Implementasi Intrusion Detection System (IDS) Pada Rule Based System Menggunakan Sniffer Mode Pada Local Area Network

Muhammad Rizallul Hakim

Program Studi Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Jl. Masjid Al Ghazali, Bukit Lama, Kec. Ilir Barat I, Kota Palembang, Sumatera Selatan 30128, Indonesia

Email: rizallul.hakim300@gmail.com

Abstrak

Intrusion Detection System (IDS) sangat membantu pengguna dalam memantau dan menganalisa performa serta gangguan pada keamanan jaringan[1]. penelitian ini bertujuan untuk merancang IDS menggunakan *Snort* dengan berbasiskan web dan implementasi sistem untuk memantau aktifitas para pengguna *Hotspot*. Penelitian ini berisi analisa gangguan pada jaringan nirkabel UIR, solusi keamanan pada jaringan, proses dan cara kerja sistem IDS yang dibuat dengan basis web, serta evaluasi penerapan sistem IDS pada jaringan. Keamanan sebuah jaringan komputer diperlukan untuk menjaga integritas dan validitas data serta menjamin ketersedian layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan yang dapat merusak sistem yang ada[2].

***Kata Kunci**: Intrusion Detection System, Security Management, Hotspot, Wireless, UIR*

Abstract

Intrusion Detection System (IDS) is very helpful for users in monitoring and analyzing network security problems[1]. This research aims to design IDS using Snort with web-based and system implementation to monitor the activities of Hotspot users. This study contains an analysis of interruptions on UIR wireless networks, security solutions on the network, processes and workings of IDS systems that are made on a web basis, as well as evaluating the application of IDS systems on the network. The security of a computer network is needed to maintain the integrity and validity of the data and ensure the availability of services for its users. The system must be protected from all kinds of attacks and intrusion attempts that can damage the existing system[2].

***Keyword**: Intrusion Detection System, Security Management, Hotspot, Wireless, UIR*

1. Pendahuluan

Pada saat ini internet telah menjadi bagian penting dari gaya hidup masyarakat di seluruh dunia. internet telah merambah ke hampir semua aspek kehidupan. Intrusion Detection System merupakan usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi atau seorang user yang sah tetapi menyalahgunakan priviliges sumber daya sistem. Intrusion Detection System (IDS) atau Sistem Deteksi Penyusupan adalah sistem yang dapat melakukan deteksi penyusupan . IDS akan memberikan notifikasi jika mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal.

2. Metode

Pada saat ini di Indonesia terjadi lebih dari ratusan ribu serangan (intrusion) setiap harinya terhadap keamanan sistem jaringan internet seperti tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain, tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua pihak yang seharusnya berinteraksi, dan tindakan lain yang berpotensi untuk menghancurkan informasi yang berjalan di atas infrastruktur internet[3]. Kasus-kasus terkait insiden terhadap keamanan jaringan internet telah marak terjadi di Indonesia dan mengancam langsung pada infrastruktur strategis di Indonesia. Security Network merupakan suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada jaringan komputer. Sasaran keamanan jaringan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian

atau korupsi, seperti dijabarkan dalam kebijakan keamanan. Menurut Garfinkel dan Spafford, ahli dalam keamanan komputer, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu:

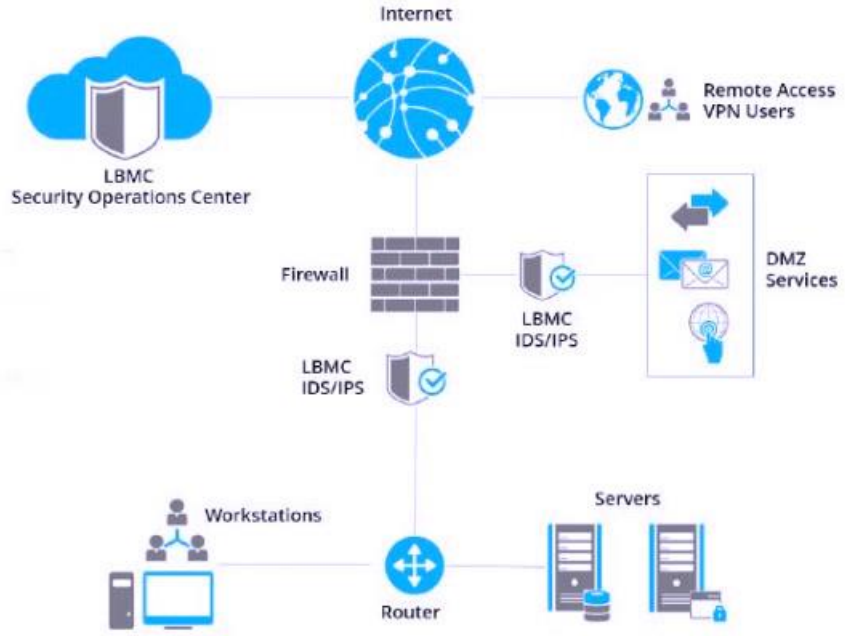
1. Availability
2. Confidentiality
3. Data Integrity
4. Control
5. Audit

Intrusion Detection System (IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan[2]. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan penyusupan.

