Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 1 Januari 2024 Hal. 162-167
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

# Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi

**Nimatul Mamuriyah[a], Stefanus Eko Prasetyo[b], Abner Onesimus Sijabat[c]**
[a]Prodi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam, nimatul@uib.ac.id
[b]Prodi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Interansional Batam, stefanus@uib.ac.id
[c]Prodi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Interansional Batam, 2032034.abner@uib.edu

Submitted: 27-11-2023, Reviewed: 12-12-2023, Accepted 29-12-2024
https://doi.org/10.47233/jteksis.v6i1.1124

***Abstract***
*With the growth of increasingly innovative technology, new media have been created to convey information, namely web applications. As technology continues to develop, Distributed Denial of Service (DDoS) attacks are becoming a serious threat to network security. This research problem arises from the increasing threat of Distributed Denial of Service (DDoS) attacks on network security, especially on web services. The research objective is to design a network security system that can protect websites from DDoS attacks. The research method uses penetration testing involving the target website, carrying out DDoS attacks with test tools, log analysis, and attack evaluation. Focusing on the use of Cloudflare's Web Application Firewall (WAF), Kali Linux, and GoldenEye test tools, this research aims to understand the effectiveness of the security system. The research results show that this security system design is successful in identifying, overcoming and reducing vulnerabilities to DDoS attacks. Penetration testing proved that Cloudflare can effectively detect and prevent DDoS attacks, while Kali Linux and GoldenEye were used as reliable testing tools. With proper implementation, this design can be widely applied to improve network security.*
***Keywords:*** *Cloudflare,*DDoS,*Firewall,GoldenEye,Kali linux*

**Abstrak**
Dengan tumbuhnya teknologi yang semakin inovatif, telah menciptakan media baru untuk menyampaikan informasi yaitu aplikasi web. Ketika teknologi terus berkembang, serangan Denial of Service Terdistribusi (DDoS) menjadi ancaman serius terhadap keamanan jaringan. Masalah penelitian ini muncul dari meningkatnya ancaman serangan Denial of Service Terdistribusi (DDoS) terhadap keamanan jaringan, khususnya pada layanan web. Tujuan penelitian adalah merancang sistem keamanan jaringan yang dapat melindungi website dari serangan DDoS. Metode penelitian menggunakan pengujian penetrasi dengan melibatkan target website, pelaksanaan serangan DDoS dengan alat uji, analisis log, dan evaluasi serangan. Dengan fokus pada penggunaan Web Application Firewall (WAF) Cloudflare, Kali Linux, dan alat uji GoldenEye, penelitian ini bertujuan untuk memahami keefektifan sistem keamanan. Hasil penelitian menunjukkan bahwa rancangan sistem keamanan ini berhasil mengidentifikasi, mengatasi, dan mengurangi kerentanan terhadap serangan DDoS. Pengujian penetrasi membuktikan bahwa Cloudflare dapat efektif mendeteksi dan mencegah serangan DDoS, sementara Kali Linux dan GoldenEye digunakan sebagai alat uji yang andal. Dengan implementasi yang tepat, rancangan ini dapat diterapkan secara luas untuk meningkatkan keamanan jaringan.
**Keywords:** *Cloudflare,*DDoS,*Firewall,GoldenEye,Kali linux*



## PENDAHULUAN

Kemajuan teknologi saat ini mengalami kemajuan yang sangat pesat, karena kemajuan teknologi selalu beriringan dengan kemajuan ilmu pengetahuan. [1]. Teknologi yang ada pada saat ini diperlukan untuk menyebarkan informasi secara luas dan tanpa batas [2], [3]. Masyarakat dituntut untuk dapat mengadopsi kemajuan teknologi [4]. Semakin berkembangnya internet juga berdampak banyaknya kejahatan internet yang terjadi [5].Namun tidak boleh diabaikan bahwa penggunaan internet juga mempunyai resiko dan kerugian. Salah satu contohnya adalah ancaman dari oknum tidak bertanggung jawab yang dikenal dengan sebutan hacker [6]. Jumlah ancaman dan serangan keamanan siber terus bertambah, dan standar keamanan seperti Intrusion Detection Systems, access control system, dan firewall seringkali tidak cukup untuk melindungi server dari penyerang [7]. Menurut [8] untuk mencegah serangan siber, harus melakukan uji penetrasi terlebih dahulu untuk mendapatkan informasi tentang celah yang dapat ditembus oleh hacker. Penetration testing dilakukan untuk menguji kerentanan website untuk menghasilkan website yang aman [9].

