JOEICT (Jurnal Of Education and Information Communication Technologi)
Volume 1, Nomor 1, Bulan 2017: 6 – 16

PENCEGAHAN FLOODING PADA JARINGAN KOMPUTER MENGGUNAKAN METODE BLOKIR IP DAN PORT, SNORT DAN WIRESHARK

Dini Nur Apriliani[1)], Mega Ayu Sasmita[2)], dan Aisyah Trisna Windari[3)]
[1, 2) 3)] Pendidikan Teknologi Informasi STKIP PGRI Tulungagung
Jalan Mayor Sujadi Nomer 07 Tulungagung
e-mail: dnurapriliani@gmail.com [1)], megaayusasmita@gmail.com [2)], aisyah.trisna10@gmail.com [3)]

ABSTRAK

Di jaman sekarang penggunaan internet sangatlah penting, tidak hanya dibidang telekomunikasi, internet pun sangat di butuhkan di perusahaan seperti di bidang perbankan, sebuah perusahaan harus menjaga keamanan servernya agar tidak di manfaatkan oleh orang yang tidak bertanggung jawab. Keamanan jaringan komputer sangatlah penting terlebih pada keamanan server, Karena serangan pada server bisa terjadi kapan saja dan dimana saja. Baik saat administrator sedang bekerja maupun tidak bekerja, maka dari itu dibutuhkan sistem keamanan pada server untuk melindungi serangan dari jaringan, Jenis serangan flooding maupun syn flooding. Untuk itu kami akan memaparkan perbedaan dari tiga cara pencegahan flooding data pada jaringan komputer yaitu yang pertama menggunakan metode blokir ip dan port, yang kedua menggunakan snort, dan yang ketiga menggunakan wireshark. Kami akan memaparkan perbedaan dari rancangannya dan pengujiannya.

Kata Kunci: Blokir IP, flooding data, snort dan wireshark.

ABSTRACT

In today's internet usage is important, not only in the field of telecommunications, the Internet was very in need in the company as in the fields of banking, a company must maintain the security of the server that is not utilized by people who are not responsible. Network security is important especially on the security server, because the attack on the server can happen anytime and anywhere. Whether administrators are working or not working, and therefore needed a security system on the server to protect from network attacks, and SYN flooding attack type flooding. Therefore, we will describe the differences of the three ways to prevent flooding of data on a computer network that is the first to use the method to block ip and port, which both use the snort, and the third uses wireshark. We will explain the differences from the design and testing.

***Keywords**: Block IP, flooding the data, snort, and wireshark.*

I. PENDAHULUAN

Saat ini banyak perusahaan yang telah memanfaatkan teknologi internet sebagai sarana komunikasi data untuk melaksanakan rutinitas harian perusahaan dalam oprasional perusahaan. 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 di 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. 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 dengan internet sering kali mendapatkan gangguan baik data yang dimiliki maupun peralatannya. Kerugian yang diderita akan hal ini bisa dibilang tidak kecil. Dalam faktor keamanan ini biasanya perusahaan menempatkan administrator untuk menjaga. Dari hasil penelitian sebelumnya network administrator dituntut dapat menjaga sistem yang dibangun dari serangan hacker atau seorang client yang

ingin merusak sistem. Otentikasi user merupakan menu yang harus ada untuk memberikan hak akses pada client [1].

Dalam faktor keamanan ini biasanya perusahaan mendapatkan administrator untuk bekerja. Tetapi fungsi administrator tentunya akan terbatas waktunya, pada saat jam kerja. Meskipun di jam kerja pun kadang kala karena terlalu banyaknya aliran data yang diterima oleh server adalah data yang di harapakan atau data yang tidak diharapkan. Sedangkan suatu serangan ke system keamanan yang bisa terjadi kapan saja. Baik pada saat administrator sedang bekerja ataupun tengah malam dimana tidak ada yang menjaga server tersebut. Dengan demikian dibutuhkan system pertahanan didalam server itu sendiri yang bisa menganalisa langsung apakah setiap paket yang masuk tersebut adalah data yang diharapkan atupun data yang tidak diharapakan. 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 mengantisipasi langsung,sehingga kerugian bisa mendekati nol atau tidak ada sama sekali [2].

