IMPLEMENTASI SERTA ANALISA MODSECURITY DAN *REVERSE PROXY* UNTUK PENCEGAHAN *DDoS ATTACK* PADA *WEB SERVER*

LAPORAN SKRIPSI

Kevin Kautsar

4817050211

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

IMPLEMENTASI SERTA ANALISA MODSECURITY DAN *REVERSE PROXY* UNTUK PENCEGAHAN *DDoS ATTACK* PADA *WEB SERVER*

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

Kevin Kautsar

4817050211

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Kevin Kautsar

NIM : 4817050211

Tanggal : 4 Juni 2021

Tanda Tangan :

HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Kevin Kautsar
NIM	:	4817050211
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Implementasi serta Analisa ModSecurity dan *Reverse Proxy* Untuk Pencegahan DDoS *Attack* pada Web *Server*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, 16 Juni 2021 dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Ayu Rosyida Zain, S.ST, M.T. ( )

Penguji I : Drs. Abdul Aziz, M.M.SI. ( )

Penguji II : Syamsi Dwi Cahya, S.S.T., M.Kom. ( )

Penguji III : Indra Hermawan, S.Kom., M.Kom. ( )

Mengetahui:

Ketua Jurusan Teknik Informatika dan Komputer

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Ayu Rosyida Zain, S.ST, M.T, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan skripsi ini;
b. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan moral dan material;
c. Sahabat, terkhusus Cahya Mulyadi, David Matius, Giovanni Cornelia, Aji Trinioferi, Farhan Ramadahan P., Laily Rachmi Tsani, seluruh anggota UKM Pankreas serta seluruh warga Politeknik Negeri Jakarta yang telah banyak membantu penulis dalam menyelesaikan laporan skripsi ini; dan
d. Terimakasih kepada idola saya Akhmad Fadli dan Azizi Shafa Asadel yang telah memberikan dukungan dan semangat kepada penulis.

Akhir kata, penulis berharap Allah S.W.T. berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini membawa manfaat bagi pembaca dan perkembangan ilmu.

Depok, 2 Juni 2021

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan dibawah ini:

Nama	: Kevin Kautsar
NIM	: 4817050211
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

Implementasi serta Analisa ModSecurity dan *Reverse Proxy* Untuk Pencegahan DDoS *Attack* Pada Web *Server*

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencamtumkan nama saya sebagai penulis/pencIPta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : ……**Jakarta**……Pada tanggal : ……**2 Juni 2021**……

Yang Menyatakan

(Kevin Kautsar)

Implementasi serta Analisa ModSecurity dan *Reverse proxy* Untuk Pencegahan DDoS *Attack* Pada Web *Server*

ABSTRAK

Saat ini penggunaan *website* sudah lumrah dilakukan. Di Indonesia sendiri *website* sudah digunakan untuk berbagai macam kebutuhan mulai dari media informasi, tempat berbelanja, tempat mendengarkan musik, dan lain sebagainya. Dengan jumlah penduduk Indonesia sebanyak 270 juta jiwa lebih tak heran penggunaan *website* dapat berjalan optimal dan banyak sekali pemanfaatannya. Diprediksi *netter* Indonesia mencapai jumlah 112 juta orang. Namun, sayangnya banyaknya pengguna *website* di Indonesia berbanding lurus dengan ancaman sebuah perangkat terkena serangan DDoS. Telah diberitakan bahwa di Indonesia serangan DDoS naik tiga kali lipat selama pandemi Covid-19. Berkaca pada permasalahan ini dilakukan penelitian bagaimana caranya agar ancaman DDoS ini bisa diatasi atau bahkan dicegah sebelum terjadinya serangan. Dengan memanfaatkan ModSecurity sebagai *web application firewall* (WAF) yang kuat dapat memberikan perlindungan dari berbagai serangan terhadap aplikasi web dan memungkinkan pemantauan lalu lintas HTTP. Selain menggunakan WAF metode *reverse proxy* juga terbukti dapat menambah daya perlindungan sebuah *server* web karena dengan metode ini membuat tidak adanya keterkaitan langsung antara *client* dan *server* utama sehingga *server* terhindar dari serangan. Hal ini dapat dibuktikan dari perbandingan tiga kali serangan dalam keadaan ModSecurity dan *reverse proxy* mati dengan keduanya menyala. Hasilnya akan berbeda setelah dilakukan penyerangan menggunakan tiga *tools* serangan DDoS berbeda. Walaupun *reverse proxy* tidak dapat memblokir serangan, namun metode ini dapat membuat jarak serangan ke target menjadi lebih jauh. Ditambah dengan kemampuan ModSecurity dalam memblokir serangan, cara ini menciptakan dua perlindungan sekaligus bagi *server* dari ancaman serangan DDoS.

