IMPLEMENTASI SISTEM PENCEGAHAN DATA *FLOODING* PADA JARINGAN KOMPUTER

Ashadi Soki Agusaputra.,S.Kom[1], M.Izman ST.,MM.,Ph.D[2] ,Baibul Tujni.,SE.MM.Si [3]
Dosen Universitas Bina Darma [1], Mahasiswa Universitas Bina Darma [2]
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el:ashadisoki@ymail.com[1], m.herdiansyah@mail.binadarma.ac.id[2],baibul@yahoo.co.id[3]

abstract : Internet has so many benefits and public, for it requires a security system in keeping the information and data available on the Internet that are not undermined by parties who are not responsible. The trend caused by the use of the internet in terms of ease of communication and data transfer. But besides the many advantages, the internet also saves a lot of very short one is a constraint in the security field. Many cases which prove that the company is connected to the internet often have disturbances in both the data held and its equipment. Losses would this not exactly small. Not to mention the damage to the equipment used by these companies, which arguably is not cheap. For that to be a system that mampi prevent outside interference that could cause flooding of data on computer networks connected to the Internet.

Keywords: data flooding, network.

Abstrak : Internet sudah begitu banyak memberikan manfaat dan bersifat publik, untuk itu dibutuhkan suatu sistem keamanan dalam menjaga informasi dan data yang ada di internet supaya tidak dirusak oleh pihak-pihak yang tidak bertanggung jawab. Kecenderungan penggunaan internet disebabkan oleh adanya kemudahan dalam hal komunikasi dan transfer data. Tetapi disamping keuntungan yang banyak tersebut, internet juga menyimpan banyak kekurangan salah satu yang sangat menjadi kendala adalah dalam bidang keamanan. Banyak kasus yang membuktikan bahwa perusahaan yang tersambung di internet sering kali mendapatkan gangguan baik dalam data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil. Belum lagi kerusakan peralatan yang digunakan oleh perusahaan tersebut, yang bisa dibilang tidak murah. Untuk itu perlu dibuat suatu sistem yang mampi mencegah terjadinya gangguan dari luar yang dapat menyebabkan terjadinya data *flooding* pada jaringan komputer yang berhubungan dengan internet.

Kata kunci : Data *flooding*, jaringan.

1. PENDAHULUAN

Perkembangan teknologi jaringan internet semakin pesat. Layanan atau fitur- fitur yang disediakan dalam jaringan internet juga begitu banyak ragamnya. Mulai dari *web server*, *File Transfer Protocol* (ftp), layanan *E-mail*, sampai *feature-feature* yang berhubungan dengan layanan transaksi yang semakin marak di dalam jaringan internet. Layanan tersebut seperti *E-Commerce*, *E-Banking*, *E-Goverment* dan sebagainya. Karena internet yang begitu banyak memberikan manfaat dan bersifat publik, maka dibutuhkan suatu sistem keamanan dalam menjaga informasi dan data yang ada di internet supaya tidak dirusak oleh pihak-pihak yang tidak bertanggung jawab yang potensial melakukan pengrusakan seperti *hacker* dan *cracker*.

Sudah banyak perusahaan yang menggunakan internet sebagai sarana dalam melaksanakan aktifitas rutin perusahaan dan aktifitas rutin lainnya. Kecenderungan penggunaan internet ini disebabkan oleh dengan adanya internet akan didapatkan kemudahan 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 internet ini.

Tetapi disamping keuntungan yang banyak tersebut, internet 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 internet sering kali mendapatkan gangguan baik dalam data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil. Belum lagi kerusakan peralatan yang digunakan oleh perusahaan tersebut, yang bisa dibilang tidak murah.

Dalam faktor keamanan ini biasanya perusahaan menempatkan administrator untuk menjaga. Karena terlalu banyaknya aliran data 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.

