APTIKOM

AMIK TUNAS BANGSA

PROSIDING

Seminar Nasional Ilmu Komputer

Pematangsiantar, 31 Agustus - 2 September 2012

snikom 2012
seminar nasional ilmu komputer

Data Warehouse & Pemanfaatannya

dalam Pengolahan Pangkalan Data Perguruan Tinggi

editor :
Prof.Dr. Muhammad Zarlis, Rahmat W. Sembiring, M.Sc.IT., Dedy Hartama,S.T.,M.Kom
Muhammad Ali, MLS., Muhammad Syafii, M.Kom

ISBN 978-602-18749-0-5

Diterbitkan oleh:
AMIK TUNAS BANGSA PEMATANGSIANTAR

Didukung Oleh:
Asosiasi Perguruan Tinggi Informatika dan Ilmu Komputer (APTIKOM)
PT. Telkom Indonesia, Tbk

Seminar Nasional Ilmu Komputer (SNIKOM)
Printed in Indonesia, Agustus 2012

Panitia Pengarah:

Prof. Dr. Herman Mawengkang

Prof. Dr. Richardus Eko Indrajit

Prof. Dr. Zainal Hasibuan

Prof. Dr. Muhammad Zarlis

Prof. Dr. Opim Salim Sitompul

Dr. Poltak Sihombing

Dr. Zakarias Situmorang

Dr. Benny B. Nasution

Daftar Isi

Rekayasa Perangkat Lunak

Sistem Terdistribusi

IMPLEMENTASI PEMROGRAMAN JAVA UNTUK ALERT INTRUSION DETECTION SYSTEM

Fadhila Nisya Tanjung[1], Muhammad Irwan Padli Nasution[2]

[1] Sekolah Tinggi Teknik Harapan Medan

[2] IAIN Sumatera Utara Medan

Abstrak

Kemajuan teknologi informasi dengan ditemukannya internet telah membuat manusia dapat berkomunikasi satu dengan lainya di belahan dunia manapun tanpa dibatasi oleh wilayah ruang dan waktu yang berbeda.. Perkembangan ini telah membawa pengaruh yang sangat besar bagi tatanan sosial, budaya dan etika dalam masyarakat global. Permasalahan keamanan informasi menjadi menempati pada posisi yang sangat penting, apalagi bila dikaitkan bahwa sekarang informasi merupakan suatu komoditi. Untuk selalu mencapai tingkat kehandalan perlu selalu dimutakhirkan tingkat sistem sekuriti sehingga akan terhindar dari pencurian informasi maupun pengrusakan informasi. Sebuah Intrusion Detection System (IDS) sangat diperlukan untuk memberikan peringatan dini kepada administrator saat terjadi sebuah aktifitas tertentu yang mencurigakan dengan mengacu pada pola serangan yang terdapat pada signature atau rule, sehingga administrator dapat melakukan tindakan pencegahan. Dengan pemrograman Java dapat dikembangkan sebuah interface sehingga alert dari IDS tersebut dapat diterima administrator melalui sebuah pesan singkat (SMS).

Kata kunci: ***internet, informasi, Java, security, SMS***

1. Pendahuluan

Terhubungnya LAN atau komputer ke Internet telah membuka potensi adanya lubang keamanan *(security hole)* yang tidak dapat ditutupi dengan mekanisme keamanan secara fisik. Dengan membuat sistem keamanan komputer maka akan melindungi data dan informasi agar tidak dapat dibaca oleh orang yang tidak berhak serta mencegah agar orang yang tidak berhak tidak dapat menyisipkan atau menghapusnya. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan tersebut. Para administrator tidak mampu mengetahui dengan cepat apa yang telah terjadi, sehingga dibutuhkan waktu yang cukup lama untuk mengaudit sistem guna mencari permasalahan yang telah terjadi. Untuk mengatasi masalah tersebut dibutuhkan suatu *tools* yang mampu mendeteksi lebih awal terjadinya serangan atau kegiatan yang merugikan suatu jaringan. *Intrusion Detection System* merupakan suatu solusi yang sangat tepat untuk keperluan tersebut. Selain daripada itu sistem deteksi intrusi ini akan berfungsi secara maksimal jika ada seorang administrator yang terus memonitor jaringan, jika tidak maka peringatan / *alert* yang dikeluarkan tidak akan terbaca dan tindakan pencegahan pun tidak bisa di lakukan. Akan demikian masih diperlukan sebuah interface lainnya sehingga jaringan dapat terus termonitor. Dengan pemrograman *Java* dapat dikembangkan sebuah antar muka untuk melakukan pengiriman alert *Intrusion Detection System* melalui sebuah SMS kepada administrator

sehingga administrator dapat melakukan tindakan yang diperlukan untuk mengamankan jaringan. Dengan demikian akan memudahkan administrator untuk memonitor jaringan dimanapun ia berada.

