PERANCANGAN DAN IMPLEMENTASI INTRUSION DETECTION SYSTEM DI JARINGAN UNIVERSITAS DIPONEGORO

Dyakso Anindito Nugroho[1)], Adian Fatchur Rochim[2)] , Eko Didik Widianto[2)]
Jurusan Teknik Sistem Komputer, Fakultas Teknik, Universitas Diponegoro,
Jln. Prof. Sudharto, Tembalang, Semarang, Indonesia
email : dyakso2008@yahoo.com

Abstact, The use of information technology gives the advantage of open access for its users, but a new problem arises that there is a threat from unauthorized users. Intrusion Detection System (IDS) is applied to assist administrator to monitoring network security. IDS displays illegal access information in a raw form which is require more time to read the detected threats.

This final project aims to design an IDS with web application which is made for pulling information on IDS sensor database, then processing and representing them in tables and graphs that are easy to understand. The web application also has IpTables firewall module to block attacker's IP address . The hardware used is Cisco IPS 4240, two computers Compaq Presario 4010F as client and gateway, and Cisco Catalyst 2960 switch. The software used is Ubuntu 12.0 LTS Precise operating system, BackTrack 5 R1 operating system, PHP 5.4 programming language, MySQL 5 database, and web-based system configuration tool Webmin.

Testing is done using several BackTrack applications with the aim of Cisco IPS 4240 is capable of detecting accordance with the applicable rules. Each events of any attack attempt or threat was obtained from IDS sensor database in XML form. XML file is sent using Security Device Event Exchange (SDEE) protocol. The web application is tested by looking at the output tables and graphs that displays the appropriate results of sensor detection.

This study generated an intrusion detection system that is easier to monitor. Network packets copied by the Cisco 2960 switch and then forwarded to the sensor. Intruder detection is done by Cisco IPS 4240 sensor. Log detection processed by the web application into tables and graphs. Intrusion detection systems are intended to improve network security.

***Keywords**: Intrusion Detection System (IDS), Cisco IPS 4240, web application, XML*

1. PENDAHULUAN

1.1 Latar Belakang

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.

Administrator membutuhkan suatu sistem yang dapat menginformasikan ancaman-ancaman yang mungkin terjadi secara optimal dalam waktu cepat. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem.

Penelitian ini ditujukan untuk merancang dan mengimplementasikan Intrusion Detection System (Sistem Deteksi Penyusup) untuk membantu administrator dalam memantau kondisi jaringan dan menganalisa paket-paket berbahaya. Perangkat yang digunakan adalah sensor Cisco IPS (Intrusion Prevention System) 4240, *switch* Cisco Catalyst 2960 dan sebuah *web server*.

1.2. Tujuan

Tujuan dari penelitian tugas akhir ini adalah untuk mengimplementasikan *intrusion detection system* untuk mereprentasikan dan menampilkan *log* informasi akses ilegal pada jaringan yang dihasilkan sensor dalam tabel dan grafik agar lebih mudah dipahami.

1.3. Batasan Masalah

Batasan masalah penelitian tugas akhir ini adalah :

1. Jaringan terdiri dari 1 klien, 1 server, 1 switch, dan 1 sensor dengan media komunikasi kabel.
2. Sensor Cisco IPS 4240 digunakan sebagai sensor untuk mendeteksi serangan.
3. Perangkat lunak Apache 2.2 digunakan sebagai *web server* untuk menampilkan *log* yang dihasilkan sensor yang dikembangkan menggunakan bahasa pemrograman PHP 5.4.
4. Sistem operasi server menggunakan Linux Ubuntu Precise 12.0.

