Journal of Technology and System Information Vol: 1, No 4, 2024, Page: 1-10

Implementasi *Firewall* pada Linux untuk Pencegahan Dari Serangan DoS

Muhammad Rafid Habibi Tambunan*, Shelvie Nidya Neyman

Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Serangan *Denial of Service* (DoS) merupakan ancaman serius bagi ketersediaan layanan jaringan yang dapat menyebabkan gangguan signifikan. Jurnal ini membahas implementasi *firewall* dan *iptables* sebagai solusi efektif untuk mengatasi serangan DoS. Dengan menggunakan *firewall*, lalu lintas jaringan yang mencurigakan dapat difilter dan akses yang tidak diinginkan dapat diblokir. Sementara itu, *iptables* memberikan kontrol granular untuk mengatur aturan kebijakan keamanan secara spesifik. Studi kasus dalam jurnal ini menunjukkan bahwa kombinasi *firewall* dan *iptables* secara signifikan mengurangi dampak serangan DoS terhadap jaringan. Evaluasi menunjukkan peningkatan kinerja dan stabilitas jaringan yang dilindungi dengan metode ini. Kesimpulan artikel menegaskan bahwa implementasi *firewall* dan *iptables* merupakan pendekatan yang efisien dalam memperkuat keamanan jaringan terhadap serangan DoS, dengan menggambarkan strategi yang dapat diadopsi oleh organisasi untuk meningkatkan ketahanan mereka terhadap ancaman tersebut. Dengan memperhatikan hasil evaluasi dan studi kasus yang disajikan, implementasi *firewall* dan *iptables* menjadi pilihan yang tepat bagi organisasi yang ingin meningkatkan keamanan jaringan mereka dan mengurangi risiko serangan DoS.

Kata Kunci: *Firewall, Iptables*, Serangan DoS, Keamanan Jaringan, Lalu Lintas

DOI: https://doi.org/10.47134/jtsi.v1i4.2648
*Correspondence: Muhammad Rafid Habibi Tambunan
Email: rafidhabibi@apps.ipb.ac.id

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

Abstract: *Denial of Service (DoS) attacks pose a serious threat to network service availability, causing significant disruptions. This journal discusses the implementation of firewalls and iptables as effective solutions to counter DoS attacks. By using firewalls, suspicious network traffic can be filtered and unwanted access can be blocked. Meanwhile, iptables provides granular control to set specific security policy rules.The availability of network services is seriously threatened by denial of service (DoS) assaults, which can cause major disruptions. The use of iptables and firewalls as practical defenses against DoS assaults is covered in this journal. Firewalls are a useful tool for filtering suspicious network traffic and blocking unauthorized access. In the meanwhile, you can establish custom security policy rules with granular control thanks to iptables. This journal's case study shows how iptables and firewalls work together to dramatically lessen the damage that DoS attacks can do to a network. Evaluations reveal that networks secured by this technique operate more reliably and perform better. The article's conclusion states that putting firewalls and iptables in place is a practical way to bolster network security against DoS attacks, providing businesses with a list of tactics to improve their resistance to cyber attacks.*

Keywords: *Firewall, Iptables, DoS Attack, Network Security, Traffic Filtering*

Pendahuluan

Keamanan siber adalah suatu upaya untuk melindungi sistem jaringan dan data dari serangan *cyber* yang dapat merusak atau menghilangkan data (Arlis & Sahari, 2019). Dalam mengkaji sinergi antara Badan Siber dan Sandi Negara dengan aktor non-negara dalam menghadapi peretasan data dan informasi kritis di Indonesia, beberapa landasan teori yang digunakan adalah Teori Strategi, Teori Ancaman Siber, Teori Hacking, Teori CyberSecurity, Keamanan Data dan Informasi, Keamanan Data dan Informasi Kritis, Teori Sinergi, dan Teori Crowdsourcing (Vania et al., 2023).

