KAJIAN PENERAPAN METODE *INTRUSION PREVENTION SYSTEM* DI JARINGAN INTERNET DAN INTRANET UNIVERSITAS RIAU

Irfan Kurniadi H*, Irsan Taufik Ali**
*Mahasiswa Program Studi Teknik Elektro, **Dosen Teknik Elektro
Laboratorium Komputer dan Jaringan
Program Studi Teknik Elektro S1, Fakultas Teknik Universitas Riau
Kampus Binawidya Km 12,5 Simpang Baru Panam, Pekanbaru 28293
Jurusan Teknik Elektro Universitas Riau
Email: irfanhamzah10@gmail.com

ABSTRACT

The development of Information Technology makes an information security is very important, especially on a network connected to the internet. The imbalance between every development of a technology is not accompanied by developments in the security system itself, thus quite a lot of systems are still weak. This weakness is able to create a threat, either from within or from outside. The security system used by the University of Riau today is the Firewall-DMZ security system that is a security system that controls, supervises, filters and identifies incoming traffic and protects servers that are accessible to the public. Intrusion Prevention System as a security system that can prevent a threat to the information network. Intrusion Prevention System (IPS) combines firewall techniques and Intrusion Detection System (IDS) methods very well. This technology can prevent attacks that will enter the local network by checking and recording all data packets and recognizing the sensor data packets, when an attack has been identified, Intrusion Prevention System (IPS) will deny access and record all identified data packets. The result of this research is to apply snort security system based on snort network of Riau University by simulating some attack experiments that are resolved well by IPS, so it can be a consideration for University Computer Center of Riau to implement security system which is automated in intranet and internet university Riau.

Keywords : Intrusion Prevention System, IPS, IDS, Snort, Network Security, Network.

I. PENDAHULUAN

Perkembangan ilmu pengetahuan dan teknologi informasi semakin hari semakin berkembang khususnya jaringan komputer yang pada saat ini telah menjadi satu hal paling mendasar pada suatu lembaga pendidikan. Hal ini menyebabkan penggunaan jaringan komputer menjadi kebutuhan pokok bagi setiap lembaga pendidikan. Universitas Riau (UR) merupakan sebuah lembaga pendidikan yang besar, baik dilihat dari segi luas kawasan maupun dari jumlah mahasiswa, dosen dan pegawai, sehingga Universitas Riau membutuhkan suatu jaringan informasi yang aman dan efektif.

Keamanan jaringan komputer sebagai bahan dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak. Berbagai macam strategi dan *tools* telah tersedia untuk mengganggu, menyerang bahkan merusak suatu jaringan.

Namun untuk mendukung keamanan jaringan *internet* civitas akademika Universitas Riau, dibutuhkan sebuah sistem keamanan jaringan informasi yang ketat. Metode itu disebut *Intrusion Prevention System* yang disingkat dengan *IPS*, yaitu metode otomatisasi terhadap sistem deteksi dan prevensi secara langsung.

Intrusion Prevention System (*IPS*) merupakan suatu metode yang dikembangkan dimana memiliki kemampuan untuk mendeteksi serangan dan gangguan terhadap jaringan, untuk selanjutnya dilakukan tindakan pencegahan terhadap serangan tersebut. Kemampuan terbaik dari *Intrusion Prevention System* (*IPS*) adalah membatalkan sebuah serangan sebelum serangan tersebut dijalankan. Hal ini dapat dilakukan dengan mengenali kriteria-kriteria serangan yang biasanya dilakukan.

Metode *Intrusion Prevention System* (*IPS*) merupakan pengembangan metode keamanan dari *Intrusion Detection System* (*IDS*) yang hanya berfungsi untuk mendeteksi aktivitas mencurigakan dalam sebuah sistem jaringan dan melakukan analisis serta mencari bukti dari percobaan intrusi/penyusupan. Dikarenakan banyaknya ancaman-ancaman terhadap jaringan maka dikembangkanlah teknologi *Intrusion Detection System* (*IDS*) menjadi *Intrusion Prevention System* (*IPS*) yang berfungsi untuk mengidentifikasi jaringan dari aktivitas yang berbahaya, mencatatkan informasi, memblokir atau menghentikan, dan melaporkan kegiatan berbahaya tersebut.

Berdasarkan penelitian oleh Alamsyah pada tahun 2011 yang berjudul "Implementasi Keamanan *Intrusion Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) Menggunakan *ClearOS*". Pada penelitian ini dibahas bagaimana seorang *administrator* dapat tertipu terhadap beberapa serangan yang tidak dapat diklasifikasikan jika hanya dengan menggunakan *firewall* saja, sehingga digunakanlah *Intrusion Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) sebagai pelengkap teknologi keamanan jaringan. Sistem pertahanan akan dapat mengambil tindakan sesuai dengan data pengklasifikasian yang jelas dan dapat menindak lanjuti laporan dari data yang sudah valid. Sistem jaringan *internet* pada umumnya yang ada saat ini memiliki *router* dan *server* yang memiliki *IP Address Public* sendiri-sendiri. Dengan adanya *IP Public* dapat menimbulkan adanya *port-port* yang terbuka pada *server*, serhingga dalam mengakses *internet* dapat menimbulkan serangan atau ancaman ke *server* tersebut. Metode yang digunakan yaitu mengkonfigurasi aplikasi sistem *Snort Intrusion Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) dengan menggunakan sistem operasi *ClearOS*, kemudian menambahkan aplikasi *Snort* sebagai *Intrusion Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) pada *internet gateway*. Hasil yang diperoleh dari penerapan *Intrusion Detection System* (*IDS*) dan penerapan *Intrusion Prevention System* (*IPS*) menggunakan *snort* yaitu sistem dapat mengawasi trafik yang terjadi pada jaringan *internet* di Universitas Tadulako Palu. *Snort* dapat memonitoring trafik pada komputer *server* dan menyimpan hasil deteksi dan pencegah jika ada penyusup yang memasuki sistem komputer *server*.