2. LANDASAN TEORI

2.1 Prinsip IDS

Intrusion detection adalah proses *monitoring event* yang terjadi dalam suatu jaringan atau suatu sistem komputer dan menganalisanya untuk mengetahui adanya tanda-tanda insiden yang mungkin terjadi. Tanda ini bisa saja mengindikasikan adanya pelanggaran atau ancaman terhadap kebijakan keamanan komputer yang diterapkan. Insiden bisa terjadi oleh berbagai sebab, seperti *malware* (misalnya *worm*, *spyware*), akses yang tidak diijinkan, pengguna legal yang menyalahgunakan hak-hak mereka atau mencoba untuk mendapatkan hak tambahan yang bukan wewenangnya. Beberapa insiden tidak berbahaya dan biasanya dikarenakan *human error*, misalnya seseorang salah ketik alamat komputer dan kemudian tanpa sadar mencoba untuk terhubung ke sistem yang berbeda tanpa otorisasi. Sedangkan *intrusion detection system* adalah adalah perangkat lunak yang mengotomatisasi proses deteksi intrusi (penyusup).

2.2 Komponen IDS

Komponen yang umumnya terdapat pada IDS adalah sebagai berikut:

1. Sensor atau Agen

Sensor dan agen berfungsi untuk memantau dan menganalisa aktivitas jaringan. Istilah sensor lebih mengacu pada IDS yang memantau jaringan, termasuk *network-based*, jaringan nirkabel, dan *network behavior analysis*. Istilah agen lebih mengacu pada *Host-based* IDS.

2. *Server* Manajemen

Server Manajemen adalah perangkat sentral yang menerima informasi dari sensor atau agen dan mengelolanya. Beberapa *server* mampu menganalisa *event* yang disediakan sensor atau agen dan dapat mengidentifikasinya sementara sensor atau agen tidak dapat melakukannya. Lingkungan pengembangan IDS yang kecil tidak membutuhkan *server*, walaupun sebagian besar pengembangan IDS menggunakan *server*. Lingkungan pengembangan IDS yang besar dan kompleks biasanya terdapat beberapa *server*, dan pada beberapa kasus terdapat *management server* dengan tingkatan yang berbeda satu sama lain.

3. *Server* Basis Data

Server Basis Data adalah tempat penyimpanan untuk informasi *event* yang dideteksi oleh sensor, agen, dan atau *management server*. Banyak teknologi IDS yang mendukung *database server*.

4. Konsol

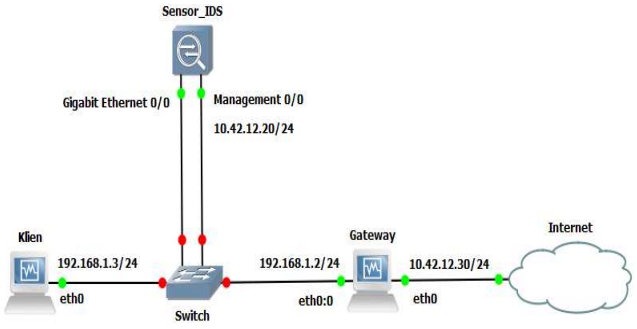
Konsol adalah program yang menyediakan antarmuka untuk pengguna IDS dan administrator. Beberapa konsol hanya digunakan untuk keperluan administrasi, seperti mengkonfigurasi sensor atau agen, sedangkan konsol yang khusus digunakan untuk *monitoring* dan analisa. Beberapa konsol lain menyediakan fungsi keduanya, administrasi dan *monitoring*.

3. PERANCANGAN SISTEM

3.1 Perancangan Sistem Secara Umum

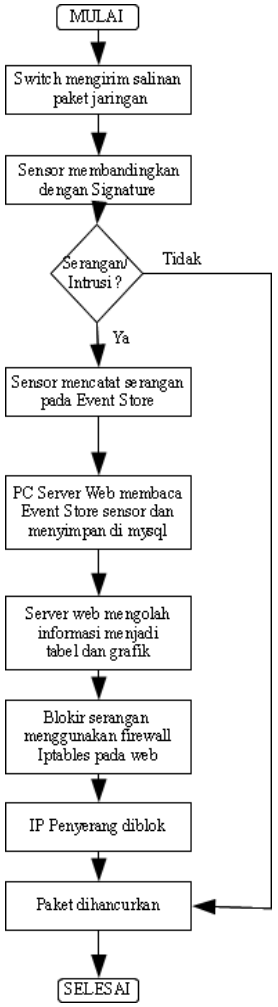
Perancangan sistem ini membutuhkan satu komputer klien dengan OS BackTrack 5 R1, satu komputer sebagai *server web* menggunakan OS Ubuntu 12.0, sebuah Cisco Switch dan sebuah sensor Cisco IPS 4240 versi 7.0(2).E4.

