SISTEM DETEKSI PENYUSUPAN JARINGAN KOMPUTER PADA LABORATORIUM KOMPUTER FAKULTAS TEKNIK UNIVERSITAS ISLAM ATTAHIRIYAH

Wahyu Nur Cholifah, Ahmad Syarif
Fakultas Teknik Universitas Islam Attahiriyah
Jl. Melayu Kecil III No. 15, Tebet, Jakarta
wahyu_nc@yahoo.co.id

Abstrak

Latar belakang penelitian ini adalah sistem deteksi penyusupan jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem yang ada pada saat ini tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis. Pada penelitian ini akan didesain dan diimplementasikan suatu sistem deteksi penyusupan jaringan yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan, melakukan tindakan penanggulangan serangan lebih lanjut.Tujuan Penelitian ini adalah mendesain dan mengimplementasikan sistem deteksi penyusupan pada jaringan komputer yang tersedia di laboratorium komputer fakultas teknik. Menganalisa sistem deteksi penyusupan jaringan dalam menangani gangguan terhadap sistem jaringan komputer yang ada.Metode Penelitian ini menggunakan 3 metode antara lain : studi kepustakaan penelitian ini dilakukan degan cara membaca, mencatat, mengumpulkan dan mempelajari karya tulis atau buku – buku yang mempunyai hubungan dengan masalah yang diteliti. Selain itu, penelitian juga dilakukan dengan melakukan wawancara pada pihak – pihak terkait yang membantu penyelesaian pembuatan tulisan ini. Konfigurasiadalah tahap peng*install*an dan konfigurasi sistim pendeteksi penyusup. dimana dimulai dari instalasi dan konfigurasi sistem sampai melakukan tahap *trouble shooting*. Pengujiansistim pendeteksi penyusup harus dilakukan untuk mendapatkan hasil yang maksimal, uji coba dilakukan dengan menguji hasil konfigurasi.Hasil yang Dicapai adalah mengatasi gangguan penyusupan di jaringan komputer pada jaringan internet Laboratorium Komputer Fakultas Teknik Universitas Islam Atahiriyah agar jaringan internet dapat mengetahui adanya kegiatan penyusupan.Simpulannya adalah Usulan Sistim Deteksi Penyusupan yang telah dibuat di labkom FT uniat dapat diterapkan dengan baik dan tepat. Usulan ini mampu memonitor jika ada penyusup yang akan memasuki jaringan komputer secara tidak sah

Kata kunci: deteksi, penyusupan, jaringan komputer

Pendahuluan

Pada era teknologi informasi saat ini, hampir seluruh informasi yang penting bagi suatu institusi dapat diakses oleh para penggunanya. Keterbukaan akses tersebut memunculkan berbagai masalah baru, antara lain : pemeliharaan validitas dan integritas data atau informasi tersebut, jaminan ketersediaan informasi bagi pengguna yang berhak, pencegahan akses informasi dari yang tidak berhak serta pencegahan akses sistem dari yang tidak berhak.

Sistem pertahanan sistem terhadap aktivitas gangguan yang ada saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi. Apabila gangguan tersebut telah berhasil membuat jaringan mengalami malfungsi, administrator tidak dapat lagi mengakses sistem secara remote. Sehingga administrator tidak dapat melakukan pemulihan sistem dengan cepat.

Karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman-ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat secara otomatis dan memungkinkan

administrator mengakses sistem walaupun terjadi malfungsi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem deteksi penyusupan jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem yang ada pada saat ini tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis.

Pada penelitian ini akan didesain dan diimplementasikan suatu sistem deteksi penyusupan jaringan yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan, melakukan tindakan penanggulangan serangan lebih lanjut.

Analisa Sistem yang Berjalan

Sampai dengan saat ini tahun 2012-an fakultas teknik hanya memiliki 2 (dua) laboratorium komputer yang digunakan untuk perkuliahan praktikum dan sudah memiliki jaringan komputer dengan fasilitas internet. Sistem yang berjalan pada Laboratorium Komputer Fakultas Teknik Universitas Islam Attahiriyah adalah sebagai berikut :