Jika web server mati, maka akses informasi yang di dapat akan terganggu.kelumpuhan web server juga dapat disebabkan oleh beberapa serangan salah satunya yaitu adalah Distributed Denial of Service

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 1 Januari 2024 Hal. 162-167
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

(DDoS) [10]. Ada banyak varian serangan DDoS, termasuk serangan DDoS HTTP lambat. Serangan ini terjadi ketika sejumlah besar permintaan HTTP yang tidak lengkap dikirim, yang jumlahnya bertambah tetapi tidak pernah selesai, sehingga memaksa server web untuk tetap membuka koneksi. Koneksi terbuka dapat dengan mudah menghabiskan sumber daya dan mencegah klien sah mengakses layanan di server web [11]. DDoS adalah suatu jenis serangan yang dilakukan oleh suatu attacker yang bertujuan untuk membanjiri lalu lintas jaringan dengan tujuan menghabiskan sumber daya yang dimiliki oleh suatu komputer atau server [12]. DDoS telah dikenal pada komunitas jaringan sejak awal 1980. Sasaran serangan DDoS dapat meliputi situs web bisnis, layanan cloud, lembaga pemerintah, institusi keuangan, media, serta infrastruktur kritis untuk menyebabkan gangguan dan ketidakstabilan dalam layanan online [13]. Serangan DDoS melibatkan penggunaan sejumlah besar perangkat yang terinfeksi atau dikendalikan oleh penyerang untuk secara bersamaan membanjiri target dengan lalu lintas data, menyebabkan penurunan kinerja atau bahkan kegagalan sistem [14], [15]. Hal ini dikarenakan satu layanan pada server di lakukan permintaan berkali-kali oleh penyerang.

[16] Penetration testing dapat difungsikan sebagai sarana untuk mengidentifikasi serta mengatasi kelemahan dalam infrastruktur jaringan, yang menunjukkan sejauh mana tingkat kerentanannya terhadap potensi serangan. Dengan mengatasi aspek tersebut, diharapkan organisasi dapat mengurangi kelemahan dalam sistem dan jaringan sebanyak mungkin, sehingga meningkatkan tingkat keamanan jaringan.

Serangan DDoS telah menjadi salah satu ancaman yang serius, dengan bahayanya terungkap pada minggu kedua bulan Agustus 2011 di Hong Kong, sebagaimana dilaporkan oleh cyber threat.id. Pada tanggal 12-13 Agustus 2011, serangan DDoS tersebut menyebabkan kelumpuhan pada server HKExnews.hk, mengakibatkan penangguhan sejumlah perdagangan besar di pasar keuangan terbesar ketiga di Asia. Perusahaan-perusahaan terkemuka seperti HSBC, Cathay Pacific Airways, dan HKEx sendiri, yang memiliki nilai pasar gabungan sekitar HK$ 1,5 triliun, terpaksa menghentikan kegiatan mereka [17].

Pada tahun 2019, menurut data yang dikumpulkan oleh Kaspersky DDoS Protection pada tanggal 11 November 2019, terjadi peningkatan sebesar 30% dalam serangan DDoS selama triwulan 3 dibandingkan dengan triwulan sebelumnya, dan tercatat kenaikan sebesar 32% jika dibandingkan dengan triwulan 3 tahun 2018. Peningkatan signifikan ini dipengaruhi oleh lonjakan aktivitas DDoS pada awal tahun ajaran, dengan sebagian besar serangan (53%) terdeteksi pada bulan September 2019. Kaspersky juga mengungkapkan bahwa 60% dari serangan yang berhasil dicegah ditujukan kepada sekolah dan situs jurnal elektronik [17].

Berdasarkan pemantauan sistem elektronik yang terkait dengan penyelenggaraan PON XX di Indonesia, terdapat sekitar 112.762.000 akses ke domain-domain yang terkait dengan PON 2021. Anomali trafik lainnya yang dicatat melalui pemantauan BSSN pada sistem elektronik yang terkait dengan penyelenggaraan PON XX 2021 adalah adanya upaya percobaan serangan DDoS [18].

