IMPLEMENTASI REVERSE PROXY DAN MODSECURITY UNTUK MENINGKATKAN KEAMANAN DAN PERFORMA PADA SERVER LINUX

Muhammad Ariyanda Zulyadiansyah, Lalu A.Syamsul Irfan Akbar, Dwi Ratnasari

Jurusan Teknik Elektro Universitas Mataram
[1]ariyanda2107@gmail.com, [2]laluirfan@gmail.com, [3]tsabat.wyk@gmail.com

ABSTRAK

Reverse proxy sebagai peningkatan performa dan keamanan pada server Linux telah menjadi solusi yang efektif dalam menghadapi tantangan meningkatnya lalu lintas web dan serangan terhadap server. Makalah ini membahas peran dan manfaat penggunaan reverse proxy dalam meningkatkan performa dan keamanan pada server Linux.

Pada tugas ini menjelaskan keuntungan dari caching yang disediakan oleh reverse proxy. Melalui penyimpanan sementara (cache) konten statis, reverse proxy dapat mengurangi waktu respon dan meminimalkan beban server backend, sehingga meningkatkan performa secara signifikan.

Kemudian, tugas akhir ini membahas kemampuan reverse proxy dalam melindungi server dari serangan dengan menyediakan lapisan keamanan tambahan. Reverse proxy dapat berfungsi sebagai filter untuk mencegah berbagai macam serangan contohnya dalam kasus ini yakni SQL Injection.

Pada percobaan yang dilakukan, Reverse proxy mampu meningkatkan performa dari 15,58 detik menjadi 9,28 detik. Ini menunjukkan peningkatan performa sebesar 40,43 %. Sedangkan untuk keamanan reverse proxy terbukti mampu memblokir serangan sql injection dengan bantuan aplikasi modsecurity didalamnya.

ABSTRACT

Reverse proxy as a performance and security enhancement on Linux servers has become an effective solution in addressing the challenges of increasing web traffic and server attacks. This paper discusses the role and benefits of using reverse proxy in improving performance and security on Linux servers.

This study explains the advantages of caching provided by reverse proxy. By caching static content, the reverse proxy can reduce response time and minimize the load on the backend server, thus significantly improving performance.

Furthermore, this final project discusses the ability of reverse proxy to protect servers from attacks by providing an additional layer of security. Reverse proxy can function as a filter to prevent various types of attacks, such as SQL Injection in this case.

In the experiment conducted, the reverse proxy was able to improve performance from 15.58 seconds to 9.28 seconds, indicating a performance improvement of 40.43%. As for security, the reverse proxy proved capable of blocking SQL injection attacks with the help of the modsecurity application integrated within it.

PENDAHULUAN

Website adalah kumpulan dari banyak halaman-halaman yang berisikan suatu hal dalam sebuah domain ataupun sub domain (Mahendra, 2017). Tempatnya berada di dalam *World Wide Web* di dalam internet. Website juga dapat diartikan sebagai sebuah halaman yang berisi data, baik data teks, gambar, suara dan lainya yang dapat diakses secara online. Indonesia menempati peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet di mana pada tahun 2021 diperkirakan netter Indonesia mencapai 112 juta orang (*Arianto,Taufik.2021)*.

Dalam era digital yang semakin berkembang saat ini,performa web server sangatlah penting bagi keberhasilan suatu bisnis online. Semakin cepat dan stabil sebuah situs web, semakin besar kemungkinan situs tersebut untuk mendapatkan pengunjung dan penghasilan yang lebih banyak.

Seiring berkembangnya penggunan internet diwaktu sekarang, timbulah beberapa ancaman dari sisi penyedia website dimana webserver mereka, terjadi di serang yang dapat mencuri data maupun merusak server. BSSN (Badan Siber dan Sandi Negara) mencatat terdapat 1,637,973,022 anomali serangan yang berupa Mylobot, Miningpool, Ddos, SQL Injection dan lain-lain. Serangan terbanyak yang dilakukan yakni Mylobot 730,946,488 (*Arianto,Taufik.2021)*.

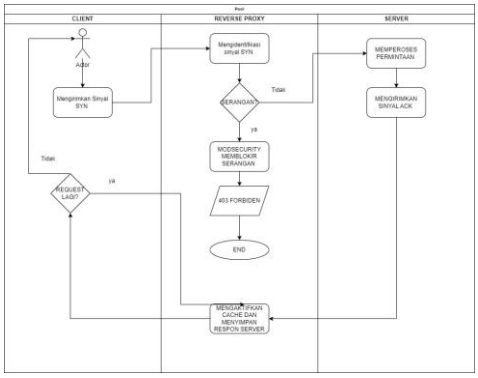
Untuk mengatasi permasalahan keamanan pada penggunaan internet dan meminimalisir kerugian dari serangan heacker maka Dengan ModSecurity dan reverse proxy ini bisa dikatakan efektif dalam menangani masalah ancaman serangan. Karena ModSecurity dapat diimplementasikan dengan berbagai aturan sesuai kebutuhan sehingga serangan dapat dikenali dan dicegah sesuai rule yang telah ditetapkan. Metode reverse proxy dapat menambah tingkat perlindungan sebuah server dari serangan karena metode ini membuat klien tidak memiliki hubungan langsung dengan server utama sehingga kontak antara server dengan pelaku penyerang dapat berkurang.