1. Akses internet yang digunakan pada Laboratorium Komputer Fakultas Teknik Universitas Islam Attahiriyah adalah menggunakan Internet Service Provider (ISP) dari PT. Telkom speedy dengan kecepatan (bandwidth 1 Mbps).
2. Perangkat keras (modem ADSL) menggunakan *3Com OfficeConnect ADSLWireless 54 Mbps 11g Firewall Router* dengan 2 (dua) model jaringan seperti : menggunakan Kabel (UTP Rj 45) dan Wirelless.
3. Untuk *Internet Protocol* (IP Address), tiap komputer *Client* akan diberikan *IP Address* secara otomatis menggunakan *Dynamic Host Configuration Protocol* (*DHCP*) dari Modem ADSL 3Com.
4. Bagi yang mengakses internet dengan Wirelless terdapat hak akses (password) sebelum koneksi ke internet.
5. Tidak ada sistim monitoring pendeteksi penyusup

Kelemahan Sistem yang Berjalan

Adapun beberapa kelemahan dari sistem yang berjalan sebagai berikut :

1. Koordinator Laboratorium Komputer Fakultas Teknik tidak dapat mengelola proses pemantauan (monitoring) terhadap jaringan lokal area.
2. Apabila ada penyusup yang ingin merusak jaringan internet maka koordinator tidak dapat mengetahui adanya penyusup.

Usulan Pemecahan Masalah

Berdasarkan kendala tersebut diatas maka perlu dibuat suatu sistem jaringan internet yang dapat mengatasi gangguan penyusupan di jaringan komputer pada jaringan internet Laboratorium Komputer Fakultas Teknik Universitas Islam Atahiriyah agar jaringan internet dapat mengetahui adanya kegiatan penyusupan.

Komponen-Komponen Pembangunan IDS Snort

Untuk membangun sistem intrusion detection diperlukan beberapa komponen yang perlu diintegrasikan menjadi satu kesatuan sistem. Komponenkomponen tersebut meliputi :

1. *SNORT*

   Download versi terbaru snort untuk sistem operasi windows dapat didownload di situs http://www.snort.org.

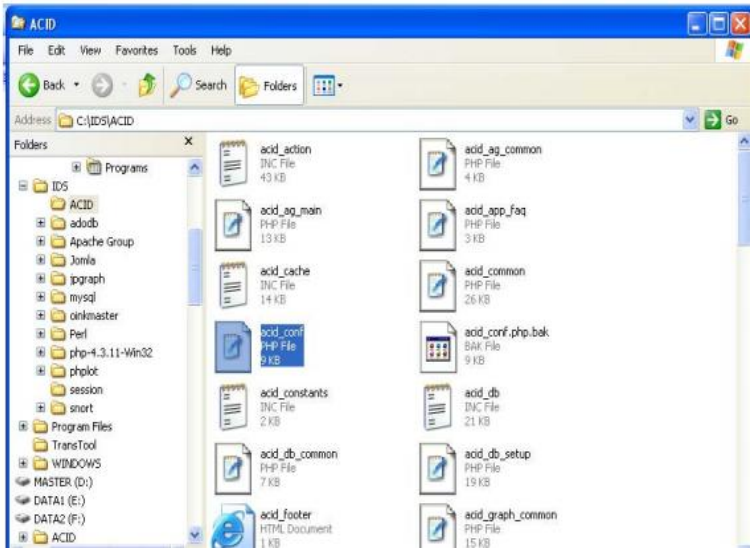
2. *WINPCAP*
   Pada sistem operasi unix sudah tersedia library yang mampu meng-*capture* paket pada jaringan yaitu libcap dan ikut disertakan pada CD instalasinya, akan tetapi untuk sistem windows belum mempunyai library yang mampu mengcapture paket pada jaringan komputer dan gunakan winpcap version 3.1 atau lebih tinggi,untuk mendownloadnya kunjungi situs http://www.winpcap.org.
3. *OINKMASTER*
   Seperti antivirus yang memerlukan *update, rules snort* juga perlu di *update*. *Update* dilakukan untuk memperoleh rule terbaru sehingga nantinya dapat diperoleh sebah rule yang mampu mengetahui jenis-jenis serangan baru. Oinkmaster dapat di download di http://www.oinkmaster.com
4. *ACTIVE PERL*
   Untuk menjalankan *oinkmaster* diperlukan bahasa pemrograman perl, karena oinkmaster dikembangkan dengan menggunakan bahasa pemograman perl. *Active perl* dapat di download gratis di situs http://www.perl.com
5. *MYSQL*
   Database yang digunakan adalah MySQL yang diinstall pada sistem berbasis Windows atau sistem operasi lain yang mendukung database MySQL. Alert IDS akan disimpan pada database mysql. Alasan pemilihan MySQL sebagai program database yang digunakan antara lain :
   a. Sifatnya yang open source dan murah
   b. Cukup stabil pada hardware dengan spesifikasi yang relatif rendah

