Vol. 4, No. 2, Januari 2018 ISSN : 2407-5043

# PENERAPAN *SMS GATEWAY* DAN *PACKET FILTER* PADA PENGEMBANGAN *SECURITY ALERT SYSTEM* JARINGAN KOMPUTER

**Kurniati**
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Palembang
Universitas Bina Darma, Jln. Jenderal Ahmad Yani No.03 Palembang
E-mail : kurniati@binadarma.ac.id

***Abstrak***

Berdasarkan hasil analisis Indonesia *Security Incident Response Team Internet Infrastructure* (ID-SIRTII) menunjukan begitu banyaknya peringatan ancaman keamanan jaringan dan kerentanan sistem yang terjadi 3 tahun terakhir ini. Tingginya angka insiden yang tidak disadari oleh pemilik sistem ini terjadi akibat banyak sekali kelemahan yang dimiliki oleh sistem yang diterapkan secara parsial meskipun sebagian besar telah memiliki instrument pengamanan. Penerapan SMS *Gateway* dan *Packet Filter* pada *Security Alert System* jaringan komputer dan meningkatkan kesadaran akan keamanan dari pengelola sistem dengan meningkatkan *self protection* adalah cara untuk mengatasi masalah tersebut. Kedua cara tersebut berdasarkan studi literatur dapat mengurangi ancaman yang akan terjadi, yaitu dengan melakukan report status dari sistem secara *real-time* kepada administrator agar dapat memantau *availabilty* dari sistem yang dikelola secara berkala dengan member alert melalui media SMS tanpa harus seorang administrator berada di tempat. Sehingga, diharapkan juga dapat mengurangi beban kerja seorang administrator dalam memantau ancaman serangan dari luar terhadap jaringan komputer.

***Kata Kunci****: keamanan jaringan, sms gateway, NIDS, paket filter, self protection.*

## 1. PENDAHULUAN

### 1.1. Latar Belakang

Berdasarkan data statistik Tren Serangan Siber Nasional 2016 dan Prediksi 2017 yang dilakukan oleh Iwan Sumantri Ketua NCSD (National Cyber Security Defence) Wakil Ketua IDSIRTII – Kemenkominfo menunjukan bahwa tren serangan terbesar masih diarahkan pada *service port* 53 dengan total mencapai 135.672.984 pada tahun 2016 dengan serangan paling dominan adalah *DoS* dan *Web Injection* (*A1- Owasp*) yang mana serangan terbesar berasal dari Indonesia dengan target Indonesia. Sedangkan pada tahun 2017 di prediksi akan terjadi peningkatan serangan *Malware* yang lebih beragam, dengan banyaknya implementasi IoT (*Internet of Things*), sehingga memunculkan beberapa isu serangan baru dalam bentuk: *Botnet of Things (BoT)*, *Ransomware of Things*, dan *Mobile malware*. Menurut Singh (2017), berdasarkan data laporan peringatan ancaman keamanan dan kerentanan system pada laporan ID-SIRTII, banyak laporan dari sumber terbuka terhadap sebuah kampanye *ransomware* yang tersebar luas mempengaruhi berbagai organisasi dengan laporan puluhan ribu infeksi di 74 negara, termasuk Amerika Serikat, Inggris, Spanyol, Rusia, Taiwan, Prancis, dan Jepang. Perangkat lunak ini bisa berjalan dalam 27 bahasa yang berbeda. Versi terbaru dari varian *ransomware* ini, yang dikenal sebagai *WannaCry*, *WCry*, atau *Wanna Decryptor*, ditemukan pada pagi hari tanggal 12 Mei 2017 oleh seorang peneliti keamanan independen dan telah menyebar dengan cepat selama beberapa jam, dengan laporan awal dimulai sekitar pukul 4.00 pagi menunjukkan uang tebusan yang diminta sebesar 1781 bitcoin, kira-kira $ 300 US. *Alert* ini adalah hasil upaya antara Departemen Keamanan Dalam Negeri (DHS) Pusat Integrasi Cybersecurity and Communications Integration Nasional ( NCCIC) dan Federal Bureau of Investigation ( FBI ) untuk menyoroti ancaman *cyber*. DHS dan FBI terus mengupayakan informasi ancaman yang terkait dengan sistem pemerintah federal, negara bagian, dan pemerintah daerah. Permasalahan yang muncul pada penerapan

kemananan jaringan komputer tidak hanya berasal dari luar (eksternal) seperti usaha pembobolan keamanandari pihak luar tetapi kendala yang terjadi juga berasal dari internal yaitu 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.

