SISTEM FLOODING DATA

Peniarsih, Noor Muhamadi
peniarsih18@gmail.com, noormuhamadi@yahoo.com

ABSTRAK

Banyak kasus yang membuktikan bahwa perusahaan yang terhubung ke internet sering kali mendapatkan gangguan, baik itu gangguan data maupun gangguan peralatan yang dimilikinya. Kerugian yang diakibatkan oleh hal tersebut tidaklah kecil. Untuk mengatasi masalah ini umumnya perusahaan menempatkan administrator untuk mengontrol penggunaan jaringan, tetapi administrator tentunya memiliki keterbatasan waktu. Pada saat jam kerja misalnya, kadang kala karena terlalu banyaknya aliran data tentunya administrator akan kesulitan menganalisa data-data yang lewat tersebut. Sedangkan suatu serangan bisa terjadi kapan saja. Baik pada saat administrator sedang bekerja ataupun tengah malam di mana administrator sedang istirahat dalam memantau data-data yang lewat dalam jaringannya. Salah satu serangan yang biasa terjadi adalah *flooding* data, akibat dari serangan *flooding* ini kinerja sistem akan terhambat dan jaringan tidak berfungsi seperti yang diharapkan. Oleh karena itu dalam penelitian ini akan membahas tentang bagaimana merancang dan membangun sistem yang mampu mendeteksi data *flood* sekaligus melakukan *blocking* pada data yang terbukti *flood*. Perkembangan teknologi jaringan internet di era sekarang ini semakin pesat, Kemudahan dan kepraktisan merupakan alasan dipilihnya internet sebagai salah satu sarana untuk membantu aktifitas suatu perusahaan, keuntungan yang diberikan juga sangat banyak, tetapi disamping keuntungan tersebut, internet juga banyak menyimpan kekurangan yang sangat mengkhawatirkan bagi para penggunanya. Salah satunya adalah bidang keamanan. Penelitian kuantitatif dilakukan untuk mengetahui mana data yang dianggap *flood* atau tidak dengan cara membandingkan berapa banyak paket yang terkirim dalam satuan waktu dengan standar maksimum paket yang telah ditentukan sebagai parameter data *flood*. Metode penelitian yang digunakan adalah metode penelitian studi literatur pada buku-buku dan sumber-sumber lain yang tercantum pada daftar pustaka. Jenis penelitian yang digunakan adalah penelitian eksperimen, dan juga penelitian kuantitatif.

Key Words : Jaringan, Flood,Sistem , Data

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi jaringan internet di era sekarang ini semakin pesat. Layanan atau fitur-fitur yang disediakan oleh jaringan internet juga begitu banyak ragamnya. Mulai dari *web server*, *File Transfer Protocol* (ftp), layanan *e-mail*, sampai fitur-fitur yang berhubungan dengan layanan transaksi juga sudah dapat ditemukan di dalam jaringan internet. Layanan tersebut seperti *e-commerce, e-banking, e-goverment* dan sebagainya.

Di samping keuntungan yang banyak tersebut, internet juga banyak menyimpan kekurangan yang sangat mengkhawatirkan bagi para penggunanya. Salah satunya adalah bidang keamanan. Banyak kasus yang membuktikan bahwa perusahaan yang terhubung ke internet sering kali mendapatkan gangguan, baik itu gangguan data maupun gangguan peralatan yang dimilikinya. Kerugian yang diakibatkan oleh hal tersebut tidaklah kecil. Kasus pencurian dan manipulasi data perusahaan saja dapat mengakibatkan kerugian hingga miliyaran rupiah, begitu pun kerusakan peralatan

yang digunakannya, dapat menyebabkan kerugian yang sangat besar. Saat ini sudah banyak perusahaan yang menggunakan internet sebagai sarana untuk melakukan aktifitas rutinnya. Tidak hanya perusahaan yang bergerak dalam bidang telekomunikasi saja yang menggunakan internet, tetapi juga perusahaan yang lain sudah menggunakan internet. Kecenderungan penggunaan internet pada perusahaan disebabkan karena dengan adanya internet maka perusahaan akan dimudahkan aktifitasnya baik dalam berkomunikasi maupun dalam mentransfer data.

Hal ini bisa dilihat pada bidang perbankan, sistem komunikasi data akan membantu perusahaan tersebut dalam melayani nasabahnya, begitu juga dalam bidang *marketing*, suatu barang hasil industri perusahaan dapat dengan mudah untuk dipublikasikan. Kemudahan dan kepraktisan merupakan alasan dipilihnya internet sebagai salah satu sarana untuk membantu aktifitas suatu perusahaan. Pada umumnya ancaman yang terjadi di dalam jaringan komputer antara lain: *Spamming, Sniffer, Virus, Cracker, Flood attack.* Dari berbagai ancaman jaringan komputer tersebut, salah satu yang berbahaya adalah terjadinya *flood attack* (pembanjiran data). *Flood attack* merupakan jenis serangan yang dilakukan dengan cara server dikirimkan permintaan (umumnya palsu) yang diluar perkiraan sehingga server tidak dapat menerima permintaan lain atau bahkan *down, hang,* dan *crash*.