2. METODOLOGI PENELITAN

2.1 Metode Penelitian

Metode yang digunakan dalam penyusunan laporan penelitian ini adalah metode deskriptif. Menurut Sugiyono (2004:11): ”Penelitian deskriptif adalah penelitian yang dilakukan untuk mengetahui nilai variable mandiri, baik satu variable atau lebih (*independent*) tanpa membuat perbandingan, atau menghubungkan dengan variable yang lain.”

Metode penelitian ini digunakan untuk mengungkapkan gambaran yang jelas mengenai keadaan dalam instansi berdasarkan data yang diperoleh, dengan cara mengumpulkan dan menganalisis data tersebut dan mengubahnya menjadi informasi baru yang digunakan dalam menunjang pengambilan keputusan dalam perusahaan.

2.2 Metode Pengumpulan Data

Teknik pengumpulan data dilakukan melalui penelitian kepustakaan dan penelitian lapangan serta observasi lapangan.

2.3 Metode Analisis

Berdasar metode penelitian yang digunakan yaitu metode deskriptif, maka dalam penelitian ini metode analisis yang digunakan yaitu metode statistik. Metode statistik merupakan seperangkat teknik matematik untuk mengumpulkan,

mengorganisasi, menganalisis dan menginterpretasi data angka. Metode statistik digunakan untuk membuat deskripsi dan analisis. Metode Statistik diterapkan secara tepat didasarkan pada jawaban-jawaban dari pertanyaan-pertanyaan yang perlu dipahami sebagai berikut:

a. Fakta-fakta apakah yang akan dikumpulkan untuk memberikan informasi yang dibutuhkan dalam menjawab hipotesis
b. Bagaimana fakta itu akan diseleksi, dikumpulkan, diorganisasikan dan dianalisis.
c. Asumsi-asumsi apakah yang mendasari metodologi statistik yang hendak dipakai.
d. Kesimpulan-kesimpulan apakah yang hendak ditarik secara valid dari analisis data.

2.4 Data Flooding

Traffic data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan kelambatan dalam pengiriman dan penerimaan data. Pengiriman data tersebut dapat mengakibatkan lambatnya jalur *traffic* yang ada dalam jaringan, dan juga bisa mengakibatkan kerugian lain yang cukup berarti. Pengiriman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna biasa disebut *flood*. (Pratama, 2010).

Data flooding merupakan suatu kejadian di dalam jaringan dimana dalam jaringan tersebut terjadi suatu transfer data dalam jumlah yang besar sehingga mengganggu kinerja komputer yang terhubung di dalam jaringan tersebut, hal ini kemungkinan bisa disebabkan adanya serangan dari luar yang biasa disebut dengan DOS/DDOS (*Denial of Service/ Distributed Denial of Services*) yaitu serangan pada jaringan komputer yang berusaha untuk menghabiskan sumber daya sebuah peralatan komputer, sehingga jaringan komputer menjadi terganggu. (Utomo, 2011:93).

Sedangkan teori lain menyatakan serangan *SYN flood* adalah serangan yang terjadi saat sebuah jaringan dipenuhi paket-paket SYN yang menginisiasi koneksi-koneksi yang tidak lengkap dan jaringan ini tidak dapat memproses koneksi yang sah. (Thomas, 2005 : 46).

2.5 Jaringan Komputer

Menurut Sukmaaji dan Rianto (2008; hal : 1), jaringan komputer adalah sekelompok komputer otonom yang saling berhubungan satu dengan lainnya menggunakan protocol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, aplikasi, dan perangkat keras secara bersama-sama.

Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data/informasi, berbagi resource yang dimiliki, seperti file, printer, media penyimpanan (hardisk, floppy disk, cd-rom, flash disk, dll). Data yang berupa teks, audio,. maupun video bergerak melalui media kabel atau tanpa kabel sehingga memungkinkan pengguna komputer dalam jaringan komputer dapat saling bertukar file/data, mencetak pada printer yang sama dan menggunakan hardware/ software yang terhubung dalam jaringan secara bersama-sama. Tiap kornputer, printer atau periperal yang terhubung dalam jaringan disebut dengan node. Sebuah

jaringan komputer sekurang-kurangnya terdiri dari dua unit komputer atau lebih, dapat berjumlah puluhan komputer, ribuan, atau bahkan jutaan node yang saling terhubung satu sama lain.