Seorang *administrator* harus melakukan pemantauan kondisi sistem setiap saat. Sehingga, administrator dapat mengetahui apakah sistem berjalan secara normal tanpa adanya gangguan dari dalam maupun dari luar. Pada kondisi ini, system keamanan sangat bergantung penuh terhadap kesiagaan dari seorang *administrato*r dalam melakukan penjagaan keamanan terutama pada penerapan pengamanan sistem secara parsial. Hal inilah yang menjadi faktor utama sering munculnya kerentanan sistem dan mengakibatkan gangguan dikarenakan kelengahan administrator dalam melakukan *monitoring* terhadap celah keamanan sistem yang tidak terdeteksi. Pada tulisan ini, penulis akan membahas bagaimana cara meningkatan *self protection* dengan menerapkan beberapa aplikasi berbeda sebagai *security alert* jaringan komputer. Beberapa aplikasi yang dapat digunakan adalah paket *capture,* paket *filter* dan SMS *gateway*. Aplikasi ini bersinergi untuk melakukan *monitoring* guna melaporkan *report* status dari sistem secara *real-time* kepada administrator agar dapat memantau *availabilty* dari sistem yang dikelola secara berkala melalui SMS *gateway*.

### 1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka penulis merumuskan masalah dalam penelitian ini adalah :

1. Bagaimana cara menerapkan *SMS Gateway* dan *Packet Filter* pada penerapan *Security Alert system* jaringan komputer ?
2. Bagaimana cara meningkatkan kesadaran akan keamanan dari pengelola sistem dengan meningkatkan *self protection*?

## 2. METODOLOGI

### 2.1. Desain Penelitian

Penelitian ini dibuat berdasarkan studi literatur terhadap permasalahan yang sering terjadi dalam *security system*. Permasalahan keamanan tersebut dilihat dari dua sisi yaitu permalahan eksternal dan internal. Percobaan penyusupan yang dilakukan untuk melakukan pencurian data ataupun dengan tujuan lain itu merupakan contoh permasalahan keamanan dari sisi eksternal sedangkan dari sisi internal contohnya penerapan keamanan yang dilakukan secara parsial, pengabaian manajemen sistem dan kelalaian yang dilakukan oleh seorang pengelola (administrator) yang disebabkan kurangnya kesadaran terhadap diri sendiri (*self protection*). Penelitian ini bertujuan meningkatkan kesadaran akan keamanan dari pengelola sistem dengan meningkatkan *self protection*.

Peningkatan dilakukan dengan melakukan integrasi terhadap beberapa aplikasi untuk memberikan *report* secara *real-time* kepada *administrator*. Sehingga, pekerjaan seorang *administrator* akan lebih dipermudah karena sistem dapat dikelola tanpa harus berada dilokasi sistem untuk melakukan pengecekan secara langsung dan akan menekan tingkat insiden yang terjadi dikarenakan rendahnya *self protection* dari pengelola.

### 2.2. Pendekatan Penelitian

Penelitian dilakukan berdasarkan beberapa literatur yang membahas secara detail tentang aplikasi sistem *monitoring* terhadap aliran data dan distribusi informasi menggunakan SMS *gateway* untuk melakukan *real-time report* kepada administrator. Studi literatur dilakukan dengan mengumpulkan data berupa jurnal-jurnal ilmiah, laporan-laporan tahunan dari badan terkait dan hasil

survei. Data diperoleh dari studi literatur yang diambil melalui situs jurnal internasional dan situs resmi dari badan terkait yang mengeluarkan laporan serta melakukan survei mengenai keamanan jaringan komputer. Dengan data yang diperoleh maka berguna dalam melakukan pengembangan sistem yang akan yang dibangun dengan mengintegrasikan modul-modul aplikasi yang diunduh melalui situs-situs *open source* dan forum terkait yang banyak membahas tentang sistem keamanan jaringan komputer menjadi satu.

