KONTROL SISTEM KEAMANAN JARINGAN KOMPUTER BERBASIS JAVA

Tisy Darmala Mahargiyani[1], M. Zen Hadi S.[2], Haryadi Amran D.[3]
[1]Politeknik Elektronika Negeri Surabaya, Jurusan Teknik Telekomunikasi
[2]Laboratorium *Digital Communication*, Politeknik Elektronika Negeri Surabaya
[3]Laboratorium *Multimedia*, Politeknik Elektronika Negeri Surabaya

Institut Teknologi Sepuluh Nopember, Surabaya 60111
Email : **zeezee.tizzy@gmail.com**

ABSTRAK

Seiring dengan perkembangan jaman, kinerja yang cepat adalah hal yang penting untuk menjadi pertimbangan pilihan dalam suatu sistem. Pengolahan data atau informasi adalah hal mendasar yang pasti akan ditemui di masa – masa mendatang. Seperti halnya sistem yang dibangun untuk proyek akhir ini, pengolahan data dengan sistem database menjadi pendukung utamanya. Pengontrolan jaringan komputer yang dilakukan secara on line melalui telepon seluler dengan media GPRSnya akan terkoneksi dengan sistem database server. Dengan didukung telepon seluler beraplikasi Java yang berfungsi memberi tampilan pada telepon seluler dan dengan PHP sebagai bahasa scripting, PHP akan terkoneksi dengan Snort (IDS) dan Tripwire untuk melakukan proses kontrol jaringan komputer.

Kata Kunci : Snort (IDS), Tripwire, PHP, GPRS.

1. PENDAHULUAN

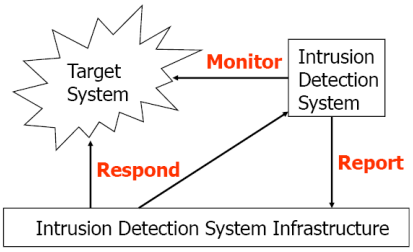
Kesibukan yang telah menyita waktu dan memerlukan suatu konsentrasi, tentunya menjadikan manusia untuk mencari alternatif kemudahan dan kepastian untuk memperoleh sebuah informasi. Untuk itu pengembangan suatu teknologi telekomunikasi bergerak merupakan sebuah usaha untuk memenuhi tuntutan masyarakat akan suatu masalah guna mendapatkan suatu informasi. Dalam penelitian kali ini, sistem kontrol diaplikasikan untuk mengontrol keamanan jaringan komputer. Pengontrolan suatu sistem jaringan komputer dapat dilakukan secara jarak jauh, dengan kata lain tanpa harus datang ke lokasi dimana sistem itu berada merupakan salah satu tuntutan masyarakat akan kemajuan teknologi yang mampu memberikan sebuah efisiensi waktu. Kasus yang diambil dalam kemudahan melakukan pengontrolan sistem adalah pengontrolan sistem jaringan komputer. Melalui aplikasi Java yang dibangun dengan menggunakan bahasa pemrograman Java Micro (J2ME) pada telepon seluler maka pengguna (*user*) dapat mengetahui adanya serangan (*attack*) dari luar yang menuju ke sistem untuk selanjutnya dapat melakukan pengontrolan terhadap sistem tersebut.

2. LANDASAN TEORI

a. Snort Intrusion Detection System

Deteksi Penyusupan (Intrusion Detection) adalah aktivitas untuk mendetaksi penyusupan secara cepat dengan menggunakan program khusus yang otomatis. Program yang dipergunakan biasanya disebut sebagai Intrusion Detection System (IDS).
Snort memiliki 3 buah mode, yaitu :

