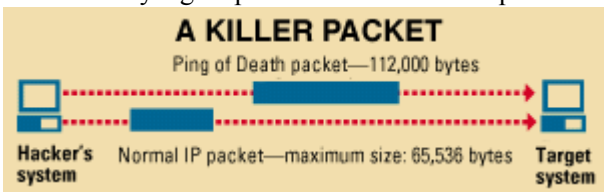
Ensiklopedia Serangan Denial of Service

Onno W Purbo
onno@indo.net.id

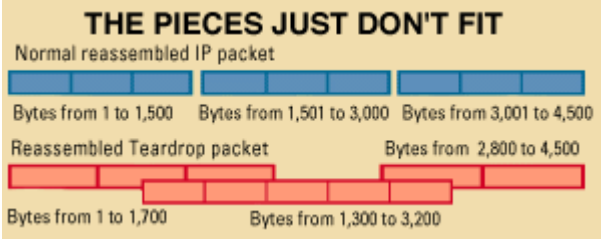
Tulisan ini merupakan saduran bebas dari tulisan yang sama di PC Magazine http://205.181.113.18/pcmag/pctech/content/17/08/nt1708.002.html dan juga hacktech.org (http://www.hacktech.org). Denial of Service (DoS) merupakan serangan di Internet yang termasuk cukup di takuti karena akan menyebabkan mesin / server tidak bisa beroperasi sama sekali & tidak bisa memberikan servis. Tulisan ini akan mencoba memberikan gambaran secara garis besar teknik dari berbagai serangan telak tersebut. Beberapa teknik telak yang sering digunakan, antara lain adalah:

- Ping of Death.
- Teardrop.
- SYN Attack
- Land Attack
- Smurf Attack
- UDP Flood

Ping of Death menggunakan program utility ping yang ada di sistem operasi komputer. Biasanya ping digunakan untuk men-cek berapa waktu yang dibutuhkan untuk mengirimkan sejumlah data tertentu dari satu komputer ke komputer lain. Panjang maksimum data yang dapat dikirim menurut spesifikasi protokol IP adalah 65,536 byte. Pada Ping of Death data yang dikirim melebihi maksimum paket yang di ijinkan menurut spesifikasi protokol IP. 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. Serangan ini sudah tidak baru lagi, semua vendor sistem operasi telah memperbaiki sistem-nya untuk menangani kiriman paket yang oversize.



Teardrop – teknik ini dikembangkan dengan cara mengeksplotasi proses disassembly-reassembly paket data. Dalam jaringan Internet, seringkali data harus di potong kecil-kecil untuk menjamin reliabilitas & proses multiple akses jaringan. Potongan paket data ini, kadang harus dipotong ulang menjadi lebih kecil lagi pada saat di salurkan melalui saluran Wide Area Network (WAN) agar pada saat melalui saluran WAN yang tidak reliable proses pengiriman data menjadi lebih reliable. Pada proses pemotongan data paket yang normal setiap potongan di berikan informasi offset data yang kira-kira berbunyi "potongan paket ini merupakan potongan 600 byte dari total 800 byte paket yang

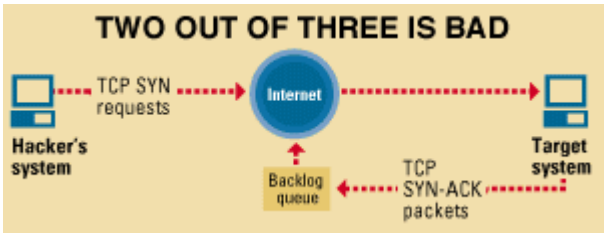


dikirim". Program teardrop akan memanipulasi offset potongan data sehingga akhirnya terjadi overlapping antara paket yang diterima di bagian penerima setelah potongan-potongan paket ini di reassembly. Seringkali, overlapping ini menimbulkan system yang crash, hang & reboot di ujung sebelah sana.

SYN Attack- kelemahan dari spesifikasi TCP/IP, dia terbuka terhadap serangan paket SYN. Paket SYN dikirimkan pada saat memulai handshake (jabat tangan) antara dia aplikasi sebelum transaksi / pengiriman data dilakukan. Pada kondisi normal, aplikasi klien akan mengirimkan paket TCP SYN untuk mensinkronisasi paket pada aplikasi di server (penerima). Server (penerima) akan mengirimkan respond berupa acknowledgement 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. Dalam serangan SYN flood (banjir paket SYN), klien akan membanjiri server dengan banyak paket TCP SYN. Setiap paket TCP SYN yang dikirim akan menyebabkan server menjawab dengan paket TCP SYN ACK. Server (penerima) akan terus mencatat (membuat antrian backlog) untuk menunggu responds TCP ACK dari klien yang mengirimkan paket TCP SYN.