Keamanan jaringan komputer merupakan hal yang sangat penting dalam priotitas keberadaannya. Dalam hal ini keamanan jaringan komputer dibagi menjadi 2 bagian yaitu keamanan secara fisik (hardware) dan keamanan secara non-fisik(software). Gangguan tersebut dapat berupa gangguan dari dalam (internal) ataupun gangguan dari luar (eksternal). Gangguan internal merupakan gangguan yang berasal dari lingkup dalam jaringan infrastruktur tersebut. Dalam hal ini adalah gangguan dari pihak-pihak yang telah mengetahui kondisi keamanan dan kelemahan jaringan tersebut. Gangguan eksternal adalah gangguan yang memang berasal dari pihak luar yang ingin mencoba atau dengan sengaja ingin menembus keamanan yang telah ada. Gangguan eksternal biasanya lebih sering terjadi pada jaringan eksternal, seperti web server, telnet, FTP, SSH server.

Pada dasarnya pengamanan jaringan dibagi menjadi dua jenis yaitu rule based dan adaptive system. Sistem rule based mendeteksi suatu serangan berdasarkan aturan- aturan yang sudah di definisikan pada kumpulan data aturan sedangkan adaptive-system dapat mengenali jenis serangan baru dengan cara membandingkan kondisi saat ini dengan kondisi normal suatu sistem [3].

II. LANDASAN TEORI

1. Blokir IP

   Pemblokiran IP tersebut disesuaikan dengan operating system yang ada di router, apakah Windows 2000, linuk ataukah FreeBSD :

   a. WINDOWS 2000

      Di dalam windows 2000 server telah dilengkapi dengan cara untuk mengatur IP baik itu mengeblok IP maupun melewatkan suatu IP. Program tersebut adalah IPSECPOL. Utility ini hampir sama kegunaannya pada iptables dan ipchains dalam program LINUX. Hanya saja untuk utility ini hanya bekerja pada windows 2000 server.

      Pengaturan IPSECPOL pada tampilan windows dapat dijumpai pada "IP Security Policies on Local Machine" yang berada pada "Computer Configuration *Security Settings*" di MMC *(Microsoft Management Console).* Yang pada defaultnya terdapat 3 ketentuan yang telah ditetapkan, yaitu :

      1) Client (Respond Only)

         Digunakan oleh client untuk memberikan respon kepada *windows 2000 server* pada saat ada permintaan menggunakan servis yang ada didalamnya.

      2) Secure Server (Require Security)

         Ketentuan ini digunakan pada *windows 2000 server* dan *windows 2000 host* yang menghasilkan *networkbased services* untuk meyakin kan bawa tidak ada *non-authentication* dan *non-encryption traffic* yang di abaikan.

3) Server (Request Security)
Ketentuan ini hampir sama dengan ketentuan yang ada pada *Secure Server*, yang menjadi perbedaan adalah pada ketentuan ini terdapat ketentuan untuk mengadakan hubungan enkripsi pada tingkat lebih tinggi di *user*.

b. Linux
Untuk sistem pemblokiran dengan menggunakan operating system ini dengan menggunakan aplikasi yang sudah tersedia yaitu dengan menggunakan IPTABLES atau IPCHAINS tergantung versi yang digunakan. Pada aplikasi ini tersedia berbagai fungsi tentang *routing* baik *forwarding*, *accepting* ataupun *bloking*.

c. FreeBSD
FreeBSD juga mempunyai aplikasi untuk pengaturan routing yang fungsinya mirip dengan IPTABLES pada linux ataupun IPSECPOL pada windows, hanya saja pada sistem FreeBSD untuk pengaturannya menggunakan perintah IPFW [1].

