ANALISIS EXPLOTASI KEAMANAN WEB DENIAL OF SERVICE ATTACK

Junita Juwita Siregar

Computer Science Department, School of Computer Science, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
juwita_siregar@binus.ac.id

ABSTRACT

Internet network which is public and global is unsafe, so the security of public Internet-based information system needs to be considered. When a data is sent from one computer to another on the Internet, it will pass through a number of other computers that are meant to give the user an opportunity to take over one or several computers. denial of service attacks is one of the web security systems which can inhibit the activity of the work of a service even turn it off, so the authorized user cannot use the service. There is an attempt of certain parties to prevent a user access to a system or network by flooding the traffic network with so much data from unregistered users. It makes the user unable to log into the network system. The purpose of this paper is to analyze the cause of the denial of service attack on a web system using literature study. The result of this research is a method to overcome denial of service attack as well as the prevention techniques. This study concludes that securing techniques should be implemented extra carefully on DoS attacks (Denial-of-Service Attacks). Therefore, the attacker cannot overwhelm the network IP address and disrupt communication between a server and its client that may reject user's request access to a system or a network service provided by a host.

Keywords: *server, denial of service, attack, internet, network*

ABSTRAK

Jaringan internet yang bersifat publik dan global pada dasarnya tidak aman, sehingga keamanan sistem informasi berbasis Internet perlu diperhatikan. Pada saat data terkirim dari suatu komputer ke komputer yang lain di dalam Internet, data itu akan melewati sejumlah komputer lain yang berarti akan memberi kesempatan pada user tersebut untuk mengambil alih satu atau beberapa komputer. denial of service adalah salah satu serangan pada sistem keamanan web yang dapat menghambat aktivitas kerja sebuah layanan (service) atau mematikannya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Latar Belakang paper ini adalah adanya usaha dari pihak tertentu untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Tujuan dari penulisan paper ini adalah untuk menganalisis penyebab terjadinya serangan denial of service pada suatu sistem web. Metode penelitian yang digunakan adalah metode Literatur studi pustaka. Hasil dari penelitian ini adalah metode mengatasi dan teknik pencegahan searangan denial of service attack. Kesimpulan paper ini adalah diperlukan suatu tehnik pengamanan yang ekstra hati-hati pada serangan DoS (Denial-of-Service Attacks). Hal ini bertujuan agar penyerang tidak dapat membanjiri IP address jaringan dan mengganggu komunikasi antara sebuah server dan kliennya, sehingga akses request seorang pengguna terhadap sistem atau sebuah layanan jaringan yang disediakan oleh sebuah host tidak ditolak.

Kata kunci: *server, denial of service, attack, internet, jaringan*

PENDAHULUAN

Internet adalah rangkaian atau jaringan sejumlah komputer yang saling berhubungan. Internet berasal dari kata *interconnected-networking*. Internet merupakan jaringan global yang menghubungkan suatu jaringan (*network*) dengan jaringan lainnya di seluruh dunia (Tittel (2005).

Meningkatnya ancaman keamanan suatu web disebabkan ketidaktahuan akan kelemahan dari suatu apalikasi web dan penyebabnya.

World wide web (*WWW*) atau dipersingkat menjadi *web*, adalah sebuah sistem di mana informasi dalam bentuk teks, gambar dan suara dipresentasikan dalam bentuk hypertext dan dapat diakses oleh perangkat lunak yang disebut browser. Informasi di web pada umumnya ditulis dalam format HTML (Sugianto, 2003). Protokol standar yang digunakan dalam mengakses dokumen HTML adalah HTTP. HTTP (*Hypertext Transfer Protocol*) adalah protokol yang menentukan aturan yang perlu diikuti oleh web browser dan web server (Wardhana dan Makodian, 2010).

Salah satu *exploitas*i kelemahan aplikasi web adalah *denial of service* (DoS). Menurut Herlambang (2010), denial of service adalah aktifitas menghambat kerja sebuah layanan *(service*) atau mematikan-nya, sehingga user yang berhak/berkepentingan tidak dapat menggunakan layanan tersebut. Pada dasarnya denial of service merupakan serangan yang sulit di atasi. Hal ini disebabkan oleh resiko layanan publik di mana admin akan berada pada kondisi yang membingungkan antara layanan dan kenyamanan terhadap keamanan.

