SISTEM NOTIFIKASI SMS TERHADAP TINDAKAN PENYUSUPAN PADA JARINGAN KOMPUTER DI BIRO TIK UNIVERSITAS MUHAMMADIYAH MAGELANG

Dhimas Radhito [1] Andi Widiyanto [2], Bambang Pujiarto [3]

Prodi Teknik Informatika Universitas Muhammadiyah Magelang
[1] dhiradhim@gmail.com, [2] andi.widiyanto@ummgl.ac.id, [3] amadheos@gmail.com

ABSTRAK

Seorang administrator jaringan bertugas untuk memastikan jaringan komputer selalu aman dari tindakan penyusupan atau serangan dan memastikan ketersediaan layanan bagi para pengguna. Tindakan penyusupan atau serangan bisa terjadi kapan saja. Ada beberapa serangan yang tidak dapat ditangani oleh sistem keamanan jaringan sehingga peran administrator sangat penting untuk melindungi jaringan komputer. Penelitian ini bertujuan untuk membangun sebuah sistem notifikasi sms ketika ditemukan serangan yang membutuhkan tindakan administrator pada jaringan komputer. Sistem yang dibangun menggunakan Snort sebagai Intrusion Detection System yang berfungsi untuk mendeteksi semua aktifitas yang terjadi di dalam jaringan, sehingga bila ditemukan serangan yang membutuhkan tindakan administrator, maka notifikasi akan dikirimkan kepada administrator. Gammu sebagai SMS Gateway bertugas untuk mengirimkan notifikasi kepada administrator melalui sms. Setelah sistem ini diterapkan, sistem ini mampu mendeteksi aktifitas jaringan yang terjadi di BIRO TIK Universitas Muhammadiyah Magelang dengan persentase terbesar yaitu misc-activity sebesar 82.596% dan persentase terkecil yaitu unknown sebesar 0.001%. Selain itu, lalu lintas data yang dianggap berbahaya dan membutuhkan tindakan langsung oleh administrator akan diproses sebagai notifikasi yang dikirimkan ke administrator melalui sms. Jika ditemukan ada beberapa data yang memiliki jenis serangan, IP sumber, IP tujuan dan waktu serangan yang sama, maka sistem akan mengirimkan 1 notifikasi terhadap beberapa data yang sama.

Kata Kunci:Keamanan jaringan,Intrution Detection System SMS Gateway

A. Pendahuluan

Perkembangan teknologi terutama di bidang jaringan komputer dan internet berkembang sangat pesat. Komputer yang dulu bersifat berdiri sendiri, sekarang sudah jarang ditemukan. Kebutuhan akan transfer data yang cepat dan praktis membuat jaringan komputer sangat dibutuhkan. Universitas Muhammadiyah Magelang sebagai salah satu Universitas Swasta di Indonesia sangat memerlukan jaringan komputer hampir di seluruh kegiatan baik perkuliahan maupun administrasi. Seluruh staf maupun mahasiswa memiliki hak untuk menggunakan jaringan komputer yang telah disediakan oleh pihak universitas. Akses ke dalam jaringan komputer di Universitas Muhammadiyah Magelang tidak terbatas hanya pada jaringan lokal atau intranet saja, tetapi juga dapat diakses melalui internet. Hal ini

dapat mengakibatkan berbagai macam resiko terutama pada bidang keamanan jaringan komputer.

Keamanan jaringan merupakan suatu tindakan yang berhubungan dengan deteksi dan pencegahan terhadap tindakan yang dianggap merugikan. Pada tahun 2014, kejahatan pada bidang jaringan komputer di Indonesia mencapai angka 48.4 juta (Rudiantara, 2015). Seorang administrator bertugas untuk mengelola dan menjamin bahwa jaringan komputer yang ia jaga terhindar dari tindakan penyusupan serta menjamin ketersediaan layanan bagi penggunanya. Seperti halnya di Universitas Muhammadiyah Magelang, terdapat biro khusus yang bertugas menangani lalu lintas data dan ketersediaan layanan bagi para penggunanya.

Kendala yang sering dialami oleh administrator adalah tindakan penyusupan bisa terjadi kapan saja, bila administrator tidak segera melakukan tindak pencegahan karena telat mendeteksi penyerangan maka dapat berakibat fatal. Demi keamanan sebuah jaringan komputer, maka dibutuhkan sebuah sistem yang dapat memberikan peringatan dini terhadap tindak penyusupan yang dilakukan pengguna yang tidak bertanggung jawab.