METODE

Metodologi penelitian ilmiah adalah prosedur secara ilmiah untuk mendapatkan data sehingga memenuhi tujuan penelitian. Metodologi yang digunakan oleh penulis dalam penulisan skripsi ini diambil berdasarkan tahapan-tahapan yang dilakukan dalam perancangan sistem, metode ini digunakan agar penulis dapat memiliki urutan kerja yang efisien. Adapun tahap-tahap yang akan dilakukan adalah sebagai berikut:

Gambar 1 Metode Penelitian

RANCANGAN ALUR KERJA SISTEM



Gambar 2 Diagram Rancangan Kerja Sistem

Proses kerja sistem yang akan di buat. Setiap request sistem yang di buat oleh client akan di proses reverse proxy.

Pada reverse proxy terdapat IDS (Intrusion Detection Sistem) yang berfungsi sebagai mengidentifikasi paket yang dikirim ke server apakah terdapat ancaman. Apabila pada paket yang dikirimkan oleh client terdapat ancaman maka modsecurity akan memblokir serangan tersebut.

INSTALASI SISTEM

Pada tahap ini dilakukan instalasi yang di gunakan untuk membangun sistem yang di inginkan.

- Instalasi nginx
- Instalasi modsecurity
- Instalasi burp suite
- Instalasi PHP
- Instalasi MYSQL

CONFIGURASI

Tahap ini merupakan tentang ulasan tahap configurasi dari setiap componen yang ada pada metode ini.

1. Configurasi REVERSE PROXY
   - Menginstal Ubuntu server pada reverse proxy
   - Menginstal nginx
   - Mengkonfigurasi reverse proxy
   - Menghubungkan antara reverse proxy dan server asli
   - Mengkonfigurasi firewall pada reverse proxy untuk mencegah serangan terhadap reverse proxy
   - Menginstal wireshark untuk memonitoring

2. Configurasi Server asli
   - Menghubungkan API agar server dapat saling berkomunikasi
   - Menginstal apache bachmark

3. Configurasi PC Attacker
   - Menginstal NMAP untuk memetakan server Target
   - Menginstal SYN FLOODING ATTACKER.

PERANCANGAN UJICOBA

Pada pengujian kali ini dilakukan dengan cara menghubungkan beberapa perangkat yakni server, reverse proxy, dan client. Adapun topologi yang digunakan yakni topologi tanpa menggunakan reverse proxy dan menggunakan reverse proxy.

Gambar 3 Pengujian Tanpa Reverse Proxy

Gambar 4 Pengujian Menggunakan Reverse Proxy

Pada tahapan ini akan di aktifkan rules pada modsecurity yang berfungsi untuk memblokir serangan dari client. Adapun tahap – tahap ujicoba yang dilakukan yakni :

1. Mengjicoba performa server setelah dan sesudah menggunakan reverse proxy
2. Menguji rules untuk memblokir serangan SQL ijection
3. menguji relus untuk memblokir serangan DDOS

HASIL DAN PEMBAHASAN

Pada tahap pengujian di lakukan menggunakan OS Ubuntu 22.04 LTS dan webserver NGINX 18.00 dengan Reverse proxy sebagai perangkat pengaman yang telah di instal modsecuriy sebagai sistem firewall yang berguna untuk memblokir serangan yang di lakukan penyerang terhadap webserver. Ujicoba ini bertujuan untuk mengetahui apakah serangan yang dilakukan oleh penyerang dapat merusak atau mencuri data pada webserver serta menguji reverse proxy dapat meningkatkan performa pada webserver tersebut.

UJICOBA PERFORMA SISTEM

No	time taken for test (s)	total transfer (bytes)	transfer rate (kb/s)	time per request (ms)
1	16,747	16830000	976,59	3,349
2	11,003	16830000	1484,81	2,201
3	12,776	16830000	1312,66	2,599
4	20,711	16830000	775,51	5,112
5	11,912	16830000	1496,22	2,272
6	14,889	16830000	1098,79	3,019
7	16,989	16830000	955,33	3,492
8	15,566	16830000	1029,77	3,121
9	16,212	16830000	996,13	3,266
10	19,022	16830000	883,31	4,893
Rata"	15,5827	16830000	1100,912	3,3324

Tabel 1 Pengujian Tanpa Reverse Proxy

pengujian tanpa menggunakan reverse proxy didapatkan hasil seperti pada tabel 4.1 rata – rata untuk time taken request sebesar detik dimana time taken request menandakan waktu yang digunakan server untuk mengirim data. Total transfer rata-rata yang di dapat di terima yakni 16730000 byte. Sedangkan rata-rata transfer rate yang didapatkan yakni 1100,912 kb/s . serta time per request rata-rata yang didapatkan 3,3324 ms yang dimana time per request menandakan waktu yang digunakan untuk 1 kali melakukan request ke server.

