INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN RASPBERRY PI 3 BERBASIS SNORT STUDI KASUS: STMIK STIKOM INDONESIA

[1]I Kadek Susila Satwika, [2]I Wayan Sudiarsa, [3]Made Hanindia Prami Swari
[1,2]STMIK STIKOM Indonesia, [3]UPN "Veteran" Jawa Timur
Email: [1]susila.satwika@stiki-indonesia.ac.id, [2]sudiarsa@stiki-indonesia.ac.id,
[3]madehanindia.fik@upnjatim.ac.id

Abstrak. *Keamanan jaringan komputer dan Server menjadi salah satu hal yang harus diutamakan. Pentingnya menjaga keamanan jaringan komputer membantu dalam menjaga informasi, data-data, serta menjaga peralatan dapat berfungsi dengan baik dan memberikan akses hanya untuk pengguna yang sah. Penelitian ini, membangun IDS (Intrusion Detection System) pada jaringan dan Server menggunakan Raspberry Pi berbasis Snort yang dapat memonitoring aktivitas Server ketika terjadi sebuah serangan dengan mengirimkan notifikasi melalui SMS (Short Message Service) ke handphone administrator jaringan secara realtime. Sistem ini diujikan dengan tiga jenis serangan yaitu PING Attack, Port Scanning, dan DOS/DDoS Attack. Dalam setiap serangan, Raspberry Pi dipantau dalam hal Penggunaan CPU, Memory (RAM), dan Beban Jaringan. Pada saat terjadi serangan terhadap Komputer Server, Snort dapat menampilkan dan menghasilkan alert yang akan disimpan pada Log Snort, setelah itu data serangan ditampilkan pada website BASE (Basic Analysis and Security Engine) sekaligus dikirimkan ke handphone administrator jaringan melalui SMS Gateway. Dari hasil pengujian masing-masing serangan, pada saaat terjadi serangan, penggunaan sumber daya pada Raspberry Pi 3 Model B untuk serangan PING Attack, Port Scanning, dan DOS/DDoS Attack meningkat dalam hal penggunaan CPU, Memory (RAM), dan Beban Jaringan.*

Kata Kunci: Jaringan Komputer, Server, Raspberry Pi, IDS, SNORT.

Keamanan jaringan komputer dan *Server* menjadi salah satu hal yang harus diutamakan, terlebih bagi seorang administrator jaringan untuk mencegah dan mengidentifikasi pengguna yang tidak sah dari jaringan komputer. Tujuan dari keamanan jaringan komputer adalah untuk menjaga stabilitas, integritas, dan validitas data. Pentingnya menjaga keamanan jaringan komputer membantu dalam menjaga informasi, data-data, serta menjaga peralatan dapat berfungsi dengan baik dan memberikan akses hanya untuk pengguna yang sah. Dengan menjaga keamanan jaringan komputer dapat menghindari resiko terjadinya penyusupan atau ancaman yang mengakibatkan kerusakan pada jaringan komputer. Dampak dari tidak menjaga keamanan jaringan komputer dapat mengakibatkan terjadinya interuption, interception, modification, dan fabrication dalam jaringan komputer. Salah satu cara untuk meningkatkan keamanan jaringan komputer adalah dengan mengimplementasikan IDS. IDS adalah sebuah sistem yang dapat mendeteksi adanya pengguna tak ter-autorisasi pada sebuah sistem jaringan [1]. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan, maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan.

STMIK STIKOM Indonesia merupakan salah satu perguruan tinggi di Bali yang memiliki infrastruktur jaringan komputer dan *Server*. Terdapat permasalahan yaitu selama ini tidak ada sistem monitoring keamanan pada jaringan komputer dan *Server*. Ketika terjadi sebuah serangan terhadap *Server* yang berada di STMIK STIKOM Indonesia, administrator jaringan tidak mengetahui adanya sebuah serangan, sumber serangan, dan tujuan dari serangan yang dilakukan oleh seseorang yang bisa mengakibatkan kerusakan pada *Server*. Keamanan jaringan dan *Server* di STMIK STIKOM Indonesia masih menggunakan security bawaan MikroTik dan sistem *firewall*. Untuk itu administrator jaringan memerlukan sebuah sistem yang dapat mendeteksi adanya sebuah serangan yang dapat mengakibatkan kerusakan dan memantau keamanan pada *Server* yang berada di STMIK STIKOM Indonesia.