Intrusion Detection adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus. Program yang digunakan untuk pendeteksian disebut sebagai IDS (Intrusion Detection System). Tipe Dasar IDS yaitu:

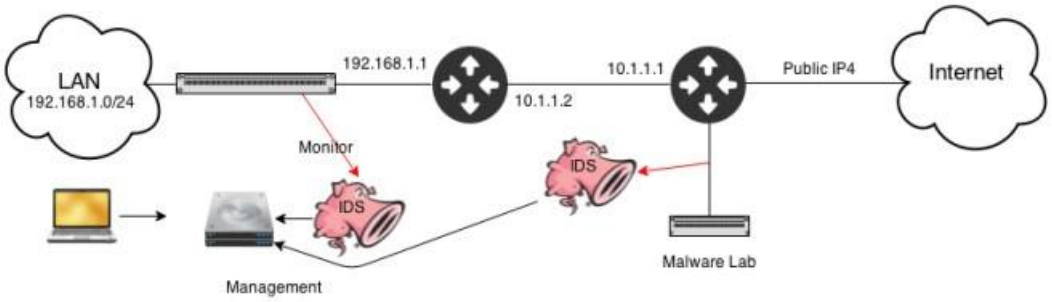
1. Rule-based systems, berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mendeteksi Kemudian lintas sesuai dengan data dari database, maka pendeteksian tersebut langsung dikategorikan sebagai penyusupan.
2. Adaptive systems, sama seperti Rule-based tetapi ditambah dengan teknik lain yaitu membuka kemungkinan untuk mendeteksi metode penyusupan yang baru.

Pendekatan yang digunakan dalam rule-based system ada dua, yaitu Preemptory (pencegahan) dan Reactionary (reaksi). Perbedaan dari kedua pendekatan tersebut adalah dalam waktu saja. Dalam Preemptory akan memperhatikan semua Kemudian-lintas jaringan. Apabila paket mencurigakan ditemukan maka program akan melakukan tindakan yang sesuai dengan paket mencurigakan tersebut. Reactionary, program hanya mengamati log. Jika ditemukan paket mencurigakan, program akan melakukan tindakan sesuai dengan paket tersebut



Gambar 1. Cara Kerja IDS

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[4]. Snort IDS merupakan IDS open source yang secara defacto menjadi standar IDS di industri. Snort dapat didownload di situs www.snort.org. Snort dapat diimplementasikan dalam jaringan yang multiplatform, salah satu kelebihannya adalah mampu mengirimkan alert dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui SMB. Snort dapat berkerja dalam 3 mode yaitu sniffer mode (penyadap), packet logger dan network intrusion detection mode[5]. Adapun cara kerja snort dapat dilihat pada gambar 3 dibawah :

