PERANCANGAN KEAMANAN JARINGAN KOMPUTER PADA *LAYER APPLICATION* BERBASIS *INTRUSION PREVENTION SYSTEM* (IPS) YANG DI INTEGRASIKAN DENGAN *ACCESS CONTROL LIST* (ACLs) (Studi Kasus : Politeknik TEDC Bandung)

Dahlan
Teknik Komputer Politeknik TEDC Bandung
Email: dahlantea.1976@gmail.com

Abstrak

Jaringan Komputer yang ada di Politeknik TEDC antar departemen satu dengan departemen yang lain saling terhubung dalam jaringan Lokal Area Network, untuk membagi segmentasi jaringan berdasar pada fungsi, project team, atau aplikasi organisasi dengan mengabaikan penempatan fisik atau koneksi ke jaringan, oleh karena itu perlu di buatkan *workgroup* sesuai dengan departemen. User yang terhubung dalam jaringan tersebut tentunya berkesempatan untuk mengakses ke sumber daya padahal sebagian user tidak diperbolehkan karena tidak mempunyai kepentingan terhadap sumber daya tersebut. Untuk menseleksi user yang boleh akses (*permit*) atau di tolak (*deny*) pada akses ke sumber daya tentunya di perlukan penangan lebih selektif terhadap permintaan user. Begitu juga dalam melakukan pencegahan dini terhadap penyusup yang dapat merusak sebuah *system* maka di perlukan penanganan, agar *system* jaringan akan selalu terjaga dari penyusup dan aplikasi-aplikasi yang mencurigakan.Untuk melakukan pembagian segmentasi jaringan di Politeknik TEDC di buatkan *Virtual Local Area Network (* VLAN *)* yang secara logika membagi jaringan ke dalam *broadcast domain* berbeda sehingga paket *switch* antara port yang ditunjuk untuk VLAN yang sama. VLAN diciptakan untuk menyediakan layanan segmentasi biasa yang diberikan oleh router fisik dalam konfigurasi LAN. Router pada topologi VLAN menyediakan penyaringan broadcast, keamanan, mengatur alur lalu lintas dan mengatur Otorisasi terhadap *user* dengan menerapkan konsep *Access Control List (ACLs)* yang dapat di konfigurasi pada router. Sedangkan *Intrution Prevention System* (IPS) yan g di terapkan pada *Server* dengan mengunakan *Snort* sebagi *tools* nya dan Acid-MySQL sebagai *Database* Snort, bertujuan untuk mencegah jika adanya penyusup atau aplikasi yang mencurigakan. Sehingga dengan adanya perancangan keamanan jaringan komputer yang *berbasis Intrution Prevention System* dan dengan *Access Contrlol List* (ACLs) yang di terapkan di Politeknik TEDC di harapkan dapat mengamankan jaringan komputer dengan mendeteksi secara dini jika adanya *intruder* yang akan merusak pada sistem jaringan dan juga dapat mengatur otorisasi terhadap *user* yang mengakses sumber daya dalam segmentasi jaringan .

Kata kunci: VLAN, ACLs, IPS, Snort, Acid-MySQL , Keamanan Jaringan

Abstrack

Computer Networks in the TEDC Polytechnic between departments one with interconnected departments within the Local Area Network , to divide network segmentation based on function, project team, or organizational application with physical access or connection to the network, therefore need to make workgroup appropriate with the department. Users who are connected in the network of course the opportunity to access to the resources of some users are not allowed because it has no interest in those resources. To select users who may have access (permission) or deny access to resources of course need more selective handling of user requests. So also in doing early prevention of intruders that can damage a system then in need awake, so that the system will always be awake from the intruder and suspicious applications. To divide network segmentation at TEDC Polytechnic, create a Virtual Local Area Network (VLAN) that logically connects into different broadcast domains with switch packets between ports designated for the same VLAN. VLANs are created to provide the usual segmentation services provided by physical routers in LAN configuration. Routers in VLAN topologies provide broadcast filtering, security, workflow manage and access. Access Control Lists (ACLs) that can be configured on the router. While the Intrution Prevention System (IPS) is applied to the Server by using Snort as its tool and Acid-MySQL as the Snort Database, the option to prevent any intruders or suspicious applications. With the design of network security based on Intrution Prevention System and with Access Contrlol List (ACLs) which applied in TEDC Polytechnic in can can computer network with early if there is intruder that will damage on network system and also can arrange authorization to user access in network segmentation.

