PENGGUNAAN SISTEM IDS (*Intrution detection System*) UNTUK PENGAMANAN JARINGAN DAN KOMPUTER

MUHAMMAD RUDYANTO ARIEF
rudy@amikom.ac.id
http://rudy.amikom.ac.id

Abstraksi

Penggunaan internet saat ini merupakan suatu kebutuhan yang tidak dapat di tunda-tunda lagi keberadaannya. Dengan internet menjadikan segala sesuatunya lebih mudah. Karena sifat internet yang 24x7x12 (24 jam sehari, 7 hari seminggu, 12 bulan setahun) sehingga orang tetap dapat berkomunikasi dimanapun dan kapanpun tanpa batasan waktu dan jarak. Namun dibalik semua kemudahan dan keuntungan yang didapatkan dengan hadirnya internet maka muncul pula masalah yang mengikutinya. Masalah tersebut adalah masalah keamanan data yang dikirimkan melalui internet. Semua tahu bahwa di internet tidak ada yang menjadi pemilik terhadap sesuatu. Sehingga setiap orang berhak melakukan apapun di internet termasuk hal-hal yang merugikan orang lain. Untuk mengatasi masalah keamanan jaringan dan komputer ada banyak pendekatan yang dapat dilakukan. Salah satunya adalah dengan menerapkan sistem IDS (*Intrution Detection System*).

Kata Kunci : *IDS, Firewall, Port, SNORT*

Apa itu IDS?

IDS (*Intrution Detection System*) adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan. Dalam banyak kasus IDS juga merespon terhadap *traffic* yang tidak normal/ anomali melalui aksi pemblokiran seorang user atau alamat IP (*Internet Protocol*) sumber dari usaha pengaksesan jaringan.

IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda yang intinya berfungsi untuk mendeteksi *traffic* yang mencurigakan didalam sebuah jaringan. Beberapa jenis IDS adalah : yang berbasis jaringan (NIDS) dan berbasis host (HIDS). Ada IDS yang bekerja dengan cara mendeteksi berdasarkan pada pencarian ciri-ciri khusus dari percobaan yang sering dilakukan. Cara ini hampir sama dengan cara kerja perangkat lunak antivirus dalam mendeteksi dan melindungi sistem terhadap ancaman. Kemudian ada juga IDS yang bekerja dengan cara mendeteksi berdasarkan pada pembandingan pola *traffic* normal yang ada dan kemudian mencari ketidaknormalan *traffic* yang ada. Ada IDS yang fungsinya hanya sebagai pengawas dan pemberi peringatan ketika terjadi serangan dan ada juga IDS yang bekerja tidak hanya sebagai pengawas dan pemberi peringatan melainkan juga dapat melakukan sebuah kegiatan yang merespon adanya percobaan serangan terhadap sistem jaringan dan komputer.

Jenis-jenis IDS

NIDS (*Network Intrusion Detection System*)

IDS jenis ini ditempatkan disebuah tempat/ titik yang strategis atau sebuah titik didalam sebuah jaringan untuk melakukan pengawasan terhadap *traffic* yang menuju dan berasal dari semua alat-alat (*devices*) dalam jaringan. Idealnya semua *traffic* yang berasal dari luar dan dalam jaringan di lakukan di *scan*, namun cara ini dapat menyebabkan *bottleneck* yang mengganggu kecepatan akses di seluruh jaringan.

HIDS (*Host Intrution Detection System*)

IDS jenis ini berjalan pada *host* yang berdiri sendiri atau perlengkapan dalam sebuah jaringan. Sebuah HIDS melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada user atau administrator sistem jaringan akan adanya kegiatan-kegiatan yang mencurigakan yang terdeteksi oleh HIDS.

Signature Based

IDS yang berbasis pada *signature* akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data *signature* yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui. Cara ini hampir sama dengan cara kerja aplikasi antivirus dalam melakukan deteksi terhadap *malware*. Intinya adalah akan terjadi keterlambatan antara terdeteksinya sebuah serangan di internet dengan *signature* yang digunakan untuk melakukan deteksi yang di implementasikan didalam basis data IDS yang digunakan. Jadi bisa saja basis data *signature* yang digunakan dalam sistem IDS ini tidak mampu mendeteksi adanya sebuah percobaan serangan terhadap jaringan karena informasi jenis serangan ini tidak terdapat dalam basis dat *signature* sistem IDS ini. Selama waktu keterlambatan tersebut sistem IDS tidak dapat mendeteksi adanya jenis serangan baru.

