IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053

Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal

Yudhi Arta
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Riau
e-mail : yudhiarta@eng.uir.ac.id

Abstract

Intrusion Detection System (IDS) helps users in monitoring and analyzing disruptions to network security. The purpose of this research is to design IDS using Snort with web based interface and system implementation to monitor the activities of Hotspot users of Islamic University of Riau. This study contains an analysis of UIR wireless network interference, the proposed network security solutions, processes and workings of IDS systems created on a web basis, as well as evaluation of the implementation of IDS systems on the network. The security of a computer network is necessary to maintain the validity and integrity of data and ensure the availability of services for its users. The system must be protected from all sorts of attacks and intrusion attempts that could damage the existing system.

Keywords*: UIR, IDS, Hotspot, Wireless, Security.*

Abstrak

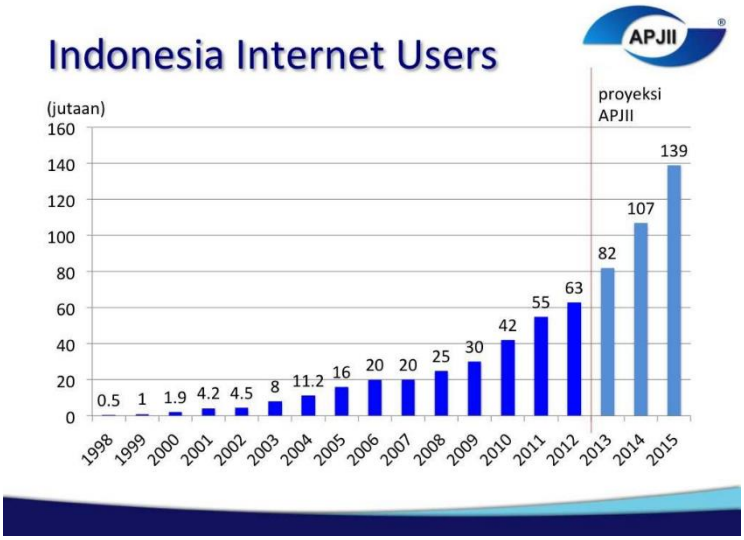
Intrusion Detection System (IDS) membantu pengguna dalam memonitor dan menganalisa gangguan pada keamanan jaringan. Tujuan penelitian ini adalah merancang IDS menggunakan Snort dengan tampilan antarmuka berbasiskan web dan implementasi sistem untuk memantau aktifitas para pengguna Hotspot Universitas Islam Riau. Penelitian ini berisi analisa gangguan pada jaringan nirkabel UIR, usulan solusi keamanan pada jaringan, proses dan cara kerja sistem IDS yang dibuat dengan basis web, serta evaluasi penerapan sistem IDS pada jaringan. Keamanan sebuah jaringan komputer diperlukan untuk menjaga validitas dan integritas data serta menjamin ketersedian layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan yang dapat merusak sistem yang ada.

Kata kunci : UIR, *IDS, Hotspot, Nirkabel*, Keamanan.

1. PENDAHULUAN

Internet pada abad 21 telah menjadi bagian penting dari gaya hidup masyarakat di seluruh dunia. internet telah merambah ke hampir semua aspek kehidupan, dari sebagai penunjang pekerjaan, hiburan, edukasi dan lain – lain. Pengguna internet pun tiap tahunnya terus meningkat, situs APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mencatat 82 juta orang telah menggunakan jasa internet, dan diproyeksikan angka tersebut akan meningkat menjadi 107 juta orang dan 139 juta orang pada tahun 2014 dan 2015 (R.Rustam, 2013).

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053



Gambar 1. Data Pengguna Internet di Indonesia (sumber: apjii.or.id)

Intrusion Detection System yang nantinya akan disebut IDS merupakan usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal cracker) atau seorang user yang sah tetapi menyalahgunakan *privilige*s sumber daya sistem. *Intrusion Detection System* (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi *software dan hardware*) yang berusaha melakukan deteksi penyusupan . IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal.

Di sisi lain, sebuah sistem pencegahan penyusupan (IPS) merupakan perangkat lunak yang memiliki semua kemampuan sistem deteksi intrusi dan juga dapat mencoba untuk menghentikan insiden yang mungkin terjadi.

