Smart Comp: Jurnalnya Orang Pintar Komputer
Volume 15, Nomor 3, Juli 2026, hlm. 787-796 P-ISSN : 2089-676X
Terakreditasi Sinta, Peringkat 4, SK No. 295/C/C3/KPT/2026 E-ISSN : 2549-0796
DOI : 10.30591/smartcomp.v15i3.10421

Analisis Dampak Serangan HTTP Slowloris Terhadap Performa dan Ketersediaan Server Web Lokal

Faranisa Ulya Ashari[*1], Erica Rahmawati[2], Nela Soca Putri Ardana[3], Susanto[4]
[1,2,3,4]Teknik Informatika, Fakultas Teknologi Informasi dan Komunikasi, Universitas Semarang
Email: [*1]faranisaulyaashari@gmail.com, [2]ericarahmawati800@gmail.com, [3]nellasoca34@gmail.com, [4]susanto@usm.ac.id

(Naskah masuk: *27 Juni 2026*, diterima untuk diterbitkan: *8 Juli 2026*)

Abstrak: *Server web merupakan komponen kritis dalam infrastruktur teknologi informasi yang rentan terhadap serangan Denial of Service (DoS), salah satunya HTTP Slowloris. Penelitian ini bertujuan untuk menganalisis dampak kuantitatif serangan HTTP Slowloris terhadap performa dan ketersediaan server web lokal berbasis XAMPP pada lingkungan Local Area Network (LAN). Pengujian dilakukan secara terkontrol menggunakan tiga perangkat dengan peran masing-masing sebagai server, pemantau, dan penyerang. Serangan disimulasikan menggunakan Nmap Scripting Engine dengan skrip http-slowloris, sementara analisis trafik jaringan dilakukan menggunakan Wireshark. Hasil pengujian menunjukkan bahwa serangan HTTP Slowloris menyebabkan peningkatan jumlah paket TCP aktif dari 10 paket menjadi 6.058 paket pada intensitas tertinggi, waktu respons server meningkat dari 28 ms menjadi 126.000 ms (2,1 menit), serta layanan mengalami degradasi berupa status pending dan canceled mulai pada parallelism 200. Temuan ini mengonfirmasi bahwa serangan HTTP Slowloris efektif melumpuhkan ketersediaan layanan web meskipun tidak membebani bandwidth secara signifikan, sehingga menegaskan perlunya penerapan mitigasi seperti pembatasan jumlah koneksi per klien pada konfigurasi server.*

Kata Kunci – *HTTP Slowloris ; Denial of Service (DoS) ; Nmap ; Wireshark ; Keamanan Jaringan*

Analysis of HTTP Slowloris Attack Impact on the Performance and Availability of Local Web Servers

Abstract: *Web servers are critical components of information technology infrastructure that are vulnerable to Denial of Service (DoS) attacks, one of which is HTTP Slowloris. This study aims to quantitatively analyze the impact of HTTP Slowloris attacks on the performance and availability of a local XAMPP-based web server within a Local Area Network (LAN) environment. Controlled experiments were conducted using three devices assigned as server, monitor, and attacker. The attack was simulated using the Nmap Scripting Engine with the http-slowloris script, while network traffic analysis was performed using Wireshark. The results show that the HTTP Slowloris attack caused active TCP packets to increase from 10 packets to 6,058 packets at peak intensity, server response time increased from 28 ms to 126,000 ms (2.1 minutes), and service degradation in the form of pending and canceled status began at parallelism 200. These findings confirm that HTTP Slowloris attacks effectively disrupt web service availability without significantly consuming bandwidth, highlighting the need for mitigations such as per-client connection limiting in server configurations.*

Keywords – *HTTP Slowloris ; Denial of Service (DoS) ; Nmap ; Wireshark ; Network Security*

