JURNAL LITEK : Jurnal Listrik Telekomunikasi Elektronika, Vol. 20, No. 2, September 2023, pp. 49~53
pISSN: 1693-8097; eISSN: 2549-8762

ANALISIS *MODSECURITY* DAN *MODANTILORIS* PADA SERANGAN *DDOS SLOWHTTP* TERHADAP *WEB SERVER*

Fariz Fadhilah[1], Eka Wahyudi[2*], Eko Fajar Cahyadi[3]

[1,2,3)]Program Studi Teknik Telekomunikasi, Institut Teknologi Telkom Purwokerto

Email: 19101072@ittelkom-pwt.ac.id[1], ekofajarcahyadi@ittelkom-pwt.ac.id[3]
Email Korespondensi: ekawahyudi@ittelkom-pwt.ac.id[2]

Abstrak – *Web server* merupakan server yang memberikan layanan berbasis web dan harus mampu melayani pengguna saat dibutuhkam. Namun tidak menutup kemungkinan *web server* dapat mengalami gangguan akibat ancaman dan serangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Gangguan keamanan ini di kenal dengan *DDoS* (*Distributed Denial of Service*). Serangan *DDoS* membuat *client* sah dari sebuah jaringan tidak dapat mengakses layanan *web server*. Penerapan *modsecurity* sebagai keamanan jaringan berfungsi untuk menyaring, memantau, dan memblokir *HTTP* pada *open system interconnection* dan *modantiloris* mencegah klien dari memonopoli slot koneksi tetapi tidak menjatuhkan koneksi yang lambat sebagai pengaman jaringan menawarkan solusi pada isu keamanan jaringan. Penelitian ini membandingkan implementasi antara *modsecurity* dan *modantiloris* yang bertujuan untuk mengetahui perbedaan performansi berdasarkan 4 parameter pengujian, yaitu *CPU usage, throughput, response time,* dan *packet loss.* Pengujian dilakukan dengan 4 skenario dengan masing-masing skenario dilakukan sebanyak 15 kali. Hasil pengujian dengan parameter *CPU usage*, *modantiloris* lebih unggul dari *modsecurity* dengan perolehan rata-rata 1,90% untuk *modsecurity* dan 1,65% untuk *modantiloris*. Pada hasil pengujian dengan parameter *response time*, *modantiloris* lebih unggul dari *modsecurity* dengan perolehan rata-rata 11,29 detik untuk *modantiloris* dan 744,24 detik untuk *modsecurity*. Pada hasil pengujian dengan parameter *throughput*, *modantiloris* lebih unggul dari *modsecurity* dengan perolehan nilai 73,87 KBps untuk *modsecurity* dan 197,3 KBps untuk *modantiloris*. Pada hasil pengujian dengan parameter *packet loss*, *modantiloris* lebih unggul dari *modsecurity* dengan perolehan nilai 0% untuk *modantiloris* dan 0,3746% untuk *modsecurity*.

Kata-kata kunci: Web server*, *Modsecurity*, *Modantiloris*, *Serangan DDoS

Abstract – A web server is a server that provides web-based services and must be able to serve users when needed. However, it is possible that the web server may experience disruption due to threats and attacks carried out by irresponsible parties. This security breach is known as DDoS (Distributed Denial of Service). DDoS attacks prevent legitimate clients from a network from accessing web server services. The application of modsecurity as network security functions to filter, monitor, and block HTTP on open system interconnection and modality prevents clients from monopolizing connection slots but does not drop slow connections as network security offers a solution to network security issues. This study compares the implementation of modsecurity and modtilloris which aims to determine differences in performance based on 4 test parameters, namely CPU usage, throughput, response time, and packet loss. Testing was carried out with 4 scenarios with each scenario being carried out 15 times. The test results with the CPU usage parameter show that modtilloris is superior to mod security with an average gain of 1.90% for modsecurity and 1.65% for modiloris. In the test results with the response time parameter, modtilloris is superior to modsecurity with an average acquisition of 11.29 seconds for modilloris and 744.24 seconds for modsecurity . In the test results with the throughput parameter, modtilloris is superior to modsecurity with a value of 73.87KBps for mod security and 197.3KBps for modilloris. In the test results with the packet loss parameter, modantilloris is superior to modsecurity with a score of 0% for modilloris and 0.3746% for modsecurity.