2.Keamanan Informasi

Pada dasarnya seorang pengguna komputer sangat membutuhkan rasa kenyamanan ketika sedang mengoperasikannya. Kenyamanan tersebut dapat diperoleh salah satunya dari keamanan sistem yang dipakai. Berbicara mengenai keamanan sistem, ada dua hal yang sering diperdebatkan yaitu mengenai istilah keamanan dan proteksi. Pertama-tama harus dapat dibedakan antara keamanan dengan proteksi. Proteksi biasanya menyangkut faktor -faktor internal sistem yang ada di dalam komputer. Sebenarnya tujuan dari proteksi adalah untuk mencegah penggunaan akses-akses yang tidak seharusnya (*accidental access*). Akan tetapi keamanan mempertimbangkan faktor-faktor eksternal (lingkungan) di luar sistem dan faktor proteksi terhadap sumber daya sistem. Melihat perbedaan ini, terlihat jelas bahwa keamanan mencakup hal yang lebih luas dibandingkan dengan proteksi. Dengan mempertimbangkan aspek-aspek tersebut sehingga dibutuhkanlah suatu keamanan sistem untuk menanggulangi kemungkinan akses data penting (rahasia) dari orang-orang yang tidak seharusnya mengakses data tersebut. Akan tetapi, dalam kenyataannya tidak ada satu sistem komputerpun yang memiliki sistem keamanan sempurna. Dengan demikian, setidaknya terdapat suatu mekanisme tersendiri untuk mencegah ataupun mengurangi kemungkinan-kemungkinan gangguan terhadap keamanan sistem. Sistem operasi hanya satu porsi kecil dari seluruh perangkat lunak pada sistem. Tetapi karena peran sistem operasi mengendalikan pengaksesan ke sumber daya, jika perangkat lunak lain meminta pengaksesan, maka sistem operasi menempati posisi yang penting dalam pengamanan sistem. Keamanan sistem terbagi menjadi 3, yaitu:

1. Keamanan eksternal (*External Security*),
   Berkaitan dengan pengamanan fasilitas komputer dari penyusup, bencana alam, dll.
2. Keamanan *Interface* Pemakai (*User Interface Security*),
   Berkaitan dengan identikasi pemakai sebelum mengakses program dan data.
3. Keamanan *Internal* (*Internal Security*),
   Berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi untuk menjaga integritas program dan data.

2.1 Aspek Ancaman Keamanan

Serangan terhadap kemanan sistem informasi dapat dilihat dari sudut peranan komputer yang fungsinya adalah sebagai penyedia informasi. Ada beberapa kemungkinan serangan yaitu :

1. *Interruption*
   Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan pada ketersediaan dari sistem sehingga informasi dan data yang ada dalam sistem komputer dirusak dan dihapus, hal ini berdampak saat informasi dan data dibutuhkan maka data dan informasi tersebut tidak ada lagi. Contoh serangan adalah *"denial of service attact"*.
2. *Interception*
   Merupakan ancaman terhadap kerahsiaan. Pihak yang tidak berwenang berhasil mengakses aset dan informasi dimana informasi tersebut disimpan. Contoh dari serangan ini adalah penyadapan (*wiretapping*)
3. *Modification*
   Merupakan ancaman terhadap integritas. Pihak yang tidak berwenang tidak saja berhasil mengakses, tetapi dapat juga mengubah data. Contoh dari serangan ini adalah mengubah pesan dari *website* dengan pesan yang merugikan pemilik *website*
4. *Fabrication*
   Merupakan ancaman terhadap integritas. Pihak yang tidak berhasil meniru dan memalsukan suatu informasi yang ada sehingga pihak yang menerima informasi tersebut menyangka informasi tersebut berasa dari pihak yang dikehendaki oleh sipenerima informasi. Contoh dari serangan jenis ini adalah memasukkan pesan palsu seperti *e-mail* palsu kedalam jaringan komputer.

2.2 Alert

Alert adalah *User Interface* yang bertujuan untuk menyampaikan pemberitahuan kepada *user* dalam selang waktu tertentu sebelum diproses tampilan berikutnya**.** *Alert* dapat terdiri dari *text string* (untaian kata) dan *image* (gambar). Visualisasi dari *alert* dapat diatur berdasarkan tipe dari pemberitahuannya.

Kecenderungan penggunaan *Alert* adalah untuk memberitahu user tentang suatu kesalahan (*errors*) dan kondisi lain yang tidak biasa.

Jenis – jenis *alert* antara lain :

1. Info
   Jenis a*lert* info adalah menyediakan informasi yg umum kepada user. Contohnya : *simple splash screen*
2. *Warning*
   Jenis a*lert warning* adalah isyarat untuk memper ingati user ada operasi yang bila dilakukan berpotensi bahaya.
   Contohnya: *Warning : this operation will erase your data*
3. *Error*
   Jenis *alert error* adalah isyarat untuk memper-ingati user bahwa terjadi operasi yang salah.
   Contohnya: *There is not enough room to install the application.*
4. Alarm
   Jenis a*lert* alarm adalah isyarat untuk memper-ingati user bahwa ada kegiatan terjadwal.
   Contohnya : *Staff meeting in five minutes*
5. *Confirmation*
   Jenis *alert confirmation* adalah isyarat untuk memberitahu tentang status dari operasi yang dilakukan oleh user.
   Contohnya: "*Saved!*" yang memberitahukan bahwa operasi penyimpanan telah selesai dilakukan.

2.3 Intrusion Detection System (IDS)

Intrusion adalah usaha untuk masuk dan atau menyalahgunakan sistem yang ada. *Intrusion Detection System* atau disingkat 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).