1. PENDAHULUAN

Infrastruktur teknologi informasi modern sangat bergantung pada ketersediaan layanan berbasis web yang berkesinambungan. Server web memiliki peran sebagai gerbang penting dalam penyampaian informasi, layanan elektronik, dan aplikasi berbasis jaringan sehingga menjadikannya aset kritis yang harus selalu tersedia bagi pengguna. Kelumpuhan pada server web dapat mengganggu proses akses informasi oleh pengguna secara menyeluruh [1]. Kondisi ketergantungan terhadap layanan web yang tinggi, berbanding lurus dengan meningkatnya ancaman keamanan siber, terkhusus pada serangan yang menargetkan ketersediaan layanan. Berdasarkan kajian yang dilakukan oleh Tripathi dan Hubballi, serangan pada lapisan aplikasi merupakan ancaman yang

bersifat tersembunyi dan menargetkan aplikasi tertentu pada korban, dengan tujuan menguras sumber daya seperti memori, CPU, dan bandwidth sehingga melanggar komponen utama keamanan siber yaitu ketersediaan layanan [2].

Salah satu bentuk serangan pada lapisan aplikasi yang paling efektif dan sulit dideteksi adalah serangan *Denial of Service* (DoS) HTTP Slowloris. Berbeda dengan adanya serangan DoS konvensional yang membanjiri server dengan volume trafik yang besar, Slowloris bekerja dengan membuka sejumlah koneksi HTTP ke server secara bersamaan namun tidak pernah menyelesaikannya, sehingga memaksa server mempertahankan koneksi-koneksi tersebut hingga kapasitas maksimum tercapai bahkan tidak mampu melayani permintaan pengguna sah [3]. Serangan ini menggunakan bandwidth minimal namun mampu menghabiskan seluruh sumber daya server, menjadikannya sulit untuk dibedakan dari lalu lintas jaringan normal [2]. Sabri dkk. melakukan simulasi serangan Slowloris menggunakan ActivePerl pada server berbasis Apache dan mengonfirmasi bahwa serangan ini berhasil membuat website tidak dapat diakses oleh pengguna sah bahkan setelah cache browser dibersihkan, membuktikan tingginya efektivitas serangan ini terhadap layanan web [4].

Performa server web merupakan salah satu aspek penting dalam menjaga kualitas layanan yang diterima pengguna. Salah satu parameter yang umum digunakan untuk mengevaluasi performa server adalah waktu respons (response time), yaitu waktu yang dibutuhkan server untuk memberikan tanggapan terhadap permintaan pengguna. Semakin kecil nilai waktu respons yang dihasilkan, semakin baik performa layanan yang diberikan oleh server web [5]. Selain itu, pada kondisi serangan jaringan, performa server juga dapat diamati melalui perubahan jumlah koneksi aktif serta tingkat keberhasilan akses pengguna terhadap layanan yang disediakan.

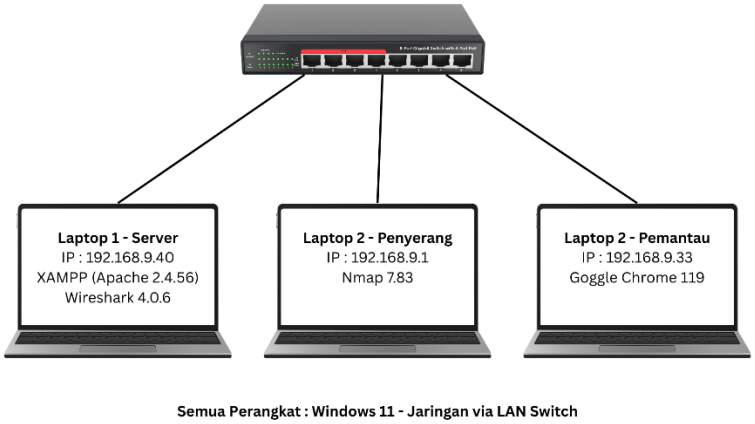
Sejumlah penelitian terdahulu telah mengkaji berbagai aspek keamanan jaringan yang relevan dengan topik ini. Hawarizmi dkk. menggunakan sistem deteksi serangan DDoS pada Software Defined Network menggunakan metode entropy dan memperoleh akurasi deteksi tertinggi sebesar 72,85% dari 30 kali percobaan [6]. Putra mengimplementasikan keamanan jaringan pada protokol FTP menggunakan Intrusion Prevention System berbasis Mikrotik sebagai upaya mitigasi terhadap ancaman jaringan [7]. Murthy dkk. menganalisis performa HTTP pada server Apache2 selama serangan Slowloris berlangsung dan memantau metrik connection time, latency, page load time, dan inter-packet arrival time, serta menggunakan Monte Carlo simulation untuk menentukan nilai threshold deteksi [3]. Dari sisi metodologi pengujian, Pratama dan Servanda menggunakan Nmap dan HPING3 untuk menganalisis serangan DDoS Ping of Death secara forensik dan berhasil mengidentifikasi karakteristik trafik serangan [8]. Mamuriyah dkk. merancang sistem keamanan jaringan terhadap serangan DDoS menggunakan metode pengujian penetrasi dengan GoldenEye pada Kali Linux dan menunjukkan bahwa sistem keamanan yang dibangun berhasil mengidentifikasi serta mengurangi kerentanan terhadap serangan [1].

