Analisis Tingkat Efektivitas *IPTables* Pada *Web Server* Sistem Operasi Linux Dari Serangan *Slowloris*

Muhammad Fabian Anshor,
Teknik Informatika dan Komputer
Politeknik Negeri Jakarta
Depok, Indonesia
muhammad.fabiananshor.tik18@mhsw.pnj.ac.id

ABSTRAK

Perkembangan teknologi jaringan dari tahun ke tahun semakin meningkat, dengan adanya internet dan menjamurnya *Web Server*, menjadi suatu keharusan untuk meningkatkan pemahaman tentang jaringan di seluruh dunia, dan untuk mendapatkan gambaran global tentang interaksi dan kunjungan *Web Server*. Dalam penerapan teknologi tersebut dibutuhkan *Web Server* yang dapat berjalan dengan baik, dengan memberikan layanan data yang mempunyai fungsi untuk menerima permintaan *HTTP* atau *HTTPS* dengan cara menjaga keamanan *Web Server* dari berbagai gangguan atau serangan menjadi hal yang penting. Seiring dengan perkembangan teknologi informasi maka dapat menimbulkan jenis kejahatan dalam teknologi terkhusus pada *web server*. Salah satu jenis kejahatan yang dapat terjadi ialah serangan *Distribute Denial of Service (DDoS) Slowloris*, yang mana jenis serangan difokuskan pada mengganggu ketersediaan layanan. Untuk mengatasi jenis serangan tersebut dengan cara yang sederhana dan cepat dapat diterapkan menggunakan metode pemasangan *firewall* dengan *tools filtering IPTables* dengan cara melakukan penelitian mengenai pengujian dan analisis perbandingan dari sebelum dan sesudah penerapan metode *IPTables* terhadap serangan *Slowloris*, menggunakan konfigurasi *IPTables* sangat efektif untuk mengamankan data, karena konfigurasi *IP tables* yang sederhana juga dapat membatasi dan memblock *IP* secara langsung atau keseluruhan kepada penyerang yang dapat mengatasi penyerangan..

Kata Kunci : *Web Server*, *IPTables*, *Slowloris*, *Firewall*, *Distribute Denail of Service (DDoS)*, Ubuntu, Kali linux, *SSL*.

I. PENDAHULUAN

Perkembangan teknologi jaringan dari tahun ke tahun semakin meningkat, dengan adanya internet dan menjamurnya *web server*, menjadi suatu keharusan untuk meningkatkan pemahaman tentang jaringan di seluruh dunia, dan untuk mendapatkan gambaran global tentang interaksi dan kunjungan *web server*. Pada tahun 2011 jumlah situs web langsung mencapai sekitar 367 Jutaan dan domain terdaftar mencapai 555 Juta, dengan begitu lebih banyak mendapatkan sumber informasi dan komunikasi dapat dilakukan dengan mudah dan cepat [1] Banyak pengguna yang memanfaatkan kemajuan teknologi ini dan juga menjadi peranan besar untuk *web server* karena menjadi salah satu bagian yang banyak digunakan, *web server* berguna sebagai tempat *web aplikasi* dan sebagai penerima *request* dari *client*. Salah satu jenis serangan yang sering terjadi ialah Serangan *Distribute Denial of Service (DDoS) Slowloris*, yang mana jenis serangan difokuskan pada mengganggu ketersediaan layanan. Serangan seperti itu bisa memakan banyak bentuk, mulai dari serangan fisik Lingkungan IT, hingga kelebihan jaringan kapasitas koneksi, atau melalui pemanfaatan kelemahan aplikasi [2]Sebagian besar serangan Cyber diluncurkan untuk menembus keamanan dengan membajak data dan informasi yang berharga. Penyerang membanjiri server dengan lalu lintas berlebih yang besar cukup untuk menguras disk, memenuhkan koneksi atau menjadikan *buffering* pada jaringan komunikasi [3] Dengan mempelajari masalah tidak tersedianya kemampuan situs *web* dan kinerja jaringan yang menurun, maka dilakukan mitigasi *DDoS* yang berbeda teknik yang muncul, jenis serangan ini termasuk serangan berbasis *volume* dan sangat bertarget yaitu *slowloris* [4]adalah serangan