Tujuan penelitian ini menggunakan website sebagai target DDoS yang dilindungi oleh *Web Application Firewall* (WAF) *Cloudflare* untuk dilakukan *penetration testing* dengan menggunakan kali linux untuk menguji keamanan dan kerentanan website terhadap serangan dari DDoS, penelitian ini dilakukan untuk mengetahui *Cloudflare* bekerja secara maksimal untuk serangan dari *hacker*. Dalam kasus Rancangan Sistem Keamanan Jaringan dari serangan DDoS menggunakan Metode Pengujian Penetrasi, berikut adalah beberapa poin yang mungkin relevan untuk disertakan dalam tinjauan pustaka:

1. Definisi Serangan DDoS:

DDoS adalah suatu jenis serangan yang dilakukan oleh suatu attacker yang bertujuan untuk membanjiri lalu lintas jaringan supaya menghabiskan sumber daya yang dimiliki oleh suatu komputer atau server[12].

2. Metode Pengujian Penetrasi:

Metode Pengujian Penetrasi merupakan pendekatan yang umum digunakan untuk menguji keamanan sistem, termasuk jaringan, dengan tujuan mengidentifikasi dan memastikan keberadaan potensi celah keamanan. Pendekatan ini bertujuan memberikan kemudahan bagi administrator atau pemilik jaringan dalam melakukan tindakan pencegahan sejak dini sebelum kemungkinan serangan terjadi [19].

3. Keamanan Jaringan:

untuk melindungi dari serangan DDoS menggunakan Cloudflare yang berfungsi untuk meningkatkan kinerja, keamanan, dan ketersediaan situs web [20].

4. Pentingnya Pemantauan Jaringan:

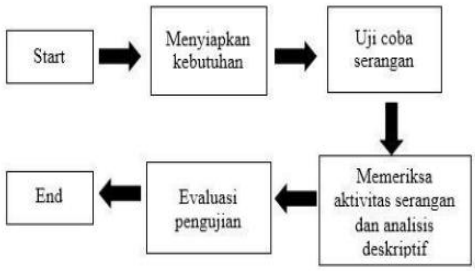
Pemantauan jaringan yang efektif sangat penting dalam mendeteksi dan merespons serangan DDoS secara cepat.

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 1 Januari 2024 Hal. 162-167
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

## METODE PENELITIAN

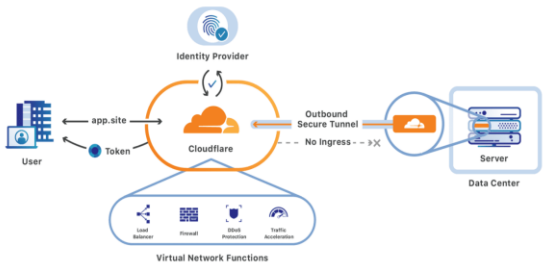
Dalam penelitian ini melakukan beberapa tahapan penelitian yang sudah ditentukan. Berikut merupakan gambar tahapan yang dilakukan.




Gambar 1 Diagram Alur Penelitian

Pada Gambar 1, dapat dijelaskan bahwa penulis menyiapkan website sebagai target untuk dilakukan nya uji coba serangan DDoS, setelah melakukan penyerangan menganalisis log dan mengevaluasi serangan untuk dibuatkan keamanan pada website tersebut.

Dalam rangka penelitian ini, Kali Linux digunakan sebagai perangkat lunak pengujian penetrasi pada komputer. Sistem operasi opensource ini tersedia secara bebas untuk umum, dirancang khusus untuk berbagai kegiatan keamanan informasi seperti pengujian penetrasi, riset keamanan, forensik komputer, dan rekayasa balik [18]. *GoldenEye* sebagai alat ini dapat digunakan untuk menguji apakah suatu situs rentan terhadap serangan DDoS [21]. Untuk sistem keamanan terhadap website, digunakan *WAF Cloudflare* yang menjadi *firewall* yang memonitor, filter, dan melakukan pemblokiran data yang berasal dari serangan DDOS ke website atau aplikasi web [22]. Penelitian ini menggunakan topologi keamanan seperti dibawah ini.



