Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

Analisis dan Pencegahan Serangan DDoS Pada Jaringan Skala Besar

Rakhmadi Rahman, Ghina R.S Odja

Prodi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Juni 2024
Revisi Juni 2024
Diterima Juli 2024

Kata Kunci:
Serangan DDoS (Distributed Denial of Service), Jaringan skala besar, Pencegahan dan mitigasi serangan DDoS, Teknologi keamanan cyber, Analisis pola serangan DDoS, Dampak teknis dan finansial serangan DDoS, Strategi keamanan komprehensif.

*Penulis Korespondensi:
ghinarsodja@gmail.com

ABSTRAK

Evolusi teknologi jaringan telah mencapai masa kritis, dan arsitektur Internet saat ini mencapai batasnya dalam memenuhi kebutuhan modern. Serangan DDoS (Distributed Denial of Service) adalah salah satu ancaman terbesar di dunia keamanan siber saat ini. Serangan-serangan ini dapat menimbulkan dampak teknis dan ekonomi yang signifikan terhadap korbannya. Tujuan dari penelitian ini adalah untuk mengidentifikasi jenis serangan DDoS yang menargetkan jaringan besar dan menemukan cara efektif untuk mencegah dan mengurangi dampak serangan tersebut. Fokus penelitian mencakup pengklasifikasian jenis serangan DDoS, analisis pola serangan umum, dan evaluasi teknik pencegahan dan mitigasi yang paling efektif. Temuan kami menunjukkan bahwa serangan DDoS pada jaringan besar dapat dikategorikan menjadi serangan lapisan aplikasi dan serangan volumetrik. Simulasi serangan DDoS dilakukan untuk menganalisis dampak dan menguji efektivitas pertahanan menggunakan iptables. Penelitian ini bertujuan untuk mengembangkan strategi keamanan komprehensif untuk melindungi jaringan besar dari ancaman DDoS.

ABSTRACT

The evolution of network technology has reached a critical juncture, and the current architecture of the Internet has reached its limits in meeting modern needs. DDoS (Distributed Denial of Service) attacks are one of the biggest threats in the cybersecurity world today. These attacks can have significant technical and economic impacts on their victims. The goal of this study is to identify the types of DDoS attacks that target large networks and find effective ways to prevent and mitigate the impact of such attacks. The focus of the research includes classifying the types of DDoS attacks, analyzing common attack patterns, and evaluating the most effective prevention and mitigation techniques. Our findings suggest that DDoS attacks on large networks can be categorized into application-layer attacks and volumetric attacks. DDoS attack simulations are conducted to analyze the impact and test the effectiveness of the defense using iptables. The research aims to develop a comprehensive security strategy to protect large networks from DDoS threats.

PENDAHULUAN

Perkembangan teknologi jaringan telah mencapai titik kritis di mana arsitektur internet yang ada saat ini mulai menunjukkan keterbatasan dalam menghadapi tuntutan modern. Seiring dengan pertumbuhan pesat jumlah perangkat yang terhubung ke internet dan peningkatan volume data yang dikirimkan, kebutuhan akan arsitektur internet yang lebih canggih menjadi semakin mendesak. Arsitektur internet generasi saat ini, yang didesain beberapa dekade yang lalu, dirancang untuk lingkungan yang jauh lebih sederhana dibandingkan dengan kondisi teknologi dan ancaman keamanan yang ada saat ini.

Serangan DDoS (Distributed Denial of Service) merupakan salah satu ancaman utama dalam dunia keamanan *cyber* saat ini. Serangan ini melibatkan penggunaan jaringan komputer yang terdistribusi secara geografis untuk secara simultan mengirimkan lalu lintas yang besar ke sebuah target, dengan tujuan untuk mengganggu atau menghentikan layanan yang disediakan oleh target tersebut. Serangan DDoS memanfaatkan kelemahan infrastruktur jaringan target, seperti bandwidth atau sumber daya komputasi, dengan cara membanjiri target tersebut dengan permintaan lalu lintas yang melebihi kapasitas normalnya. yang mengakibatkan layanan yang diserang menjadi tidak responsif atau tidak dapat diakses sama sekali bagi pengguna yang sah.

