IMPLEMENTASI INTRUSION SYSTEM (IDS) SNORT
PADA LABORATORIUM JARINGAN KOMPUTER

ABSTRAK

Laboratorium pengembangan jaringan komputer merupakan salah satu laboratorium yang dimiliki Universitas, bertugas menyelenggarakan kegiatan pelatihan mengenai jaringan komputer bagi seluruh civitas akademika. Di dalam laboratorium ini terdapat 30 komputer klien yang digunakan oleh peserta pelatihan. Komputer-komputer tersebut terhubung melalui sebuah patch-panel box (berisi beberapa hub dan switch) dan 1 buah PC router. Keamanan sebuah jaringan komputer diperlukan untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha Intrusi yang dapat merusak sistem yang ada. Untuk mengidentifikasi adanya Intrusi atau pemindaian oleh pihak-pihak yang tidak memiliki otoritas maka laboratorium pengembangan jaringan komputer menggunakan sebuah sistem pendeteksi intrusi - Intrusion Detection System melalui snort.

Kata kunci : IDS, Jaringan, Keamanan.

[1]Miftahul Jannah
[2]Hustinawati
[3]Rangga Wildani

Fakultas Teknologi Industri
Teknik Informatika
Universitas Gunadarma
[1,2]{miftah, hustina}@staff.gunadarma.ac.id
[3]rangga_wildani@student.gunadarma.ac.id

PENDAHULUAN

Sebuah jaringan komputer telah didefinisikan sebagai sebuah kumpulan sistem yang terhubung satu sama lain untuk pengiriman informasi atau menyerupai jaring laba-laba. Sebuah jaringan komputer memiliki tingkat kompleksitas yang tinggi karena semua terhubung ke dalam jaringan tersebut.

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 Intrusi atau pemindaian oleh pihak yang tidak berhak.

Intrusion Detection System yang nantinya akan disebut IDS merupakan usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal *cracker*) atau seorang *user* yang sah tetapi menyalahgunakan *privilege* sumber daya sistem. *Intrusion Detection System* (IDS) atau Sistem Deteksi Intrusi adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi Intrusi. IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal.

Di sisi lain, sebuah sistem pencegahan intrusi merupakan software yang memiliki semua kemampuan sistem deteksi intrusi dan juga dapat mencoba untuk menghentikan insiden yang mungkin terjadi.

TINJAUAN PUSTAKA

A. Jaringan Komputer

Jaringan komputer ialah himpunan "interkoneksi" antara 2 komputer *autonomous* atau lebih terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan *autonomous* (tidak melakukan kontrol terhadap komputer lain dengan akses penuh).

Secara umum jaringan komputer terbagi menjadi 3, yaitu :

1. LAN (*Local Area Network*) yang dibatasi oleh area yang relatif kecil.
2. MAN (*Metropolitan Area Network*) yang meliputi area yang lebih besar dari LAN. Dalam hal ini menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yag lebih besar
3. WAN (*Wide Area Network*) yaitu jaringan yang biasanya sudah menggunakan media wireless, sarana satelit, ataupun kabel serat optik, karena jangkauannya yang lebih luas.

Pada dasarnya setiap jaringan komputer ada yang berfungsi sebagai *klien* dan juga *server*. Tetapi tidak sedikit juga jaringan yang memiliki komputer khusus didedikasikan sebagai *server* sedangkan yang lain sebagai *klien*. Ada juga yang menjadikan komputer khusus berfungsi sebagai *server* saja, atau juga sebaliknya komputer hanya digunakan hanya sebagai *klien* saja.

Karena itu berdasarkan fungsinya maka ada dua jenis jaringan komputer, yaitu :

1. Client - Server
   jaringan *client-server* adalah jaringan komputer dimana suatu unit computer yang berfungsi sebagai server yang hanya memberikan layanan bagi komputer lain, dan client yang juga hanya meminta layanan dari server.
2. Peer-to-peer
   Jaringan *peer-to-peer* adalah suatu model dimana tiap PC dapat memakai resource pada PC lain atau memberikan resourcenya untuk dipakai PC lain. Dengan kata lain dapat berfungsi sebagai client maupun sebagai server pada periode yang sama.

