PERBANDINGAN PERFORMANSI ANTARA SIGNATURE BASED DAN ANOMALY BASED DALAM PENDETEKSIAN INTRUSI

Noviana Sagita[1], Niken Dwi Cahyani[2], Fazmah Arif Yulianto[3]

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

Abstrak

Intrusion Detection System (IDS) adalah tool, metode, sumber daya yang dapat memonitor atau mengamati aktifitas-aktifitas untuk mengidentifikasi peristiwa berbahaya atau mencurigakan. Peristiwa yang berbahaya atau mencurigakan itu bisa disebut dengan intrusi atau serangan. Dalam mendeteksi intrusi, IDS menggunakan 2 teknik utama yaitu Signature Based Detection dan Anomaly Based Detection. Pada tugas akhir ini, dibangun 2 buah sistem untuk mendeteksi adanya intrusi, yaitu sistem yang berbasis signature dan sistem yang berbasis anomaly. Masing-masing sistem memiliki rancangan yang berbeda. Untuk IDS yang berbasis signature digunakan tools Snort, sedangkan untuk IDS yang berbasis anomaly menggunakan tools Ourmon. Kedua sistem tersebut diuji dengan studi kasus yang sama. Studi kasus yang diuji ada 4 macam, yaitu 3 macam studi kasus yang berupa serangan port scanning, denial of service jenis SYN Flood, dan exploit serta 1 studi kasus yang bukan berupa serangan seperti aktifitas download suatu file. Analisis yang dilakukan adalah analisis akurasi, penggunaan resource, dan kesalahan dalam pendeteksian (false positive dan false negative). Dari pengujian keempat studi kasus tersebut, dapat disimpulkan bahwa untuk IDS Signature bisa mendeteksi serangan port scanning, denial of service, dan exploit, sedangkan IDS Anomaly hanya bisa mendeteksi serangan denial of service dan mendeteksi aktifitas download yang sebenarnya bukan merupakan serangan.

Kata Kunci : Intrusion Detection System (IDS), Signature Based, dan Anomaly Based

Abstract

Intrusion Detection System (IDS) is a tool, a method, a resource which can monitor or observe activities to identify dangerous or suspicious event. Dangerous or suspicious event can be called intrusion or attack. In detecting a n intrusion, IDS uses 2 main technique which are Signature Based Detection and Anomaly Based Detection. In this final project, 2 systems is built to detect intrusion, which are a signature based system and anomaly based system. Each system has different design. For signature based IDS, Snort tools is used, whereas for anomaly based IDS, Ourmon tools is used. Both of the system is tested with the same case study. There are 4 case study, which are 3 case study on port scanning attac, denial of service SYN Flood type, and exploit, then 1 case study that is not an attack type like file download activitiy. The analysis done is accuracy analysis, resource usage analysis, and error on detection (false positive and false negative). From the 4 case testing, it can be concluded that for signature IDS can detect port scanning, denial of service and exploit, where anomaly IDS can only detect denial of service attack and download activity which is not an attack.

Keywords : Intrusion Detection System (IDS), Signature Based, and Anomaly Based

BAB I
PENDAHULUAN

1.1 Latar belakang masalah

Setiap sistem yang ada pasti menginginkan keamanan yang handal untuk melindungi sistemnya dari serangan-serangan luar. Sebagian besar serangan yang masuk ke sistem adalah serangan untuk merusak. Untuk mengetahui serangan itu berbahaya atau tidak, bisa dilakukan dengan pendeteksian jenis serangan yang masuk.

Intrusion Detection System (IDS) merupakan sebuah perangkat lunak yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem maupun jaringan. Dengan kata lain, IDS merupakan sistem untuk mendeteksi intrusi yang dilakukan oleh *intruder*. Dalam mendeteksi suatu intrusi, IDS menggunakan 2 teknik, yaitu dengan teknik *Signature-based detection* dan *Anomaly-based detection*. Teknik pendeteksian berbasis *signature* yaitu dengan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan peyusupan. Sedangkan pendeteksian berbasis *anomaly* yaitu dengan memperhatikan lalu lintas yang dipantau dan membandingkan dengan lalu lintas normal.[3] Jika ada kejadian yang tidak biasa maka akan dianggap sebagai serangan. Teknik *signature* dan *anomaly* merupakan teknik untuk mendeteksi adanya intrusi. Semua jenis serangan yang ada belum bisa dideteksi oleh suatu IDS dengan satu teknik tertentu. Ada serangan yang hanya bisa dideteksi dengan teknik *anomaly-based* dan ada juga serangan tertentu yang hanya bisa dideteksi dengan teknik *signature-based*. Oleh karena itu diperlukan satu penelitian dan pengujian untuk mengetahui kemampuan dari teknik IDS tertentu dalam mendeteksi sebuah serangan.

1.2 Perumusan Masalah

Dengan melihat pada latar belakang di atas, permasalahan yang akan dijabarkan dan diteliti adalah kerja dari teknik *signature* dan *anomaly* dalam menghadapi berbagai macam serangan yang masuk.

