Journal of Technology and System Information Vol: 1, No 4, 2024, Page: 1-11

Pengaruh Serangan *Slow* HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest

Tiara Safitrah*, Antonio Banggas Gregory Sinaga, Muhammad Alghifari, Shelvie Nidya Neyman

IPB University

Abstrak: Penelitian ini bertujuan untuk menganalisis dampak serangan *Denial of Service* (DoS) terhadap performa dan ketersediaan layanan web, dengan menggunakan alamat domain hydrolevi.foxlust.my.id sebagai sampel pengujian. Topik ini dipilih karena serangan DoS dapat menyebabkan kerugian finansial dan kerusakan reputasi yang signifikan bagi pemilik situs web. Metode yang digunakan adalah pendekatan eksperimental melalui simulasi serangan menggunakan alat slowhttptest untuk mengukur respons server terhadap serangan *Slow* HTTP DoS. Hasil penelitian menunjukkan bahwa serangan DoS menyebabkan penurunan performa layanan web yang signifikan, memperlambat respons terhadap permintaan pengguna, dan meningkatkan risiko kesalahan sistem. Visualisasi menggunakan *EtherApe* mengindikasikan peningkatan lalu lintas jaringan yang berlebihan, sehingga layanan web tidak dapat diakses setelah serangan berjalan selama 171 detik. Hal ini menegaskan bahwa server tidak mampu menangani beban serangan tersebut. Oleh karena itu, sangat penting bagi pemilik server untuk menerapkan langkah-langkah pencegahan seperti peningkatan kapasitas server, implementasi solusi anti-DoS, dan penggunaan jaringan *Content Delivery Network* (CDN). Penelitian ini menekankan pentingnya kesiapsiagaan dan langkah-langkah mitigasi dalam menghadapi ancaman keamanan siber guna memastikan kelancaran layanan web.

Kata Kunci: *Denial of Service*, Keamanan Siber, Layanan Web, *Slow* HTTP DoS, Slowhttptest

DOI: https://doi.org/10.47134/jtsi.v1i4.2663
*Correspondence: Tiara Safitrah
Email: tiarasafitrah@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *This study aims to analyze the impact of Denial of Service (DoS) attacks on the performance and availability of web services, using the domain address hydrolevi.foxlust.my.id as a test sample. This topic was chosen because DoS attacks can cause significant financial losses and reputational damage to website owners. The method used is an experimental approach through attack simulation using the slowhttptest tool to measure the server's response to Slow HTTP DoS attacks. The results of the study indicate that DoS attacks cause significant web services performance degradation, slow down responses to user requests, and increase the risk of system errors. Visualization using EtherApe indicated an excessive increase in network traffic, rendering the web service inaccessible after the attack had been running for 171 seconds. This confirms that the server was unable to handle the attack load. Therefore, it is crucial for server owners to implement preventive measures such as increasing server capacity, implementing anti-DoS solutions, and using Content Delivery Networks (CDN). This study emphasizes the importance of preparedness and mitigation measures in facing cyber security threats to ensure the smooth operation of web services.*

Keywords: *Cyber Security, Denial of Service, Slow HTTP DoS, Slowhttptest, Web Service*

Pendahuluan

Seiring dengan pesatnya perkembangan internet, berbagai jenis serangan melalui jaringan semakin meningkat (Munawar & Putri, 2020). Hal ini mengakibatkan layanan yang diberikan menjadi kurang aman, terutama yang terkoneksi melalui jaringan komputer. Oleh karena itu, penting untuk meningkatkan keamanan server yang digunakan. Keamanan jaringan memainkan peran krusial dalam melindungi informasi dan sistem, menjaga integritas dan ketersediaan informasi, serta memastikan privasi dan perlindungan data (Sumar et al., 2024).

Keamanan siber atau yang sering disebut sebagai keamanan informasi digital, adalah disiplin ilmu yang berfokus pada perlindungan sistem komputer, jaringan, program, dan data dari serangan, kerusakan, atau akses yang tidak sah. Keamanan siber mencakup semua langkah-langkah teknis dan administratif yang diambil untuk melindungi informasi digital dari berbagai ancaman. Ancaman tersebut bisa berupa serangan siber, *malware*, *hacking*, dan banyak lagi (Wahib et al., 2022).

Keamanan siber terdiri dari tiga komponen utama yang dikenal sebagai CIA triad, yaitu kerahasiaan, integritas, dan ketersediaan (Anggraeni et al., 2022). Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang melalui teknik seperti enkripsi dan manajemen akses. Integritas menjaga keakuratan dan kelengkapan informasi serta mencegah perubahan oleh pihak yang tidak berwenang dengan menggunakan kontrol akses, *hash*, dan metode verifikasi lainnya. Sedangkan ketersediaan memastikan bahwa sistem dan data tersedia bagi pengguna yang berwenang saat dibutuhkan, dengan langkah-langkah seperti perencanaan pemulihan bencana, redundansi sistem, dan mitigasi serangan DoS (Harahap et al., 2023).