Keywords: *VLAN, ACL, IPS, Snort, Asam-MySQL, Network Security*

I. PENDAHULUAN

Jaringan komputer bukanlah sesuatu yang baru saat ini. Hampir di setiap perusahaan/institusi termasuk di Politeknik TEDC Bandung terdapat jaringan komputer, Di Politeknik TEDC Bandung seluruh departemen terhubung dalam satu jaringan Lokal Area yang dapat mengakses sumber daya baik lewat jaringan lokal maupun Internet. Tidak adanya pemisah segmentasi menimbulkan sulitnya melakukan pengontrolan terhadap seluruh user.

Protocol Application Layer digunakan untuk pertukaran data antara program yang berjalan pada source dan host tujuan. Dengan kata lain, application layer berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses dalam sebuah jaringan, tentunya perlu dilakukan pengamanan.

Untuk mempermudah pengontrolan user agar sesuai dengan fungsinya, maka di Politeknik TEDC Bandung perlu di buatkan segmentasi dengan menerapkan access control list sebagai pengatur hak akses dan *intrusion prevention system* merupakan system pengamanan terhadap alplikasi-aplikasi yang mencurigakan yang dilakukan melaui *application layer.*

II. LANDASAN TEORI

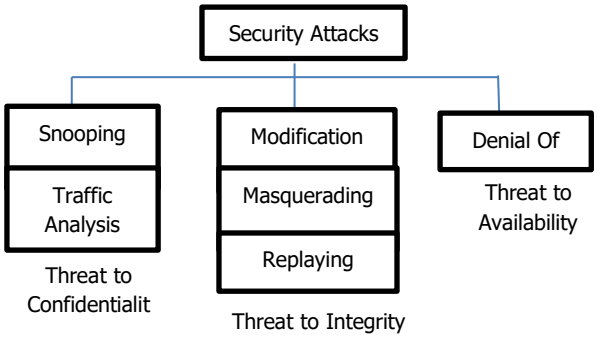
Perancangan adalah penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi perancangan sistem dapat dirancang dalam bentuk bagan alir sistem (*system flowchart*), yang merupakan alat bentuk grafik yang dapat digunakan untuk menunjukan urutan-urutan proses dari sistem (Nafisah, 2003 : 2)

Prinsip Keamanan Jaringan

Behrouz, 2010 menyatakan bahwa keamanan jaringan komputer akan tercapai apabila memenuhi 3 kreteria sebagai berikut :

1. ***Confidentiality*** : merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan infromasi yang diberikan kepada pihak lain.
2. ***Integrity*** : keaslian pesan yang dikirim melalui sebuah jaringan dan dapat di pastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalan pengiriman informasi tersebut.
3. ***Availability*** : aspek *availability* atau ketersediaan berhubungan dengan ketersedian informasi ketika dibutuhkan. Sistem informasi yang di sekarang atau di bobol dapat menghambat atau meniadakan akses ke informaihatsi.

Seperti yang terlihat pada gambar 2.1 relasi dibawah ini, memperlihatkan bahwa setiap ancaman yang akan terjadi pada CIA merupakan hal yang perlu penanganan agar ketercapain keamanan pada sebuah jaringan komputer dapat di realisasikan.



Gambar 1. Relasi untuk mencapai sebuah keamanan jaringan
(Sumber : Behrouz, 2010)

Jenis – Jenis Serangan

Menurut Taufik Wicaksosno (UI) , dalam Tesisnya Rancang Bangun dan Implementasi IDS/IPS pada server untuk meningkatkan keamanan jaringan mengatakan bahwa : ancaman dan serangan yang terjadi dalam sistem jaringan komputer beraneka ragam, ada beberapa contoh serangan yang sering terjadi di jaringan komputer antara lain :

A. ***Back Office*** **(BO) :** adalah sebuah alat bantu remote administrasi komputer jarak jauh yang dapat digunakan untuk mengontrol sistem operasi Microsoft Windows. Meskipun pada dasarnya alat bantu ini merupakan salah satu bentuk Trojan Horse, yang dapat digunakan untuk mendapatkan hak akses dan kontrol penuh terhadap target, program ini menawarkan banyak fitur khususnya untuk mengendalikan operasi Windows NT. Tampilan yang digunakan sangatlah mudah dan sangat sederhana, sehingga para peretas pemula pun dapat menggunakannya.