Anomaly Based

IDS jenis ini akan mengawasi *traffic* dalam jaringan dan melakukan perbandingan *traffic* yang terjadi dengan rata-rata *traffic* yang ada (stabil). Sistem akan melakukan identifikasi apa yang dimaksud dengan jaringan “normal” dalam jaringan tersebut, berapa banyak *bandwidth* yang biasanya digunakan di jaringan tersebut, protolkol apa yang digunakan, port-port dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika dideteksi ada yang tidak normal, atau secara signifikan berbeda dari kebiasaan yang ada.

Passive IDS

IDS jenis ini hanya berfungsi sebagai pendeteksi dan pemberi peringatan. Ketika *traffic* yang mencurigakan atau membahayakan terdeteksi oleh IDS maka IDS akan membangkitkan sistem pemberi peringatan yang dimiliki dan dikirimkan ke administrator atau user dan selanjutnya terserah kepada administrator apa tindakan yang akan dilakukan terhadap hasil laporan IDS.

Reactive IDS

IDS jenis ini tidak hanya melakukan deteksi terhadap *traffic* yang mencurigakan dan membahayakan kemudian memberi peringatan kepada administrator tetapi juga mengambil tindakan pro aktif untuk merespon terhadap serangan yang ada. Biasanya dengan melakukan pemblokiran terhadap *traffic* jaringan selanjutnya dari alamat IP sumber atau user jika alamat IP sumber atau user tersebut mencoba untuk melakukan serangan lagi terhadap sistem jaringan di waktu selanjutnya.

Implementasi IDS di dunia nyata/ *real world*

Salah satu contoh penerapan IDS di dunia nyata adalah dengan menerapkan sistem IDS yang bersifat *open source* dan gratis. Contohnya SNORT. Aplikasi Snort tersedia dalam beberapa macam *platform* dan sistem operasi termasuk Linux dan Window$. Snort memiliki banyak pemakai di jaringan karena selain gratis, Snort juga dilengkapi dengan *support system* di internet sehingga dapat dilakukan *updating signature* terhadap Snort yang ada sehingga dapat melakukan deteksi terhadap jenis serangan terbaru di internet.

IDS tidak dapat bekerja sendiri jika digunakan untuk mengamankan sebuah jaringan. IDS harus digunakan bersama-sama dengan *firewall*. Ada garis batas yang tegas antara *firewall* dan IDS. Juga ada teknologi yang disebut dengan IPS (*Intrusion Prevention System*). IPS pada dasarnya adalah sebuah *firewall* yang dikombinasikan dengan level jaringan dan level aplikasi dengan sebuah *reactive* IDS untuk melindungi jaringan secara pro aktif.

Pada dasarnya, *firewall* adalah titik pertama dalam garis pertahanan sebuah sistem jaringan komputer. Seharusnya *firewall* diatur agar melakukan penolakan (*DENY*) terhadap semua *traffic* yang masuk kedalam sistem dan kemudian membuka lubang-lubang yang perlu saja. Jadi tidak semua lubang dibuka ketika sistem melakukan hubungan ke jaringan luar. Idealnya *firewall* diatur dengan konfigurasi seperti diatas. Beberapa port yang harus dibuka untuk melakukan hubungan keluar adalah port 80 untuk mengakses internet atau port 21 untuk FTP file server. Tiap-tiap port ini mungkin penting untuk tetap dibuka tetapi lubang-lubang ini juga merupakan potensi kelemahan atas terjadinya serangan yang akan masuk kedalam jaringan. *Firewall* tidak dapat melakukan pemblokiran terhadap jenis serangan ini karena administrator sistem telah melakukan konfigurasi terhadap *firewall* untuk membuka kedua port tersebut. Untuk tetap dapat memantau *traffic* yang terjadi di kedua port yang terbuka

tersebut dibutuhkan sebuah sistem yang dapat melakukan deteksi terhadap *traffic* yang membahayakan dan berpotensi menjadi sebuah serangan. Disinilah fungsi IDS dibutuhkan. Dapat saja digunakan/ di implementasikan sebuah NIDS melalui seluruh jaringan atau sebuah HIDS pada alat-alat tertentu yang dirasa berpotensi terhadap serangan. IDS akan me-monitor *traffic* yang masuk dan keluar jaringan dan meng-identifikasi *trafic* yang mencurigakan dan membahayakan yang mungkin saja dapat melewati *firewall* atau dapat saja berasal dari dalam jaringan. Jadi IDS tidak hanya mendeteksi serangan dari luar tetapi juga potensi serangan dari dalam jaringan sendiri.