II. LANDASAN TEORI

Konsep Dasar Keamanan Jaringan

Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi suatu penggunaan yang tidak sah dari jaringan komputer. Penanggung jawab keamanan jaringan (*Administrator*) harus dapat memastikan bahwa prinsip dasar keamanan jaringan tidak akan dilanggar oleh aktivitas subjek jaringan atau pengguna. Ada

beberapa prinsip dasar keamanan jaringan yaitu seperti berikut ini.

- Kerahasiaan (*confidentiality*)
  Obyek yang terdapat didalam sebuah jaringan apapun tidak boleh diumbar sepenuhnya ke semua orang apalagi kepada pengguna yang tidak memiliki hak akses atau wewenang terhadap suatu obyek jaringan tersebut.
- Integritas (*integrity*)
  Setiap obyek yang diterima dalam suatu jaringan harus dijaga keasliannya. Ini berarti bahwa dalam pengiriman obyek dari sumber hingga sampai ke tujuan tidak boleh mengalami perubahan.
- Ketersediaan (*availability*)
  Setiap pengguna yang memiliki hak akses terhadap obyek tertentu sesuai dengan wewenangnya harus diberikan kemudahan untuk mengakses hingga tidak terkendala apapun.

Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung (*direct*) ataupun tidak langsung (*indirect*) mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Secara umum, terdapat 3 hal dalam konsep keamanan jaringan, sebagai berikut.

- Resiko (*risk*)
  Resiko adalah untuk menyatakan besarnya kemungkinan gangguan yang muncul terhadap jaringan.
- Ancaman (*threat*)
  Ancaman merupakan kemungkinan gangguan yang muncul terhadap jaringan.
- Kerapuhan Sistem (*vulnerability*)
  Kerapuhan menyatakan kelemahan-kelemahan pada sistem yang memungkinkan terjadinya gangguan. (Firman Anggoro, Gelar Budiman, dan Prajna Deshanta Ibnugraha, 2010)

Pengertian Penyusup (Intruder) Jaringan Komputer

Penyusup (*intruder*) merupakan orang atau kumpulan orang yang melakukan tindakan tidak tepat (*incorrect*), yang menyimpang (*anomaly*), dan tidak pantas (*inappropriate*) terhadap suatu jaringan komputer. Beberapa tujuan dari seorang penyusup yaitu :

- Hanya ingin tahu sistem dan data yang ada pada suatu sistem jaringan komputer yang dijadikan sasaran. Penyusup seperti ini disebut *The Curius*.
- Membuat sistem jaringan menjadi *down*, atau mengubah tampilan dari suatu situs web. Penyusup ini disebut *The Malicious*.
- Ingin tahu data apa saja yang ada didalam jaringan komputer kemudian memanfaatkannya untuk mendapatkan uang.
- Berusaha untuk menggunakan sumber daya didalam sistem jaringan komputer untuk memperoleh popularitas. Penyusup ini disebut *The High Profile Intruder*.

Jenis Ancaman Terhadap Jaringan

Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut.

- *Probe*
  Probe atau yang biasa disebut *probing* adalah suatu usaha untuk mengakses sistem atau mendapatkan informasi tentang sistem. Contoh sederhana dari *probing* adalah percobaan *log in* ke suatu *account* yang tidak digunakan. *Probing* dapat dianalogikan dengan menguji kenop-

kenop pintu untuk mencari pintu yang tidak dikunci sehingga dapat masuk dengan mudah. *Probing* tidak begitu berbahaya bagi sistem jaringan kita namun biasanya diikuti oleh tindakan lain yang lebih membahayakan keamanan.

- *Scan*
  Scan adalah *probing* dalam jumlah besar menggunakan suatu *tool*. *Scan* biasanya merupakan awal dari serangan langsung terhadap sistem yang oleh pelakunya ditemukan mudah diserang.
- *Account Compromise*
  Merupakan penggunaan *account* sebuah komputer secara ilegal oleh seseorang yang bukan pemilik *account* tersebut. *Account Compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data.
- *Root Compromise*
  Hampir sama dengan *account compromise*, dengan perbedaan *account* yang digunakan secara ilegal adalah *account* yang mempunyai *privelege* sebagai *administrator* sistem. Akibat yang ditimbulkan bisa mengubah kinerja sistem, menjalankan program yang tidak sah.
- *Packet Sniffer*
  Packet sniffer adalah sebuah program yang menangkap (*capture*) data dari paket yang lewat di jaringan. Data tersebut bisa termasuk *user name*, *password*, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk *text*. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan *user name* dan *password*. Dengan *password* itu pelaku dapat mengirimkan serangan besar-besaran ke sistem.
- *Denial of Service* (*DoS*)
  Denial of service (*DoS*) bertujuan untuk mencegah pengguna mendapatkan layanan dari sistem. Serangan *DoS* dapat terjadi dalam banyak bentuk.
  Penyerang dapat membanjiri (*flood*) jaringan dengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti *process control block* (*PCB*) atau *pending network connection*. Penyerang juga mungkin saja mengacaukan komponen fisik dari jaringan atau memanipulasi data yang sedang dikirim termasuk data yang terenkripsi.
- *IP Spoofing*
  Sebuah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan *firewall* dan menipu *host* penerima data.
- *DNS Forgery*
  Salah satu cara yang dapat dilakukan oleh seseorang untuk mencuri data-data penting orang lain adalah dengan cara melakukan penipuan. Salah satu bentuk penipuan yang bisa dilakukan adalah penipuan data-data *DNS*.
- *Trojan Horse*
  Program yang disisipkan tanpa pengetahuan si pemilik komputer, dapat dikendalikan dari jarak jauh & memakai *timer*.