Permasalahan di atas dapat diatasi dengan sistem IDS (*Intrusion Detection System*). Dari penelitian terdahulu yang telah dilakukan [2][3], dapat disimpulkan bahwa dengan menggunakan sistem IDS dapat mendeteksi aktivitas yang mencurigakan dalam jaringan komputer. Salah satu aplikasi berbasis IDS yang dapat digunakan dalam pengamanan jaringan adalah Snort. Snort merupakan

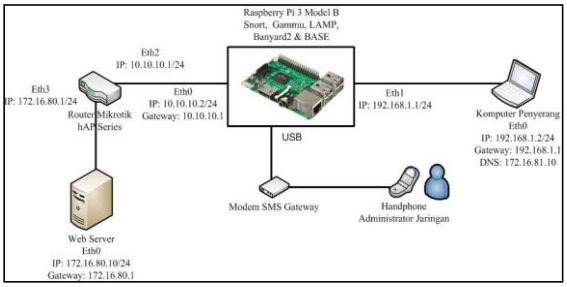
software open-source yang bebas digunakan, dimodifikasi sesuai dengan kebutuhan dan dapat mendeteksi suatu usaha penyusupan pada suatu jaringan komputer. Penelitian diatas menunjukkan bahwa IDS menggunakan Snort sudah banyak diterapkan oleh berbagai pihak, dimana pada penelitiannya, sistem IDS digunakan pada komputer stand alone. Sedangkan pada penelitian ini, akan menggunakan Raspbery Pi 3 Model B sebagai perangkat IDS berbasis aplikasi Snort. Raspberry Pi adalah komputer berukuran kecil yang menggabungkan komponen dan fungsi-fungsi komputer serta elektronika kedalam satu chip (*Embedded System*) yang dapat melakukan banyak hal [4]. Saat ini Raspberry Pi sudah banyak digunakan oleh masyarakat dunia, terbukti dengan banyaknya implementasi Raspberry Pi yang mendukung era *Internet Of Thing* ataupun *Internet Of Everything* [5]. Beberapa penelitian yang menggunakan Raspberry Pi sebagai *Server* [6][7] menguatkan penelitian ini untuk menggunakan Raspberry Pi sebagai *server* pada sistem IDS berbasis aplikasi Snort.

Pada penelitian ini Sistem IDS menggunakan Raspberry Pi 3 Model B berbasis Snort yang akan diujikan dengan tiga buah jenis serangan yaitu PING *Attack*, *Port Scanning* dan DOS/DDoS *Attack*. Dalam setiap serangan yang dilakukan, Raspberry Pi 3 Model B akan dipantau dalam hal penggunaan CPU, *Memory* (RAM) dan penggunaan Beban Jaringan. Pemberitahuan jika terjadi serangan atau terdeteksi aktivitas yang tidak wajar pada jaringan komputer, akan ditampilkan melalui *website* BASE dan mengirimkan notifikasi melalui SMS (*Short Message Service*) ke handphone administrator jaringan secara *realtime*. Dari hasil pengujian yang telah dilakukan didapatkan hasil bahwa sistem IDS dapat berjalan dengan lancar dan berhasil memberikan notifikasi kepada administrator jaringan.

I. Metodologi

Untuk lebih jelasnya tentang sistem pendeteksi intrusi pada jaringan dan *Server* menggunakan *Raspberry Pi* berbasis aplikasi *Snort* ini dapat dilihat pada gambar 1.

Pada Gambar 1, tentang topologi sistem pendeteksi intrusi pada jaringan dan *Server* menggunakan *Raspberry Pi* berbasis aplikasi *Snort*, terlihat *Raspberry Pi 3 Model B* dan Komputer Penyerang terhubung dengan media kabel. Pada *Raspberry Pi 3 Model B* terpasang modem SMS *Gateway* dengan media USB. Modem SMS *Gateway* ini akan mengirimkan SMS *alert* ke *handphone* administrator jaringan. Topologi jaringan ini menggunakan skema IP *address* kelas C dengan *network* 172.16.80.0/24, 10.10.10.0/24 dan 192.168.1.0/24. *Raspberry Pi 3 Model B* memiliki 2 (dua) IP *address* yaitu pada *Eth0* IP *address*nya 10.10.10.2/24 dan pada *Eth1* IP *address*nya 192.168.1.1/24, *Router MikroTik* memiliki 2 (dua) IP *address* yaitu pada *Eth3* IP *address*nya 172.16.80.1/24 dan pada *Eth2* IP *address*nya 10.10.10.1/24, Komputer *Server* memiliki IP *address* 172.16.80.10/24, Sedangkan Komputer Penyerang memiliki IP *address* 192.168.1.2/24 dengan *Gateway* 192.168.1.1 dan DNS menggunakan IP *address* 172.16.80.10 Komputer *Server*.