protocol yang artinya serangan kepada *application layer* yang dikembangkan sedemikian rupa sehingga server menunggu banyak permintaan. Dalam hal ini permintaan sangat lambat sehingga server turun [5] . Hal ini mengakibatkan keamanan dari keseluruhan sistem harus selalu diukur dan ditingkatkan. *Firewall* adalah salah satu solusi terbaik karena hanya dengan mengandalkan peran *HTTPS* dalam *web* tidak dapat berperan banyak dan akurat dalam keamanan *web server*. *Advance Policy Firewall* adalah *firewall* berbasis *IPTables* yang dirancang untuk kebutuhan internet saat ini dan dijalankan di *Linux* [6] . Implementasi sistem keamanan *firewall* dengan menggunakan konfigurasi *Iptables* ini sebagai alternatif cara untuk mengamankan data dari oknum atau pihak yang tidak bertanggung jawab [7] . Hal ini memiliki beberapa kelebihan antara konfigurasi *IPTables* dengan cara lain untuk mengamankan data dari jenis penyerangan *slowloris* yang menargetkan protokol *TCP/IP (HTTP* dan *HTTPS*) [8]. Konfigurasi *IPTables* sangat efektif untuk mengamankan data, karena konfigurasi *IPTables* dapat membatasi dan memblock ip secara langsung atau keseluruhan [9] Penggunaan sistem operasi *linux Ubuntu* digunakan untuk mendukung konfigurasi *IPTables* sebagai *firewall*[10]. Masalah pada web server yang mengalami banyak jenis serangan yang sangat merugikan, salah satunya ialah jenis *slowloris*, oleh karena itu cara pengamanan *web server* dapat dilakukan diantaranya dengan memasang *firewall*. *Firewall* berperan sebagai keamanan pada *web server* karena dapat menggunakan *tools IPTables* yang hanya ada di *firewall* dan dapat mengatasi permasalahan tersebut dengan dipasangkan pada *web server*. Penelitian ini akan menguji keefektivitasan *IPTables* dengan tingkat keamanan pada *web server* sebelum dan setelah menggunakan *IPTables*, dengan metode penyerangan *Slowloris* terhadap *web server*.

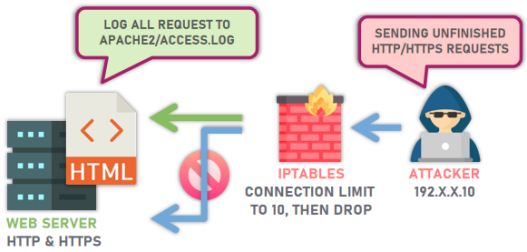
II. TINJAUAN PUSTAKA

Penelitian ini menganalisis tingkat efektivitas *IPTables* pada server dari serangan *slowloris. Slowloris* adalah salah satu *tools* dari *DoS attack* yang akan digunakan untuk penguji cobaan pnyerangan terhadap server. Dengan begitu dilakukannya mitigasi menggunakan metode *firewall* dengan *tools IPTables*. Penelitian ini memiliki tahapan yaitu pertama pengumpulan data studi lapangan dengan mengumpulkan informasi atau jurnal – jurnal tekait degan penelitian. Tahapan kedua adalah perancangan sistem dengan mengambarkan tentang sistem yang akan dibuat sesuai dengan kebutuhan yang diperlukan, tahapan ketiga implementasi sistem dilakukan sebagai penerapan dari perancangan sistem, tahap keempat pengujian sistem mengetahui apakah penerapan tersebut memiliki hasil yang sesuai dengan rumusan masalah dan tujuan penulisan, tahap kelima pada tahapan ini pembuatan laporan hasil penelitian akan dilakukan sebagai bahan evaluasi dan pengetahuan baru.

III. PERENCANAAN DAN REALISASI

3.1 Rancangan Penelitian

Penelitian ini berfokus pada analisis tingkat efektivitas *IP Tables* sebelum dan setelah dipasangkan pada web server terhadap serangan *slowloris* yang menyerang *HTTP* dan *HTTPS* pada *web server*. Secara umum gambaran sistem dapat dilihat pada gambar 1.



Gambar 1. Gambaran umum sistem

Pada *Attacker* akan mencoba melakukan *pentesting* menggunakan metode *DoS Attack* yang akan membanjiri server dan membuat siapapun tidak akan bisa mengkases server tersebut. *Attacker* bukan hanya menyerang ke *HTTP* server melainkan menyerang *HTTPS*. Setiap *IP Address* yang masuk ke dalam server akan otomatis tercatat didalam *access log*, begitupun bisa mengetahui alamat IP yang mencurigakan, dengan begitu admin server bisa melihat *IP Attacker* telah tercatat disana. Setelah mengetahui bahwa server telah diserang maka untuk menahan serangan tersebut *IPTables* akan digunakan. *IPTables* dapat menahan serangan *Attacker* dengan cara pemberian batas koneksi pada *IP Attacker* yang tercatat di *access log*, setelah itu *IP Attacker* akan di *drop* dan *block* sehingga tidak bisa akses kembali ke dalam server.