Perencanaan Keamanan Jaringan Informasi

Untuk menjamin keamanan dalam jaringan, perlu dilakukan perencanaan

keamanan yang matang berdasarkan prosedur dan kebijakan dalam keamanan jaringan. Perencanaan tersebut akan membantu dalam hal-hal berikut ini :

- Menentukan data atau informasi apa saja yang harus dilindungi.
- Menentukan berapa besar biaya yang harus ditanamkan dalam melindunginya.
- Menentukan siapa yang bertanggung jawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagian tersebut.

Metode Keamanan Jaringan

Dalam merencanakan suatu keamanan jaringan, ada beberapa metode yang dapat diterapkan. Metode-metode tersebut adalah sebagai berikut :

- Pembatasan Akses Pada Suatu Jaringan

  Ada 3 beberapa konsep yang ada dalam pembatasan akses jaringan, yakni sebagai berikut :

1. *Internal Password Authentication* .
2. *Server-based Password authentication*
3. *Firewall* dan *Routing Control*

- Menggunakan Metode Enkripsi Tertentu

  Dasar enkripsi cukup sederhana. Pengirim menjalankan fungsi enkripsi pada pesan *plaintext*, *ciphertext* yang dihasilkan kemudian dikirimkan lewat jaringan, dan penerima menjalankan fungsi dekripsi (*decryiption*) untuk mendapatkan *plaintext* semula. Proses enkripsi atau dekripsi tergantung pada kunci (*key*) rahasia yang hanya diketahui oleh pengirim dan penerima. Ketika kunci dan enkripsi ini digunakan, sulit bagi penyadap untuk mematahkan *ciphertext*, sehingga komunikasi data antara pengirim dan penerima aman.

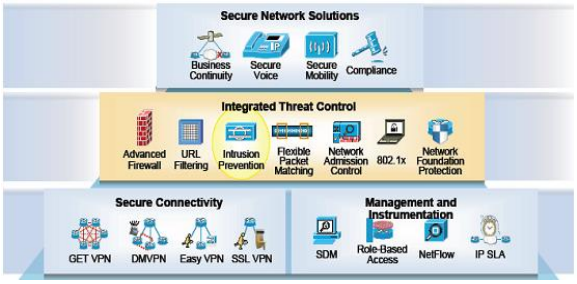
- Pemonitoran Terjadwal Terhadap Jaringan

  Proses memonitor dan melakukan administrasi terhadap keamanan jaringan dengan menggunakan *schedule* yang telah ditetapkan, hal ini berfungsi untuk mengetahui berapa banyak dan apa saja trafik yang pernah terhubung ke sistem jaringan.

Intrusion Prevention System

Intrusion Prevention System (*IPS*) adalah sebuah metode yang sering digunakan untuk membangun sistem keamanan komputer, *Intrusion Prevention System* (*IPS*) mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (*IDS*) dengan sangat baik. Teknologi ini dapat mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket data sensor, disaat serangan telah teridentifikasi, *Intrusion Prevention System* (*IPS*) akan menolak akses (*blocking*) dan mencatat (*log*) semua paket data yang teridentifikasi tersebut.

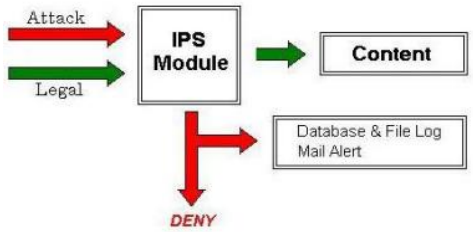
Jadi *Intrusion Prevention System* (*IPS*) bertindak seperti layaknya *firewall* yang akan melakukan *allow* dan *block* yang dikombinasikan seperti *Intrusion Detection System* (*IDS*) yang dapat mendeteksi paket secara detail. *Intrusion Prevention System* (*IPS*) menggunakan *signatures* untuk mendeteksi aktivitas trafik di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat dicegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi *early detection* dan *prevention* menjadi penekanan pada *Intrusion Prevention System* (*IPS*) ini. (Deris Setiawan, 2010)



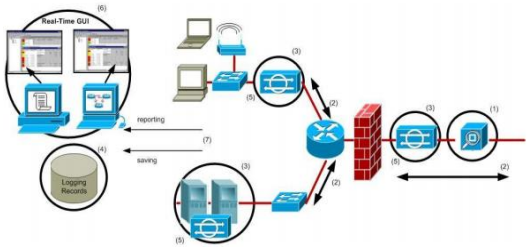
Gambar 1. All in One Security

Cara Kerja *IPS*

Intrusion Prevention System (*IPS*) akan mengirimkan sebuah peringatan (*alert*) kepada *network* atau sistem *administrator* ketika suatu hal yang mencurigakan terdeteksi, memungkinkan *administrator* dapat memilih sebuah tindakan untuk diambil ketika terjadi sebuah *event*. *Intrusion Prevention System* (*IPS*) dapat memonitor seluruh jaringan, *wireless network protocol*, perilaku jaringan (*network behaviour*) dan dan trafik sebuah komputer. Setiap *Intrusion Prevention System* (*IPS*) menggunakan metode deteksi tertentu untuk menganalisis resiko.



