RANCANG MODEL SISTEM KEAMANAN MENGGUNAKAN *INTRUSION PREVENTIONSYSTEM* DENGAN METODE *RULE BASED* : STUDI KASUS KPDE PROVINSI JAMBI

Abdul Rahim
Program Studi Teknik Informatika, STIKOM Dinamika Bangsa
Jl. Jendral Sudirman Thehok - Jambi
E-Mail :abdulrahim@stikom-db.ac.id

ABSTRAK

Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia jaringan komputer, hal ini disebabkan tingginya ancaman yang mencurigakan dan serangan dari Internet. Keamanan komputer merupakan salah satu kunci yang dapat mempengaruhi tingkat reliability, termasuk performance dan availability pada suatu internetwork. Ancaman pada suatu jaringan komputer dapat berasal dari jaringan itu sendiri maupun dari jaringan internet, hal ini dapat disebabkan karena terdapat sumber daya yang bersifat publik sehingga untuk menjaga sumber daya yang ada pada jaringan komputer tersebut dibutuhkan suatu sistem khusus agar jaringan serta layanan-layanan yang terdapat pada jaringan tersebut tetap dapat digunakan dengan baik. Salah satu teknik untuk mengamankan sumber daya yang terdapat di jaringan komputer adalah dengan menggunakan intrusion detection system (IDS) atau sistem deteksi penyusup, dimana dengan adanya sistem deteksi penyusup, maka aktivitas jaringan yang mencurigakan dapat segera diketahui, selain itu dapat dilakukan tindakan pencegahan atau yang dikenal dengan nama intrusion prevention system (IPS). Dalam penelitian ini membahas tentang rancang model sistem keamanan menggunakan intrusion prevention system dengan metode rule based untuk melakukan pengamanan pada sumber daya jaringan komputer. Metode pengujian yang digunakan adalah metode pengujian blackbox testing, IDS akan diimplementasikan pada sistem operasi berbasis linux dan sistem pencegahan akan diimplementasikan pada iptables dan perangkat router gateway. Hasil dari penelitian ini berupa sistem pencegah penyusup (IPS) yang dapat meningkatkan keamanan sumber daya jaringan komputer dari ancaman baik yang berasal dari jaringan internet maupun intranet.

Kata Kunci : keamanan komputer, keamanan server, intrusion detection system, intrusion prevention system, sistem pencegahan.

ABSTRACT

Computer security systems, in recent years has become a major focus in the world of computer networks, this is due to the high threat of suspicious and attacks from the Internet. Computer security is one of the keys that can affect the level of reliability, including performance and availability on an internetwork. Threats to a computer network can be derived from the network itself or from the internet, this can be caused because there are public resources so as to maintain the existing resources in the computer network needs a special system to the network and the services that are on the network can still be used with either. One technique to secure the resources contained in a computer network is to use intrusion detection system (IDS) or intruder detection systems, where the presence of an intruder detection system, the suspicious network activity can be immediately known, but it can be done or that precautions known as intrusion prevention system (IPS). In this study discusses about the model design of security systems using intrusion prevention system with rule-based method for providing security in computer network resources. Testing method used is the method of testing blackbox testing, IDS will be implemented on a Linux-based operating system and prevention system will be implemented in iptables and gateway router device. The results of this study in the form of an intruder prevention systems (IPS) that can improve the security of computer network resources from threats originating from the Internet or intranet

Keywords: Computer security, server security, intrusion detection systems, intrusion prevention systems, computer network security, the prevention system.

1. PENDAHULUAN

Sistem Keamanan Komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia jaringan komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (suspicious threat) dan serangan dari Internet. Keamanan Komputer (Security) merupakan salah satu kunci yang dapat mempengaruhi tingkat Reliability (termasuk performance dan availability) suatu internetwork. Jika kita lihat dan beranjak dari data CSI/FBI survey, saat ini telah banyak perusahaan yang membelanjakan uangnya untuk terhindar dari masalah keamanan ini dan sementara itu juga untuk mengamankan sistemnya, banyak perusahaan tersebut telah menggunakan sistem dengan mengkombinasikan beberapa teknologi sistem keamanan, dimana hampir 69% nya menggunakan solusi dari *Intrusion Prevention System*[3].

Jaringan komputer pada Kantor Pengelola Data Elektronik atau KPDE Provinsi Jambi pada awalnya adalah jaringan yang menghubungkan beberapa perangkat komputer di lingkungan KPDE Provinsi jambi, namun seiring perkembangan dan berjalannya waktu, saat ini KPDE Provinsi Jambi menjadi jaringan utama *(backbone)* yang menghubungkan 46 instansi pemerintahan atau satuan kerja perangkat daerah (SKPD) provinsi jambi. Selain sebagai penyedia jaringan internet bagi instansi pemerintah, pada jaringan komputer KPDE provinsi jambi juga terdapat banyak komputer server dengan berbagai layanan yang berfungsi untuk mendukung kinerja instansi-instansi pemerintahan di provinsi jambi melalui aplikasi-aplikasi yang bisa diakses dari jaringan komputer baik intranet maupun internet.

Seiring berkembangnya jaringan komputer pada KPDE Provinsi Jambi, penerapan model sistem keamanan jaringan komputer sudah seharusnya menjadi fokus paling utama dikarenakan banyaknya layanan yang bersifat publik dengan resiko keamanan yang tinggi dan juga tidak adanya sistem keamanan yang dapat meminimalisasikan resiko keamanan pada data ataupun aplikasi di jaringan komputer tersebut. Hal ini dapat diketahui dari beberapa kali terjadi serangan pada aplikasi berbasis web di lingkungan KPDE Provinsi Jambi yang mengakibatkan perubahan tampilan informasi ataupun sampai dengan kehilangan data.

Dari uraian latar belakang penelitian, sehingga teridentifikasi masalah dalam penilitian ini sebagai berikut : 1) Perkembangan jaringan komputer serta layanan-layanan yang terdapat pada jaringan komputer di KPDE Provinsi Jambi yang begitu cepat sehingga membutuhkan rancangan model sistem keamanan yang dapat melindungi sumber daya pada jaringan tersebut; 2) Belum adanya sistem keamanan yang dapat mendeteksi dan mencegah penyusup pada jaringan komputer server KPDE Provinsi Jambi; 3) Terdapat jaringan komputer server pada KPDE Provinsi Jambi yang memiliki berbagai fungsi dan layanan yang dapat diakses baik dari jaringan intranet maupun internet sehingga menimbulkan resiko keamanan pada layanan tersebut.