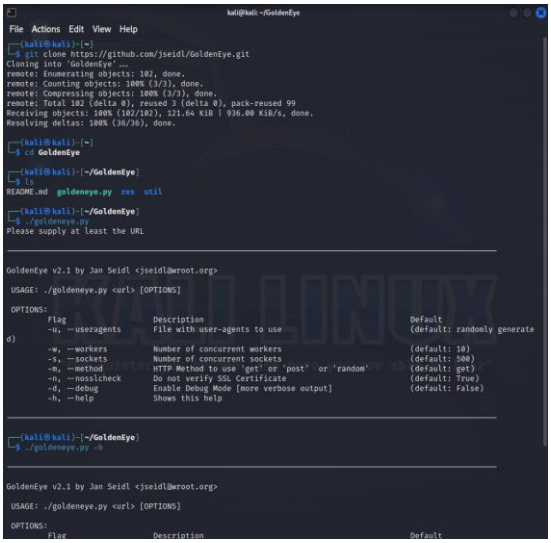

Gambar 2 Topologi Keamanan

Topologi keamanan dapat dilihat pada Gambar 2, dengan *Cloudflare* melibatkan penerapan beberapa lapisan perlindungan yang dirancang untuk memitigasi risiko keamanan pada aplikasi dan situs web. Secara umum, Cloudflare Web Application Firewall (*WAF*) ditempatkan di depan server asal untuk mendeteksi dan memblokir serangan berbasis web. Layanan DDoS protection *Cloudflare* diterapkan pada lapisan global, mengamankan infrastruktur dari serangan denial-of-service. SSL/TLS termination di *Cloudflare* memastikan enkripsi lalu lintas antara pengguna dan server, sementara fitur Access Control dapat digunakan untuk memberlakukan kebijakan akses berbasis identitas. Selain itu, *Cloudflare* menyediakan alat pemantauan dan analisis untuk melacak kinerja dan keamanan, sementara pengaturan DNS yang cermat memperkuat keamanan dan kecepatan resolusi. Terakhir, manajemen identitas yang ketat dan otentikasi kuat membantu melindungi akses ke dashboard dan API *Cloudflare*. Dengan kombinasi ini, topologi keamanan *Cloudflare* memberikan perlindungan menyeluruh dan peningkatan kinerja bagi aplikasi dan situs web.

## HASIL DAN PEMBAHASAN

Dengan memanfaatkan layanan Web Application Firewall *Cloudflare* menunjukkan bahwa WAF mampu secara efektif mendeteksi dan mencegah serangan berbasis web terutama pada serangan DDOS menggunakan tool *GoldenEye* untuk website yang akan diserang.

Hal ini dibuktikan dengan melakukan simulasi serangan pada website yang di *monitoring log* dengan *Cloudflare* dan berikutnya menambahkan WAF pada website tersebut. Pertama, mendownload tool *GoldenEye* di *Kali linux* seperti pada Gambar 3.



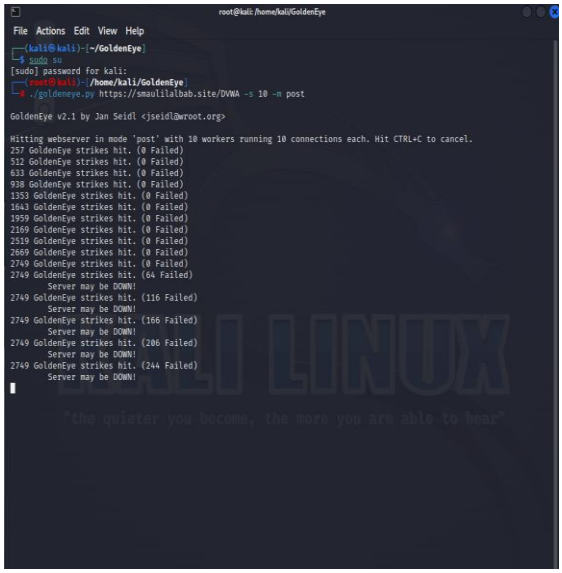

Gambar 3 GoldenEye

Dengan membanjiri server target dengan sejumlah besar permintaan, *GoldenEye* bertujuan untuk menekan daya tahan server, menyebabkan penurunan kinerja atau bahkan penonaktifan

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 1 Januari 2024 Hal. 162-167
http://jurnal.unidha.ac.id/index.php/jteksis

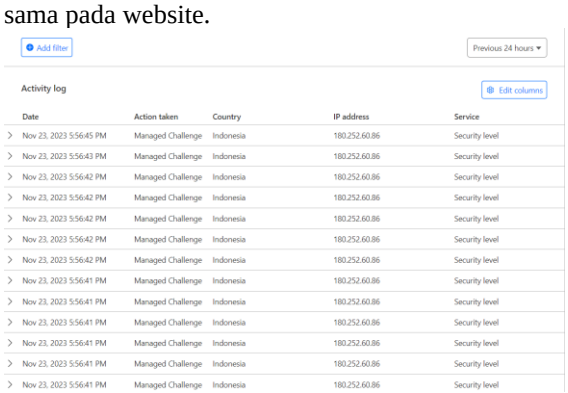
E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

sementara layanan seperti yang terlihat pada Gambar 4.