2. Flooding data

a. Data
Data merupakan kumpulan huruf atau angka yangbelum diolah sehingga tidak memiliki arti, atau bisa juga disebut sebagai catatan atas kumpulan fakta. Data merupakan bentuk jamak dari *datum*, berasal dari bahasa latin yang berarti "sesuatu yang diberikan". Dalam penggunaan seharihari data berarti suatu peryataan yang diterima secara apa adanya. Pernyataan ini adalah hasil pengukuran atau pengamatan suatu variable yang bentuknya dapat berupa angka, kata-kata citra. Dalam fakta yang dikumpulkan untuk menjadi data. Data kemudian diolah sehingga dapat diaturkan secara jelas dan tepat sehingga dapat dimengerti oleh orng lain yang tidak langsung mengalaminya sendiri, hal ini dinamakan *deskripsi*. Pemillihan banyak data sesuai dengan persamaan atau perbedaan yang dikandungnya dinamakan klasifikasi.

b. Flooding
Pengiraman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna disebut dengan *Flood Data,* adakalanya data-data yang berbedah dalam *traffic* merupakan data yang tidak perlu. Data-data tersebut memang sengaja dikirim oleh seseorang meneruskan jaringan data yang ada. Pengiriman data tersebut dapat mengakibatkan lambatnya jalur *traffic* yang ada dalam jaringan dan juga bias mengakibatkan kerugian lain yang cukup berarti, misalnya kerusakan *program* karena adanya *intruder* yang masuk kedalam jaringan. *Traffic* data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Pada jam-jam sibuk *traffic* suatu data akan sangat padat, sehingga *traffic* data tersebut akan terganggu. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan kelambatan dalam pengiriman dan penerimaan data [2].
Traffic data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Pada jamjam sibuk traffic suatu data akan sangat padat, sehingga traffic data tersebut akan terganggu. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan kelambatan dalam pengiriman dan penerimaan data. Macam-macam Flood attack :

a. Ping of death
Pengiriman paket *echo request* ICMP ke dalam suatu jaringan secara berlebihan. Pengiriman paket ini dapat mengakibatkan sistem crash, hang ataupun *reboot*

b. Smurf Attack
Hampir sama dengan *Ping of death* tetapi untuk *smurf attack* paket ICMP tidak dikirim secara langsung ke korban, melainkan melalui perantara. Pada awalnya dikirim sebuah paket ICMP *echo request* ke sebuah *host* lain, paket ini bertujuan agar host tersebut mengirimkan paket ICMP PING secara terus menerus ke korban terakhirnya.

c. *Syn Flooding*
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 tujuan akan terus menunggu paket tersebut dengan menyimpannya kedalam *backlog*. Meskipun besar paket kecil, tetapi apabila pengiriman SYN tersebut terus menerus akan memperbesar *backlog*. Hal yang terjadi apabila backlog sudah besar akan mengakibatkan host tujuan akan otomatis menolak semua paket SYN yang datang, sehingga host tersebut tidak bisa dikoneksi oleh host-host yang lain.

d. *UDP flood*
Pengiriman data UDP secara berlebihan kedalam suatu jaringan, pengiriman UDP *flood* ini akan membentuk suatu jalur hubungan dengan suatu *servis* UDP dari *host* tujuan. Flood UDP ini akan mengirimkan karakter-karakter yang akan mengetes jaringan korban. Sehingga terjadi aliran data yang tidak perlu dalam jaringan korban tersebut [1].

3. Snort
Snort merupakan suatu perangakat lunak untuk menditeksi penyusup dan mampu menganalisa paket yang melintas jaringan secara *real time traffic* dan *logging* ke dalam *database* serta mampu mendeteksi berbagai serangan yang berasal dari dalam jaringan maupun diluar jaringan. www.Snort.org [2].