2. METODOLOGI PENELITIAN

Peningkatan jumlah pengguna jasa internet menunjukkan semakin banyak lapisan masyarakat Indonesia yang menikmati dampak positif dari layanan internet, namun tentunya hal ini menuntut langkah pengamanan yang lebih baik untuk menghadapi ancaman serangan yang datang baik dari dalam maupun luar negeri. Pada saat ini di Indonesia terjadi lebih dari ratusan ribu serangan (*intrusi*on) setiap harinya terhadap keamanan internet seperti tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain, tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua pihak yang seharusnya berinteraksi, dan tindakan lain yang berpotensi untuk menghancurkan informasi yang berjalan di atas infrastruktur internet. Kasus-kasus terkait insiden terhadap keamanan internet telah marak terjadi di Indonesia dan mengancam langsung pada infrastruktur strategis di Indonesia. Data dari Id-SIRTII (*Indonesia Security Incident Response Team on Internet Infrastructure*) mencatat pada kurun waktu bulan Januari – September 2013, total serangan intrusi mencapai 42 juta serangan dimana yang tertinggi terjadi pada tanggal 5 April 2013 yaitu sebesar 517 ribu serangan intrusi.

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053

Tabel 1. Total Jumlah Serangan (Intrusi) di Indonesia dalam jutaan (sumber: Id-SIRTII)

Jan	Feb	Mar	Apr	Mei	Jun	Jul	Ags	Sep
2.4	1.9	10.7	9.9	5.8	3.1	3.8	2	2.4

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan. Menurut Garfinkel dan Spafford, ahli dalam komputer security, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu:

1. *Availability*
2. *Confidentiality*
3. *Data Integrity*
4. *Control*
5. *Audit*

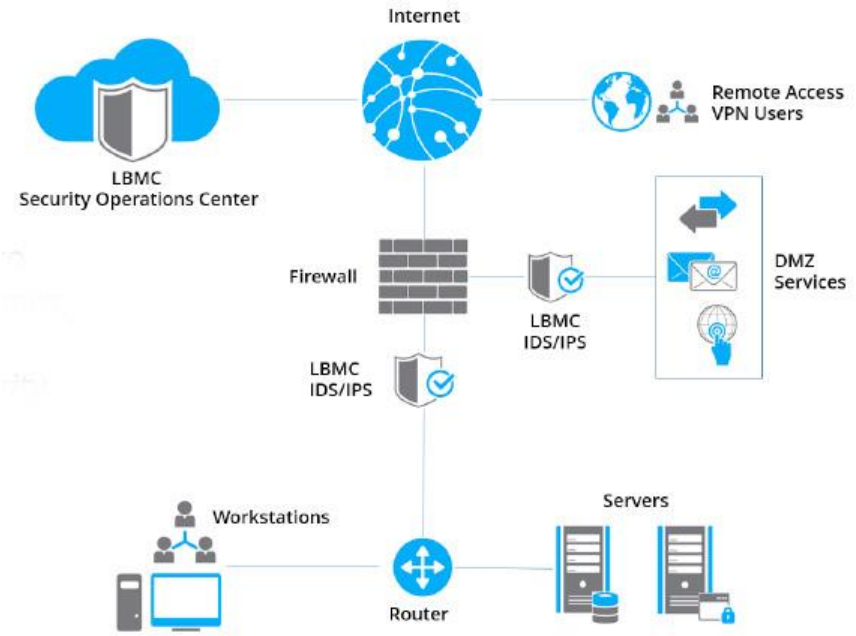
Intrusion Detection System (IDS) adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

Deteksi penyusupan (*Intrusion Detection*) adalah aktivitas untuk mendeteksi penyusupan secara cepat dengan menggunakan program khusus. Program yang digunakan untuk pendeteksian disebut sebagai IDS (*Intrusion Detection System*). Tipe Dasar IDS adalah

1. *Rule-based systems*, berdasarkan atas database dari tanda penyusupan atau serangan yang telah dikenal. Jika IDS mendeteksi Kemudian lintas sesuai dengan data dari database, maka pendeteksian tersebut langsung dikategorikan sebagai penyusupan.
2. *Adaptive systems*, sama seperti *Rule-based* tetapi ditambah dengan teknik lain yaitu membuka kemungkinan untuk mendeteksi metode penyusupan yang baru.