2.6 Keamanan Jaringan

Pada dasarnya sistem jaringan komputer merupakan sistem jaringan yang terbuka, artinya pengguna (*user*) dalam jaringan tersebut dapat mengakses *resource* yang tersedia. Metode kriptografi merupakan salah metode yang digunakan untuk mengacak data, sehingga orang lain tidak dapat membaca data yang dikirimkan. Adapun jenis-jenis ancaman dapat dijelaskan sebagai berikut : (Utomo, 2002 : 91).

2.6.1 DOS/DDOS

Denial of Services dan *Distributed Denial of Services* adalah sebuah bentuk serangan yang bertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu. Salah satu bentuk serangan ini adalah '*SYN Flood Attack*', yang mengandalkan kelemahan dalam sistem '*three-way-handshake*'. '*Three-way-handshake*' adalah proses awal dalam melakukan koneksi dengan protokol TCP. Proses ini dimulai dengan pihak klien mengirimkan paket dengan tanda SYN. Lalu kemudian pihak server akan menjawab dengan mengirimkan paket dengan tanda SYN dan ACK. Terakhir, pihak klien akan mengirimkan paket ACK. (Utomo, 2002 : 93)

2.6.2 Micro-blocks

Ketika ada sebuah host menerima paket inisiasi, maka host akan mengalokasikan ruang memori yang sangat kecil, sehingga host tersebut bisa menerima koneksi lebih banyak. Diharapkan ruang memori dapat menampung semua koneksi yang dikirimkan, sampai terjadi *connection-time-out*, dimana koneksi-koneksi yang stale, yaitu koneksi yang tidak menyelesaikan proses '*three-way-handshake*' atau sudah lama tidak ada transaksi data, akan dihapuskan dari memori dan memberikan ruang bagi koneksi-koneksi baru. Metode ini tidak terlalu efektif karena bergantung pada kecepatan serangan dilakukan, apabila ternyata kecepatan paket serangan datang lebih cepat daripada lamanya waktu yang perlu ditunggu agar terjadi *connection-time-out* pada paket-paket yang stale, make ruang memori yang dapat dialokasikan akan tetap habis. (Utomo, 2003 : 98)

2.6.3 SYN Cookies

Ketika menerima paket inisiasi, host penerima akan mengirimkan paket tantangan yang harus dijawab pengirim, sebelum host penerima mengalokasikan memori yang dibutuhkan. Tantangan yang diberikan adalah berupa paket *SYN-ACK* dengan nomor urut khusus yang merupakan hasil dari fungsi hash dengan input alamat IP pengirim, nomor port, dan lain-lain. Jawaban dari pengirim akan mengandung nomor urut tersebut. Tetapi untuk melakukan perhitungan hash membutuhkan sumber-daya komputasi yang cukup besar, sehingga banyak server-server yang aplikasinya membutuhkan kemampuan komputasi tinggi tidak mempergunakan metode ini. Metode ini merubah waktu pengalokasian memori, yang

tadinya pada awal dari proses '*threeway-handshake*', menjadi diakhir dari proses tersebut. (Utomo, 2003 : 98)

2.6.4 Packet Sniffing

Packet Sniffing adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan karena pada dasarnya semua koneksi ethernet adalah koneksi yang bersifat broadcast, di mana semua host dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah host. Pada keadaan normal, hanya host yang menjadi tujuan paket yang akan memproses paket tersebut sedangkan host yang lainnya akan mengacuhkan paketpaket tersebut. Namun pada keadaan tertentu, sebuah host bisa merubah konfigurasi sehingga host tersebut akan memproses semua paket yang dikirimkan oleh host lainnya. (Utomo, 2003 : 99).