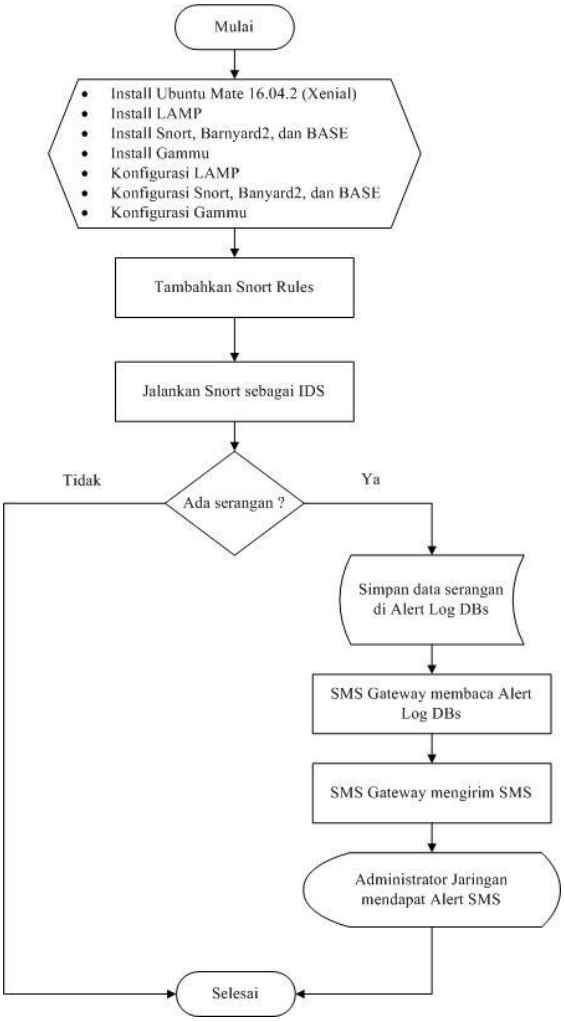
Gambar 1. Topologi Jaringan Dan *Server* Pada Sistem IDS Menggunakan *Raspberry Pi* Berbasis *Snort*

Pengujian dilakukan dengan cara melakukan berbagai macam serangan terhadap Komputer *Server* dan Raspberry Pi 3 Model B yang berisi sistem IDS (*Intrusion Detection System*) berbasis aplikasi Snort akan mendeteksi berbagai macam serangan yang terjadi pada Komputer *Server* tersebut. Yang bertindak sebagai penyerang dalam skenario ini adalah Komputer Penyerang yang menggunakan media kabel UTP sebagai penghubung antara Komputer Penyerang dengan Raspberry Pi 3 Model B. Serangan yang akan diujikan pada penelitian ini adalah PING *Attack*, Port Scanning, dan DOS/DDoS *Attack*. Pada setiap pengujian serangan, parameter Raspberry Pi 3 Model B yang berisi sistem IDS (*Intrusion Detection System*) berbasis aplikasi Snort yang berupa CPU, Memory (RAM) dan Beban Jaringan akan di monitoring untuk perbandingan sebelum terjadinya serangan dan pada saat terjadinya serangan.

