ADMINISTRASI INTRUSION DETECTIN SISTEM (IDS) BERBASIS WEB

Indra Zulkarnain[1], Fazmah Arief Yulianto[2], Endro Ariyanto[3]

[1]Teknik Informatika, Fakultas Ilmu Terapan, Universitas Telkom

Abstrak

Ancaman terhadap komputer yang tehubung pada jaringan setiap harinya selalu mengalami peningkatan. Berbagai ancaman seperti deface pada webserver, percobaan untuk menembus firewall serta serangan terhadap aplikasi yang berjalan pada server serta sistem operasi yang berjalan diatasnya selalu mengintai setiap saat.

Intrusion Detection Sistem (IDS) adalah sistem yang mendeteksi adanya percobaan intrusi secara otomatis. Tentu saja IDS hanyalah sebagai alat pelengkap dari sebuah sistem keamanan jaringan. Hal ini dikarenakan tingkatan IDS yang tidak terlalu penting karena sifatnya hanya sebagai pendeteksi intrusi saja. Namun demikian apabila dilengkapi dengan alat yang tepat maka sistem IDS ini dapat menjadi alat yang sangat berguna bagi seorang admin jaringan untuk mendeteksi intrusi.

Dengan tujuan inilah Proyek Akhir dengan judul Administrasi IDS berbasis Web ini disusun. Untuk memenuhi kebutuhan akan interface IDS yang mampu membuat IDS tersebut menjadi tools yang lebih berguna sehingga dapat mencapai tujuan yang diharapkan yaitu melihat intrusi apa saja yang terjadi di jaringan, asal dan tujuan serangan , jenis dan banyaknya serangan yang terjadi dalam beberapa selang waktu, serta dapat menampilkannya dalam bentuk grafik dan lebih jauh lagi dapat melakukan blocking apabila terjadi serangan yang terlebih dahulu diinputkan oleh admin.

Kata Kunci : IDS, intrusi, serangan, firewall, monitoring.

Abstract

The posing of threatening of computer which connect into network today had badly increased. Many threatening like deface in webserver, attempting to penetrated a firewall and also an attack to the application which run into a server and an operating sistem always happened anytime. Intrusion Detection Sistem (IDS) is a sistem which can detect any intrutition automatically. Of course IDS only be a complement of network security sistem. This is caused by the level of IDS and its purposed only to detect an Intrusion. But, if its equipped with right tools, IDS can be a powerfull sistem to a network administrator for detect Intrusion.

With this purposed, this final assignment which titled Web Based IDS Administration is published. For covering the needed of IDS interface which can make IDS became usefully tool until it reach out the purpose which are for look what Intrusion that happening on the network, source and target of attack, kind of attack and how many attack that happening in the interval seconds, and also can make it appeared in form of graphics and by far to do a blocking if the attack has ben inputed by administrator previously.

Keywords : IDS, Intrusion, attack, firewall, monitoring.

1. Pendahuluan

1.1 Latar belakang

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi merupakan hal yang 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. Administrasi IDS berbasis Web merupakan salah satu cara untuk melakukan administrasi dengan menggunakan interface web.

Sebagai contoh seorang administrator sebuah server yang telah menginstall aplikasi IDS sebagai penyokong security pada sebuah perusahaan tentu saja ingin melihat berapa banyak ip yang mencoba menjadi penyusup pada jaringan perusahaan tersebut.

Sistem yang akan dibuat adalah sebuah interface web untuk memanajemen sebuah server IDS sehingga nantinya admin (admin server IDS) dapat melakukan pemantauan terhadap trafik jaringan dengan lebih maksimal. Serta dapat mengetahui masalah yang ada pada jaringan dan mengambil langkah selanjutnya dengan lebih baik dan effisien.