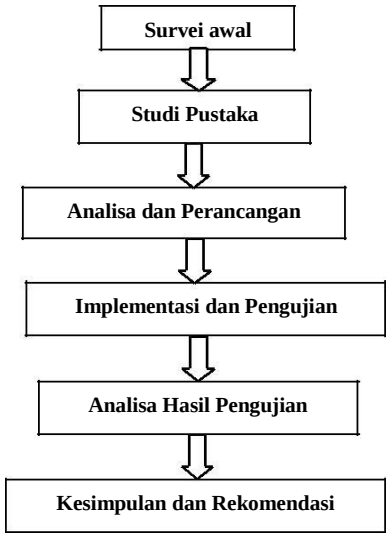
Dalam penelitian ini agar pembahasan dapat dilakukan secara terarah dan tercapai sesuai dengan harapan, sehingga dapat dirumuskan beberapa batasan masalah sebagai berikut : 1) Model sistem keamanan deteksi dan pencegahan penyusup dirancang untuk melindungi jaringan komputer server; 2) Keamanan yang dilindungi pada jaringan komputer server difokuskan pada serangan *port scanning* dan *SQL Injection*; 3) Pengujian sistem keamanan dilakukan dengan cara uji publik dengan metode *time space sampling.*

Tujuan penelitian ini adalah untuk membuat rancang model sistem keamanan jaringan sehingga dapat melindungi sumber daya jaringan komputer server yang terdapat pada jaringan komputer KPDE Provinsi Jambi. Sebagai bahan masukkan untuk KPDE Provinsi Jambi dalam penerapan sistem keamanan jaringan komputer.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Tahapan-tahapan penelitian dapat dideskripsikan sebagai berikut :



Gambar 1. Tahapan Penelitian

Penjelasan deskripsi langkah penelitian adalah :

1. Survei Awal
   Langkah ini bertujuan untuk mengetahui kondisi jaringan komputer yang ada saat ini. Survei awal merupakan salah satu metode pengumpulan data dengan teknik wawancara dan observasi pada *stakeholder* objek penelitian yang melibatkan antara lain Kepala Bagian Teknologi dan Jaringan beserta staf dan Kepala Bagian Aplikasi dan Pengembangan Sistem beserta staf untuk mengetahui kondisi awal jaringan komputer serta hal-hal lain terkait dengan permasalahan keamanan jaringan komputer server.
2. Studi Pustaka
   Pada tahap ini, peneliti melakukan studi pustaka yang berkaitan dengan Model Sistem Keamanan Jaringan Komputer. Studi pustaka dilakukan dengan mempelajari konsep Sistem Keamanan Jaringan, Teknik *de-militarized zone* dan *intrusion detection system*, *intrusion prevention system* serta aspek keamanan pada jaringan komputer.
3. Analisis dan Perancangan
   Setelah mengetahui kondisi lapangan dan melakukan studi pustaka, tahap selanjutnya adalah melakukan Analisis dan perancangan model sistem keamanan jaringan komputer. Berikut adalah tahapan Analisis yang akan dilakukan oleh penulis:
   a. Analisis topologi jaringan komputer.
      Pada tahap ini, penulis melakukan Analisis terkait topologi jaringan yang digunakan untuk mengetahui apakah topologi jaringan yang digunakan mendukung sistem keamanan pencegahan penyusup.
   b. Analisis jaringan komputer
      Pada tahap ini, penulis melakukan pengumpulan data-data terkait dengan jaringan komputer yang meliputi perangkat keras, perangkat lunak yang digunakan dan layanan-layanan yang disediakan pada jaringan komputer KPDE Provinsi Jambi baik layanan yang bersifat publik mauun private.

   Setelah melakukan Analisis, penulis melanjutkan pada tahapan perancangan. Berikut adalah tahapan perancangan yang penulis lakukan :
   a. Perancangan Model Topologi Jaringan Komputer. Pada tahap ini penulis melakukan perancangan topologi jaringan komputer yang mendukung sistem keamanan menggunakan teknik DMZ dan IPS.
   b. Perancangan DMZ Area
      Pada tahap ini, penulis melakukan perancangan untuk membuat area DMZ, dimana tahapan ini berhubungan dengan hasil Analisis perangkat keras dan layanan-layanan yang terdapat pada jaringan komputer, pada tahapan ini juga, penulis melakukan perancangan alamat IP yang nantinya digunakan untuk *area dmz.*

c. Perancangan IDS
   Pada tahap ini penulis melakukan perancangan sistem deteksi penyusup atau IDS menggunakan Sistem Operasi berbasis Linux dan menggunakan aplikasi *snort* sebagai *Intrusion Detection System*. Penulis juga mengatur dan menambahkan *rule-rule* yang nantinya akan digunakan oleh aplikasi *snort*. Perancangan IDS menggunakan database mysql dan didukung dengan antaramuka *snorby* untuk mempermudah pengolahan data.
d. Perancangan IPS
   Pada tahap ini, penulis mengAnalisis *alert* yang di hasilkan oleh *rule* sistem IDS yang tersimpan dalam database MySQL kemudian hasil Analisis ini menjadi masukkan untuk merancang IPS yang di implementasikan pada *firewall filter* di perangkat *router gateway* (mikrotik) menggunakan bahasa pemrograman *PHP*, *Linux Bash* serta MySQL *Trigger*.

4. Implementasi dan Pengujian
   Pada tahap ini, penulis fokus pada implementasi dan melakukan pengujian sistem keamanan jaringan. Pengujian akan dilakukan pada sisi pengguna jaringan dengan mencoba mengakses alamat-alamat tertentu pada jaringan server untuk melihat apakah sistem keamanan telah bekerja seperti yang diharapkan. Pada tahap pengujian, alat bantu yang digunakan penulis antara lain aplikasi *NMAP*, *Acunetix WebScanner*, *darkMySQLi*, *SQLmap* dan mengakses alamat-alamat yang di anggap mencurigakan oleh server IDS.
   Berikut adalah kondisi yang akan diuji oleh penulis :
   a. Kondisi sebelum menggunakan sistem keamanan.
      Penulis melakukan Analisis keamanan jaringan komputer dengan percobaan serangan seperti *SQL Injection* pada layanan berbasis Web dan melakukan aktivitas *port scanning* untuk mencari tahu port yang terbuka pada server-server yang ada.
   b. Kondisi setelah menggunakan sistem keamanan.
      Penulis melakukan pengujian melakukan serangan *SQL Injection* pada layanan berbasis Web dan melakukan aktivitas *port scanning* untuk mengetahui apakah sistem keamanan telah bekerja dengan baik.
5. Analisis Hasil Implementasi
   Pada tahap ini penulis mengAnalisis hasil implementasi yaitu apakah sistem mampu mendeteksi serangan serangan *SQL Injection* dan aktivitas port scanning. Selain itu Analisis hasil juga akan melakukan pengolahan data dari sisten yang telah di implementasikan dalam rentang waktu tertentu.
6. Kesimpulan dan Rekomendasi
   Pada tahap ini penulis mengambil kesimpulan dan memberikan rekomendasi terhadap sistem keamanan yang telah diimplementasikan.

