Journal of Internet and Software Engineering Vol: 1, No 3, 2024, Page: 1-10

Implementasi *Firewall* Menggunakan *Iptables* untuk Melindungi Server dari Serangan DDoS

Ihda Rahmadaniar*, Daffa Adrian Ahmadi Tondang, Brilliant Sandynigy Fernando, Aep Setiawan
Teknologi Rekayasa Komputer, Sekolah Vokasi, Institut Pertanian Bogor

Abstrak: Dalam era digital yang semakin berkembang pesat, keamanan siber menjadi krusial bagi keberlanjutan operasional sistem informasi. Serangan *Distributed Denial of Service* (DDoS) merupakan ancaman serius bagi *web server* yang melayani aplikasi kritikal. Serangan ini dapat menyebabkan *server* tidak dapat diakses oleh pengguna yang sah dengan membanjiri *server* dengan lalu lintas berlebihan, mengganggu ketersediaan layanan. Untuk melindungi *web server* dari serangan DDoS, salah satu metode efektif adalah mengimplementasikan *firewall* menggunakan *iptables*. *Iptables* adalah utilitas *firewall* di sistem operasi Linux yang dapat dikonfigurasi untuk memfilter lalu lintas jaringan berdasarkan berbagai kriteria. Penelitian ini bertujuan mengimplementasikan aturan *iptables* untuk melindungi *web server* Apache2 dari serangan DDoS. Pengaturan dilakukan pada *server* Apache2 di Ubuntu sebagai target serangan dan Kali Linux sebagai *platform* untuk melancarkan serangan DDoS. Dengan mensimulasikan serangan dan menerapkan perlindungan menggunakan *iptables,* penelitian ini menunjukkan efektivitas metode ini dalam menjaga keamanan dan ketersediaan layanan *web*. Penelitian ini juga memberikan pemahaman praktis tentang cara serangan DDoS dilakukan dan bagaimana mereka dapat diatasi secara efisien. Hasil penelitian diharapkan memberikan kontribusi berarti dalam bidang keamanan siber, khususnya dalam mitigasi serangan DDoS menggunakan *firewall iptables*, serta memberikan panduan bagi administrator jaringan dalam melindungi infrastruktur *web* mereka.

Kata kunci: Apache2, Ddos, *Firewall*, *Iptables*, Keamanan Siber

DOI: https://doi.org/10.47134/pjise.v1i3.2564
*Correspondence: Ihda Rahmadaniar
Email: ihdarahmadaniar@apps.ipb.ac.id

Received: 21-04-2024
Accepted: 01-05-2024
Published: 31-06-2024

Abstract: *In the rapidly evolving digital era, cybersecurity is crucial for the sustainability of information systems. Distributed Denial of Service (DDoS) attacks pose a serious threat to web servers hosting critical applications by flooding them with excessive traffic, rendering them inaccessible to legitimate users. Implementing a firewall using iptables, a Linux utility for filtering network traffic, is an effective method to protect against such attacks. This research aims to implement iptables rules to safeguard the Apache2 web server from DDoS attacks. The setup involves using Apache2 on Ubuntu as the target server and Kali Linux to launch the DDoS attack. By simulating these attacks and applying iptables protection, this study demonstrates the method's effectiveness in ensuring web service security and availability. Additionally, it provides practical insights into executing and countering DDoS attacks efficiently. The findings are expected to contribute significantly to cybersecurity, especially in DDoS mitigation using iptables, and offer guidance for network administrators in securing web infrastructures.*

Keywords: *Apache2, Cyber Security, Ddos, Firewall, Iptables*

Pendahuluan

Dalam era digital yang semakin berkembang pesat, keamanan siber menjadi salah satu aspek yang sangat krusial bagi keberlanjutan operasional berbagai sistem informasi. Serangan siber, terutama serangan *Distributed Denial of Service* (DDoS), telah menjadi ancaman serius bagi *web server* yang melayani berbagai aplikasi kritikal (Parulian et al., 2021). Serangan DDoS dapat menyebabkan *server* tidak dapat diakses oleh pengguna yang sah dengan membanjiri *server* dengan lalu lintas yang berlebihan, sehingga mengganggu ketersediaan layanan (Ridho & Arman, 2020). Oleh karena itu, diperlukan solusi yang efektif untuk melindungi *web server* dari jenis serangan ini.