Akibat dari kejadian tersebut maka jaringan komputer tidak lagi berfungsi seperti yang diharapkan, karena dampak dari serangan akan menghabiskan *resource*, menghabiskan RAM, hardisk penuh dengan data-data yang tidak penting, sehingga semua aktifitas terganggu, permintaan yang penting dari seorang user tidak bisa lagi dilayani, karena server sibuk dengan permintaan-permintaan yang tidak jelas. Untuk mengatasi masalah ini umumnya perusahaan menempatkan administrator untuk mengontrol penggunaan jaringan, tetapi administrator tentunya memiliki keterbatasan waktu. Pada saat jam kerja misalnya, kadang kala karena terlalu banyaknya aliran data tentunya administrator akan kesulitan menganalisa data-data yang lewat tersebut. Sedangkan suatu serangan bisa terjadi kapan saja. Baik pada saat administrator sedang bekerja ataupun tengah malam di mana administrator sedang istirahat dalam memantau data-data yang lewat dalam jaringannya. Oleh karena itu dalam mengatasi masalah seperti di atas dibutuhkan sistem ke dalam jaringan. Sistem diusahakan mampu membedakan apakah ini data *flood* atau tidak, jika data tersebut terbukti data *flood*, diusahakan agar sistem bisa mengambil tindakan untuk mengantisifasi hal tersebut agar tidak menimbulkan kerugian yang besar.

Akan lebih baik jika server bisa mengantisipasi langsung, sehingga kerugian bisa mendekati nol atau tidak sama sekali.Fungsi dari sistem ini nantinya adalah bagaimana sistem dapat mengambil data, sistem dapat mengklasifikasikan data-data yang ada, kemampuan sistem untuk mendeteksi *flood*, serta kemampuan sistem melakukan *blocking* pada data yang terbukti *flood.*

PEMBAHASAN

A. Landasan Teori

Jaringan komputer (*computer network*) atau sering disingkat jaringan saja adalah hubungan dua buah simpul (umumnya berupa komputer) atau lebih yang ditujukan untuk melakukan pertukaran data atau untuk berbagi perangkat lunak, perangkat keras, dan bahkan

berbagi kekuatan pemprosesan.

Salah satu contoh jaringan komputer adalah internet. Jaringan ini menghubungkan jutaan komputer yang tersebar di seluruh dunia. Siapapun orangnya bisa terhubung dalam jaringan ini. Kebutuhan akan adanya jaringan internet meningkat dengan pesat, hal ini disebabkan karena internet banyak memberikan keuntungan pada pemakai. Keuntungan pertama yang diperoleh dari internet adalah kemudahan dalam memperoleh informasi. Internet memungkinkan siapapun mengakses berita-berita terkini melalui koran-koran elektronik, mengakses literaturliteratur berupa *e-book*, makalah, riset, dan katalog, hal ini sudah dapat diperoleh secara *online*. Kedua, internet mendukung transaksi dan operasi bisnis atau yang dikenal dengan sebutan *e-business.* Melalui internet maka akan dimungkinkan untuk melakukan pembelian barang secara *online*. Kemudahan-kemudahan ini telah membuat sebagian masyarakat menjadikan internet sebagai kebutuhan primer.

Sebelum era penggunaan jaringan komputer, penggunaan komputer terbatas untuk mesin-mesin *standalone* yang terpisah dan independen 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 manfaat dari penggunaan jaringan komputer:

1. Berbagi perangkat keras
   Perangkat keras semacam harddisk, printer, CD-ROM drive, dan bahkan modem dapat digunakan oleh sejumlah komputer tanpa perlu melepas dan memasang kembali pada salah satu komputer yang akan memakainya. Peranti cukup dipasang pada sebuah komputer atau dihubungkan ke suatu peralatan khusus dan semua komputer dapat mengaksesnya. Cara seperti ini dapat menghemat biaya.
2. Berbagi program atau data
   Program ataupun data dimungkinkan untuk disimpan pada sebuah komputer yang bertindak sebagai server (yang melayani komputer-komputer yang akan membutuhkan data atau program). Cara seperti ini memungkinkan sebuah perusahaan untuk membeli sebuah perangkat lunak seperti pengolah data dan dipasang pada server, hal ini akan memungkinkan semua orang yang memerlukannya dapat mengakses program tersebut. Cara seperti ini lebih menghemat biaya dari pada kalau membeli program untuk setiap komputer. Penempatan data pada sebuah server juga memberikan keuntungan; antara lain menghindari duplikasi data dan ketidakkonsistenan. Data disimpan secara terpusat pada sebuah komputer, bukan pada setiap komputer pemakai sehingga tidak terjadi duplikasi data. Setiap perubahan pada suatu data oleh seseorang akan segera bisa diketahui oleh orang lain. Dengan cara seperti ini data selalu dalam keadaan terbaru. Perlu diketahui ketidakkonsistenan terjadi jika data yang sama disimpan pada tempat berbeda dan suatu ketika terjadi perubahan pada satu lokasi tidak diikuti perubahan pada lokasi lain. Mendukung kecepatan berkomunikasi. Dengan adanya dukungan jaringan komputer, komunikasi dapat dilakukan lebih cepat. Para pemakai komputer dapat mengirimkan surat elektronis dengan mudah dan bahkan dapat berkomunikasi secara langsung melalui tulisan (*chating*) ataupun melalui *telecon-*

ferens. Memudahkan pengaksesan informasi.