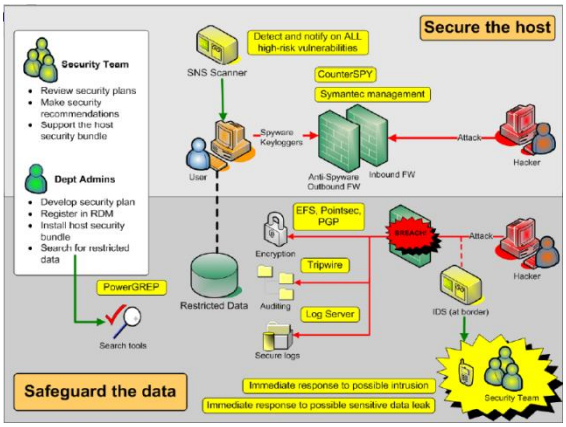
- Sniffer mode, untuk melihat paket yang lewat dijaringan.
- Packet logger mode, untuk mencatat semua paket yang lewat di jaringan untuk dianalisa dikemudian hari.
- Intrusion Detection mode, pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.



Gambar Infrstruktur Sistem Snort IDS

b. Tripwire (File Integrity Check)

Tripwire merupakan salah satu tool untuk pemeriksaan integritas system yang digunakan untuk memonitor perubahan yang terjadi pada sebuah system. Tripwire mampu mengecek file atau program dan membandingkannya dengan database sebelumnya. Tripwire bekerja dengan membuat sebuah database informasi semua file sistem dan menyimpannya pada suatu file. Setiap kali tripwire dijalankan untuk melakukan pengecekan, file sistem hasil pemeriksaan akan dibandingkan dengan database yang pernah dibuat. Setelah tripwire dijalankan, secara otomatis akan melakukan pembuatan database sistem. Kemudian secara periodik akan selalu melaporkan setiap perubahan pada file dan direktori.



Gambar Penempatan Konfigurasi Tripwire

c. Java 2 Micro Edition (J2ME)

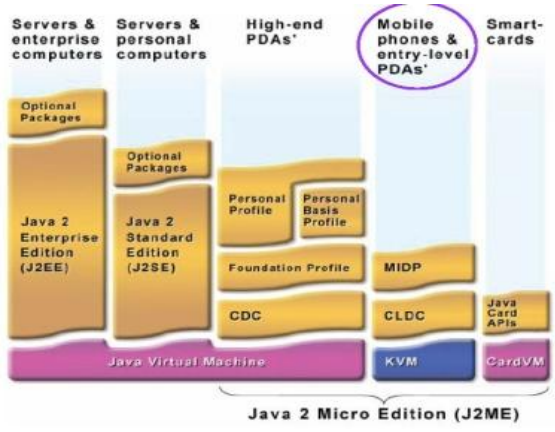
Penjelasan tentang mengenai Java 2 Platform Micro Edition (J2ME) adalah salah satu dari produk Sun Microsystems. Java 2 Platform Micro Edition (J2ME) merupakan bagian dari platform Java 2. Bahasa pemrograman yang digunakan mirip dengan bahasa pemrograman C++ tetapi secara fundamental berbeda. C++ menggunakan pointer-pointer yang kurang aman dan mengharuskan programmer untuk mengalokasikan dan mengosongkan memori. Sedangkan Java menggunakan typesafe object references dan setiap memori yang tidak digunakan akan dikosongkan secara otomatis. Java juga mendukung multiple inheritance dengan konstruksi yang lebih baik, yaitu Interface.

Device yang bisa diprogram dengan J2ME antara lain mulai dari dari smart card hingga PDA. Masing – masing device tersebut memiliki kemampuan komputasi yang berbeda seperti :

Smart card memiliki memori < 1 Mb, dengan kecepatan prosesor yang rendah.

PDA saat ini memiliki memori > 8Mb dengan kecepatan prosesor yang tinggi.

Untuk lebih lengkapnya lihat gambar dibawah ini.



Gambar pembagian Kelas Java

d. GPRS

GPRS merupakan teknologi generasi kedua yang akan meramaikan maraknya standar jaringan mobile yang sudah ada, seperti GSM dan TDMA. Kecepatan transmisi data diharapkan dapat naik dari 9.6 Kbps menjadi 115 Kbps. GPRS memiliki kemampuan foto dan video dengan kecepatn tinggi. Kemampuan tambahan yang dimiliki GPRS adalah pertama dapat memelihara keutuhan komunikasi data dan suara pada saat sedang bergerak. Kedua user dapat segera terhubung ke nomor yang dituju kapan saja jika diinginkan tidak tergantung pada lokasi berada sekarang serta tanpa mengalami delay yang lama. Ketiga dengan tingkat kecepatan yang dimiliki GPRS sangat memungkinkan untuk mendownload file.