Gambar 4 Serangan DdoS

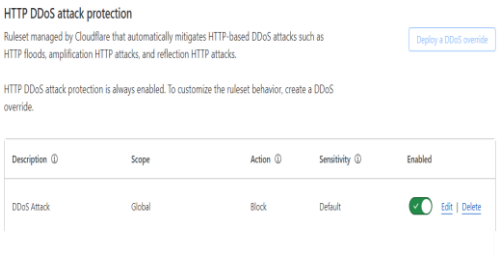
Gambar 4 dapat dijelaskan dengan perintah goldeneye.py -s 10, meminta goldeneye untuk menjalankan 10 koneksi dan 10 workers secara bersamaan. Dapat dilihat peningkatan permintaan yang dikirimkan kepada target sehingga mendapatkan informasi target tidak mampu menerima permintaan lagi. Pada Gambar 5, tercatat permintaan yang begitu banyak dari alamat IP yang sama pada website.




Gambar 5 Log serangan DDoS

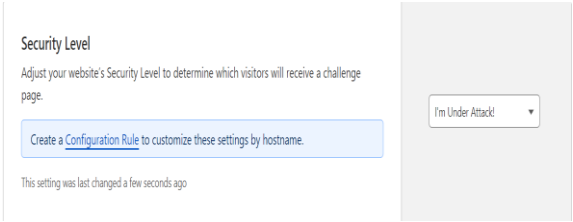
Selanjutnya melakukan penambahan *rules* pada *WAF* untuk mencegah serangan DDoS seperti pada Gambar 6, pertama yaitu mengaktifkan *HTTP* DDoS attack protection, yang dirancang untuk melindungi suatu sistem atau layanan web dari serangan DDoS yang menargetkan protokol *HTTP* seperti Gambar 7.


Gambar 6 Rules pada WAF



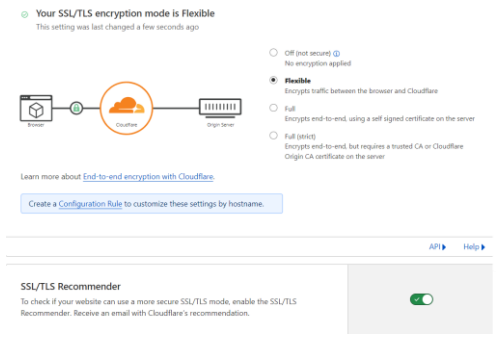

Gambar 7 setting HTTP DDoS attack protection

Kedua mengaktifkan mode " *I'm under attack*" seperti Gambar 8. Ketika fitur ini diaktifkan, *Cloudflare* akan memberlakukan lebih banyak langkah keamanan untuk melindungi situs web atau aplikasi Anda dari serangan siber.



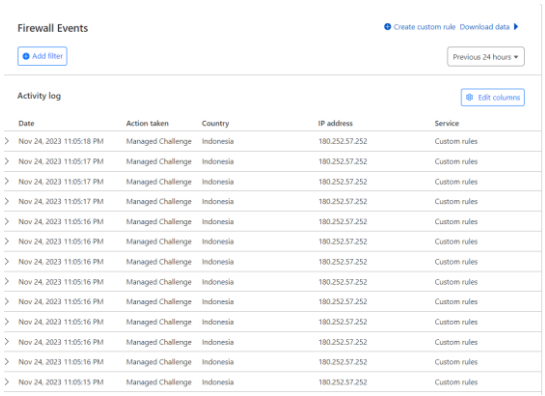

Gambar 8 Seting Security Level

Ketiga membuat *SSL/TLS encryption* menjadi *flexible*, menunjukkan bahwa lalu lintas antara pengguna dan Cloudflare dienkripsi dengan *SSL/TLS* seperti pada Gambar 9.