Hal yang pertama dilakukan adalah menginstall sistem operasi Ubuntu Mate

16.04.2 (Xenial) pada Raspberry Pi 3 Model B. Apabila sistem operasi Ubuntu Mate 16.04.2 (Xenial) sudah terinstall, selanjutnya menginstall dan konfigurasi LAMP (Linux Apache MySQL PHP) , setelah itu menginstall dan konfigurasi aplikasi Barnyard2 yang berfungsi sebagai penerjemah output dari Snort menjadi database MySQL, setelah itu menginstall dan konfigurasi BASE (Basic Analysis and Security Engine) sebagai tampilan website untuk memonitoring terjadinya serangan terhadap Komputer *Server*, selanjutnya menginstall dan konfigurasi software Gammu untuk menjembatani modem pada SMS Gateway dengan Raspberry Pi 3 Model B. Setelah itu dilanjutkan dengan menginstall aplikasi Snort 2.9.11.1. Snort memerlukan beberapa konfigurasi dan Rules untuk bekerja, untuk itu konfigurasikan dan tambahkan Rules yang tepat untuk serangan PING *Attack*, Port Scanning, dan DOS/DDoS *Attack*. Perlu diketahui, Snort memiliki tiga mode pengoperasia, yaitu Snifing Mode, Packet Logger Mode, dan NIDS (Network Intrusion Detection System) Mode. Setelah Snort berhasil dikonfigurasi dan Rules sudah ditambahkan kemudian jalankan Snort menjadi NIDS (*Network Intrusion Detection System*) Mode.

Pada tahap ini, Snort sudah berjalan dan memindai semua paket yang masuk maupun keluar. Apabila Snort menangkap adanya aktivitas yang sesuai dengan Rules yang ada atau dengan kata lain adanya upaya serangan terhadap Komputer *Server* tersebut, maka Raspberry Pi 3 Model B yang berisi sistem IDS (Intrusion Detection System) berbasis aplikasi Snort akan mencatat paket tersebut dan menyimpannya di Alert Log Database. Semua data yang ada di Alert Log Database ini dikirimkan ke handphone administrator jaringan sebagai alert, untuk itu Gammu akan membaca isi dari Alert Log Database dan langsung mengirimkan alert berupa pesan serangan melalui modem SMS Gateway ke nomor handphone administrator jaringan yang telah ditentukan. Administrator jaringan akan segera menerima pesan serangan yang terjadi dan dapat mengambil tindakan lebih lanjut terhadap Komputer *Server* yang berada di STMIK STIKOM Indonesia.



Gambar 2. *Flowchart* IDS Pada *Raspberry Pi*

II. Hasil dan Pembahasan

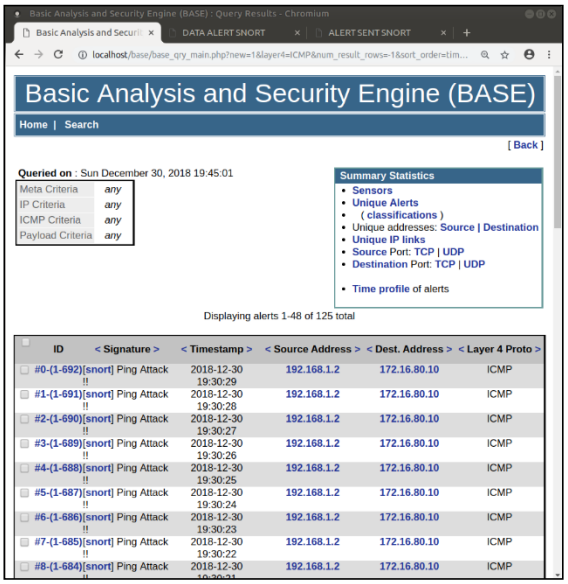
Pengujian akan dilakukan dengan 3 tahap yaitu pertama akan dilakukan pengujian mengenai serangan *ping attack*, selanjutnya akan dilakukan pengujian serangan Port Scanning, dan yang terakhir adalah pengujian serangan DOS/DDoS *Attack*.

PING *Attack*

Pengujian pertama adalah melakukan PING *Attack* ke *server* tujuan. Komputer penyerang melakukan PING terhadap Komputer *Server* dengan besar paket yang dikirimkan adalah 30500 bytes secara terus menerus**.**