Meskipun penelitian-penelitian tersebut telah memberikan kontribusi yang berarti, sebagian besar berfokus pada deteksi atau mitigasi serangan secara umum dan belum mengukur dampak kuantitatif serangan HTTP Slowloris secara spesifik pada lingkungan server web lokal yang terkontrol. Oleh karena itu, penelitian ini bertujuan untuk menganalisis dampak kuantitatif serangan HTTP Slowloris terhadap performa dan ketersediaan server web lokal berbasis Apache XAMPP dalam lingkungan *Local Area Network* (LAN). Pengujian dilakukan menggunakan *Nmap Scripting Engine* dengan beberapa variasi jumlah koneksi paralel, sedangkan analisis trafik jaringan dilakukan menggunakan Wireshark. Hasil penelitian ini diharapkan dapat memberikan gambaran yang jelas dan terukur mengenai dampak serangan HTTP Slowloris, sekaligus menjadi dasar dalam merancang strategi mitigasi yang lebih efektif pada server web lokal.

2. METODE PENELITIAN

2.1. Lingkungan Pengujian

Pengujian dilakukan dalam lingkungan jaringan Local Area Network (LAN) yang terkontrol menggunakan tiga unit laptop yang dihubungkan melalui switch dengan kecepatan 1 Gbps. Seluruh perangkat menggunakan sistem operasi Windows 11 untuk menjaga konsistensi konfigurasi lingkungan pengujian. Konfigurasi masing-masing perangkat disajikan pada Gambar 1.



Gambar 1. Topologi Jaringan

Server web dijalankan menggunakan XAMPP versi 8.2.4 yang mencakup Apache HTTP Server versi 2.4.56, PHP versi 8.2.4, dan MySQL (MariaDB) sebagai sistem manajemen basis data. Website yang diuji merupakan website internal restoran berbasis database yang hanya dapat diakses dalam jaringan lokal dan tidak dipublikasikan ke internet publik. Penggunaan website berbasis database bertujuan untuk mensimulasikan kondisi web server yang lebih realistis dalam mengamati dampak serangan terhadap layanan yang sedang aktif. Wireshark dijalankan pada Laptop 1 (server) agar seluruh trafik masuk dari penyerang dapat tertangkap secara langsung.

2.2. Tools yang Digunakan

Tabel 1. Tools yang Digunakan dalam Pengujian

Tools	Versi	Fungsi
Nmap	7.83	Simulasi serangan Slowloris menggunakan Nmap Scripting Engine (NSE) dengan skrip http-slowloris
Wireshark	4.0.6	Analisis dan verifikasi pola trafik jaringan serta pencatatan koneksi TCP pada Laptop 1 (Server)
Google Chrome	119	Pemantauan waktu respons dan status ketersediaan website dari sisi pemantau (Laptop 3)

Nmap Scripting Engine (NSE) digunakan sebagai alat untuk mensimulasikan serangan HTTP Slowloris karena kemampuannya dalam melakukan pengujian keamanan jaringan secara terstruktur dan dapat dikontrol [8]. Wireshark digunakan untuk menangkap dan menganalisis

trafik jaringan selama pengujian berlangsung, sehingga perubahan pola koneksi TCP dapat diidentifikasi secara langsung [9].