B. *Denial of Service* (DoS) : adalah serangan terhadap komputer server didalam jaringan internet dengan cara menghabiskan resource, yang dimiliki komputer tersebut sampai komputer tersebut tidak dapat menjalakan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk mendapatkan akses layanan dari komputer yang diserang tersebut. Dalam sebuah serangan *Denial of Service*, penyerang akan mencoba mencegah hak akses seorang pengguna terhadap sistem jaringan dengan menggunakan beberapa cara diantaranya :
   - Membanjiri lalulintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang ari pengguna yang sah/terdaftar menjadi tidak dapat mengakses ke sistem jaringan. Teknik ini disebut teknik *Traffic Flooding.*
   - Membanjiri jaringan dengan banyak reques terhadap sebuah layanan jaringan yang disediakan oleh sebuah *client* sehingga *request* yang datang dari penguna yang sah/ terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik tersebut disebut *Request Flooding.*

C. ***Port Scaning*** **:** Merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan komputer. Dari hasil scaning akan didapat letak kelemahan sistem tersebut. Pada dasarnya *port scaning* mudah di diteksi, tetapi metode penyerangan akan melakukan penyerangan dengan menyembunyikan serangan tersebut.

D. ***Teardrop :*** Merupakan suatu teknik yang dikembangakan dengan mengekploitasi proses *assembly – reassembly* paket data.

E. ***IP- Spooping*** : Adalah suatu teknik serangan yang rumit yang terdiri dari beberapa komponen. Ini adalah ekploitasi keamanan yang bekerja dengan menipu komputer, seolah – olah yang menggunakan komputer tersebut adalah orang lain. Hal ini terjadi karena *design flow* (salah rancang). Lubang keamanan yang dapat dikatagorikan kedalam sebuah kesalahan design urutan nomor *sequense numbering* dari paket TCP/IP.

F. ***Smurf Attack*** *:* Serangan jenis ini biasanya dilakukan dengan menggukan *IP Spoofing,* yaitu merubah nomor IP dari datangnya *reques*. Dengan menggunakan *IP Spoofing,* respon tadi dialamatkan ke komputer yang IP nya di Spoof, akibatnya komputer tersebut akan menerima banyak paket sehingga dapat menyebabkan boros *Bandwith*

G. ***UDP Flood :*** Pada dasarnya mengkaitkan dua buah sistem tanpa disadari. Dengan cara s*poofing* , *User Datagram Protocol* (UDP) *flood attack* akan menempel pada service UDP *chargen* disalah satu mesin yang digunakan untuk keperluan "percobaan" akan mengiriman sekolompok karakter ke mesin lain, yang di program untuk mengreques setiap kiriman karakter yang diterima melalaui *service chargen.* Karena paket UDP itu di *Spoofing* diantara kedua mesin tersebut maka yang terjadi adalah banjir karakter tersebut tanpa henti.

H. ***ICMP Flood :*** Seorang penyerang akan mengekploitasi sistem tujuan dengan maksud untuk sutu target *client* menjadi *crash,* yang disebabkan oleh pengirman sejumlah paket yan cukup besar kearah target *client.*

Untuk mencapai tujuan keamanan jaringan tersebut di atas maka di butuhkan sebuah metode yang dapat melindungi sistem dari ancaman internal maupun eksternal. Salah satu metode tersebut adalah *Intrusion Prevention System* (IPS) yang diintegrasiskan dengan *Access Control List* (ACLs).

Intrusion Preventation System (IPS)

Dwi Kuswanto, 2014: "unjuk kerja *intrusion prevention system* (IPS) berbasis *sucirata* pada jaringan lokal area *network", Intrusion Preventing System* (IPS) merupakan jenis metode pengamanan jaringan baik software atau hardware yang dapat memonitor aktivitas yang tidak diinginkan atau intrusion dengan cara melihat konten aplikasi yang dapat langsung bereaksi untuk untuk mencegah aktivitas tersebut. IPS merupakan pengembangan dari IDS. Sebagai pengembangann dari teknologi *firewall*, IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan port atau IP *address* seperti *firewall* umumnya. IDS Selain dapat memantau dan monitoring, IPS dapat juga mengambil kebijakan dengan memblok paket yang lewat dengan cara "melapor" ke *firewall*. Metode IPS untuk melakukan seleksi apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut yakni *Signature-based Detection System*

dan *Anomaly-based Intrusion Detection System*. IPS merupakan pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, IPS mengombinasikan teknik *firewall* dan metode *intrusion detection system* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk kejaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi. Jadi IPS bertidak seperti layaknya *firewall* yang akan mengizinkan atau menghalangi paket data (Alder, 2007).

Secara khusus, IPS memiliki empat komponen utama, yaitu:

1. *Normalisasi traffic* : menginterpretasikan *traffic* jaringan dan melakukan analisa terhadap paket yang disusun kembali, seperti halnya fungsi *block* sederhana.
2. *Detection engine* : mendeteksi *traffic* jaringan dan melakukan *pattern matching* terhadap tabel acuan dan respon yang sesuai.
3. *Service scanner* : membangun suatu tabel acuan untuk mengelompokkan informasi.
4. *Traffic shaper* : membentuk dan mengatur *traffic* jaringan pada *bandwith*.

