JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (print)
Vol. IV No. 2, Jun 2018, hlm. 165 – 170 ISSN 2550-0201 (online)
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

PERANCANGAN SISTEM PENCEGAHAN *FLOODING* PADA JARINGAN

Herman Saputra[1], & Nofriadi[2]
[1,2]Sistem Komputer, STMIK Royal Kisaran
***e-mail*:** royal_herman85@yahoo.com[1], nofriadi.royal85@yahoo.com[2]

Abstract: An attack into a computer network Server can happen anytime. Whether the administrator is working or not. Thus needed a defense system within the server itself that can analyze directly whether each incoming packet is expected data or unexpected data. If the package is an unexpected data, it is attempted that the computer can take action that is by blocking the IP origin of the package. Modeling a system used to overcome flooding data on a network. The system is designed by creating an active firewall that can define any data entered into the server, whether the data that came it is a data flood or data required by the user. Modeling is made using the Delphi programming language, and in ip address based computer network environments.

Keywords**:** *flooding, computer networking, ip blocking, data packets, tcp/ip*

Abstrak: Suatu serangan ke dalam Server jaringan computer dapat terjadi kapan saja. Baik pada saat administrator sedang kerja atupun 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 mendifinisikan setiap data yang masuk kedalam server, apakah data yang datang itu merupakan sebuah data flood atau data yang diperlukan oleh user. Pemodelan dibuat dengan menggunakan bahasa pemrograman Delphi, dan dalam lingkungan jaringan computer berbasis ip address.

Keyword: syaraf tiruan, *backpropagation*, peramalan, pariwisata

PENDAHULUAN

Sudah banyaknya perusahaan yang menggunakan internet 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 internet, tetapi juga perusahaan lain yang tidak bergerak di bidang tersebut. 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 perusa-

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (print)
Vol. IV No. 2, Jun 2018, hlm. 165 – 170 ISSN 2550-0201 (online)
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

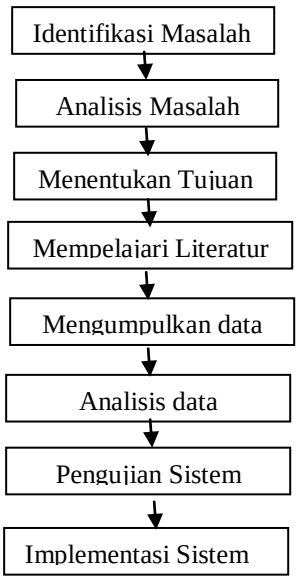
haan tersebut untuk melayani para nasabahnya, juga dalam bidang marketing suatu barang hasil industri suatu perusahaan. Kemudahan dan kepraktisan merupakan kunci dari mengapa dipilihnya internet ini.

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. 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.

METODOLOGI

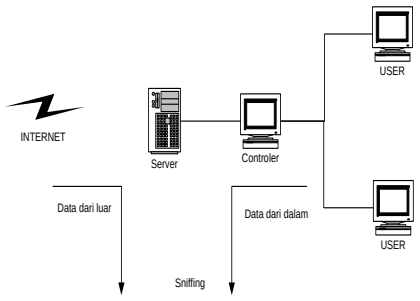
Kerangka kerja (*frame work*) yang digunakan di dalam penelitian.



Gambar 1. Kerangka Kerja

Desain Pengambilan Data

Dalam pengambilai data di windows 2000 kita perlu menempatkan sniffer untuk memperoleh header dari data itu. Seperti tertuang dalam gambar 2.



Gambar 2. Desain pengambilan Data

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (print)
Vol. IV No. 2, Jun 2018, hlm. 165 – 170 ISSN 2550-0201 (online)
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

HASIL DAN PEMBAHASAN

Pemrosesan data base ICMP dan UDP

Pada data yang menggunakan ICMP data yang ditampilkan adalah dengan cara sebagai berikut:

proses dilakukan adalah mengacu pada setiap periodik waktu yang ditentukan dalam variabel option yang telah ditetapkan sebelumnya. Apabila data paket datang memenuhi kriteria pertama data disimpan dalam database sedangkan bila tidak maka data dihapus langsung karena kriterianya tidak terpenuhi. Setelah waktu yang ditetapkan data kembali di lakukan cek apakah memenuhi kriteria kedua maka data langsung dimasukkan ke tabel list lain untuk diproses selanjutnya.

Pemrosesan database pada paket TCP

Berbeda dengan penanganan data base pada UDP ataupun ICMP, 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.

