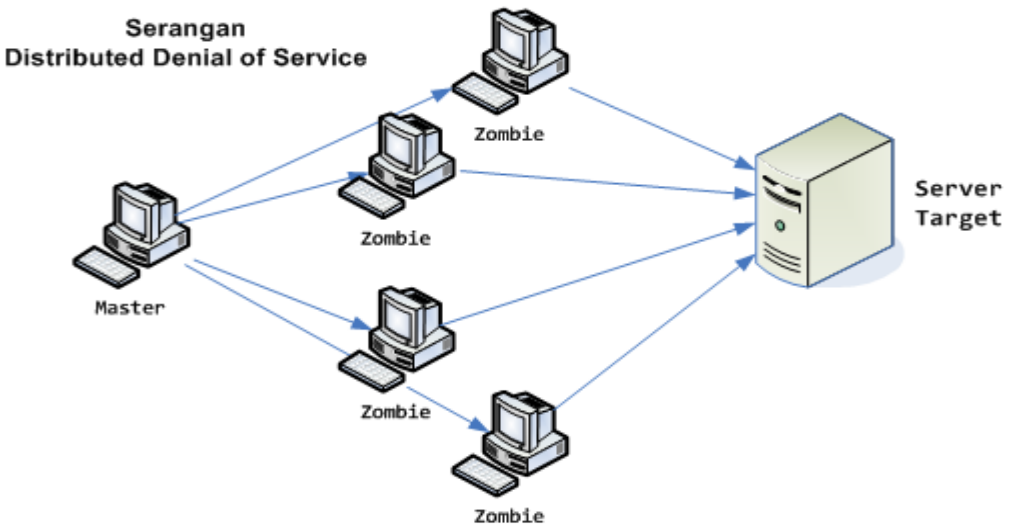
Waspadalah terhadap serangan DDoS

Serangan DDoS merupakan salah satu serangan yang cukup mudah dilakukan, hal tersebut terbukti karena banyak tools untuk melakukan serangan DDoS yang telah beredar diinternet. Sampai dengan sekarang ini serangan DDoS menjadi serangan yang sangat populer, banyak server yang telah terkena serangan DDoS. Serangan DDoS tidak hanya server yang menjadi target, komputer host juga bisa menjadi target serangan DDoS.

Distributed Denial of Service (DDoS)

Serangan Distributed Denial of Service atau biasa disebut DDoS terjadi apabila *attacker* atau yang sering terdengan dengan istilah hacker, merusak host atau server yang ada sehingga host atau server tersebut sulit untuk diakses atau berkomuniksi secara lancar didalam suatu network. Serangan Distributed Denial of Service merupakan serangan yang membanjiri atau memenuhi traffic jaringan dari suatu layanan dengan cara mengirim sebuah paket secara masif, sehingga membuat suatu service sulit untuk diakses atau terganggunya konektivitas jaringan yang digunakan untuk mengakses suatu service.

Distributed Denial of Service dapat membuat suatu server kehabisan sumber daya yang dimana dapat berupa *bandwidth*, *memory*, *CPU*, dan lain sebagainya. Server yang terkena serangan DDoS biasanya tidak akan mampu menahan laju traffic yang terlalu padat, sehingga membuat suatu service menjadi sulit diakses dan bahkan dapat mengalami kerusakan. Pada dasarnya serangan Distributed Denial of Service sama dengan serangan Denial of Service atau DoS hanya saja serangan DDoS tidak hanya menggunakan satu host untuk menyerang, melainkan dilakukan dengan banyak sumber atau host yang biasanya disebut dengan “Zombie” yang dikendalikan oleh *attacker*. Berikut merupakan ilustrasi dari serangan Distributed Denial of Service.



Serangan DDoS memiliki beberapa jenis yang dikenal adalah sebagai berikut.

- Ping of Death attack **:** serangan ini menggunakan metode "Ping", metode tersebut biasanya digunakan untuk mengecek posisi dari sebuah alamat IP situs/website. Metode tersebut terkadang digunakan oleh *attacker* yang digunakan untuk mengirimkan data berukuran hingga 65kb secara masif.
- UDP Flooding attack **:** metode serangan ini hampir mirip dengan Ping of Death, hanya saja untuk serangan ini menggunakan protokol UDP sebagai paket serangan, sehingga membuat target akan mengalami hang dikarenakan kesulitan menangani data flooding dalam jumlah besar.
- Syn Flooding attack **:** serangan ini hanya terjadi saat dua device sudah melakukan komunikasi 3-way handshake. *Attacker* akan mengirimkan pesan "*syn ask*" ke device target dalam jumlah besar, sehingga membuat target mengalami hang.
- Remote Controlled attack **:** metode serangan ini menggunakan beberapa komputer dengan server besar milik orang lain yang akan dikendalikan oleh *attacker* untuk menyerang target. Hal tersebut bertujuan agar *attacker* tidak terlacak.
- Smurf attack **:** merupakan serangan ddos yang memanfaatkan protokol ICMP (Internet Control Message Protocol) echo request yang biasa digunakan pada saat proses broadcast identitas ke alamat broadcast dalam sebuah jaringan, yang berarti pada saat melakukan broadcast, semua komputer yang terkoneksi di jaringan yang sama akan mengirim reply ke *attacker*. Hal ini akan mempengaruhi kecepatan traffic data didalam jaringan, karena komputer yang tidak dikirim request oleh *attacker* itu ikut mengirim sebuah reply.

