MENGENAL JENIS-JENIS SERANGAN DoS (*Denial Of Service*) TERHADAP SISTEM JARINGAN

Muhammad Rudyanto Arief

Abstraksi

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu – The Art of War

Kutipan diatas adalah isi salah satu chapter buku "The Art of War" Sun Tzu. Kutipan diatas sangat tepat untuk pengamanan jaringan dan komputer di internet. Karena tidak ada yang aman jika sudah berada di internet. Untuk mengamankan sistem jaringan maka harus diketahui jenis-jenis serangan apa yang akan menyerang sebuah sistem jaringan. Salah satu jenis serangan yang paling banyak digunakan adalah dengan menggunakan metode DoS (*Denial of Service*).

Kata Kunci : *DoS, Land Attack, Ping of Death, Teardrop, IP Spoofing*

Apa itu Serangan DoS?

Serangan Denial of Service (DoS) adalah sebuah aksi membanjiri saluran atau sesumber lain dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakai lain.

Bagaimana cara kerja DoS?

Dalam tipe koneksi jaringan biasa, user mengirimkan sebuah pesan untuk menanyakan otentikasi user yang bersangkutan ke server. Kemudian server merespon permintaan user tersebut dengan memberikan jawaban persetujuan otentikasi ke user tersebut. User tersebut mendapatkan ijin otentikasi selanjutnya dapat masuk kedalam sistem.

Dalam serangan DoS, user akan mengirimkan beberapa permintaan otentikasi ke server, dengan memenuhi *bandwidth* server. Semua permintaan yang dilakukan oleh user memiliki alamat pengembalian yang salah, sehingga server tidak dapat menemukan user yang bersangkutan ketika ingin mencoba mengirimkan persetujuan otentikasi yang diminta oleh user tersebut. Server akan menunggu, kadang-kadang lebih dari beberapa menit, sebelum menutup koneksi atas user tersebut. Ketika koneksi tersebut ditutup, penyerang akan mengirimkan permintaan baru kepada server, dan proses otentikasi akan dimulai lagi dari awal. Begitu seterusnya sehingga mengikat layanan yang diberikan server untuk jangka waktu tidak terbatas. Jika hal tersebut terjadi maka user lain yang ingin mengakses sesumber (*resouces*) didalam jaringan tersebut tidak dapat melakukan koneksi karena server tersebut disibukkan oleh permintaan otentikasi user yang melakukan serangan DoS tadi.

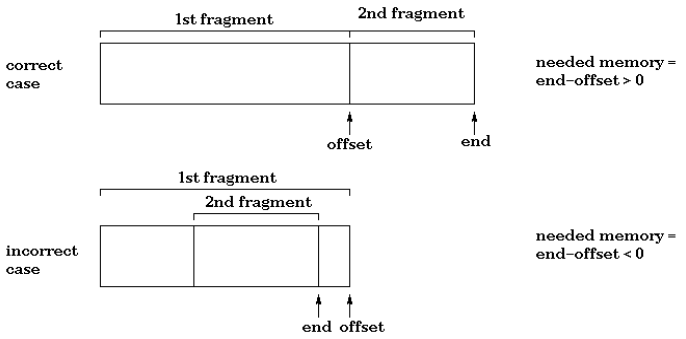
Jenis-jenis serangan yang termasuk kategori DoS

Teardrop

Teardrop adalah salah satu tipe serangan Denial Of Service (DOS). Teardrop adalah sebuah serangan yang memanfaatkan kelemahan yang ditemukan pada internet protocol dalam pengiriman paket. Ketika sebuah paket diproses, dalam penerapannya biasanya dilakukan pengecekan apakah paket yang diberikan terlalu panjang atau tidak tapi tidak melakukan pengecekan apakah paket tersebut terlalu pendek dan dibatasi.

Gambar berikut ini menjelaskan bagaimana proses serangan teardrop terjadi. Tumpukan menerima fragmen/ penggalan pertama paket yang dikirimkan dan mengalokasikan memeori untuk fragmen tersebut. Offset paket berikutnya diletakkan pada akhir dari area memori seperti akhir pointer. Tumpukan menyangka datagram berikutnya mulai pada offset dan menghitung akhir dari pointer untuk menunjukkan akhir dari paket baru yang dikirim, ini berarti ukuran paket pertama ditambah ukuran paket kedua dikurangi IP header kedua yang terbuang. Jumlah dari memori yang dibutuhkan = akhir offset. Tetapi offsetnya di-*spoof* pada paket kedua dan ditempatkan kedalam area memori pertama. Tumpukan mencoba untuk menyusun kembali untuk membetulkan susunannya, tetapi jika paket kedua lumayan pendek, maka pointernya akan berubah tempatnya. Pointer offset akan tetap menuju pada akhir dari paket pertama tetapi akhir pointer kemudian menuju kedalam area memori, bukan pada akhir dari paket pertama. Hasil perhitungan memori yang diperlukan = end-offset adalah negatif/ minus. Pada langkah selanjutnya adalah mengalokasikan

memori untuk paket baru, prosedur pengalokasian memori dapat gagal karena diberikan angka negatif sebagai sebuah argument. Kesalahan dalam pengalokasian memori dapat menyebabkan host crash/ system crash.



gambar 1. Proses kerja Teardrop attack.