Snort merupakan sebuah perangkat lunak Intrusion Detection System (IDS) yang berfungsi untuk memonitor jaringan dari aktivitas yang berbahaya. Aktifitas yang berbahaya dapat berupa penyusupan oleh orang yang tidak memiliki hak otorisasi ataupun pengguna yang menyalahgunakan kewenangan yang diberikan. Snort akan memantau jaringan, bila terdapat aktifitas mencurigakan maka snort akan memberikan peringatan melalui pesan singkat yang akan dikirimkan melalui sebuah aplikasi *sms gateway* bernama gammu.

B. Tinjauan Pustaka

1. Jaringan Komputer

   Jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan yang lainnya menggunakan protokol komunikasi sehingga dapat seling berbagi informasi, aplikasi dan perangkat keras secara bersama-sama. Jaringan komputer juga membantu perusahaan dalam melayani pelanggan dengan lebih efektif. (Febriyudhi, 2013).

2. *Transmission Control Protocol/Internet Protocol* (TCP/IP)

   TCP/IP adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam suatu jaringan. Prinsip pembagian lapisan pada TCP/IP menjadi protokol komunikasi data yang mudah disesuaikan dan dapat diterapkan di setiap jenis komputer dan antar-muka jaringan. Oleh karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu (Wardoyo dkk., 2014).

3. Intrusion Detection System (IDS)
   Intrusion Detection System adalah sebuah alarm keamanan yang dikonfigurasi untuk melakukan pengamatan terhadap access point, aktifitas host dan kegiatan penyusupan. Cara paling sederhana untuk mendefinisikan IDS mungkin tergantung dari bagaimana mendeskripsikan IDS sehagai tool spesial yang dapat membaca dan mengintepretasikan isi dari file-file log dari router, firewall server dan perangkat jaringan lainnya. Secara lebih spesifik, Intrusion Detection System adalah sebuah sistem yang dapat mendeteksi adanya penggunaan tak ter-autorisasi (unauthorized use) pada sebuah sistem jaringan. (Affandi dan Setyowibowo, 2014)
4. Snort
   Mutaqin (2016) menyatakan bahwa snort merupakan sebuah aplikasi atau tool sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Dalam praktiknya, snort sangat andal untuk membentuk logging paket-paket dan analisis trafik-trafik secara real-time dalam jaringan berbasis TCP/IP.
5. Kelas Serangan
   Merujuk pada buku yang ditulis oleh Cheswick W.R. dkk. (2003) kelas serangan dibagi menjadi 10 kelas, diantaranya Pencurian Password, Social Engineering, Bugs dan Backdoors, Kegagalan Autentikasi, Kegagalan Protokol, Kebocoran Informasi, Exponential Attacks, Denial-of-Service (DoS), Botnets dan Serangan Aktif.
6. Barnyard2
   Barnyard2 merupakan *tool open source* sebagai penerjemah alert unified dan log dari Snort. Barnyard2 dapat meningkatkan efisiensi. Snort dengan cara mengurangi beban pada sensor deteksi. Barnyard2 bekerja dengan membaca log dari snort yang berbentuk unified2 dan memasukannya kedalam database. Jika database tidak tersedia maka Barnyard2 akan memasukan semua data ketika database tersedia kembali sehingga tidak ada alert atau log yang hilang (Harjono dan Wicaksono, 2014).
7. Basic Analysis Security Engine (BASE)
   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. Fungsi utama BASE adalah memberikan GUI (Graphic User Interface) pada Snort IDS sehingga memudahkan dalam melihat log yang tercatat dalam database (Mutaqin, 2016).
8. Short Message Service (SMS)
   Short Message service (SMS) sebagai sebuah layanan yang

