**Analisis Serangan DDoS Menggunakan Tools slowhttptest Dan Penanganan Dengan Nginx**

Budi Amin1, Muhamad Usri Yusron 2\*

1,2Institut Teknologi Nasional Bandung

*1muhamad.usri @mhs.itenas.ac.id 2budi.amin@mhs.itenas.ac.id*

| **ABSTRACT** |
| --- |
| *Distributed Denial of Service (DDoS) attacks are a serious threat to network security that can result in significant service disruption. Based on reports from the CloudFlare site for the United States, there is a 600% increase in attacks targeting Cryptocurrency companies in the second quarter of 2023. This research analyzes DDoS attacks using the slowhttptest tool to simulate attacks and evaluate the effectiveness of Nginx in handling these attacks. Slowhttptest is a tool designed to test how a server handles slow and inefficient connections, which is a common technique in DDoS attacks. The research results show that Nginx is able to identify and reduce the impact of DDoS attacks with proper configuration, such as setting connection limits and using additional security modules. This research provides important insights into DDoS attack mitigation strategies and shows the importance of good server setup to maintain service availability.*  **Keywords:** *DDoS Attacks, Slowhttptest, Nginx, Cyber ​​Security* |
| **ABSTRAK** |
| Serangan Distributed Denial of Service (DDoS) adalah salah satu ancaman serius dalam keamanan jaringan yang dapat mengakibatkan terganggunya layanan secara signifikan. Berdasarkan laporan dari situs *CloudFlare* untuk area Amerika Serikat terdapat peningkatan serangan sebesar 600% yang menargetkan perusahaan *Cryptocurrency* dalam kuartal ke-dua 2023. Penelitian ini menganalisis serangan DDoS dengan menggunakan tools slowhttptest untuk mensimulasikan serangan dan mengevaluasi efektivitas Nginx dalam menangani serangan tersebut. Slowhttptest adalah alat yang dirancang untuk menguji bagaimana server menangani koneksi yang lambat dan tidak efisien, yang merupakan teknik umum dalam serangan DDoS. Hasil penelitian menunjukkan bahwa Nginx mampu mengidentifikasi dan mengurangi dampak serangan DDoS dengan konfigurasi yang tepat, seperti pengaturan batas koneksi dan penggunaan modul keamanan tambahan. Penelitian ini memberikan wawasan penting tentang strategi mitigasi serangan DDoS dan menunjukkan pentingnya pengaturan server yang baik untuk menjaga ketersediaan layanan.  **Keywords:** Serangan*DDoS, Slowhttptest, Nginx, Keamanan Jaringan* |
|  |

**PENDAHULUAN**

Terus meningkatnya kecepatan internet dari waktu ke waktu selalu diikuti meningkatnya pula serangan cyber criminals dari tahun ketahuan. Tahun 2018 yang lalu jumlah serangan DDoS terus menurun, membuat para ahli Kaspersky Lab berasumsi bahwa penjahat cyber yang telah melakukan serangan DDoS untuk keuntungan finansial telah mengalihkan perhatian mereka ke sumber pendapatan lain (seperti penambangan crypto). Namun, statistik untuk Q1 2019 bertentangan dengan tren ini dan menunjukkan bahwa jumlah serangan DDoS yang diblokir oleh Kaspersky DDoS Protection telah tumbuh dengan mengejutkan 84%, jika dibandingkan dengan Q4 2018.

Serangan *Distributed Denial-of-Service (DDoS)* merupakan salah satu ancaman keamanan siber yang paling umum dan paling bahaya di era digital saat ini. Serangan HTTP DoS yang lambat adalah salah satu metode serangan DoS yang menargetkan server HTTP, metode ini menghambat layanan dengan menjenuhkan kumpulan koneksi dengan permintaan yang lambat dan banyak. Serangan ini bertujuan untuk melumpuhkan layanan online dengan membanjiri server target dengan trafik data yang berlebihan, sehingga mengakibatkan server tidak dapat melayani permintaan yang sah dari pengguna. Serangan DDoS dapat menyebabkan kerugian finansial yang signifikan bagi organisasi, serta merusak reputasi dan mengganggu operasi bisnis.

Salah satu metode yang sering digunakan dalam serangan DDoS adalah menggunakan tools *slowhttptest.* Tools ini dapat menghasilkan permintaan HTTP yang lambat dan tidak sah dalam jumlah besar, sehingga membebani server target dan menyebabkannya menjadi tidak responsive. Slowhttptest sendiri adalah salah satu alat penyerang DDoS, ini terutama karena ia menggunakan protokol HTTP untuk terhubung dengan server dan untuk menjaga sumber daya tetap sibuk seperti CPU dan RAM. Untuk menangkal serangan DDoS yang menggunakan tools slowhttptest, server web seperti Nginx dapat dikonfigurasikan dengan berbagai aturan dan modul keamanan.

