JURNAL TEKNOLOGI REKAYASA INFORMASI DAN KOMPUTER
E-ISSN: 2797-1724, DOI: 10.30811/jtrik.v8i2.7449
Vol. 8 No. 2 September 2025 pp. 48-56

Implementasi Keamanan Jaringan Dengan Metode Web Application Firewall (WAF)

Nurhayati[1], Atthariq [1*], Aswandi[1]

[1] Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

Coresponding Author :tthariq.huzaifah@pnl.ac.id

Article info: Diterima 20/07/2025, Direvisi 05/08/2025, Diterima 08/08/2025

ABSTRAK

Keamanan jaringan komputer merupakan bagian sebuah sistem yang sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan pengguna dari mana dan kapan saja. Dengan pemanfaatan jaringan digunakan dapat mengancam keamanan pada jaringan yang digunakan. Pada penelitian ini akan dibangun sebuah keamanan jaringan berbasis aplikasi sebagai solusi untuk meningkatkan tingkat perlindungan dan deteksi terhadap serangan cyber yang mengancam aplikasi dan data yang disimpan dalam lingkup jaringan tersebut. Penelitian ini mengajukan penerapan keamanan jaringan dengan metode Web Application Firewall pada dinas komunikasi dan informatika aceh tengah. Dimana pemanfaatan teknologi informasi dan internet pada diskominfo aceh tengah untuk mendukung keamanan web belum optimal. Web application firewall adalah keamanan yang dirancang untuk melindungi dari serangan cyber dan ancaman keamanan. Hasil pengujian yang telah dilakukan sebanyak 60 kali percobaan dengan jenis serangan SQL Injection, Cross Site Scripting (XSS), dan Denial Of Service (DoS) menunjukan kualitas sangat tinggi yaitu 100%. Bedasarkan hasil pengujian dapat disimpulkan bahwa menerapkan metodeWAF lebih baik dalam melindungi keamanan web dari sernagan cyber.

Kata kunci: satu, dua, tiga, empat, lima

1. PENDAHULUAN

Dalam era teknologi jaringan internet yang terus berkembang, keamanan jaringan menjadi sangat penting dalam menjaga integritas dan kerahasiaan informasi. Sebagai bagian tak terpisahkan dari jaringan komputer, keamanan jaringan memainkan peran krusial dalam mencegah akses yang tidak sah dan melindungi pengguna dari ancaman keamanan.

Saat ini keamanan jaringan pada Dinas Komunikasi dan Informatika Aceh Tengah belum optimalnya pemanfaatan teknologi informasi berbasis internet untuk mendukung keamanan siber, yang menyebabkan jaringan mereka menjadi rentan terhadap serangan terhadap situs web yang mereka gunakan.

Untuk mengatasi masalah ini, dengan memanfaatkan web application firewall berbasis aplikasi, serangan cyber seperti SQL Injection, Cross Site Scrpting (XSS), dan Denial Of Service (DoS), dapat diatasi dengan baik. Pengelolaan yang baik dapat mengurangi ancaman keamanan pada jaringan yang digunakan sehingga jaringan tersebut dapat dioptimalkan dengan baik.

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Analisis Performance Web Application Firewall ModSecurity dan Shadow Daemon Dalam Keamanan Web Server Apache". Dalam penelitian ini, peneliti mengusulkan penggunaan WAF untuk meningkatkan keamanan jaringan dengan menggunakan ModSecurity. Penelitian ini mengidentifikasi sernagan SQL Injection, dan Cross Site Scripting (XSS). Hal ini memberikan pemahaman yang lebih mendalam tentang potensi kerentanan yang dapat dieksploitasi dalam system[1].

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering". Penelitian menerapkan port blocking dan firewall filtering untuk meminimalisir risiko masuknya virus yang dapat memicu serangan pada suatu jaringan[2].

