Jurnal KomtekInfo , Vol.7 No.2 Tahun 2020
e-ISSN : 2502-8758 || p-ISSN : 2356-0010
DOI : 10.35134/komtekinfo.v7i2
Page : 159-170

Intruder Detection Monitoring System in Computer Networks Using Snort Based Sms Alert

(Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Berbasis Sms Alert **)**

Heri Yanto[1)], Febrihadi[2)]

[1, 2] Universitas Putra Indonesia YPTK Padang, Indonesia
E-mail: dimazheriyanto@gmail.com

Abstrak

Keamanan jaringan merupakan faktor yang penting dalam menjamin data. Keamanan yang terjamin dapat menghindari kerugian yang disebabkan oleh serangan yang terjadi di dalam jaringan. Administrator sangat berperan penting dalam menjaga keamanan data atau file, namun administrator tidak dapat setiap saat untuk mengawasi keamanan jaringan tersebut. Masalah ini dapat diatasi dengan menambahkan suatu sistem untuk deteksi lalu lintas data atau disebut dengan IDS. IDS akan dihubungkan dengan sms Alert sehingga administrator dapat menerima notifikasi gangguan pada jaringan. Dalam penelitian ini, peneliti melakukan analisis dan pengujian terhadap masalah yang timbul sehingga akan menghasilkan sebuah sistem yang mampu mendeteksi serangan atau gangguan pada jaringan secara cepat dan dapat memberikan peringatan kepada administrator jaringan, sehingga administrator dapat mengambil langkah antisipasi terhadap gangguan tersebut. Serangan dapat terdeteksi dari pola serangan yang berada pada rule IDS sehingga penyusup yang mencoba masuk akan terdeteksi dan sistem akan mengirimkan sms notisipasi kepada administrator.

Kata kunci: *Monitoring, Network, Snort, IDS, SMS Alert*

Abstract [Times New Roman 10 points]

Network security is an important factor in guaranteeing data. Guaranteed security can avoid losses caused by attacks that occur in the network. Administrators play an important role in maintaining data or file security, but administrators cannot at all times monitor the security of the network. This problem can be overcome by adding a system for data traffic detection or called IDS. IDS will be linked by SMS Alert so that administrators can receive notifications of interruptions on the network. In this study, researchers conduct analysis and testing of problems that arise so that it will produce a system that is able to detect attacks or disruptions on the network quickly and can provide warnings to network administrators, so that administrators can take steps to anticipate these disruptions. Attacks can be detected from the pattern of attacks that are in the IDS rule so that intruders who try to enter will be detected and the system will send an SMS notification to the administrator.

Keywords: Monitoring, Network, Snort, IDS, SMS Alert

1. Pendahuluan

Jaringan merupakan salah satu proses untuk mencegah dan memonitoring penggunaan jaringan yang tidak sah dari jaringan komputer. Tujuannya yaitu untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Salah satu software yang dapat digunakan untuk memonitoring jaringan adalah Snort. Snort adalah sebuah software open source ringkas yang sangat berguna untuk mengamati aktivitas dalam suatu jaringan komputer. (Suryayusra, Imam Solikin, & Maria Ulfa Desember 2017). Snort dapat digunakan sebagai suatu NIDS (Network Intrusion Detection System) yang ber-skala ringan (lightweight), dan software ini menggunakan sistem peraturan-peraturan (rules system) yang dapat dibuat sesuai kebutuhah untuk melakukan deteksi dan pencatatan (logging) terhadap berbagai macam serangan pada jaringan komputer. Selain itu Snort juga memiliki beberapa mode yang dapat digunakan untuk mengamankan suatu jaringan seperti sniffer mode, packet logger mode, NIDS mode dan Inline mode

Submitted : 18 April 2020 Accepted : 25 April 2020 Published : 26 April 2020
DOI : 10.35134/komtekinfo.v7i2.1392

(Justin 2016). Sistem keamanan firewall tidaklah cukup untuk meminimalkan terjadinya serangan terhadap suatu jaringan komputer. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator jaringan tidak bisa mengetahui dengan pasti apa yang sedang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk diatasi. Sekolah Menengah Kejuruan (SMK) Raja Mas merupakan salah satu sekolah yang berupaya meningkatkan mutu pendidikan di daerah dan menciptakan Sumber Daya Manusia (SDM) yang berkompeten dan potensial, terampil dan mempunyai keahlian (life skill) yang mampu bersaing didunia kerja/industri. Salah satu metode yang dipakai adalah meningkatkan mutu mengajar dan belajar dengan cara membangun sistem keamanan jaringan. Sistem keamanan jaringan merupakan suatu bentuk keamanan jaringan. Tujuan utamanya adalah untuk memberikan keamanan jaringan serta keamanan data sekolah dalam proses belajar dan mengajar agar tidak mudah diretas oleh pihak yang tidak bertanggung jawab. Oleh karena itu, untuk mengatasi permasalahan yang ada, perlu dibangun sebuah sistem keamanan jaringan pada SMK Raja Mas yang dapat digunakan untuk memonitoring aktivitas sebuah server secara realtime dengan menggunakan Snort dan mengirimkan notifikasi serangan yang terekam pada Snort melalui SMS (Short Message Service) Alert pada smartphone administrator jaringan.

