Sistem Untuk Mendeteksi Adanya Penyusup
(IDS : Intrusion Detection System)

Jutono Gondohanindijo
Fakultas Ilmu Komputer Universitas AKI

Abstract

By the increasing use of network computer system in daily life, this system increasingly will be the target of crime, either by our enemies or by a real villain. IDS (Intrusion Detection System) is used to detect suspicious activity in a system or network. An attack or intrusion can be defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" (Sundaram, 1996). IDS will monitor traffic data on a network or retrieve data from the log file. IDS will analyze and with a certain algorithm will give warning to a network administrator.

Key words*: System, crime, intrusion, detection, integrity, administrator.*

Pengertian IDS

IDS (*Intrusion Detection System*) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

Intrusion adalah aktivitas tidak sah atau tidak diinginkan yang mengganggu konfidensialitas, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem. IDS akan memonitor lalulintas data pada sebuah jaringan atau mengambil data dari berkas log. IDS akan menganalisa dan dengan algoritma tertentu akan memutuskan untuk memberi peringatan kepada seorang administrator jaringan atau tidak.

IDS (*Intrusion Detection System*) sendiri mempunyai beberapa pengertian yaitu:

a. Sistem untuk mendeteksi adanya *intrusion* yang dilakukan oleh *intruder* (pengganggu atau penyusup) dalam jaringan. Pada awal serangan, intruder biasanya hanya mengexplore data. Namun, pada tingkat yang lebih serius intruder berusaha untuk mendapat akses ke sistem seperti membaca data rahasia, memodifikasi data tanpa permisi, mengurangi hak akses ke sistem sampai menghentikan sistem.

b. Sistem keamanan yang bekerja bersama Firewall untuk mengatasi Intrusion. *Intrusion* itu sendiri didefinisikan sebagai kegiatan yang bersifat *anomaly, incorrect, inappropite* yang terjadi di jaringan atau di host tersebut. Intrusion tersebut kemudian akan diubah menjadi *rules* ke dalam IDS (*Intrusion Detection System*).
c. Sebuah metode pengamanan jaringan dengan melakukan pendeteksian terhadap gangguan – gangguan atau intrusion yang mengganggu.
d. Sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.

Arsitektur IDS

IDS umumnya berdasar pada arsitektur *multi-tier* dari:

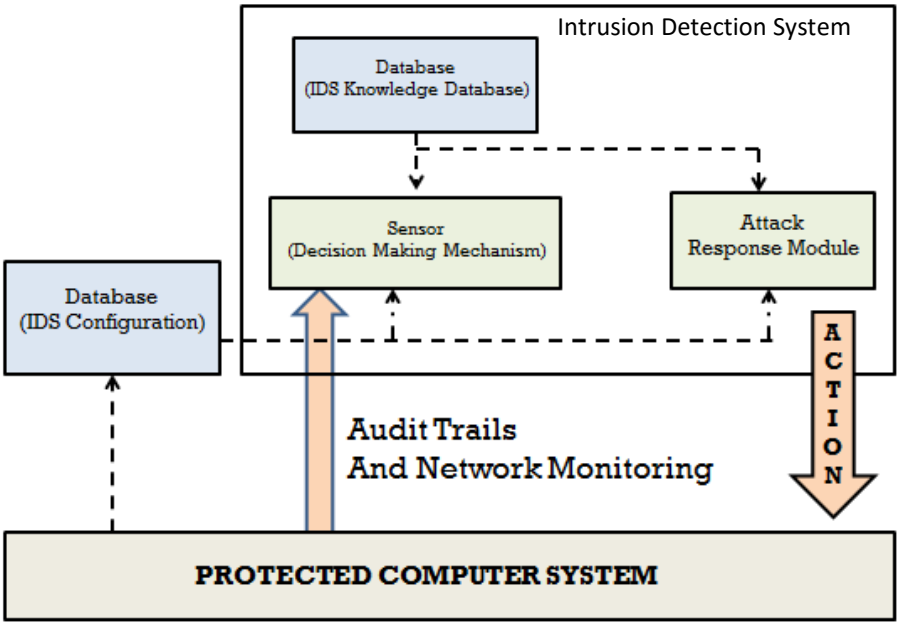
1. Teknologi deteksi, yang bergantung pada:
   a. Sensor: biasanya disebut engine/probe, merupakan teknologi yang memungkinkan IDS untuk memantau sejumlah besar traffic.
   b. Agents: Software yang di install pada suatu PC untuk memantau file atau fungsi tertentu. Dan melakukan pelaporan jika terjadi sesuatu.
   c. Collector: seperti agent, tetapi lebih kecil, dan tidak membuat keputusan, tetapi hanya menyampaikan ke manager pusat.
2. Analisis data: Proses analisis data dan data mining sejumlah besar data dilakukan oleh lapisan*(layer),* kadang diletakkan pada pusat data/server.
3. Manajemen konfigurasi/GUI : Biasa disebut juga console merupakan antarmuka operator dengan IDS.

