IMPLEMENTASI SNORT SEBAGAI INTRUSION DETECTION SYSTEM (IDS) PADA JARINGAN INTERNET SMK KARYA MULIA MUARO

(STUDI KASUS SMK KARYA MULIA MUARO)

TUGAS AKHIR

Oleh

DESWIRA HARNETI
06110124

Program Studi Teknik Komputer
Konsentrasi : Teknologi Komputer dan Jaringan
Jurusan Teknologi Informasi

POLITEKNIK UNIVERSITAS ANDALAS
PADANG
2009

ABSTRAK

Seiring dengan perkembangan Teknologi Informasi saat ini yang selalu berubah, menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan Internet. Namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi tidak diiringi dengan perkembangan pada sistem keamanan itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan harus ditingkatkan dinding keamanannya.

Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Serangan tersebut berupa serangan Hacker yang bermaksud merusak jaringan komputer yang terkoneksi pada Internet ataupun mencuri informasi penting yang ada pada jaringan tersebut.

Hadirnya firewall telah banyak membantu dalam pengamanan, akan tetapi seiring berkembangnya teknologi sekarang ini, firewall saja belum bisa menjamin keamanan sepenuhnya. Karena itu telah berkembang teknologi *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) sebagai pembantu pengaman data pada suatu jaringan komputer. Dengan adanya IDS dan IPS, maka serangan-serangan tersebut lebih dapat dicegah ataupun dihilangkan. IDS berguna untuk mendeteksi adanya serangan dari penyusup (serangan dari dalam) IPS berguna untuk mendeteksi serangan dan menindaklanjutinya dengan pemblokan serangan.

Kata Kunci : Intrusion Detection System (IDS), *firewall, Snort, ACID, MySQL*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era teknologi informasi saat ini, hampir seluruh informasi yang penting bagi suatu institusi dapat diakses oleh para penggunanya. Keterbukaan akses tersebut memunculkan masalah baru seperti :

1. Pemeliharaan validitas dan integrasi data/informasi tersebut.
2. Jaminan ketersediaan informasi bagi pengguna.
3. Pencegahan dari informasi yang tidak berhak.
4. Pencegahan akses sistem dari yang tidak berhak.

Sistem pertahanan terhadap aktivitas di atas biasanya dilakukan secara manual oleh sistem administrator. Hal ini dapat membuat kecepatan administrator dalam menanggulangi gangguan di atas berkurang dan dapat menyebabkan malfungsi pada sistem sehingga sistem administrator tidak dapat mengakses jaringan secara *remote* yang mengakibatkan sistem administrator tidak dapat melakukan pemulihan sistem secara cepat.

Oleh karena itu penulis mengangkat judul "**Implementasi Snort sebagai *Intrusion Detection System* (IDS) pada Jaringan Internet SMK Karya Mulia Muaro**" agar nantinya dapat melakukan pencatatan (*logging*) terhadap aktivitas yang terjadi dalam jaringan komputer dan sistem IDS tersebut dapat menanggulangi ancaman secara *optional* dalam waktu yang cepat dan secara akurat. Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan menganalisa paket yang melewati jaringan secara *real time traffic* dan *logging*

ke dalam *database* serta mampu mendeteksi serangan yang berasal dari luar jaringan, selain itu juga snort merupakan *software* yang bersifat gratis yang dapat di*download* secara bebas dan dapat diimplementasikan dihampir semua *flatform* sistem operasi.

1.2 Rumusan Masalah

Masalah yang terjadi di SMK yang menyebabkan harus dibangunnya snort adalah :

1. Sering terjadi akses dari *network* lain yang merugikan/membebani jaringan yang belum diketahui.
2. Banyaknya aktifitas *illegal* yang terjadi dalam jaringan seperti *flooding* dan *eksploit*.
3. Sering terputusnya koneksi yang ada dan kemungkinan disebabkan oleh aktifitas yang *illegal*.

1.3 Tujuan

Adapun tujuan dari studi yang ingin dicapai antara lain adalah :

1. Untuk melihat dan mengetahui bagaimana snort sebagai komponen IDS melakukan *logging* dan *monitoring* aktifitas jaringan.
2. Untuk melihat apakah snort mampu melakukan deteksi terhadap aktifitas yang *illegal* dalam jaringan komputer.
3. Menerapkan beberapa *rule* untuk mengatasi aktifitas *illegal* seperti *flooding* dan *eksploit*.

BAB V

PENUTUP

Berdasarkan perancangan, implementasi dan pengujian dengan judul Implementasi Snort Sebagai *Intrusion Detection System* (IDS) pada jaringan Internet SMK Karya Mulia maka dapat diambil kesimpulan dan batasan kemampuan sistem serta saran yang merupakan hasil dari penulisan tugas akhir ini.

5.1 Kesimpulan

Berdasarkan perancangan, implementasi dan pengujian maka dapat ditarik kesimpulan sebagai berikut :

1. Penggunaan snort sebagai paket *logger* sudah sangat baik untuk diterapkan. Selain hasil *capture* yang optimal juga didukung dengan *monitoring* berbasis web yang memudahkan seorang admin untuk melakukan administrasi jaringan.
2. Dukungan dari pengembang snort dalam melakukan *update vurnereability* terhadap *rule snort* schingga aplikasi ini sangat tangguh karena selalu *up-to-date*.
3. Administrator harus memasukkan *rule* ke firewall secara manual berdasarkan *log* snort karena snort belum mampu melakukan bloking terhadap serangan secara otomatis.
4. Sistem *security* jaringan selalu berbanding terbalik dengan kenyamanan akses pengguna.

DAFTAR PUSTAKA

Ariyus. Dony. (2007). *Intrusion Detection System*. Andi.Yogyakarta.

Hartono, Puji. (2006). *Sistem pencegahan Penyusupan pada Jaringan Berbasis Snort IDS dan IPTables Firewall*.

IGN Mantra. (2008). Proceeding, Seminar Ilmiah Nasional Komputer dan Sistem Intelijen. KOMMIT.

Lamell. Todd. (2004). *Cisco Certified Network*, Gramedia Pustaka.

Niall Mansfield. (2005). *Practical TCP/IP - Mendesain, Menggunakan, dan Troubleshooting Jaringan TCP/IP di Linux dan Windows*, Andi offset.

Sarosa, Moechammad. (2000). *Jaringan Komputer Data Link. Network & Issue*. Yogyakarta.

Tanenbaum, AS. (1996). *Computer Networks*. Prentise Hall.

W.Purbo, Onno. (2000). *TCP/IP*, Elexmedia Computindo

http://budi.insan.co.id/courses/security/2006/puji_report.pdf. Mei 2009

http://student.eepis-its.edu/~izankboy/laporan/Jaringan/ccna2-1.pdf. Mei 2009

http://www.snort.org/assets/110/Snort_2.8.4.1_FC11.pdf. Mei 2009

http://www.snort.org/assets/82/snort_manual.pdf. Mei 2009

www.Netfilter.org/Iptables. Mei 2009