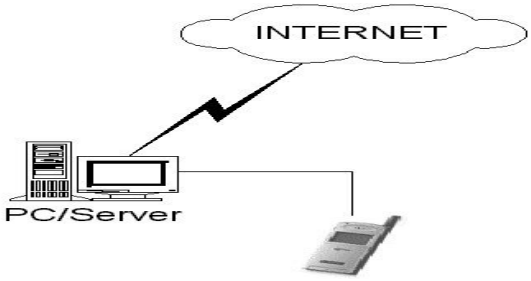
2. Tinjauan Literatur

Menurut (Asep Fauzi Mutaqin, 2016), jaringan komputer pada umumnya termasuk dalam pokok bahasan dalam bidang telekomunikasi, ilmu komputer, teknologi informasi, dan teknik komputer. Sifat dari jaringan komputer adalah memungkinkan adanya transfer data antar komputer atau perangkat yang terhubung di dalamnya. Contoh jaringan yang lazim digunakan adalah LAN (*local area network)*, WAN (*wide area network*), wireless LAN dan WAN (WLAN & WWAN). Sebuah jaringan komputer dihubungkan menggunakan berbagai medium, seperti kabel twisted pair, kabel tembaga, kabel koaksial, kabel serat optik, dan berbagai macam teknologi wireless. LAMP (Linux, Apache, MySQL, PHP) adalah sebuah *bundle software* untuk webserver yang terdiri dari Linux, Apache HTTPD *Server,* MySQL, serta PHP/Python/Perl. Paket yang terdapat pada LAMP dapat bervariasi, sehingga *compiler* PHP dapat juga diintegrasikan dengan Python atau Perl sesuai dengan kebutuhan (Asep Fauzi Mutaqin, 2016). Menurut (Asep Fauzi Mutaqin, 2016),Base adalah sebuah *interface web* untuk melakukan analisis dari intrusi yang snort telah deteksi pada jaringan. BASE ditulis oleh kevin johnson adalah program analisis sistem jaringan berbasis PHP yang mencari dan memproses database dari *security event* yang dihasilkan oleh berbagai program monitoring jaringan, *firewall,* atau sensor IDS. *Intrusion Detection System* (disingkat IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan) (Miftahul Jannah, Hustinawati dan Rangga Wildani, 2016). Pada dasarnya terdapat dua macam IDS, yaitu :

1. NIDS
NIDS akan melakukan pemantauan terhadap seluruh bagian pada jaringan dengan mengumpulkan paket-paket data yang terdapat pada jaringan tersebut serta melakukan analisa dan menentukan apakah paket-paket tersebut merupakan paket normal atau paket serangan.
2. HIDS (*Host Intrusion Detection System*)
HIDS hanya melakukan pemantauan pada perangkat komputer tertentu dalam jaringan. HIDS biasanya akan memantau kejadian seperti kesalahan *login* berkali-kali dan melakukan pengecekan pada *file* (Asep Fauzi Mutaqin, 2016).

Sedangkan untuk snort penulis menggunakan barnyard2. Barnyard2 adalah *tool open source* sebagai penerjemah *alert unified* dan log dari snort. Barnyard dapat meningkatkan efisiensi snort dengan cara mengurangi beban pada sensor deteksi. Barnyard2 bekerja dengan membaca *snort's unified logging output files* dan memasukkannya ke dalam database. Jika database tidak tersedia maka barnyard2 akan memasukkan semua data ketika database tersedia kembali sehingga tidak ada *alert* atau *log* yang hilang

(Sofana, Iwan. 2008). Sms alert digunakan untuk menggantikan sms *gateway*, walaupun fungsi dan caranya hamper sama namun sms alert hanya memberikan alert atau semacam alarm untuk mendeteksi ketika terjadi sebuah serangan.