Definisi dan Konsep Snort

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara real time traffic dan logging ke dalam database serta mampu mendereksi berbagai serangan yang berasal dari luar jaringan (Ariyus, 2007: 45) Snort bisa digunakan pada platform sistem operasi Linux. BSD, solaris, Windows, dan sistem operasi lainnya.

Snort sudah di-download lebih dari 3 juta orang. Hal ini menandakan bahwa snort merupakan suatu intrusion detection system yang dipakai banyak orang di dunia. Snort bisa di operasikan dengan tiga mode (Ariyus, 2007:146) yaitu:

a. Paket *Sniffer*: Untuk melihat paket yang lewat di jaringan.
b. Paket *logger*: Untuk mencatat semua paket yang lewat di jaringan untuk dianalisis di kemudian hari.
c. NIDS deteksi penyusup pada network: Pada mode ini soon akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

III. METODE PENELITIAN

Action research menurut Davison, Martinsons dan Knock (2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu :

a. Tahap pertama *(Diagnosing)*
Melakukan identifikasi masalah-masalah pokok yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan. Peneliti melakukan diagnosa terhadap infrastruktur jaringan komputer di Politeknik TEDC Bandung

b. Tahap kedua *(Action Planning)*
Peneliti memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat. Pada tahap ini peneliti melakukan rencana tindakan yang akan dilakukan pada jaringan dengan membuat Perancangan Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

c. Tahap ketiga *(Action Taking)*
Peneliti melakukan tindakan disertai dengan implementasi rencana yang telah dibuat dan mengamati kinerja Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

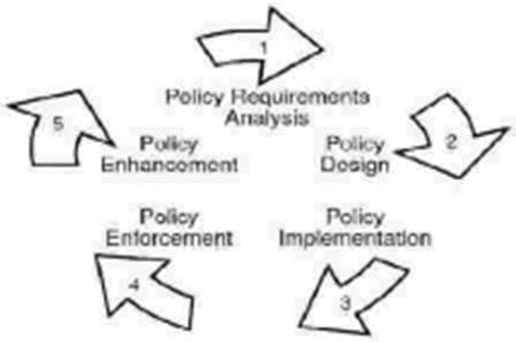
d. **Tahap keempat *(Evaluating)***
Peneliti melakukan evaluasi hasil temuan setelah proses implementasi, pada tahapan evaluasi penelitian yang dilakukan adalah hasil implementasi Perancangan Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS) Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

e. **Tahap kelima *(Learning)***
Setelah masa implementasi *(action research)* dianggap cukup, kemudian peneliti melaksanakan *review* tahap demi tahap dan memahami prinsip kinerja Keamanan Jaringan Komputer Pada Layer Application Berbasis Intrusion Prevention System (IPS)

Yang di Integrasikan Dengan Access Control List (ACLs) di Politeknik TEDC.

Metode Pengembangan System

Security Policy Development Life Cycle (SPDLC) adalah suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tindakan awal dan akhirya dalam membangun sebuah keamanan jaringan komputer mencangkup lima tahap yaitu *Analysis, Design, Implemematlon, Enforcement, dan Enhancement* (Wahsheh and Foss, 2008: 1121).



Gambar 1. *Security Policy Development Life Cycle* (SPDLC)
(Sumber: Wahsheh and Foss, 2008:1121)

1. Analysis

Pada tahap ini dilakukan perumusan masalah, mengidentifikasi konsep dari IPS, ACLs dan beberapa perangkat jaringan, mengumpulkan data dan mengidentifikasi kebutuhan seluruh komponen sistem tersebut, sehingga spesifikasi kebutuhan sistem keamanan jaringan komputer pada layer Application dengan metode IPS dan ACLs dapat diperjelas dan terperinci.

2. Design

Pada tahap ini yang dilakukan adalah Merancang topologi jaringan untuk simulasi *Virtual Local Area Network* sebagai representasi lingkungan jaringan sebenarnya dan merancang penggunaan sistem operasi dan aplikasi pada server, client dan komputer penyusup. Rancangan topologi jaringan dibangun dengan menggunakan Cisco Packet Tracer 5.0 yang sudah terinstal.

3. Implementation

Implementasi atau penerapan detail rancangan topologi dan rancangan sistem pada lingkungan nyata sebagai simulasi Virtual Local Area Network. Detail rancangan akan digunakan dapat dilihat sebagai instruksi atau panduan tahap implementasi agar sistem yang dibangun dapat relevan dengan sistem yang sudah dirancang. Proses implementasi terdiri dari instalasi dan konfigurasi. Dengan mengumpulkan seluruh perangkat yang dibutuhkan.