2.3. Skenario Pengujian

Pengujian dilakukan dalam empat skenario sebagaimana disajikan pada Tabel 2.

Tabel 2. Skenario Pengujian

Skenario	Kondisi	Parallelism	Keterangan
1	Normal (Baseline)	-	Akses website tanpa serangan
2	Serangan Slowloris	100	100 koneksi paralel
3	Serangan Slowloris	200	200 koneksi paralel
4	Serangan Slowloris	400	400 koneksi paralel

2.3.1. Pengujian Kondisi Normal (Baseline)

Pengujian baseline dilakukan sebelum serangan dijalankan dengan mengakses website internal melalui browser Chrome pada Laptop 3 (Pemantau). Pada kondisi ini dicatat waktu respons server dan waktu pemuatan halaman melalui Chrome DevTools (F12 → tab Network), serta pola trafik jaringan direkam menggunakan Wireshark pada Laptop 1 (Server).

2.3.2. Simulasi Serangan HTTP Slowloris

Serangan HTTP Slowloris disimulasikan menggunakan Nmap Scripting Engine dari laptop penyerang dengan perintah sebagai berikut:

```
nmap -Pn -p 80 --script http-slowloris --max-parallelism [100/200/400] 192.168.9.40
```

Serangan bekerja dengan membuka sejumlah koneksi HTTP secara bersamaan ke server tanpa menyelesaikannya, sehingga memaksa server mempertahankan koneksi-koneksi tersebut hingga kapasitas maksimum tercapai [3][4]. Variasi jumlah koneksi paralel sebesar 100, 200, dan 400 digunakan untuk mengamati perbedaan dampak berdasarkan intensitas serangan.

2.3.3. Monitoring dan Pengambilan Data

Selama serangan berlangsung, Laptop 3 (Pemantau) mencatat waktu respons server, status HTTP, dan kondisi akses melalui Chrome DevTools, sementara Wireshark pada Laptop 1 (Server) merekam seluruh trafik jaringan secara bersamaan. Pemantauan dilakukan secara berulang selama durasi serangan berlangsung dan kondisi yang representatif dari setiap skenario dicatat untuk keperluan analisis. Setelah serangan dihentikan, dicatat pula waktu pemulihan server hingga website dapat kembali diakses secara normal.

2.4. Parameter Pengujian

Parameter pengujian disajikan pada Tabel 3 berikut.

Tabel 3. Parameter Pengujian

Aspek	Parameter	Cara Pengukuran	Satuan
Performa	Waktu respons server	Chrome DevTools → kolom Time pada baris pertama	ms

Performa	Waktu pemuatan halaman	Chrome DevTools → Finish di bagian bawah	ms/menit
Ketersediaan	Status layanan	Kode status HTTP (200 OK / canceled / pending)	–
Ketersediaan	Waktu hingga gangguan	Selisih waktu dari mulai serangan hingga status berubah	detik
Jaringan	Koneksi TCP ke server	Total paket TCP dari penyerang ke server (Wireshark CSV)	jumlah
Jaringan	Half-open connections	Filter: tcp.flags.syn==1 && tcp.flags.ack==0	jumlah paket
Jaringan	Retransmisi TCP	Filter Wireshark: tcp.analysis.retransmission	jumlah paket
Jaringan	HTTP dari penyerang	Paket HTTP yang dikirim penyerang ke server	Jumlah

