Pencegahan Serangan DDOS *Syn Flood* Terhadap Web Server

Fikri Rizqillah Hasani[1], Sardjono[2], R. Yadi Rakhman A[3]
Fakultas Teknologi dan Informatika
Universitas Informatika dan Bisnis Indonesia
Bandung, Indonesia
e-mail: [1]fikri.rh20@student.unibi.ac.id, [2]sardjono@unibi.ac.id, [3]r.yadi@unibi.ac.id

Correspondence : *e-mail*: [1]fikri.rh20@student.unibi.ac.id

Diajukan: 30 Juli 2024; Direvisi: 22 Agustus 2024; Diterima: 23 Agustus 2024

Abstrak

Sebuah web server menjadi kebutuhan yang sangat penting pada era digitalisasi seperti sekarang ini, tentu hal itu menjadi tantangan terhadap ketahanan web server untuk tahan terhadap serangan yang dapat menganggu kinerja pelayanan. Data dari Badan Siber dan Sandi Negara (BSSN) menyebutkan bahwa total trafik anomali pada tahun 2023 berjumlah sebesar 403.990.813 anomali. BSSN juga melakukan prediksi ancaman siber yang akan muncul pada tahun 2024 salah satunya adalah Distributed Denial of Service (DDoS). Dalam penelitian ini bertujuan untuk melakukan pencegahan terhadap sebuah web server agar dapat tahan terhadap serangan DDoS jenis SYN Flood. Peneliti menggunakan Hping3 dan LOIC sebagai alat bantu untuk melakukan uji coba penyerangan, hasil dari uji coba serangan tersebut mampu membuat penggunaan CPU pada web server menigkat secara signifikan. Pencegahan dilakukan dengan cara membuat sebuah script bash (.sh) yang berisikan beberapa aturan firewall yang mampu untuk menekan serangan DDoS SYN Flood. Hasil dari pencegahan tersebut script yang dibuat mampu untuk menekan serangan terhadap performa CPU hingga 75%.

Kata kunci: *DDoS, SYN Flood, Web Server, Hping3, LOIC.*

Abstract

A web server is a very important requirement in the current era of digitalization, of course this is a challenge for the web server's resilience to withstand attacks that can disrupt service performance. Data from the National Cyber and Crypto Agency (BSSN) states that the total anomalous traffic in 2023 will amount to 403,990,813 anomalies. BSSN also predicts cyber threats that will emerge in 2024, one of which is Distributed Denial of Service (DDoS). This research aims to prevent a web server from being able to withstand SYN Flood type DDoS attacks. Researchers used Hping3 and LOIC as tools to carry out attack tests. The results of these attack tests were able to increase CPU usage on the web server significantly. Prevention is carried out by creating a bash script (.sh) which contains several firewall rules that are able to suppress SYN Flood DDoS attacks. As a result of this prevention, the script created was able to suppress attacks on CPU performance by up to 75%.

Keywords*: DDoS, SYN Flood, Web Server, Hping3, LOIC.*

1. Pendahuluan

Dalam era digitalisasi seperti sekarang ini, web server menjadi sebuah kunci dalam menyediakan pelayanan-pelayanan yang bersifat *online* seperti situs web, penyimpanan cloud, aplikasi berbasis *website*, media informasi, dan lain-lain. Ketersediaan web server menjadi hal yang sangat penting bagi keberlangsungan bisnis, institusi, maupun setiap individu yang menggunakan layanan-layanan tersebut. Keamanan sebuah web server merupakan sebuah aspek penting untuk diperhatikan oleh setiap pihak yang merasa terlibat dalam keberlangsungan sebuah *website* dari serangan – serangan yang mampu untuk merusak sumber daya sehingga sebuah web server menjadi tidak bisa digunakan.

Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN) dalam laporannya berjudul lanskap keamanan siber indonesia 2023 menyebutkan bahwa Total trafik anomali di indonesia berjumlah sebesar 403.990.813 anomali dengan jenis anomali yang tertinggi yaitu Generic Trojan RAT. Dalam kasus serangan

terhadap *website* sendiri dalam laporan tersebut tercatat sebanyak 189 kasus dan yang paling banyak ditemukan adalah kasus insiden *web defacement*. Badan Siber dan Sandi Negara juga telah melakukan analisis terhadap serangan dan memprediksi potensi ancaman siber yang di prediksi akan muncul pada tahun 2024. Ancaman siber tersebut diantaranya adalah *web defacement, ransomware, phising*, dan *Distributed Denial of Service* (DDoS) [1].

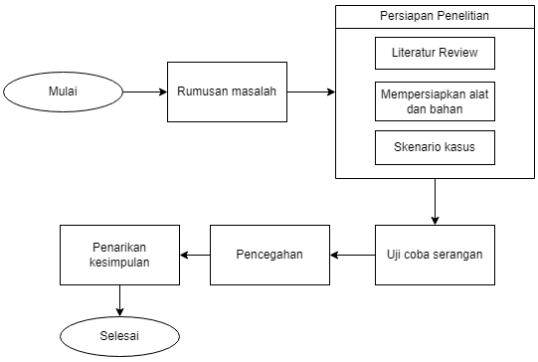
Serangan *Distributed Denial of Service* atau yang biasa disebut dengan DDoS adalah salah satu jenis serangan *cyber* yang dilakukan dengan cara mengirimkan lalu lintas palsu secara terus menerus kepada sebuah sistem atau server. Akibatnya, server yang diserang tidak mampu untuk menampung lalu lintas sehingga menyebabkan server tersebut "*down*" [2] [3]. Jenis serangan ini biasanya menyerang melalui jaringan, layanan *online*, ataupun sebuah *website* dengan tujuan agar server tidak dapat menampung lalu lintas atau trafik, yang dimana dampak nya adalah membuat server menjadi "*down*" [4] [5]. Selama serangan DDoS, rangkaian data bot atau botnet akan membanjiri situs web atau layanan digital dan permintaan HTTP [6] [7]. Pada dasarnya beberapa komputer akan menyerang satu buah server selama serangan berlangsung, hal ini menyebabkan sumber daya yang digunakan oleh sebuah server akan penuh dan dampaknya layanan akan tertunda atau bahkan hingga terganggu. [8] [9]

Terdapat beberapa serangan DDoS yang sebelumnya pernah terjadi di Indonesia, melansir dari CNN Indonesia bahwa serangan DDoS terbaru terjadi pada *website* KPU. Menurut Koordinator Divisi Data dan Informasi KPU Betty Epsilon Idroos mengatakan bahwa terdapat ratusan juta data DDoS yang menyerang kepada *website* KPU [10] [11]. Dampak dari serangan DDoS ini dapat bermacam-macam salah satunya adalah tidak dapatnya mengakses sumber daya yang disediakan oleh web server, tentu hal tersebut menjadi sangat merugikan terutama bagi *website* pengelola media informasi [12] [13]. Salah satu jenis serangan DDoS yang banyak digunakan adalah SYN Flood, menurut Zeebaree et al dalam penelitiannya yang berjudul "*Impact Analysis of SYN Flood DDoS Attack on HAProxy ana NLB Cluster-Based Web Servers*" menyebutkan bahwa serangan SYN Flood adalah metode serangan DDoS yang paling banyak digunakan dan memiliki dampak yang serius terhadap jaringan publik [14].

Berdasarkan permasalahan tersebut, penulis melakukan penelitian tentang pencegahan serangan DDoS SYN Flood dengan tujuan dari penelitian ini adalah untuk membuat modul yang mampu untuk mencegah serangan dalam bahasa bash (.sh) yang diharapkan mampu untuk menekan serangan agar tidak terlalu membanjiri web server.