4. Enforcement

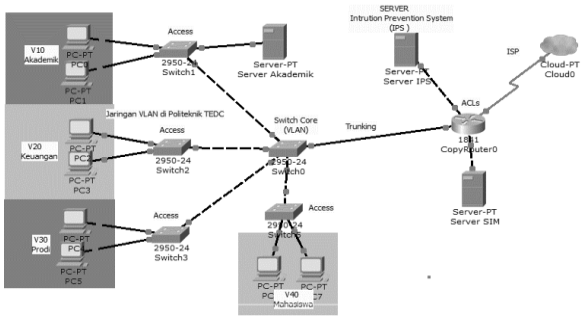
Dimana tahap ini penting. Proses pelaksanaan atau penyelenggaraan dilakuakan melalui aktivitas pengoprasian dan pengamatan sistem yang sudah dibangun dan diterapkan apakah sistem IPS, Access Control List dan Pembagian Segmentasi jaringan sudah berjalan dengan benar dan baik.

5. Enhancement

Pada fase atau tahap ini dilakukan aktivitas perbaikan terhadap perancangan dan sistem yang telah dibangun

IV. HASIL DAN PEMBAHASAN

Pada tahap ini penulis mendefinisikan bahwa jaringan yang ada di Politeknik TEDC semua departemen, seperti bagian Keuangan, Akademik, Prodi, Mahasiswa dan Dosen semua terhubung dalam jaringan LAN, yang tentunya terhubung dalam jaringan lokal area network dalam satu segmentasi. Tahapan dalam pembagian segmentasi jaringan guna mempermudah pengontrolan hak akses atau penerapan ACLs, sehingga terbentuk workgroup yang lebih mudah dalam pengontrolan user terhadap akses Sumber Daya. Dan Pengoperasian dan Uji Coba Pada tahap ini dilakukan uji coba (*testing*) terhadap konfigurasi Keamanan Jaringan pada Application Layer berbasis IPS yang diintegrasikan dengan ACLs yang telah didapat dari proses sebelumnya. Uji coba yang dilakukan dengan metode *enforcement*. Pengujian dilakukan dengan melakukan: Pengujian *host scanning* (anggry ipscan), Pengujian *port scanning* (zenmap), Pengujian *HTTP attacking,* Pengujian *SSH* dan Pengujian *ping of death* serta Gambar topologi di bawah ini adalah rancangan yang akan di bangun untuk perancangan keamanan jaringan pada *apllication layer* berbasis *intrusion prevention system* yang diintegrasikan dengan *access control list.*



Gambar 2. Topologi pengembangan *security*

Tabel 1. Pembuatan segmentasi jaringan

No	VLAN ID	Nama Vlan	Port
1	10	AKADEMIK	3-8
2	20	PRODI	9- 14
3	30	KEUANGAN	15-20
4	40	KESISWAAN	21 -24

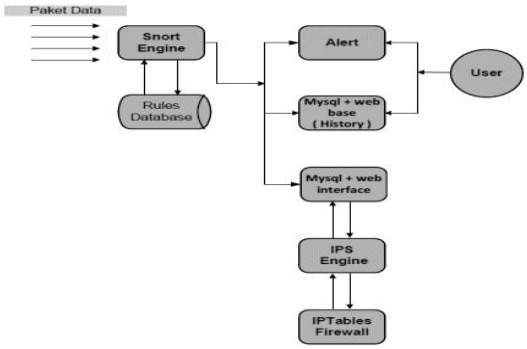
Tabel 2. Pembagian IP addressing

No	VLAN ID	Nama Vlan	Type
1	10	192.168.1.0 /26	DHCP
2	20	192.168.1.64 /27	DHCP
3	30	192.168.1.96 /27	DHCP
4	40	192.168.1.128 /28	DHCP
5	SERVER1	192.168.11.100 /24	STATIC
6	SERVER2	192.168.100.100/24	STATIC

Tabel 3. Komponen Perancangan IPS, ACLs dan VLA

Mesin	Komponen	Keterangan
Router Cisco	-	Digunakan dalam konfigurasi untuk mengatur trafik dan otorisasi pada penerapan Access Control List
Switch Ciso Manageble		Digunakan dalam konfigurasi untuk membagi segmentasi jaringan
Sensor IPS	1. IDS a. Snort Engine b. Rule Snort 2. Data Base System 3. IPS Engine 4. IP Tables 5. Monitoring System	Sensor ini digunakan untuk mengintegrasikan fungsi menganalisi traffic sebuah sistem jaringan dan mendeteksi aktivitas intruder (Snort), Pengelola Output Snortsam, Management console dan alert dari Snort, dan IP Table sebagai *Firewall*
Client Linux Backtrack 4 R2	1. Backtrack *tools*	Mendefinisikan sebagai client dan juga untuk pengujian sistem sensor

