https://doi.org/10.32815/jitika.v19i1.1070

Vol. 19, No. 1, Tahun 2025

Jurnal Ilmiah Teknologi Informasi Asia

Halaman Situs Jurnal: https://jurnal.asia.ac.id/index.php/jitika

Artikel

Analisis Tingkat Efektivitas Cloudflare, Docker dan Nginx Proxy Manager Sebagai Sarana untuk Meningkatkan Keamanan Web

Mochamad Yusuf Setiya Putra [a,*], Arif Saivul Affandi [a]

[a] *Universitas Merdeka Malang, Malang, 65146, Indonesia*

Abstrak*—Keamanan siber semakin menjadi isu krusial seiring dengan berkembangnya teknologi dan meningkatnya ancaman serangan terhadap aplikasi berbasis web. Penelitian ini bertujuan untuk menganalisis tingkat efektivitas implementasi teknologi Cloudflare, Docker dan Nginx Proxy Manager, baik secara individu maupun kombinasi, sebagai lapisan keamanan tambahan dalam meningkatkan keamanan aplikasi web dari berbagai ancaman tersebut. Pendekatan kuantitatif dengan metode quasi eksperimental serta desain eksperimen *posttest-only control group* digunakan dalam penelitian ini. Kelompok kontrol dalam penelitian ini adalah sistem tanpa lapisan keamanan tambahan yang digunakan sebagai baseline pengukuran tingkat keamanan sistem, sedangkan kelompok eksperimen terbagi menjadi tiga yaitu sistem dengan Cloudflare saja, sistem dengan Docker dan Nginx Proxy Manager saja, serta sistem dengan kombinasi ketiganya. Pengujian dilakukan dengan menggunakan beberapa jenis serangan seperti DDoS, *brute force attack*, XSS, dan SQL *injections*, menggunakan alat seperti Slowhttptest, Burp Suite, XSSer, dan SQL Map. Hasil dari pengujian dianalisa dengan analisis deskriptif untuk jenis data kategorikal, dan secara statistik untuk data numerik menggunakan uji One Way Anova atau Kruskal Wallis, serta uji lanjutan *post-hoc*. Hasil penelitian menunjukkan sistem dengan kombinasi Cloudflare, Docker dan Nginx Proxy Manager memberikan perlindungan paling optimal dengan penurunan jumlah serangan berhasil hingga 52% pada DDoS, 69% pada *brute force attack*, 75% pada XSS, dan 100% pada SQL *injection* serta menunjukkan hasil yang signifikan dibandingkan sistem tradisional maupun dengan sistem yang menggunakan teknologi keamanan secara individu.

Kata kunci*— *cloudflare; docker; keamanan siber; nginx proxy manager

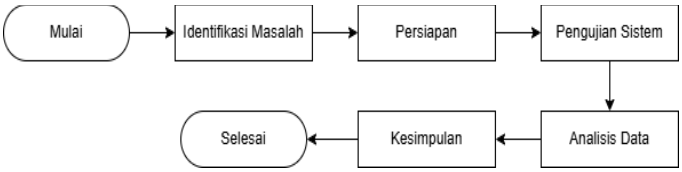
1. Pendahuluan

Keamanan siber masih menjadi isu krusial di tengah pesatnya perkembangan teknologi saat ini. Seiring bertambahnya penggunaan internet dan teknologi berbasis web, tindakan kejahatan yang terjadi di ranah digital atau biasa disebut dengan istilah *cyber crime* menjadi semakin kompleks dan meningkat (Wahib et al., 2022). Menurut data yang dikutip dari BSSN pada bulan Agustus tahun 2024 saja di Indonesia telah terjadi sekitar 14.918.178 anomali trafik yang berpotensi sebagai aktivitas serangan siber (Id-SIRTII/CC, 2024). Beragam serangan siber yang dapat mengancam aplikasi web seperti DDoS, *brute force attack*, XSS, dan *SQL Injection* menjadi semakin populer dan dapat berpotensi merugikan banyak pihak terkait (Fortinet, 2024).

Serangan *Distributed Denial of Service* atau DDoS merupakan jenis serangan yang bertujuan untuk membanjiri server dengan banyak *request* sehingga dapat mengakibatkan server menjadi *down* (Firmansyah, 2021). *Brute force attack* merupakan serangan siber yang berjalan dengan cara memecahkan masalah dengan mencoba berbagai jenis kemungkinan kombinasi *password* sehingga dapat memperoleh kombinasi yang benar (Rahmah, 2023). XSS atau *Cross-site Scripting* menjadi jenis serangan yang paling mudah karena dapat dilakukan tanpa

* Penulis korespondensi.
Alamat E-mail: yusufuyaimub87@gmail.com (M. Y. S. Putra)

Email para penulis: MYSP (yusufuyaimub87@gmail.com), ASA (fandi@unmer.ac.id),
Digital Object Identifier 10.32815/jitika.v19i1.1070
Manuskrip dikirim 22 November 2024; direvisi 11 Desember 2024; diterima 20 Desember 2024.
ISSN: 2580-8397(O), 0852-730X(P).



