IMPLEMENTASI SISTEM KEAMANAN JARINGAN DENGAN MENGGUNAKAN INTRUSION DETECTION SISTEM (IDS)

STUDI KASUS : UNIVERSITAS SATYA NEGARA INDONESIA

SKRIPSI

Program Studi TEKNIK INFORMATIKA

OLEH :

NAMA : AGIL SAPUTRO

NIM : 011201503125086

FAKULTAS TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

J A K A R T A

2016

IMPLEMENTASI SISTEM KEMANAN JARINGAN DENGAN MENGGUNAKAN INTRUSION DETECTION SISTEM (IDS)

(STUDI KASUS : UNIVERSITAS SATYA NEGARA INDONESIA)

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar

SARJANA TEKNIK

Program Studi TEKNIK INFORMATIKA

OLEH :

NAMA : AGIL SAPUTRO

NIM : 011201503125086

FAKULTAS TEKNIK

UNIVERSITAS SATYA NEGARA INDONESIA

J A K A R T A

2016

ABSTRAK

Kelemahan sistem keamanan jaringan akan dimanfaatkan oleh penyusup (intruder) untuk melakukan serangan dengan cara mencuri data dan merusak jaringan komputer. Pada penelitian ini dilakukannya pencegahan penyusupan menggunakan Snort IDS dan Honeyd. Snort IDS ini bekerja dengan cara mendeteksi serangan yang telah dilakukan oleh penyusup (intruder). Setelah serangan berhasil terdeteksi, maka serangan tersebut akan dibelokkan ke server palsu (Honeyd).

Kata Kunci : Snort IDS, honeyd, penyusup, kinerja system.

ABSTRACT

Network security system weaknesses will be exploited by an intruder (Intruder) to carry out an attack with a way to steal data and damage computer networks. In this study, done using Snort IDS intrusion prevention and Honeyd. IDS Snort works by detecting attacks that have been carried out by the intruder (Intruder). After a successful attack is detected, then the attack will be diverted to a fake server (Honeyd).

Keywords: Snort IDS, Honeyd, intruder, the system performance.

KATA PENGANTAR

Dengan mengucapkan puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "**IMPLEMENTASI SISTEM JARINGAN DENGAN MENGGUNAKAN INTRUSION DETECTION SISTEM (IDS) (STUDI KASUS : UNIVERSITAS SATYA NEGARA INDONESIA)"**

Adapun maksud penyusunan skripsi ini adalah untuk memenuhi syarat dalam memperoleh gelar sarjana jenjang Strata 1 (Satu) program studi Teknik Informatika Fakultas Teknik Universitas Satya Negara Indonesia.

Dalam penulisan skripsi ini penulis banyak mendapatkan dukungan dan bantuan dari berbagai pihak yang sangat besar artinya bagi penulis. Oleh karena itu penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Ibu Ir. Nunung, Msi selaku Dekan Fakultas Teknik USNI.
2. Bapak Safrizal, ST, M.Kom, selaku Ketua Jurusan Teknik Informatika
3. Bapak Sukarno BN, S.Kom., M.Kom, selaku pembimbing pertama yang telah meluangkan waktu dan pikiran untuk memberikan bimbingan dan arahannya yang terbaik sehingga skripsi ini dapat selesai.
4. Bapak Faizal Zuli, M.Kom.,MTA. selaku pembimbing kedua yang telah meluangkan waktu dan pikiran untuk memberikan bimbingan dan arahannya yang terbaik sehingga skripsi ini dapat selesai.

5. Bapak Nanto, ST, yang telah memberikan waktu serta penjelasan tentang sistem Jaringan di Universitas Satya Negara Indonesi.
6. Seluruh Dosen Universitas Satya Negara Indonesia beserta para stafnya, yang telah memberikan ilmu dan membantu selama masa pendidikan.
7. Kedua Orang tua dan Keluarga yang telah memberikan doa serta dukungan baik moril maupun materil.
8. Alumni Aso dan bang Prian.
9. Sahabat seperjuangan Muhammad Ainul Yakin, Andry Mulyawan, Imam Wahyudi, Yoga Pratama, Irma Afliani, Richa Ashari, Ega, Susi atas dukungan dan bantuannya.
10. Semua rekan-rekan mahasiswa Teknik Informatika dan seluruh teman-teman Fakultas Teknik.

Penulis menyadari sepenuhnya dan mengharapkan saran dan masukan yang bersifat membangun demi bertambah baiknya tulisan ini dimasa yang akan datang, dengan tujuan dapat bermanfaat bagi pihak – pihak yang terkait dengan penulisan ini dan bagi kita semua.

Jakarta,

Penulis

DAFTAR ISI

BAB II LANDASAN TEORI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

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 atau pemindaian oleh pihak yang tidak berhak. Banyak serangan yang terjadi pada jaringan komputer dapat diketahui setelah adanya kejadian-kejadian yang aneh pada jaringan. Para administrator tidak bisa mengetahui dengan pasti apa yang terjadi, sehingga dibutuhkan waktu yang cukup lama untuk mengaudit sistem guna mencari permasalahan yang telah terjadi. Untuk mengatasi masalah tersebut dibutuhkan suatu tools yang mampu mendeteksi lebih awal terjadinya intruder atau kegiatan yang merugikan suatu jaringan.

Pada Kampus Universitas Satya Negara Indonesia yang memiliki puluhan komputer yang terhubung dengan Network dan mempunyai koneksi Internet tanpa ada pengamanan atau pendeteksian lalu lintas data atau paket-paket yang masuk, hacker atau pihak yang tidak bertanggung jawab dapat menganalisa lalu berusaha melakukan koreksi melalui aplikasi tertentu. Hal inilah yang

mengakibatkan penurunan performa jaringan maupun komputer. IDS (Intrussion Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan.

Iptables adalah firewall bawaan Linux yang bekerja mengatur lalu lintas data dalam komputer, baik yang masuk ke komputer, keluar dari komputer, maupun sekedar melewati komputer. Contohnya honeyd adalah server palsu yang merupakan sebuah produk honeypot dengan interaksi rendah dengan berfungsi mensimulasikan tingkah laku sebuah computer beserta sistem operasinya.

Dalam pengerjaan penelitian ini telah dilakukan perancangan dan analisis kinerja Snort IDS (Intrusion Detection System) dan Honeyd yang dapat melindungi server dari serangan penyusup. Dengan adanya sistem keamanan jaringan ini dapat mempermudah administator melindungi server dari serangan penyusup (intruder).

Berdasarkan permasalahan yang ada diatas, Penulis menetapkan judul penelitian yang akan dilakukan sebagai berikut : " IMPLEMENTASI SISTEM KEMANAN JARINGAN DENGAN MENGGUNAKAN INTRUSION DETECTION SISTEM (IDS)".

B. Rumusan Masalah

Berdasarkan latar belakang di atas maka perumusan masalah dalam penelitian ini adalah " Bagaimana Mengimplementasikan Sistem keamanan jaringan dengan Intrusion Detection System IDS pada Universitas Satya Negara Indonesia USNI?"

C. Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah bagaimana Intrusion Detection System (IDS) mendeteksi PING ATTACK dan serangan DDOS terhadap server utama Universitas Satya Negara Indonesia.

D. Tujuan dan Manfaat Penilitan

i. Tujuan Penelitian

Tujuan dari penelitian ini adalah mengimplentasikan sistem keamanan jaringan pada server utama Universitas Satya Negara Indonesia.

ii. Manfaat Penelitian

Penelitian ini dilakukan dengan harapan dapat memberikan manfaat, diantaranya :

a. Mempermudah dalam memonitoring sistem jaringan komputer yang ada di Universitas Satya Negara Indonesia.
b. Membantu dalam mendeteksi serangan terhadap server utama Universitas Satya Negara Indonesia.

E. Metode Penelitian

Metode penelitian menggunakan cara pengumpulan data dan evaluasi langsung pada sistem yang berjalan. Pengumpulan data dilakukan untuk data pokok maupun data yang bersifat pendukung. Data tersebut kemudian digunakan

sebagai acuan dasar pengembangan sistem agar dapat memberikan solusi yang paling baik. Penelitian dilakukan dengan langkah-langkah sebagai berikut :

I. Studi Pustaka

Pada penulisan ini membaca dan mempelajari referensi yang ada sebagai pelengkap, serta mencari referensi tambahan dari internet dan buku mengenai sistem keamanan jaringan dengan Intrusion Detection System (IDS) yang diperlukan untuk melakukan penulisan skripsi.

II. Studi Literatur

Penelitian untuk mendapatkan gambaran yang menyeluruh tentang apa yang sudah dikerjakan orang lain dan bagaimana cara kerjanya, kemudian seberapa berbeda penelitian yang akan kita lakukan. Materi yang digunakan pada bahan studi literatur antara lain buku, jurnal, paper bahkan artikel blog dari para akademisi.

III. Studi Wawancara

Pengumpulan data yang dilakukan dalam menunjang kelengkapan data melalui metode wawancara atau interview. Penulis melakukan tanya jawab dengan pihak yang bertanggung jawab dalam Jaringan yang ada di Universitas Satya Negara Indonesia.

IV. Observasi

Penulis melakukan dengan cara pengamatan langsung ke objek penelitian dan mewawancarai atau bertanya langsung kepada pihak - pihak yang terkait tentang permasalahan jaringan yang ada untuk membuat rancang bangun jaringan sesuai dengan apa yang dibutuhkan.

F. Sistematika Penulisan

Penulisan Tugas Akhir ini terdiri dari lima bagian utama yang dapat dijelaskan sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat, metodelogi penelitian yang diperoleh dari tugas akhir ini.

BAB II LANDASAN TEORI

Bab ini Berisi penjelasan tentang landasan teori yang digunakan dalam penelitian. Diuraikan pula tentang tinjauan pustaka, sistem komunikasi, protokol komunikasi, keamnan jaringan komputer, manfaat kemanan jaringan, perangkat lunak jaringan (software), perangkat keras jaringan (Hardware), konsep keamanan jaringan.

BAB III METODE PENELITIAN

Bab ini menjelaskan tentang tinjauan objek penelitian, struktur organisasi UPT-PUSTIKOM, visi dan misi UPT-PUSTIKOM, metode pengumpulan data, metode pengembangan sistem keamanan jaringan, kerangka pemikiran.

BAB IV ANALISA DAN PERANCANGAN

Bab ini menjelaskan tentang analisa penyelesaian masalah, analisa sistem berjalan, analisa Sistem usulan, analisa spesifikasi software yang dibutuhkan.

BAB V HASIL DAN IMPLEMENTASI

Bab ini menjelaskan tentang hasil, tujuan pengujian, implementasi, perbedaan system yang diserang dengan system yang tidak diserang, PING ATTACK dan serangn DDOS.

BAB VI KESIMPULAN DAN SARAN

Bab ini menjelaskan tentang kesimpulan dan saran pada tugas akhir ini.

