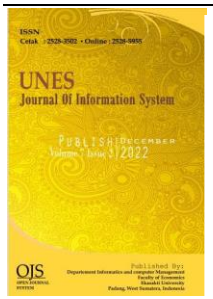


UNES Journal of Information System

Volume 8, Issue 1, December 2023

P-ISSN 2528-3502

E-ISSN 2528-5955

Open Access at: https://fe.ekasakti.org/index.php/UJIS

ANCAMAN DENIAL OF SERVICE ATTACK DALAM EKSPLOITASI KEAMANAN SISTEM INFORMASI

THREAT OF DENIAL OF SERVICE ATTACK IN INFORMATION SYSTEM SECURITY EXPLOITATION

Erwin Ginting[1], Jessima[2], Putri Sahara[3], Siti Nurhaliza Tambunan[4]

[1,2,3,4)] Program Studi Sistem Informasi Fakultas Teknik dan Ilmu Komputer Universitas Potensi Utama.

E-mail: erwinginting82@gmail.com[1], jessimaj522@gmail.com[2], syhrputry00@gmail.com[3], nurhalizatambunans@gmail.com[4].

INFO ARTIKEL

Koresponden:

Erwin Ginting

erwinginting82@gmail.com

Kata kunci

Ancaman, Keamanan, Eksploitasi, Denial of Service attack.

Website: https://fe.ekasakti.org/index.php/UJIS

Hal: 009 - 019

ABSTRAK

Banyak ancaman atau serangan eksploitasi yang terjadi didalam keamanan sistem informasi salah satunya adalah penyerangan dengan menggunakan Denial of Service attack (Dos). Walaupun keamanan sistem informasi terkait sebuah data memiliki pengamanan yang kuat, hal itu tidak menjamin bebas dari ancaman serangan. Denial of Service attack merupakan bentuk ancaman penyerangan eksploitasi yang dilakukan untuk mengeksploitasi sebuah komputer ataupun server didalam jaringan internet dengan cara menghabiskan sumber dan melumpuhkan sistem yang dijadikan sasaran, sehingga sistem tersebut tidak dapat menyediakan berbagai servis yang diminta. Jurnal ini bertujuan untuk memberikan pemahaman keamanan sistem informasi mengenai berbagai ancaman eksploitasi keamanan sistem informasi terutama ancaman serangan DoS dan memberikan solusi pencegahan yang dapat digunakan. Dengan menggunakan metode Literatur studi pustaka hasil jurnal ini menemukan pencegahanan terhadap penyerangan DoS. Kesimpulan yang di dapat adalah mengetahui keamanan sistem informasi dalam menjaga suatu kerahasiaan data dan informasi dari ancaman eksploitasi keamanan sistem informasi, serta mengetahui bagaimana pencegahan yang dapat dilakukan untuk menghindari serangan Denial of Service attack.

ARTICLE INFO

Corresponden:
Erwin Ginting
erwinginting82@gmail.com

Keywords:
Threats, Security, Exploits, Denial of Service attacks

Website:
https://fe.ekasakti.org/index.php/UJIS

Page: **009 – 019**

ABSTRACT

There are many threats or exploitation attacks that occur in information system security, one of which is an attack using a Denial of Service attack (DoS). Even though information system security related to data has strong security, it does not guarantee that it is free from the threat of attack. Denial of Service attack is a form of exploitation attack threat that is carried out to exploit a computer or server in the internet network by consuming resources and paralyzing the target system, so that the system cannot provide the various services requested. This journal aims to provide an understanding of information system security regarding various threats of information system security exploitation, especially the threat of DoS attacks and provide preventive solutions that can be used. By using the literature study method, the results of this journal found prevention against DoS attacks. The conclusion that can be drawn is to know the security of information systems in maintaining the confidentiality of data and information from the threat of exploitation of information system security, and to know how prevention can be done to avoid Denial of Service attacks.

PENDAHULUAN

Saat ini keamanan sistem informasi merupakan salah satu bagian terpenting didalam seluruh aspek dalam mengamankan berbagai data dan informasi penting. Keamanan sistem informasi adalah suatu cara perlindungan terhadap segala jenis sumber daya informasi dari penyalahgunaan pihak yang tidak memiliki wewenang dalam mengelolanya dan bertujuan untuk memastikan bahwa pengguna yang mengakses data adalah pihak yang benar-benar memiliki hak atas data dan informasi tersebut.

