IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT
Pada Laboratorium Jaringan Komputer LePKom Universitas Gunadarma

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

[1,2,3)]Fakultas Teknologi Industri Jurusan Teknik Informatika
Universitas Gunadarma

ABSTRAK

Laboratorium pengembangan jaringan komputer merupakan salah satu laboratorium yang dimiliki oleh Universitas Gunadarma yang bertugas menyelenggarakan kegiatan pelatihan mengenai jaringan komputer bagi seluruh civitas akademika Universitas Gunadarma. Di dalam laboratorium ini terdapat 30 komputer client 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 ketersedian layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan yang dapat merusak sistem yang ada. Untuk mengidentifikasi adanya penyusupan atau pemindaian oleh pihak-pihak yang tidak memiliki otoritas maka laboratorium pengembangan jaringan komputer menggunakan sebuah pendeteksi IDS (*Intrusion Detection System*) melalui snort IDS.

Kata kunci : IDS, Jaringan, Keamanan.

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 kedalam 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 penyusupan 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* sumberdaya sistem. *Intrusion Detection System* (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusupan . IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal.

Di sisi lain, sebuah sistem pencegahan penyusupan (IPS) merupakan perangkat lunak 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 sekumpulan komputer yang saling berhubungan dan berkomunikasi untuk bertukar data dan informasi atau berbagi *hardware*. Sebuah jaringan terhubung dengan sebuah sistem komunikasi yang membutuhkan *medium* sebagai pembawa sinyal *(carrier)*. Dimana Sistem Transmisi sinyal bisa berupa kabel, cahaya, dan lain-lain. Untuk dapat menyampaikan data Sistem Komunikasi juga membutuhkan aturan*(Rule/Protocol)*.

Berdasarkan luas area atau skala, jaringan komputer diklasifikasikan menjadi 3, yaitu :

1. LAN (*local area betwork*) yang hanya mencakup wilayah kecil
2. MAN (*Metropolitan Area Network*) yang merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN
3. WAN (*Wide Area Network*) yaitu jaringan komputer yang membutuhkan hubungan telekomunikasi jarak jauh sebagai media penghubung antar jaringan melalui jarak yang cukup jauh.

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

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

1. Server-client

   jaringan *Client-server* adalah jaringan komputer yang menggunakan beberapa komputer sebagai *server* dan beberapa komputer sebagai *client*-nya. Sebuah *service*/layanan bisa diberikan oleh sebuah komputer atau lebih komputer *server*. Dan komputer *client* dapat mengakses data
2. Peer-to-peer

   Jaringan *peer-to-peer* biasa disebut dengan *Point-to-point* adalah jaringan komputer dimana setiap *host* dapat hanya bertugas menjadi *server* atau juga hanya menjadi *client* secara bersamaan

B. Standar OSI

Dalam suatu jaringan komputer, untuk dapat saling berkomunikasi dibutuhkannya suatu bahasa yang 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 dibuatlah standarisasi. Suatu standar yang banyak digunakan saat ini adalah standar OSI *(Open System Interconction)* yang dikembangkan oleh ISO *(International Standart Organisasion)*. Pada model standar OSI ini ditetapkan model lapisan atau *layer* dimana setiap lapisan memiliki fungsi masing-masing. Pada standar OSI terdapat 7 lapisan/*layer*, diantaranya sebagai berikut:

1. Application
2. Presentation
3. Session
4. Transport
5. Network
6. Data Link
7. 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 *standart 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.

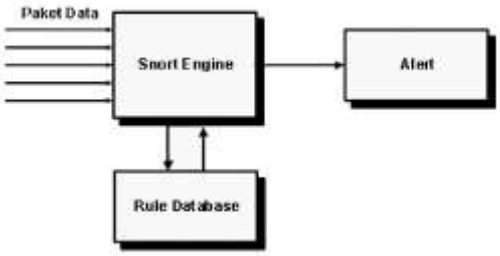
Menurut Garfinkel dan Spafford, ahli dalam komputer security, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu:

1. Availability
2. Confidentiality
3. Data Integrity
4. Control
5. Audit

F. IDS (Intrusion Detection System)

Intrusion Detection System (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).



