REMEDIASI SERANGAN DDOS MENGGUNAKAN TRAFFIC LIMITER PADA FLASK API

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

MUHAMMAD SABIRIN

20.83.0491

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

HALAMAN PERSETUJUAN

SKRIPSI

REMEDIASI SERANGAN DDOS MENGGUNAKAN TRAFFIC LIMITER PADA FLASK API

yang disusun dan diajukan oleh

MUHAMMAD SABIRIN

20.83.0491

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 16 Oktober 2024

Dosen Pembimbing,

WAHID MIFTAHUL ASHARI, S.Kom., M.T
NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

REMEDIASI SERANGAN DDOS MENGGUNAKAN TRAFFIC LIMITER PADA FLASK API

yang disusun dan diajukan oleh

MUHAMMAD SABIRIN

20.83.0491

Telah dipertahankan di depan Dewan Penguji
pada tanggal 16 Oktober 2024

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, M.Kom **NIK. 190302456**	
Andika Agus Slameto, M.Kom **NIK. 190302109**	
Wahid Miftahul Ashari, S.Kom., M.T **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : MUHAMMAD SABIRIN
NIM : 20.83.0491

Menyatakan bahwa Skripsi dengan judul berikut:

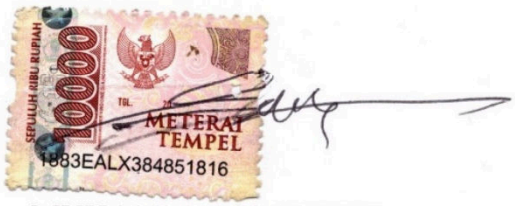
REMEDIASI SERANGAN DDOS MENGGUNAKAN TRAFFIC LIMITER PADA FLASK API

Dosen Pembimbing :
WAHID MIFTAHUL ASHARI, S.Kom., M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta,

Yang Menyatakan,



MUHAMMAD SABIRIN

HALAMAN PERSEMBAHAN

Saya mengucapkan rasa terima kasih dan penghargaan yang setinggi-tingginya kepada kedua orang tua saya atas dukungan dan doa yang tak henti-hentinya diberikan sepanjang perjalanan penulisan skripsi ini. Tanpa bantuan dan dorongan mereka, saya mungkin tidak akan mampu menyelesaikan skripsi ini dengan baik..

KATA PENGANTAR

Segala puji dan syukur penulis haturkan kepada Allah SWT atas izin, rahmat, dan hidaiyah-Nya penulisan skripsi dengan judul "Remediasi Serangan DdoS Menggunakan Traffic Limitter menggunakan Flask API" dapat selesai dengan baik. Penulis berharap hasil penelitian ini dapat memberikan manfaat bagi banyak pihak.

Sholawat serta salam semoga tetap tercurahkan kepada junjungan kita Nabi Muhammad SAW yang senantiasa kita harapkan syafa'atnya di hari akhir. Penyusunan skripsi ini merupakan salah satu syarat untuk memperoleh gelar Strata 1 dalam program studi teknik komputer Universitas Amikom Yogyakarta. Dalam penyusunan skripsi ini berbagai pihak telah memberikan dorongan, bantuan, serta masukan sehingga dalam kesempatan ini penulis menyampaikan terima kasih yang sebesar- besarnya kepada :

1. Alm. Bapak, ibu, dan kakak penulis yang senantiasa memberikan dukungan, do'a, dan motivasi unituk penulis dalam menyelesaikan pendidikan di Universitas Amikom Yogyakarta
2. Bapak Prof. Dr. M. Suyanto, M.M, selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al-Fatta, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Dony Ariyus, M.Kom selaku Kepala Prodi Teknik Komputer
5. Bapak Wahid Miftahul Ashari, S.Kom., M.T selaku dosen pembimbing
6. Surya Pratama dan teman lainnya yang membantu dan mendukung dalam proses menyusun skripsi

Yogyakarta,
Muhammad Sabirin

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

Ω	Tahanan Listrik
μ	Konstanta gesekan
ANFIS	Adaptive Network Fuzzy Inference System
SVM	Support Vector Machines

DAFTAR ISTILAH

Vektor	besaran yang mempunyai arah
Eigen Value	akar akar persamaan

INTISARI

Serangan Distributed Denial-of-Service (DDoS) merupakan ancaman signifikan bagi aplikasi web modern, termasuk API Flask yang sering digunakan dalam pengembangan aplikasi web berbasis Python. Penelitian ini mengajukan serta mengimplementasikan solusi untuk meredam serangan DDoS melalui penggunaan traffic limiter pada API Flask. Traffic limiter berfungsi untuk mengatur dan membatasi jumlah permintaan yang dapat diterima oleh API dalam jangka waktu tertentu. Pendekatan ini terbukti efektif dalam mengurangi dampak serangan DDoS dengan memastikan hanya permintaan yang sah dan sesuai batas yang telah ditentukan yang dapat dieksekusi.

Penelitian ini mencakup langkah-langkah implementasi traffic limiter secara konkret menggunakan berbagai pustaka Python yang tersedia, serta integrasinya dengan API Flask. Evaluasi dilakukan melalui simulasi serangan DDoS dan pengujian kinerja pada sistem yang telah diimplementasikan. Hasil pengujian menunjukkan bahwa traffic limiter mampu secara signifikan menurunkan tingkat keberhasilan serangan DDoS dengan menjaga ketersediaan layanan API untuk pengguna yang sah.

Dengan demikian, solusi ini tidak hanya menambah keamanan tetapi juga memastikan stabilitas dan kinerja API Flask dalam menghadapi serangan DDoS. Penelitian ini memberikan kontribusi penting dalam pengembangan metode mitigasi serangan DDoS yang praktis dan efektif, khususnya pada lingkungan pengembangan web modern yang menggunakan Flask dan Python.

Kata kunci: *DdoS, Traffic Limitter, Flask, Remediasi*

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks are a significant threat to modern web applications, including the Flask API which is often used in Python-based web application development. This study proposes and implements a solution to mitigate DDoS attacks by using a traffic limiter on the Flask API. Traffic limiters function to regulate and limit the number of requests that can be received by an API within a certain period of time. This approach has proven effective in reducing the impact of DDoS attacks by ensuring that only legitimate requests that meet the specified limits can be executed.

This study includes concrete steps for implementing traffic limiters using various available Python libraries, as well as their integration with the Flask API. Evaluations are carried out through DDoS attack simulations and performance testing on the implemented system. The test results show that traffic limiters are able to significantly reduce the success rate of DDoS attacks by maintaining the availability of API services for legitimate users.

Thus, this solution not only increases security but also ensures the stability and performance of the Flask API in the face of DDoS attacks. This study makes an important contribution to the development of practical and effective DDoS attack mitigation methods, especially in modern web development environments that use Flask and Python..

Keyword**:** *DDoS, Traffic Limitter, Flask, remediation*