1.2 Rumusan masalah

Berdasarkan latar belakang proyek akhir ini, perumusan masalah dapat dilihat sebagai berikut :

1. Kurang efesiennya pemantauan terhadap server IDS karena admin harus membaca log secara manual dengan basis konsole.
2. Besar kemungkinan terjadinya kesalahan dalam pembacaan data yang telah dikumpulkan oleh IDS, karena data tidak tersusun rapi dan jelas.
3. Tidak dapat ditarik kesimpulan berapa banyak serangan yang terjadi dalam selang waktu tertentu dan berasal dari mana sajakah serangan terbanyak berasal.
4. Cara pembuatan suatu perangkat lunak yang dapat membantu pengolahan data yang telah dikumpulkan oleh sever IDS agar dapat dimengerti bahkan oleh seorang admin yang baru mengenal apa itu IDS.
5. Cara penyajian data yang telah dikumpulkan oleh IDS dalam bentuk web.

Pada PA ini akan digunakan web berbasiskan PHP sebagai sebuah interface dari server IDS.

1.3 Batasan masalah

Dalam pembuatan Proyek Akhir ini dibutuhkan batasan-batasan masalah agar tidak menyimpang dan mencegah meluasnya ruang lingkup persoalan yang harus ditangani.

Batasan-batasannya adalah:

1. Intrusion Detection Sistem (IDS) yang digunakan adalah snort.
2. Hanya menangani konfigurasi IDS agar dapat melakukan listening terhadap serangan yang terjadi dan tidak membahas lebih jauh dari itu.

3. Hanya melakukan pem-*block*-an / peng-*trust*-an berdasarkan IP yang terlog sebagai penyerang dan tidak melakukan pemblockan lebih jauh dari itu.
4. Database yang digunakan adalah MySQL.
5. Aplikasi ini hanya menangani masalah view attack, konfigurasi snort (general), blocking IP, manajemen user (admin).
6. Aplikasi ini hanya dijalankan pada subnet gedung E (subnet 200).

1.4 Tujuan

Tujuan dari Proyek Akhir ini adalah membangun sebuah aplikasi interface IDS berbasis web yang mampu :

1. Melihat banyaknya intrusi yang terjadi dalam permenit, perhari, perminggu, perbulan, pertahun menggunakan display grafik.
2. Melakukan setting terhadap server IDS.
3. Melakukan monitoring berapa banyak paket yang berada pada jaringan.
4. Melakukan blocking terhadap ip yang paling banyak melakukan intrusi.
5. Melakukan allow terhadap ip yang bersifat melakukan intrusi untuk riset atau testing.
6. Menyajikan data dalam bentuk laporan, baik berupa tabel, grafik, maupun fisik.
7. Membuat suatu perangkat lunak yang dapat membantu pengolahan data yang telah dikumpulkan oleh sever IDS agar dapat dimengerti bahkan oleh seorang admin yang baru mengenal apa itu IDS.

1.5 Metode Penelitian

Pengerjaan Proyek Akhir yang berjudul Administrasi IDS berbasis Web ini menggunakan pemodelan sistem *Waterfall.* Dengan menggunakan metode ini maka sebuah proyek akan dibagi menjadi beberapa aktifitas, yaitu Problem Definition (Perumusan Masalah), Studi Kelayakan, Analisa, Design, dan Implementasi. Setiap proses baru dapat dijalankan setelah proses sebelumnya telah selesai dikerjakan. Berikut ini adalah penjelasan mengenai aktifitas-aktifitas di atas.

1. *Problem Definition* (Perumusan Masalah)
   Dalam problem definition ini akan ditentukan mengenai permasalahan yang akan ditangani oleh aplikasi.
2. Analisa Sistem
   Analisa digunakan untuk mencari permasalahan yang belum terdefinisi dalam *problem definiton.* Hal ini penting supaya pengerjaan tahap-tahap selanjutnya dapat berjalan dengan baik.
3. Desain
   Pada tahap design dibuat desain antar muka (*interface*) aplikasi, desain *database*, pengkodean, program dan prosedur yang digunakan, dan spesifikasi hardware dan sofware.
4. Implementasi
   Implementasi akan dibagi menjadi 2 tahap yaitu:

1. *Development (Coding)*
   Pada tahap *development (coding)*, hasil dari tahap desain akan diimplementasikan disini meliputi pembuatan *user interface*, *database*, pengkodean, dan penulisan program. Aplikasi ini sendiri nantinya akan dibuat dengan metode terstruktur.
2. *Testing*
   Pada tahap ini akan diadakan pengujian terhadap aplikasi yang telah dibuat. Pada penelitian ini pengujian terhadap aplikasi akan difokuskan pada pengujian fungsionalitasnya.