Gambar 1. Bagian-Bagian IDS

G. Snort IDS

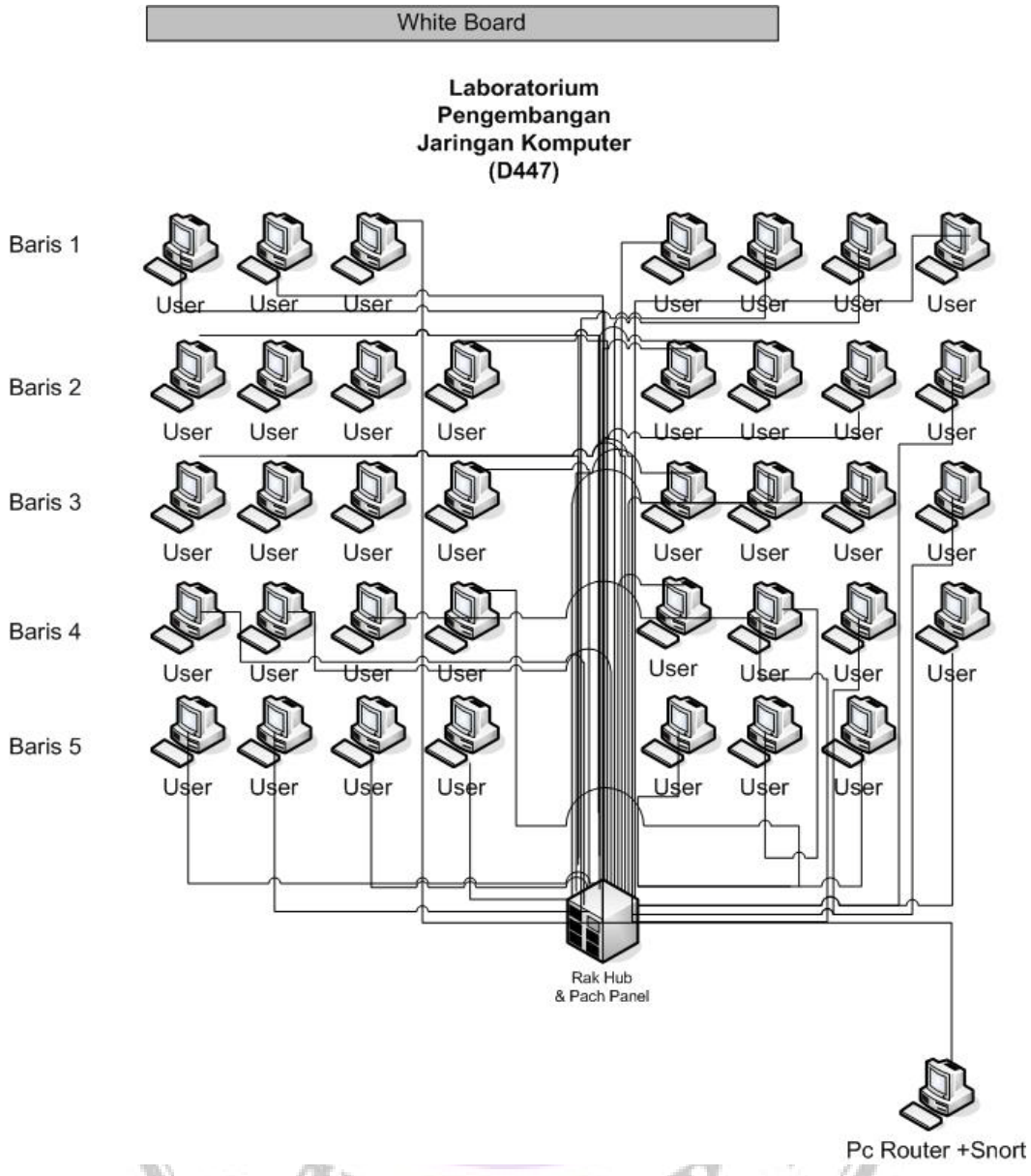
Snort IDS merupakan IDS open source yang secara defacto menjadi standar IDS di industri. Snort dapat didownload di situs www.snort.org. Snort dapat diimplementasikan dalam jaringan yang multiplatform, salah satu kelebihannya adalah mampu mengirimkan alert dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui SMB. Snort dapat berkerja dalam 3 mode: sniffer mode (penyadap), packet logger dan network intrusion detection mode.

PEMBAHASAN

Laboratorium Jaringan komputer LePKom adalah salah satu bagian laboratorium dari lembaga pengembangan komputerisasi di Universitas Gunadarma yang mengadakan pelatihan mengenai jaringan komputer kepada civitas akademika Universitas Gunadarma.