Perkembangan teknologi telah memperburuk dampak dari serangan DDoS ini. Dengan makin banyaknya perangkat yang terhubung ke internet, baik melalui *Internet of Things* (IoT), komputer pribadi, atau perangkat mobile, potensi untuk membentuk botnet yang besar untuk melancarkan serangan semakin meningkat. Botnet ini sering kali terdiri dari ribuan hingga jutaan perangkat yang dikompromikan dan dikendalikan tanpa sepengetahuan pemiliknya.

Dampak dari serangan DDoS tidak hanya bersifat teknis, tetapi juga dapat memiliki konsekuensi finansial yang serius bagi korban. Perusahaan dapat mengalami kerugian besar karena *downtime* yang tidak terduga pada layanan mereka, yang pada gilirannya dapat mempengaruhi reputasi dan kepercayaan pelanggan. Untuk melawan serangan DDoS, industri keamanan *cyber* terus mengembangkan strategi dan teknologi baru. Ini termasuk penggunaan sistem deteksi dini yang lebih canggih, teknik mitigasi lalu lintas yang adaptif, dan penggunaan layanan proteksi DDoS yang disediakan oleh penyedia layanan keamanan atau CDN (Content Delivery Network).

RUMUSAN MASALAH

A. Apa saja jenis-jenis serangan DDoS yang umum terjadi pada jaringan skala besar?
B. Bagaimana cara yang efektif untuk mencegah dan mengurangi dampak serangan DDoS?

TUJUAN

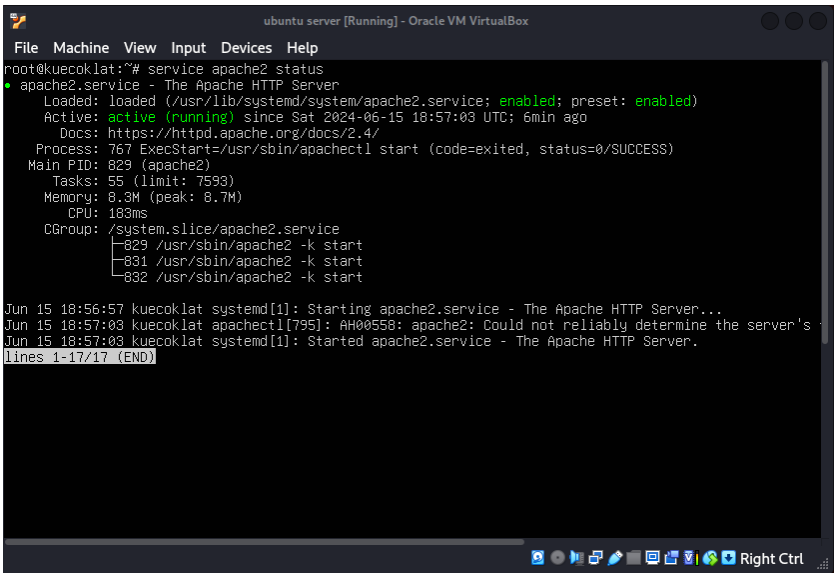
Penelitian ini bertujuan untuk mengidentifikasi jenis-jenis serangan DDoS yang menargetkan jaringan skala besar dan menemukan metode yang efektif untuk mencegah serta mengurangi dampak serangan tersebut. Fokus penelitian ini meliputi pengkategorian tipe-tipe serangan DDoS, analisis pola serangan yang umum, dan evaluasi teknologi pencegahan serta teknik mitigasi yang paling efektif. Hasil penelitian ini diharapkan dapat mengembangkan strategi keamanan yang komprehensif untuk melindungi jaringan skala besar dari ancaman DDoS.