Serangan *Denial of Service* (DoS) menjadi salah satu ancaman utama dalam keamanan siber, terutama terhadap layanan web yang sangat bergantung pada ketersediaan dan performa server (Tyas et al., 2022). *Denial of Service* (DoS) merupakan salah satu bentuk serangan siber yang bertujuan untuk membuat sebuah layanan, jaringan, atau sumber daya sistem menjadi tidak tersedia bagi pengguna yang sah dengan cara membanjiri sistem dengan lalu lintas yang berlebihan atau menyebabkan kegagalan sistem. Serangan DoS dapat membuat layanan internet tidak dapat diakses oleh pengguna yang dimaksudkan dengan mengganggu operasi normal server, layanan, atau infrastruktur jaringan (Wicaksono & Suartana, 2023).

Salah satu bentuk serangan DoS yang semakin mendapat perhatian adalah *Slow* HTTP DoS. Serangan ini mengeksploitasi kelemahan dalam penanganan koneksi HTTP oleh server web dengan mengirimkan permintaan HTTP secara lambat, sehingga menghabiskan sumber daya server secara berlebihan tanpa memerlukan *bandwidth* yang besar dari pihak penyerang. HTTP adalah dasar dari segala pertukaran data di internet, yang memungkinkan pengguna untuk mengakses berbagai sumber daya seperti halaman web, gambar, dan video. HTTP menggunakan *port* 80 secara *default* untuk transmisi data, meskipun bisa dikonfigurasi untuk menggunakan *port* lain (Zabar & Novianto, 2015). Secara mendasar, HTTP berfungsi sebagai protokol *request-response*, di mana klien

mengirimkan permintaan ke server, dan server merespons dengan data yang diminta (Munadi et al., 2019).

Serangan *Slow* HTTP DoS beroperasi dengan mengirimkan permintaan HTTP secara perlahan, menjaga koneksi tetap terbuka, dan mencegah server menutupnya. Teknik ini dapat memanfaatkan beberapa jenis serangan seperti *Slowloris, Slow POST*, dan *Slow Read*. Menurut penelitian yang dilakukan oleh Molavi (2020), serangan *Slowloris* dapat mempertahankan ribuan koneksi terbuka dengan mengirimkan *header* HTTP secara perlahan, sedangkan serangan *Slow POST* menggunakan kecepatan transfer data yang sangat rendah untuk mengirimkan data *POST* (Arman, 2020).

Penelitian lainnya menunjukkan bahwa serangan *Slow* HTTP DoS tidak memerlukan sumber daya yang besar dari sisi penyerang, namun sangat efektif dalam mengeksploitasi batas koneksi simultan server web. Hal ini menyebabkan server kehabisan slot koneksi yang tersedia, sehingga permintaan sah dari pengguna terblokir atau tertunda. Dalam beberapa kasus, serangan ini bahkan dapat menyebabkan server *crash* (Geges & Wibisono, 2015).

Dalam penelitian ini, akan berfokus pada pengaruh serangan *Slow* HTTP DoS terhadap layanan web hydrolevi.foxlust.my.id dengan menggunakan alat pengujian slowhttptest. Alat ini memungkinkan simulasi serangan untuk mengevaluasi sejauh mana serangan dapat mempengaruhi performa dan ketersediaan layanan web. Berdasarkan studi sebelumnya, serangan *Slow* HTTP dapat menyebabkan degradasi performa server yang signifikan, bahkan hingga menyebabkan *downtime* total pada server yang tidak dilengkapi dengan mekanisme mitigasi yang memadai (Firmansyah, 2021).

Slowhttptest digunakan untuk mengukur dampak serangan *Slow* HTTP DoS pada berbagai konfigurasi server web. Slowhttptest telah terbukti efektif dalam mengidentifikasi kelemahan server terhadap serangan tipe ini. Pengujian melibatkan beberapa skenario serangan dengan berbagai parameter, seperti jumlah koneksi, interval pengiriman data, dan durasi serangan (Kemp et al., 2023).

Hasil penelitian ini diharapkan dapat memberikan wawasan yang lebih mendalam tentang mekanisme serangan *Slow* HTTP DoS dan bagaimana mereka dapat mempengaruhi layanan web. Selain itu, studi ini bertujuan untuk mengembangkan rekomendasi praktis untuk meningkatkan ketahanan server web terhadap serangan semacam ini. Menurut studi Zheng dkk (2022), memahami karakteristik serangan dan respons server yang tepat adalah kunci dalam merancang sistem pertahanan yang efektif (Zheng et al., 2022).

Secara keseluruhan, penelitian ini bertujuan untuk memberikan kontribusi terhadap pemahaman yang lebih baik tentang serangan *Slow* HTTP DoS dan solusi mitigasinya. Diharapkan bahwa hasil dari studi ini dapat menjadi referensi bagi pengembang dan administrator sistem dalam merancang dan mengelola infrastruktur web yang lebih aman dan tangguh.

Metode

Pendekatan Penelitian

Penelitian ini mengadopsi pendekatan eksperimental dengan tujuan utama untuk mendalami pengalaman, persepsi, dan pandangan peserta terhadap peristiwa atau fenomena yang diamati (Akbar et al., 2023). Fokus utamanya adalah pada pengaruh yang disebabkan oleh serangan *Denial of Service* (DoS), khususnya serangan *Slow* HTTP DoS. Dengan memanfaatkan metode eksperimental, penelitian ini memberikan pemahaman yang lebih mendalam tentang respons sistem terhadap serangan tersebut, serta mengevaluasi kinerja dan kemampuan sistem dalam memitigasi dampak negatif dari serangan DoS.

