# Analisa dan Implementasi *Network Intrusion Prevention System* di Jaringan Universitas Sam Ratulangi

Mohamad Nurul Huda Monoarfa, Xaverius B.N. Najoan, ST.,MT., Alicia A.E. Sinsuw, ST., MT.
Jurusan Teknik Elektro-FT, UNSRAT, Manado-95115,
Email:110213013@student.unsrat.ac.id, xnajoan@unsrat.ac.id, alicia.sinsuw@unsrat.ac.id

***Abstract - Network security system becoming the most important thing for securing a network system, the attack that can disturb even damaged connection system between the connected devices will caused serious effect. To get security in a network sometimes we have to dealing with discomfort in use, this thing is often become a consideration in implementation of a network security system.***

***NIPS (Network Intrusion Prevention System) method able to detect and Drop on attack. Besides this method can do implementation on Linux operating system, using Snort in inline mode and able to prevent the attack that can harm.***

***System configuration built at Sam Ratulangi University local network that design to representation the test. Analysis results from every test conclude that each action taken by attackers on the network can be known and prevent, so that can be handle before it cause more damage.***

***Keywords : Network Security, Network Intrusion Prevention System, Denial of Service, Linux, Snort***

**Abstrak - Sistem keamanan jaringan menjadi hal yang sangat penting dalam menjaga sebuah jaringan, serangan yang bisa mengganggu bahkan merusak sistem koneksi antar perangkat yang terhubung akan sangat merugikan. Untuk mendapatkan keamanan dalam sebuah jaringan terkadang kita harus merasakan ketidaknyamanan dalam penggunaannya, hal inilah yang seringkali menjadi pertimbangan dalam penerapan sebuah sistem keamanan jaringan.**

**Metode NIPS (Network Intrusion Prevention System) mampu mendeteksi serangan dan melakukan Drop pada serangan. Melakukan penerapan pada sistem operasi Linux menggunakan Snort dalam mode inline dan mampu mencegah dari serangan yang dapat mengancam.**

**Konfigurasi sistem dibangun dalam jaringan local Universitas Sam Ratulangi yang dirancang untuk merepresentasikan pengujian. Hasil analisis dari setiap pengujian yang dilakukan menyimpulkan bahwa setiap tindakan yang dilakukan oleh penyerang terhadap jaringan dapat diketahui dan dicegah, sehingga dapat dilakukan penanganan sebelum terjadi kerusakan lebih luas.**

**Kata Kunci : Keamanan Jaringan, Network Intrusion Prevention System, Denial of Service, Linux, Snort.**

## I. PENDAHULUAN

Sudah bukan merupakan rahasia lagi bahwa internet dan teknologi informasi telah memberikan begitu banyak manfaat signifikan bagi kehidupan manusia. Dampak dari penerapan teknologi informasi ini begitu terasa di berbagai sektor kehidupan, seperti pemerintahan, ekonomi, dan terutama pendidikan. Secara umum, yang disebut jaringan komputer adalah beberapa komputer yang saling terhubung dan melakukan komunikasi satu dengan yang lain menggunakan perangkat keras jaringan (*ethernet card, token ring, bridge, modem*, dan lainnya). Komputer yang berada dalam suatu jaringan dapat melakukan tukar-menukar informasi/data dengan komputer lain yang berada dalam jaringan tersebut. Penggunaan suatu computer dapat melihat dan mengakses data pada komputer lain dalam jaringan apabila dilakukan file sharing.

Seperti mata uang dengan dua sisi, selain sisi manfaat yang ditawarkan, terdapat pula sisi resiko yang dapat memberikan dampak negatif, yang menimbulkan masalah baru yang sangat mengancam yaitu masalah keamanan jaringan. Ancaman keamanan ini banyak sekali ditemukan oleh user seperti *virus, Malicious, Trojan, Worm, DoS, Hacker, Spoofing, Sniffing, Spamming, Crackers* dan lain sebagainya, yang membuat taknyaman serta mengancam sistem dan data pada saat kejadian ini menyerang jaringan. Semakin besar suatu jaringan maka semakin kompleks administrasi dari jaringan itu, oleh karena itu diperlukan suatu pencegahan dan metode untuk memonitor ancaman-ancaman dalam jaringan.

Keamanan jaringan komputer sebagai bagian 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. Sistem keamanan komputer, dalam beberapa tahun ini telah

Hal ini disebabkan tingginya ancaman yang mencurigakan (*Suspicious Threat*) dan serangan dari internet. Keamanan komputer merupakan salah satu kunci yang dapat mempengaruhi tingkat Reliability (keandalan) termasuk *performance* (kinerja) dan *Availability* (ketersediaan) suatu internetwork.

Universitas Sam Ratulangi merupaka salah satu instansi yang aktivitasnya didiukung oleh layanan jaringan internet, mulai dari mengolah data yang ada, diantaranya KRS (Kartu Rencana Studi*) online, mail server* dan *web portal* di tiap unit kerja. Administrator jaringan Universitas Sam Ratulangi membangun sistem keamanan jaringan dengan menerapkan sistem firewall dan proxy server pada tiap unit server.

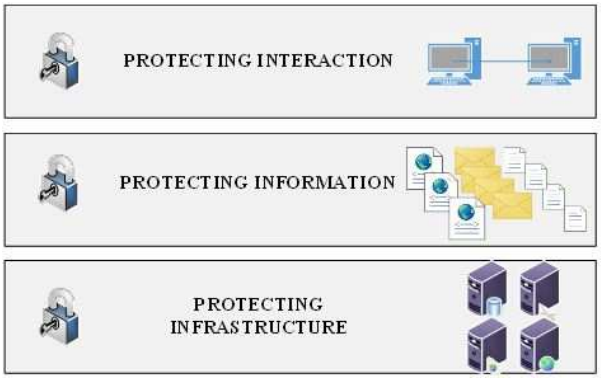
Oleh karena itu, penerapan NIPS (*Network Intrusion Prevention System*) diusulkan sebagai salah satu solusi yang dapat digunakan untuk membantu pengaturan dalam memonitor kondisi jaringan, menganalisa paket-paket serta mencegah segala yang dapat membahayakan jaringan tersebut, hal ini bertujuan untuk mengatasi segala ancaman seperti *hacker, cracker* dan user yang tidak dikenal.

## II. LANDASAN TEORI

Menurut definisi, jaringan komputer (*computer network*) adalah himpunan interkoneksi sejumlah komputer *autonomous*. Kata "*autonomous*" mengandung pengertian bahwa komputer tersebut memiliki kendali atas dirinya sendiri. Bukan merupakan bagian komputer lain, seperti sistem terminal yang biasa digunakan pada komputer *mainframe*. Komputer juga tidak mengendalikan komputer lain yang dapat mengakibatkan komputer lain *restart, shutdown*, merusak file, dan sebagainya.