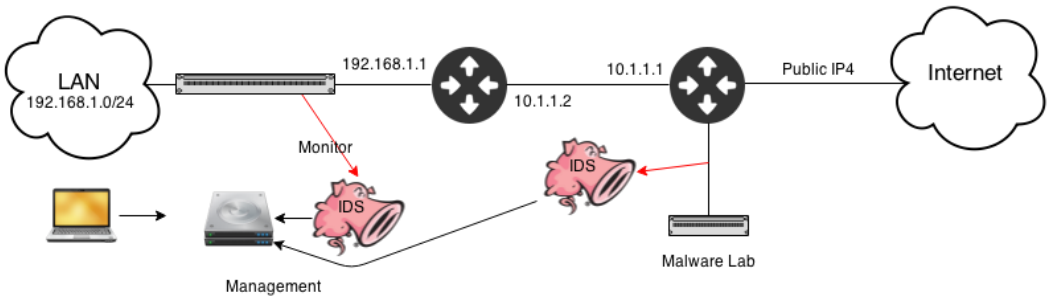
Pendekatan yang digunakan dalam *rule-based system* ada dua, yaitu *Preemptory* (pencegahan) dan *Reactionary* (reaksi). Perbedaan dari kedua pendekatan tersebut adalah dalam waktu saja. Dalam Preemptory akan memperhatikan semua Kemudian-lintas jaringan. Apabila paket mencurigakan ditemukan maka program akan melakukan tindakan yang sesuai dengan paket mencurigakan tersebut. *Reactionary*, program hanya mengamati log. Jika ditemukan paket mencurigakan, program akan melakukan tindakan sesuai dengan paket tersebut.

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053



Gambar 2. Cara Kerja IDS

Snort IDS merupakan IDS open source yang secara defacto menjadi standar IDS di industri. Snort dapat didownload di situs www.snort.org. Snort dapat diimplementasikan dalam jaringan yang *multiplatform*, salah satu kelebihannya adalah mampu mengirimkan *alert* dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui SMB. Snort dapat berkerja dalam 3 mode yaitu *sniffer mode* (penyadap), *packet logger* dan *network intrusion detection mode*. Adapun cara kerja snort dapat dilihat pada gambar 3 dibawah :



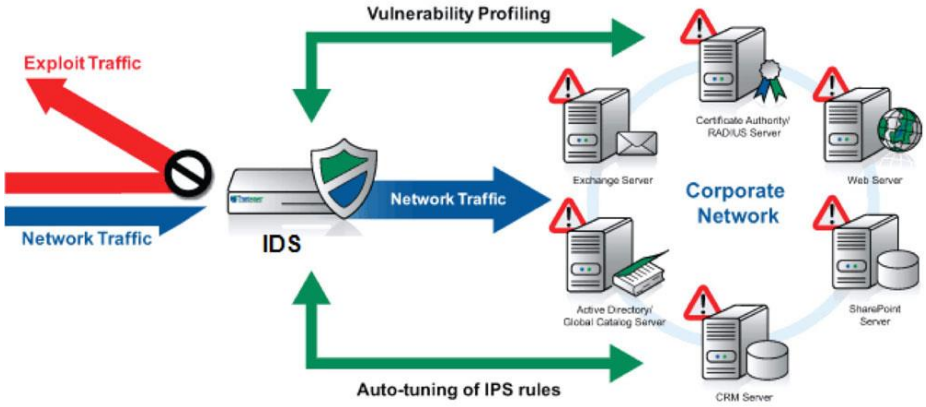
Gambar 3. Cara Kerja SNORT

3. HASIL DAN PEMBAHASAN

Dalam metodologi penelitian diatas dapat disimpulkan bahwa permasalahan yang dihadapi adalah serangan pada jaringan lokal. Metodologi yang dapat digunakan untuk meningkatkan keamanan sebuah jaringan adalah dengan membuat sebuah sistem kemanan yang dapat membaca serangan baik dari dalam maupun luar. Dengan adanya *Intrusin Detection System* ini dapat mengatasi masalah yang dihadapi pada jaringan lokal. Dengan adanya *IDS* tersebut maka dapat dibangun sebuah *topologi* yang dapat membantu kinerja dari segi keamanan, infrastruktur dan lainnya. *IDS* ini sendiri juga berfungsi