Pada jurnal ini akan membahas salah satu permasalahan yang ada pada keamanan sistem informasi yaitu eksploitasi terhadap keamanan sistem informasi. Eksploitasi sendiri berarti bersikap atau berperilaku yang diskriminatif dengan sewenang-wenang (Suharto).

Eksploitasi keamanan sistem informasi adalah suatu tindakan diskriminatif yang menyerang sebuah sistem atau server yang menyebabkan kerugian bagi siapa saja yang mengalami penyerangan tersebut. Oleh karena itu, walaupun sudah digunakannya keamanan sistem informasi dalam mengamankan data dan informasi penting, itu tidak menjamin sepenuhnya data atau informasi tersebut terbebas dari berbagai serangan yang akan terjadi pada kemudian hari.

Pembuatan jurnal ini bertujuan untuk memberikan pemahaman seputar keamanan sistem informasi mengenai berbagai ancaman eksploitasi keamanan sistem informasi terutama ancaman serangan dan memberikan solusi yang dapat digunakan sebagai pencegahan terjadinya DoS.

METODE PENELITIAN

Metode yang digunakan dalam pembuatan jurnal ini adalah metode penelitian kualitatif dengan menggunakan literatur studi pustaka. Dengan menggunakan beberapa sumber bacaan mengenai pembahasan serupa terkait ancaman dan eksploitasi keamanan sistem informasi serta DoS sehingga dapat menyusun jurnal ini. Sumber-sumber yang dijadikan acuan pembuatan jurnal ini seperti penelitian terdahulu, jurnal, ataupun buku-buku yang berhubungan dengan ancaman, keamanan sistem informasi, dan eksploitasi DoS. Melalui berbagai sumber referensi tersebut diharapkan dapat dijadikan sebagai landasan teoritis yang kuat karena relevan dengan jurnal ini. Setelah dilakukannya literatur studi pustaka maka akan diperoleh berbagai data dan informasi mengenai Denial of Service attack yang dimana selanjutnya data dan informasi tersebut dapat digunakan sebagai bahan untuk menganalisis dan mengetahui lebih mendalam lagi serta menemukan pencegahan Denial of Service attack (DoS).

HASIL DAN PEMBAHASAN

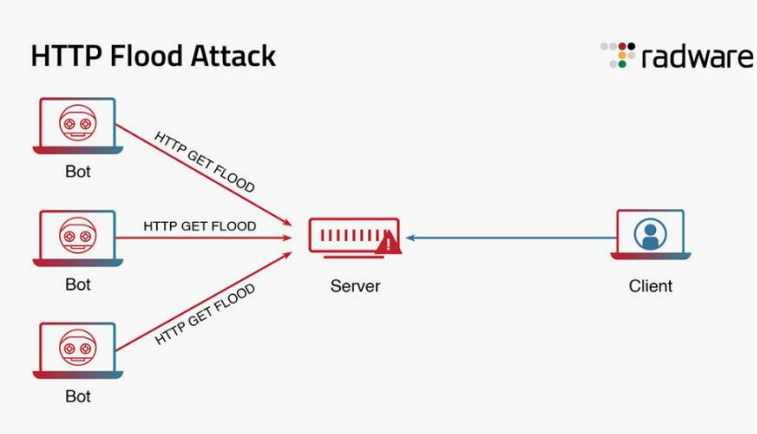
Denial of Service attack (DoS) merupakan bentuk ancaman penyerangan yang bertujuan untuk mengeksploitasi sebuah komputer ataupun server didalam jaringan internet dengan cara menghabiskan sumber dan melumpuhkan sistem yang dijadikan sasaran, sehingga sistem tersebut tidak dapat menyediakan berbagai servis yang diminta oleh pengguna. Dapat disimpulkan juga bahwa DoS memberhentikan suatu server atau sistem yang menyebabkan server atau sistem itu tidak berguna.