Gambar 9 Setting SSL/TLS

Setelah ketiga pengaturan dijalankan diulangi serangan yang sama menggunakan *goldeneye*, menunjukkan bahwa dengan penambahan WAF serangan DDoS pada website dapat dicegah seperti pada Gambar 10.



| Date | Action taken | Country | IP address | Service |
|---|---|---|---|---|
| Nov 24, 2023 11:05:18 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:17 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:17 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:17 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:16 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |
| Nov 24, 2023 11:05:15 PM | Managed Challenge | Indonesia | 180.252.57.252 | Custom rules |

Gambar 10 Log DDoS setelah dijalankan

## SIMPULAN

Dalam kesimpulan, rancangan sistem keamanan jaringan yang telah melibatkan metode pengujian penetrasi membuktikan keefektifannya dalam meningkatkan ketangguhan dan kesiapsiagaan terhadap serangan DDoS. Melalui identifikasi dan penanganan titik lemah serta kerentanan yang mungkin dieksploitasi oleh serangan, sistem telah diperkuat dengan implementasi filter lalu lintas cerdas, konfigurasi firewall yang ketat, dan pembaruan sistem teratur. Pengujian penetrasi tidak hanya memperbaiki kelemahan yang ada, tetapi juga menyediakan wawasan kritis untuk menyusun rencana tanggap darurat yang efektif. Dengan demikian, rancangan sistem keamanan jaringan yang telah mengintegrasikan pengujian penetrasi memberikan landasan yang kokoh dalam melindungi ketersediaan layanan dan meminimalkan dampak serangan DDoS.

Untuk meningkatkan lagi ketangguhan rancangan sistem keamanan jaringan terhadap serangan DDoS, beberapa saran dapat diterapkan. Pertama, perlu memperkuat filter lalu lintas dengan mempertimbangkan penggunaan layanan proteksi DDoS dari penyedia seperti *Cloudflare*, yang dapat memberikan lapisan perlindungan tambahan. Selanjutnya, disarankan untuk secara teratur melakukan pembaruan sistem dan perangkat lunak untuk mengatasi potensi kerentanan. Penting juga untuk memperhatikan konfigurasi firewall dan memastikan bahwa aturan diterapkan secara efektif. Selain itu, untuk meminimalkan dampak serangan, penyusunan rencana tanggap darurat harus diperbarui dan diuji secara berkala.

## DAFTAR PUSTAKA

[1] I. K. D. G. Supartha and I. P. A. S. Wijaya, “Analisis Kinerja Sistem Penilaian Lomba Tari Bali Berbasis Mobile,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 5, no. 1, pp. 7–12, Jan. 2023, doi: 10.47233/jteksis.v5i1.721.

[2] S. E. Prasetyo and N. Hassanah, “Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode ISSAF,” *Jurnal Ilmiah Informatika (JIF)*, 2021.

[3] S. Defit and U. YPTK Padang, “Prediksi Tingkat Kebutuhan Bandwidth Jangka Panjang Menggunakan Metode Algortima Backpropagation,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 4, no. 1, 2022, doi: 10.47233/jteksis.v4i1.310.

[4] A. Faidlatul Habibah, F. Shabira, and I. Irwansyah, “Pengaplikasian Teori Penetrasi Sosial pada Aplikasi Online Dating,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 3, no. 1, pp. 44–53, Jan. 2021, doi: 10.47233/jteksis.v3i1.183.

[5] G. Wijaya and Leo, “Merancang Dan Mengimplementasikan Keamanan Jaringan Dan Server Di PT Karya Mura Niaga,” 2022, [Online]. Available: http://journal.uib.ac.id/index.php/nacospro

[6] T. Purnama *et al.*, “IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) SNORT SEBAGAI SISTEM KEAMANAN MENGGUNAKAN WHATSAPP DAN TELEGRAM SEBAGAI MEDIA NOTIFIKASI,” vol. 14, no. 2, pp. 358–369, 2023, [Online]. Available: http://ejurnal.provisi.ac.id/index.php/JTIKP□page358

[7] B. Arifwidodo, Y. Syuhada, and S. Ikhwan, “Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS Analysis of Mikrotik Performance Against Brute Force and DDoS Attacks,” *jurnal TCHNO.COM*, vol. 20, no. 3, pp. 392–399, 2021.

