Analisis Kelakuan *Denial-of-Service attack* (DoS *attack*) pada Jaringan Komputer dengan Pendekatan pada Level Sekuritas

S.Nurwenda[1], B.Irawan[1], Irzaman[2]
[1]Jurusan Teknik informatika, FT, Jl. Dipati Ukur Bandung
[2]Jurusan Fisika, FMIPA IPB, Jl. Raya Pajajaran Bogor

Abstract
Denial of Service (DoS) attack is a serious threat for computer network such as Local Area Network(LAN), and internet. DoS attack can consume memory, CPU, and network resources and damage or shutdown the operation of the resource under attack (victim). A common DoS attack floods a network with bogus traffic so that legitimate users may not be able to communicate.
Key code : computer networks, network security , Denial of Service (DoS) attack

Abstrak
Denial of Service (DoS) attack adalah ancaman yang serius untuk jaringan komputer seperti Lokal Area network (LAN), dan internet. *DoS attack* dapat mengkonsumsi memory, CPU, dan sumber daya jaringan, dan dapat menyebabkan kerusakan atau *shutdown* terhadap sumber daya operasi yang berada di dalam serangan (korban). Secara umum serangan DoS adalah membanjiri suatu jaringan dengan lalu lintas palsu sedemikian sehingga para pemakai sah tidak mungkin mampu untuk berkomunikasi.
Kata kunci : jaringan komputer, keamanan jaringan, , *Denial of Service (DoS) attack*

1. Pendahuluan

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data bergerak melalui kabel-kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan perangkat keras atau perangkat lunak yang terhubung dengan jaringan[1].Sumber daya jaringan yang sangat berharga antara lain komputer, database dan layanan-layanan lain yang disediakan oleh jasa jaringan. Jaringan ini sangat dibutuhkan oleh user dikarenakan layanan-layanan tersebut memudahkan pekerjaan sehingga pekerjaan tersebut lebih efisien. Bila layanan ini rusak atau tidak dapat bekerja, maka akan menyebabkan hilangnya produktifitas[2].

Terhubungnya LAN atau komputer ke internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mekanisme keamanan secara fisik. Hal ini tentunya menarik minat para *hacker* (pembobol) dan *intruder* (penyusup) untuk terus bereksperimen guna menemukan dan mempergunakan setiap kelemahan yang ada dari konfigurasi sistem informasi yang telah ditetapkan. Salah satu serangan ini dikenal dengan *Denial of Service attack* (DoS attack) [3].

Denial of Service merupakan serangan dengan ditandai oleh suatu usaha yang eksplisit dari penyerang untuk mencegah para pemakai yang sah menggunakan jasa pelayanan jaringan. Serangan *Denial of Service* utamanya bertujuan melumpuhkan komputer atau jaringan [2]. Ada beberapa motif penyerang dalam melakukan *Denial of Service* yaitu: status sub-kultural, untuk mendapatkan akses, balas dendam, alasan politik, dan alasan ekonomi [4].

Tujuan dari penelitian ini adalah untuk mempelajari dan menganalisis serangan *Denial of Service* untuk mendapatkan solusi terbaik dalam menaggulangi serangan *DoS* ini.

2. Metodologi

Dalam pelaksanaannya, penelitian dilakukan di Jurusan Teknik Informatika UNIKOM, terhitung mulai Maret 2004 sampai dengan Juni 2004.

Metode yang digunakan dalam penelitian ini adalah dengan metode deskriptif kualitatif melalui studi pustaka dan dokumenter dari berbagai buku dan literature yang berhubungan dengan objek penelitian yang di hadapi. Alat dan bahan yang digunakan dalam penelitian antara lain : seperangkat komputer Amd Athlon Xp 1,2 Ghz, memori 128 MB, dan VGA 64 MB, serta perangkat lunak menggunakan sistem operasi Windows XP dan Macromedia *Flash* 5.