Kata Kunci : ModSecurity, *reverse proxy*, DDoS *attack*, *Web server*, jaringan

Implementation and Analysis of ModSecurity and Reverse Proxy For Prevention of DDoS Attacks on Web Servers

ABSTRACT

Nowadays the usage of the website becoming a common thing. In Indonesia itself the website has been used for variety of needs ranging from information media, shopping, listening to music, and so forth. With the approximately 270 million population of Indonesia made the usage of the website can run optimally and having a variety of utilization. It has been predicted that Indonesia's netter has reached 112 million people who are risked of being threatened by DDoS attacks. It has been reported that in Indonesia DDoS attacks has tripled during the Covid-19 pandemic. Reflecting on this problem, research was conducted to seek resolutions to prevent DDoS attack. Utilizing ModSecurity as a powerful web application firewall (WAF) could provide protection from various attacks against web applications and enable monitoring of HTTP traffic. In addition to using WAF, reverse proxy method has also proved to increase the protection of a web server. Because of this method, it helped to dissipate direct connection between the client and the main server in order to avoid the attacks. This could be proven from the comparison of three attacks in a ModSecurity state and reverse proxy off with both on. The result would be different after the attack using three different DDoS attack tools. Although reverse proxies could not block attacks, this method would widen the gap of the attack's distance to the target even further. Supported with ModSecurity's ability to block attacks, it develops two protections at once for servers from DDoS attack threats.

Keywords : *ModSecurity, reverse proxy, DDoS attack, Web server, network*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Website adalah kumpulan dari halaman-halaman situs yang terangkum dalam sebuah domain atau subdomain. 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* (Josi, 2017). Indonesia menempati peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet di mana pada tahun 2017 diperkirakan *netter* Indonesia mencapai 112 juta orang (Pranoto, et al., 2018). Namun, sayangnya banyaknya pengguna *website* berjalan lurus dengan besarnya ancaman bagi penyedia dan pengguna layanan *website*. Serangan yang sering ditemui pada *website* salah satunya adalah DDoS *attack*. Termuat dalam laman liputan6.com bahwa serangan DDoS naik tiga kali lipat selama pandemi Covid-19. Hal ini disebabkan, hampir semua kegiatan-baik itu belajar, bekerja, atau bersantai-bergeser ke dalam bentuk *online* (Yuslianson, 2021).

Serangan DDoS merupakan varian lain dari DoS yang cara kerja nya sama dengan DoS namun serangan dilakukan oleh beberapa komputer dengan tujuan *server* tertentu (Somani, et al., 2017). Berkaca dari masalah ini lah dicari bagaimana caranya agar ancaman DDoS ini bisa diatasi atau bahkan dicegah sebelum terjadinya serangan. Salah satunya dengan memanfaatkan ModSecurity. ModSecurity merupakan *web application firewall* (WAF) yang dikembangkan oleh Trustwave's SpiderLabs. ModSecurity memiliki bahasa pemrograman berbasis *event* yang kuat yang memberikan perlindungan dari berbagai serangan terhadap aplikasi web dan memungkinkan pemantauan lalu lintas HTTP, *logging* dan analisis secara *real-time* (Siregar, 2018). Selain menggunakan ModSecurity, *Reverse proxy* juga dapat dimanfaatkan dalam melakukan pencegahan dari serangan DDoS. *Reverse proxy* mengatur agar sebuah *server* dapat berperan menjadi perantara antara klien dengan *server* utama. Sehingga metode ini membuat tidak adanya hubungan langsung antara klien dan *server* utama