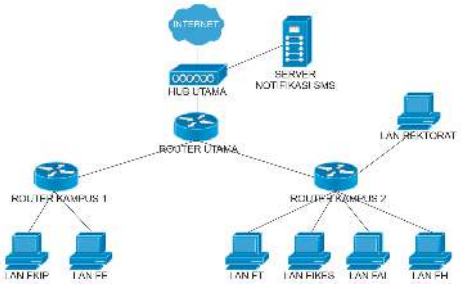
memungkinkan dilakukannya pengiriman pesan dalam bentuk alphanumeric antara terminal pelanggan atau dengan sistem eksternal seperti email, paging, voice mail dan lain-lain. Message pertama dikirimkan menggunakan SMS dilakukan pada bulan Desember 1992, dikirimkan dari sebuah Personal Computer (PC) ke telepon mobile (bergerak) dalam jaringan GSM milik Vodafone Inggris. Perkembangan kemudian ke benua Amerika, dipelopori oleh beberapa operator komunikasi bergerak berbasis digital seperti BellSouth Mobility, PrimeCo, Nextel dan beberapa operator lain. Teknologi digital yang digunakan bervariasi dari yang berbasis GSM, Time Division Multiple Access (TDMA), hingga Code Division Multiple Access (CDMA) (Adiyanto dkk., 2013)

9. Gammu

Gammu merupakan aplikasi open source di bawah lisensi GPL (General Public License) yang digunakan untuk membangun SMS Gateway. Banyak dari pengembang software yang menggunakan aplikasi ini sebagai sarana untuk membangun SMS Gateway dengan menggunakan bahasa pemrograman tertentu. Penggunaan gammu memungkinkan untuk membangun aplikasi SMS Gateway sesuai kebutuhan yang diperlukan mulai dari mengirim SMS, menerima SMS, kirim SMS massal, kirim SMS otomatis, membuat SMS auto respons, dan membuat SMS terjadwal (Aryani dkk., 2015).

C. Metode

1. Perancangan Jaringan



Gambar 1 Perancangan Jaringan

Desain jaringan yang dirancang menerapkan IDS di dalam jaringan BIRO TIK Universitas Muhammadiyah Magelang, sehingga lalu lintas data yang menuju BIRO TIK akan dimonitor dan dianalisa menurut aturan-aturan yang ada. Bila ditemukan adanya serangan yang membutuhkan tindakan administrator, Snort akan mencatat hasil serangan ke dalam database dan akan mengirimkan sebuah notifikasi berupa sms yang dikirimkan kepada administrator jaringan melalui modem GSM yang terpasang pada server notifikasi sms.

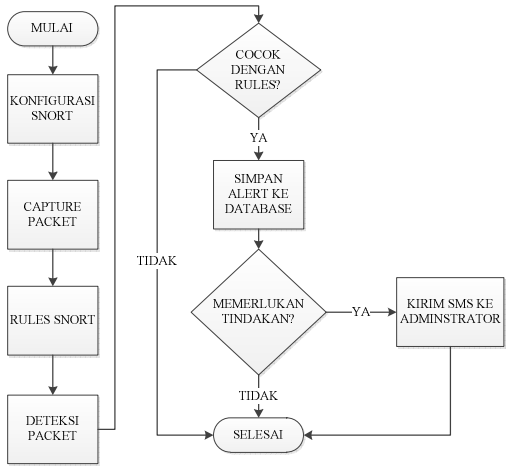
2. Klasifikasi serangan

Snort sebagai IDS memiliki kelemahan yaitu adanya false positives atau kesalahan dalam deteksi paket sehingga paket normal yang ditangkap oleh Snort dianggap sebagai sebuah serangan. Hal ini menyebabkan banyaknya notifikasi dengan isi false positives yang diterima oleh administrator sehingga memberatkan kinerja sistem. Tipe serangan akan dibagi menjadi 2, yaitu serangan yang membutuhkan tindakan administrator langsung dan serangan yang tidak memerlukan penanganan administrator

Tabel 1 Klasifikasi Serangan Berdasarkan Tindakan yang Diperlukan

No	Tindakan	Tipe Serangan
1	Memerlukan tindakan administrator	successful-recon-limited, successful-recon-largescale, successful-dos, attempted-user, unsuccessful-user, successful-user, attempted-admin, successful-admin, shellcode-detect, trojan-activity, denial-of-service, web-application-attack, inappropriate-content, policy-violation, file-format, malware-cnc, client-side-exploit
2	Tidak memerlukan penanganan administrator	attempted-recon, attempted-dos, non-standard-protocol, web-application-activity, misc-attack, default-login-attempt, rpc-portmap-decode, suspicious-filename-detect, suspicious-login, system-call-detect, bad-unknown, sdf, not-suspicious, unknown, string-detect, unusual-client-port-connection, network-scan, protocol-command-decode, misc-activity, icmp-event, tcp-connection