Keywords: Web server*, *Modsecurity*, *Modantiloris*, *Serangan DDoS

I. PENDAHULUAN

Lumpuhnya *web server* dapat menganggu proses *client* dalam mengakses informasi. Kelumpuhan *web server* dapat diakibatkan oleh beberapa serangan, salah satunya adalah *Distributed Denial of Service* (*DDoS*) [1]. Serangan *DDoS* memiliki banyak varian, diantaranya adalah serangan *DDoS slowhttp,* yang bekerja dimana sejumlah besar permintaan HTTP tidak lengkap dikirim, menambah jumlah tetapi tidak pernah menyelesaikan permintaan sehingga memaksa *web server* untuk tetap menjaga koneksi terbuka [2]. Koneksi yang terbuka dapat dengan mudah untuk diambil sumber daya sehingga membuat *client* sah tidak dapat mengakses *web server*.

Penerapan *modsecurity* sebagai pengamanan jaringan menawarkan solusi pada isu keamanan jaringan. Penggunaan *modsecurity* sebagai keamanan jaringan

berfungsi untuk menyaring, memantau, dan memblokir *HTTP* pada O*pen System Interconnection (OSI)* layer ke-7. *Modsecurity* akan menganalisis permintan *get* dan *post* yang terdapat dalam *HTTP* yang kemudian dicocokan dengan aturan *firewall* yang telah dikonfigurasikan untuk kemudian dilakukan pemblokiran dan penolakan akses ke aplikasi *web* apabila terdapat sebuah lalu lintas yang mencurigakan [3]. *Modantiloris* mencegah klien dari memonopoli slot koneksi tetapi tidak menjatuhkan koneksi yang lambat [2].

Pada tahun 2021, Pahlawan dan Panca [4], membahas perbandingan penerapan metode pengaman *modsecurity* dan *modevasive* pada *web server* terhadap serangan *slow headers*, yang bertujuan untuk mengetahui metode pengamanan terbaik terhadap serangan *DoS slow headers* menggunakan pengukuran *time out*. Namun, penelitian tersebut tidak terdapat parameter *CPU usage, throughput, request time,* dan *packet loss* sebagai parameter pengujian. Dalam penelitian ini mengusulkan perbandingan dua metode untuk mengetahui penerapan pengamanan terbaik pada *web server*.

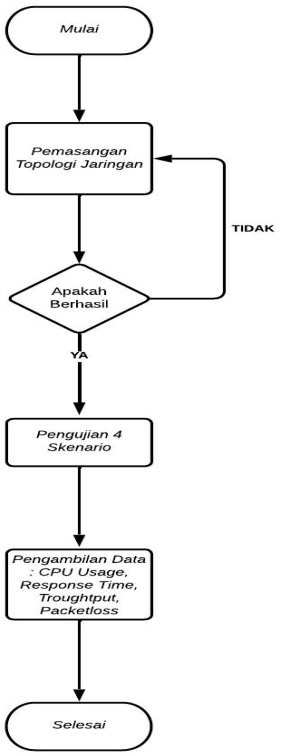
Berdasarkan latar belakang tersebut, maka dilakukan penelitian "Analisis *Modsecurity* dan *Modantiloris* pada Serangan *DDoS Slowhttp* terhadap *Web Server*". Dalam penelitian ini dibahas perbandingan pengamanan jaringan menggunakan *modsecurity* dan *modantiloris* dengan parameter pengujian *CPU usage, throughput, request time, dan packet loss* sebagai parameter pengujian.

II. METODOLOGI

Metode penelitian yang digunakan adalah metode eksperimen. Penelitian ini mengimplementasikan *modsecurity* dan *modantiloris* sebagai pengaman pada *web server*. Penelitian di Laboratorium Pengolahan Sinyal Digital Institut Teknologi Telkom Purwokerto.

A. Alur Penelitian

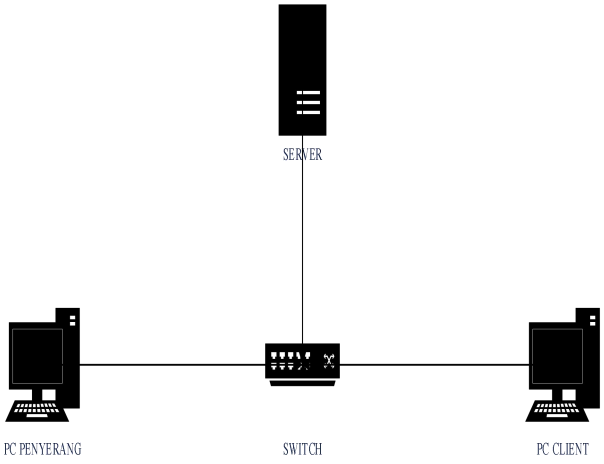
Alur penelitian terdiri dari beberapa langkah-langkah yang digunakan dalam perancangan sistem perbandingan *modsecurity* dengan *modantiloris* agar terstruktur dengan baik. Pada Gambar 1 disajikan alur penelitian dalam bentuk *flowchart*.



