ANALISIS KEAMANAN KOMPUTER TERHADAP SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDOS)

Hartini Ramli[1*], Maharaja Yasin Alifsyah[2]
Universitas Negeri Makassar
[1*]hartini.ramli@unm.ac.id
[2]marufkamil213@gmail.com

Abstract - Distributed Denial of Service (DDoS) is a type of active attack, an attack that can overwhelm a system by flooding a computer or server with network traffic, disrupting user services. The goal of this attack is usually to disable services and disconnect from the compromised computer or network. The impact is very large for companies or agencies that offer services. Victims of these attacks are unable to provide the services they are supposed to. Due to a bug or constraint on the server you are trying to use and one of the ways to deal with these attacks is to use a computer network firewall, which is useful for protecting computers from various outer space attacks. If the computer has a firewall security system, it is likely that no one on the Internet can access the data on the connected computer or web server. Firewall, works like a partition or wall that blocks the computer from the Internet. This "firewall" allows you to control what data, information, and activity can be transferred from the Internet to your computer and vice versa. With better data security and can avoid DDOS attacks that want to be carried out by irresponsible parties.

Keywords: DDOS, Network, Computer, Firewall, Server

1. PENDAHULUAN

Saat ini perkembangan komputer Internet telah berkontribusi pada kenyamanan hidup masyarakat. Namun disadari atau tidak, ada potensi bahaya di balik kemudahan penggunaan internet. Dalam dunia nyata kita sehari-hari, sebagian dari kita tidak menyadari banyak potensi risiko keamanan saat komputer tersambung ke Internet [1]. Hal ini karena sebagian besar komputer digunakan di area yang relatif kecil seperti lingkungan keluarga, tempat kerja atau sekolah/kampus. Jika kita menggunakannya dalam skala besar, akan ada masalah.

Ketika data dikirim dari satu komputer ke komputer lain di Internet, data tersebut melewati beberapa komputer lain, yang berarti bahwa pengguna memiliki kemampuan untuk mengambil alih satu atau lebih komputer. Pemblokiran layanan terdesentralisasi adalah serangan terhadap sistem keamanan jaringan, yang dapat mencegah pekerjaan layanan (layanan) atau menutupnya sedemikian rupa sehingga pengguna yang berwenang/berminat tidak dapat menggunakan layanan tersebut [2]. Penelitian ini membahas bentuk dan faktor ancaman keamanan informasi dan beberapa saran untuk meningkatkan pencegahan ancaman keamanan informasi.

Keamanan informasi merupakan hal yang sangat penting dalam dunia teknologi informasi. Di era teknologi informasi saat ini, layanan pelanggan mutlak diperlukan untuk tetap kompetitif. Ada banyak cara untuk mencegah seseorang/lembaga/perusahaan menyediakan layanan ini. Hal ini sangat mungkin terjadi ketika layanan ditawarkan melalui saluran yang disebut kurang aman (Internet) yang terhubung melalui jaringan [3]. Server sebagai penyedia layanan sering terkena serangan berganda, meskipun tidak semua target datang dari politik atau bisnis. Namun, beberapa dari mereka juga tampak mendapatkan rasa hormat tertentu di komunitas atau di klub

Dari uraian di atas, penulis dapat merumuskan permasalahannya, yaitu Bagaimana proses Terjadinya Serangan tersebut ? dan Bagaimana cara mencegah serangan Distributed Denial Of Service Attack?. Adapaun tujuan dari penelitian ini adalah mampu Mengetahui proses terjadinya Distributed Denial Of Service Attack dan Mengetahui pencegahan apa yang dapat dilakukan untuk menghalangi ancaman tersebut terjadi.

2. TINJAUAN PUSTAKA

2.1 Denial of Service Attack (Dos)

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[4]. DoS merupakan serangan yang dapat menyebabkan kerusakan yang serius pada sistem, sehingga diperlukan sebuah sistem yang dapat mendeteksi serangan ini dengan baik [5].

