JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

Simulasi Analisis Serangan DDOS Pada Beberapa Alamat Website Untuk Evaluasi Ketahanan Sistem

Elvi Ningsih Telaumbanua[1], Darwis Setiawan Waruwu[2], Kevin Rewardi Harefa[3], Christine Jenny Puspita Zega[4], Ivataro Laoli[5], Ofelius Laia[6*]

[1,2,3,4,5,6] Fakultas Sains dan Teknologi, Program Studi Teknologi Informasi, Universitas Nias, Gunungsitoli, Indonesia
E-mail: [1]elviningsihtel24@gmail.com, [2]darwissetiwanwaruwu@gmail.com, [3]kevinharefa2020@gmail.com, [4]jennyzega@gmail.com, [5]ivatarolaoly2@gmail.com, [6]ofeliuslaia@gmail.com
(* Email Corresponding Author: ofeliuslaia@gmail.com)
Received: 23 June 2025 | Revision: 28 June 2025 | Accepted: 30 June 2025

Abstrak

Dalam berbagai bidang, lebih banyak orang menggunakan situs web karena kemajuan teknologi informasi. Namun, hal ini juga meningkatkan kemungkinan serangan siber, terutama serangan Distributed Denial of Service (DDoS), yang meminliki kemampuan untuk melumpuhkan layanan dengan membanjiri sistem target. Tujuan penelitian ini untuk mensimulasikan dan menganalisis serangan DDoS pada berbagai alamat situs web untuk mengevaluasi ketahanan sistem. Simulasi serangan dalam lingkungan terkendali dan analisis performa sistem digunakan sebagai teknik. Hasil ini menunjukkan bahwa ketahanan situs bervariasi tergantung konfigurasi dan sistem keamanannya. Studi ini menunjukkan bahwa strategi mitigasi sangat penting untuk memperkuat pertahanan terhadap serangan DDoS.

Kata kunci: DDoS, keamanan siber, situs web, simulasi, ketahanan sistem.

Abstract

In various fields, more people are using websites due to the advancement of information technology. However, it also increases the likelihood of cyberattacks, especially Distributed Denial of Service (DDoS) attacks, which have the ability to disable services by flooding the target system. The purpose of this study was to simulate and analyze DDoS attacks on various website addresses to evaluate the resilience of the system. Simulating attacks in a controlled environment and analyzing system performance are used as techniques. These results show that the resilience of a site varies depending on its configuration and security system. This study shows that mitigation strategies are essential to strengthen defenses against DDoS attacks.

Keywords: DDoS, cybersecurity, websites, simulations, system resilience.

1. PENDAHULUAN

Ancaman serangan siber telah menjadi isu global yang semakin mendesak untuk diantisipasi seiring dengan pesatnya perkembangan teknologi informasi. Transformasi digital di berbagai sektor, mulai dari pemerintahan, bisnis, pendidikan, hingga layanan kesehatan, menjadikan sistem informasi dan jaringan komputer sebagai tulang punggung operasional. Di balik manfaat yang dihadirkan, penggunaan teknologi secara masif ini membuka peluang bagi pihak-pihak tidak bertanggung jawab untuk melakukan eksploitasi melalui berbagai bentuk serangan siber. Risiko terhadap keamanan data, privasi, dan keberlanjutan layanan menjadi semakin tinggi, sehingga serangan siber tidak lagi sekadar ancaman teknis, tetapi juga berdampak langsung pada aspek sosial, ekonomi, dan reputasi organisasi. Kondisi ini mendorong setiap individu, perusahaan, dan lembaga pemerintah untuk membangun sistem pertahanan yang tangguh agar mampu mendeteksi, mencegah, dan merespons ancaman dengan cepat dan tepat.

Salah satu serangan yang paling sering menjadi sorotan dalam ranah keamanan siber adalah Distributed Denial of Service (DDoS). DDoS merupakan jenis serangan yang ditujukan untuk melumpuhkan sistem atau mengganggu akses terhadap layanan dengan membanjiri target menggunakan lalu lintas data dalam jumlah besar dari berbagai sumber secara bersamaan. Serangan ini dapat menyebabkan sistem tidak mampu melayani permintaan yang sah, sehingga berdampak pada terhentinya layanan, kerugian finansial, serta menurunnya tingkat kepercayaan pengguna[1]. Situs web sebagai gerbang utama berbagai layanan digital menjadi target utama serangan ini karena sifatnya yang terbuka untuk umum dan kompleksitas sistem yang mendukungnya. Ketika sebuah situs web gagal memberikan layanan secara optimal akibat serangan, dampaknya tidak hanya dirasakan oleh pengelola sistem, tetapi juga oleh seluruh pengguna yang bergantung pada layanan tersebut.