2.7 Metode Pencegahan

Data *flood* sebagian besar disebabkan karena adanya exploitasi *buffer overflow*. Pencegahan berikut ini dilihat dari sisi seorang programmer, dengan memasukkan beberapa script program ke dalam aplikasi yang sedang dibangun. Berikut adalah tindakan yang bisa dilakukan untuk menghindari terjadinya eksploitasi *buffer overflow*. (Utomo, 2002 : 98).

a. Memvalidasi Data

Sebuah program yang berjalan dengan *privilge* tinggi, mengharuskan untuk melindungi semua data dan harus menganggap semua data yang masuk dicurigai.

b. *Buffer Non-Executable*

Konsepnya adalah membuat *segment* data sebuah program tidak dapat dieksekusi. Dengan menjadikannya tidak dapat dieksekusi, maka tidaklah mungkin bagi penyerang untuk mengeksekusi kode yang mereka masukkan ke *buffer input* program korban. Cara ini digunakan pada sistem operasi komputer lama, tetapi pada sistem operasi UNIX dan MS Windows teknik ini tidak digunakan, karena keduanya tergantung pada kemampuan memasukkan kode dinamis ke dalam *segment* data program untuk mendukung berbagai optimisasi kinerja.

c. *Array Bounds* Checking

Meskipun memasukkan kode adalah sebuah tindakan pilihan bagi serangan *buffer overflow*, pengkorupsian aliran kendali merupakan hal yang penting. Dengan menggunakan metode *array bound checking akan* menghentikan *vunerability* dan serangan *buffer overflow*. Jika sebuah *array* tidak dapat di-*overflow*, maka *array* tidak dapat digunakan untuk mengkorupsi program yang terletak di alamat memori berikutnya. Untuk mengimplementasikan metode ini, semua pembacaan dan penulisan ke *array* yang harus diperiksa untuk memastikan bahwa mereka tidak melampaui batasan *array*.

d. Memeriksa Index

Indeks yang digunakan untuk memanipulasi sebuah *array* harus diperiksa dengan teliti.

2.8 Analisis dan Perancangan Sistem

2.8.1 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
5. Sistem harus bersifat multiuser dan multitasking. Dikembangkan dengan alat bantu yang mudah digunakan.

2.8.2 Sistem Operasi dan Alat Bantu yang Digunakan

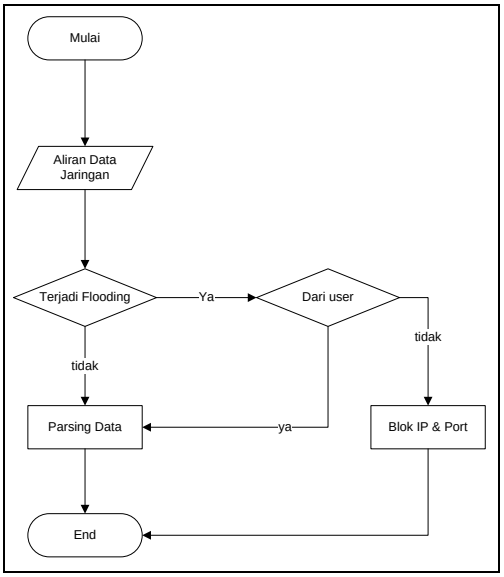
Setelah spesifikasi dari sistem dan mekanisme kerja sistem telah dapat dijabarkan maka proses selanjutnya adalah memilih sistem operasi dan tool yang akan digunakan untuk membangun sistem tersebut. Alat Bantu tersebut merupakan paket aplikasi dan bahasa pemrograman yang memiliki kemampuan sesuai dengan kebutuhan untuk membangun sistem ini. Sub bab berikut ini akan membahas mengenai sistem operasi dan alat bantu yang akan digunakan. Pembahasan meliputi deskripsi umum, kegunaan dan keunggulan sistem tersebut.