Gambar 1: SMS *Gateway*

Software yang akan digunakan untuk koneksi ponsel ke komputer dalam penelitian ini adalah Gammu (GNU *All Mobile Management Utilities*). Menurut Hermaduanti (2009) Gammu merupakan *software* yang bersifat *open source* yang digunakan sebagai *tool* untuk mengembangkan aplikasi SMS *Gateway*, cukup mudah diimplementasikan, dan tidak berbayar. Kelebihan Gammu dari *tool* SMS *gateway* lainnya adalah:

a. Gammu dapat dijalankan di sistem operasi Linux maupun Windows.
b. Banyak *device* yang kompatibel di Gammu.
c. Gammu menggunakan *database* MySQL untuk menyimpan SMS yang ada pada kotak masuk (*inbox*) maupun untuk mengirim pesan, sehingga dapat dibuat *interface* yang berbasis web maupun desktop.
d. Baik kabel data USB maupun serial, semuanya kompatibel di Gammu.

Konfigurasi :

1. gammurc

File gammurc digunakan untuk konfigurasi port yang digunakan media koneksi untuk terhubung ke komputer. Selain itu, file gammurc juga digunakan untuk mendefinisikan tipe koneksi yang digunakan oleh media koneksi.

2. smsdrc

File smsdrc digunakan untuk konfigurasi *database* yang akan digunakan oleh aplikasi gammu. Nama *database*-nya adalah "smsd" (Mohammad Yasir, 2010).

3. Metodologi

Makna penelitian secara sederhana adalah bagaimana mengetahui sesuatu yang dilakukan melalui cara tertentu dengan prosedur yang sistematis. Maka penulis membentuk kerangka penelitian sebagai berikut :

A.Tahapan Penelitian

Tahapan penelitian ini menjelaskan langkah-langkah dalam melakukan pencatatan data serta mengumpulkan beberapa laporan yang di perlukan untuk dapat dijadikan pedoman dalam pembuatan penelitian ini, yaitu:

1. Survei Penelitian
   Survei Melakukan pendekatan terhadap objek penelitian. Tujuan dari tahap ini adalah untuk mengetahui permasalahan yang terjadi secara tepat, sehingga diharapkan penelitian dapat memberikan solusi yang paling optimal terhadap pemecahan permasalahan tersebut, melakukan Study Literatur yaitu mencari jurnal dan buku yang berkaitan dengan implementasi dari Snort.

2. Pengumpulan Data
   Dalam melakukan proses pengumpulan data, penulis terlebihdahulu melakukan studi kepustakaan sebagai rujukan dalam pengumpulan data, kemudian penulis melakukan pengumpulan data dilapangan dengan melakukan wawancara.

3. Analisa Data

Untuk melakukan penelitian, penulis melakukan analisa terhadap data-data yang telah dikumpulkan serta menganalisa sistem yang akan dijalankan sebagai solusi dari perumusan masalah yang didapat.

a. Analisa Data

Pada tahap ini dilakukan pengumpulan data yang nantinya akan diolah seperti data *flowchart*, *system* topologi jaringan, dan data lainnya yang akan melengkapi kriteria pembangunan sistem.

b. Analisa Proses

Metode yang di gunakan dalam penelitian ini ada 1 metode yaitu *snort.* Dimana metode snort digunakan untuk komunikasi dua computer menggunakan *port* pada arsitektur jaringan SMK Raja Mas Karena dengan menggunakan metode *snort* kita dapat mengontrol port yang terbuka dan mengamankan hak akses dari yang *user* tidak memiliki akses tertentu.

c. Analisa Sistem

Analisis sistem merupakan dasar dalam merencanakan dan merancang sistem yang akan diterapkan. Analisa sistem dilakukan untuk mengetahui dan mengembangkan sistem yang sedang berjalan. Sistem ini memerlukan beberapa *client* yang akan dihubungkan ke jaringan server.

4. Perancangan

Perancangan dilakukan setelah adanya analisa dari sebuah sistem. Perancangan sistem adalah suatu langkah untuk memenuhi kebutuhan pemakaian *user.* Dalam hal ini memberikan gambaran gamblang dalam pembuatan program komputer hingga dapat dipahami para *user* nantinya. Adapun perancangan yang akan dilakukan dalam penelitian adalah sebagai berikut:

a. Perancangan Model

Perancangan yang dilakukan yaitu dengan menggunakan UML (*Unified Modelling Languge)* sebagai alat untuk menjalankan suatu jalan dari analisa yang dibuat penulis. UML yang akan dibuat penulis yaitu sebagai berikut:

1. Use Case Diagram
2. Class Diagram
3. Sequence Diagram
4. Collaboration Diagram
5. Activity Diagram

5. Implementasi

Pada implementasi ini peneliti akan membahas mengenai *system monitoring* keamanan jaringan yang akan di implementasikan, penelitian ini akan menggunakan *sms alert* dan *snort* sebagai system keamanan jaringan dan pemberitahuan ke administrator.