Sensor Cisco IPS 4240 dikonfigurasi menggunakan dua antarmuka, Gigabit Ethernet0/0 sebagai antarmuka pemantauan dan Management0/0 sebagai antarmuka perintah dan kontrol. Sensor dirancang untuk dapat mengirim event melalui fitur server *web* milik sensor. Event akan dikomunikasikan dalam dokumen XML melalui servis HTTP port 80. Switch pada jaringan menggunakan *port mirroring*, yaitu untuk mengkopi paket jaringan ke antarmuka pemantauan sensor.



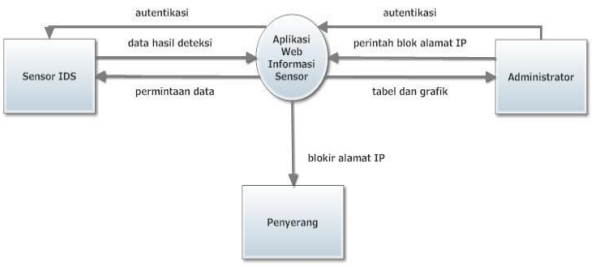
Gambar 1 Topologi Lengkap Jaringan

Sistem yang akan diimplementasikan nantinya terdiri dari tiga poin penting, yaitu target serangan, penyerang, dan sensor. Sensor mendeteksi serangan kemudian mengolah hasil deteksi menjadi tabel dan grafik.



Gambar 2. Flowchart Kinerja Sensor

Perancangan ini menggunakan beberapa metode pemodelan pemrograman terstruktur yaitu DFD (*Data Flow Diagram*) yang telah menjadi standar dalam industri untuk mengetahui aliran data dalam sebuah program



Gambar 3. DFD level 0 aplikasi web

DFD *level* 1 yang ditunjukkan Gambar 3.6 terdiri dari empat proses, yaitu :

1. Login *web*

Merupakan proses autentikasi administrator yang mengakses akan aplikasi *web*. Tabel dan grafik hasil deteksi sensor dapat diakses setelah *login* sukses.

2. Pengambilan informasi sensor

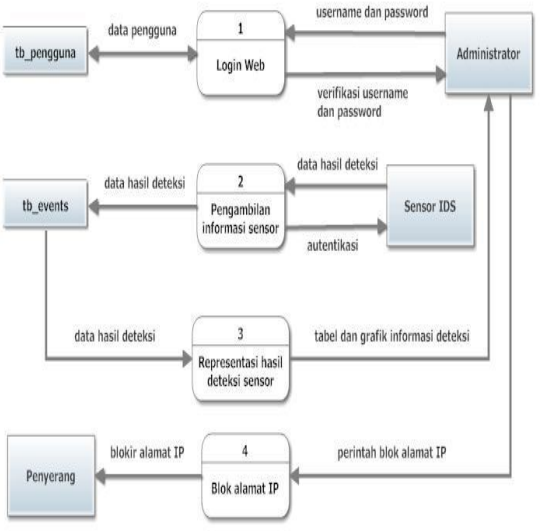
Merupakan proses pengambilan informasi dari sumber utamanya yaitu Sensor IDS kemudian disimpan dalam tabel `tb_events`. Autentikasi *username* dan *password* sensor dibutuhkan sebelum dapat mengambil informasi dari sensor.

3. Representasi hasil deteksi sensor

Merupakan proses pengambilan hasil deteksi dari tabel `tb_events` kemudian mengolahnya menjadi tabel dan grafik untuk ditampilkan ke pengguna *web* (administrator).