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053

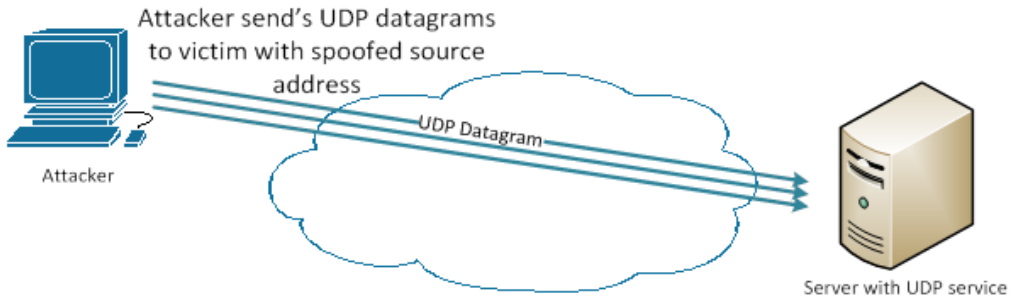
meningkatkan kinerja dan juga estabilitas kerja dari keamanan sistem itu sendiri. Uraian kerja akan dijelaskan di dalam kerangka kerja yang nantinya menjelaskan prosedur maupun langkah – langkah yang akan dihadapi dalam membangun atau mengukur *Intrusion Detection System* ini. Tahap awal adalah menganalisa dan merancang apa – apa saja yang dibutuhkan dalam pembangunan *IDS* ini. Lalu dilanjutkan dengan pengujian beserta membuat laporan hasil kinerja dari *IDS* tersebut dalam sebuah tabel.



Gambar 4. Kerangka Kerja Penelitian

Untuk perancangan topologi *Intrusion Detection System* hampir sama seperti dengan topologi yang hampir banyak digunakan. Dalam hal ini, *Cloud computing* mempunyai satu master dan beberapa *node* / *client* / *slave* yang nantinya akan di-*manage* oleh master *Cloud*. Virtual machine disini digunakan sebagai fasilitator untuk membangun dan mengukur kinerja performance dari cloud. Hampir keseluruhan perusahaan besar sudah menerapkan *Cloud* sejak awal komputasi mereka dibangun.

Pada skenario pengujian IDS berbasis Snort ini, akan dilakukan simulasi percobaan penyerangan (*attack*) dengan melakukan serangan *Denial of Service* (DoS attack). Serangan ini pada dasarnya merupakan suatu aktivitas dengan tujuan utama menghentikan atau meniadakan layanan sistem atau jaringan komputer sehingga pengguna tidak dapat menikmati fungsionalitas dari layanan tersebut. Contoh dari serangan *denial of service* yang digunakan dalam pengujian ini adalah dengan melakukan UDP (*User Datagram Protocol*) flooding. UDP flooding terjadi setelah jaringan "dibanjiri" dengan paket – paket UDP yang menyerang ke port – port secara random, atau menyerang ke port tertentu yang rentan terhadap serangan. Berikut mekanisme dari serangan UDP port :



Gambar 5. Mekanisme simulasi penyerangan UDP flooding

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053

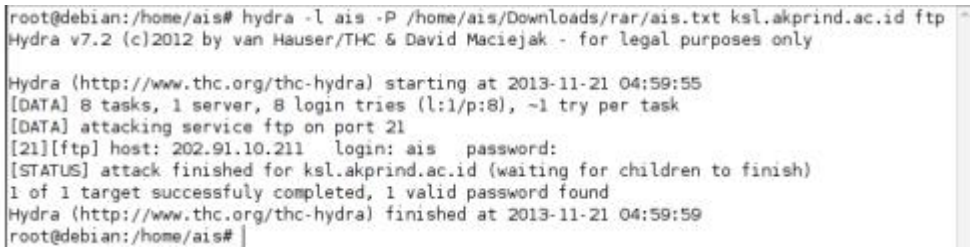
Adapun langkah – langkah Install pada Snort :

