UNIVERSITAS
ATMA JAYA YOGYAKARTA

ISSN : 2089-9815

PROCEEDING SENTIKA 2014

http://fti.uajy.ac.id/sentika

15 Maret 2014

Auditorium Kampus Bonaventura
Universitas Atma Jaya Yogyakarta

PROCEEDING SENTIKA 2014
ISSN 2089-9815

15 Maret 2014

Alamat Redaksi & Distribusi
Tata Usaha Fakultas Teknologi Industri
Universitas Atma Jaya Yogyakarta
Jln. Babarsari No. 43, Yogyakarta 55281
Telp. (0274) 487711 Fax. (0274) 485223

E-mail : sentika@uajy.ac.id
Website : http://fti.uajy.ac.id/sentika/

Proceeding Sentika 2014 diterbitkan oleh Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta sebagai media untuk menyalurkan pemahaman tentang aspek-aspek teknologi teknologi informasi berupa hasil penelitian lapangan atau laboratorium maupun studi pustaka yang melengkapi *event* Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA) 2014.

ISSN: 2089-9813

ANALISA DAN PENGEMBANGAN SISTEM PERINGATAN KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SMS GATEWAY DAN PAKET FILTER

Mario A. A. Gobel[1], Suyoto[2], Thomas Suselo[3]
[1]*Program Studi Teknik Informatika, Fakultas Teknologi Industro, Universitas Atma Jaya Yogyakarta*
Jl. Babarsari 43 Yogyakarta 55281
Telp. (0274) 48758
[2]*Jurusan Magister Teknik Informatika, Program Pasca Sarjana, Universitas Atma Jaya Yogyakarta*
Jl. Babarsari 43 Yogyakarta 55281
E-mail: arizald.vg@gmail.com

ABSTRAK

Pada laporan tahunan Indonesia Security Incident Response Team Internet Infrastructure (ID-SIRTII) telah mengadakan survey random sampling tentang kesiapan sistem dan prosedur terhadap sejumlah perusahaan serta instansi pemerintah di berbagai sektor yang bisa dianggap strategis dan kritikal. Hasilnya meskipun sebagian besar telah memiliki instrument pengamanan namun banyak sekali kelemahan akibat sistem yang diterapkan secara parsial, pengabaian oleh manajemen, kelalaian dan masih rendahnya sikap perilaku pengamanan sendiri (self protection), semua ini mengakibatkan tingginya angka insiden yang tidak disadari oleh pemilik sistem (Salahuddien, 2009). Pada tulisan ini akan difokuskan membahas peningkatan self protection atau perilaku pengamanan sendiri administrator, yaitu bagaimana dengan melakukan report status dari sistem secara real-time kepada administrator agar dapat memantau availabilty dari sistem yang dikelola. Hasil penelitian ini dapat disimpulkan bahwa peningkatan sikap self protection dapat dilakukan dengan sistem peringatan yang dapat memberikan laporan peringatan secara berkala. Hal ini tentu diharapkan juga dapat mengurangi beban kerja administrator.
Kata Kunci: keamanan jaringan, sms gateway, NIDS, paket filter, self protection

ABSTRACT

In the annual report of Indonesia Security Incident Response Team Internet Infrastructure (ID - SIRTII) has conduct random sampling survey on the readiness of systems and procedures against a number of companies and government agencies in a variety of sectors that can be considered strategic and critical . The result though most have had a security instrument , but a lot of weaknesses due partially implemented system , neglect by management , negligence and the low security behavior attitudes (self protection) , all of this results in a high number of incidents that are not recognized by the system owner (Salahuddien , 2009) . This paper will focus on discussing the increase in "self protection" or safety behaviors own administrator , ie how to do report the status of the system in real-time to the administrator in order to monitor the availabilty of the managed system . The results of this study it can be concluded that the increase in the attitude of "self- protection" can be done with a warning system that can alert periodically reports . This course is also expected to reduce the workload of administrators .
Keywords: keamanan jaringan, sms gateway, NIDS, paket filter, self protection

1. PENDAHULUAN

Tren serangan terbesar diarahkan pada port 53 dengan total mencapai 300.000 serangan atau 12.000 serangan perhari. Serangan kedua terbesar diarahkan pada port 1434 dengan total serangan mencapai 278.000 serangan atau 8.000 serangan perhari, sedangkan serangan ketiga terbesar diarahkan pada port 1433 dengan total serangan 225.000 atau 7.000 serangan per hari. Puncak serangan terjadi pada tanggal 20 Oktober 2012 yang ditujukan pada port 53 dimana mencapai 21.000 serangan Penyebab insiden tertinggi lainnya adalah diakibatkan oleh kesalaha prosedur pengamanan dan kelalaian pengelola sisitem, kemudian akibat pengabaian dan ketiadaan prosedur serta pengelolaan sistem pengamanan yang memadai (Salahuddien, 2009).