Adapun sistem operasi yang akan digunakan adalah windows XP yang akan diinstalasi ke dalam sebuah jaringan komputer. Aplikasi akan diinstalasi ke dalam jaringan komputer dengan topologi star. Pertimbangan menggunakan topologi ini memiliki kelebihan antara lain :

1. Kerusakan pada satu saluran hanya akan mempengaruhi jaringan pada saluran tersebut dan *client* yang terpaut
2. Tingkat keamanan termasuk tinggi
3. Tahan terhadap lalu lintas jaringan yg sibuk
4. Penambahan dan pengurangan *client* dapat dilakukan dengan mudah
5. Tidak mengganggu bagian jaringan lain
6. Kontrol terpusat
7. Kemudahan deteksi dan isolasi kesalahan kerusakan
8. Kemudahan pengelolaan jaringan

2.8.3 Desain Sistem Secara Umum

Secara garis besar sistem yang akan dibangun adalah sebagai berikut :

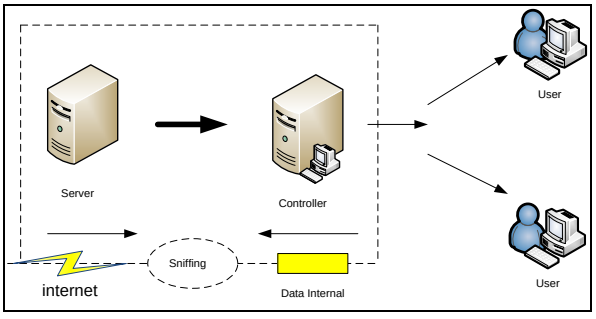


Gambar 1 Desain umum program blokir otomatis pada *flood*

Dari gambar di atas dapat dijelaskan input dari program adalah data jaringan yang masuk kemudian akan di proses apakah data yang ada tersebut melakukan *flooding* atau tidak. Jika data yang datang adalah *flooding* atau serangan dari komputer luar maka sistem akan mencari apakah data merupakan permintaan user atau tidak. Jika data datangnya dari luar yang tidak diinginkan maka secara otomatis akan memblok ip dan port darimana data itu berasal dan jika data berasal dari user maka data akan ditujukan kepada tujuanya.

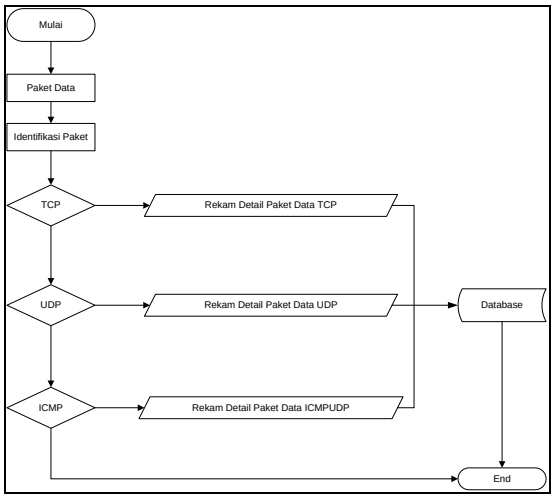
2.8.4 Desain Pengambilan Data

Jika menggunakan Windows *server* sebagai *router* tentunya hal tersebut akan tidak bisa dilakukan secara langsung. Karena kita harus mengambil data dari paket tersebut secara detail, walaupun yang akan kita ambil hanya sebatas header dari data. Bukan keseluruhan dari paket tersebut untuk menjaga privasi user dari *server*. Dengan demikian kita perlu menempatkan *sniffer* untuk memperoleh header dari data itu.. Seperti yang tergambar sebagai berikut :



Gambar 2 Proses pengambilan data

Dari gambar di atas dapat dijelaskan bahwa data yang akan masuk atau keluar dibelokkan terlebih dahulu untuk diambil datanya sebelum dilanjutkan ketujuan sebenarnya. Di dalam pembelokan ini tidak berarti bahwa data paket ditahan dulu untuk di teliti melainkan data hanya yang datang maupun keluar di-*capture header*-nya.