Penelitian ini berkaitan dengan penelitian sebelumnya yang berjudul "Implementasi Sistem Keamanan Web Server Menggunakan Pfsense". Metode yang digunakan Pfsense digunakan sebagai mampu mendeteksi gangguan keamanan terhadap web server dan melakukan pemblokiran otomatis dalam durasi tertentu. Fokus penelitian adalah menggunakan Pfsense sedangkan penelitian tugas akhir ini menggunakan metode web application firewall (WAF)[3].

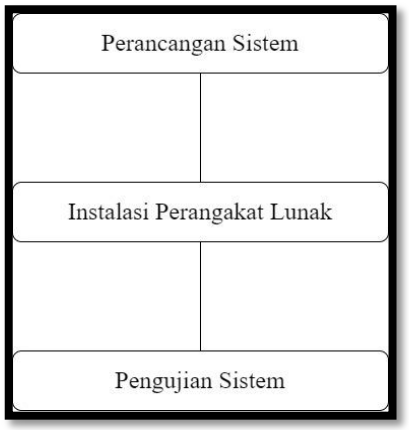
Penelitian ini berkaitan dengan penelitian sebelumnya yang berjudul "Analisis Keamanan Webserver Menggunakan Penetration Test", menggunakan metode penetration test untuk mengetahui tingkat keamanan dan kerentananan dari web sebagai suatu bentuk perlindungan dari tindak kejahatan hacker dan dapat memberikan hasil perkiraan tingkat kerentanan aplikasi web serta dapat membuat keputusan mengenai resiko tersebut[4].

Penelitian ini berkaitan dengan penelitian sebelumnya dengan judul "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen", menggunakan firewall security port untuk mengamankan suatu jaringan dari port yang terbuka, sedangkan penelitian pada tugas akhir ini menggunakan metode web application firewall (WAF)[5].

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan pada penelitian ini adalah metode web application firewall adalah alat yang digunakan untuk melindungi aplikasi web dari berbagai jenis ancaman keamanan, serangan, yang ditargetkan pada aplikasi web, serta melindungi data sensitif yang diproses oleh aplikasi tersebut. Dengan menggunakan web application firewall serangan yang masuk pada web akan diblokir oleh waf sendiri, hal ini dapat mengurangi terjadinya serangan pada jaringan yang digunakan.

1. Metode Penelitian

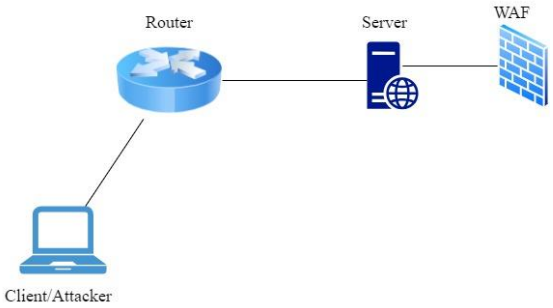


Gambar 1 Metode Penelitian

Penjelasan dari metode penelitian:

a. Perancangan sistem
   Sistem yang diperlukan pada penelitian ini dikonfigurasi menggunakan dengan beberapa perangkat lunak yaitu Web Application Firewall server WAF akan mendeteksi dan memblokir serangan-serangan yang mencurigakan.
b. Instalasi perangkat lunak
   Perangkat lunak yang akan digunakan untuk merancang suatu sistem yang dapat mendeteksi adanya penyusup ataupun serangan yaitu web application firewall, yang sebelumnya membutuhkan tools ataupun komponen yang diperlukan untuk membangun sistem tersebut yang nantinya akan bekerja sama untuk mendapatkan hasil yang maksimal.
c. Pengujian sistem
   Pengujian sistem dilakukan dengan mencoba serangan dan selanjutkan akan dideteksi oleh sistem WAF sehingga diharapkan dapat menampilkan hasil yang sempurna