IDS dapat saja menjadi sebuah alat yang hebat untuk melakukan pengawasan secara pro aktif dan melakukan perlindungan jaringan dari kegiatan-kegiatan yang membahayakan, bagaimanapun juga IDS cenderung dapat memberikan peringatan yang salah. Intinya tidak ada sistem yang sempurna untuk mengamankan sebuah jaringan komputer. Ketika menggunakan IDS maka sistem administrasi harus sering melakukan *tune-up* terhadap sistem IDS yang di implementasikan. IDS juga harus di konfigurasi secara tepat untuk mampu mendeteksi apa itu *trafic* yang normal dalam jaringan dan apa itu *traffic* yang membahayakan. Untuk mendefinisikan hal tersebut diatas diperlukan seorang administrator sistem yang mampu memberikan respon terhadap sistem pemberi peringatan IDS. Dibutuhkan pengertian apa arti peringatan tersebut dan bagaimana meng-efektifkan respon tersebut.

Idealnya IDS ditempatkan bersama-sama dengan *firewall* dan di tiap titik yang berpotensi untuk mendapat serangan. Seperti diletakkan di server utama dari sebuah sistem jaringan yang berhubungan langsung dengan jaringan luar. Selain di server utama IDS dapat juga diletakkan di *Gateway* yang merupakan penghubung antara jaringan internal dengan internet. IDS sendiri berbeda dengan *firewall*. Jika IDS bekerja hanya sebagai pendeteksi dan pemberi peringatan dini terhadap kondisi jaringan yang berpotensi merusak sistem jaringan maka *firewall* bekerja untuk mencari tahu ada tidaknya gangguan kemudian menghentikan gangguan tersebut sebelum benar-benar masuk kedalam sistem jaringan. *Firewall* juga membatasi akses antara jaringan dengan tujuan untuk mencegah terjadinya gangguan tetapi tidak memberi tanda akan adanya serangan yang berasal dari dalam jaringan itu sendiri. IDS mengevaluasi gangguan yang mencurigakan ketika kegiatan tersebut terjadi dan langsung memberikan peringatan. IDS juga mengawasi serangan yang berasal dari dalam sistem jaringan tersebut. Sehingga dalam implementasinya IDS dan *Firewall* selalu digunakan bersama-sama sebagai sistem pengamanan jaringan dan komputer.

Kesimpulan

Sebagai salah satu sistem pengamanan jaringan dan komputer, IDS hanya cocok digunakan sebagai salah satu sistem pengamanan dan tidak dapat dijadikan sebagai satu-satunya sistem tunggal untuk mengamankan jaringan. Karena karakteristik IDS yang hanya berfungsi sebagai pendeteksi dan pemberi peringatan terhadap gangguan yang datang dari luar dan dalam sistem jairngan itu sendiri. Sehingga IDS harus dikombinasikan dengan beberapa metode pengamanan lain untuk melengkapi kekurangan-kekurangan yang dimiliki oleh IDS. Misalnya dengan menggunakan *Firewall* sebagai tambahan. Banyak aplikasi IDS yang ada saat ini, namun yang paling banyak digunakan adalah aplikasi SNORT. Karena selain *free* Snort juga mendukung semua *platform* dan berbagai macam sistem operasi. Selain itu Snort juga berbasis *open source*.

Daftar Pustaka

- http://netsecurity.about.com/cs/hackertools/a/aa030504p.htm (From Tony Bradley, CISSP, MCSE2k, MCSA, A+)
- http://www.webopedia.com/TERM/I/intrusion_detection_system.html
- http://css.its.psu.edu/netpeople/May2002/sos501.html