B. Standar OSI

Dalam suatu jaringan komputer, untuk dapat saling berkomunikasi dibutuhkannya suatu bahasa pemersatu. Hal ini biasa disebut dengan Protokol. Protokol adalah sekumpulan aturan-aturan yang mendefinisikan bagaimana peralatan-peralatan dalam jaringan dapat berkomunikasi. Agar setiap peralatan jaringan dari suatu *vendor* dapat saling berkomunikasi dibuat standarisasi. Suatu standar yang banyak digunakan saat ini adalah standar *Open System Interconnection* (OSI) yang dikembangkan oleh *International Standard Organization* (ISO). Pada model standar OSI ini ditetapkan model lapisan atau *layer*, setiap lapisan memiliki fungsi masing-masing. Pada standar OSI terdapat 7 lapisan/ *layer*, yaitu Application, Presentation, Session, Transport, Network, Data Link dan Physical.

C. Transmission Control Protocol/ Internet Protocol (TCP/ IP)

Pada awalnya TCP/ IP diciptakan khusus untuk komunikasi jaringan DARPA. TCP/ IP kemudian digunakan sebagai protokol jaringan yang digunakan oleh distribusi *Berkeley Software* yaitu UNIX. Tetapi sekarang TCP/ IP menjadi *standard de facto* untuk komunikasi *internetwork*, *server*, dan protokol transportasi bagi internet yang menjadikan jutaan komputer dapat berkomunikasi secara global.

D. IP Address

Agar tiap-tiap komputer yang saling terhubung dengan jaringan dapat saling berkomunikasi satu dengan yang lainnya dibutuhkan suatu tata cara pengalamatan pada jaringan komputer. Dengan konsep dasar dari protokol TCP/ IP, setiap komputer yang terhubung pada jaringan TCP/ IP harus mempunyai suatu alamat unik. Alamat ini dikenal sebagai *Internet Protocol Number* (IP *Number*/ IP *Address*).

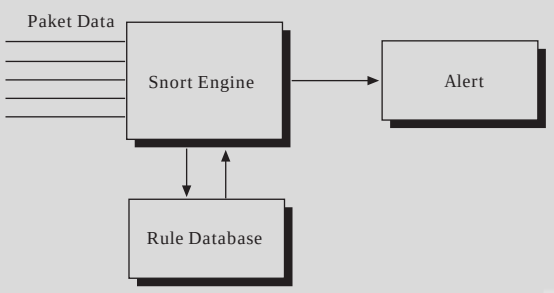
E. Keamanan Komputer

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan.

Menurut Garfinkel dan Spafford, ahli dalam keamanan komputer, komputer dikatakan aman jika bisa diandalkan dan softwarenya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu Availability, Confidentiality, Data Integrity, Control dan Audit.

F. Intrusion Detection System (IDS)

Intrusion Detection System (disingkat IDS) adalah sebuah aplikasi software atau hardware 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).