### *A. Keamanan Jaringan dan Informasi*

Serangan yang cenderung bersifat destruktif tersebut sudah selayaknya harus ditangkal dan dihindari agar tidak merugikan banyak pihak. Oleh karena itu sejumlah usaha pengamanan jaringan harus dilakukan oleh mereka yang berkepentingan. Secara fisik ada tiga cara memproteksi. Cara pertama adalah memproteksi infrastruktur tempat mengalirnya data dan informasi dalam proses transmisi. Secara fisik maupun operasional harus dilindungi dan diproteksi dari beraneka ragam potensi gangguan yang mungkin timbul. Cara kedua adalah memproteksi data, informasi, atau konten yang ada dan / atau mengalir dalam sebuah sistem komunikasi dan teknologi informasi. Metode seperti penyandian atau kriptografi informasi merupakan salah satu cara umum dan ampuh untuk dilaksanakan oleh para stakeholder teknologi informasi. Dengan disandikannya atau diacaknya data maupun pesan elektronik tersebut, maka akan mempersulit para




*Gambar 1. Jenis-jenis Proteksi*

pencuri data untuk mengetahui isi sesungguhnya. Untuk memahami lebih lanjut berikut gambar 1 menjelaskan tentang jenis-jenis proteksi pada jaringan dan informasi. Cara ketiga adalah melakukan proteksi terhadap komponen-komponen terkait dengan proses interaksi. Mulai dari pemilihan jenis media dan perangkat lunak komunikasi *email, chatting, browsing, blogging* dan lain sebagainya – hingga melakukan setting konfigurasi program agar keamanan proses interaksi yang melibatkan transaksi keuangan misalnya, perlu ditambahkan mekanisme standar pengamanan dan prosedur khusus agar tidak terjadi kebocoran dan pencurian data.

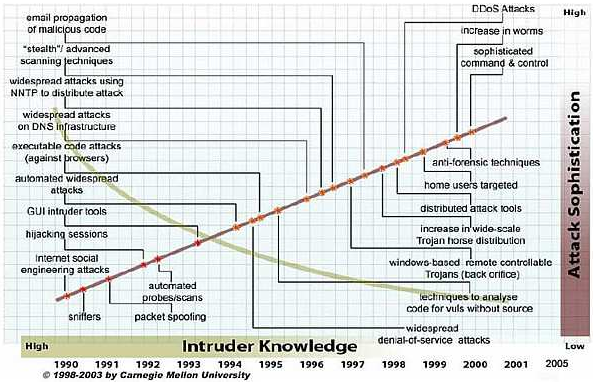
### *B. Ancaman dan Serangan Sistem Jaringan*

Suatu jaringan terdiri dari banyak titik terminal (*nodes*) yang disambungkan satu sama lain menjadi garis komunikasi. Fungsi tertentu dilakukan pada terminal-terminal tersebut misalnya penyimpanan data atau meneruskan data yang dikirim ke terminal yang lain, routing dan rerouting, melakukan suatu tindakan apabila terjadi kegagalan fungsi, penggunaan oleh user, dan lain-lain. Oleh karena itu, resiko pada masing-masing node sangat tinggi, dibandingkan dengan jaringan sendiri.

Beberapa resiko keamanan jaringan diantaranya:

- Mengakses jaringan atau aplikasi oleh user yang tidak memiliki wewenang dari terminal sendiri atau dari nodes network lain.
- Mengganggu atau mengacaukan pengiriman data yang rahasia dengan mencegat dan memanipulasi.
- Kegagalan jaringan atau putus hubungan jaringan.

Serangan atau ancaman terhadap jaringan yang merupakan pintu gerbang untuk menyerang sistem suatu instansi. Sesuai dengan sifat dan karakteristiknya,




*Gambar 2. Berbagai jenis serangan ke system*

semakin lama model serangan yang ada semakin kompleks dan sulit dideteksi dan dicegah. Gambar 2 menjelaskan berbagai jenis serangan yang terjadi dari tahun ke tahun.

### *C. Intrusion Prevention System*

Intrusion Prevention System adalah sebuah aplikasi yang bekerja untuk mendeteksi aktivitas mencurigakan, dan melakukan pencegahan terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti bagaimana mestinnya.

Produk IPS sendiri dapat berupa perangkat keras (Hardware) atau perangkat lunak (Software). Secara umum, ada dua jenis IPS, yaitu *Host-based Intrusion Prevention System* (HIPS) dan *Network Intrusion Prevention System* (NIPS).

- *Host Based* IPS (HIPS) bekerja dengan memaksa sekelompok perangkat lunak fundamental untuk berkovensi secara konstan. Hal ini disebut dengan *Application Binary Interface* (ABI).
- *Network Based* IPS (NIPS) melakukan pantauan dan proteksi dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan *firewall*. NIPS biasanya dibangun dengan tujuan tertentu, sama halnya dengan *switch* dan *router*.Beberapa teknologi sudah diterapkan pada NIPS, seperti *signature matching*, analisa protocol dan kelainan pada protocol, identifikasi dari pola trafik, dan sebagainya. NIPS dibuat untuk menganalisa, mendeteksi, dan melaporkan seluruh arus data dan disetting dengan konfigurasi kebijakan keamanan NIPS, sehingga segala serangan yang datang dapat langsung terdeteksi dan langsung di blokir.

### *D. Protokol-protokol Jaringan*

Protokol merupakan himpunan aturan-aturan yang memungkinkan komputer satu dapat berhubungan dengan komputer yang lain. Aturan-aturan ini meliputi tatacara bagaimana agar komputer bisa saling berkomunikasi, biasanya berupa bentuk (model) komunikasi, waktu (saat berkomunikasi), barisan (traffic saat berkomunikasi), pemeriksaan error saat transmisi data, dan lain-lain.

Protokol jaringan adalah berbagai protokol yang terdapat dari lapisan teratas sampai terbawah yang ada dalam sederetan protokol. Dipandang dari sudut komunikasi data, ada beberapa protocol yang banyak digunakan pada jaringan komputer, di antaranya:

- TCP/IP merupakan protokol standar pada jaringan internet yang tidak tergantung pada jenis komputer yang digunakan. Dengan menggunakan TCP/IP akan memungkinkan berbagai komputer (seperti PC IBM/Machintosh/Sun/HP/ dll) berinteraksi satu dengan lain tanpa mengalami masalah yang berarti. Barangkali perlu dicatat bahwa TCP/IP adalah perlengkapan standar pada sistem operasi *UNIX* dan turunannya. Saat ini mesin Novell, SUN maupun Machintosh sudah dilengkapi protokol standar TCP/IP ini.
- *User Datagram Protocol* (UDP) adalah sebuah protokol yang bekerja pada transport layer, mulai digunakan dan dikembangkan oleh *US Department of Defence* (DoD) untuk digunakan bersama protokol IP di network layer. Protokol UDP memberikan alternatif transport untuk proses yang tidak membutuhkan pengiriman yang handal. UDP tidak handal karena tidak menjamin pengiriman data atau perlindungan duplikasi. UDP tidak mengurus masalah penerimaan aliran data dan pembuatan segmen yang sesuai untuk IP.

### *E.Ubuntu*

Ubuntu adalah salah satu distro linux yang berbasis Debian dan didistribusikan secara *freeware*. Ubuntu merupakan sistem operasi yang mengemas paket secara lengkap. Ubuntu merilis versi terbarunya setiap 6 bulan sekali dan setiap upgrade ataupun update-nya bersifat gratis. Ubuntu juga menyediakan versi *Long Time Support* (LTS). Versi ini akan di-support selama 3 tahun untuk versi desktop dan 5 tahun untuk *versi server*.