Gambar 2. Cara Kerja *Intrusion Prevention System* (*IPS*)



Gambar 3. Topologi dan Terminologi dalam Implementasi *Intrusion Prevention System* (*IPS*)

III. METODE PENELITIAN

Alat dan Bahan

Perancangan suatu sistem keamanan jaringan merupakan hal utama yang dibutuhkan seorang *network administrator* dalam mencegah berbagai macam serangan. Simulasi jaringan dibangun untuk melihat kebutuhan suatu jaringan, dalam hal ini *network administrator* dapat mengkoordinasikan dan mengelola jaringan sebelum jaringan bisa direalisasikan. Berikut ini merupakan spesifikasi untuk merancang simulasi sistem keamanan jaringan dengan menggunakan metode *Intrusion Prevention System* (*IPS*).

1. *Server*

a. Hardware

- Type Laptop : Asus A43E Series
- Processor : Intel®Core™ i3
- OS : Ubuntu 14.04 LTS
- Memory : 2048 MB RAM
- HDD : 30 GB

b. Software

- *Snort* 2.9.7.2
- *IPTables firewall*

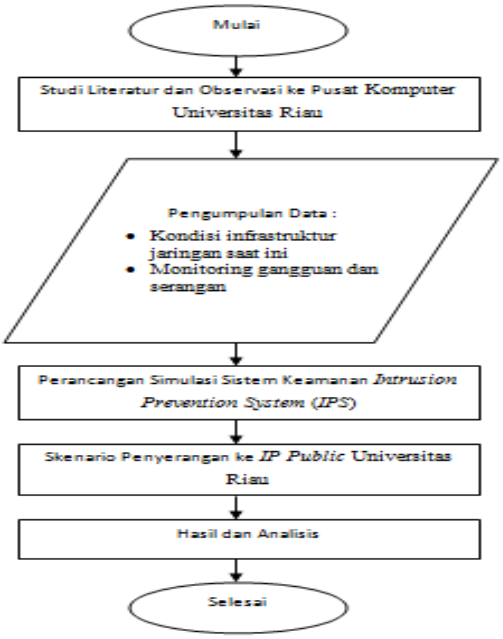
2. *Attacker*

a. Hardware

- Type Laptop : Acer Aspire 4736
- Processor : Intel®Centrino™T6600
- OS : Windows 7 Ultimate
- Memory : 2048 MB RAM
- HDD : 250 GB

b. Metode Serangan

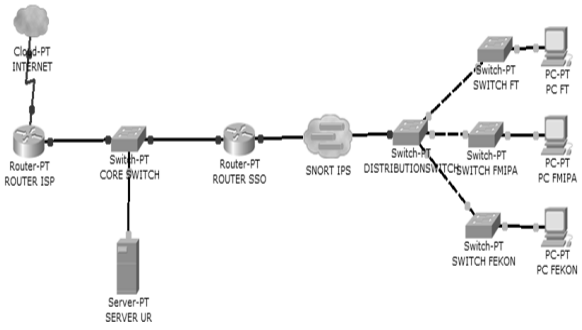
- *Ping of Death*
- *Host Scanning*
- *Port Scanning*
- *HTTP Attacking*
- Pengujian *SSH*



Gambar 4. Diagram Alir Penelitian

Analisa Sistem yang Akan Dikembangkan

Perancangan sistem keamanan ini yaitu dengan hanya melakukan simulasi sebuah *server* yang akan dikonfigurasi menggunakan *Snort* dan *IPTables firewall*. Untuk penyusupan atau serangan akan dilakukan oleh sebuah pc attacker.



Gambar 5. Rancangan Jaringan UR dengan Snort IPS

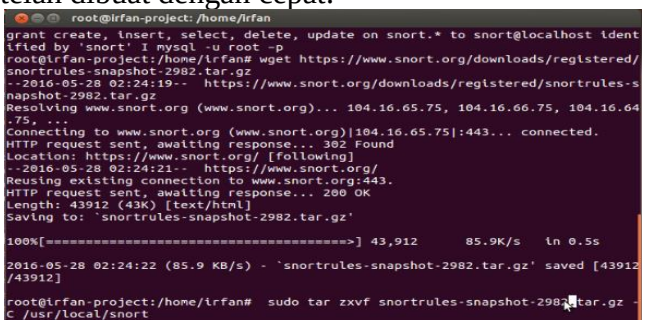
Implementasi dan Pengujian

Tahap implementasi adalah tahap dimana konfigurasi sistem dilakukan, yaitu dengan mengkonfigurasi server yang berbasis snort pada system operasi Ubuntu 14.04 Lts. Setelah konfigurasi telah dilakukan tahap berikutnya yaitu pengujian simulasi, dengan menggunakan skema sederhana yaitu sebuah pc server dengan snort IPS dan sebuah pc attacker/client dengan beberapa tools untuk penyerangan jaringan komputer.

Gambar 5. Skema simulasi pengujian/penyerangan

Instalasi

Sebelum mengkonfigurasi, hal yang harus dilakukan pertama yaitu instalasi semua package library yang dibutuhkan. Untuk menginstal paket serta mengkonfigurasi *NIPS* harus menggunakan *terminal*, yaitu sebuah *tools* yang bekerja menggunakan baris perintah yang berisi perintah untuk mengeksekusi perintah yang telah dibuat dengan cepat.