3. PEMBAHASAN HASIL PENELITIAN

3.1 Analisis Sistem

Pada proses Analisis sistem, penulis mendeskripsikan hal-hal terkait kebutuhan sistem keamanan seperti Analisis topologi jaringan, perangkat jaringan, penggunaan IP address dan layanan-layanan yang terdapat pada jaringan komputer. Analisis sistem akan menjawab pertanyaan apa yang akan dikerjakan selanjutnya terkait dengan mekanisme sistem keamanan yang akan diterapkan serta *rule-rule* apa saja yang akan diterapkan pada sistem deteksi keamanan. Hasil Analisis ini akan divisualisasikan dan didokumentasikan dengan pertimbangan perubahan topologi jaringan yang mendukung sistem keamanan, perancangan DMZ area serta perancangan sistem deteksi dan pencegahan penyusup.

3.2 Analisis Keamanan Jaringan Komputer

1. Analisis keamanan jaringan komputer dilakukan untuk mengetahui celah keamanan pada jaringan komputer server. Analisis ini difokuskan pada serangan *port scanning* pada server-server dan *SQL Injection* pada aplikasi berbasis web. Pada proses Analisis keamanan jaringan komputer server, penulis menggunakan teknik wawancara dan *penetration testing*.
2. Pada proses wawancara, penulis mendapatkan informasi tentang insiden-insiden serangan yang pernah terjadi pada aplikasi berbasis web di jaringan komputer server KPDE Provinsi Jambi tahun selama 2014 sebagai berikut :

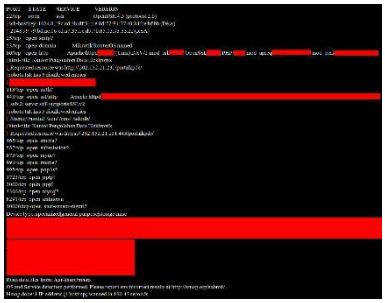
Tabel 1.
Data Serangan 2013-2014

TANGGAL	DOMAIN	SERANGAN
20-10-2013	jambiprov.go.id	Deface
22-12-2013	jambiprov.go.id	Deface
17-01-2014	e-office.jambiprov.go.id	SQL Injection (Internal audit)
14-03-2014	disbudpar.jambiprov.go.id	SQL Injection (Internal audit)
02-05-2014	dispora.jambiprov.go.id	SQL Injection (Internal audit)
01-08-2014	jdih.jambiprov.go.id	PHP Shell Injection

Untuk menganalisis celah keamanan *port scanning*, penulis menggunakan aplikasi bantu *nmap* atau *network mapping*. Penulis menggunakan perintah berikut pada terminal linux:

 # nmap –v –A jambiprov.go.id

Berikut adalah hasil *port scanning* menggunakan aplikasi *nmap* berbasis console :



Gambar 2. Analisis Port Scanning

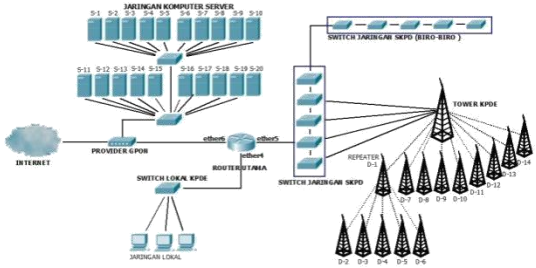
Berdasarkan gambar 2, terlihat informasi port yang terbuka beserta aplikasi yang menggunakan port tersebut di server milik provinsi jambi yang beralamat di jambiprov.go.id dengan alamat IP 202.152.X.231. Selain itu, penulis melakukan analisis teknik serangan *SQL Injection* dengan melakukan percobaan pada URL yang terdapat di domain dan subdomain jambiprov.go.id yang dipilih secara acak menggunakan aplikasi *acunetix web scanner vulnerability*. Berikut adalah hasil scan aplikasi *acunetix* yang menemukan beberapa kelemahan :

Gambar 3. Analisis Aplikasi Web

Domain yang penulis tujukan pada percobaan serangan Aplikasi Web adalah http://disbudpar.jambiprov.go.id, hasil dari scan aplikasi *acunetix* menampilkan bahwa terdapat 27 ancaman dengan tingkat tinggi (*high).*

3.3 Analisa Topologi dan Layanan

Analisis topologi jaringan komputer, dimana Analisis ini bertujuan untuk mengetahui apakah topologi jaringan komputer yang digunakan dapat mendukung model sistem keamanan yang akan di gunakan. Berikut adalah topologi jaringan komputer KPDE provinsi jambi.



Gambar 4. Topologi Jaringan

Pada gambar 4 dapat dilihat bahwa topologi jaringan komputer KPDE provinsi jambi menempatkan posisi jaringan *server* terhubung langsung ke jaringan internet melalui *switch*, dimana setiap *server* menggunakan alamat IP publik. Berikut adalah alokasi alamat IP yang digunakan oleh jaringan KPDE provinsi jambi :

Tabel 2.
Alokasi Alamat IP

Iface	Perangkat Jaringan	Alokasi Alamat IP
Ether4	Jaringan lokal KPDE	172.16.X.0/24
Ether5	Jaringan SKPD dengan kode D yang terdiri dari 46 SKPD	172.16.X.0/24
Jaringan Server	Komputer Server dengan kode S yang terdiri dari 20 server	202.152.X.224/27
Gpon	Gateway Internet	61.8.X.154/30

Berdasarkan Analisis topologi di gambar 4 dan alokasi alamat IP pada tabel 2 dapat diambil kesimpulan bahwa tidak ada parimeter yang memisahkan antara jaringan komputer server dan jaringan internet, sehingga hal ini menimbulkan resiko-resiko tersendiri karena tidak ada sistem keamanan yang melindungi jaringan komputer server baik dari jaringan internet maupun dari jaringan intranet. Pada tahap Analisis ini dapat diambil kesimpulan bahwa perlu adanya perubahan topologi jaringan dan alokasi alamat IP yang digunakan di KPDE provinsi jambi agar dapat mendukung model sistem keamanan jaringan komputer.