Salah satu metode yang dapat digunakan untuk melindungi *web server* dari serangan DDoS adalah dengan mengimplementasikan *firewall* menggunakan *iptables* (Widianto & Sulistyo, 2021). *Iptables* merupakan utilitas *firewall* yang tersedia di sistem operasi berbasis Linux dan dapat dikonfigurasi untuk memfilter lalu lintas jaringan berdasarkan berbagai kriteria (Hawari & Kurniawan, 2016). Dengan konfigurasi yang tepat, *iptables* dapat digunakan untuk mendeteksi dan memblokir lalu lintas berbahaya, sehingga menjaga kestabilan dan ketersediaan *web server* (Nida & Adrian, 2023).

Penelitian ini bertujuan untuk mengimplementasikan serangkaian aturan *iptables* yang dapat melindungi *web server* Apache2 dari serangan DDoS. Proses ini mencakup pengaturan *server* Apache2 pada sistem operasi Ubuntu sebagai target serangan dan penggunaan Kali Linux sebagai *platform* untuk melancarkan serangan DDoS. Dengan menyimulasikan serangan DDoS dan menerapkan perlindungan menggunakan *iptables*, penelitian ini bertujuan untuk menunjukkan efektivitas metode ini dalam menjaga keamanan dan ketersediaan layanan *web*.

Selain itu, penelitian ini juga bertujuan untuk memberikan pemahaman praktis tentang bagaimana serangan DDoS dilakukan dan bagaimana mereka dapat diatasi secara efisien. Menggunakan dua sistem operasi berbeda, yaitu Ubuntu dan Kali Linux, memungkinkan pengujian yang komprehensif dan mendalam terhadap skenario serangan dan perlindungan. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi yang berarti dalam bidang keamanan siber, khususnya dalam mitigasi serangan DDoS menggunakan *firewall iptables*.

Dengan demikian, penelitian ini tidak hanya berfokus pada deteksi dan mitigasi serangan DDoS, tetapi juga memberikan wawasan tentang langkah-langkah praktis yang dapat diambil oleh administrator jaringan untuk melindungi infrastruktur *web* mereka. Kesimpulan dari penelitian ini diharapkan dapat menjadi panduan bagi pengembang dan profesional keamanan siber dalam mengimplementasikan strategi perlindungan yang efektif terhadap ancaman siber yang semakin kompleks dan beragam.

Metode

Penelitian ini menggunakan pendekatan kombinasi antara metode studi literatur dan studi kasus untuk mengevaluasi efektivitas penggunaan *iptables* dalam mitigasi serangan *Distributed Denial of Service* (DDoS) pada *web server* Apache2. Metodologi ini dipilih untuk mendapatkan pemahaman yang mendalam dan komprehensif mengenai strategi perlindungan terhadap serangan DDoS serta penerapan praktisnya di lingkungan nyata.

Studi literatur dilakukan untuk mengumpulkan dan menganalisis informasi yang relevan dari berbagai sumber akademis dan teknis. Proses ini dimulai dengan mengidentifikasi dan mengumpulkan sumber-sumber seperti buku, jurnal, artikel ilmiah, laporan penelitian, dan dokumentasi teknis yang berkaitan dengan serangan DDoS, *iptables*, dan keamanan *web server*. Selanjutnya, dilakukan telaah kritis terhadap literatur yang terkumpul untuk memahami berbagai jenis serangan DDoS, dampaknya pada *web server*, dan metode mitigasinya.

Analisis ini membantu mengidentifikasi konsep dan teknik utama dalam penggunaan *iptables* sebagai *firewall* untuk melindungi *server* dari serangan DDoS. Selain itu, studi literatur ini juga bertujuan untuk menentukan celah-celah dalam penelitian yang ada dan area yang memerlukan eksplorasi lebih lanjut, terutama dalam konteks aplikasi praktis *iptables* untuk mitigasi serangan DDoS.