2.5. Etika Pengujian

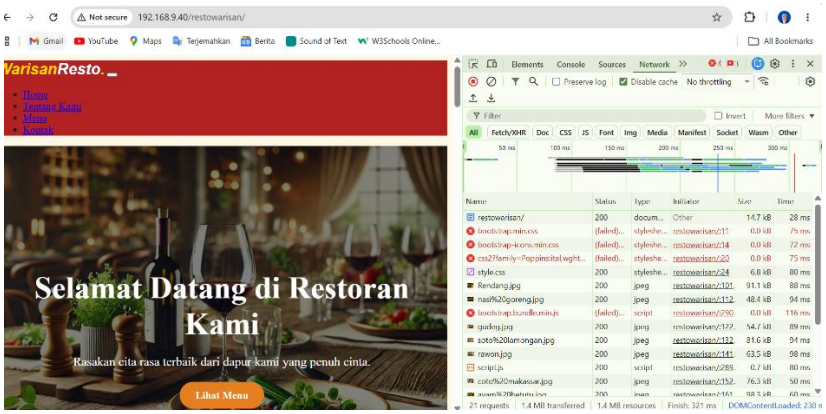
Seluruh pengujian dilakukan pada sistem dan website internal yang sepenuhnya dimiliki dan dikelola oleh peneliti. Website yang diuji tidak dapat diakses dari internet dan hanya tersedia dalam jaringan lokal sehingga tidak mengganggu sistem atau pengguna lain. Penelitian ini dilakukan semata-mata untuk tujuan akademik dan pengembangan ilmu pengetahuan di bidang keamanan jaringan.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Pengujian Kondisi Normal (Baseline)

Pengujian baseline dilakukan untuk memperoleh gambaran awal performa layanan website sebelum serangan dijalankan. Laptop 3 (Pemantau) mengakses website internal WarisanResto melalui Chrome dan hasilnya dipantau melalui Chrome DevTools, sementara trafik jaringan direkam oleh Wireshark pada Laptop 1 (Server).

Pada kondisi normal, website berhasil diakses dengan lancar. Dokumen utama (restowarisan/) mendapat respons dengan status 200 OK dalam waktu 28 ms, dan seluruh halaman selesai dimuat dalam 321 ms dengan total 21 requests dan 1,4 MB data ditransfer. Waktu respons yang cepat dan stabil ini mencerminkan kondisi server yang berfungsi optimal, sesuai dengan pernyataan Riswandi dan Kasim bahwa semakin kecil nilai waktu respons yang dihasilkan, semakin baik performa layanan yang diberikan oleh server web [5]. Hasil capture Wireshark menunjukkan pola trafik yang normal, tanpa adanya half-open connections maupun retransmisi paket TCP.



Gambar 2. Web server dalam kondisi normal

Tabel 4. Hasil Pengujian Kondisi Normal (Baseline)

Parameter	Nilai
Waktu respons server (restowarisan/)	28 ms
Finish (total muat halaman)	321 ms
Status HTTP	200 OK
Total request	21 Requests
Data ditransfer	1,4 MB
Paket TCP (penyerang→server)	10 paket
Half-open connections	0
Retransmisi TCP	0

3.2. Hasil Pengujian Serangan Slowloris Parallelism 100

Serangan Slowloris dengan 100 koneksi paralel dijalankan dari Laptop 2 (Penyerang) ke Laptop 1 (Server). Pada intensitas ini, server masih mampu merespons permintaan dari pemantau meskipun beban trafik meningkat secara signifikan.

Dokumen utama masih mendapat respons 200 OK dalam waktu 30 ms dengan total waktu muat 474 ms - meningkat sekitar 47,7% dibandingkan kondisi baseline (321 ms). Dari data Wireshark, jumlah paket TCP dari penyerang ke server meningkat drastis menjadi 1.542 paket disertai 414 HTTP requests dari penyerang dan mulai terdeteksi 11 kali retransmisi TCP yang mengindikasikan awal munculnya gangguan pada komunikasi jaringan. Meskipun belum terjadi kegagalan akses dari sisi pemantau, peningkatan trafik ini menunjukkan server mulai menanggung beban koneksi tambahan akibat serangan [3].