DAFTAR PUSTAKA

LAMPIRAN

BAB II

LANDASAN TEORI

A. Tinjauan Pustaka

Referensi yang digunakan penulis untuk penulisan skripsi ini adalah diambil dari beberapa buku cetak, skripsi dan jurnal ilmiah yang terdapat di Jurnal dan beberapa universitas atau perguruan tinggi lainnya. Salah satu jurnal ilmiah yang penulis jadikan bahan sebagai tinjuan pustaka adalah jurnal ilmiah yang disusun oleh Angga Saputra dengan judul "**Desain Sistem Pendeteksi Serangan Jaringan Komputer Pada Kantor Dinas Perhubungan Komunikasi Dan Informatika Musi Banyuasin".**

1. Server

Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. Terkadang istilah server disebut sebagai web server. Namun umumnya orang lebih suka menyebutnya sebagai 'server' saja. Sebuah server didukung dengan prosesor yang bersifat scalable dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus. Sistem operasi ini berbeda dengan sistem operasi yang biasanya. Jika kita biasa menggunakan sistem operasi windows, MacOS dll, maka sistem operasi dari server ini mungkin berbeda. Sistem Operasi dari server adalah sistem operasi jaringan atau network operating system. Server juga bertugas untuk menjalankan software administratif. Yakni software yang mengontrol akses terhadap jaringan dan sumber daya yang

terdapat di dalamnya. Hal ini termasuk file atau alat pencetak (printer), dan memberikan akses kepada workstation anggota jaringan. Di dalam sistem operasi server, umumnya terdapat berbagai macam service yang menggunakan arsitektur klien/server. Contoh dari service yang diberikan oleh server ini antara lain Mail Server, DHCP Server, HTTP Server, DNS Server , FTP Server dan lain lain. Setiap sistem operasi server umumnya merangkai berbagai layanan tersebut . Atau bisa juga layanan tersebut diperoleh dari pihak ketiga. Setiap layanan tersebut akan merespons terhadap request dari klien. Contoh sistem operasi server adalah Windows NT 3.51, dan dilanjutkan dengan Windows NT 4.0. Saat ini sistem yang cukup populer adalah Windows 2000 Server dan Windows Server 2003, kemudian Sun Solaris, Unix, dan GNU/Linux. Pada umumnya, sebuah server terhubung dengan client dengan kabel UTP dan sebuah Network Card. Kartu jaringan ini biasanya berupa kartu PCI atau ISA.

2. Macam-Macam Server

Macam-macam server atau jenis-jenis server dapat kita golongkan dalam beberapa golongan jjika kita lihat dari fungsinya. Misalnya:

a. **Server aplikasi (application server)**

Server aplikasi adalah server yang digunakan untuk menyimpan berbagai macam aplikasi yang dapat diakses oleh client

b. **Server data (data server)**

Server data sendiri digunakan untuk menyimpan data baik yang digunakan client secara langsung maupun data yang diproses oleh server aplikasi.

c. **Server proxy (proxy server)**

Server proxy berfungsi untuk mengatur lalu lintas di jaringan melalui pengaturan proxy. Orang awam lebih mengenal proxy server untuk mengkoneksikan komputer client ke Internet.

B. Jaringan Komputer

Jaringan adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam kesatuan.informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga penggunaan jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama danbersama-sama menggunakan hardware dan software yang berhubungan dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node. Sebuah jaringan komputer dapat memiliki dua, puluhan, ribuan atau bahkan jutaan node. (todd Lammle, 2007).

C. Manfaat Jaringan Komputer

Banyak sekali manfaat yang dapat di peroleh dalam suatu jaringan komputer:

a. Jaringan komputer memungkinkan seorang dapat mengakses file yang dimilikinya (upload) atau file orang lain yang telah di izinkan untuk di akses (download), dimana pun dan kapan pun.
b. Jaringan komputer memungkinkan proses pengiriman data dapat berlangsung cepat dan efisien.
c. Jaringan komputer memungkinkan adanya sharing hardware antar client nya.

d. Jaringan komputer memungkinkan sesorang berhubungan dengan orang lain di berbagai negara dengan berupa teks, gambar, audio, dan video secara real time.

e. Jaringan komputer dapat menekan biaya operasional, seperti pemakaian kertas, pengiriman suatu surat atau berkas, telepon serta pembelian hardware jaringan.

D. Jenis – Jenis Jaringan

a. Local Area Network (LAN)

Local Area Network (LAN), adalah jaringan komputer dengan jangkauan area yang terbatas dan hubungan fisik antar komputer saling berdekatan. Misalnya jaringan komputer disebuah kantor, labolatorium, kampus. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk pemakaian bersama sumber daya dan saling bertukar informasi.

b. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), adalah penggabungan dari beberapa jaringan LAN ke dalam lingkungan area yang lebih besar, sebagai contoh yaitu : jaringan pada Bank ataupun kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. Pada dasarnya MAN merupakan versi LAN yang berukuran lebih besar dan biasanya

menggunakan teknologi yang sama dengan LAN. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

c. Wide Area Network (WAN)

Wide Area Network (WAN), adalah jaringan computer dengan area geografi yang paling luas, antar negara, antar benua bahkan keluar angkasa.. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program pemakai.

d. Jaringan Nirkabel (Tanpa Kabel)

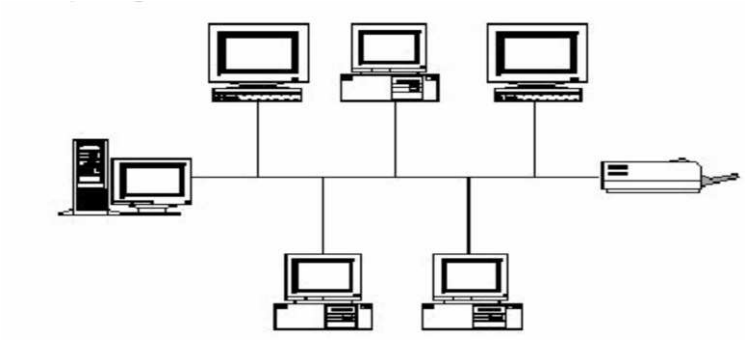
Jaringan Nirkabel adalah jaringan yang tidak menggunakan media kabel sebagai media penyampaian data. Jaringan nirkabel mengirimkan data melalui udara menggunakan base stations atau access points, yang mengirimkan frekuensi radio, yang terhubung ke Ethernet hub atau server. Dengan berada di area yang telah menyediakan layanan nirkabel, kita dapat terhubung ke internet menggunakan laptop, PDA, telepon genggam, atau perangkat nirkabel lain. Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan. Hal ini karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit.

E. Topologi Jaringan

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, oken-ring, star dan peer-to-peer network. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri.

a. Topologi Bus

Jenis topologi bus ini menggunakan kabel tunggal, seluruh komputer saling berhubungan secara langsung hanya menggunakan satu kabel saja. Kabel yang menghubungkan jaringan ini adalah kabel koaksial dan dilekatkan menggunakan T-Connector. Untuk memaksimalkan penggunaan jaringan ini sebaiknya menggunakan kabel Fiber Optic karena kestabilan resistensi sehingga dapat mengirimkan data lebih baik.



Gambar 2.1 Topologi bus

Keuntungan :

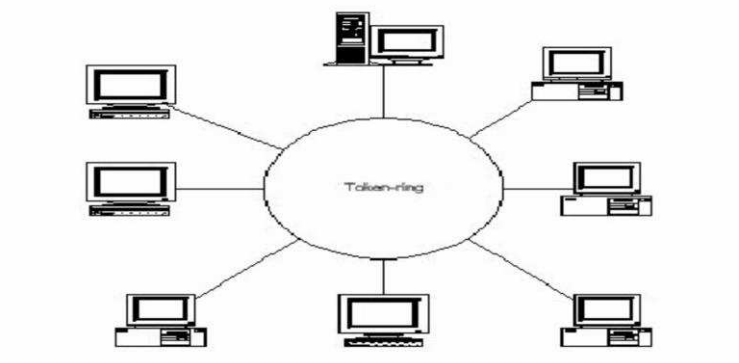
a) Hemat kabel, karena pada topologi bus hanya menggunakan kabel tunggal dan terpusat sebagai media transmisi sehingga tidak membutuhkan banyak kabel.
b) Layout kabel sederhana, pada pemasangan topologi bus rancangan dan skema kabel yang digunakan sangat sederhana sehingga mudah dalam pemasangannya.
c) Pengembangan jaringan komputer atau penambahan komputer baru baik sebagai server maupun client dapat dilakukan dengan mudah tanpa mengganggu komputer atau workstation yang lain.

Kerugian :

a) Kepadatan lalu lintas pada jalur utama, karena topologi bus menggunakan kabel terpusat sebagai media transmisi maka lalu lintas data akan sangat padat pada kabel utama.
b) Jika kabel utama mengalami gangguan maka seluruh jaringan akan mengalami gangguan pula.
c) Diperlukan repeater sebagai penguat sinyal jika akan menambahkan workstation dengan lokasi yang jauh.
d) Deteksi dan isolasi kesalahan sangat kecil sehingga jika jaringan mengalami gangguan, maka akan lebih sulit untuk mengidentifikasi kesalahan yang ada.

b. Topologi Token Ring

Metode token-ring (sering disebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama.Jaringan akan disebut sebagai loop, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.



Gambar 2.2 Topologi Ring

Keuntungan :

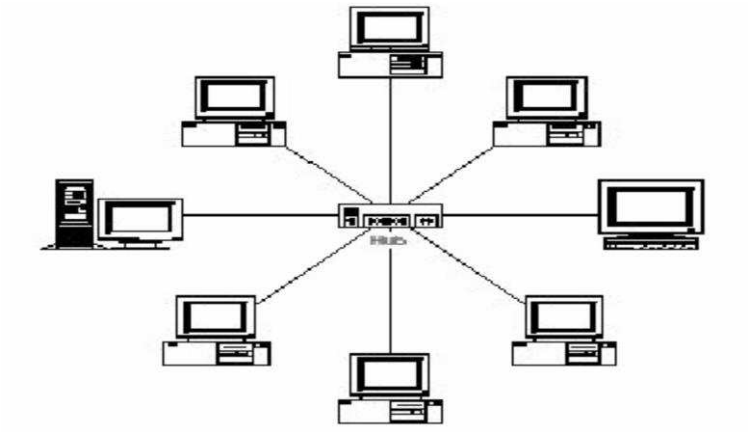
a) Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari server.
b) Identifikasi kerusakan mudah karena sinyal data selalu bergerak lurus dari perangkat pengirim sampai perangkat tujuan.
c) Dalam proses instalasi dan rekonfigurasi secara fisik maupun logik mudah karena terhubung satu dan hanya satu dengan perangkat lainnya.

Kerugian :

a) Penambahan terminal /node menjadi lebih sulit bila port sudah habis.
b) Jika salah satu terminal mengalami kerusakan, maka semua terminal pada jaringan tidak dapat digunakan.

c. **Topologi Star**

Kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya. Simpul pusat dinamakan stasium primer atau server dan lainnya dinamakan stasiun sekunder atau client server. Setelah hubungan jaringan dimulai oleh server maka setiap client server sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server.



Gambar 2.3 Topologi Star

Keuntungan :

a) Cukup mudah untuk mengubah dan menambah komputer ke dalam jaringan yang menggunakan topologi star tanpa mengganggu aktvitas jaringan yang sedang berlangsung.
b) Apabila satu komputer yang mengalami kerusakan dalam jaringan maka komputer tersebut tidak akan membuat mati seluruh jaringan star.
c) Kita dapat menggunakan beberapa tipe kabel di dalam jaringan yang sama dengan hub yang dapat mengakomodasi tipe kabel yang berbeda.
d) Arus lalulintas informasi data lebih optimal.

Kerugian :

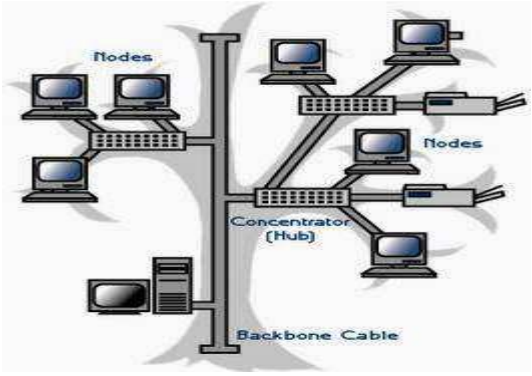
a) Memiliki satu titik kesalahan, terletak pada hub. Jika hub pusat mengalami kegagalan, maka seluruh jaringan akan gagal untuk beroperasi.
b) Membutuhkan lebih banyak kabel karena semua kabel jaringan harus ditarik ke satu central point, jadi lebih banyak membutuhkan lebih banyak kabel daripada topologi jaringan yang lain.
c) Jumlah terminal terbatas, tergantung dari port yang ada pada hub.

d. Topologi Tree

Topologi tree ini merupakan hasil pengembangan dari topologi star dan topologi bus yang terdiri dari kumpulan topologi star dan dihubungkan dengan 1 topologi bus. Topologi tree biasanya disebut juga topologi jaringan bertingkat dan digunakan interkoneksi antar sentral.