Jaringan pada laboratorium jaringan komputer LePKom merupakan jaringan LAN. Topologi jaringan yang digunakan adalah topologi star dikarenakan topologi ini lebih mudah dalam *maintanance* dan juga mudah dalam melakukan perubahan bila sewaktu-waktu ada penambahan komputer.

Laboratorium ini memiliki 30 komputer *client* yang terhubung ke dalam *patch panel box* (gabungan beberapa hub dan switch) dan 1 buah PC *router* yang juga berperan sebagai PC yang didalamnya terdapat Snort sebagai IDS (*Intrusion Detection System*). Alamat IP *private* yang digunakan memakai network 192.168.16.0 dan Netmask 255.255.255.0.



Gambar 2.Topologi Jaringan Laboratorium Jaringan Komputer LePKom

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.

Perangkat Keras dan Perangkat Lunak Yang Digunakan

Untuk membangun sebuah *Server* yang terintegrasi dengan sistem IDS sebenarnya tidak membutuhkan Perangkat Keras *(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 *client* yang akan menggunkan fasilitas dari *server*.

- **Spesifikasi perangkat keras untuk server**

Processor	: Intel Pentium 4 2,8 GHz
RAM	: 512 MB
Harddisk	: 80 GB
CDROM	: ASUS 52X
VGA	: NVIDIA GEFORCE 2 MX 64 MB Innovation
LAN card	: 3COM GB LOM(3C940) 2 buah
Client	: 30 Client
Monitor	: LG CRT 14”

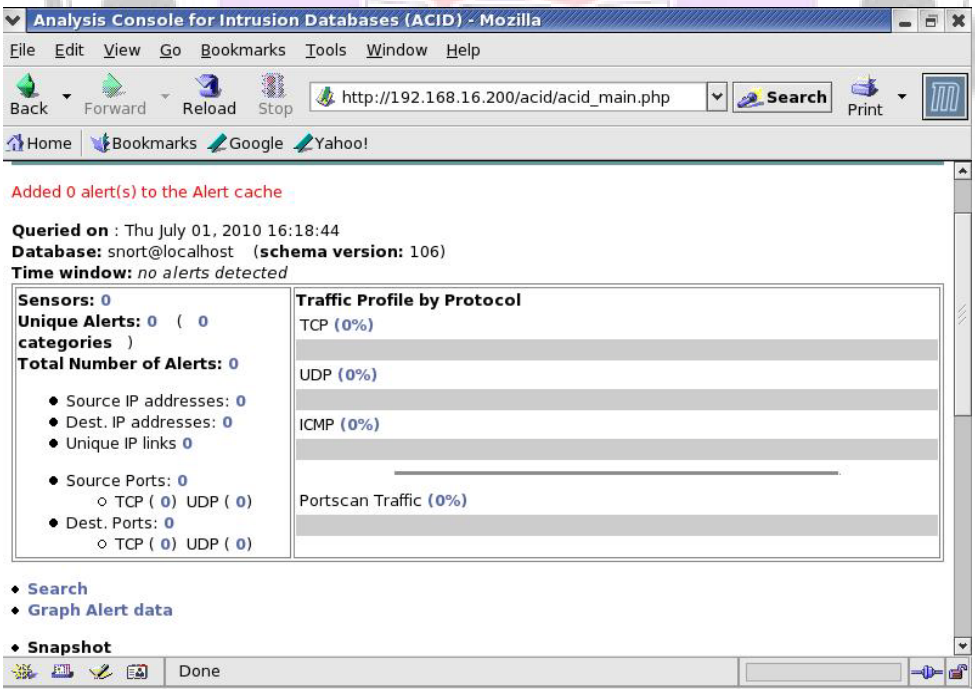
- **Spesifikasi perangkat keras untuk Client**

Processor	: AMD ATHLON 1,15 GHZ
RAM	: 256 MB
Harddisk	: 20 GB
VGA	: Inode 3D 32 MB
LAN card	: Dlink DFE 538TX
Monitor	: Beam CRT 14”