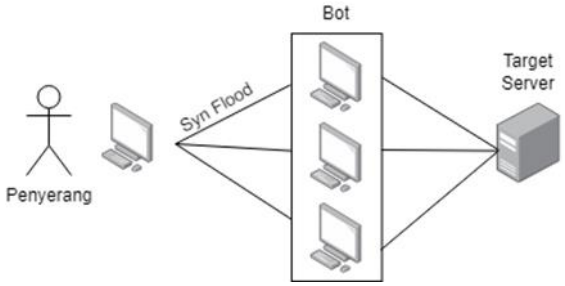
2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini merupakan metode eksperimental, dimana metode ini adalah lebih berfokus kepada pengujian yang dilakukan dalam penelitian [15]. Dalam metode ini, variabel independen adalah faktor yang dimanipulasi oleh peneliti untuk mengamati efeknya. Sementara variabel dependen adalah respon atau hasil yang diukur. Proses penelitian dimulai pada tahap persiapan yaitu mempersiapkan apa-apa saja yang dibutuhkan dalam penelitian. Tahap tahap penelitian bisa dilihat pada Gambar 1.



Gambar 1. Metodologi Penelitian

Skenario kasus dalam metodologi penelitian ini menggambarkan skenario serangan yang akan dilakukan dalam penelitian ini. Skenario kasus dapat dilihat pada Gambar 2.



Gambar 2. Skenario Serangan

Gambaran dari skenario kasus yang digunakan adalah seorang penyerang melakukan serangan DDoS SYN Flood menggunakan beberapa botnet yang ditujukan kepada target web server.

3. Hasil dan Pembahasan

Hasil dari penelitian ini adalah menciptakannya sebuah *script* bahasa bash(.sh) yang mampu untuk menekan atau mengurangi kinerja dari serangan DDoS SYN Flood.

3.1. Uji Coba Serangan

Pada tahap ini akan dijelaskan mengenai beberapa langkah yang dilakukan untuk menguji coba serangan menggunakan 2 (dua) alat yaitu Hping3 dan LOIC. Tujuan dari uji coba serangan ini adalah untuk menguji ketahanan web server dengan serangan DDoS SYN Flood dan dampak apa yang diterima web server ketika serangan dilakukan. Pengujian dilakukan dengan memantau kinerja server sebelum, selama, dan setelah penyerangan. Beberapa hal yang akan dipantau adalah penggunaan sumber daya web server seperti penggunaan CPU dan memory.

3.1.1. Tahap Persiapan

Tahap persiapan ini merupakan tahap awal dari penelitian yang dilakukan. Dalam tahap ini peneliti menjelaskan beberapa alat dan bahan yang digunakan dalam penelitian dan mempersiapkan spesifikasi web server yang akan dijadikan target penyerangan.

3.1.2. Port Scanning

Untuk memulai serangan maka kita harus mencari tahu terlebih dahulu port mana yang terbuka dari web server yang akan kita serang. Alat yang digunakan untuk *port scanning* ini adalah NMAP (*Network Mapper*). Hasil dari port scanning menggunakann NMAP dapat dilihat pada Gambar 3.

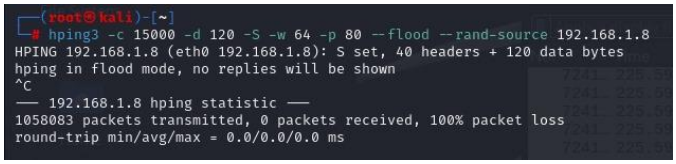
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 09:15 EDT
Nmap scan report for 192.168.1.8
Host is up (0.0030s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:ED:3F:80 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Gambar 3. Hasil *Port Scanning*

Berdasarkan hasil scanning dasar menggunakan NMAP menunjukkan bahwa port yang terbuka yaitu port 80 dengan state '*open'* yang berarti port tersebut statusnya adalah terbuka, Dengan terbukanya port 80 ini maka bisa dilakukan penyerangan DDoS menggunakan port 80 yang terbuka itu.