4. Blok alamat IP

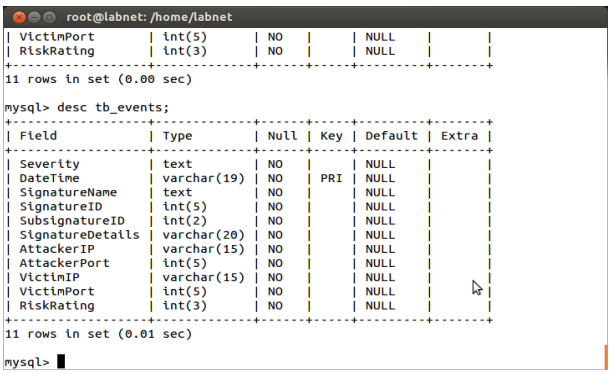
Merupakan proses kelanjutan setelah administrator sukses *login* ke aplikasi *web* dan melihat hasil deteksi sensor, administrator dapat memblokir alamat IP yang dianggap berbahaya



Gambar 4. DFD level 1 aplikasi web

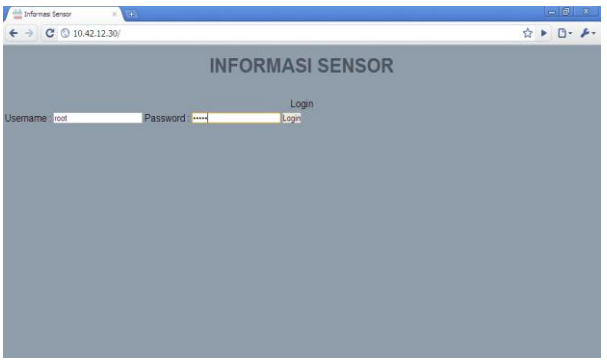
4. IMPLEMENTASI SISTEM

Implementasi yang dimaksud adalah usaha yang dilakukan untuk mengaplikasikan perancangan dengan harapan dapat menciptakan IDS yang sesuai dengan tujuan penelitian. Implementasi ini meliputi instalasi dan konfigurasi sistem operasi BackTrack 5 R1, PHP, MySQL, dan sensor Cisco IPS 4240.



Gambar 5. Tampilan basis data hasil deteksi sensor

Implementasi server web dilakukan sesuai perancangan yang telah dilakukan sebelumnya. Tampilan awal web adalah form validasi pengguna (administrator).

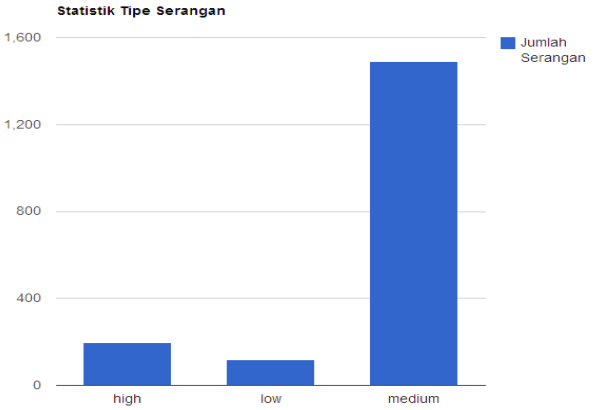


Gambar 6. Tampilan awal web

Tampilan halaman utama setelah *login* berisi menu Grafik Kategori Serangan, Grafik Penyerang, Grafik Korban Serangan, Tabel Daftar Serangan, Blok Alamat IP dan menu Logout.

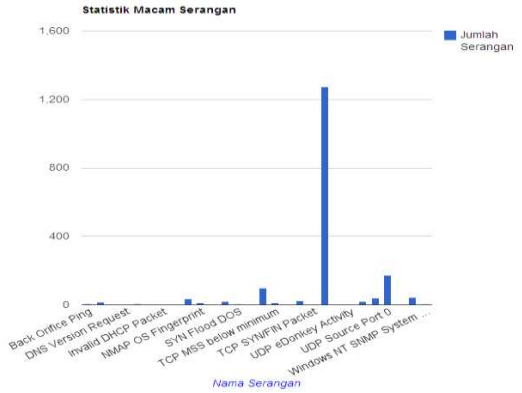
Gambar 7. Tampilan halaman utama

Submenu Tingkat Serangan berisi statistik serangan yang terjadi, apakah serangan termasuk kategori *low*, *medium*, atau *high*.