Jaringan komputer memudahkan pengaksesan informasi. Walaupun seseorang bepergian dia akan tetap bisa mengakses data yang terdapat pada server ketika dia membutuhkannya. Pertumbuhan internet salah satu implementasi jaringan terbesar di dunia, memungkinkan segala informasi yang ada di dunia dapat dengan mudah didapatkan. Siapapun dapat membaca berita tentang hari ini, hasil riset, atau bahkan katalog-katalog yang berisi penawaran barang.

Dengan banyaknya manfaat yang diberikan oleh jaringan komputer maka kebutuhan akan pemanfaatan jaringan dalam melakukan komunikasi data berkembang pesat dari waktu ke waktu, ditambah dengan koneksi internet yang semakin murah. Suatu jaringan komputer LAN dibangun dengan memperhatikan arsitektur standar yang dibuat lembaga standar industri dunia. Standar jaringan yang saat ini diakui dunia adalah *The Open System Connection* atau OSI yang dibuat oleh lembaga ISO (*The International Standard Organization*), Amerika Serikat. Seluruh fungsi kerja jaringan komputer dan komunikasi antar terminal diatur dalam standar ini. OSI adalah suatu standar komunikasi antar mesin yang terdiri atas 7 lapisan. Ketujuh lapisan tersebut mempunyai peran dan fungsi yang berbeda antara satu dengan yang lainnya. Setiap *layer* bertanggung jawab secara khusus pada proses komunikasi data. Misal, satu *layer* bertanggung jawab untuk membentuk koneksi antarperangkat, sementara *layer* lainnya bertanggung jawab untuk mengoreksi terjadinya *error* selama proses transfer data berlangsung. Model layer OSI dibagi dalam dua group: *upper layer* dan *lower layer*. *upper layer* fokus pada aplikasi pengguna dan bagaimana file direpresentasikan di komputer. Untuk *Network Engineer*, bagian utama yang menjadi perhatian adalah pada *lower layer*. *Lower layer adalah* intisari komunikasi data melalui jaringan aktual.

Tujuan utama penggunaan model OSI adalah untuk membantu *desainer* jaringan memahami fungsi dari tiap-tiap *layer* yang terhubung dengan aliran komunikasi data, termasuk jenis-jenis protokol jaringan dan metode transmisi. Model dibagi menjadi 7 *layer*, dengan karakteristik dan fungsi masing-masing.

Fungsi dari ketujuh lapisan tersebut adalah:

1) Physical layer

Physical layer berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan, dan pengkabelan. Selain itu layer ini juga mendefinisikan bagaimana *Network Interface Card (NIC)* berinteraksi dengan media *wire* atau *wireless*.

2) Data link layer

Data link layer berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut *frame*. Awal dan akhir *frame* ditandai dengan susunan bit khusus, sehingga *frame* tersusun dalam bit yang terdiri atas *address-field*, *control-field*, *data-field*, dan *error-control-field*, yang masing-masing memiliki fungsi tertentu. *Address-field* berisi alamat node pengirim (*source*) dan penerima (*destination*). *Control-field* dipakai untuk menandai adanya perbedaan jenis dari *data-link-frame*, termasuk *frame* data dan *frame* yang dipakai untuk mengatur *datalink-channel*. *Data-field* berisi data asli yang dikirimkan bersama *frame*. *Error-control-field* dipakai untuk mendeteksi adanya *data-link-*

frame. Datalink-layer merupakan *layer* pertama yang terlihat memiliki perhatian kepada pendeteksian error. *Error-control-field* umumnya berisi hasil pengecekan secara hardware yang dipergunakan untuk mendeteksi adanya error.

3) Network layer

Network-layer berfungsi mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan melakukan *routing* melalui *intern etworking* dengan menggunakan router dan switch layer-3. Pada layer ini juga dilakukan proses deteksi error dan transmisi ulang paket-paket yang error.

4) Transport layer

Transport layer berfungsi memecah data menjadi paket-paket data serta memberikan nomor urut setiap paket sehingga dapat disusun kembali setelah diterima. Paket yang diterima secara sukses akan diberi tanda (*acknowledgement*). Sedangkan paket yang rusak atau hilang ditengah jalan akan dikirim ulang.

5) Session layer

Berfungsi untuk mendefinisikan bagaimana koneksi dimulai, dipelihara, dan diakhiri. Selain itu, di *level* ini juga dilakukan resolusi nama. *Layer session*, sering disalahartikan sebagai prosedur logon pada network.