A. Bentuk-Bentuk Denial of Service attack

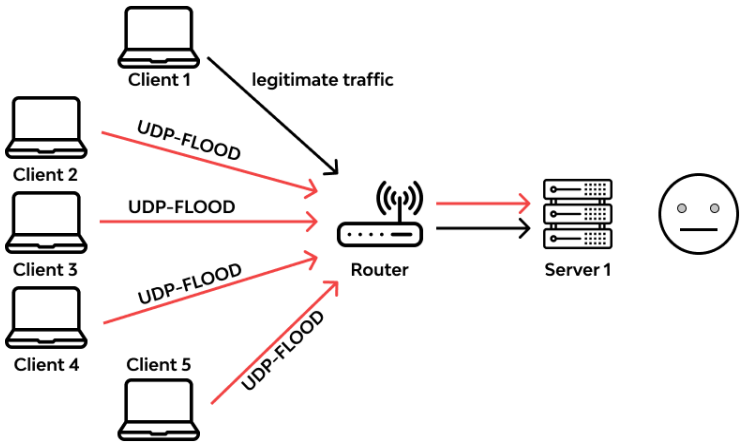
Berbagai bentuk-bentuk umum Denial of Service attack antara lain:

1. **Serangan Flood**

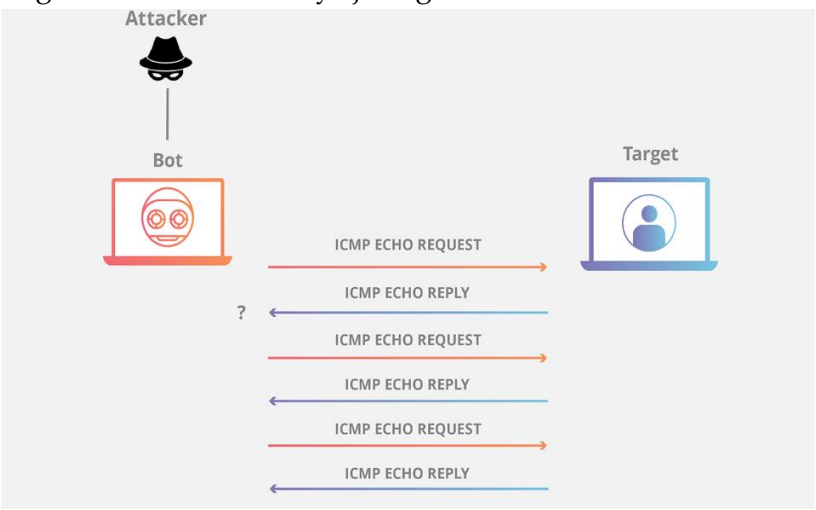
   Serangan ini melibatkan pengiriman lalu lintas yang berlebihan ke jaringan atau sistem target. Serangan ini bertujuan untuk menghabiskan sumber daya jaringan, seperti bandwidth, memori, atau daya pemrosesan, sehingga sistem menjadi tidak responsif terhadap pengguna yang sah.



2. **Serangan Flood UDP**
   Pengirim mengirimkan banyak paket UDP palsu ke target untuk menghabiskan sumber daya jaringan.

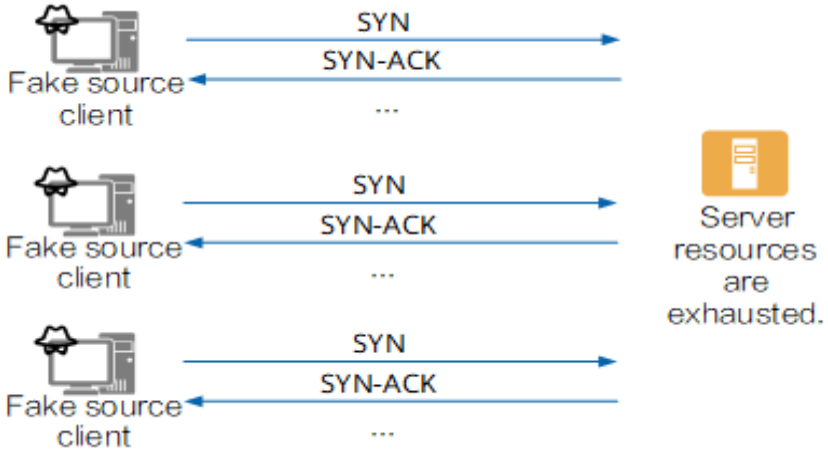


3. **Serangan Flood ICMP**
   Pengirim mengirimkan banyak permintaan ICMP Echo (ping) palsu ke target untuk menghabiskan sumber daya jaringan.