   Mysql dapat di download pada situs http://www.mysql.com, Untuk administrasi dan maintenance sistem database dibuat suatu interface berbasis web yang dibuat dengan bahasa pemrograman PHP. Fungsi utama dari interface ini adalah untuk mengedit atau mengupdate entry database yang dijadikan input bagi sistem yang lain.
6. *Analysis Console for Intrusion Databases* (ACID)
   Analysis Console for Intrusion Databases (ACID) merupakan *PHPbased* analysis engine yang berfungsi untuk mencari dan mengolah database dari alert network sekuriti yang dibangkitkan oleh perangkat lunak pendeteksi intrusi (IDS). Dapat di implementasikan pada sistem yang mendukung PHP seperti linux, BSD, Solaris dan OS lainnya. ACID adalah perangkat lunak yang open-source dan didistribusikan dibawah lisensi GPL. Kali ini menggunakan ACID-0.9.6b23. ACID dapat di download pada situs http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html.
7. *PHP*: Hypertext Preprocessor (PHP)
   PHP merupakan bahasa pemrograman berbasis web. Bahasa ini mempunyai kelebihan yaitu kompabilitasnya dengan berbagai macam jenis database, dukungan dengan berbagai macam jenis sistem operasi. PHP lebih cocok dan umum digunakan jika di gabungkan dengan database mysql. Mysql dengan PHP seakan-akan dua hal yang tidak dapat dipisahkan. PHP nantinya akan digunakan untuk menampilkan alert yang dihasilkan oleh snort. Alert tersebut nantinya akan ditampilkan dengan menggunakan ACID. PHP dapat di download pada situs http://www.php.net
8. *Web server Apache*
   Web server yang akan digunakan adalah web server apache. Webserver tersebut nantinya akan diintegrasikan bersama-sama dengan PHP. Web server apache dapat didownload di situs http://www.apache.net
9. ADODB
   ADODB, sebuah library abstraksi untuk menggabungkan PHP ke berbagai database seperti MySQL dan *Postgre* SQL. ADODB dapat didwonload di http://adodb.sourceforge.net.
10. Phplot dan Jpgraph.
    Merupakan library untuk membuat grafik yang baik di PHP. Library ini nantinya akan digunakan bersama-sama dengan komponen yang lainnya. Phplot dapat di download pada situs http://www.phplot.com, dan Jpgraph dapat didownload di http://www.aditus.nu/jpgraph/.

Konfigurasi ACID

Analysis Console for Intrusion Databases (ACID) merupakan PHP-based analysis engine yang berfungsi untuk mencari dan mengolah database dari alert network sekuriti yang dibangkitkan oleh perangkat lunak pendeteksi intrusi (IDS).

Dapat di implementasikan pada sistem yang mendukung PHP seperti linux, BSD, Solaris dan OS lainnya. ACID adalah perangkat lunak yang open-source dan didistribusikan dibawah lisensi GPL. Penulis kali ini menggunakan ACID-0.9.6b23. ACID dapat di download pada situshttp://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html. Setelah berhasil mendownload ekstrak file ke direktori C:\IDS, *rename*-lah sehingga diperoleh direktori C:\IDS\acid.