Teknik Pengumpulan dan Analisis Data

Dalam penelitian eksperimental ini, teknik pengumpulan data akan menggunakan alat yang disebut slowhttptest untuk menyimulasikan serangan *Slow* HTTP DoS terhadap layanan web yang dituju. Slowhttptest adalah alat yang dirancang khusus untuk menyebabkan serangan ini dengan cara mengirimkan permintaan HTTP yang lambat atau tidak lengkap ke server web target. Proses pengumpulan data akan dimulai dengan konfigurasi parameter-parameter tertentu dalam slowhttptest, seperti laju transfer data, jumlah koneksi, dan durasi serangan.

Setelah dikonfigurasi, alat akan mulai meluncurkan serangan terhadap server web target yang sedang diuji. Selama serangan berlangsung, data akan terus dipantau dan dicatat untuk menganalisis dampak serangan terhadap ketersediaan dan kinerja layanan web. Data yang dikumpulkan dapat mencakup waktu respons server, kecepatan pemrosesan permintaan, dan tingkat ketersediaan layanan. Analisis data ini akan memberikan pemahaman yang mendalam tentang bagaimana serangan *Slow* HTTP DoS mempengaruhi layanan web dan memungkinkan peneliti untuk mengidentifikasi kerentanan potensial dan mengembangkan strategi perlindungan yang lebih efektif.

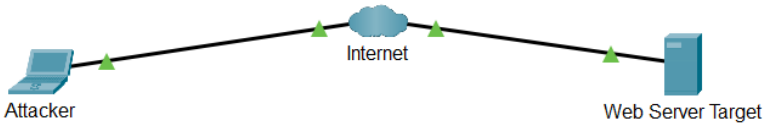
Sumber Daya Penelitian

Sumber daya yang diperlukan dalam penelitian ini adalah sebagai berikut:

1. Komputer atau PC
2. Koneksi Internet
3. *Virtual Machine* Kali Linux
4. *Tool* Slowhttptest
5. *Web Server Target*

Skema Jaringan

Dalam skema yang terlihat pada Gambar 1, penelitian akan berkonsentrasi pada pengaruh serangan *Slow* HTTP DoS terhadap layanan web yang disediakan oleh server target. Pengguna akan mengakses layanan web langsung melalui internet, dan penyerang akan meluncurkan serangan terhadap target server web.



Gambar 1. Skema jaringan serangan DoS

1. Internet
   Internet berperan sebagai sumber utama lalu lintas data yang mencakup semua informasi yang dikirim dan diterima oleh pengguna (Rustam, 2017).
2. Penyerang (*Attacker*)
   Penyerang adalah individu atau kelompok yang bertujuan untuk mengganggu ketersediaan layanan suatu sistem atau jaringan dengan cara membanjiri target dengan lalu lintas data yang tidak biasa atau tidak sah. Penyerang menggunakan serangan *Slow* HTTP DoS untuk mengganggu layanan web yang disediakan oleh target server (Hermawan, 2012).
3. *Web Server Target*
   Web server target merupakan server web yang menjadi sasaran serangan *Slow* HTTP DoS. Server web ini menyediakan layanan web yang diakses oleh pengguna melalui internet (Siregar, 2013). Layanan web adalah sistem perangkat lunak yang dirancang untuk mendukung interaksi mesin-ke-mesin melalui jaringan, biasanya menggunakan protokol HTTP (Purnamasari, 2012). Layanan ini memungkinkan aplikasi untuk berkomunikasi satu sama lain dan berbagi data secara *real-time*, terlepas dari sistem operasi atau bahasa pemrograman yang digunakan (Frisca et al., 2023).

Hasil dan Pembahasan

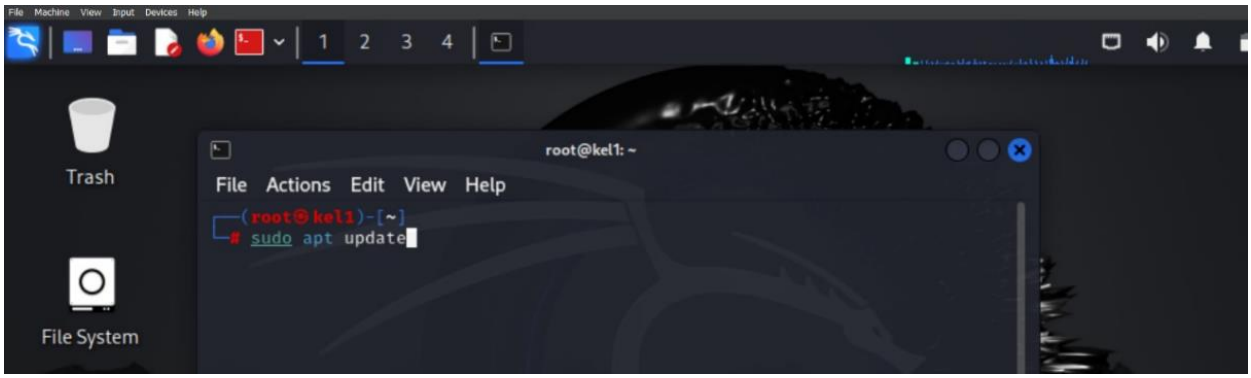
Untuk melakukan serangan DoS, perlu dilakukan konfigurasi pada virtual machine Kali Linux sebagai media simulasi serangan DoS slowhttptest. Serangan DoS akan dilakukan terhadap server web hydrolevi.foxlust.my.id. Berikut ini adalah langkah-langkah yang perlu dilakukan untuk melakukan serangan *Slow* HTTP DoS terhadap layanan web hydrolevi.foxlust.my.id.