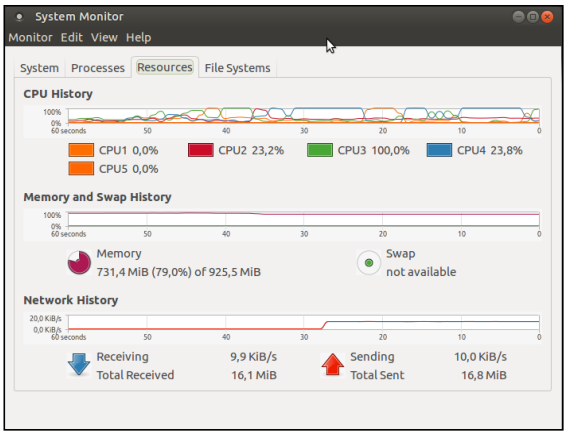
Pada Gambar 3, terlihat pada tabel Signature berisi Ping *Attack* !! ini adalah nama dari sebuah serangan yang dilakukan, pada Timestamp berisi 2018-12-30 19:30:29 ini adalah waktu serangan yang dilakukan, pada Source Address berisi 192.168.1.2 ini

merupakan IP Address yang dimiliki oleh host yang melakukan serangan terhadap Komputer *Server*, pada Dest. Address berisi 172.16.80.10 ini merupakan IP Address yang diserang, dan yang terakhir pada Layer 4 Proto berisi ICMP ini merupakan protokol apa yang digunakan untuk melakukan serang tersebut.



Gambar 3. *Flowchart* IDS Pada *Raspberry Pi*

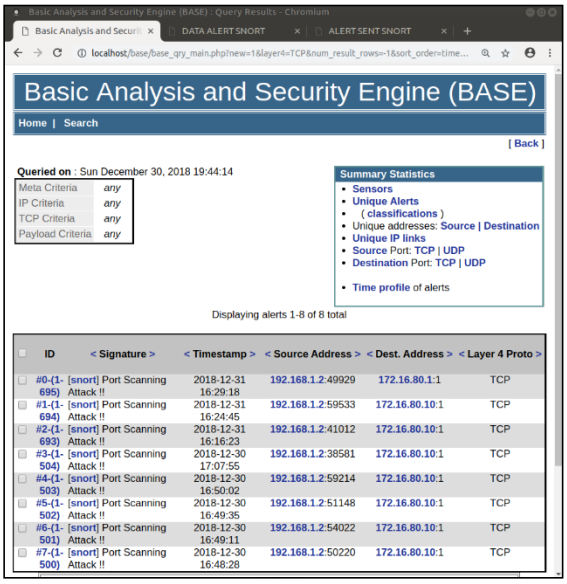
Gambar 4 menunjukan hasil monitoring pada saat terjadi serangan PING *Attack* rata-rata penggunaaan CPU naik menjadi 100,0%, penggunaan RAM sebesar 731,4 MiB (79,0%), dan yang terakhir beban jaringan untuk sent naik menjadi 10,0 KiB/s dan receiving-nya naik menjadi 9,9 KiB/s.



Gambar 4. Hasil Monitoring Pada Saat Terjadi Serangan PING *Attack*

Port Scanning

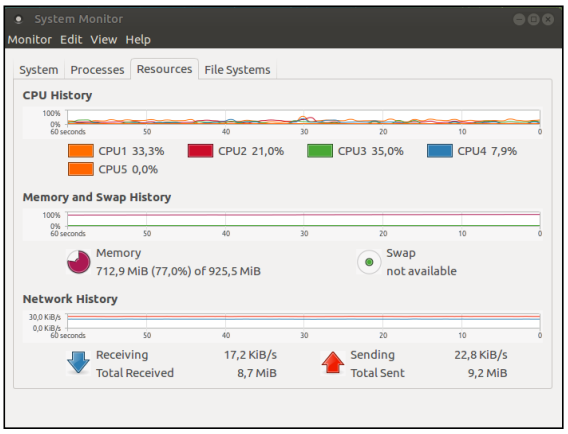
Pengujian selanjutnya adalah pengujian *port scanning* pada *server*. Pengujian *port scanning* pada *case* ini menggunakan tools *Nmap-Zenmap*.



Gambar 5. Hasil Monitoring Pada Saat Terjadi Serangan PING *Attack*

Pada Gambar 5, terlihat pada tabel Signature berisi Port Scanning *Attack* !! ini adalah nama dari sebuah serangan yang dilakukan, pada Timestamp berisi 2018-12-31 16:24:45 ini adalah waktu serangan yang dilakukan, pada Source Address berisi 192.168.1.2 ini merupakan IP Address yang dimiliki oleh host yang melakukan serangan terhadap Komputer *Server*, pada Dest. Address berisi 172.16.80.10 ini merupakan IP Address yang diserang, dan yang terakhir pada Layer 4 Proto berisi TCP ini merupakan protokol apa yang digunakan untuk melakukan serang tersebut.