2.2. Distribution Denial ofService (DDoS)

Distribution Denial of Service (DDoS) adalah salah satu jenis serangan aktif, yaitu serangan yang dapat menyebabkan hilangnya data dan habisnya daya yang dimiliki suatu sistem dengan cara membanjiri traffic jaringan suatu komputer atau server sehingga layanan user terganggu. (Satmoko, Sukarno and Jadied, 2018)

2.3. Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dan saling berhubungan antara yang satu dengan yang lain untuk melakukan tugas-tugasnya. (Mufadhol, 2012)

2.4. Cisco Pocket Tracer

Packet Tracer adalah program simulasi jaringan yang memungkinkan siswa untuk bereksperimen dengan perilaku jaringan dari perusahaan Cisco Networks. Yang digunakan dalam simulasi ini adalah packet tracer versi student 6.2 untuk mensimulasikan rancangan jaringan untuk mengenal perilaku jaringan dengan mode routing tertentu ataupun konsep jaringan lainnya seperti Spanning Tree, ACL dll. (Santoso, 2016)

3. METODE PENELITIAN

3.1 Jenis Penelitian

Komputer terhadap serangan distributed denial of service (ddos)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. Kepustakaan (library research) mengumpulkan berbagai informasi yang berhubungan dengan teknik distributed denial of service dari buku-buku dan jurnal.

3.2 Batas Penelitian

Dalam penelitian ini, penulis membatasi masalah yang akan dianalisis agar tidak terjadi penyimpangan

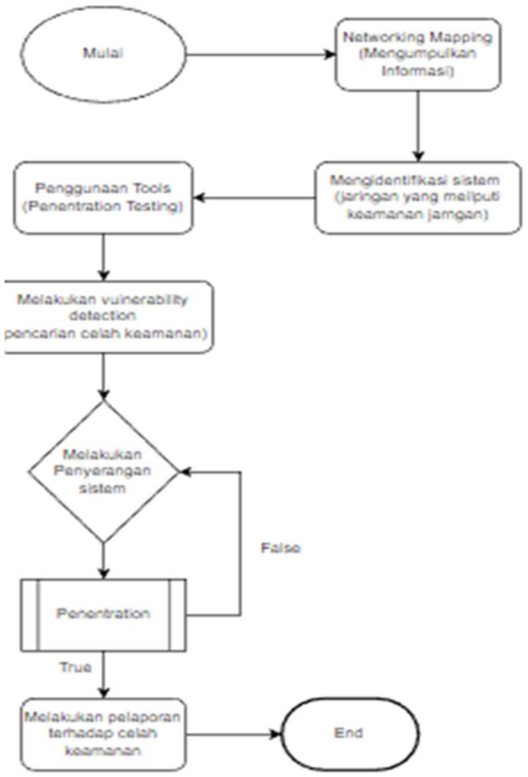
1. Penelitian tidak dimaksudkan untuk menentukan tingkat keamanan situs web.
2. Penulis tidak mengimplementasikan perbaikan keamanan jaringan yang ada, hanya analisis dan saran yang harus diterapkan.

3.3 Pengumpulan Data

Dalam penelitian ini ada beberapa metode yang digunakan untuk mengumpulkan data dan bahan yang diinginkan yaitu: pengumpulan data yang dilakukan adalah dengan observasi, studi pustaka dan dokumentasi.

1. Observasi
   Metode ini dilakukan dengan cara pengamatan pada kasus-kasus lainnya dan melakukan pencatatan informasi yang berkaitan dengan obyek penelitian.
2. Studi Pustaka
   Studi Kepustakaan adalah metode pengumpulan data dengan membaca buku referensi atau dokumentasi yang berhubungan dengan penelitian tentang keamanan jaringan.Dalam hal ini juga dilakukan browsing untuk mencari data atau dokumentasi yang berhubungan dengan obyek yang sedang diteliti.
3. Dokumentasi
   Peneliti melakukan pengumpulan data melalui dokumen-dokumen atau arsip yang berhubungan dengan topic penelitian.