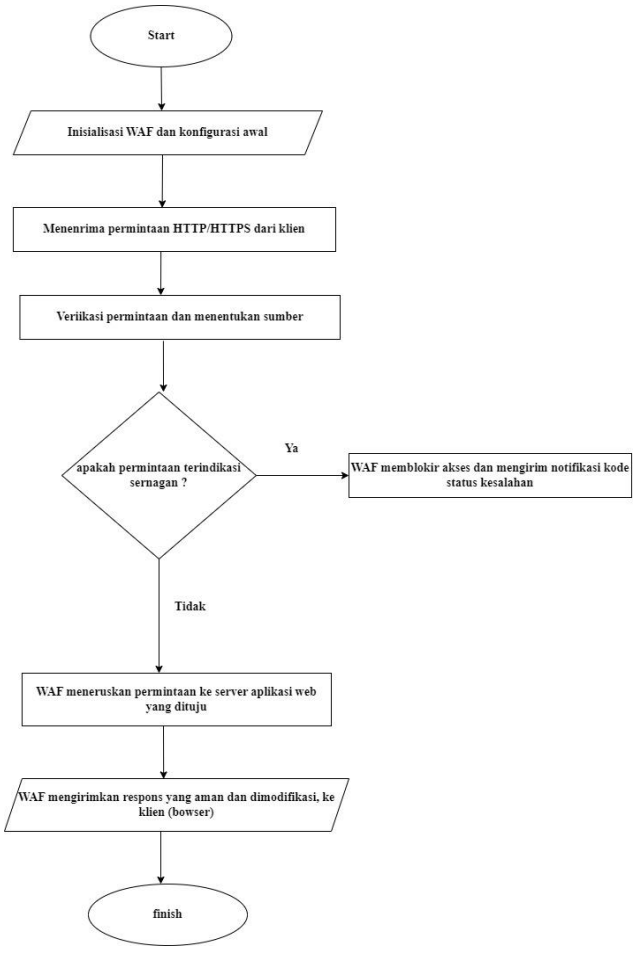
2. Arsitektur Jaringan



Gambar 2 Arsitektur Jaringan

Pada rancangan arsitektur gambar 2 akan diimplementasikan pada Dinas Komunikasi dan Informatika Aceh Tengah dengan tujuan untuk mengamankan aplikasi web dari serangan cyber. Komputer pada rancangan topologi akan terhubung dalam satu jaringan menggunakan ip public dan dapat menggunakan untuk berbagi data dan komunikasi.

Adapun Flowchart dari proses implementasi web application firewall dapat dilihat pada gambar 3.



Gambar 3 Flowchart web application firewall

3. World Wide Web (Web)

World wide web (web) adalah komputer yang dapat menyimpan file-file termasuk penyimpanan database, database dibutuhkan untuk halaman web. Web suatu program yang dapat dirancang untuk proses informasi-informasi dari server komputer pada jaringan internet. Web dapat menampilkan informasi berupa teks, gambar bergerak dan gambar tidak bergerak, animasi, audio. Web juga dapat diartikan sebagai alat bantu untuk

dapat menciptakan sistem informasi global yang mudah berdasarkan hypertext[6].

4. Mikrotik Router

Mikrotik router adalah sistem operasi berbasis Linux yang digunakan untuk menjadikan PC berbasis Intel atau AMD (personal komputer) dan digunakan untuk menghubungkan 2 jenis atau lebih. Sedangkan mikrotik adalah sistem opreasi yang bisa menghubungkan banyak perangkat[7]. Mikrotik Router dapat dilihat pada gambar 4 berikut.

Gambar 4 . Mikrotik Router

5. Web Application Firewall

WAF adalah aplikasi firewall khusus untuk aplikasi berbasis HTTP (web). WAF berada di garis depan dari semua pemantauan lalu lintas situs web. Firewall aplikasi web adalah sistem keamanan yang memantau, memfilter, dan juga memblokir data pengguna/pengunjung dari aplikasi atau situs web[8].