6. Pengujian

Pengujian *system* keamanan jaringan merupakan tahap akhir dalam melakukan *testing*, guna untuk mengetahui kesalahan dalam penerepan.Pengujian dilakukan dengan melihat apakah *system* tersebut sudah berjalan dengan benar dan sesuai dengan perancangan yang dilakukan.

1.Pengujian keamanan dilakukan oleh *administrator* agar kemanan jaringan yang dirancang dapat diketahui kekurangan dan kesesuaian dengan perintah yang akan dijalankan.
2.Untuk mengetahui bug sistem yang dijalankan dengan menggunakan aplikasi yang bersifat *open source* yaitu Gammu.

7. Hasil

Hasil dari penelitian ini akan menghasilkan sebuah system monitoring keamanan jaringan pada *system* operasi, yang dapat mendeteksi secara cepat dan mudah adanya bentuk serangan ke *admininistrator* dengan cara pemberitahuan melalui *sms alert* ke administrator menggunakan snort dan gammu.

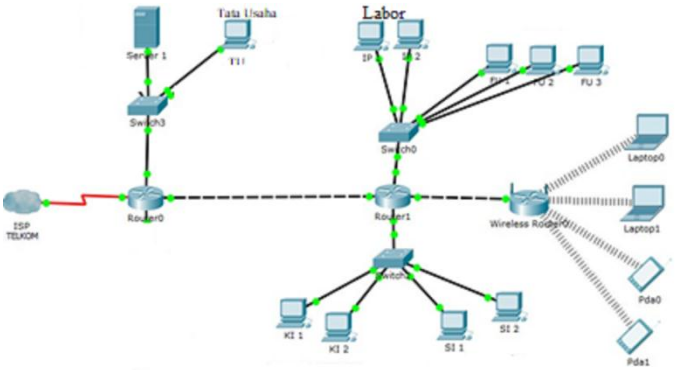
4. Hasil dan Diskusi

4.1 Analisa Data

Tahap analisa data merupakan tahap yang paling penting dalam pengembangan sebuah sistem, karena pada tahap inilah nanti akan dilakukan evaluasi kinerja, identifikasi terhadap masalah yang ada, rancangan sistem dan langkah-langkah yang dibutuhkan untuk perancangan yang diinginkan sampai pada analisis yang diharapkan.

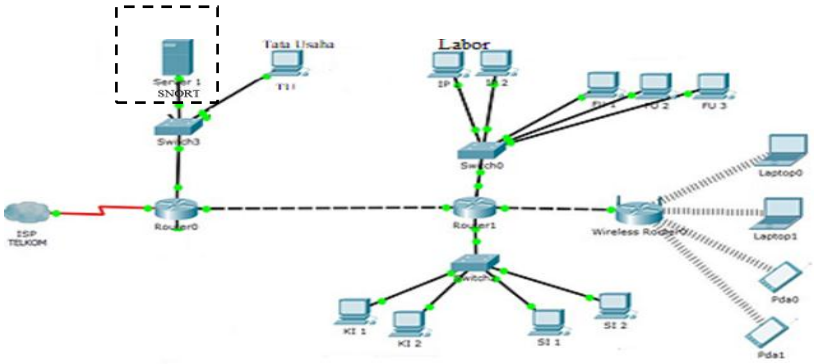
4.1.1 Perancangan Topologi Jaringan Usulan

Berdasarkan data topologi yang didapat peniliti tidak akan merubah bentuk dari topologi jaringan pada SMK. Pada perancangan topologi jaringan usulan ini hanya akan menambahkan *system* keamanan jaringan pada server SMK. Dibawah ini merupakan bentuk dari skema topologi jaringan awal sebelum diberikan system keamananan server pada perancangan topologi.



Gambar 3: Topologi Jaringan Usulan Awal

Pada gambar diatas topologi jaringan usulan awal yang digunakan pada SMK tersebut yang sebelumnya belum menggunakan keamanan jaringan server sehingga client yang tidak memiliki akses tertentu dapat melakukan serangan terhadap server sehingga tidak aman pada system jaringan server tersebut maka peniliti melakukan perancangan topologi pada arsitektur jaringan server pada SMK dengan menambahkan *system* keamanan jaringan *server* yaitu dengan menggunakan SNORT. seperti gambar dibawah ini :