Studi kasus dilakukan untuk menguji dan mengevaluasi penerapan aturan *iptables* dalam mitigasi serangan DDoS pada lingkungan nyata. Kasus studi ini melibatkan dua sistem operasi: Ubuntu sebagai server Apache2 dan Kali Linux sebagai mesin penyerang. Konfigurasi *server* Apache2 di Ubuntu dan penyiapan SSH di kedua sistem operasi dilakukan untuk keperluan *remote access* dan monitoring. Pada tahap ini, serangan DDoS disimulasikan menggunakan Kali Linux untuk melancarkan serangan terhadap *web server* Apache2 yang berjalan di Ubuntu. Teknik yang digunakan termasuk pengiriman sejumlah besar permintaan SYN untuk membanjiri *server*.

Setelah serangan DDoS dilancarkan, langkah berikutnya adalah menyusun dan menerapkan aturan *iptables* pada *server* Ubuntu untuk mendeteksi dan memitigasi serangan tersebut. Aturan yang diterapkan mencakup pembatasan jumlah koneksi SYN per detik dan pemblokiran lalu lintas berbahaya. Data performa *server* dikumpulkan sebelum, selama, dan setelah serangan DDoS, mencakup waktu respon, tingkat keberhasilan permintaan, dan penggunaan sumber daya. Analisis data dilakukan untuk mengevaluasi dampak serangan DDoS dan efektivitas perlindungan yang diterapkan.

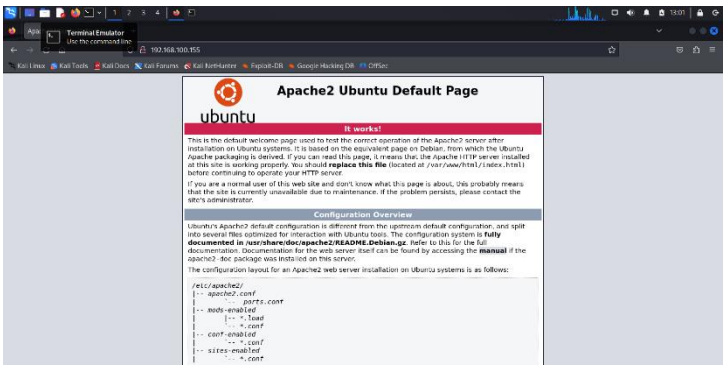
Hasil dan Pembahasan

Penelitian ini bertujuan untuk mengevaluasi efektivitas penggunaan aturan *iptables* dalam perlindungan terhadap serangan *Distributed Denial of Service* (DDoS) pada *server web* Apache2, serta untuk menguji respons *server* terhadap serangan tersebut. Dalam rangka mencapai tujuan tersebut, serangkaian langkah-langkah telah diimplementasikan dan dievaluasi. Langkah pertama melibatkan konfigurasi pada dua sistem operasi yang digunakan, yaitu Kali Linux dan Ubuntu.

Tabel 1. Spesifikasi OS pada Virtual Box

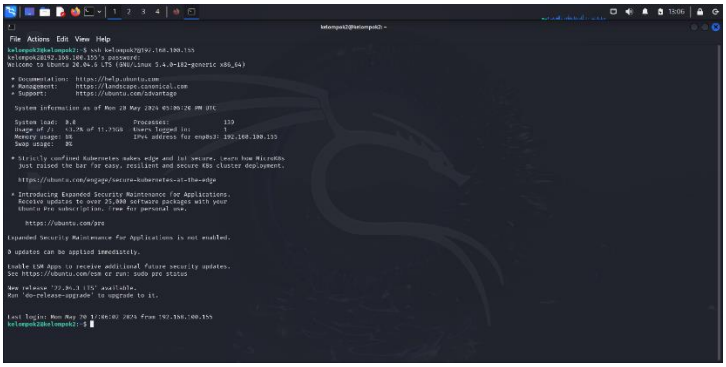
OS	Kali Linux	Ubuntu
Versi	Kali Linux 2024.1	Ubuntu 20.04.6
RAM	2048 MB	4096 MB
CPU	2	2
Penyimpanan	25 GB	25 GB
Jaringan	*Bridge Adapter*	*Bridge Adapter*

Dalam tabel di atas, konfigurasi spesifikasi OS disusun untuk mesin virtual menggunakan VirtualBox. Konfigurasi tersebut mencakup beberapa aspek penting seperti versi OS, alokasi RAM, jumlah core CPU, kapasitas penyimpanan, dan konfigurasi jaringan. Dengan menggunakan konfigurasi ini, kedua mesin virtual Kali Linux dan Ubuntu dapat dijalankan secara efisien dalam lingkungan VirtualBox, memungkinkan untuk pengujian penelitian ini dengan aman dan efektif (Purwoko & Hilal, 2019).