3. HASIL DAN PEMBAHASAN

Proses yang dilakukan untuk menemukan meningkatkan keamanan pada jaringan dan aplikasi web server. Pengujian ini dilakukan untuk mengetahui sejauh mana tingkat keberhasilan sistem aplikasi web application firewall untuk mengatasi serangan pada jaringan dan web yang digunakan.

1. Konfigurasi web application firewall

Website yang akan diterapkan ini adalah website sederhana yang digunakan untuk pengujian keamanan web server dengan menggunakan firewall berbasis web application firewall (WAF) yang dalam hal ini akan menggunakan modsecurity. Adapun hasil dari desain aplikasi web yang sudah dibuat dapat dilihat seperti gambar berikut.

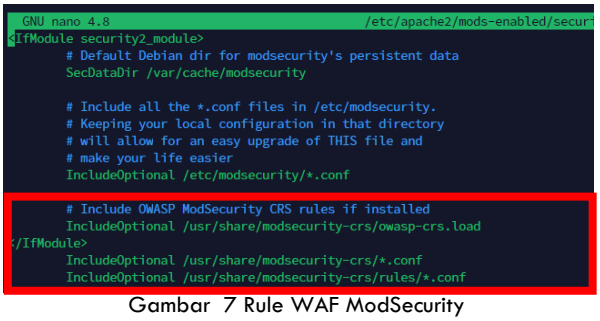
Gambar 5 Tampilan aplikasi web

2. Implementasi WAF

Untuk melakukan implementasi firewall dalam sistem keamanan web server, langkah yang harus dilakukan adalah menambahkan rule modSecurity terlebih dahulu. Untuk memastikan module firewall modSecurity sudah terpasang dengan benar dapat dilakukan dengan mengetikkan perintah “apachectl -M | grep --color security” dan “ls -l /var/log/apache2/modsec_audit.log”. Adapun hasil dari instalasi tersebut dapat dilihat seperti berikut ini.

Gambar 6 Hasil instalasi module modsecurity

Setelah berhasil menambahkan rule modsecurity pada web server, berikut tampilan rule modsecurity.



Gambar 7 Rule WAF ModSecurity

Pada gambar diatas merupakan rule modsecurity yang telah aktif digunakan pada web server, kegunaan dari rule modsecurity diatas untuk mencegah serangan cyber pada web yang akan diuji. Untuk melakukan konfigurasi terhadap rule firewall yang sudah di implementasikan seperti Gambar 7, dapat dilakukan dengan mengetikkan perintah "nano /etc/modsecurity/modsecurity.conf" sehingga dapat melakukan konfigurasi terhadap file firewall yang sudah diterapkan.

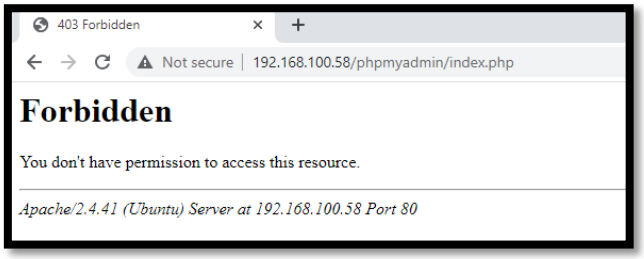
3. Hasil Pengujian

a. Pengujian SQL Injection

Pengujian ini dilakukan dengan dua skenario yaitu melakukan SQL injection sebelum WAF diterapkan dan setelah WAF diterapkan. Pengujian sql injection menggunakan phpmyadmin dimana pada saat pengujian terlebih dahulu memasukan nama pengguna dan password. Adapun hasil pengujian SQL injection sebelum WAF diterapkan dapat dilihat pada gambar dibawah ini.

Gambar 8 Sql injection sebelum waf diterapkan

Hasil dari pengujian ini adalah tidak berhasil login dengan menggunakan kode pada sql injection, karena penggunaan karakter khusus yang dapat memicu serangan tersebut. Selanjutnya pengujian kedua dilakukan saat WAF di terapkan. Adapun hasilnya dapat dilihat pada gambar berikut.