Gambar 6. Tampilan Terminal pada Ubuntu

Untuk mengeksekusi paket harus menggunakan perintah *root* agar administrator mempunyai hak akses untuk mengelola sistem. Langkah yang pertama yaitu masuk sebagai *root*.

Instalasi Package

```
# sudo apt-get install nmap
# sudo apt-get install nbtscan
# sudo apt-get install apache2
```

```
# sudo apt-get install php5-gd
# sudo apt-get install libpcap0.8-dev
# sudo apt-get install libpcre3-dev
# sudo apt-get install g++
# sudo apt-get install bison
# sudo apt-get install flex
# sudo apt-get install libpcap-ruby
# sudo apt-get install autoconf
# sudo apt-get install libtool
```

Instalasi DAQ

```
# wget
https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
# tar -zxf daq-2.0.6.tar.gz && cd daq-2.0.6
```

Instalasi *Snort*

Snort adalah sebuah aplikasi atau *tools* keamanan jaringan yang fungsinya untuk mendeteksi adanya gangguan-gangguan didalam jaringan, seperti penyusupan, pemindaian, penyerangan, dan ancaman lainnya, sekaligus juga melakukan pencegahan. *Snort* sangat bisa diandalkan untuk membuat *logging* paket-paket dan analisis trafik data secara *real-time* dalam jaringan berbasis *TCP/IP*. Disini snort yang digunakan adalah versi terbaru yaitu snort 2.9.9.0.

```
#     wget
https://www.snort.org/downloads/snort/snort-2.9.9.0.tar.gz
# tar -zxf snort-2.9.9.0.tar.gz && cd snort-2.9.9.0
#     ./configure             --enable-dynamicplugin --enable-perfprofiling --enable-ipv6   --enable-zlib   --enable-reload
# make && make install
```

Instalasi *Blockit*

```
$wget
http://www.teknofx.com/proggie/blockit-1.4.3a.tar.gz
$tar   zxvf   blockit-1.4.3a.tar.gz   -C /tmp/

$cd /tmp/blockit-1.4.3a/
$sudo sh install.sh
[/usr/local/blockit]: /etc/blockit
ln: `/etc/blockit/conf' and `/etc/blockit/conf' are the same file
Do you want to configure MySQL support? [y/n]: y
    Enter Username : ips
Enter Password : xxxx
If using PF add a line saying 'anchor blockit' in your /etc/pf.conf!
```

Konfigurasi

Setelah melakukan instalasi dengan sukses, langkah selanjutnya yaitu konfigurasi NIPS.

Snort Configuration

```
       Local Network
        ----------
        var HOME_NET
[10.10.10.0/24,172.10.10.0/24]
       ----------

       Rules Path
       ----------
       var RULE_PATH rules/
       output database: log, mysql,
    user=dudul password=xxxx
    dbname=snort-log host=localhost
         -----------.
```

Running

Setelah semua instalasi dan konfigurasi sudah selesai sekarang waktunya untuk menjalankan NIPS nya. Disini penulis akan menjalankan snort dan IPS untuk memonitoring *traffic* yang berasal dari Internet sehingga dijalankan di *interface eth0* (*IP Public*).

```
$sudo cp /usr/local/blockit/bin/blockit /usr/sbin/blockit
  $sudo blockit

  Loaded 2 addresses from /etc/blockit/blockit.ignore
  Loaded 0 addresses from /etc/blockit/blockit.sigid
  Loaded 0 addresses from /etc/blockit/blockit.hosts
  Becoming a daemon..

  $sudo snort -D -K ascii -i eth0 -c /etc/snort2.6/snort.conf
  $sudo ps afx | grep snort

  32419 ?        Ss     0:00 snort -D -K ascii -i eth0 -c
/etc/snort2.6/snort.conf
```

Pengujian

Pada tahapan ini menggambarkan kondisi-kondisi yang terjadi apabila sistem dijalankan. Pengujian (*testing*) yang akan dilakukan menggunakan beberapa metode yaitu diantaranya adalah sebagai berikut :

- *Host Scanning*
- *Port Scanning*
- *HTTP Attacking*
- Pengujian *SSH*
- *Ping of Death*

IV. HASIL DAN PEMBAHASAN

- **Pengujian *Host Scanning***

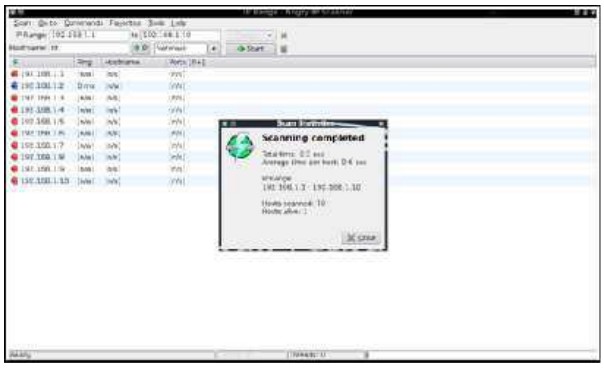
Pada pengujian ini dilakukan percobaan pengamatan terhadap *host* yang ada pada jaringan. Berikut contoh pengujian serangan yang dilakukan menggunakan aplikasi *Angry IPScan*.