1. **METODE**

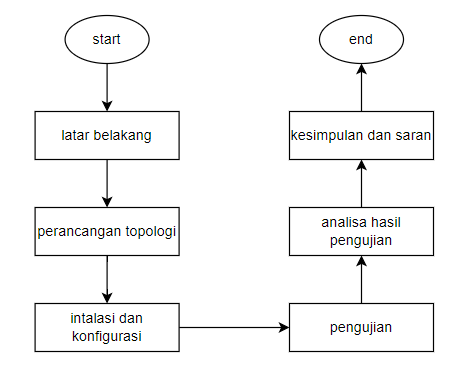
Setup tools dan software yang dibutuhkan untuk mengimplementasikan pengujian ini dapat dilihat pada tabel 1.1 dibawah ini.

| **no** | **tools dan software** | **versi** |
| --- | --- | --- |
| 1 | Virtual Box Machine | 7.0 atau terbaru |
| 2 | Kali Linux | 2024-1 atau terbaru |
| 3 | Slowhttptest | - |

Tabel 1.1 setup software

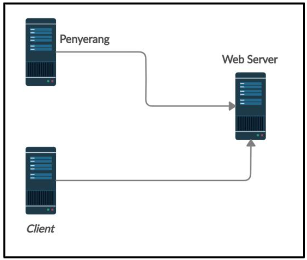
2.1 Implementasi Serangan

Metodologi serangan ini melalui beberapa tahapan yang direpresentasikan dalam suatu kerangka kerja yang digambarkan melalui diagram alir yang meliputi perancangan,pengujian,dan proses analisis untuk memberikan gambaran secara umum bagaimana melakukan serangan terhadap suatu situs menggunakan tools dari slowhttptest.

Gambar 1 Diagram alir kerangka kerja

Penjelasan dari tiap langkah dalam diagram alir diatas adalah sebagai berikut:

1. Latar belakang, mengumpulkan sumber dan data dari penelitian sebelumnya sehingga menjadi penentu dalam memilih tema dalam penelitian kali ini yang kemudian dituangkan dalam bab pendahuluan.
2. Perancangan topologi untuk memberikan gambaran secara luas bagaimana metode serangan ini berjalan.



Gambar 2. Topologi Serangan

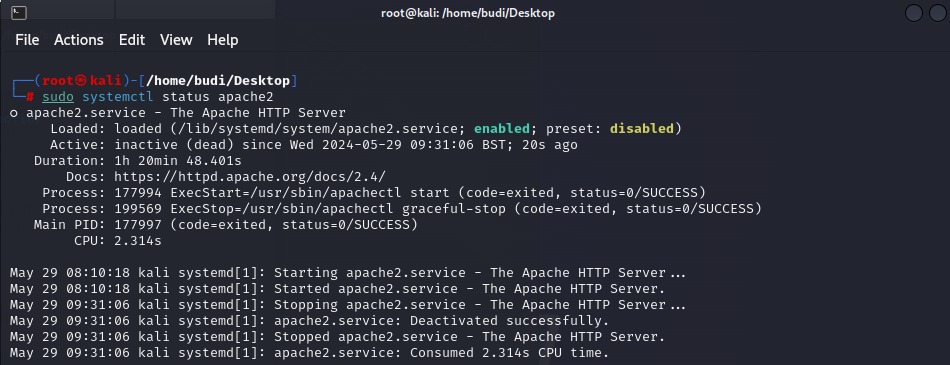
# Instalasi dan konfigurasi dilakukan menggunakan sistem operasi *Kali Linux* di dalam mesin virtual box.

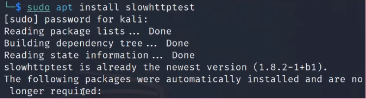
1-Install virtual box versi terbaru dari sumber terpercaya (<https://www.virtualbox.org/>)

2- Install kali linux melalui situs resmi *Kali Linux* (<https://www.virtualbox.org/>)

3- Konfigurasi *Kali Linux* di dalam virtual box.