Seiring berjalannya waktu, metode serangan DDoS terus berkembang dan semakin sulit untuk dideteksi dengan teknik konvensional. Salah satu bentuk serangan DDoS yang lebih canggih dan berbahaya adalah slow HTTP attack.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

Berbeda dengan serangan DDoS tradisional yang mengandalkan volume lalu lintas data yang besar, slow HTTP attack bekerja dengan mengirim permintaan HTTP secara perlahan dan terus-menerus sehingga server target tetap mempertahankan koneksi dan akhirnya kehabisan sumber daya. Lalu lintas yang dihasilkan serangan ini menyerupai lalu lintas normal, sehingga sulit untuk dibedakan oleh sistem keamanan standar. Serangan ini mengeksploitasi kelemahan pada manajemen koneksi server dan dapat menyebabkan server menjadi tidak responsif meskipun tidak terjadi lonjakan lalu lintas yang mencolok. Ancaman ini semakin relevan dalam infrastruktur modern seperti cloud computing dan shared hosting, di mana satu server digunakan untuk melayani banyak layanan sekaligus. Sebuah serangan pada satu layanan dapat berdampak pada layanan lainnya yang berbagi sumber daya yang sama, sehingga berpotensi melumpuhkan sistem secara lebih luas.

Berbagai penelitian telah dilakukan untuk mengkaji dampak dan mekanisme serangan slow HTTP DoS. [2] dalam penelitiannya yang berjudul Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest, menemukan bahwa serangan ini secara signifikan dapat menurunkan performa server, meningkatkan jumlah error, dan menimbulkan potensi kelebihan beban yang membahayakan keberlangsungan layanan. Penelitian tersebut menekankan perlunya peningkatan kesadaran dan edukasi tentang pentingnya perlindungan terhadap serangan siber. Sementara itu, [3], melalui penelitiannya Penggunaan Slowhttptest untuk Menguji Kerentanan Jaringan terhadap Flooding Attack, menunjukkan bahwa slowhttptest merupakan alat yang efektif untuk mensimulasikan serangan dan mendeteksi kerentanan sistem terhadap serangan flooding, termasuk slow HTTP DoS. Penelitian ini menyoroti adanya penurunan kecepatan akses dan menurunnya performa server secara signifikan saat serangan berlangsung. Selain itu, penelitian yang dilakukan oleh [4] dalam Dampak Denial of Service pada Perusahaan Perbankan di Indonesia mengungkapkan bahwa serangan DoS dan turunannya dapat mengganggu operasional sektor perbankan, merugikan nasabah, dan menurunkan reputasi lembaga keuangan. Oleh karena itu, lembaga keuangan disarankan untuk menerapkan langkah-langkah pengamanan tingkat lanjut dan melakukan pengujian berkala terhadap sistem mereka.

Berdasarkan studi-studi terdahulu tersebut, dapat disimpulkan bahwa serangan DDoS, khususnya jenis slow HTTP, memberikan dampak nyata terhadap performa dan keberlangsungan sistem yang menjadi target. Meskipun berbagai upaya mitigasi telah dikembangkan, para penyerang terus mencari celah baru dengan memanfaatkan teknik yang semakin halus dan sulit dideteksi. Oleh karena itu, penting untuk melakukan kajian dan simulasi berkelanjutan guna memahami karakteristik serangan serta menguji efektivitas strategi mitigasi yang ada.

Penelitian ini bertujuan untuk memberikan kontribusi dalam bidang keamanan siber dengan melakukan simulasi dan analisis terhadap serangan slow HTTP DoS menggunakan alat slowhttptest. Fokus utama penelitian ini adalah mengevaluasi ketahanan sistem terhadap serangan, mengidentifikasi pola serangan, serta merumuskan strategi mitigasi yang relevan dengan desain dan karakteristik sistem yang diuji. Dengan demikian, hasil penelitian diharapkan dapat memberikan gambaran praktis mengenai kelemahan sistem serta menjadi dasar perencanaan pengembangan strategi keamanan siber yang lebih adaptif, efektif, dan mampu mengantisipasi dinamika ancaman siber di masa depan. Penelitian ini juga diharapkan dapat memperkaya literatur terkait mekanisme serangan DDoS dan slow HTTP attack, serta memberikan rekomendasi yang aplikatif bagi praktisi keamanan sistem dalam merancang dan mengimplementasikan sistem perlindungan yang lebih tangguh.

2. METODE

2.1. Tahap Penelitian

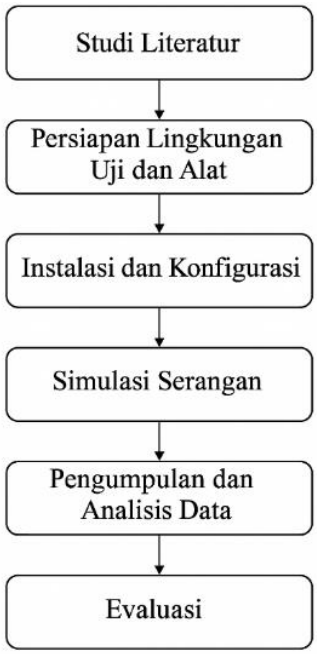
Metode yang digunakan dalam penelitian ini adalah metode pendekatan eksperimental. Menurut Gay (1981), metode eksperimental adalah metode penelitian untuk menguji hipotesis menyangkut hubungan kausal (sebab akibat) secara benar. Tujuan metode ini adalah untuk mengetahui pengaruh dari suatu tindakan terhadap kelompok tertentu. Kemudian, hasilnya dibandingkan dengan kelompok lain yang mendapatkan tindakan berbeda. Fokus utamanya adalah pada pengaruh yang disebabkan oleh serangan DDoS.