3.4 Analisa Layanan Jaringan

Analisis layanan jaringan komputer didasarkan pada hasil wawancara pada objek penelitian terkait dengan layanan apa saja yang ada pada jaringan komputer KPDE provinsi jambi. Tahapan Analisis layanan jaringan berguna untuk mengetahui aturan-aturan apa saja yang nantinya akan diterapkan pada model sistem keamanan deteksi dan pencegahan. Berdasarkan hasil wawancara yang telah dilakukan dapat disimpulkan sebagai berikut :

1. Penyedia layanan jaringan internet untuk SKPD di lingkungan provinsi jambi.
2. Terdapat layanan sistem informasi yang bersifat publik yang dapat diakses oleh masyarakan luas antara lain :
    a. Sistem Informasi Profil Satuan Kerja Perangkat Daerah berbasis web.
    b. Sistem Informasi Pengolahan data Online berbasis web.
3. Terdapat layanan yang bersifat private yang hanya bisa diakses oleh Satuan Kerja Perangkat Daerah se-Provinsi Jambi.
    a. Aplikasi Handkey
    b. Aplikasi CCTV
    c. Mail Server
    4. Berikut adalah daftar layanan web yang terdapat di KPDE Provinsi Jambi.

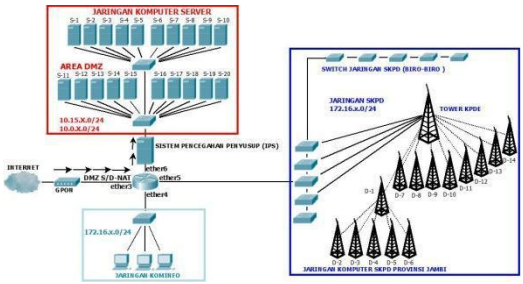
Tabel 3.
Daftar Layanan/Domain

DOMAIN/SUBDOMAIN	IP PUBLIK
Domain : jambiprov.go.id	202.152.X.231
Rekaplpse	202.152.X.231
Rsj	202.152.X.231
Repo	202.152.X.231

Snorby	202.152.X.231
Disbudpar	202.152.X.231
Sakip	202.152.X.231
Esdm	202.152.X.231
Bpmdppt	202.152.X.231
Biropem	202.152.X.231
Satpolpp	119.82.X.4
Bappeda	182.23.X.85
Dkp	202.152.X.231
Samisake	202.152.X.231
Jdih	202.152.X.231
Korpri	202.152.X.231
Pertambangan	202.152.X.231
Bpmpp	202.152.X.231
Ppls	202.152.X.231
Bkd	202.152.X.231
Bakorlu	202.152.X.231
Dispora	202.152.X.231
e-office	202.152.X.231
Lpse	202.152.X.227
lpse.meranginkab.go.id	202.152.X.230
Portalkpde	202.152.X.231
Handkey	202.152.X.231
Mail	202.152.X.226
ptsp1	202.152.X.231
Situationroom	202.152.X.231

3.5 Perancangan Topologi dan Model Sistem Demiliterized Zone

Pada tahapan perancangan model sistem keamanan, penulis menjelaskan tahapan-tahapan yang dilakukan dalam perancangan model sistem keamanan yaitu perancangan topologi jaringan yang mendukung *area dmz* dan model sistem keamanan deteksi serta pencegahan penyusup. Berikut adalah topologi yang di rancang :



Gambar 5. Perancangan Topologi Jaringan Komputer

Pada gambar 5 dapat dilihat penulis melakukan perubahan pada topologi jaringan komputer agar mendukung *area dmz* dimana antara jaringan server dan jaringan lainnya terdapat pemisah yaitu perangkat *router*. Sehingga perangkat *router* dapat mengatur layanan apa saja yang bisa diakses dari jaringan internet maupun jaringan intranet. Selain itu penulis juga menempatkan perangkat deteksi penyusup antara *router* dan jaringan komputer server agar dapat mengAnalisis dan mendeteksi lalu lintas jaringan yang dianggap mencurigakan. Setelah melakukan perancangan topologi jaringan yang mendukung *areaDMZ*, penulis melanjutkan dengan perancangan alamat IP seperti tabel 4 :

Tabel 4.
Alokasi Alamat IP DMZ

Interface	**Perangkat Jaringan**	**Alokasi Alamat**
Ether3	Gateway Internet	61.8.x.154/30
Ether4	Jaringan lokal KPDE	172.16.x.0/24
Ether5	Jaringan lokal SKPD	172.16.x.0/24
Ether6	Jaringan Komputer Server	10.15.X.0/24 10.0.X.0/24 202.152.x.224/27

Pada tabel 4 diatas, *router ether2* memiliki 3 alamat IP, dimana alamat IP 10.15.X.0/24, 10.0.X.0/24 digunakan untuk jaringan komputer server dan IP 202.152.X.224/27 digunakan untuk *area dmz* dengan menggunakan teknik *dst-nat* pada perangkat *router*berikut adalah tabel *dst-nat* yang akan di implementasikan pada *router* :

Tabel 5.
Tabel dst-nat

LAYANAN/WEB	DST-ADDRESS	DST-PORT	DST-ADDR	DST-PORT
jambiprov.go.id	202.152.X.231	22,80	10.0.X.2	22,80
rekaplpse	202.152.X.231	22,80	10.15.X.16	22,80
rsj	202.152.X.231	22,80	10.15.X.11	22,80
repo	202.152.X.231	22,80	10.15.X.12	22,80
snorby	202.152.X.231	22,80	10.15.X.3	22,80
disbudpar	202.152.X.231	22,80	10.0.X.2	22,80
sakip	202.152.X.231	22,80	10.0.X.2	22,80
esdm	202.152.X.231	22,80	10.0.X.2	22,80
bpmdppt	202.152.X.231	22,80	10.0.X.2	22,80
biropem	202.152.X.231	22,80	10.0.X.2	22,80
satpolpp	119.82.X.4	80	119.82.X.4	80
bappeda	182.23.X.85	80	182.23.X.85	80
dkp	202.152.X.231	22,80	10.0.X.2	22,80
samisake	202.152.X.231	22,80	10.0.X.2	22,80
jdih	202.152.X.231	22,80	10.0.X.2	22,80
korpri	202.152.X.231	22,80	10.0.X.2	22,80
pertambangan	202.152.X.231	22,80	10.0.X.2	22,80
bpmpp	202.152.X.231	22,80	10.0.X.2	22,80
ppls	202.152.X.231	22,80	10.0.X.2	22,80
bkd	202.152.X.231	22,80	10.0.X.2	22,80
bakorlu	202.152.X.231	22,80	10.0.X.2	22,80
dispora	202.152.X.231	22,80	10.0.X.2	22,80
e-office	202.152.X.231	22,80	10.0.X.4	22,80
lpse	202.152.X.227	22,80	10.15.X.15	22,80
lpse.meranginkab	202.152.X.230	22,80	10.0.X.10	22,80
portalkpde	202.152.X.231	22,80	10.0.X.3	22,80
handkey	202.152.X.231	22,80	10.0.X.6	22,80
mail	202.152.X.226	22, 25, 465, 587, 993, 995, 7071	10.0.X.7	22, 25, 465, 587, 993, 995, 7071
ptsp1	202.152.X.231	22,80	10.0.X.11	22,80
situationroom	202.152.X.231	22,80	10.0.X.12	22,80