3.1.1 Perancangan Sistem Koneksi Web Server

Sistem konfigurasi pada penelitian ini dirancang untuk mendapatkan informasi alamat IP dari Ubuntu, yaitu dengan alamat IP 192.168.100.135 yang mana akan

dikoneksikan ke web server melalui client dengan OS windows 10 berupa *HTTP* dan *HTTPS*.

Setting pada Virtual Box agar menjadikan network bertipe bridge, yang mana untuk bisa saling terkoneksi antara sesama jaringan dengan mudah, penjelasan diatas dapat dilihat pada gambar 3. Adapun juga setting system base memory minimal 2GB agar tidak mengalami leg pada Ubuntu di Virtual Box.

Koneksi yang telah dilakukan ke dalam web server menggunakan *mode incognito* agar lebih privasi saat menggunakannya. Adapun juga percobaan koneksi ini berupa *HTTP* dan *HTTPS* menggunakan *IP Address* 192.168.100.110 melalui client dengan OS Windows 10.

3.1.2 Perancangan Pengujian

3.1.2.1 Proses Pengujian Serangan

1. Menyiapkan virtual box sebagai wadah tools penyerangan.
2. Install dan setting sistem operasi Kali linux di virtual box menggunakan network bertipe bridge adapter agar bisa saling terkoneksi tools satu dengan yang lain sebagai tools penyerangan.
3. Cek IP Address pada Kali linux sebagai identitas penyerangan dengan perintah "ifconfig".
4. Melakukan penyerangan ke web server HTTP dan HTTPS menggunakan metode Distribute Denial of Service (DDoS) dengan tools slowloris menggunakan perintah "slowhttptest –c 3000 –H –u http://192.168.100.135 –g –o report1" dan "slowhttptest –c 3000 –H –u https://192.168.100.135 –g –o report2".
5. Hasil penyerangan dapat dilihat dan tercatat pada file ".html".

3.1.2.2 Proses Pengujian Bangun dan Mitigasi Server

1. Menyiapkan virtual box sebagai wadah tools web server.
2. Install dan setting sistem operasi Ubuntu di virtual box menggunakan network bertipe bridge adapter agar bisa saling terkoneksi tools satu dengan yang lain sebagai tools web server.
3. Cek IP Address pada Ubuntu sebagai identitas.
4. Install "Apache2" di Ubuntu yang akan menjadi web server dengan perintah "sudo apt-get install apache2".
5.Dilakukan restart dengan perintah "sudo/etc/init.d/apache2 restart" dan juga pengecekan status dengan perintah "sudo /etc/init.d/apache2 status" untuk memastikan bahwa server sudah running.
6. Percobaan koneksi awal HTTP dan HTTPS ke server dengan memasukan IP Address 192.168.100.135.
7. Pengecekan history akses di access log denga perintah "sudo tail –f /var/log/apache2//access.log".
8. Setelah penyerangan, pengecekan access log kembali untuk memfilter IP Address attacker yang membuat server down melakukan metode pengamanan filtering IP Tables dengan menuliskan perintah pengamanan IP Tables pada *HTTP* dan *HTTPS*.
9. Melakukan drop dan blok pada IP Address attacker yang memenuhi layanan server, sehingga tidak bisa melakukan penyerangan serupa kembali.

3.1.4 Analisis Data

Berdasarkan data yang telah diperoleh dari hasil pengujian fungsional dan resistensi terhadap slowloris maka selanjutnya data tersebut akan diolah untuk menghitung tingkat keberhasilan sistem dalam menanggulangi serangan slowloris sehingga dapat mencari jawaban atas pertanyaan atau permasalahan yang dirumuskan sebelumnya. Pengujian tersebut bertujuan untuk memperoleh data yang berguna untuk pengambilan kesimpulan.

3.2 Objek Penelitian

Dalam penelitian ini, objek penelitian yang diteliti adalah pengamanan *web server* menggunakan *IPTables* dari serangan *slowloris*, untuk menganalisis tingkat efektivitas dari *IPTables* pada *web server* yang dilakukan pada sistem operasi linux. Penerapan keamanan pada *web server* sangat perlu dilakukan agar dapat mengatasi serangan *slowloris* yang dapat menginterferensi dan membanjiri jaringan *web server* selama proses pengiriman data berlangsung. Dengan menggunakan metode *netfilter* atau *filtering* menggunakan *iptables* berbasis *firewall* sistem operasi linux, maka dapat meningkatkan keamanan *web server* dalam proses pengiriman data dan menanggulangi serangan *slowloris*.