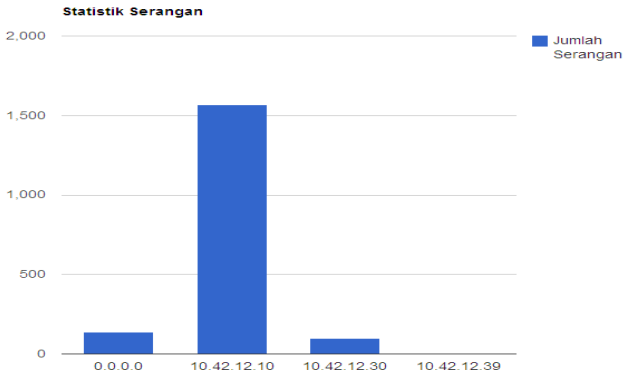
Gambar 8. Tampilan submenu Tingkat Serangan

Submenu Macam Serangan beris istatistik macam-macam serangan yang terdeteksi beserta jumlah serangannya.



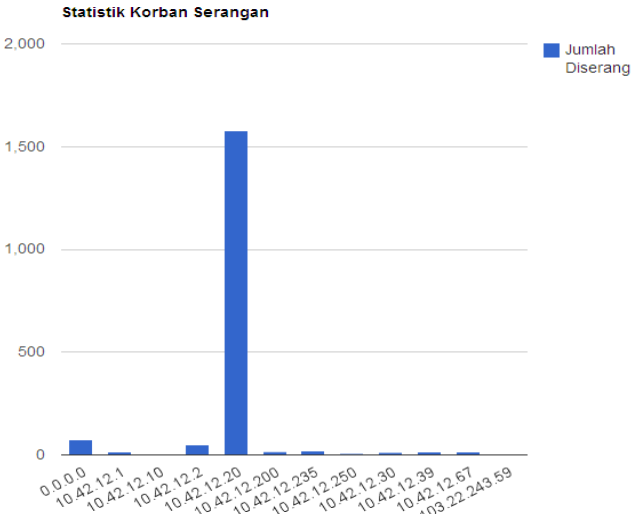
Gambar 9. Tampilan submenu Macam Serangan

Submenu Alamat IP Penyerang beris statistic alamat IP yang berusaha menyerang beserta jumlah usahanya.



Gambar 10. Tampilan submenu Alamat IP Penyerang

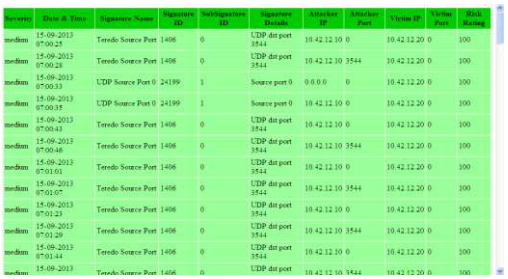
Submenu Alamat IP Korban berisi statistik alamat IP korban yang diserang beserta jumlah dari berapa kali diserang.



Gambar 11. Tampilan submenu Alamat IP Korban

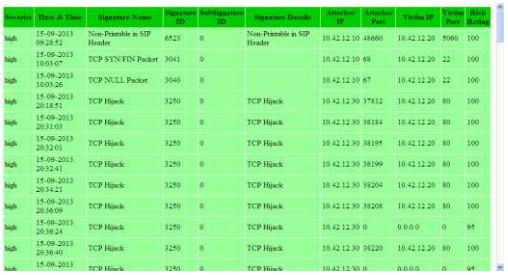
Submenu Semua Serangan menampilkan serangan kategori rendah, menengah, dan tinggi.

Tabel 1.. Tampilan submenu Semua Serangan



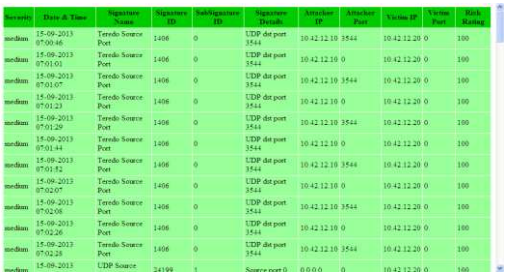
Submenu Serangan Kategori Tinggi hanya menampilkan serangan kategori tinggi.