Teknologi transmisi data GSM berupa GPRS adalah sebuah teknologi yang dipergunakan untuk pelayanan data wireless seperti pada wireless internet atau intranet serta pelayanan multimedia.

e. PHP (Hypertext PreProcessor)

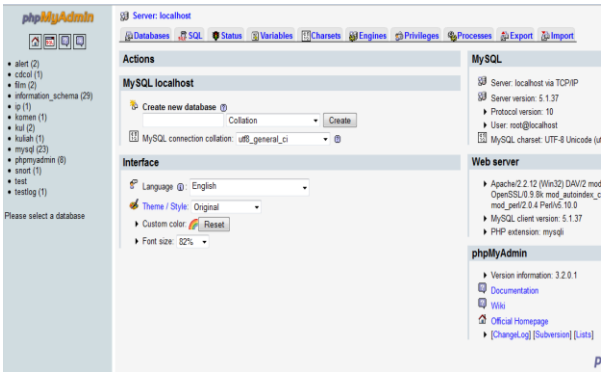
PHP merupakan script yang menyatu dengan HTML dan berada pada server (*server side HTML embedded scripting*). PHP ini dapat digunakan untuk membuat beragam aplikasi komplek yang membutuhkan koneksi ke database.

Kode PHP umumnya diawali dengan <? diakhiri dengan ?>. pasangan kedua kode inilah yang berfungsi sebagai tag kode PHP. Berdasarkan tag inilah pihak server dapat memahami kode PHP dan kemudian memprosesnya, dan hasilnya dikirim ke browser. Berikut adalah contoh *syntax* dari PHP script :

```
<?php
$txt1="Selamat Datang";
$txt2="di PENS";
echo $txt1 . $txt2 ;
?>
```

f. MySQL

MySQL merupakan server basis data yang menggunakan teknik relasional untuk menghubungkan antar tabel – tabel dalam basis data. MySQL juga menyediakan source programnya secara terbuka (*open source*) sehingga orang lain dapat mengubah atau menambah kemampuan dari MySQL untuk keperluan khusus secara pribadi. Dikarenakan kemampuannya yang handal dan didukung dengan system *multi-user* dan *multi-thread*, maka MySQL dapatlah bersaing dengan beberapa produk server basis data commercial seperti MS Server 7, Oracle dan lainnya. Berikut adalah tampilan dari MySQL :



Gambar Database MySQL

g. Integrasi antara PHP dengan MySQL

Untuk mengintegrasikan PHP dengan system database MySQL, perlu adanya sebuah file yang berekstensi .php atau .php3 dapat dieksekusi langsung lewat sebuah browser dengan menyembunyikan kode – kode pemrograman PHP, dan menampilkan kode – kode html yang dimengerti oleh browser. PHP inilah yang digunakan sebagi antar muka ke web atau user sekaligus penghubung dengan database. Contoh PHP script yang digunakan untuk integrasi PHP dengan MySQL adalah seperti dibawah ini :

```
<?php
$conn=mysql_connect("localhost","root","") or die ("koneksi2 gagal");
mysql_select_db("alert",$conn);
$hasil = mysql_query("select * from alert1",$conn);
while($row=mysql_fetch_row($hasil)){
echo $row[0];
echo "\n";
echo $row[1];
echo "\n";
}
?>
```

Script diatas digunakan untuk mengambil data dari database, dimana data yang akan diambil adalah data dari table alert1 pada database alert. Hasil pengambilan data tersebut ditampilkan pada web server.

h. IP Public

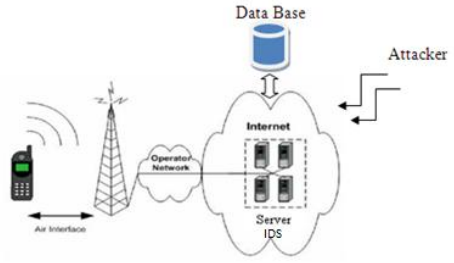
IP Public adalah IP yang bisa diakses langsung oleh internet. Analoginya IP Public itu seperti nomer telepon rumah atau nomer HP yang bisa ditelepon langsung oleh semua orang.