Linux adalah sebuah sistem operasi yang relatif aman dan populer digunakan dalam berbagai aplikasi. Dalam beberapa penelitian, Linux digunakan sebagai sistem operasi server utama, seperti dalam penelitian yang menggunakan Slowloris untuk melakukan serangan DoS (Hawari & Kurniawan, 2016). DoS (*Denial of Service*) adalah sebuah serangan yang menghabiskan *resource* komputer target sehingga tidak dapat diakses. Serangan DoS dapat dilakukan dengan cara membanjiri *traffic* jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari komputer lain tidak dapat diolah. Penelitian telah dilakukan untuk menguji efektivitas IDS (*Intrusion Detection System*) dalam menghadapi serangan DoS (Fadhlillah et al., 2019).

Implementasi *firewall* pada Linux sangat penting untuk mencegah serangan DoS (*Denial of Service*). Serangan DoS adalah suatu jenis serangan jaringan yang bertujuan untuk mengganggu kinerja sistem jaringan dengan cara mengirimkan paket-paket yang tidak diinginkan secara berlebihan (Haris et al., 2022). Dengan demikian, sistem jaringan tidak dapat berfungsi dengan normal dan menjadi tidak responsif. Dalam beberapa tahun terakhir, serangan DoS telah menjadi salah satu ancaman keamanan jaringan yang paling umum (Dehan Pratama et al., 2022). Serangan ini dapat dilakukan dengan cara mengirimkan paket-paket yang tidak diinginkan secara berlebihan, sehingga sistem jaringan tidak dapat berfungsi dengan normal. Oleh karena itu, perlu dilakukan implementasi *firewall* yang efektif untuk mencegah serangan DoS ini.

Firewall adalah aplikasi yang berfungsi sebagai pertahanan pertama untuk melindungi sistem jaringan dari ancaman yang berasal dari luar (Noor et al., 2020). Dalam Linux, *firewall* yang paling populer digunakan adalah *iptables* (Widianto & Sulistyo, 2021). *Iptables* menggunakan tabel dan rantai (*tables and chains*) untuk mengatur lalu lintas jaringan dan memfilter paket berdasarkan alamat IP, port, protokol, dan kriteria lainnya (Sugianti et al., 2020). Implementasi *firewall* pada Linux Ubuntu menggunakan *iptables* dapat meningkatkan keamanan sistem dengan menerapkan aturan yang membatasi akses yang tidak diinginkan (Khadafi et al., 2019). Proses implementasi ini melibatkan beberapa langkah, seperti membuat rantai baru, menambahkan aturan, dan mengaktifkan *iptables*. Dengan demikian, implementasi *firewall* pada Linux sangat penting untuk mencegah serangan DoS dan melindungi sistem jaringan dari ancaman lainnya. Oleh karena itu, perlu dilakukan penelitian lebih lanjut untuk meningkatkan keamanan sistem jaringan dengan menggunakan *firewall* yang efektif.

Metode

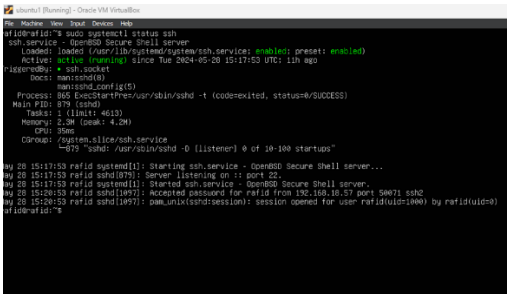
Proyek ini dilakukan selama periode 4 minggu terhitung dari pertemuan ke 10 di bulan April hingga pertemuan ke 14 di bulan Mei di Sekolah Vokasi IPB University, yang

terletak di Jalan Kumbang No. 14, Babakan, Bogor Tengah, Kota Bogor, Jawa Barat. Selama periode ini, akan dilakukan serangkaian kegiatan proyek yang meliputi pengumpulan data, analisis, implementasi, dan evaluasi. Metodologi yang akan digunakan dalam proyek ini akan mencakup langkah-langkah berikut:

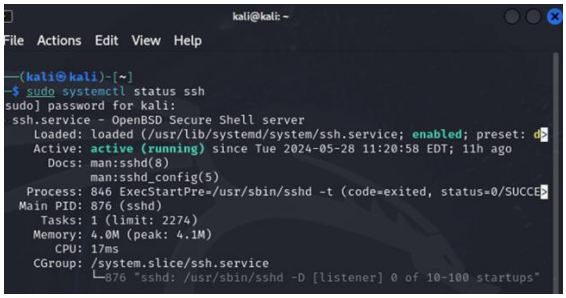
1. Analisis Kebutuhan dan Identifikasi Ancaman
   - Analisis Kebutuhan: Mengidentifikasi kebutuhan keamanan sistem jaringan, termasuk jenis layanan yang perlu dilindungi dan tingkat risiko yang terkait.
   - Identifikasi Ancaman: Menganalisis berbagai jenis serangan DoS yang mungkin terjadi dan potensi dampaknya terhadap sistem jaringan.
2. Penelitian dan Studi Literatur
   - Studi Literatur: Melakukan penelitian mendalam tentang teknik-teknik pencegahan serangan DoS yang telah ada, termasuk penggunaan *iptables* dalam *firewall* Linux.
   - Evaluasi *Best Practices*: Menganalisis praktik terbaik dalam mengoptimalkan konfigurasi *firewall* dan penggunaan *iptables* untuk melindungi sistem jaringan dari serangan DoS.
3. Perencanaan Implementasi
   - Desain Konfigurasi *Firewall*: Merancang konfigurasi *firewall* yang efektif berdasarkan temuan dari studi literatur dan analisis kebutuhan.
   - Pemilihan Alat dan Teknologi: Memilih alat dan teknologi yang tepat untuk implementasi konfigurasi *firewall*, termasuk pemilihan versi *iptables* yang sesuai.
4. Implementasi dan Pengujian
   - Konfigurasi *Firewall*: Menerapkan konfigurasi *firewall* yang telah dirancang, termasuk aturan-aturan *iptables* yang relevan.
   - Pengujian Fungsional: Melakukan pengujian fungsional untuk memastikan bahwa *firewall* beroperasi sesuai dengan yang diharapkan dan dapat mencegah serangan DoS dengan efektif.

Hasil dan Pembahasan

1. Konfigurasi SSH pada OS Ubuntu dan Kali Linux



Gambar 1. Status SSH di Ubuntu



Gambar 2. Status SSH di Kali Linux

Langkah pertama dalam menganalisis kebutuhan adalah memahami persyaratan konfigurasi SSH pada sistem Ubuntu dan Kali Linux, serta konfigurasi Apache2 pada sistem Ubuntu. Untuk konfigurasi SSH, diperlukan pemahaman tentang langkah-langkah yang diperlukan untuk meningkatkan keamanan, seperti mengubah *port default*, membatasi

akses berbasis IP, menggunakan otentikasi kunci publik, dan mengaktifkan fitur-fitur keamanan seperti pembaruan otomatis (Desmira & Wiryadinata, 2022).

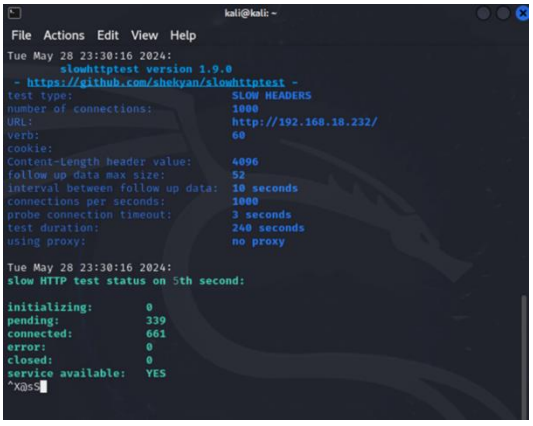
2. Konfigurasi *Web Server* Apache2

Konfigurasi web server Apache2 di Ubuntu memerlukan perhatian terhadap beberapa poin penting. Pertama, adalah mengatur konfigurasi situs untuk masing-masing situs web yang di-*host* oleh *server*. Dalam konfigurasi ini, perlu ditentukan direktori root, pengaturan akses, pengaturan SSL (jika digunakan), dan pengaturan lainnya yang spesifik untuk setiap situs (Barends et al., 2022). Selanjutnya, pengaturan modul juga krusial untuk diperhatikan, di mana Anda dapat mengaktifkan atau menonaktifkan modul Apache2 sesuai kebutuhan.