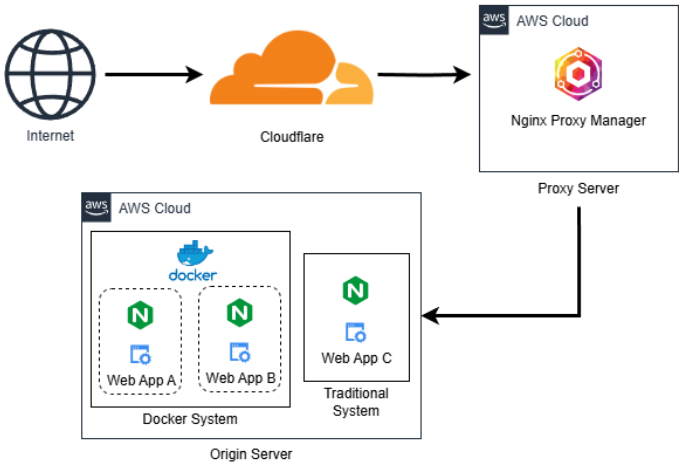
Gambar 1. Diagram Alur Penelitian

memakai *tools* yang rumit dan dengan hanya menuliskan *script* berbahaya ke dalam *form* yang terdapat di sebuah aplikasi web (Laleb, 2023). *SQL Injection* atau injeksi SQL adalah serangan yang berjalan dengan melakukan eksploitasi keamanan website melalui berbagai upaya pengiriman *query* SQL berbahaya dalam sistem, sehingga *hacker* dapat melakukan eksploitasi seperti modifikasi, mengambil, hingga menghapus *database* tanpa perlu hak istimewa (Prasetyo et al., 2024).

Dalam meningkatkan keamanan aplikasi web dari beragam jenis serangan yang sudah disebutkan diatas, perlu diperhatikan upaya keamanan mulai dari tahap pengembangan aplikasi. Developer dapat menerapkan pendekatan *secure coding* untuk meningkatkan keamanan aplikasi dalam mencegah serangan *SQL Injection*, dengan melakukan validasi pada URL, validasi data, menggunakan PDO dalam mengeksekusi *query*, serta tokenisasi sesi (Harefa et al., 2021). Namun, langkah-langkah tersebut hanya memberikan perlindungan pada level aplikasi dan sering kali tidak cukup dalam menghadapi ancaman yang lebih kompleks dan terfokus pada jaringan. Oleh karena itu strategi keamanan tambahan diperlukan untuk memberikan perlindungan lebih menyeluruh terhadap ancaman yang semakin kompleks seperti dengan penggunaan *firewall* sebagai barikade perlindungan jaringan dari akses yang tidak sah, serta melindungi jaringan dari lalu lintas yang mencurigakan (Satriyawan & Susanto, 2023).

Pemanfaatan teknologi Cloudflare, Docker dan Nginx Proxy Manager dalam hal ini dapat digunakan untuk menambah lapisan keamanan aplikasi web dari sisi jaringan. Dari penelitian yang dilakukan oleh Kusuma (2022) menjelaskan bahwa Cloudflare merupakan penyedia layanan keamanan aplikasi berbasis web yang memiliki beragam fitur di dalamnya seperti *Web Application Firewall* (WAF), *Content Delivery Network* (CDN), dan mitigasi *DDoS* sehingga dapat dimanfaatkan untuk meningkatkan keamanan aplikasi berbasis web yang dikonfigurasikan di dalamnya. Penelitian lain yang dilakukan oleh Ekaputra & Affandi (2023) menyatakan bahwa pemanfaatan Docker dan Nginx Proxy Manager sebagai lapisan tambahan dapat berfungsi untuk meningkatkan fleksibilitas pengaturan server yang lebih aman melalui *reverse proxy* dan isolasi kontainer.

Dari beberapa penelitian tersebut meskipun teknologi Cloudflare, Docker dan Nginx Proxy Manager sudah banyak digunakan dalam konteks keamanan, namun belum ada penelitian relevan yang mengkaji dengan dalam tentang efektivitas kombinasi ketiga teknologi ini dalam menghadapi ancaman siber yang beragam seperti DDoS, *brute force attack*, XSS, dan *SQL Injection*, kebanyakan masih berfokus pada analisa terhadap penggunaan teknologi secara individual. Penelitian ini menawarkan pendekatan unik dengan integrasi tiga teknologi tersebut sebagai lapisan keamanan tambahan aplikasi web dari sisi jaringan. Analisis tidak hanya mengevaluasi performa



Gambar 2. Topologi Arsitektur Sistem

teknologi secara individual, tetapi juga mengkaji tingkat efektivitas kombinasi ketiganya apakah lebih efektif digunakan secara individu atau secara kombinasi dalam menghadapi berbagai jenis ancaman siber yang telah diujikan.