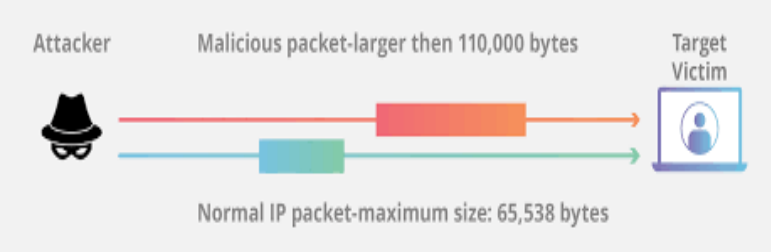
4. **Serangan SYN Flood**

Serangan ini mengeksploitasi kerentanan dalam mekanisme protokol TCP (Transmission Control Protocol) untuk mengirimkan banyak permintaan koneksi SYN palsu ke target. Hal ini menyebabkan target kehabisan sumber daya dalam menangani permintaan koneksi dan mengakibatkan penolakan akses ke layanan yang sah.



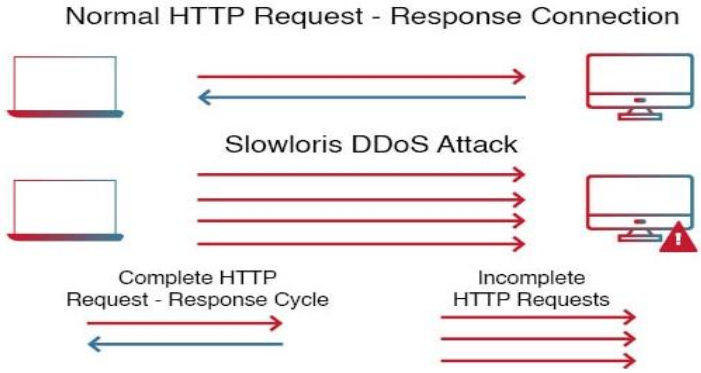
5. **Serangan Ping of Death**

Serangan ini melibatkan pengiriman paket ping (ICMP) yang sangat besar atau yang mengandung data yang salah ke target. Paket yang terlalu besar dapat menyebabkan sistem atau perangkat jaringan mengalami kegagalan atau kecelakaan.



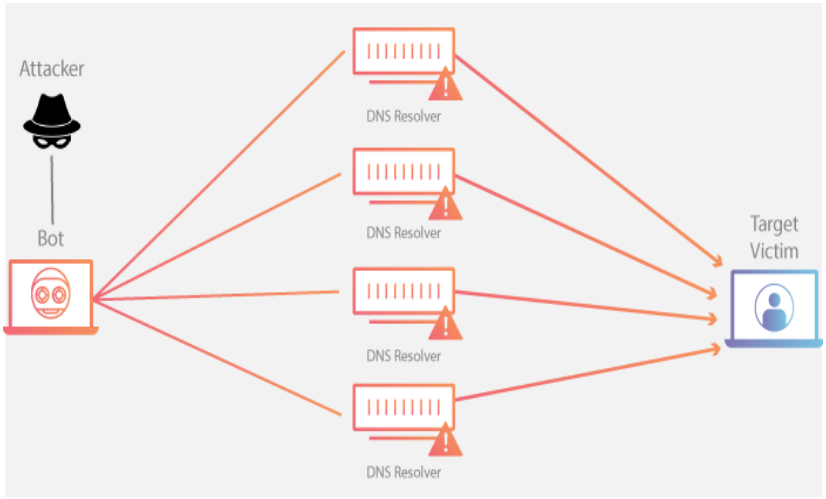
6. **Serangan Slowloris**

Serangan ini melibatkan pengiriman permintaan HTTP yang tidak lengkap atau sangat lambat ke server web target. Serangan ini bertujuan untuk mempertahankan koneksi terbuka dengan server dan menghabiskan sumber daya server yang tersedia, seperti slot koneksi atau memori.