Gambar 1. Web Server Apache2 pada IP Ubuntu

Dari konfigurasi yang telah dilakukan, peneliti memperoleh alamat IP untuk kedua OS tersebut, yaitu 192.168.100.155 untuk Ubuntu dan 192.168.100.154 untuk Kali Linux. Selanjutnya, peneliti mengonfigurasi layanan SSH pada kedua OS serta mengatur web *server* Apache2 pada OS Ubuntu. Dengan konfigurasi ini, peneliti dapat menjalankan koneksi SSH ke masing-masing OS dan mengelola layanan *web server* Apache2 di OS Ubuntu. Langkah-langkah ini memungkinkan peneliti untuk melakukan pengujian dan analisis terkait keamanan dan responsibilitas sistem di kedua OS secara terpisah, serta untuk memvalidasi efektivitas perlindungan yang diterapkan terhadap serangan DDoS pada *server web* Apache2.



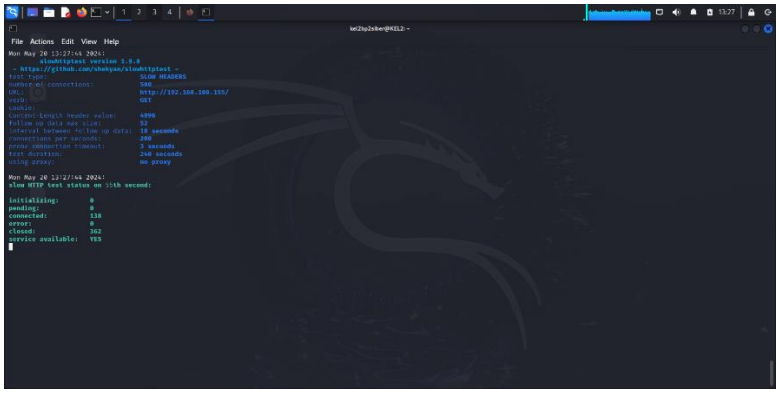
Gambar 2. Akses SSH dari Kali Linux ke Ubuntu

Setelah konfigurasi awal selesai, peneliti melakukan pengecekan terhadap konektivitas SSH dari Kali Linux ke Ubuntu. Dengan menggunakan perintah SSH, peneliti memeriksa apakah koneksi antara kedua sistem operasi berfungsi dengan baik (Aulianita et al., 2021). Langkah ini penting untuk memastikan bahwa pengaturan jaringan dan layanan SSH telah dikonfigurasi dengan benar, sehingga memungkinkan akses yang aman dan terenkripsi antara kedua OS. Dengan berhasilnya pengecekan konektivitas SSH, peneliti dapat melanjutkan ke tahap berikutnya dalam penelitian, termasuk pengujian dan

implementasi aturan *iptables* serta pengujian serangan DDoS terhadap *web server* Apache2 yang berjalan pada OS Ubuntu.

Dalam rangka implementasi aturan *iptables* untuk melindungi *server* dari serangan *Distributed Denial of Service* (DDoS), langkah-langkah yang dilakukan peneliti disusun secara berurutan sebagai berikut:

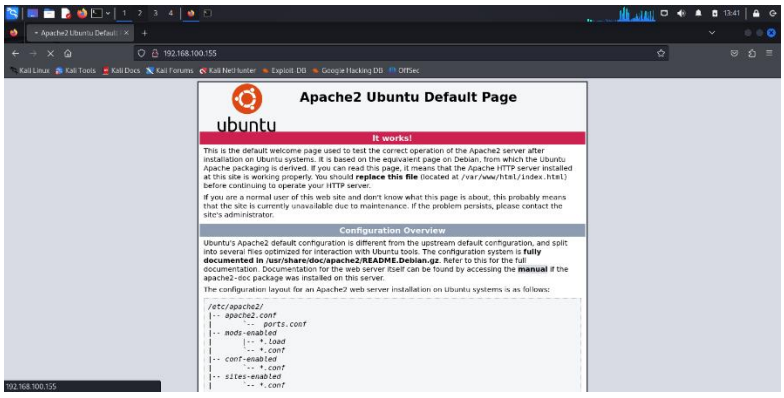
1. Simulasi Serangan dengan *slowhttptest*