Gambar 3. Web Server Apache2 Sebelum Penyerangan

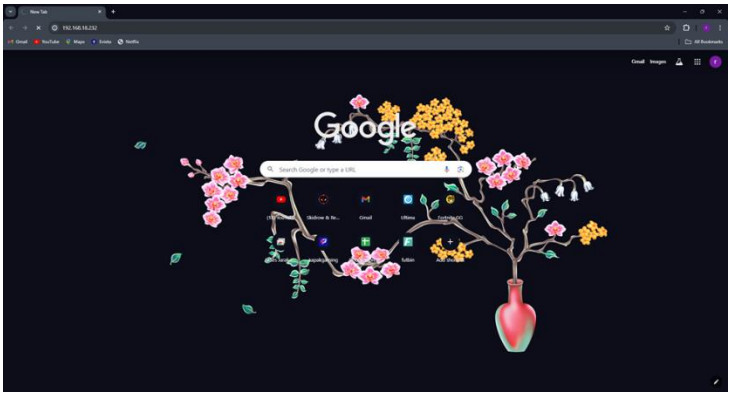
Pada gambar di atas, terlihat bahwa web server Apache2 di Ubuntu telah berhasil dikonfigurasi dengan baik dan berjalan tanpa hambatan yang signifikan seperti lag atau lemot karena belum dilakukan penyerangan DoS dari Kali Linux. Kinerja server terlihat stabil dan responsif terhadap permintaan pengguna, menunjukkan bahwa konfigurasi yang telah diterapkan berfungsi dengan baik dalam menjaga keandalan sistem (Iqbal et al., 2020). Meskipun belum ada serangan yang terdeteksi, tindakan preventif telah diambil dengan mengaktifkan fitur keamanan seperti *mod_security* untuk melindungi server dari potensi serangan DoS (Pratiwi & Adrian, 2024).

3. Simulasi Serangan DoS



Gambar 4. Simulasi Serangan

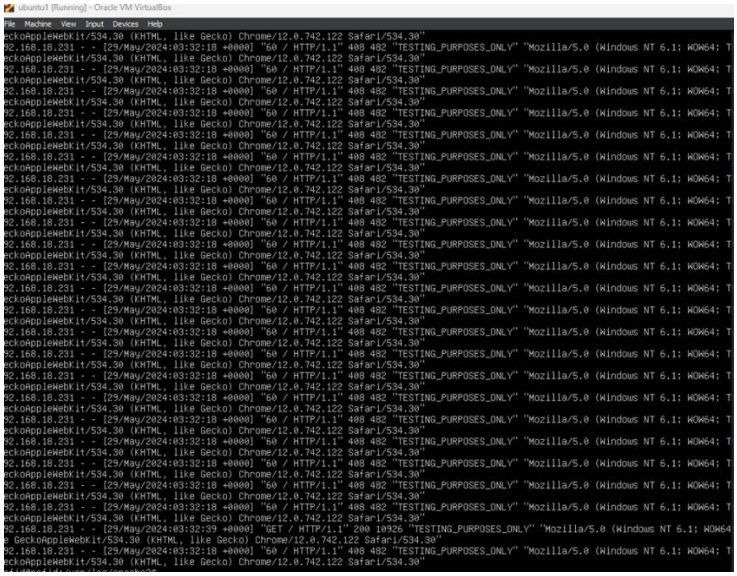
Langkah pertama dalam penelitian adalah melakukan simulasi serangan menggunakan tool slowhttptest. Perintah "slowhttptest -c 100 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://192.168.18.232/ -x 24 -p 3" digunakan untuk memberikan serangan lambat (slow HTTP) terhadap server web sejumlah 100 koneksi simultan dan 200 byte yang akan dikirim dalam setiap putaran. Simulasi ini memungkinkan peneliti untuk mengevaluasi kemampuan server dalam menangani serangan jenis ini dan untuk menilai apakah perlindungan *iptables* efektif dalam mengatasi serangan (Suherdi, 2021).