Penelitian ini di lakukan melalui beberapa tahapan sistematis, yaitu :

1. **Studi Literatur.** Mengumpulkan dan mempelajari referensi tentang flooding attack, serangan DoS/DDoS, dan penggunaan alat slowhttptest untuk pengujian keamanan jaringan.
2. **Persiapan Lingkungan Uji dan Alat.** Mempersiapkan virtual box dengan sistem operasi Ubuntu/Kali Linux serta target 10 situs we publik.
   Website yang diuji coba adalah random, dengan tujuan mengetahui kerentanan dari website tersebut. Namun, keseluruhan website yang diuji coba adalah website blog pribadi.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

3. **Instalasi dan Konfigurasi.** Menjalankan perintah *sudo apt update* dan *sudo apt install slowhttptest* untuk menginstal alat.
4. **Simulasi Serangan.** Serangan dilakukan menggunakan parameter slowhttptest -c 10000 -H -o slowhttptest -i 10 -r 50 -t Get *alamat situs* -x 20 -p 3. Ini dilakukan untuk menguji ketahanan situs terhadap slow HTTP attack.
5. **Pengumpulan dan Analisis Data.** Hasil pengujian direkam dalam bentuk **output HTML** dan **pengamatan langsung** terhadap status situs: apakah tetap online, lambat, atau tidak merespon.
6. **Evaluasi.** Data hasil serangan dibandingkan berdasarkan **jumlah koneksi terbuka**, **waktu respon**, dan **status situs**. Evaluasi bertujuan untuk menentukan kerentanan masing-masing situs.



Gambar 1 Tahap Penelitian

Tabel 1. Parameter Slowhttptest yang Digunakan

Parameter	**Arti**	**Penjelasan Lengkap**
-c 10000	Connections	Membuka 10000 koneksi server target (total koneksi uji)
-H	HTTP slow headers	Menggunakan metode serangan slow headers, yaitu mengirim header HTTP dengan sangat lambat agar server tetap membuka koneksi
-o slowhttptest	Output file prefix	Nama file output (uji coba). Akan menghasilkan file HTML bernama slowhttptest.html di folder kerja
-i 10	Interval	Jeda antar data yang dikirimkan selama koneksi aktif, yaitu 10 detik. Semakin tinggi, semakin lambat
-r 50	Rate	Membuka 50 koneksi baru perdetik hingga mencapai jumlah -c
-t GET	Test type	Tipe serangan: Slow HTTP GET request, yakni mengirim permintaan GET secara perlahan agar server tetap sibuk

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

-u alamat website	URL	Target situs yang akan diuji
-x 20	Max per IP	Maksimal 20 koneksi simultan dari satu ip. Ini digunakan untuk membatasi koneksi per alamat IP
-p 3	Pipelining	Mengatur agar dalam satu koneksi bisa di kirimkan 3 permintaan secara berurutan, tanpa menunggu respons dari yang sebelumnya

2.2. Spesifikasi Alat dan Bahan

Alat dan bahan yang digunakan dalam penelitian ini meliputi perangkat keras dan perangkat lunak dengan spesifikasi sebagai berikut:

Tabel 2. Spesifikasi Komputer

Komponen	Spesifikasi
Prosesor (CPU)	Intel(R)Celeron(R) N4120 CPU @ 1.10GHz 1.10 GHz
Memori (RAM)	4.00 GB
Penyimpanan	256 GB SSD
Sistem Operasi	Kali Linux 2023 4 (64-bit)
Koneksi Jaringan	Wi-Fi 802.11ac (terhubung ke jaringan lokal)

Tabel 3. Perangkat Yang Digunakan

Perangkat Lunak	Versi/Jenis	Fungsi
SlowHTTPTest	v1.8	Alat untuk mensimulasikan serangan Slow HTTP DoS
Wireshark	v4.0.0	Alat untuk memantau lalu lintas jaringan selama serangan
Peramban Web (Browser)	Google Chrome, Mozilla Firefox	Untuk mengakses dan memantau situs web target
Terminal/Konsole	Bawaan ubuntu server	Untuk menjalankan perintah SlowHTTPTest