➢ Kondisi Snort *Network Intrusion Prevention System* tidak aktif

Gambar 7. Percobaan *Host Scanning* Sukses

Dari pengamatan diatas terlihat bahwa pengujian *host scanning* pada *range* IP *address* 192.168.1.1 ke 192.168.1.10 berhasil ketika snort tidak dalam keadaan aktif. Dengan melakukan *host scanning*, penyerang bisa mengetahui *host*-host V-5 mana saja dalam keadaan aktif. Pada percobaan diatas, IP *address server* NIPS yaitu: 192.168.1.1 dan IP *address* penyerang: 192.168.1.2.

➢ Kondisi Snort *Network Intrusion Prevention System* aktif



Gambar 8. Percobaan *Host Scanning* Gagal

Dari pengamatan diatas terlihat bahwa percobaan *host scanning* gagal dengan tidak dijumpai IP *address server*. Yang terlihat hanya IP *address* dari penyerang.

Deskripsi dan Prekondisi	Tools dan IP address penyusup	Prosedur Pengujian	Keluaran yang diharapkan	Hasil dan Kesimpulan
Snort Network Intrusion Prevention System (NIPS) dalam keadaan aktif	Angry IPScan 192.168.1.2	Penyusup melakukan scanning host yang aktif	Tampil IP address penyusup dalam bentuk alert dan system melakukan blocking IP address dan serangan	Tampil IP address penyusup dalam bentuk alert pada terminal dan acidbase Kesimpulan pengujian : Berhasil

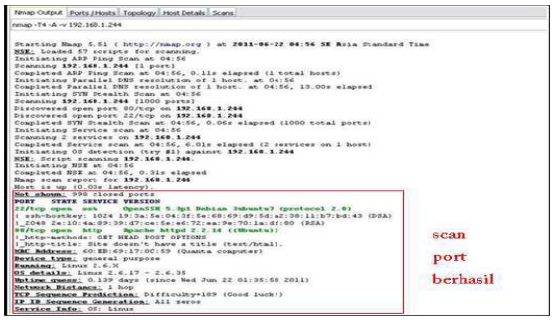
Tabel 1. Pengujian *Host Scanning* Pada *Server Snort* IPS

- **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.

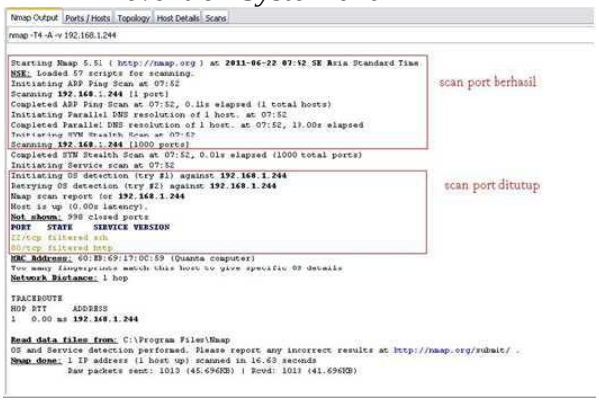
➢ Kondisi Snort *Network Intrusion Prevention System* tidak aktif.



Gambar 9. Percobaan *Port Scanning* Sukses

Dari pengamatan diatas terlihat bahwa pengujian *port scanning* ke *server snort IPS* berhasil ketika snort tidak dalam keadaan aktif. Dengan melakukan *port scanning*, penyerang bisa mengetahui *port-port* mana saja yang terbuka dan dapat diakses. Dari gambar diatas terlihat bahwa *port* 22 (ssh) dan *port* 80 (HTTP) terbuka dan dapat diakses.

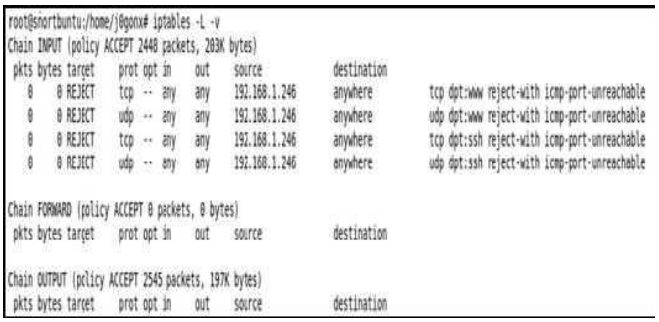
- Kondisi Snort *Network Intrusion Prevention System* aktif



Gambar 10. Percobaan *Port Scanning* Gagal

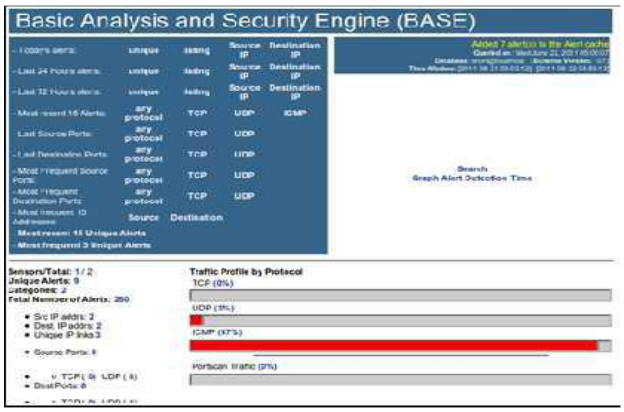
Dari gambar di atas terlihat bahwa *snort NIPS* telah bekerja dengan baik, hal ini ditunjukkan dengan tertutupnya *port* 22 (ssh) dan *port* 80 (HTTP) ditandai dengan *filtered*.