### 2.3. Metode Analisa

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

### 2.4. Analisa perancangan

Tujuan dari dilakukannya analisa adalah untuk mengetahui akan kebutuhan sistem yang diteliti. guna mencapai tujuan dari penelitian yang dilakukan. Sehingga, akan dilakukan desain atau perancangan purwarupa sistem yang dikembangkan dalam bentuk algoritma deskriptif, skema ataupun mekanisme kerja sistem.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Hasil

Berdasarkan hasil analisa dan pengembangan konsep yang dilakukan oleh peneliti, 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 Indonesia adalah pengamanan yang diterapkan secara parsial.

### 3.2. Pembahasan

Kebutuhan dari perancangan mekanisme sistem *real-time report* yang akan dibahas pada bagian ini terbagi atas beberapa bagian dilihat dari tujuan pengembangan konsep yaitu bagaimana mekanisme, skema konsep kerja dan algoritma siatem dalam melakukan *real-time report* kepada *administrator* ketika sistem terjadi kondisi anomali. Kondisi ini terjadi apabila adanya aktifitas berupa aliran paket data yang keluar masuk secara ilegal yang seharusnya tidak terjadi pada sistem, seperti aktifitas yang terjadi di luar kebijakan keamanan yang telah ditetapkan oleh seorang *administrator*.

#### 3.2.1 Kebutuhan Dasar Sistem

Berdasarkan hasil di atas untuk membangun sistem ini terdapat beberapa aplikasi dasar yang dapat digunakan. Beberapa aplikasi tersebut dapat diintegrasikan menjadi satu dan bersinergi guna mencapai tujuan dari penelitan ini. Apalikasi yang dibutuhkan diantaranya adalah:

1. *Packet capture,* digunakan sebagai basis untuk berbagai macam sistem keamanan. Contoh produk dari *packet capture* adalah manajemen trafik data, pengukuran trafik jaringan komputer dan

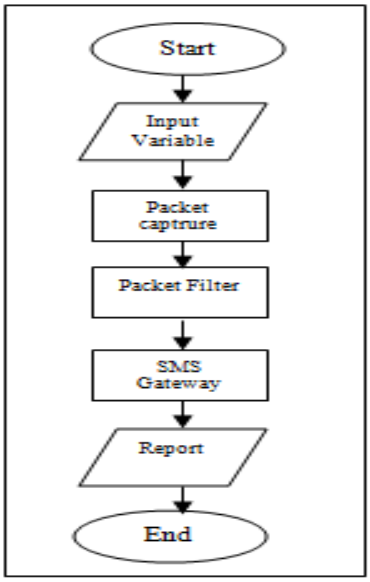
*sniffing* (Aluvala, 2011).

2. *Packet filter*, merupakan alat yang berguna untuk menempatkan kontrol akses ke lalu lintas IP guna melakukan pemblokiran paket data berdasarkan kriteria tertentu seperti protokol yang digunakan dan berbagai karakteristik protokol (Aluvala, 2011).
3. *SMS gateway* merupakan salah satu model distribusi informasi yang memberikan efektifitas pada keperluan yang *real-time* karena pesan dapat didistribusikan kapan saja dan pengguna dapat menerima informasi secara langsung (Katankar and Thakare, 2010).

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*.

### 3.2.2 Algoritma

Bentuk algortima dari konsep kerja dari sistem *real-time report* dapat dilihat pada gambar.1 berikut ini:

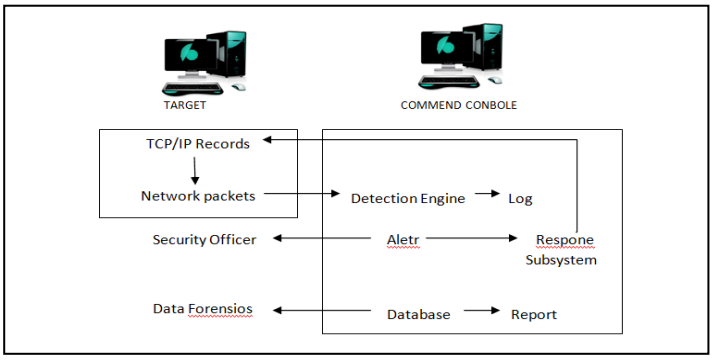



**Gambar 1.** Flowchart *Real-Time Report*

Proses yang dimulai dengan menginputkan variabel yang menjadi parameter, kemudian dilanjutkan dengan meng-*capture* paket data yang mengalir. Pada tahap ini, penyaringan dilakukan berdasarkan variabel parameter. Data akan diteruskan ke aplikasi SMS *gateway* jika terdapat data yang masuk dalam klasifikasi parameter. Pada akhir proses data akan dikirimkan sebagai *report* kepada *administrator* yang sekaligus menjadi akhir tujuan sistem.