[8] M. Risiko, S. Siber, T. Tan, and B. Soewito, “MANAJEMEN RISIKO SERANGAN SIBER MENGGUNAKAN FRAMEWORK NIST CYBERSECURITY DI UNIVERSITAS ZXC,” *Journal of Information System, Applied, Management, Accounting and Research*, vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

[9] S. E. Prasetyo, N. Hasanah, and G. Wijaya, “Pengujian Keamanan Learning Management System TutorLMS Terhadap Kerentanan Insecure Design dan Broken Access Control,” *Telcomatics*, vol. 7, no. 2, Dec. 2022, doi: 10.37253/telcomatics.v7i2.7357.

[10] F. Fadhilah, E. Wahyudi, and E. F. Cahyadi, “ANALISIS MODSECURITY DAN MODANTILORIS PADA SERANGAN DDOS SLOWHTTP TERHADAP WEB SERVER,” *Jurnal Listrik Telekomunikasi Elektronika*, vol. 20, no. 2, pp. 2549–8762, 2023, [Online]. Available: http://192.168.121.221/

[11] Suliman, A. Achmad, and adnan, “IMPLEMENTASI HONEYPOT DAN PORT KNOCKING DALAM MENDETEKSI SERANGAN DDoS ATTACK PADA SERVER JARINGAN,” *SEMANTIK : TEKNIK INFORMASI*, vol. 7, no. 1, pp. 1–5, 2021, doi: 10.5281/zenodo.5034918.

[12] Kusuma Artha Hendita Gregorius, “Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19,” *Journal of Informatics and Advanced Computing (JIAC)*, 2022.

[13] M. Adam, E. I. Alwi, and I. As’ad, “ANALISIS FORENSIK TERHADAP SERANGAN DDOS PING OF DEATH PADA SERVER,” *CYBER SECURITY DAN FORENSIK DIGITAL (CSFD)*, vol. 5, no. 1, pp. 23–31, 2022.

[14] E. Nofarita, “IMPLEMENTASI APLIKASI SOFTWARE NATURAL NETWORK MENDETEKSI TINGKATAN SERANGAN DDOS PADA JARINGAN KOMPUTER,” vol. 14, no. 2, pp. 268–277, 2021, [Online]. Available: http://journal.stekom.ac.id/index.php/elkom□page268

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

[15] M. N. Faiz, O. Somantri, and A. W. Muhammad, "Rekayasa Fitur Berbasis Machine Learning untuk Mendeteksi Serangan DDoS," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi* |, vol. 11, no. 3, 2022.

[16] J. A. Ginting and I. G. G. Ngurah Suryantara, "PENGUJIAN KERENTANAN SISTEM DENGAN MENGGUNAKAN METODE PENETRATION TESTING DI UNIVERSITAS XYZ," *Infotech: Journal of Technology Information*, vol. 7, no. 1, pp. 41–46, Jun. 2021, doi: 10.37365/jti.v7i1.105.

[17] A. Fauzi *et al.*, "Penerapan Random Forest dan Adaboost untuk Klasifikasi Serangan DDoS," *Journal on Education*, vol. 05, no. 03, pp. 7925–7937, 2023.

[18] H. Alfidzar and B. Parga Zen, "Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Guna Mendeteksi Serangan DOS Pada Server," *Journal of Informatics, Information System, Software Engineering and Applications*, vol. 4, no. 2, pp. 32–045, 2022, doi: 10.20895/INISTA.V4I2.

[19] F. Fachri, "OPTIMASI KEAMANAN WEB SERVER TERHADAP SERANGAN BRUTE-FORCE MENGGUNAKAN PENETRATION TESTING," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 10, no. 1, pp. 51–58, 2023, doi: 10.25126/jtiik.2023105872.

[20] H. Setiawan, M. Agus Munandar, L. W. Astuti, and P. Korespondensi, "PENGGUNAAN METODE SIGNATURED BASED DALAM PENGENALAN POLA SERANGAN DI JARINGAN KOMPUTER," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 8, no. 3, pp. 517–524, 2021, doi: 10.25126/jtiik.202184200.

[21] M. Hafiz Hawarizmi, M. T. Kurniawan, and M. Fathinuddin, "Sistem Deteksi Serangan Ddos pada Software Defined Network Menggunakan Metode Entropy," *SMART COMP :JURNALNYA ORANG PINTAR KOMPUTER*, 2022.

[22] S. Adhar and U. Saprudin, "Implementasi Cloudflare Zero Trust Dalam Mendeteksi Aktivitas Cryptojcking Pada Jaringan Komputer," *Jurnal Teknologi Komputer dan Sistem Informasi (JTKSI)*, 2023.