Pada jaringan ini memiliki beberapa tingkatan simpul yang ditetapkan dengan suatu hirarki, gambarannya adalah semakin tinggi kedudukannya maka semakin tinggi pula hirarki-nya. Setiap simpul yang memiliki kedudukan tinggi dapat mengatur simpul yang memiliki kedudukan yang rendah. Data dikirim dari pusat simpul kemudian bergerak menuju simpul rendah dan menuju ke simpul yang lebih tinggi terlebih dahulu.

Topologi tree ini memiliki keuntungan dan kerugian yang sama dengan topologi star antara lain :



Gambar 2.4 Topologi Tree

Keuntungan :

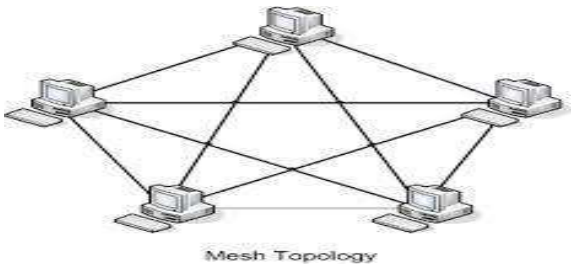
a) Deteksi kesalahan mudah dilakukan
b) Perubahan bentuk suatu kelompok mudah dilakukan dan tidak mengganggu jaringan lain
c) Mudah melakukan control

Kerugian :

a) Menggunakan banyak kabel
b) Sering terjadi tabrakan data
c) Jika simpul yang lebih tinggi rusak maka simpul yang lebih rendah akan terganggu juga
d) Cara kerja lambat

e. Topologi Mesh

Topologi Mesh merupakan rangkaian jaringan yang saling terhubung secara mutlak dimana setiap perangkat komputer akan terhubung secara langsung ke setiap titik perangkat lainnya. Setiap titik komputer akan mempunyai titik yang siap untuk berkomunikasi secara langsung dengan titik perangkat komputer lain yang menjadi tujuannya.



Gambar 2.5 Topologi Mesh

Keuntungan :

a) Dinamis dalam memperbaiki setiap kerusakan titik jaringan komputer
b) Data langsung dikirimkan ke tujuan tanpa harus melalui komputer lain
c) Data lebih cepat proses pengiriman data
d) Jika terjadi kerusakan pada salah satu komputer tidak akan mengganggu komputer lainnya

Kerugian :

a) Biaya untuk memasangnya sangat besar
b) Perlu banyak kabel
c) Sulitnya pada saat melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya.

F. Perangkat Lunak Jaringan (Software)

Merupakan program yang berisi intruksi atau perintah yang dimengerti oleh komputer untuk melakukan kegiatan seperti menghitung, menggambar, dan menghasilkan suara. Sehingga ada komunikasi antara komputer dengan pemakai. Komponen – komponen perangkat lunak pada jaringan :

a. Sistem Operasi Jaringan adalah sebuah program yang mengendalikan dan mengatur lalu-lintas suatu network serta menyediakan pelayanan kepada komputer-komputer yang terdapat pada network tersebut
b. Network Adapter Driver adalah program agar NIC dapat terdeteksi di computer terutama untuk OS windows 98 dan 2000, untuk Windows XP biasanya auto detect, berfungsi untuk mengaktifkan dan mengkonfigurasi network adapter tersebut disesuaikan dengan lingkungan dimana network card tersebut dipasang agar dapat digunakan untuk melakukan komunikasi data.

G. Perangkat keras Jaringan (Hardware)

Untuk membuat suatu jaringan komputer, diperlukan perlengkapan sebagai berikut:

a. Minimal ada satu komputer yang berlaku sebagai server(pusat data).
b. Ada komputer workstation (tempat kerja).
c. Sistem operasi pendukung jarinngan seperti Win NT, Netware, Linux, dsb.
d. Peripheral jaringan seperti network interface Card NIC,Hub,dll.

H. Sistem Keamanan Jaringan

Keamanan jaringan adalah suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

I. Intrusion Detection System (IDS)

IDS (Intrussion Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan.

J. Intrusion Protection System (IPS)

IPS (Intrusin Protection System) adalah penggabungan antara IDS dan ip table. Sehingga system ini dapat mendeteksi jika ada penyusup (intruder) melakukan serangan ke jaringan lokal kita dan juga mencatat semua paket data yang masuk. Oleh karena itu IPS dapat memblock semua serangan yang dilakukan oleh intruder dan juga mencatat semua log yang teridentifikasi. Berbeda dengan IDS yang hanya bisa mencatat atau memberi notifikasi bila ada serangan masuk. IPS juga bisa menggunakan signature untuk mendeteksi traffic dalam jaringan, sehingga pencegahan serangan dapat dilakukan sedini mungkin.

K. Honeyd

Honeyd adalah gambaran server palsu yang merupakan sebuah produk honeypot dengan interaksi rendah dengan berfungsi mensimulasikan tingkah laku sebuah computer beserta sistem operasinya.

L. Snort

Snort adalah NIDS yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah opensource project. Versi komersial dari snort dibuat oleh Sourcefire.

M. Jenis – jenis system keamanan Jaringan

Sebuah jaringan komputer harus memiliki untuk menghindari berbagai macam serangan oleh para hacker/cracker. Bagi para administrator jaringan pun harus jeli dalam menggunakan jenis sistem keamanan yang digunakan. Pada dasarnya jenis keamanan dibagi menjadi 5 jenis, yaitu:

a. Keamanan Fisik

Keamanan fisik lebih ditekankan pada hardware. Hal ini digunakan untuk melindungi hardware tetap dalam kondisi baik untuk melakukan operasi pada jaringan.

b. Keamanan Jaringan

Keamanan jenis ini lebih bertipe ke abstrak. Jadi kemanan ini dilakukan oleh benda yang tidak tampak, baik itu menggunakan software atau perintah lainnya. Contoh pengamanan jaringan adalah dengan menggunakan firewall ataupun proxy yang digunakan untuk mem filter user yang akan menggunakan jaringan.

c. Otorisasi akses

Otorisasi akses adalah penggunaan password atau kata sandi jika kita ingin mengakses sesuatu di jaringan. Hal ini dimaksudkan untuk

memastikan hanya user tertentu saja yang diperbolehkan untuk mengakses jaringan.

d. Proteksi Virus

Virus adalah sebuah metode penyerangan sistem komputer dengan menggunakan sebuah program yang dapat membuat sistem kacau dan mengalami kerusakan. Virus sendiri bisa diatasi dengan menginstall antivirus pada komputer dan selalu update databasenya yang terbaru.

e. Penanganan bencana

Perencanaan bencana adalah Perencanaan langkah-langkah yang akan diambil jika terjadi bencana yang mengakibatkan rusaknya sebuah system.

BAB III

METODE PENELITIAN

A. Tinjauan Objek Penelitian

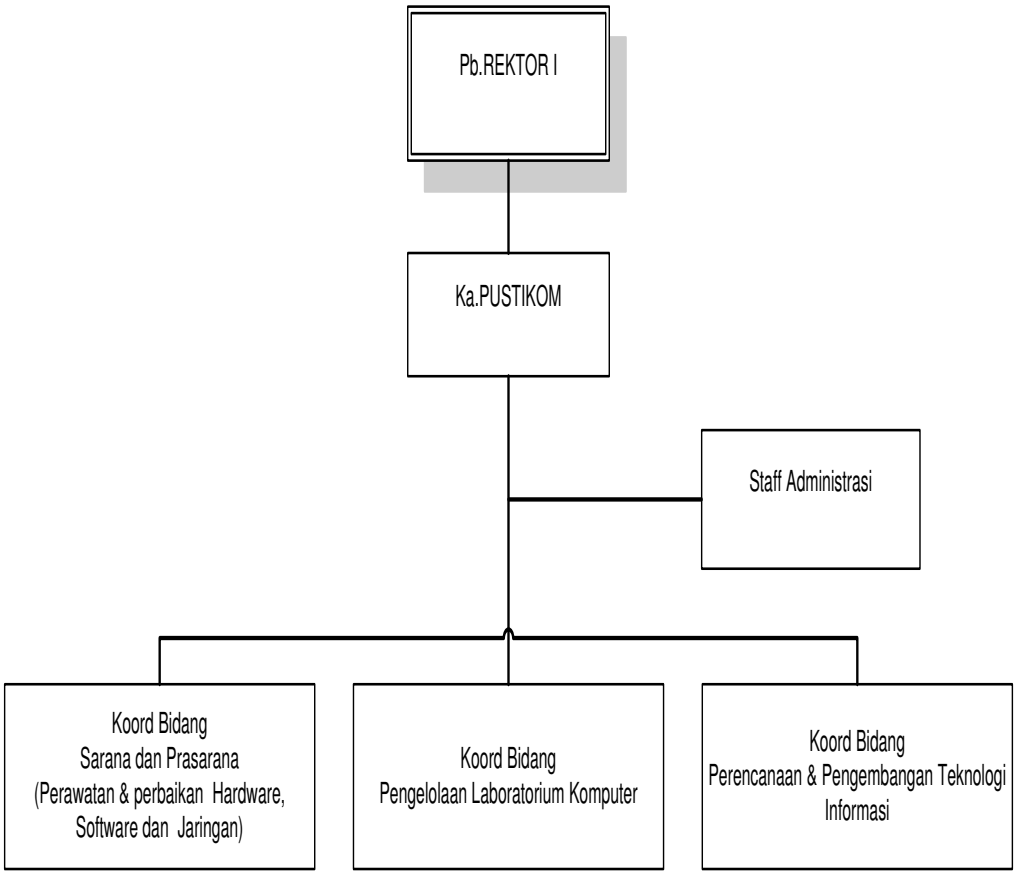
Objek penelitian ini adalah Universitas Satya Negara Indonesia. Universitas Satya Negara Indonesia berlokasi di Jl. Arteri Pondok Indah No. 11 Kebayoran Lama - Jakarta Selatan. Universitas Satya Negara Indonesia mempunyai Visi sebagai Perguruan Tinggi unggul dalam pengembangan ilmu pengetahuan, teknologi dan seni yang berorientasi kewirausahaan dan profesional di tingkat Nasional pada tahun 2025, dengan Misi:

1. Mengembangkan dan menyajikan pengajaran ilmu pengetahuan, teknologi dan seni yang menunjang wawasan dan budaya kewirausahaan.
2. Menyediakan akses dan lingkungan belajar yang kondusif bagi pembudayaan, penumbuhan dan pengembangan kewirausahaan.
3. Menanamkan jiwa kewirausahaan dan keterampilan bisnis secara empiris untuk menghasilkan wirausaha baru.

Untuk mencapai visi Universitas Satya Negara Indonesia yang unggul dalam pengembangan ilmu pengetahuan, teknologi dan seni yang berorientasi kewirausahaan di tingkat Nasional pada tahun 2025, diimplementasikan melalui tiga tahap rencana strategis (renstra) yakni :

1. Rencana Strategis tahap pertama Tahun 2011-2016, dengan focus pertumbuhan dan kemandirian.
2. Rencana Strategis tahap kedua Tahun 2016-2021, dengan focus pengembangan.
3. Rencana Strategis tahap ketiga Tahun 2021-2026, dengan focus optimalisasi pencapaian visi.