HASIL DAN PEMBAHASAN

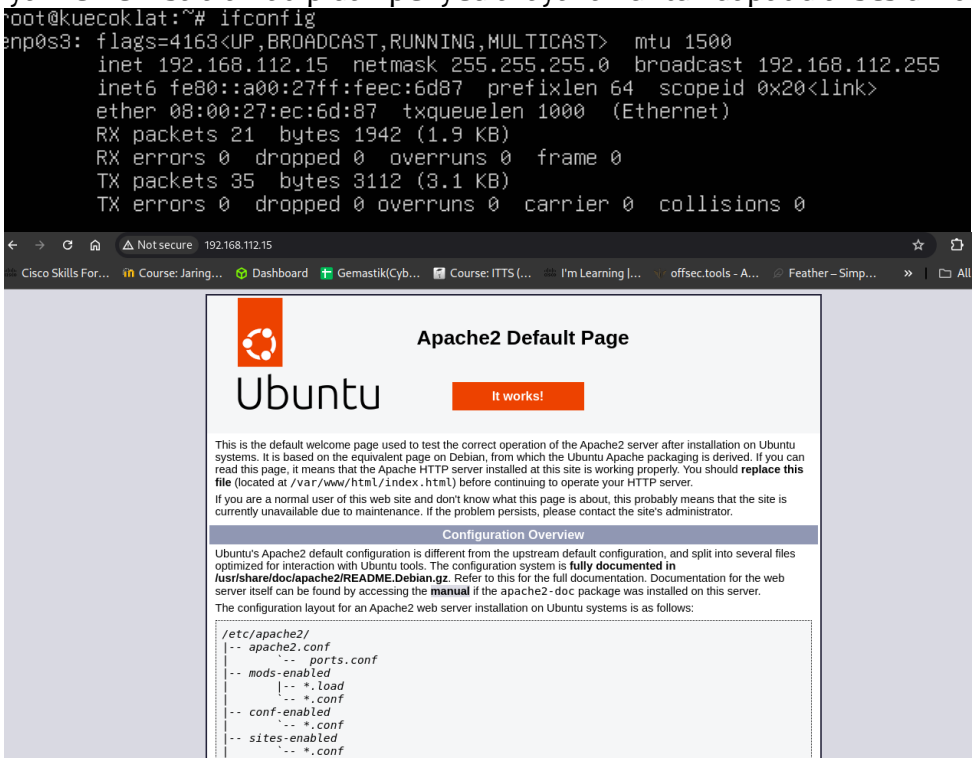
Serangan DDoS (Distributed Denial of Service) pada jaringan skala besar dapat dikategorikan menjadi beberapa jenis, termasuk serangan pada layer aplikasi dan serangan volumetrik. Serangan DDoS layer aplikasi melibatkan penggunaan program atau alat yang dirancang untuk melancarkan serangan dengan tujuan membuat layanan atau sumber daya jaringan tidak tersedia bagi pengguna yang sah. Ini dicapai dengan membanjiri server target dengan trafik berlebihan yang mengakibatkan server tidak dapat menangani permintaan yang sah. Di sisi lain, serangan volumetrik DDoS bertujuan untuk membanjiri target dengan sejumlah besar data, sehingga target kewalahan dan tidak dapat melayani permintaan yang sah. Berbeda dengan serangan aplikasi yang fokus pada mengganggu fungsi spesifik dari target, serangan volumetrik berusaha untuk mengonsumsi seluruh bandwidth yang tersedia, menyebabkan gangguan pada tingkat jaringan. Kedua jenis serangan ini, meskipun berbeda dalam pendekatan, sama-sama berpotensi mengganggu operasional jaringan secara signifikan.

Dalam penelitian ini, saya melakukan simulasi serangan DDoS untuk menganalisis dampaknya dan menguji efektivitas mitigasinya menggunakan iptables. Simulasi ini dilakukan dengan memanfaatkan dua mesin virtual, yaitu Ubuntu Server sebagai target dan Kali Linux sebagai platform untuk melancarkan serangan.

1. **Persiapan:** Kami menyiapkan dua mesin virtual: satu dengan Ubuntu Server yang menjalankan layanan Apache2, dan satu lagi dengan Kali Linux yang dilengkapi dengan alat slowhttptest untuk melancarkan serangan. Selain itu, koneksi jaringan internet yang stabil juga diperlukan.
2. Sebelum memulai serangan, langkah awal yang dapat kita lakukan adalah dengan membuat sebuah layanan yang dibuat pada ubuntu server dalam hal ini kita menggunakan server apache2.