sehingga klien terhindar dari serangan dari luar, pun juga sama dengan *server* utama yang terlindungi dari serangan dari penyerang.

Dengan ModSecurity dan *reverse proxy* ini bisa dikatakan efektif dalam menangani masalah ancaman DDoS. 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 DDoS karena metode ini membuat klien tidak memiliki hubungan langsung dengan *server* utama sehingga kontak antara *server* dengan pelaku penyerang DDoS dapat berkurang.

Penilitian Farid Ridho dalam "Analisis Kinerja ModSecurity (Studi Kasus: Pencegahan Terhadap Serangan SQL Injection)" hanya membahas ModSecurity dalam mencegah serangan SQL *injection*. Dan pada penelitian "Implementasi Squid Sebagai *Reverse proxy* Untuk Keperluan Backup *Server*" yang disusun oleh Cahya dan Ibnu menggunakan metode *reverse proxy* hanya untuk *backup server*. Padahal keduanya bisa dipadukan untuk memproteksi *Website* dari serangan DDoS. Pada penelitian ini akan terfokus pada pencegahan serangan DDoS pada *Website*. Penelitan kali ini dilakukan dengan menggunakan VirtualBox versi dengan Ubuntu sebagai sistem operasi, menggunakan Apache2 sebagai web *server*, dan NGINX sebagai *reverse proxy*-nya. Penelitian ini bertujuan serupa dengan penelitian yang dilakukan oleh Agung, et al., bahwa mengimplementasikan WAF pada aplikasi berbasis *web* dengan menggunakan ModSecurity dan *reverse proxy* dapat menambah fungsi keamanan web. Namun, kali ini lebih fokus pada serangan DDoS.

1.2 Perumusan Masalah

Perumusan masalah yang terdapat pada Implementasi ModSecurity dan *Reverse proxy* Untuk Pencegahan DDoS *Attack* pada Web *Server* ini adalah sebagai berikut:

1. Bagaimana implementasi ModSecurity dan *reverse proxy* pada web *server*,
2. Bagaimana efektivitas keamanan ModSecurity dan *reverse proxy* pada web *server* untuk serangan DDoS.

1.3 Batasan Masalah

Batasan masalah yang ditentukan dalam laporan skripsi Implementasi ModSecurity dan *Reverse proxy* Untuk Pencegahan DDoS *Attack* pada Web *Server* adalah:

1. Penelitian disimulasikan dalam skala kecil (menggunakan VirtualBox 6.1.18),
2. Penelitian ini disimulasikan dengan melibatkan sebuah perangkat *attacker*, sebuah perangkat *reverse proxy*, dan sebuah *server*,
3. Penelitian ini menggunakan web *server* Apache 2.4.46,
4. WAF (*Web Application Firewall*) yang diterapkan adalah ModSecurity,
5. *Configure rules* pada ModSecurity menggunakan *Open Web Application Security Project Core Rule Set* (OWASP CRS).
6. Menggunakan NGINX 1.20.0 sebagai *reverse proxy* pada Ubuntu 18.04.2,
7. Metode serangan yang akan dilakukan adalah DDoS menggunakan *file bash script*, GoldenEye, dan Hulk DDoS Attack.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari tulisan ini adalah untuk merancang, membangun, dan mengevaluasi tingkat keamanan penggunaan ModSecurity dan *Reverse proxy* pada *web server* untuk pencegahan serangan DDoS.