2. Metode

Pendekatan kuantitatif dengan metode *quasi eksperimental* digunakan dalam penelitian ini. *Quasi eksperimental* adalah salah satu jenis penelitian eksperimen yang bertujuan untuk menguji hubungan sebab akibat, namun tidak dilakukan pengacakan secara penuh terhadap kelompok kontrol dan kelompok eksperimen (Rustamana et al., 2024). Desain eksperimen *posttest-only control group* juga digunakan karena cocok dengan tujuan penelitian ingin mengukur dampak penerapan teknologi keamanan tambahan terhadap tingkat keamanan sistem setelah diterapkan perlakuan atau *Treatment* (Rikatsih et al., 2020). Penelitian ini menggunakan 2 jenis kelompok diantaranya adalah kelompok tanpa intervensi (kelompok kontrol) dan kelompok yang menerima perlakuan (kelompok eksperimen). Kelompok kontrol mencakup sistem tanpa dilengkapi teknologi keamanan tambahan yang digunakan sebagai *baseline* pengukuran tingkat keamanan sistem, sementara kelompok eksperimen terbagi menjadi tiga skenario yaitu sistem dengan Cloudflare, sistem dengan Docker dan Nginx Proxy Manager, serta sistem dengan kombinasi Cloudflare, Docker dan Nginx Proxy Manager. Prosedur yang dilakukan dalam penelitian mencakup beberapa tahap, meliputi identifikasi masalah hingga penarikan kesimpulan yang diperoleh.

2.1. *Identifikasi Masalah*

Gambar 1 menampilkan diagram alur proses penelitian ini. Tahap awal penelitian akan dilakukan identifikasi masalah terkait kebutuhan untuk meningkatkan keamanan aplikasi berbasis web dari berbagai jenis potensi serangan siber. Identifikasi tersebut mencakup pemahaman akan jenis-jenis ancaman yang dapat membahayakan aplikasi, serta berbagai jenis teknologi yang akan dipakai dalam penelitian. Teknologi tersebut termasuk pemanfaatan Cloudflare, Docker, dan Nginx Proxy Manager. Teknologi-teknologi ini dipilih karena perannya dalam memberikan lapisan keamanan tambahan pada

Tabel 1. Hasil Pengujian DDoS

No Uji	Tanpa Perlindungan	Cloudflare	Docker & Nginx Proxy Manager	Kombinasi
1	786	473	496	439
2	789	501	504	486
3	793	491	504	465
4	790	496	504	491
5	788	497	504	431
...	...	...	...	...
10	792	485	504	489
Mitigasi Serangan	21%	51%	50%	52%

aplikasi web melalui mitigasi ancaman, isolasi sistem, dan pengelolaan lalu lintas jaringan.

2.2. Persiapan

Persiapan lingkungan uji dilakukan dengan penyusunan arsitektur sistem berdasarkan kebutuhan pengujian. Persiapan arsitektur sistem dilakukan pada layanan *cloud* milik Amazon Web Service dengan gambaran sistem yang mengacu pada Gambar 2.

2.3. Pengujian Sistem

Pengujian dilakukan dengan simulasi serangan DDoS, *brute force attack*, XSS, dan *SQL Injection* pada setiap kelompok uji. Setiap pengujian dilakukan pengulangan sebanyak 10 kali untuk memperoleh hasil yang valid. Pengujian tersebut menggunakan beberapa alat yang sesuai untuk setiap jenis serangan, yaitu slowhttptest untuk simulasi DDoS, Burp Suite untuk *brute force attack*, XSSer untuk serangan XSS, serta SQLMap untuk serangan *SQL Injection*. Data yang dikumpulkan untuk dianalisis berupa jumlah serangan berhasil menembus sistem untuk jenis serangan DDoS, *brute force attack*, dan XSS, serta status keberhasilan serangan untuk *SQL Injection*.

2.4. Analisis Data

Data dari hasil pengujian dikumpulkan dan dianalisis untuk menentukan perbedaan signifikansi antar kelompok. Analisis statistik akan digunakan untuk memberikan pemahaman yang objektif dan terukur mengenai efektivitas setiap teknologi baik itu Cloudflare, Docker dan Nginx Proxy Manager yang terbagi dalam setiap kelompok uji. Dengan menggunakan metode statistik, hasil pengujian dapat diinterpretasikan secara lebih akurat, sehingga memungkinkan untuk menilai sejauh mana perbedaan signifikan antara setiap kelompok uji dalam menahan serangan siber.

