Faktor Exacta Vol. 5 No. 1: 1-14
ISSN: 1979 276X

ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS)

RUDI HERMAWAN
rh001unindra@gmail.com
Program Studi Teknik Informatika
Fakultas Teknik, Matematika dan Ilmu Pengetahuan Alam
Universitas Indraprasta PGRI

Abstrak. Masalah kemanan komputer merupakan faktor yang sangat penting untuk diperhatikan dan dikelola dengan baik oleh sistem administrator. Di era teknologi informasi saat ini, layanan kepada konsumen menjadi hal yang mutlak untuk bisa bertahan dalam persaingan usaha. Banyak sekali cara yang ditempuh untuk menghalangi seseorang/perusahaan untuk dapat memberikan layanan yang optimal. Hal ini sangat mungkin bila layanan yang diberikan melalui koneksi internet yang dapat dikatakan kurang aman. Beberapa serangan terhadap server sebagai penyedia layanan kerap dilakukan oleh hacker, walaupun tidak semua tujuan yang dilakukan berlandaskan pada bisnis atau politik belaka. Namun beberapa diantaranya juga merupakan sebagai aksi unjuk gigi guna memperoleh prestise tertentu di sebuah komunitas atau perkumpulan. Serangan *DOS (Denial Of Service)* dan *DDOS (Distributed Denial Of Service)* adalah serangan yang bisa sering kita jumpai diantara serangan - serangan lainnya. *DOS* dan *DDOS* sendiri pada dasarnya adalah sama, namun DDOS adalah serangan yang lebih terstruktur. DDOS dengan mekanisme yang pada dasarnya sama dengan *DOS* namun memiliki dampak yang umumnya jauh lebih besar dibandingkan dengan DOS. Mekanisme serangan DOS maupun *DDOS* dan cara penanggulangannya sangat penting untuk diketahui dan dipelajari bagi sistem administrator mengingat serangan ini dapat menggagu kinerja server. Dampak serangan DDOS akan menyebabkan bandwidth yang digunakan oleh korban akan habis yang mengakibatkan terputusnya koneksi antar server, Bila serangan DDOS tidak segera ditanggulangi dapat menyebabkan kerusakan secara permanen terhadap hardware dan software korban.

Kata kunci: keamanan komputer, server, DOS, DDOS, Internet

Abstract. Computer security issues is a very important factor to be considered and managed well by the system administrator. In the current era of information technology, customer service to be paramount to survive in the competition. A lot of ways adopted to prevent a person / company to provide optimal service. It is quite possible when services are provided through an internet connection that can be said to be less safe. Some of the attacks against the server as a service provider is often done by hackers, although not all the goals that made based on business or politics. But some of them also is an act of performance gear in order to obtain a certain prestige in a community or society. DOS attack (Denial Of Service) and DDOS (Distributed Denial Of Service) is an attack that could often encountered between attacks - another attack. DOS and DDOS itself is basically the same, but the DDOS attack that was more structured. DDOS with a mechanism which is essentially the same as DOS, but has an impact which is generally much larger than the DOS. DOS or DDOS attack mechanisms and ways to overcome them is essential to be known and studied for the system administrator can remember this attack menggagu server performance. Impact of DDOS attack will cause the bandwidth used by the victim will be depleted resulting in breaking of the connection between the

server, if not immediately controlled DDOS attacks can cause permanent damage to the hardware and software offering.

Key words: computer security, server, DOS, DDOS, Internet

PENDAHULUAN

Keamanan merupakan hal yang sangat penting dalam dunia teknologi informasi. Di era teknologi informasi saat ini, pelayanan kepada konsumen menjadi hal yang mutlak untuk bertahan dalam persaingan. Banyak sekali cara yang ditempuh untuk menghalangi seseorang / instansi / perusahaan guna memberikan pelayanan tersebut. Hal ini menjadi sangat mungkin bila pelayanan yang diberikan melalui jalur yang dapat dikatakan kurang aman (internet) yang terkoneksikan melalui jaringan. Beberapa serangan kepada server sebagai penyedia layanan kerap dilakukan, walaupun tidak semua tujuan yang dilakukan berlandaskan pada politik,atau bisnis belaka. Namun beberapa diantaranya juga merupakan unjuk gigi guna memperoleh prestise tertentu di sebuah komunitas atau perkumpulan. Serangan *DOS (Denial Of Service)* dan *DDOS (Distributed Denial Of Service)* adalah serangan yang mungkin bisa sering kita jumpai diantara serangan serangan lainnya.

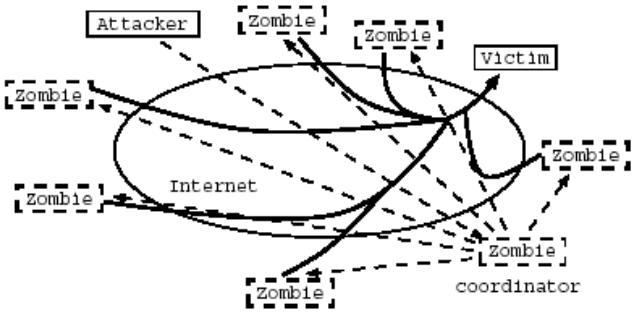
DOS dan *DDOS* sendiri pada dasarnya adalah sama , namun DDOS adalah serangan yang dapat dikatakan terstrukur. Dengan mekanisme yang pada dasarnya sama dengan *DOS* namun memiliki dampak yang umumnya jauh lebih besar dibandingkan dengan DOS. Mekanisme serangan DOS, *DDOS* dan cara penanggulangannya dapat kita angkat, mengingat banyaknya serangan yang terjadi. Walaupun belum banyak orang yang mengerti, namun tidak ada salahnya dijadikan pembelajaran untuk menambah pengetahuan mengenai jenis serangan yang cukup fatal ini. Cara penanggulangannya pun menarik untuk diangkat, sebagai bahan pertimbangan bila suatu saat tanpa kita tahu serangan ini menjadikan kita sebagai tergetnya. Dunia maya adalah dunia yang sangat sulit ditebak, kita tidak sepenuhnya tahu siapa lawan bicara kita. Apakah ia orang yang sebenarnya. Apakah orang yang sedang kita ajak bicara berhati bersih,atau mungkin sedang mengamati kita dari belahan dunia lain. Mungkin kata – kata yang sering kita dengar dan saya baca dari beberapa tulisan mengenai *"Don't trust anyone in cyber, be paranoid"* tidak sepenuhnya salah. Sebab dunia cyber adalah dunia yang sulit untuk ditebak. Dengan mengetahui mekanisme serangan diharapkan kita dapat mengetahui cara lain yang mungkin lebih ampuh untuk mengatasi serangan *DOS* ini.