Tabel 5. Hasil Pengujian Serangan Slowloris Parallelism 100

Parameter	Kondisi Normal	Parallelism 100	Perubahan
Waktu respons (ms)	28 ms	30 ms	+7,1%
Finish (ms)	321 ms	474 ms	+47,7%
Status HTTP	200 OK	200 OK	Stabil
Paket TCP ke server	10	1.542	+15.320%
Half-open connections	0	0	-
Retransmisi TCP	0	11	Meningkat
HTTP dari penyerang	1	414	Meningkat

3.3. Hasil Pengujian Serangan Slowloris Parallelism 200

Peningkatan koneksi paralel menjadi 200 menghasilkan dampak yang lebih nyata. Pada fase awal serangan, sebagian permintaan masih mendapat respons 200 OK dengan waktu 11 ms, namun

resource pendukung halaman seperti gambar mulai menunjukkan status (pending) menandakan server tidak lagi mampu menyelesaikan semua koneksi HTTP secara bersamaan. Pada fase serangan yang lebih intens, permintaan utama berakhir dengan status (canceled) setelah menunggu selama 1.600 ms (1,60 detik) - meningkat sekitar 5.614% dibandingkan waktu respons normal 28 ms.

Kondisi ini selaras dengan yang dikemukakan Tripathi dan Hubballi bahwa serangan application layer DoS mampu menguras sumber daya server seperti memori, CPU, dan kapasitas koneksi, sehingga server tidak dapat melayani permintaan pengguna sah meskipun beban bandwidth tidak signifikan [2]. Data Wireshark menunjukkan paket TCP dari penyerang ke server mencapai 2.344 paket dengan 734 FIN/RST dan 8 retransmisi TCP.

Tabel 6. Hasil Pengujian Serangan Slowloris Parallelism 200

Parameter	Kondisi Normal	Parallelism 200	Perubahan
Waktu respons (ms)	28 ms	11 ms (awal) → 1.600 ms (canceled)	Meningkat drastis
Status HTTP	200 OK	200 OK → pending → canceled	Terdegradasi
Paket TCP ke server	10	2.344	+23.340%
FIN/RST dari penyerang	2	734	Meningkat
Half-open connections	0	0	-
Retransmisi TCP	0	8	Meningkat
HTTP dari penyerang	1	401	Meningkat

3.4. Hasil Pengujian Serangan Slowloris Parallelism 400

Skenario 400 koneksi paralel menghasilkan dampak paling signifikan. Waktu respons server melonjak drastis hingga 2,1 menit (126.000 ms) dan 1,9 menit (114.000 ms) pada beberapa percobaan peningkatan lebih dari 4.000 kali lipat dibandingkan kondisi normal. Kondisi pending juga terjadi sebagaimana pada parallelism 200, di mana server tidak mampu memproses permintaan baru dari pemantau. Hal ini mengonfirmasi mekanisme Slowloris yang dijabarkan oleh Sabri dkk., yaitu bahwa server dipaksa mempertahankan koneksi yang tidak diselesaikan hingga tidak sanggup melayani pengguna sah [4].

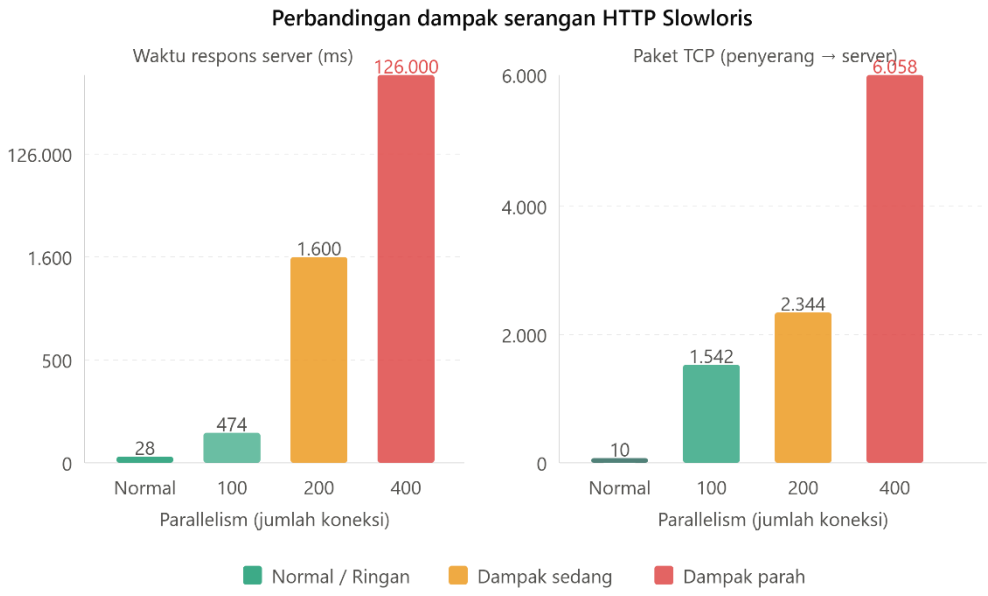
Data Wireshark menunjukkan eskalasi yang signifikan: paket TCP dari penyerang ke server mencapai 6.058 paket, dengan 2.124 paket SYN yang mengindikasikan pembukaan koneksi secara masif. Jumlah half-open connections terdeteksi sebanyak 763 koneksi merupakan satu-satunya skenario di mana half-open connections terdeteksi secara signifikan, mengonfirmasi secara langsung mekanisme inti serangan Slowloris [4]. Retransmisi TCP juga melonjak tajam menjadi 69 kali, menandakan gangguan komunikasi jaringan yang semakin parah akibat beban koneksi yang berlebihan.