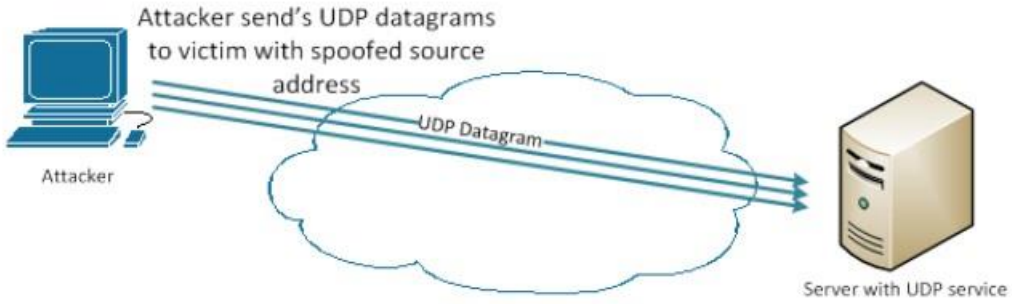


GAMBAR 2. Cara kerja Snort

3. Hasil dan Pembahasan

Dalam metodologi diatas dapat disimpulkan bahwa permasalahan yang dihadapi adalah serangan pada jaringan lokal. Metodologi yang dapat digunakan untuk meningkatkan keamanan sebuah jaringan adalah dengan membuat sebuah sistem kemanan yang dapat membaca serangan baik dari dalam maupun luar. Dengan adanya IDS tersebut maka dapat dibangun sebuah topologi yang dapat membantu kinerja dari segi keamanan, infrastruktur dan lainnya. IDS ini sendiri juga berfungsi meningkatkan kinerja dan juga estabilitas kerja dari keamanan sistem itu sendiri. Uraian kerja akan dijelaskan di dalam kerangka kerja yang nantinya menjelaskan prosedur maupun langkah – langkah yang akan dihadapi dalam membangun atau mengukur Intrusion Detection System ini. Pertama adalah menganalisa dan merancang apa saja yang dibutuhkan dalam pembangunan IDS ini. Lalu dilanjutkan dengan pengujian beserta membuat hasil kinerja dari IDS tersebut kedalam sebuah tabel.

Pada skenario pengujian IDS berbasis Snort ini, akan dilakukan simulasi percobaan penyerangan dengan melakukan serangan Denial of Service (DoS attack). Serangan ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan sistem atau jaringan komputer sehingga pengguna tidak dapat menikmati fungsi dari layanan tersebut. Contoh dari serangan denial of service yang digunakan dalam pengujian ini adalah dengan melakukan UDP (User Datagram Protocol) flooding. UDP flooding terjadi setelah jaringan “dibanjiri” dengan paket – paket UDP yang menyerang ke port – port secara random, atau menyerang ke port tertentu yang rentan terhadap serangan. Berikut mekanisme dari serangan UDP port :



Gambar 3. Mekanisme simulasi penyerangan UDP flooding

Langkah selanjutnya adalah melakukan blocking terhadap Alamat IP yang dianggap sebagai penyusup dan sistem akan memberikan laporan kepada administrator melalui web monitoring mengenai adanya penyusup yang mencoba masuk ke dalam sistem. Tabel 2 menunjukkan kemampuan dari sistem untuk mengelola hasil output dari snort untuk mengenali terjadinya serangan sampai terjadinya proses blocking menggunakan iptables dari beberapa sampel yang telah diuji.

NO	IP ADDRESS	WAKTU SERANGAN	WAKTU BLOCKING	SELISIH (DETIK)
1	192.168.100.1	08:36:24	08:36:30	5 detik
2	192.168.100.2	22:30:54	22:30:59	5 detik
3	192.168.100.3	18:08:37	18:08:44	7 detik
4	192.168.100.4	9:10:18	9:10:27	5 detik
5	192.168.100.1	23:34:24	23:34:31	7 detik
6	192.168.100.2	12.15.35	12.15.31	4 detik
7	192.168.100.1	14:14:35	14:14:39	4 detik
8	192.168.100.1	07:51:39	7:52:45	6 detik

Table 1. Selisih Waktu Saat Blocking

4. Kesimpulan

Hasil penelitian menunjukkan bahwa setiap ada serangan yang datang dari luar menuju host atau server yang didalamnya terdapat IDS yang sedang berjalan, maka sistem akan memberikan informasi mengenai data serangan yang telah masuk kedalam sistem kita. Disamping dapat mendeteksi jumlah paket data serangan UDP Flooding, Snort dapat juga mendeteksi alamat IP si penyerang.

5. Referensi

[1] D. M. Informatika, F. Teknik, and U. N. Surabaya, “STANDAR MODEL MANAJEMEN FCAPS Alfanaini Ibnu Febry Kurniawan Abstrak,” vol. 6, pp. 52–61, 2016.

[2] Y. Arta, “Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal,” *It J. Res. Dev.*, vol. 2, no. 1, pp. 43–50, 2017.

[3] A. P. Segara, R. Primananda, and S. R. Akbar, “Implementasi MQTT (Message Queuing Telemetry Transport) pada Sistem Monitoring Jaringan berbasis SNMP (Simple Network Management Protocol),” *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 2, pp. 695–702, 2018.

[4] A. Faisol and I. I. Muttaqin, “Implementasi Sensor Monitoring Pada Jaringan Wi-Fi (Hotspot) Berbasis Snort,” *J. Teknol. Inf. dan Terap.*, vol. 5, no. 2, pp. 141–146, 2019.

[5] F. A. Masse, A. N. Hidayat, and Badrianto, “Penerapan Network Intrusion Detection System Menggunakan Snort Berbasis Database MySQL Pada Hotspot Kota,” *J. Elektron. Sist. Inf. Dan Komput.*, vol. 1, no. 2, pp. 1–16, 2015.