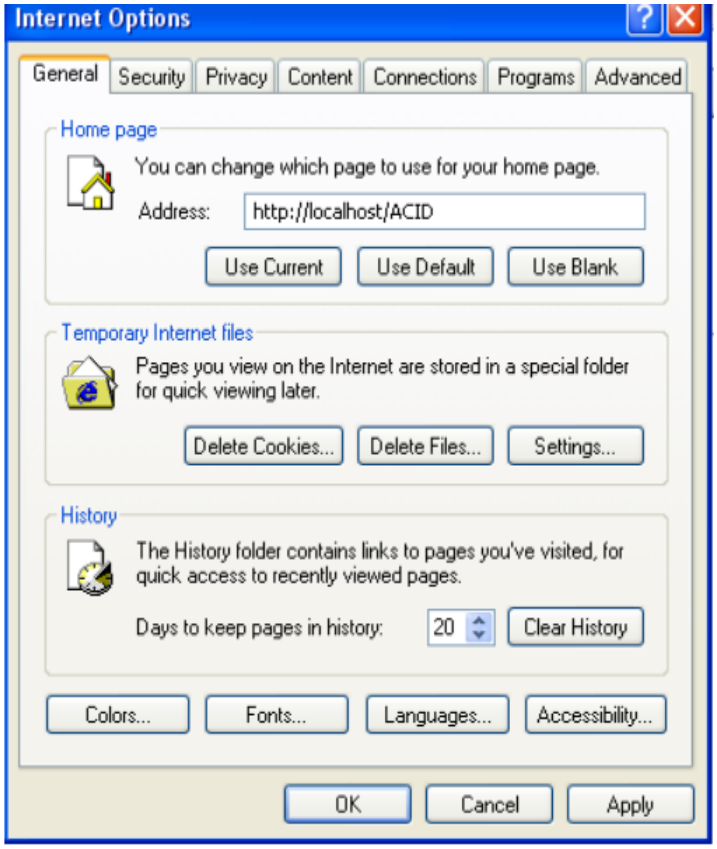


Gambar 1
Rename File Acid_conf

Langkah selanjutnya adalah melakukan konfigurasi ACID, buka file acid_conf.php dengan menggunakan editor wordpad atau notepad editlah beberapa baris sebagai berikut :

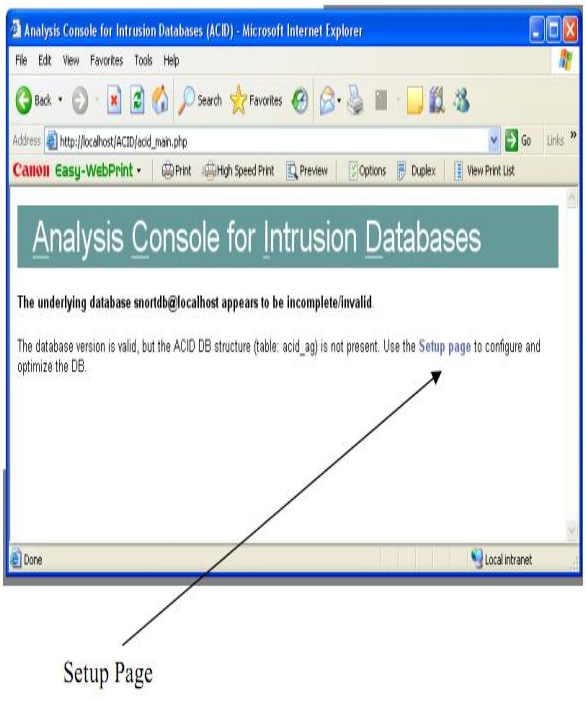
```
$DBlib_path = "c:\IDS\adodb";
$alert_dbname   = "snortdb";
$alert_host     = "localhost";
$alert_port     = "3306";
$alert_user     = "snort";
$alert_password = "snort";
$archive_dbname   = "archive";
$archive_host     = "localhost";
$archive_port     = "3306";
$archive_user     = "archive";
$archive_password = "archive";
$ChartLib_path = "c:\IDS\phplot";
```

Setelah selesai melakukan konfigurasi simpan file tersebut. Buka web browser internet explorer arahkan default browser ke http://localhost/ACID, dimaksudkan agar setiap pertama kali membuka internet explorer halaman pertama yang terbuka adalah http://localhost/ACID. Buka internet explorer pilih Tools Æ Internet Options, lakukan setting seperti gambar dibawah ini :



Gambar 2
Internet Option

Kemudian tekan tombol apply, otomatis browser akan membuka links ke http://localhost/ACID setiap pertama kali membuka web browser tersebut. Buka kembali Internet Explorer, apabila semua konfigurasi berhsil dan tidak terdapat error maka akan muncul permintaan untuk membuat tabel baru pada database, tekan links Setup Pages, seperti gambar berikut ini.

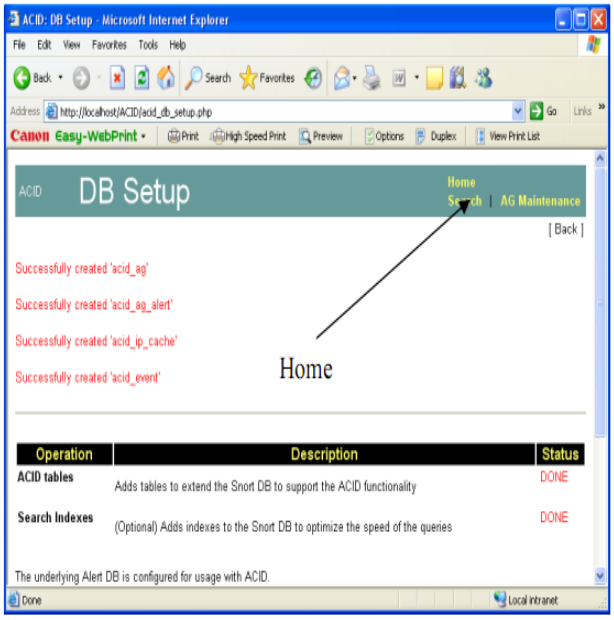


Gambar 3
Setup Page ACID

Langkah selanjutnya menambah table ACID ke dalam database snort, klik Create ACID AG