Gbr. 1 Alur Tahapan Penelitian

B. Topologi Jaringan

Perancangan topologi jaringan yang digunakan ditunjukkan pada Gambar 2. Perangkat yang digunakan yaitu menggunakan satu perangkat komputer yang di operasikan sebagai *web server*, satu perangkat komputer dioperasikan sebagai penyerang dan satu perangkat komputer yang berperan sebagai *client* sah. Masing-masing perangkat dihubungkan menggunakan perangkat *switch* dengan media kabel RJ 45 dengan tipe *straight-through.*



Gbr. 2 Topologi Jaringan

Pada *web server* yang digunakan adalah *apache web server* yang dilengkapi dengan sistem keamanan *modsecurity* dan *modantiloris*. Pada *server* akan dilakukan pengambilan data pada saat sebelum dan sesudah serangan. Pada perangkat sisi penyerang terpasang sistem operasi *Kali Linux* dan *Ubuntu* untuk melancarkan serangan *DDoS slow HTTP* menggunakan *tools slowhttptest* secara bersamaan yang mengarah ke *web server*.

C. Skenario Pengujian

Tahapan pengujian dilakukan dengan 4 skenario pengujian berikut:

1. Skenario 1

   Skenario 1 dilakukan dengan pengukuran sebanyak 15 kali menggunakan *tools HTTPERF* dan *SYSTAT* dengan 4 parameter, yaitu *CPU usage, response time, delay,* dan *packet loss* dalam kondisi *web server* tanpa *firewall* dan tanpa melancarkan serangan *DDoS Slowhttp.*

2. Skenario 2

   Skenario 2 dilakukan pengujian dengan melancarkan serangan *DDoS slowhttp* sebanyak 15 kali menggunakan *tools slowhttptest* untuk pengukuran menggunakan *HTTPERF* dan *SYSTAT* dengan 4 parameter, yaitu *CPU usage, response time, delay,* dan *packet loss* dalam kondisi *web server* terpasang *modsecurity* sebagai *firewall* dan *PC attacker* melakukan *scanning* kerentanan *web server* dengan menggunakan *tools Nmap*. Dalam penyerangan *DDoS slowhttp*, menggunakan aplikasi *slowhttptest* dengan perintah :
   "*slowhttptest* -c 2000 -H -g -o 192.168.121.221 -I 320 -r 10 -t GET -u http://192.168.121.221/ index.php -x 24 -p"

3. Skenario 3

   Skenario 3 dilakukan pengujian dengan melancarkan serangan DDoS *slowhttp* sebanyak 15 kali dalam kondisi web server terpasang modantiloris sebagai firewall.

4. Skenario 4

   Skenario 4 dilakukan pengujian dengan melancarkan serangan DDoS *slowhttp* sebanyak 15 kali dalam kondisi *web server* terpasang *modantiloris* dan *modsecurity* sebagai *firewall*.

III. HASIL DAN PEMBAHASAN

Pada tahap ini membahas tentang hasil implementasi dari *mod*security dan *modantiloris* pada *web server*. Hasil uji coba mencakup 4 skenario pengujian berdasarkan parameter *CPU usage*, *response time*, *throughput*, dan *packet loss*. Hasil data kemudian dibandingkan antara *modsecurity* dengan *modantiloris* untuk menentukan jenis *firewall* yang memiliki performasi lebih baik pada implementasi *web server*.

A. *CPU usage*

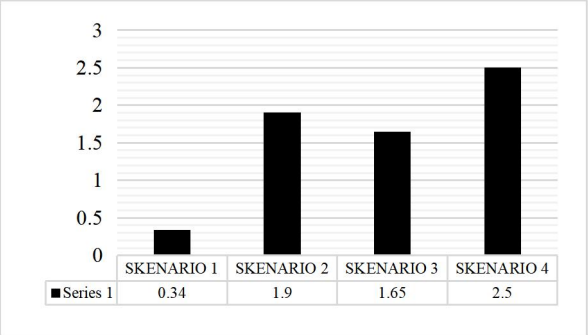
Pada skenario 1 pengujian *CPU usage* dengan nilai rata-rata sebesar 0,34% yang dihasilkan dari 15 kali percobaan. Perolehan nilai tersebut dikarenakan PC *web server* sedang tidak menerima banyak permintaan atau serangan yang merupakan serangan *DDoS slowhttp* sehingga CPU pada PC *web server* tidak bekerja secara keras.