Menurut Salahuddien (2009), pada laporan tahunan Indonesia Security Incident Response Team Internet Infrastructure (ID-SIRTII) juga telah mengadakan *survey random sampling* tentang kesiapan sistem dan prosedur terhadap sejumlah perusahaan serta instansi pemerintah di berbagai sektor yang bisa dianggap strategis dan kritikal. Hasilnya meskipun sebagian besar telah memiliki instrument pengamanan namun banyak sekali kelemahan akibat sistem yang diterapkan secara parsial, pengabaian oleh manajemen, kelalaian dan masih rendahnya sikap perilaku pengamanan sendiri (*self protection*), semua ini mengakibatkan tingginya angka insiden yang tidak disadari oleh pemilik sistem.

ISSN: 2089-9813

Pada penelitian ini yang menjadi pokok pembahasan adalah permasalahan yang muncul dari penerapan kemananan jaringan komputer, karena permasalan yang muncul bukan hanya datang dari luar seperti usaha-usaha pembobolan terhadap keamanan tersebut tetapi kendala yang terjadi akibat penerapan dari sekuritas itu sendiri. Keterbatasan *resource* dalam penerapan sistem keamanan, sistem yang diterapkan secara parsial, pengabaian oleh manajemen, kelalaian dan masih rendahnya sikap perilaku pengamanan sendiri (*self protection*) menjadi beberapa kendala utama.

Analogi yang dapat dicontohkan misalkan pada kasus *administrator* yang harus setiap saat memantau kondisi sistem agar dapat berjalan normal tanpa ada gangguan dari dalam maupun dari luar, pada kondisi ini sistem keamanan akan bergantung penuh pada kesiagaan *administrator* dalam menjaga keamanan terutama pada sistem dengan pengamanan yang diterapkan secara parsial. Hal ini menjadikan sistem rentan mendapat gangguan dikarenakan kelengahan *administrator* dalam melakukan monitoring terhadap keamanan sistem atau pun dalam menutupi celah keamanan yang tidak terpantau selalu menjadi kasus yang sering muncul.

Pada tulisan ini akan dibahas tentang bagaimana meningkatan *self protection* dengan menerapkan beberapa aplikasi berbeda. Beberapa aplikasi yang digunakan antara lain SMS *gateway*, paket *capture* dan paket *filter*. Aplikasi ini bersinergi untuk melakukan monitoring terhadap aliran paket data dan melaporkan status sistem secara *real-time* kepada *administrator* melalui SMS *gateway*.

2. TINJAUAN PUSTAKA

2.1 Deteksi Intrusi

Deteksi intrusi adalah proses *monitoring* komputer atau jaringan untuk aktivitas atau kegiatan yang tidak sah. IDS juga dapat digunakan untuk memonitor lalu lintas jaringan, sehingga mendeteksi jika sistem sedang ditargetkan oleh serangan jaringan (Darapareddy and Gummadi, 2012). Terdapat dua tipe dasar deteksi intrusi : berbasis *host* (HIDS) dan berbasis jaringan (NIDS). Masing-masing memiliki pendekatan yang berbeda untuk memonitor dan mengamankan data. HIDS berbasis *host* memeriksa data yang diselenggarakan pada masing-masing komputer yang berfungsi sebagai tuan rumah, mereka sangat efektif untuk mendeteksi pelanggaran *insider*. Contoh IDS berbasis *host* adalah keamanan Windows NT/2000 dengan penggunaan Log dan Syslog UNIX. Di sisi lain jaringan berbasis sistem deteksi intrusi (NIDS) menganalisis paket data yang melalui jaringan aktual. Paket diperiksa dan dibandingkan dengan data empiris untuk memverifikasi apakah mereka alam berbahaya atau jinak. Contoh dari NIDS adalah Snort, yang merupakan jaringan sistem deteksi intrusi *open source* yang melakukan analisis lalu lintas *real-time*. Sistem Deteksi Intrusi (IDS) merupakan salah satu model sistem keamanan yang banyak diterapkam karena efektifitas dan efisiensi yang dimiliki (Faizal et all, 2009), (Victor et all, 2010).