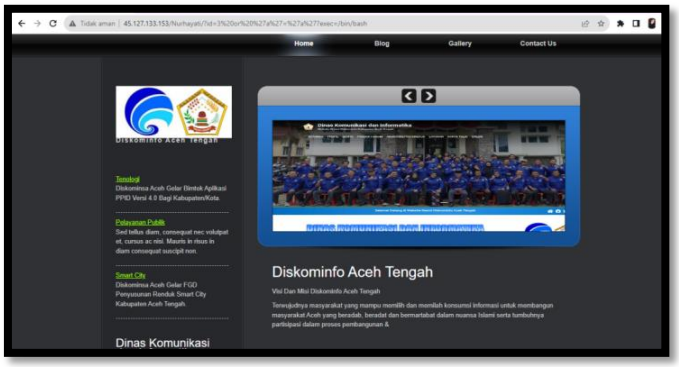


Gambar 9 Sql injection sesudah waf diterapkan

Pengujian ini dijalankan sebanyak 20 kali pada web menggunakan phpmyadmin dengan teknik SQL injection dan WAF (Web Application Firewall) berhasil terdeteksi. Dalam setiap pengujian, melakukan serangan injeksi SQL menggunakan berbagai teknik dan pola yang biasa digunakan oleh penyerang. Pengujian sql injection tidak berhasil login dengan menggunakan kode SQL Injection dan menampilkan pesan 404 Forbiden.

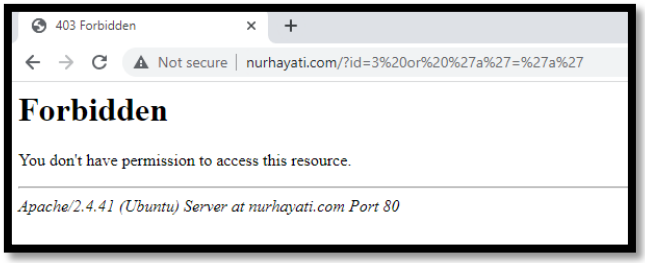
b. Pengujian cross site scripting (XSS)

Pengujian ini dilakukan dengan dua skenario yaitu melakukan cross site scripting sebelum WAF diterapkan dan setelah WAF diterapkan. dimana pada pengujian cross site cripting tersebut kita memasukan scriptnya langsung pada web yang akan diuji. Adapun hasil pengujian cross site scripting sebelum WAF diterapkan dapat dilihat pada gambar dibawah ini.



Gambar 10 Cross site scripting sebelum WAF diterapkan

Hasil dari pengujian pada gambar diatas adalah berhasil login pada web, karena WAF belum diterapkan pada server, jadi semua serangan yang ingin masuk pada web dapat berhasil login. Selanjutnya pengujian kedua dilakukan saat WAF di terapkan. Adapun hasilnya dapat dilihat pada gambar berikut.

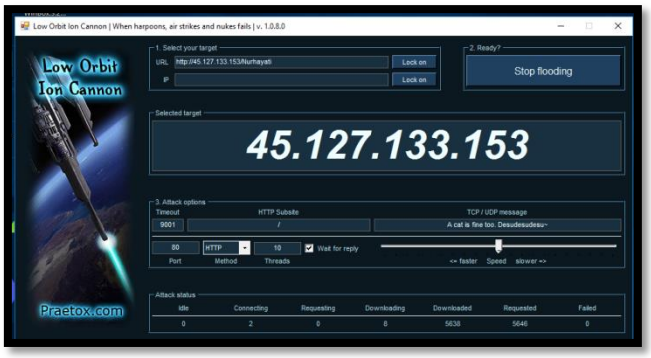


Gambar 11 Cross site scripting sesudah WAF diterapkan

Hasil dari pengujian cross site cripting adalah dengan memasukkan sintax script url "?exec=/bin/bash dan /?id=3%20or%20%27a%27=%27a%27" maka server akan mengeksekusi perintah tersebut. Pada pegujian yang dilakukan serangan XSS tidak berpengaruh pada aplikasi web server, dan ketika modsecurity dalam keadaan aktif serangan XSS akan dideteksi oleh server modsecurity dengan respone halaman seperti pada gambar 11, hal ini karena pada modsecurity mempunyai rule untuk menyaring request yang berpotensi serangan.