### 3.2.3. Analisa dan Arsitektur Sistem

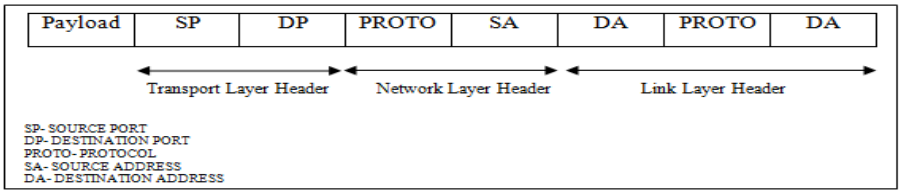
Peringatan Deteksi intrusi terbagi atas dua bagian yaitu deteksi intrusi berbasis jaringan dan deteksi intrusi berbasis *host*. Deteksi intrusi berbasis jaringan (NIDS) merupakan deteksi intrusi yang digunakan pada penelitian ini karena pendeteksian dilakukan pada aliran data pada jaringan komputer. Sistem SMS *gateway* yang telah dikombinasikan dengan arsitektur dasar akan berfungsi sebagai *alert* dan menghasilkan *real-time report*. Sehingga, cukup efektif dalam memberikan peringatan kepada *administrator*. Dimana *alert* dari *detection engine* diteruskan pada *security officer* (*administrator*) melalui SMS *gateway*.




**Gambar 2.** Asitektur Standar NIDS (Anitha, 2011)

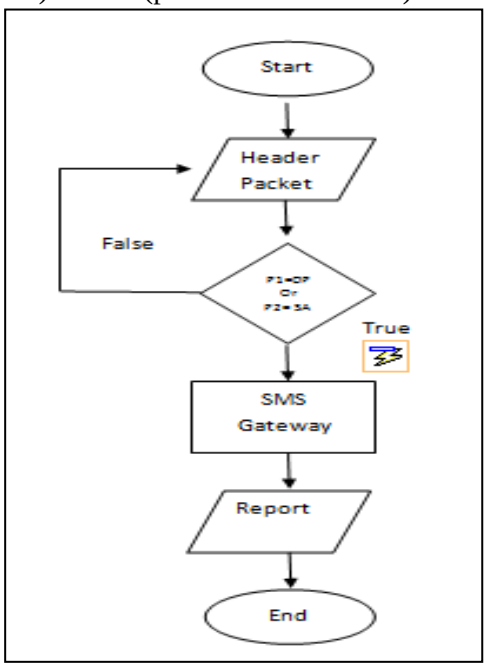
### 3.2.4. Penyaringan data

Proses penyaringan aliran data yang ter-*capture* dilakukan berdasarkan parameter yang ditentukan oleh *administrator*. Variabel parameter ini digunakan sebagai acuan dalam melakukan penyaringan. Namun, berbeda fungsi dengan *firewall* yang melakukan fungsi *droping packet*, dikarenakan penyaringan ini memiliki fungsi sebagai pengaman tambahan dari yang dilakukan oleh *firewall* yaitu hanya difokuskan pada dua variabel yaitu *port* dan IP *address* sehingga pengecekan paket data hanya terbatas pada *destination port* (DP) dan *source* address (SA).




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

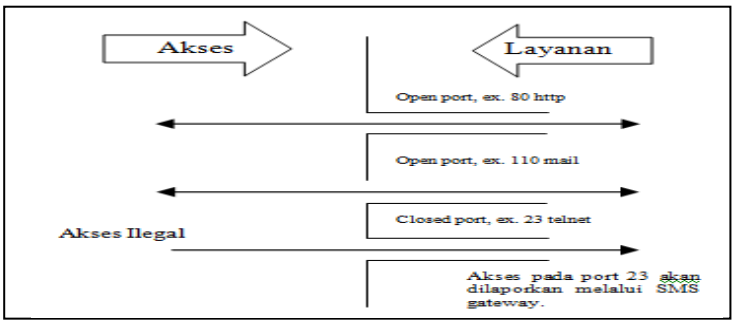
Berdasarkan konsep yang telah dijelaskan sebelumnya maka hasilnya dapat digambarkan dalam bentuk algoritma *flowchart* seperti pada Gambar 4. Pada gambar tersebut, proses penyaringan berdasarkan atas dua variabel utama sebagai parameter untuk melakukan pengecekan *header* paket data yaitu SA (*source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