IV. HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Dalam penelitian ini pastinya membutuhkan beberapa hal yang harus dipersiapkkan sebelum memulai untuk meneliti. Kebutuhan dalam pembuatan penelitian ini meliputi dua hal, yaitu kebutuhan penelitian dan kebutuhan sistem.

4.1.1 Kebutuhan Penelitian

Pada penelitian ini memiliki dua hal yang dibutuhkan yaitu perangkat keras dan lunak. Adapun kebutuhan perangkat keras seperti laptop untuk melakukan pengkodean serta pembutan laporan penelitian dengan spesifikasi yang dapat dilihat pada tabel 1.

Tabel 1. Spesifikasi *Hardware*

1.	Laptop	: Lenovo
2.	Sistem Operasi	: Windows 10 pro
3.	RAM	: 8 GB
4.	Processor	: Intel I3 64-bit

Berikut perangkat lunak/tools yang dibutuhkan dalam melakukan implementasi penelitian adalah:

Tabel 2. Spesifikasi *Software*

1.	VirtualBox 5.2. 42r	: Virtual Machine
2.	KaliLinux 6.0.0 r 127566	: OS Tools Slowloris
3.	Ubuntu 20.04	: Web Server
4.	Windows 10 (Google Mode Incognito)	: Client dan pengujian
5.	MS Word 2016	: Pembuatan Laporan
6.	Power Point 2016	: Pembuatan Presentasi

4.1.2 Kebutuhan Sistem

Pada kebutuhan sistem, untuk pembuatan penelitian membutuhkan data yang berupa data perbandingan yang akan diteliti pada penelitian ini. Serta dibutuhkan pula sebuah grafik yang digunakan untuk mempermudah cara baca hasil penelitian.

Data perbandingan yang digunakan dalam penelitian ini dari hasil penguji cobaan penyerangan web server yang belum dan sudah dimitigasi dengan *IPTables* didalam sistem operasi Kali linux, yang mana memiliki fitur yang dapat membantu memudahkan pembacaan dari hasil pengujian dengan menggunakan grafik.

4.2 Perancangan Sistem

4.2.1 Perancangan *Slowloris*

Dalam perancangan Slowloris dengan sistem operasi Kali linux, ditujukan untuk sebagai attacker pada penelitian ini berikut yang dilakukan ialah :

1. Running sistem operasi Kali linux pada Virtual box.
2. Running terminal pada Kali linux.
3. Cek IP address attacker di Kali linux.
4. Instalasi dan konfigurasi penyerangan pada server menggunakan target IP address server dengan Slowloris.
5. Setelah penyerangan berhasil, dapat mengeluarkan report hasil penyerangan berupa grafik dan data angka.

4.2.2 Perancangan *IPTables*

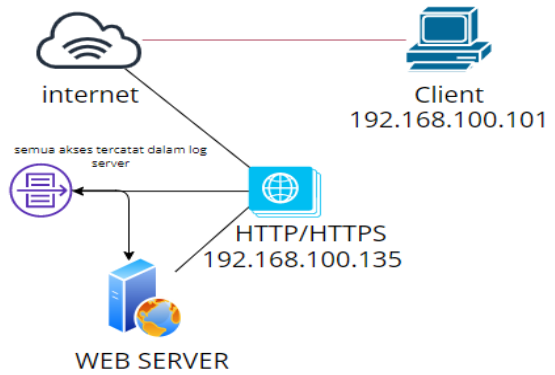
Dalam perancangan IPTables dengan sistem operasi Ubuntu, ditujukan untuk memitigasi serangan dari Slowloris yang membahayakan server dalam penelitian ini, berikut yang dilakukan ialah :

1. Running sistem operasi Ubuntu pada Virtual box.
2. Running terminal pada Ubuntu.
3. Melakukan pengecekan pada akses log server.
4. IP attacker terdeteksi sebagai request palsu yang berulang.
5. Melakukan Intalasi dan konfigurasi mitigasi pada server dengan drop dan block IP attacker.
6. Server kembali normal dan berhasil dimitigasi dari serangan Slowloris.