Macam-macam cara mengatasi serangan DDoS.

Serangan DDoS merupakan sebuah serangan yang dapat membuat suatu system terjadi hang, hal tersebut dikarenakan system tidak dapat menahan laju paket data yang dikirim oleh *attacker* dalam jumlah yang besar. Berikut merupakan cara mengatasi serangan DDoS.

- Selalu memperbarui (update) patch pada sistem keamanan untuk menutupi celah keamanan yang bisa saja muncul pada sistem operasi komputer atau server yang digunakan.
- Untuk mengatasi serangan Syn Flooding, yaitu dengan menggunakan *firewall*. *Firewall* berfungsi untuk menyaring paket data yang masuk dan keluar melalui traffic jaringan yang digunakan pada komputer atau server. Maka dari itu gunakanlah rules dalam firewall agar dapat menahan atau mencegah paket data yang tidak diketahui tersebut masuk dan keluar.
- Jika komputer server dijadikan "Zombie" oleh *attacker* untuk melakukan serangan Remote Controlled attack, maka lakukanlah pengecekan terhadap aktivitas yang janggal pada komputer server.

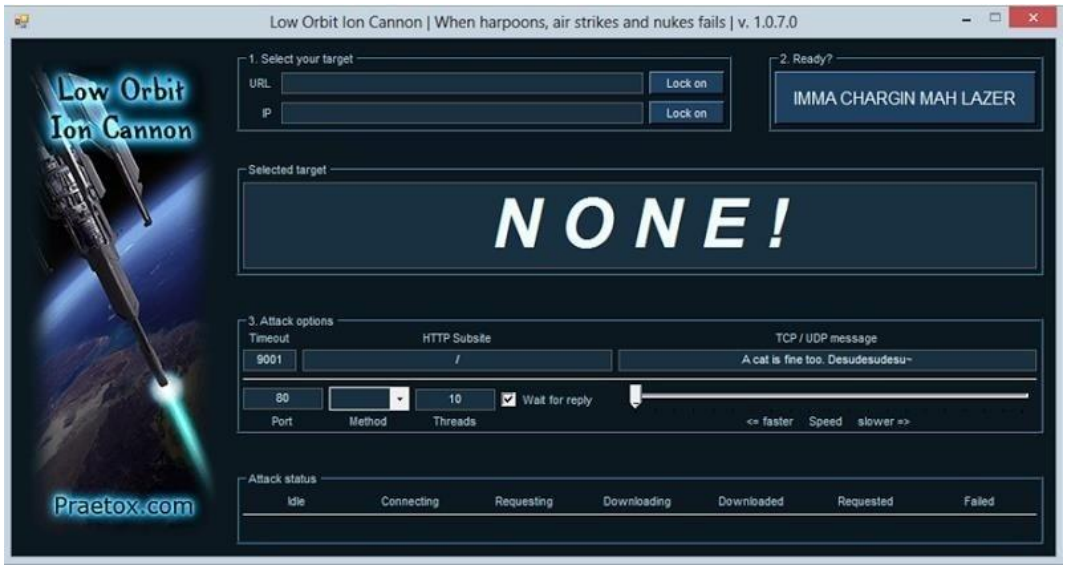
Pengecekan tersebut dapat dilakukan dengan mengatur dan mengkombinasikan firewall dengan mesin IDS (Intrusion Detection System) untuk mengurangi dampak serangan. Berbeda jika komputer server yang dijadikan target atau terkena serangan Remote Controlled attack, maka harus melakukan blocking pada *IP Address* dan *Port*.

- Untuk mengatasi serangan UDP Flooding, dapat dilakukan penolakan paket data yang datang dari luar jaringan dan mematikan semua layanan UDP yang masuk ke komputer server.
- Serangan DDoS Smurf attack dapat diatasi dengan cara men-disable broadcast address pada router. Tidak hanya itu, dapat juga diatasi dengan cara melakukan filtering (menyaring) permintaan ICMP echo request pada firewall atau dengan cara membatasi traffic ICMP agar persentasenya kecil dari seluruh traffic yang ada pada jaringan komputer.
- Gunakanlah tools atau software kemanan jaringan komputer yang terpercaya, misalnya seperti software antivirus yang sudah banyak beredar diinternet.

Macam-macam tools DDoS yang sering digunakan.

- LOIC

LOIC (Low Orbit Ion Cannon) merupakan software yang paling populer digunakan untuk melakukan serangan DDoS. Software berbasis Windows ini efektif untuk kmengirimkan banyak jumlah paket ICMP atau UDP ke target. Berikut merupakan tampilan dari tools LOIC.



- HOIC

HOIC (High Orbit Ion Cannon) merupakan software khusus untuk membanjiri HTTP dengan request acak HTTP GET dan POST. HOIC juga bisa digunakan untuk melakukan serangan ke 256 domain secara bersamaan.

- HULK

HULK (HTTP Unbearable Load King) merupakan sebuah script python yang dibuat dengan tujuan untuk membuat suatu server kebingungan sehingga akan mengurangi kemampuannya dalam mengatasi serangan DDoS. Berikut tampilan dari HULK saat dirunning.