Pengolahan Data ICMP

Pengolahan data-data paket yang menggunakan ICMP, untuk mengan-tisipasi flood data yang disebabkan oleh paket yang menggunakan protokol ICMP. Dari bab sebelumnya diketahui bahwa kebanyakan flood yang disebabkan oleh paket yang menggunakan protokol ICMP adalah PING Flood. Pada kondisi normalnya penggunaan protokol ICMP untuk suatu kegiatan PING adalah paket dalam ukuran yang kecil, besar normalnya adalah 56 byte. Tentunya untuk kondisi suatu bandwith 128 kbps hal ini dapat diabaikan. Tetapi dalam kondisi lain hal ini sangatlah mengganggu, misalnya pada jam-jam sibuk. Akan mengakibatkan lambatnya alur keluar masuknya data. Dengan asumsi tersebut tentunya pengiriman paket ICMP dengan skala besar akan sangat lah mengganggu. Untuk itu diberi batasan bahwa paket ICMP yang masuk adalah kurang dari 100 byte. Sedangkan paket ICMP besar tidak diperbolehkan masuk, atau bisa dianggap sebagai flood ICMP. Begitu pula perlu juga dibatasi bahwa paket ICMP dari luar hanya diperbolehkan 5 buah paket dalam setiap detiknya

Pengolahan Data UDP

Seperti halnya protokol ICMP pengiriman paket melalui UDP juga merupakan jenis pengiriman paket berupa datagram. Yang pada skala normalnya juga merupakan paket data yang berukuran kecil. Penggunaan protokol ini pun juga termasuk jarang digunakan untuk hubungan antar host, mengingat sifatnya yang tidak baik keamanannya. Sehingga apabila ada hubungan UDP dengan kontinuitas yang tinggi atau besar paket UDP nya besar bisa dianggap sebagai suatu flooding.

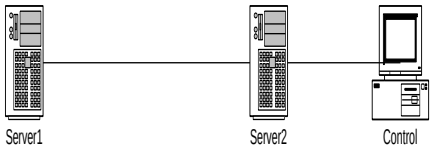
Desain Pemblokiran IP

Setelah data terbukti melakukan flooding pada jaringan maka sistem akan mengirimpkan paket UDP ke server untuk mengirimkan perintah blooking kepada IP yang besangkutan. Sebelumnya program daemon sudah diletakkan didalam server terlebih dahulu dan dijalankannya,untuk program daemon akan ditanyakan pakah paket UDP sama dengan nol,jika sama maka data akan ditujukan ketujuan-nya,sebaliknya jika tidak maka data akan diblok

Prototype Jaringan Internet

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. Bisa dilihat koneksi sebagai berikut:

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (print)
Vol. IV No. 2, Jun 2018, hlm. 165 – 170 ISSN 2550-0201 (online)
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi



Gambar 3. Prototype jaringan uji coba

Dalam hal ini server 2 adalah host kita, sedangkan kontrol adalah komputer tempat program penguji berada.

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.

Konfigurasi sistem

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

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. Didalam komputer ini diletakkan 2 buah LAN card yang di gunakan sebagai routing data dari dalam dan data luar. Untuk itu komputer ini dilengkapi dengan Windows 2000 server. Untuk pengesetan IP dilakukan sebagai berikut

ETH 0 :
IP : 192.168.0.1
Netmask :255.255.255.240
Gateway : 192.168.0.3

ETH 1 :
IP : 192.168.0.5
Netmask :255.255.255.0

Selain windows 2000 server 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.

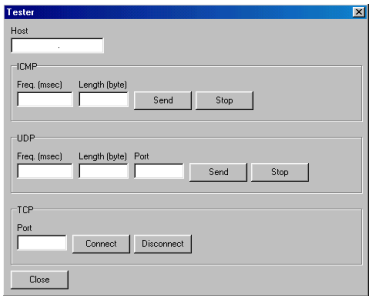
Komputer pengontrol

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 : 192.168.0.3
Netmask : 255.255.255.0
Gateway : 192.168.0.1

Program Penguji

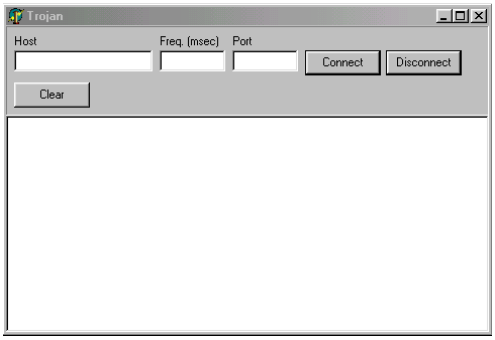
Untuk mengetahui program jalan atau tidak tentunya harus disimulasikan suatu kejadian yang mencerminkan keadaan yang sebenarnya. Untuk mendapatkan suatu flood yang disebabkan protokol dalam keadaan sebenarnya adalah susah dan jarang terjadi, sehingga dibuat suatu program yang digunakan mengirimkan paket-paket data melalui protokol TCP, UDP dan ICMP.

Pada program ini akan mengirimkan paket-paket secara kontinyu dan ukuran yang beraneka ragam sesuai yang diinginkan. Port yang digunakan juga bisa di tentukan sebelumnya, sehingga dapat menyerupai flood yang sebenarnya.