- Pengamatan di *server Network Intrusion Prevention System*



Gambar 11. Pengamatan Pengamanan

Dari pengamatan yang dilakukan di kedua sisi, baik sisi penyerang dan sisi sistem pencegahan penyusupan, dapat disimpulkan bahwa fungsional sistem ini telah berjalan seperti yang dirancang. Serangan-serangan jenis lain juga akan di *block* oleh sistem tergantung kelengkapan *rule snort*.



Gambar 12. *Alert* yang disimpan ke dalam *database*

Deskripsi dan Prekondisi	Tools dan IP address penyusup	Prosedur Pengujian	Keluaran yang diharapkan	Hasil dan Kesimpulan
Snort Network Intrusion Prevention System (NIPS) dalam keadaan aktif	Zenmap 192.168.1.2	Penyusup melakukan scanning port yang aktif	Tampil IP address penyusup dalam bentuk alert dan sistem melakukan blocking IP address dan serangan	Tampil IP address penyusup dalam bentuk alert pada terminal dan acidbase

Tabel 2. Pengujian Port Scanning Pada *Server Snort* IPS

- **Pengujian *HTTP Attacking***

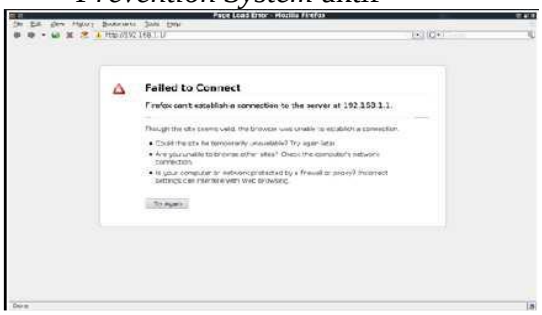
Pada pengujian ini, penyerang akan mengakses *localhost* dari Snort NIPS.

➢ Kondisi Snort *Network Intrusion Prevention System* tidak aktif.

Gambar 13. Akses *Localhost* Berhasil

Dari pengamatan diatas dapat dilihat bahwa akses ke *localhost* ke *server* NIPS berhasil ketika Snort dalam keadaan tidak aktif.

- Kondisi Snort *Network Intrusion Prevention System* aktif



Gambar 14. Akses *Localhost* Gagal

Dari pengamatan diatas dapat dilihat bahwa akses ke *localhost* ke *server* NIPS gagal ketika Snort dalam keadaan aktif.

Deskripsi dan Prekondisi	Tools dan IP address penyusup	Prosedur Pengujian	Keluaran yang diharapkan	Hasil dan Kesimpulan
Snort Network Intrusion Prevention System (NIPS) dalam keadaan aktif	Mozilla Web Browser 192.168.1.2	Penyusup melakukan HTTP Attacking pada *server* NIPS	Tampil IP address penyusup dalam bentuk alert dan sistem melakukan blocking IP address dan serangan	Tampil IP address penyusup dalam bentuk alert pada terminal dan acidbase Kesimpulan pengujian : Berhasil

Tabel 3. Pengujian HTTP Attacking Pada *Server Snort IPS*

- **Pengujian Akses SSH**

Pada pengujian ini, penyerang akan mengakses Snort NIPS melalui SSH

➢ Kondisi Snort *Network Intrusion Prevention System* tidak aktif

Gambar 15. Akses SSH Berhasil

➢ Kondisi Snort *Network Intrusion Prevention System* aktif

Gambar 16. Akses SSH Gagal

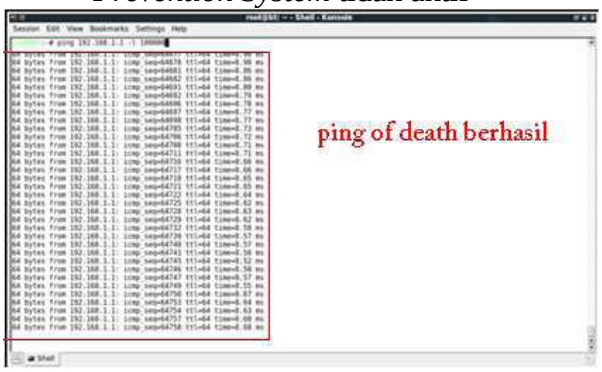
Deskripsi dan Prekondisi	Tools dan IP address penyusup	Prosedur Pengujian	Keluaran yang diharapkan	Hasil dan Kesimpulan
Snort Network Intrusion Prevention System (NIPS) dalam keadaan aktif	SSH 192.168.1.2	Penyusup melakukan login SSH pada *server* NIPS	Tampil IP address penyusup dalam bentuk alert dan sistem melakukan blocking IP address dan serangan	Tampil IP address penyusup dalam bentuk alert pada terminal dan acidbase Kesimpulan pengujian : Berhasil

Tabel 4. Pengujian *SSH Attacking* Pada *Server Snort IPS*

- **Pengujian *Ping of Death***

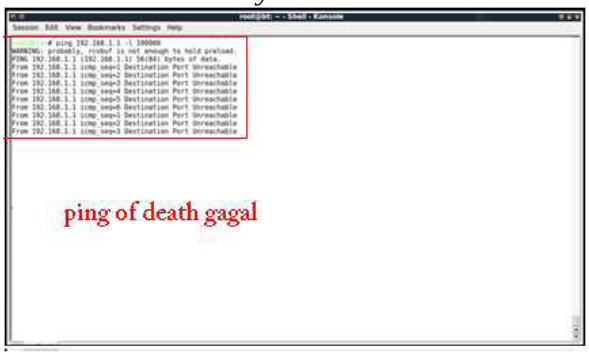
Pada pengujian ini, penyerang akan melakukan *Denial of Service* (DoS) berupa *Ping of Death*, yaitu dengan mengirimkan paket ICMP dalam jumlah besar ke *server* NIPS.