2.2 Paket Data

Paket data adalah entitas dasar dari semua sistem komunikasi. Keamanan jaringan demikian berarti keamanan dari paket data. Sebuah paket data adalah blok yang paling dasar komunikasi yang melibatkan aliran streamline terbatas replika lainnya untuk mengirimkan informasi dari satu perangkat ke perangkat lainnya. Sebuah paket data yang terkandung dalam segmen data yang menimpan informasi lain seperti protokol yang digunakan, tujuan *hardware* alamat dan lain-lain. Singkatnya, identitas setiap paket yang datang dari sumber tidak bisa diandalkan dapat dideteksi dengan mempelajari isinya. Manajemen trafik data, pengukuran trafik jaringan komputer dan *sniffing* adalah beberapa produk dari *packet capture, packet capture* juga digunakan sebagai basis untuk berbagai macam sistem keamanan (Suri and Batra, 2012), (Aluvala, 2011).

2.3 Paket Filter

Informasi yang ditransmisikan pada jaringan dalam bentuk "paket", dengan kata lain informasi dibagi menjadi potongan-potongan kecil pada sumbernya, ditransmisikan dan kembali berkumpul pada penerima akhir. *Firewall* memeriksa bagian yang relevan dari sebuah paket dan hanya memungkinkan orang-orang yang sesuai dengan konfigurasi yang akan berhasil dikirim. Inilah sebabnya, beberapa paket yang tepat dikonfigurasi salah yang ditolak oleh *firewall*. Dalam kasus *firewall proxy*, lalu lintas tidak pernah mengalir langsung antara jaringan. Sebaliknya, *proxy repackages* permintaan dan tanggapan. Tidak ada host internal dapat diakses secara langsung dari jaringan eksternal dan tidak ada host eksternal secara langsung dapat diakses oleh host internal. Pekerjaan utama dari *firewall* adalah *Packet Filtering*, yang mengontrol akses dengan memeriksa paket berdasarkan isi dari *header* paket (Lindqvist et all, 2010), (Arai, 2012).

Salah satu cara untuk menerapkan *firewall* adalah untuk memanfaatkan apa yang disebut *packet filtering*. *Packet filtering* telah terbukti menjadi alat yang berguna untuk menempatkan kontrol akses ke lalu lintas IP. *Packet filtering* yang dapat digunakan untuk memblokir paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol. Data sebagai sumber dan alamat tujuan, UDP dan TCP, port asal dan tujuan dapat digunakan dalam keputusan penyaringan. Metode ini juga banyak digunakan dalam sistem monitoring jaringan, dengan menerapkannya pengguna dapat memantau aktifitas

ISSN: 2089-9813

pada jaringan setiap saat (Aluvala, 2011), (Al-Mukhtar, 2012).

2.4 SMS Gateway

Distribusi informasi yang baik menjadikan suatu sistem informasi menjadi lebih optimal dalam penerapannya, terdapat berbagai macam kebutuhan distribusi informasi sesuai dengan keperluan yang variatif. Salah satu model distribusi informasi yang saat ini masih banyak digunakan adalah SMS Gateway, model ini memberikan efektifitas pada keperluan yang *real-time* dikarenakan pesan yang dapat didistribusikan kapan saja dan pengguna dapat menerima informasi secara langsung. SMS Gateway adalah sebuah perangkat atau layanan yang menawarkan SMS transit, mengubah pesan untuk lalulintas jaringan selular dari media lain atau sebaliknya, sehingga memungkinkan pengiriman atau penerimaan pesan SMS dengan atau tanpa menggunakan ponsel. SMS Gateway adalah cara yang paling cepat dan handal untuk SMS *massal/bulk*. Sistem ini juga dikembangkan untuk meningkatkan keamanan pengguna (Katankar and Thakare, 2010).