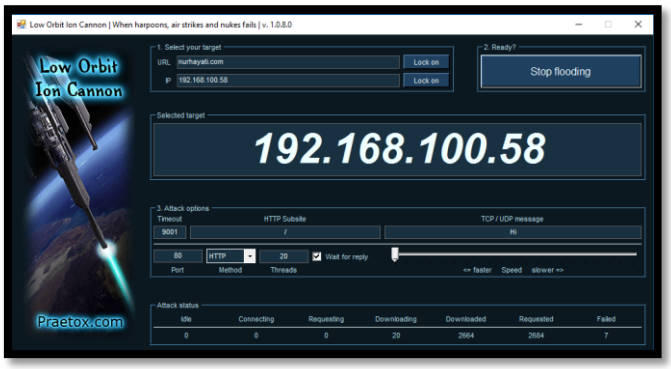
c. Pengujian Denial of service (DoS)

Pengujian ini dilakukan dengan dua skenario yaitu melakukan denial of service sebelum WAF diterapkan dan setelah WAF diterapkan. dimana pada pengujian denial of service tersebut menggunakan aplikasi LOIC, pada aplikasi LOIC tersebut kita perlu memasukan alamat ip dan nama web yang akan diuji. Adapun hasil pengujian denial of service sebelum WAF diterapkan dapat dilihat pada gambar dibawah ini.



Gambar 12 Denial of service sebelum WAF diterapkan

Pada pengujian denial of service pada gambar diatas menjelaskan bahwa serangan denial of service berhasil login pada web, karena WAF belum diterapkan pada server. Pada tampilan aplikasi loic tersebut pada bagian Connecting berhasil masuk pada web, jika web application firewall berfungsi pada server maka pada bagian Failed akan terdeteksi oleh server. Selanjutnya pengujian kedua dilakukan saat WAF di terapkan. Adapun hasilnya dapat dilihat pada gambar berikut.



Gambar 13 Denial of service sesudah WAF diterapkan

Pada gambar diatas menjelaskan bahwa saat WAF diterapkan pada server, serangan denial of service dapat mencegah serangan tersebut yang dapat menganggu keamanan web pada server. Pada aplikasi tersebut menjelaskan bahwa pada bagian Connecting tidak terdeteksi, sedangkan pada bagian Failed terdapat angka 7 yang berarti serangan tersebut dapat diatasi oleh web application firewall yang ingin mausk pada web yang diguankan.

4. Analisis Perbandingan Sebelum dan Sesudah Metode WAF

Tabel I REKAPITULASI PERBANDINGAN SEBELUM DAN SEDUDAH METODE WAF

No	Jenis Serangan	Sebelum Metode WAF	Sesudah Metode WAF
1	SQL Injection	Gagal diatasi oleh WAF	Berhasil diatasi oleh WAF
2	Cross Site Scripting	Gagal diatasi oleh WAF	Berhasil diatasi oleh WAF
3	Denial Of Service (DoS)	Gagal diatasi oleh WAF	Berhasil diatasi oleh WAF

Berdasarkan hasil rekapitulasi pada table 1 perbandingan serangan sebelum metode WAF dan sesudah metode WAF. Adapun hasil dari perbandingan sebelum dan sesudah metode WAF dapat diperoleh hasil pengukuran sebagai berikut:

1) Perbandingan Sql Injection
   Hasil perbandingan sql injection sebelum dan sesudah penerapan metode WAF pada table diatas menunjukan bahwa metode mempengaruhi keamanan pada web. Sebelum penerapan metode WAF web tidak dapat diatasi oleh sql injection, karena penggunaan karakter khusus yang dapat memicu serangan tersebut. Sedangkan setelah penerapan metode WAF server dapat mendeteksi dan mengatasi serangan yang ingin merusak keamanan web pada server.