➢ Kondisi Snort *Network Intrusion Prevention System* tidak aktif



Gambar 17. *Ping Of Death* Berhasil

➢ Kondisi Snort *Network Intrusion Prevention System* aktif



Gambar 18. *Ping Of Death* Gagal

Deskripsi dan Prekondisi	Tools dan IP address penyusup	Prosedur Pengujian	Keluaran yang diharapkan	Hasil dan Kesimpulan
Snort Network Intrusion Prevention System (NIPS) dalam keadaan aktif	Terminal 192.168.1.2	Penyusup melakukan ping of death pada *server* NIPS	Tampil IP address penyusup dalam bentuk alert dan sistem melakukan blocking IP address dan serangan	Tampil IP address penyusup dalam bentuk alert pada terminal dan acidbase Kesimpulan pengujian : Berhasil

Tabel 5. Pengujian *Ping Of Death* Pada *Server Snort IPS*

- **Analisa Hasil Pengujian**

Implementasi	Kelas Uji	Hasil	Deskripsi
Snort Network Intrusion Prevention System (NIPS)	Percobaan serangan penyusupan	Sesuai	Menghasilkan analisa yang seusai dengan metode yang digunakan dan konfigurasi yang dilakukan

Tabel 6. Hasil Pengujian *Snort Intrusion Prevention System* (*IPS*)

V. KESIMPULAN DAN SARAN

Kesimpulan

- Snort *Network Intrusion Prevention System* (NIPS) sangat cocok dikonfigurasikan pada sistem operasi Linux Ubuntu karena kemudahan dalam penggunaan dan kecocokan komponen utama dan komponen pendukung untuk mengkonfigurasikan Snort NIPS pada sistem operasi Linux Ubuntu.
- Snort NIPS bekerja dengan cara membangun sebuah Snort *engine* yang memonitor paket data dan mencocokkannya pada *rule* Snort. Jika paket data diidentifikasi sebagai serangan, *rule* akan memerintahkan *firewall* (IPTables) untuk mem-*block* serangan tersebut.
- Suatu serangan dapat terdeteksi atau tidak oleh Snort *engine* tergantung pada pola serangan yang ada pada *rule database* snort. Jika pola serangan tidak terdefinisi pada *rule database*, maka serangan akan dianggap sebagai paket data biasa.
- Snort *Network Intrusion Prevention System* (NIPS) mampu mendeteksi dan melakukan pencegahan terhadap serangan penyusupan berupa *host scanning* menggunakan *tool Angry IPScan*, *port scanning* menggunakan *tool Zenmap*, *http attacking* menggunakan *tool Mozilla*, *ssh*

attacking dan *ping of death* menggunakan *terminal* pada sistem operasi Linux Backtrack.

Saran

- Mengkonfigurasikan Snort secara otomatis dengan tampilan *Graphical User Interface* (GUI) agar memudahkan *network administrator* dalam mengelola dan meng-*update* Snort dan *Rules* Snort.
- Snort juga dapat digunakan sebagai sistem pencegah penyusupan dengan konfigurasi sms *server* agar pemberitahuan tentang penyusupan pada jaringan dapat segera diketahui oleh *network administrator* melalui pesan sms.

DAFTAR PUSTAKA

Setiawan, Deris.,(2010), Jurnal : *Intrusion Prevention System* (*IPS*) dan Tantangan dalam pengembanganya. (Dosen Jurusan Sistem Komputer FASILKOM UNSRI).

Shafi Imran Muhammad dkk. 2010. *Effectiveness of Intrusion Prevention Systems (IPS) in fast networks, Blekinge Institute Technology of Sweden*

Jr. Nathaniel Abraham S. dkk. 2009. Perancangan dan Implementasi *Intrusion Detection System* Pada Jaringan Nirkabel BINUS *University*, Jurusan Teknik Informatika, Universitas Bina Nusantara

Ariyadi Tamsir. 2012. Implementasi *Intrusion Prevention System (IPS)* Pada Jaringan Komputer Kampus B Universitas Bina Darma.

Jannah Miftahul dkk. 2014. Implementasi *Intrusion Detection System (IDS) Snort* Pada Laboratorium Jaringan Komputer LePKom Universitas Gunadarma Fakultas Teknologi Industri Jurusan Teknik Informatika Universitas Gunadarma

Hartono, Puji.,(2006), Jurnal : Sistem Pencegahan Penyusupan pada Jaringan berbasis *Snort IDS* dan *IPTables Firewall*.

Slamet. 2014. *Intrusion Preventing System* Pada Jaringan Wireless STIKOM Surabaya Menggunakan *SNORT* dan *IPTables*. Program Studi S1 Sistem Informasi, Institut Bisnis dan Informatika Stikom Surabaya.

Gondohanindijo Jutono. 2012. *IPS (Intrusion Prevention System)* Untuk Mencegah Tindak Penyusupan / Intrusi. Fakultas Ilmu Komputer Universitas AKI. Majalah Ilmiah INFORMATIKA Vol. 3 No. 3.

Tom, Thomas. 2005. *Networking Security First-Step*. Yogyakarta : Andi

SnortTM Users Manual. 2016. http://www.snort.org/. The Snort Project

Snort FAQ. 2016. http://www.snort.org/. The Snort Project