2.3.1 Jenis Intrusion Detection System

Terdapat dua jenis IDS, yaitu :

1. *Host-Based Intrusion Detection System* (HIDS)
   Host-Based IDS memperoleh informasi dari data yang dihasilkan oleh system pada sebuah komputer yang diamati. Data *Host-Based* IDS biasanya berupa log yang dihasilkan dengan memonitor system file, event, dan keamanan pada Windows NT dan syslog pada lingkungan system operasi UNIX. Saat terjadi perubahan pada log tersebut, dilakukan analisis untuk mengetahui apakah sama dengan pola yang ada pada *database* IDS.
2. *Network-Based Intrusion Detection System* (NIDS)
   Network IDS menempati jaringan secara langsung dan melihat semua aliran yang melewati jaringan. *Network-Based* IDS merupakan strategi yang efektif untuk melihat *traffic* masuk / keluar maupun *traffic* diantara *host* ataupun diantara segmen jaringan lokal.

Pada *Intrusion Detection System*, pengenalan terhadap penyusup dibagi menjadi dua bagian yaitu :

1. *Anomaly detection* (deteksi penyimpangan)
   Anomaly detector mengidentifikasi perilaku tak lazim yang terjadi dalam *host* atau *network*. *Detector* berfungsi dengan asumsi bahwa serangan tersebut berbeda dengan aktivitas normal. Serangan itu dapat dideteksi dengan *system* yang mampu mengidentifikasikan perbedaan tersebut. *Anomaly detector* menyusun profil yang merepresentasikan kebiasaan *user* yang normal, *host* atau koneksi jaringan. Profil tersebut dibangun atas data historis yang dikumpulkan dalam periode operasi normal. Selanjutnya *detector* mengumpulkan data peristiwa dan menggunakan langkah – langkah yang beragam ketika aktivitas yang diamati menyimpang dari normal.
2. *Misuse detection*
   Detektor melakukan analisis terhadap aktifitas sistem, mencari *event* atau set *event* yang cocok dengan pola perilaku yang dikenali sebagai serangan. Pola perilaku serangan tersebut disebut sebagai *signatures*, sehingga *misuse detection* banyak dikenal sebagai *signatures based detection*.

2.4 Snort

Menurut Ariyus (2006), Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam *database* serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. 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 dapat digunakan pada sistem operasi Linux, Windows, BSD, Solaris dan sistem operasi lainnya. Snort merupakan *network based* IDS yang menggunakan metode Signature Based Detection, menganalisis paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya.

2.4.1 Mode Pengoperasian SNORT

SNORT memiliki 3 mode pengoperasian, yaitu:

1. *Sniffer Mode*: untuk melihat paket yang lewat di jaringan
2. *Packet logger mode*, untuk mencatat semua paket yang lewat di jaringan untuk dianalisis di kemudian hari.
3. *Intrusion Detection mode*, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan *setup* dari berbagai *rules* / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan.

SNORT memiliki beberapa komponen antara lain :

1. *Rule* Snort

   Rule pada Snort digunakan untuk menentukan paket tersebut dianggap serangan atau bukan. Rule terdiri dari dua bagian yaitu *rule header* dan *rule option*. *Rule header* terdiri dari tindakan (*action*), IP *address source* dan IP *address destination*, Protokol dan Port. Sedangkan pada *Rule Option* memiliki beberapa keyword yang memiliki fungsi yang berbeda-beda. Pada percobaan ini, digunakan beberapa kata kunci pada *rule option*, diantaranya :

   a. **msg:** akan mencetak pesan dari alert yang ditunjukkan pada file log
   b. **sid:** digunakan untuk identifikasi snort rules.
   c. **rev**: mengidentifikasikan revisi dari snort rules
   d. **classtype**: mengklasifikasikan serangan
   e. **content:** digunakan untuk mencari isi yang spesifik pada paket payload dan memicu tanggapan (response) berdasarkan paket tersebut.
   f. **reference**: digunakan untuk mencari informasi lebih detail mengenai rule tersebut

   Berikut adalah sebuah contoh rule yang terdapat pada Snort :

   a. Rule dengan Signature ICMP Ping Windows

      alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING Windows"; itype:8; content:"abcdefghijklmnop"; depth:16; reference:arachnids,169; classtype: misc-activity; sid:382; rev:7;)

   b. Rule dengan Signature ICMP Ping

      alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING"; icode:0; itype:8; classtype:misc-activity; sid:384; rev:5;)

Dari rule seperti di atas IDS Snort akan menyatakan apakah sebuah paket data dianggap sebagai serangan atau bukan, paket data akan dicocokkan dengan rule IDS, jika terdapat dalam rule, maka paket data tersebut dianggap sebagai penyusupan/serangan dan demikian juga sebaliknya jika tidak ada dalam rule maka dianggap bukan penyusupan/serangan. Rule Snort terbaru antara lain: attack-responses.rules, bad-traffic.rules, ddos.rules, oracle.rules, scan.rules, web-cgi.rules, backdoor.rules, bleeding.rules, bleeding-attack_response.rules, bleeding-dos.rules, bleeding-drop.rules, pop2.rules, bleeding-drop-BLOCK.rules, bleeding-dshield.rules, bleeding-dshield-BLOCK.rules, bleeding-exploit.rules, bleeding-game.rules, bleeding-inappropriate.rules, bleeding-malware.rules, bleeding-p2p.rules, bleeding-policy.rules, bleeding-scan.rules, bleeding-virus.rules, bleeding-web.rules, botnet-cnc.rules, content-replace.rules, experimental.rules, dns.rules, nntp.rules, rservices.rules, web-attacks.rules, local.rules, web-

client.rules, exploit.rules, smtp.rules, web-coldfusion.rules, chat.rules, finger.rules, snmp.rules, web-frontpage.rules, misc.rules, sql.rules, web-iis.rules, icmp-info.rules, multimedia.rules, pop3.rules, telnet.rules, web-misc.rules, decoder.rules, ddos.rules, icmp.rules, mysql.rules, tftp.rules, web-php.rules, deleted.rules, imap.rules, netbios.rules, rpc.rules, virus.rules, x11.rules