### *F. Snort*

Snort merupakan salah satu *tool Network Intrusion Prevention System* (NIPS). Snort ditulis oleh Martin Roesch dan sekarang dikelola oleh *Sourcefire*, di mana Roesch bertindak sebagai pendiri dan CTO *(Chief of Technical Officer*). Versi entrerprise dari snort terintegrasi dengan hardware tertentu dan jasa dukungan komersial dijual oleh *Sourcefire*. Secara Prinsip snort memerankan tiga fungsi utama:

- Sebagai penangkal program-program sniffer paket-paket.
- Sebagai packet logger (berguna untuk men-debug trafik-trafik jaringan).
- Sebagai system pencegah intrusi untuk system-sistem jaringan.

## III. METODOLOGI PENELITIAN

### *A. Metode Pengumpulan Data*

*1) Studi Pustaka*

Studi Pustaka merupakan metode pengumpulan data melalui buku atau browsing internet yang dijadikan sebagai acuan analisa penelitian tentang Network Intrusion Prevention System.

*2) Studi Lapangan*

Penulis melakukan penelitian di UPT Teknologi dan Informasi Universitas Sam Ratulangi

### *B. Metode Pengembangan Sistem*

SPDLC (*Security Policy Development Life Cycle)* adalah metode yang menetapkan strategi untuk melakukan pembaharuan suatu organisasi dari sistem jaringan, siklus hidup pengembangan sistem jaringan didefinisikan pada sejumlah fase. SPDLC yang diambil melakukan penelitian dalam tahap :

1) *Analysis*

TABEL I. SPESIFIKASI SISTEM YANG AKAN DIBANGUN

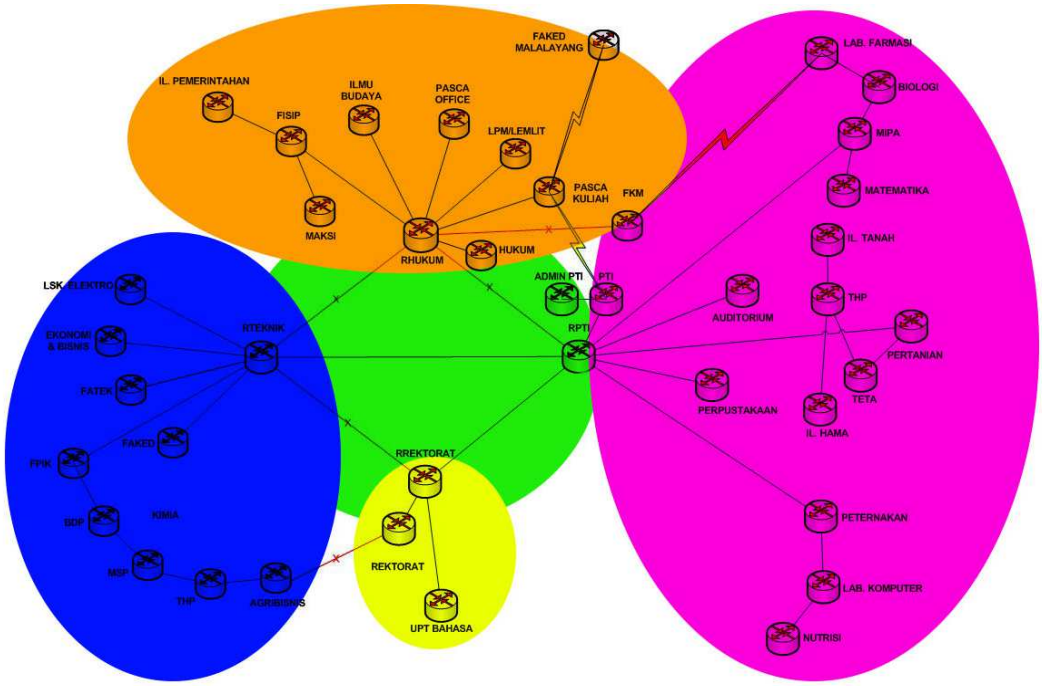
| Sistem | Keterangan |
|---|---|
| Network Intrusion Prevention System | Yaitu Sistem yang dibangun untuk mencegah terjadinya serangan-serangan dari intruder |
| Victim Server | Bertindak sebagai server yang akan digunakan sebagai tujuan dari penyerangan |
| Clients | Bertindak sebagai system client segmen jaringan local. Difungsikan sebagai system penyerang untuk menguji fungsional *NIPS*. |

TABEL II. SPESIFIKASI *SOFTWARE* YANG DIBUTUHKAN

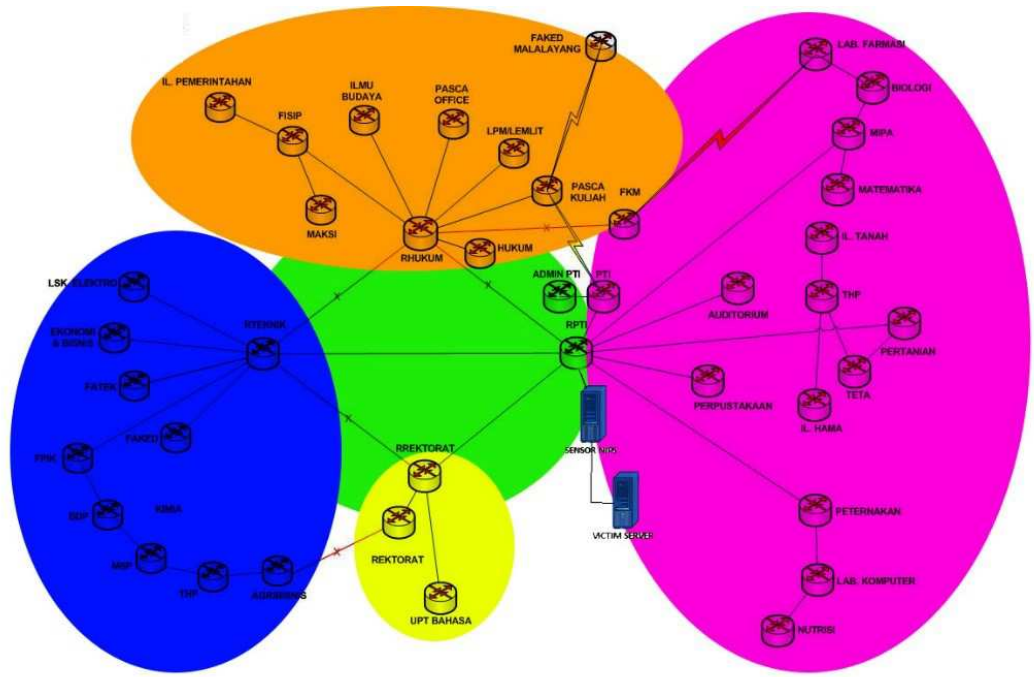
| No | Spesifikasi Software | Keterangan |
|---|---|---|
| **I** | **Sistem Operasi** | |
| 1 | Ubuntu 14.04 | Sistem Operasi yang digunakan pada sensor NIPS dan victim server |
| 2 | Kali Linux 2.0 | Sistem Operasi client difungsikan sebagai penyerang dan menguji fungsionalitas mesin sensor NIPS |
| **II** | **Software Perangcangan Topologi** | |
| 1 | Microsoft Visio | |
| **III** | **Software sensor *NIPS*** | |
| 1 | Snort | Program *NIPS* Open Source |
| **IV** | **Software Penguji Serangan *NIPS*** | |
| 1 | Http brute force | Program yang dijalankan dengan NMAP |