No	time taken for test (s)	total transfer (bytes)	transfer rate (kb/s)	time per request (ms)
1	8,01	16830000	2051,81	1,602
2	7,535	16830004	2181,35	1,507
3	9,54	16830004	1722,74	1,908
4	12,1655	16830004	1298,74	2,531
5	9,744	16830004	1686,78	1,949
6	8,433	16830000	1948,85	1,687
7	9,048	16830000	1816,52	1,801
8	9,13	16830000	1800,23	1,826
9	10,893	16830000	1508,86	2,179
10	8,347	16830000	1969,07	1,669
Rata"	9,28455	16830001,6	1798,495	1,8659

Tabel 2 Pengujian Menggunakan Reverse Proxy

Pada pengujian performa pada webserver menggunakan reverse proxy didapatkan hasil pada

tabel 4.2 didapatkan hasil rata-rata time taken for test sebesar 9,28455 second. Total transfer 16830001,1 byte. Transfer rate 1798,495 kb/s. Time per request 1,8659.

Nilai	time taken for test (s)	total transfer (bytes	transfer rate (kb/s)	time per request (ms)
Nilai Rata - Rata Tidak Menggunakan *Reverse Proxy*	15,5827	16830000	1100,912	3,3324
Nilai Rata - Rata Menggunakan *Reverse Proxy*	9,28455	16830001,6	1798,495	1,8659
Persentase kenaikan performa pada *Reverse Proxy*	40%		39%	44%

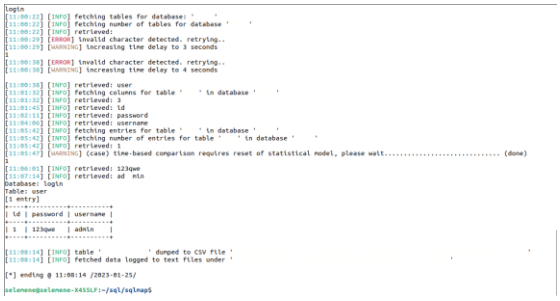
Tabel 3 Persentase Peningkatan Performa

peningkatan kecepatan pada server yang menggunakan reverse proxy, peningkatan untuk *time taken for test* meningkat sampai angka 40 % dan transfer rate meningkat 39% dari performa sebelumnya. Pada kecepatan untuk melayani setiap permintaan atau time per request meningkat sebesar 44%. Peningkatan ini dikarenakan sistem pada nginx mengaktifkan filtur cache kepada web browser yang dimana nginx memberikan perintah dan izin untuk menyimpan data dari webserver ke web browser yang kita punya. Apabila web browser menginginkan akses ke webserver yang sama maka web browser akan mengakses data penyimpanan sementara pada memori yang dimana proses ini akan menyebabkan waktu akses menjadi lebih cepat.

UJICOBA KEAMANAN SISTEM

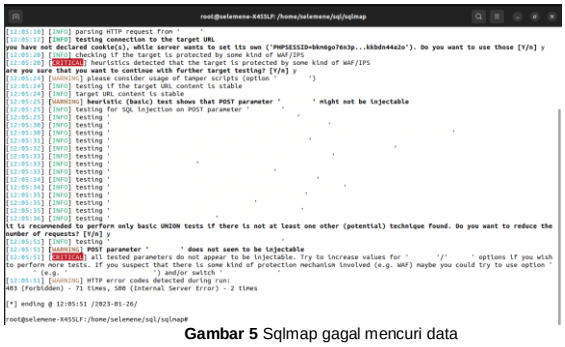
Pada pengujian sistem keamanan menggunakan Modsecurity versi 3.0 yang di jalankan pada OS Ubuntu 22.04 LTS yang dimana sistem keamanan di letakan pada sistem reverse proxy. Dengan sistem penyerangan menggunakan tools SQL ijection yang berfungsi mencuri data informasi yang terdapat di dalam database.

Pada pengujicobaan pertama pada sistem tidak terhubung dengan reverse proxy dan di dapatkan bahwa sql ijection mampu mengambil data yang telah di simpan di dalam database.