3. Alur Kerja Sistem



Gambar 2 Alur Kerja Sistem

Gambar 2 menjelaskan alur kerja sistem yang akan dibangun. Hal yang pertama dilakukan adalah konfigurasi Snort sebagai IDS. Langkah selanjutnya IDS akan melakukan monitoring lalu lintas paket data pada jaringan, paket yang lewat akan dicocokkan berdasarkan rule yang telah dibuat. Apabila tidak ditemukan kecocokan antara paket dengan rules maka proses berakhir. Jika ditemukan kecocokan paket dengan rules yang telah dibuat, sistem akan menyimpan deteksi serangan tersebut ke dalam database. Jika record pada database memerlukan tindakan administrator, maka sistem akan mengirimkan notifikasi kepada administrator melalui sms. Jika record pada database bisa ditangani oleh sistem, maka sistem tidak akan mengirimkan notifikasi kepada administrator dan proses selesai

4. Metode Pengujian
   a. Pengujian LAN
      Pengujian pada lingkup LAN menggunakan beberapa metode diantaranya Network Mapping, Brute Force, Cross Site Scripting dan SQL Injection. Pengujian ini dilakukan untuk menguji apakah sistem yang dibuat mampu mendeteksi serangan yang menuju BIRO TIK Universitas Muhammadiyah Magelang dan mampu mengirimkan notifikasi kepada administrator jika ditemukan serangan yang membutuhkan tindakan

administrator. Pengujian tersebut dapat dilihat pada tabel pengujian berikut:

Tabel 2 Pengujian Sistem

3	Cross Site Scripting	Browser	<script>alert("Percobaan XSS Inject") </script>	Muncul pesan peringatan berisi "Percobaan XSS Inject"
			<script>alert(document.cookie)</script>	Muncul pesan peringatan berisi "security=low; PHPSESSID= 6k232dkspm 5lk2sj1gpdk1ej v7"
4	SQL Injection	Sqlmap	sqlmap -u "http://192.168.3.212/dvwa/vu lnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=6k 232dkspm5lk2sj1gpdk1ejv7" --dbs	Daftar database pada host berhasil ditampilkan
			sqlmap -u "http://192.168.3.212/dvwa/vu lnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=6k 232dkspm5lk2sj1gpdk1ejv7" -D dvwa --tables	Daftar tabel pada database dvwa berhasil ditampilkan
			sqlmap -u "http://192.168.3.212/dvwa/vu lnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=6k 232dkspm5lk2sj1gpdk1ejv7" -D dvwa --dump	Isi tabel pada database dvwa berhasil ditampilkan

No	Jenis Serangan	Tools	Pengujian	Pengamatan
1	Network Mapping	Nmap	nmap 192.168.3.212	Port dan service pada host dapat ditampilkan
2	Brute Force	Hydra	hydra 192.168.3.212 -L /usr/share /wordlists/user.txt -P /usr/share/ wordlists/pass.txt http-get-form "/dvwa/vulnerabilities/brute/index .php:username="USER"&passwo rd="PASS"&Login=Login:Userna me and/or password incorrect.:H= Cookie: security=low;PHPSESSID =6k232dkspm5lk2sj1gpdk1ejv7"	Username dan password ditemukan
		Patator	Patator http_fuzz method=GET url="http://192.168.3.212/dvwa/ vulnerabilities/brute/?username= FILE1&password=FILE0& Login=Login" 1=/usr/share/word lists/user.txt 0=/usr/share/wordlists /pass.txt header="Cookie: security =low; PHPSESSID=6k232dkspm5 lk2sj1gpdk1ejv7" follow=0 accept_cookie=0 --threads=10 timeout=20 -x ignore: fgrep= 'Username and/or password incorrect.'	Username dan password ditemukan

b. Pengujian di BIRO TIK
Setelah dilakukan pengujian pada lingkup LAN, maka dilakukan pengujian dengan menerapkan sistem pada jaringan BIRO TIK Universitas Muhammadiyah Magelang. Pengujian dilakukan selama 12 hari mulai tanggal 12-23 Desember 2016. Dalam kurun waktu tersebut didapatkan 236.878 data serangan pada jaringan di BIRO TIK Universitas Muhammadiyah Magelang. Data tersebut dapat dilihat pada tabel dibawah ini :