Metode penanggulangan yang di jelaskan pada tulisan ini adalah metode yang umum, yang biasanya diterapkan oleh orang-orang yang lebih berpengalaman dalam jaringan. Metode penanggulangan dan mekanisme penyerangan didapatkan dari beberapa literatur dari beberapa ahli.

TINJAUAN PUSTAKA

Perkembangan aplikasi dan teknologi jaringan internet di saat sekarang ini semakin maju pesat. Fiturfitur layanan yang disediakan dalam jaringan internet juga begitu banyak ragamnya. Mulai dari web server, *File Transfer Protocol (ftp)*, layanan E-mail, sampai fitur-fituryang berhubungan dengan layanan transaksi yang semakin marak di dalam jaringan internet. Layanan tersebut seperti *Electronic Commerce (ECommerce)*, *Electronic Banking (E-Banking)*, *Electronic Goverment (EGov)* dan sebagainya. Karena internet yang begitu banyak memberikan manfaat dan bersifat publik, maka dibutuhkan suatu sistem keamanan dalam menjaga informasi yang ada di internet supaya tidak dirusak oleh pihak-pihak yang potensial melakukan pengrusakan seperti *hacker* dan *cracker*.

Salah satu jenis serangan pengrusakan yang dilakukan adalah dengan menghambat atau memutus ketersedian informasi ketika dibutuhkan serangan seperti ini disebut *Denial Of Service attack (DOS)*. Proses serangan ini dikerjakan oleh hacker/penyerang dengan cara server dikirimi layanan permintaan (biasanya palsu) atau permintaan yang secara terus menerus sehingga server tidak dapat melayani permintaan lain atau bahkan *down, hang, dan crash.* Apabila serangan DOS tersebut dilakukan secara terdistribusi maka jenis serangan tersebut disebut *Distributed Denial of Service attack (DDOS)*. Yakni *attacker* (penyerang) dapat men-*crack* beberapa mesin menjadi *zombie,* kemudian mesin yang menjadi zombie mengendalikan beberapa mesin lagi menjadi zombie-zombie, akhirnya attacker akan mengendalikan zombie-zombie tersebut secara terdistribusi menyerang korban (*victim*) untuk meniadakan ketersedian informasi dari korban. Gambaran tentang jenis serangan ini dapat dilihat pada gambar 1.



Gambar 1. Skema serangan DDOS

Beberapa website yang diserang dengan menggunakan prinsip *DDOS* adalah Ebay, Amazon, Buy.com , CNN.com, dan Yahoo.com. Karena begitu hebatnya efek dari serangan DDOS ini bagi websitewebsite tersebut sampai website-website tersebut mengalami kerugian yang cukup banyak untuk menanggulangi serangan ini. Sehingga dibutuhkan suatu teknik pencegahan untuk mendeteksi dan mencegah serangan *DDOS* ini.

Klasifikasi Umum Serangan (*Attack*)

Sebelum membahas secara detail mekanisme menanggulangi DDoS attack, lebih dahulu membahas uraian tentang klasifikasi ancaman keamanan komputer secara umum. Serangan pada *IT (Information Technologi)* menurut tujuan dari *cracker* dapat diklasifikasikan ke dalam [Bellavin, S.M., W.R. Cheswick. Firewalls and Internet Security. Addison Wesley Longmen, 1994]:

- *Denial of service (DOS):* sasaran utama serangan adalah merusak layanan yang disediakan, sehingga layanan menjadi tidak tersedia.
- *Intrusion:* pihak yang tidak berwenang berusaha memperoleh akses sistem, tujuan seperti ini adalah gambaran klasik dari seorang *hacker*. Mereka biasanya berusaha mencapai tujuannya keluar dari sistem dengan melakukan beberapa pengrusakan pada sistem, kemudian melaporkan ke *administrator* bahwa ada "*bug"*
- ditemukan dalam sistem.
- *Information Theft* [Pencurian informasi]: sasaran utama dari jenis serangan ini adalah berusaha mengakses informasi yang dibatasi pengaksesannya (*restricted*), informasi yang sensitif.

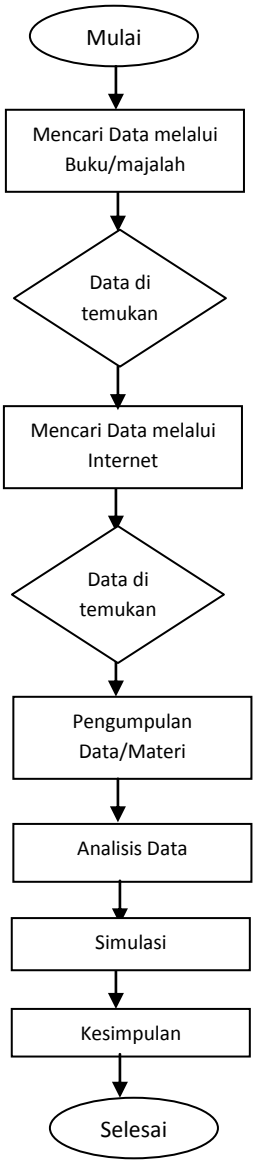
- *Modification:* disini *attacker* dengan aktif berusaha mengubah informasi yang ada dalam sistem. Jenis serangan macam ini semakin hari jumlahnya bertambah seperti mengubah isi website.

Definisi DOS dan DDOS

Ada beberapa definisi dari DOS, FAQ dari WWW. Security mendefinisikan DoS sebagai berikut: … suatu serangan yang dilakukan untuk membuat komputer atau jaringan komputer tidak dapat menyediakan layanan secara normal. Pada umumnya serangan DOS menargetkan serangan pada bandwidth jaringan komputer atau koneksi jaringan (*connectivity*). *Bandwidth attack* membanjiri jaringan dengan volume traffic yang tinggi, sehingga semua *resources* (sumber daya) yang ada, tidak dapat melayani *request* (permintaan) dari *legitimate user* (user yang sah). *Connectivity attack* membanjiri komputer dengan volume request koneksi yang tinggi, sehingga semua *resources* sistem operasi komputer yang ada tidak dapat memproses lebih lama *request* dari *legitimate user*.