1.4.2 Manfaat

Dari penelitian ini, dapat diketahui apakah ModSecurity dan *Reverse proxy* efektif dalam mencegah terjadinya serangan DDoS pada web *server*.

1.5 Metode Pelaksanaan

Penelitian ini dilakukan menggunakan metode sebagai berikut :

1. Pengumpulan Data

   Dilakukan dengan mencari data atau informasi terkait masalah yang dijadikan topik penelitian melalui studi litelatur dari buku-buku dan jurnal penelitian yang berhubungan dengan topik penelitian.
2. Membuat Perancangan Sistem

Setelah mendapat referensi dari berbagai sumber dan mendapat bayangan alur kerja yang diinginkan. Dilakukan perancangan desain sistem yang akan dibuat.

3. Implementasi Sistem

   Dilakukan tahapan-tahapan kerja sesuai dengan rancangan sistem yang telah dibuat.

4. Pengujian

   Dilakukan pengujian berupa serangan DDoS sebelum dan sudah pengaplikasian ModSecurity dan *reverse proxy* dan mencoba beberapa kali metode yang telah dIPahami untuk memastikan metode ini benar telah mengamankan *Website*.

5. Analisa Hasil Pengujian

   Setelah mencatat hasil pengujian. Data dikumpulkan dan dianalisa satu per satu untuk dibandingkan antara serangan sebelum dan setelah dilakukan pengimplementasian ModSecurity dan *reverse proxy*.

6. Penyusunan Laporan Penelitian

   Setelah data didapat, Penulis menyimpulkan hasil temuannya.

BAB V
PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil dari penelitian "Implementasi ModSecurity dan Reverse Proxy Untuk Pencegahan DDoS Attack pada Web *Server*" yang telah dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut:

1. Ketiga serangan tidak dapat ditolak hanya dengan pengimplementasian *reverse proxy*. Namun, dengan jarak tempuh yang lebih jauh dari komputer penyerang ke *server* utama waktu yang dibutuhkan untuk sebuah serangan mencapai tujuan menjadi lebih lama 53,12509ms sehingga dapat menghambat laju kerja serangan,
2. Ketiga serangan dapat ditolak dengan pengimplementasian WAF ModSecurity,
3. Ketiga serangan dapat ditolak dengan pengimplementasian *reverse proxy* dan ModSecurity. Dapat dikatakan dengan pengimplementasian keduanya sebuah *server* memiliki dua perlindungan sekaligus.

5.2 SARAN

Saran yang dapat diusulkan pada penelitian ini adalah :

1. Bisa dikembangkan dengan adanya tampilan GUI dalam setiap langkah baik pada pengimplementasian ModSecurity maupun pada pengaturan *reversed proxy*.
2. ModSecurity dapat mengembangkan tampilan yang lebih mudah dimengerti bagi orang awam agar mudah dalam melakukan pengaturan dan tampilan operasi.
3. Untuk bisa dilakukan penelitian dengan skala yang lebih besar untuk mengetahui relibilitas dari metode ini.

DAFTAR PUSTAKA

Apache, 2021. *APACHE HTTP SERVER PROJECT.* [Online] Available at: https://httpd.apache.org/ABOUT_APACHE.html [Accessed 25 5 2021].

Arnaldy, D. & Hati, T. S., 2020. Performance Analysis Of Reverse Proxy And Web Application Firewall With Telegram Bot As Attack Notification On Web *Server*. *IEEE,* p. 1.

Carl Albing, J. V., 2008. The bash Shell. In: J. Bleiel, ed. *bash Cookbook: Solutions and Examples for bash Users.* Sebastopol: O'Reilly Media, Inc., p. 21.

Fitri, C. N., 2017. IMPLEMENTASI SQUID SEBAGAI REVERSE PROXY UNTUK KEPERLUAN BACKUP *SERVER*. *Jurnal Manajemen Informasi,* Volume 8, p. 30.