3. METODOLOGI PENELITIAN

3.1 Desain Penelitian

Penelitian ini dibuat berdasarkan studi terhadap beberapa literatur dimana permasalahan yang sering muncul dalam pengamanan suatu sistem. Permasalahan keamanan yang sering terjadi terdiri dari dua sisi yaitu eksternal dan internal, dari sisi external misalnya percobaan penyusupan untuk pencurian data ataupun tujuan lain sedangkan dari sisi internal misalnya penerapan keamanan secara parsial, pengabaian dan kelalaian oleh pengelola karena kurangnya kesadaran (*self protection*). Berdasarkan beberapa permasalahan diatas permasalahan diatas penelitian ini difokuskan pada permasalahan keamanan yang muncul dari sisi internal terutama dalam meningkatkan kesadaran akan pengamanan sendiri (*self protection*). Kelalaian dari pengelola (*administrator*) seringkali menjadi permasalahan internal yang muncul karena pengecekan yang jarang dilakukan dan terkadang pengecekan dilakukan setelah adanya gangguan serius yang terjadi seperti sistem *down*, layanan yang diberikan berhenti ataupun sistem telah disusupi (*defacing*, *identity theft*, *maleware* dll). Penelitian ini bertujuan meningkatkan kesadaran akan keamanan dari pengelola sistem dengan meningkatkan *self protection*.

Peningkatan dilakukan dengan mengintegrasikan beberapa aplikasi untuk memberikan *report* secara *real-time* kepada *administrator*. *Administrator* bertugas mengecek dan memastikan sistem yang dikelola berjalan dengan normal, hal ini mengharuskan *administrator* untuk dapat terus memantau sistem setiap saat. Penelitian ini dirancang agar seorang *administrator* dapat mengetahui kondisi serta status sistem yang dikelola setiap saat secara *real-time* sehingga untuk mengetahui kondisi sistem *administrator* tidak harus berada dilokasi sistem untuk melakukan pengecekan secara langsung. Hasil dari tulisan ini diharapkan selain mengurangi beban kerja dari pengelola tetapi juga dapat menekan tingkat insiden yang terjadi dikarenakan kelalaian ataupun rendahnya *self protection* dari pengelola.

3.2 Pendekatan Penelitian

Penelitian dilakukan berdasarkan beberapa literatur yang membahas secara detail tentang aplikasi sistem *monitoring* terhadap aliran data dan distribusi informasi menggunakan SMS *gateway*. Pendekatan dilakukan dengan mengintegrasikan aplikasi berbeda untuk melakukan *real-time report* kepada administrator. Beberapa aplikasi yang digunakan untuk memenuhi tujuan dari penelitian ini antara lain:

a. *Packet capture*
   Manajemen trafik data, pengukuran trafik jaringan komputer dan *sniffing* adalah beberapa produk dari *packet capture, packet capture* juga digunakan sebagai basis untuk berbagai macam sistem keamanan (Aluvala, 2011).
b. Packet filter
   Salah satu cara untuk menerapkan *firewall* adalah untuk memanfaatkan apa yang disebut *packet filtering*. *Packet filtering* telah terbukti menjadi alat yang berguna untuk menempatkan kontrol akses ke lalu lintas IP. *Packet filtering* yang dapat digunakan untuk memblokir paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol (Aluvala, 2011).
c. SMS gateway
   Salah satu model distribusi informasi yang saat ini masih banyak digunakan adalah SMS Gateway, model ini memberikan efektifitas pada keperluan yang *real-time* dikarenakan pesan yang dapat didistribusikan kapan saja dan pengguna dapat menerima informasi secara langsung (Katankar and Thakare, 2010).

Integrasi dari dari aplikasi tersebut dengan tujuan dapat bersinergi menghasilkan suatu fungsi baru untuk mencapai tujuan dari penelitian ini berdasarkan rancangan penelitian yang telah digambarkan sebelumnya.

3.3 Pengumpulan Data

Data dikumpulkan berdasarkan keterkaitan variabel-variabel yang digunakan sebagai bahan acuan dalam penelitian ini. Data yang digunakan antara lain untuk penulisan dan pengembangan skema sistem.

Studi literatur dilakukan dengan mengumpulkan data berupa jurnal-jurnal ilmiah, laporan-laporan tahunan dari badan terkait dan hasil survei. Data ini

ISSN: 2089-9813

digunakan untuk penulisan laporan sebagai latar belakang pembuktian adanya celah yang menjadi permasalaha dalam sistem keamanan dari sisi internal. Pengumpulan data literatur diambil dari situs-situs jurnal internasional dan situs resmi dari badan terkait yang mengeluarkan laporan serta melakukan survei mengenai keamanan jaringan komputer. Data berikut adalah data yang dibutuhkan dalam pengembangan purwarupa dari sistem yang akan dibangun yaitu berupa modul-modul aplikasi yang nantinya akan diintegrasikan menjadi satu. Modul-modul ini diunduh dari situs-situs *open source* dan forum-forum terkait yang banyak membahas tentang sistem keamanan jaringan komputer.