J.D. Howard mendefinisikan DOS: Apabila hardware, software, dan data komputer tidak dapat terjaga ketersediaannya, maka produktivitas operasional jadi turun, walaupun tidak ada kerusakan yang terjadi. Denial of Service dapat mencakup kedua keadaan tersebut yang secara disengaja maupun tidak disengaja melakukan serangan kepada ketersediaan sistem (*systemavailability*). Perpektif yang muncul tanpa melihat sebab yang terjadi adalah apabila layanan diibaratkan tersedia, padahal tidak ada, sehingga mengakibatkan layanan *denied* (tidak ada). Suatu serangan, bagaimanapun, adalah suatu tindakan disengaja. Denial of Service attack diyakini berlangsung ketika mengakses ke komputer atau resource jaringan dengan sengaja di blocked atau hak aksesnya diturunkan dari user lain. Serangan ini tidak perlu merusak data secara langsung, atau permanen (walaupun mereka dapat melakukannya), tetapi mereka dengan sengaja berkompromi (mengganggu) ketersediaan dari *resource*. Macam serangan DoS attack umumnya melalui jaringan, dimana target utama dari serangan adalah *website* yang popouler seperti contoh yang disebutkan pada pendahuluan. Umumnya site-site tersebut mempunyai banyak hardware yang mereka gunakan, sehingga *attacker* akan bekerja keras untuk menyerang. Website normalnya terdiri dari beberapa web-server dengan sistem load balancing dan memiliki koneksi jaringan multi megabit. Sebagai konsekuensi attacker harus menemukan jalur baru untuk menaklukkan sistem. *Attacker* tidak menggunakan satu host dalam penyerangan mereka, tetapi menggunakan beberapa ratus bahkan ribuan komputer untuk melakukan serangan yang terkoordinir. Jenis serangan seperti ini disebut *Distributed Denial of Service attack (DDoS attack)*. FAQ dari WWW. Security pada *Distributed Denial of Service(DdoS) attack* mendefinisikan jenis serangan ini sebagai berikut: *Distributed Denial of Service(DDoS) attack* menggunakan banyak komputer untuk mengkordinir DoS attack ke satu atau lebih target korban. Penggunaan teknologi *client/server attacker* dapat mengefektifkan Denial of Service dengan memanfaatkan *resource* dari bagian komputer yang tanpa disadari bertindak sebagai *platform* serangan. Sehingga program master *DDoS* diinstall pada salah satu komputer dengan menggunakan *account* yang telah dicuri. Program master pada saat waktu yang ditentukan akan melakukan komunikasi ke sejumlah program "agent" yang akhirnya menginstall program tersebut dikomputer-komputer yang terhubung dengan internet. Ketika agent menerima command memulai serangan, penggunaan teknologi clien/server program master dapat mengendalikan ratusan bahkan ribuan komputer yang memiliki program agent untuk memulai serangan dalam beberapa detik. Aggregat *bandwidth* dari sejumlah besar program agent mungkin lebih besar dari kapasitas *uplink* dari website tersebut. Sehingga efek dari serangan ini lebih utama ke *IP Router* atau tidak dapat akses internet.

Kerangka Pemikiran



Gambar 2. Kerangka Pemikiran

METODE PENELITIAN

Studi pustaka dilakukan untuk mendapatkan data pendukung yang ada kaitannya dengan keamanan komputer dalam hal pengumpulan data mengenai bagaimana model atau konsep maupun prosedur yang digunakan dalam melakukan serangan DDOS. Dimaksudkan juga untuk mempelajari kasus-kasus yang terjadi di didalam jaringan Internet. Seperti yang telah dibahas sebelumnya, menurut J.D. Howard mendefinisikan DOS adalah: "Apabila hardware, software, dan data komputer tidak dapat terjaga ketersediaannya, maka produktivitas operasional jadi turun, walaupun tidak ada kerusakan yang terjadi. *Denial of Service* dapat mencakup kedua keadaan tersebut yang secara disengaja maupun tidak disengaja melakukan serangan kepada ketersediaan sistem (*system availability*). Perpektif yang muncul tanpa melihat sebab yang terjadi adalah apabila layanan diibaratkan tersedia, padahal tidak ada, sehingga mengakibatkan layanan

denied (tidak ada). Suatu serangan, bagaimanapun, adalah suatu tindakan disengaja. *Denial of Service attack* diyakini berlangsung ketika mengakses ke komputer atau resource jaringan dengan sengaja di blocked atau hak aksesnya diturunkan dari *user* lain. Serangan ini tidak perlu merusak data secara langsung, atau permanen (walaupun mereka dapat melakukannya), tetapi mereka dengan sengaja berkompromi (mengganggu) ketersediaan dari *resource"*.