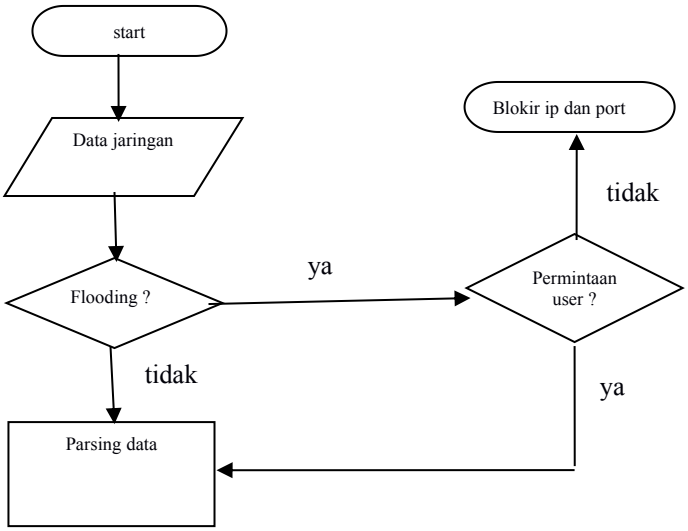
4. Wireshark
Wireshark banyak digunakan dalam memecahkan *troubleshooting* dijaringan untuk memeriksa keamanan jaringan, men-debug implementasi protocol jaringan dalam software mereka, melakukan *debugging* implementasi paket protocol, serta belajar. protocol dan banyak juga digunakan untuk sniffer atau mengendus data-data privasi dijaringan. Wireshark ini diibaratkan sebagai media atau tool yang dapat dipakai oleh user untuk penggunaanya, apakah untuk kebaikan atau kejahatan. Hal ini karena wireshark dapat digunakan untuk mencari informasi yang sensitif yang berkeliaran pada jaringan, contoh nya kata sandi, cookie dan lain sebagainnya. Wireshark dapat menganalisis paket data secara real time. Artinya aplikasi wireshark ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah di tentukan oleh user sebelumnya. Wireshark dapat menganalisa paket data secara real time artinya, aplikasi wireshark akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya. Jika Komputer terhubung dengan jaringan kecepatan tinggi dan pada computer sedang digunakan aplikasi berbasis jaringan, aplikasi wireshark akan menampilakan banyak sekali paket data dan menimbulkan kebingungan karena ada begitu banyak paket data jaringan yang muncul. Aplikasi wireshark dapat memfilter jenis protocol tertentu yang ingin ditampilkan [3].

III. PERANCANGAN SISTEM

Dalam bab ini kami akan memaparkan tentang perancangan sistem pada keamanan jariangan computer untuk pencegahan flooding data dari tiga jurnal yg telah kami review. Dalam jurnal pertama membahas metode blokir ip dan port bersisi tetang perancangan sistem secara umum, rancangan pengambilan data, rancangan pengidentifikasian data dan rancangan pemblokiran ip. Pada jurnal ke dua tentang pencegahan flooding data mennggunakan snort berisi tentang perancangan diagram alir sistem dan perancangan desain pengambilan data. Sedangkan jurnal ke tiga tentang pencegahan aktivitas illegal menggunakan wireshark berisi perancangan sistem jaringan untuk aktifitas illegal.