3. Hasil dan Pembahasan

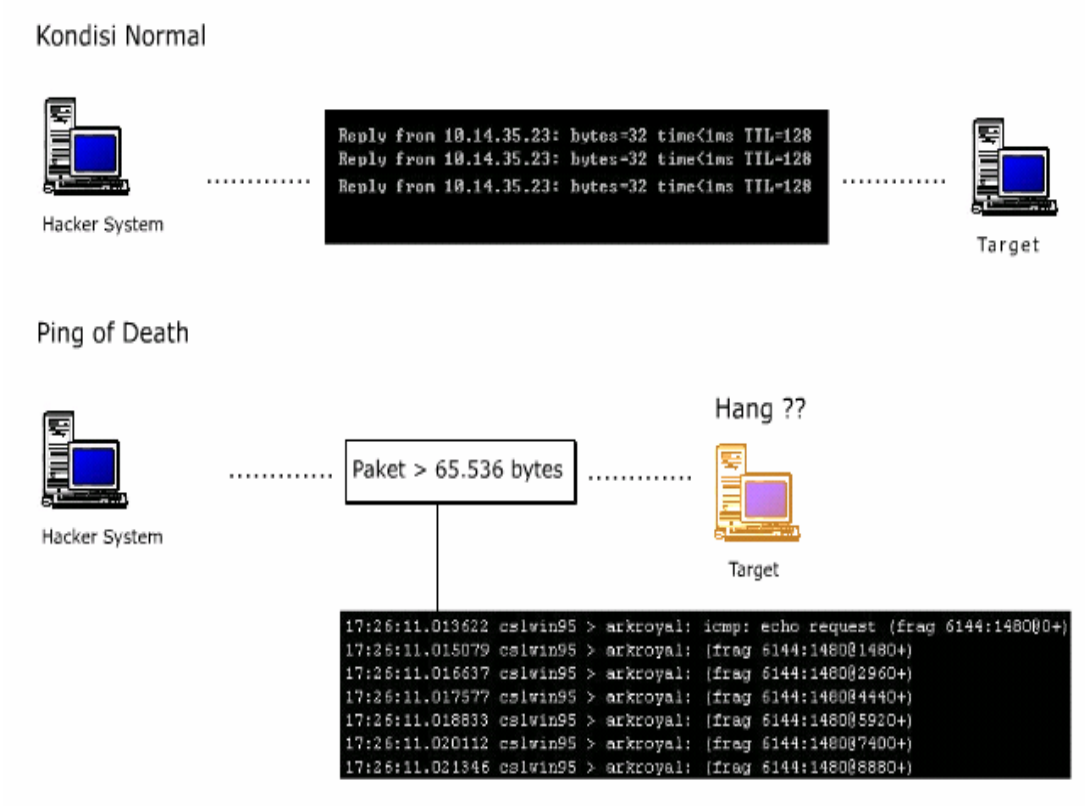
Denial of Service adalah aktifitas menghambat kerja sebuah layanan (servis) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut.[4]

Tujuan serangan seperti ini berakibat server korban jadi kewalahan melayani *request* yang terkirim dan berakhir dengan menghentikan aktivitas atau berhenti dengan sendirinya karena tak mampu melayani *request*. Kadang serangan yang dilakukan dengan cara ini dapat merusak atau mematikan sistem secara keseluruhan.[2] Sistem yang diserang dapat menjadi “bengong” (*hang*, *crash*), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi)[3].

Beberapa tipe serangan *Denial of Service Attack antara lain : Ping of Death, SYN Attack, Land Attack, Smurf Attack, dan UDP Flood*.[5]

1. *Ping of Death* [3,5]

Pada kondisi normal program utility ping digunakan untuk men-cek beberapa waktu yang dibutuhkan untuk mengirimkan sejumlah data dari suatu komputer ke komputer lain, dimana panjang maksimum paket data yang dapat dikirimkan menurut spesifikasi protokol IP adalah 65.536 byte. Gambar 1. menunjukkan program utility ping dan alur serangan *Ping of Death.* Pada *Ping of Death* data yang dikirim melebihi maksimum paket yang di ijinkan menurut spesifikasi protokol IP. *Ping of Death* mengeksploitasi kelemahan didalam *reassembly* kembali fragmen paket IP. Ketika data dikirimkan ke jaringan, paket IP sering berubah menjadi potongan paket yang lebih kecil. *Ping of Death* akan memanipulasi *offset* potongan data sehingga akhirnya terjadi *overlapping* antara paket yang diterima di bagian penerima setelah potongan-potongan paket ini di *reassembly*.