Langkah Penyerangan

1. Gambar di bawah ini merupakan tampilan Kali Linux yang telah diinstal sebelumnya. Masuk mengunakan *username* dan *password* yang telah dibuat.

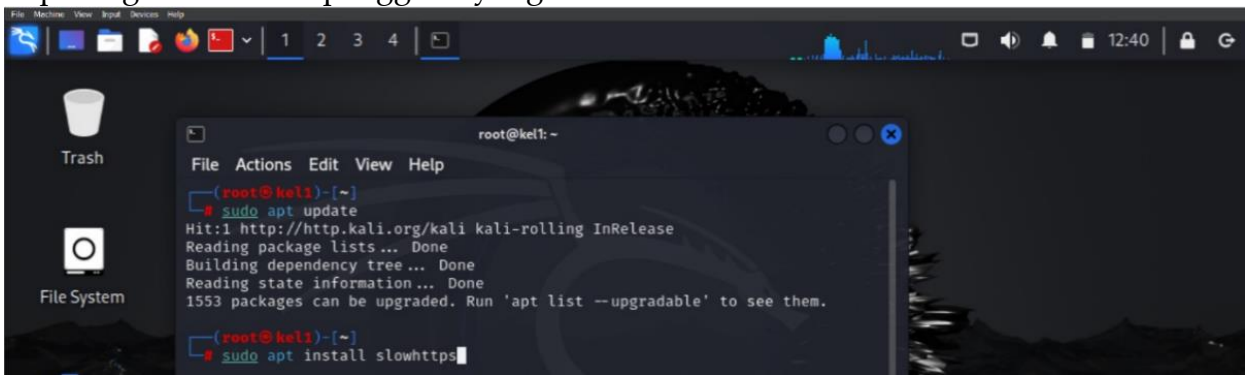
Gambar 2. Tampilan *log in* dalam Kali Linux

2. Selanjutnya, masuk ke dalam *Command Prompt* sebagai "*root*" dan jalankan perintah "**sudo apt update**" untuk memperbarui daftar paket perangkat lunak yang tersedia di sistem tersebut.



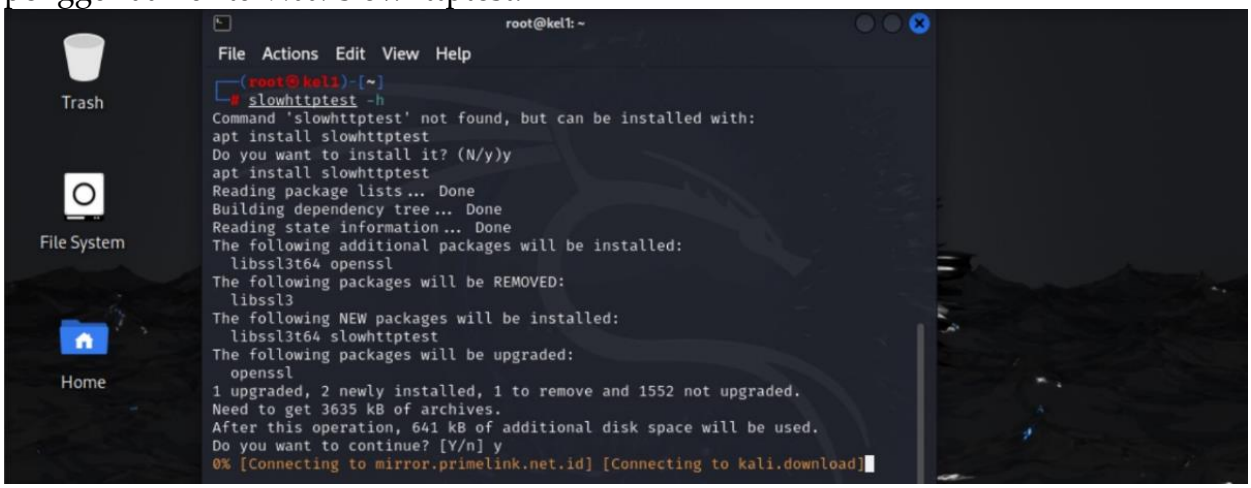
Gambar 3. Memperbarui paket dalam Kali Linux

3. Jalankan perintah "**sudo apt install slowhttps**" untuk menginstal *tool* slowhttptest. Alat ini dirancang untuk melakukan *stress test* jaringan dengan cara mensimulasikan berbagai jenis serangan *Denial of Service* (DoS). Serangan DoS bertujuan untuk membanjiri sistem target dengan *traffic* yang berlebihan, sehingga membuatnya tidak responsif atau tidak dapat digunakan oleh pengguna yang sah.