TABEL III. SPESIFIKASI *HARDWARE* YANG DIBUTUHKAN

| No | Spesifikasi Hardware | Spesifikasi Unit |
|---|---|---|
| **I** | **Perangkat Unit Host** | |
| 1 | PC Mesin Sensor | Proccessor Intel I5, Memory 8 GB, Harddisk 1TB |
| 2 | PC Victim Server | Proccessor Intel I5, Memory 4 GB, Harddisk 1TB |
| **II** | **Perangkat Jaringan** | |
| 1 | *Switch* | Cisco Small Business |
| 2 | *Network Interface Card (NIC)* | TP-Link 1Gbps |
| 3 | Kabel UTP | Kabel UTP cat 5e |




*Gambar 3. Topologi Jaringan UNSRAT sebelum diterapkan NIPS*




*Gambar 4. Topologi Jaringan UNSRAT setelah diterapkan NIPS*

Pada tahap ini dilakukan perumusan masalah, mengidentifikasi konsep dari NIPS, dan beberapa perangkat jaringan, mengumpulkan data dan mengidentifikasi kebutuhan seluruh kompunen sistem tersebut, sehingga spesifikasi kebutuhan sistem NIPS dan Snort dapat diperjelas dan perinci. Model SPDLC memulai siklus pengembangan sistem jaringannya pada tahap analisis. Pada tahap ini di analisa spesifikasi sistem yang akan dibangun, perangkat yang dibutuhkan seperti perangkat lunak *(software*) dan perangkat keras *(hardware*) yang dibutuhkan untuk sistem NIPS pada jaringan UNSRAT.

Dalam sistem yang akan dibangun (lihat tabel I) tentu membutuhkan *Hardware* dan *Software* guna menunjang sistem NIPS, berikut adalah spesifikasi *Hardware* dan *Software* yang digunakan. Tabel II dan tabel III menjelaskan tentang spesifikasi *hardware* dan *software* yang dipakai.

*2) Design*

Tahap ini merupakan perancangan mendefinisikan "bagaimana cara sistem tersebut dapat berjalan". Pada fase ini dilakukan desain sistem sesuai dengan data dari fase analisa. Pada tahap ini yang dilakukan adalah :

- Merancang topologi jaringan untuk peletakkan sensor NIPS.
- Merancang penggunaan sistem operasi dan aplikasi pada *Victim Server*,sensor NIPS dan komputer penyusup. Rancangan topologi jaringan dibangun dengan menggunakan Microsoft Visio yang di instal.

  Pada tahap ini ditentukukan sistem yang dibangun dan mendefinisikan konfigurasi yang dibutuhkan untuk menjamin sistem jaringan komputer agar dapat berjalan dengan baik**.** Gambar 3 adalah topologi jaringan UNSRAT sebelum penerapan NIPS.

NIPS ditempatkan diantara *Victim Server* seperti pada gambar 4 dan jaringan lokal untuk melakukan pengawasan terhadap *Traffic* data yang berasal dari semua alat-alat jaringan dan menuju *Victim Server*. Semua *Traffic* yang menuju *ke Victim Server* di Scan atau diperiksa untuk memastikan apakah Paket-paket data yang dikirimkan tidak terindikasi sebagai sebuah intrusi.

3) *Implementation*

Dimana fase ini, rancangan solusi pada fase perancangan digunakan sebagai panduan instruksi implementasi pada ruanglingkup WAN (*Wide Area Network*). Aktivitas yang dilakukan pada fase ini diantaranya adalah instalasi dan konfigurasi terhadap topologi jaringan, NIPS Snort dan perangkat lainnya.

Detail rancangan akan digunakan 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. Perangkat ini meliputi *hardware* dan *software*. Setelah itu, menempatkan seluruh perangkat sesuai dengan topologi yang sudah dibuat. Setelah semua unit terhubung satu sama lain, proses selanjutnya adalah mengkonfigurasi setiap unit agar dapat berkomunikasi satu dengan lainnya.

Perangkat *switch* yang digunakan tidak membutuhkan konfigurasi. Sejumlah parameter dari unit mesin sensor NIPS dan *Victim Server* yang harus dikonfigurasi adalah alamat internet protocol, subnet mask, alamat IP *gateway*,IP *Route* dan alamat IP DNS. Setelah instalasi dan konfigurasi selesai dilakukan, proses selanjutnya adalah pengujian untuk memastikan fungsionalitas koneksi, hal ini dimaksudkan untuk menjamin agar mesin yang satu dapat berkomunikasi dengan unit mesin lain.

*4) Enforcement*

Setelah tahap implementasi adalah tahap Enforcement dimana tahap ini penting. Proses pelaksanaan atau penyelenggaraan dilakukan melalui aktivitas pengoprasian dan pengamatan sistem yang sudah dibangun dan diterapkan apakah sistem NIPS sudah berjalan dengan benar dan baik. Pengujian skenario yang dilakukan yaitu :

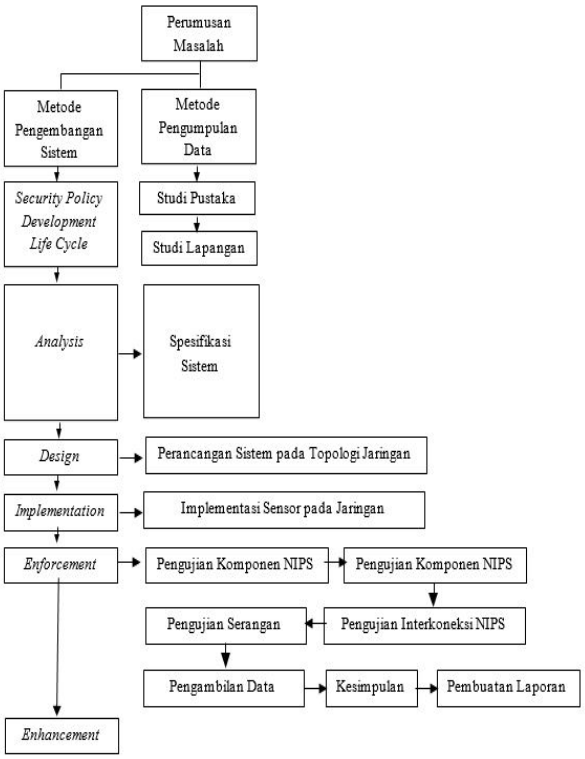
- Skenario pengujian komponen NIPS.
- Skenario pengujian fungsionalitas interkoneksi NIPS.
- Skenario pengujian serangan.

Pengujian serangan yang dilakukan menggunakan aplikasi *Http Brute Force Attack* yang dapat memecahkan password dari *Victim Server* sehingga menyebabkan diketahuinya *password server* oleh orang-orang yang tidak berhak dan menyebabkan turunnya performa server.