Gambar 3. Melakukan Serangan DDoS ke *Web Server* pada Ubuntu

Langkah pertama dalam penelitian adalah melakukan simulasi serangan menggunakan *tool slowhttptest*. Perintah ***"slowhttptest -c 500 -H -g -o slowhttp -i 10 -r 500 -t GET -u http://192.168.100.155/ -x 24 -p 3"*** digunakan untuk memberikan serangan lambat (slow HTTP) terhadap server web (Pratiwi & Adrian, 2024). Simulasi ini memungkinkan peneliti untuk mengevaluasi kemampuan *server* dalam menangani serangan jenis ini dan untuk menilai apakah perlindungan *iptables* efektif dalam mengatasi serangan.

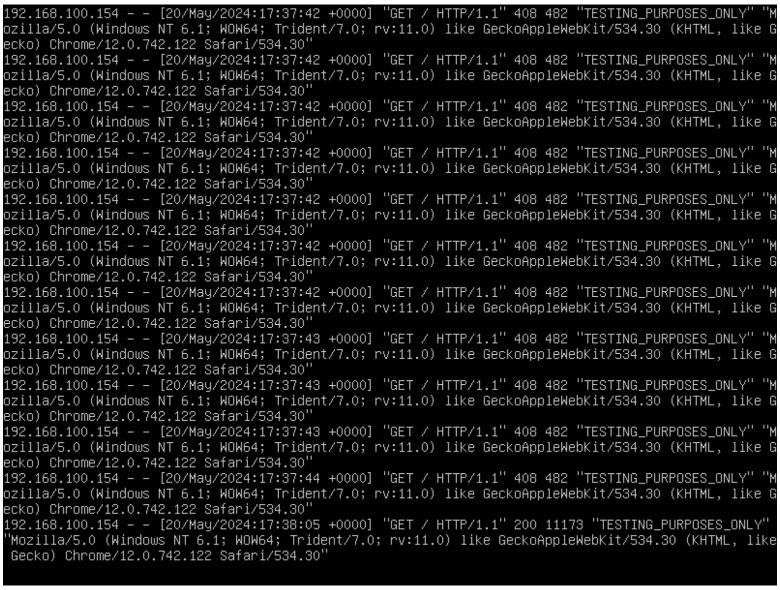
2. Akses *Web Server* dan Cek Log Aktivitas untuk Mendeteksi Serangan



Gambar 4. Mengakses *Web Server* Saat Terjadi Penyerangan

Setelah melakukan simulasi serangan, peneliti mengakses kembali *web server* Apache2 dan menemukan bahwa akses menjadi sangat lambat dan sering mengalami lag. Hal ini menunjukkan bahwa serangan *slow* HTTP berhasil mempengaruhi kinerja *server*, menyebabkan penurunan kecepatan akses dan responsibilitas. Kondisi ini menegaskan

dampak nyata dari serangan DDoS terhadap *server web*, yang berpotensi mengganggu layanan dan pengalaman pengguna (Noor et al., 2020).

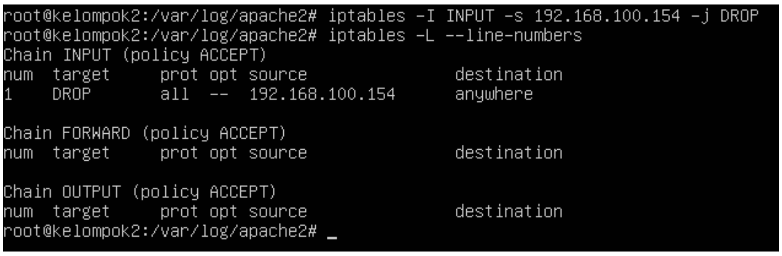


```
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:42 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:43 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:43 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:43 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:37:44 +0000] "GET / HTTP/1.1" 408 482 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
192.168.100.154 - - [20/May/2024:17:38:05 +0000] "GET / HTTP/1.1" 200 11173 "TESTING_PURPOSES_ONLY" "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like GeckoAppleWebKit/534.30 (KHTML, like Gecko) Chrome/12.0.742.122 Safari/534.30"
```