Gambar 5. Kondisi Web Server saat Penyerangan

Setelah dilakukan serangan DoS melalui Kali Linux menggunakan slowhttptest, terlihat bahwa web server Apache2 di Ubuntu mengalami sedikit keterlambatan saat diakses. Hal ini mungkin disebabkan oleh beban tambahan yang dihasilkan oleh serangan, di mana server harus menangani jumlah koneksi dan lalu lintas yang lebih besar dari biasanya. Meskipun keterlambatan ini mungkin tidak signifikan pada awalnya, namun jika serangan berlanjut atau meningkat dalam intensitasnya, dapat mengakibatkan penurunan kinerja yang lebih parah bahkan hingga layanan menjadi tidak tersedia.

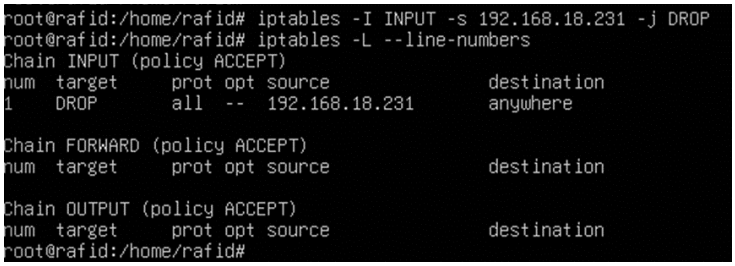
4. Pengecekan Log Aktivitas di Ubuntu



Gambar 6. Pengecekan Log Aktivitas

Setelah simulasi serangan selesai, peneliti melanjutkan dengan mengevaluasi aktivitas server web Apache2 melalui pemeriksaan file access.log di direktori /var/log/apache2/. Dalam proses ini, peneliti berhasil mengidentifikasi alamat IP penyerang, yaitu 192.168.18.231, serta mengamati aktivitas lain yang mencurigakan yang mungkin terjadi selama serangan. Analisis log ini menjadi kunci dalam memahami serangan, membantu peneliti mengenali pola dan sifat serangan, serta merumuskan strategi perlindungan yang lebih efektif untuk masa mendatang. Tindakan ini memberikan wawasan yang berharga dalam menangani dan mencegah serangan siber, serta menjadi dasar untuk penelitian lebih lanjut dalam bidang keamanan sistem informasi.

5. Menangani Serangan DoS



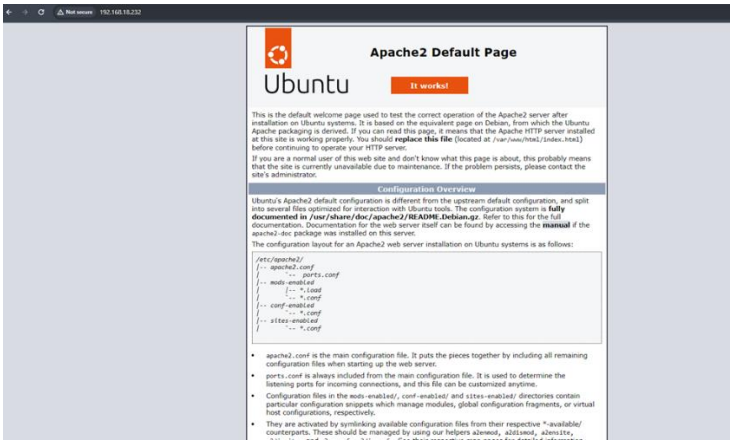
Gambar 7. Memblokir Akses IP Penyerang

Setelah mendapatkan alamat IP penyerang, peneliti mulai menangani serangan tersebut demi mengamankan integritas sistem. Dengan langkah tersebut, peneliti menerapkan aturan atau *rules iptables* untuk memblokir akses dari IP penyerang dengan menggunakan perintah "iptables -I INPUT -s 192.168.18.231 -j DROP". Tindakan ini bertujuan untuk secara efektif menonaktifkan akses dari penyerang ke server, sehingga mengurangi dampak serangan dan melindungi infrastruktur jaringan dari kerentanan yang mungkin dimanfaatkan oleh serangan selanjutnya (Yuliana & Tarmedi, 2016).