Hipotesa dari penelitian Tugas Akhir ini adalah untuk contoh kasus serangan *scanning* dan *exploit* lebih baik menerapkan IDS yang berbasis *signature* dan untuk contoh kasus *denial of service* lebih baik menerapkan IDS berbasis *anomaly*.

1.3 Batasan Masalah

Adapun batasan-batasan masalah dalam Tugas Akhir ini adalah sebagai berikut:

1. Untuk cara signature, *tool* yang digunakan untuk mendeteksi serangan adalah Snort.
2. Untuk cara anomaly, *tool* yang digunakan untuk mendeteksi *anomaly* adalah Ourmon.
3. Contoh kasus yang akan dilakukan ada 4 macam, yaitu 3 kasus yang berupa serangan (serangan *port scanning*, *exploit*, dan *Denial of Service* (DoS) jenis *SYN Flood Attack*) dan 1 kasus bukan serangan (*download file*).
4. Jaringan yang digunakan dalam pengujian adalah jaringan Lab Computer System IT Telkom.

1.4 Tujuan

Adapun beberapa tujuan dalam Tugas Akhir ini yaitu :

1. Melakukan pendeteksian serangan dengan cara *signature* dan *anomaly*.
2. Menganalisis performansi pendeteksian serangan dengan cara *signature* dan cara *anomaly*. Performansi dilihat dari sisi akurasi (banyaknya serangan yang bisa dideteksi), penggunaan resource CPU dan RAM pada IDS, dan kesalahan deteksi (*false positive* dan *false negative*).
3. Menentukan cara terbaik dalam pendeteksian serangan berdasarkan kasus tertentu.

1.5 Metodologi Penyelesaian Masalah

Metodologi yang digunakan dalam memecahkan permasalahan-permasalahan dalam Tugas Akhir ini terdiri dari enam tahap, yaitu:

1. Studi Literatur
   Pada tahap ini dilakukan pengumpulan dan pencarian literatur yang berhubungan dengan topik yang dianalisis, yaitu literatur tentang *intrusion detection system*, *signature based*, *anomaly based*, Snort, Ourmon, dan jenis serangan/intrusi.
2. Tahap Pendalaman Materi
   Pada tahap ini dilakukan pendalaman materi dengan membaca artikel-artikel yang berhubungan dengan *Intrusion Detection System* terutama cara kerja dari pendeteksian berbasis *signature* dan *anomaly*, serta tutorial dari *tools* yang rencananya akan digunakan, misalnya Snort dan Ourmon.
3. Tahap Analisis dan Perancangan
   Melakukan analisis bagaimana melakukan penerapan dari ilmu yang sudah didapat dalam studi literatur dan pendalaman materi untuk diimplementasikan pada tugas akhir. Untuk pendeteksian serangan dengan cara *signature* digunakan Snort. Menginstall Snort dan membangun *rule-rule* yang berhubungan dengan pencegahan serangan. Dalam masalah ini

penyerangan akan dilakukan pada sebuah komputer *server*. *Rules* tersebut dapat dianggap sebagai basisdata. Data *traffic* yang masuk akan dicocokkan dengan *rule* tersebut, apabila cocok maka dianggap sebagai serangan. Untuk pendeteksian serangan dengan cara *anomaly*, digunakan tool Ourmon. Ourmon merupakan sebuah sistem monitoring jaringan dan dapat mendeteksi adanya anomali. Anomali bisa dideteksi dengan memperhatikan grafik dimana jika grafik yang terlihat berbeda sangat jauh dari keadaan normal, maka bisa dianggap sebagai anomali. Dalam kasus ini, hal yang sangat mempengaruhi dalam metode *signature* adalah rule, yaitu seberapa kuat rule tersebut dalam menghadapi sebuah serangan. Sedangkan untuk metode *anomaly*, hal yang sangat berpengaruh adalah keadaan jaringan normalnya.

4. Tahap Implementasi

   Membangun dua buah komputer penyerang (*attacker*), komputer server (target), dan komputer yang telah terpasang IDS untuk melakukan pendeteksian serangan. IDS *signature* dan IDS *anomaly* berada dalam satu buah komputer yang sama. *Attacker* akan mencoba melakukan beberapa serangan ke komputer target. Lalu komputer IDS dapat mendeteksi apakah itu serangan atau bukan. Pendeteksian dilakukan dengan dua buah *tools*, yaitu dengan Snort dan Ourmon. Jaringan yang rencananya akan digunakan adalah jaringan Lab Computer System IT Telkom .

5. Tahap Pengujian dan Analisis Hasil

   a. Menguji dengan beberapa contoh kasus penyerangan yaitu dengan komputer *attacker* sebagai penyerang untuk menyerang komputer target. Pengujian dilakukan secara *real-time*. Contoh serangannya yaitu serangan *port scanning*, *exploit*, dan *denial of service*.

   b. Mengevaluasi performansi dilihat dari sisi akurasi (banyaknya serangan yang bisa dideteksi), penggunaan resource CPU dan RAM pada IDS, dan kesalahan deteksi (*false positive* dan *false negative*). Dengan dilakukan beberapa kasus pengujian, maka akan bisa diambil kesimpulan untuk kasus tertentu cocok menggunakan metode *signature* atau *anomaly*.