Gambar 1. Bagian IDS

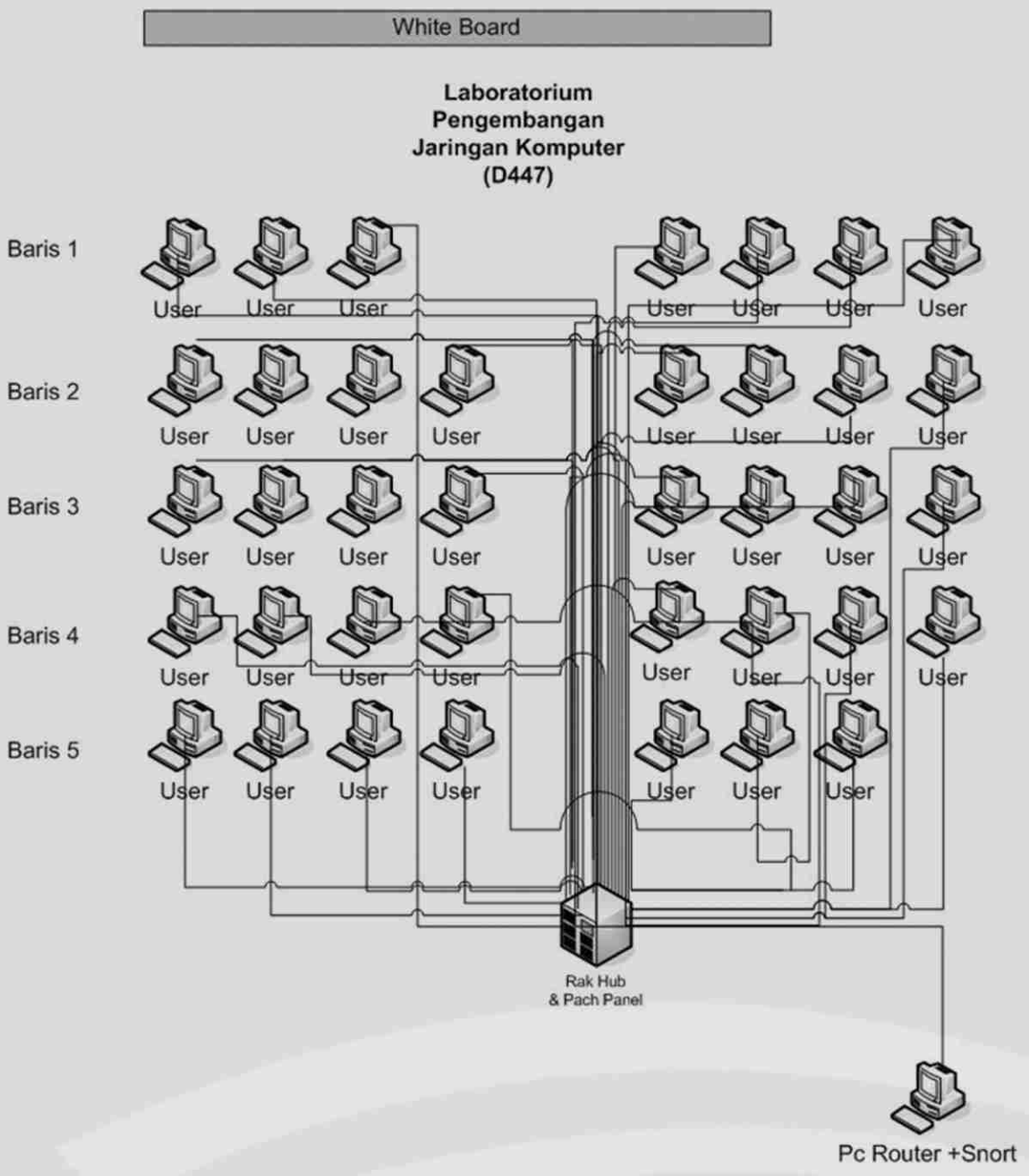
G. Snort IDS

Snort IDS merupakan IDS open source yang secara de facto menjadi standar IDS di industri. Snort dapat diunduh di situs www.snort.org. Snort dapat diimplementasikan dalam jaringan yang multi platform. Salah satu kelebihannya adalah mampu mengirimkan alert dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui *Server Messager Block* (SMB). Snort dapat bekerja dalam 3 mode, mode penyadap (sniffer), packet logger dan mode network intrusion detection.

PEMBAHASAN

Laboratorium Jaringan Komputer adalah salah satu bagian laboratorium dari Lembaga Pengembangan Komputerisasi di Universitas Gunadarma yang mengadakan pelatihan mengenai jaringan komputer kepada civitas akademika.

Jaringan pada Laboratorium Jaringan Komputer merupakan jaringan LAN, terlihat pada gambar 2. Topologi jaringan yang digunakan adalah topologi star dikarenakan topologi ini lebih mudah dalam pemeliharaan dan juga mudah dalam melakukan perubahan bila sewaktu-waktu ada penambahan komputer.



Gambar 2.Topologi Jaringan Laboratorium Jaringan Komputer LePKom

Laboratorium ini memiliki 38 komputer klien yang terhubung ke dalam *patch panel box* (gabungan beberapa hub dan switch) dan 1 buah PC *router* yang juga berperan sebagai PC yang di dalamnya terdapat Snort sebagai IDS. Alamat IP privat yang digunakan memakai network 192.168.16.0 dan Netmask 255.255.255.0.

Dalam pembuatan IDS untuk laboratorium jaringan komputer ini meliputi beberapa komponen dari penggunaan teknologi IDS yaitu :

a. Sensor or Agent

Sensor dan agen memantau dan menganalisis aktivitas. Istilah sensor biasanya digunakan untuk IDS yang memantau jaringan, termasuk berbasis jaringan dan *wireless*.

b. Management Server

Management server adalah sebuah alat/ sistem yang mengatur semua kinerja dari sensor atau agent yang bekerja dan berfungsi untuk menerima semua laporan yang masuk.

c. Database Server

Sebuah *server* yang berguna untuk menyimpan semua kejadian yang dicatat oleh sensor atau agent yang sedang bekerja, agar laporannya dapat terekam yang berguna untuk proses administrasi jaringan selanjutnya.

Hardware dan Software Yang Digunakan

Untuk membangun sebuah *Server* yang terintegrasi dengan sistem IDS sebenarnya tidak membutuhkan *hardware* yang tinggi, tetapi semakin baik spesifikasi *hardware* yang digunakan akan semakin baik pula kinerja *server* tersebut. Kebutuhan *hardware* tersebut bergantung pada besarnya sistem yang akan dibuat dan banyaknya klien yang akan menggunakan fasilitas dari *server*. Ada pun spesifikasi hardware dan software yang digunakan terlihat pada tabel 1.