Sensor bertugas untuk memfilter informasi dan mendiscard data yang tidak relevan dari sekumpulan kejadian yang terhubung dengan sistem terproteksi, misalnya mendeteksi aktivitas-aktivitas yang mencurigakan. Analis dilakukan dengan menggunakan database yang berisi kebijakan dalam mendeteksi. Di dalamnya terdapat tanda tangan penyerang, deskripsi perilaku normal, dan parameter yang penting (misal, nilai ambang batas). Database ini mengatur konfigurasi parameter IDS, termasuk mode komunikasi dengan modul tanggap.

Sensor diintegrasikan dengan sejumlah komponen yang bertanggung

jawab untuk pengumpulan data. Metode pengumpulan ini ditentukan oleh kebijakan dari *event generator* yang akan menjelaskan mode filtering dari suatu deskripsi informasi.

Event generator (misalnya: sistem operasi, jaringan, dan aplikasi) akan membuat sebuah kebijakan yang konsisten dalam mengeset sekumpulan kejadian yang mungkin seperti adanya sebuah log atau audit dari sistem atau paket jaringan. Berikut ini adalah diagram arsitektur IDS:



Gambar1: Diagram Arsitektur IDS

Sifat – sifat IDS

Pada umumnya, IDS mempunyai sifat-sifat sebagai berikut:

a. Suitability

Aplikasi IDS yang cenderung fokuspada skema manajemen dan arsitektur jaringan yang dihadapkannya.

b. Flexibility

Aplikasi IDS yang mampu beradaptasi dengan spesifikasi jaringan yang akan dideteksi oleh aplikasi tersebut.

c. Protection

Aplikasi IDS yang secara ketat memproteksi gangguan yang sifatnya utama dan berbahaya.

d. Interoperability

Aplikasi IDS yang secara umum mampu beroperasi secara baik dengan perangkat-perangkat keamanan jaringan serta manajemen jaringan lainnya.

e. Comprehensiveness

Kelengkapan yang dimiliki oleh aplikasi IDS ini mampu melakukan sistem pendeteksian secara menyeluruh seperti pemblokiran semua yang berbentuk Java Applet, memonitor isi dari suatu email.

f. Event Management

Konsep IDS yang mampu melakukan proses manajemen suatu jaringan serta proses pelaporan pada saat dilakukan setiap pelacakan, bahkan aplikasi ini mampu melakukan updating pada sistem basis data pola suatu gangguan.

g. Active Response

Pendeteksi gangguan ini mampu secara cepat untuk mengkonfigurasi saat munculnya suatu gangguan, biasanya aplikasi ini berintegrasi dengan aplikasi lainnya seperti aplikasi Firewall serta aplikasi IDS ini dapat mengkonfigurasi ulang spesifikasi router pada jaringannya.