2. Snort *Engine*
   Snort Engine merupakan program yang berjalan sebagai daemon proses yang selalu bekerja untuk membaca paket data dan kemudian membandingkannya dengan rule snort.
3. *Alert*
   Alert merupakan catatan serangan pada deteksi penyusupan. Jika snort engine menyatakan paket data yang lewat sebagai serangan, maka snort engine akan mengirimkan alert berupa log file. Untuk kebutuhan analisa, *alert* dapat disimpan di dalam database.

   Contoh alert sebagai berikut :

   [**] [1:499:3] ICMP Large ICMP Packet [**] [Classification : Potentially Bad Traffic] [Priority : 2] 05/09-20:15:14.895348
   10.1.4.113 -> 10.1.3.126 ICMP TTL : 128 TOS:0x0 ID:6316
   IpLen:20 DgmLen:65528 Type:8 Code:0 ID:512 Seq:3072 ECHO
   [Xref => http://www.whitehats.com/info/IDS246]

Contoh alert di atas merupakan alert ketika terdapat paket data dalam ukuran besar dari IP Address **10.1.4.113 ke 10.1.3.126** yang diangap sebagai serangan oleh Snort karena pola paket data tersebut terdapat dalam rule snort.

3. Bahasa Pemrograman Java

Java adalah bahasa pemrograman berorientasi objek murni yang dibuat berdasarkan kemampuan - kemampuan terbaik bahasa pemrograman objek sebelumnya (C++, Ada, Simula). Java diciptakan oleh **James Gosling**, developer dari Sun Microsystems pada tahun 1991, dengan nama semula Oak. Konon Oak adalah pohon semacam Jati yang terlihat dari jendela tempat pembuatanya bekerja. Ada yang mengatakan bahwa Oak adalah singkatan dari "*Object Application Kernel*". Pada Januari 1995, karena nama Oak kurang komersial, maka diganti menjadi *Java*. Kelebihan Bahasa Programan Java antara lain :

1. *Multiplatform*
   Kelebihan utama dari Java ialah dapat dijalankan di beberapa *platform* / sistem operasi komputer, sesuai dengan prinsip "tulis sekali, jalankan di mana saja". Dengan kelebihan ini pemrogram cukup menulis sebuah program Java dan dikompilasi (diubah, dari bahasa yang dimengerti manusia menjadi bahasa mesin / *bytecode*) sekali lalu hasilnya dapat dijalankan di atas beberapa *platform* tanpa perubahan. Kelebihan ini memungkinkan sebuah program berbasis Java dikerjakan di atas *operating system Linux* tetapi dijalankan dengan baik di atas *Microsoft Windows*. *Platform* yang didukung sampai saat ini adalah *Microsoft Windows, Linux, Mac OS dan Sun Solaris*.
2. OOP (*Object Oriented Programming* - Pemrogram Berorientasi Objek)
3. Perpustakaan Kelas Yang Lengkap, Java terkenal dengan kelengkapan *library* / perpustakaan (kumpulan program yang disertakan dalam pemrograman java) yang sangat memudahkan dalam penggunaan oleh para pemrogram untuk membangun aplikasinya. Kelengkapan perpustakaan ini ditambah dengan keberadaan komunitas Java yang besar yang terus menerus membuat perpustakaan-perpustakaan baru untuk melingkupi seluruh kebutuhan pembangunan aplikasi.
4. Bergaya C++, memiliki sintaks seperti bahasa pemrograman C++ sehingga menarik banyak pemrogram C++ untuk pindah ke Java.

Program Java dapat dibedakan mejadi dua jenis, yaitu :

1. Applet adalah program yang dibuat dengan Java, dapat diletakkan pada *Web browser*. Dalam hal ini *browser* yang digunakan adalah yang memiliki kemampuan Java (seperti : Netscape Navigator, Internet Explorer, dan HorJava)
2. Aplikasi adalah program Java yang bersifat umum. Aplikasi dapat dijalankan secara langsung, tidak perlu perangkat lunak *browser* untuk menjalankannya.