B. Struktur Organisasi UPT-PUSTIKOM



Gambar 3.1 Struktur Organisasi

1. Kepala UPT-PUSTIKOM

Kepala UPT-PUSTIKOM yang di pimpin oleh Zulkifli,S.Kom.,M.Kom, yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung Jawab kepada Pembantu Rektor 1 Bidang Akademik dan Perencanaan Sistem Informasi yang berhubungan dengan segala kebijakan dan kegiatan dibidang pelayanan teknologi informasi dan komputer di Universitas Satya Negara Indonesia.
b. Penanggung jawab operasional UPT dalam bidang Teknologi Informasi dan Komputer dalam lingkungan Universitas Satya Negara Indonesia dengan mendayagunakan seluruh sumber daya secara terencana dan terukur.
c. Melakukan perencanaan, pelaksanaan, pemantauan, evaluasi dan koordinasi segala kegiatan yang berhubungan dengan kebutuhan dan perkembangan UPT-PUSTIKOM.
d. Melakukan pelaporan tentang kondisi dan perkembangan yang berhubungan dengan UPT-PUSTIKOM.
e. Melakukan inovasi-inovasi yang berhubungan dengan perkembangan Teknologi Informasi dan Komputer untuk kepentingan USNI.
f. Mengembangkan program – program terkait kerjasama dan bisnis di bidang Teknologi Informasi, Sistem Informasi dan Komputer.

2. Koord Bidang Perawatan Hardware, Software dan Jaringan

Koord Bidang Perawatan Hardware, Software dan Jaringan yang di koordinasi oleh Nanto,ST, yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung jawab kepada Kepala UPT-PUSTIKOM dan mengkoordinir semua teknisi di bidang teknologi informasi (TI) dan computer di lingkungan USNI
b. Merencanakan dan mengadakan sarana, prasarana TI dan Komputer.
c. Menginventarisasi dan memelihara peralatan TI dan Komputer di semua unit kegiatan.
d. Melakukan pengawasan dan pemeliharaan ruangan – ruangan, peralatan-peralatan dan dokumen-dokumen terkait UPT-PUSTIKOM.
e. Membantu tugas teknis koordinator laboratorium komputer dan koordinator system informasi pada UPT-PUSTIKOM.

3. Koord Bidang Pengelolaan Lab Komputer

Koord Bidang Pengelolaan Lab Komputer yang di kordinasi oleh Zulkifli,S.Kom.,M.Kom, yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung jawab kepada kepala UPT-PUSTIKOM dan mengkoordinir staf laboran yang menangani semua kegiatan laboratorium komputer di lingkungan USNI.

b. Mengelola seluruh laboratorium komputer yang ada di lingkungan USNI di bantu oleh staf laboratorium computer.
c. Merencanakan, mengadakan, menginventarisir dan memelihara alat dan bahan untuk kegiatan praktikum di laboratorium komputer.
d. Melaksanakan perbaikan dan pemeliharaan fasilitas dan alat di laboratorium computer.
e. Membantu Dosen dalam menyiapkan pelaksanaan kegiatan praktikum di laboratorium komputer.
f. Membantu Kepala UPT – PUSTIKOM dalam mengembangkan kerjasama dengan pihak luar untuk pemanfaat dan peningkatan fasilitas laboratorium computer.
g. Mengelola unit produksi dengan mengoptimalkan sarana laboratorium komputer.

4. Koordinator Bidang Pengembangan Sistem Informasi

Koordinator Bidang Pengembangan Sistem Informasi yang di kordinasi oleh Imammudin,ST, yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung jawab kepada Kepala UPT-PUSTIKOM dan mengkoordinir semua Staff programmer dilingkungan USNI, baik yang bertugas di UPT-PUSTIKOM maupun di unit-unit lain.
b. Merencanakan pengembangan System Informasi Manajemen di lingkungan USNI.

c. Memelihara kelangsungan operasional dan pengembangan SIM di USNI.

d. Mengkoordinir pemantauan , evaluasi dan pelaporan SIM USNI secara regular.

e. Merencanakan pelatihan dan pendidikan SDM pengelola SIM USNI diberbagai unit pengguna.

5. Perawatan Lab Komputer

Perawatan Lab Komputer yang di kordinasi oleh Mukmin, yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung Jawab kepada koordinator bidang pengelolaan laboratorium komputer dan mendukung kelancaran kegiatan laboratorium untuk kegiatan pengajaran, penelitian dan pengabdian pada masyarakat.

b. Menyiapkan dan memelihara perangkat unit tingkat laboratorium;

c. Mendukung layanan teknis dan pelatihan komputer;

d. Mendata kebutuhan bahan dan alat untuk kegiatan administrasi dan kegiatan akademik.

e. Mengusulkan pengadaan bahan dan alat untuk kegiatan praktikum komputer.

f. Mendata dan mengatur penggunaan alat dan bahan untuk kegiatan praktikum.

g. Menjaga kebersihan dan keamanan laboratorium komputer.

6. Perawatan Komputer Unit Kerja

Perawatan Komputer Unit Kerja di kordinasi oleh Adiyanto, yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung Jawab kepada koordinator sarana dan prasarana UPT-PUSTIKOM dan mendukung kebutuhan teknis dalam unit kerja Universitas.
b. Membantu segala kegiatan pemantauan, inventarisasi dan pemeliharaan peralatan dan ruangan yang berada di bawah naungan Ka.UPT – PUSTIKOM.
c. Mendukung kelancaran kegiatan yang dilaksanakan oleh Ka.UPT-PUSTIKOM.

7. Staff Administrasi UPT

Staff Administrasi UPT yang mempunyai tugas dalam melaksanakan tanggung jawab yaitu :

a. Bertanggung Jawab kepada kepala UPT-PUSTIKOM dan mendukung kebutuhan secara administrasi disemua bidang dalam lingkungan UPT-PUSTIKOM.
b. Membantu segala kegiatan Analisis, pemantauan, inventarisasi dan pemeliharaan peralatan serta ruangan yang berada di bawah naungan Ka.UPT – PUSTIKOM.
c. Mendukung kelancaran kegiatan yang dilaksanakan oleh Ka.UPT-PUSTIKOM.

d. Melakukan administrasi dan surat menyurat yang berhubungan dengan kegiatan UPT-PUSTIKOM.
e. Melakukan Update WEB USNI dan WEB UPT-PUSTIKOM secara continue
f. Membantu untuk menganalisa terhadap kebutuhan perangkat IT dan Komputer yang akan diganti.
g. Membantu melakukan pengontrolan dan membantu pengisian form kerja setiap koordinator bidang.
h. Melakukan pencatatan atau dokumentasi dan monitoring yang berhubungan dengan Teknologi Informasi dan Komputer dalam Kampus Universitas Satya Negara Indonesia.

C. Visi Dan Misi UPT-PUSTIKOM

1. Visi

Menjadikan pusat pelayanan dan pengembangan teknologi informasi dan komputer di Universitas Satya Negara Indonesia yang lebih cerdas dan trampil.

2. Misi

a. Melayani kebutuhan yang berhubungan dengan Perawatan, Perbaikan, Pengadaan dan Pengembangan ICT.
b. Penyebaran ilmu pengetahuan dan Teknologi informasi
c. Peningkatan efektifitas dan efisiensi kegiatan universitas
d. Pemasaran informasi melalui teknologi informasi

e. Peningkatan kualitas pelayanan pada civitas akademik berbasis Teknologi Informasi.

D. Metode Pengumpulan Data

Pada tahapan ini penulis melakukan pengumpulan data dan informasi dengan membaca jurnal referensi yang di jadikan acuan dalam penelitian, kemudian penulis merancang sistem sesuai dengan kebutuhan pengguna.

1. Wawancara

Pada tahap ini penulis melakukan pertanyaan yang bertujuan memperoleh informasi. Wawancara dilakukan pada saat observasi berlangsung dengan Bapak Nanto,ST, yang bertugas mengelola jaringan di Universitas Satya Negara Indonesia guna mendapatkan informasi dan data mengenai system jaringan yang ada di perguruan tinggi selama ini.

2. Studi Pustaka

Metode ini dilakukan untuk melengkapi dalam penulisan skripsi dengan cara mengumpulkan data ataupun infromasi dari berbagai sumber bacaan yang berkaitan dengan keamanan jaringan apa yang diperlukan penulis sebagai penunjang dalam penyusunan, penulisan dan perancangan.

3. Studi Literatur

Pada metode ini penulis melakukan dengan cara mencari jurnal – jurnal yang berhubungan dengan keamanan jaringan dari penelitian yang sudah pernah dilakukan. penulis mengutip jurnal dan mencari kekurangan

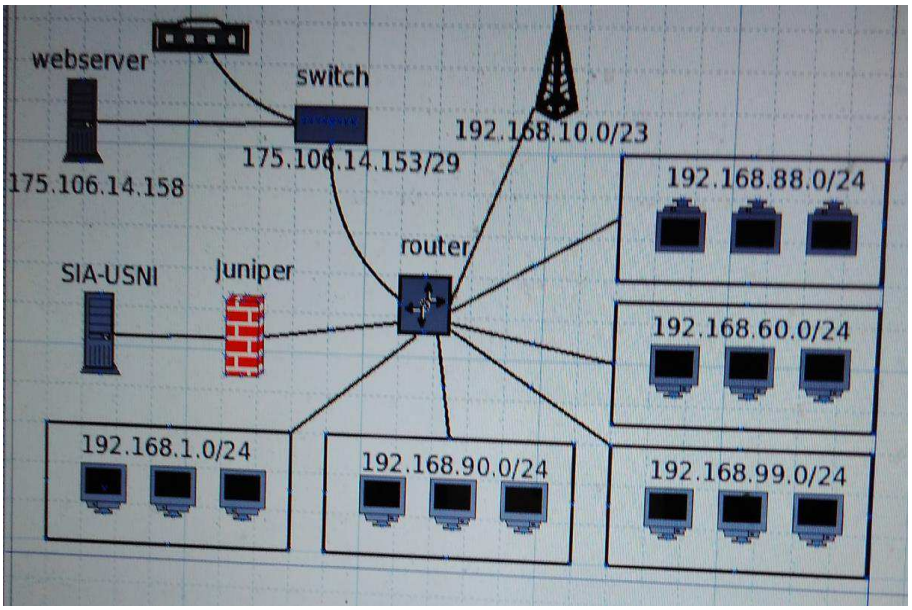
sistem keamanan yang sudah di buat oleh Angga Saputra dalam jurnalnya yang berjudul **Desain Sistem Pendeteksi Serangan Jaringan Komputer Pada Kantor Dinas Perhubungan Komunikasi Dan Informatika Musi Banyuasin**. Yang akan nantinya dijadikan acuan untuk penelitian penulis yang akan digunakan untuk melengkapi kekurangan dari penelitian sebelumnya.

4. Observasi

Pada tahap ini penulis memperoleh berbagai data secara pengamatan dan peninjauan langsung terhadap objek penelitian untuk mengetahui gambaran masalah yang terjadi di Universitas Satya Negara Indonesia.

E. Analisis Sistem Keamanan

Jaringan komputer pada Universitas Satya Negara Indonesia secara umum dapat digambarkan melalui topologi jaringan sebagai berikut :



Gambar 3.2 Topologi Star yang ada di USNI

Pada jaringan komputer Universitas Satya Negara Indoensia belum terinstall pendeteksi serangan seperti IDS untuk mendeteksi gangguan dari intruder. Dimana hanya PC-Local yang memiliki firewall (Juniper) yang terhubung langsung dengan jaringan internet berfungsi untuk mengawasi aktifitas pada komputer client, PC-Server belum ditanamkan system pendeteksi intruder hanya bertugas membagikan koneksi internet ke seluruh komputer client melalui router dan switch.

F. Analisa Masalah Keamanan Jaringan

Masalah keamanan jaringan pada tempat penulis melakukan penelitian ini adalah kurangnya pengamanan terhadap sistem penyimpanan data mahasiswa , sehingga mahasiswa dapat dengan mudah masuk kedalam system dan dengan mudah mengetahui nilainya tanpa harus login terlebih dahulu, Selain itu tempat penulis melakukan penelitian masih menggunakan Ip address v4 yang masih umum digunakan dalam jaringan dan belum memiliki fitur IpSec.