Serangan *denial of service* telah dikenal untuk komunitas jaringan sejak awal 1980. Dampak akhir dari aktifitas ini mengakibatkan tehambatnya aktifitas korban yang dapat berakibat sangat fatal (dalam kasus tertentu). Target serangan *DoS attack* bisa ditujukan ke berbagai bagian jaringan. Bisa ke *routing devices, web, electronic mail*, atau server *Domain Name System.* Serangan ini bertujuan membuat server *shutdown, reboot, crash,* atau"*not responding*". Server adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan computer (Oetomo, 2003).

Serangan ini menghasilkan kerusakan yang sifatnya persisten artinya kondisi denial of service akan tetap terjadi walaupun *attacker* sudah berhenti menyerang, dan server baru normal kembali setelah di-*restart /reboot.*

Pada dasarnya denial of service merupakan serangan yang sulit di atasi, hal ini disebabkan oleh resiko layanan publik di mana admin akan berada pada kondisi yang membingungkan antara layanan dan kenyamanan terhadap keamanan. Seperti yang kita tahu, kenyamanan berbanding terbalik dengan keamanan. Maka dari itu, resiko yang mungkin timbul selalu mengikuti hukum ini.

Berdasarkan permasalahan keamanan jaringan di atas, studi ini bertujuan untuk mengetahui lebih banyak lagi tentang sistem atau metode yang digunakan dalam penyerangan denial of service, dampak-dampak yang ditimbulkan DoS dan pengamanan yang perlu dilakukan untuk mencegah terjadinyan denial of service *Attack*. Selain itu untuk mengetahui apakah serangan denial of service pada suatu sistem jaringan menimbulkan kerugian sistem pada suatu web server?

Beberapa penelitian terdahulu telah membahas masalah denial of service *Attack* ini seperti *Analysis of a* denial of service *Attack on TCP* , denial of service *Attack Techniques: Analysis, Implementation and Comparison* dan lain sebagainya. Berdasarkan penjelasan permasalahan keamanan Jaringan Web di atas penulis tertarik untuk membahas Analisis Exploitasi Keamanan Web denial of service *Attack*. Dalam studi ini penulis membahas celah lubang keamanan jaringan web yang berpotensi mendapat serangan denial of service *Attack.*

METODE

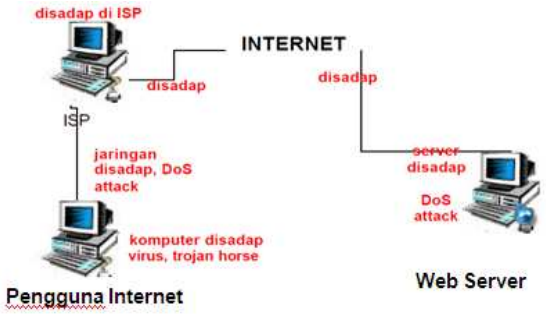
Analisis exploitasi keamanan web denial of service *attack* ini menggunakan metodologi sebagai berikut: (1) penelitian lapangan (*field research*) –mengumpulkan data-data yang berhubungan dengan denial of service *Attack* dari permasalahan yang terjadi pada sebuah web; (2) penelitian kepustakaan (*library research*) – mengumpulkan berbagai informasi yang berhubungan dengan teknik denial of service *Attack* dan pencegahannya dari buku-buku dan jurnal.

HASIL DAN PEMBAHASAN

Denial-of-Service attack adalah serangan yang dilakukan oleh *hacker* untuk melumpuhkan suatu sistem jaringan web dengan membanjiri server dengan jumlah lalu lintas data yang tinggi, atau melakukan *request data* ke sebuah server sehingga server tidak lagi dapat memberikan layanan dan menjadi *crash.*

Cara Kerja Serangan Denial of Service

Denial of service merupakan serangan yang dibuat oleh *hacker* yang mengirimkan *request* dalam jumlah yang sangat besar dan dalam waktu yang bersamaan, sehingga server menjadi kelebihan beban dan tidak bisa melayani user lainnya. Secara umum hubungan antara pengguna Internet sebuah website (Web Server) dapat dilihat pada Gambar 1 di bawah ini:



Gambar 1 Vulnerability keamanan sistem jaringan

Pengguna terhubung ke Internet melalui layanan *Internet Service Provider* (ISP), baik dengan menggunakan modem DSL, modem kabel, *wireless*, maupun dengan menggunakan *leased line.* ISP atau penyelenggara jasa internet (PJI) adalah sebuah perusahaan atau sebuah organisasi yang menyediakan jasa layanan koneksi akses internet untuk perseorangan, perkantoran, kampus, sekolah, dan lain-lain (Sukamaaji dan Rianto, 2008). ISP ini kemudian terhubung ke Internet melalui *network provider* (atau *upstream*). Di sisi Web Server, terjadi hal yang serupa. Server Internet terhubung ke Internet melalui ISP atau *network provider* lainnya. Gambar 1 tersebut juga menunjukkan beberapa potensi lubang keamanan (*security hole*).

Teknik Melakukan Serangan Denial of Service

Melakukan DoS sebenarnya bukanlah hal yang sulit. Beberapa caranya adalah sebagai berikut: (1) mematikan server yaitu *one shot*, *one kill* untuk membuat server menjadi *crash*, *hang, reboot*; (2) menyibukkan server dengan mengirim banyak sekali *request*. Bisa dengan tanpa bug/*vulnerability,*

mengexploitasi bug/ vulnerability, yaitu mengirim banyak specially crafted *request*, atau normal *request*, yaitu mengirim banyak *request* normal seperti pengguna biasa.

Tipe - Tipe Serangan Denial of Service

SYN Flooding

SYN Flooding merupakan network denial of service yang memanfaatkan *loophole* pada saat koneksi TCP/IP terbentuk. Kernel Linux terbaru (2.0.30 dan yang lebih baru) telah mempunyai opsi konfigurasi untuk mencegah denial of service dengan mencegah menolak cracker untuk mengakses sistem. Pada kasus ini, terjadilah pengiriman permintaan buka koneksi TCP pada FTP, Website, maupun banyak layanan lainnya. SYN Packet sendiri telah di modifikasi oleh si penyerang, di mana SYN-ACK (Atau *reply* dari pada SYN Packet) dari server akan tertuju kepada komputer atau mesin yang tidak akan pernah membalas.

Pentium FOOF Bug

Ini adalah serangan denial of service terhadap prosessor Pentium yang menyebabkan sistem menjadi *reboot*. Hal ini tidak bergantung terhadap jenis sistem operasi yang digunakan tetapi lebih spesifik lagi terhadap prosessor yang digunakan yaitu pentium.

Ping Flooding

Ping Flooding adalah *brute force* denial of service sederhana. Jika serangan dilakukan oleh penyerang dengan bandwidth yang lebih baik dari korban, maka mesin korban tidak dapat mengirimkan paket data ke dalam jaringan (*network*). Hal ini terjadi karena mesin korban di banjiri (*flood*) oleh peket-paket ICMP.

Saat server yang tidak terproteksi menerima paket melebihi batas ukuran yang telah ditentukan dalam protokol IP, server tersebut biasanya *crash*, *hang*, atau melakukan *reboot* sehingga layanan menjadi terganggu Paket serangan *Ping flooding* dapat dengan mudah direkayasa sehingga tidak bisa diketahui asal sesungguhnya dari mana, dan penyerang hanya perlu mengetahui alamat IP dari komputer yang ingin diserangnya.

Apache Benchmark

Program-program Benchmark WWW, digunakan untuk mengukur kinerja (kekuatan) suatu web server. Namun tidak tertutup kemungkinan untuk melakukan penyalahgunaan.

Menggantung Socket

Penyerang hanya melakukan koneksi lalu diam, pada saat itu apache akan menunggu selama waktu yang ditetukan direktif *Time Ou*t (default 5 menit). Dengan mengirimkan *request* simultan yang cukup banyak penyerang akan memaksa batasan maksimal MaxClients. Dampak yang terjadi, klien yang mengakses apache akan tertunda. Selain itu, apabila backlog TCP terlampaui, akan terjadi penolakan, seolah-olah server korban tewas.

Serangan Input Flooding

Remote Buffer Overflow menghasilkan *segmentation fault* (seg_fault) dapat terjadi secara remote jika demon atau server tidak melakukan verifikasi input sehingga input membanjiri *buffer* dan menyebabkan program dihentikan secara paksa.

