

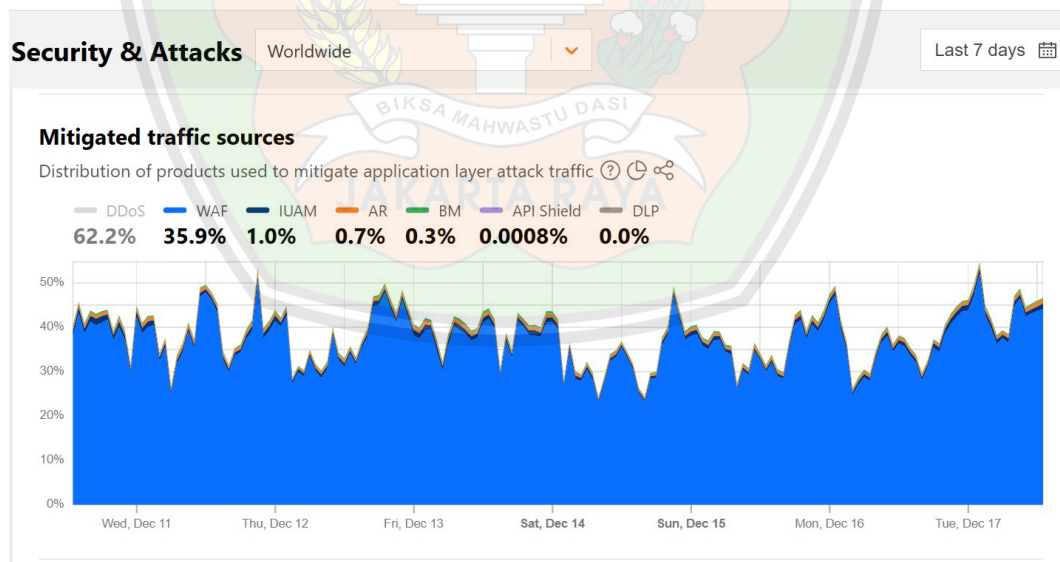
BAB I

PENDAHULUAN

1.1 Latar Belakang

Serangan *Distributed Denial of Service* (DDoS) adalah serangan yang bertujuan untuk mencegah pengguna sahnya mengakses layanan online, seperti situs web, dengan membanjiri server atau jaringan dengan banyak trafik internet. Serangan ini dilakukan oleh sejumlah komputer yang telah dikompromikan dan tergabung dalam jaringan botnet secara bersamaan. Serangan *Distributed Denial of Service* (DDoS) dapat menyebabkan sebuah website menjadi tidak dapat diakses, sehingga pengguna tidak dapat menggunakan atau mengakses layanan yang ditawarkan olehnya. Serangan *Distributed Denial of Service* (DDoS) juga dapat merusak reputasi perusahaan karena website tersebut sering mengalami downtime.

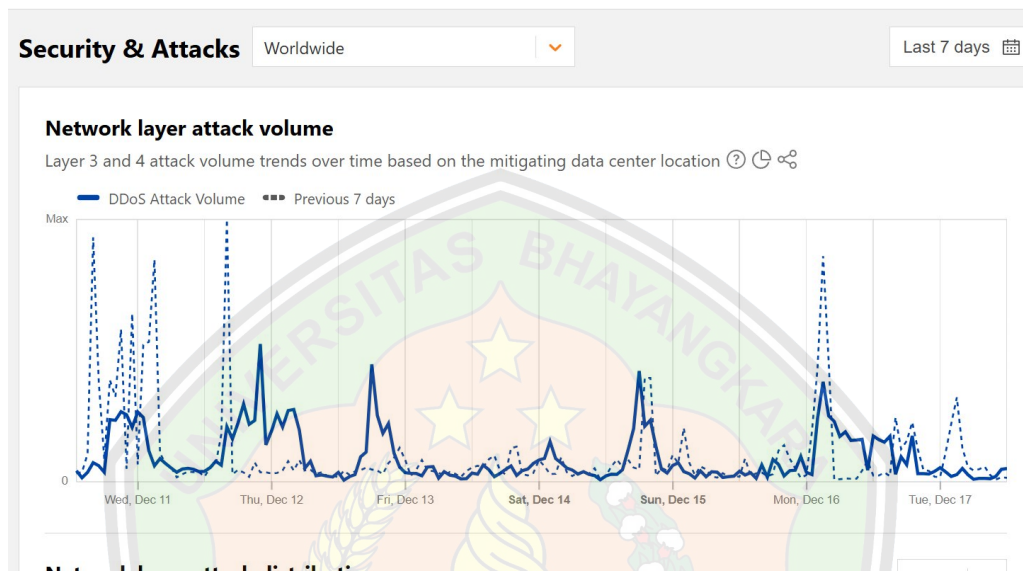
Pelanggan mungkin merasa perusahaan tidak aman atau tidak dapat diandalkan. Lonjakan lalu lintas yang berlebihan dapat menyebabkan downtime pada website, yang dapat menyebabkan pengalaman pengguna yang buruk, konversi, dan kepuasan pelanggan. Namun, serangan tidak selalu menyebabkan downtime.