Gambar 3. Pengidentifikasian data paket

Paket yang datang selanjutnya akan diidentifikasikan apakah data tersebut merupakan data untuk ICMP, UDP atau data TCP. Setelah didapatkan rincian dari paket paket yang datang tersebut kemudian data dari paket-paket tersebut dimasukkan kedalam database. Tujuan pemasukkan ke dalam database adalah agar lebih memudahkan dalam pengolahan data tsecara keseluruhan dalam suatu kesatuan data. Data yang diolah bukan data yang ditampilkan saja tetapi semua data yang keluar dan masuk dari jaringan. Selain itu juga digunakan untuk mengurangi penggunaan dari besar data yang tersimpan. Karena semakin besar data yang harus diolah akan mengakibatkan kelambanan dari proses secara keseluruhan. Kemungkinan terburuk yang terjadi adalah program akan mengalami *overflow* atau *crash*.

3. HASIL

Aplikasi yang dihasilkan terdiri dari 3 (tiga) buah aplikasi yaitu :

1. *Tester* : berfungsi untuk melakukan testing terhadap aplikasi anti *flooding*. Fungsi *tester* ini untuk mengirimkan data-data ke jaringan yang nantinya akan dideteksi oleh aplikasi *anti flooding* yang selanjutnya dapat dikontrol apakah data yang dikirimkan akan diblokir atau dikirimkan.
2. Trojan : berfungsi sebagai *responder* dari aplikasi anti *flood* dan *tester* yang diinstalasi pada komputer jaringan.
3. Monitoring : merupakan program inti dari aplikasi anti *flooding*. Aplikasi ini digunakan untuk mencegah terjadinya pengiriman data yang tidak diperlukan di dalam jaringan.

3.1 Pembahasan

3.1.1 Batasan Implementasi

Batasan Implementasi yang dimaksud hanya sebatas pada tahap pembuatan perangkat lunak berdasarkan hasil rancangan pada bab sebelumnya. Pada tahap pembuatan, perangkat lunak ini, penulis mempergunakan bahasa pemograman *Microsoft Visual Basic 6.0*. Implementasi dibatasi pada jaringan komputer yang berbasis windows.

3.1.2 Batasan Pengujian

Dalam batasan pengujian ini, yang akan diuji dari sistem ini adalah :

1. Kemampuan sistem untuk mengklasifikasikan data-data yang ada
2. Kemampuan sistem untuk menyimpan data kedalam database
3. Kemampuan sistem untuk mendeteksi aliran data dalam jaringan.
4. Kemampuan sistem untuk melakukan *bloocking* pada data yang yang tidak diinginkan dalam jaringan yang akan menyebabkan penurunan kinerja jaringan.

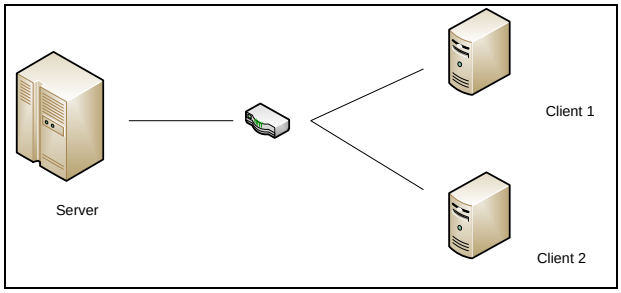
3.1.3 Teknik Pengujian

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 prototype LAN tersebut
4. Melakukan flooding ke host yang telah diberi sistem
5. Melihat hasil dari sistem apakah data *flood* dapat di blok atau tidak