h. Support

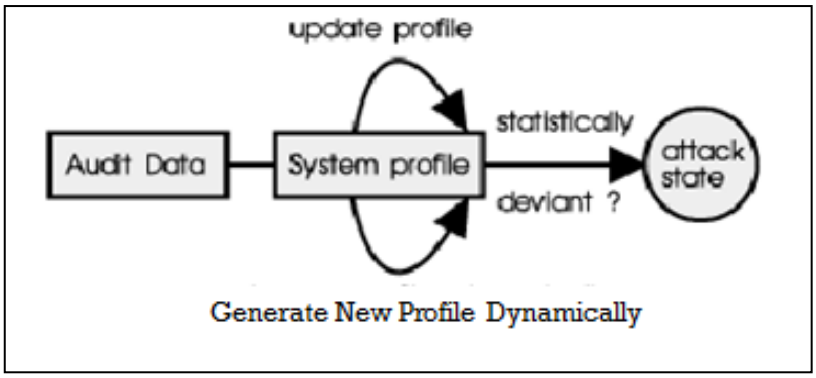
Lebih bersifat mendukung pada suatu jenis produk apabila diintegrasikan dengan aplikasi lain.

Teknik deteksi IDS

Berikut ini adalah teknik deteksi yang digunakan dalam IDS:

a. Teknik Deteksi Anomali (Anomaly Detection/Behavior Based)

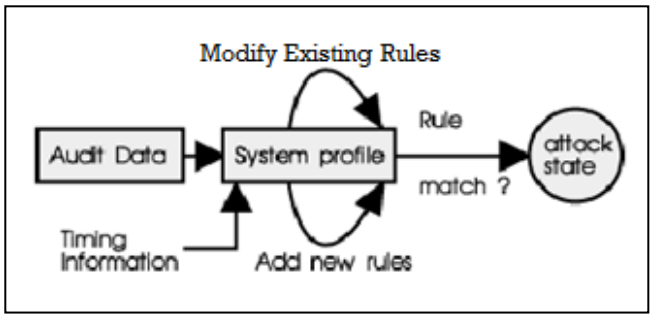
Behavior Base adalah cara kerja IDS (*Intrusion Detection System*) dengan mendeteksi adanya penyusupan dengan mengamati adanya kejanggalan – kejanggalan pada sistem, yaitu adanya keanehan dan kejanggalan dari kondisi pada saat sistem normal, sebagai contoh : adanya penggunaan memory yang melonjak secara terus menerus atau terdapatnya koneksi secara paralel dari satu IP dalam jumlah banyak dan dalam waktu yang bersamaan. Kondisi tersebut dianggap kejanggalan yang selanjutnya oleh IDS Anomaly Based ini dianggap sebagai serangan.



Gambar 2 : Typical Anomaly Detection System

b. Teknik Deteksi Penyalahgunaan (Misuse Detection/ Knowledge Based)

Knowledge Based adalah IDS mengenali adanya penyusupan dengan cara menyadap paket data kemudian membandingkannya dengan database rule pada IDS tersebut. Database rule tersebut dapat berisi signature – signature paket serangan. Jika pattern atau pola paket data tersebut terdapat kesamaan dengan rule pada database rule pada IDS maka paket data tersebut dianggap sebagai serangan.