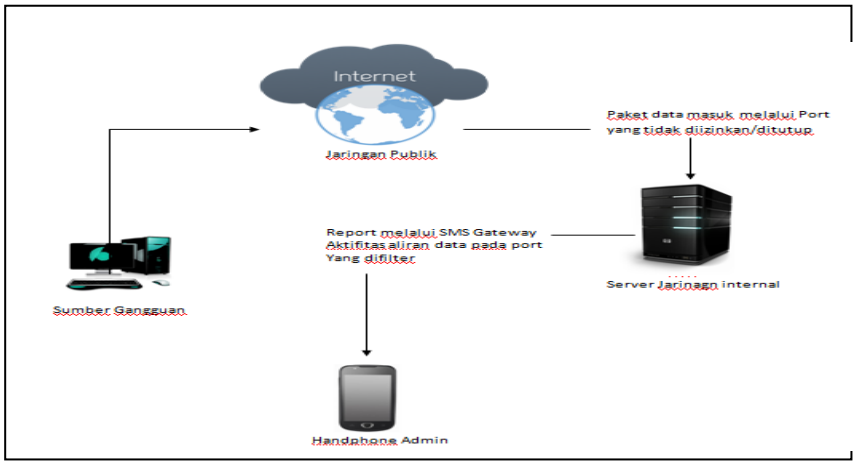

**Gambar 4.** *Flowchart* Penyaringan Data

### 3.2.5. Arsitektur sistem

Sebuah sistem hanya akan memberikan beberapa layanan pada *port* tertentu dengan memberikan batasan hak akses *port* yang telah ditetapkan sebagai parameter penyaringan. Sehingga, seorang *administrator* akan mendapatkan laporan secara *real-time* seperti dijelaskan pada gambar 5 dan gambar 6 di bawah ini :



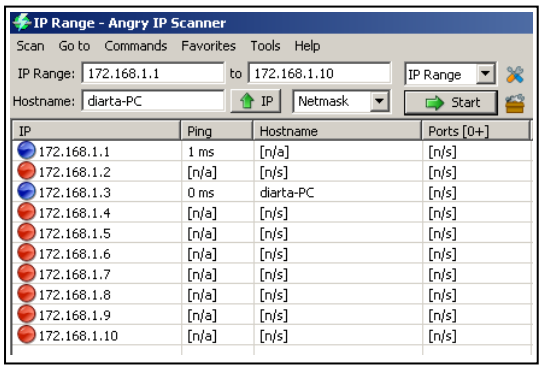

**Gambar 5.** Skenario Pemicu Peringatan




**Gambar 6.** Arsitektur Sistem

### 3.2.6. Pengujian Sistem

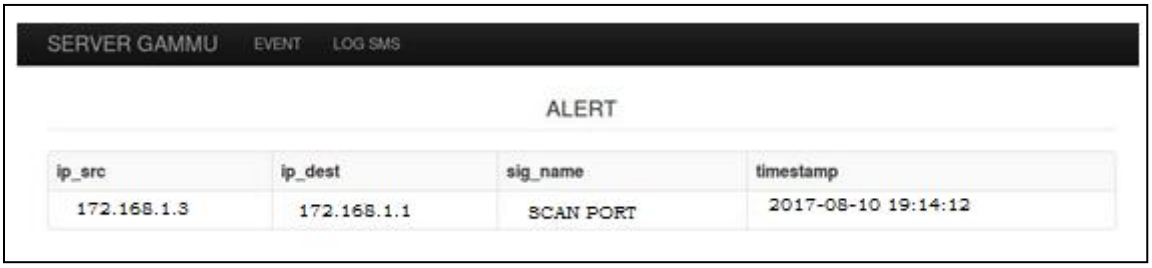
Pengujian dilakukan dengan menghubungkan dua komputer, dimana terdiri dari komputer *server* dan komputer *attacker*. Komputer *attacker* akan melakukan serangan dengan melakukan *scaning* menggunakan *Angry IP*. Pengujian dilakukan dengan tujuannya membuktikkan bahwa *administrator* dapat menerima notifikasi *alert* dari serangan yang dilakukan.