Tempat antrian backlog ini tentunya terbatas & biasanya kecil di memori. Pada saat antrian backlog ini penuh, sistem tidak akan merespond paket TCP SYN lain yang masuk – dalam bahasa sederhana-nya sistem tampak bengong / hang. Sialnya paket TCP SYN ACK yang masuk antrian backlog hanya akan dibuang dari backlog pada saat terjadi time out dari timer TCP yang menandakan tidak ada responds dari klien pengirim. Biasanya internal timer TCP ini di set cukup lama. Kunci SYN attack adalah dengan membanjiri server dengan paket TCP SYN menggunakan alamat IP sumber (source) yang kacau. Akibatnya, karena alamat IP sumber (source) tersebut tidak ada, jelas tidak akan ada TCP ACK yang akan di kirim sebagai responds dari responds paket TCP SYN ACK.

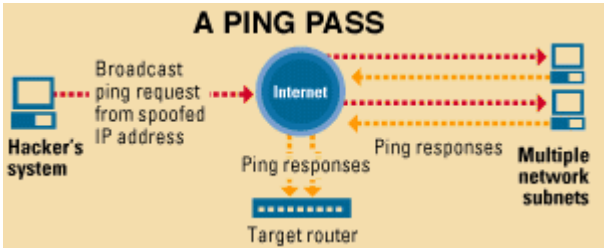
Dengan cara ini, server akan tampak seperti bengong & tidak memproses responds dalam waktu yang lama. Berbagai vendor komputer sekarang telah menambahkan pertahanan untuk SYN attack ini & juga programmer firewall juga menjamin bahwa firewall mereka tidak mengirimkan packet dengan alamat IP sumber (source) yang kacau.



Land Attack – dalam Land attack – gabungan sederhana dari SYN attack – hacker membanjiri jaringan dengan paket TCP SYN dengan alamat IP sumber dari sistem yang di serang. Biarpun dengan perbaikan SYN attack di atas, Land attack ternyata menimbulkan masalah pada beberapa sistem. Serangan jenis ini relatif baru, beberapa vendor sistem operasi telah menyediakan perbaikannya. Cara lain untuk mempertahankan jaringan dari serangan Land attack ini adalah dengan memfilter pada software firewall anda dari semua paket yang masuk dari alamat IP yang diketahui tidak baik. Paket yang dikirim dari internal sistem anda biasanya tidak baik, oleh karena itu ada baiknya di filter alamat 10.0.0.0-10.255.255.255, 127.0.0.0-127.255.255.255, 172.16.0.0-172.31.255.255, dan 192.168.0.0-192.168.255.255.

Smurf Attack - jauh lebih menyeramkan dari serangan Smurf di cerita kartun. Smurf attack adalah serangan secara paksa pada fitur spesifikasi IP yang kita kenal sebagai direct broadcast addressing. Seorang Smurf hacker biasanya membanjiri router kita dengan paket permintaan echo Internet Control

Message Protocol (ICMP) yang kita kenal sebagai aplikasi ping. Karena alamat IP tujuan pada paket yang dikirim adalah alamat broadcast dari jaringan anda, maka router akan mengirimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Kalau ada banyak host di jaringan, maka akan terhadi trafik ICMP echo respons & permintaan dalam jumlah yang sangat besar. Lebih sial lagi jika si hacker ini memilih untuk men-spoof alamat IP sumber permintaan ICMP tersebut, akibatnya ICMP trafik tidak hanya akan memacetkan jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di spoof – jaringan ini di kenal sebagai jaringan korban (victim).



Untuk menjaga agar jaringan kita tidak menjadi perantara bagi serangan Smurf ini, maka broadcast addressing harus di matikan di router kecuali jika kita sangat membutuhkannya untuk keperluan multicast, yang saat ini belum 100% di definikan. Alternatif lain, dengan cara memfilter permohonan ICMP echo pada firewall. Untuk menghindari agar jaringan kita tidak menjadi korban Smurf attack, ada baiknya kita mempunyai upstream firewall (di hulu) yang di set untuk memfilter ICMP echo atau membatasi trafik echo agar presentasinya kecil dibandingkan trafik jaringan secara keseluruhan.

UDP Flood pada dasarnya mengkaitkan dua (2) sistem tanpa disadarinya. Dengan cara spoofing, User Datagram Protocol (UDP) flood attack akan menempel pada servis UDP chargen di salah satu mesin, yang untuk keperluan "percobaan" akan mengirimkan sekelompok karakter ke mesin lain, yang di program untuk meng-echo setiap kiriman karakter yang di terima melalui servis chargen. 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. Untuk menanggulangi UDP flood, anda dapat men-disable semua servis UDP di semua mesin di jaringan, atau yang lebih mudah memfilter pada firewall semua servis UDP yang masuk. Karena UDP dirancang untuk diagnostik internal, maka masih aman jika menolak semua paket UDP dari Internet. Tapi jika kita menghilangkan semua trafik UDP, maka beberapa aplikasi yang betul seperti RealAudio, yang menggunakan UDP sebagai mekanisme transportasi, tidak akan jalan.