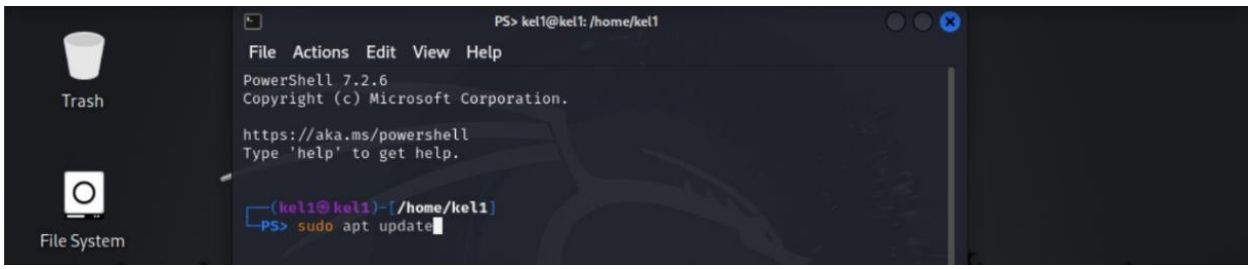
Gambar 4. Menginstal slowhttptest

4. Jalankan perintah "**slowhttptest -h**" untuk menampilkan menu bantuan atau instruksi penggunaan untuk *tool* slowhttptest.



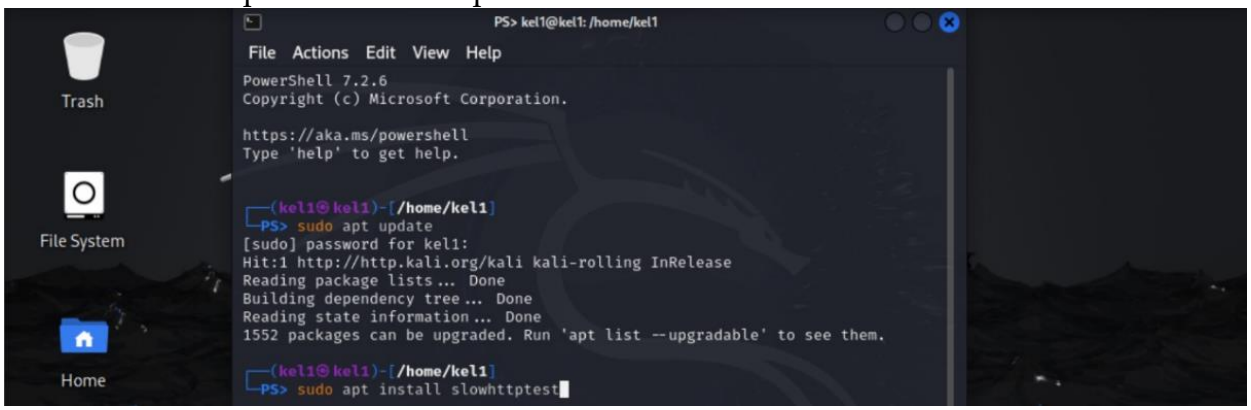
Gambar 5. Menampilkan menu bantuan dalam slowhttptest

5. Pada tahap ini masuk ke dalam *PowerShell* sebagai kel1, lalu pindah ke dalam direktori kel1 dengan menggunakan perintah "**cd /home/kel1**". Jalankan perintah "**sudo apt update**" untuk memperbarui daftar paket perangkat lunak yang tersedia pada direktori tersebut.



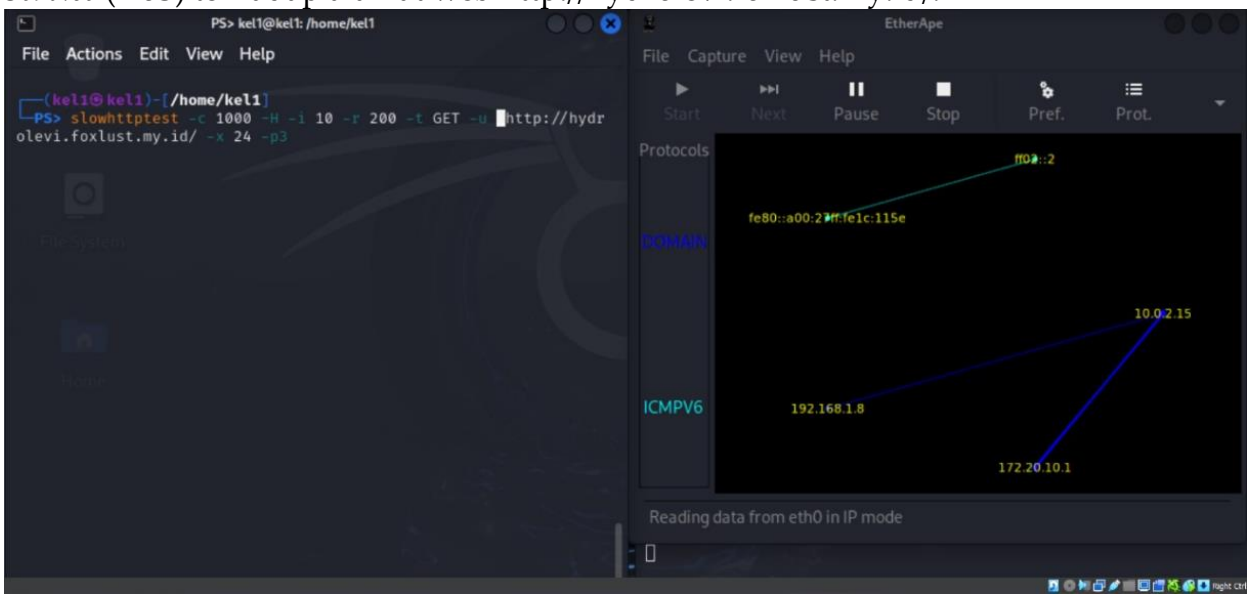
Gambar 6. Memperbarui paket dalam Kali Linux dengan *powershell*

6. Jalankan perintah "**sudo apt install slowhttptest**" yang bertujuan untuk menginstall *tool* bernama slowhttptest di sistem operasi Linux berbasis Debian atau Ubuntu.