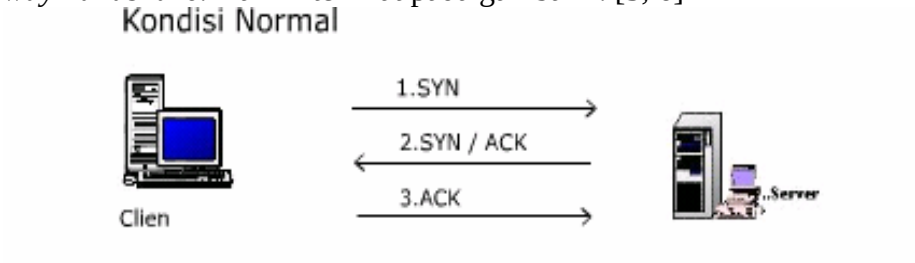


Gambar 1. Skema program utility ping dan serangan *Ping of Death* [5]

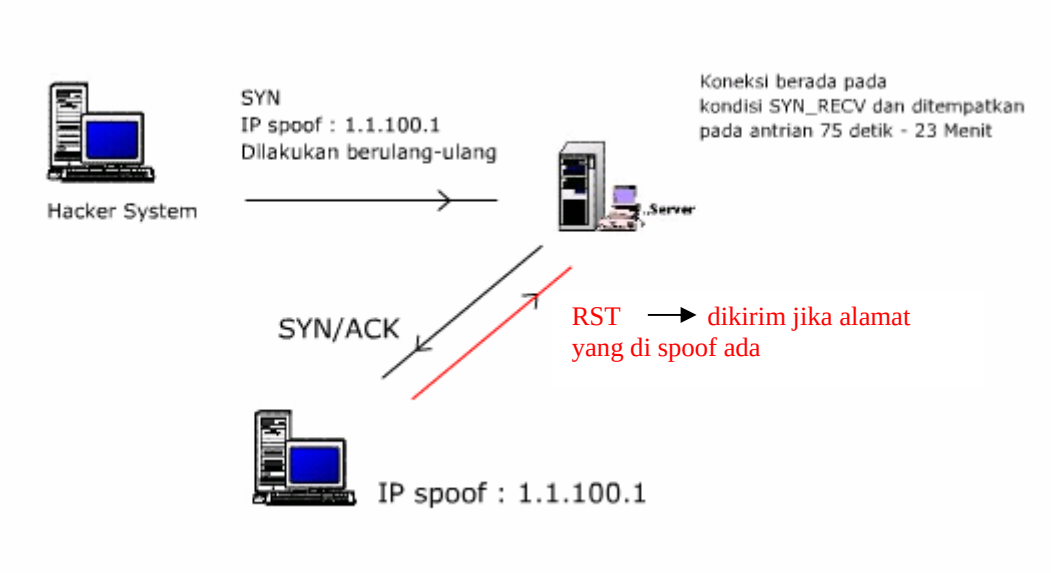
Konsekuensinya, pada sistem yang tidak siap akan menyebabkan sistem tersebut crash (tewas), hang (bengong) atau reboot (booting ulang) pada saat sistem tersebut menerima paket yang demikian panjang

2. *SYN Attack*

Pada kondisi normal, aplikasi klien akan mengirimkan paket TCP SYN untuk mensinkronisasi paket pada aplikasi di server (penerima). Server (penerima) akan mengirimkan respond acknowledgement berupa paket TCP SYN ACK. Setelah paket TCP SYN ACK di terima dengan baik oleh klien (pengirim), maka klien (pengirim) akan mengirimkan paket ACK sebagai tanda transaksi pengiriman / penerimaan data akan di mulai. Proses ini disebut juga dengan *three-way handshake*. Hal ini terlihat pada gambar 2. [5, 6]



Gambar 2. skema koneksi TCP *three-way handshake.* [6]

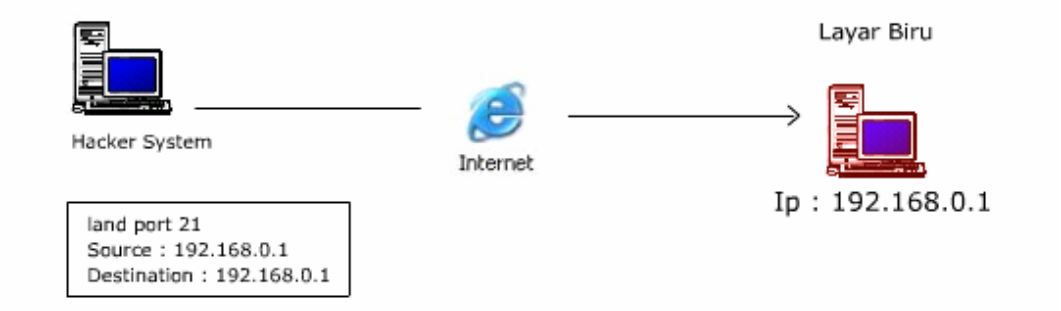


Gambar 3. Skema serangan *SYN* [7]