Gambar 6 menunjukan hasil monitoring pada saat terjadi serangan Port Scanning rata-rata penggunaaan CPU naik menjadi 35,0 %, penggunaan RAM naik sebesar 712,9 MiB (77,0%), dan yang terakhir untuk beban jaringan masih 22,8 KiB/s untuk sent dan 17,2 KiB/s.

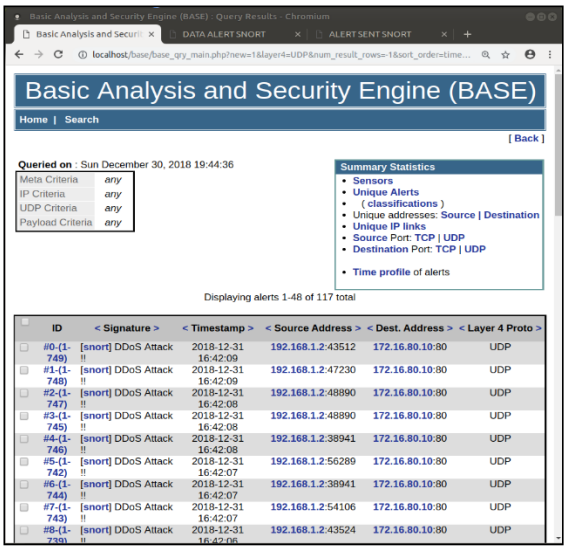


Gambar 6. Hasil Monitoring Pada Saat Terjadi Serangan *Port Scanning*

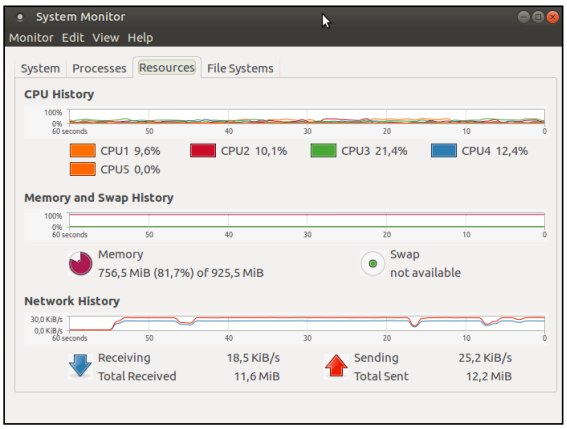
DOS/Ddos *Attack*

Pengujian selanjutnya adalah pengujian DOS/DDoS *Attack* pada *server*. Pengujian DOS/DDoS *Attack* pada *case* ini menggunakan tools LOIC *(Low Orbit Ion Cannon)*.

Pada Gambar 7, terlihat pada tabel Signature berisi DOS/DDoS *Attack* !! ini adalah nama dari sebuah serangan yang dilakukan, pada Timestamp berisi 2018-12-31 16:42:09 ini adalah waktu serangan yang dilakukan, pada Source Address berisi 192.168.1.2 ini merupakan IP Address yang dimiliki oleh host yang melakukan serangan terhadap Komputer *Server*, pada Dest. Address berisi 172.16.80.10 ini merupakan IP Address yang diserang, dan yang terakhir pada Layer 4 Proto berisi UDP ini merupakan protokol apa yang digunakan untuk melakukan serang tersebut.



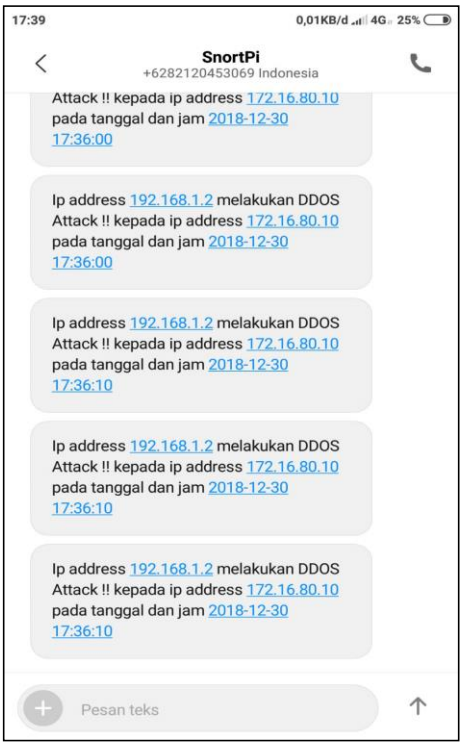
Gambar 7. Hasil Monitoring Pada Saat Terjadi Serangan *Port Scanning*