Gambar 1.1 statistik mitigasi traffic serangan

Sumber: radar.cloudflare.com [1]

Pada gambar 1.1 di perlihatkan Data mitigasi trafik serangan *Distributed Denial of Service* (DDoS) menunjukkan bahwa, dari berbagai jenis serangan cyber di seluruh dunia, serangan Distributed Denial of Service (DDoS) adalah yang paling dominan dan menghasilkan trafik tertinggi dan pesan terbesar. Ini menunjukkan bahwa 62,2 persen dari traffic yang dimitigasi adalah upaya untuk mengatasi serangan *Distributed Denial of Service* (DDoS).



Gambar 1.2 Network layer attack volume

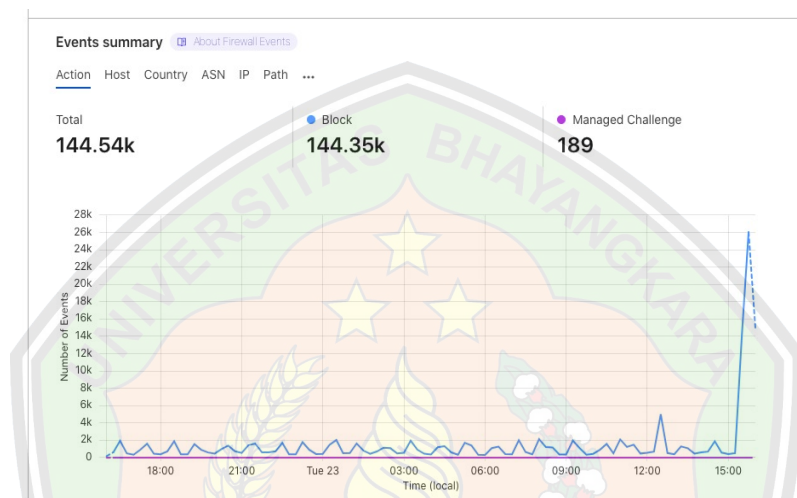
Sumber: rada.cloudflare.com[1]

Pada Gambar 1.2 di perlihatkan sebuah grafik yang menampilkan volume serangan pada lapisan jaringan (*Network layer*), khususnya pada Lapisan 3 dan 4 dalam model OSI, yang kemungkinan besar terkait dengan serangan *Distributed Denial of Service* (DDoS).

Proses yang dilakukan untuk menjaga situs web dari berbagai ancaman dan serangan yang dapat merusak, memungkinkan akses secara tidak sah, atau mengganggu fungsinya. Tujuan utama keamanan website adalah untuk melindungi data yang disimpan dan dikirim melalui situs web dan memastikan bahwa situs tersebut tetap beroperasi dengan baik untuk penggunaanya.

DISWAY adalah akronim dari nama Dahlan Iskan dan kode penulisan yang dia gunakan sejak dia menjadi jurnalis. Kehadiran DISWAY berasal dari keinginan Dahlan Iskan untuk terus berbagi ide, gagasan, dan pemikirannya melalui tulisan. Blog pribadinya, disway.id, yang didirikan pada 2018, adalah tempat upaya tersebut diwujudkan. Berlokasi di Jalan Palmera Barat No.353,

kompleks kampus Widuri, Blok A1-3, Grogol Utara, Kecamatan Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12210, DISWAY.ID adalah situs web resminya. Salah satu masalah dengan Disway.id adalah ada pihak yang tidak bertanggung jawab yang melakukan serangan *Distributed Denial of Service* (DDoS) terhadap situs berita resminya. Jika ini terus dibiarkan, server disway.id akan down dan pengguna yang ingin membaca berita tidak akan bisa mengaksesnya. Untuk mengatasi masalah ini, Disway.id menggunakan cloudfare.



Gambar 1.3 Laporan penyerangan DDOS Disway.id

Sumber: cloudflare.com(2024) [2]

Pada gambar 1.3 Data menunjukkan serangan *Distributed Denial of Service* (DDoS) yang dilakukan oleh individu yang tidak bertanggung jawab. Jumlah total serangan *Distributed Denial of Service* (DDoS) mencapai 144.540.00, dengan 144.350.00 serangan yang berhasil di block, menunjukkan bahwa jumlah serangan *Distributed Denial of Service* (DDoS) ini sangat besar. Antara pukul 18:00 dan 15:00, jumlah peristiwa relatif rendah dan stabil di bawah 2000 peristiwa, menunjukkan bahwa aktivitas ancaman masih terkendali dan rendah. Namun, pada pukul 15:00, lonjakan trafik firewall tiba-tiba meningkat menjadi 26.000 hingga 28.000 peristiwa dalam waktu singkat. Lonjakan ini mengakibatkan serangan besar atau upaya akses ilegal yang tiba-tiba meningkat, seperti serangan *Distributed Denial of Service* (DDoS).

Dengan menggunakan metode pengiriman konten jaringan yang memiliki fitur perlindungan *Distributed Denial of Service* (DDoS), pengguna dapat melindungi website mereka dari serangan *Distributed Denial of Service* (DDoS).