G. Usulan Pemecahan Masalah Jaringan

Solusi yang dapat diusulkan agar dapat meningkatkan pengamanan di server Universitas Satya Negara Indonesia, sebagai berikut :

1. Mengkonfigurasikan server USNI dengan Intrusion Detection System sehingga apabila ada mahasiswa yang mencoba masuk kedalam system dapat terdeteksi oleh system.
2. Menambahkan Firewall pada setiap protocol jaringan yang dapat membatasi aktivitas client.

H. Kebutuhan Perangkat Keras

Dari hasil analisis yang telah dilakukan khususnya pada perangkat keras (hardware) yang digunakan dalam penelitian ini memiliki spesifikasi sebagai berikut :

1. PC server sensor IDS snort
2. PC Client (penyerang)
3. Modem WIFI

I. Kebutuhan Perangkat Lunak

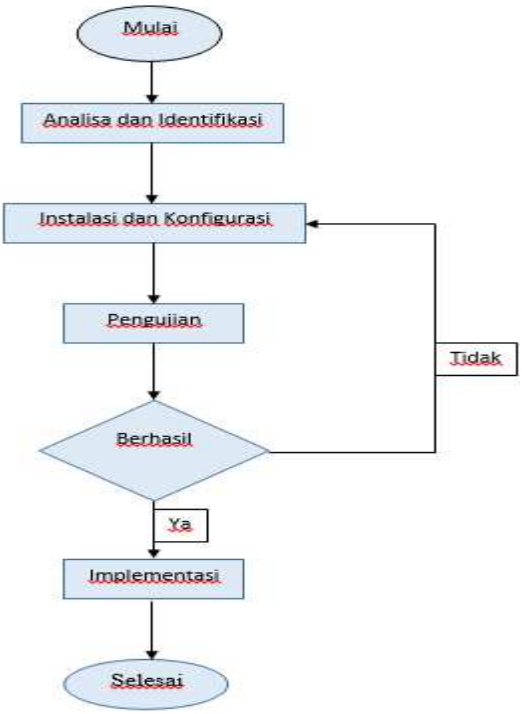
Adapun perangkat lunak (software) yang digunakan dalam membangun sistem keamanan jaringan IDS snort sebagai berikut :

1. Linux Ubuntu 15.10
2. Windows (penyerang)
3. Snort
4. Honeyd
5. Bamyard
6. Apache Web Server
7. Database MYSQL server
8. IPtable

J. Kerangka Berfikir

Penulis melakukan pendekatan pengembangan sistem dengan menggunakan metode Network Development Life cycle (NDLC) untuk menerapkan konsep sistem keamanan jaringan di Universitas Satya Negara Indonesia. Penulis

membuat gambaran dari sistem IDS yang dikombinasikan dengan tindak pencegahan serangan. Kerangka berfikir menunjukkan gambaran tentang jalannya sistem keamanan jaringan IDS yang tampak pada gambar 3.3.



Gambar 3.3 Kerangka Berfikir

BAB IV

PERANCANGAN SISTEM

A. Instalasi IDS Snort

IDS Snort adalah pendeteksi intrusi jaringan dan sistem pencegahan. Ini adalah Melakukan deteksi dengan menggunakan berbagai metode, termasuk aturan-berbasis deteksi, deteksi anomali, dan analisis heuristik Kemudian lintas jaringan.

1. Tahapan - tahapan Instalasi IDS Snort

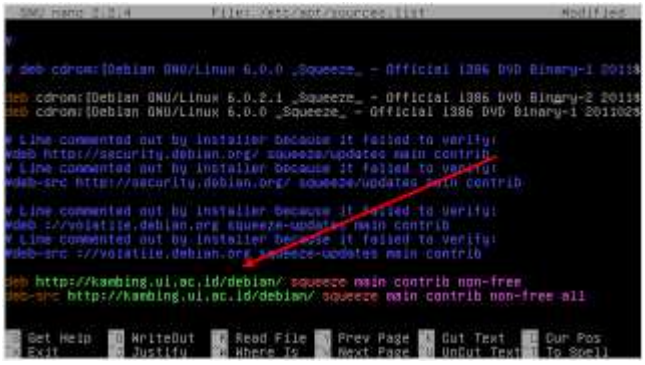
Berikut adalah tahapan – tahapan instalasi snort IDS pada server Utama. Langkah – langkahnya sebagai berikut :

a. Ketikan Perintah

```
# nano /etc/apt/sources.list
```

b. Lalu Copykan Source dibawah ini

```
deb http://kambing.ui.ac.id/debian/ squeeze main
contrib                                    non-free
deb-src  http://kambing.ui.ac.id/debian/  squeeze
main contrib non-free
```



Gambar 4.1 Source.list

Setelah itu update :

apt – get Update

c. Selanjutnya Install Aplikasi – aplikasi yang dibutuhkan :

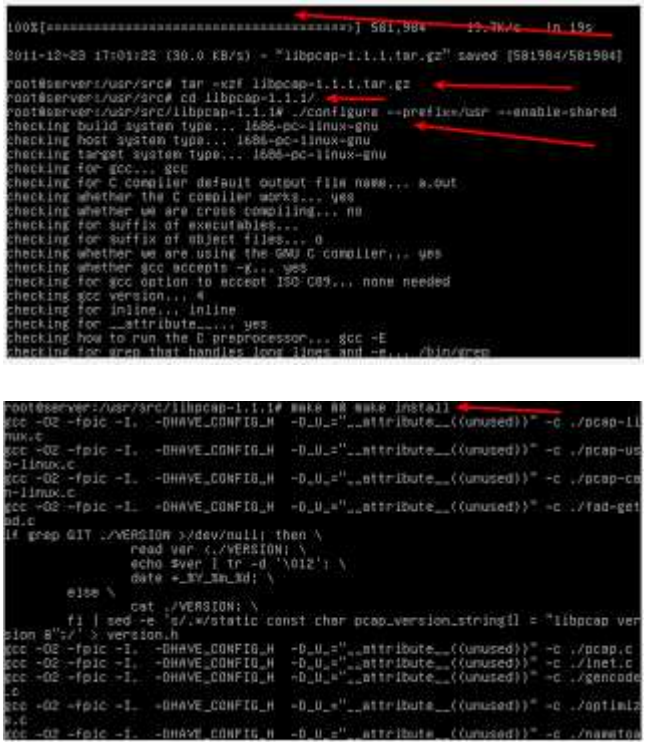
 # apt-get install apache2 libapache2-mod-php5 libwww-perl mysql-server mysql-common mysql-client php5-mysql libnet1 libnet1-dev libpcre3 libpcre3-dev autoconf libcrypt-ssleay-perl php5-gd php-pear libphp-adodb php5-cli libtool libssl-dev gcc-4.4 g++ automake gcc make flex bison apache2-doc ca-certificates.

Setelah itu jika muncul gambar seperti ini tekan oke :

Gambar 4.2 Konfigurasi Libcap

d. Kalo udah, sekarang install libpcapnya (kita masih berada di dalam direktori /usr/src):

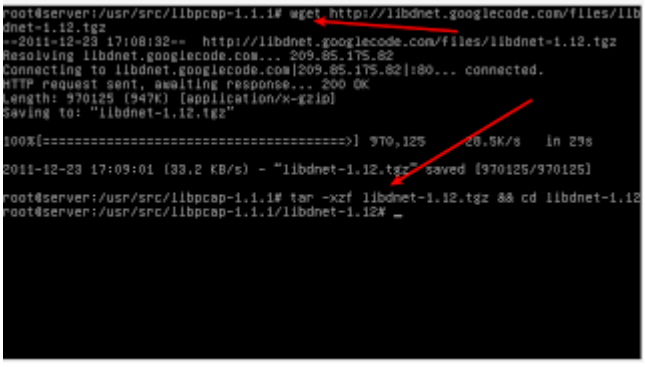
apt – get Install libcap



Gambar 4.3 Instalasi Libcap

e. lanjutt. sekarang install libdnet nya :

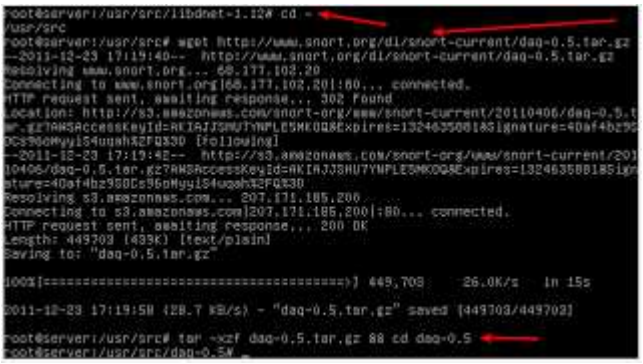
apt – get install libdnet



Gambar 4.4 Instalasi Libdnet

f. Setelah selesai, Install Daq nya :

apt – get Install Daq

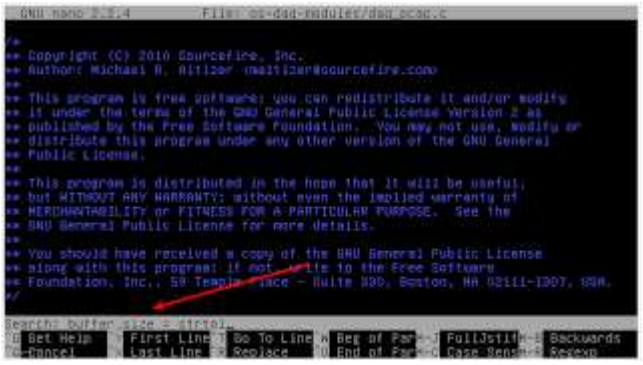


Gambar 4.5 Instalasi Daq

Setelah itu edit daq:

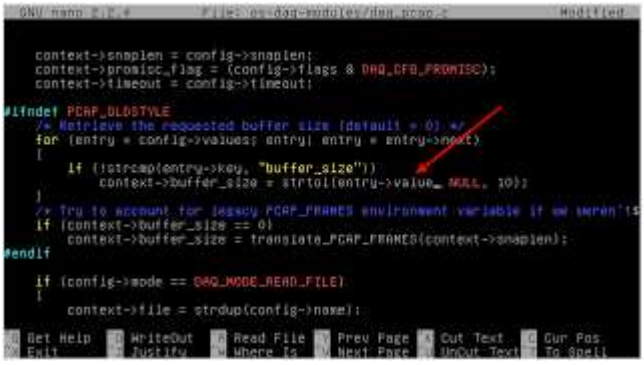
nano os-daq-modules/daq_pcap.c

tekan **ctrl+w**, lalu cari kata kunci **buffer_size = strtol**



Gambar 4.6 Daq Modules

kalo udah ketemu, ganti **context->buffer_size = strtol(entry->key, NULL, 10);** menjadi **context->buffer_size = strtol(entry->value, NULL, 10);**

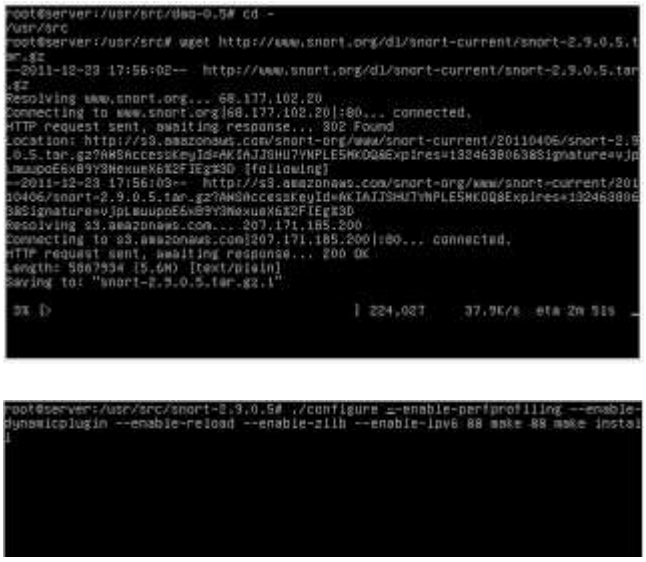


Gambar 4.7 Daq Snort

Maka hasil nya akan seperti ini. Lalu Exit and Save.