4.2.3 Perancangan Topology dan Alur *IPTables*

Berikut ini ialah gambar rancangan topology dari skema normal, penyerangan dan mitigasi yang akan dilakukan :

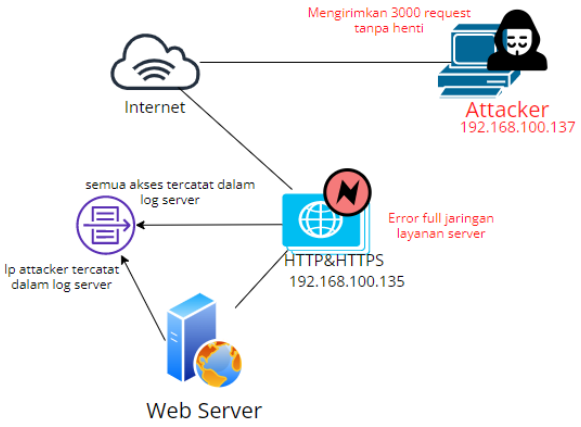
Pada hasil gambar 9 menjelaskan topology normal koneksi client ke web server yang memiliki IP address 192.168.100.101 dengan bantuan internet sehingga dapat terkoneksi dengan web server, gambar 9 juga menjelaskan ketika client berhasil koneksi ke web server maka akan tercatat di akses log server.



Gambar 9. Topology normal

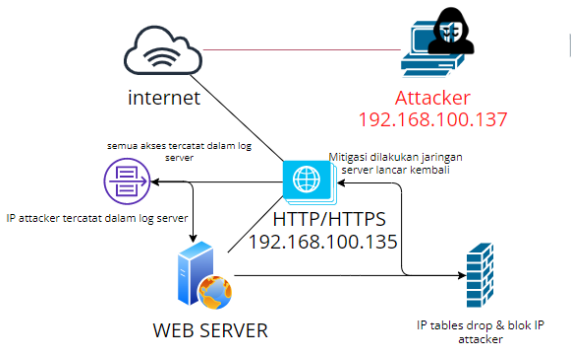
Setelah menjelaskan topology normal, pada penelitian ini juga akan menjelaskan topology penyerangan,

yang mana ketika attacker melakukan penyerangan terhadap server dengan IP address 192.168.100.137 merusak jaringan dari server dengan mengirimkan 3000 request bersamaan sehingga permintaan layanan dari client HTTP dan HTTPS dengan IP address 192.168.100.135 tidak bisa dilakukan yang menyebabkan server tidak dapat diakses atau 'server down' karena layanan server sudah dipenuhi dengan ulah attacker yang melakukan DDoS dengan tools Slowloris, mengetahui adanya penyerangan terhadap server karena admin melihat dari akses log server yang mencatat banyak IP address yang sama dan berulang dengan permintaan yang tak biasa. Penjelasan sesuai dengan hasil gambar yang dapat dilihat pada gambar 10.



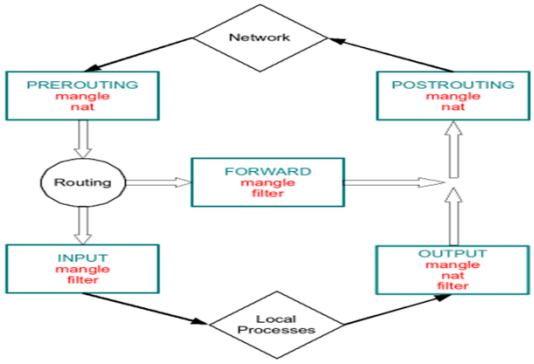
Gambar 10. Topology penyerangan slowloris

Selanjutnya setelah menjelaskan topology normal dan penyerangan, maka ada topology mitigasi yang dapat recovery kinerja dari server sehingga server dapat berjalan normal kembali yaitu dengan pengamanan IPTables salah satu trik jitu yang bisa mematahkan serangan DDoS attack (Slowloris) dengan cara drop dan block IP attacker dengan cepat dan efektif. Berikut skema topology mitigasi IPTables dapat dilihat pada gambar 11.



Gambar 11. Topology mitigasi *IPTables*

Selanjutnya setelah menjelaskan dari topology pengujian ini, disini akan menjelaskan cara kerja dari pengamanan IPTables pada web server dari serangan Slowloris yang dapat dilihat pada hasil gambar 12.