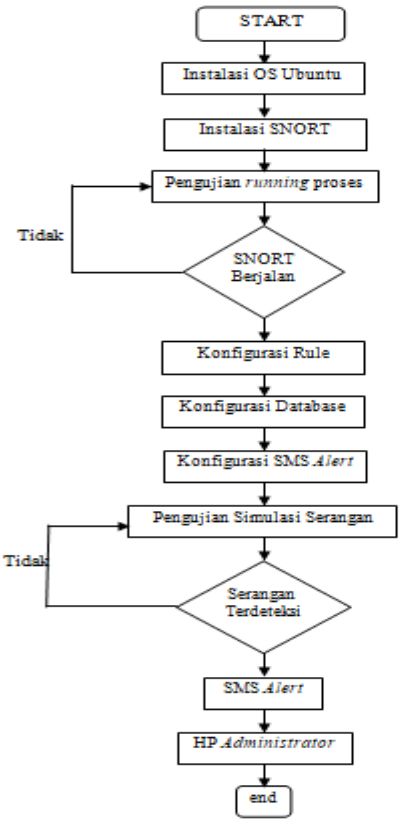


Gambar 4: Topoligi Jaringan Usulan

Berdasarkan gambar 4.4 diatas menjelaskan bahwa *server* diberikan keamanan *SNORT* yang dapat mendeteksi setiap serangan pada server dan kemudian aka nada pemberitahuan pada Hp *administrator* sehingga penyerang langsung dapat terdeteksi.

4.1.2 Flowchart Proses Sistem Keamanan

Pada tahap ini akan menjelaskan suatu bagan dengansimbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya dalam suatu program. Flowchart menunjukkan alur kerja atau apa yang sedang dikerjakan didalam sistem secara keseluruhan dan menjelaskan urutan dari prosedur-prosedur yang ada di dalam sistem. Dalam tahap ini sistem monitotring keamana memiliki flowchart pada gambar dibawah ini:



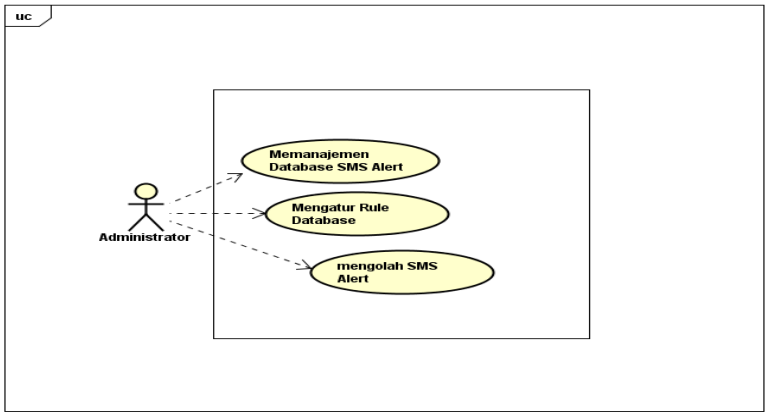
Gambar 5: Flowchart Perencanaan Sistem Keamanan

4.2 Perancangan Model

Aplikasi ini dirancang menggunakan alat bantu berupa UML (*Unified Modelling Language*) agar mempermudah memindahkan konsep sistem yang dirancang ke dalam bentuk program, dimana perancangannya digambarkan dalam bentuk diagram-diagram berikut :

4.2.1 Use Case diagram

Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem, yang ditekankan adalah "apa" yang diperbuat sistem, dan bukan "bagaimana". Sebuah *use case* merepresentasikan sebuah interaksi antara aktor dengan sistem. *Use Case* Diagram darisistem yang dirancang dapat digambarkan seperti pada Gambar berikut :

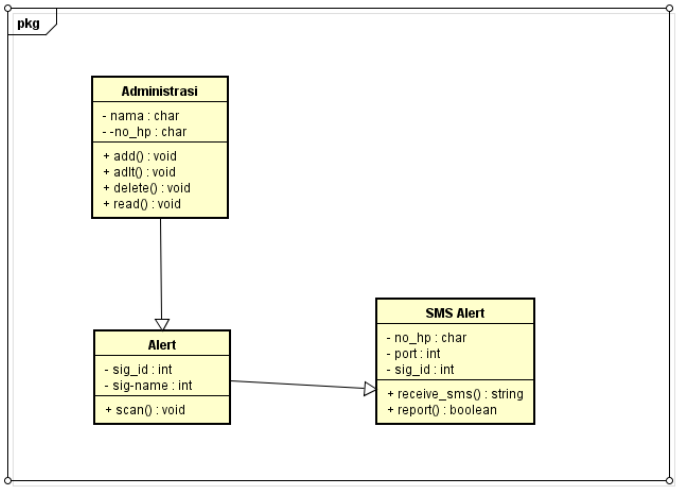


Gambar 6: *Use Case* Diagram

Dalam gambar diatas menunjukkan beberapa fitur-fitur yang dapat dijalankan oleh *admininistrator*. Pada sistem ini *administrator* memiliki akses untuk melihat dan mengatur atau memanajemen database SMS alert yang telah dikirim dari mesi pendeteksi SNORT melalui short sms, serta dapat mengatur rule snort alert yang akan dideteksi oleh IDS. Dan juga *administrator* dapat mengolah pesan singkat yang dikirm secara otomatis jika ada serangan atau penyusup dalam jaringan ke Hp *Administrator*.