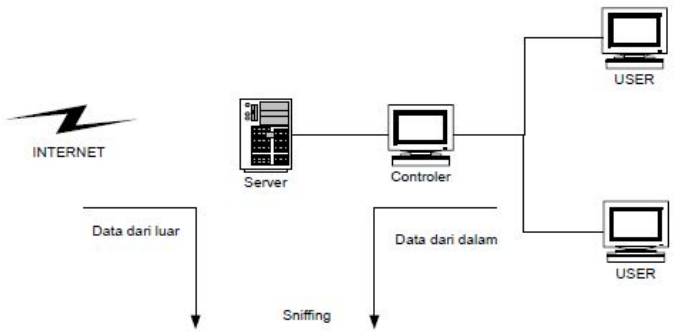
A. PERANCANGAN SISTEM MENGGUNAKAN METODE BLOKIR IP DAN PORT

1. Rancangan sistem secara umum



Gambar 1. Design umum program blokir otomatis pada flood

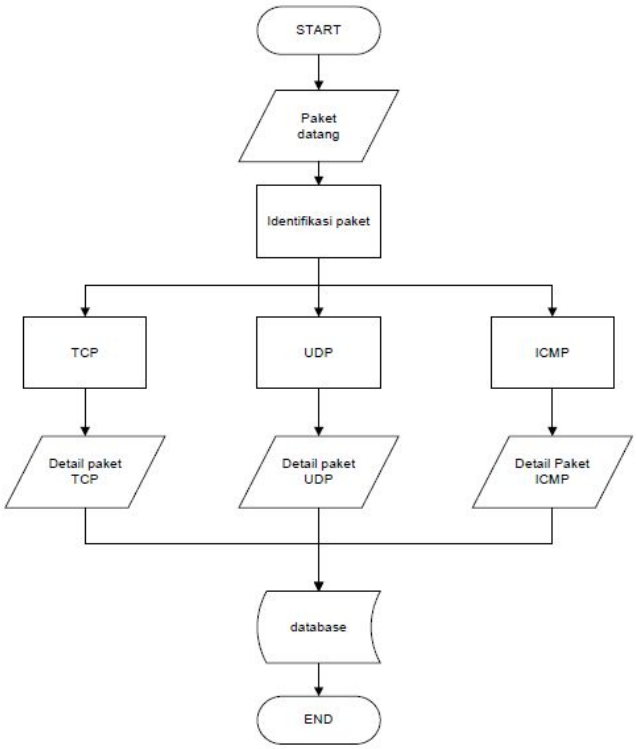
2. Rancangan Pengambilan Data



Gambar 2. Proses pengambilan data

Dari gambar 2 proses pengambilan data dapat dijelaskan setiap data yang masuk ataupun keluar akan di belokan terlebih dahulu untuk diambil data headernya sebelum dilanjutkan ketujuan sebenarnya.

3. Rancangan Pengidentifikasian Data



Gambar 3. Proses pengidentifikasian data

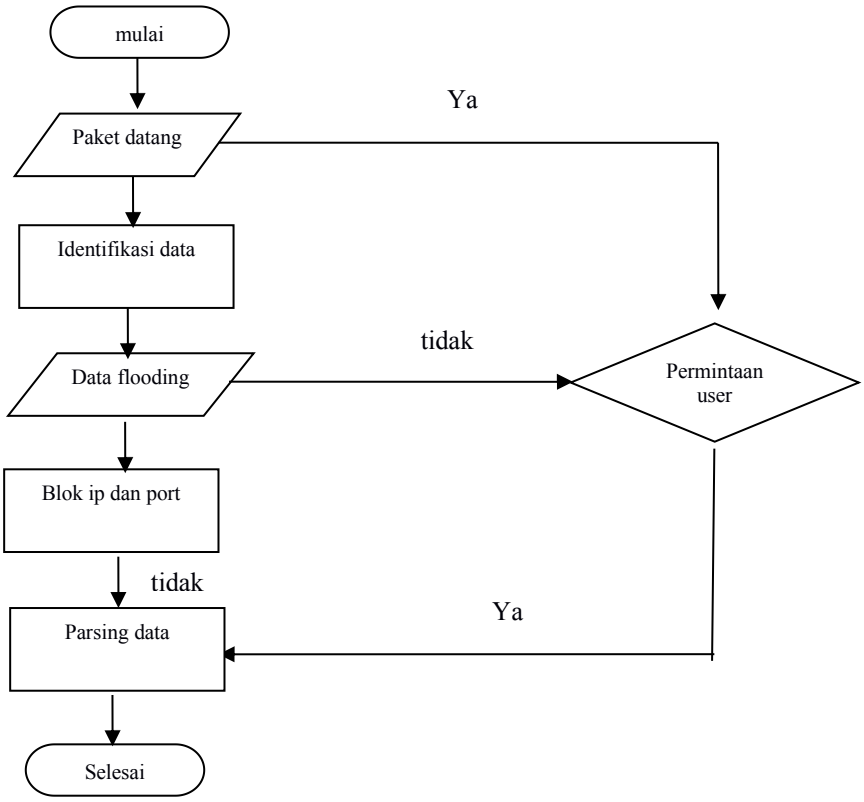
Dari gambar 3 proses pengidentifikasian data dengan mengetahui header dari setiap paket yang masuk maka dapat mengetahui data dari paketnya, kemudian bisa mengklasifikasikan setiap data tersebut apakah paket TCP, UDP, atau ICMP.

4. Pemblokiran IP

Dan yg terakhir adalah membuat rancangan pemblokiran ip dimana jika data terbukti melakukan flooding data maka sistem akam mengirimkan paket UDP ke server untuk mengirimkan perintah bloking kepada ip yg bersangkutan. Kemudian program daemon ditanyakan apakah paket UDP sama dengan nol, jika sama maka data akan di tujukan ketujuannya, jika tidak maka data akan ditolak.