6) Persentation layer

Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan

7) Aplication layer

Berfungsi sebagai antarmuka (penghubung) aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan.

Dari ketujuh lapisan ini hanya *physical layer* yang merupakan perangkat keras selebihnya merupakan perangkat lunak. *Physical layer* merupakan media penghubung untuk mengirimkan informasi digital dari satu komputer ke komputer lainnya yang secara fisik dapat dilihat. Berbagai bentuk perangkat keras telah dikembangkan untuk keperluan ini. Satu diantaranya yang cukup banyak digunakan untuk keperluan jaringan komputer local (LAN) di Indonesia adalah ARCnet.

Salah satu protokol yang dikembangkan sebelum OSI adalah TCP/IP, namun demikian lapisan-lapisan pada TCP/IP tidak sepenuhnya cocok dengan lapisan OSI. Protokol TCP/IP hanya dibuat atas lima lapisan saja: *physical, data link*, *network*, *transport* dan *application*. Hanya lapisan-lapisan aplikasi pada TCP/IP mencakupi tiga lapisan OSI teratas. Khusus layer keempat, protokol TCP/IP mendefinisikan 2 buah protokol yakni *Transmision Control Protokol* (TCP) dan *User Datagram Protokol* (UDP). Sementara itu pada lapisan ketiga, TCP/IP mendefinisikan sebagai Internetworking Protokol (IP), namun ada beberapa protokol lain yang mendukung pergerakan data pada lapisan ini.

B. Tinjauan Pustaka

Dari uraian pada pembahasan sebelumnya telah dijelaskan dan dipaparkan tentang akibat atau dampak yang ditimbulkan oleh serangan *flooding data* (salah satunya *SYN flood*). Mengingat sangat besarnya kerugian yang dapat ditimbulkan oleh serangan ini maka dicobalah berbagai cara pencegahan.

Ada beberapa cara yang biasa dilakukan untuk mencegah dan mengurangi efek dari *SYN Flooding*, yakni sebagai berikut:

1) Meningkatkan ukuran buffer koneksi TCP untuk meningkatkan jumlah percobaan pembuatan koneksi yang dapat dilakukan secara simultan. Hal ini memang menjadi solusi sementara, karena penyerang juga mungkin meningkatkan ukuran paket *SYN* yang ia kirimkan untuk memenuhi buffer tersebut.
2) Mengurangi nilai waktu kapan sebuah percobaan pembuatan koneksi TCP menjadi "timed-out". Hal ini akan menjadi solusi sementara, jika jaringan berada dalam keadaan sibuk atau lambat.
3) Mengimplementasikan pendeteksian paket yang masuk ke dalam router, sehingga memblokir semua serangan yang menggunakan alamat palsu. Hal ini juga menjadi solusi sementara, karena tidak semua ISP mengimplementasikan fitur seperti ini
4) Memantau *firewall* dan mengkonfigurasikannya untuk memblokir serangan *SYN flood* ketika hal tersebut terjadi. Pendekatan ini merupakan pendekatan yang sering dilakukan oleh banyak organisasi, apalagi jika ditambah dengan *Intrusion Prevention System* (IPS), meski hal ini membutuhkan kejelian dari seorang administrator jaringan untuk memantau catatan (*log*) dari IPS dan *firewall* yang diatur. Bahkan, dengan kedua perangkat tersebut, klien-klien yang valid dapat ditolaknya karena konfigurasi yang tidak benar.

Dinil Mon Divakaran, Hema A. Murthy and Timothy A. Gonsalves, dalam jurnalnya *detection of syn flooding attacks using linear prediction analysis.* Dalam mendeteksi paket *flooding* mereka menggunakan metode *Linear Prediction*, mereka menganalisa paket dengan cara membandingkan perbedaan antara paket *SYN* dengan paket *SYN + ACK* , berapa interval waktu yang dibutuhkan server dalam mengirim paket *SYN + ACK* setelah menerima paket *SYN*. Mereka mengakui dalam kesimpulannya bahwa akan terjadi keterlambatan pendeteksian jika hal ini dilakukan. Berbeda dengan metode yang digunakan dalam penelitian ini, dalam hal pendeteksian datanya, apakah itu data *flood* atau tidak yaitu dengan cara menganalisa interval waktu berapa banyak paket TCP yang terkirim dalam satuan waktu, apakah besar paketnya lebih besar dari maksimum paket *SYN* yang telah ditentukan, selanjutnya dengan menganalisan port yang digunakan, jika port yang digunakan tidak tersedia (diidentifikasi sebagai penyusup) maka ip pengirim akan langsung diblok, apabila menggunakan port yang tersedia, baru diperiksa besarnya paket *SYN* apakah melebihi maksimum paket yang ditentukan, jika "YA" maka paket tersebut telah teridentifikasi sebagai data *flood* maka secara otomatis sistem akan melakukan pemblokiran ip pengirim.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian studi literatur pada buku-buku dan sumber-sumber lain yang tercantum pada daftar pustaka.

A. Lokasi Penelitian

Penelitian ini dilakukan di tempat-tempat yang memiliki *Local Area Network* yang terkoneksi ke internet maupun tidak terkoneksi ke internet.