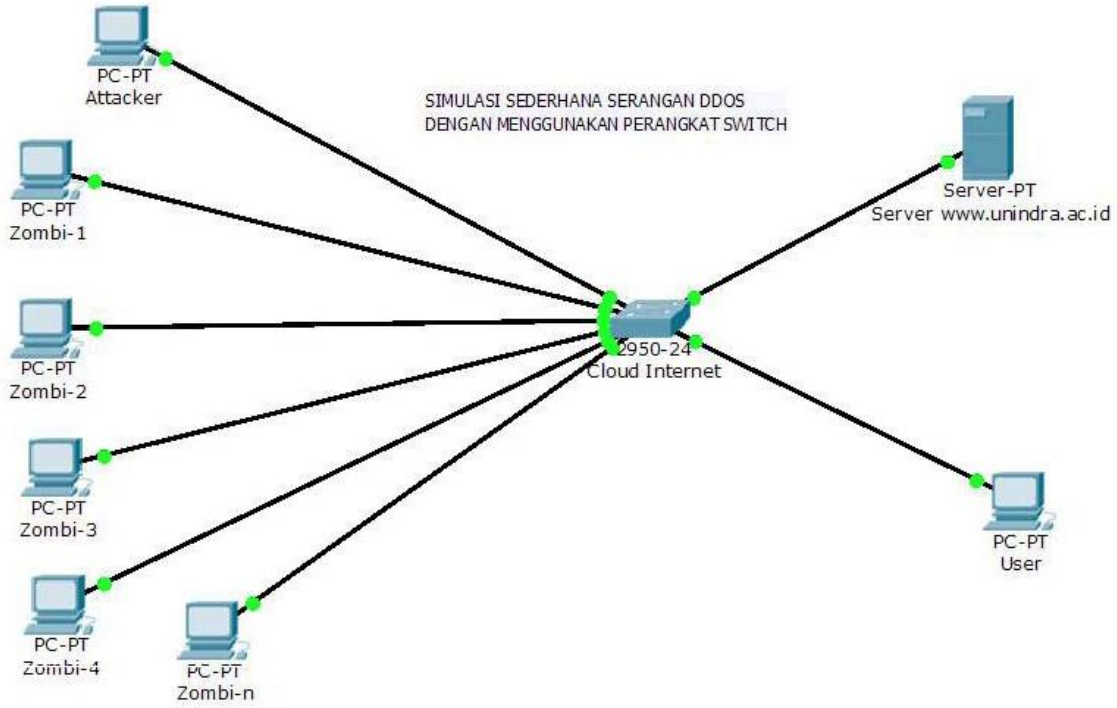
Menurut Stuart McClure, dkk, didalam buku *"HACKING EXPOSED"* bahwa berbagai alat dan teknik penyerang digunakan untuk menumbangkan target sistem keamanan. Sering kali, keamanan dari sebuah sistem atau jaringan akan menggagalkan penyerang yang tidak ahli. Merasa frustasi dan tidak berdaya, penyerang akan meluncurkan serangan DDOS sebagai pilihan terakhir. Di samping motif frustasi seseorang, individu mungkin memiliki dendam pribadi atau politik terhadap seseorang atau beberapa organisasi. Pakar keamanan banyak percaya bahwa jenis serangan akan meningkat karena perkembangan sistem Windows NT/95/98. Lingkungan windows adalah target favorit banyak penyerang. Selain itu, banyak alat DDOS sekarang *"point and click"* dan memerlukan keterampilan teknis yang sangat sedikit untuk menjalankannya.

HASIL DAN PEMBAHASAN

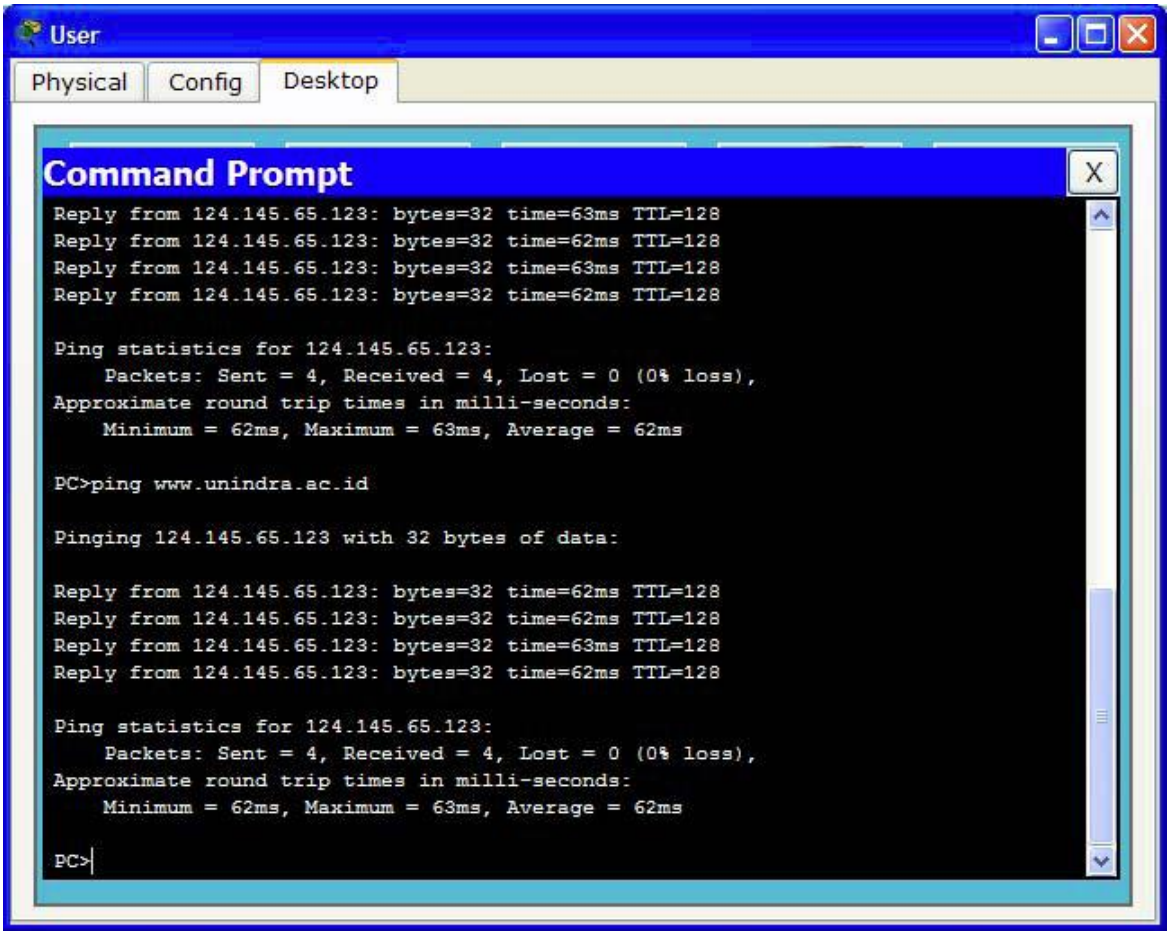
DDOS merupakan salah satu serangan yang banyak ditemui dalam dunia *networking* saat ini. Kita tidak pernah tahu kapan akan mendapatkan serangan ini. Serangan DDOS dapat terjadi kapan saja pada jaringan dan dapat ditujukan ke siapa saja, bahkan ke personal. Namun biasanya yang paling sering terkena dampaknya adalah serverserver besar seperti yahoo, google, serta perbankan yang secara langsung memberikan pelayanannya melalui jaringan. Bila kita memutuskan untuk memberikan pelayanan melalui jalur *networking*, kita harus siap menanggung risikonya, salah satunya adalah serangan DDOS. Serangan ini biasanya bertujuan untuk mematikan pelayanan dan dari komputer atau jaringan yang diserang. Dampaknya akan sangat besar bagi perusahaan atau instansi yang menyediakan jasa terutama bagi perbankan. Korban yang terkena serangan ini tidak dapat memberikan pelayanan yang seharusnya. Serangan DDOS ini dapat menghambat bahkan mematikan pelayanan pada sebuah sistem sehingga pengguna yang absah tidak dapat menerima atau mendapatkan pelayanan yang seharusnya. Bayangkan saja bila sebuah perusahaan banking tidak dapat memberikan pelayanan kepada nasabahnya, maka akan sangat fatal akibatnya bagi kelangsungan perusahaan tersebut. Atau sebuah provider internet yang tidak dapat memberikan bandwidthnya kepada klien, maka akan berdampak tidak hanya kepada provider tersebut yang harus membayar jaminan koneksi sesuai yang mereka terapkan namun juga kepada penyewa koneksi. Bila salah satu penyewanya adalah sebuah warnet atau bahkan banking, tentunya akan berdampak luas.Serangan DDOS ini pada dasarnya sulit untuk dideteksi, kecuali jika penyerang telah melakukan beberapa kali percobaan dengan alamat IP sama. Tentunya akan sangat mudah untuk membloknya. DDOS cukup sulit untuk diatasi karena serangan ini pada dasarnya juga berkaitan dengan pelayanan yang diberikan, sebuah sistem dengan tingkat keamanan tinggi biasanya memberikan kenyamanan yang rendah bagi penggunanya. Bayangkan bila server Yahoo dijadikan perantara untuk menyerang, tentu akan sangat membingungkan bagi Administrator di sebuah penyedia jasa internet. Sang Administrator tidak bisa asal melakukan blok alamat IP dari Yahoo karena akan terkena dampaknya adalah pengguna jasa internet tersebut.

