PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN WEBSERVER SECARA OTOMATIS DAN INTERAKTIF MENGGUNAKAN APLIKASI AIRIDS DAN .HTACCESS FILE

Eko Budi Arifianto[1], Yudha Purwanto[2], Asep Mulyana[3]

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

Abstrak

Security atau keamanan merupakan hal yang sangat penting dalam membangun sebuah server web. Banyak sekali data-data yang sangat penting yang tersimpan di suatu database server sebuah web. Jika webserver tersebut tidak memiliki suatu sistem keamanan yang memadahi, maka para hacker akan dengan mudah mencuri data-data penting yang tersimpan di database webserver tersebut.

Tujuan dari proyek akhir ini adalah untuk membuat sistem keamanan suatu webserver yang dapat bekerja secara otomatis atau tanpa campur tangan dari administrator jaringan, dan interaktif atau administrator dapat dengan mudah berintraksi dengan system keamanan yang dibuat. Sistem keamanan web server ini dibuat menggunakan aplikasi dari IDS (Intrussion Detection System), firewall, database system, monitoring system, dan aplikasi dari SMS gateway. Sistem kerja dari proyek ini adalah ketika IDS mendeteksi adanya attacker yang sedang melakukan scanning port, IDS akan mengeluarkan peringatan alert yang menginformasikan tentang IP address hacker. Alert ini yang akan masuk ke dalam database system, iptables firewall, dan SMS gateway.

Setalah proyek akhir ini diimplementasikan, dapat diambil kesimpulan bahwa dengan adanya sistem keamanan webserver yang dibuat, dapat lebih mempermudah kerja administrator, karena administrator tidak perlu memonitor webservernya dan tidak perlu melakukan pengeblokan terhadap intruder atau penyusup secara manual. Karena sistem keamanan webserver ini bisa melakukan pengeblokan terhadap intruder atau penyusup secara otomatis. Selain itu sistem keamanan yang telah diimplementasikan ini tidak terlalu membebani alur traffic yang melewati jaringan, sehingga tidak mempengaruhi kinerja dari webserver.

Kata Kunci : IDS,Scanning port, firewall, SMS Gateway, IP address, iptables

Abstract
Security or safety is of paramount importance in building a web server. Lots of data is very important that stored in a database server of a web. If your web server does not have an adequate security system, then the hackers would easily steal sensitive data stored on the webserver database.

The purpose of this final project is to create a webserver security system that can work automatically or without the intervention of network administrators, and interactive or administrator can easily berintraksi with security systems are made. Web server security system is made using the application of the IDS (Intrussion Detection System), firewalls, database systems, monitoring systems, and applications from the SMS gateway. Working system of the project is when the IDS detects attackers who are doing port scanning, IDS Alert will issue a warning that tells you the IP address of hackers. This Alert will be entered into the database system, iptables firewall, and SMS gateway.

The results of this project is expected to generate a web server security system that can detect and automatically block intruders and interactive. Automatic in this case the system can detect and block intruders without the intervention from the admin. Meanwhile, the interactive security system can interact with the administrator of the network, so the admin can monitor the performance of the network security system.

Keywords : IDS, port scanning, firewall, SMS Gateway, IP address, snort, iptables

BAB I

PENDAHULUAN

1.1 Latar Belakang

Security atau keamanan merupakan hal yang sangat penting dalam membangun sebuah jaringan komputer dalam hal ini sebuah *server web*. Banyak sekali data-data yang sangat penting yang tersimpan di suatu *database server* sebuah *web*. Untuk itu diperlukan suatu sistem keamanan yang mumpuni untuk mengamankan data-data yang tersimpan di *database server* tersebut. Jika *web server* tersebut tidak memiliki suatu sistem keamanan yang canggih, maka para *hacker* akan dengan mudah mencuri data-data penting yang tersimpan di *database webserver* tersebut.

Sistem pertahanan terhadap aktivitas gangguan yang ada saat ini umumnya dilakukan secara manual oleh *administrator*. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan *administrator* dalam merespon gangguan yang terjadi. Apabila gangguan tersebut telah berhasil membuat jaringan mengalami *malfungsi*, *administrator* tidak dapat lagi mengakses sistem secara *remote*. Sehingga *administrator* tidak dapat melakukan pemulihan sistem dengan cepat.

Karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman-ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat secara otomatis dan memungkinkan *administrator* mengakses sistem walaupun terjadi *malfungsi* jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

1.2 Maksud dan Tujuan

Adapun maksud dan tujuan penulisan Proyek Akhir ini sebagai berikut:

1. Dapat mengkonfigurasi s*nort* yang merupakan jenis dari *Intrussion Detection System* agar dapat menjadi sebuah sistem keamanan jaringan yang dapat mendeteksi dan memblok intrusi dalam jaringan secara otomatis.
2. Membuat Sebuah halaman *web* yang berisi data performansi dari sistem keamanan jaringan yang dibuat dan berfungsi sebagai interaksi antara admin jaringan dengan sistem kamanan yang dibuat.
3. Dapat mengkonfigurasi *IDS, database system, firewall* dan SMS *gateway* dan *web* interaksi agar menjadi suatu aplikasi AIRIDS.
4. Mengintegrasikan antara AIRIDS dengan *.htaccess file* agar dapat berkerja bersama dalam melakukan deteksi dan *blocking* intrusi jaringan.
5. Mendesain dan mengimplementasikan sistem deteksi penyusupan jaringan yang otomatis.
6. Menganalisa performansi sistem deteksi penyusupan jaringan dalam menangani gangguan terhadap sistem

1.3 Perumusan Masalah

Permasalahan yang dijadikan objek pada Proyek Akhir ini adalah:

1. Bagaimana mengkonfigurasi *snort* agar menjadi sebuah sistem keamanan *web server* yang dapat mendeteksi dan memblok intrusi dalam jaringan secara otomatis?
2. Bagaimana Membuat Sebuah halaman *web* yang berisi data performansi dari sistem keamanan jaringan yang dibuat dan berfungsi sebagai interaksi antara admin jaringan dengan sistem kamanan yang dibuat.
3. Bagaimana mengkonfigurasi *IDS, database system, firewall* dan SMS *Gateway* agar menjadi suatu aplikasi AIRIDS?
4. Bagaimana mengintegrasikan antara AIRIDS dengan *.htaccess file* agar dapat berkerja bersama dalam melakukan deteksi dan *blocking* intrusi jaringan.
5. Bagaimana mengimplementasikan sebuah sistem keamanan jaringan secara otomatis?