**Gambar 7.** *Scanning* dengan Angry IP

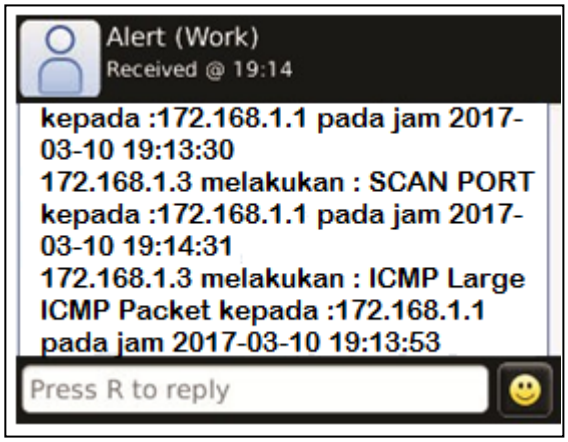
Berdasarkan gambar di atas terlihat komputer sedang melakukan *scaning* dan berhasil menemukan beberapa IP *address*. Kemudian, setelah melakukan serangan melalui komputer *attacker*,

IDS secara otomatis mengirimkan notifikasi ke *administrator* melalui sms berupa *alert* notifikasi terjadinya serangan. Hal ini dapat dilihat pada gambar berikut ini:




**Gambar 8.** *Alert* Notifikasi Terjadinya Serangan


**Gambar 9**. Log Sms




**Gambar 10.** Notifikasi *Alert* di Ponsel

Berdasarkan pengujian di atas menunjukkan bahwa apabila terjadi serangan yang berasal dari komputer *attacker* menuju komputer *server*. *Intrusion Detection System* pada saat berjalan akan memberikan notifikasi berupa *alert* kepada administrator secara otomatis melalui SMS.

### 3.2.7. Data Report

Data *report* yang diterima oleh seorang *administrator* melalui SMS *gateway* berupa data hasil *filtering* yang diidentifikasi sebagai aktifitas anomali. Dimana Panjang konten *report* yang disampaikan melalui SMS *gateway* akan dibatasi dengan jumlah maksimum karakter pada per satu SMS yaitu 160 karakter. Sedangkan, *source address*, *destination port* dan jumlah akses merupakan format laporan yang disampaikan dengan beberapa ketentuan yaitu akses dari *source address* yang

belum dilaporkan sebelumnya sehingga mencegah pengiriman laporan secara berulang. Dimana jumlah akses terdiri dari 5 *source address* berbeda dengan batas maksimum karakter seperti yang telah dijelaskan sebelumnya.

## 4. KESIMPULAN

Berdasarkan dengan hasil analisa dan pengujian yang telah dilakukan oleh penulis maka, dapat diambil kesimpulan sebagai berikut :

1. Bahwa dengan menerapkan *SMS Gateway* dan *Packet Filter* pada *Security Alert System* jaringan komputer sangat bermanfaat bagi *administrator*. Dimana saat *Intrusion Detection System* pada saat berjalan akan memberikan notifikasi berupa *alert* kepada *administrator* secara otomatis melalui SMS ketika komputer *attacker* melakukan serangan ke komputer *server*.
2. Sedangkan dengan melakukan peningkatan sikap *self protection* pada seorang *administrator* maka sistem peringatan dapat memberikan laporan peringatan secara berkala tanpa harus setiap saat melakukan pengecekan langsung terhadap sistem. Sehingga, diharapkan dapat mengurangi beban kerja *administrator*. Selain itu, sistem ini dapat diterapkan sebagai alternatif sistem keamanan tambahan pada sistem dengan pengamanan yang parsial.

## DAFTAR 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.

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

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

Sumantri, Iwan. 2017. *Tren Serangan Siber Nasional 2016 Dan Prediksi 2017.* [Online] Available at: *https://www.owasp.org/images/4/47/Iwan-OWASP-Cyber-Security-Trends-2017.pdf*. [Accessed 2 Januari 2018].

Singh, Sudeep.2017. *Alert (TA17-132A).* [Online] Available at: *https://www.owasp.org/images/4/47/Iwan-OWASP-Cyber-Security-Trends-2017.pdf https://idsirtii.or.id/peringatan.html*. [Accessed 2 Januari 2018].