Pada skenario 2 diperoleh nilai rata-rata 1,90%. Perolehan nilai tersebut karena terjadi serangan *DDoS slowhttp. Modsecurity* yang telah terpasang pada *web server* bekerja memindai dan memblokir serangan. Hal tersebut dapat menaikan *CPU usage.*

Pada skenario 3 diperoleh nilai rata-rata 1.65%. Perolehan nilai tersebut karena terjadi serangan *DDoS slowhttp.* M*odantiloris* yang telah terpasang pada *web server* bekerja memindai dan me-*reject* serangan. Hal tersebut dapat menaikan *CPU usage.*

Pada skenario 4 diperoleh nilai rata-rata 2,05%. Perolehan nilai tersebut karena terjadi serangan *DDoS slowhttp. Modsecurity* dan *modantiloris* yang telah terpasang pada *web server* bekerja memindai dan memblokir serangan secara bersamaan.

Gambar 3 adalah Grafik CPU *Usage* untuk 4 skenario pengujian.



Gbr. 3 CPU *Usage* (%)

B. *Response Time*

Pada Skenario 1 pengujian *response time* dengan nilai rata-rata 46,3s. Perolehan nilai dikarenakan PC *web server* sedang tidak menerima serangan *DDoS slowhttp*.

Pada skenario 2 diperoleh nilai rata-rata 744,24 s. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modsecurity* sebagai pengaman. M*odsecurity* dapat memblokir serangan berdasarkan rules *Modsecurity Blocking Evaluation*, sehingga membuat *web server* dapat melayani permintaan *client* sah dengan lebih efisien.

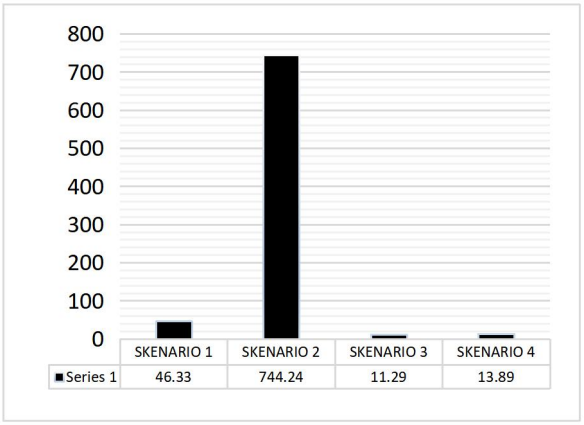
Pada skenario 3 diperoleh nilai rata-rata 11,29 s. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* di lengkapi dengan *modantiloris* sebagai pengaman, dan *modantiloris* dapat menolak serangan.

Pada skenario 4 diperoleh nilai rata-rata 13,89s. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modsecurity* dan *modantiloris* sebagai pengaman. *Modsecurity* mengidentifikasi serangan untuk diblokir sedangkan *modantiloris* me*reject* seluruh serangan.

Gambar 4 adalah Grafik *Response Time* untuk 4 skenario pengujian.

C. *Throughput*

Pada Skenario 1 pengujian *throughput* dengan nilai rata-rata 1001,1KBps. Perolehan nilai ini dikarenakan PC *web server* sedang tidak menerima serangan *DDoS slowhttp*.



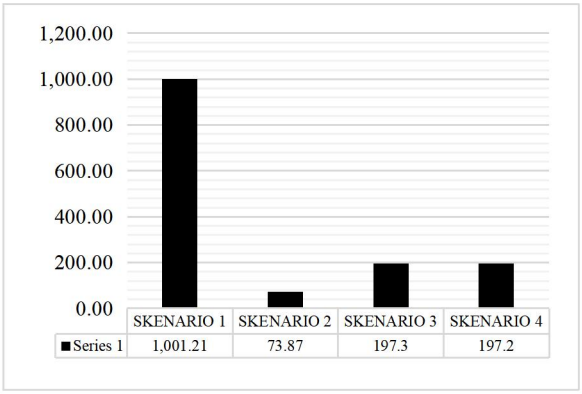
Gbr. 4 *Response Time* (s)

Pada skenario 2 diperoleh nilai rata-rata 73.87 KBps. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modsecurity* sebagai pengaman, dan *modsecurity* memblokir serangan berdasarkan *rules Modsecurity Blocking Evaluation* yang membutuhkan waktu untuk melakukan pemblokiran.