Dalam serangan *SYN flood* (banjir paket SYN) seperti terlihat pada gambar 3. Hacker mengirimkan paket SYN yang source addressnya telah dispoof menjadi suatu address yang tidak ada dan dikirimkan ke Server. Server membalas dengan mengirimkan SYN/ACK ke alamat palsu (spoof), dan port yang digunakan berada pada kondisi SYN_RECV. Jika seandainya alamat Spoff (palsu) tersebut ada (terdapat system/komputer) maka akan membalas dengan paket RST karena merasa tidak memulai koneksi.[6]. Karena alamat palsu tersebut tidak ada maka koneksi yang telah dialokasikan pada port server tersebut akan berada pada keaadaan menunggu (75 detik – 23 menit). Dengan cara ini, server akan tampak seperti bengong dan tidak memproses responds dalam waktu yang lama.[6]

3. *LAND attack*[3,5]

Dalam *LAND attack*, Hacker menyerang server yang dituju dengan mengirimkan paket TCP SYN palsu yang seolah-olah berasal dari server yang dituju. Dengan kata lain, *Source* dan *Destination address* dari paket dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung. Apabila serangan diarahkan kepada sistem Windows 95, maka sistem yang tidak diproteksi akan menjadi hang (dan bisa keluar layar biru). Hal ini terlihat pada gambar 4.



Gambar 4. Skema serangan *LAND*[7]

4. *Smurf Attack*[3,5,6]

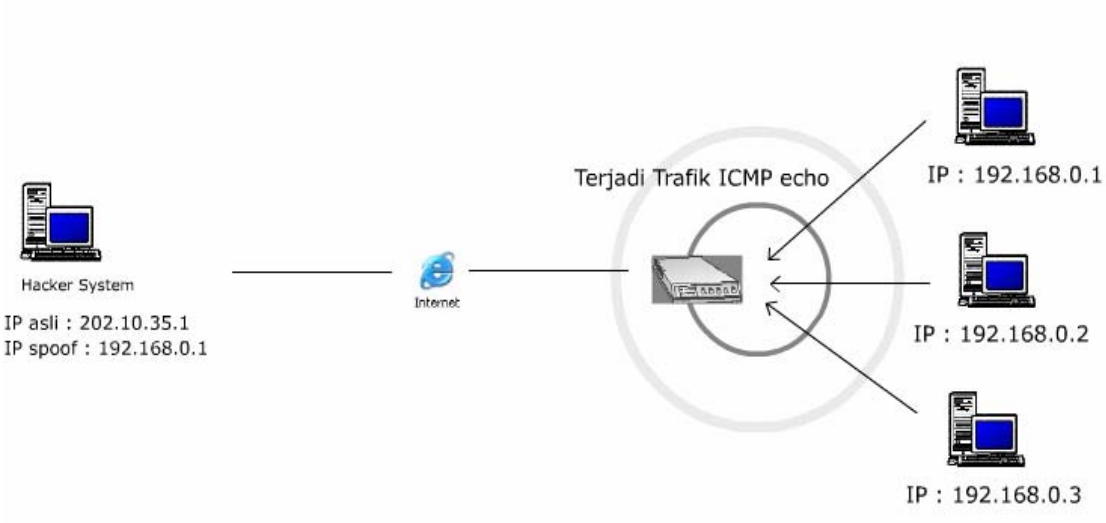
Pada *Smurf attack,* hacker membanjiri router dengan paket permintaan echo Internet Control Message Protocol (ICMP) yang di kenal sebagai aplikasi ping. Karena alamat IP tujuan pada paket yang dikirim adalah alamat broadcast dari jaringan, maka router akan mengirimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Kalau ada banyak host di jaringan, maka akan terjadi trafik ICMP echo respons & permintaan dalam jumlah yang sangat besar.

Pada gambar 5 si hacker ini memilih untuk men-spoof alamat IP sumber permintaan ICMP tersebut, Dengan menggunakan *IP spoofing*, respon dari *ping* tadi dialamatkan ke komputer yang IPnya di*spoof*. Akibatnya komputer tersebut akan menerima banyak paket. Akibatnya terjadi ICMP trafik yang tidak hanya akan memacetkan jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di spoof.