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, sistem yang tidak diproteksi akan menjadi *hang* (dan bisa keluar layar biru).

Serangan Smurf

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

Tear Drop

TearDrop mengirimkan paket *Fragmented IP* ke komputer (Windows) yang terhubung ke jaringan (*network*). Serangan ini memanfaatkan *overlapping* ip fragment, bug yang terdapat pada Windowx 9x dan NT. Dampak yang timbul dari serangan ini adalah *blue screen of death.*

Tool Denial of Service Attack

Denial of service dapat secara otomatis memanfaatkan komputer yang terinfeksi, komputer ini disebut zombie dalam jargon. Zombie adalah sistem-sistem yang telah disusupi oleh program DDoS *Trojan* untuk melancarkan serangan DDoS terhadap sebuah host di jaringan.

Berikut adalah beberapa tools yang dapat digunakan untuk melakukan denial of service *Attack.* Pertama adalah KOD (*kiss of death*) untuk menyerang Ms.Windows pada port 139 (*port netbios-ssn*). Fungsi utama dari tool ini adalah membuat *hang/blue screen of death* pada komputer korban. Kedua adalah *bonk/boink*. *Bong* merupakan dasar dari teardrop (teardrop.c). *Boink* merupakan perbaikan dari bonk.c yang dapat membuat crash mesin MS. Windows 9x dan NT. Ketiga adalah jolt. Cara kerja jolt yaitu mengirimkan serangkaian *spoofed and fragmented* ICMP *packet* yang tinggi sekali kepada korban. Keempat adalah NetCat. Netcat adalah suatu utilitas kecil dengan kemampuan besar. Netcat tesedia untuk sistem operasi Windows maupun Linux. Pada sistem operasi Windows, paling baik dijalankan pada Windows NT, walaupun pada Windows 95/98/ME maupun XP, dapat juga.Netcat bertindak sebagai utilitas inetd yang ganas, yang mampu menjalankan remote command (seperti mengaktifkan shell command line) dengan cara membentuk koneksi TCP atau UDP ke suatu *listening port*. Terakhir adalah NesTea. Tool ini dapat membekukan Linux dengan Versi kernel2.0. ke bawah dan Windows versi awal. Versi perbaikan dari NesTea dikenal dengan NesTea2.

Dampak Serangan Denial of Service

Salah satu dampaknya adalah menghabiskan *resources*. Pada dasarnya, untuk melumpuhkan sebuah layanan dibutuhkan pemakaian *resource* yang besar, sehingga komputer/mesin yang diserang kehabisan *resource* dan menjadi *hang*. Beberapa jenis *resource* yang dihabiskan di antaranya: (1) bandwidth; (2) kernel tables – serangan pada kernel tables bisa berakibat sangat buruk pada sistem. Alokasi memori kepada kernel juga merupakan target serangan yang sensitif. Kernel memiliki kernel *map limit*. Jika sistem mencapai posisi ini, sistem tidak bisa lagi mengalokasikan *memory* untuk kernel dan sistem harus *reboot*; (3) RAM – serangan denial of service banyak menghabiskan RAM sehingga

sistem harus di-*reboot*; (4) disk – serangan klasik banyak dilakukan dengan memenuhi Disk. Penyerang dapat juga mencoba untuk menggunakan *disk space* dengan cara-cara lain,seperti dengan sengaja membuat *error* yang mengharuskan *log* dan menempatkan *file* dalam area atau jaringan FTP tanpa nama (anonymous), untuk informasi konfigurasi yang sesuai untuk FTP tanpa nama *cache*; (5) INETD – sekali saja *INETD crash*, semua *service* (layanan) yang melalui INETD tidak akan bekerja. Konfigurasi informasi akan rusak atau berubah.