B. Teknik Pengumpulan Data

Dalam pengumpulan data, digunakan dua metode, yaitu penelitian kepustakaan dan penelitian laboratorium, yaitu:

1. *Library research* atau penelitian kepustakaan yaitu cara mengumpulkan data dengan jalan mengutip pendapat-pendapat para ahli dari buku-buku bacaan yang ada kaitannya

dengan pembahasan penelitian ini.

2. *Labor research* atau penelitian labor yaitu mengumpulkan data dengan melakukan praktek ujicoba rancangan sistem pada laboratorium komputer.

C. Jenis Penelitian

Dalam penelitian ini, jenis penelitian yang digunakan adalah penelitian kuantitatif yang diuji secara eksperimen. Penelitian kuantitatif dilakukan untuk mengetahui mana data yang dianggap *flood* atau tidak dengan cara membandingkan berapa banyak paket yang terkirim dalam satuan waktu dengan maksimum paket yang telah ditentukan.

D. Tahapan Penelitian

Tahapan yang dilakukan dalam kegiatan penelitian:

1. Pengumpulan Data
   Mengumpulkan data-data yang diperlukan untuk merancang dan membangun sistem dengan menggunakan teknik pengumpulan data yang telah dijelaskan sebelumnya.
2. Pengolahan dan analisis data
   Pengolahan dan analisis data yang dilakukan dengan menggunakan data-data yang diperoleh dari proses pengumpulan data.
3. Perancangan
   Dilakukan perancangan spesifikasi sistem, mekanisme sistem, alat bantu dan sistem operasi yang digunakan, selain sistem secara umum, pengambilan data pada jaringan, identifikasi data dan proses data.
4. Implementasi
   Setelah dilakukan perancangan spesifikasi sistem, mekanisme sistem, alat bantu dan sistem yang digunakan, selain sistem secara umum, pengambilan data dari jaringan, identifikasi data dan proses data, kemudian diimplementasikan dalam program.
5. Pengujian
   Setelah melakukan pengimplementasian ke dalam program, kemudian program akan dicoba dengan teknik *black box* yaitu dengan menguji fungsionalitas system, dan efektifitas sistem, cara pengujiannya sebagai berikut:
   a. Membangun sebuah jaringan yang menggambarkan hubungan host-tohost
   b. Melakukan konfigurasi pada sistem
   c. Melakukan monitoring pada prototype LAN tersebut
   d. Melakukan flooding ke host yang telah diberi sistem
   e. Mengamati dan mengukur efektifitas bloking data flood

ANALISIS DAN PERANCANGAN SISTEM

Proses yang digunakan untuk merancang dan mengimplementasikan sistem pengamanan server yang akan dibuat. Pembahasan yang akan dilakukan meliputi spesifikasi dan mekanisme kerja program yang diinginkan. Setelah itu berlanjut ke pembahasan mengenai alat Bantu yang akan digunakan. Setelah masing-masing alat bantu itu dijabarkan, pembahasan menyentuh hal-hal yang lebih spesifik dari sistem, yaitu bagaimana data diambil dan bagaimana pengolahan data-data tersebut.

Kemudian akan dijabarkan secara lebih jelas mengenai desain sistem secara keseluruhan. Proses implementasinya dijelaskan melalui algoritma dari program-program yang akan di buat.

Dalam mendesain sistem ini digunakan flowchart untuk membantu dalam mengkomunikasikan logika program sistem yang akan dirancang.

A. Spesifikasi Sistem

Sebelum melakukan proses pembuatan sistem, terlebih dahulu ditentukan spesifikasi sistem. Spesifikasi sistem akan menjadi titik tolak sekaligus menjadi acuan untuk pembuatan sistem dan juga menentukan kapabilitas dan kemampuan apa saja yang harus bisa dipenuhi sistem yang dimaksud.

Sistem yang dibangun memiliki spesifikasi sebagi berikut:

1. Sistem beroperasi pada platform Windows.
2. Sistem yang digunakan harus bisa mengambil data-data dari jaringan.
3. semua data yang dikumpulkan disimpan dalam database
4. *Resource* yang digunakan harus seminimal mungkin

B. Desain Sistem Secara Umum

Input dari program adalah data jaringan yang masuk kemudian akan diproses apakah data yang ada tersebut melakukan flooding atau tidak. Jika data yang datang adalah flooding maka secara otomatis akan memblok ip dan port dari mana data itu berasal dan kalau ya berarti data akan ditujukan kepada tujuanya.

Dalam pendeteksian data flooding, pertama sistem akan melihat apakah data merupakan data kiriman atau data dari dalam. Jika data merupakan data kiriman maka akan dicek *port* yang digunakan tersedia atau tidak. Jika tidak tersedia maka langsung diblock. Jika port tersedia, paket-paket tersebut dicek , apakah paket tersebut merupakan paket TCP syn. Jika paket TCP syn lebih besar dari TCP syn maksimum yang ditetapkan maka akan diblock.