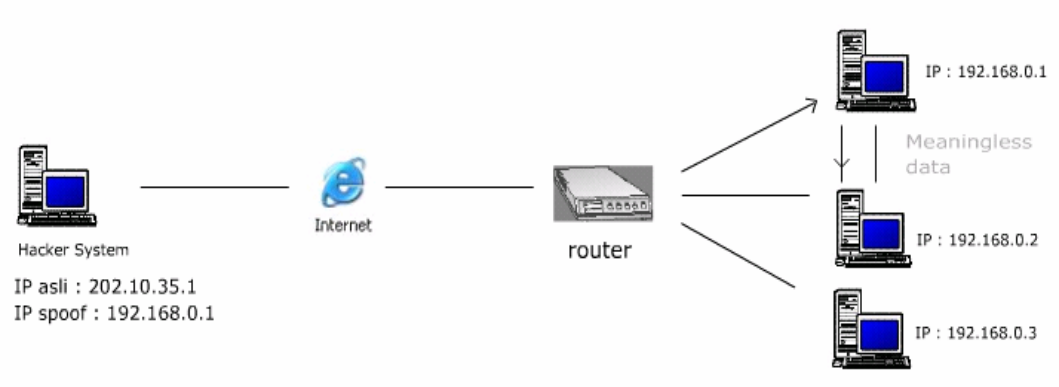
5. *UDP Attack*[5]

Pada *UDP attack* dengan cara spoofing, User Datagram Protocol (UDP) *flood attack* akan menempel pada servis UDP chargen di salah satu mesin, yang akan mengirimkan sekelompok karakter ke mesin lain, yang di program untuk meng-echo setiap kiriman karakter yang di terima melalui servis chargen. Hal ini ditunjukkan oleh gambar 6 dimana *UDP Flood* ini pada dasarnya mengkaitkan dua (2) sistem tanpa disadarinya. Karena paket UDP tersebut di spoofing antara ke dua mesin tersebut, maka yang terjadi adalah banjir tanpa henti kiriman karakter yang tidak berguna antara ke dua mesin tersebut.

Perbandingan Serangan *Denial of Service* dapat dilihat pada tabel 1.



Gambar 5. Skema serangan *Smurf Attack*[7]



Gambar 6. Skema serangan UDP[5]

Tabel 1. Perbandingan Serangan *Denial of Service*

No	Jenis Serangan	Efek Serangan	Penanggulangan
1.	*Ping of Death.*	- *Crash* - *Hang* - *Reboot*	- memblok ping yang telah di fragmen - mempatch sistem operasi
2.	*SYN Attack.*	- *Hang* - Tidak memproses respon dalam waktu lama	- Mempatch Sistem Operasi - Meningkatkan ukuran antrian koneksi (antrian SYN ACK). - Menurunkan waktu tunggu untuk melakukan *three-way handshake*.
3.	*Land Attack.*	- *Hang* - Layar biru (windows 95) - CPU load 100% (windows NT)	- Mempatch sistem operasi - Memfilter pada software firewall dari semua paket yang masuk dari alamat IP yang diketahui tidak baik.
4.	*Smurf Attack.*	- Terjadi trafik ICMP echo respons & permintaan dalam jumlah yang sangat besar.	- Broadcast Address di router harus dimatikan. - Memfilter permohonan ICMP echo atau menolak ping ke alamat Broadcast pada firewall
5.	*UDP Attack*	- terjadi banjir tanpa henti kiriman karakter yang tidak berguna antara ke dua mesin tersebut	- Men-disable semua servis UDP di semua mesin di jaringan - Memfilter pada firewall semua servis UDP yang masuk. Karena UDP dirancang untuk diagnostik internal, maka masih aman jika menolak semua paket UDP dari Internet.

4. Kesimpulan

Denial of Service (DoS) attack merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan layanannya (*denial of service*) atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapatbermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi "bengong" (*hang*, *crash*), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).

Serangan denial of service berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan DoS tidak ada yang dicuri. Akan tetapi, serangan DoS dapat mengakibatkan kerugian finansial.

DAFTAR PUSTAKA

[1] Yuhefizar, *Tutorial Komputer dan Jaringan,* ilmukomputer.com, hal. 9 (2003).

[2] B. Sadono, *Tinjauan Tentang Buffer Overflow dan denial of Service Attack*, ITB Bandung, Bandung, hal. 15 – 16 (2003).

[3] B. Rahardjo, *Keamanan Sistem Informasi Berbasis Internet,* Pt. Insan Infonesia, Bandung, hal. 89 – 92 (2002).

[4] H. Sammir, *Serangan Denial of service,* infokomputer.com, hal. 1 – 2 (2003).

[5] O.W. Purbo, *Ensiklopedia Serangan Denial of Service Attack*, infokomputer.com, hal. 1 – 3 (2003).

[6] S. Mclure, J. Scambray, G. Kurtz, *Hacking Exposed*, McGraw-Hill, Osborne, hal. 504 – 525 (2001).

[7] Arif, *Eksploitasi Keamanan,* Presentasi Telkom Training Center, Bandung, (2002).