OPTIMALISASI KINERJA WEB SERVER DALAM MENANGANI SERANG DDOS

Velen Shinta Pramesti[1], Febi Wulan Dini[2], Glanes Cindy Terampe[3]
velenshinta.31@gmail.com[1], febiwulandini004@gmail.com[2], glanesscindy@gmail.com[3],
Universitas Teknologi Yogyakarta

ABSTRAK

Serangan Distributed Denial of Service (DDoS) merupakan ancaman serius bagi infrastruktur web server, yang dapat menyebabkan gangguan layanan dan kerugian finansial yang signifikan. Untuk mengatasi risiko ini, penelitian ini bertujuan untuk mengoptimalkan kinerja web server dalam menghadapi serangan DDoS. Metodologi penelitian ini mencakup pemodelan serangan DDoS, implementasi teknik mitigasi, dan evaluasi kinerja web server melalui serangkaian pengujian eksperimental. Kami menggunakan simulasi serangan DDoS di lingkungan laboratorium untuk mengukur kinerja web server sebelum dan setelah penerapan strategi mitigasi, termasuk tuning konfigurasi server dan penggunaan alat pengamanan. Hasil penelitian menunjukkan bahwa dengan menerapkan strategi yang tepat, kinerja web server dapat ditingkatkan secara signifikan dalam menghadapi serangan DDoS, dengan mengurangi waktu tanggap dan mempertahankan ketersediaan layanan. Implikasi praktis dari penelitian ini adalah adopsi strategi mitigasi yang efektif untuk meningkatkan ketahanan infrastruktur web terhadap serangan DDoS. Temuan ini memberikan kontribusi penting untuk pemahaman tentang strategi optimal dalam memperkuat keamanan web server dan infrastruktur online lainnya.
Kata Kunci*:* DDoS Mitigation, Traffic Filtering, Load Balancing

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a serious threat to web server infrastructure, which can cause service disruptions and significant financial losses. To overcome this risk, this research aims to optimize web server performance in the face of DDoS attacks. This research methodology includes modeling DDoS attacks, implementing mitigation techniques, and evaluating web server performance through a series of experimental tests. We used simulated DDoS attacks in a laboratory environment to measure web server performance before and after implementing mitigation strategies, including tuning server configurations and using security tools. The research results show that by implementing the right strategy, web server performance can be significantly improved in the face of DDoS attacks, by reducing response time and maintaining service availability. The practical implication of this research is the adoption of effective mitigation strategies to increase the resilience of web infrastructure against DDoS attacks. These findings provide an important contribution to the understanding of optimal strategies for strengthening the security of web servers and other online infrastructure.
Keywords: *DDoS Mitigation, Traffic Filtering, Load Balancing.*

PENDAHULUAN

Latar belakang

Web server adalah salah satu jenis server yang khusus ditujukan untuk ditujukan untuk menyediakan layanan permintaan di web. Bekerja dengan cara menyimpan, memproses, dan mengirimkan file dari website ke komputer klien yang memintanya.

Dalam penggunaan web server terdapat beberapa masalah salah satunya serangan

DDOS. Serangan DDos adalah serangan yang menyebabkan web server tidak dapat diakses oleh pengguna yang dituju dengan memberikan permintaan yang berlebihan agar sistem terbebani dan membuat beberapa permintaan tidak terpenuhi.

Serangan DDOS muncul pada tahun 1999, tiga tahun setelah serangan DDOS klasik muncul, yang memakai tehnik SYN Flooding, yang menyebabkan beberapa web server internet mengalami down time. Awal Februarii 2000, serangan besar telah terjadi, mengakibatkan beberapa situs web terkenal Amazon, eBay, CNN, dan Yahoo! downtime beberapa jam. Kemudian terdapat serangan lagi yang terjadi pada bulan Oktober 2002 ketika 9 dari 13 root DNS Server diserang DDOS yang besar yang disebut dengan Ping Flood. Hal tersebut menyebabkan beberapa server tersebut pada tiap detiknya menerima lebih dari 150.000 request paket Internet Control Message Protocol (ICMP).

Rumusan Masalah

1. Bagaimana dampak serangan ddos dalam kinerja web server?
2. Apa saja teknik & metode yang umumnya digunakan untuk mencegah serangan ddos pada web server.
3. Bagaimana efektivitas teknik2 mintigasi dalam mengatasi serangan ddos terhadap kinerja web server?

Tujuan

1. Menganalisis dampak serangan DDoS terhadap kinerja web server dalam konteks kehilangan ketersedian layanan, penuruna kinerja, dan potensi kerusakan data.