Selain itu, IP public juga merupakan IP yang biasanya terhubung oleh jaringan luas (internet). Jika IP Public yang digunakan adalah IP dynamic maka alokasi IPnya bisa berubah-ubah biasanya menggunakan DHCP server pada PC yang digunakan menggunakan setting automatic. Sedangkan jika yang digunakan adalah IP static maka IPnya tetap pada PC yang digunakan menggunakan setting manual.

Ketika kita berlangganan internet dedicated ke ISP (penyedia layanan internet) yang menjadi member APNIC baik secara langsung atau tidak, umumnya kita akan mendapatkan IP Public. Supaya IP bias diakses, kita perlu melakukan konfigurasi jaringan kita dengan IP transit supaya IP public bias diakses/dikenali.

3. METODOLOGI

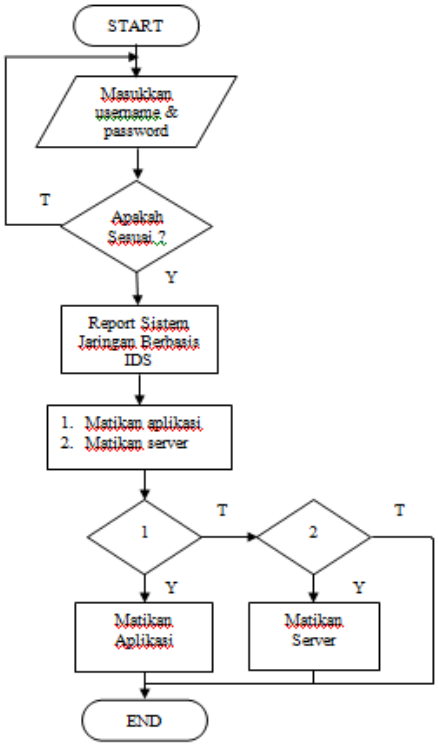
Perancangan Sistem



Gambar perencanaan Sistem

Proses diawali dari munculnya serangan dari luar yang masuk ke web server yang terkoneksi dengan internet. Kemudian report serangan dikirim secara on-line dan diterima oleh client menggunakan telepon seluler. Client dapat mengantisipasi serangan dengan mengontrolnya secara langsung melalui telepon selulernya. Terdapat 2 pilihan antisipasi yaitu yang pertama adalah mematikan server dan yang kedua adalah mematikan web servernya.

Proses tersebut juga akan dijelaskan lebih lsnjut melalui flowchart yang digambarkan seperti dibawah ini



Gambar Flowchart Sistem

Dari flowchart diatas dapat dilihat bahwa admin (client) dapat mengakses alert jaringan dengan memasukkan username dan password yang sesuai. Jika username ataupun password yang digunakan tidak sesuai maka admin tidak dapat mengakses alert dan akan keluar dari aplikasi atau keluar ke menu awal.
Saat admin berhasil masuk dan mengakses alert, alert dari sistem yang digunakan akan terkirim ke telepon seluler yang digunakan oleh admin. Setelah admin menerima dan membaca alert, admin dapat melakukan feedback ke sisi server dengan cara mematikan web server ataupun mematikan PC server.

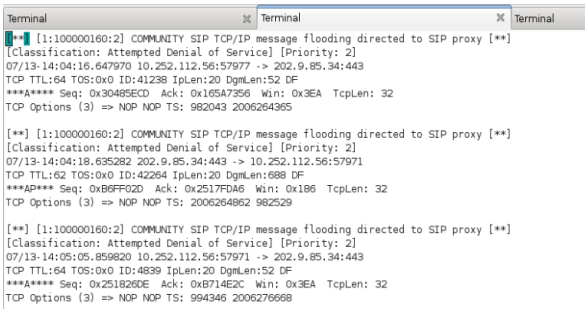
3.1 Instalasi Snort IDS
Instalasi Snort melalui terminal dapat dilakukan dengan menjalankan perintah sebagai berikut :

apt-get install snort

Kemudian masukkan range network atau nomor IP PC yang akan dilakukan analisa system :