Gambar 5. Log Aktivitas pada Ubuntu Saat Penyerangan

Setelah simulasi serangan dilakukan, peneliti memeriksa log aktivitas *server web* Apache2 untuk melihat apakah ada tanda-tanda serangan yang terdeteksi. Dengan memeriksa file *access.log* di direktori */var/log/apache2/*, peneliti dapat mengidentifikasi alamat IP penyerang yaitu 192.168.100.154 dan aktivitas lain yang mencurigakan.

3. Implementasi Aturan iptables untuk Memproteksi Server



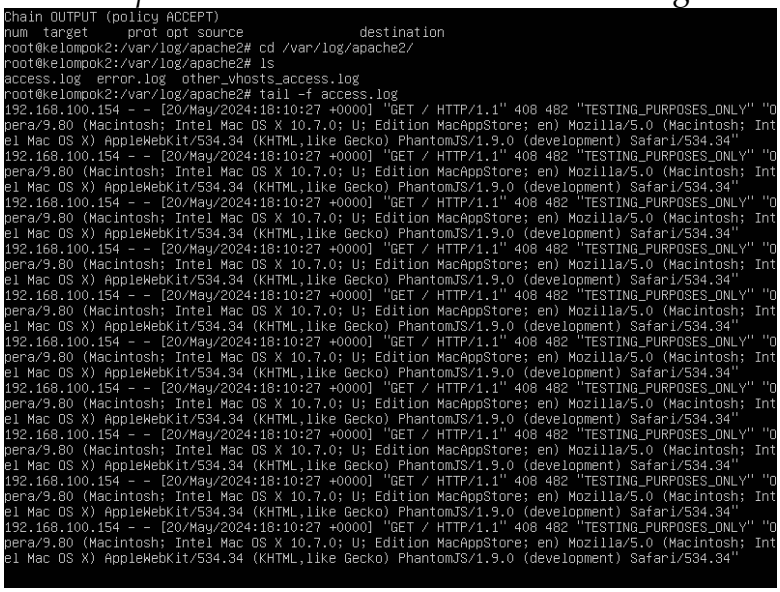
```
root@kelompok2:/var/log/apache2# iptables -I INPUT -s 192.168.100.154 -j DROP
root@kelompok2:/var/log/apache2# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  192.168.100.154      anywhere

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@kelompok2:/var/log/apache2# _
```

Gambar 6. Memblokir Akses IP Penyerang

Setelah mendeteksi serangan, peneliti menerapkan aturan *iptables* untuk memproteksi server. Perintah ***"iptables -I INPUT -s 192.168.100.154 -j DROP"*** digunakan untuk memblokir akses dari alamat IP penyerang, sehingga memungkinkan *server* untuk menolak akses dari sumber yang dipandang berpotensi berbahaya. Aturan ini bertujuan untuk menghentikan serangan dan melindungi *server* dari ancaman lebih lanjut (Fadhlillah et al., 2019). Kemudian, perintah ***"iptables -L --line-numbers"*** dijalankan untuk memeriksa apakah aturan *iptables* yang diterapkan untuk melindungi *server* sudah terimplementasi dengan benar atau belum (Santoso, 2020).

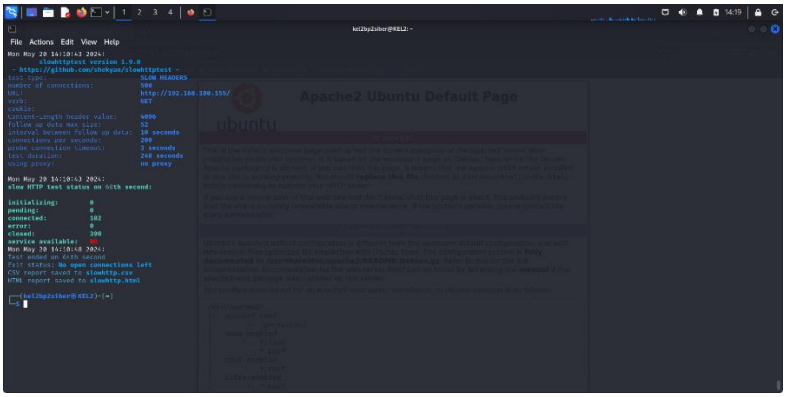
4. Cek Log Aktivitas untuk Melihat Apakah Serangan Sudah Terhenti