3.1 Komponen Java

Beberapa komponen yang terdapat pada bahasa pemrograman Java terdiri dari :

a. JVM (*Java Virtual Machine*)

Java dapat berjalan pada sebuah sistem operasi membutuhkan *Java Virtual Machine* (JVM). JVM sendiri terdiri dari *Java Runtime Environment* (JRE) *dan Java Development Kit* (JDK). *Sun Microsystems* mengeluarkan tiga kelas paket Java, yaitu:

1. J2-SE JRE (hanya berisi JRE)
2. J2- SE SDK (berisi JDK + JRE)
3. J2-EE SDK (berisi JDK+JRE dan tools untuk aplikasi enterprise).

b. IDE *(Integrated Development Environment)*

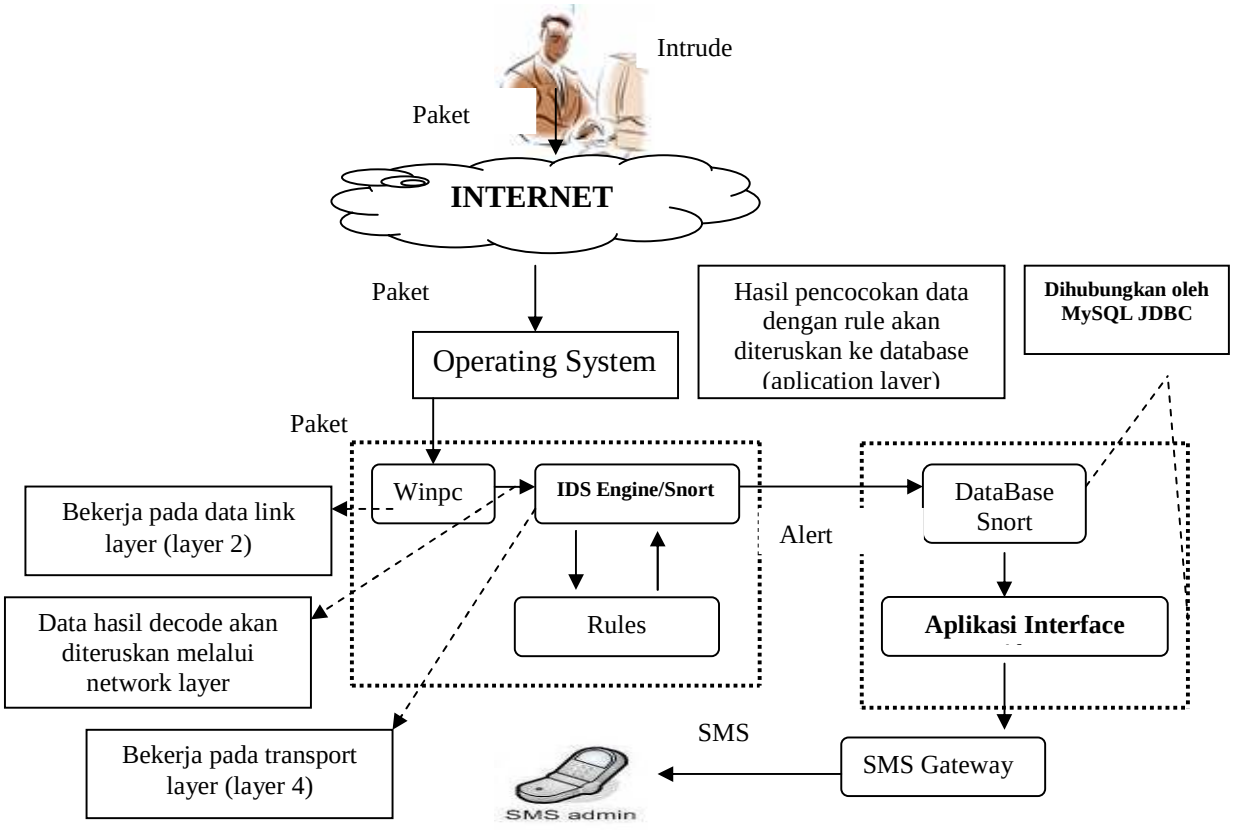
IDE (*Integrated Development Environment*) adalah sebuah *editor* pemrograman sebuah bahasa. Untuk Java sendiri ada banyak IDE yang tersedia dipasaran baik yang bersifat gratis (*freeware*) ataupun yang berbayar. Beberapa IDE yang populer antara lain, JCreator (*www.jcreator.com*), Netbeans (*www.netbeans.org*), JBuilder (*www.borland.com/jbuilder*), dan lain-lain.

c. Class

Unit yang paling mendasar dalam pemrograman java adalah class. Class adalah komponen aplikasi yang menangani kode dan data dalam pemrograman java.

4.Cara Kerja Aplikasi IDS

Aplikasi yang dikembangkan akan mengintegrasikan alert IDS dengan antarmuka yang dirancang menggunakan bahasa pemrograman Java, sehingga alert IDS tersebut dapat diterima administrator melalui SMS dimanapun ia berada. Mekanisme kerjanya seperti Gambar 1 berikut.



Gambar 1. Cara Kerja Aplikasi IDS

Dari Gambar 1 dapat dijelaskan cara kerja aplikasi IDS sebagai berikut :

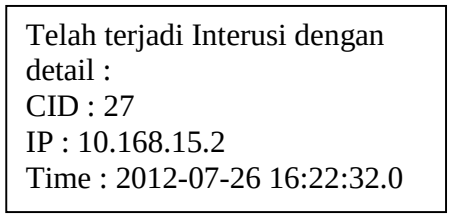
Paket data yang dikirim oleh intruder / heacker melalui internet akan masuk ke sistem operasi pada komputer server melalui media kabel (ethernet) , lalu paket data tersebut ditangkap atau dideteksi oleh paket *capture library*. Paket *capture library* merupakan perangkat lunak yang mengambil paket data dari