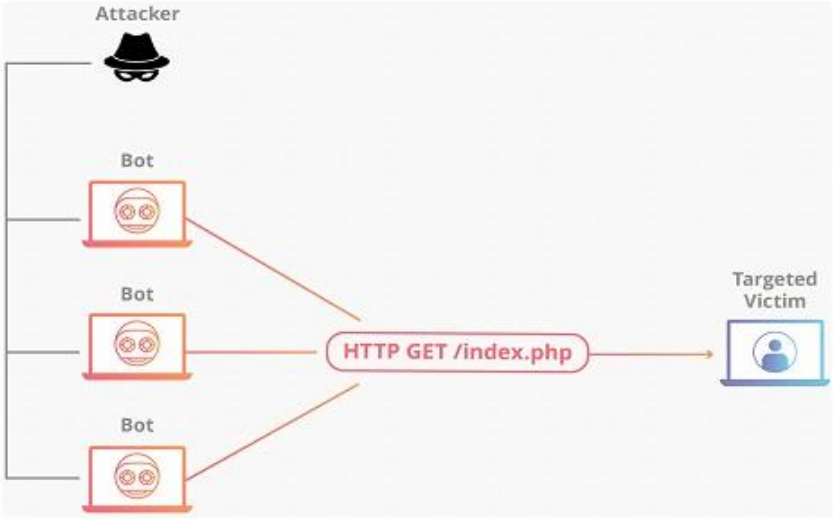
7. **Serangan DNS Amplification**

Serangan ini melibatkan pengiriman permintaan DNS yang sangat besar dengan menggunakan alamat IP palsu sebagai sumber permintaan. Permintaan DNS besar ini akan diarahkan ke server yang menjadi target, menghabiskan sumber daya server dan mengganggu layanan DNS yang sah.



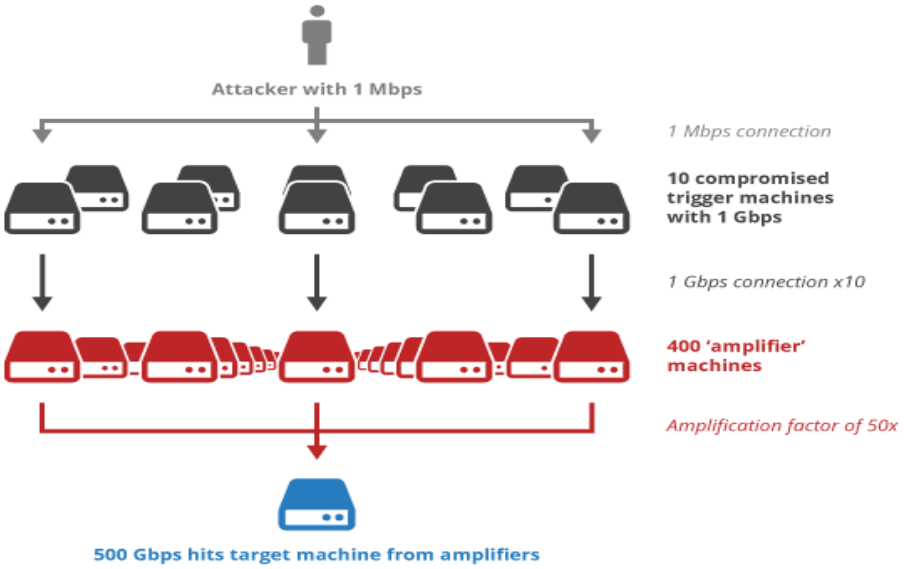
8. **Serangan Distribusi Denial of Service (DDoS)**

DDoS melibatkan serangan DoS yang dilakukan secara bersamaan dari banyak sumber yang terdistribusi di seluruh jaringan. DDoS sering melibatkan penggunaan botnet, yaitu jaringan komputer yang telah terinfeksi dan dikendalikan oleh penyerang.