Setelah menerapkan aturan *iptables*, peneliti kembali memeriksa log aktivitas *server* di */var/log/apache2/ access.log* untuk memastikan bahwa serangan telah terhenti. Peneliti mencari tanda-tanda bahwa alamat IP penyerang tidak lagi dapat mengakses *server*, yang menunjukkan bahwa aturan *iptables* telah berhasil memblokir serangan.



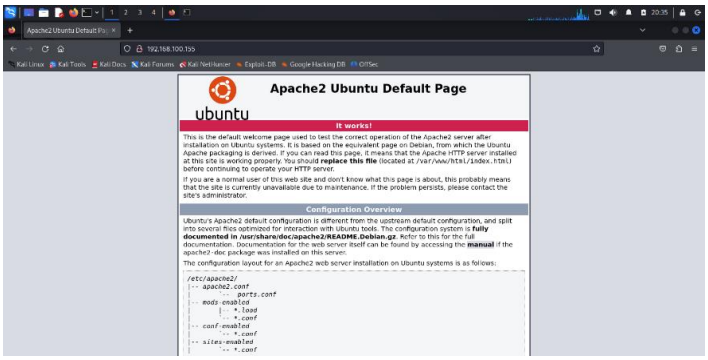
Gambar 7. Pengecekan Kembali pada Log Aktivitas

Dapat dilihat seperti pada gambar di bawah ini, pada log aktivitas serangan di Kali Linux yang digunakan sebagai mesin penyerang, bahwa serangan telah berhenti pada percobaan ke-64. Hal ini menunjukkan bahwa implementasi aturan *iptables* berhasil memblokir akses dari IP penyerang (Arwananing Tyas et al., 2022). Dengan demikian, peneliti berhasil menghentikan serangan DDoS yang sedang berlangsung.



Gambar 8. Aktivitas Serangan telah Terhenti

Selanjutnya, peneliti juga melakukan pengecekan dengan mengakses kembali *web server* Apache2 yang berjalan di Ubuntu. Hasilnya menunjukkan bahwa akses ke *web server* sudah kembali normal, tidak ada lagi kelambatan atau lag yang sebelumnya terjadi. Hal ini menegaskan bahwa tindakan proteksi yang diterapkan melalui aturan *iptables* telah berhasil menghentikan serangan DDoS dan memulihkan performa *server* (Dehan Pratama et al., 2022).



Gambar 9. Mengakses Web Server Setelah Serangan Terhenti

Bukti ini memperkuat bahwa langkah-langkah yang diambil untuk melindungi *server* web dari ancaman serangan DDoS efektif. Implementasi aturan *iptables* yang dilakukan mampu mengenali dan memutus koneksi dari sumber yang mencurigakan, sehingga mencegah kerusakan lebih lanjut pada *server*. Keberhasilan ini juga menunjukkan bahwa solusi yang diterapkan dapat diandalkan untuk menjaga kestabilan dan keamanan *server* dalam menghadapi serangan serupa di masa mendatang.

5. Menghapus Aturan Blokir Akses IP Penyerang

```
root@kelompok2:/home/kelompok2# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    DROP       all  --  192.168.100.154      anywhere

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@kelompok2:/home/kelompok2# iptables -D INPUT 1
root@kelompok2:/home/kelompok2# iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
root@kelompok2:/home/kelompok2#
```

Gambar 10. Menghapus Aturan Blokir Akses IP Penyerang

Kemudian, peneliti juga memiliki opsi untuk menghapus aturan pemblokiran akses dari IP penyerang menggunakan perintah ***"iptables -D INPUT [nomor baris]"***. Langkah ini dilakukan jika serangan tersebut hanya merupakan simulasi atau bagian dari percobaan penelitian seperti yang dilakukan oleh peneliti. Dengan menghapus aturan pemblokiran, *web server* Apache2 dapat diakses kembali tanpa hambatan dari IP yang sebelumnya diblokir (Kusuma, 2022).