Address range for the local network :
192.168.0.0/16

Snort IDS dapat berjalan pada packet logging mode. Hasil pembacaan Snort IDS dapat dilihat pada direktori /var/log/snort/snort.log. berikut adalah tampilan alert dari Snort :



3.2 Instalasi Tripwire

Dari terminal, install Tripwire kemudian masukkan password baru agar dapat melakukan proses pengecekan data.

apt-get install tripwire

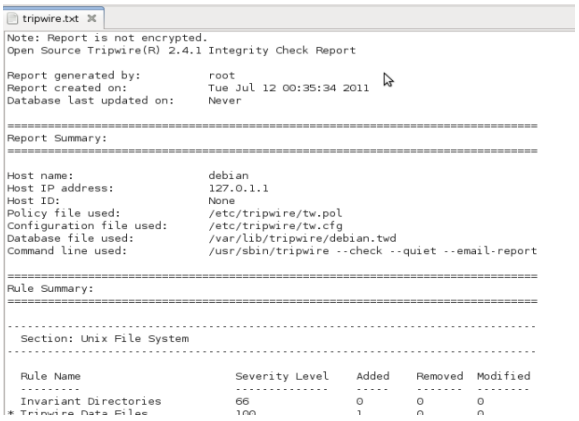
Selanjutnya adalah membuat kata kunci yang digunakan untuk menjalankan tripwire.

Enter the site-key passphrase:
Repeat the site-key passphrase:
Generating key (this may take several minutes)...Key generation
complete.
Enter the local key passphrase:
Repeat the local keyfile passphrase:
Generating key (this may take several minutes)...Key

Untuk melakukan pengecekan apakah terjadi perubahan file dalam sistem, penulis melakukan perintah ini melalui terminal.

tripwire –check

Alert yang dihasilkan oleh Tripwire IDS berupa jumlah data yang mengalami kebocoran. Alert dapat dilihat dalam bentuk print out seperti dibawah ini :



Gambar Alert Tripwire

3.3 Pembuatan Program Java

Pembuatan program dapat dilakukan. Program Java yang digunakan adalah program J2ME dimana program tersebut merupakan program Java berbasis mobility.
Program interkoneksi clinet server dibutuhkan pada J2ME ini karena program tersebut akan digunakan untuk mengambil data dari database, dimana database tersebut berisi kumpulan alert dari sistem. Program tersebut membutuhkan script PHP sebagai jembatan interkoneksi client server.

```
public void doDownload1(){
    t5 = new Form("Network by IDS");
    pesan = "";
    String URLsite = "http://127.0.0.1/tampil.php?";
    //String p1;
    HttpConnection con = null;
    InputStream in = null;
    StringBuffer data = new StringBuffer();
    try{
       con = (HttpConnection)Connector.open(URLsite);
       in = con.openInputStream();
       int ch;
       while((ch = in.read())!=-1){
          data.append((char)ch);
       }
       pesan = data.toString();
       t5.append(pesan);
       t5.addCommand(keluarCmd);
       t5.addCommand(okCmd);
       t5.setCommandListener(this);
       Display.getDisplay(this).setCurrent(t5);
    } catch (IOException e) {}
 }
```

4. PENGUJIAN DAN ANALISA

4.1 Pengujian Login Admin

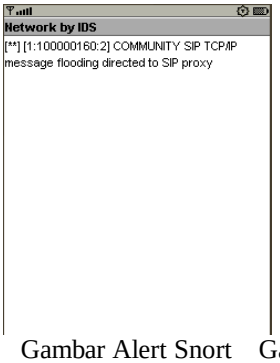
Form login terdiri dari username dan password, dimana username dan password telah ditentukan bahwa username = admin dan password = admin.