B. PERANCANGAN SISTEM MENGGUNAKAN SNORT

1. Rancangan Diagram alir



Gambar 4. Proses diagram alir

Seperti halnya pada perancangan sebelumnya, dalam perancangan sistem menggunakan snort hal yang pertama dilakukan juga mebuat rancangan diagram alir data atau flowchart. Dimana alurnya adalah data jaringan yang masuk akan diproses apakah data tersebut melakukan flooding, jika data yang masuk adalah flooding maka computer akan menyelidiki apakah permintaan user atau tidak. Jika tidak maka akan secara otomatis akan memblok ip dan port dari mana dia berasal, tetapi jika tidak maka akan ditujukan kepada tujuannya.

2. Rancangan desain pengambilan data

Kemudian dilanjutkan dengan rancangan design pengambilan data, dalam perancangan sistem menggunakan snort proses pengambilan data pada BASE (Basic Analysis and Security Engine) membaca log yang ditulis pada snort secara otomatis kemudian BASE akan menampilkannya sebagai alarm dan list log dengan antar muka yang mudah dipahami dan dapat dilihat oleh administrator. Dengan proses yang sama seperti jurnal sebelumnya yaitu data yang masuk maupun keluar akan dibelokan terlebih dahulu untuk di capture headernya yang tertera pada gambar 2.

C. PERANCANGAN SISTEM MENGGUNAKAN WIRESHARK

Berbeda dengan perancangan dalam jurnal sebelumnya, dalam perancangan sistem menggunakan wireshark lebih merujuk pada aktifitas illegal. Seperti yg telah dijelaskan dalam jurnal, user diberikan hak akses berupa proses upload maka pada sistem yang akan dibangun menggunakan pembatas harddisk dengan menggunakan disk quota, jadi user tidak bisa melakukan upload secara sembarang karena telah dibatasi quota untuk melakuakan proses upload. Proses yang dilakukan tersebut diawasi oleh wireshark agar *user* dapat dengan aman meng-*upload* data tanpa perlu mengkawatirkan ada yang menyusupi pada saat melakukan *upload* data

tersebut. Untuk melakukan *capture packet* sesuai dengan keinginan dari *user* dimana setelah memilih salah satu *interface* yang akan dipantau aktivitas jaringan secara *online*[3].

IV. PENGUJIAN SISTEM

Pada bab ini akan dibahas hasil pengujian dari tiga jurnal yang telah kami review sebelumnya. Ketiga jurnal berisi tentang pencegahan flooding data pada keamanan jaringan komputer. Pada jurnal pertama membahas tentang pengujian sistem, pengujian ketahanan sistem pada flooding data, pengujian dengan protocol UDP dan pengujian dengan protocol TCP. Sedangkan pada jurnal kedua membahas tentang proses pengujian SYN flooding attack dan pengujiang ping of death. Dan pada jurnal ketiga membahas tentang hasil pengujian menggunakan wireshark.

A. PENGUJIAN SISTEM MENGGUNAKAN METODE BLOKIR IP DAN PORT

1. Pengujian sistem
   Sistem yang dibangun 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 proses pengiriman data [1]

2. Pengujian ketahanan sistem pada flooding data

   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 lecil dari 100 byte)
         Maksimal = 5/1 s

   Tabel 1 dan 2 pengujian flooding ICMP paket besar dan paket Kecil

Tabel 1. Paket besar

Periode (ms)	Besar paket (byte)	pemblokiran
1000	2500	Ya
500	2500	Ya
100	2500	Ya
50	2500	Ya
10	2500	Ya
1	2500	Ya

Tabel 2. Peket kecil

Periode (ms)	Besar paket (byte)	pemblokiran
1000	80	Tidak
500	80	Tidak
100	80	Ya
50	80	Ya
10	80	Ya
1	80	Ya

Pengujian pertama merupakan pengujian ketahanan sistem pada flooding data menggunakan protocol ICMP dengan aturan 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.

   b. Pengujjian 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 lecil dari 100 byte)
   Maksimal = 5/1 s