2.3. Analisis Data

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

Data yang dikumpulkan selama eksperimen dianalisis untuk mengevaluasi dampak serangan Slow HTTP DoS terhadap ketersediaan dan performa situs web target. Metode analisis data mencakup:

a. Pengukuran Waktu Respons: Pengamatan visual dan ping test sederhana dilakukan untuk memantau waktu respons situs web. Peningkatan waktu respons yang signifikan mengindikasikan dampak serangan.
b. Identifikasi Status Aksesibilitas: Perubahan status akses situs web (dari dapat diakses menjadi tidak dapat diakses, munculnya halaman error, atau loading yang sangat lama) dicatat sebagai indikator utama keberhasilan serangan.
c. Analisis Grafik SlowHTTPTest: Hasil log yang dihasilkan oleh SlowHTTPTest (dalam format HTML, sebagaimana ditunjukkan pada bagian Hasil dan Pembahasan) dianalisis.
d. Analisis Lalu Lintas Jaringan (Wireshark): Data tangkapan Wireshark dianalisis untuk memverifikasi pola serangan (misalnya, paket HTTP yang lambat dan tidak lengkap) serta mengamati beban koneksi pada sisi penyerang dan dampaknya pada target.

2.4. Pertimbangan Etika dan Izin Penggunaan Situs Target

Penelitian ini dilakukan dengan menjunjung tinggi etika penelitian dan tanggung jawab. Situs web yang menjadi target pengujian sebagian besar adalah situs blog pribadi. Terkait situs web yang aktif, pengujian dilakukan dengan batas koneksi dan durasi yang tidak menyebabkan downtime berkepanjangan bagi pengguna sah. Tujuan utama adalah untuk mengamati respons server dan bukan untuk menyebabkan kerusakan yang disengaja.

2.5. Metode Penyelesaian Masalah

Penelitian ini bertujuan untuk mengidentifikasi kerentanan layanan web terhadap serangan Slow HTTP, khususnya dari sisi kemampuan sistem dalam menangani koneksi lambat yang terus-menerus. Untuk menyelesaikan permasalahan ini, digunakan pendekatan eksperimen dengan simulasi serangan secara terkontrol menggunakan alat bantu SlowHTTPTest. Langkah-langkah yang diambil bertujuan untuk mengidentifikasi sejauh mana sebuah sistem dapat bertahan dari ancaman serangan DDoS yang disimulasikan dalam lingkungan yang terkendali. Langkah pertama yang dilakukan adalah studi literatur, yaitu mengumpulkan referensi dari berbagai sumber terpercaya seperti jurnal ilmiah, artikel keamanan jaringan, dan dokumentasi teknis mengenai jenis-jenis serangan DDoS dan cara mitigasinya. Tujuannya adalah untuk memahami karakteristik serangan dan metode pengujian yang relevan.Setelah skenario simulasi siap, dilakukan implementasi serangan DDoS terhadap website yang telah ditentukan. Serangan dijalankan dengan pengaturan tertentu seperti jumlah koneksi, durasi serangan, dan jenis paket data yang dikirimkan.Selama proses simulasi berlangsung, dilakukan monitoring sistem secara real-time untuk mencatat parameter penting seperti respon server, penggunaan bandwidth, performa CPU, serta waktu akses halaman. Monitoring dilakukan menggunakan alat bantu seperti Wireshark dan Netstat. Data yang terkumpul kemudian dianalisis secara menyeluruh untuk mengetahui sejauh mana masing-masing sistem mampu menahan tekanan serangan. Hasil analisis digunakan untuk mengevaluasi kekuatan dan kelemahan sistem, serta memberikan gambaran tentang dampak nyata dari serangan DDoS terhadap ketersediaan layanan.

3. HASIL DAN PEMBAHASAN

3.1. Hasil

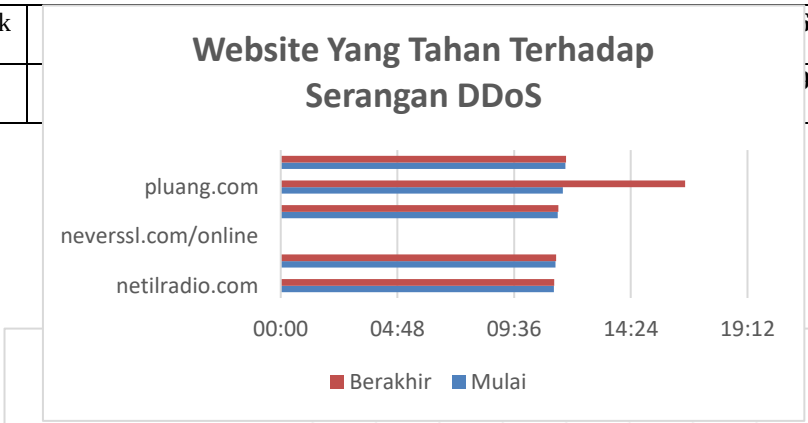
Dari simulasi yang dilakukan terhadap 10 website, berikut adalah hasilnya :