Data yang bersifat kategorikal akan dianalisis menggunakan analisis deskriptif untuk menggambarkan hasil serangan secara umum, sedangkan hasil pengujian dengan bentuk data numerik akan dilakukan uji normalitas terlebih dahulu untuk mengetahui bentuk distribusi data. Setelah uji normalitas dilakukan, untuk menguji adanya signifikansi perbedaan 2 kelompok atau lebih akan digunakan uji parametrik *One Way* Anova apabila distribusi data bersifat normal. Namun apabila tidak, analisis akan dilakukan menggunakan uji non-parametrik Kruskal-Wallis (Sugiyono, 2017). Apabila ditemukan perbedaan signifikan antar kelompok, analisis lanjutan dengan uji *post-hoc* akan dilakukan untuk mengetahui perbedaan spesifik antar kelompok dan menentukan kelompok mana yang paling efektif menghadapi serangan.

2.5. Pengambilan Kesimpulan

Pada tahap pengambilan kesimpulan, penelitian ini akan menyimpulkan hasil dari pengujian dan analisa mengenai pengaruh teknologi terhadap tingkat keamanan sistem. Kesimpulan akan mencakup efektivitas masing-masing teknologi yang terbagi dalam setiap kelompok uji dalam menahan dan memitigasi serangan yang telah dilakukan, serta menyimpulkan apakah ketiga teknologi lebih efektif digunakan secara individu atau secara kombinasi dalam menambah tingkat keamanan aplikasi berbasis web.

3. Hasil dan Pembahasan

Hasil dari pengujian yang telah dilakukan terhadap setiap kelompok uji dengan menggunakan jenis simulasi serangan DDoS, *brute force attack*, XSS, dan *SQL Injection* akan disajikan dan dianalisis secara statistik maupun secara deskriptif untuk memberikan pemahaman yang lebih mendalam tentang efektivitas dari teknologi yang terbagi dalam setiap kelompok uji. Analisis ini mencakup perbandingan hasil pengujian dari setiap skenario serta penilaian terhadap kemampuan masing-masing teknologi, baik secara individu maupun dalam kombinasi, dalam menghadapi ancaman keamanan.

3.1. Hasil Pengujian DDoS

Jumlah serangan berhasil hasil dari pengujian DDoS yang telah dilakukan pada setiap kelompok uji dengan frekuensi serangan 1000 koneksi setiap satu kali uji adalah pada Tabel 1. Hasil dari pengujian DDoS pada setiap kelompok uji menunjukkan hasil yang bervariasi. Sistem dikatakan lebih aman jika presentase mitigasi serangan lebih besar. Data yang diperoleh merupakan data numerik yang dapat dianalisis lebih lanjut secara statistik. Oleh karena itu hasil uji DDoS pada tahap selanjutnya akan dilakukan analisa secara statistik untuk mengetahui signifikansi hasil uji setiap kelompok.

3.2. Hasil Pengujian Brute Force Attack

Jumlah serangan berhasil yang diperoleh dari pengujian *brute force attack* yang digunakan untuk menebak kredensial

Tabel 2. Hasil Pengujian *Brute Force Attack*

No Uji	Tanpa Perlindungan	Cloudflare	Docker & Nginx Proxy Manager	Kombinasi
1	40	13	40	4
2	40	14	40	14
3	40	14	40	13
4	40	13	40	13
5	40	10	40	13
...	...	...	...	...
10	40	14	40	14
Mitigasi Serangan	0%	67%	0%	69%

Tabel 3. Hasil Pengujian XSS

No Uji	Tanpa Perlindungan	Cloudflare	Docker & Nginx Proxy Manager	Kombinasi
1	1094	926	392	392
2	1095	914	392	392
3	897	926	392	282
4	921	924	277	312
5	905	926	318	302
...	...	...	...	...
10	1092	922	319	306
Mitigasi Serangan	20%	28%	74%	75%

Tabel 4. Hasil Pengujian SQL *Injection*

No Uji	Tanpa Perlindungan	Cloudflare	Docker & Nginx Proxy Manager	Kombinasi
1	Akses Berhasil	Akses Terblokir	Akses Berhasil	Akses Terblokir
2	Akses Berhasil	Akses Terblokir	Akses Berhasil	Akses Terblokir
3	Akses Berhasil	Akses Terblokir	Akses Berhasil	Akses Terblokir
4	Akses Berhasil	Akses Terblokir	Akses Berhasil	Akses Terblokir
5	Akses Berhasil	Akses Terblokir	Akses Berhasil	Akses Terblokir
...	...	...	...	...
10	Akses Berhasil	Akses Terblokir	Akses Berhasil	Akses Terblokir

login, pada setiap kelompok uji dengan jumlah 40 *payload* kombinasi *password* setiap satu kali uji pada Tabel 2. Hasil uji *brute force attack* menunjukkan terdapat beberapa kelompok uji yang menghasilkan data konstan, seperti pada kelompok sistem tanpa perlindungan dan sistem dengan Docker dan Nginx Proxy Manager yang masing-masing menghasilkan angka konstan yaitu 40. Meskipun demikian perbedaan antar kelompok masih dapat dianalisis menggunakan analisis statistik untuk melihat signifikansi perbedaan dari setiap kelompok uji.