Setelah itu, peneliti mengecek kembali log aktivitas untuk memastikan bahwa serangan telah berhasil dihentikan dan tidak ada lagi aktivitas mencurigakan dari alamat IP penyerang. Dengan melakukan verifikasi ini, peneliti dapat memastikan bahwa langkah-langkah mitigasi yang diambil telah berhasil dan server kembali beroperasi dengan normal tanpa gangguan lebih lanjut dari serangan tersebut. Hal ini juga memberikan keyakinan bahwa metode yang digunakan untuk mengatasi serangan dapat diterapkan kembali jika diperlukan di masa mendatang.

Gambar 8. Serangan Gagal Dilakukan

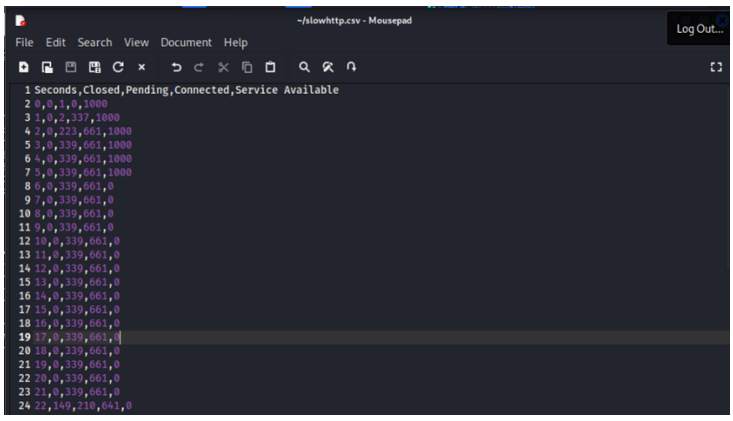
Kemudian peneliti mencoba untuk menyerang kembali web server Apache2 di Ubuntu, namun serangan tersebut tidak berhasil. Hal ini menandakan bahwa aturan *iptables* yang diterapkan efektif dalam memblokir akses dari alamat IP penyerang. Dengan demikian, peneliti berhasil meningkatkan keamanan server terhadap serangan serupa di masa depan. Kesuksesan ini menunjukkan bahwa langkah-langkah mitigasi yang diambil, termasuk pemblokiran IP penyerang, mampu melindungi server dari ancaman DoS, memastikan stabilitas dan ketersediaan layanan web bagi pengguna.