Metode Pencegahan Denial of Service Attack

Dalam menghadapi sebagian besar bahaya di Internet khususnya denial of service, disarankan melakukan beberapa hal berikut ini: (1) menutup *services* atau protokol-protokol yang dianggap tidak perlu melalui firewall. Firewall menganalisis paket data dan mempelajari komputer yang dituju oleh paket data, Protokol yang digunakan dan Isi paket data; (2) menggunakan firewall, yang dapat memblokir paket data dari alamat-alamat tertentu, memblokir pemakaian protokol tertentu, dan menolak paket data dengan kata-kata tertentu di dalamnya; (3) menonaktifkan IP *directed broadcast* untuk *subnetwork* dalam domain guna mencegah serangan ini; (4) mengaktifkan pengelolaan kuota ruangan penyimpanan bagi semua akun pengguna, termasuk yang digunakan oleh layanan jaringan; (5) mengimplementasikan penapisan paket pada *router* untuk mengurangi efek dari SYN Flooding; (6) memasang patch sistem operasi jaringan, baik komponen kernelnya atau komponen layanan jaringan seperti halnya HTTP Server dan lainnya; (7) melakukan *backup* terhadap konfigurasi sistem dan menerapkan kebijakan password yang relatif rumit; (8) mencegah serangan non elektronik – admin bisa menerapkan peraturan tegas dan sanksi untuk mencegah user melakukan serangan dari dalam; (9) menggunakan PortSentry, yaitu program yang dirancang untuk mendeteksi dan menanggapi kegiatan port scan pada sebuah mesin secara real- *time*. PortSentry akan bereaksi terhadap usaha port scan dari lawan dengan cara memblokir penyerang secara realtime dari usaha *auto-scanner*, probe penyelidik, maupun serangan terhadap sistem.PortSentry akan melaporkan semua kejanggalan dan pelanggaran kepada software daemon syslog lokal maupun remote yang berisi nama sistem, waktu serangan, IP penyerang maupun nomor port TCP atau UDP tempat serangan di lakukan.

PENUTUP

Berdasarkan pembahasan di atas, penulis dapat menyimpulkan beberapa hal.

Pertama, serangan denial of service*,* adalah jenis serangan terhadap sistem jaringan di mana penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, seperti: (1) membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai *traffic flooding*; (2) membanjiri jaringan dengan banyak *request* terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga *request* yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai *request flooding*; (3) mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara,termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

Kedua, beberapa *tool* yang digunakan untuk melakukan serangan DoS pun banyak dikembangkan setelah itu (bahkan beberapa tool dapat diperoleh secara bebas), termasuk *Bonk, LAND, Smurf, Snork, WinNuke, dan Teardrop*. Cara yang paling sederhana adalah dengan mengirimkan beberapa paket ICMP dalam ukuran yang besar secara terus menerus yang dilakukan pada lebih dari satu sesi ICMP. Teknik ini disebut juga sebagai ICMP Flooding.

Ketiga, denial of service merupakan serangan yang sulit di atasi, hal ini disebabkan oleh resiko layanan publik di mana admin akan berada pada kondisi yang membingungkan antara layanan dan kenyamanan terhadap keamanan**.**

Saran yang dapat penulis berikan adalah sebagai berikut: (1) lakukan pencegahan serangan DoS dengan menutup servis servis/protokol protokol yang dianggap tidak perlu melalui firewall; (2) non aktifkan IP *directed broadcast* untuk *subnetwork subnetwork* dalam domain untuk mencegah serangan ini; (3) gunakan filter pada permintaan *ICMP echo pada firewall* yang mengizinkan paket paket dengan IP address yang sah yang melewati jaringan komputer kita.

DAFTAR PUSTAKA

Herlambang, M. Linto. (2010). *Buku Putih Cracker: Kupas Tuntas DOS Attack + Cara Penanggulangannya*. Yogyakarta: Andi Publiser.

Oetomo, Budi Sutedjo Dharma. (2003). *Konsep dan Perancangan Jaringan Komputer*. Yogyakarta: Andi Offset.

Sugianto, David. (2003). *LDL Membangun Website dengan PHP.* Jakarta: D@takom.

Sukamaaji, Anjik dan Rianto. (2008). *Jaringan Komputer: Konsep Dasar Pengembangan Jaringan & Keamanan Jaringan (Subnet, VLSM, Routing, DES, PGP, & Firewall)*. Jakarta:Andi Offset.

Tittel, Ed. (2005). *Schaum's Outlines: Computer Networking (Jaringan Komputer).* (Irzam Hardiansyah, terj.). Surabaya: Erlangga.

Wardhana, Lingga dan Makodian, Nuraksa. (2010). *Teknologi Wireless Communication Dan Wireless Broadband*. Jakarta: Andi Offset.