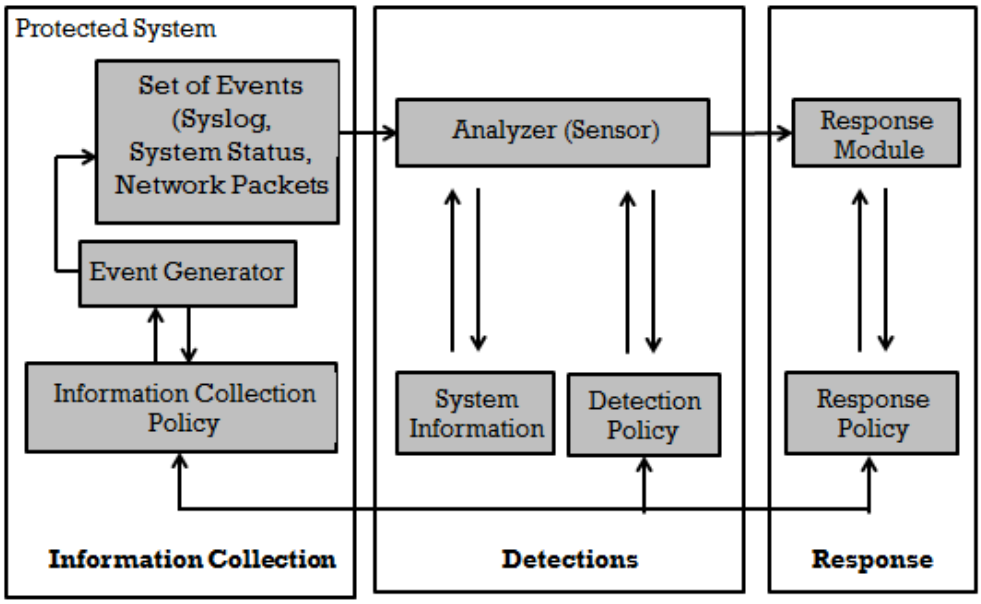


Gambar 3 : Typical Misuse Detection System

Cara kerja IDS

IDS melindungi sistem komputer dengan mendeteksi serangan dan menghentikannya. Awalnya, IDS melakukan pencegahan intrusi. Untuk itu, IDS mengidentifikasi penyebab intrusi dengan cara membandingkan antara event yang dicurigai sebagai intrusi dengan signature yang ada. Saat sebuah intrusi telah terdeteksi, maka IDS akan mengirim sejenis peringatan ke administrator. Langkah selanjutnya dimulai dengan melakukan policy terhadap administrator dan IDS itu sendiri.

Komponen yang menyusun kerja sebuah IDS bisa dilihat pada diagram berikut:



Gambar 4 : Komponen Kerja Sebuah IDS

Ada beberapa cara bagaimana IDS bekerja. Cara yang paling populer adalah dengan menggunakan pendeteksian berbasis signature (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.

Cara lainnya adalah dengan mendeteksi adanya anomali, teknik yang lainnya adalah dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap log sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

Jenis – jenis IDS

Jenis – jenis IDS dapat dikategorikan sebagai berikut:

1. *Network-based Intrusion Detection System (NIDS)*

Memantau Anomali di Jaringan dan mampu mendeteksi seluruh host yang berada dalam satu jaringan. Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Contoh: melihat adanya network scanning.

2. *Host-based Intrusion Detection System (HIDS)*

Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya firewall, web server, atau server yang terkoneksi ke Internet. Contoh: memonitor logfile, process dan file ownership.

Kelebihan dan Kelemahan IDS

IDS memiliki beberapa kelebihan diantaranya sebagai berikut:

a. Memiliki Akurasi keamanan yang baik
   IDS telah memiliki ketelitian tinggi, yaitu mampu secara realtime mendeteksi dan melakukan blocking terhadap tindakan yang mencurigakan. IDS juga mampu memeriksa dan menganalisa pattern objek secara menyeluruh yang dipergunakan serta membedakan paket data yang keluar masuk dalam lalu lintas jaringan sehingga dapat mengenal benar karakteristik trafic penyerang.
b. Mampu Mendeteksi dan Mencegah Serangan.
   IDS dapat mendeteksi serangan dan juga mampu untuk melakukan pencegahan terhadap serangan tersebut.
c. Memiliki cakupan yang Luas dalam Mengenal Proses Attacking.
   IDS memiliki pengetahuan yang luas, dapat mengenal serangan apa yang belum dikenalnya dan mampu mendeteksi segala sesuatu yang mencurigakan.
d. Dapat memberikan Informasi tentang ancaman – ancaman yang terjadi.
e. Memiliki tingkat Forensik yang canggih dan mampu menghasilkan reporting yang baik.
f. Memiliki sensor yang dapat dipercaya untuk memastikan pendeteksian dan pencegahan

Sedangkan kelemahan IDS sendiri adalah:

a. Alarm palsu

Sering terjadinya alarm ataupun gangguan yang bersifat palsu, yaitu paket data yang datang terdeteksi sebagai intrusion karena tidak sesuai dengan rule–rule yang dibuat. Setelah diteliti ternyata hanya paket data biasa dan tidak berbahaya.