Serangan teardrop mengirimkan satu atau lebig paket UDP yang telah dipecah ke sebuah host, dan dengan ukuran fragmen yang benar dan fragmen offset yang salah, pengalokasian memori pada host tujuan menjadi gagal.

IP Soofing

IP Spoofing adalah suatu trik *hacking* yang dilakukan pada suatu server dengan tujuan untuk mengecoh komputer target agar mengira sedang menerima data bukan dari komputer yang mengirim data tersebut, melainkan komputer target mengira menerima data dari komputer lain yang memiliki IP Addres yang berbeda dari komputer sebenarnya yang telah mengirim data. Suatu contoh dari IP Spoofing adalah sebagai berikut :

Misalkan :
IP Address komputer sumber yang mengirim data adalah 203.45.98.1
IP Address komputer yang akan dijadikan target adalah 202.14.12.1
IP Address sistem yang digunakan untuk mengirimkan data adalah 173.23.45.89

Secara normal komputer target akan mengidentifikasi IP Address dari komputer yang mengirimkan data adalah 203.45.98.1, namun dalam trik IP Spoofing komputer target akan mengira bahwa data yang dikirim adalah dari komputer dengan IP Address 173.23.45.89.

IP Spoofing adalah suatu teknik yang sulit untuk dilakukan karena pada kenyataannya saat melakukan teknik ini penyerang (*hacker*) tidak mendapatkan pesan atau *feedback* dari proses yang telah dilakukan apakah berhasil atau gagal. Hal ini biasa disebut dengan *blind attack*, dimana *hacker* akan selalu berasumsi bahwa serangan yang dilakukannya sudah berjalan dengan benar.

Permasalahan utama dari teknik ini adalah walaupun komputer sumber berhasil mengirim data dengan IP Address komputer sumber yang telah disamarkan, dan komputer yang menjadi target telah mempercayai bahwa data telah dikirm oleh komputer dengan IP Address yang dipalsukan, kemudian komputer target akan membalas melalui IP Address yang dipalsukan, bukan IP Address komputer sumber.

IP Spoofing dilakukan dengan menggunakan konsep *three-way handshake* agar terjadi koneksi TCP/IP. Secara normal *three-way handshake* yang terjadi adalah:

1. Komputer sumber mengirim paket SYN ke komputer target
2. Komputer target mengirim kembali paket SYN/ACK ke komputer sumber
3. Komputer sumber akan mengakui paket SYN dr komputer target dengan mengirim balasan berupa paket SYN ke komputer target.

Adapun yang terjadi dalam IP Spoofing adalah :

1. Komputer sumber mengirim paket SYN ke komputer target tapi dengan menggunakan IP Address yang telah dipalsukan.
2. Komputer target akan mengirim paket SYN/ACK kepada komputer dengan IP Address yang palsu tersebut. Dalam hal ini tidak ada cara bagi komputer sumber untuk menentukan kapan dan apakah komputer target benar-benar membalas dengan mengirimkan paket SYN/ACK ke IP Address yang telah dipalsukan tersebut. Hal ini merupakan bagian yang tidak diketahui oleh komputer sumber (*blind part*) dan komputer sumber hanya dapat berasumsi bahwa komputer target telah mengirim paket SYN/ACK ke IP Addres yang telah dipalsukan tersebut.
3. Kemudian setelah beberapa waktu komputer sumber harus mengirimkan paket SYN ke komputer target untuk mengakui bahwa komputer dengan IP Address yang palsu telah menerima paket SYN/ACK.

Koneksi TCP/IP hanya akan terjadi jika dan hanya jika ketiga langkah di atas terjadi.

LAND Attack

LAND Attack atau biasa juga disebut LAND DoS Attack bekerja dengan cara mengirimkan paket SYN dengan IP Address yang telah dipalsukan – yang biasa digunakan pada *handshake* antara *client* dan *host* – dari suatu *host* ke semua *port* yang sedang terbuka dan mendengarkan. Jika paket diatur untuk memiliki IP Address sumber (*source*) dan tujuan (*destination*) yang sama, maka pada saat paket ini dikirim ke sebuah mesin (melalui IP Spoofing) akan dapat membohongi atau mengecoh mesin tersebut agar mengira bahwa mesin itu sendiri yang telah mengirim paket tersebut, dimana hal ini dapat mengakibatkan mesin *crash* (tergantung dari sistem operasi yang terdapat pada mesin tersebut).