C. Desain Pengambilan Data

Data tidak secara keseluruhan diambil karena untuk menjaga privasi user, (hanya header-header paket tersebut yang diambil). Olehnya ituperlua danya sniffer untuk memperoleh header dari data tersebut.

Data yang akan masuk dibelokkan terlebih dahulu untuk diambil datanya sebelum dilanjutkan ke tujuan sebenarnya. Di dalam pembelokan ini tidak berarti bahwa data paket ditahan dulu untuk diteliti, melainkan data hanya di-*capture* headernya.

D. Desain Pengidentikasian Data

Menurut standar protokol yang ada sekarang ini hampir semuanya menggunakan struktur data Ethernet II sebagai struktur untuk mengirimkan atau menerima data. Struktur data dalam Ethernet II itu sendiri disebut frame. Format frame Ethernet II adalah sebagai berikut:

Tabel Format frame Ethernet II

Preamble (8 octets)	Destination Address (6 octets)	Source Address (6 octets)	Type (2 octets)	Data (46-1500 octets)	FCS (3 octets)

Awalnya mengandung serangkaian 8 bit dengan pola tertentu yang memberitahu node penerimaan setiap suatu frame yang dimulai. Untuk alamat tujuan dan sumber masing-masing 48 bit (6 oktet). Field type menunjukkan jenis data dari field data, dengan besar 16 bit (2 oktet).

Dengan mengetahui header dari setiap paket yang masuk dapat kita peroleh data-data dari paket, yang kemudian kita bisa mengklasifikasikan setiap data yang datang apakah itu paket TCP, UDP atau juga ICMP. Beserta semua keterangan dari mana paket itu berasal, kemana tujuannya, juga besar dari paket tersebut.

Paket yang datang kemudian akan diidentifikasikan apakah data tersebut merupakan paket TCP.Setelah didapatkan rincian dari paket paket yang datang tersebut, maka data kemudian dimasukkan ke dalam database. Tujuan memasukkan data ke dalam database agar lebih mudah dalam mengoalah data tersebut dalam suatu kesatuan data. Data yang diolah bukan data yang ditampilkan saja tetapi semua data yang lewat dalam jaringan. Selain itu juga digunakan untuk mengurangi besarnya data yang tersimpan. Semakin besar data yang harus diolah akan mengakibatkan kelambanan dari proses secara keseluruhan. Kemungkinan terburuk yang terjadi adalah program akan mengalami *overflow* atau *crash*.

E. Pemprosesan database pada paket TCP

Pengolahan data paket TCP hanya ditujukan pada TCP SYN saja, dan penggunaan port dari paket tersebut. Untuk data paket yang lainya misalnya ACK ataupun SYN ACK tidak ditampilkan untuk mempersingkat waktu tampilan dan juga untuk menanggulangi komputer tempat program berlangsung akan *crash* ataupun *hang*.

F. Desain Pengolahan Data

Setelah semua data dari paket-paket tersebut masuk ke dalam database maka yang dilakukan selanjutnya adalah pengolahan data. Pengolahan ini ditujukan untuk menentukan apakah data yang datang termasuk data yang flood atau bukan. Proses pengolahan ini dilakukan terpisah antar protokol. Karena setiap protokol mempunyai karakteristik sendiri-sendiri (yang ditekankan di sini adalah paket TCP seperti pada batasan masalah). Flood yang disebabkan oleh TCP mungkin lebih jelas karena jenis flood yang digunakan adalah SYN TCP flood, yaitu pengiriman paket TCP untuk *request* koneksi hubungan host-to-host. Meskipun demikian flood yang diakibatkan oleh TCP juga akan mengganggun koneksi tersebut. Mengingat paket TCP amerupakan paket yang membutuhkan bandwith yang besar. Dengan demikian untuk mendefinisikan apakah suatu paket TCP termasuk data flood adalah dengan cara melihat berapa kali munculnya paket TCP SYN dalam satuan waktu. Apabila ternyata melebihi batasan maka bisa di kategorikan dalam flood TCP SYN.

G. Desain Pemblokiran IP

Setelah informasi paket TCP didapat, maka akan dicek apakah paket tersebut menggunakan port yang aktif atau tidak. Jika paket menggunakan port yang tidak aktif, maka alamat ip asal paket dan port yang digunakan akan diblok oleh sistem. Jika paket yang datang menggunakan port yang aktif, maka data alamat IP sumber dan port yang digunakan akan dimasukkan ke dalam *suspect list*. Setelah itu dicek apakah jumlah paket melebihi jumlah maksimum paket yang diizinkan. Jika melebihi maka alamat IP sumber paket dan port yang digunakan akan diblok. Jika tidak paket akan diteruskan.

H. Implementasi

Di dalam program ini terdapat variabel-variabel yang perlu disetting terlebih dahulu untuk mengatur bagaimana program itu bekerja.