g. Setelah Itu Install snort nya :

apt – get Install Snort



Gambar 4.8. Instalasi Snort

B. Tahapan – tahapan Konfigurasi IDS

Berikut adalah tahapan – tahapan konfigurasi Snort IDS server , Langkah – langkah nya :

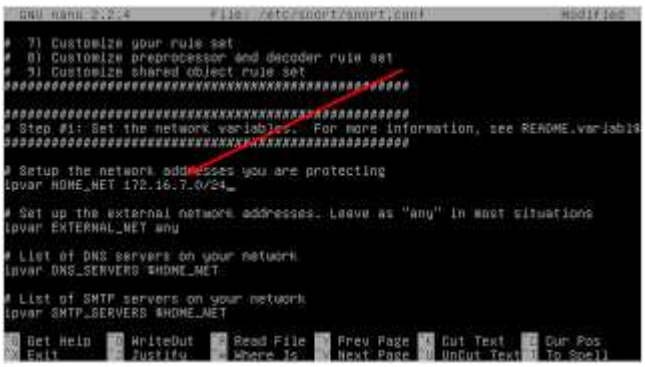
1. Edit file snort.conf

   # nano /etc/snort/snort.conf

   Lalu cari kata ipvar HOME_NET, lalu edit bagian ini :

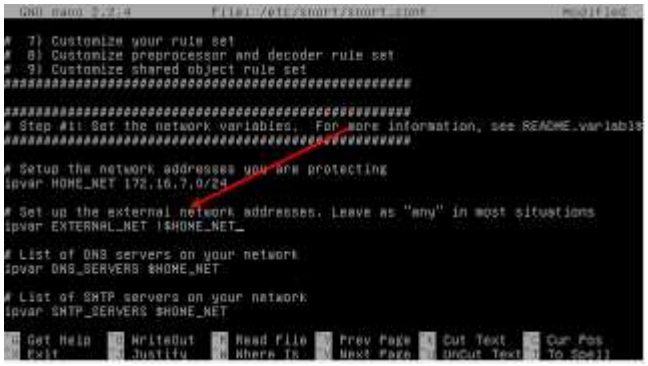
   ipvar HOME_NET any menjadi **ipvar HOME_NET 192.168.1.1/24**

   ini ip network yang ingin anda protect.



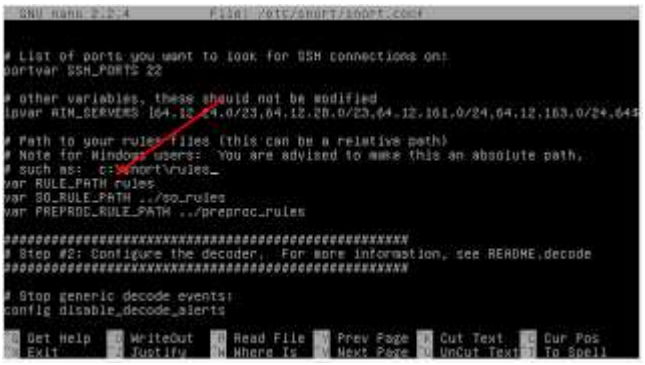
Gambar 4.9 Konfigurasi Snort

Tidak jauh dari ipvar HOME_NET, kebawah sedikit edit baris **ipvar EXTERNAL_NET any** menjadi **ipvar EXTERNAL_NET !$HOME_NET**



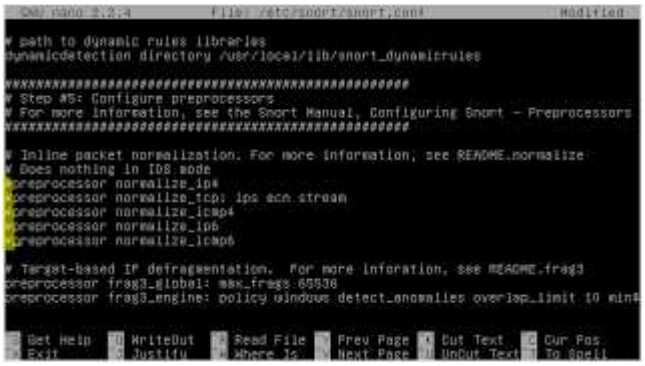
Gambar 4.10 Pembuatan RULE

Search kata kunci **var RULE_PATH** lalu hilangkan kedua tanda titik dan tanda garis miring di depan kata **./rules**sehingga dari yang semula **var RULE_PATH ../rules** menjadi **var RULE_PATH rules** :



Gambar 4.11 Konfigurasi Preprocessor

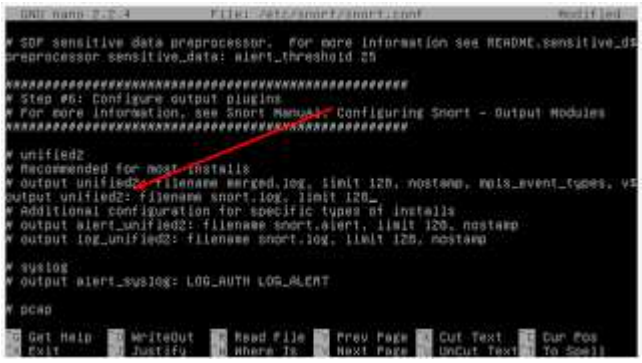
Ketik kata kunci **preprocessor normalize**, dan beri tanda pagar di depan semua kata-kata yang bertuliskan**prepocessor normalize** dari baris 186 sampai 190. Lebih jelasnya lihat gambar dibawah ini :



Gambar 4.12 Preprocessor

Search kata kunci **output unified2**. lalu tambahkan satu baris dibawahnya dengan tulisan berikut :

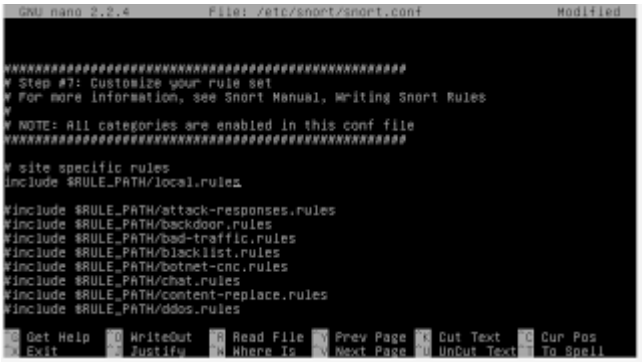
output unified2: filename snort.log, limit 128

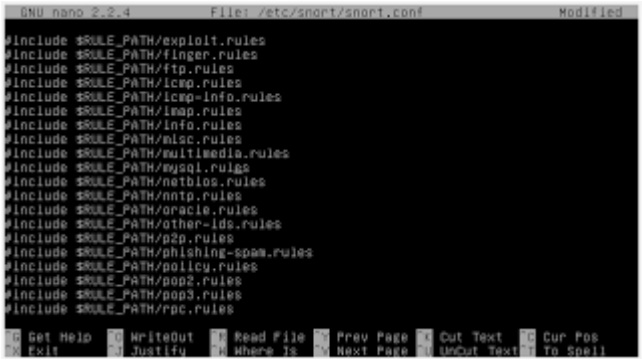


Gambar 4.13 Output Unifield

Search kata kunci **RULE_PATH** lalu beri tanda pagar di depan semua kata-kata yang mengandung kata **include**

$RULE_PATH selain **include $RULE_PATH local.rules**





Gambar 4.15 Perintah RULE

Save dan tutup filenya.

BAB V

HASIL DAN IMPLEMENTASI

A. Hasil

Hasil yang diperoleh dengan menganalisa dan perancangan sistem jaringan pada bab IV di uji dan di implementasikan.

1. Hasil Rancangan IDS SNORT

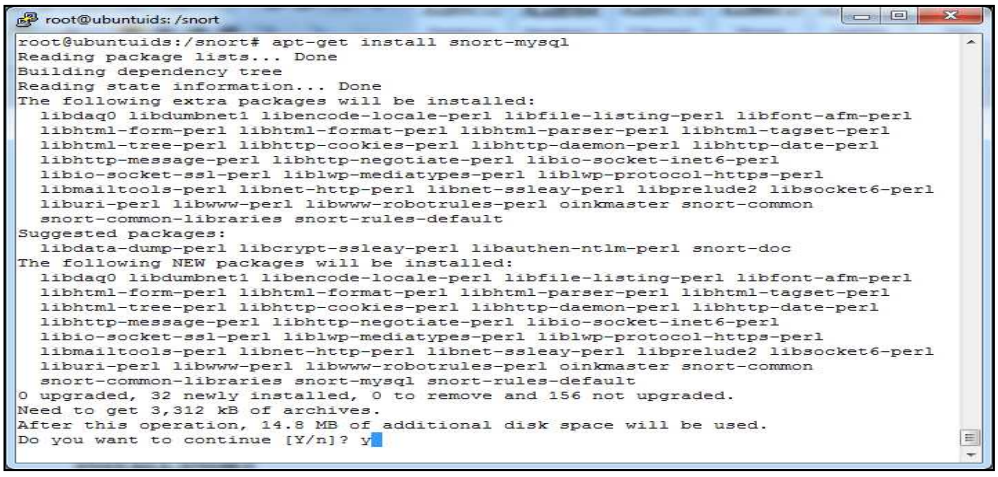
Proses installasi linux Ubuntu Server 15.00 LTS dilakukan sebagai tahap awal proses implementasi, setelah selesai proses installasi sistem dilanjutkan installasi komponen tambahan atau pendukung sensor alat deteksi snort . Adapun paket software pendukung IDS atau aplikasi yang diinstall adalah mysql-server, libpcap0.8-dev, libmysqlclient15-dev, bison, flex, apache2, php5, libapache2-mod-php5, php5-gd, php5-mysql, libtool, libpcre3-dev dan php-pear dengan menggunakan perintah apt-get install, Kemudian membuat folder snort, kemudian download file base.tar.gz dan adodb.tar.gz dengan menggunakan perintah wget.

No.	Instalasi paket pendukung mesin sensor IDS
1.	apt-get install mysql-server
2.	apt-get install mysql-client
3.	apt-get install php5-mysql
4.	apt-get install php5-gd
5.	apt-get install php5-dev
6.	apt-get install php-image-graph
7	apt-get install php-image-canvas
8.	apt-get install php-pear
9.	apt-get install libphp-adodb
10.	apt-get install libpcre3
11.	apt-get install libpcre3-dev
12.	apt-get install libpcap0.8
13.	apt-get install libgd2-xpm

Tabel 5.1 Aplikasi Pendukung

2. Instalasi Aplikasi SNORT

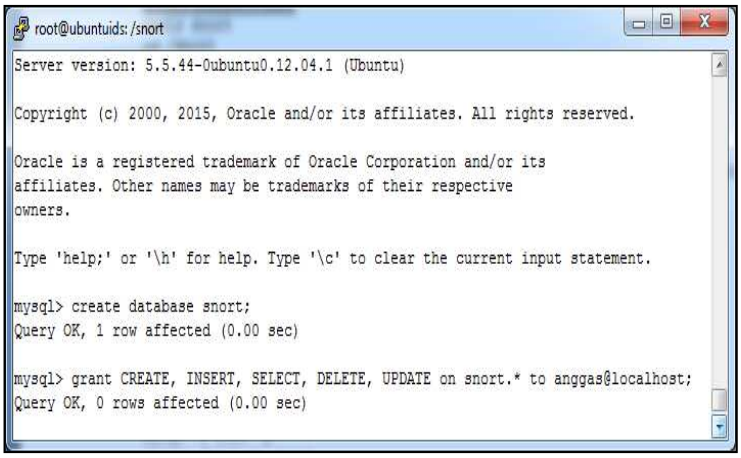
Pada tahap ini penulis melakukan installasi sensor snort-mysql dengan menggunakan perintah apt-get install, dimana proses installasi dilakukan secara online melalui repository Linux Ubuntu Server 12.04 LTS seperti pada Gambar 5.