Tabel 7. Hasil Pengujian Serangan Slowloris Parallelism 400

Parameter	Kondisi Normal	Parallelism 400	Perubahan
Waktu respons (ms)	28 ms	126.000 ms (maks)	+449.900%
Status HTTP	200 OK	pending → 200 OK (sangat lambat)	Terdegradasi parah
Paket TCP ke server	10	6.058	+60.480%
SYN dari penyerang	0	2.124	Meningkat drastis
Half-open connections	0	763	Terdeteksi signifikan
Retransmisi TCP	0	69	Meningkat drastis
HTTP dari penyerang	1	401	Meningkat

3.5. *Analisis dan Pembahasan*

Berdasarkan keseluruhan hasil pengujian, terdapat pola eskalasi dampak yang konsisten seiring meningkatnya jumlah koneksi paralel serangan HTTP Slowloris. Perbandingan lengkap seluruh skenario disajikan pada Gambar 3.



Gambar 3. Perbandingan Hasil Seluruh Skenario

Pada parallelism 100, server masih mampu mempertahankan layanan karena jumlah koneksi yang dibuka penyerang belum mencapai batas kapasitas thread Apache 2.4.56. Hal ini selaras dengan temuan Murthy dkk. yang menyatakan bahwa dampak Slowloris bergantung pada kapasitas maksimum koneksi yang dikonfigurasi pada server target [3]. Peningkatan trafik TCP sebesar 15.320% dan mulai terdeteksinya retransmisi menunjukkan server sudah menanggung beban tambahan, meskipun layanan masih tersedia.

Pada parallelism 200, mulai terlihat gejala resource exhaustion yang ditandai status pending dan canceled. Serangan Slowloris terbukti efektif karena tidak memerlukan bandwidth besar namun mampu menguras kapasitas koneksi server sesuai dengan kajian Tripathi dan Hubballi tentang karakteristik serangan DoS pada lapisan aplikasi [2]. Kondisi ini juga dikonfirmasi oleh Fitri dkk. yang menemukan bahwa mekanisme honeypot diperlukan justru karena Slowloris mampu melumpuhkan Apache meski tanpa volume trafik tinggi [10].

Pada parallelism 400, dampak paling ekstrem terlihat dari lonjakan waktu respons hingga 2,1 menit dan terdeteksinya 763 half-open connections. Fenomena half-open connections ini secara langsung mengonfirmasi mekanisme inti Slowloris yang dijelaskan Sabri dkk., yaitu server dipaksa mempertahankan ratusan sesi HTTP yang tidak diselesaikan hingga sumber daya thread Apache habis [4]. Peningkatan retransmisi TCP sebanyak 69 kali juga mengindikasikan gangguan serius pada komunikasi jaringan sebagaimana yang dapat diidentifikasi melalui analisis trafik Wireshark [9].