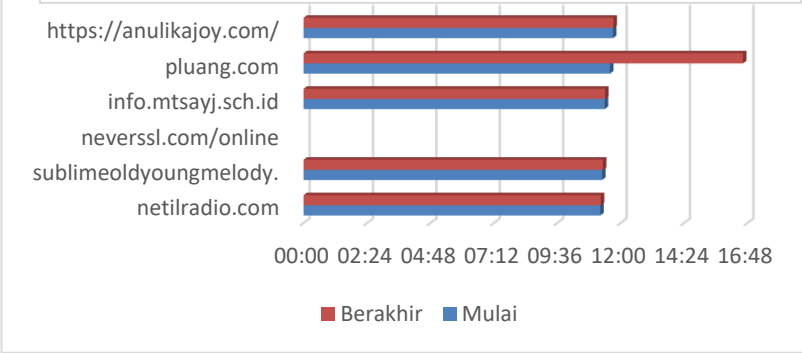
Tabel 4. Website Yang Tahan Terhadap Serangan DDoS

Website	Mulai	Berakhir	Initializing	Pending	Connection	Error	Closed	Service Avaible
Bykwest.com	**10:27**	**10:31**	**0**	**61**	**354**	**0**	**8503**	**Yes**
Albinotonnina.com	**10:32**	**10:37**	**0**	**40**	**8750**	**0**	**11**	**Yes**
christyannejones.com	**10:38**	**10:43**	**0**	**45**	**1168**	**0**	**8079**	**Yes**

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

byexperience.co.uk			**Yes**
example.com			**No**





Tabel 5. Website Yang Rentan Terhadap Serangan DDoS

Website	Mulai	Berakhir	Initializing	Pending	Connection	Error	Closed	Service Avaible
netilradio.com	**11:14**	**11:15**	**0**	**327**	**1010**	**0**	**820**	**NO**
sublimeoldyoungmelody.	**11:18**	**11:20**	**0**	**2078**	**1373**	**0**	**3603**	**NO**
info.mtsayj.sch.id	**11:24**	**11:25**	**0**	**85**	**0**	**0**	**1511**	**NO**
pluang.com	**11:36**	**16:38**	**0**	**1566**	**189**	**0**	**3979**	**NO**
https://anulikajoy.com/	**11:43**	**11:44**	**0**	**72**	**0**	**0**	**1318**	**NO**

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

Gambar 4. Website Yang Rentan Terhadap Serangan DDoS

3.2. Pembahasan

Tujuan simulasi ini adalah untuk mengukur ketahanan berbagai situs web terhadap serangan DDoS (Distributed Denial of Service) tipe slow HTTP. Dalam simulasi ini digunakan alat bernama SlowHTTPTest, yang dikembangkan untuk menguji kerentanan server web terhadap serangan-serangan lambat seperti Slowloris, slow headers, dan slow body. Serangan ini memanfaatkan fakta bahwa sebagian besar server web memiliki batas waktu tertentu (timeout) untuk koneksi yang lambat. Jika batas ini dimanfaatkan secara agresif oleh penyerang dengan koneksi yang dibuat tetap aktif namun lambat, server bisa kehabisan slot koneksi untuk melayani permintaan sah dari pengguna.Parameter yang Digunakan

- Mulai dan Berakhir: Waktu dimulainya dan berakhirnya pengujian.
- Initializing: Jumlah koneksi yang masih dalam proses inisialisasi.
- Pending: Jumlah koneksi yang tertunda/tidak terjawab.
- Connection: Koneksi yang berhasil dibuka ke server.
- Error: Jumlah koneksi yang gagal/tidak merespon.
- Closed: Jumlah koneksi yang ditutup oleh server.
- Service Available: Status apakah layanan situs masih dapat diakses (Yes/No)

a. Analisis Data Terhadap Situs Yang Aman terhadap Serangan DDoS

1. Bykwest.com
    - Koneksi berhasil: 354
    - Pending: 61
    - Closed: 8503
    - Status: Service Available (Yes)
    - Analisis: Situs ini menunjukkan mekanisme pertahanan yang memadai. Server secara aktif menutup koneksi yang dianggap mencurigakan atau terlalu lambat (8503 koneksi), namun masih berhasil membuka 354 koneksi aktif. Fakta bahwa layanan tetap tersedia menunjukkan bahwa server memiliki sistem manajemen koneksi yang efektif, kemungkinan menggunakan algoritma untuk memutuskan koneksi lambat.