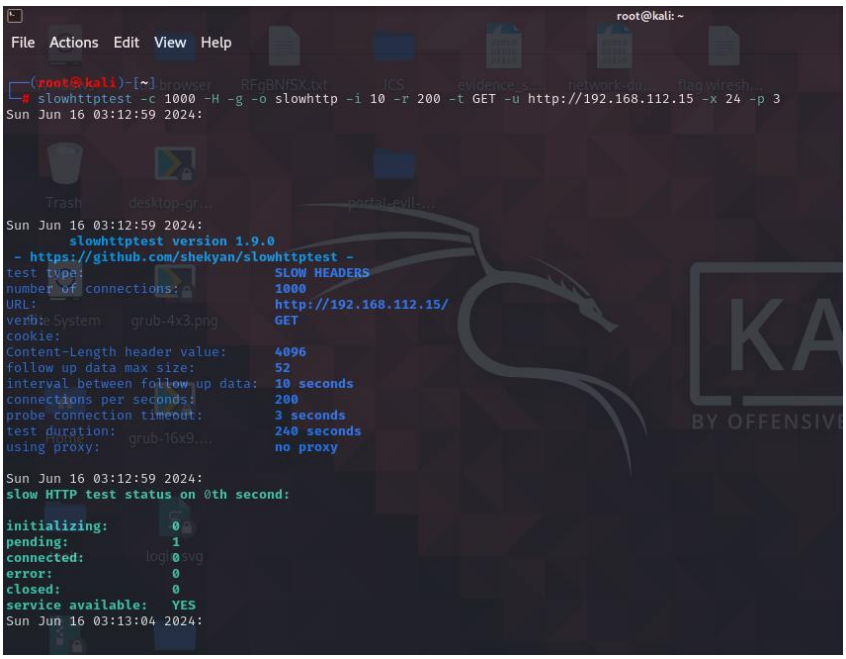


3. Selanjutnya memeriksa alamat ip dari penyedia layanan untuk dapat diakses di komputer lain.

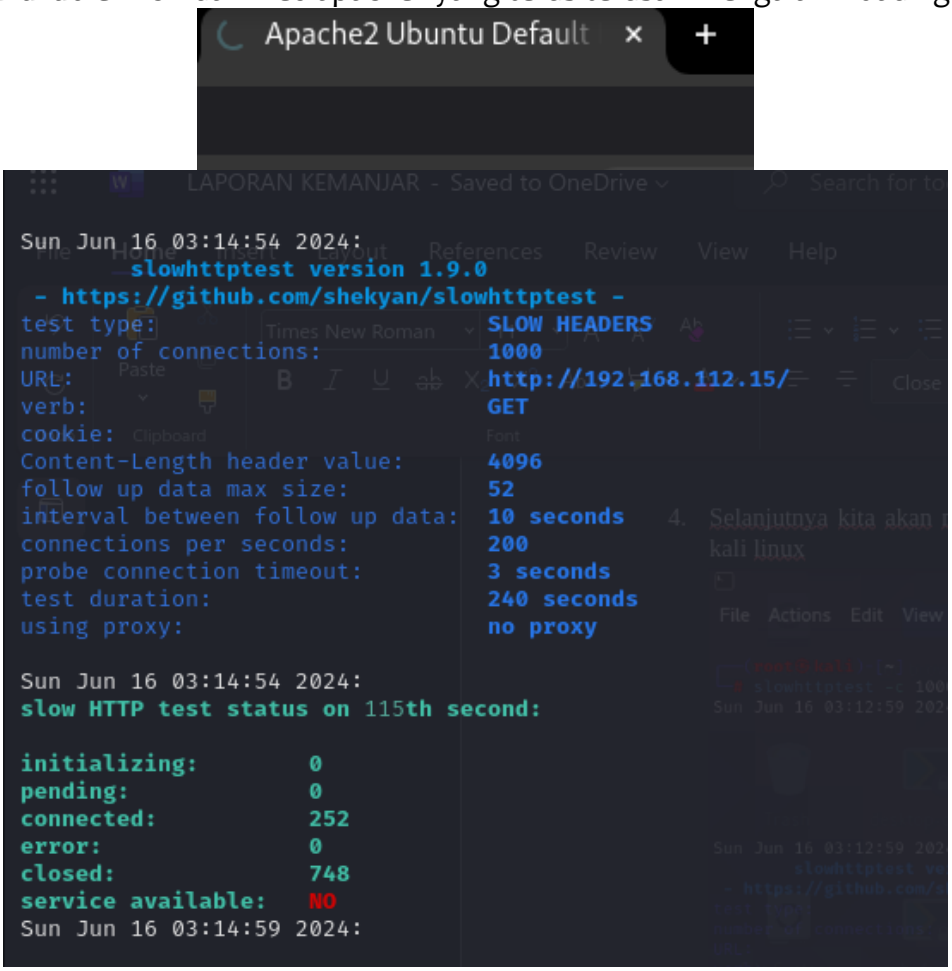


Terlihat bahwa alamat ip address penyedia layanan adalah **192.168.112.15** dan server apache telah aktif