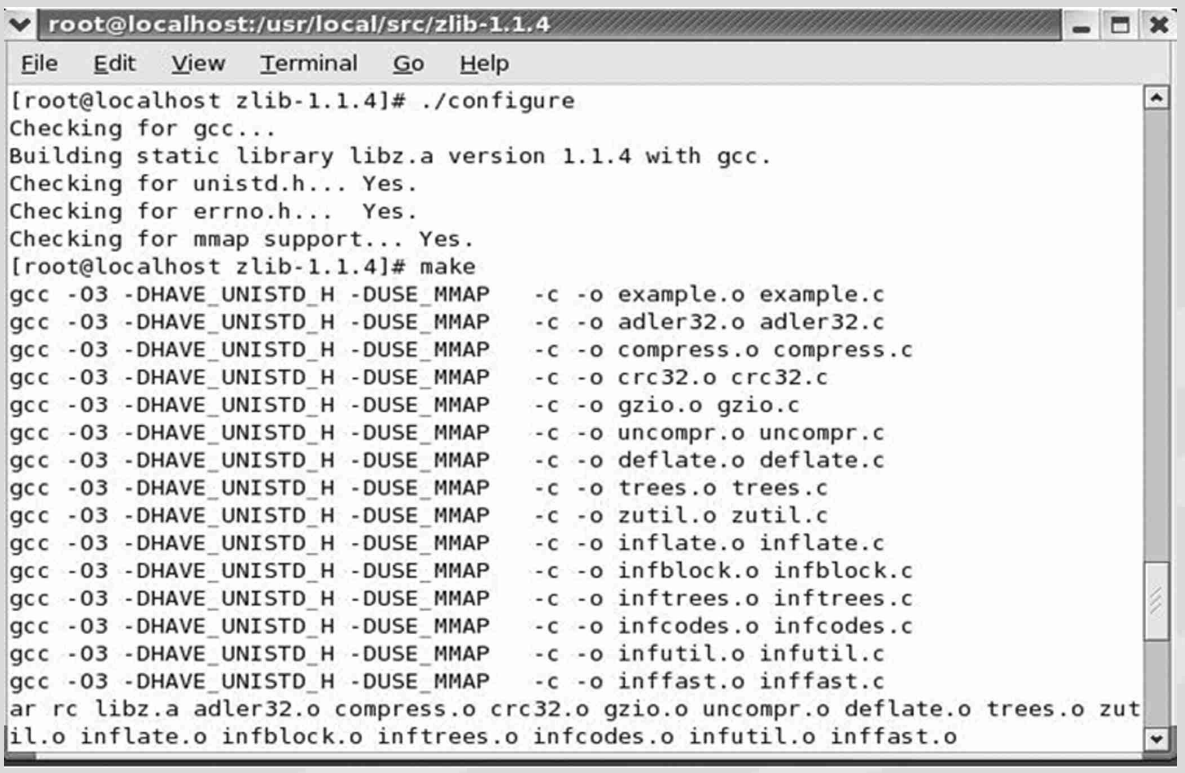
Zlib adalah sebuah komponen kompresi data *library*, *zlib* menyediakan kompresi di memori dan fungsi dekompresi termasuk memeriksa integritas data terkompresi. Gambar 3 memperlihatkan konfigurasi file *zlib*,sehingga file tersebut siap untuk dipakai.

LibPcap merupakan salah satu komponen yang juga penting untuk proses penangkapan *alert* untuk snort yaitu sebuah *library* yang dapat menangkap paket dan protokol jaringan yang berjalan pada jaringan.

Dalam pembuatan server IDS menggunakan MySQL sebagai database untuk menyimpan semua kegiatan (event) yang terjadi dalam sebuah sistem jaringan. Selanjutnya pemilihan dan konfigurasi *web server* dan pada pembuatan IDS