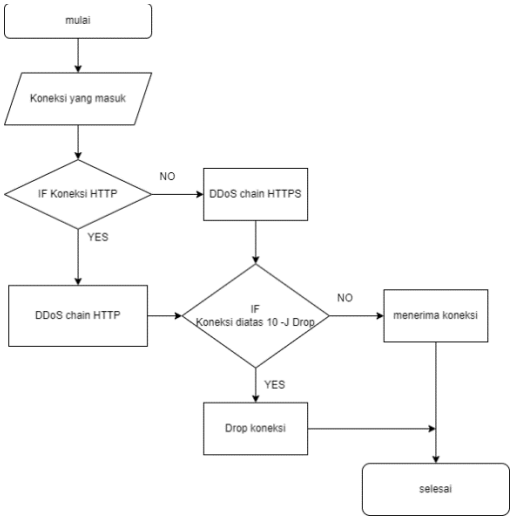


Gambar 12. Alur kerja *IPTables*

1. Perjalanan paket yang ditujukan bagi host lokal

   a. Paket berada pada jaringan fisik (Network) dan masuk ke interface jaringan.
   b. Paket masuk ke rantai PREROUTING pada tabel MANGLE dan tabel NAT.
   c. Paket mengalami Routing.
   d. Paket masuk ke rantai INPUT pada tabel MANGLE dan tabel FILTER untuk mengalami proses penyaringan.
   e. Paket akan masuk ke proses lokal (Local Process).

Setelah menjelaskan topology dari pengujian ini maka kali ini akan menjelaskan flowchart dari IPTables sebagai pengamanan terhadap web server yang dapat dilihat pada gambar 13.



Gambar 13. *Flowchart IPTables*

4.3 Implementasi Sistem

Implementasi sistem merupakan tahapan penerapan perangkat lunak yang telah dilaksanakan, diterapkan dan dirancang/didesain untuk kemudian dijalankan sepenuhnya. Tahap ini merupakan tahap dimana sistem siap untuk dioperasikan pada pengujian ini.

4.4 Pengujian

Dalam Pengujian ini dilakukan untuk melakukan pengamanan web server terhadap serangan yang menggunakan metode slowloris dengan beberapa tahapan yang diakhiri dengan mitigasi oleh filtering iptables. Pengujian ini menampilkan report berupa statistik diagram sebagai hasil penguji cobaan perbandingan pengamanan iptables pada web server dari serangan slowloris.

Dalam penelitian ini, pengujian terdiri dari:

1. Instalasi dan pengaturan jaringan internet pada virtual box.
2. Instalasi sistem operasi Ubuntu di virtual box.
3. Instalasi sistem operasi Kali Linux di virtual box.
4. Pengecekan IP address pada Ubuntu.
5. Pengecekan IP address pada Kali Linux.
6.Instalasi dan konfigurasi pembangunan server apache Ubuntu.
7. Uji koneksi pada server menggunakan HTTP dan HTTPS.
8. Percobaan serangan dengan Slowloris.
9. Percobaan mitigasi dengan IP Tables.

4.4.1 Deskripsi Pengujian

• Pengujian fungsional

Pengujian fungsional bertujuan untuk mengetahui apakah sistem yang telah dibangun telah memenuhi kebutuhan fungsional yaitu sistem dapat melakukan proses pengamanan pada server yang terserang slowloris dan berjalan pada protokol *HTTP* dan *HTPPS*. Pengujian fungsional yang akan dilakukan meliputi sebagai berikut:

1) Server dapat terkoneksi dengan web aplikasi HTTP dan HTTPS
2) Server dapat mendeteksi attacker dengan access log
3) Server dapat memitigasi serangan dari attacker dengan IPTables

• Pengujian resistansi

Pengujian ini dilakukan untuk mengetahui apakah sistem memiliki resistansi atau ketahanan terhadap serangan yang ditentukan berdasarkan lingkup penelitian ini. Serangan yang akan dilakukan untuk menguji sistem ini adalah *DoS attack* dengan melakukan teknik slowloris. *Attacker* akan melakukan serangan *slowloris* dengan melambatkan kinerja server dengan mengirimkan 3000 *request* sehingga server menjadi down dan tidak dapat melayani *request* dari client yang sah. Pada tahap pengujian ini akan dapat dilihat perbedaan antara sebelum menerapkan *IPTables* dan setelah menerapkan *IPTables* pada sistem terhadap keamanan pertukaran data yang dilakukan antara *client* dengan server.

4.4.2 Prosedur Pengujian

Berikut ini merupakan prosedur pengujian yang akan dilakukan pada pengujian fungsional dan pengujian resistansi.