2) Perbandingan Cross Site Scripting
   Hasil perbandingan cross site scripting sebelum dan sesudah penerapan metode WAF pada table 1 menunjukan bahwa metode mempengaruhi keamanan web pada server. Sebelum penerapan metode WAF serangan cross site scripting tidak dapat dicegah oleh server. Sedangkan sesudah metode WAF yang diterapkan dalam server dapat mencegah serangan cross site scripting yang ingin merusak keamanan web pada server.
3) Perbandingan Denial Of Service (DoS)
   Hasil perbandingan denial of service sebelum dan sesudah metode WAF pada table 1 menunjukan bahwa metode WAF mempenaruhi keamanan pada web. Sebelum metode WAF diterapkan pada server, serangan denial of service dapat mempengaruhi keamanan web. Sedangkan sesudah diterapkan metode WAF, server dapat mencegah serangan tersebut yang dapat menganggu keamanan web pada server.

5. Hasil pengujian

Setelah melakukan pengujian serangan maka diperoleh sebuah hasil dari pengujian tersebut yang akan dianalisa. Hasil pengujian dapat dilihat pada table 1 dengan jenis serangan SQL Injection, Cross Site Scripting dan Denial Of Service.

Tabel II HASIL PENGUJIAN SERANGAN

Jenis Serangan	Terdeteksi	Tidak terdeteksi	Hasil pengujian
SQL Injection	✓		20
Cross Site Scripting	✓		20
Denial Of Service (DoS)	✓		20
Total Pengujian			60

Pada table diatas menunjukan bahwa serangan pada web server dapat dideteksi oleh modsecurity, serangan SQL Injection, cross site scripting, dan denial of service berdasarkan Core Rule Set yang ada pada modsecurity, rule set berisi aturan untuk menyaring request dari client yang berpotensi serangan berdasarkan parameter yang diberikan oleh rule pada modsecurity. Dalam pengujian sebanyak 60 kali percobaan terhadap ketiga serangan yang dilakukan pada server. Waf mampu mengatasi serangan yang dilakukan pada server tersebut secara berulang-ulang. Sehingga ketika client atau attacker menyerang web server dengan jenis serangan ini maka modsecurity akan memberikan respon 403.

6. Hasil Persentase sesudah WAF diterapkan

Pada hasil Persentase pengujian Cross site Scripting, SQL Injection, dan Denial Of Service (DDOS) yang dilakukan dapat dilihat dari tabel 3 dibawah:

Tabel III HASIL REKAPITULASI PERSENTASE SESUDAH WAF DITERAPKAN

Jenis Serangan	Terdeteksi	Tidak terdeteksi	Hasil pengujian
SQL Injection	✓		20
Cross Site Scripting	✓		20
Denial Of Service (DoS)	✓		20
Total Pengujian			60

Hasil pada pengujian web server menggunakan web application firewall pada tabel tersebut memberikan gambaran yang jelas tentang persentase serangan yang berhasil terdeteksi oleh sistem keamanan. Dengan adanya tingkat keberhasilan yang signifikan ini memberikan keyakinan dalam melindungi web server dari serangan yang berpotensi merusak dan mempertahankan integritas sistem. Data yang diperoleh dari hasil pengujian yang dilakukan, kemudian di analisis dengan cara menghitung persentase pengamatan yang dilakukan pada setiap pengujian yang dilakukan. Untuk menghitung persentase tersebut digunakan rumus sebagai berikut:

$$\text{Persen\%} = \frac{\text{Jumlah Bagian}}{\text{Jumlah Total}} \text{X } 100\ \%$$