1. Masuk ke terminal root pada debian anda.
2. Ketik ***Apt-get install snort-mysql***
3. Masukkan ***any***, Kemudian tekan **OK**

Setelah mengintal snort maka langkah selanjutnya mengkonfigurasi snort. Adapun konfigurasi Snort sebagai berikut :

1. Buka Terminal, Kemudian tulis ***pico /etc/snort/snort.conf***
2. Untuk lebih mudah gunakan search yaitu CTRL+W Kemudian Sintaks ***dbstart***
3. Ketik :
   output database: log, mysql, user=snortuser password=snortpassword dbname=snort host=localhost antara (#DBSTART#) dengan (#DBBEND#)
4. Cari kata → ***redalert***, Hilangkan tanda comment (#) dari bagian ***ruletype redalert{}***
5. Ganti bagian ***output database*** dari ***ruletype redalert{}*** dengan :
   output database: log, mysql, user=snortuser password=snortpas sword host=localhost
   dbname=snort
6. Kemudian kita jalankan Snort dengan perintah :
   snort –u snort –c /etc/snort/snort.conf
7. CTRL+c untuk mengakhiri
8. Buka file crontab dan edit, Kemudian tulis ***pico/etc/crontab***
9. Tambahkan perintah dibawah ini di baris paling akhir.
   @reboot root snort -u snort -c /etc/snort/snort.conf >> /dev/null
10. Reboot lagi, maka pesan error tetap akan tampil
11. Kemudian tulis ***rm /etc/snort/db-pending-config***
12. Kemudian tulis ***pico /etc/default/snort*** pada bagian paling bawah, ubah nilai bagian ALLOW_UNAVAILABLE dari no menjadi yes.
13. Save kemudian exit
14. Kemudian tulis ***pico /etc/snort/snort.conf*** cari bagian eth0 di (var HOME_NET $ eth0 _ADDRESS), hilangkan tanda comment (#), ganti eth0 jadi eth1.

Pengujian dilakukan dengan melakukan koneksi FTP pada *server* secara remote menggunakan *tools* hydra untuk melakukan serangan dengan cara mencocokkan username dan password yang digunakan untuk *login* sebagaimana tampak pada Gambar 6.



Gambar 6. Serangan FTP

Berdasarkan hasil pengujian yang dilakukan dapat diketahui kemampuan dari sistem yang dibuat mampu untuk mengolah data output dari IDS snort serta dapat mengenali segala aktifitas yang dilakukan intruder dalam usaha untuk menyusup ke dalam sistem dengan menggunakan *ping flood, syn attack, port scanner*, SSH dan FTP

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053

berdasarkan rule yang telah diterapkan. Proses selanjutnya adalah dilakukan *blocking* terhadap IP address yang dianggap sebagai intruder dan sistem akan memberikan laporan kepada administrator melalui media jejaring sosial dan web monitoring mengenai adanya intruder yang mencoba masuk ke dalam sistem. Tabel 2 menunjukkan kemampuan dari sistem untuk mengelola hasil output dari snort untuk mengenali terjadinya serangan sampai terjadinya proses *blocking* menggunakan iptables dari beberapa sampel yang telah diujicobakan.

Tabel 2. Selisih Waktu Yang Dibutuhkan Untuk Blocking

NO	IP ADDRESS	WAKTU SERANGAN	WAKTU BLOCKING	SELISIH (DETIK)
1	192.168.100.1	08:36:24	08:36:30	5 detik
2	192.168.100.2	22:30:54	22:30:59	5 detik
3	192.168.100.3	18:08:37	18:08:44	7 detik
4	192.168.100.4	9:10:18	9:10:27	5 detik
5	192.168.100.1	23:34:24	23:34:31	7 detik
6	192.168.100.2	12.15.35	12.15.31	4 detik
7	192.168.100.1	14:14:35	14:14:39	4 detik
8	192.168.100.1	07:51:39	7:52:45	6 detik