1. Pengujian Fungsional

Pada pengujian ini perangkat client dan juga server akan berjalan pada satu area jaringan lokal yang sama. Pengujian ini dilakukan bertujuan untuk mengetahui apakah server dapat menerima koneksi dari client. Client yang digunakan dengan google mode incognito pada windows 10 serta *menggunakan protocol TCP (HTTP dan HTTPS)* untuk mengkoneksikan ke server. Server harus dapat melakukan pencatatan akses untuk setiap client yang masuk dan IP attacker dan mengamankan server dari attacker dengan menggunakan IPTables dengan mudah dan cepat. Jika IP attacker yang diterima oleh server maka pengamanan IPTables bekerja dengan melakukan pembatasan koneksi dan juga melakukan drop dan block pada attacker. Jika pengujian mitigasi berhasil Maka jaringan server akan bisa berjalan dengan normal tanpa ada buffering ketika client mencoba untuk mengakses server. Seluruh kebutuhan fungsional yang harus dipenuhi oleh sistem ini tertera pada tabel 3.

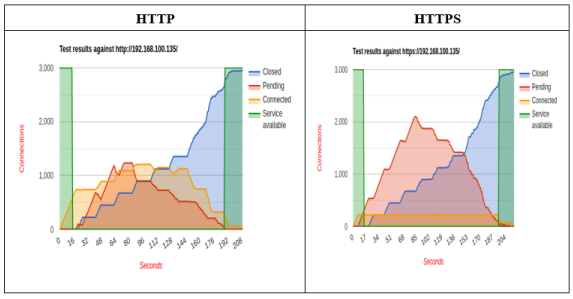
No.	Kebutuhan Fungsional
1.	Server dapat terkoneksi dengan web aplikasi *HTTP* dan *HTTPS*
2.	Server dapat mendeteksi attacker dengan access log
3.	Server dapat memitigasi serangan dari attacker menggunakan *IPTables*
4.	*IPTables* dapat digunakan dengan mudah dan efektif untuk pengamanan web server dari serangan *slowloris*
5.	*Slowloris* dapat di *drop* dan *block* dengan *IPTables* sehingga tidak berpengaruh dalam penyerangannya terhadap *web server*

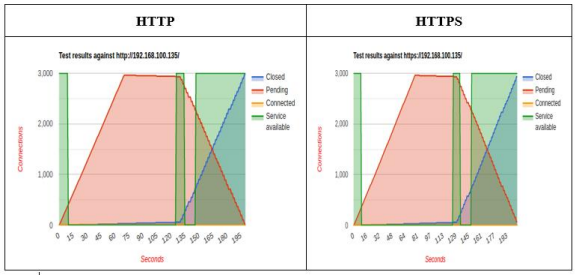
2. Pengujian Resistansi

Pengujian ini dilakukan untuk mengetahui apakah sistem yang telah dibangun dapat menangkal serangan *DoS attack*. Serangan ini akan dilakukan oleh attacker melalui sistem operasi kali linux yang berjalan pada mesin virtual. Attacker akan melakukan teknik slowloris yang akan melambatkan jalan server dengan mengirimkan 3000 request pada server sehingga client tidak bisa mengakses server dikarenakan server down. Pada pengujian ini akan dapat diketahui apakah penerapan protokol keamanan *IPTables* pada sistem dapat menangkal serangan yang dilakukan oleh *attacker*.

HTTP		
Parameter Percobaan	**Report1 (Sebelum Mitigasi)**	**Report3 (Sesudah Mitigasi)**
CLOSED	**3000**	**3000**
PENDING	**1233**	**2950**
CONNECTED	**1209**	**10**
SERVICE AVAILABLE	**NO**	**YES**

HTTPS		
Parameter Percobaan	**Report2 (Sebelum Mitigasi)**	**Report4 (Sesudah Mitigasi)**
CLOSED	**3000**	**3000**
PENDING	**2100**	**2950**
CONNECTED	**225**	**10**
SERVICE AVAILABLE	**NO**	**YES**





V. SIMPULAN DAN SARAN

A. SIMPULAN

Kesimpulan yang dapat dicapai dari hasil penelitian ini adalah: Dalam halnya ancaman *DoS* dengan *tools Slowloris*, terutama yang menargetkan terhadap *Web Server*, *protokol HTTPS* tidak bermain peran besar dalam halnya menangulangi ancaman tersebut. Untuk itu, maka penggunaan fitur *firewall* dengan *tools Iptables* yang sederhana dan efektif, baik itu host-based ataupun dedicated, akan berintegrasi dengan baik pada server untuk mengelola dan mengatur *traffic* yang kiranya boleh diizinkan ataupun yang tidak. Oleh karena itu penggunaan *tools IPTables* ini dapat mengamankan *Web Server* dari serangan *Slowloris* dengan cara yang sederhana dan mudah diterapkan sekaligus tepat pada sasaran, yaitu merujuk kepada pengamanan protokol *TCP (HTTP dan HTTPS*) yang dapat dikatakan memiliki tingkat keefektivitasan cukup baik dari hasil pengujian, percobaan dan perbandingan dengan jurnal penelitian sejenis, sehingga percobaan serangan yang dilakukan dapat langsung diatasi dengan hadirnya *IPTables* sebagai *tools* daripada *firewall* berbasis sistem operasi linux.