3.3. Hasil Pengujian XSS

Jumlah serangan berhasil pada pengujian XSS yang dilakukan pada setiap kelompok uji, dengan jumlah *payload* sebanyak 1291 *script* berbahaya disajikan pada tabel 3. Hasil dari pengujian serangan *Cross-site Scripting* (XSS) menunjukkan nilai yang bervariasi. Hasil tersebut akan dikatakan lebih baik jika persentase mitigasi serangan lebih besar. Dikarenakan data hasil uji XSS merupakan jenis data numerik, maka akan dilakukan analisis secara statistik untuk melihat signifikansi perbedaan antar kelompok uji.

3.4. Hasil Pengujian SQL Injection

Status keberhasilan serangan pada pengujian *SQL Injection* yang dilakukan pada setiap kelompok uji dengan tahapan dan konfigurasi sama setiap satu kali uji terlampir pada tabel 4. Data hasil pengujian serangan *SQL Injection* menunjukkan bentuk data kategorial. Dengan demikian analisa secara deskriptif akan digunakan untuk menggambarkan presentasi hasil pengujian secara umum.

3.5. Uji Normalitas Hasil Pengujian

Hasil dari pengujian keamanan selanjutnya akan dilakukan analisa untuk mengetahui perbedaan signifikansi antar

Tabel 5. Hasil Pengujian SQL *Injection*

Serangan	Kelompok	Sig.
DDoS	Tanpa Perlindungan	.814
	Cloudflare	.224
	Docker & Nginx Proxy Manager	.000
	Kombinasi	.039
Brute Force Attack	Tanpa Perlindungan	.
	Cloudflare	.000
	Docker & Nginx Proxy Manager	.
	Kombinasi	.000
XSS	Tanpa Perlindungan	.000
	Cloudflare	.002
	Docker & Nginx Proxy Manager	.045
	Kombinasi	.013

Tabel 6. Uji Kruskal Wallis DDoS

	Serangan Berhasil
Kruskal-Wallis H	33.270
Df	3
Asymp. Sig	.000

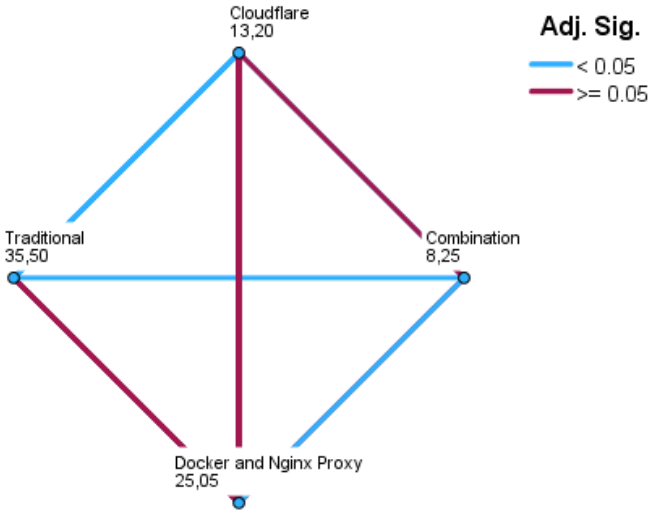
kelompok uji. Namun untuk melihat bentuk distribusi data jumlah serangan berhasil pada jenis serangan DDoS, *brute force attack*, dan XSS yang berupa data numerik, uji normalitas akan terlebih dahulu dilakukan menggunakan metode Shapiro-Wilk, karena jumlah data kurang dari 40 dari setiap kelompok (Haryono et al., 2023). Hasil dari uji normalitas yang telah dilakukan menghasilkan nilai signifikansi seperti pada Tabel 5.

Hasil dari uji normalitas menunjukkan bahwa terdapat beberapa kelompok yang memiliki nilai signifikansi < 0,05, nilai ini mengindikasikan kelompok tersebut tidak memenuhi asumsi normalitas. Selanjutnya pada jenis serangan *brute force attack*, terdapat nilai signifikansi yang hanya menunjukkan "." dikarenakan hasil dari pengujian menghasilkan data yang konstan. Hal ini menunjukkan bahwa data tersebut tidak memiliki variasi sama sekali dan tidak memenuhi asumsi normalitas. Dikarenakan terdapat beberapa kelompok yang tidak memenuhi asumsi normalitas pada setiap jenis serangan, maka untuk menjaga keakuratan hasil analisis akan dilakukan uji beda non-parametrik Kruskal-Wallis.