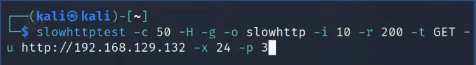
4- Masuk terminal Kali Linux untuk mengecek status apache.

gambar 3. cek status apache

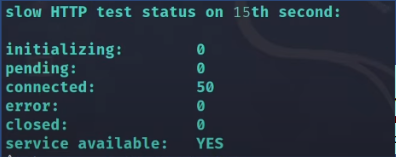
5- Menginstall tools slowhttptest.

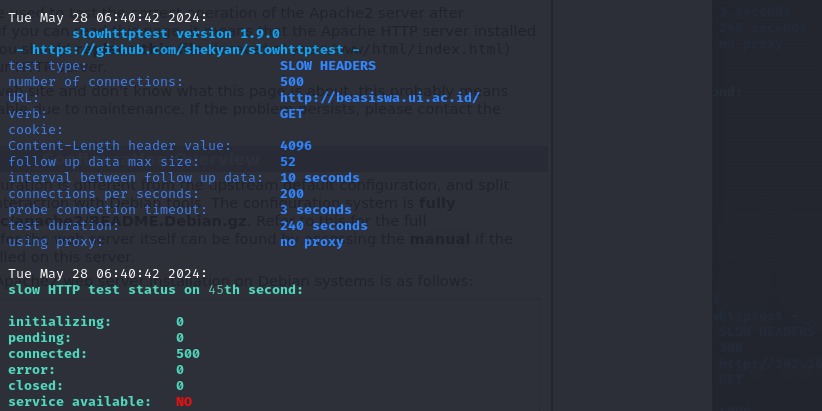
Gambar 4. Install slowhttptest

6- Melakukan serangan dengan tools slowhttptest

Gambar 5. Penggunaan slowhttptest

1. Pengujian, melakukan pengujian serangan menggunakan tools slowhttptest dengan memberikan jumlah koneksi yang berbeda dalam satu server untuk menemukan titik tertinggi suatu server dapat me-manage permintaan data.

Gambar 6.1. Respon hasil serangan tools slowhttptest

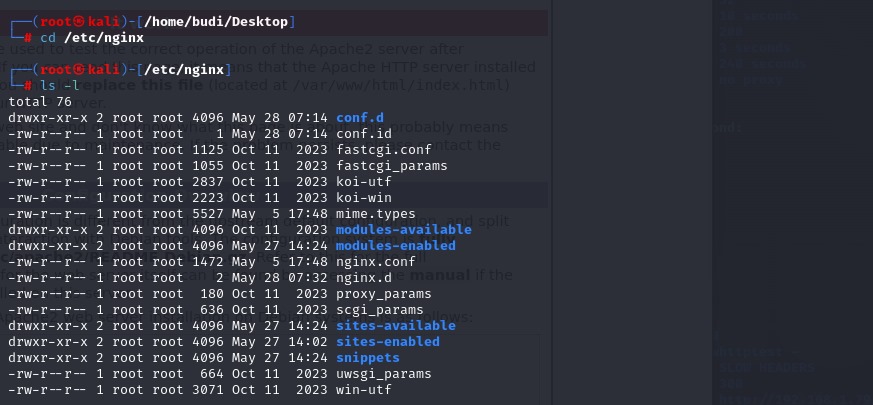
Gambar 6.2 Respon hasil serangan tools slowhttptest

1. Analisa hasil pengujian, berdasarkan metode penyerangan menggunakan tools slowhttptest terhadap IP:192.168.1.79 dengan diberikan koneksi sebanyak 50 kali dalam 15 detik maka server masih mampu menahan, sedangkan jika diberikan koneksi sebanyak 500 kali dalam 45 detik maka server sudah tidak mampu menahan koneksi yang terlalu banyak.

2.2 Implementasi Pertahanan

Metode pertahanan dilakukan menggunakan *nginx* yang dapat membatasi permintaan koneksi yang terlalu berlebihan sehingga server akan tetap berjalan secara normal dengan mengatur batas waktu yang diizinkan untuk membaca header dan body dari client.

2.2.1 Langkah pertahanan

1. Masuk ke dalam folder *nginx* dari dalam terminal
2. Masuk dalam file nginx.d

(sudo nano nginx.d)

Gambar 8. Masuk file nginx.d

1. Konfigurasi file nginx.d

# 

# 

# 

# 

# 

# 

Gambar 9. Konfigurasi file nginx.d

1. Cek kembali ke server atau website untuk memastikan sudah kembali berjalan normal

# 

# **KESIMPULAN**

Dengan memahami serangan DDoS (Distributed Denial of Service) dengan menggunakan tools seperti SlowHTTPTest, kami telah menguraikan berbagai aspek teknis dan implikasi dari metode serangan ini. SlowHTTPTest adalah alat yang dirancang untuk mensimulasikan serangan HTTP yang lambat, bertujuan untuk menguji ketahanan server web terhadap serangan yang memanfaatkan koneksi lambat atau tidak lengkap. Serangan ini berfungsi dengan cara memonopoli sumber daya server hingga server tidak mampu merespon permintaan valid lainnya, sehingga menyebabkan layanan menjadi tidak tersedia bagi pengguna yang sah.