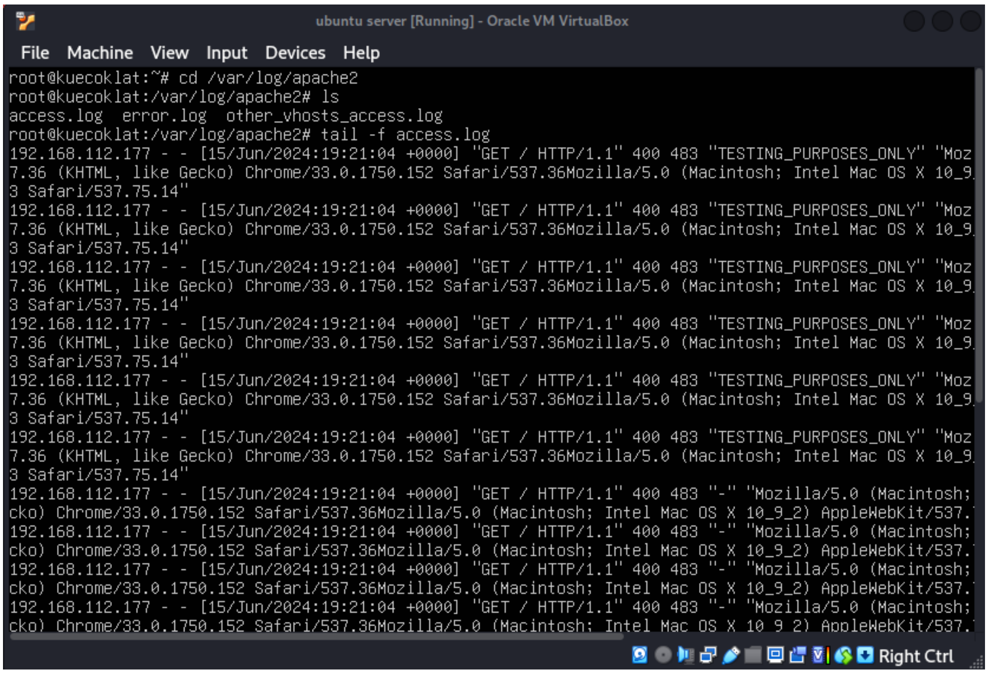
4. Selanjutnya kita akan melakukan sebuah penyerangan menggunakan tools slowhttptest pada os kali linux.



5. Tanda bahwa server sudah berhasil terkena serangan ddos adalah terdapat sebuah tulisan **"service available: NO"** dan web apache2 yang terus terusan mengalami loading.