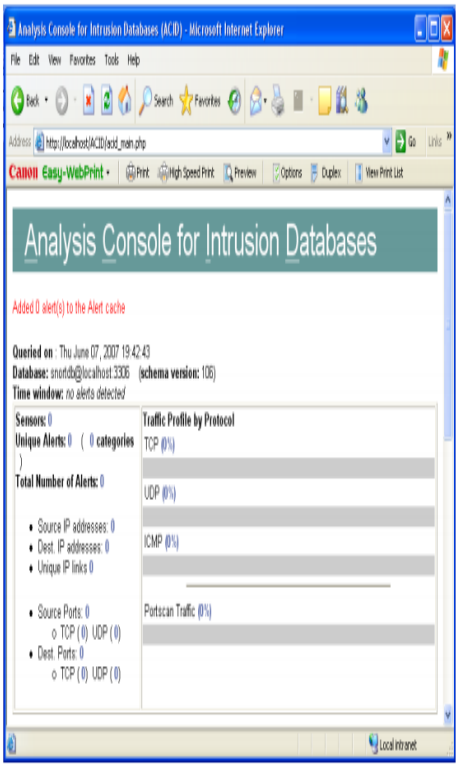
Gambar 4
Create ACID AG

Apabila tidak terjadi error dalam proses, maka akan muncul pesan "Successfully created acid_ag", "Successfully created acid_ag_alert", "Successfully created acid_ip_cache", "Successfully created acid_event". Klik Home untuk kembali ke menu awal.



Gambar 5
Home ACID AG

Sekarang jaringan komputer dapat dimonitoring



Gambar 6
Hasil Monitoring Jaringan

Snort akan memonitor jaringan kita dan akan menghasilkan alert, alert tersebut akan ditampilkan oleh ACID dan hanya akan membahas bagaimana menampilkan alert snort. Gambar dibawah ini menunjukkan ACID dengan alert snortnya.

Gambar 7
ACID dengan Alert Snort

Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat ditarik kesimpulan sebagai berikut :(1) Analisis yang dilakukan pada jaringan internet laboratorium komputer fakultas teknik adalah menggunakan Network Intrusion Detection System (NIDS). Secara sederhana NIDS akan mendeteksi semua serangan melalui jaringan komputer baik internet maupun intranet yang ada di laboratorium komputer fakultas teknik; (2)Untuk menangani adanya penyusupan di jaringan internet laboratorium komputer fakultas teknik maka memerlukan alat bantu atau tools perangkat lunak seperti : Snort, winpcap, oinkmaster, active perl, mysl,acid, phpapache, adodb,serta phplot dan jpgraph; (3) Dengan adanya sistim deteksi penyusupan menggunakan aplikasi perangkat lunak Snort IDS makamampu mengatasi dan memonitorterhadap gangguan penyusupan di jaringan komputer khususnya pada jaringan internet Laboratorium Komputer Fakultas Teknik Universitas Islam Atahiriyah.

Daftar Pustaka

Bambang Sugiantoro, "Kajian Aplikasi Mobile Agent Untuk Deteksi Penyusupan Pada Jaringan Komputer", Yogyakarta, 2006.

Charlie Scott,Paul Wolfe, and Bert Hayes, "Snort For Dummies", Wiley Publishing, inc , 2004.

Helmi Zein Nuri, "Instalasi Moodle Pada Sistem Operasi Windows Xp", Yogyakarta, 2006.

Michael E. Steele, "Snort Installation Manual Windows NT4 Server, 2000, & XP (All Versions)", www.silicondefense.com, 2003.

Michael Keri, "OpenIDS Installation and configuration guide 1.0", www.prowling.nu, 2005.

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

Puji Hartono, "Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall", Bandung, 2006.

Ryan Russel, "Snort Intrusion 2.0 Intrusion Detection", Syngress, 2003.

Sourcefire, Inc, "Snort User Manual", [http://www.snort.org], diakses tanggal 26 Desember 2011.