Gambar 8. Hasil Monitoring Pada Saat Terjadi Serangan DOS/DDoS *Attack*

Gambar 8, menunjukan hasil monitoring pada saat terjadi serangan DOS/DDoS *Attack* rata-rata penggunaaan CPU naik menjadi 21,4%, penggunaan RAM naik sebesar 756,5 MiB (81,7%) , dan yang terakhir beban jaringan untuk sent naik menjadi 25,2 KiB/s dan receiving-nya naik menjadi 18,5 KiB/s.

Semua pengujian yang telah dilakukan, system IDS yang telah dibuat dilengkapi dengan fitur sms gateway yang dapat memberikan notifikasi kepada *user* apabila terjadi serangan. Gambar 9 menunjukkan salah satu contoh notifikasi melalui sms yang terkirim ke handphone user.



Gambar 9. SMS Alert DOS/DDoS *Attack* Pada *Handphone* Administrator Jaringan

Dari pengujian ini dapat dikatakan bahwa sistem pendeteksi intrusi pada jaringan dan *Server* menggunakan Raspberry Pi berbasis Snort melalui pemberitahuan SMS Gateway ini berhasil memberikan peringatan berupa SMS alert ke handphone administrator apabila terjadi serangan DOS/DDoS *Attack* terhadap Komputer *Server*.

III. Kesimpulan

Berdasarkan pengujian dan pembahasan yang telah dilakukan maka dapat diambil kesimpulan terhadap Sistem Pendeteksi Intrusi Pada Jaringan Dan *Server* Menggunakan Raspberry Pi Berbasis Snort di STMIK STIKOM Indonesia sebagai berikut:

1. Sistem pendeteksi intrusi pada jaringan dan *Server* yang diterapkan menggunakan Raspberry Pi 3 Model B sebagai *Server* IDS (Intrusion Detection System), Snort sebagai mesin pendeteksi utama, Barnyard2 sebagai pembaca hasil dari keluaran Snort dan menyimpannya ke dalam database, BASE (Basic Analysis and Security Engine) sebagai tampilan informasi serangan dalam bentuk website, serta Gammu sebagai SMS Gateway untuk mengirimkan alert ke handphone administrator jaringan.
2. Sistem pendeteksi intrusi pada jaringan dan *Server* menggunakan Raspberry Pi berbasis Snort yang diterapkan telah berhasil dibangun dan diujikan. Secara keseluruhan, sistem ini dapat memberi peringatan dini adanya upaya serangan terhadap Komputer *Server*.
3. Dari hasil pengujian masing-masing serangan, dapat dilihat pada saaat terjadi serangan, penggunaan sumber daya pada Raspberry Pi 3 Model B untuk serangan PING *Attack*, Port Scanning, dan DOS/DDoS *Attack* meningkat dalam hal penggunaan CPU, Memory (RAM), dan Beban Jaringan.

IV. Daftar Pustaka

[1] Beale, jay 2003. Snort 2.0 Intrusion Detection, Inc. Masachusset: Syngress Publishing.

[2] Masse, F. A., dan Hidayat, A. N. 2015. "Penerapan Network Intrusion Detection System Menggunakan Snort Berbasis", *1*(2), 1–16.

[3] Affandi, M., dan Setyowibowo, S. (n.d.). "Implementasi Snort Sebagai Alat Pendeteksi Intrusi", *4*(2).

[4] Kurniawan, A. 2015. "Raspberry Pi Wireless Networks", 138.

[5] Foundation, R. P. 2015. Raspberry Pi The Complete Manual The Essential Handbook For All Raspberry Pi Users.

[6] Rizki, M., Soegiarto, D., dkk. 2015. "Implementasi Mini *Server* Berbasis Security Proxy Dengan Menggunakan Raspberry Pi Secara", *1*(2), 1030–1042

[7] Prihatmoko, D. 2017. "Pemanfaatan Raspberry Pi Sebagai *Server* Web Untuk Penjadwalan Kontrol Lampu Jarak Jauh". Jurnal Infotel, *9*(1), 84–91.