NIC (*Network ID Card*). Paket data itu adalah paket data Lapisan Data Link (layer 2 pada OSI model) yang biasanya disebut *frame* yang masih belum diproses. Pada sistem Linux dan Unix Snort menggunakan libpcap, sedangkan pada sistem windows snort menggunakan winpcap. Setelah itu *packet decoder* pada snort mengambil *frame* Lapisan 2 (Data link) yang dikirimkan oleh packet capture library dan kemudian memecahnya. Pertama – tama komponen ini melakukan *decode* terhadap *frame* Lapisan 2, kemudian paket Lapisan 3 (protokol IP), lalu kemudian paket Lapisan 4 (paket TCP atau UDP). Setelah proses *decode* selesai dilakukan, Snort telah mempunyai semua informasi masing – masing protokol untuk pemrosesan lebih lanjut. Setelah itu komponen *Detection engine* pada snort mengambil informasi dari *packet decoder* yang kemudian memproses data itu pada lapisan Transport dan Application, membandingkan data yang terkandung dalam paket dengan *rules* yang juga merupakan *plug-in* dari komponen ini.

Pada saat adanya kecocokan / kemiripan paket data yang diterima dengan *rules* yang ada, Snort akan menghasilkan peringatan dan kemudian melakukan *logging*. Snort mendukung beberapa variasi keluaran, seperti keluaran dalam format teks atau *biner*. *Logging* juga bisa dilakukan ke dalam *database* ataupun *syslog*. Pada aplikasi ini *logging* akan dilakukan ke dalam database MySQL. Pada proses setelah inilah aplikasi yang dikembangkan akan bekerja. *Alert* terbaru pada *database* akan diproses oleh aplikasi *interface* dan akan dikirimkan ke administarator melalui fasilitas SMS menggunakan SMS gateway gammu. Pesan yang akan dikirimkan kepada administrator yaitu :

a. CID yang diambil dari table Event pada field CID
b. IP intruder yang diambil dari table iphdr pada field ip_src
c. Waktu intrusi yang diambil dari table event pada field timestamp
d. Signature yang diambil dari table signature pada field sig_name

Contoh sebuah SMS interusi sebagai berikut :



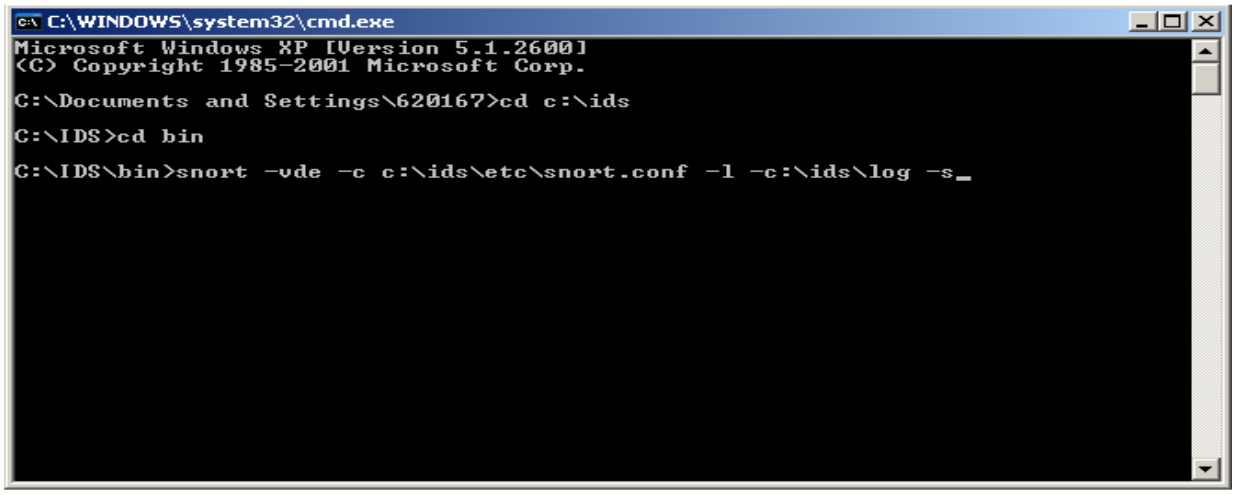
Gambar 2. Tampilan Alert SMS Interusi

Dalam hal ini dapat digunakan beberapa software yang sudah jadi sebagai utility pendukung yaitu winpcap, snort dan rulenya sebagai IDS serta gammu sebagai SMS gateway. SNORT dapat mendeteksi banyak jenis serangan diantaranya :

1. *Port Scanner*
2. *Denial of Services (DOS)*
3. *Brute Force and Dictionary*
4. *Ping of death*
5. dsb

5.Pengujian Aplikasi

Pada pengujian ini dilakukan pada sebuah sistem operasi berbasis windows. Proses awal yang dilakukan adalah menjalankan aplikasi SNORT dengan cara mengetikan perintah untuk mengaktifkan SNORT. Adapun perintahnya dapat dilihat seperti pada Gambar 3 berikut:



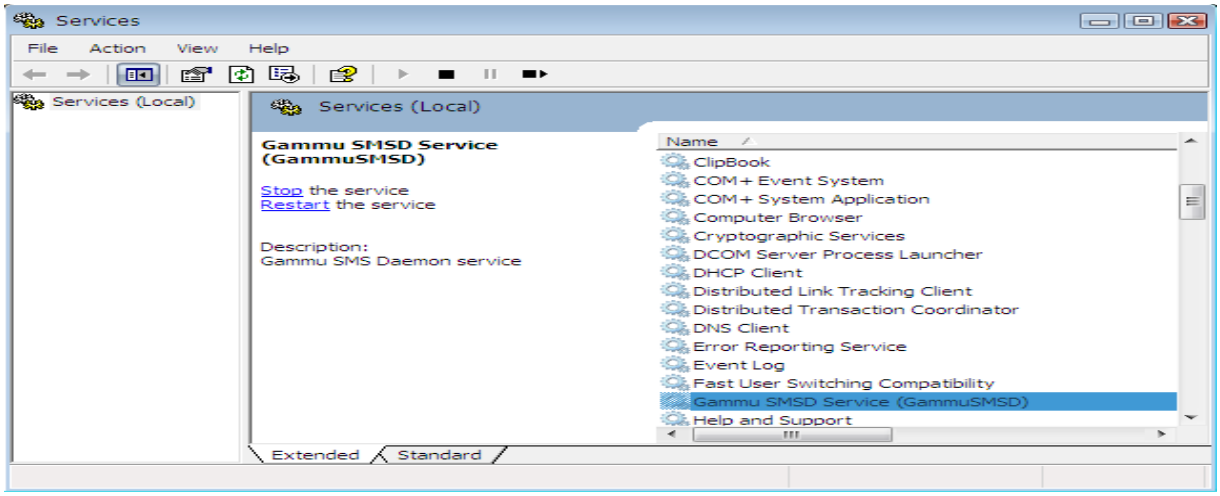
Gambar 3. Running Snort

Penjelasan dari parameter perintah **-vde** di atas adalah:

-v : perintah untuk melihat header TCP/IP paket yang lewat
-d : perintah untuk melihat isi paket
-e : perintah untuk melihat header link layer paket seperti ethernet header.
-c : perintah untuk membaca konfigurasi pada file snort.conf

c:\ids\snort\etc\snort.conf direktori dimana konfigurasi snort berada yaitu snort.conf.
-l : perintah untuk mendefinisikan tempat log snort berada.
c:\ids\snort\log direktori tempat menyimpan log snort.
-s : perintah agar alert masuk ke syslog

Untuk memastikan apakah Snort telah berjalan dengan baik atau belum, dapat dilihat melalui Task Manager → Processes. Jika terdapat SNORT.exe maka berarti Snort sudah aktif. Berikutnya harus diaktifkan service gammu. Service gammu dapat dijalankan dari Control Panel → Administrative Tools → Service → Cari Gammu SMSD Service (GammuSMSD) → Lalu klik Start, Service gammu yang sudah aktif dapat dilihat seperti pada gambar berikut :

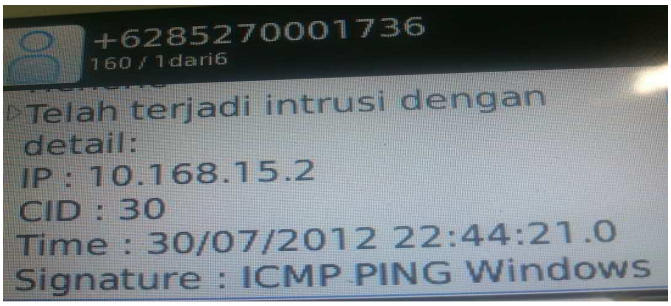


Gambar 4. Running Gammu

Aplikasi antar muka yang dijalankan untuk membaca *alert* terbaru pada database adalah **sms.bat** sehingga pembacaan paket data yang masuk ke *database* dapat dilakukan secara terus – menerus. Selanjutnya aplikasi sudah berjalan dan untuk pengujian sistem intrusi dapat dilakukan dengan cara mengirimkan sebuah paket ICMP dalam ukuran besar sehingga dikategorikan oleh Snort sebagai DDOS attack (denial of service). Berikut contoh pengujian yang dilakukan melalui *client* di jaringan internal.

ping 10.168.15.1 -l 10000
Pinging 10.168.15.1 with 10000 bytes of data:
Reply from 10.168.15.1: bytes=10000 time<1ms TTL=64
Reply from 10.168.15.1: bytes=10000 time<1ms TTL=64
Reply from 10.168.15.1: bytes=10000 time<1ms TTL=64
Reply from 10.168.15.1: bytes=10000 time<1ms TTL=64
Ping statistics for 10.168.15.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times ini mili – second:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