2. Albinotonnina.com
    - Koneksi berhasil sangat tinggi: 8750
    - Pending sangat rendah: 40
    - Closed: 11
    - Status: Service Available (Yes)
    - Analisis: Ini adalah situs yang paling tangguh dalam simulasi ini. Dengan hampir seluruh koneksi berhasil dibuka dan sangat sedikit yang tertunda atau ditutup, server menunjukkan efisiensi tinggi dalam menangani lalu lintas lambat. Bisa jadi server dilengkapi load balancer atau proxy yang menangani HTTP secara efisien.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

3. Christyannejones.com
    - Koneksi : 1168
    - Pending : 45
    - Closed: 8079
    - Status: Service Available (Yes)
    - Analisis: Sama seperti bykwest.com, situs ini memiliki banyak koneksi tertutup, menandakan sistem filtering berjalan. Namun, server tetap responsif terhadap koneksi yang layak. Ini menunjukkan pendekatan yang adaptif dalam manajemen trafik.
4. Pluang.com
    - Koneksi : 189
    - Pending : 1566
    - Closed: 3979
    - Status: Service Available (NO)
    - Analisis: Server mengalami kesulitan dalam menyaring koneksi lambat. Jumlah pending sangat tinggi, yang berarti permintaan pengguna nyata kemungkinan tertahan atau terblokir. Server tidak mampu membedakan koneksi sah dan koneksi berbahaya secara efektif.
5. Anulikajoy.com
    - Koneksi : 0
    - Pending : 72
    - Closed: 1318
    - Status: Service Available (NO)
    - Analisis: Semua koneksi ditutup atau dibiarkan menunggu tanpa tanggapan. Tidak ada koneksi aktif yang berhasil, yang menunjukkan kemungkinan server segera menolak semua permintaan saat mendeteksi lonjakan trafik, atau server tidak memiliki mekanisme untuk menangani slow

Berdasarkan simulasi serangan menggunakan SlowHTTPTest, dapat disimpulkan bahwa:

- Albinotonnina.com adalah situs yang paling tahan terhadap serangan DDoS slow HTTP, dengan koneksi aktif tinggi dan hampir tidak ada gangguan.
- example.com merupakan yang paling rentan, dengan layanan tidak tersedia setelah simulasi.
- Situs lain seperti bykwest.com, christyannejones.com, dan byexperience.co.uk menunjukkan ketahanan cukup baik, walaupun ada yang memiliki koneksi tertunda tinggi.

b. **Analisis Data Terhadap Situs Yang Rentan terhadap Serangan DDoS**

1. Netilradio.com
    - Koneksi berhasil: 1010
    - Pending: 327
    - Closed: 820
    - Status: Service Available (NO)
    - Analisis: Meskipun banyak koneksi berhasil dibuka, layanan tetap tidak tersedia. Ini menunjukkan bahwa koneksi yang berhasil tidak cukup untuk menjaga kestabilan sistem. Bisa jadi server overload secara internal atau tidak mampu memberikan layanan setelah koneksi dibuka.
2. Sublinemelodyyoungmelody
    - Koneksi : 1373
    - Pending sangat tinggi : 2078
    - Closed: 3603
    - Status: Service Available (NO)
    - Analisis: Situs ini memiliki jumlah pending yang sangat tinggi, menunjukkan bahwa server mengalami bottleneck yang serius dalam memproses permintaan lambat. Akibatnya, sistem tidak dapat merespons koneksi aktif secara konsisten.

3. Info.mtsayi.sch.id

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

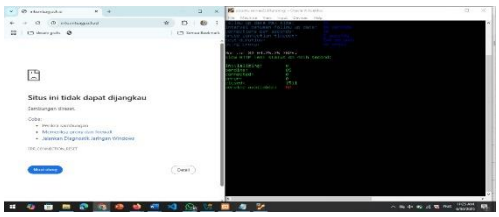
- Koneksi : 0
- Pending : 85
- Closed: 1511
- Status: Service Available (NO)
- Analisis: Tidak ada koneksi yang berhasil, menandakan sistem tidak siap untuk menghadapi serangan jenis ini. Server langsung memutus semua koneksi tanpa mencoba memprosesnya, atau mungkin firewall atau sistem IDS/IPS langsung memblokir lalu lintas.

4. byexperience.co.uk
    - Koneksi : 1031
    - Pending sangat tinggi: 6733
    - Closed: 2236
    - Status: Service Available (Yes)
    - Analisis: Meskipun banyak koneksi tertunda, server masih bisa mempertahankan layanan. Hal ini menunjukkan bahwa server memiliki strategi manajemen beban seperti pengalokasian ulang resource atau throttling yang cukup baik.
5. Example.com
    - Koneksi : 585
    - Pending : 266
    - Closed: 9149
    - Status: Service Available (Yes)
    - Analisis: Layanan tidak tersedia meskipun koneksi berhasil masih ada. Ini menunjukkan bahwa koneksi aktif tidak cukup kuat untuk menjaga sistem tetap stabil. Bisa jadi server overload akibat an proses dari koneksi lambat.

c. Contoh Perbandingan Sampel

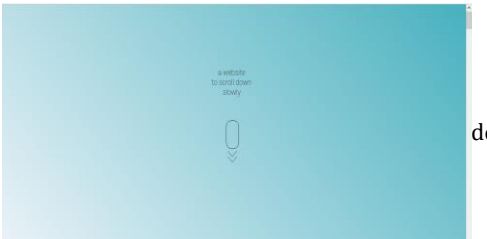
1. **Website https://albinotonnina.com/**
   Salah satu gambar di bawah ini merupakan sampel dari website yang aman terhadap serangan DDoS. Gambar 2 merupakah tampilan awal sebelum serangan dimulai dan gambar 3 merupakan hasil setelah serangan di mulai. Serangan di mulai selama 6 menit, dan hasilnya website tersebut tetap aman.