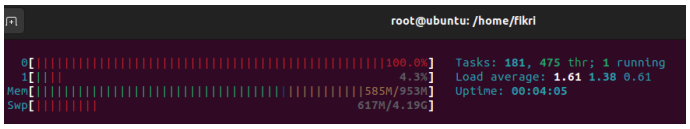
3.1.3. Serangan Menggunakan Hping3

Uji coba serangan yang pertama ini akan menggunakan salah satu alat dari linux yaitu Hping3. Serangan akan dilakukan selama 5 menit dan hasil yang akan diambil adalah dengan melihat pergerakan kinerja dari web server yang ditargetkan.



Gambar 4. Serangan Hping3

Setelah dilakukan penyerangan selama 5 menit menggunakan Hping3 bisa dilihat terdapat 1058083 paket yang dikirim oleh Hping3 kepada target web server dengan metode SYN Flood.

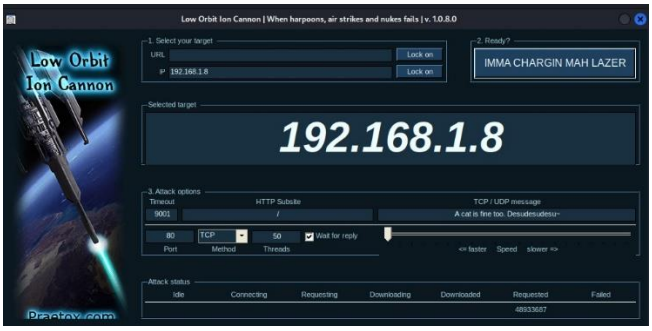


Gambar 5. Performa Web Server Ketika Serangan Hping3

Selama penyerangan berlangsung dapat dilihat pada gambar 5 bahwa pemakaian sumber daya CPU dari web server naik secara drastis bahkan hampir menyentuh angka 100%.

3.1.4. Serangan Menggunakan LOIC

Uji coba serangan berikutnya menggunakan alat yang bernama *Low Orbit Ion Canon* (LOIC). Kita akan melihat apakah LOIC ini bisa lebih baik dalam melakukan serangan DDoS dibandingkan dengan menggunakan Hping3. Dikarenakan LOIC ini alat yang riskan dan berpotensi menimbulkan malware maka peneliti menggunakan LOIC ini di kali linux tidak secara langsung menggunakan laptop yang digunakan oleh peneliti. Serangan akan dilakukan selama 5 menit dan hasil yang akan diambil adalah dengan melihat pergerakan kinerja dari web server yang ditargetkan.



Gambar 6. Serangan LOIC

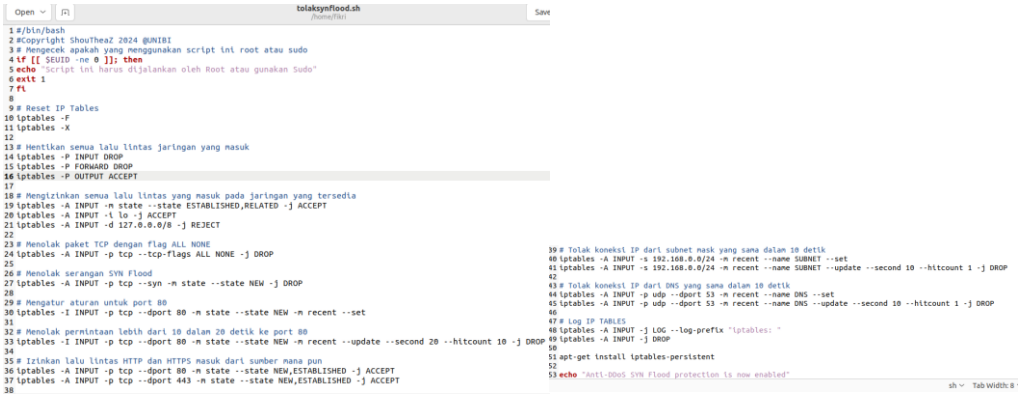
Ketika serangan LOIC dilakukan terdapat 48933687 paket data yang dikirimkan kepada web server yang menjadi target.