Mempelajari teknik dan metode deteksi ddos yang sudah ada serta menganalisis kelebihan dan kekurangan nya dalam mendeteksi serangan dengan cepat dan akurat

METODOLOGI

Web server

Web server atau server web adalah perangkat lunak pada server yang berfungsi untuk menerima permintaan di halaman web melalui protokol HTTP dan HTTPs dari client yang sering disebut brower, setelah itu mengirimkan hasil permintaan dalam bentuk halaman web yang berbentuk sebuah dokumen HTML.

Serangan DDoS

DDoS (Distributed Denial of Service) adalah serangan yang menggangu hak akses milik pengguna server yang dilakukan secara masif. Secara umum serangan DDoS terdapat beberapa jenis, serangan dengan basis bandwidth, basis lalu lintas jaringan, dan basis aplikasi.

Serangan DDOS dilakukan dengan menghambat atau memutus ketersedian informasi. Serangan ini dilakukan oleh hacker/penyerang dengan cara mengirim banyak sekali layanan permintaan sehingga server terhambat dalam menerima permintaan lain. Apabila serangan DOS dilakukan secara terdistribusi maka serangan tersebut dikenal dengan nama Distributed Denial of Service attack (DDOS). Konsep dari serangan DDOS adalah attacker (penyerang) dapat menyerang beberapa jaringan server, kemudian server yang sudah diserang akan mengendalikan server – server yang lain secara terdistribusi untuk menghambat atau bahkan meniadakan ketersedian informasi dari korban.

Contoh website yang mengalami serangan DDOS adalah Ebay, CNN.com, Amazon, dan Yahoo.com. Karena hebatnya dampak dari serangan DDOS, sehingga website-

website tersebut mengalami kerugian untuk menangani serangan ini. Oleh karena itu, sangat dibutuhkan teknik pencegahan untuk mencegah dan mendeteksi serangan DDOS ini.

ICMP

(Internet Control Message Protocol) termasuk inti dari protokol internet. ICMP digunakan oleh sistem jaringan komputer untuk mengirim pesan. Berbeda dengan TCP dan UDP, ICMP digunakan tidak secara langsung oleh aplikasi jaringan pengguna. Salah satu pengecualian adalah aplikasi ping yang dapat mengirim (echo reply) dan menerima (echo request) pesan, untuk mengetahui apakah komputer tujuan dapat menerima dan menentukan waktu yang dibutuhkan paket yang dikirim dapat dibalas oleh komputer tujuan.

HASIL DAN PEMBAHASAN

Serangan DDoS merupakan tantangan yang kompleks karena sulit dideteksi dan sulit diatasi tanpa mengganggu layanan yang seharusnya diberikan kepada pengguna yang sah. Bahkan, dalam beberapa kasus, para penyerang dapat menggunakan infrastruktur yang sah, seperti server Yahoo, untuk melancarkan serangan mereka, membuat tugas administrator jaringan semakin rumit. Kebijakan untuk mengatasi serangan DDoS seringkali memerlukan keseimbangan antara keamanan dan kenyamanan pengguna. Meskipun langkahlangkah pengamanan yang ketat dapat membantu melindungi infrastruktur jaringan dari serangan, tetapi juga berpotensi mengganggu layanan yang sah. Oleh karena itu, para administrator jaringan harus bijaksana dalam merancang strategi mitigasi yang efektif tanpa mengorbankan pengalaman pengguna yang positif.

KESIMPULAN

Penelitian ini menunjukkan betapa pentingnya meningkatkan kinerja web server dalam menghadapi serangan DDoS. Dengan menerapkan teknik mitigasi yang tepat, kami berhasil meningkatkan ketahanan web server terhadap serangan DDoS. Hal ini dapat memberikan pemahaman lebih baik tentang bagaimana melindungi infrastruktur online dari serangan cyber yang merusak. Diharapkan hasil ini dapat membantu dalam mengembangkan solusi yang lebih baik untuk melindungi layanan online dan menjaga ketersediaan internet bagi pengguna.

DAFTAR PUSTAKA

Ridho.A.M., & Arman.M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan, Jurnal SISFOKOM
(sistem Informasi dan Komputer), 09, 373-379.
(Arman.A., & Rachmat.A. (2020). Implementasi Sistem Kemanan Web server Menggunakan Pesense. Jurnal
Sistem Komputer Musirawas, 05,
13 -23
Hermawan.R. (2015). Analisis Konsep dan
Cara Kerja Serangan Komputer Distributed Denial Of Service (DDoS). Jurnal Universitas Indraprasta PGRI, 5,
1- 14
Tantriawan.H., Yunmar.R.A., Setiawan.

A.,& Suryadi.M. (2021).Deteksi Distributed Denial of Service (DDos) Menggunakan Fuzzy Logic Sugeno. Indonesian Journal Of Machine Learning and Computer Science, 1, 144 - 154.
Junaedi.R.F. 2018. Kemanan Jaringan Komputer. Ilmu Komunikasi Universitas Sriwijaya, 2 - 4..