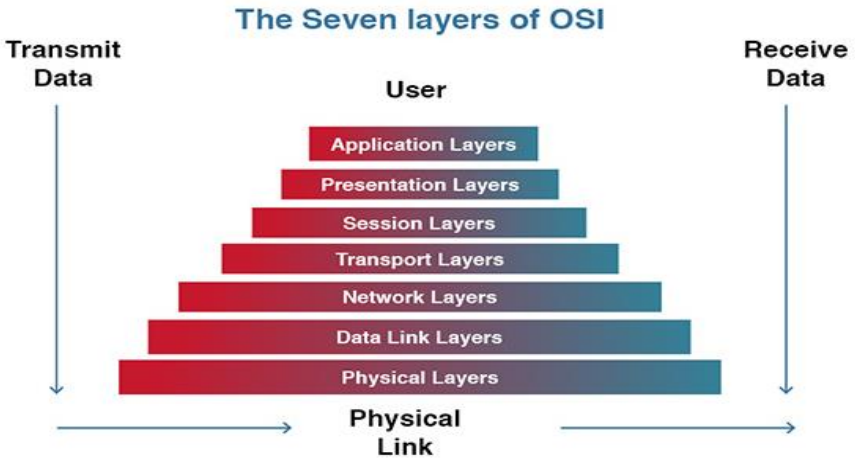
9. **Serangan Amplification**

Serangan ini menggunakan layanan yang dapat mengirimkan respon yang jauh lebih besar daripada permintaan yang dikirim oleh penyerang. Serangan ini memanfaatkan kerentanan dalam protokol yang digunakan, seperti NTP (Network Time Protocol) atau SNMP (Simple Network Management Protocol).



10. Serangan Application Layer (Layer 7)

Serangan ini bertujuan untuk mengganggu atau meniadakan layanan pada tingkat aplikasi. Contoh serangan ini termasuk serangan HTTP GET/POST, serangan SQL injection, atau serangan XSS (Cross-Site Scripting).



B. Motif Denial of Service attack (DoS)

Beberapa motif para pelaku DoS antara lain:

1. Untuk mendapatkan akses sasaran yang dituju secara gratis.
2. Sebagai wadah balas dendam terhadap serangan yang mungkin pernah dilakukan terhadapnya.
3. Untuk menjatuhkan jaringan yang menyebabkan kericuhan server yang diserang, misalnya pada server atau sistem pemerintahan.
4. Untuk menjatuhkan website penjualan online agar korban mengalami kerugian.
5. Untuk menunjukkan bakatnya dalam menyerang sebuah server atau sistem.

C. Dampak Denial of Service attack (DoS)

Serangan Denial of Service attack merupakan serangan yang melumpuhkan suatu layanan yang dibutuhkan oleh pengguna sehingga berdampak habisnya resource pada komputer yang diserang.

Resource yang dihabiskan oleh DoS yaitu:

1. Bandwidth
2. Kernel Tables
3. RAM
4. Disk
5. INETD

D. Kasus Denial of Service attack (DoS)

1. Kasus yang pernah terjadi di Indonesia

Serangan oleh anak komunitas YogyaFree terhadap website kaskus pada tahun 2008. Serangan ini berlangsung pada 16-17 Mei 2008. Serangan yang dilakukan oleh komunitas yogyafree ini mengakibatkan situs kaskus tidak dapat di akses dan corrupt. Penyerangan ini mengakibatkan thread-thread yang telah dibuat terpaksa dikunci (locked) oleh administrator kaskus. Karena hal ini berlangsung cukup lama akhirnya administrator kaskus terpaksa mematikan server kaskus. Penyerangan ini meruapakan balasan dari komunitas yogyafree terhadap kaskus, menurut sumber penyerangan ini dilakukan karena yogyafree telah dicela pada salah satu forum di kaskus. Beberapa waktu terjadilah pertikaian antara dua komunitas ini. Dari kejadian ini kaskus meluncurkan server baru yang lebih dilengkapi dengan pengamanan data yang tangguh dan siap untuk menghadapi berbagai serangan dari berbagai pihak.