Sistem keamanan ini bertujuan untuk mencegah dan melindungi jaringan *layer Applicaion* dengan kemampuan merespon serta aksi terhadap suatu intrusi sesuai dengan kebijakan keamanan. Untuk lebih jelas seperti gambarkan sebagai berikut:



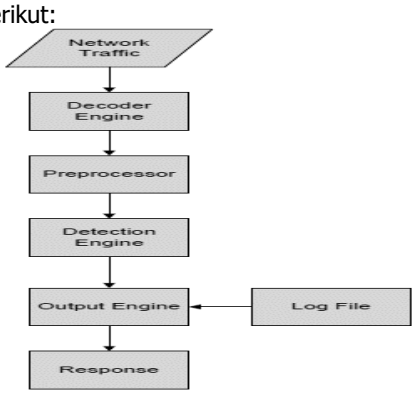
Gambar 3. Hubungan antara sensor snort
(Sumber : Gullett, 2011)

Dari diagram pada gambar 3 IPS yang akan dipakai merupakan integrasi dari beberapa aplikasi *open source* dimana ada beberapa modul yang akan digunakan didalamnya diantaranya sebagai berikut :

1. Snort *Engine*
   Snort *Engine* merupakan program yang selalu bekerja untuk membacapaket data dan kemudian membandingkan dengan *rule* Snort.

```
root@myubuntu:~# ps aux | grep snort
snort    2656  0.1  1.9  58376 38164 ?      Ss   23:08   0:00 /usr/sbin/snort -m
027 -D -d -l /var/log/snort -u snort -g snort -c /etc/snort/snort.conf -S
HOME_NET=[192.168.1.0/24] -i eth0
root     2847  0.0  0.0   3324   812 pts/0    S+   23:12   0:00 grep --color=auto
```

Perintah diatas menunjukkan bahwa Snort *Engine* dalam keadaan aktif dengan proses ID 2847 dan dijalankan oleh *user* "root". Cara kerja *snort* akan digambarkan pada *flowchart* berikut:



Gambar 4. *Flowchart Snort Engine*
(Sumber : Gullett, 2011)

2. *Rule* Snort

   Rule Snort merupakan *database* yang berisi pola-pola serangan berupa *signature* jenis-jenis serangan. Contoh *rule* Snort:

```
alert tcp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC
tcp port 0 traffic"; flow:stateless; classtype:misc-activity; sid:524; rev:8;)
alert udp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC
udp port 0 traffic"; reference:bugtraq,576; reference:cve,1999-0675;
reference:nessus,10074;
```

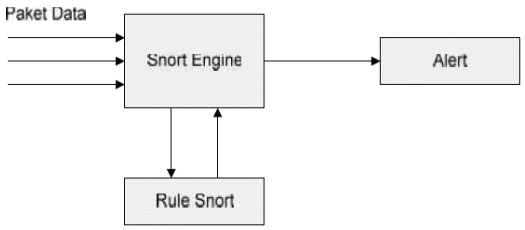
   Rule diatas terdiri dari 2 bagian yaitu : *header* dan *option.* Bagian "alert tcp $EXTERNAL_NET any <> $HOME_NET 0" dan "alert udp $EXTERNAL_NET any <> $HOME_NET 0" adalah *header* dan selebihnya merupakan bagian dari *option*. Dari *rule* Snort ini akan dikelompokkan apakah sebuah paket data yang lewat dianggap sebagai sebuah serangan penyusupan atau bukan.

3. *Alert*

   Alert merupakan catatan serangan pada deteksi serangan penyusupan. Jika *rule* Snort mendefiniskan paket data yang lewat sebagai serangan penyusupan, maka Snort *Engine* akan mengirimkan *alert* berupa *log* ke dalam *database*.

```
06/13-12:45:56.208898  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority:
3] {PROTO:255} 192.168.1.246 -> 192.168.1.244
06/13-12:45:56.208897  [**] [122:1:0] (portscan) TCP Portscan [**] [Priority:
3] {PROTO:255} 192.168.1.246 -> 192.168.1.244
```

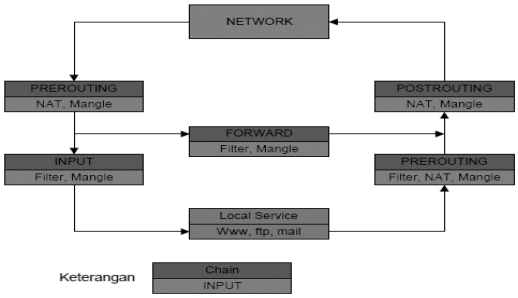
   Contoh diatas merupakan *alert* hasil *scanning port* TCP dari IP 192.168.1.246 ke IP 192.168.1.244 yang disimpan oleh Snort *Engine* ke dalam *alert* dan dianggap sebagai sebuah serangan oleh Snort karena pola paket data tersebut terdapat dalam *rule* Snort. Hubungan ketiga komponen IDS dijelaskan dalam gambar berikut:



Gambar 5. Komponen Alert Snort
(Sumber : Gullett, 2011)

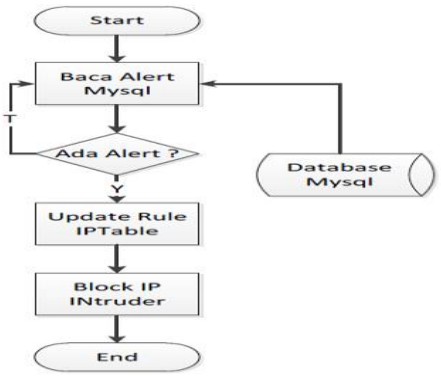
4. IP Table

   Firewall digunakan untuk membuka dan menutup akses sesuai dengan rule yang dibuat, dalam hal ini *rule* akan dinamis sesuai dengan kondisi yang dideteksi oleh IDS. *Firewall* yang digunakan dalam eksperimen ini adalah *Iptables* yang merupakan *firewall* bawaan *Linux*



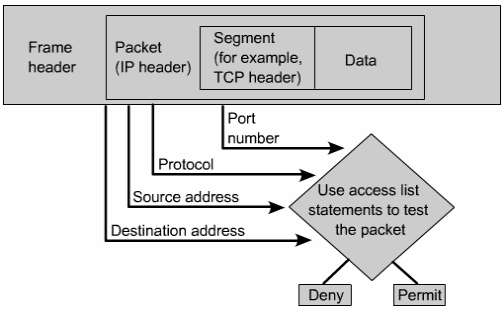
Gambar 6. Skema filterisasi
(Sumber : Gullett, 2011)

IPS *engine* merupakan sistem yang akan membaca alert kemudian memerintahkan *firewall* untuk menutup akses paket data dari penyerang. Cara kerja IPS *engine* digambarkan dalam *flowchart* berikut ini:



Gambar 7. *Flowchar IPS Engine*
(Sumber : Gullett, 2011)

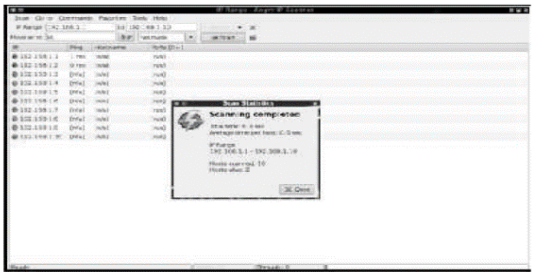
Sedangkan dalam menentukan hak ases apakan user boleh mengakses sumber daya atau sebaliknya maka dilakukan konfigurasi pada router dengan Access Control List (ACLs) bisa di lihat pa gambar di bawah ini:



Gambar 8. Cara kerja Access Control List
(Sumber : Lammle, 2007)

A. Pengujian *Host Scanning*

Pada pengujian ini dilakukan percobaan pengamatan terhadap *host* yang ada pada jaringan. Berikut contoh pengujian serangan yang dilakukan menggunakan aplikasi Angry IPScan.



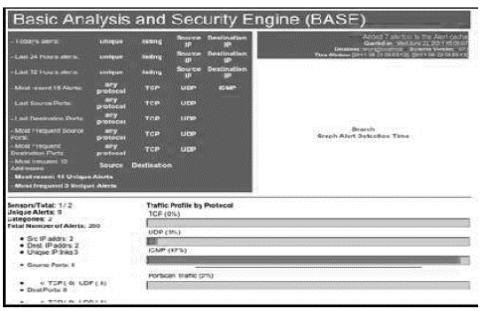
Gambar 9. Kondisi Snort Network Intrusion Prevention System tidak aktif

B. Pengujian *Port Scanning*

Pada pengujian ini dilakukan percobaan pengamatan *port-port* yang terbuka. Berikut contoh pengujian serangan yang dilakukan menggunakan aplikasi zenmap. Pengamatan di komputer penyerang.

Gambar 10. Kondisi Snort *Network Intrusion Prevention System* tidak aktif

C. Pengamatan *Database* Snort Melalui Acidbase



Gambar 11. Database snort melalui acidbase

D. Pengujian Akses *Localhost*

Pada pengujian ini, penyerang akan mengakses *localhost* dari Snort NIPS.