3.4 Metode Analisa

3.4.1 Kepustakaan

Penelitian dilakukan dengan pembelajaran pada naskah-naskah jurnal ilmiah, buku-buku dan literatur yang terkait dengan penelitian ini. Pemebelajaran ini bertujuan untuk merancang acuan dasar dari penelitan ini sebagai bahan pengembangan ide dan wawasan.

3.4.2 Analisa perancangan

Analisa dilakukan untuk mengetahui kebutuhan sistem yang akan diteliti sehingga dapat mencapai tujuan dari penelitian yang dilakukan, disamping itu dari hasil analisa ini akan dilakukan desain atau perancangan purwarupa sistem yang dikembangkan dalam bentuk algoritma deskriptif, skema ataupun mekanisme kerja sistem.

4. PEMBAHASAN

Kebutuhan dari perancangan mekanisme sistem *real-time report* yang akan dibahas pada bagian ini dipecah dalam beberapa bagian, dimana tujuan dari pengembangan konsep yaitu bagaimana mekanisme, algoritma dan skema konsep kerja sistem dalam melakukan *real-time report* kepada pengelola sistem (*administrator*) ketika terjadi kondisi anomali pada sistem. Kondisi anomali pada sistem sendiri didasarkan pada kebijakan yang ditetapkan oleh *administrator*.

4.1 Kondisi Anomali

Kondisi anomali terjadi apabila adanya aktifitas ilegal yang tidak dijinkan pada sistem, pada dasarnya kondisi anomali terjadi apabila aktifitas yang terjadi diluar dari kebijakan keamanan yang telah ditetapkan oleh administrator. Kondisi anomali yang difokuskan pada penelitan ini adalah kondisi anomali pada aliran paket data yang masuk dan keluar dari sistem. Paket data yang ditandai sebagai paket data ilegal yang dikategorikan sebagai aktifitas anomali pada penelitan ini fokus pada *port* yang digunakan dan alamat IP (*internet protocol*). Sebagai contoh terdapat beberapa *port* yang biasa digunakan untuk layanan yang diberikan oleh aplikasi pada sistem, Apabila terdeteksi paket data melalui *port* lain yang tidak diijinkan maka hal ini dapat dinyatakan ilegal untuk dilaporkan kepada *administrator*.

4.2 Kebutuhan Dasar Sistem

Terdapat beberapa aplikasi dasar yang dibutuhkan untuk membangun sistem ini. Aplikasi-aplikasi tersebut diintegrasikan menjadi satu dan bersinergi mencapai tujuan dari penelitan ini. Apalikasi yang dibutuhkan sebagai dasar dari sistem ini antara lain:

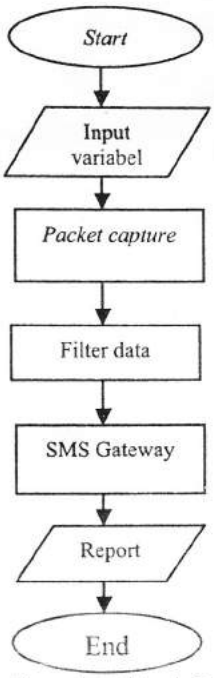
a. *Packet capture*
   Fungsi aplikasi ini sebagai pembaca aliran paket data yang keluar dan masuk pada sistem yang dikelola.
b. *Packet filter*
   Paket filter bertugas memisahkan data dari paket data yang telah di-*capture*, dimana pemisahan berdasarkan kebijakan keamanan yang ditetapkan oleh *administrator*.
c. SMS *gateway*
   SMS gateway berfungsi melakukan distribusi informasi (*real-time report*). Pemilihan SMS *gateway* dikarenakan informasi dapat langsung tersampaikan kepada *administrator* melalui SMS tanpa terkendala permasalahan lain misalnya koneksi internet pada ponsel.

Integrasi dari beberapa aplikasi dasar ini dapat dikategorikan sebagai Network Intrusion Detection System (NIDS), hal ini dikarenakan teknik ini memiliki pendekatan yang sama yakni *monitoring*.

4.3 Algoritma

Konsep kerja dari sistem *real-time report* akan dijelaskan pada bagian ini dalam bentuk algortima. Hasil dari analisa kebutuhan sistem maka didapatkan algoritma sebagai berikut seperti terlihat pada Gambar 1.