Tabel 1.
Spesifikasi Hardware dan Software Laboratorium

Spesifikasi hardware untuk server		Spesifikasi hardware untuk Klien	
Processor	: Intel Pentium 4 2,8 GHz	Processor	: AMD ATHLON 1,15 GHZ
RAM	: 512 MB	RAM	: 256 MB
Harddisk	: 80 GB	Harddisk	: 20 GB
CDROM	: ASUS 52X	VGA	: Inode 3D 32 MB
VGA	: NVIDIA GEFORCE 2 MX 64 MB Innovation	LAN card	: Dlink DFE 538TX
LAN card	: 3COM GB LOM(3C940) 2 buah	Monitor	: Beam CRT 14"
Klien	: 30 Klien		
Monitor	: LG CRT 14"		
Spesifikasi Software Untuk Server		**Spesifikasi Software Untuk Klien**	
1. *Linux-RedHat-9.0*		1. Sistem Operasi Windows XP	
2. *Zlib 1.1.4*		2. *Nmap-Zenmap GUI*	
3. *libpcap-0.7.2*			
4. *mysql-4.0.14*			
5. *httpd-2.0.47*			
6. *php-4.3.2*			
7. *snort-2.0.1*			
8. *jpgraph-1.12.2*			
9. *adodb370*			
10. *acid-0.9.6b23*			



Gambar 3. Konfigurasi Zlib

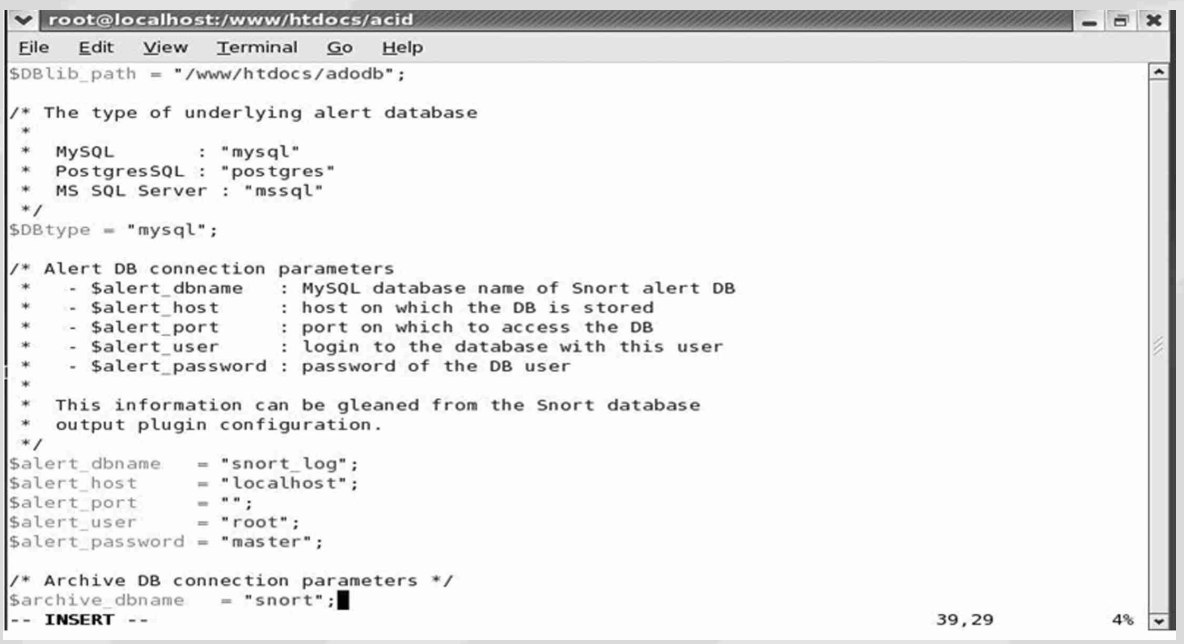
server ini menggunakan *apache web server*. Hal ini dikarenakan hasil akhir dari *report* Snort akan ditampilkan dengan tampilan *web* (*web base*)

JPGraph adalah *library* dari PHP yang bersifat *object oriented*. Fungsi utama dari *library* ini adalah untuk menggambar grafik pada *browser* sesuai dengan data yang ada.

file ADODB berisi semua file yang berhubungan dengan pembetukan *web base* php yang nantinya akan dipakai oleh konfigurasi ACID

ACID (*Analysis Console for Intrusion Databases*) adalah sebuah perangkat lunak yang berfungsi sebagai pengolah semua data *security event* dan akan ditampilkan dalam bentuk *web base* yang telah terkoneksi dengan *database* MySQL. Gambar 4 memperlihatkan konfigurasi file *acid_conf.php* yang berada di direktori */www/htdocs/acid/*. Konfigurasi acid berguna untuk memilih tipe database yang akan digunakan untuk menjadi database server. Jika telah menentukan tipe database yang akan dipakai,maka langkah selanjutnya adalah memberikan informasi untuk database server yang terdiri dari : *$alert_dbname, $alert_host, $alert_port, $alert_user, $alert_password.*

Tahap berikutnya setelah melakukan konfigurasi ACID adalah mengatur ACID *DB Structure* dimana kegunaannya adalah untuk membuat *tables database* yang akan digunakan oleh ACID. ACID yang telah diberi *tables* sudah dapat beroperasi dengan mengetikkan http://192.168.16.200/acid/acid_main.php. pada browser seperti pada gambar 5.