Gambar 7. Menginstal slowhttptest dengan *powershell*

7. Jalankan perintah "**slowhttptest -c 1000 -H -i 10 -r 200 -t GET –u http://hydrolevi.foxlust.my.id/ -x 24 -p3**" untuk menyimulasikan serangan *Denial of Service* (DoS) terhadap alamat web http://hydrolevi.foxlust.my.id/.



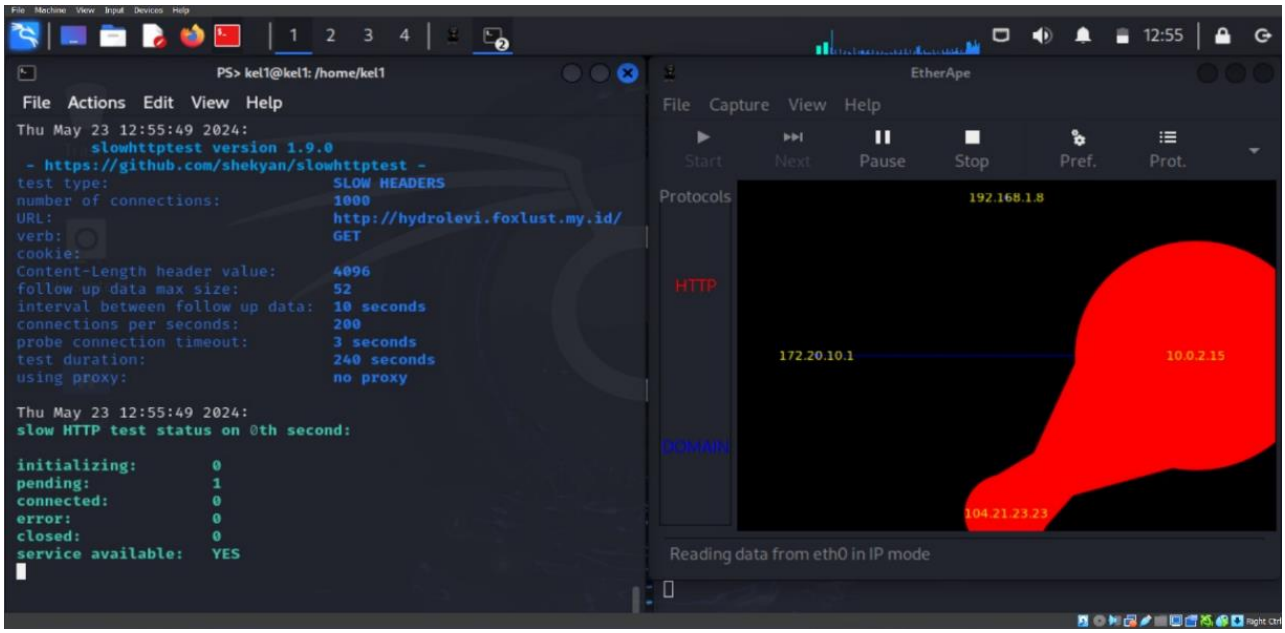
Gambar 8. Menyimulasikan serangan DoS

Berikut adalah penjelasan parameter yang digunakan:

- **slowhttptest**
  Alat yang digunakan untuk menyimulasikan serangan *Slow* HTTP DoS.
- **-c 1000**
  Parameter ini digunakan untuk menentukan jumlah koneksi klien yang digunakan dalam tes. Dalam hal ini, alat akan mencoba membuka 1000 koneksi simultan ke server target.
- **-H**
  Menentukan bahwa tes akan menggunakan metode serangan *Slow* HTTP *Header*. Hal ini berarti alat akan mengirimkan *header* HTTP dengan sangat lambat untuk membuat server sibuk.
- **-i 10**
  Parameter ini menentukan interval waktu dalam detik antara dua paket *header* HTTP berturut-turut. Setiap 10 detik, alat akan mengirimkan sebagian kecil dari *header* HTTP.
- **-r 200**
  Parameter ini menentukan laju koneksi, yaitu berapa banyak koneksi baru yang dibuka per detik. Dalam hal ini, alat akan mencoba membuka 200 koneksi baru setiap detik.
- **-t GET**
  Parameter ini menentukan jenis permintaan HTTP yang digunakan dalam tes. Dalam hal ini, metode HTTP GET akan digunakan.
- **-u http://hydrolevi.foxlust.my.id/**
  Merupakan URL target dari web yang akan diuji. Dalam hal ini, targetnya adalah http://hydrolevi.foxlust.my.id/.
- **-x 24**
  Merupakan durasi maksimum dalam jam untuk menjalankan tes. Tes akan berjalan selama 24 jam kecuali dihentikan secara manual.
- **-p 3**
  Menentukan jumlah paket yang akan dikirimkan dalam setiap interval waktu yang ditentukan oleh -i. Dalam hal ini, 3 paket akan dikirimkan setiap 10 detik.