3.1.4 Prototype Jaringan Internet

Dalam pengujian ini akan digunakan tolopologi jaringan star, akan dibangun suatu koneksi yang menunjukkan koneksi internet. Prototype tersebut adalah sebagai berikut. Akan diletakkan 1 buah *server* yang berfungsi sebagai *Server*. Dan 2 buah *client* pada *server* yang sudah diberi program tersebut. Bisa dilihat koneksi sebagai berikut:



Gambar 4. Prototype jaringan uji coba

Dalam hal ini *server* 1 adalah host, sedangkan kontrol adalah komputer tempat program penguji berada yang berada di *client* 1. Spesifikasi dari jaringan tersebut adalah sebagai berikut:

a. *Server*

Procesor : Pentium IV

Memory : 256 MB

b. Controler dan Attacker

Procesor : Laptop dengan processor setara Pentium IV

Memory : 1 GB

Disini diletakan control yang berfungsi sebagai client dan pengontrol, fungsi *client* untuk memberikan input dari dalam sehingga diketahui data berasal dari dalam. Sedangkan control merupakan tempat program diletakkan, peletakan program di *client* dimaksudkan untuk tidak mengganggu kerja *router*.

3.1.5 Konfigurasi sistem

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

1. Komputer *server*

Komputer ini berfungsi sebagai host yang kita miliki yang akan di gunakan sebagai korban dari *flooding* data. Komputer ini dirancang agar bisa melakukan pemblokiran IP kalau host 1 melakukan *flooding*. Di dalam komputer ini diletakkan 2 buah LAN card yang di gunakan sebagai routing data dari dalam dan data luar. Untuk itu komputer ini dilengkapi dengan aplikasi *operating sistem Windows XP*. Untuk pengesetan IP dilakukan sebagai berikut :

ETH 0 :

IP : 192.168.181.33

Netmask :255.255.255.0

Gateway : 192.168.1.181.1

2. Komputer pengontrol

Selain *windows XP* sebagai *operating system* juga diletakkan dua buah program. :

a. Program Daemon

Program ini berfungsi agar komputer ini dapat diperintah oleh komputer kontrol untuk melakukan pemblokiran IP apabila komputer kontrol mendapatkan *flooding* data.

b. Program Trojan

Program ini digunakan untuk membuka jalan bagi komputer *server* 1 agar dapat melakukan *flooding* TCP SYN.

3. Komputer pengontrol

Komputer yang sudah dilengkapi dengan program pengontrol atau sistem yang akan diuji, dengan menggunakan windows 98 sebagai *operating systemnya*. Pengesetan IP dilakukan sebagai berikut:

IP : 192.168.181.34

Netmask : 255.255.255.0

Gateway : 192.168.181.1

3.1.6 Pengujian Ketahanan Sistem Pada *Flooding* Data

Pada bagian ini akan diperlihatkan ketahanan sistem dengan melakukan pemberian sistem dengan paket data *flooding* melalui protokol UDP, TCP dan ICMP

a. Pengujian Dengan Protokol Icmp

Kondisi awal :

1. Panjang data maksimal = 100 byte
2. Frekuensi paket besar (lebih besar dari 100 byte) maksimal = 5 / 10 s
3. Frekuensi paket kecil (lebih kecil dari 100 byte) maksimal = 5 / 1 s

Tabel 1 Pengujian *Flooding* ICMP Paket Besar dan Paket Kecil

Paket besar		
Periode (ms)	**Besar paket (byte)**	**Pemblokiran**
1000	32768	Ya
500	32768	Ya
100	32768	Ya
50	32768	Ya
10	32768	Ya
1	32768	Ya
Paket kecil		
Periode (ms)	**Besar paket (byte)**	**Pemblokiran**
1000	1024	Tidak
500	1024	Tidak
100	1024	Ya
50	1024	Ya
10	1024	Ya
1	1024	Ya