Hal ini penting untuk mengembalikan kondisi jaringan ke keadaan normal setelah pengujian selesai, memastikan bahwa tidak ada gangguan akses bagi pengguna yang sah (Haris et al., 2022). Penghapusan aturan ini juga memungkinkan peneliti untuk melakukan pengujian ulang atau eksperimen lainnya di masa depan, tanpa harus terganggu oleh aturan pemblokiran yang sudah tidak diperlukan lagi. Dengan demikian, *server* tetap dalam kondisi optimal untuk melayani kebutuhan pengguna dan menjalankan fungsinya dengan baik.

Simpulan

Hasil dari simulasi serangan menunjukkan bahwa *server web* mengalami kelambatan dan lag yang signifikan, menandakan bahwa serangan berhasil mempengaruhi kinerja *server*. Peneliti kemudian menerapkan aturan *iptables* dengan perintah ***"iptables -I INPUT -s [IP penyerang] -j DROP"*** untuk memblokir akses dari IP penyerang. Setelah aturan diterapkan, peneliti memantau dan menganalisis log aktivitas *server* untuk memastikan bahwa serangan telah berhenti.

Pemantauan lebih lanjut menggunakan perintah ***"iptables -L --line-numbers"*** memastikan bahwa aturan *iptables* telah terimplementasi dengan benar. Peneliti juga mengecek kembali akses ke *web server* dan menemukan bahwa performa *server* telah kembali normal, tanpa kelambatan atau lag.

Kesimpulannya, penelitian ini berhasil menunjukkan bahwa aturan *iptables* efektif dalam melindungi *server web* dari serangan DDoS. Implementasi aturan *iptables* dapat secara efektif memblokir akses dari sumber yang mencurigakan, memulihkan kinerja *server*, dan menjaga stabilitas layanan. Selain itu, kemampuan untuk menghapus aturan pemblokiran setelah percobaan membuktikan fleksibilitas dan kepraktisan metode ini dalam pengelolaan keamanan *server*. Dengan langkah-langkah ini, *server* dapat tetap aman dan responsif terhadap ancaman serangan serupa di masa mendatang.

Daftar Pustaka

Arwananing Tyas, Z., Firdonsyah, A., & Ramdhani, W. (2022). Analisis Keamanan Jaringan dari Serangan DoS pada Sistem Inventaris Sanggar Tari Natya Lakshita menggunakan IDS. Informatics Journal, 7(3), 258–267.

Aulianita, R., Musyaffa, man, & Martiwi, R. (2021). Penggunaan Metode IDS Dalam Implementasi Firewall Pada Jaringan Untuk Deteksi Serangan Distributed Denial Of Service (DDoS). Jusikom : Jurnal Sistem Komputer Musirawas Rizki Aulianita, Dkk, 6(2), 94–104.

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

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.

Kusuma, G. H. A. (2022). Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19. Journal of Informatics and Advanced Computing (JIAC), 3(1), 52–56.

Nida, H., & Adrian, R. (2023). Analisis Perbedaan Pengaruh Penggunaan Iptables Chains dalam Mencegah Denial of Service (DoS) pada Jaringan IoT. Journal of Internet and Software Engineering, 4(1), 12–17.

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.

Parulian, S., Pratiwi, D. A., & Cahya Yustina, M. (2021). Ancaman dan Solusi Serangan Siber di Indonesia. Jurnal TECHNET: Telecommunications, Networks, Electronics, and Computer Technologies, 1(2), 86–92. http://ejournal.upi.edu/index.php/TELNECT/

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), 63–75. https://doi.org/10.28932/jutisi.v10i1.6995

Purwoko, M., & Hilal, H. (2019). Analisis Penerapan Firewall Nftables Sebagai Sistem Keamanan Server Pada Mesin Virtualisasi. Jurnal Telekomunikasi Dan Komputer, 9(1), 1–22. https://doi.org/10.22441/incomtech.v9i1.5676

Ridho, M. A., & Arman, M. (2020). Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan. Jurnal Sisfokom (Sistem Informasi Dan Komputer), 9(3), 373–379. https://doi.org/10.32736/sisfokom.v9i3.945

Santoso, J. D. (2020). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. INFOS Journal, 1(3), 44–50.

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/