1.6 Sistematika Penulisan Laporan

Dalam pembuatan Proyek Akhir ini, penulis menggunakan sistematika penulisan sebagai berikut:

BAB I Pendahuluan
Dalam bagian pendahuluan akan dijelaskan tentang latar belakang tujuan penulisan, ruang lingkup masalah, tujuan penelitian, pembatasan masalah, metode penyelesaian masalah, serta sistematika penulisan laporan.

BAB II Landasan Teori
Berisi teori yang mendasari penyusunan dan pembuatan penelitian ini.

BAB III Desain dan Perancangan Aplikasi
Berisi tentang perancangan aplikasi meliputi perancangan *database* (ER Diagram), desain User Interface dan Data Diagram.

BAB IV Implementasi dan Pengujian
Berisi implementasi aplikasi di komputer *client*. Untuk pengujian hanya difokuskan pada pengujian fungsionalitasnya saja.

BAB V Penutup
Merupakan bab terakhir yang memuat kesimpulan dari keseluruhan Sistem Administrasi IDS berbasis Web.

5. Penutup

5.1 Kesimpulan

Berdasarkan analisis hasil implementasi maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak dapat mengolah dan mengelola data hasil intrusi dengan menggunakan interface berbasis web dan database sebagai penyimpanannya.
2. Perangkat lunak dapat membuat laporan dari hasil pengolahan data intrusi yang terjadi dalam permenit, perhari, perminggu, perbulan, pertahun menggunakan display grafik.
3. Melihat banyaknya intrusi Perangkat lunak dapat melakukan setting terhadap server IDS.
4. Perangkat lunak dapat melakukan monitoring berapa banyak paket yang berada pada jaringan.
5. Perangkat lunak dapat melakukan blocking terhadap ip yang paling banyak melakukan intrusi.
6. Perangkat lunak dapat melakukan allow terhadap ip yang bersifat melakukan intrusi untuk riset atau testing.

5.2 Saran

Untuk pengembangan sistem yang lebih baik, maka penulis memberikan saran sebagai berikut :

Sebaiknya aplikasi ini dapat menampilan data dengan lebih baik dan dapat melakukan alert dengan lebih baik juga seperti dengan memberikan suara yang berbeda untuk alert yang berbeda.

Daftar Pustaka

[CAR05] Carty, Aidan, ”Building An IDS Solution Using SNORT”, 2005.

[CPB04] Charlie Scott,Paul Wolfe, and Bert Hayes, “Snort For Dummies”, 2004.

[ERJ05] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley , “Network Security Bible”, 2005.

[HAR04] Harper, Patrick, “Snort Install Manual”, 2004.

[HAR05] Harper, Patrick, “Snort, Apache, SSL, PHP, MySQL, and BASE Install on CentOS 4 (or RHEL 4)”, 2005.

[KAD01] Kadir, Abdul, ”Dasar Pemrograman Web Dinamis Menggunakan PHP”, 2001.

[POW00] Purbo, Onno W., Wiharjito, Tony., “Keamanan Jaringan Internet”, Elex Media Komputindo, 2000.

[SIL00] Silberschatz, Korth, “Database Sistem Concept”, MC Graw Hill, 2000.

[SID01] Sidik, Bertha Ir, ”Pemrograman Web dengan PHP”, Informatika, Bandung, 2001.

[TOK03] Tokash, Keith, “How to setup and secure Snort, MySQL and Acid on FreeBSD 4.7 Release”, 2003.