Tabel 3 dan 4 pengujian flooding ICMP paket besar dan paket Kecil

Tabel 3. Paket besar

Periode (ms)	Besar paket (byte)	pemblokiran
1000	2500	Ya
500	2500	Ya
100	2500	Ya
50	2500	Ya
10	2500	Ya
1	2500	Ya

Tabel 4. Peket kecil

Periode (ms)	Besar paket (byte)	pemblokiran
1000	80	Tidak
500	80	Tidak
100	80	Ya
50	80	Ya
10	80	Ya
1	80	Ya

Pengujian kedua menggunakan protocol UDP, dengan aturan Data-data UDP yang datang apabila melewati batas ketentuan akan di blok sedang yang tidak melwati akan diteruskan.

c. Pengujian menggunakan TCP
   Kondisi awal :
   1. pengecekan setiap = 10 s
   2. banyak TCP SYN maksimal (dalam satu kali pengecekan) = 5 s

Port yang diperbolehkan :8080,3128,80

Tabel 5 dan 6 pengujian flooding TCP

Tabel 5. Pengiriman dalam port yg diperbolehkan

port	Periode TCP SYN	pemblokiran
8080	2000	Ya
8080	1000	Ya
8080	500	Ya
8080	100	Ya
8080	10	Ya
8080	1	Ya

Tabel 6. Pengiriman dalam port yang tidak diperbolehkan

port	Periode TCP SYN	pemblokiran
5000	2000	Ya
5000	1000	Ya
5000	500	Ya
5000	100	Ya
5000	10	Ya
5000	1	Ya

Pengujian ketiga menggunakan protokol TCP, Pengiriman data TCP melalui port yang tidak diperbolehkan 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.

B. PENGUJIAN SISTEM MENGGUNAKAN SNORT

1. Pengujian SYN Flooding Attack
   Pada pengujian pertama yaitu pengujian SYN floofing attack. *Syn Attack* terjadi bila suatu *host* hanya mengirimkan paket *SYN TCP* saja secara kontinyu tanpa mengirimkan paket *ACK* sebagai konfirmasinya. Hal ini akan menyebabkan *host* tujuan akan terus menunggu paket tersebut dengan menyimpan keadalam *baclog.* Meskipun ukuran paket kecil, tetapi apapbila pengiriman *SYN t*erus menerus akan memperbesar

backlog. Hal ini terjadi apabila *backlog* sudah besar akan mengakibatkan host tujuan akan otomatis menolak semua paket *SYN* yang datang, sehingga host tersebut tidak akan otomatis menolak semua paket *SYN* yang datang, sehingga host tersebut tidak bisa koneksi oleh *host-host* yang lain.

Pengujian dilakukan dengan menggunakan perintah cmd dengan IP client 192.168.1.15 dengan target ke IP korban 192.168.1.10. contoh serangan paket ke target. Ping 192.168.1.10 –l 10000 –n 10000 –t. Serangan ini melibatkan satu komputer / koneksi internet untuk (membanjiri) sebuah server dengan paket ICMP/TCP/UDP,tujuan dari serangan ini adalah untuk membuat bandwith server menjadi overload, sehingga server tidak bisa lagi menangani trafik yang masuk dan server akhirnya down, seperti gambar 5.

Gambar 5. Contoh serangan menggunakan SYN Flooding Attack

2. Pengujian Ping of Death

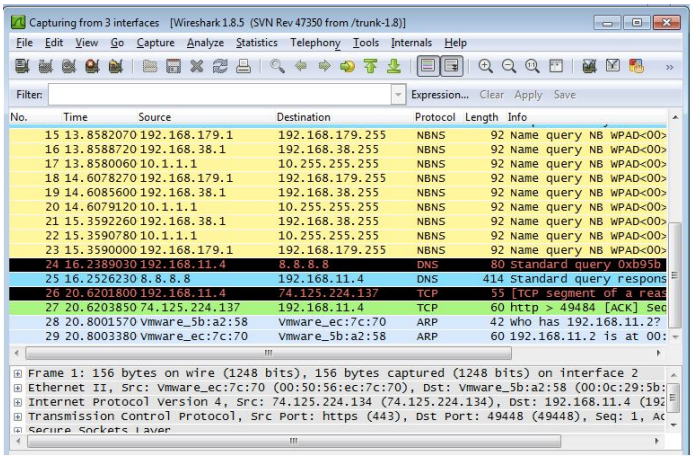
Sedangkan pada pengujian kedua yaitu pengujian *Ping Of Death* merupakan pengiriman paket echo request ICMP ke dalam suatu jaringan secara berlebihan. Pengiriman paket ini dapat mengakibatkan sistem *crash,hang* ataupun *reboot.*