1. Pada groupbox *List Adapters* akan ditampilkan *Network Interface Card* yang ditemukan, dan terdapat option untuk memilih adapter mana yang diaktifkan.
2. Pada groupbox *List Allowed Port* merupakan penentuan port-port apa saja yang bisa digunakan.
3. Pada groupbox *List Blocked Ip Address* akan ditampilan ip yang telah diblok yang terbukti melakukan serangan *flood.*
4. Pada groupbox *Capture Command Control* terdapat Button *Start, labelEdit* untuk pengisian pemantauan paket (dalam satuan detik), durasi pengecekan paket TCP (dalam satuan detik), banyaknya paket TCP yang akan dilewatkan.
5. Pada groupbox *Ip Monitor* akan ditampilkan paket-paket yang lewat dalam jaringan.
6. Pada groupbox *status* akan ditampilkan aktifitas-aktifitas paket yang lewat.

PENGUJIAN SISTEM

Pada bab ini akan dibahas mengenai pengujian terhadap sistem. Pertamatama yang akan dibahas mengenai batasan pengujian kemudian dijabarkan pula bagaimana dilakukan pengujian tersebut. Setelah itu pembahasan berlanjut ke hasil pengujian.

A. Batasan Pengujian

Yang diuji dari sistem adalah :

1. Kemampuan sistem untuk mengambil data dari ethernet card.
2. Kemampuan sistem untuk mendeteksi Flood.
3. Kemampuan sistem untuk melakukan blooking pada data yang terbukti Flood.

B. Cara pengujian

Untuk melakukan pengujian tersebut tersebut penulis melakukan hal hal berikut:

1. Menjalankan sebuah prototype dari sebuah hubungan host-to-host
2. Melakukan konfigurasi pada sistem
3. Melakukan monitoring pada proto-type LAN tersebut
4. Melakukan flooding ke host yang telah diberi sistem
5. Melihat hasil dari sistem apakah data flood dapat di blok atau tidak

C. Prototype Jaringan

Akan dibangun suatu koneksi yang menunjukkan koneksi internet. Prototype tersebut adalah sebagai berikut. Akan diletakkan 2 buah server yang berfungsi sebagai hubungan *host-to-host*. Dan sebuah client pada server yang sudah diberi program tersebut. Dalam hal ini komputer A merupakan komputer yang melakukan serangan TCP *flood,* sedangkan komputer B merupakan komputer tempat penanggulangan flooding (firewall) dijalankan.

D. Konfigurasi Pengujian

Pengaturan dari sistem untuk mendapatkan hasil pengujian seperti kejadian flooding yang nyata adalah sebagai berikut:

1. **Komputer A**
   Komputer ini berfungsi sebagai komputer yang melakukan penyerangan TCP *flood* ke komputer B. Komputer ini akan menjalankan sebuah program penguji yang akan melakukan *flooding.* Program ini akan mengirimkan paket-paket TCP syn secara terus-menerus. *Port* yang digunakan juga bisa ditentukan, sehingga dapat menyerupai *flood* yang sebenarnya. Dalam program ini akan ditentukan beberapa sampel data yang akan dikirimkan.

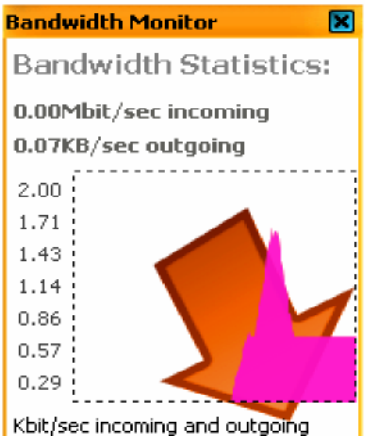
Tabel sampel data yang akan dikirim

Target	Port	Interval pengiriman data (ms)
Komputer B (10.10.1.1)	6666	3000
	8080	1000
	1433	500
	3264	100
	3306	1

2. **Komputer B**
   Komputer B merupakan komputer tempat program penanggulangan data *flooding* diletakkan. Komputer ini berfungsi sebagai host yang kita miliki yang akan digunakan sebagai korban dari *flooding* data. Komputer ini dirancang agar bisa melakukan *blocking* kalau komputer A yang melakukan *flooding*. Komputer ini juga dijalankan program trojan yang membuka sebuah service untuk membuka jalan bagi komputer A agar dapat melakukan *flooding.* Dalam program penanggulangan flooding tersebut sudah terdapat variabelvariabel yang perlu diisikan terlebih dahulu untuk mengatur bagaimana program itu bekerja

E. Hasil Pengujian

Dalam hasil pengujian ini akan dibandingkan kondisi aliran data sebelum diserang, sementara diserang, dan setelah dicegah. Untuk mengetahui hasil ini digunakan tools *Bandwidth Monitor*. Pada kondisi normal (saat komputer penyerang hanya melakukan *request* paket (ping)), paket yang terkirim 0,07 KB/s



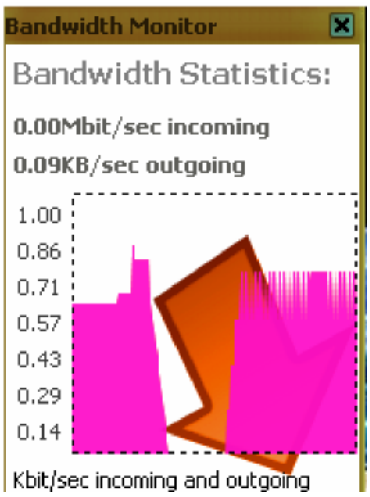
Gambar V.5 kondisi bandwidth normal

Pada kondisi selanjutnya saat komputer diserang dengan mengirimkan data sesuai dengan sampel data pada program penyerang.