4.2.2 Class Diagram

Class Diagram adalah sebuah spesifikasi yang jika diinstansi akan menghasilkan sebuah objek dan merupakan inti dari pengembangan dan desain berorientasi objek. *Class diagram* dari Analisa dan perancangan dari sistem database dan sms alert dari sistem monitoring keamanan jaringan dapat digambarkan seperti pada dibawah in.



Gambar 7: Class Diagram

Pada gambar *class diagram* diatas dapat di ketahui bahwasanya *alert* yang telah peneliti buat memiliki tiga tabel *class* yang saling terintegrasi. Tabel diatas meliputi *Admininistrator*, *alert* dan *SMS Alert. Class*

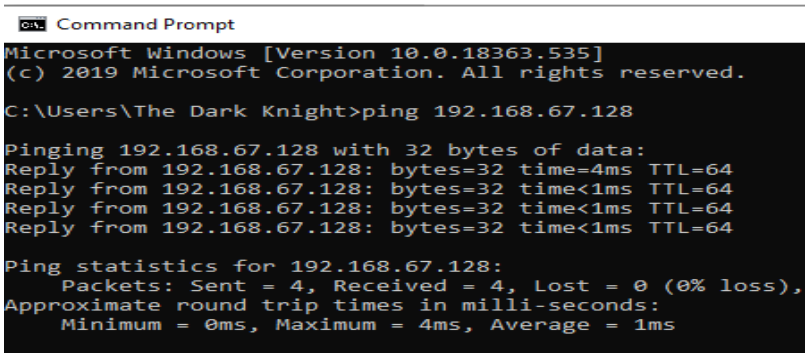
Diagram diatas saling terintegrasi dengan ditunjukkan dengan simbol anak panah yang menuju tabel yang terintegrasi.

4.3 Implementasi dan Pengujian

Pada tahap ini dilakukan pengujian terhadap sistem keamanan seperti Ping Attack dan Smurf DDOS attack.

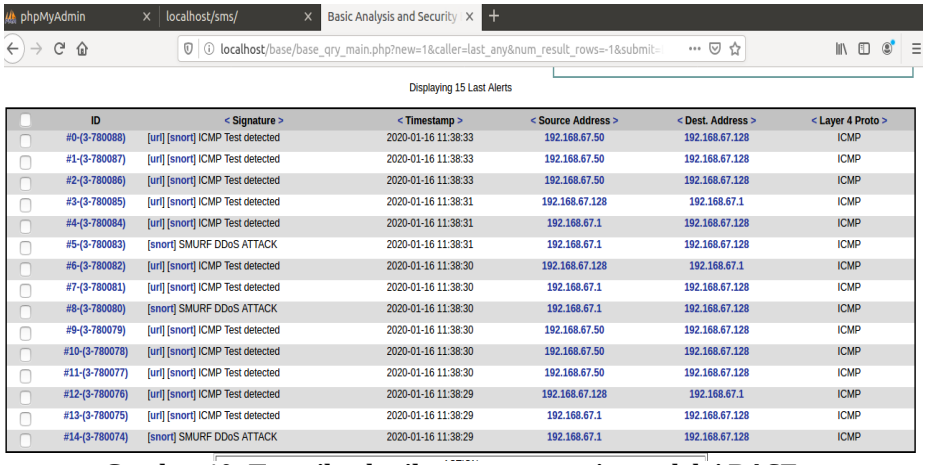
4.3.1 Pengujian menggunakan Ping Attack (ICMP Traffic)

Pengujian dilakukan dengan cara menyerang server snort dengan mengunakan command prompt. Proses penyerangan yang dilakukan yaitu dengan mengirim ping oleh komputer client ke server snort. Berikut tampilan proses penyerangan yang dijelaskan pada gambar dibawah ini :



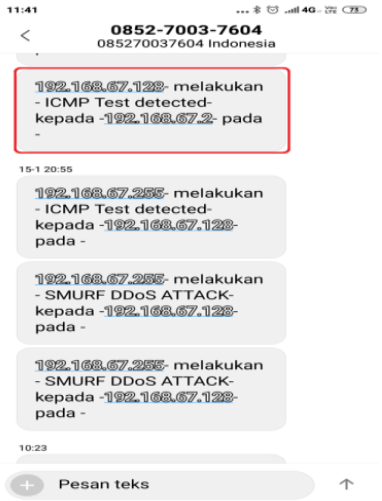
Gambar 9: Tampilan hasil Pengujian Ping Attack (ICMP Traffic)