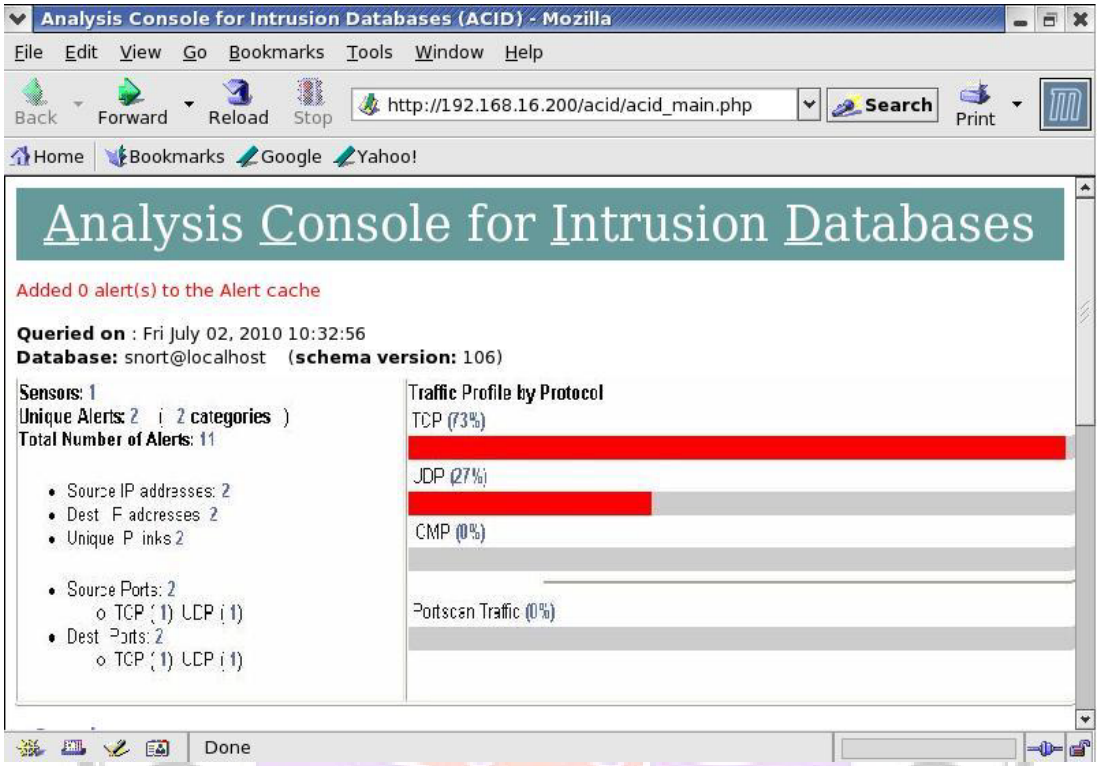
- **Spesifikasi Perangkat Lunak Untuk Server**

    1. Linux-RedHat-9.0
    2. Snort 2.0.1
    3. MySQL 4.0.14
    4. Apache 2.0.47
    5. PHP 4.3.2
    6. ADODB v3.70
    7. Acid 0.9.6b23
    8. Zlib 1.1.4
    9. JPGraph 1.12.2
    10. LibPcap 0.7.2

- **Spesifikasi Perangkat Lunak Untuk Client**
    1. Sistem Operasi Windows XP
    2. Nmap-Zenmap GUI



Gambar 3. Tampilan SNORT Dalam ACID



Gambar.4 Tampilan Alert

PENUTUP

Intrusion Detection System (IDS) berguna untuk sistem pencegahan penyusupan/serangan yang dilakukan untuk melumpuhkan sebuah komputer server suatu jaringan. Dalam percobaan yang dilakukan di laboratorium jaringan komputer LePKom Universitas Gunadarma 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. Yang dibuktikan dengan hasil pengetesan dan ditampilkan pada ACID,dimana serangan untuk beberapa port TCP sebesar 73%.

DAFTAR PUSTAKA

[1]. Caswell, Brian.2003.*Snort 2.0 Intrusion Detection*.USA:Syngress Publishing

[2]. Purbo W, Onno.*TCP/IP* .Jakarta:PT.Gramedia.1999

[3]. Yuliardi, rofiq, *Bash scripting untuk administrasi sistem Linux*. Jakarta**:**PT Elex Media Komputindo.2002.

[4] IJCSNS International Journal of Computer Science and Network 198 Security, VOL.9 No.10, October 2009

[5]. www.snort.org

[7]. www.cisco.com

[9]. www.wikipedia.org