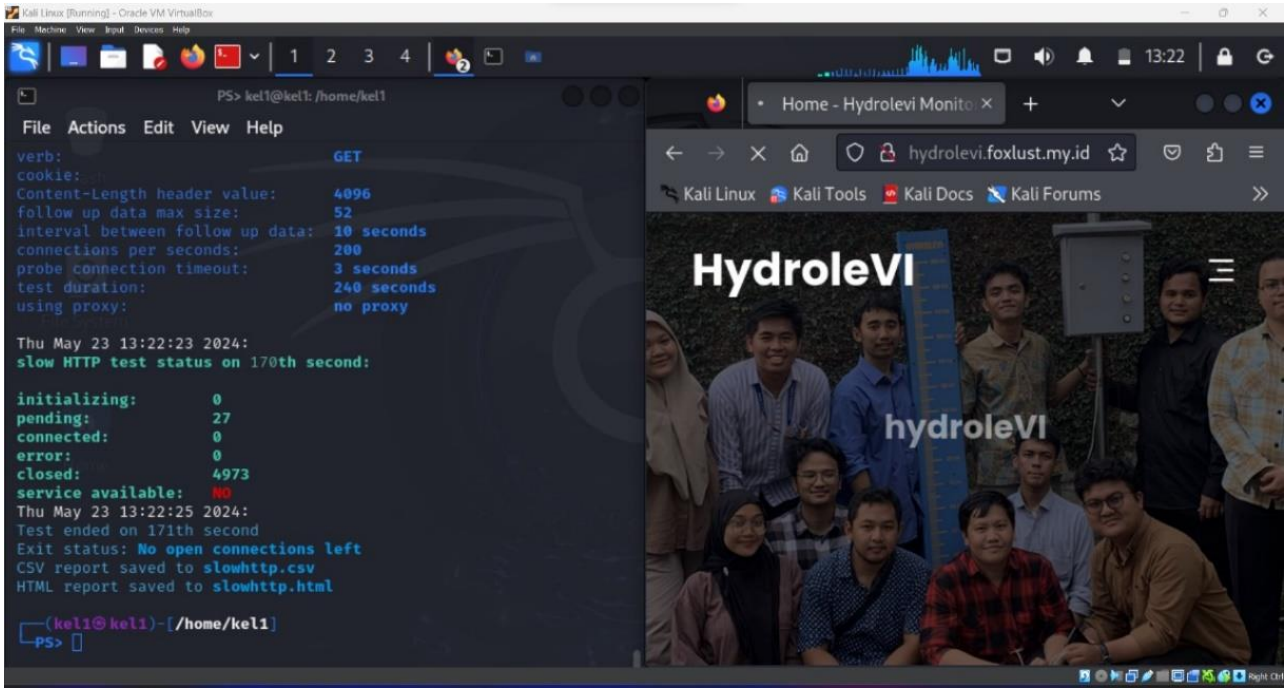
Dampak Penyerangan

Pada Gambar 9 dan Gambar 10 ditunjukkan hasil dari program slowhttptest yang sedang menyimulasikan serangan DoS terhadap server web. Gambar 9 menunjukkan hasil saat tes baru saja dimulai atau 0 sekon. Status awal menunjukkan bahwa tidak ada koneksi yang aktif atau *pending* dan layanan web masih tersedia sepenuhnya, ditunjukkan dengan status *YES*. Visualisasi dari *EtherApe* juga menunjukkan lalu lintas jaringan yang rendah atau normal tanpa adanya tanda-tanda beban tinggi atau masalah pada server.



Gambar 9. Hasil tes serangan DoS saat 0 sekon

Gambar 10 diambil setelah tes berjalan selama 171 detik, dengan waktu pada sistem menunjukkan *Thu May 23 13:22:23 2024*. Pada saat ini, ada 27 koneksi yang *pending*, 4973 koneksi yang telah ditutup, dan layanan web tidak tersedia. Hal ini berarti server tidak mampu menangani beban dari serangan *Slow* HTTP DoS, ditunjukkan dengan tidak dapat diaksesnya alamat domain yang sedang diuji. Tes berakhir dengan pesan *No open connections left* yang menunjukkan bahwa semua koneksi telah ditutup serta hasil tes disimpan dalam file slowhttp.csv dan slowhttp.html.



Gambar 10. Hasil tes serangan DoS setelah berjalan 171 sekon

Simpulan

Simulasi serangan *Denial of Service* (DoS) terhadap server web hydrolevi.foxlust.my.id menunjukkan konsekuensi serius yang dapat dialami oleh pemilik layanan web dan penggunanya. Hasil penelitian ini menunjukkan bahwa serangan *Slow* HTTP DoS secara signifikan dapat menurunkan performa server, meningkatkan tingkat *error*, dan menyebabkan potensi *overload* yang berdampak pada kerugian finansial, kerusakan reputasi, dan gangguan operasional bisnis. Pengujian menggunakan alat slowhttptest memperlihatkan efektivitasnya dalam mendeteksi kerentanan terhadap serangan *Slow* HTTP DoS, sehingga menjadi komponen penting dalam pengujian keamanan.