b. Variants

Mengetahui sukses atau tidaknya, sebuah set signature harus cukup unik untuk memberikan peringatan atau alert pada saat yang memang berbahaya. Kesulitannya adalah kode-kode untuk exploit itu dengan mudahnya dimodifikasi oleh penyerangnya, jadi sangat memungkinkan sekali banyak terjadi variasi pada kodenya.

c. False Positives

Merupakan alert yang memberitahu adanya aktifitas yang berpotensi berupa serangan, tetapi masih ada kemungkinan bahwa ternyata aktifitas tersebut bukan sebuah serangan. Kesulitannya adalah apabila jumlah alert banyak dan sulit untuk menyaring mana yang memang benar-benar serangan atau bukan.

d. False Negatives

Kelemahan ini terjadi pada kondisi dimana IDS tidak dapat mendeteksi adanya serangan, karena tidak mengenal signature-nya. Jadi IDS tidak memberikan alert, walaupun sebenarnya serangan terhadap sistem tersebut sedang berlangsung.

e. Data Overload

Hal ini merupakan aspek yang tidak berhubungan secara langsung dengan teknik IDS yang digunakan, tetapi sangatlah penting bila melihat dari segi seberapa besar efisiensi dan efektifitas hasil kerja analis dalam menganalisa data-data dalam IDS secara keseluruhan.

Contoh program IDS

Ada banyak program yang bisa dipakai untuk IDS diantaranya adalah:

a. Tcplogd

Program yang mendeteksi *stealth scan. Stealth scan* adalah scanning yang dilakukan tanpa harus membuat sebuah sesi tcp. Sebuah koneksi tcp dapat terbentuk jika klien mengirimkan paket dan server mengirimkan kembali paketnya dengan urutan tertentu, secara terus menerus sehingga sesi tcp dapat berjalan. Stealth scan memutuskan koneksi tcp sebelum klien menerima kembali jawaban dari server. Scanning

model ini biasanya tidak terdeteksi oleh log umum di linux.

b. HostSentry

Program yang mendeteksi login anomali. Anomali disini termasuk perilaku aneh (*bizzare behaviour*), anomali waktu (*time anomalies*), dan anomali lokal (*local anomalies*).

c. Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort merupakan sebuah produk terbuka yang dikembangkan oleh Marty Roesch dan tersedia gratis. Snort bisa digunakan pada sistem operasi Linux, Windows, BSD dan Solaris. Snort merupakan IDS berbasis jaringan yang menggunakan metode deteksi rule based, menganalisis paket data apakah sesuai dengan jenis serangan yang sudah diketahui olehnya.

Kesimpulan

Betapapun banyaknya administrator yang bertugas untuk mendeteksi atau menganalisis intrusi secara manual tidaklah efektif jika dibandingkan dengan penggunaan komponen pendeteksi intrusi seperti IDS. Meskipun demikian, tidak ada jawaban yang jelas mengenai teknik mana yang lebih baik karena masing-masing memiliki kelebihan dan kelemahan. Bukan IDS yang mengamankan suatu organisasi, tetapi orang-orang yang me-managenya. Untuk mencapai tingkat keamanan yang maximum, maka sebaiknya kita memadukan kedua teknologi keamanan yaitu IDS dan Firewall.

Daftar Pustaka

Sundaram, A. (1996),*An Introduction to Intrusion Detection System,*. USA: Whitepaper.

Unila.(n.d.). Retrieved January 23, 2011, from http://blog.unila.ac.id/zoehellmie87/2010/09/18/intrusion-detection-system/

Wardhani, H. M. (n.d.). Retrieved January 29, 2011, from http://helenamayawardhani.wordpress.com/2010/06/07/intrusion-detection-system-s/

Wikipedia. (n.d.). Retrieved January 17, 2011, from http://id.wikipedia.org/wiki/Sistem_deteksi_intrusi