ISSN: 2089-9813



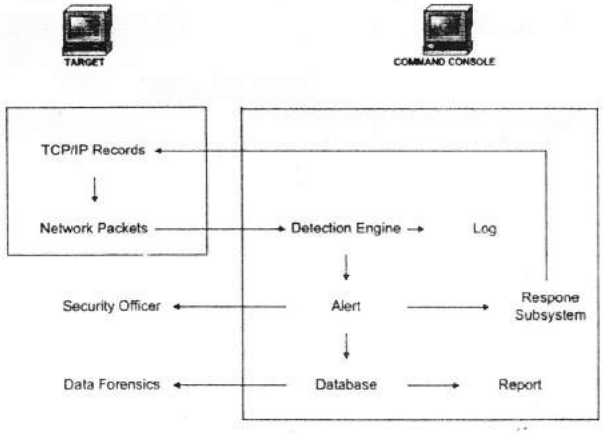
Gambar 1. Flowchart *Real-Time Report*

Proses dimulai dari menginputkan variabel yang menjadi parameter, setelah itu dilanjutkan dengan meng-*capture* paket data yang mengalir. Data hasil *capture* akan mulai di saring pada tahap ini, penyaringan yang berdasarkan variabel parameter. Apabila terdapat data yang masuk dalam klasifikasi parameter maka data akan diteruskan ke aplikasi SMS *gateway*, dari sini akan dikirimkan sebagai *report* kepada *administrator* yang sekaligus menjadi akhir proses dan dari tujuan sistem.

4.4 Analisa dan Arsitektur Sistem

4.4.1 Peringatan deteksi intrusi

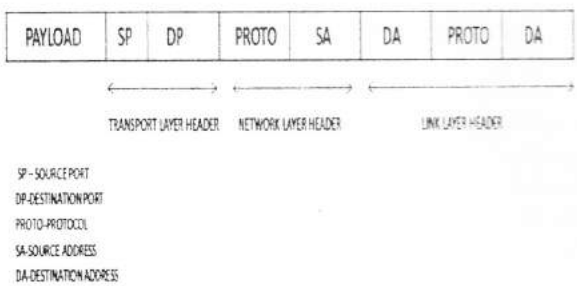
Deteksi intrusi terbagi menjadi dua yaitu deteksi intrusi berbasis jaringan dan deteksi intrusi berbasis *host*. Deteksi intrusi yang digunakan pada penelitian ini adalah deteksi intrusi berbasis jaringan (NIDS) karena pendeteksian dilakukan pada aliran data pada jaringan komputer. Seperti terlihat pada Gambar 2, adalah arsitektur standar dari deteksi intrusi berbasis jaringan. Dari arsitektur standar ini akan dikombinasikan dengan sistem SMS *gateway* yang berfungsi sebagai *alert* dengan melakukan *real-time report*. Sesuai dengan fungsi dari SMS *gateway* yang dapat mengirimkan informasi secara *real-time* maka diharapkan fungsi tersebut cukup efektif dalam memberikan peringatan kepada *administrator*. Pada Gambar 2, dijelaskan *alert* dari *detection engine* diteruskan pada *security officer* (*administrator*), *alert* ini yang akan diteruskan pada *security officer* melalui SMS *gateway*.



Gambar 2. Asitektur Standar NIDS (Anitha, 2011)

4.4.2 Penyaringan data

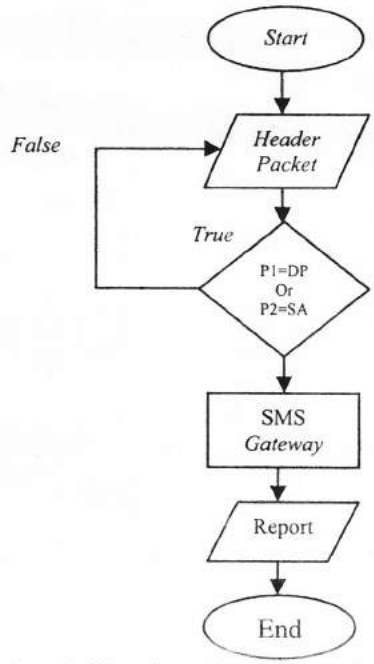
Proses penyaringan aliran data yang ter-capture dilakukan berdasarkan parameter yang ditentukan oleh *administrator*. Variabel parameter ditentukan oleh administrator yang kemudian variabel ini akan duganakan sebagai acuan dalam melakukan penyaringan. Penyaringan disini tidak berfungsi selayaknya *firewall* yang melakukan fungsi *droping packet*, hal ini karena diasumsikan penyaringan disini berfungsi terpisah sebagai pengaman tambahan dari yang dilakukan oleh *firewall*. Fungsi penyaringan data hanya difokuskan pada dua variabel yaitu *port* dan IP *address* sehingga pengecekan paket data hanya terbatas pada *destination port* (DP) dan *source* address (SA) seperti yang terlihat pada Gambar 3, penampang header paket data yang akan disaring.