*5) Enhancement*

Pada fase ini meliputi aktivitas perbaikan terhadap sistem yang telah dibangun. Fase *enhancement* melalui serangkaian proses perbaikan dilakukan untuk sejumlah tujuan:

- Memperbaiki sejumlah kesalahan yang terdapat pada penerapan sistem sebelumnya (sistem yang sudah ada).
- Menambahkan fungsionalitas atas komponen spesifik atau fitur tambahan terbaru untuk melengkapi kekurangan pada sistem sebelumnya.



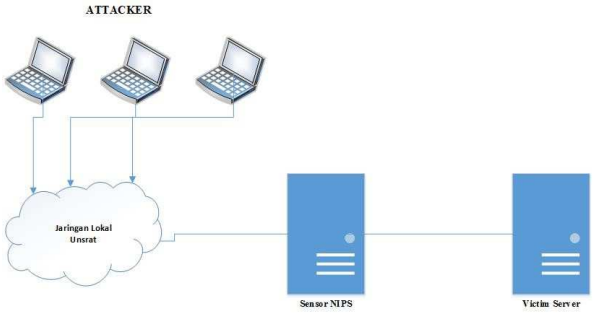

Gambar 5. Diagram Alur Penelitian

Dengan demikian, fase perbaikan dapat secara efektif menjamin kehandalan kinerja dari NIPS.

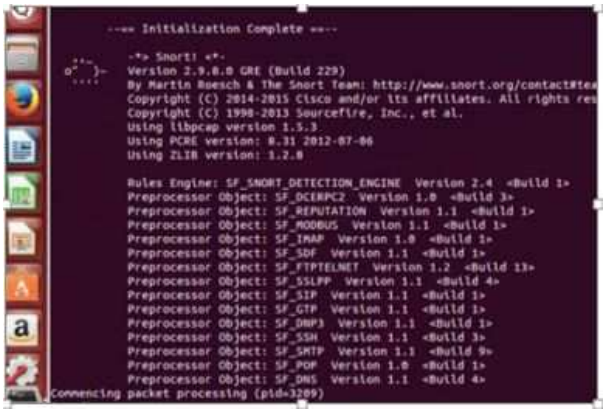
## C. *Alur Metode Penelitian*

Tahapan dalam penelitian ini telah digambarkan dalam diagram alur penelitian yang sebelum memasuki dan keluar dari model atau metode pengembang dari SPDLC terdapat beberapa tahap yang harus dilakukan. SPDLC adalah metode yang menetapkan strategi untuk melakukan pembaharuan suatu organisasi dari sistem jeringan. Tahapan-tahapan dari SPDLC yang diambil dalam melakukan peneitian pengembangan aplikasi ini mulai dari perumusan masalah sampai dengan tahap *Enhancement* dapat dilihat pada gambar 5

Pada tahap ini dilakukan perumusan masalah, mengidentifikasi konsep dari NIPS, dan beberapa perangkat jaringan, mengumpulkan data dan mengidentifikasi kebutuhan seluruh kompunen sistem tersebut, sehingga spesifikasi kebutuhan sistem NIPS dan Snort dapat diperjelas dan perinci. Model SPDLC memulai siklus pengembangan sistem jaringannya pada tahap analisis. Pada tahap ini di analisa spesifikasi sistem yang akan dibangun, perangkat yang dibutuhkan seperti perangkat lunak (*software*) dan perangkat keras *(hardware*) yang dibutuhkan untuk sistem NIPS pada jaringan UNSRAT.




*Gambar 6. Skema Pengujian Komponen NIPS*




*Gambar 7. Pengujian Fungsi Snort Inline*

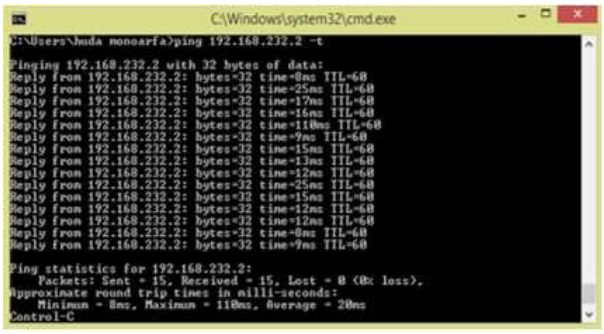
# IV. HASIL DAN PEMBAHASAN

## A. *Pengujian Komponen NIPS*

Pada pembahasan ini, dengan menggunakan beberapa aplikasi yang digunakan untuk melakukan penyerangan terhadap jaringan yang ada. Hal ini ditujukan untuk mengetahui jenis serangan apa saja yang sering dilakukan oleh para *hacker* serta serangan tersebut dilakukan melalui *port* mana saja yang sering digunakan. Jenis serangan yang akan coba dilakukan adalah berupa *Http Brute Force Attack.* Skema Pengujian seperti pada gambar 6.

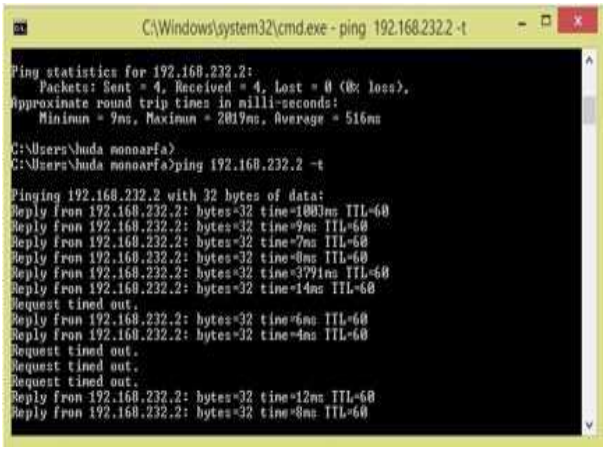
### 1) *Pengujian Snort*

Pengujian Snort pada mesin Sensor dilakukan dengan menggunakan *rules* yang telah di buat dan memastikan Snort dapat mendeteksi rules tersebut. Snort diaktifkan dengan perintah berikut, agar dapat mencetak hasilnya langsung ke layar console “sudo /usr/local/bin/snort -A console -Q -c /etc/snort/snort.conf -i eth1:eth2 –N”. hasilnya seperti pada gambar 7.