3.4 Alur Flowchart Penelitian



Gambar 1. Alur Flowchart

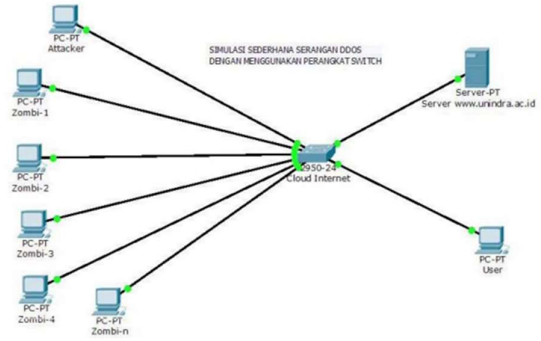
4. HASIL DAN PEMBAHASAN

DDOS adalah salah satu serangan paling umum di dunia Internet saat ini. Kita tidak pernah tahu kapan kita akan mendapatkan serangan itu. Serangan DDOS dapat terjadi secara online kapan saja dan dapat menyerang siapa saja, bahkan individu. Namun, dalam banyak kasus, masalahnya adalah server besar seperti Yahoo, Google, dan bank yang menawarkan layanan mereka langsung melalui web. Jika kita memilih untuk menawarkan layanan melalui saluran online, kita harus bersedia mengambil risiko, salah satunya adalah serangan DDOS. Tujuan serangan ini biasanya untuk menonaktifkan layanan dan memutuskan sambungan dari komputer atau jaringan yang disusupi. Dampaknya sangat besar bagi perusahaan atau instansi yang menyediakan jasa, khususnya perbankan. Korban serangan ini tidak dapat memberikan layanan yang seharusnya.

Serangan DDOS ini dapat memblokir atau bahkan menghentikan layanan sistem, sehingga pengguna yang sah tidak dapat menerima atau menerima layanan yang seharusnya. Bayangkan jika sebuah perusahaan perbankan tidak dapat memberikan pelayanan kepada nasabahnya, akibatnya bagi kelangsungan perusahaan sangat fatal. Atau penyedia internet yang tidak dapat menyediakan broadband kepada pelanggannya, tidak hanya mempengaruhi penyedia layanan tersebut, yang mungkin harus membayar jaminan koneksi, tetapi juga mereka yang menyewa koneksi tersebut. Tentu saja, jika salah satu penyewa adalah warnet atau bahkan bank, efeknya sangat luas: Serangan DDOS ini umumnya sulit dideteksi kecuali penyerang telah melakukan beberapa upaya dengan alamat IP yang sama. Tentu saja, itu akan sangat mudah untuk dicegah. DDOS cukup sulit dikalahkan karena serangan ini juga terkait secara fundamental dengan layanan yang diberikan. Suatu sistem dengan tingkat keamanan yang tinggi biasanya menawarkan kenyamanan yang kurang baik bagi penggunanya. Bayangkan jika server Yahoo digunakan sebagai proxy untuk serangan, akan sangat membingungkan administrator ISP. Administrator tidak dapat begitu saja memblokir alamat IP Yahoo karena hal itu memengaruhi pengguna layanan Internet.

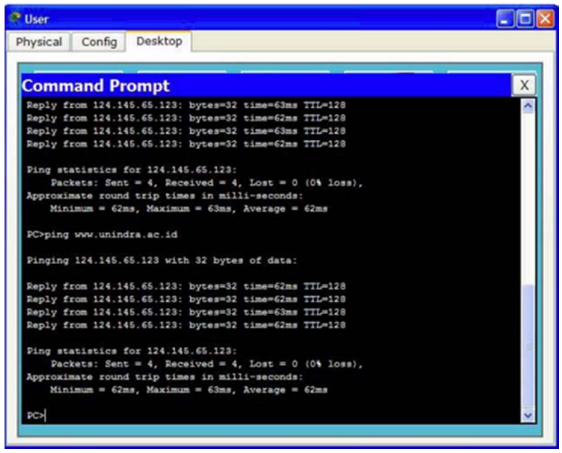
Berikut adalah contoh Simulasi Penyerangan DDOS Pada Komputer. Cara kerja DDOS untuk melakukan serangan terhadap website yang diinginkan. Sederhananya, serangan DDOS dapat dilakukan menggunakan perintah ping asli Windows. Proses ping ini menargetkan website yang menjadi korban. Jika