Dengan melihat data yang ada diatas maka semua data-data yang melewati batas yang telah ditentukan atau melewati batas ketentuan *flooding* akan dilakukan blooking pada IP-nya. Sedang data paket yang tidak melewati ketentuan akan diteruskan, seperti yang terlihat pada pengujian di data paket kecil yang mempunyai periode 1000 dan 500 ms

b. Pengujian Dengan Protokol UDP

Kondisi awal :

1. Panjang data maksimal = 100 byte
2. Frekuensi paket besar (lebih besar dari 100 byte) maksimal = 5 / 10 s
3. Frekuensi paket kecil (lebih kecil dari 100 byte) maksimal = 5 / 1 s

Tabel 2 Pengujian *Flooding* UDP Untuk Paket Besar dan Paket Kecil

Paket besar		
Periode (ms)	**Besar paket (byte)**	**Pemblokiran**
1000	32768	Ya
500	32768	Ya
100	32768	Ya
50	32768	Ya
10	32768	Ya
1	32768	Ya
Paket kecil		
Periode (ms)	**Besar paket (byte)**	**Pemblokiran**
1000	1024	Tidak
500	1024	Tidak
100	1024	Ya
50	1024	Ya
10	1024	Ya
1	1024	Ya

Data-data UDP yang datang apabila melewati batas ketentuan akan di blok sedang yang tidak melwati akan diteruskan

c. Pengujian dengan protokol TCP

Kondisi awal :

1. Pengecekan setiap = 10 s
2. Banyak TCP SYN maksimal (dalam satu kali pengecekan) = 5 s
3. Port yang diperbolehkan : 8080, 3128, 80

Tabel 3 Pengujian *flooding* TCP

Pengiriman dalam *port* yang diperbolehkan		
Port	**PeriodeTCP SYN**	**Pemblokiran**
8080	2000	Tidak
8080	1000	Ya
8080	500	Ya
8080	100	Ya
8080	10	Ya
8080	1	Ya
Pengiriman dalam *port* yang tidak diperbolehkan		
Port	**PeriodeTCP SYN**	**Pemblokiran**
5000	2000	Ya
5000	1000	Ya
5000	500	Ya
5000	100	Ya
5000	10	Ya
5000	1	Ya

Pengiriman data TCP melalui *port* yang tidak di perbolehkan langsung di blok sedangkan apabila melalui *port* yang diperbolehkan maka dilakukan pemerikasaan apakah banyak TCP SYN yang datang melebihi ketentuan atau tidak. Jika ternyata banyak data paket datang melebihi ketentuan akan dilakukan pengeblokan IP.

4. SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka dapat diambil kesimpulan sebagai berikut :

1. Sistem yang dibangun dapat mendeteksi adanya peningkatan jumlah aliran data yang menyebabkan flooding dan menurunkan kinerja jaringan.
2. Sistem dapat mengklasifikasikan dan memisahkan jenis aliran data yang masuk, apakah data tersebut menyebabkan flooding atau tidak.
3. Sistem dapat melakukan *blocking data* apabila terjadi flooding.
4. Dengan adanya aplikasi ini maka keamanan jaringan lebih terjamin dan kinerja jaringan lebih optimal.

DAFTAR RUJUKAN

Al Bahra. (2006). *Rekayasa Perangkat Lunak*. Yogyakarta: Graha Ilmu.

Kristanto. (2003). *Jaringan Komputer*. Yogyakarta: Graha Ilmu.

Sugiyono. (2005). *Metode Penelitian Bisnis*. Bandung: CV Alfabeta.

Sukma Aji. (2008). *Jaringan Komputer*. Yogyakarta: Andi.

Syahrizal. (2005). *Pengantar Jaringan Komputer*. Yogyakarta: Andi.

Thomas. (2005). *Network Security First-Step*. Yogyakarta: Andi.

Utomo. (2011). *Membangun Jaringan Komputer dan Internet*. Yogyakarta: Mediakom.

Yung. (2002). *Membangun Database dengan Visual Basic 6.0 dan Perintah SQL*. Jakarta: PT. Elex Media Komputindo.