Dalam pengamatan yang telah dilakukan, kita memiliki beberapa variabel yang penting untuk menghitung persentase keberhasilan. Variabel tersebut adalah jumlah bagian (jumlah pengujian yang berhasil), jumlah pengujian yang dilakukan (60 kali), dan jumlah total (jumlah pengujian keberhasilan, juga 60 kali). Untuk menghitung persentase keberhasilan, kita dapat menggunakan rumus berikut: Persentase Keberhasilan = Jumlah Bagian Jumlah Total × 100 % Dengan memasukkan nilai variabel yang diberikan ke dalam rumus tersebut, kita dapat menghitung persentase keberhasilan:

$$\text{Persen\%} = \frac{60}{60} \text{X } 100\ \%$$

Jadi, hasil persentase keberhasilan dari pengamatan yang dilakukan adalah 100%, yang berarti bahwa seluruh 60 pengujian yang dilakukan berhasil.

4. KESIMPULAN

Adapun kesimpulan yang dapat penulis simpulkan setelah melakukan penelitian mengenai Implementasi Keamanan Jaringan Dengan Metode Web Application Firewall adalah:

1. Pada pengujian serangan Denial Of Service (DDoS) dengan 20 kali percobaan berhasil dicegah oleh web application firewall.
2. Pada pengujian serangan Cross-Site Scripting (CSS) dengan 20 kali percobaan berhasil dicegah oleh web application firewall pada web.
3. Pada pengujian yang dilakukan, web application firewall berhasil melindungi web server dari serangan SQL Injection yang menggunakan phpMyAdmin.
4. Penerapan metode web application firewall mendapatkan kualitas lebih baik dilihat dari nilai pengujian denial of service, cross site scripting, dan sql injection yaitu 100%.
5. Metode web application firewall merupakan metode keamanan yang dapat direkomendasikan untuk menangani ancaman sql injection, cross-site scripting, dan denial of service.

REFERENSI

[1] Muharromin, M. 2023. Analisis Performance Web Application Firewall ModSecuritydan Shadow Daemon Dalam Keamanan Web Server Apache. ……, 393, 393–402.

[2] Wicaksono, D. 2022. Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering. JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), 9(2), 1380–1392. https://doi.org/10.35957/jatisi.v9i2.2103.

[3] Arman, M., & Rachmat, N. 2020. Implementasi Sistem Keamanan Web Server Menggunakan Pfsense. Jusikom : Jurnal Sistem Komputer Musirawas, 5(1), 13–23. https://doi.org/10.32767/jusikom.v5i1.752

[4] Fachri, F., Fadlil, A., & Riadi, I. 2021. Analisis Keamanan Webserver menggunakan Penetration Test. Jurnal Informatika, 8(2), 183–190. https://doi.org/10.31294/ji.v8i2.10854

[5] Nitra, R. O., & Ryansyah, M. 2019. Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen. Jurnal Sistem Dan Teknologi Informasi (JUSTIN), 7(1), 52. https://doi.org/10.26418/justin.v7i1.29979.

[6] Informasi, S., Tiket, P., Wisata, M., & Web, C. B. 2023. INTI NUSA MANDIRI. 18(1), 84–92.

[7] Yesyogya. (n.d.). materi teknologi informasi jaringan komputer jaringan mikrotik. Www.Yesjogja.Com. Retrieved March 3, 2023, from https://www.yesjogja.com/materi/teknologi-informasi/jaringan komputer/jaringan-mikrotik/.

[8] Security, W. 2023. Mengenal Web Application Firewall (WAF): Jenis, Manfaat, dan Cara Kerjanya. Idcloudhost.Com. https://idcloudhost.com/blog/apa-itu-waf/.

[9] Muhammad, A. 2022. Firewall: Pengertian, Fungsi, Manfaat, Jenis, Cara Kerjanya. Www.Niagahoster.Co.Id. https://www.niagahoster.co.id/blog/firewall-adalah/.