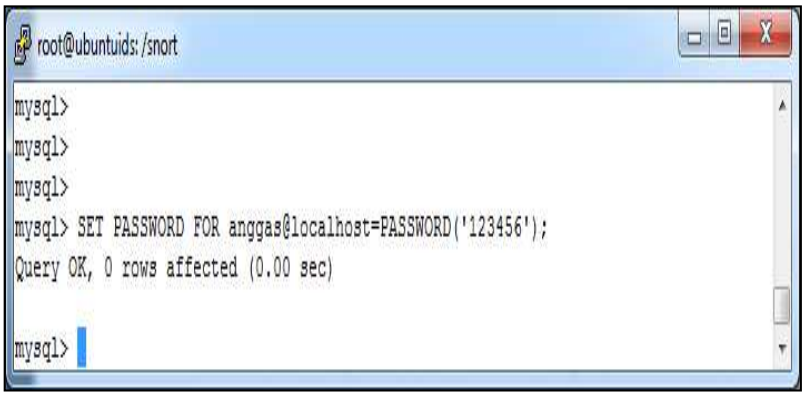
Gambar 5.1 Installasi Snort Mysql

3. Instalasi Database SNORT

Setelah aplikasi snort telah diinstall selanjutnya penulis membuat database mysql server snort dengan login sebagai user root kemudian membuat user yang berhak mengakses databases snort yaitu user ‘anggas’ dan password ‘123456’. Database snort ini digunakan untuk menyimpan alert logs dari sensor snort.



Gambar 5.2 Membuat Database



Gambar 5.3 Membuat password user

B. Pengujian Sensor IDS SNORT

Pengujian sistem ini dilakukan untuk mengetahui apakah sistem dapat berjalan sesuai dengan yang diharapkan. Untuk mengetahui apakah snort berjalan dan dapat mendeteksi intrusi pada sistem yang dipantau,dilakukan dengan cara melakukan ping dan juga mengakses web pada sistem yang dipantau. Namun sebelumnya harus dilakukan konfigurasi rule snort. Agar ketika pengujian dapat dihasilkan alert yang sesuai. Langkah selanjutnya perubahan terhadap file /etc/snort/rules/local.rules dengan rule berikut.

Alert icmp any any ->any any (msg:”test”; sid: 10001;).

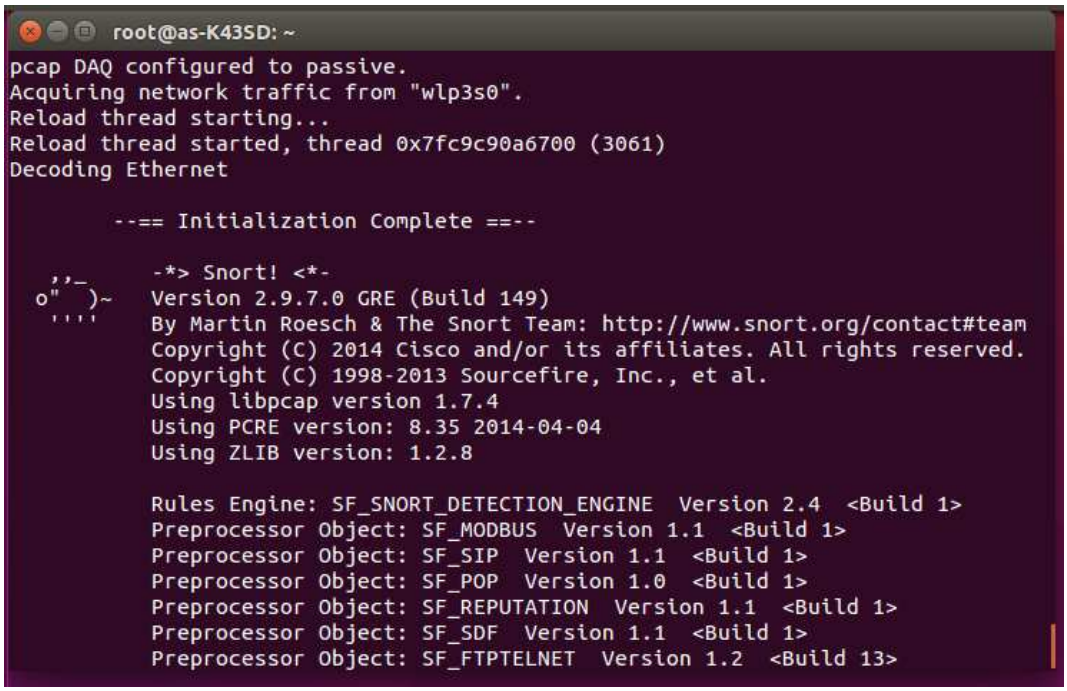
Structure	Example
Rule Actions	alert
Protocol	icmp
Source IP Address	any
Source Port	any
Direction Operator	->
Destination IP Address	any
Destination Port	any
(rule options)	(msg:"ICMP Packet"; sid:477; rev:3;)

Tabel 5.2 Pembuatan Alert

Rule diatas akan menghasilkan alert jika ada lalu lintas ICMP dari sembarang IP dan sembarang port yang menuju HOME_NET (yaitu 192.168.1.101/24 sembarang port, dan menampilkan pesan “ICMP Test” dengan klasifikasi Not Suspicious dan sid 10001:1. Penulis melakukan ping ICMP ke alamat 192.168.1.102 dari komputer client yang memiliki IP 192.168.1.103. Snort diaktifkan dengan perintah berikut agar dapat mencatat hasilnya langsung ke layar console. Tail /var/snort/alert.

C. IDS Mode Sniffing

Untuk mengaktifkan Mode Sniffing ketikan perintah #./snort –v pada terminal consol.

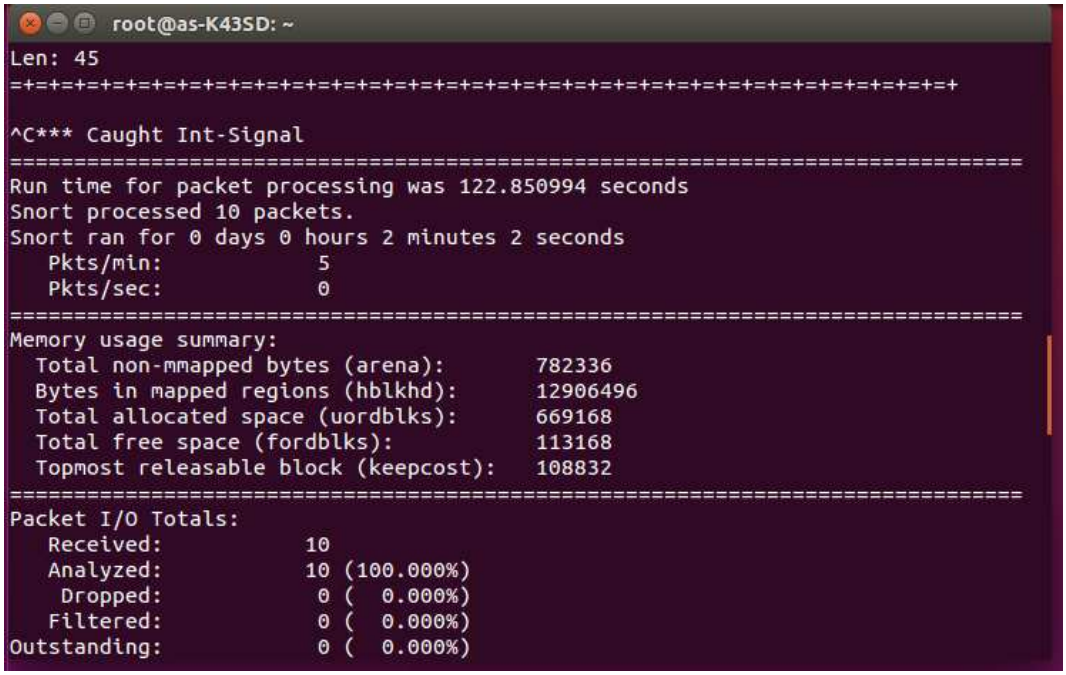


Gambar 5.4 Tampilan mode sniffing Snort

Pada tampilan di atas tidak ada masalah dalam penerapan rules Snort yang telah dibuat, sensor Snort dapat berjalan dalam mode sniffing untuk mendeteksi setiap paket yang masuk dalam jaringan server.

D. Log Paket

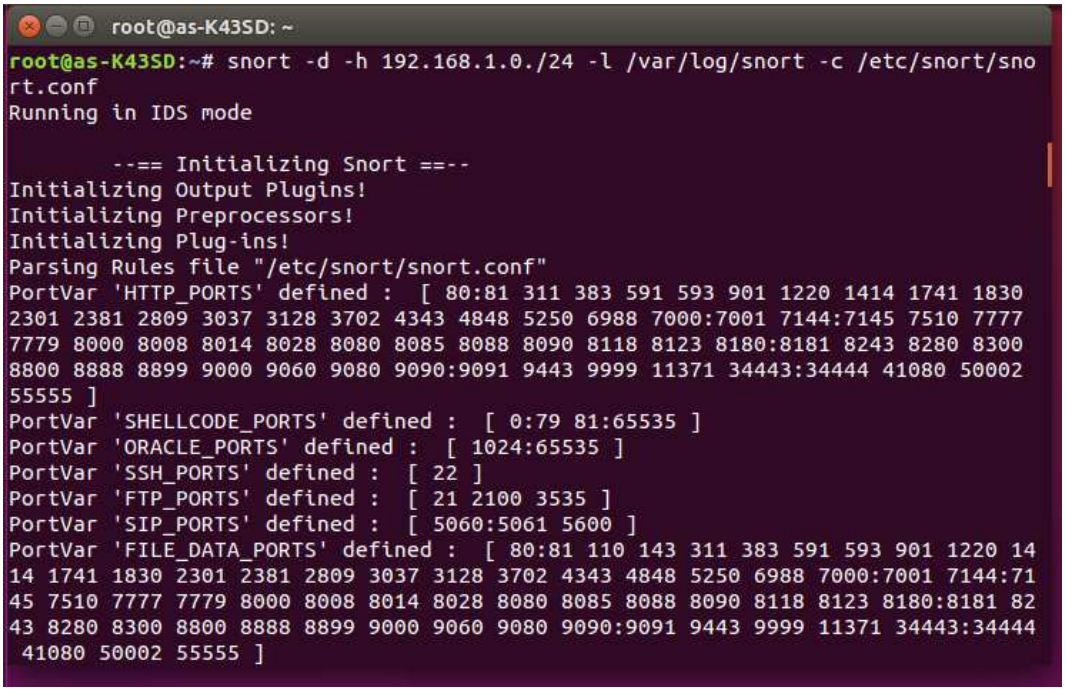
Untuk melihat paket data yang ada pada lalu lintas jaringan ketikan perintah #/var/log/snort.