Pengujian simulasi Ping of Death dilakukan dengan melakukan ping yang ada menyertakan paket data sebesar 10000 byte terhadap komputer server dari komputer client atau si penyerang. Sebuah ping berukuran 64 byte, perintah yang diberikan pada terminal adalah ping 192.168.1.10 –l 10000 –n 10000 -t, seperti gambar 6.

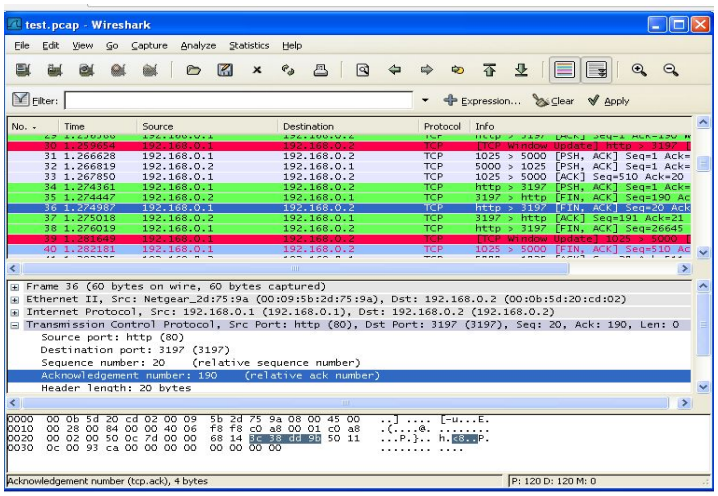
Gambar 6. Contoh serangan menggunakan Ping of Death

C. PENGUJIAN SISTEM MENGGUNAKAN WIRESHARK

Dalam pengujian ini memaparkan hasil pengujian yaitu pengujian aktivitas yang berhasil di-*ca pture* oleh wireshark terhadap informasi sumber, tujuan *protocol* dan waktu *capture*-nya. Wireshark mampu melihat atau menganalisis paket secara online maupun offline sesuai dengan keinginan user dimana setelah memilih interface yang akan di pantau aktifitasnya.



Gambar 7. Capture paket secara online



Gambar 8. Capture paket secara offline

V. KESIMPULAN

Berdasarkan data yang didapat mengenai pencegahan penyerangan flooding dapat disimpulkan bahwa perancangan sistem menggunakan metode blokir ip dan port dan perancangan sistem menggunakan snort hal yang pertama dilakukan yaitu membuat rancangan diagram alir data atau flowchart. Dengan proses yang sama yaitu data yang masuk maupun keluar akan dibelokan terlebih dahulu untuk di capture headernya. Sedangkan perancangan sistem menggunakan wireshark lebih merujuk pada aktifitas illegal.

DAFTAR PUSTAKA

[1] B. Triandi, "Sistem Keamanan Jaringan Dalam Mencegah Flooding Data Dengan Metode Bloking Ip Dan Port," *Semin. Nas. Teknol. Inf. dan Multimed.*, pp. 6–8, 2015.

[2] A. Suhadak, "Sistem Pencegahan Flooding Data pada Jaringan Komputer," *Tugas Akhir Jur. Tek. Elektro - Fak. Tek. UM*, 2010.

[3] T. M. Diansyah, J. T. Informatika, S. Tinggi, and T. Harapan, "Analisa pencegahan aktivitas ilegal didalam jaringan menggunakan wireshark," *Anal. Pencegah. Akt. Ilegal Di Dalam Jar. Menggunakan wireshark*, vol. IV, no. 2, pp. 20–23, 2015.