Pada tabel 5 terdapat tabel *dst-nat*, *dst-nat* diimplementasikan pada perangkat *router* mikrotik dengan perintah sebagai berikut :

/ip firewall nat add chain=dstnat dst-port=dst-port dst-address=ip-publik action=dst-nat protocol=tcp to-address=ip-lokal to-port=dst-port

Contoh :

/ip firewall nat add chain=dstnat dst-port=80 dst-address=202.152.X.227 action=dst-nat protocol=tcp to-address=10.15.X.15 to-port=80

Perintah diatas akan mengarahkan semua koneksi di *router* dengan tujuan alamat IP 202.152.x.227 dan tujuan port 80 akan di arahkan ke alamat jaringan server lokal yaitu, 10.15.x.15 dengan tujuan *port* 80.

Dengan menggunakan mekanisme *dst-nat* diatas, port-port lain yang terbuka pada komputer server dapat terlindungi karena bila dilakukan proses scanning, port yang terbuka hanya port 80 karena *router* hanya akan mengarahkan atau melakukan *dst-nat* pada setiap paket yang memiliki tujuan port 80 sedangkan untuk port selain 80 maka akan mengarah pada perangkat router.

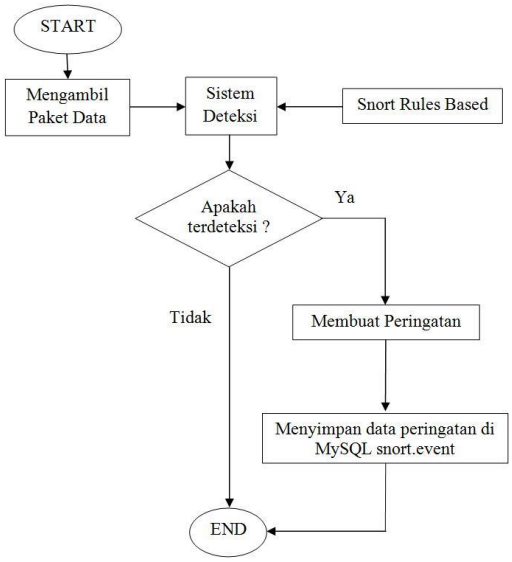
Selain menggunakan mekanisme *dst-nat*, pada tahap ini juga di rancang *firewall filter* pada *router gateway* untuk melakukan blok aktivitas *port scanning* yang dapat dilihat pada lampiran.

3.6 Perancangan Model Sistem Keamanan Deteksi

Pada tahap ini, penulis melakukan rancangan sistem keamanan yang dapat mendeteksi penyusup, perancangan sistem keamanan deteksi antara lain :

1. Instalasi sistem Operasi yang digunakan pada sistem deteksi penyusup adalah linux ubuntu server 12.04.4.
2. Instalasi aplikasi snort-mysql sebagai sistem deteksi penyusup
3. Instalasi aplikasi MySQL, PHP5 dan Apache2 sebagai aplikasi pendukung

Perancangan sistem keamanan deteksi dapat dijabarkan pada gambar berikut:



Gambar 6. Flowchart Sistem Deteksi Penyusup

Pada gambar 6 dapat dijelaskan bahwa IDS akan melakukan *capture* paket data di jaringan komputer, kemudian akan melakukan proses deteksi berdasarkan *rule based*, jika tidak terdeteksi maka proses berakhir dan jika paket terdeteksi maka IDS akan membuat *alert* yang selanjutnya akan disimpan pada database MySQL.

3.7 Perancangan Rules Based Snort

Tahapan perancangan *rules based* adalah dengan menambahkan dan memodifikasi *rules* yang terdapat pada aplikasi IDS, perancangan *rule-based* difokuskan pada *rules* untuk mendeteksi serangan *port scanning* dan *sql injection.*

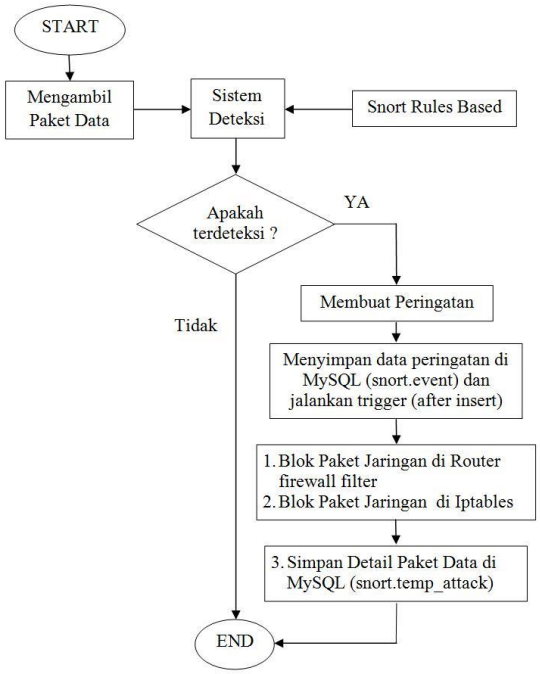
Berikut adalah *rule based* yang ditambahkan untuk mengantisipasi serangan *SQL injection*antar lain *:*

1. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN SQL Injection Single Quote"; flow:to_server,established;uricontent:"pl";pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;).
2. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN SQL Injection - Paranoid"; flow:to_server,established;uricontent:"pl";pcre:"/(\%27)|(\')|(\-\-)|(%23)|(#)/i"; classtype:Web-application-attack; sid:9099; rev:5;)
3. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN SQL Injection-Varchar"; flow:to_server,established;uricontent: "?";http_uri;content:"varchar";nocase; resp: rst_all; classtype:web-application-attack; sid:9990001; rev:1;)
4. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN SQL Injection-Concat"; flow:to_server,established;uricontent: "?";http_uri;content:"concat";nocase; resp: rst_all; classtype:web-application-attack; sid:9990001; rev:1;)
5. alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SCAN SQL Injection-Declare"; flow:to_server,established;uricontent: "?";http_uri;content:"declare";nocase; resp: rst_all; classtype:web-application-attack; sid:9990002; rev:1;)