Simulasi Serangan DOS/DDOS

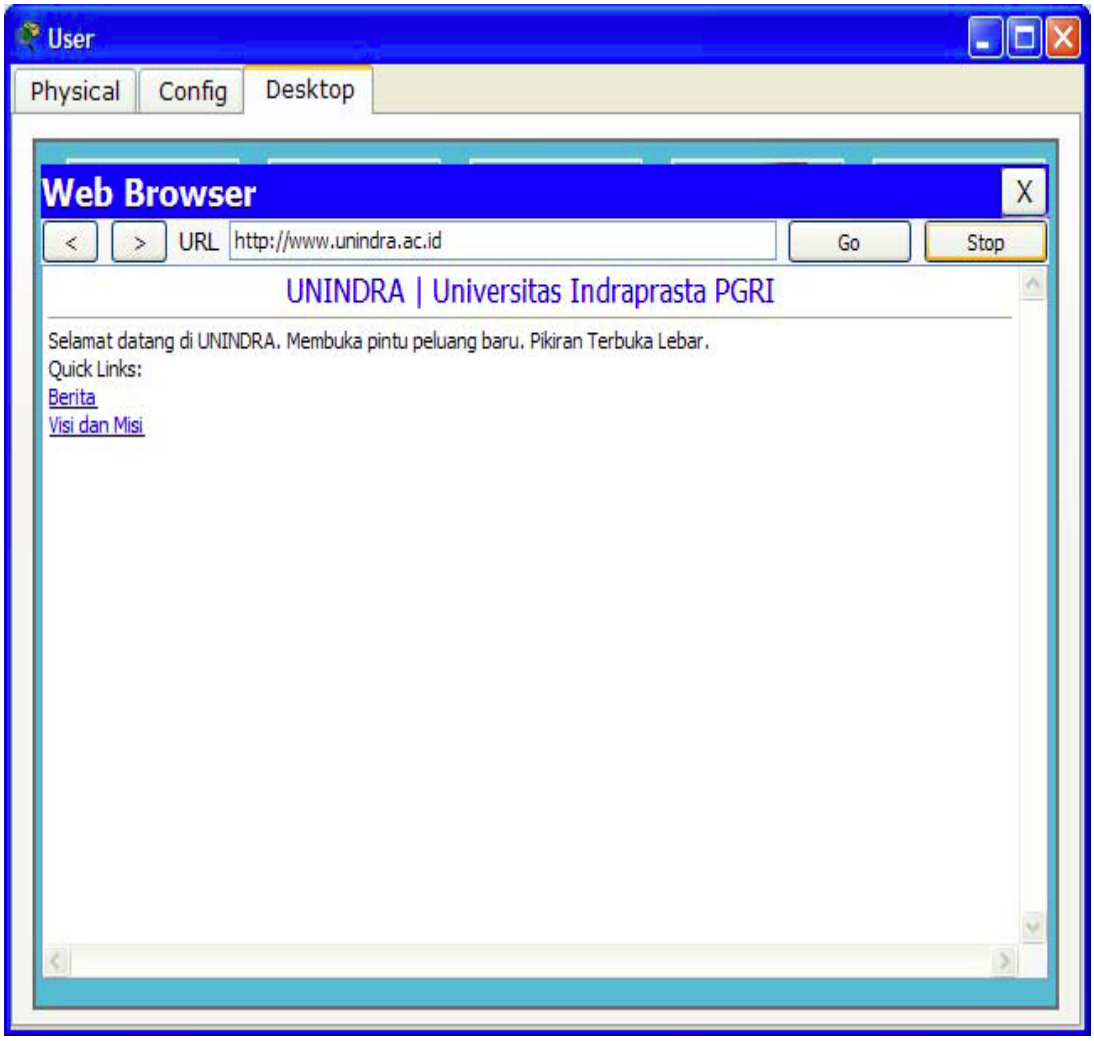
Cara kerja DDOS dalam melakukan serangan kepada situs yang diinginkan. Secara sederhana serangan DDOS bisa dilakukan dengan menggunakan perintah *ping* yang dimiliki oleh Windows. Proses *ping* ini ditujukan kepada situs yang akan menjadi korban. Jika perintah ini hanya dilakukan oleh sebuah komputer, perintah ini mungkin tidak menimbulkan efek bagi komputer korban. Namun jika perintah ini dilakukan oleh banyak komputer pada salah satu situs, maka perintah ini bisa memperlambat kerja komputer korban. Satu komputer mengirimkan mengirimkan data sebesar 32 bytes/detik ke situs yang dituju. Misalnya jika terdapat 10.000 komputer yang melakukan perintah tersebut secara bersamaan, maka kiriman data sebesar 312 Mega Bytes/detik yang diterima oleh situs yang dituju. Selanjutnya, server akan merespon kiriman yang dikirim dari 10.000 komputer secara bersamaan. Jika 312 MB/detik data yang harus di porses oleh server, dalam 1 menit saja server harus memproses kiriman data sebesar 312 MB x 60 detik = 18720 MB. Bisa ditebak, situs yang diserang dengan metode ini akan mengalami *overload*/kelebihan data, sehingga tidak sanggup memproses kiriman data yang datang terus-menerus. Komputer-komputer lain yang ikut melakukan serang tersebut disebut komputer zombie, karena sudah terinfeksi semacam adware. Jadi, si penyerang hanya memerintahkan komputer utamanya untuk mengirimkan perintah ke komputer zombie yang sudah terinfeksi agar melakukan *ping* ke situs yang dituju. Untuk melakukan simulasi serangan DDOS menggunakan software Packet Tracer. Dimana simulasi ini menggunakan perangkat Switch, yang seolah-olah sebagai *Cloud Internet.*