Gambar 7. Performa Web Server Ketika Serangan LOIC

Berdasarkan gambar 4.14 kinerja web server ketika serangan DDoS SYN Flood dilakukan menggunakan LOIC performa CPU meningkat secara drastis dari sebelum serangan dilakukan hingga menembus angka mendekati 92%. Dengan kondisi ini tentu web server akan menghabiskan sumber daya CPU secara signifikan.

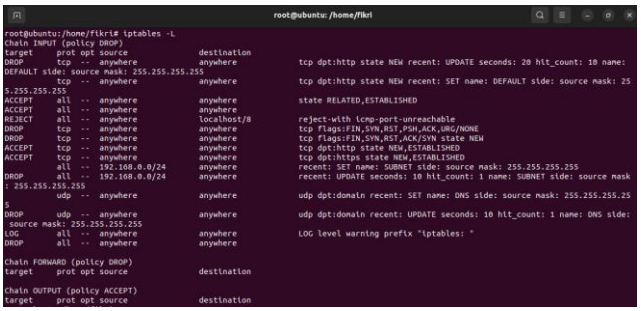
3.2. Pencegahan

Setelah melakukan penyerangan dengan 2 (dua) alat yang berbeda yaitu Hping3 dan LOIC, berikutnya untuk mencegah serangan DDoS SYN Flood dilakukan juga pencegahan sehingga bila nanti web server terkena serangan DDoS SYN Flood maka web server sudah memiliki perlindungan lebih awal dalam mencegah serangan tersebut. Mengatasi pencegahan, peneliti membuat sebuah modul file bash (.sh) yang berisikan beberapa aturan-aturan *firewall*. Modul ini berfungsi untuk mengkonfigurasi *firewall* agar dapat memblokir paket-paket kosong, memblokir paket SYN Flood, mengkonfigurasi aturan untuk port 80, dan memblokir 10 (sepuluh) paket baru yang akan terhubung ke web server dalam 10 detik.



Gambar 8. *Script* Bash Anti-DDoS SYN Flood

Cara kerja *script* ini adalah dengan *filtering* terhadap alamat ip, nantinya setiap alamat ip yang terhubung ke dalam server akan memiliki slot sendiri. Jadi koneksi yang terhubung ke server tidak menumpuk pada satu tempat. *Script* ini juga memiliki aturan yang dimana bila terdapat 10 koneksi dari subnet mask dan DNS yang sama maka akan ditolak request yang ke 11 sehingga tidak dapat melakukan koneksi ke server.



Gambar 9. *Script* Telah Terpasang

3.3. Pengujian *Script*

Pengujian *script* penolak DDoS SYN Flood yang telah dibuat, maka akan dilakukan kembali penyerangan terhadap web server yang menjadi target menggunakan 2 (dua) alat yang telah digunakan sebelumnya. Pengujian ini akan melihat kinerja CPU web server yang telah ditanamkan *script* tolaksynflood.sh.

Tabel 1. Perbandingan Performa Web Server Sebelum dan Sesudah Terpasang *Script*

Serangan	Kategori	Sebelum Terpasang *Script*	Sesudah Terpasang *Script*
Hping3	CPU	100.0%	25.3%
	Memory	585M/953M	2.0%
	SWP	617M/4.19G	555M/953M
LOIC	CPU	92.6%	5.3%
	Memory	585M/953M	582M/953M
	SWP	617M/4.19G	628M/4.19G

4. Kesimpulan

Kesimpulan dari penelitian ini yaitu pencegahan dengan menggunakan aturan *firewall* yang dibuat pada file bash dan ditanamkan pada web server mampu melakukan pencegahan terhadap serangan DDoS SYN Flood. Hal ini dibuktikan dengan berhasilnya mencegah performa serangan Hping3 dari awalnya hampir menyentuh angka 100% dapat ditekan hingga menyentuh angka 25.3%. Sedangkan untuk LOIC dari yang awalnya dapat melakukan serangan hingga menyentuh angka 92% menjadi tidak mampu melakukan serangan (0%).