6. Bagaimana menganalisa performansi dari sistem keamanan jaringan yang telah dibuat?

1.4 Batasan Masalah

Dalam penyusunan proyek akhir ini, permasalahan dibatasi dalam beberapa hal, yaitu :

1. IDS yang digunakan adalah *snort*
2. Uji coba yang dilakukan dengan menggunakan teknik *port scanning* sebagai teknik *hacking*nya.
3. Mengggunakan *Apache* sebagai *webserver* dan *Mysql* sebagai *database*nya.
4. Tidak membahas tentang cara pembuatan *webserver*.
5. Tidak membahas mengenai konten-konten *web* yang telah dibuat.
6. Tidak membahas mengenai pembuatan *web* dan konten-kontentnya

1.5 Metode Penyelesaian Masalah

Metodologi yang digunakan untuk menyelesaikan masalah adalah :

1. Studi Literatur

   Studi Literatur ini dimaksudkan untuk mencari dan mempelajari konsep dari teori pendukung terhadap perancangan yaitu dari buku, jurnal, dan referensi lain yang relevan dengan mempelajari hal-hal yang berkaitan dengan perancangan.
2. Konsultasi

   Konsultasi ini dilakukan dengan para pembimbing , yaitu memberikan bimbingan dan arahan mengenai proyek akhir.
3. Tahap Perancangan, pada tahap ini dilakukan perancangan sebuah sistem keamanan jaringan yang dapat mendeteksi dan memblok intrusi dalam jaringan secara otomatis.
4. Tahap Pengujian Sistem dan Analisa, pada tahap ini sistem keamanan jaringan yang sudah dirancang sedemikian rupa Sehingga dapat

mendeteksi adanya penyusupan dalam jaringan dan memblok intrusi-intrusi yang ada secara otomatis.

1.6 Sistematika Penulisan

Sistematika yang digunakan dalan penulisan proyek akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang masalah, maksud dan tujuan, perumusan masalah, batasan masalah, pemodelan sistem, metode penyelesaian masalah, dan sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini dikemukakan berbagai teori yang mendukung dalam pembuatan proyek ini diantranya AIRIDS, SMS *gateway*

BAB III PERANCANGAN

Berisi tentang tahap-tahap perancangan dan tahap-tahap implementasi awal sistem.

BAB IV ANALISIS HASIL SIMULASI

Bab ini membahas hasil uji performansi dari Sistem keamanan yang akan dibuat.

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan akhir dan saran pengembangan Proyek Akhir.

BAB V
PENUTUP

5.1. Kesimpulan

Dari hasil implementasi dan perancangan serta pengambilan data dan analisis yang telah dilakukan pada implementasi *Sistem Keamanan Webserver Secara Otomatis dan Interaktif menggunakan Aplikasi AIRIDS dan .htaccess File*. dapat diambil kesimpulan sebagai berikut :

1. Sistem deteksi penyusupan jaringan memiliki dampak terhadap performansi jaringan yaitu penurunan nilai *troughput* trafik yang melalui sistem tersebut.
2. Penurunan nilai *troughput* yang hanya sebesar $\pm$ 0.1022% relatif rendah dan tidak terlalu mengganggu performa sistem.
3. Seluruh IP *address* yang digunakan untuk menyerang dapat terdeteksi dengan baik. Demikian juga dengan deteksi jenis serangan yang digunakan terdeteksi dengan benar
4. Dengan sistem keamanan ini administrator tidak perlu memonitor *webserver* secara terus menerus untuk mengamankannya, karena adanya penegblokan *intruder* atau penyusup secara otomatis oleh sistem keamanan tersebut.
5. Sistem interaktif berupa SMS memberikan *administrator* informasi terkini tentang kondisi sistem serta memungkinkan *administrator* merespon secara langsung.

5.2. Saran

1. Implementasi jaringan kedepannya diharapkan bisa menjadi sistem keamanan jaringan yang lebih aktif, jadi jika sistem tersebut diserang, maka sistem tersebut tidak hanya bisa mendeteksi penyerang saja tapi bisa melakukan upaya *hacking* juga ke komputer penyerang secara otomatis.

DAFTAR PUSTAKA

1. S. Kent., R. Atkinson., IP Authentication Header, RFC 2402, November 1998.
2. Rafiudin,Rahmat, Mengganyang Hacker Dengan Snort, Andi Yogyakarta, 2010
3. http://gembong.web.id/mengenal-file-htaccess/
4. http://www.symmetrixtech.com
5. Purbo, Onno W., Wiharjito, Tony., Keamanan Jaringan Internet, Elex Media Komputindo, 2000
6. http://www.isswg.org.uk/cia.php
7. http://www.gfi.com/blog/taking-security-seriously/
8. http://snort.org/snort-manual-page.pdf
9. Wack, John. Packet Filtering Firewall.
10. http://www.snort.org
11. Linux *system administrator*. Informatika. Bandung.
12. *ModulPraktikumLaboratorium Computer and Comunication*. Bandung