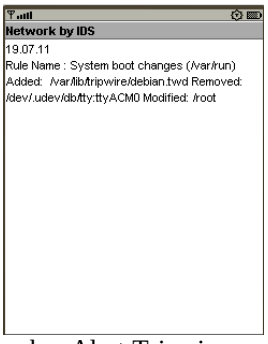
Username	Password	Sukses / Gagal
admin	admin	Sukses
Admin	admin	Gagal
admin	ADMIN	Gagal
tizzy	admin	Gagal
tizzy	tizzy	Gagal

Dapat dilihat pada table diatas, bahwa username dan password bersifat sensitive case. Sehingga besar kecilnya huruf mempengaruhi berhasil atau tidaknya login.

4.2 Pengaksesan Alert IDS Snort dan Tripwire

Alert yang diterima oleh admin (client) berupa alert dari database server. Berikut akan ditampilkan beberapa form untuk penerimaan alert dari Snort dan Tripwire IDS.





Gambar Alert Snort Gambar Alert Tripwire

Pengujian penerimaan alert dari server menggunakan emulator J2ME dilakukan sebanyak 10 kali. Dari pengujian tersebut admin membutuhkan waktu kurang lebih 00:00:15 untuk mendapatkan alert dari satu sistem yang dipilih.

Pengujian	Waktu Pengujian 11 Juli 2011	Sukses / Gagal	Waktu Penerimaan Alert
1	14.00 – 14.01	Sukses	0:00:15
2	14.05 – 14.06	Sukses	0:00:13
3	15.00 – 15.01	Sukses	0:00:16
4	15.15 – 15.16	Sukses	0:00:12
5	15.20 – 15.21	Sukses	0:00:13
6	17.11 – 17.12	Sukses	0:00:15
7	17.15 – 17.16	Sukses	0:00:15
8	17.55 – 17.56	Sukses	0:00:16
9	17.59 – 18.00	Sukses	0:00:15
10	18.09 – 18.10	Sukses	0:00:15

Gambar Hasil Pengujian Penerimaan Alert

5. KESIMPULAN

Setelah melakukan serangkaian proses pengujian terhadap system yang telah dibuat, maka adapat diambil kesimpulan bahwa :
Username dan password pada form login bersifat sensitive case, besar kecilnya huruf abjad yang digunakan berpengaruh pada bisa atau tidaknya pengaksesan aplikasi.
Alert Snort IDS menginformasikan kepada admin jika terdapat aktifitas penyerangan seperti scanning data pada server.
Alert Tripwire menginformasikan kepada admin jika terdapat bentuk perubahan data pada server.

6. DAFTAR PUSTAKA

1. Stanger, James & Patrick Lane, ”Hack Proofing – Linux : A Guide To Open Source Security”, Syngress, 2001

2. Beale, Jay, ”Snort 2.1 Intrusion Detection”, Syngress, 2002

3. Izzuddin, Edwin, ”Perancangan dan Implementasi Pemesanan Tiket Berbasis Java Micro”, Proyek Akhir Politeknik Elektronika Negeri Surabaya – Institut Teknologi Sepuluh Nopember, 2004

4. Yuan, Michael Juntao, ”Enterprise J2ME Developing Mobile Applications”, Prentice Hall Profesional Technical Reference, 2004

5. Raharjo, Budi, ”Sistem Pencegahan Penyusupan Pada Jaringan Berbasis Snort IDS dan IPTables Firewall”, Tugas Kuliah Keamanan Sistem Lanjut (EC7010), 2006

6. Sari, Kartika Yusiana, “Akses Database BAAK dan Perpustakaan PENS – ITS via GPRS”, Proyek Akhir Politeknik Elektronika Negeri Surabaya – Institut Teknologi Sepuluh Nopember, 2007

7. Hadi, M.Zen Samsono, ”Modul Network Security – Snort”, Politeknik Elektronika Negeri Surabaya, 2011

8. Hadi, M.Zen Samsono, ”Modul Network Security – Tripwire”, Politeknik Elektronika Negeri Surabaya, 2011

9. Hadi, M.Zen Samsono, ”Modul Internet Programming – J2ME”, Politeknik Elektronika Negeri Surabaya, 2011