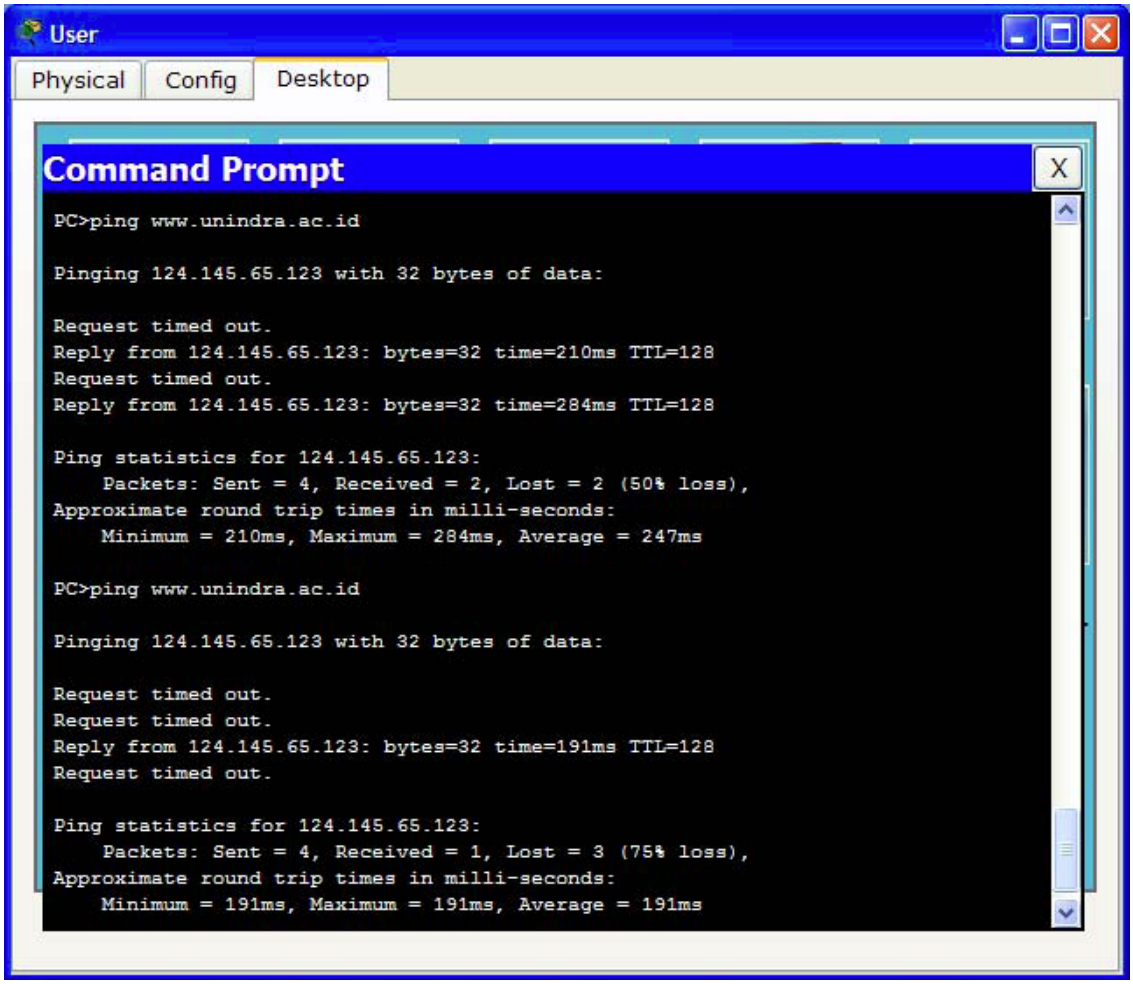
Gambar 3 Simulasi sederhana serangan DDOS