Gambar 4. Program Flood

JURTEKSI (Jurnal Teknologi dan Sistem Informasi) ISSN 2407-1811 (print)
Vol. IV No. 2, Jun 2018, hlm. 165 – 170 ISSN 2550-0201 (online)
Available online at http://jurnal.stmikroyal.ac.id/index.php/jurteksi

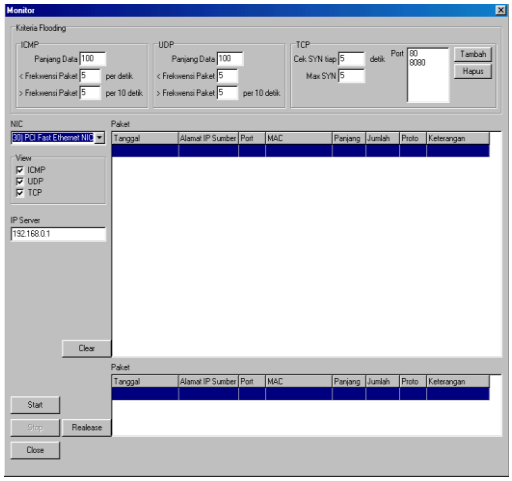


Gambar 5. Trojan TCP Flood

Hasil Pengujian

Program secara keseluruhan

Secara keseluruhan program dapat dilihat sebagai berikut:

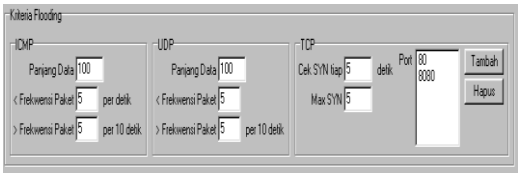


Gambar 6. Tampilan Program Keseluruhan

Didalam program tersebut sudah terdapat variabel-variabel yang perlu diisikan terlebih dahulu untuk mengatur bagaimana program itu bekerja. Variabel-variabel tersebut dibuat didasarkan atas dasar kita dapat menyesuaikan bandwith yang digunakan secara fleksibel. Tidak terbatas pada 128 kbps seperti batasan awal program ini dibuat, tetapi untuk default batasan dipakai dasar 128 kbps sebagai acuannya.

Option program

Sistem melalui option yang ada untuk mengatur apa saja yang merupakan batasan dari sistem. Option program yang harus diisikan untuk memudahkan pengaturan program. Bagian-bagian dari option program adalah:



Gambar 7. Option ICMP,UDP dan Tabel List Data Paket Datang

Kemampuan sistem dalam mengambil data

Sistem mempunyai kemampuan melihat semua paket yang datang dalam bentuk apapun. Meskipun demikian sistem hanya mengambil paket-paket dari tiga protokol utama yang biasa digunakan untuk mentransfer data. Protokol itu adalah TCP, UDP dan ICMP. Hal ini disebabkan karena flood yang biasa terjadi dalam jaringan dilakukan melalui tiga protokol tersebut. Sedangkan protokol lain hampir tidak pernah mengalami data flooding.

SIMPULAN

Berdasarkan proses dan hasil penelitian yang telah dilakukan, maka dapat diambil kesimpulan yang dapat berguna bagi para pembaca sehingga penelitian ini dapat lebih bermanfaat. Adapun kesimpulan dari penulisan penelitian ini adalah sebagai berikut:

1. Sistem dapat mendeteksi flooding data. Data yang keluar masuk akan dideteksi, sehingga semua data bisa dilihat apakah data itu merupakan flooding atau bukan, sehingga data bisa meng-klasifikasikan bahwa data tersebut benar-benar melakukan flooding atau tidak.
2. Sistem dapat bekerja meskipun di berikan flood yang besar. Karena pembatasan paket datang yang masuk

merupakan variabel yang bisa diubah besar kecilnya maka berapapun besar flood yang masuk dapat di deteksi dan diatasi, selain itu pengolahan data bukan semua data yang ada melainkan data-data yang sudah sangat terseleksi.

3. Sistem dapat bekerja meskipun tidak ada admin Karena sifat dari sistem yang otomatis keberadaan seorang admin untuk mengatur server apabila flood terjadi tidak diperlukan lagi. Sistem mampu mengatasi sendiri dengan melakukan pengambilan keputusan data masuk apakan flood atau tidak. Dan juga sekaligus melakukan tindakan akhir apabila flood benar-benar terjadi yaitu dengan melakukan blooking data.
4. Keamanan data lebih terjamin. Dengan adanya penanggulangan yang dini atas flooding data maka keamanan dari jaringan akan lebih terjamin baik dari segi kemanan alat maupun dari segi keamanan data

DAFTAR PUSTAKA

Microsoft TCP/IP, Drew Heywood, Pearson Education Pte. Ltd, 2001

Stalling, W. (2002). *Jaringan Komputer.*

Stalling, W. (2001). *Komunikasi Data dan Komputer.*

Amri, C. (2003). *Mengelola Mail Server* dengan Mdaemon.

CERT, http://www.cert.org/.

CERT Incident Note 99-04, http://www.cert.org/incident_notes/IN-99-04.html

Irawan, B. (2005). Jaringan Komputer.