Tabel 2.. Tampilan submenu Serangan Kategori Tinggi



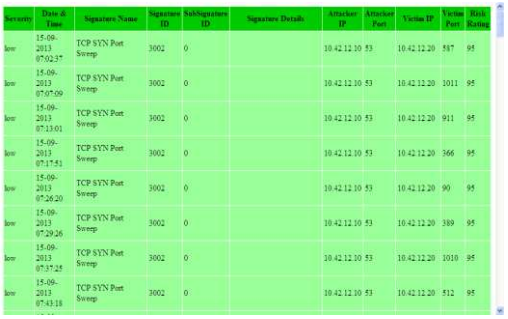
Submenu Serangan Kategori Menengah hanya menampilkan serangan kategori menengah.

Tabel 3.. Tampilan submenu Serangan Kategori Menengah



Submenu Serangan Kategori Rendah hanya menampilkan serangan kategori rendah.

Tabel 4.. Tampilan submenu Serangan Kategori Rendah



5. PENGUJIAN SISTEM

Setelah proses perancangan dan implementasi selesai dilakukan, kemudian masuk ke tahap selanjutnya yaitu pengujian. Pengujian bertujuan untuk memastikan bahwa IDS mampu mendeteksi serangan dan server web mampu mengolah hasil deteksi sensor menjadi tabel dan grafik serta firewall Iptables mampu memblokir alamat IP penyerang.

Hasil yang didapatkan pada dasarnya telah sesuai dengan hasil perancangan. Pada perangkat sensor Cisco 4240, usaha penyusupan dapat terdeteksi. Pengujian dilakukan dengan mencoba melakukan penetrasi menggunakan *tools* berikut ini.

1. Autoscan

   Komputer klien menggunakan Autoscan untuk melakukan pemindaian perangkat yang terhubung ke jaringan. Usaha ini dilakukan dengan mencoba memanfaatkan fasilitas *open trace* pada komputer target.

2. Zenmap

   Zenmap dibangun berdasarkan Nmap dengan tambahan tampilan GUI untuk memudahkan pengguna. Zenmap digunakan untuk memindai layanan atau port yang aktif pada komputer target. Tujuannya adalah dapat memanfaatkan kelemahan (*vulnerability*) pada port aktif tersebut.

3. Unicornscan

   Unicornscan adalah *tools* pemindai yang bekerja secara *asynchronous*.Unicorn scan mampu memindai menggunakan paket kosong (*null*), SYN, ACK, dan Fin.

4. Ettercap

   Ettercap digunakan untuk membanjiri komputer target dengan paket-paket tertentu sehingga komputer target tidak dapat melakukan akifitas pada jaringan. Ettercap termasuk metode DDOS (*Distributed Denial Of Service*) namun tidak menyebabkan

komputer target *hang* atau *restart* secara otomatis.

5. hping3

hping3 adalah generator paket yang bekerja pada protokol TCP/IP yang digunakan untuk analisis. Aplikasi ini digunakan untuk membanjiri komputer target dengan paket-paket UDP.

Server web diuji apakah dapat mengambil dan mengolah hasil deteksi sensor menjadi tabel dan grafik. Server web teruji mampu mengambil hasil deteksi kemudian disimpan dalam *database* kemudian mengolahnya menjadi tabel dan grafik dalam aplikasi *web*. Tabel dan grafik menunjukkan usaha-usaha penyusupan, penyerangan ataupun eksploitasi terhadap sistem, langkah selanjutnya adalah memblokir alamat IP yang dianggap berbahaya. *Firewall* Iptables mampu mengeksekusi perintah blokir alamat IP secara tepat sesuai dengan perintah blokir yang diberikan adminstrator.

Analisa kinerja semua komponen secara keseluruhan diatas menunjukkan bahwa semua komponen dapat bekerja dengan baik sesuai fungsinya..