Pada skenario 3 diperoleh nilai rata-rata 197,3 KBps, Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modantiloris* sebagai pengaman, dan *modantiloris* dapat me-*reject* seluruh serangan.

Pada skenario 4 diperoleh nilai rata-rata 197,2 KBps. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modsecurity* dan *modantiloris* sebagai pengaman, dan *modsecurity* memilah serangan untuk diblokir sedangkan *modantiloris* me-*reject* seluruh serangan.

Gambar 5 adalah Grafik *Throughput* rata-rata untuk 4 skenario pengujian.



Gbr. 5 *Throughput* Rata-rata

D. *Packet Loss*

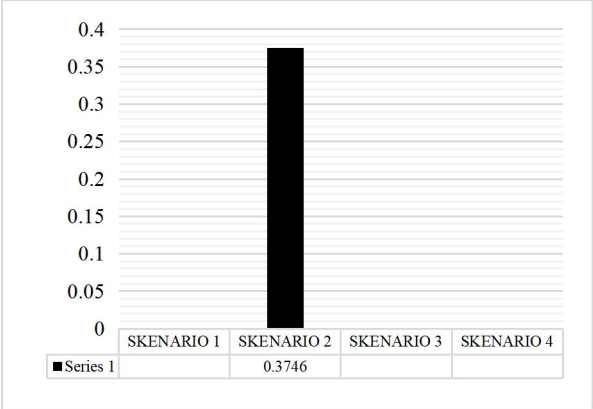
Pada Skenario 1 pengujian *packetloss* dengan nilai rata-rata 0%. Perolehan nilai ini dikarenakan PC *web server* sedang tidak menerima serangan *DDoS slowhttp* dan tidak ada paket yang hilang.

Pada skenario 2 diperoleh nilai rata-rata 0,3746%. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modsecurity* sebagai pengaman, dan *modsecurity* memblokir dan merespon serangan berdasarkan *rules Modsecurity Blocking Evaluation.*

Pada skenario 3 diperoleh nilai rata-rata 0%. Perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modantiloris* sebagai pengaman, dan *modantiloris* dapat me-*reject* seluruh serangan.

Pada skenario 4 diperoleh nilai rata-rata 0%, perolehan nilai ini dikarenakan saat terjadi serangan *DDoS slowhttp* PC *web server* dilengkapi dengan *modsecurity* dan *modantiloris* sebagai pengaman, dan *modsecurity* memilah serangan untuk diblokir sedangkan *modantiloris* me-*reject* seluruh serangan dengan maksimal.

Gambar 6 adalah Grafik *Packet Loss* rata-rata untuk 4 skenario pengujian.



Gbr. 5 *Packet Loss* Rata-rata

IV. KESIMPULAN

Modsecurity memiliki kemampuan dalam memindai jenis serangan dan memblokir serangan, sedangkan pada *modantiloris* dapat melakukan pemindaian tetapi tidak dapat mengidentifikasi jenis serangan dan dapat melakukan penolakan serangan tanpa mengidentifikasi jenis serangan, sehingga *modantiloris* unggul daripada *modsecurity* pada parameter *CPU usage* sebesar 1,65% sedangkan *modsecurity* 1,90%, *respon time* sebesar 11,29 ms sedangkan *modsecurity* 744,24ms, *Troughput sebesar* 197,3 KBps sedangkan *modsecurity* 73,87 KBps, dan *Packet Loss* sebesar 0% sedangkan *modsecurity* 0,3746%.

REFERENSI

[1] Jupriyadi, J., Hijriyanto, B., & Ulum, F. (2021). Komparasi Mod Evasive dan DDoS Deflate Untuk Mitigasi Serangan Slow Post. *Techno. Com*, *20*(1), 59-68.

[2] Arman, M. (2020). Metode Pertahanan Web Server terhadap Distributed Slow HTTP DoS Attack. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *7*(1), 56-70.

[3] Aryapranata, A. (2020). Web Application Firewall pada Situs Web Institut Bisnis Nusantara www.ibn.ac.id. *Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi Dan Sistem Komputer*, *4*(1), 55-59.

[4] Pahlawan, P. P. (2022). Perbandingan Penerapan Metode Pengamanan Mod Security dan Mod Evasive pada Web Server terhadap Serangan Slow Headers. *Journal of Engineering, Computer Science and Information Technology (JECSIT)*, *2*(1).