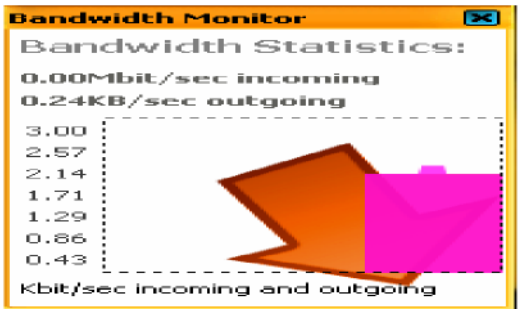
Tabel hasil monitoring saat komputer diserang

port	Interval pengiriman data (ms)	banyaknya data terkirim (KB/s)
6666	3000	0,09
8080	1000	0,24
1433	500	0,48
3264	100	2,18
3306	1	15,38

Berikut adalah gambar hasil *monitoring* dengan menggunakan *Bandwidth Monitor.*

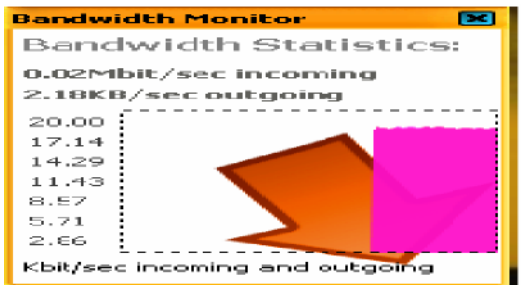


Gambar data terkirim dalam 3000 ms



Gambar data terkirim dalam 1000 ms

Gambar data terkirim dalam 500 ms



Gambar kondisi data terkirim dalam 100 ms

Gambar kondisi data terkirim dalam 1 ms

Kondisi selanjutnya saat terbukti terjadinya *flooding*, dengan menggunakan parameter data *flooding* pada program pencegah.

PENUTUP

Dari pengujian sistem yang ada maka dapat diambil kesimpulan bahwa sistem yang dibuat memiliki keunggulan sebagai berikut:

1. Sistem mampu mendeteksi apakah data yang masuk merupakan data flood atau tidak. Sistem mampu memblokir alamat IP dan port berdasarkan sumber paket yang melakukan flooding. Sistem mampu bekerja otomatis dengan memgambil keputusan apakah data yang masuk merupakan data flood atau tidak.
2. Flooding data yang terjadi hanya bisa dicegah sampai titik server saja, bisa mencegah data yang masuk ke dalam jaringan, yang bisa menyebabkan kerusakan yang lebih parah.
3. Sistem menyempurnakan sistem ini dengan menambahkan suatu komunikasi dari server ke server. Dalam hal ini hubungan server lokal ke server yang lebih tinggi.
4. Komunikasi ini adalah untuk mengadakan pemblokiran IP pada server yang lebih tinggi sehingga gangguan yang ada lebih bisa dikurangi lagi. Traffic di jaringan lokal akan kembali normal karena data yang sebelumnya datang sudah diblokir di tingkat lebih atas.

5. Flooding data juga bisa terjadi di protokol selain TCP. Oleh karena itu sistem juga perlu ditambah kemampuan untuk mencegah flooding yang menggunakan protokol lain seperti UDP dan ICMP.

DAFTAR PUSTAKA

A. Shaikh, Riaz, Ahmad Ali Iqbal, dan Kashan Samad *ANOMALY DETECTION ALGORITHMS FOR DETECTING SYN FLOODING ATTACKS,* Pakistan: NUST Institute of Information technology

Departemen Agama RI**.** *Al-qur'an dan Trejemahan.* Bandung : Diponegoro, 2005.

Dennis, Alan, *NETWORKING: in the internet age* ,John Wiley & Sons, Inc, Bloominton: 2002

DoS-Flooding-dan-DDoS, *http://blog.unikom.ac.id/10108262/G9.DoS-Floodingdan-DoS.html* (29 Agustus 2010)

Edison, Jhon dan Jhonsen, *Membangun Wireless LAN* (Jakarta : PT Alex Media Komputindo, 2006)

Apakah-tcp-ip-itu, *http://my.opera.com/winaldi/blog/2007/02/26/apakah-tcp-ip-itu* (6 juni 2010)

Divakaran , Dinil Mon, Hema A. Murthy dan Timothy A. Gonsalves *DETECTION OF SYN FLOODING ATTACKS USING LINEAR PREDICTION ANALYSIS,* (Department of Computer Science and Engineering, Indian Institute of Technology, Madras)