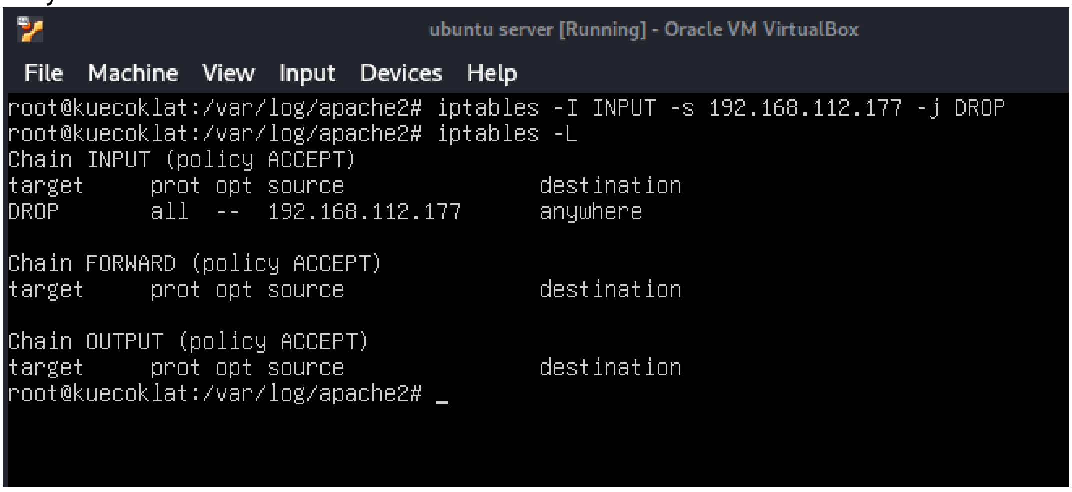


6. Untuk melihat menganalisis serangan kita bisa memeriksa file log apache yang berada pada direktori /var/log/apache2 lalu mengakses file access.log menggunakan perintah tail

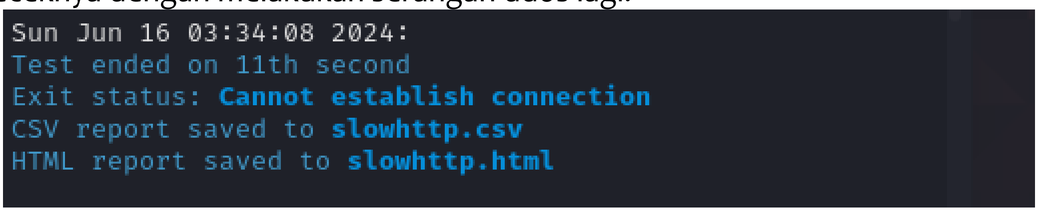


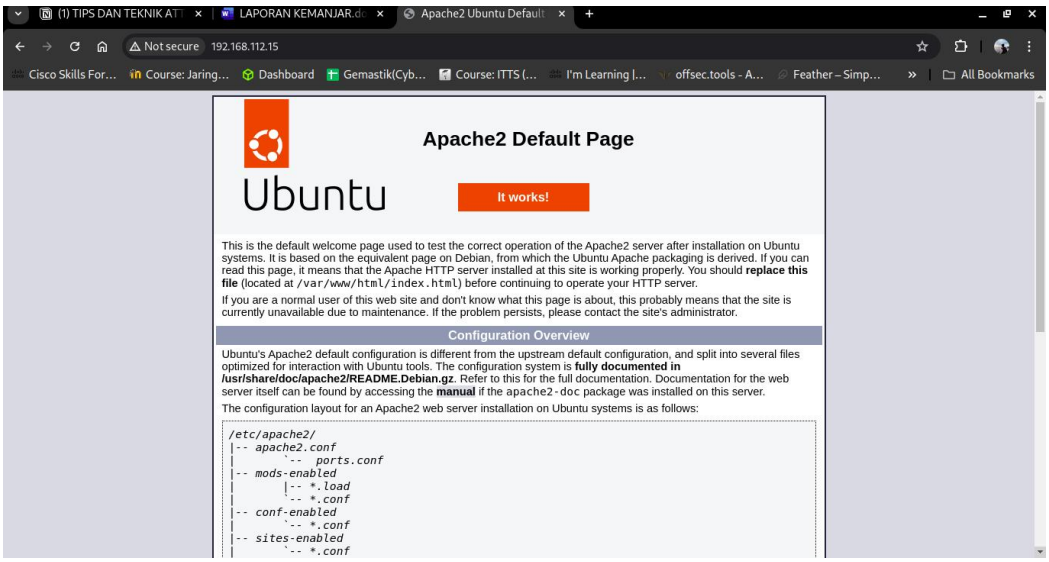
Melalui gambar diatas dapat kita ketahui bahwa alamat ip penyerang adalah **192.168.112.177**

7. Setelah mengetahui ip penyerang kita bisa memblokir serangan ddos tersebut menggunakan iptables yaitu firewall bawaan dari os linux



8. Selanjutnya setelah kita berhasil memblokir alamat ip dari si penyerang, kita bisa mengeceknya dengan melakukan serangan ddos lagi.