3.6. Analisis Signifikansi Jumlah Serangan Berhasil DDoS

Hasil dari pengujian DDoS yang berupa jumlah serangan berhasil menembus sistem, akan dilakukan uji beda Kruskal-Wallis untuk mengetahui signifikansi nilai rata-rata antar kelompok. Dari pengujian tersebut dapat dihasilkan tabel statistik Kruskal-Wallis seperti pada Tabel 6

Signifikansi dapat dilihat pada nilai Asymp. Sig. dari uji statistik Kruskal-Wallis yang menunjukkan nilai 0.000 sehingga lebih rendah dari 0.05. Dengan demikian hasil menunjukkan adanya signifikansi perbedaan pada nilai rata-rata jumlah serangan berhasil antara empat kelompok uji. Mengingat adanya perbedaan yang signifikan diantara kelompok uji, maka langkah selanjutnya akan dilakukan uji lanjutan *post-hoc* untuk menganalisis secara spesifik kelompok-kelompok mana yang memiliki perbedaan signifikan satu sama lain, dengan hasil sebagai berikut.



Gambar 3. Grafik *Pairwise Comparisons* DDoS

Berdasarkan grafik pada Gambar 3, diketahui bahwa kelompok sistem kombinasi memiliki nilai rata-rata terendah dibandingkan kelompok lainnya. Meskipun nilai tersebut rendah diantara semua kelompok uji, namun secara statistik tidak terdapat perbedaan secara signifikan dengan kelompok sistem dengan hanya menggunakan Cloudflare. Hal ini menunjukkan bahwa sistem dengan kombinasi Cloudflare, Docker dan Nginx Proxy Manager merupakan yang paling efektif digunakan terhadap serangan DDoS, meskipun secara statistik efektivitasnya setara dengan kelompok sistem yang hanya menggunakan Cloudflare secara individu.

3.7. Analisis Signifikansi Jumlah Serangan Berhasil Brute Force Attack

Hasil dari pengujian *brute force attack* yang berupa jumlah serangan berhasil akan dilakukan uji beda untuk mengetahui signifikansi nilai rata-rata antar kelompok. Hasil dari uji beda Kruskal-Wallis yang berupa tabel statistik dapat diperhatikan pada Tabel 7.

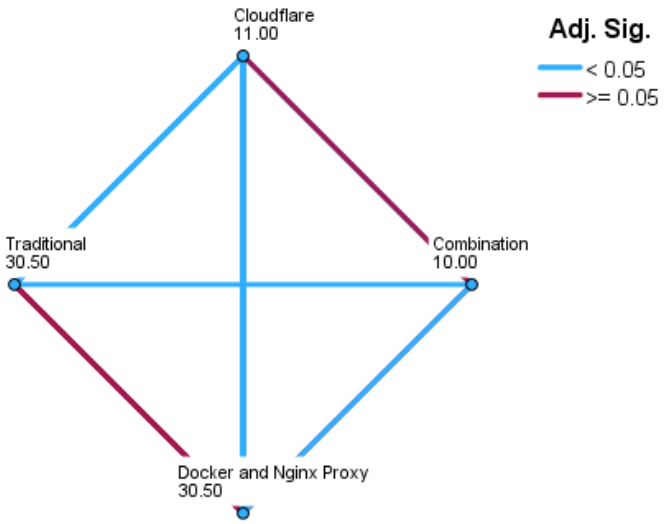
Hasil uji pada Tabel 7 menunjukkan bahwa Asymp. Sig. yang diperoleh adalah 0.000, sehingga dapat dikatakan lebih rendah dari 0.05. Nilai ini menunjukkan adanya signifikansi perbedaan pada nilai rata-rata antara keempat kelompok uji. Untuk melihat lebih mendalam perbedaan signifikansi nilai rata-rata

Tabel 7. Uji Kruskal-Wallis *brute force attack*

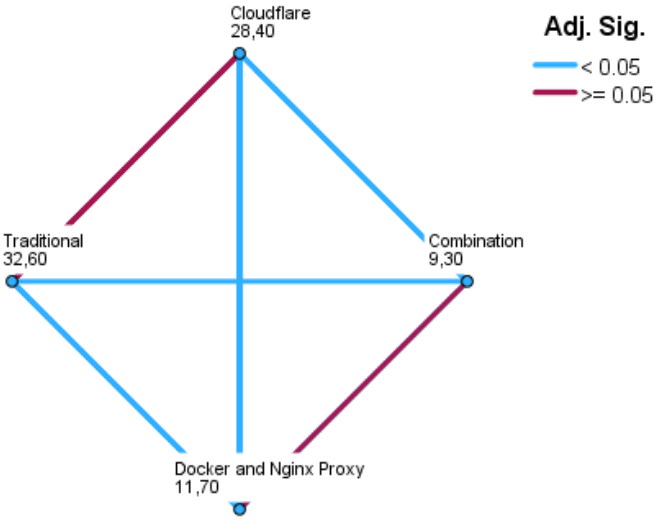
	Serangan Berhasil
Kruskal-Wallis H	34.366
Df	3
Asymp. Sig	.000

Tabel 8. Hasil Pengujian XSS

	Serangan Berhasil
Kruskal-Wallis H	30.224
Df	3
Asymp. Sig	.000



Gambar 4. Grafik *Pairwise Comparisons Brute Force Attack*



Gambar 5. Grafik *Pairwise Comparisons* XSS

pada setiap kelompok uji, akan dilakukan uji lanjutan *post-hoc* dengan hasil grafik *pairwise comparisons* seperti pada Gambar 4.