Jenis serangan ini dapat mempengaruhi mesin dengan sistem operasi Windows 95/NT, berbagai jenis dari UNIX, termasuk juga SunOS, beberapa versi BSD UNIX, serta Macintosh. Serangan ini juga dapat mempengaruhi beberapa Cisco router, dan peralatan cetak yang berbasiskan TCP/IP (TCP/IP-*based printing devices*).

LAND Attack dapat mempengaruhi berbagai sistem operasi dalam berbagai cara. Sebagai contoh, serangan jenis ini dapat menyebabkan mesin dengan sistem operasi Windows NT 4.0 (dengan *Service Pack 3* dan seluruh aplikasinya) menjadi lambat kira-kira dalam waktu 6 detik, setelah itu akan kembali normal tanpa ada efek lainnya. Serangan ini jika terjadi pada mesin dengan sistem operasi Windows 95 dapat menyebabkan baik itu *crash* maupun *lock-up*, sehingga mesin-mesin tersebut perlu di boot ulang. Sementara sebagian besar mesin dengan sistem operasi UNIX yang mendapat serangan ini akan *crash* atau *hang* dan user tidak dapat melakukan akes ke servis-servis yang terdapat pada mesin tersebut.

Ping of Death

Ping of Death adalah salah satu bentuk serangan "*ping attack*". Pada internet, bentuk serangan ini adalah bentuk serangan DoS (*denial of service attack*) yang disebabkan oleh penyerang yang dengan sengaja mengirimkan sebuah paket IP yang ukurannya lebih besar dari yang diijinkan oleh protokol IP yaitu 65.536 byte. Salah satu fitur dari TCP/IP adalah *fragmentation*, yang mengijinkan sebuah paket IP tunggal dipecah ke dalam bagian yang lebih kecil. Pada tahun 1996, para penyerang mulai mengambil keuntungan dari fitur ini, yaitu saat mereka menemukan bahwa sebuah paket yang dipecah menjadi bagian-bagian kecil dapat ditambah menjadi lebih besar dari yang

diijinkan yaitu 65.536 byte. Banyak sistem operasi tidak tahu apa yang harus dilakukan ketika menerima paket dengan ukuran yang berlebihan tersebut, sehingga akhirnya sistem operasi tersebut berhenti bekerja, *crashed*, atau *rebooted*.

Serangan ping of death sangat tidak menyenangkan karena tanda-tanda atau identitas penyerang saat mengirim paket dengan ukuran yang berlebihan dapat dengan mudah disamarkan, dan karena para penyerang tidak perlu mengetahui apapun tentang mesin yang akan mereka serang kecuali IP Addressnya. Pada akhir tahun 1997, *vendor-vendor* sistem operasi telah membuat sejumlah *patch* yang memungkinkan untuk menghindari serangan ini. Beberapa *Web site* melakukan blok terhadap pesan ping ICMP pada *firewall* yang mereka miliki untuk mencegah berbagai variasi berikutnya dari serangan jenis ini.

Ping of death juga dikenal sebagai "*long* ICMP". Variasi dari serangan ini termasuk *jolt*, *sPING*, ICMP *bug*, dan IceNewk.

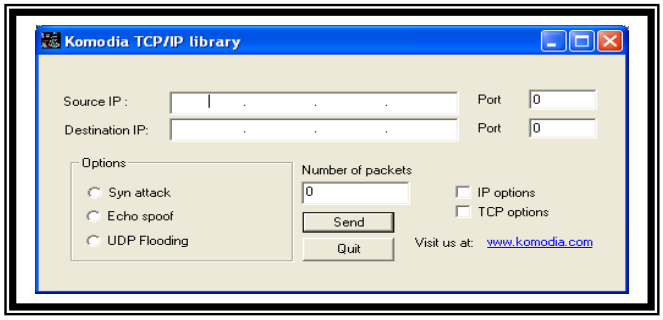
Bagaimana cara mengatasi serangan Dos?

