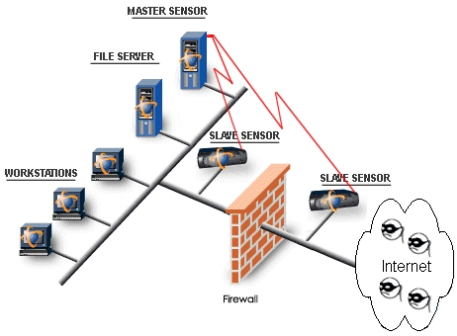
Pada dasarnya suatu intrusion detection system yang berjalan pada platform DOS dan paket capture juga dapat dilihat pada platform DOS, secara manual file log bisa disimpan pada folder log yang ada dalam subdirectory IDS.

Dengan alasan tidak user interface, maka dikembangkan oleh beberapa programmer supaya IDS lebih friendly dan user interface. Tapi untuk mendapatkan hal tersebut dibutuhkan komponen-komponen lain yang mendukung seperti PHP, BASE, PHPlot, JPgraph, Apache, adodb, Mssql. Issue yang berkembang di mailing list, banyak terdapat masalah dalam melakukakan installasi sistem, karena komponen-komponen yang mendukung belum tentu cocok satu dengan lainnya, jadi untuk mendapatkan suatu server yang bisa melakukan detection terhadap paket yang masuk dan menyimpannya alert dan log ke dalam database harus melakukan trial dan error.

Masalah yang sering terjadi dalam mendisain sistem adalah konfigurasi antara satu komponen dengan komponen lainnya, dan versi sistem operasi yang digunakan, perbedaan yang sangat mendasar dalam membangun IDS terhadap versi sistem operasi sangat mencolok, antara

freebsd, linux, dan windows, dari versi sistem operasi ini, konfigurasi terhadap sistem operasi windows lebih rumit dibandingkan dengan sistem operasi lainnya, dikarenakan disain IDS untuk windows diperlukan banyak cara, dan metode baik dari service yang digunakan dan registry yang perlu didaftarkan atau ditambahkan.

Sensor pada IDS bisa dibangun sebanyak mungkin tergantung dari sumber daya yang digunakan. Pada umumnya snort mempunyai dua macam sensor yaitu master dan slave



Gambar 12 Ilustrasi Sensor Snort

Pada dasarnya sensor merupakan awal snort untuk menganalisis paket yang masuk ke suatu jaringan komputer. Eternet card yang digunakan melakukan capture paket jaringan dengan menggunakan driver serta software winpcap.

2.6 Intrusion Detection System Menggunakan Consule

Snort menggunakan consule, memerlukan komponen tambahan yang saling support satu dan yang lainnya. Penggunaan consule untuk melihat hasil deteksi yang dilakukan snort lebih efektif dan user friendly.

Snort akan mengirim semua proses yang telah dilakukan untuk disimpan dalam file log yang terletak pada D: snort\log, kemudian dikirim ke database mssql dan kemudian dilihat pada BASE (Basic Analysis Security Engine).

Untuk keperluan snort consule diperlukan perintah di bawah ini dimasukkan ke dalam snort.conf pada bagian *"database: log to a variety of databases" Output database: log, mssql, user=snortuser password=12345 dbname=IDSCenter host=localhost port=1433 sensor_name=WinIDS*

- Log: tempat penyimpan file paket yang telah dicapture oleh snort log file akan disimpan pada subdirectory log yang ada pada directory snort.
- Mssql: adalah versi database yang digunakan untuk penyimpan alert yang dikirim melalui log file sehingga file log bisa di analisis lebih mudah dengan menggunakan interface lain.
- User : user yang digunakan untuk database
- Password : password yang digunakan untuk database
- Dbname : nama database untuk menyimpan data
- Host : host yang digunakan untuk capture data
- Port : port yang digunakan
- Sensor_name : nama sensor

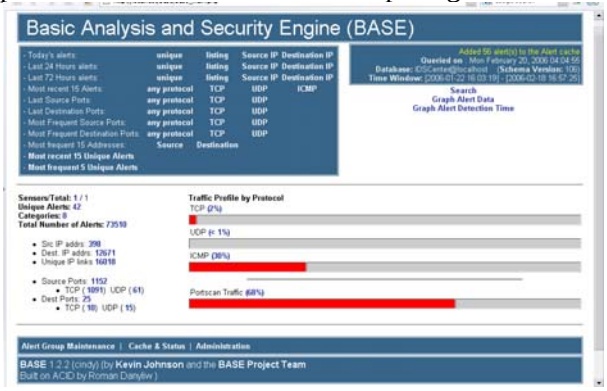
Sedangkan pada BASE hanya memberikan menukar atau mengisi perintah sebagai berikut yang terdapat pada base_conf.php pada bagian "Alert DB connection parameters" dengan menambahkan hal-hal sebagai berikut:

```
$alert_dbname   = "IDSCenter";
$alert_host     = "localhost";
$alert_port     = "";
$alert_user     = "base";
$alert_password = "678910";
```

Untuk dapat saling terkoneksi satu dengan yang lainnya dibutuhkan adodb untuk dikonfigurasi pada base dan php. Adodb merupakan jembatan antara database dengan BASE melalui brige php dan web server.

```
$DBlib_path = "d:\win-ids\adodb";
```

Serta PHP sebagai bahasa script untuk menampilkan interface bagi BASE consule.Tampilan awal dari BASE consule seperti gambar di bawah ini:



Gambar 13 Main BASE Console

Untuk memastikan base consule sudah benar-benar aktif bisa dilihat pada consule informasi yang terletak pada sudut sebelah kiri

3. Penutup

Kesimpulan dari penelitian ini adalah:

1. Membangun, Instalasi serta configurasi Intrusion Detection System pada Windows 2003 Server mengalami banyak kendala
2. IDS dengan menggunakan windows 2003 server membutuhkan banyak tambahan value dalam registry supaya IDS dapat bekerja sebagai mana mestinya
3. Membangun IDS dengan database dibutuhkan beberapa komponen supaya alert bisa disimpan dalam database, komponen tersebut seperti: MSSQL 2000 Sp4, PHP5, BASE versi 1.2.2 (Cindy), Adodb versi 4.68, Apache versi 2.0, JpGraph Versi 2.0beta, Phplot 5rc2.
4. Update rule dan signature dilakukan secara teratur, supaya IDS dapat mengenali serangan-serangan baru
5. Sistem detection IDS menggunakan dua metode yaitu metode Misuse detection dan Anomaly detection
6. Banyak terdapat alert false positive yang diakibatkan oleh pembelajaran dari system anomaly detection
7. IDS bisa mengenali type serangan baru dengan Detection Anomaly
8. File Config snort merupakan brain dari IDS, karena semua kinerja dan variable komponen didefinisikan di sini, seperti network varible, decode, preprocessor,output,rule, serta database
9. Analisis alert lebih mudah dilakukan dengan menggunakan BASE (Basic Analysis Security Engine), karena Base lebih user interface
10. BASE perlu ditambah plugin graph dengan menggunakan phplot jpgrafh yang di install langsung melalui jaringan internet
11. Sensor IDS secara umum yaitu ethernet card, web server, dan snort itu sendiri
12. Firewall membantu IDS untuk memblocking port-port yang dicurigai

Dengan keterbatasan kemampuan dan waktu yang tersedia untuk penelitian ini, maka penulis hanya membahas membangun suatu IDS dengan sistem operasi windows server 2003 dan melakukan konfigurasi sehingga alert bisa disimpan di dalam database. Mencoba komponen-komponen

tambahan yang bisa support satu dengan yang lainnya. Untuk mencapai suatu Sistem Intrusion Detection System berfungsi secara maksimal, maka penulis menyarankan beberapa hal:

1. Instalasi IDS dan komponen tambahan seharusnya menggunakan versi yang terbaru, karena issue keamanan telah diperbaiki
2. Menggunakan sensor dalam bentuk fisik Marauder - SL-Series IDS Sensors
3. Untuk memudahkan update rule dan signature, dibutuhkan program tambahan seperti Oinkmaster
4. Aktif dalam forum snort untuk mendapatkan informasi yang terbaru dan issue keamanan jaringan
5. Snort menggunakan IPS yang berfungsi sebagai pembaca alert yang akan mengirim perintah ke firewall untuk menutup port-port tertentu.
6. Snort masih perlu dikembangkan lebih lanjut, karena masih banyak terdapat kelemahan pada sistem detection khususnya anomaly detection

Daftar Pustaka

Amruta Inamdar, 2003," Intrusion Detection Systems and a Case Study of SNORT", University of Minnesota

Andry Haidar, 2004," Studi Kasus Mengenai Aplikasi Multilayer Perceptron Neural Network Pada Sistem Pendeteksi Gangguan (IDS) Berdasarkan Anomali Suatu Jaringan" Teknologi Informasi Program Pasca Sarjana Teknik Elektro Institut Teknologi Bandung

Ariyus, Dony., 2006, Membangun Intrusion Détection Pada Windows 2003 Server, Tesis, Sekolah Pascasarjana Program Studi Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.

Baker, Andrew R.and team, 2004," Snort 2.1 Intrusion Detection, Second Edition" Syngress Publishing, Inc, United States of America

Bruce Perens' Open Source Series, Intrusion Detection with SNORT - Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID

Donetti, John and Scott Elko, 2005, Network Intrusion Detector
URL: http*://ciac.llnl.gov/cstc*

Endorf, Carl Eugene and Mellander Jim., 2004, Intrusion Detection & Prevention, California, McGraw-Hill

Escamilla, Terry, 2003, Intrusion Detection: Network Security beyond the Firewall third edition, New York *John Wiley & Sons, Inc*

Honeycutt, Jerry, 2003" Microsoft Windows XP Registry Guide, Microsoft Press,United States of America.

Horton, Mike and Mugge Clinton., 2003, Network Security Portable Reference, California, McGraw-Hill

Innella, Paul, 2001, "The Evolution of Intrusion Detection Systems" URL: http://www.securityfocus.com/infocus/1514

Jacob Babbin, Simon Biles, Angela D. Orebaugh, 2005," Snort Cookbook" O'Reilly United States of America.

Jae K. Shim, Ph.D.and Anique A. Qureshi, Ph.D., CPA, CIA, 2002, The International Handbook of Komputer Security, The Glenlake Publishing Company, Ltd, Unite State of America

Kerry J.Cox, Christopher Gerg, 2004," Managing Security with Snort and IDS Tools" O'Reilly, United States of America

Rowton, Mitchell, 2005, Introduction to Network Security - Intrusion Detection, URL: http://www.securitydocs.com/library/3009

Snort™ Users Manual 2.4.0RC1 The Snort Project 16th September 2005 URL: www. Snort.org

Steele, Michael E," January 8, 2006, Master/Single - Windows Intrusion Detection System (WinIDS), Document Version 1.3