B. SARAN

Berdasarkan hasil penelitian ini, maka dapat dilakukan beberapa peningkatan yang bisa diimplementasikan, berikut diantaranya :

1. Melakukan pengembangan pengamanan yang lebih untuk membantu sehingga tidak terjadi pengklasifikasian apakah itu berpotensi menjadi ancaman yaitu dengan berpatokan pada *IP address*, bukan *MAC address*. Sehingga apabila *attacker* menggunakan *DoS* yang nantinya masing masing mesin dapat menggunakan *fake IP address* untuk me-masking IP mesin, maka server akan sangat berat untuk menerapkan *business rules* tersebut, yang dapat berakibatkan habisnya *pool address* sebelum dapat dipakai oleh *client* dari server itu sendiri.
2. Mengimplementasi serangan tambahan atau metode yang berbeda dari *slowloris* sehingga analisis dapat lebih berkembang.
3. Menerapkan tambahan protokol pada pengujian atau melakukan analisis pada protokol lain dari penyerangan yang sama, sehingga analisis bervariasi dan baru, juga bisa dikembangkan.

4. enerapkan pengujian sistem secara real (tidak virtual) selain menjadi pembeda, ini juga agar IP pada sistem tidak berubah ketika pengujian sistem dilakukan dilain jaringan atau internet, seperti menggunakan server asli yang digunakan.

DAFTAR PUSTAKA

[1] H. Artail, A. el Halabi, A. Hachem, and L. Al-Akhrass, "A framework for identifying the linkability between Web servers for enhanced internet computing and E-commerce", doi: 10.1186/s13174-016-0053-9.

[2] B. Qasim and M. Al-Musawi, "MITIGATING DoS/DDoS ATTACKS USING IPTABLES," 2012.

[3] C. Ikerionwu, A. MacGregor John-Otumu, N. v C, I. C. O, and J.-O. A. M, "An Enhanced Model for Mitigating DDoS Attacks on Linux Servers using IPTables and Bash scripts," *International Journal of Advanced Trends in Computer Applications (IJATCA)*, vol. 8, no. 2, pp. 68–74, 2021, [Online]. Available: www.ijatca.com

[4] J. Gera and B. P. Battula, "Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds," *Eurasip Journal on Information Security*, vol. 2018, no. 1, Dec. 2018, doi: 10.1186/s13635-018-0079-6.

[5] K. Kant, N. Tiwari, and M. S. Rakesh Kumar, "Denial of Service attack using Slowloris," *International Research Journal of Engineering and Technology*, 2020, [Online]. Available: www.irjet.net

[6] A. Anggrawan, R. Azhar, B. K. Triwijoyo, and M. Mayadi, "Developing Application in Anticipating DDoS Attacks on Server Computer Machines," *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 20, no. 2, pp. 427–434, May 2021, doi: 10.30812/matrik.v20i2.410.

[7] M. Singhal and M. Shalini Batra, "Design and Development of Anti-DoS/DDoS Attacks Framework Using IPtables," 2011.

[8] M. Sikora, R. Fujdiak, K. Kuchar, E. Holasova, and J. Misurec, "Generator of slow denial-of-service cyber attacks†," *Sensors*, vol. 21, no. 16, Aug. 2021, doi: 10.3390/s21165473.

[9] C. Diekmann, L. Hupel, J. Michaelis, M. Haslbeck, and G. Carle, "Verified iptables Firewall Analysis and Verification," *Journal of Automated Reasoning*, vol. 61, no. 1–4, pp. 191–242, Jun. 2018, doi: 10.1007/s10817-017-9445-1.

[10] F. H. Hsu, C. H. Lee, C. Y. Wang, R. Y. Hung, and Y. Zhuang, "Ddos flood and destination service changing sensor," *Sensors*, vol. 21, no. 6, pp. 1–17, Mar. 2021, doi: 10.3390/s21061980.