2. Kasus yang pernah terjadi di dunia

Insiden yang menyerang DDOS juga terjadi pada pertengahan tahun 2009 dimana domain.co.id sempat drop selama 4 hari akibat serangan DDOS. Hal ini menunjukkan adanya kelemahan yang sangat mendasar dalam sistem DNS CCTLD-ID. Situasi ini sangat berbahaya mengingat domain.co.id merupakan salah satu infrastruktur Internet Indonesia yang strategis. Kegagalan sistem DNS CCTLD-ID berpotensi menimbulkan kerugian ekonomi. Karena domain drop otomatis para pengguna tidak dapat mengakses situs dengan domain.co.id bagi pengguna email di yahoo.co.id. tidak dapat mengakses emailnya karena domainnya telah down. Beberapa saat setelah kejadian tersebut administrator diberitakan melakukan maintenance terhadap system keamanan domain tersebut dan sampai sekarang masih dapat dinikmati oleh masyarakat.

Pada tahun 2016 juga terjadi serangan terhadap Dyn pada tahun 2016 yang menyebabkan gangguan akses ke banyak situs web terkenal di seluruh dunia.

E. Pencegahan Denial of Service attack (DoS)

Berikut adalah beberapa langkah yang dapat diambil untuk menghindari serangan DoS:

1. **Gunakan Firewall yang Kuat**
   Pastikan sistem Anda dilindungi dengan firewall yang kuat yang dapat membatasi akses yang tidak sah ke jaringan atau sistem Anda. Konfigurasikan firewall dengan baik untuk memblokir lalu lintas yang mencurigakan.
2. **Perbarui Sistem dan Aplikasi**
   Selalu perbarui sistem operasi, perangkat lunak, dan aplikasi dengan versi terbaru yang telah dirilis oleh penyedia. Pembaruan ini sering mengatasi kerentanan keamanan yang dapat dimanfaatkan oleh serangan DoS.
3. **Gunakan Sistem Deteksi Intrusi (IDS) dan Sistem Pencegahan Intrusi (IPS)**
   Gunakan perangkat lunak IDS dan IPS yang dapat mendeteksi serangan DoS secara real-time. IDS akan memantau lalu lintas jaringan untuk mencari pola serangan yang mencurigakan, sedangkan IPS dapat mengambil tindakan otomatis untuk memblokir serangan yang terdeteksi.
4. **Batasi Koneksi Bersamaan**
   Batasi jumlah koneksi yang diizinkan ke server atau jaringan Anda. Dengan membatasi jumlah koneksi bersamaan, Anda dapat mengurangi risiko serangan DoS yang menghabiskan sumber daya server.
5. **Gunakan Layanan Penyedia CDN**
   Content Delivery Network (CDN) dapat membantu melindungi situs web Anda dari serangan DoS dengan mendistribusikan lalu lintas di berbagai server di lokasi geografis yang berbeda. Ini membantu mengurangi beban pada server Anda dan membuatnya lebih tahan terhadap serangan DoS.
6. **Implementasikan Pembatasan Bandwidth**
   Batasi jumlah bandwidth yang dapat digunakan oleh setiap koneksi atau alamat IP. Dengan membatasi bandwidth, Anda dapat memastikan bahwa satu entitas tidak dapat menghabiskan semua sumber daya jaringan Anda.
7. **Gunakan Layanan Anti-DdoS**
   Pertimbangkan untuk menggunakan layanan penyedia Anti-DDoS yang mengkhususkan diri dalam melindungi jaringan dari serangan DoS. Layanan ini dapat membantu memblokir serangan DoS sebelum mencapai jaringan Anda dan memberikan lalu lintas yang bersih ke server Anda.
8. **Tingkatkan Kapasitas Infrastruktur**
   Jika serangan DoS yang terjadi terlalu kuat untuk ditangani oleh sistem Anda, pertimbangkan untuk meningkatkan kapasitas infrastruktur Anda. Ini bisa berarti meningkatkan kecepatan internet, meningkatkan kapasitas server, atau menggunakan layanan cloud yang skalabel.
9. **Tinjau Konfigurasi Sistem**
   Pastikan konfigurasi sistem Anda diatur dengan baik dan hanya memungkinkan lalu lintas yang diperlukan. Nonaktifkan layanan atau protokol yang tidak digunakan agar tidak menjadi target serangan.
10. **Pendidikan dan Kesadaran Pengguna**
    Tingkatkan kesadaran pengguna Anda tentang serangan DoS dan praktik keamanan yang baik. Berikan pelatihan kepada karyawan Anda tentang tanda-

tanda serangan DoS dan langkah-langkah yang harus diambil dalam menghadapinya.