Untuk mengatasi terjadinya serangan DoS maka hal pertama yang dilakukan adalah dengan mengetahui jenis-jenis serangan DoS dan bagaimana cara kerjanya. Seperti strategi yang diterapkan oleh Tsun Zu dalam bukunya "The Art of War". Kita harus mengetahui kelebihan dan kelemahan penyerang sebelum melakukan serangan balasan. Setelah mengetahui cara kerja dan jenis-jenis serangan DoS maka langkah berikutnya yang paling sering digunakan adalah dengan melakukan pengaturan dengan cara penyaringan/ *filtering*, atau "*sniffer*"/ mengendus pada sebuah jaringan sebelum sebuah aliran informasi mencapai sebuah server situs web. Penyaring tersebut dapat melihat serangan dengan cara melihat pola atau meng-identifikasi kandungan/ isi dari informasi tersebut. Jika pola tersebut datang dengan frekuensi yang sering, maka penyaring dapat memberikan perintah untuk memblokir pesan yang berisikan pola-pola tersebut, melindungi web server dari serangan tersebut.

Mengenal salah satu *tool* yang digunakan untuk melakukan serangan DoS

Di internet banyak sekali *tools* yang dapat digunakan untuk menyerang sebuah sistem jaringan dengan menggunakan metode DoS. *Tool* tersebut adalah ATTCAKER. Berikut adalah penjelasan singkat tentang Attacker dan proses kerja *tool* ini.

Attacker



gambar 2 Tampilan Antar Muka perangkat lunak ATTACKER

Attacker adalah salah satu software yang digunakan untuk melakukan serangan pada level aplikasi dimana software ini mengirmkan packet pada Addres yang telah dituju. Software ini membutuhkan pengetahuan mengenai IP address yang akan diserang dan harus terlebih dahulu mencari port-port yang terbuka dari Komputer tempat IP address yang akan diserang tersebut.
Software ini terdiri dari 3 jenis serangan yang dapat dipilih yaitu :

- Syn attack
- Echo spoof
- UDP Flooding

Ketiga jenis serangan ini adalah termasuk jenis serangan DOS attack atau disebut Denial of Service Attack dimana serangan yang dilakukan akan menyebabkan terganggunya atau terhentinya kerja sistem yang diserang.

Syn Attack

Syn attack adalah serangan yang menggunakan Synhcronazation flood attack pada pertukaran data yang menggunakan three way handshake. Pada saat penyerang mengirimkan paket pada komputer yang diserang dengan menggunakan alamat internet palsu (spoofing) maka komputer yang menerima akan mengirim kembali pada pada komputer penyerang dan menunggu balasan selama kurang lebih 20 detik. Pada saat bersamaan penyerang akan mengirim paket lagi sebanyak-banyaknya sehingga komputer korban akan terjadi antrian dan akhirnya hang.

Echo spoof

Ini merupakan serangan pada port t (Echo Service) dimana penyerang akan mengirim paket pada port 7 pada komputer korban menggunakan IP lokal palsu (local host address). Echo Service akan memberikan respon pada alamat tersebut (pada dirinya sendiri) dan akan terjadi loop yang tidak terbatas. Ini akan menyebabkan sistem terganggu.

UDP flooding

Mengirim Data pada port UDP dengan menggunakan Alamat palsu. Hampir sama dengan Syn flood attacks..

Serangan menggunakan Attacker dapat dicegah melalui beberapa cara yaitu dengan menggunakan :

- Firewall dan melakukan konfigurasi yang optimal
- Memperbesar Half Open antrian pada suatu koneksi
- Membatasi Half Open Connection pada satu address sehingga tidak dapat terlalu banyak mengirim paket.
- Mengurangi waktu antrian suatu paket sehingga apabila terlalu lama merespon akan dihilangkan
- Menggunakan IDS (Intrusion Detection System)

Kesimpulan

DoS adalah tipe serangan yang sejauh ini mendapatkan perhatian yang sedikit dalam sistem keamanan informasi. Tujuan dari DoS adalah untuk memperlambat atau erusak kerja daripada jaringan komputer dan DoS sangat sulit untuk dicegah. Karena tujuan dari DoS tidak menghasilkan sesuatu yang dapat merusak sesumber didalam sistem tetapi hanya mengganggu salah satu tujuan dari mengapa internet sangat dibutuhkan saat ini yaitu Availability. Seluruh organisasi saat ini yang menggunakan internet sebagai media menjalankan bisnis perusahaannya mengutamakan *availability* sebagai satu-satunya layanan yang di andalkan. Sehingga jika layanan ini terganggu maka organisasi tersebut akan mengalami kerugian besar dalam bisnisnya. Sehingga inilah yang menyebabkan mengapa DoS harus dapat dicegah dalam mengamankan keamanan jaringan informasi.

Daftar Pustaka

- http://www.webopedia.com/TERM/D/DoS_attack.html
- http://whatis.techtarget.com/definition/0,289893,sid9_gci213591,00.html
- http://java.sun.com/sfaq/denialOfService.html
- http://www.hut.fi/~lhuovine/study/hacker98/dos.html#1.0
- http://www.komodia.com/