Strategi mitigasi yang direkomendasikan mencakup peningkatan kapasitas server, penerapan solusi anti-DoS, edukasi pengguna tentang keamanan internet, serta memiliki rencana pemulihan bencana, yang semuanya penting untuk melindungi infrastruktur server dan memastikan kelancaran layanan web. Selain itu, hasil simulasi menekankan pentingnya edukasi dan kesadaran mengenai keamanan siber, di mana pemahaman yang baik tentang ancaman dan cara pencegahannya memungkinkan baik pemilik server maupun pengguna untuk berkontribusi dalam menciptakan lingkungan internet yang lebih aman dan terpercaya.

Daftar Pustaka

Akbar, R., Weriana, Siroj, R. A., & Afgani, M. W. (2023). Experimental Reseacrch Dalam Metodologi Pendidikan. *Jurnal Ilmiah Wahana Pendidikan*, *9*(2), 465–474. https://jurnal.peneliti.net/index.php/JIWP/article/view/3165

Anggraeni, A., Ginting, J. G. A., & Ikhwan, S. (2022). Implementation of Intrusion Prevention System (IPS) to Analysis Triad Cia on Network Security Attacks on Web Server. *Jurnal Infotel*, *14*(4), 277–286. https://doi.org/10.20895/infotel.v14i4.813

Arman, M. (2020). Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(1), 56–70. https://doi.org/10.35957/jatisi.v7i1.284

Firmansyah, M. D. (2021). Analisa Keamanan Web Server terhadap Serangan Distributed Denial of Service menggunakan Modevasive. *Telcomatics*, *6*(1), 11–16. https://doi.org/10.37253/telcomatics.v6i1.4990

Frisca, G. S., Kosasi, S., Wijaya, T., Laipaka, R., & David, D. (2023). Pemanfaatan Web Service dalam Sistem Layanan Gereja Katolik Paroki Mrpd. *Naratif : Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, *5*(1), 54–70. https://doi.org/10.53580/naratif.v5i1.194

Geges, S., & Wibisono, W. (2015). Pengembangan Pencegahan Serangan Distributed Denial of Service (DDoS) pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis dan Client Puzzle. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *13*(1), 53. https://doi.org/10.12962/j24068535.v13i1.a388

Harahap, A. H., Difa Andani, C., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83.

Hermawan, R. (2012). Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (DDos). *Faktor Exacta*, *5*(1), 1–14.

Kemp, C., Calvert, C., Khoshgoftaar, T. M., & Leevy, J. L. (2023). An Approach to Application-Layer DoS Detection. *Journal of Big Data*, *10*(22), 1–30. https://doi.org/10.1186/s40537-023-00699-3

Munadi, R., Purnandi, M., & Arif, T. Y. (2019). Evaluasi Teknik Penyadapan Lalu Lintas Data Dengan Session Hijacking Pada Protokol HTTP. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *14*(2), 58–62. https://doi.org/10.30872/jim.v14i2.1798

Munawar, Z., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *2*(1), 14–20.

Purnamasari, S. D. (2012). Web Service Sebagai Solusi Integrasi Data pada Sistem Informasi Akademik Universitas Bina Darma. *Jurnal Ilmiah MATRIK*, *14*(2), 151–164.

Rustam, M. (2017). Internet dan Penggunaannya (Survei di kalangan masyarakat Kabupaten Takalar Provinsi Sulawesi Selatan). *Jurnal Studi Komunikasi Dan Media*, *21*(1), 13–24. https://doi.org/10.31445/jskm.2017.210102

Siregar, J. J. (2013). Analisis Exploitasi Keamanan Web Denial of Service Attack. *ComTech*, *4*(2), 1199–1205.

Sumar, M. R., Wahid, A., & Parenreng, J. M. (2024). Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS. *Pinisi Journal of Sciene Techonolgy*, *0*, 1–15.

Tyas, Z. A., Firdonsyah, A., & Ramdhani, W. (2022). Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS. *INFORMAL: Informatics Journal*, *7*(3), 258. https://doi.org/10.19184/isj.v7i3.34943

Wahib, P., Tunggal Narotama, A., Muhamad Rijki, N., Sahrudin, Permana, F., Sagara, D., Ibrahim Azkhal, D., Anwar, M., & Rifqi Juniawan, M. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Abdi Jurnal Publikasi*, *1*(2), 64–68. https://jurnal.portalpublikasi.id/index.php/AJP/index

Wicaksono, F. C. B., & Suartana, I. M. (2023). Deteksi Serangan Denial Of Service (DoS) pada Cloud Menggunakan Security Onion. *JINACS (Journal of Informatics and Computer Science)*, *5*(1), 111–118.

Zabar, A. A., & Novianto, F. (2015). Keamanan HTTP dan HTTPS Berbasis Web Menggunakan Sistem Operasi Kali Linux. *Komputa : Jurnal Ilmiah Komputer Dan Informatika*, *4*(2), 69–74. https://doi.org/10.34010/komputa.v4i2.2427

Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic Defenses in Cyber Security: Techniques, Methods and Challenges. *Digital Communications and Networks*, *8*(4), 422–435. https://doi.org/10.1016/j.dcan.2021.07.006