Gambar 12. Kondisi Snort Network Intrusion Prevention System tidak aktif

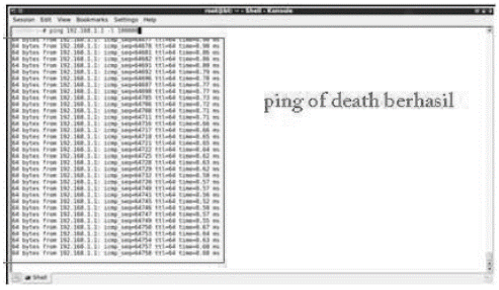
E. Pengujian Akses SSH

Pada pengujian ini, penyerang akan mengakses Snort NIPS melalui SSH.

Gambar 13. Kondisi Snort Network Intrusion Prevention System tidak aktif

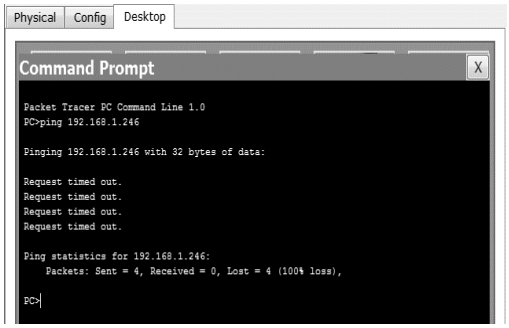
F. Pengujian *Ping of Death*

Pada pengujian ini, penyerang akan melakukan *Denial of Service* (DoS) berupa *Ping of Death*, yaitu dengan mengirimkan paket ICMP dalam jumlah besar ke *server* NIPS.



Gambar 14. Kondisi Snort *Network Intrusion Prevention System* tidak aktif

G. Pengujian *Access Control List (ACLs)*



Gambar 15. *Access Control List (ACLs)*

V. KESIMPULAN

1. Dengan adanya pemisahan segmentasi jaringan, seluruh departemen yang ada di politeknik TEDC lebih mudah dalam pengontrolan, pengaturan hak akses dan terpisah dalam sebuah workgroup. Sehingga departemen satu dengan yang lainya tidak dapat mengintervensi dalam segmentasi yang berbeda.
2. Snort *Network Intrusion Prevention System* (NIPS) mampu monitoring aktivitas dalam jaringan dan melakukan pencegahan secara dini apabila ada penyusup dan aplikasi-aplikasi yang mencurigakan, sehingga keamanan jaringan di Politeknik TEDC akan lebih aman dari user yang akan melakukan *intruder* terhadap sumber daya.
3. Keamanan jaringan merupakan aspek yang harus di perhatikan, di Politeknik TEDC semua user terhubung dalam satu jaringan, sehingga sangat sulit bagi admin jaringan dalam melakukan pengontrolan, monitoring, mengatur hak akses, dengan adanya penerapan keamanan jaringan yang berbasis IPS yang di Integrasiakan dengan ACLs di harapkan user bekerja sesuai dengan tugas dan tanggungjawabnya, jaringan komputer akan lebih aman dan nyaman, sehingga pelayanan terhadap kebutuhan informasi akan selalu tersedia.

DAFTAR PUSTAKA

Alder, Raven.(*2007). Snort IDS and IPS Toolkit. Burlington, MA 01803: Syngre Publishing, Inc.*

Ariyus, D.(2007). *Intrusion Detection System*. Yogyakarta: Andi Yogyakarta.

Behrouz A. Forouzan.(2010). *TCP/IP Protokol Suite.* Boston: McGraw Hill.

Lammle, Todd.(2007).*CCNA*. Jakarta: Elekmedia Komputindo,

Davison, R.M., Martinsons, M.G., Kock N.,(2004) *Principles Of Canonical Action Research*. Journal: Information System., 14, 65-86.

Dwi, Kuswanto.(2014).Unjuk Kerja Intrusion Preventive System (IPS) Berbasis Suricata pada Jaringan Lokal Area Network. Jurnal Ilmiah NERO, vol. 1, p. 74, 2014.

Gullett, David,(2011). *Snort 2.9.0.5 and Snort Report 1.3.1 on Ubuntu 10.04 LTS Installation Guide*. United States: Symmetrix Technologies.

Taufik, Wicaksono.(2009).Rancang Bangun dan Implementasi IDS/IPS pada Server untuk Meningkatkan Keamanan Jaringan,Skripsi.

Nafisah, Syifan.(2003). *Perancangan Aplikasi.* Yogyakarta: Graha Ilmu.

Wahsheh, Luy A and Foss, Jim Alves.(2008). *Security Polic Development: Towards a life-cycle and Logic-Based Verification Model. American Journal of Applied Sciences 5(9). Page 117-1126.*