Pada tahap perancangan model sistem keamanan pencegahan penyusup, penulis mengimplementasikan pencegahan menggunakan aplikasi *iptables* dan *firewall filter* yang terdapat pada perangkat *router*. Berikut langkah-langkah perancangan sistem keamanan pencegahan :

1. Sinkronisasi ssh key server IDS dan router mikrotik
2. Instalasi library lib_mysqludf
3. Perancangan trigger
4. Perancangan iptables
5. Perancangan router firewall filter

Penulis memanfaatkan *trigger* pada tabel *snort.event* untuk menjalankan kode-kode program yang akan melakukan pemeriksaan dan pencegahan. Berikut adalah *flowchart* sistem pencegahan penyusup yang digunakan.



Gambar 7. Flowchart Sistem Pencegahan Penyusup

Penjelasan gambar 7 yaitu jika paket data jaringan terdeteksi, IDS akan mengirimkan *alert* ke database mysql yaitu pada tabel *event*. Kemudian, setelah *alert* disimpan pada tabel *event*, terdapat trigger yang menjalankan file script php dan bash shell linux. Trigger yang dijalan yaitu :

```
DELIMITER @@
CREATE TRIGGER tg1
AFTER INSERT ON event
FOR EACH ROW
BEGIN
 DECLARE cmd CHAR(255);
 DECLARE result int(10);
 SET cmd=CONCAT("/usr/bin/php /home/ips/cmd.php >> /home/ips/log.txt");
 SET result = sys_exec(cmd);
 SET cmd=CONCAT("/bin/bash /home/ips/ipt.sh >>
 /home/ips/log.txt"); SET result = sys_exec(cmd);
 END;
@@
DELIMITER ;
```

Trigger MySQL diatas menjalankan *scriptcmd.php* yang bisa dilihat di lampiran, dimana *script cmd.php* ini akan mengambil *source address* dari paket data yang telah dideteksi, lalu *source address* tersebut akan ditulis ke file *iptables-blocklist.txt* di folder /home/ips/ untuk kemudian diproses ke *firewall filteriptables*, selain itu *scriptphp* juga akan mengirim *source address* paket data ke perangkat *router mikrotik* dan dimasukkan di *address-list* dengan nama "*attacker*" kemudian router akan melakukan *filter drop* berdasarkan *address-list* dengan nama *attacker*. Pada *script shell linux* dengan nama *ipt.sh* akan menjalankan perintah *iptables* untuk melakukan *DROP* berdasarkan alamat yang terdapat di

/home/ips/iptables-blocklist.txt dengan perintah yang bisa dilihat di lampiran dan terakhir script *cmd.php* akan menyimpan log serangan di tabel *temp_attack* sebagai log. Semua *source address* yang di *drop* akan di reset dalam waktu 24 jam.

3.8 Hasil Penelitian dan Pembahasan

Proses pengujian sistem keamanan jaringan menggunakan metode *blackbox testing* untuk menguji sistem secara fungsionalitas yaitu dengan melakukan serangan pada server maupun aplikasi berbasis di jaringan komputer server. Teknik pengujian *blackbox* juga dilakukan dengan memberikan satu set kondisi masukkan untuk menguji seluruh kebutuhan dari sistem keamanan yang telah dibangun. Skenario pengujian *blackbox* testing dilakukan dengan 2 cara yaitu

4. Testing *Port Scanner* menggunakan aplikasi *nmap.*
5. Testing *SQL Injection* menggunakan dengan Querystring dan aplikasi *acunetix web scanner*.

3.9 Port Scanning

Pengujian serangan *port scanning* dilakukan menggunakan aplikasi *nmap*. Berikut adalah hasil pengujian model sistem keamanan deteksi dan pencegahan penyusup untuk serangan port scanning :

Tabel 6.
Pengujian Port Scanning

U SE CASE	**P ORT SCANNING**
Skenario	Pengujian dilakukan dengan aplikasi nmap melalui jaringan internet.
Data Uji	1. Port Scanning teknik TCP Connect Scan 2. Port Scan teknik TCP NULL 3. Port Scan UDP Scan 4. Port Scan teknik All Scan
Host yang di Uji	1. jambiprov.go.id 2. lpse.jambiprov.go.id
Hasil yang diharapkan	1. Host Down 2. Port Close 3. Ping Request Time Out
Hasil Pengujian	Dari ke 3 data yang diuji untuk 2 host, sistem memberikan respon yang sesuai dengan hasil yang diharapkan [lihat lampiran scan attack].

Berdasarkan pengujian pada tabel 6 dapat diketahui bahwa sistem pencegahan mampu bekerja melakukan blok terhadap serangan port scanning.

3.10 SQL Injection

Tahap pengujian selanjutnya yaitu dengan pecobaan serangan *SQL Injection*, yaitu dengan menambahkan karakter-karakter khususpada URL yang terdapat di aplikasi web pada jaringan server.

Tabel 7.
Pengujian SQL Injection

NAMA *USE CASE*	**PORT SCANNING**
Skenario	Pengujian dilakukan dengan menambahkan karakter single quotes („) pada url di aplikasi web.
Data Uji	1. http://jambiprov.go.id/index.php?art-detail=2'and1=1--„ 2. http://jambiprov.go.id/index.php?bandara"or1=1"-- 3. http://dispora.jambiprov.go.id/index.php?page-news=2'and1=1--„
Host yang di Uji	1. http://jambiprov.go.id 2. http://dispora.jambiprov.go.id/
Hasil yang diharapkan	1. Browser menampilkan *this webpage is not available* 2. Ping Host memberikan balasan Request Time Out
Hasil Pengujian	Dari ke 3 data yang diuji, sistem memberikan respon yang sesuai dengan hasil yang diharapkan [lihat lampiran SQLi Attack]

Berdasarkan data di tabel 7 dapat dilihat bahwa sistem pencegahan telah bekerja dan mampu mengantisipasi serangan *SQL Injection.*

3.11 Pengujian Non-Fungsional

Proses pengujian non-fungsional yang dimaksud adalah untuk mengukur kecepatan transfer antara jaringan komputer server dan jaringan komputer lokal sehingga didapat kesimpulan apakah implementasi sistem keamanan berpengaruh pada kecepatan akses di jaringan server. Pengujian ini dilakukan dengan cara melakukan pengiriman data antara jaringan komputer server dan jaringan komputer lokal seperti yang di tunjukkan pada tabel berikut :

Tabel 8.
Pengujian Kinerja IDS

IP SRC	SERVER TUJUAN	MAKS. KECEPATAN	HASIL
172.16.251.12	jambiprov.go.id	100-1000Mbps	923Mbps
172.16.251.12	rekaplpse.jambiprov.go.id	100-1000Mbps	924Mbps
172.16.250.12	jambiprov.go.id	100-1000Mbps	922Mbps
172.16.250.12	rekaplpse.jambiprov.go.id	100-1000Mbps	910Mbps

Berdasarkan data di tabel 8 dapat disimpulkan bahwa implementasi sistem pencegahan tidak mempengaruhi kecepatan transfer data karena masih dalam rata-rata kecepatan 919Mbps.