Dari hasil pengujian dengan mengirimkan ping ke komputer server maka snort akan mendeteksi sebuah serangan dan menyimpannya ke dalam database. Untuk melihat hasil log serangan dalam bentuk Web GUI (Graphical User Interface) digunakan BASE (Basic Analysis and Security Engine). Berikut tampilan dari BASE yang di jelaskan pada dibawah in:



Gambar 10: Tampilan hasil penyerangan ping melalui BASE

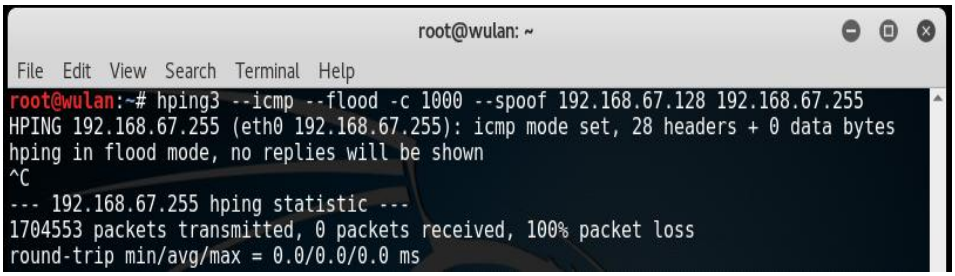
Setelah dideteksi oleh mesin snort dan masuk ke dalam database maka administrator akan menerima sms alert dari server melalui sms gateway. Berikut alert yang akan di tampilkan pada handphone administrator ketika terjadi serangan yang akan di jelaskan pada gambar dibawah ini:



Gambar 11: Tampilan SMS Alert Ping Attack

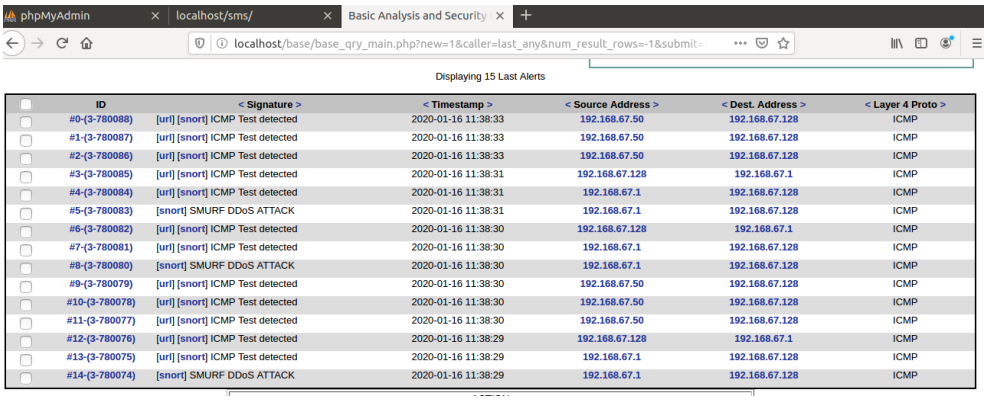
4.3.2 Pengujian menggunakan SMURF DDoS *Attack*

Pengujian dilakukan dengan cara melakukan perintah hping3 –icmp –flood –c 1000 –spoot 192.168.67.128 192.168.67.25 melalui komputer client ke server snort. Berikut tampilan proses pengujian yang dilakukan dari komputer client seperti yang dijelaskan pada gambar dibawah ini :



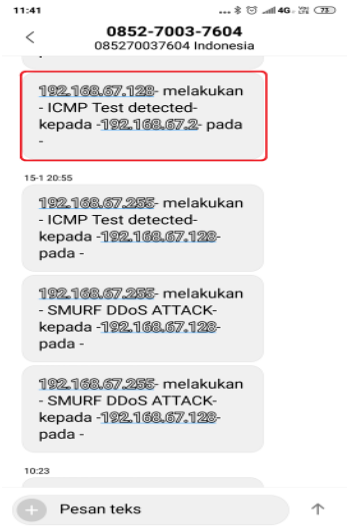
Gambar 12: Tampilan oleh Client

Dari hasil pengujian dengan mengirimkan ping SMurf ke komputer server maka snort akan mendeteksi sebuah serangan dan menyimpannya ke dalam database. Untuk melihat hasil log serangan dalam bentuk Web GUI (Graphical User Interface) digunakan BASE (Basic Analysis and Security Engine). Berikut tampilan dari BASE yang di jelaskan pada gambar dibawah ini:



Gambar 13: Tampilan hasil penyerangan SMURTF DDoS melalui BASE

Setelah dideteksi oleh mesin snort dan masuk ke dalam database maka administrator akan menerima sms alert dari server melalui sms gateway. Berikut alert yang akan di tampilkan pada handphone administrator ketika terjadi serangan yang akan di jelaskan pada gambar dibawah ini:



Gambar 14: Tampilan SMS Alert SMURF DDoS.