Daftar Pustaka

[1] Badan Siber dan Sandi Negara, "Lanskap Keamana Siber Indonesia 2023," BSSN, Jakarta Selatan, 2023.

[2] W. A. D. Ananta, T. Kurniawan dan A. Widjajarto, "Implementasi Serangan *Distributed Denial of Service* (DDoS) Menggunakan HPING3 Pada Software Defined Network (SDN) Dengan Metode PPDIOO," *SEIKO : Journal of Management & Business,* vol. 6, no. 1, pp. 266-275, 2022.

[3] A. E. Cil, K. Yildiz dan A. Buldu, "Detection of DDoS Attacks With Feed Forward Based Deep Neural Network Model," *Expert System With Applications,* vol. 3, no. 11, pp. 1-8, 2021.

[4] R. Abubakar, M. F. Majeed, A. Mehmood dan C. Maple, "An Effective Mechanism to Mitigate Real Time DDoS Attack," *IEEE Access,* vol. 8, pp. 126215-126227, 2020.

[5] N. Ahuja, G. Singal, D. Mukhopaday dan N. Kumar, "Automated DDOS attack detection in software defined networking," *Journal of Network and Computer Applications,* vol. 3, no. 12, pp. 1-8, 2021.

[6] F. Suthar dan N. Patel, "A Survey on DDoS Detection and Prevention Mechanism," *Journal of Advances in Information Technology,* pp. 444-453, 2023.

[7] M. N. Faiz, O. Somantri, A. R. Supriyono dan A. W. Muhammad, "Impact of Feature Selection Methods on Machine Learning-based for Detecting DDoS Attacks : Literature Review," *JITE (Journal of Informatics and Telecommunication Engineering),* vol. 5, no. 2, pp. 305-314, 2022.

[8] D. K. Bhattacharyya dan J. K. Kalita, DDoS Attacks Evolution, Detection. Prevention. Reaction, and Tolerance, New York: CRC Press, 2016.

[9] M. Arief, P. H. Trisnawan dan M. Data, "IMPLEMENTASI SISTEM DETEKSI SERANGAN SLOWLORIS PADA ARSITEKTUR JARINGAN SOFTWARE-DEFINED NETWORK MENGGUNAKAN RANDOM FOREST," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer,* vol. 1, no. 1, pp. 1-10, 2024.

[10] N. A. Agustin dan R. M. Firdos, "Studi Literatur: Ancaman *Cyber*crime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital," *JAMASTIKA,* vol. 3, no. 1, pp. 126-131, 2024.

[11] Y. W, Yuliadi, F. Hamdani, Y. B. Fitriana dan N. Oper, "Analisis Keamanan *Website* Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)," *KLIK: Kajian Ilmiah Informatika dan Komputer,* vol. 3, no. 6, pp. 1296-1302, 2023.

[12] İ. Özçelik dan R. Brooks, *DISTRIBUTED DENIAL OF SERVICE* ATTACKS REAL-WORLD DETECTION AND MITIGATION, Boca Raton: CRC Press, 2020.

[13] R. Sommese, K. Claffy, R. van, A. Chattopadhyay, A. Dainotti, A. Sperotto dan M. Jonker, "Investigating the impact of DDoS attacks on DNS infrastructure," *Internet Measurement Conference,* vol. 2, no. 4, pp. 51-64, 2022.

[14] S. R. Zeebaree, K. Jacksi dan R. R. Zebari, "Impact Analysis of SYN Flood DDoS Attack on HAProxy and NLB Cluster-based Web Servers," *Indonesian Journal of Electriccal Engineering and Computer Science,* pp. 505-512, 2020.

[15] N. S. D. Harahap dan M. I. P. Nasution, "INTEGRASITEKNOLOGISEMANTICWEBDALAMSISTEMDATABASE," *Kohesi: Jurnal Multidisiplin Saintek,* vol. 3, no. 11, pp. 71-80, 2024.