Gambar 4. Konfigurasi ACID

Pengujian Snort

Untuk menguji Snort yang akan ditampilkan oleh ACID dibuatlah skenario yang dimana salah satu *user* akan meng-*scan* seluruh *port* TCP dan UDP dari *server* menggunakan *Nmap-Zenmap GUI*. Hal ini menandakan akan dilakukan penyerangan terhadap *server* yang dilakukan oleh salah satu *user* dengan lebih dahulu melakukan *scanning port* pada level TCP/IP.

Pada gambar 6, terlihat dari hasil scanning yang dilakukan oleh Nmap-Zenmap GUI terdeteksi *port* yang berada di komputer *server* yaitu : port 80 (tcp),port 22 (tcp),port 3306 (tcp),port 32768 (tcp) yang semua berada di IP address 192.168.16.200 (server).

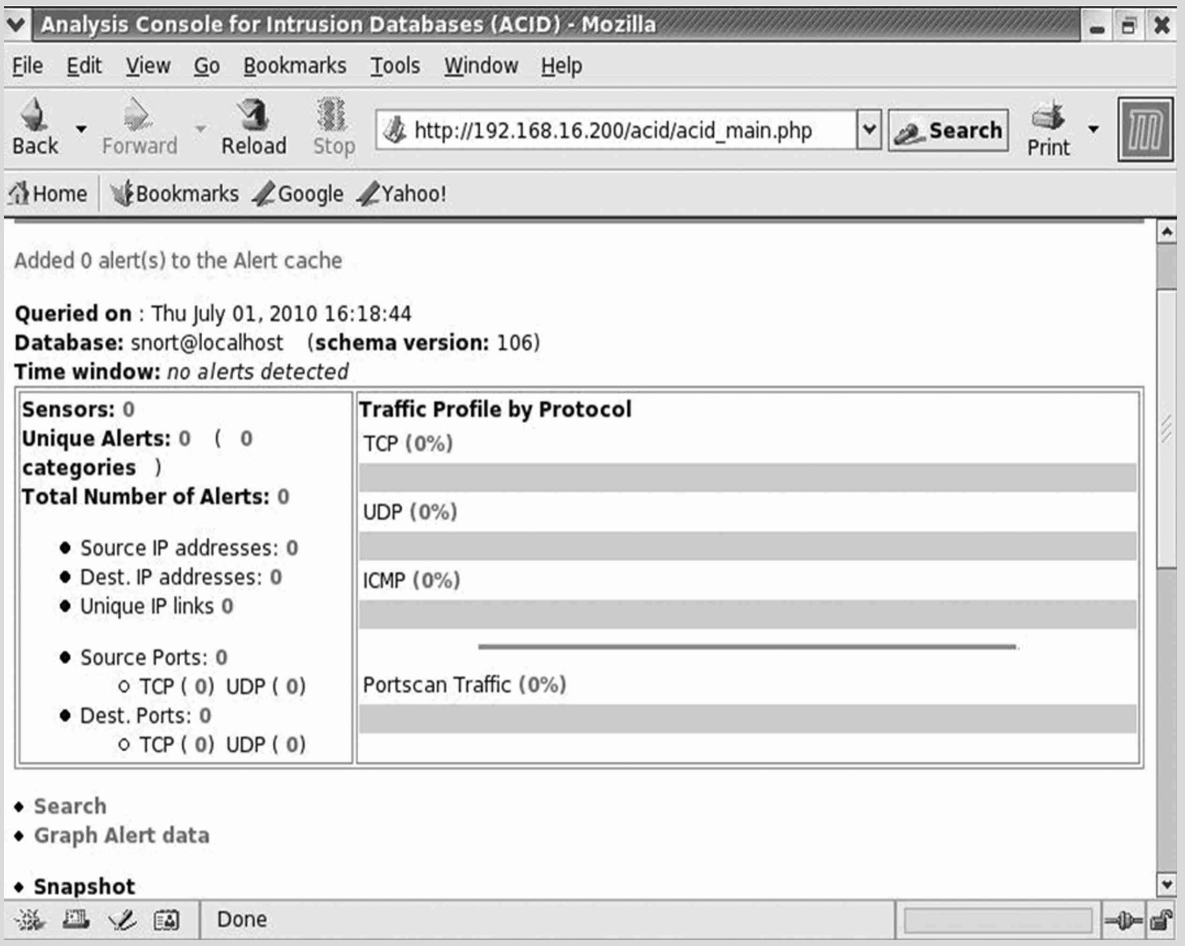
Perbedaan akan tampil pada grafik *report* di *browser* komputer *server*, yaitu terdeteksinya proses *scanning por*t oleh komputer lain.