Hamzah, A., Ismail, S. J. I. & Meisaroh, L., 2019. Implementasi Sistem Monitoring Jaringan Menggunakan Zabbix dan Web Web Application Firewall di PT PLN (Persero) Transmisi Jawa Bagian Tengah. *e-Proceeding of Applied Science,* 5(3), p. 3.

Harjono, E. B., 2016. Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *SinkrOn,* Volume 1, p. 31.

Hassen, O. A. & Ibrahim, H. k., 2020. Preventive Approach against HULK Attacks in Network Environment. *International Journal of Computing and Business Research,* 7(3), p. 4.

Josi, A., 2017. *PENERAPAN METODE PROTOTIPING DALAM PEMBANGUNAN WEBSITE DESA (STUDI KASUS DESA SUGIHAN KECAMATAN RAMBANG),* Prabumulih: Komputerisasi Akuntansi, Stmik Prabumulih, Prabumulih.

Muzaki, R. A., Briliyant, O. C. & Hasditama, M. A., 2020. Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall. *IEEE,* Issue Web Security, p. 90.

NGINX, 2021. *nginx.* [Online] Available at: https://nginx.org/en/ [Accessed 7 March 2021].

Nurkamiden, M. R., Najoan, M. E. I. & Putro, M. D., 2017. Rancang Bangun Sistem Pengendalian Perangkat Listrik Berbasis Web *Server* Menggunakan Mini PC Raspberry Pi Studi Kasus Gedung Fakultas Teknik Universitas Sam Ratulangi. *E-Journal Teknik Informatika*, Volume 11, p. 3.

Pranoto, Y. A., Rokhman, M. M. & Wibowo, S. A., 2018. APLIKASI PEMETAAN BERBASIS WEBSITE UNTUK PUSAT KESEHATAN MASYARAKAT DI WILAYAH KABUPATEN MALANG. *Jurnal MNEMONIC*, 1(PEMETAAN BERBASIS WEBSITE UNTUK PUSAT KESEHATAN MASYARAKAT KABUPATEN MALANG), p. 50.

Somani, G. et al., 2017. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. p. 1.

Tao, Y. & Chen, G., 2016. An Extensible Universal Reverse Proxy Architecture. *International Conference on Network and Information Systems for Computers*, p. 8.

Ubuntu, 2021. *The Story of Ubuntu.* [Online] Available at: https://ubuntu.com/about [Accessed 20 5 2021].

VirtualBox, 2021. *VirtualBox.* [Online] Available at: https://www.virtualbox.org/wiki/VirtualBox

Yari, I. A., Abdullahi, B. & Adeshina, S. A., 2019. Towards a Framework of Configuring and Evaluating ModSecurity WAF on Tomcat and Apache Web *Server*s. *15th International Conference on Electronics Computer and Computation*, Issue Web *Server* Security, p. 1.

Yasin, A. & Mohidin, I., 2018. DAMPAK SERANGAN DDOS PADA SOFTWARE BASED OPENFOW SWITCH DI PERANGKAT HG553. *JTech*, 6(DAMPAK SERANGAN DDOS), pp. 72-73.

Yuslianson, 2021. *LIPUTAN 6.* [Online] Available at: https://www.liputan6.com/tekno/read/4252904/serangan-ddos-naik-tiga-kali-lipat-selama-pandemi-covid-19 [Accessed 13 May 2020].

LAMPIRAN

DAFTAR RIWAYAT HIDUP PENULIS

Lahir di Surabaya, 2 Juli 1999. Lulus dari SD Muhammadiyah 1 Sidoarjo pada tahun 2011, SMPN 19 Jakarta pada tahun 2014, dan SMAN 90 Jakarta pada tahun 2017 dan Diploma II program studi *Network Administrator Professional* di CCIT-FTUI pada tahun 2019. Saat ini sedang menempuh Pendidikan Diploma IV Program Studi Teknik Informatika Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.