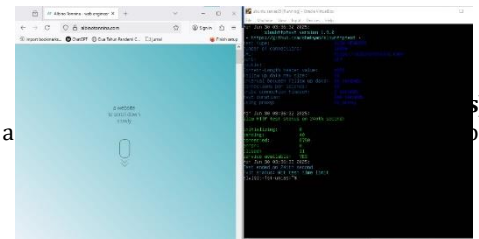
Gambar 5 Sebelum



Gambar 6 Setelah

2. **Website https://albinotonnina.com/**
   Salah satu gambar di bawah ini merupakan sampel dari website yang tidak aman terhadap serangan DDoS. Gambar 4 merupakan hasil sebelum serangan di mulai, dan gambar 5 merupakan hasil setelah serangan di mulai. Terlihat dari gambar 5 bahwa website tidak bisa diakses setelah serangan di mulai. Website langsung down setelah 1 menit serangan di jalankan.





JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

Gambar 7 Sebelum **Gambar 8** Setelah

Tabel 6. Perbandingan

Tahap	Web Tahan Serangan (Sampel)	Web Rentan (Sampel)
Tampilan Awal Web	Gambar 2: Web aman dan bisa di akses	Gambar 3: Web masih aman dan bisa diakses
Tampilan Setelah Serangan	Gambar 4: Web tetap dapat diakses normal, hanya sedikit peningkatan waktu respons.	Gambar 5: Web tidak dapat diakses, muncul pesan error atau loading sangat lama.

Berdasarkan hasil simulasi terhadap sepuluh situs web, dapat ditarik kesimpulan sebagai berikut:

- Ketahanan terhadap DDoS Slow HTTP sangat bervariasi antar situs. Situs seperti albinotonnina.com dan byexperience.co.uk mampu menangani serangan, sementara situs lain seperti example.com, pluang.com, dan anulikajoy.com tidak dapat diakses. Hal ini menunjukkan bahwa, sebagai bagian dari manajemen risiko keseluruhan, organisasi harus berinvestasi dalam ketahanan infrastruktur serta belajar tentang ancaman keamanan siber.
- Pending connection adalah indikator kuat dari kelemahan sistem. Kemungkinan server kehabisan sumber daya meningkat seiring dengan jumlah koneksi tertunda. Ini menunjukkan bahwa dalam strategi risiko TI, pemantauan terus-menerus dan penggunaan pendekatan perencanaan kapasitas diperlukan untuk mengantisipasi lonjakan trafik yang tidak biasa yang disebabkan oleh serangan.
- Koneksi ditutup (Closed) bukan berarti buruk. Sistem keamanan secara aktif menghentikan koneksi ke sejumlah situs web, termasuk bykwest.com dan christyannejones.com. Ini menunjukkan betapa pentingnya menetapkan peraturan defensive filtering sebagai bagian dari kebijakan mitigasi risiko. Strategi ini menunjukkan kemampuan untuk deteksi dini yang terintegrasi dengan kebijakan perusahaan tentang ketersediaan layanan digital.
- Jumlah koneksi berhasil (Successful Connections) mengambil peran penting dalam mempertahankan layanan. Namun, banyak koneksi harus disertai dengan kualitas layanan (QoS) yang stabil. Dalam hal manajemen risiko reputasi, contoh netilradio.com menunjukkan bahwa koneksi yang lambat menunjukkan bahwa strategi layanan berbasis SLA harus diperkuat.
- Tidak semua situs memiliki mekanisme mitigasi terhadap serangan ini. Misalnya, domain info.mtsayi.sch.id atau anulikajoy.com tidak dapat diakses dengan cepat. Ini menunjukkan kekurangan kontrol internal dan kekurangan sistem pengamanan proaktif seperti load balancer cerdas atau proxy balik. Dalam konteks manajemen risiko, ini menunjukkan betapa pentingnya melakukan evaluasi berkala terhadap posisi keamanan organisasi dan memasukkan mitigasi risiko ke dalam kebijakan TI.
- Perlu adanya sistem early detection dan filtering. Salah satu bagian penting dari strategi pengurangan risiko adalah penerapan firewall aplikasi web (WAF) dan sistem deteksi intrusi (IDS). Pola serangan seperti HTTP yang lambat dapat diidentifikasi oleh sistem dan dihentikan lebih awal. Dalam tata kelola risiko TI kontemporer, penggunaan alat-alat ini merupakan bagian dari pengendalian pencegahan, yang seharusnya sesuai dengan kebijakan keamanan organisasi dan rencana kelangsungan bisnis.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 1 Juni 2025
Hal: 368-378
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i1.406