Gambar 9. Mengakses Web Server Setelah Serangan Dihentikan

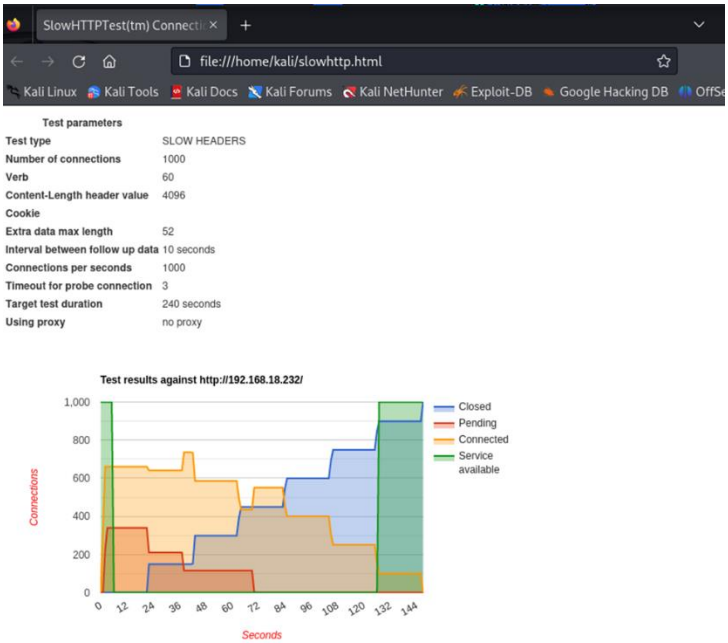
Peneliti juga memastikan kembali dengan mencoba mengakses web server Apache2 dan berhasil melakukannya tanpa mengalami lag atau kelambatan. Ini menunjukkan bahwa server berfungsi dengan baik setelah aturan *iptables* diterapkan untuk memblokir alamat IP penyerang. Langkah verifikasi ini memastikan bahwa tidak hanya serangan telah berhasil dihentikan, tetapi juga bahwa kinerja server tetap optimal dan responsif. Dengan server yang kembali beroperasi normal, pengguna dapat mengakses layanan tanpa hambatan, dan peneliti dapat mengonfirmasi bahwa tindakan mitigasi yang diambil telah sepenuhnya efektif dalam mengatasi serangan DoS. Kesuksesan ini memberikan keyakinan bahwa strategi perlindungan yang diterapkan dapat diandalkan untuk menjaga keamanan dan kinerja sistem di masa mendatang.

6. Pengecekan File *slowhttp.csv* dan *slowhttp.html*



Gambar 10. Pengecekan File slowhttp.csv

Peneliti membuka file slowhttp.csv di Kali Linux yang bertujuan untuk menganalisis hasil dari serangan DoS yang dilakukan menggunakan slowhttptest. File ini berisi data yang mencatat detail serangan, seperti waktu setiap koneksi dibuat, durasi koneksi, status koneksi, dan jumlah data yang ditransfer (Dhanapal & Nithyanandam, 2019). Analisis terhadap file ini memberikan wawasan berharga tentang bagaimana server web merespons serangan, serta titik-titik lemah yang mungkin perlu diperbaiki (Suroto, 2017).



Gambar 11. Pengecekan File slowhttp.html

Membuka file slowhttp.html di Kali Linux bertujuan untuk menganalisis hasil serangan DoS yang dilakukan menggunakan slowhttptest dalam format yang lebih mudah dibaca dan dipahami (Sharafaldin et al., 2018). File ini berisi visualisasi dan laporan yang merangkum data dari serangan, sehingga memudahkan peneliti untuk mengevaluasi dampak dan efektivitas serangan (Shabana et al., 2023).

Simpulan

Dalam proyek ini, peneliti berhasil menerapkan solusi *firewall* menggunakan *iptables* untuk melindungi sistem jaringan dari serangan DoS (*Denial of Service*). Melalui analisis kebutuhan, studi literatur, dan perencanaan implementasi yang cermat, kami berhasil merancang dan mengimplementasikan konfigurasi *firewall* yang efektif. Pengujian fungsional menunjukkan bahwa solusi yang kami terapkan mampu mencegah serangan DoS dengan baik dan memenuhi kebutuhan keamanan sistem jaringan.

Evaluasi kinerja juga menunjukkan bahwa *firewall* yang kami terapkan dapat beroperasi dengan baik tanpa mengorbankan kinerja sistem secara signifikan. Namun, ada beberapa area di mana penyesuaian dan peningkatan dapat dilakukan untuk meningkatkan efektivitas dan efisiensi *firewall*.

Daftar Pustaka

Arlis, S., & Sahari. (2019). Analisis Firewall Demilitarized Zone Dan Switch Port Security Pada Jaringan Universitas Putra Indonesia YPTK. *Jurnal KomtekInfo (Komputer Teknologi Informasi)*, *6*(1), 29–39. http://lppm.upiyptk.ac.id/ojsupi/index.php/KOMTEKINFO

Barends, J. K., Dewanta, F., & Karna, N. B. A. (2022). Perancangan dan Analisis Intrusion Prevention System Berbasis SNORT dan IPTABLES dengan Integrasi Honeypot pada Arsitektur Software Defined Network. *MULTINETICS*, *7*(2), 163–176. https://doi.org/10.32722/multinetics.v7i2.4276