3.12 Hasil Pengujian dan Evaluasi

Dalam penelitian ini, hasil pengujian dan evaluasi model sistem keamanan pencegah penyusup dilakukan dengan metode clustering atau pengelompokkan data, pengelompokkan data dilakukan berdasarkan lokasi, waktu dan teknik serangan. Sampel data didapat setelah model sistem keamanan deteksi dan pencegahan penyusup diimplementasikan selama 61 hari.

3.13 Hasil Sampling Data

Data yang didapat dari sistem keamanan pencegahan dimulai dari tanggal 26 juni 2014 sampai 26 agustus 2014.

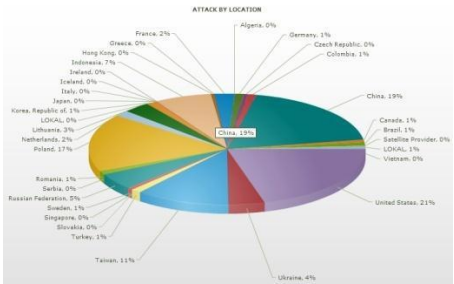
Tabel 9.
Data 26 juni 2014 - 26 agustus 2014

BULAN	JUMLAH DATA
26 Juni 2014	1038
Juli 2014	5854
26 Agustus 2014	3823
RATA-RATA DATA SETIAP BULANNYA 3572 dari 10715	

Berdasarkan data di tabel 9 dapat dilihat bahwa total data yang diterima selama 61 hari sebanyak 10715 data.

3.14 Location Clustering

Proses selanjutnya adalah mengolah data yang didapat selama 61 hari. Pada metode *location clustering*, pengelompokkan data dilakukan berdasarkan IP sumber serangan yaitu dalam bentuk lokasi negara.



Gambar 8. Grafik Serangan Berdasarkan Lokasi

Hasil sampling data diatas di kemudian di persempit seperti pada tabel berikut :

Tabel 10.
Data Lokasi Serangan

SUMBER SERANGAN	JUMLAH SERANGAN
China	**2115 (19.7%)**
United States	**2104 (19.6%)**
Poland	1504 (14%)
Taiwan	1274 (11.9%)
Indonesia	813 (7.6%)

Berdasarkan data di tabel 10 dapat di lihat bahwa serangan paling banyak berasal dari negara China dan United States.

3.15 Time Clustering

Selanjutnya *time clustering* yaitu pengelompokkan data berdasarkan waktu serangan itu terjadi. Pengelompokkan dibagi menjadi 3 yaitu

c. Jam 08:00:00 – 16:59:00
d. Jam 17:00:00 – 23:59:00
e. Jam 00:00:00 – 07:59:00

Tabel 11.
Data Serangan dari Jam 08:00:00 – 16:59:00

WAKTU SERANGAN	JUMLAH SERANGAN
08:23:28	666
09:00:10	530
10:05:24	553
11:02:54	620
12:13:55	489
13:18:33	303
14:15:49	961
15:14:27	583
16:34:30	577
TOTAL SERANGAN 5282	

Tabel 12.
Data Serangan dari Jam 17:00:00 – 23:59:00

WAKTU SERANGAN	JUMLAH SERANGAN
17:01:12	566
18:02:47	428
19:32:10	315
20:03:32	418
21:06:22	324
22:23:53	371
23:18:25	170
TOTAL SERANGAN 2592	

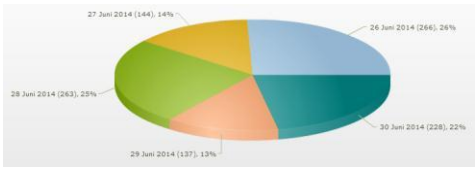
Tabel 13.
Data Serangan dari Jam 00:00:00 – 07:59:00

NO	WAKTU SERANGAN	JUMLAH SERANGAN
1	00:18:46	101
2	01:53:59	82
3	02:24:46	190
4	03:01:09	143
5	04:27:44	128
6	05:43:18	384
7	06:42:36	947
8	07:16:25	866
TOTAL SERANGAN 2841		

Berdasarkan data di tabel 11,12 dan 13, maka dapat diambil kesimpulan bahwa jumlah serangan paling banyak terjadi di jam **08:00:00 – 16:59:00** yaitu dengan total serangan **5282**.

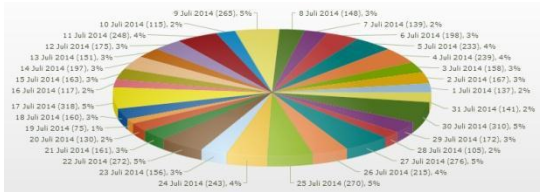
Bila dilihat serangan berdasarkan lokasi dan berdasarkan waktu serangan maka dapat diambil kesimpulan bahwa serangan paling banyak berasal dari negara US dan china dimana 2 negara ini adalah negara penghasil spam paling banyak (kaspersky, 2013).

Pengelompokkan data selanjutnya yaitu pengelompokkan data perhari dalam setiap bulannya. Hal ini dilakukan untuk mendapatkan rata-rata serangan setiap harinya.



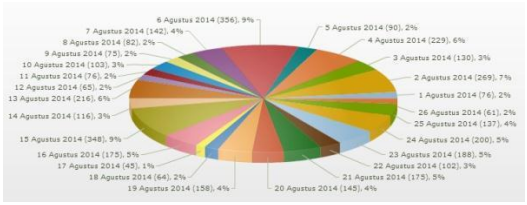
Gambar 9. Data serangan bulan juni

Berdasarkan data di tabel 9 dapat diambil kesimpulan bahwa rata-rata serangan di 5 hari terakhir bulan juni sebanyak 208 serangan.