Tabel 3 Serangan di BIRO TIK

ID Classtype Serangan	Classtype Serangan	Jumlah	Persentase
2	unknown	3	0.001%
7	attempted-dos	13	0.005%
14	rpc-portmap-decode	33	0.014%
27	web-application-activity	125	0.053%
26	protocol-command-decode	352	0.149%
23	network-scan	968	0.409%
30	misc-attack	10.089	4.259%
4	attempted-recon	10.731	4.530%
3	bad-unknown	18.913	7.984%
29	misc-activity	195.651	82.596%
TOTAL		236.878	

Data serangan pada tabel 3 memiliki classtype yang masih bisa ditangani oleh sistem sehingga termasuk ke dalam klasifikasi serangan yang tidak membutuhkan tindakan administrator.

D. Hasil dan Pembahasan

1. Hasil
Setelah dilakukan perancangan, implementasi dan pengujian sistem, maka dapat disimpulkan bahwa sistem yang dibangun telah sesuai dengan tujuan penelitian yaitu membangun sebuah sistem yang mampu mengirimkan notifikasi sms ketika ditemukan tindakan penyusupan pada jaringan komputer di BIRO TIK Universitas Muhammadiyah Magelang. Hal ini dapat dibuktikan melalui pengujian pada Local Area Network, sistem mampu mengirimkan notifikasi ketika dilakukan pengujian dengan metode yang termasuk dalam kategori berbahaya dan membutuhkan tindakan administrator

Gambar 3 Notifikasi SMS ke Administrator.

Terdapat perbedaan dalam jumlah serangan yang berbahaya dan notifikasi yang dikirimkan. Jumlah serangan yang berbahaya tercatat ada 37, sedangkan notifikasi yang dikirimkan berjumlah 23.

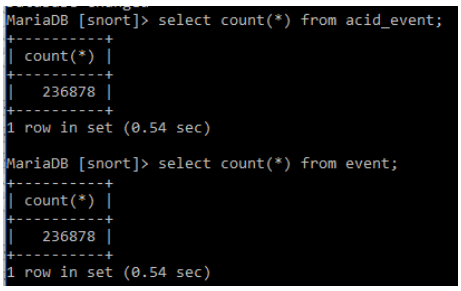
Gambar 4 Total Data Serangan Berbahaya

Gambar 5 Total Data Notifikasi

Setelah sistem diimplementasikan selama 12 hari pada BIRO TIK Universitas Muhammadiyah Magelang, tidak ditemukan adanya tindakan yang berbahaya sehingga sistem tidak mengirimkan notifikasi kepada administrator.

2. Pembahasan
   a. Deteksi Serangan oleh Sistem Berdasarkan hasil pengujian di atas, sistem telah mampu mendeteksi aktifitas yang terjadi di dalam jaringan berdasarkan rule yang ada baik yang dikategorikan sebagai aktifitas biasa maupun aktifitas yang dianggap berbahaya. Seluruh aktifitas di dalam jaringan yang tercatat telah berhasil ditampilkan dalam tampilan website dan dapat dipantau oleh administrator.
   b. Pengiriman Notifikasi
      Berdasarkan hasil pengujian diatas, pengiriman notifikasi terhadap tindakan penyusupan dalam jaringan telah berhasil dilakukan. Seluruh aktifitas di dalam jaringan yang dianggap berbahaya dan memerlukan tindakan adminitrator dapat dikirimkan melalui media sms. Pembagian kelas serangan berdasarkan tindakan yang diperlukan seperti pada tabel 1 telah berhasil diimplementasikan ke dalam sistem sehingga hanya aktifitas yang termasuk ke dalam kategori 1 saja yang akan diproses sebagai notifikasi, sedangkan aktifitas yang termasuk ke dalam kategori 2 hanya akan tercatat dalam database dan ditampilkan ke dalam website.
      Pada gambar 4 dan 5 terdapat perbedaan jumlah serangan berbahaya dan notifikasi yang dikirimkan. Perbedaan jumlah tersebut terjadi karena terdapat data dengan tipe serangan, IP sumber, IP tujuan dan waktu serangan yang sam
   c. Hasil Akhir
      Setelah sistem diimplementasikan pada BIRO TIK, dapat disimpulkan bahwa modul-modul yang saling berkaitan secara keseluruhan telah

berfungsi dengan baik. Hal ini dapat dilihat pada tabel event dan acid_event. Jumlah data yang tercatat menunjukkan hasil yang sama, artinya seluruh hasil yang telah dicatat ke dalam tabel event oleh snort dan barnyard2 telah berhasil dimasukkan ke dalam tabel acid_event untuk ditampikan ke dalam aplikasi BASE.