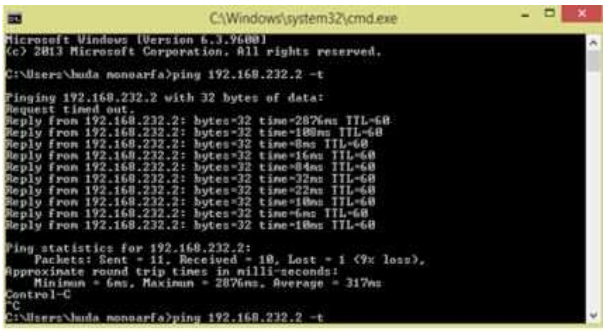



*Gambar 8.Uji Coba Jaringan Sebelum Penyerangan*

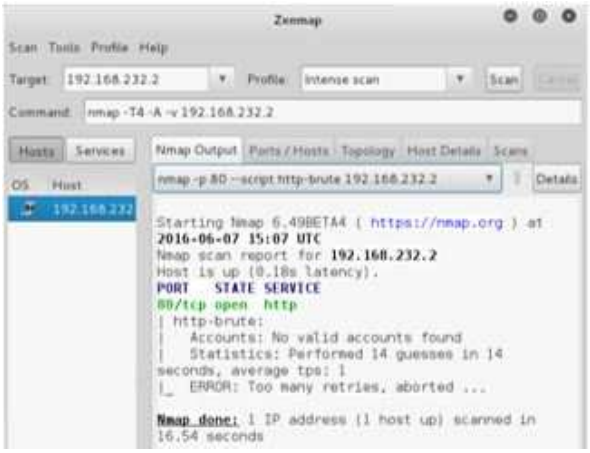

*Gambar 9. Serangan Brute Force Attack*



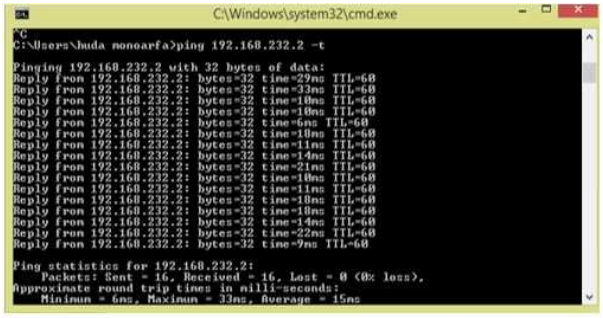

*Gambar 10. Uji coba Pada Saat Terjadi Serangan*



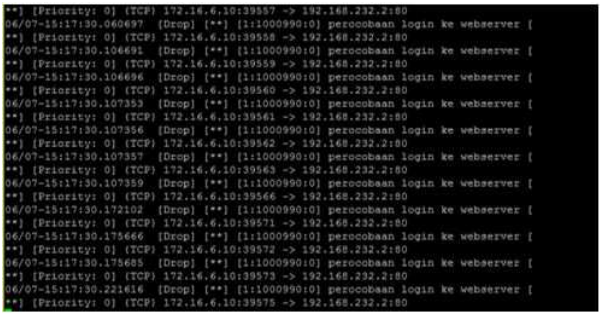

*Gambar 11. Uji coba Jaringan Pada Saat Pemasangan Sensor NIPS*



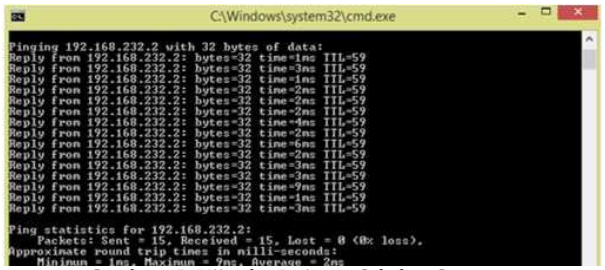

*Gambar 12. Serangan Brute Force Attack*




*Gambar 13. Uji coba Jaringan Pada Saat Serangan*

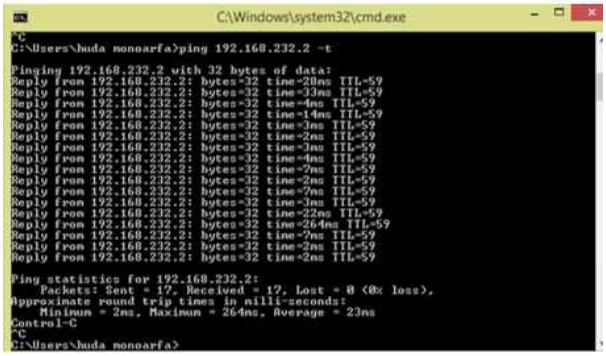



*Gambar 14. Tampilan Dari Hasil Penanganan Serangan*

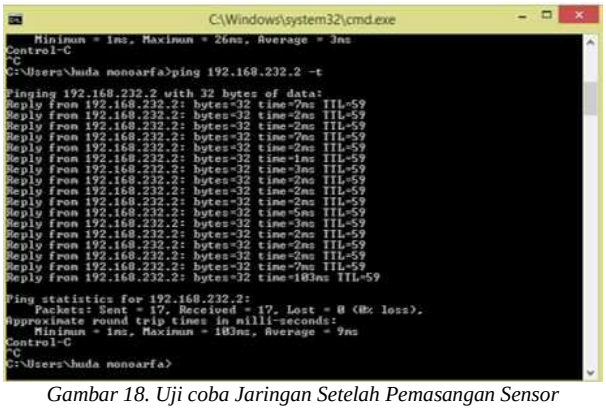



*Gambar 15. Uji coba Jaringan Sebelum Serangan*

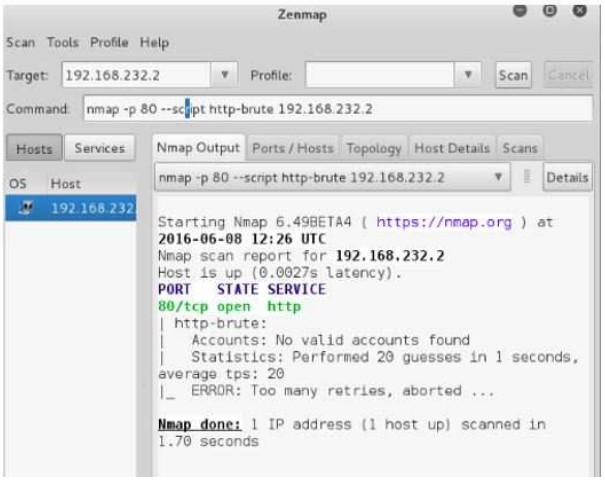

*Gambar 16. Serangan Brute Force Attack*




*Gambar 17. Uji coba Jaringan pada Saat Terjadi Serangan*

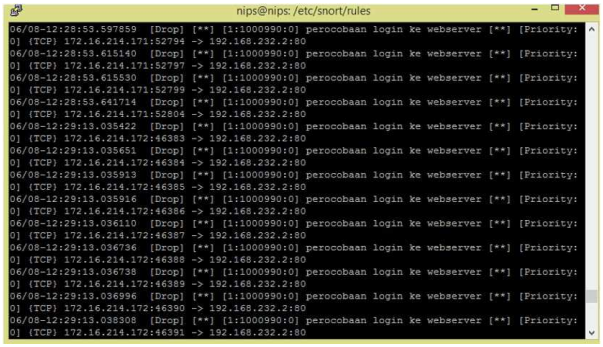



*Gambar 18. Uji coba Jaringan Setelah Pemasangan Sensor*




*Gambar 19. Serangan Brute Force Attack*


*Gambar 20. Uji coba Jaringan Pada Saat Terjadi Serangan*




*Gambar 21. Tampilan Dari Hasil Penanganan Server*

## *B. Pengujian NIPS*

1) Skenario 1 : Serangan dilakukan dari *Router* Kedokteran Malalayang.
   Pada tahap pertama skenario ini, dilakukan penyerangan serta proses alisis jenis serangan. Langkah awal yang dilakukan adalah menguji apakan *Victim Server* tersebut dalam keadaan aktif atau tidak dengan catatan sensor NIPS belum diaktifkan. Uji coba dilakukan dengan cara melakukan PING ke *Victim Server* (PING 192.168.232.2) seperti pada gambar 8.