Tabel 5.. Tampilan submenu Serangan Kategori Rendah

No	Nama	Terdeteksi oleh sistem (Ya/Tidak)	Dapat diblokir (Ya/Tidak)	Event dapat ditampilkan di web (Ya/Tidak)
1	Autoscan	Ya	Ya	Ya
2	Zenmap	Ya	Ya	Ya
3	Unicornscan	Ya	Ya	Ya
4	Ettercap	Ya	Ya	Ya
5	hping3	Ya	Ya	Ya

6. PENUTUP

6.1 Kesimpulan

1. Sensor Cisco IPS 4240 bekerja sebagai IDS dalam mode *promiscuous*.
2. Sensor mampu mendeteksi dan mencatat serangan Autoscan, Zenmap, Unicornscan, dan hping3.
3. Sensor memiliki dua jenis antarmuka yang berbeda fungsinya, yaitu antarmuka pemantauan untuk mendeteksi paket dan antarmuka perintah dan kontrol untuk keperluan manajemen sensor.
4. Sensor menyimpan kejadian-kejadian dalam bentuk XML melalui protokol Security Device Event Exchange (SDEE) dengan ukuran maksimal 800 KiloByte tiap satu permintaan.
5. *Aplikasi web* mampu menampilkan hasil deteksi sensor yang berupa data mentah menjadi bentuk tabel dan grafik.

1.2 Saran

1. Aplikasi *web* dapat dikembangkan menjadi aplikasi dekstop yang berkomunikasi dengan sensor menggunakan protokol SDEE.
2. Kemampuan memblokir sebaiknya dibuat otomatis (skrip program) yang dikembangkan dengan Bahasa Pemrograman Perl.

DAFTAR PUSTAKA

[1] Ariewijaya. *Optimalisasi Network Security Dengan Mengkombinasikan Instrusion Detection System dan Firewall pada Web Server*. Skripsi Jurusan Teknik Informastika Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta. 2011.

[2] Carter, Earl. dan Jonathan, Hogue. *Intrusion prevention fundamentals*. Pearson Education India, 2006.

[3] "Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.0". Diakses 26 Maret 2013. http://www.cisco.com/en/US/docs/security/ips/7.0/configuration/guide/cli/cli_setup.html

[4] "Cisco Secure Intrusion Detection System" . Diakses 6 April 2013. http://docstore.mik.ua/cisco/pdf/security/CCSP_CSID4.0_Knet.pdf

[5] "Docs for Webmin". Diakses 17 Mei 2013. http://doxfer.webmin.com/ Webmin

[6] Hakim, Lukamanul. *Jalan Pintas Menjadi Master PHP*. Yogyakarta : Lokomedia, 2009.

[7] Hartono, Puji. *Sistem Pencegahan Penyusupan pada Jaringan Berbasis Snort IDS dan IPTables Firewall*. Yogyakarta : Andi, 2006.

[8] Hirin A.M dan Virgi. *Cepat Mahir Pemrograman Web demgan PHP dan MySQL*. Jakarta : Prestasi Pustakaraya, 2011.

[9] Kimin, Hans Verdian. *Perancangan Sistem Keamanan Jaringan Komputer Berbasis Snort Intrusion Detection System dan IpTables Firewall*. Skripsi Departemen Teknik Elektro Fakultas Teknik Universitas Sumatra Utara Medan. 2010.

[10] Kurniawan, Heri. *Trik Membuat Web Template dengan PHP & CSS*. Yogyakarta : Lokomedia, 2011.

[11] Rowland, Craig H. *Intrusion detection system*. U.S. Patent No. 6,405,318. 11 Jun. 2002.

[12] Scarfone, Karen. dan Mell, Peter. "Guide To Intrusion Detection and Prevention System (IDPS)". Diakses 17 Mei 2013. http://csrc.nist.gov/ publications/nistpubs/800-94/ SP800-94.pdf

[13] "SDEE and IPS". Diakses 9 April 2013. https://supportforums.cisco.com/ docs/DOC-12515

[14] Supriyanto, Aji. *Penyajian Dokumen XML dengan Teknik Pengikatan Data*. Fakultas Teknologi Informasi Universitas Stikubank Semarang. 2005.

[15] "Xpath Examples". Diakses 20 April 2013. http://msdn.microsoft.com/en-us/library/ms256086(v=vs.110).aspx