Dari grafik pada Gambar 4, dapat diketahui kelompok sistem kombinasi memiliki hasil nilai rata-rata terendah diantara semua kelompok, tetapi tidak berbeda secara signifikan dengan kelompok sistem yang hanya menggunakan Cloudflare. Hasil tersebut menunjukkan bahwa sistem dengan kombinasi Cloudflare, Docker dan Nginx Proxy Manager merupakan yang paling efektif digunakan dalam menghadapi jenis serangan *brute force attack,* namun secara statistik efektivitasnya sebanding dengan sistem yang hanya menggunakan Cloudflare secara individu.

3.8. Analisis Signifikansi Jumlah Serangan Berhasil XSS

Uji Kruskal-Wallis akan digunakan untuk mengukur signifikansi perbedaan nilai rata-rata antar kelompok uji pada hasil pengujian serangan *Cross-site Scripting* (XSS). Hasil dari uji yang telah dilakukan menghasilkan tabel statistik Kruskal-Wallis seperti pada Tabel 8.

Pada Tabel 8, terlihat bahwa hasil menunjukkan nilai Asymp. Sig. sebesar 0.000, sehingga lebih rendah dari 0.05. Ini menunjukkan terdapat signifikansi perbedaan dalam nilai rata-rata antara kelompok-kelompok yang diuji. Untuk menganalisis lebih lanjut perbedaan signifikan ini, uji lanjutan *post-hoc* akan dilakukan, yang hasilnya dapat dilihat pada grafik *pairwise comparisons* pada Gambar 5.

Berdasarkan hasil uji *post-hoc* seperti pada Gambar 5, kelompok sistem kombinasi memiliki hasil rata-rata paling rendah diantara semua kelompok uji, namun hasil tersebut tidak berbeda secara signifikan dengan kelompok sistem Docker dan Nginx Proxy Manager. Hal ini menunjukkan bahwa kelompok sistem kombinasi Cloudflare, Docker dan Nginx Proxy Manager menjadi yang paling efektif dalam menangani jenis serangan *Cross-site Scripting* (XSS), meskipun secara statistik sebanding dengan sistem yang hanya menggunakan Docker dan Nginx Proxy Manager.

3.9. Analisis Signifikansi Jumlah Serangan Berhasil SQL Injection

Dari hasil uji *SQL Injection,* data yang diperoleh berupa status keberhasilan serangan dengan tipe data kategorial. Oleh karena itu akan dilakukan analisa secara deskriptif untuk menggambarkan hasil uji secara umum. Adapun gambaran umum dari hasil pengujian dapat diperhatikan pada Tabel 9 sebagai berikut.

Tabel 9. Persentase Keberhasilan SQL *Injection*

Kelompok	Serangan Berhasil	Serangan Gagal	Persentase Keberhasilan
Tanpa Perlindungan	10	0	100%
Cloudflare	0	10	0%
Docker & Nginx Proxy Manager	10	0	100%
Kombinasi	0	10	0%

Dari Tabel 9, dapat disimpulkan bahwa kelompok sistem yang hanya menggunakan Cloudflare dan kelompok sistem kombinasi dapat secara 100% melindungi dari percobaan serangan *SQL Injection*. Sedangkan kelompok sistem tanpa perlindungan serta kelompok sistem Docker dan Nginx Proxy Manager masih dapat ditembus pada semua percobaan serangan *SQL Injection*.

4. Kesimpulan dan Saran

Dari hasil pengujian serta analisa yang sudah dilakukan menunjukkan hasil bahwa kombinasi dari ketiga teknologi Cloudflare, Docker dan Nginx Proxy Manager dapat memberikan perlindungan yang paling efektif terhadap serangan yang telah diujikan dibandingkan penggunaan teknologi secara individual. Semua teknologi dapat memberikan perlindungan berlapis yang optimal, kelemahan dari satu teknologi dapat ditutupi oleh teknologi lainnya serta tingkat keamanan dari satu teknologi dapat bertambah dengan pengaruh teknologi lainnya. Cloudflare dapat memberikan dampak besar perlindungan dari hampir semua jenis serangan yang sudah diujikan dengan fitur keamanan yang dimilikinya. Namun pada jenis serangan XSS, penggunaan Cloudflare secara individu memberikan hasil yang kurang efektif karena tidak memberikan signifikansi perbedaan dengan kelompok sistem tradisional. Docker dan Nginx Proxy Manager dapat memberikan lapisan keamanan tambahan dalam skenario keamanan berlapis, namun penggunaan teknologi ini saja secara individu masih kurang efektif tanpa dilengkapi Cloudflare. Tetapi dalam penelitian ini Docker dan Nginx Proxy Manager dapat memberikan peningkatan signifikan keamanan sistem dalam menghadapi jenis serangan XSS.