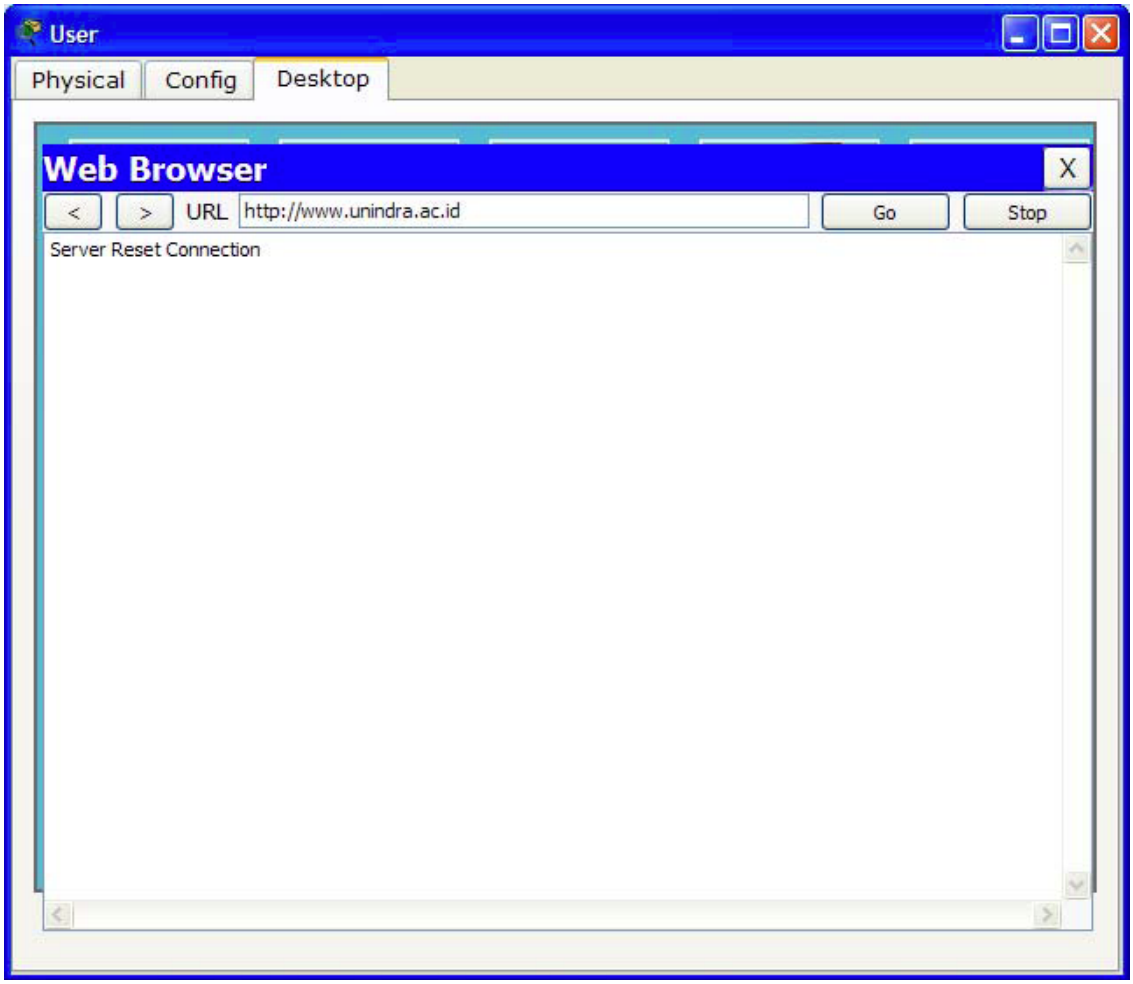
Gambar 4 Tes ping www.unindra.ac.id sebelum serangan DDOS



Gambar 5 Tes Browsing www.unindra.ac.id sebelum serangan DDOS



Gambar 6 Tes ping www.unindra.ac.id setelah serangan DDOS



Gambar 7. Tes Browsing www.unindra.ac.id setelah serangan DDOS

Implikasi Serangan DDOS

Serangan DDOS telah menjadi senjata pilihan semula untuk teroris cyber seperti kita mendatangkan elektronik milenium baru. Ini sering lebih mudah untuk mengganggu operasi jaringan atau sistem dibandingkan benar-benar mendapatkan akses. Jaringan protokol seperti TCP / IP dirancang untuk digunakan dalam sebuah komunitas terbuka dan terpercaya, dan saat ini inkarnasi dari protocol versi-4 memiliki kekurangan yang melekat. Selain itu, banyak sistem operasi dan perangkat jaringan memiliki kelemahan dalam tumpukan jaringan yang melemahkan kemampuan untuk menahan serangan DDOS. Sementara banyak alat yang tersedia untuk melancarkan serangan DDOS, penting untuk mengidentifikasi jenis Anda mungkin menemukan dan memahami bagaimana untuk mendeteksi dan mencegah serangan.

Jenis-jenis serangan DDOS, diantaranya:

a. Ping of Death

   Merupakan serangan klasik yang dulu sering digunakan. Serangan ini dilancarkan dengan menggunakan utility ping pada sebuah sistem operasi. Ping biasanya digunakan untuk memeriksa keberadaan sebuah host. Sekarang sistem seperti ini sudah tidak terlalu ampuh lagi, karena banyak sistem yang telah meng-update patchnya dan menutup lubang-lubang tersebut. Ditambah semakin canggihnya

teknologi dan semakin lebarnya bandwidth yang telah tersedia sehingga serangan ini tidak lagi menimbulkan dampak yang signifikan bagi sebuah sistem.

b. Syn Flooding
Serangan Syn Flooding dilakukan dengan cara memanfaatkan kelemahan protokol pada saat terjadinya proses *handshake*. Saat dua buah komputer memutuskan untuk memulai melakukan komunikasi, komputer pengirim (penyerang) akan mengirimkan *syn*, penerima (target) pun akan menjawab dengan mengirimkan *sync ack* kepaada komputer pengirim. Seharusnya setelah menerima *syn ack* dari penerima pengirim mengirimkan ack kepada penerima untuk melakukan proses *handshake*. Namun pada kenyataan, pengirim justru mengirimkan banyak paket *syn* kepada penerima yang mengakibatkan penerima harus terus menjawab permintaan dari pengirim. Serangan seperti ini tentunya akan menghambat penerima memberikan pelayanan kepada *user* yang abash.

c. Remote Controled Attack
Remote Controled Attack pada dasarnya adalah mengendalikan beberapa jaringan lain untuk menyerang target. Penyerangan dengan tipe ini biasanya akan berdampak besar, karena biasanya server-server untuk menyerang mempunyai bandwidth yang besar. Penyerang juga dengan leluasa dapat mengontrol targetnya dan menyembunyikan diri dibalik server-server tersebut. Umumnya tooltool mempunyai tipe *Master* dan *Client* atau *agent.* Master merupakan computer master yang telah dikuasai oleh penyerang dan akan digunakan untuk memberikan perintah guna melancarkan serangan. Sedangkan *client* adalah komputer zombie yang telah berhasil dikuasai oleh penyerang, kemudian penyerang menanamkan aplikasi client yang siap menunggu perintah untuk menyerang target.

d. UDP Flood
Serangan ini memanfaatkan protocol UDP yang bersifat *connectionless* untuk menyerang target. Karena sifatnya itulah UDP flood cukup mudah dilakukan. Sejumlah paket data yang besar dikirimkan begitu saja kepada korban. Korban yang terkejut dan tidak siap menerima serangan ini tentu akan bingung, dan pada beberapa kasus computer tersebut akan *hang* karena besarnya paket data yang dikirimkan. Penyerang dapat menggunakan teknik *spoofed* untuk menyembunyikan identitasnya.

e. Smurf Attack
Merupakan penyerangan dengan memanfaatkan *ICMP echo request* yang sering digunakan pada saat melakukan broadcast identitas kepada broadcast address dalam sebuah jaringan. Saat melakukan broadcast pada broadcast address, semua komputer yang terkoneksi ke dalam jaringan akan ikut menjawab dan memadatkan trafik di jaringan karena komputer-komputer yang tidak ditanya turut memberikan request tersebut. Serangan mungkin tidak berpengaruh begitu besar jika jumlah zombie yang digunakan sedikit. Namun jika jumlah yang digunakan terdiri dari puluhan bahkan ratusan sistem,bukanlah hal yang tidak mungkin bila *server* korban tersebut *crash*.