Kemudian setelah melakukan uji coba jaringan, dilakukan pula uji coba serangan dengan cara mengirimkan *Http Brute Force Attack* ke *Victim Server* tanpa pengaktifan sensor.

Terlihat gambar 9 yakni ketika serangan diluncurkan dengan mengetikkan *command* pada aplikasi zenmap yaitu *nmap –script http-brute –p 80 192.168.232.2.* dari data pada serangan dapat dilihat bahwa telah melancarkan 39 kali percobaan login dengan waktu 25 detik kemudian menemukan *account = web* dan *password = web* dari *Victim Server*. Pada saat yang bersamaan juga dilakukan uji coba jaringan pada saat terjadi serangan tanpa pengaktifan sensor NIPS ditunjukkan pada gambar 10.

Dapat dilihat bahwa terjadi perubahan pada para Time atau waktu yang dibutuhkan packet untuk mencapai *Victim Server*.

Kemudian setelah itu dilakukan tahap kedua yaitu mengulangi langkah pertama tapi kali ini dengan mengaktifkan sensor NIPS. Hal yang pertama dilakukan adalah melakukan uji coba jaringan setelah pemasangan sensor NIPS, dapat dilihat pada gambar 11.

Dapat dilihat pada gambar 11, bahwa jaringan terlihat cukup stabil setelah pemasangan sensor NIPS. Langkah selanjutnya yaitu pengujian serangan terhadap *Victim Server* setelah pemasangan sensor NIPS, serangan yang dilakukan tetap sama seperti tipe serangan sebelumnya yakni *http-brute force attack* seperti pada gambar 11.

Dari hasil serangan pada gambar 12, dapat dilihat bahwa penyerang tidak dapat menemukan *Account* dan *Password* dari *Victim Server*. Hal ini berarti sensor NIPS dapat mencegah serangan sebelum menembus *Victim Server.*

Pada gambar 13, dapat dilihat bahwa meskipun terjadi serangan tetapi tidak mempengaruhi waktu tempuh *packet* ke *Victim Server*.

Dari gambar 14 dapat dilihat bahwa sensor NIPS berhasil melakukan *Drop packet* yang terindikasi serangan.

2) Skenario 2 : Serangan Dilakukan di Router LSK Elektro.

Hal pertama yang dilakukan adalah menguji apakan *Victim Server* tersebut dalam keadaan aktif atau tidak dengan catatan sensor NIPS belum diaktifkan. Uji coba dilakukan dengan cara melakukan PING ke *Victim Server* (PING 192.168.232.2) seperti pada gambar 15.

Kemudian setelah dilakukan uji coba jaringan, selanjutnya dilakukan uji coba serangan dengan cara melakukan *http brute Force Attack* terhadap *Victim Server* tanpa pengaktifan sensor, seperti gambar 16.

Terlihat gambar 16 yakni ketika serangan diluncurkan dengan mengetikkan *command* pada aplikasi zenmap yaitu *nmap –script http-brute –p* 80 192.168.232.2. dari data pada serangan dapat dilihat bahwa telah melancarkan 39 kali percobaan login dengan waktu 25 detik kemudian menemukan *account = web dan password = web* dari *Victim Server*. Pada saat yang bersamaan juga dilakukan uji coba jaringan pada saat terjadi serangan tanpa pengaktifan sensor NIPS, dapat dilihat pada gambar 17.

Dapat dilihat bahwa terjadi perubahan pada Time atau waktu yang dibutuhkan packet untuk mencapai *Victim Server*.

Kemudian setelah itu dilakukan tahap kedua yaitu mengulangi langkah pertama tapi kali ini dengan mengaktifkan sensor NIPS. Hal yang pertama dilakukan adalah melakukan uji coba jaringan setelah pemasangan sensor NIPS.

Dapat dilihat pada gambar 18 bahwa jaringan terlihat cukup stabil setelah pemasangan sensor NIPS. Langkah selanjutnya yaitu pengujian serangan terhadap *Victim Server* setelah pemasangan sensor NIPS, serangan yang dilakukan tetap sama seperti tipe serangan sebelumnya yakni http-brute *force attack*, seperti pada gambar 19.

Dari hasil serangan pada gambar 19 dapat dilihat bahwa penyerang tidak dapat menemukan Account dan Password dari *Victim Server*. Hal ini berarti sensor NIPS dapat mencegah serangan sebelum menembus *Victim Server*.

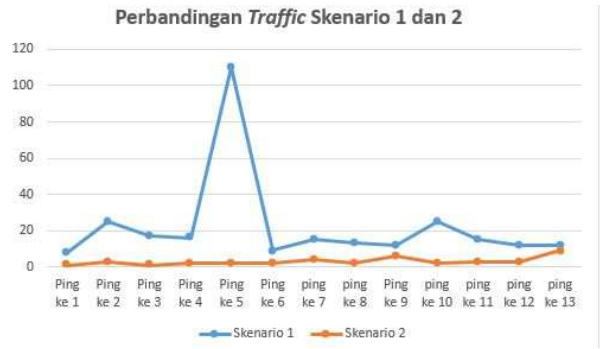
Pada gambar 20, dapat dilihat meskipun terjadi serangan tetapi waktu tempuh *packet* ke server tetap stabil.

Pada gambar 21 dapat dilihat bahwa sensor NIPS berhasil melakukan Drop packet yang terindikasi serangan.

Hal yang membedakan antara Skenario 1 dan skenario 2 adalah media transmisi data. *Router* Kedokteran malalayang menggunakan media transmisi radio agar bisa terhubung ke *Victim Server* sedangkan *Router* LSK Elektro Menggunakan media transmisi *Fiber Optic.*

### *C. Analisa Traffic*

Analisa *Traffic* yang dilakukan berupa perbandingan *Traffic* yang terjadi antara skenario 1 dan skenario 2, baik kondisi sebelum dan sesudah penerapan sensor.




*Grafik 1. Perbandingan Traffic Awal Pada Skenario 1 dan 2*


*Grafik 2. Perbandingan Grafik Pada Saat Terjadi Serangan*


*Grafik 3. Perbandingan Traffic Skenario 1 dan 2 pada penerapan sensor NIPS*


*Grafik 4. Perbandingan Traffic Pada Saat Server Diserang*

1) *Analisa Traffic Sebelum Penerapan Sensor NIPS.*
Analisa ini meliputi perbandingan Traffic yang terjadi antara skenario 1 dan skenario 2 sebelum penerapan sensor.
Dari Grafik 1, dapat dilihat bahwa pada skenario 1 membutuhkan waktu lebih besar untuk mencapai *Victim Server*, dengan waktu maksimum terletak pada ping ke 5 dengan waktu 110ms, sedangkan pada skenario 2 waktu maksimum yang dibutuhkan untuk mencapai *Victim Server* adalah 9ms.