Gambar 3. Header Paket Data (Raaj et all, 2013)

Berdasarkan konsep yang telah dijelaskan sebelumnya maka hasilnya dapat digambarkan dalam bentuk algoritma *flowchart* pada Gambar 4. Proses penyaringan ini berdasarkan dua variabel utama yang menjadi parameter dalam melakukan pengecekan *header* paket data yaitu SA (*source address*), DP (*destination port*), sedangkan pembanding yang menjadi parameter adalah P1 (parameter port) dan P2 (parameter IP *address*).

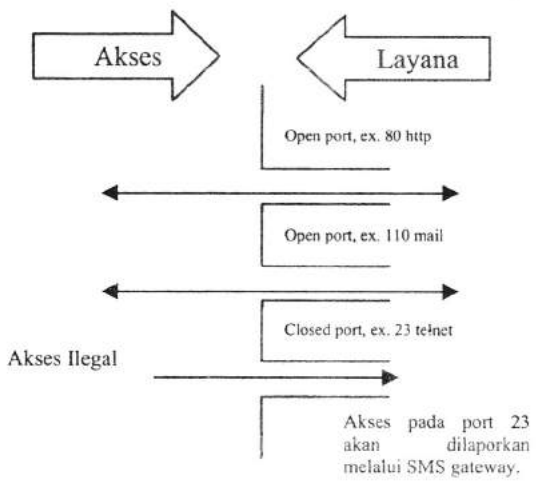
ISSN: 2089-9813



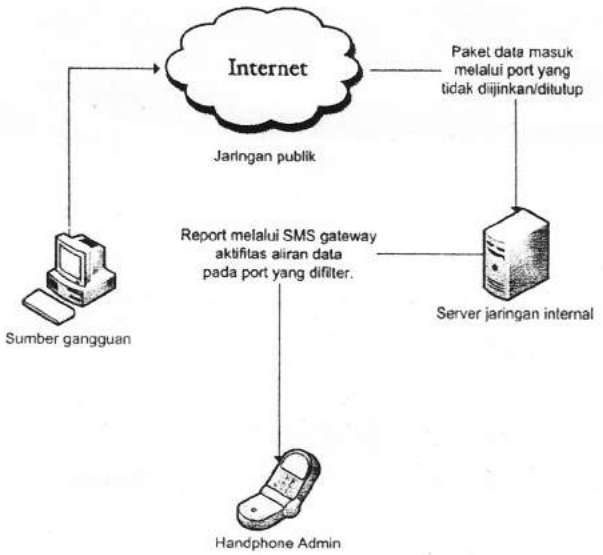
Gambar 4. *Flowchart* Penyaringan Data

4.4.3 Arsitektur sistem

Skenario yang dapat digambarkan adalah ketika sebuah sistem hanya memberikan beberapa layanan pada *port* tertentu, sedangkan akses yang masuk dari jaringan eksternal melalui *port* yang tidak termasuk dalam layanan sistem atau *port* yang telah ditetapkan sebagai parameter penyaringan maka aktifitas ini akan dilaporkan secara *real-time* kepada administrator. Seperti dijelaskan pada Gambar 5 mekanisme inti, setiap akses yang masuk melalui *port* yang tidak diijinkan maka akan dilaporkan sedangkan arsitektur sistem secara keseluruhan dijelaskan pada Gambar 6.



Gambar 5. Skenario Pemicu Peringatan



Gambar 6. Arsitektur Sistem

4.4.4 Data report

Data report yang akan disampaikan pada *administrator* melalui SMS *gateway* adalah data hasil *filtering* yang dikategorikan sebagai aktifitas anomali. Panjang konten laporan yang disampaikan melalui SMS *gateway* dibatasi pada jumlah maksimum karakter pada per satu SMS yaitu 160 karakter. Selanjutnya format laporan yang disampaikan berisi *source address*, *destination port* dan jumlah akses. Report dikirimkan dengan beberapa ketentuan yaitu akses dari *source address* yang belum dilaporkan sebelumnya sehingga mencegah pengiriman laporan secara berulang, jumlah akses dari terdiri dari 5 *source address* berbeda. Report dibatasi pada 5 *source address* karena panjang konten yang terbatas pada maksimum karakter seperti yang telah dijelaskan diatas.