perintah ini dijalankan hanya dari satu komputer, mungkin tidak akan berpengaruh pada komputer korban. Namun, jika perintah ini dijalankan di banyak komputer dalam satu tempat, perintah ini dapat memperlambat komputer korban. Komputer mengirimkan data ke situs web target dengan kecepatan 32 byte per detik. Misalnya, jika 10.000 komputer menjalankan perintah pada saat yang sama, situs target akan menerima kecepatan transfer data sebesar 312 megabita/detik. Juga, server menanggapi pesan yang dikirim oleh 10.000 komputer secara bersamaan. Jika server perlu memproses data sebesar 312 Mb/s, server harus memproses ukuran transfer data sebesar 312 Mb x 60 detik = 18720 Mb dalam 1 menit. Dapat diperkirakan bahwa situs web yang diserang dengan metode ini akan mengalami kelebihan beban, membuat mereka tidak dapat mengatasi aliran data yang terus-menerus. Komputer lain yang terlibat dalam serangan itu dikenal sebagai komputer zombie karena menerima bentuk adware. Jadi penyerang cukup menginstruksikan komputer host untuk mengirim perintah ke komputer zombie yang terinfeksi untuk melakukan ping ke situs target. Simulasikan serangan DDOS menggunakan perangkat lunak Packet Tracer. Simulasi ini menggunakan switch yang terlihat seperti cloud internet. Pada simulasi untuk melakukan serangan ddos, langkah pertama membuat tapologi dari applikasi cisco pocket server



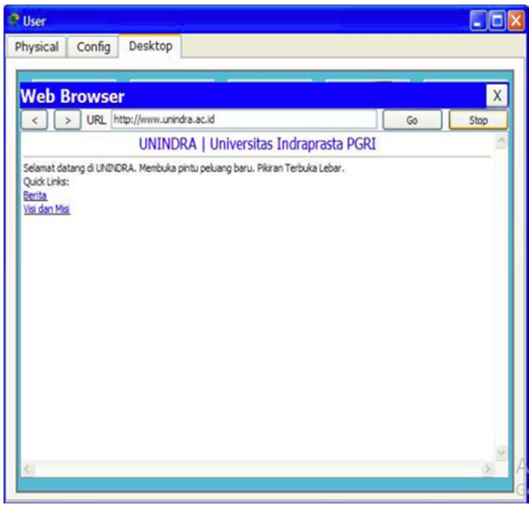
Gambar 2. Topologi Pada Cisco Pocket Server

Pada tapologi diatas, kita menggunakan 7 buah Personal Computer (PC), 1 buah server dan 1 switch 2950-24 yang seolah-olah adalah Cloud Internet. Pada Tapologi Diatas Telah Masuk 1 Attacker Dan PC Zombie Yang Telah 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.



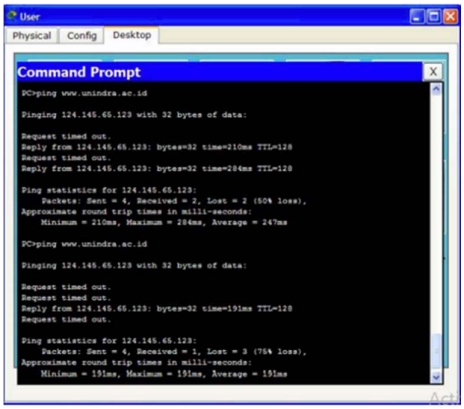
Gambar 3. Test Ping Pada User

Pada Gambar 3 diatas merupakan test ping user ketika ingin memasuki website yang ingin dituju