Melalui penggunaan SlowHTTPTest, kami dapat mengeksplorasi beberapa jenis serangan HTTP yang lambat seperti Slowloris, Slow POST, dan Slow Read. Masing-masing jenis serangan ini mengeksploitasi kelemahan dalam cara server menangani koneksi HTTP. Misalnya, Slowloris mencoba mempertahankan sebanyak mungkin koneksi terbuka ke server target dengan mengirimkan header HTTP yang tidak lengkap, sementara Slow POST mengirimkan data POST dengan sangat lambat. Serangan ini menunjukkan betapa pentingnya memiliki mekanisme keamanan yang memadai di tingkat server untuk mendeteksi dan memitigasi serangan semacam ini.

Selain itu, penggunaan SlowHTTPTest dalam pengujian keamanan menunjukkan pentingnya tindakan pencegahan seperti konfigurasi firewall yang tepat, penerapan batas waktu koneksi (timeout) yang lebih agresif, serta penggunaan layanan mitigasi DDoS yang dapat mengenali dan merespon serangan ini secara otomatis. Menguji server dengan alat seperti SlowHTTPTest memungkinkan administrator untuk mengidentifikasi potensi kelemahan dan memperkuat infrastruktur mereka sebelum terjadi serangan yang sesungguhnya.

Secara keseluruhan, studi tentang serangan DDoS menggunakan SlowHTTPTest menekankan pentingnya pemahaman mendalam tentang vektor serangan yang mungkin dan perlunya pendekatan proaktif dalam pengelolaan keamanan siber. Dengan terus memperbarui dan memperkuat mekanisme pertahanan, organisasi dapat lebih siap menghadapi ancaman yang terus berkembang dalam lanskap digital saat ini. SlowHTTPTest bukan hanya alat untuk penyerang, tetapi juga merupakan alat penting bagi para profesional keamanan untuk mengasah kemampuan mereka dalam melindungi aset digital yang berharga.

**DAFTAR PUSTAKA**

Al-, J., Mahdi, S., Supervisor, A.-S., & Ericsson, M. (n.d.). *Performance comparison between Apache and NGINX under slow rate DoS attacks*.

Aziz, A., & Tampati, T. (2015). Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan Nginx. In *Analisis Web Server untuk Pengembangan Hosting Server Institusi: Pembandingan Kinerja Web Server Apache dengan Nginx JURNAL MULTINETICS* (Vol. 1, Issue 2).

*document*. (n.d.).

Gonzalez, H., Gosselin-Lavigne, M. A., Stakhanova, N., & Ghorbani, A. A. (n.d.). *The Impact of Application Layer Denial of Service Attacks*.

*PENDETEKSIAN SERANGAN DDOS (DISTRIBUTED DENIAL OF SERVICE) MENGGUNAKAN IDS (INTRUSION DETECTION SYSTEM)*. (n.d.).

Pratiwi, D. Y. D., & Adrian, R. (2024). Deteksi Dan Mitigasi Serangan Distributed Denial of Service Pada Software Defined Network. *Jurnal Teknik Informatika Dan Sistem Informasi*, *10*(1). https://doi.org/10.28932/jutisi.v10i1.6995

Putra, R. S., Mayasari, R., Bogi, N., & Karna, A. (n.d.). *IMPLEMENTATION AND ANALYSIS VIRTUAL NETWORK SECUTIRY WITH HIPS SNORT ON WEB SERVER SERVICE AGAINTS DOS AND DDOS ATTACK*.

Sikora, M., Fujdiak, R., Kuchar, K., Holasova, E., & Misurec, J. (2021). Generator of slow denial-of-service cyber attacks†. *Sensors*, *21*(16). https://doi.org/10.3390/s21165473

Zankoya Zaxo, Duhok Polytechnic University, IEEE Computational Intelligence Society. Iraq Chapter., IEEE Communications Society. Iraq Chapter., & Institute of Electrical and Electronics Engineers. (n.d.). *International Conference on Advanced Science and Engineering : book of abstracts & program book : October 9-11, 2018*.