Pada gambar t Terlihat tampilan *alert* pada ACID terdapat *report* protocol mana saja yang terserang dari komputer *server*. Terdapat lebih banyak protocol TCP (*Transmission Control Protocol*) yang terserang dibandingkan dengan protocol UDP (*User Datagram Protocol)*.

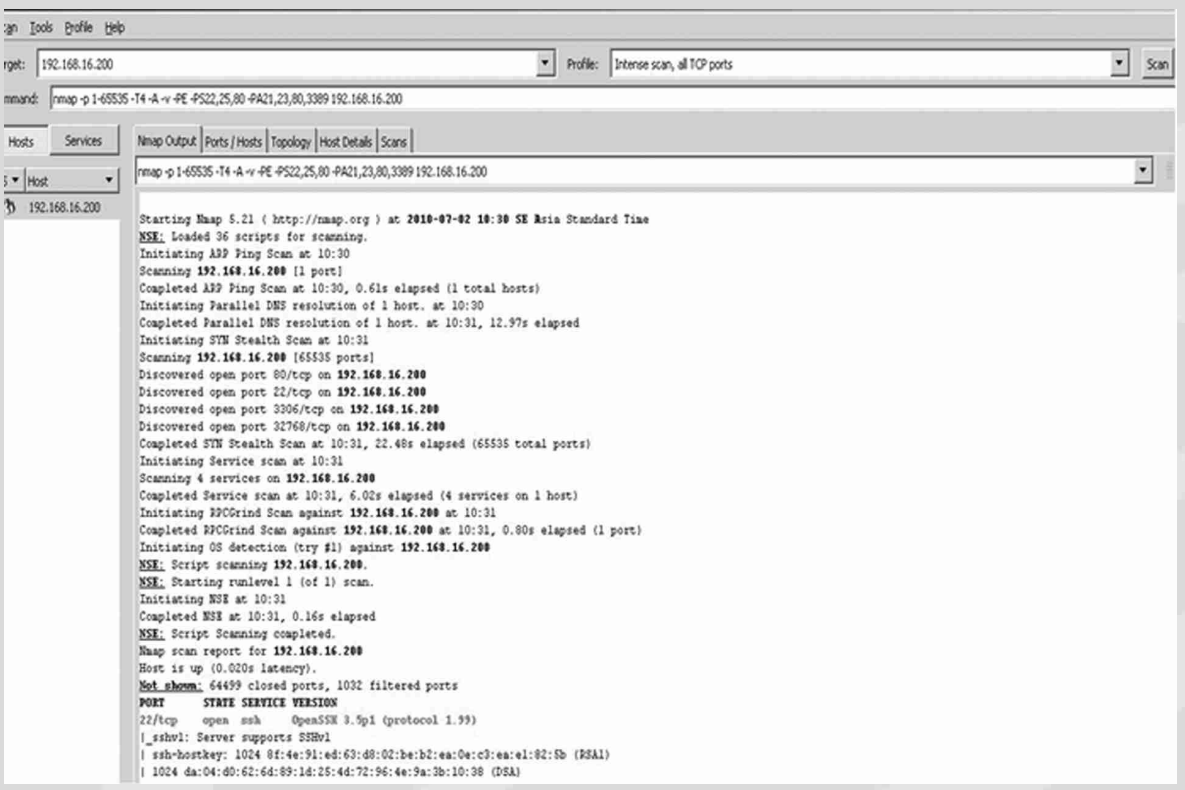
Dapat dipastikan protokol di komputer *server* yang rentan dan terbuka terhadap serangan penyusup yang didominasi oleh protokol TCP,seperti web *server*, ftp *server* dan semua layanan yang menggunakan protocol TCP.