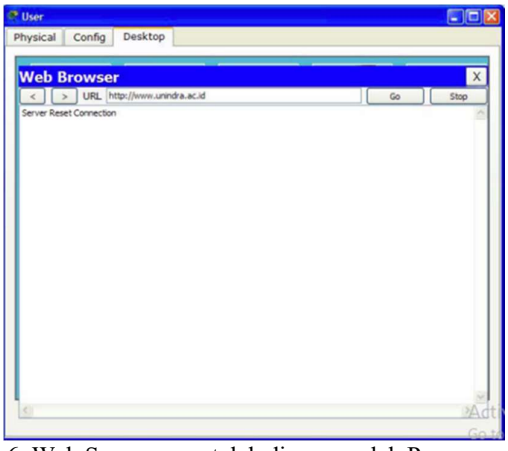


Gambar 4. Web Yang Telah Berhasil Diakses Oleh User

Setelah melakukan test ping, user pun bisa melakukan test pada website yang telah dibuat. Pada gambar 4 diatas adalah website sebelum terjadinya serangan DDOS.



Gambar 5. Test Ping User Ketika Serangan Telah Terjadi



Gambar 6. Web Server yang telah diserang oleh Penyerang DDOS

Setelah terjadinya penyerangan, user pun tak dapat membuka website tersebut. 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. Adapun 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.

5. KESIMPULAN

Aplikasi penjualan sepatu berbasis web ini tentunya bisa dijadikan sebagai solusi dari permasalahan yang ada. Dengan adanya aplikasi ini akan sangat bermanfaat dalam mempromosikan produk ke jangkauan yang lebih luas, dapat meningkatkan kualitas pelayanan pelanggan, berjualan melalui internet agar dapat menjangkau kapan saja, dimana saja dan meningkatkan kemampuan persaingan usaha. Selain itu, aplikasi web penjualan sepatu ini digunakan sebagai sarana untuk menyimpan dan mengelola data transaksi jual beli bagi pemilik agar berjalan lebih efisien dan efektif dalam mengembangkan usaha. Berdasarkan hasil penelitian analisis keamanan komputer terhadap serangan DDoS diperoleh Kesimpulan bahwa DDoS adalah salah satu jenis serangan aktif, yaitu serangan yang dapat menyebabkan hilangnya data dan habisnya daya yang dimiliki suatu sistem dengan cara membanjiri traffic jaringan suatu komputer atau server sehingga layanan user terganggu. Lebih lanjut lagi, Salah satu pencegahan serangan ini ialah Gunakan firewall yang dapat mengatasi masalah serangan ini, Cara lain adalah dengan memperbesar jumlah maksimum koneksi syn yang dapat berlangsung ke server. Salah satu bentuk cara penyerangan DDOS adalah ialah dengan menggunakan perintah ping. 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 computer korban

REFERENCES

[1] Mufadhol (2012) "SimulasiSimulation, T., Network, C., & Tracer, C. P. (n.d.). Simulasi jaringan komputer menggunakan cisco packet tracer (. jaringan komputer menggunakan cisco packet tracer (," Mufadhol.
[2] Santoso, K. (2016) "Konfigurasi dan Analisis Performansi Routing OSPF pada Jaringan LAN dengan Simulator Cisco Packet Tracer Versi 6.2," Jurnal Kajian Teknik Elektro, 1(1), pp. 67–78.
[3] Satmoko, D. B., Sukarno, P. and Jadied, E. M. (2018) "Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square," e-Proceeding of Engineering, 5(3), pp. 7877–7985.
[4] Siregar, J. J. (2013) "Analisis Explotasi Keamanan Web Denial of Service Attack," ComTech: Computer, Mathematics and Engineering Applications, 4(2), p. 1199. doi: 10.21512/comtech.v4i2.2597.
[5] Winanto, C. A. (2016) "Deteksi serangan Denial of Service mengunakan Artificial Immune System," Computer Engineering, 2(Faculty of Computer Science, Sriwijaya University), pp. 456–459.