5. Kesimpulan

Dari penulisan penelitian ini mulai dari tahapan analisa permasalahan yang ada hingga pengujian sistem yang baru dirancang maka dapat diambil beberapa kesimpulan, yaitu :

a. Sistem monitoring keamanan jaringan yang dibuat dapat mampu mendeteksi penyusup dengan pemberitahuan SMS *Alert* ke *handphone administrator*.
b. Dengan menggunakan sistem monitoring keamanan jaringan yang telah dirancang, tingkat keamanan lebih terjamin untuk menyimpan file atau data-data penting.
c. Dengan Sistem monitoring keamanan jaringan yang dibangun ini dapat menjadi solusi mudah untuk mendeteksi bentuk serangan yang ada.

Referensi

[1] Imama, Chusnul, and Aries Dwi Indriyanti. 2013. "Penerapan Case Based Reasoning Dengan Algoritma Nearest Neighbor Untuk Analisis Pemberian Kredit di Lembaga Pembiayaan." *Jurnal Manajemen Informatika* 2.01
[2] Kusrini, “Aplikasi Sistem Pakar, and Aplikasi Sistem Pendukung Keputusan. 2007."Andi Offset."
[3] Kusrini, 2007. *Konsep dan Aplikasi Sistem Pendukung* KeputusanYogyakarta: Andi. Larry, Roy, “Jurus kilat mahir *HTML & CSS [secara otodidak]*.” Jakarta Timur: Dunia Komputer.
[4] Padilah, Fitri Pauziah, Gunawan Abdillah, and Faiza Renaldi. 2016."Rekomendasi Penanganan Anak Berkebutuhan Khusus Pada Sekolah Luar Biasa Negeri Citeureup Menggunakan Case Based Reasoning Dan Nearest Neighbors.2013." *Prosiding SNST Fakultas Teknik* 1.
[5] Rosa, Ariani Sukamto, and Muhammad Shalahuddin.2013. "Rekayasa perangkat lunak terstruktur dan berorientasi objek." *Bandung: Informatika*.
[6] Sumarlin, Sumarlin. 2015."Implementasi Algoritma K-Nearest Neighbor Sebagai Pendukung Keputusan Klasifikasi Penerima Beasiswa PPA dan BBM." *JSINBIS (Jurnal Sistem Informasi Bisnis)* 5.1.

[7] Tim, E. M. S. 2014. "Teori dan Praktik PHP-MySQL untuk Pemula." *Jakarta: PT Elex Media Komputindo*.

[8] Sibero, Alexander FK. "Web Programming Power Pack." (2013).

[9] Abdul Aziz, dan Arry Budi Kurnia 2015. Monitoring Seragan Pada Jaringan Komputer Menggunakan Snort Berbasis SMS GATEWAY. POLITEKNOLOGI VOL. 14. No.2 MEI 2015.

[10] Asep Fauzi Mutaqin 2016. Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS *Alert* dengan Snort. Jurnal Sistem dan Teknologi Informasi (JUSTIN) Vol. 1, No. 1, (2016).

[11] Puji Hartono. 2005, Sistem Pencegahan Penyusupan pada Jaringan berbasis *Snort* IDS dan IPTables Firewall

[12] Suryayusra, Imam Solikin, Maria Ulfa. 2017. Penerapan Sistem Keamanan Jaringan Smk Negeri 1 Indralaya Utara Dengan Mikrotik. Jurnal Ilmiah MATRIK Vol.19 No.3, Desember 2017:197-206.

[13] Triandini, Rizki, 2016, Implementasi Intrusion Detection System Menggunakan SNORT, Barnyard2 dan BASE Pada Sistem Operasi Linux. Bandung : 2016.

[14] Yasir, Mohamad. 2010. Membangun Software Monitoring Jaringan Dengan Sms Alert.

[15] Sofana, iwan, 2018. Membangun Jaringan Komputer.

[16] yanto, heri. (2018). SISTEM PENDUKUNG KEPUTUSAN UNTUK SELEKSI USULAN PENGAJUAN SERTIFIKASI GURU MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBOR BERBASIS WEB. *Jurnal KomtekInfo*, *5*(2), 42-50