PENUTUP

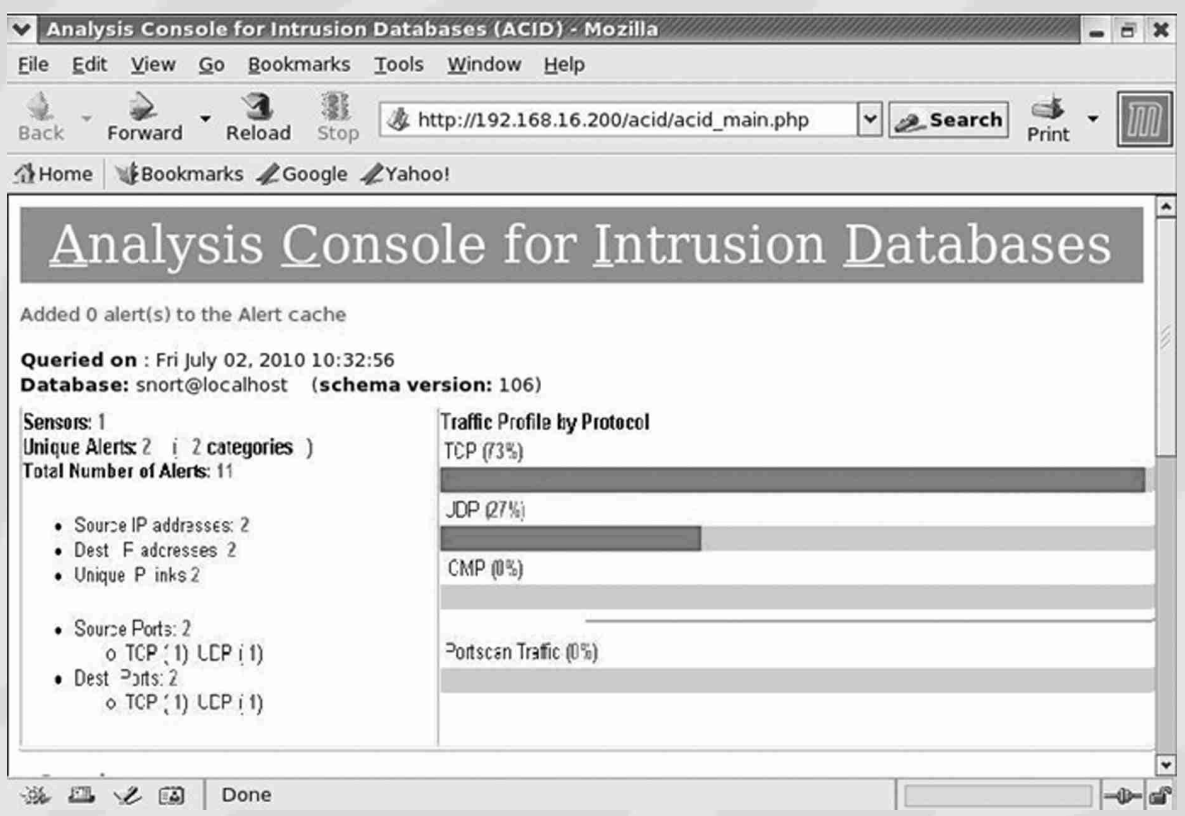
Intrusion Detection System (IDS) berguna untuk sistem pencegahan intrusi/ serangan yang dilakukan untuk melumpuhkan sebuah komputer server suatu jaringan. Dalam percobaan yang dilakukan di Laboratorium Jaringan Komputer Lepkom Universitas Gunadarma dapat dipastikan protokol di komputer *server* yang rentan dan terbuka terhadap serangan penyusup didominasi oleh protokol TCP, seperti *web server*, ftp *server* dan semua layanan yang menggunakan protocol TCP. Hal ini dibuktikan dengan hasil pengujian dan ditampilkan pada ACID, dimana serangan untuk beberapa port TCP sebesar 73%.



Gambar 5. ACID Sudah Siap Beroperasi



Gambar 6. Proses Scanning Port TCP/UDP menggunakan Nmap-Zenmap GUI



Gambar 7. Tampilan Alert

DAFTAR PUSTAKA

Caswell, Brian. 2003. *Snort 2.0 Intrusion Detection*. Syngress Publishing. USA.

Purbo, Onno W. 1998. *Buku Pintar Internet:TCP/IP*. Elex Media Komputindo. Jakarta.

Rehman, . 2003. *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID*. Prentice Hall of New Jersey.

Syafrizal, Melwin.2005. *Pengantar Jaringan Komputer*. C.V. Andi Offset.Yogyakarta.

Tanenbaum ,Andrew S. 2006. *Computer Networks. 2nd Edition*. Prentice Hall

Yuliardi, Rofiq. 2002. *Bash Scripting Untuk Administrasi Sistem Linux*. PT Elex Media Komputindo. Jakarta.

Jin Yu, Eun. 2009. *Network Intrusion Detection Systems for High Security Networkings*. IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.10,

Lehtinen,Rick. Russel, Deborah. Sr, 2006. *Computer Security Basic*. O'Reilly Media, Inc