Selanjutnya adalah perbandingan Traffic jaringan setelah di serang :

Dari Grafik 2 dapat dilihat bahwa pada skenario 1 membutuhkan waktu lebih besar untuk mencapai *Victim Server*, dengan waktu maksimum terletak pada ping ke 5 dengan waktu 3791ms, sedangkan pada skenario 2 waktu maksimum yang dibutuhkan untuk mencapai *Victim Server* adalah 264ms.

2) *Analisa Traffic Setelah Penerapan Sensor NIPS*
Analisa ini meliputi perbandingan *Traffic* yang terjadi antara skenario 1 dan skenario 2 setelah penerapan sensor.

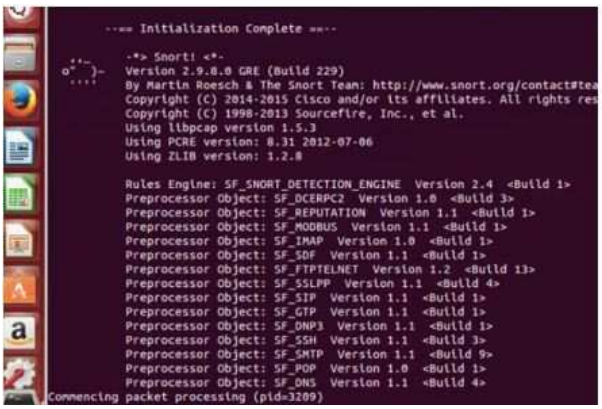
Dari Grafik 3, dapat dilihat bahwa pada skenario 1 membutuhkan waktu lebih besar untuk mencapai *Victim Server*, dengan waktu maksimum terletak pada ping ke 1 dengan waktu 2876ms, sedangkan pada skenario 2 waktu maksimum yang dibutuhkan untuk mencapai *Victim Server* adalah 103ms.

Selanjutnya adalah perbandingan *Traffic* jaringan setelah di serang :
Dari Grafik 4 dapat dilihat bahwa pada skenario 1 membutuhkan waktu lebih besar untuk mencapai *Victim Server*, dengan waktu maksimum terletak pada ping ke 2 dengan waktu 33ms, sedangkan pada skenario 2 waktu maksimum yang dibutuhkan untuk mencapai *Victim Server* adalah 5ms.

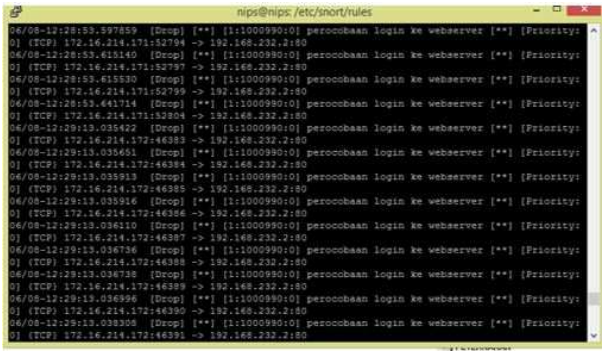
Dapat disimpulkan bahwa yang mempengaruhi *Traffic* jaringan antara Skenari 1 dan 2 adalah media transmisi dan juga jarak tempuh dari router ke *Victim Server*.

*D. Analisa Proses Pencegahan (Prevention)*

Proses ini aktif ketika terjedi penyerangan, pendeksian dan pencegahan dilakukan oleh sensor NIPS terjadi di snort pada saat packet melewati sensor, sensor melakukan *scan* terhadap *packet-packet* yang lewat dan memastikan bahwa packet tersebut aman dan kemudian di teruskan ke *Victim Server*, jika sensor mendeteksi




*Gambar 22. Tampilan Mesin Sensor Sebelum penyerangan*




*Gambar 23. Tampilan Sensor NIPS Pada Saat Penyerangan*

adanya kejanggalan maka secara automatis sensor men drop packet tersebut dan tak di teruskan ke *Victim Server*. Tampilan sensor NIPS snort sebelum terjadi serangan dapat dilihat pada gambar 22.

Pada saat terdeteksi, hasil dari proses analisis pendeteksian serangan yang dilakukan yaitu jumlah serangan, waktu terjadinya serangan, banyaknya paket data serangan yang dikirim, *IP Address* dari intruder dan langsung di cegah oleh sensor. Gambar 23 adalah tampilan kondisi pendeteksian saat sedan terjadinya serangan.

## V. KESIMPULAN DAN SARAN

### *A. Kesimpulan*

1) Sistem NIPS dalam mencegah serangan yang terjadi adalah dengan melakukan *scanning* terhadap sejumlah packet dan *Traffic* yang melewati sensor dalam jaringan.
2) Mekanisme sistem kerja snort yang telah berhasil di implementasikan dengan baik. Dalam pengujian sistem snort dilakukan dengan *Brute Force Attack*.
3) Pencegahan yang dapat dilakukan terhadap penyerangan adalah dengan menggunakan snort inline dipadukan dengan IPtables.

### *B. Saran*

1) Dianjurkan untuk menggunakan *Snort Enterprise* yang sudah terintgrasi dengan Cisco.
2) Menggunakan teknik pengujian lanjutan terhadap ancaman keamanan jaringan.

## DAFTAR PUSTAKA

[1] B. R. Andrew And J. Esler, " Snort IDS and IPS Toolkit", Syngress Publishing, Inc. Burlington, 2007

[2] B. Ari, " Ubuntu From Zero", Jasakom, Jakarta, 2010

[3] G.P. Reinhard," Invasi Terorisme ke Cyberspace", Yayasan Pengembangan Kajian Ilmu Kepolisian. Jakarta, 2015

[4] IBISA, " Keamanan Sistem Informasi". ANDI Yogyakarta, Yogyakarta, 2010

[5] I. E. Ricardus."Konsep dan Strategi Keamanan Informasi di Dunia Cyber", Graham Ilmu, Yogyakarta, 2014

[6] R. Mentang, "Perancangan dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS)", Skripsi Program S1 Teknik Informatika Universitas Sam Ratulangi, Manado, 2016.

[7] R. Rahmat, " Mengganyang Hacker dengan SNORT". ANDI Yogyakarta, Yogyakarta, 2010

[8] S. Iwan, " Teori dan Modul Praktikum Jaringan Komputer". Modula, Bandung, 2010

[9] S. Melwin, "Pengantar Jaringan Komputer". ANDI Yogyakarta, Yogyakarta, 2005

**Mohamad Nurul Huda Monoarfa** lahir Oktober 1993 pada tahun 2011 memulai pendidikan di Fakultas Teknik Universitas Sam Ratulangi Manado di Jurusan Teknik Elektro, dengan mengambil konsentrasi Minat Teknik Sistem Komputer pada tahun 2013. Dalam menempuh pendidikan penulis juga pernah melaksanakan Kerja Praktek yang bertempat di UPT. Teknologi Informasi Dan Komunikasi Universitas Sam Ratulangi pada Februari 2015 dan selesai melaksanakan pendidikan di Fakultas Teknik Elektro Universitas Sam Ratulangi Manado Agustus 2016, minat penilitiannya adalah tentang Analisa dan Implementasi *Network Intrusion Prevention System* di Jaringan Universitas Sam Ratulangi.