Gambar 6 Jumlah data Tabel event dan acid_event

Berdasarkan tabel 3, total serangan berjumlah 236.878. Persentase terbesar data serangan yang tercatat memiliki classtype misc-activity dengan persentase 82.596% dan data serangan terkecil memiliki persentase 0.001% dengan classtype unknown. Seluruh serangan yang terjadi di BIRO TIK Universitas Muhammadiyah Magelang dapat ditangani oleh sistem dan tidak membutuhkan tindakan administrator sehingga sistem tidak mengirimkan notifikasi kepada administrator.

E. Kesimpulan

Berdasarkan implementasi dan penjelasan yang telah dijabarkan pada bab-bab sebelumnya, maka dapat diambil kesimpulan bahwa Snort sebagai IDS mampu mendeteksi aktifitas jaringan yang terjadi di BIRO TIK Universitas Muhammadiyah Magelang dengan persentase terbesar yaitu classtype misc-activity sebesar 82.596% dan persentase terkecil yaitu classtype unknown sebesar 0.001%. Gammu mampu mengirimkan notifikasi ketika ditemukan tindakan penyusupan pada jaringan komputer, tetapi jumlah notifikasi yang dikirimkan tidak sesuai dengan jumlah serangan yang tercatat dikarenakan adanya beberapa serangan dengan jenis serangan, ip sumber, ip tujuan dan waktu serangan yang sama sehingga hanya dikirimkan 1 notifikasi untuk serangan dengan nilai yang sama.

7. DAFTAR PUSTAKA

[1] Adiyanto, Suraya, & Sutanta E. 2013. Integrasi Aplikasi Web dan SMS Gateway pada TPI Gempolsari menggunakan PHP dan MySQL. *Jurnal JARKOM, Vol. 1 No. 1, 49-56, Desember 2013.*

[2] Affandi M., & Setyowibowo S. 2014. Implementasi Snort sebagai Alat Pendeteksi Intrusi menggunakan Linux. *Jurnal Teknologi Informasi, Vol. 4 No. 2, 98 – 112, Tahun 2013.*

[3] Aryani D., Setiadi A., & Alfiah F. 2015. Aplikasi Web Pengiriman dan Penerimaan SMS dengan Gammu SMS Engine Berbasis PHP. *ISSN : 1978 -8282, Volume 8 No.3, 174 – 190, Mei 2015.*

[4] Cheswick W.R., Bellovin S.M., & Rubin A.D. 2003. *Firewalls and Internet Security Second Edition - Repelling the Wily Hacker*. Addison-Wesley.

[5] Febriyudi R. 2013. Analisis Pengembangan Jaringan Komputer Lokal pada Rumah Sakit Muhammadiyah Palembang. Universitas Bina Darma, Palembang.

[6] Harjono, & Wicaksono A.P. 2014. Sistem Deteksi Intrusi dengan Snort. *JUITA ISSN: 2086-9398 Vol. III Nomor 1, 31 – 34, Mei 2014.*

[7] Mutaqin A.F. 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, Tahun 2016.*

[8] Rudiantara. 2015. *Laporan Kinerja Kementerian Komunikasi dan Informatika Tahun 2014.* Kementerian Komunikasi dan Informatika.

[9] Utami A.S.P., & Lidyawati L. 2013. Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd. *Jurnal Reka Elkomika, Volume 1 No. 4, 317-327, Tahun 2013.*

[10] Wardoyo S., Riyadi T. & Fahrizal R. 2014. Analisis Performa File Transport Protocol pada Perbandingan Metode Ipv4 Murni, Ipv6 Murni dan Tunneling 6to4 Berbasis Router Mikrotik. *Jurnal Nasional Teknik Elektro Vol: 3 No. 2, 106-117, September 2014.*

[11] Wildani R. 2012. *Implementasi* Intrusion System (IDS) Snort pada Laboratorium Jaringan Komputer. *UG Jurnal, Volume 6 No. 05 Tahun 2012.*o.