Gambar 5.5 Tampilan Log Paket

E. Aktifkan Mode IDS

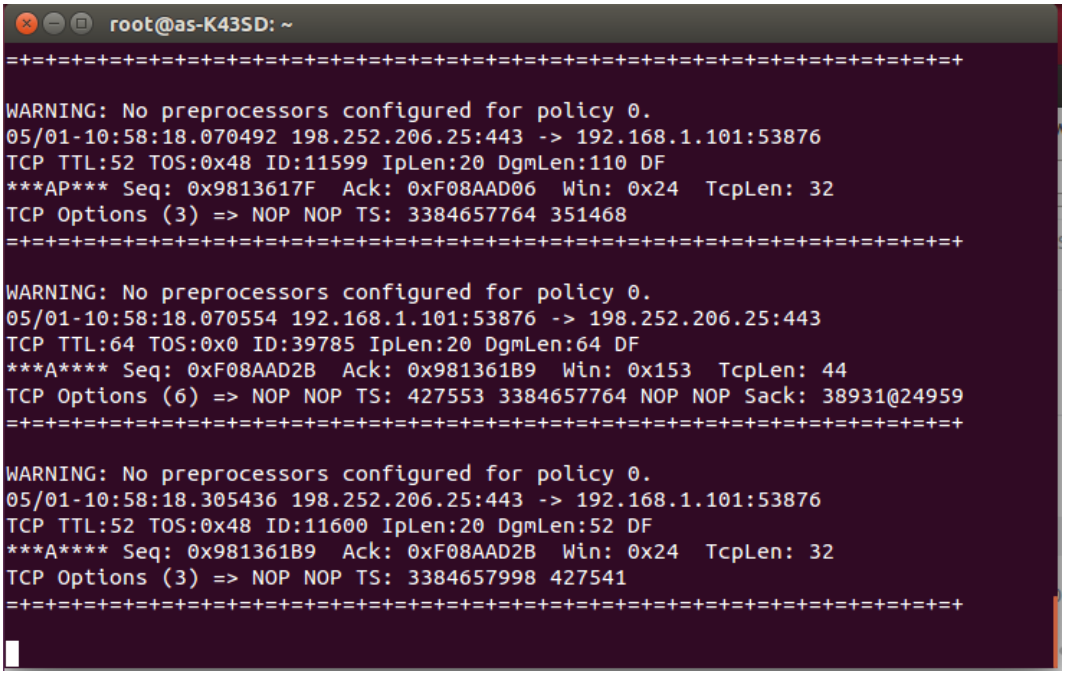
Untuk mengaktikan mode IDS pada snort ketikan perintah #snort –d –h 192.168.1.0/24 –l /var/log/snort –c /etc/snort/snort.conf pada mode ini IDS sudah dapat mendeteksi ping yang di lakukan oleh intruder.



Gambar 5.6 Menjalankan IDS

F. Pengiriman Paket dan Ping Attack

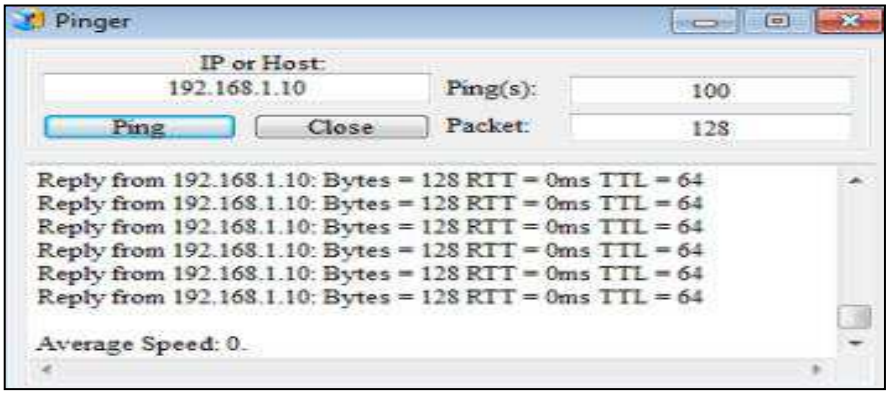
Pada saat intruder melakukan pengiriman paket dan melakukan ping semuanya dapat terdeteksi oleh IDS snort.



Gambar 5.7 Pemantauan Lalu Lintas Jaringan

1. Ping attack

Pada dasarnya, traffic ICMP yang diproduksi perintah ping, dianggap sebagai suatu serangan karena dapat dipergunakan intruder/penyusup untuk mendapatkan informasi mengenai mesin komputer target, memastikan apakah host target dalam keadaaan aktif atau tidak. Pada kasus ini penulis mensimulasikan dan menganalisis jenis serangan berprotokol ICMP. Pada tahap ini penulis melakukan ping attack ICMP dari mesin intruder/penyusup dengan menggunakan aplikasi Net Tools kepada mesin Server IDS snort.



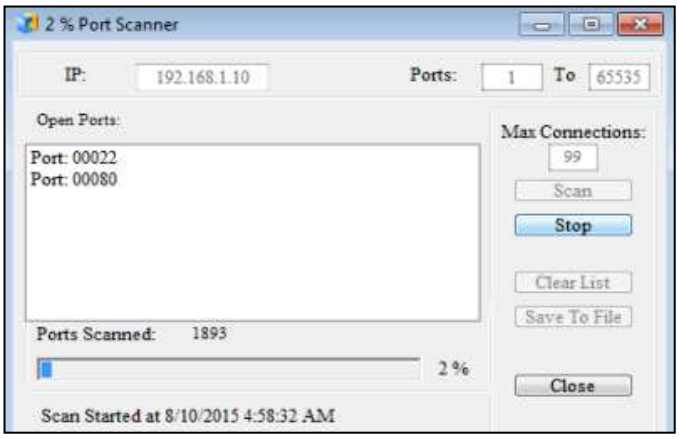
Gambar 5.8 Flooding Ping Attack

Dari Gambar 12, penyerangan dilakukan oleh penyusup dengan mengirimkan paket data dengan kapasitas 128 byte dan melakukan proses ping sebanyak 100x pada ip server yaitu 192.168.1.10, hal yang dinamakan ping attack dengan tujuan membuat sistem menjadi crash atau hang, ping attack merupakan jenis serangan DOS atau flooding yang dilancarkan melalui pengiriman paket-paket tertentu, biasanya paket-paket sederhana dengan jumlah yang sangat banyak dengan maksud mengacaukan keadaan jaringan target.

2. Port Scanning

Merupakan suatu proses untuk mencari dan membuka port pada suatu jaringan komputer. Hasil dari scanning tersebut akan didapatkan letak kelemahan sistem tersebut. Pada pengujian ini penulis akan mensimulasikan dan menganalisis aktivitas port scanning dengan menggunakan net tools, yang dilakukan dengan menggunakan alamat IP sebagai target yaitu 192.168.1.10. Yang dilakukan oleh penyerang (client) pada jaringan IDS Snort. Sebelum melakukan serangan terlebih dahulu

kita harus membuat rules/signature untuk mendefinisikan jenis aktivitas ini. Berdasarkan analisis traffic penulis mendefinisikan Net Tools ping sebagai berikut : alert icmp any any -> any any (msg:"ICMP PING NMAP attack; dzise:0; itype:8: rev 1; sid: 100003;). Keterangan rules : "ICMP PING NMAP attack"; berukuran paket obyte; menggunakan tipe icmp 8; revisi rules pertama: nomor identitas rules 100003. Setelah Snort telah direstart langkah terakhir adalah melancarkan serangan dengan menggunakan Net tools seperti gambar dibawah ini :



Gambar 5.9 Flooding Port Scanner

Pada Gambar 13 merupakan penyusupan dengan melakukan port scanner untuk melihat port yang aktif pada server untuk mencari celah keamanan pada port yang aktif tersebut.

3. Digital Blaster (flooding attack)

Aplikasi Digital Blaster (Digiblast) merupakan aplikasi yang digunakan oleh penyerang untuk menguji sensor snort yang telah dirancang. Penyerangan dilakukan oleh penyusup dengan melakukan

serangan flooding terhadap port 80 pada ip address server atau alat deteksi 192.168.1.10 yang berfungsi menbanjiri paket jaringan dengan menggunakan aplikasi Digiblast yang membuat sistem server menjadi hang.

Gambar 5.10 Flooding protocol tcp/udp

BAB VI

KESIMPULAN DAN SARAN

A. Kesimpulan

Dari penelitian ini di peroleh kesimpulan adalah sebagai berikut :

Telah berhasil mengimplementasikan sistem IDS pada server Universitas Satya Negara Indonesia sehingga staff IT dapat memantau jaringan dan dapat mengetahui apabila ada penyusup yang mencoba masuk kedalam sistem.

B. Saran

Berdasarkan kesimpulan-kesimpulan yang telah di kemukakan, dapat diajukan beberapa saran untuk pengembangan lebih lanjut antara lain:

1. Untuk meningkatkan segi keamanan di jaringan lokal, dapat menambahkan server active directory dengan menggunakan sistem operasi Windows Server dan Linux
2. Menanamkan IDS dan IPS pada server Universitas Satya Negara Indonesia agar dapat membatu administrator dalam memantau lalu lintas jaringan.
3. Dalam pemilihan ISP (Internet Service Provider) memilih kualitas bandwith yang baik agar tidak terjadi koneksi yang lambat dikarenakan tidak sesuai kapasitas bandwith yang digunakan di jaringan Lokal.

DAFTAR PUSTAKA

Andi. 2009. “Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9”, Yogyakarta

Cartealy, Imam. 2013. “ Linux Networking “, Yogyakarta

Diarta, E. 2013. Sistem Monitoring Deteksi Penyusup Dalam Daringan Komputer Menggunakan Snort Pada Ubuntu 12.04 Berbasis SMS Gateway.

Eichel, Zee. 2008. Attacking Side With Backtrack. www.indonesianbacktrack.or.id. 19 Maret 2012

Fauzi, S. R. (2010). Implementasi Intrusion Detection And Prevention System Di PT. Telekomunikasi Indonesia. Bandung: Politeknik Telkom.

FUI. 2011. Ebook Ubuntu Indonesia. Forum Ubuntu-Indonesia.Com. Diakses 15 Februari 2014

Rahman, Rizal. 2013, Mahir Administrasi Server Dan Router Dengan Linux Ubuntu Server 12.04 LTS. 8 April 2016

Rafiudin, Rahmat. 2010. *“Mengganyang Hacker dengan Snort”*, Yogyakarta.

Rainer Bye, et al, 2009, “Design and Modeling of Collaboration Architecture for Security”, International Symposium Collaborative Technologies and Systems.

Prihasmoro, Agung, Sukma. 2014, “ Simulasi Sistem Deteksi Penyusup Dalam Jaringan Komputer Berbasis Web Interface Serta Pencegahan Untuk Meningkatkan Keamanan ”, Jurusan Tekik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta, Jurnal JARKOM Vol. 2 No. 1, http://journal.akprind.ac.id/index.php/jarkom/article/view/322, 8 April 2016

Saputra, Angga. 2012, " Desain Sistem Pendeteksi Serangan Jaringan Komputer. Desain Sistem Pendeteksi Serangan Jaringan Komputer Pada Kantor Dinas Perhubungan Komunikasi Dan Informatika Musi Banyuasin ", Palembang. http://digilib.binadarma.ac.id/gdl.php?mod=browse&op=read&id=123-123-anggasaput-6944&newlang=english 8 April 2016

Utami, Putri, Syaimi, Agita. 2013, " Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd ", Vol.1 No.4 2337-439X, http://ejurnal.itenas.ac.id/index.php/rekaelkomika/article/view/273, 8 April 2016

SURAT PERNYATAAN KARYA SENDIRI

Yang bertandatangan dibawah ini :

Nama : AGIL SAPUTRO

NIM : 011201503125086

Program Studi : Teknik Informatika

Menyatakan bahwa Skripsi/Tugas Akhir ini adalah murni hasil karya sendiri dan seluruh isi Skripsi/Tugas Akhir menjadi tanggung jawab saya sendiri. Apabila saya mengutip dari karya orang lain maka saya mencantumkan sumbernya sesuai dengan ketentuan yang berlaku. Saya bersedia dikenai sanksi pembatalan Skripsi/Tugas Akhir ini apabila terbukti melakukan tindakan plagiat (penjiplakan)

Demikian pernyataan ini saya buat dengan sebenarnya

Jakarta,

(Agil Saputro)

011201503125086


UNIVERSITAS SATYA NEGARA INDONESIA
USNI
YAYASAN ABDI KARYA