4.5 Hasil

Berdasarkan hasil analisa dan pengembangan konsep yang dilakukan maka didapatkan dengan penerapan sistem ini dapat memberikan kontribusi secara langsung dalam meningkatkan perilaku pengamanan sendiri atau *self protection*. Hal ini dikarenakan dengan memberikan laporan secara real-time membuat *administrator* yang memiliki kesadaran akan *self protection* yang rendah ataupun yang tidak bisa melakukan pengecekan sistem secara langsung dapat mengetahui kondisi sistem melalui ponsel dimana setiap orang pasti selalu dekat dengan ponselnya, begitupun dengan *administrator*.

Selain itu hasil dari sistem ini juga diharapkan dapat mengurangi beban kerja dari *administrator* maupun menjadi alternatif sistem keamanan pada instansi ataupun organisasi yang memiliki keterbatasan *resource* dalam mengamankan sistem mereka. Seperti yang telah dibahas bahwa salah satu dari kelemahan sistem keamanan yang ada di

ISSN: 2089-9813

Indonesia adalah pengamanan yang diterapkan secara parsial.

5. KESIMPULAN

Dari hasil penelitian ini dapat disimpulkan bahwa peningkatan sikap *self protection* dapat dilakukan dengan sistem peringatan yang dapat memberikan laporan peringatan secara berkala. Hal ini tentu diharapkan juga dapat mengurangi beban kerja *administrator* yang tidak harus setiap saat melakukan pengecekan langsung terhadap sistem. Disisi lain sistem ini dapat diterapkan sebagai alternatif sistem keamanan tambahan pada sistem dengan pengamanan yang parsial.

PUSTAKA

Aluvala. 2011. *Inter-domain Packet Filters to Control IP-Forging: Research Journal of Computer Systems Engineering – An International Journal*, vol. 2, no. 2, pp. 67-72.

Arai, M. 2012. TCP/IP *Visualization Systems with a Packet Capturing Function: International Journal of Information and Education Technology,* vol.2, no.4 , 291-293.

Al-Mukhtar, M.M. 2012. *Development of a Flexible Real-Time Monitor for an Enterprise Network: International Jurnal of Computer Applications*. vol.42, no. 21, pp. 42-47.

Anitha, M. 2011. *Network Security Using Linux Intrusion Detection System: International Journal of Research in Computer Science*. vol. 2, no. 1, pp. 33-38.

Darapareddy, B. & Gummadi, V. 2012. *An Advanced Honeypot System for Efficient Capture and Analysis of Network Attack Traffic: International Journal of Engineering Trends and Technology,* vol.3, no.5.

Faizal, M. et all. 2009. *Threshold Verification Technique for Network Intrusion Detection System: International Journal of Computer Science and Telecommunications,* vol.2, no.1 , pp. 1-8.

Katankar and Thakare, V. M. 2010. *Short Message Service using SMS Gateway: International Journal of Computer Science and Engineering , 2* (4), pp. 1487-1491.

Kizza, J. M. (2005). *Computer Network Security.* Chattanooga: Springer.

Lindqvist, J. et all. 2010. *Enterprise Network Packet Filtering for Mobile Cryptographic Identities: International Journal of Handheld Computing Research,* vol.1, no.1, January , pp. 79-94.

Raaj S, V. et all. 2013. *An Effective Packet Filtering Mechanism For Reducing Complexity: International Journal of Emerging Technology and Advanced Engineering,* vol.3, no.1, , pp. 215-219.

Salahuddien, M. 2010. Pertahanan Keamanan Informasi Nasional: Laporan Tahunan ID-SIRTII.

Stallings, W. 2006. *Cryptography and Network Security Principles and Practices.*(Edisi ke-4). New Jersey: Pearson Prentice Hall.

Suri and Brata. 2012. *Comparative Study of Network Monitoring Tools: International Journal of Innovative Technology and Exploring Engineering,* vol.1, no.3, pp. 63-65.

Victor, G., Rao, M. and Venkaiah, V. 2010. *Intrusion Detection Systems - Analysis and Containment of False Positives Alerts: International Journal of Computer Applications,* vol.5, no.8, pp. 27-33.