Dehan Pratama, M., Nova, F., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. http://jurnal-itsi.org

Desmira, D., & Wiryadinata, R. (2022). Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knockking. *INSANtek*, *3*(1), 1–5. https://doi.org/10.31294/instk.v3i1.552

Dhanapal, A., & Nithyanandam, P. (2019). The Slow HTTP DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. *Scalable Computing: Practice and Experience*, *20*(4), 669–685. https://doi.org/10.12694/scpe.v20i4.1569

Fadhlillah, A. S., Nyoman Bogi, D. R., & Irawan, A. I. (2019). Analisis Performansi IDS Menggunakan Metode Deteksi Anomaly-Based Terhadap Serangan Dos. *E-Proceeding of Engineering*, *6*(2), 3398–3405.

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika : Jurnal Sistem Komputer*, *11*(1), 67–76. https://doi.org/10.34010/komputika.v11i1.5227

Hawari, M. S., & Kurniawan, I. F. (2016). Penerapan Iptables Firewall Pada Linux Dengan Menggunakan Fedora. *Jurnal Manajemen Informatika*, *6*.

Iqbal, M., Arini, A., & Suseno, H. B. (2020). ANALISA DAN SIMULASI KEAMANAN JARINGAN UBUNTU SERVER DENGAN PORT KNOCKING, HONEYPOT, IPTABLES, ICMP. *Cyber Security Dan Forensik Digital*, *3*(1), 27–32. https://doi.org/10.14421/csecurity.2020.3.1.1933

Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. (2019). Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server. *Jurnal Ilmiah NERO*, *4*(3), 181–188.

Noor, E., Chandra, J. C., Informatika, M., Informasi, T., Luhur, U. B., Ciledug, J. R., Utara, P., Lama, K., & Selatan, J. (2020). Implementasi Firewall Pada Smp Yadika 5 Jakarta. *Jurnal IDEALIS*, *3*(1), 449–456.

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

Shabana, Singh, U. K., Raghuvanshi, A., & Rathore, V. (2023). TOWARDS IDENTIFICATION OF VULNERABILITIES AND THEIR EXPLOITS USING PENETRATION TESTING

TOOLS. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(1), 1792–1798. https://doi.org/10.56726/IRJMETS33212

Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108–116. https://doi.org/10.5220/0006639801080116

Sugianti, N., Galuh, Y., Fatia, S., Fahmi, K., Holle, H., Teknik Informatika, J., Sains, F., Teknologi, D., Negeri, I., Malik, M., Malang, I., Gajayana, J., 50, N., Lowokwaru, K., Malang, K., & Timur, J. (2020). Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno. In *JANUARI* (Vol. 4, Issue 3).

Suherdi, D. (2021). Pemanfaatan Firewall Pada Jaringan Mengunankan Mikrotik RB951Ui – 2HnD. *J-SISKO TECH (Jurnal Teknologi Sistem Informasi Dan Sistem Komputer TGD)*, *4*(2), 173. https://doi.org/10.53513/jsk.v4i2.3304

Suroto, S. (2017). A Review of Defense Against Slow HTTP Attack. *JOIV : International Journal on Informatics Visualization*, *1*(4), 127–134. https://doi.org/10.30630/joiv.1.4.51

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Widianto, T. K., & Sulistyo, W. (2021). Implementasi Iptables Firewall dan Intrusion Detection System Untuk Mencegah Serangan DDoS Pada Linux Server. *MEANS (Media Informasi Analisa Dan Sistem)*, *6*(1), 19–23. http://ejournal.ust.ac.id/index.php/Jurnal_Means/

Yuliana, Y., & Tarmedi, E. (2016). PENGARUH PERBEDAAN INDIVIDU TERHADAP KEPUTUSAN MENGGUNAKAN SISTEM OPERASI LINUX. *Journal of Business Management Education (JBME)*, *1*(1), 176–182. https://doi.org/10.17509/jbme.v1i1.2286