Gambar 10. Data serangan bulan juli

Berdasarkan data di tabel 10 dapat diambil kesimpulan bahwa rata-rata serangan perhari selama bulan juli terjadi sebanyak 189 serangan.



Gambar 11. Data serangan bulan agustus

Berdasarkan data di tabel 11 dapat diambil kesimpulan bahwa rata-rata perhari serangan selama bulan agustus terjadi sebanyak 147 serangan.

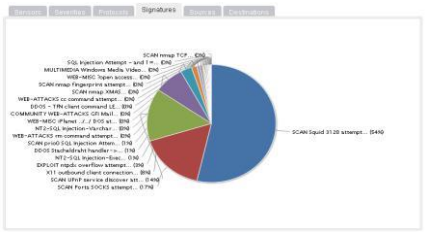
Tabel 14.
Rata-rata serangan perhari

Bulan	Rata-Rata Serangan Perhari
Juni	208
Juli	189
Agustus	147

Dengan menggabungkan data selama 61 hari dalam setiap bulannya dapat di ambil kesimpulan bahwa setiap harinya terjadi rata-rata 181 serangan.

3.16 Technique Clustering

Selain berdasarkan rentang waktu, pengelompokkan data juga dilakukan dengan mengelompokkan serangan berdasarkan teknik serangan atau *technique clustering*:



Gambar 12. Grafik berdasarkan teknik serangan

Gambar 12 menunjukkan grafik teknik serangan yang paling banyak digunakan adalah Scan ada port 3128 atau port proxy server.

3.17 Hasil Kinerja Sistem Pencegahan

Kemampuan kinerja sistem pencegahan penyusup diukur dengan :

δ = d/n

d = jumlah serangan yang mampu di blok

n = jumlah serangan yang berhasil dideteksi

δ = 797/825* 100

Kinerja sistem pencegahan penyusup dapat disimpulkan mampu melakukan pencegahan mencapai **96%**.

4. PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan hasil penelitian yang telah dibahas di bab sebelumnya maka dalam penelitian Rancang Model Sistem Keamanan Jaringan Komputer menggunakan *Intrusion Prevention System* dengan *Metode rule based* : studi kasus KPDE Provinsi Jambi dapat diambil kesimpulan sebagi berikut :

c. Rancang model sistem keamanan telah sesuai menggunakan metode rules based.
d. Rancang Model Sistem Keamanan dapat bekerja dengan baik dalam melindungi jaringan komputer server dari serangan Port Scanning dan SQL Injection.
e. Pengujian kinerja sistem pencegahan menunjukkan nilai yang baik
f. Rancang model sistem keamanan pencegahan penyusup dapat digunakan untuk mencegah ataupun meminimalisir serangan terhadap layanan-layanan yang terdapat di jaringan komputer server KPDE Provinsi Jambi.

4.2. Saran

Berdasarkan hasil penelitian, implikasi dan kesimpulan, selanjutnya peneliti dapat memberikan beberapa saran yang relevan dengan hasil penelitian. Saran ini berupa masukan-masukan yang ditujukan ke organisasi/obyek penelitian dan untuk penelitian selanjutnya.

2 Diperlukan kajian lebih lanjut dalam implementasi rule SQL Injection karena beberapa akses normal ke aplikasi berbasis web tidak bisa dilakukan dikarenakan URL mengandung kata-kata yang di blok oleh sistem keamanan.
3 Diperlukan update *rules based* secara berkala.

DAFTAR PUSTAKA

1. Alamsyah. “Implementasi Keamanan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) menggunakan CLEAROS”. Jurnal SMARTek, Vol.9 No.3. (Agustus, 2011) : 224-229.
2. Cisco “Network Address Translation (NAT) FAQ”. 2013. http://www.cisco.com (Diakses 10 Mei
3. 2014).
4. Deris Stiawan. “Intrusion Prevention System (IPS) Tantangan dalam Pengembangannya”. Artikel.
5. Fasilkom, Universitas Sriwijaya,2012.
6. Dony Ariyus “Intrusion Detection System Sistem Pendeteksi Penyusup pada Jaringan Komputer”.
7. Yogyakarta : andi. 2007
8. Highsec.es “Topologi IPS”. 2012.http://highsec.es(Diakses 10 Mei 2014).
9. Howtonetwork.net "Topologi IPS". 2012. http:// howtonetwork.net (Diakses 10 Mei 2014).
10. K.K, Mookhey and Burghate, Nilesh. “*Detection of SQL Injection and Cross-site Scripting Attacks*”. 2010. http://www.symantec.com. (Diakses 10 Mei 2014).
11. Narrang, Pratik "Snort's Architecture". 2012. Mailing List Archive". http://seclists.org (Diakses 10 Mei 2014).
12. Nurinda Saumananda Suroso. "Verifikasi Prediksi Hujan dengan Observasi Berbasis Masyarakat Aplikasi Android". Jurnal,. Institut Teknologi Bandung, 2013.

13. Owasp.org "SQL Injection". 2014. https://www.owasp.org/index.php/SQL_Injection (Diakses 10 Mei 2014).
14. Passeri Paolo "September 2012 Cyber Attacks Statistics". 2012. http://hackmageddon.com/ (Diakses 10 Mei 2014).
15. Patel, Nishid D, et.al., "An analysis of Network Intrusion Detection System using SNORT". International Journal for Scientific Research & Development, Vol. 1, Issue 3, 2013.
16. Powerbiz.net.au "dst-nat". 2010.http://powerbiz.net.au(Diakses 10 Mei 2014).
17. Seclist.org "Arsitektur Snort". http://seclist.org (Diakses 10 Mei 2014).
18. Sukirmanto. "Rancang Bangun dan Implementasi Keamanan Jaringan komputer menggunakan metode Intrusion Detection System (IDS) pada SMP islam terpadi PAPB". Skripsi. Universitas Semarang. 2004.
19. Satria Muhammad Nugraha. "Implementasi Intrusion Detection System untuk Filtering Paket Data (Studi Kasus : Yayasan Pembinaan Pendidikan Nusantara)". Skripsi,. Universitas Islam Negeri Syarif Hidayatullah, 2010.
20. Tech-faq.com "Topologi DMZ". 2012. http://tech-faq.com (Diakses 10 Mei 2014).
21. Wikipedia "Keamanan Komputer". 2014. http://id.wikipedia.org (Diakses 10 Mei 2014).
22. Wiki.mikrotik.com "Network Security". 2010. http://wiki.mikrotik.com (Diakses 10 Mei 2014).
23. Yoga Nurjaman, et.al., "Pengembangan Sistem Remote Access Jaringan Berbasisclient". Jurnal Algorithma, Vol.9, (2012).