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa setiap ada serangan yang datang dari luar menuju host atau server yang didalamnya terdapat IDS yang sedang berjalan, maka sistem akan memberikan informasi mengenai data serangan yang telah masuk kedalam sistem kita. Disamping dapat mendeteksi jumlah paket data serangan UDP *Flooding*, Snort dapat juga mendeteksi alamat IP si penyerang. Dalam hasil uji coba ini trafik yang terdeteksi di Snort sebagian besar adalah trafik IP versi 4 dengan jumlah 2697493 paket data dibandingkan dengan trafik IP versi 6 yang masih belum banyak dengan jumlah 74 paket data. Meskipun demikian, dengan semakin menurunnya jumlah slot untuk IP versi 4 diperkirakan trafik dengan IP versi 6 akan meningkat di masa depan. Adapun rata – rata deteksi serangan 6 detik.

DAFTAR PUSTAKA

[1] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Statistik Pengguna Internet di Indonesia, 2013, http://www.apjii.or.id/v2/read/page/halaman-data/9/statistik.html
[2] Indrajit, Richardus E. (2011). Manajemen Keamanan Informasi dan Internet. (Edisi Pertama). Jakarta: Informatika.
[3] Rehman, Rafeeq U. (2003). Intrusion Detection Systems with Snort, New Jersey: Prentice Hall.
[4] Scott, C., Wolfe, P. and Hayes, B. (2004). Snort for Dummies, Indianapolis: Wiley Publishing.
[5] Tanenbaum A., & Wetherall D., (2010). Computer Networks. (5th Edition). New Jersey : Prentice Hall.

IT Journal Research and Development
Vol.2, No.1, Agustus 2017 e-ISSN: 2528-4053

[6] Aditya Gagat Hanggara analisis dan implementasi intrusion detection system direktorat keamanan informasi kementerian komunikasi dan informatika, 2013.
[7] Ratnaningsih, I., 2012, Sistem Keamanan Jaringan Komputer menggunakan Intrusion Detection System (IDS) pada Linux, Skripsi, IST AKPRIND, Yogyakarta.
[8] Simarmata, J., 2006, Pengamanan Sistem Komputer, Andi, Yogyakarta.
[9] Y. Arta, E. A. Kadir, and D. Suryani, "KNOPPIX: Parallel computer design and results comparison speed analysis used AMDAHL theory," in *Information and Communication Technology (ICoICT), 2016 4th International Conference on*, 2016, pp. 1–5.
[10] Y. Arta, "KOSTUMISASI UBUNTU 9.10 UNTUK KEGIATAN PEMBELAJARAN DI BIDANG JARINGAN KOMPUTER (Studi kasus: TEKNIK INFORMATIKA FAKULTAS SAINS DAN TEKNOLOGI UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU)." Universitas Islam Negeri Sultan Syarif Kasim Riau, 2010.
[11] Yudhi Arta, "Asterik : Implementasi Voice Over Internet Protocol (VoIP) Pada Biro Administrasi Informatika Teknologi Universitas Islam Riau," *J. Sains*, vol. 4, no. 1, pp. 562–568, 2015.
[12] Y. Arta, "Penerapan Metode Round Robin Pada Jaringan Multihoming Di Computer Cluster," *Inf. Technol. J. Res. Dev.*, vol. 1, no. 2, pp. 26–35, 2017.
[13] Y. Arta, "Asterisk: Implementasi Voice Over Internet Protocol (VOIP) Pada Biro Administrasi Informatika Teknologi Universitas Islam Riau," *J. Relev. Akurasi Dan Tepat Waktu*, vol. 4, no. 1, pp. 562–568, 2015.
[14] Y. Arta, "ANALISA KINERJA PARALLEL COMPUTING DENGAN MENGGUNAKAN PERHITUNGAN HUKUM AMDAHL BERBASISKAN LINUX," *J. Inf. Pendidik.*, vol. 6, no. 2, 2013.
[15] Y. Arta, "Implementasi Computer Cluster Berbasis Open Source Untuk Penyeimbang Beban Sistem Dan Jaringan Komputer," *J. Tek. Inform. dan Sist. Inf.*, vol. 2, no. 1, 2016.