Adapun saran bagi penelitian selanjutnya antara lain supaya mempertimbangkan penggunaan layanan Cloudflare versi berbayar untuk mendapatkan fitur keamanan lebih lanjut. Selain itu, disarankan untuk melakukan pengujian dengan lebih banyak variasi serangan dan pengujian pada lingkungan dengan *trafic* yang lebih tinggi untuk mengetahui sejauh mana teknologi dapat menangani volume serangan yang lebih besar. Selain itu agar dapat mempertimbangkan menambah teknologi lapisan keamanan tambahan lainnya, seperti penggunaan *Web Application Firewall* (WAF) yang lebih canggih atau menambahkan IDS/IPS (*Intrusion Detection/Prevention Systems*), untuk mengeksplorasi kombinasi teknologi yang lebih optimal dalam meningkatkan keamanan aplikasi berbasis web.

5. Daftar Rujukan

Ekaputra, A. R., & Affandi, A. S. (2023). Pemanfaatan layanan cloud computing dan docker container untuk meningkatkan kinerja aplikasi web. *Journal of Information System and Application Development*, *1*(2), 138–147. https://doi.org/10.26905/jisad.v1i2.11084

Firmansyah, M. D. (2021). Analisa Keamanan Web Server Terhadap Serangan Distributed Denial of Service Menggunakan Modevasive. *Telcomatics*, *6*(1). https://doi.org/10.37253/telcomatics.v6i1.4990

Fortinet. (2024). *What Is A Cyber Attack?* . Fortinet. https://www.fortinet.com/uk/resources/cyberglossary/types-of-cyber-attacks

Harefa, J., Prajena, G., Alexander, A., Muhamad, A., Dewa, E. V. S., & Yuliandry, S. (2021). SEA WAF: The Prevention of SQL Injection Attacks on Web Applications. *Advances in Science, Technology and Engineering Systems Journal*, *6*(2), 405–411. https://doi.org/10.25046/aj060247

Haryono, E., Slamet, M., & Septian, D. (2023). *Statistika SPSS 28* (N. Rismawati, Ed.). Widina Bhakti Persada Bandung.

Id-SIRTII/CC. (2024). *Laporan Hasil Monitoring*. Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center. https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html

Kusuma, G. H. A. (2022). Sistem Firewall untuk Pencegahan DDOS Attack di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC)*, *3*(1).

Laleb, I. (2023). Analisis Cross-Site Scripting (XSS) Injection – Reflected XSS And Stored XSS Mengggunakan Framework OWASP 10. *Jurnal Ilmiah Flash*, *8*(1), 36. https://doi.org/10.32511/flash.v8i1.952

Prasetyo, S. E., Haeruddin, H., & Ariesryo, K. (2024). Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall. *Antivirus : Jurnal Ilmiah Teknik Informatika*, *18*(1), 27–36. https://doi.org/10.35457/antivirus.v18i1.3339

Rikatsih, N., Andary, R. W., Shaleh, M., Hadiningrum, L. P., Irwandy, I., Prisusanti, R. D., Nggaba, M. E., Hadi, P., Sihombing, B., Setiawan, J., & Saloom, G. (2020). *Metodologi Penelitian di Berbagai Bidang*. Media Sains Indonesia.

Rustamana, A., Wahyuningsih, P., Azka, M. F., & Wahyu, P. (2024). Penelitian Metode Kuantitatif. *Sindoro: Cendikia Pendidikan*, *5*(6).

Rahmah, S. A. (2023). Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web. *Journal of Computers and Digital Business*, *2*(3), 112–119. https://doi.org/10.56427/jcbd.v2i3.235

Satriyawan, H., & Susanto, D. S. (2023). Optimasi Keamanan Smart Grid Melalui Autentikasi Dua Lapis: Meningkatkan Efisiensi dan Privasi dalam Era Digital. *Jurnal RESTIKOM : Riset Teknik Informatika Dan Komputer*, *5*(3), 319–333. https://doi.org/10.52005/restikom.v5i3.254

Sugiyono, S. (2017). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabet.

Wahib, P., Narotama, A. T., Rijki, N. M., Sahrudin, S., Permana, F., Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security Awareness untuk meningkatkan literasi digita. *Abdi Jurnal Publikasi*, *1*(2).

Foto dan biografi para penulis (Mochamad Yusuf Setiya Putra dan Arif Saivul Affandi) tidak tersedia pada saat publikasi.