***Gambar 4 SQL** map mendapatkan data dari database*

Pada pengujian kedua *server* terlebih dahulu akan dihubungkan ke *server reverse proxy* yang telah terinstal *modsecurity V3.0. Modsecurity* pada sistem ini digunakan sebagai sistem *firewall* yang berguna untuk memblokir serangan yang masuk ke sistem *web server*.



Gambar 5 Sqlmap gagal mencuri data

Pada tahap ini *SQLMAP* tidak dapat menemukan *database* pada sistem *webserver* target dikarenakan pada gambar tersebut didapatkan hasil dengan status "*CRITICAL"* yang berarti bahwa segala variabel atau parameter yang ditemukan tidak dapat di-*injection* dikarenakan sudah diaktifkannya sistem keamanan *webserver* yaitu *ModSecurity*

sehingga hasilnya didapatkan yaitu ditolaknya akses ke *webserver* dengan kode 403 *Forbidden*.

KESIMPULAN

Berdasarkan penelitian yang sudah dilakukan, terdapat beberapa hal yang bisa penulis simpulkan antara lain sebagai berikut.

1. Penerapan Reverse Proxy pada webserver dapat meningkatkan performa, dengan cara mengaktifkan sistem cache untuk mempercepat memberikan respon pada client. Peningkatan performa pada server pada indikator time taken for test yakni sebesar 40%,transfer rate sebesar 39%, serta time per request sebesar 44%. Pada pengujian ini hasilnya sangat di pengaruhi oleh koneksi internet yang digunakan.
2. Penerapan dari sistem keamanan *Web Application Firewall ModSecurity* dapat memberikan keamanan *web server*, khususnya dari serangan *SQL Injection*. *ModSecurity* menyaring *request* dengan mengacu pada *OWASP rule* yang berisi berbagai *variabel* dan metakarakter *SQL* yang akan diawasi. Pada pengujian ini *rule* yang di taruh pada *reverse proxy*. Serta webserver yang diamankan hanya yang terhubung ke *reverse proxy*.

SARAN

Ada beberapa saran yang dapat penulis berikan apabila penelitian ini akan dikembangkan kembali antara lain sebagai berikut :

1. Saat pembuatan suatau aplikasi agar membatasi permission yang digunakan oleh sistem agar data yang terserang hanya pada permission yang diperbolehkan.
2. Saat melakukan perancangan sistem sebaiknya sistem dirancang dimana server dapat melakukan backup data apabila terjadi serangan agar mengurangi resiko kehilangan data.
3. *Sistem keamanan sebaiknya dibuat secara berlapis agar sistem lebih dapat diamankan dengan cara lebih baik.*

DAFTAR PUSTAKA

Aditya,Krisna (2011) Analisa Pemanfaatan Reverse Proxy Untuk Meningkatkan Efesiensi Pelayanan WEB Server: Universitas Islam Indonesia Yogyakarta.

Atmaji, E. S. J., & Susanto, B. M. (2016). Monitoring Keamanan Jaringan Komputer Menggunakan Network Intrussion Detection System (NIDS), 118–122.

Digdo, G. P. (2016). Melumpuhkan Hacker dengan Web Application Firewall. Yogyakarta: Andi.

Data, Mahendra (2017) *Optimizing Single Low-End LAMP Server Using NGINX Reverse Proxy Caching: International Conference on Sustainable Information Engineering and Technology (SIET)*

Izzati,Khairunnisa Andining (2018) Analisa Penerapan MODSECURITY Sebagai WEB Application Firewall (WAF) Pada Web Server: STMIK Bumi Gora.

Idhom,Muhammad(2022)Implementasi Reverse Proxy pada Hostingan WEB server di Docker Container:UPN

Mukhtar,Basem Ibrahim (2020) *Evaluating the Modsecurity Web Application Firewall Against SQL Injection Attacks:ICCES.*

Mentang, R., Sinsuw, A. A. E., & Najoan, X. B. N. (2015). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System, 5(7), 35–44.

Wahana Komputer. 2009, Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9. Yogyakarta: Penerbit ANDI Yogyakarta.

Semarang: Penerbit WAHANA KOMPUTER

Arianto,Taufik.2021,Lanskap Keamanan Siber Indonesia 2021.BSSN(Badan Siber dan Sandi Negara):www.bssn.go.id/

B. Mohammed Riyaz dan K. Thilagam (2015).,"Efficient web application firewall using mod_security" Journal of Network and Computer Applications

A. Valizadeh dan M. Saberi (2017),"Modsecurity-based intrusion detection system for web applications": International Journal of Information Security.

W. Huang dan X. Chen (2017),"Design and implementation of a web application firewall based on modsecurity": Journal of Information Security and Applications.

J. Jayakumar dan K. Thilagam,(2018)."An intelligent web application firewall using modsecurity for SQL injection and cross-site scripting attacks"Security and Communication Networks.

C.-M. Kuo(2015)."Scalable web application firewall using modsecurity in cloud environments", Computers & Security