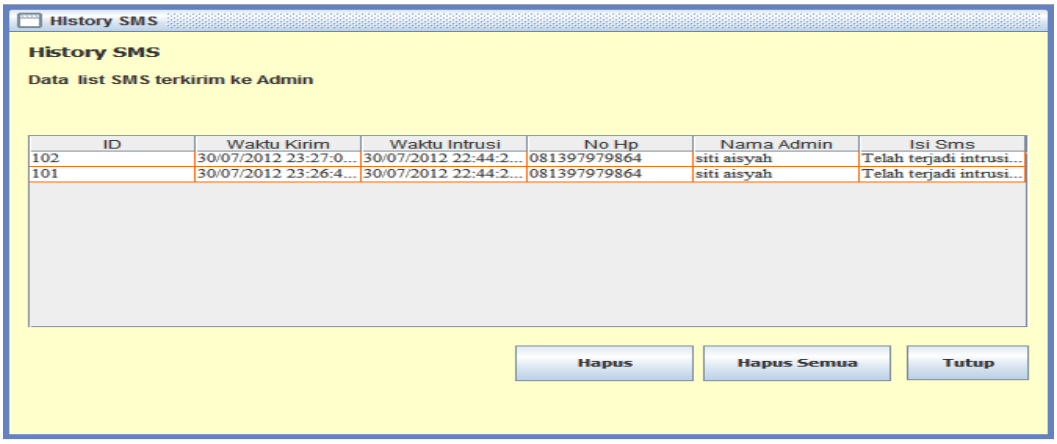
DDOS attack ini akan segera terdeteksi oleh snort engine yang kemudian snort engine akan mengirimkan sebuah *alert* ke *alert* log dan program eksekusi pengiriman *alert* IDS untuk mengambil data terbaru yang terdapat pada *database* dan langsung diproses untuk dikirim ke administrator melalui sebuah SMS. Gambar berikut sebuah contoh tampilan yang diterima dari telepon selular administrator melalui SMS.



Gambar 5. Tampilan SMS di Telepon Seluler

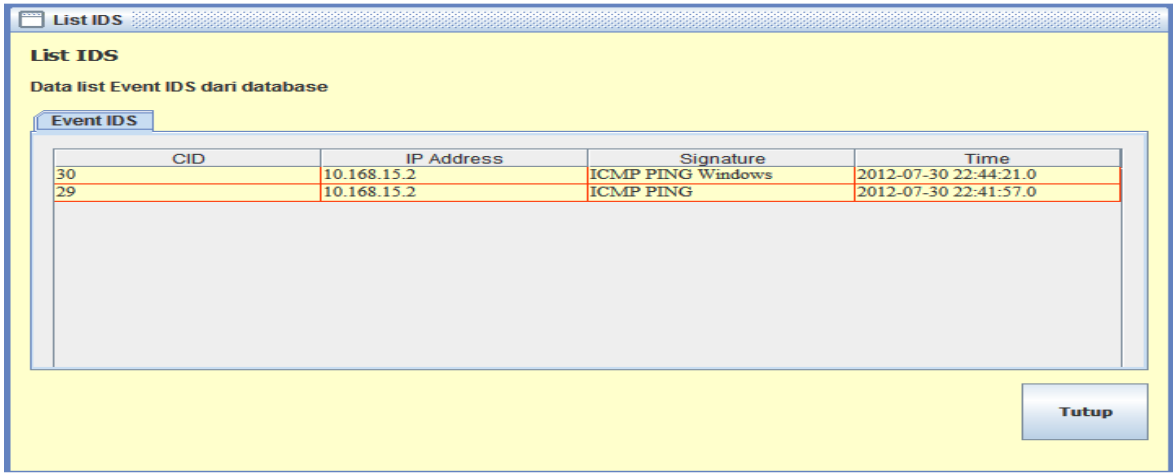
Dari hasil pengujian dapat dilihat pada pada status berikut :

1. History SMS
   Dari history ini dapat dilihat informasi seperti : ID, Waktu Kirim SMS, Waktu intrusi, No HP Admin, Nama Admin dan Isi SMS Intrusi.



Gambar 6. Status Pengiriman SMS Alert

2. List IDS
   Dari List IDS ini dapat dilihat informasi seperti CID, Hostname, IP intruder, Signature dan Waktu Intrusi



Gambar 7. Status Interusi Yang Terjadi

6.Kesimpulan

Perkembangan pertukaran data dan informasi secara elektronik membutuhkan semakin tingginya akan keamanan komputer dalam sebuah jaringan baik jaringan internal maupun jaringan external. IDS merupakan sebuah aplikasi yang dapat mendeteksi aktivitas 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). Lahirnya JAVA dengan *platform independent* dan *open source* telah membawa dampak yang sangat signifikan di dalam pemrograman untuk membuat berbagai aplikasi yang dapat mengintegrasikan berbagai perangkat IT. Dengan pemrograman JAVA dapat digunakan dalam membuat suatu interface untuk pengiriman *alert* IDS yang akan dikirimkan ke telepon selular melalui sebuah SMS sehingga akan membantu administrator untuk tetap memonitor keadaan jaringan dikantornya walaupun dia tidak berada di kantor.

7.Daftar Pustaka

[1] Ariyus, Dony, 2006, ***Membangun Intrusion Detection Pada Windows 2003 Server***, Tesis, Sekolah Pascasarjana Program Studi Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.
[2] Harold, Elliotte Rusty, 2005, ***Java™ Network Programming,*** Third Edition, O'Reilly Media, Inc., United States of America
[3] Nasution, Muhammad Irwan Padli, 2008, ***Java Bahasa Pemrograman Masa Depan,*** Buletin Ilmiah STT Harapan Medan; ISSN:0853-5175; Edisi 005, Maret 2008; hal.37-44
[4] Schildt, Herbert, 2005, ***Java™: A Beginner's Guide, Third Edition,*** McGraw-Hill/Osborne, USA
[5] Thomas, Tom, 2004, ***Networking Security first - step,*** Penerbit Andi, Yogyakarta.
[6] http://www.snort.org/snort-rules/cli diakses tanggal 13 Agustus 2012