Solusi Penanggulangan Serangan DDOS

beberapa cara menanggulangi atau menghindari dari serangan DDOS, yaitu:

a) Ping of Death umumnya tidak terlalu berpengaruh pada sistem saat ini, namun ada baiknya selalu meng-*update* patch guna menutupi celah-celah keamanan yang ada pada sistem operasi.
b) Gunakan firewall yang dapat mengatasi masalah serangan ini, aturlah kebijaksanaan firewall untuk tidak meneruskan paket data yang tidak diketahui dengan jelas asalnya. Cara lain adalah dengan memperbesar jumlah maksimum koneksi syn yang dapat berlangsung ke server.

c) Bila Anda pemilik server yang dijadikan zombie, tersedia banyak aplikasi atau software untuk mendeteksi *tools trinoo* ini. Selalu waspada pada aktivitas yang terasa aneh di server Anda dan lakukan pengecekan secara berkala. Walaupun pada praktiknya sangat sulit untuk mendeteksi serangan ini, pengaturan dan kombinasi *firewall* dan *ids* mungkin dapat cukup membantu. Tentunya dengan kebijakan atau policy yang tepat. Lakukan *blocking IP address* dan port jika Anda terkena serangan dan laporkan kepada pemilik server yang menjadi zombie.
d) Dapat dilakukan dengan menolak paket data yang datang dari luar jaringan, dan mematikan semua *service UDP* yang masuk. Walaupun dengan cara ini dapat mematikan beberapa aplikasi yang menggunakan protokol UDP. Namun cara ini cukup efektif untuk mengatasi serangan ini.
e) Smurf dapat diatasi dengan men-*disable broadcast addressing* di *router*, kecuali bila benar-benar membutuhkannya. Cara lainnya adalah dengan melakukan *filtering* pada permintaan ICMP echo pada *firewall*. Cara lain yang dapat dilakukan adalah dengan membatasi trafik ICMP agar persentasenya kecil dari keseluruhan trafik yang terjadi pada jaringan.

PENUTUP

Kesimpulan

Setelah mempelajari pengetahuan mengenai serangan DDOS dan menganalisanya serta juga solusi untuk menghindari sari serangan DDOS dengan tingkatan yang berbeda, maka ditarik beberapa kesimpulan yang dapat dirinci seperti dibawah ini:

a. Keamanan Komputer merupakan hal yang sangat penting dalam dunia teknologi informasi terutama di era teknologi informasi saat ini, pelayanan kepada konsumen menjadi hal yang mutlak untuk bertahan dalam persaingan.
b. Serangan DOS (Denial Of Service) dan DDOS (Distributed Denial Of Service) merupakan salah satu serangan yang mungkin bisa sering dijumpai diantara serangan serangan komputer lainnya.
c. Beberapa website yang diserang dengan menggunakan prinsip DDOS adalah Ebay, Amazon,Buy.com,CNN.com, dan Yahoo.com.
d. Banyak alat dan teknik penyerang digunakan untuk menumbangkan target sistem keamanan. Kadang kala, keamanan dari sebuah sistem atau jaringan akan menggagalkan penyerang yang tidak ahli. Merasa frustasi dan tidak berdaya, penyerang akan meluncurkan serangan DDOS sebagai pilihan terakhir.
e. Motif seseorang atau beberapa orang adalah selain motif frustasi seseorang, individu mungkin memiliki dendam pribadi atau politik terhadap seseorang atau beberapa organisasi.
f. Serangan DOS/DDOS meningkat seiring perkembangan dari sistem operasi Windows.
g. Serangan DOS/DDOS dapat terjadi kapan saja pada jaringan dan dapat ditujukan ke siapa saja, bahkan ke personal. Namun biasanya yang paling sering terkena dampaknya adalah server-server besar.
h. Serangan DOS/DDOS biasanya bertujuan untuk mematikan pelayanan dan dari komputer atau jaringan yang diserang. Dampaknya akan sangat besar bagi perusahaan atau instansi yang menyediakan jasa terutama bagi perbankan.

Saran

Berdasarkan hasil analisa mengenai dampak suatu system akibat serangan DOS/DDOS, saran yang mungkin dapat bermanfaat bagi perkembangan ilmu komputer umumnya dan khususnya civitas akademi UNINDRA adalah sebagai berikut:

a. Kita sebaiknya selalu mengikuti perkembangan dunia komputer karena perkembangan komputer itu sangat cepat.
b. Hendaknya kita mengikuti pelatihan-pelatihan komputer terutama pelatihan mengenai Keamanan Komputer.
c. Setiap orang harus memiliki pengetahuan bagaimana cara ber-Etika Komputer sehingga memiliki rasa tanggung jawab dalam menjaga property, privasi, dan aksesbilitas dirinya maupun orang lain.
d. Segera bertindak jika komputer kita terdapat hal-hal yang mencurigakan.
e. Penyedia Layanan *(Provider) internet* diharapkan mengawasi jalur-jalur komunikasi internet pelanggannya dan segera bertindak bila ada laporan dari pelanggannya.

DAFTAR PUSTAKA

McClure,Stuart. Joel Scambray. George Kurtz. 2001. ***Hacking Exposed: Network Security Secrets and Solutions,Third Edition***. California: Corel VENTURATM.

Prabawati, Th.Ari. 2010. **Tutorial 5 Hari: Belajar Hacking dari Nol**. Semarang: Wahana Komputer.

http://virus-it.blogspot.com/2011/02/konsep-serangan-dos-ddos-dancara.html. Konsep Serangan DoS, DDoS dan Cara Mencegahnya.

http://id.wikipedia.org/wiki/Serangan_DoS. Serangan DOS.