SIMPULAN

Berdasarkan penjabaran jurnal diatas maka dapat ditarik kesimpulan bahwa seluruh data dan informasi yang sudah dianggap terjamin keamanannya dan bebas dari berbagai ancaman serangan ternyata tidak sepenuhnya. Salah satunya serangan yang cukup terkenal adalah Denial of Service attack (DoS). Denial of Service attack (DoS) merupakan bentuk ancaman penyerangan yang bertujuan untuk mengeksploitasi sebuah komputer ataupun server didalam jaringan internet dengan cara menghabiskan sumber dan melumpuhkan sistem yang dijadikan sasaran, sehingga sistem tersebut tidak dapat menyediakan berbagai servis yang diminta oleh pengguna.

Denial of Service attack (DoS) bukan ancaman serangan yang dapat dihapuskan secara permanen. Namun untuk mencegah terjadinya penyerangan DoS terhadap data, informasi, atau server yang dimiliki dapat melakukan berbagai tahapan yang sudah dijelaskan sebelumnya. Motif serangan DoS salah satunya adalah untuk mendapatkan akses sasaran yang dituju secara gratis serta membuat server yang diakses down sehingga menyebabkan kerugian.

DAFTAR PUSTAKA

Siregar, J. J. (2013). Analisis explotasi keamanan web denial of service attack. ComTech: Computer, Mathematics and Engineering Applications, 4(2), 1199-1205.

Vanderma, R. D., & Mallisza, D. (2023). APLIKASI PENJADWALAN ANTAR JEMPUT LAUNDRY BERBASIS WEB PADA SAVA LAUNDRY. Jurnal Manajemen Teknologi Informatika, 1(1), 34-47.

Weriza, J., Malisza, D., Dahri, N., & Susanti, M. (2021). RESTAURANT MENU DESIGN MUARO NEW SAND JAMAK. Dinasti International Journal of Digital Business Management, 2(6), 1063-1069.

Hartanto, S. (2013). Penanganan Serangan Penolakan Layanan (Denial of Service Attack) Dalam Jaringan Berbasis IP. Jurnal Elektrokrisna, 1(3), 133-144.

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). Jurnal Sistim Informasi dan Teknologi, 115-123.

Walad, S. I., Zarlis, M., & Efendi, M. I. S. (2021, March). Analysis of denial of service attack on web security systems. In Journal of Physics: Conference Series (Vol. 1811, No. 1, p. 012127). IOP Publishing.

Fanani, G., & Riadi, I. (2020). Analysis of Digital Evidence on Denial of Service (DoS) Attack Log Based. Buletin Ilmiah Sarjana Teknik Elektro, 2(2), 70-74.

Dwiyatno, S., Sari, A. P., Irawan, A., & Safig, S. (2019). Pendeteksi Serangan Ddos (Distributed Denial of Service) Menggunakan Honeypot di PT. Torini Jaya Abadi. Jurnal Sistem Informasi dan Informatika (SIMIKA), 2(2), 64-80.

Azmi, A. Y. F., AG, J. G., & Wahyudi, E. (2022). Analisis Network Security pada Layanan Wifi Indihome Terhadap Serangan Denial of Service (DOS). Jurnal Litek: Jurnal Listrik Telekomunikasi Elektronika, 19(1), 8-12.

Shakti, K. W. (2021). Implementasi Intrusion Prevention System (IPS) Untuk Mengatasi Serangan Distributed Denial Of Services (DDOS) Pada Website (Doctoral dissertation, Institut Teknologi Telkom Purwokerto).

Kohar, A., & Putro, H. P. (2014). Ancaman Keamanan pada Sistem Informasi Manajemen Rumah Sakit. In *Seminar Nasional Informatika Medis (SNIMed)*.

Fauzi, R., Muhyidin, Y., & Singasatia, D. (2023). Sistem Keamanan Jaringan Komputer Berbasis Teknik Intrusion Detection System (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS). *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, *7*(1), 72-86.

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding Sains dan Teknologi*, *2*(1), 216-221.