Gambar 1.4 Tampilan Website Disway.id

Sumber: disway.id (2024) [3]

Pada gambar 1.4 di perlihatkan tampilan website disway.id yang selalu terkena serangan *Distributed Denial of Service* (DDoS) pada tiap bulan nya oleh oknum yang tidak bertanggung jawab. Oleh karena itu penulis memilih judul “**Analisis keamanan website menggunakan content delivery network terhadap serangan ddos pada kantor berita online disway.id**”.

1.2 Identifikasi Masalah

Berdasarkan latar belakang di atas, maka penulis menyimpulkan identifikasi masalah penelitian, sebagai berikut :

1. Adanya serangan *Distributed Denial of Service* (DDoS) yang mengganggu web server disway.id yang datang setiap saat tanpa bisa di prediksi.
2. serangan *Distributed Denial of Service* (DDoS) terhadap web server Disway.id menyebabkan website menjadi lambat dan sulit diakses oleh pengguna.

1.3 Rumusan Masalah

Berdasarkan masalah yang ada, penulis merumuskan masalah yang ada di dalam penelitian yaitu “Bagaimana menganalisis kinerja Keamanan Website dari serangan *Distributed Denial of Service* (DDoS) Menggunakan metode *METODE CONTENT DELIVERY NETWORK (cloudflare)*” Yang memiliki Fitur *Distributed Denial of Service* (DDoS) Protection.

1.4 Batasan Masalah

Berdasarkan latar belakang diatas, maka penulis menyimpulkan batasan masalah sebagai berikut :

1. Penelitian berfokus pada pencegahan serangan siber *Distributed Denial of Service* (DDoS) menggunakan platform Cloudflare pada website Disway.id.
2. Analisis ditujukan hanya pada serangan *Distributed Denial of Service* (DDoS), karena jenis serangan ini yang sering mengganggu server website..
3. Tools yang di gunakan adalah Grafana k6 untuk melakukan pengujian.
4. Penelitian hanya mencakup pengujian sistem keamanan terhadap jumlah serangan, sumber serangan, serta traffic serangan *Distributed Denial of Service* (DDoS) yang berdampak pada server Disway.id.

1.5 Tujuan Penelitian

Berikut tujuan dilakukannya penelitian ini :

1. Menerapkan fitur keamanan Cloudflare CDN dengan perlindungan DDoS protection untuk menganalisis efektivitasnya dalam mencegah serangan *Distributed Denial of Service* (DDoS) pada Disway.id.
2. Mengidentifikasi jumlah, sumber, dan pola traffic serangan *Distributed Denial of* (DDoS) terhadap web server Disway.id secara berkala.
3. Memberikan rekomendasi penguatan kapasitas server serta pengaturan ulang konfigurasi keamanan firewall untuk meningkatkan perlindungan terhadap serangan.

1.6 Manfaat Penelitian

Berikut manfaat dilakukannya penelitian ini :

1. Pengujian memastikan bahwa sistem mitigasi *Distributed Denial of Service* (DDoS) Cloudflare berkerja dengan baik dalam mendeteksi serangan *Distributed Denial of Service* (DDoS) dan menghentikan serangan nya.
2. menjadikan cloudflare salah satu rekomendasi untuk perlindungan website.
3. Pengujian *Distributed Denial of Service* (DDoS) membantu menemukan kelemahan pada infrastuktur Disway.id
4. Membuktikan bahwa cloudflare dapat melindungi website dari serangan DDOS atau yang lain.

1.7 Sistematika Penulisan

Untuk mempermudah dan memperjelas dalam pembahasan masalah pada penulisan skripsi ini, penulis menyusun skripsi ini dengan sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada BAB I ini menjelaskan latar belakang, identifikasi masalah, Rumusan Masalah, Batasan Masalah, Tujuan dan Manfaat Penelitian, dan terakhir Sistematika Penelitian.

BAB II TINJAUAN PUSTAKA

Pada BAB II ini memberikan penjelasan tentang landasan teori yang mendukung dan terkait dengan penelitian yang dilakukan. Penjelasan ini diambil *from* buku-buku, jurnal, serta sumber lain untuk penyelesaian tugas skripsi ini.

BAB III METODOLOGI PENELITIAN

Pada BAB III ini memberikan metode yang digunakan yaitu METODE *Content Delivery Network (cloudfare)* Dengan pengumpulan data berupa observasi, wawancara, studi Pustaka. Dengan menggunakan metode ini di harapkan menghasilkan hasil yang maksimal.

BAB IV HASIL DAN PEMBAHASAN

Pada BAB IV ini membahas mengenai hasil proses perancangan atau hasil dari penelitian yang dilakukan dan deskripsinya, serta pembahasan mengenai hasil penelitian.

BAB V PENUTUP

Pada BAB V ini membahas mengenai kesimpulan umum hasil penelitian serta saran yang ditunjukkan kepada pihak yang mendapat manfaat dari hasil penelitian.