Seperti yang terlihat pada gambar diatas, gambar pertama memunculkan error ketika kita menyerang menggunakan tools slowhttptest dengan pesan error **Exit status : Cannot establish connection**, dan pada gambar kedua web server apache masih dapat dibuka.

KESIMPULAN DAN SARAN

Penelitian ini mengidentifikasi dan menganalisis jenis-jenis serangan DDoS yang dapat mengancam jaringan skala besar, khususnya serangan pada layer aplikasi dan volumetrik. Simulasi serangan DDoS menunjukkan bahwa serangan ini dapat menyebabkan gangguan besar pada layanan jaringan, membuat layanan tidak tersedia bagi pengguna yang sah. Namun, penelitian ini juga menunjukkan bahwa penggunaan iptables dapat menjadi solusi mitigasi yang efektif untuk memblokir serangan tersebut. Analisis log dan pemblokiran IP penyerang berhasil memulihkan fungsi normal server, menunjukkan bahwa langkah-langkah mitigasi yang tepat dapat mengurangi dampak serangan DDoS secara signifikan.

Untuk meningkatkan ketahanan terhadap serangan DDoS, organisasi perlu memastikan bahwa infrastruktur jaringan dan server memiliki kapasitas yang memadai untuk menangani lonjakan lalu lintas yang tiba-tiba, termasuk memperluas bandwidth dan meningkatkan kapasitas perangkat keras. Selain iptables, disarankan untuk menggunakan solusi mitigasi DDoS berbasis cloud dan perangkat lunak khusus yang dapat mendeteksi dan menanggapi berbagai jenis serangan secara real-time. Penting juga untuk melakukan pemantauan jaringan secara berkelanjutan dan menganalisis lalu lintas untuk mendeteksi aktivitas mencurigakan sejak dini, memungkinkan respons yang cepat terhadap potensi serangan. Memberikan pelatihan kepada staf IT mengenai cara mengidentifikasi dan menangani serangan DDoS dapat meningkatkan kesiapan organisasi dalam menghadapi ancaman tersebut. Selain itu, bekerja sama dengan penyedia layanan keamanan yang memiliki keahlian dalam mitigasi DDoS dapat memberikan perlindungan tambahan dan memastikan jaringan tetap aman dari ancaman yang semakin canggih. Dengan menerapkan langkah-langkah ini, organisasi dapat meningkatkan ketahanan jaringan mereka terhadap serangan DDoS, memastikan kelangsungan layanan, dan meminimalkan dampak finansial serta reputasi yang mungkin timbul dari serangan tersebut.

REFERENSI

Ramli, H., & Alifsyah, M. Y. (2023). Analisis Keamanan Komputer Terhadap Serangan Distributed Denial of Service (DDOS). *Journal of Renewable Energy and Smart Device*, *1*(1), 25-30.

Mardiyanto, B., Indriyani, T., Suartana, I. M., & Kunci, K. (2016). Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless. *Integer Journal*, *1*(2), 32-42.

Suartana, I., Indriyani, T., & Mardiyanto, B. (2017). Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless. *INTEGER: Journal of Information Technology*, *1*(2).

Rahmadaniar, I., Tondang, D. A. A., Fernando, B. S., & Setiawan, A. (2024). Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS. *Journal of Internet and Software Engineering*, *1*(3), 10-10.

Adrian, R., & Isnianto, N. (2016). Analisa Pengaruh Variasi Serangan DDoS Pada Performa Router. *Pros. Semin. Nas. Teknol. Terap. SV UGM*, 1257-1259.