4. KESIMPULAN

Untuk menilai ketahanan situs web, penelitian ini mensimulasikan dan menganalisis serangan DDoS dengan menggunakan teknik serangan HTTP yang lambat. Hasil simulasi dengan "slowhttptest" menunjukkan perbedaan ketahanan. Dari sepuluh situs, lima rentan terhadap serangan dengan penurunan performa atau penurunan, sementara lima lainnya lebih tahan, dan dua tetap stabil. Konfigurasi timeout, batas koneksi per IP, penggunaan CDN/WAF, dan kapasitas hosting adalah komponen penting. Konfigurasi sistem dan ketahanan terhadap DDoS sangat terkait. Penelitian ini menegaskan bahwa penerapan kebijakan keamanan siber yang kuat, penilaian konfigurasi server, dan alat untuk mitigasi dan pemantauan trafik sangat penting. Penelitian tambahan dengan cakupan target dan teknik mitigasi yang lebih luas disarankan.

REFERENCES

[1] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, "Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 6, no. 1, pp. 162–167, 2024, doi: 10.47233/jteksis.v6i1.1124.

[2] T. Safitrah, A. B. G. Sinaga, M. Alghifari, and S. N. Neyman, "Pengaruh Serangan Slow HTTP DoS terhadap Layanan Web: Studi Eksperimental dengan Slowhttptest," *J. Technol. Syst. Inf.*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/jtsi.v1i4.2663.

[3] A. Muslim, D. Rachmatullah, M. Refa, T. Ramdhani, S. Informasi, and U. Pamulang, "Penggunaan Slowhttptest Untuk Menguji Kerentangan Jaringan Terhadap Flooding Attack," vol. XIX, no. 03, pp. 12–16.

[4] M. Julda Alhafiz, A. Fauzi, A. Dwiansyah, B. Revana Indriani, F. Maulana Andhito Putra, and R. Ridho Ridwani, "Dampak Denial of Service pada Perusahaan Perbankan di Indonesia," *J. Ilmu Multidisplin*, vol. 2, no. 1, pp. 114–120, 2023, doi: 10.38035/jim.v2i1.233.

[5] A. Hudaya and R. Primananda, "Analisis Perbandingan Dampak Serangan Distributed Denial of Service pada Protokol Routing OSPF dan IS-IS," *J. Pengemb. Teknol. ...*, vol. 7, no. 4, pp. 1656–1661, 2023, [Online]. Available: http://j-ptiik.ub.ac.id

[6] F. Hamdani, Y. Bella Fitriana, and N. Oper, "KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST)," *Media Online)*, vol. 3, no. 6, pp. 1296–1302, 2023, doi: 10.30865/klik.v3i6.830.

[7] M. A. Ridho and M. Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 3, pp. 373–379, 2020, doi: 10.32736/sisfokom.v9i3.945.

[8] T. A. Madina and M. Fadhli, "Analisis Serangan DDOS pada Website Prodi Pendidikan Teknologi Informasi," vol. 7, no. 6, pp. 1730–1737, 2024.

[9] A. Afifah Rodhiyatun Nisa, Ananditto Daffa Wijayanto, Arya Prabudi Jaya Priana, and A. Setiawan, "Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website," *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 17, 2024, doi: 10.47134/pjise.v1i3.2612.

[10] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 1, pp. 172–180, 2022, [Online]. Available: http://j-ptiik.ub.ac.id

[11] M. R. Sumar, A. Wahid, and J. M. Parenreng, "Sistem Keamanan Jaringan Terhadap Serangan DOS (Denial Of Service) Menggunakan Snort Dan Firewall Berbasis Linux OS," *Pinisi J. Sciene Techonolgy*, vol. 0, pp. 1–15, 2024.

[12] S. Geges and W. Wibisono, "Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle," *JUTI J. Ilm. Teknol. Inf.*, vol. 13, no. 1, p. 53, 2015, doi: 10.12962/j24068535.v13i1.a388.

[13] I. M. W. Bhaskara, I. P. G. H. Suputra, I. M. Widiartha, I. G. A. G. A. Kadyanan, I. G. N. A. C. Putra, and I. B. G. Dwidasmara, "Klasifikasi Serangan Distributed Denial of Service (DDoS) Menggunakan Random Forest Dengan CFS," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 11, no. 2, p. 215, 2022, doi: 10.24843/jlk.2022.v11.i02.p01.

[14] Z. Dwi Alfaeni, N. Fahriani, J. Raya Sutorejo No, D. Sutorejo, K. Mulyorejo, and J. Timur, "Deteksi Serangan Ddos Pada Jaringan Rt/Rw-Net Desa Ketanen Dengan Metode Intrusion Detection System (IDS) Menggunakan Snort," *Semin. Nas. Teknol. Inf. Ilmu Komput.*, vol. 2, no. 1, pp. 28–34, 2023.

[15] J. T. Informasi *et al.*, "Literature Review Mekanisme Pertahanan Terhadap Serangan Distributed Denial Of Service (DDOS)," vol. 10, no. 2, 2024.