6. Tahap Pembuatan Laporan

   Pada tahap ini dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi berdasarkan analisis hasil penelitian Tugas Akhir ini.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I Pendahuluan

Bab ini menguraikan tugas akhir ini secara umum, meliputi latar belakang masalah, perumusan masalah, tujuan, batasan masalah, dan metode yang digunakan.

BAB II Dasar Teori

Bab ini membahas mengenai uraian teori yang berhubungan dengan *Intrusion Detection System*, *Signature Based Detection*, dan *Anomaly Based Detection*.

BAB III Analisis Perancangan dan Implementasi

Bab ini berisi analisis kebutuhan dari sistem dan masalah-masalah yang ada di dalamnya. Dari tahap analisis kemudian dilanjutkan ke tahap perancangan dan implementasi.

BAB IV Pengujian dan Analisis

Bab ini membahas mengenai pengujian hasil implementasi yang telah dilakukan pada bab sebelumnya. Pengujian dilakukan dengan melakukan beberapa serangan dan membandingkan hasil yang didapat pada kedua metode. Tahap Pengujian dilanjutkan dengan tahap analisis hasil pengujian.

BAB V Kesimpulan dan Saran

Berisi kesimpulan dari penulisan Tugas Akhir ini dan saran-saran yang diperlukan untuk pengembangan lebih lanjut.

BAB V
KESIMPULAN dan SARAN

5.1 Kesimpulan

- Dari sisi akurasi, IDS *Signature* bisa mendeteksi semua jenis serangan (*port scanning*, *exploit*, dan *denial of service*), sedangkan IDS *Anomaly* hanya bisa mendeteksi serangan *denial of service*.
- Dari sisi penggunaan *resource*, IDS *Signature* menggunakan *resource* RAM yang lebih besar, sedangkan IDS *Anomaly* menggunakan *resource* CPU yang lebih besar.
- Dari sisi kesalahan deteksi, IDS *Signature* tidak ditemukan *false positive* maupun *false negative*, sedangkan pada IDS Anomaly ditemukan *false positive* dan *false negative*.

5.2 Saran

- Pengujian dilakukan dengan menerapkan studi kasus yang lain seperti *spoofing*, *malicious code*, *man in the middle attack*, dll.
- Membuat suatu IDS yang menggabungkan antara metode *Signature-based* dengan *Anomaly-based*.

Daftar Pustaka

[1] Ariyus, Doni. 2007. *Intrusion Detection System*, Yogyakarta, Andi.

[2] Beale, Jay. 2007. *Snort IDS and IPS Toolkit*, Burlington, Syngress Publishing.

[3] Beale, Jay, Caswell, Brian, dan Poor, Mike. 2004. *Snort 2.1 Intrusion Detection Second Edition*, Rockland, Syngress Publishing.

[4] Binkley, James dan Massey, Bart. 2005. *Ourmon and Network Monitoring Performance*, USENIX Annual Technical Conference.

[5] Budimulia, Ananda. 2006. *Anomaly Detection pada Intrusion Detection System (IDS) menggunakan metode clustering*, Kumpulan TA/PA Institut Teknologi Telkom, Bandung.

[6] Cisco. 2007. *Cisco CCNA Exploration 4*. Cisco System.

[7] Cox J, Kerry dan Gerg, Christoper. 2004. *Managing Security with Snort and IDS Tools*, United States of America, O'Reilly.

[8] Littlejohn Shinder, Debra. 2002. *Scene Of The Cybercrime : Computer Forensics Handbook*, Rockland, Syngress Publishing.

[9] Ourmon : A Technical Explanation of the Architecture and Filters http://ourmon.cat.pdx.edu/ourmon/info.html diakses pada tanggal 2 Oktober 2010.

[10] Ourmon - Network Monitoring and Anomaly Detection System http://ourmon.cat.pdx.edu/ourmon/index.html diakses pada tanggal 2 Oktober 2010.

[11] Pfleeger, Charles. 2006. *Security in Computing*, Fourth Edition, New Jersey, Prentice Hall.

[12] Rehman Ur, Rafeeq. 2003. *Intrusion Detection Systems with Snort*, New Jersey, Prentice Hall.

[13] Scarfone, Karen dan Mell, Peter. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Gaithersburg, National Institute of Standards and Technology.

[14] Scott, Charlie, Wolfe, Paul, dan Hayes, Bert. *Snort for Dummies*, Indianapolis, Wiley Publishing.

[15] Tesink, Sebastiaan. 2007. *Improving Intrusion Detection Systems through Machine Learning*, ILK Research Group Tilburg University.

[16] The Snort Project. 2009. *Snort Users Manual 2.8.5*, Sourcefire.