Fenomena menarik yang ditemukan adalah kemampuan server untuk sesekali merespons dengan waktu normal (27–283 ms) pada parallelism 400. Hal ini terjadi karena Nmap Slowloris bekerja secara siklikal, melepaskan dan membuka kembali koneksi secara bergantian, sehingga terdapat jendela waktu singkat di mana thread Apache tersedia. Meski begitu, kondisi ini tidak dapat diandalkan karena sebagian besar waktu server berada dalam kondisi terbebani penuh, yang

secara keseluruhan mengonfirmasi bahwa serangan HTTP Slowloris efektif dalam menurunkan performa dan ketersediaan server web lokal.

4. KESIMPULAN

Berdasarkan hasil pengujian dan analisis yang telah dilakukan terhadap dampak serangan HTTP Slowloris pada server web lokal berbasis Apache XAMPP dalam lingkungan LAN, dapat disimpulkan sebagai berikut:

1. Serangan HTTP Slowloris terbukti efektif dalam menurunkan performa dan ketersediaan server web lokal. Pada kondisi normal, server merespons permintaan dalam waktu 28 ms dengan status 200 OK. Seiring meningkatnya intensitas serangan, waktu respons meningkat drastis hingga mencapai 126.000 ms (2,1 menit) pada parallelism 400 - peningkatan lebih dari 4.000 kali lipat dibandingkan kondisi normal.
2. Dampak serangan bersifat progresif sesuai jumlah koneksi paralel yang digunakan. Pada parallelism 100, layanan masih dapat dipertahankan dengan waktu respons 30 ms dan status 200 OK, meskipun trafik TCP meningkat drastis dari 10 menjadi 1.542 paket. Pada parallelism 200, mulai muncul status pending dan canceled yang menandakan resource exhaustion. Pada parallelism 400, terjadi gangguan layanan paling parah dengan terdeteksinya 763 half-open connections dan 69 retransmisi TCP.
3. Serangan HTTP Slowloris mampu melumpuhkan server web tanpa memerlukan bandwidth yang besar. Mekanisme serangan yang membuka koneksi HTTP secara masif tanpa menyelesaikannya terbukti efektif menguras kapasitas thread Apache hingga server tidak mampu melayani permintaan pengguna sah, meskipun kondisi jaringan secara keseluruhan tidak terbebani secara signifikan.
4. Analisis trafik menggunakan Wireshark mengonfirmasi karakteristik serangan Slowloris secara kuantitatif, khususnya pada parallelism 400 yang menunjukkan 2.124 paket SYN dan 763 half-open connections — membuktikan bahwa server dipaksa mempertahankan ratusan koneksi HTTP yang tidak diselesaikan secara bersamaan.
5. Hasil penelitian ini diharapkan dapat menjadi referensi dalam merancang strategi mitigasi yang efektif terhadap serangan HTTP Slowloris, seperti pembatasan jumlah koneksi per klien, konfigurasi timeout koneksi yang lebih ketat, serta penggunaan modul keamanan tambahan pada server Apache.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Komunikasi, Universitas Semarang yang telah memberikan dukungan akademik selama proses penelitian ini berlangsung. Penulis juga menyampaikan apresiasi kepada seluruh tim editorial dan reviewer Smart Comp: Jurnalnya Orang Pintar Komputer atas masukan dan proses penelaahan yang konstruktif. Semoga hasil penelitian ini dapat memberikan kontribusi yang bermanfaat bagi pengembangan ilmu pengetahuan di bidang keamanan jaringan dan infrastruktur teknologi informasi.

DAFTAR PUSTAKA

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

[2] N. Tripathi and N. Hubballi, "Application layer denial-of-service attacks and defense mechanisms: A survey," ACM Comput. Surv., vol. 54, no. 4, 2022, doi: 10.1145/3448291.

[3] A. A. Murthy, P. M. John, and R. M. B. Kasturi Nagappasetty, "Hypertext transfer protocol performance analysis in traditional and software defined networks during Slowloris attack," International Journal of Electrical and Computer Engineering, vol. 13, no. 4, pp. 4268–4279, 2023, doi: 10.11591/ijece.v13i4.pp4268-4279.

[4] S. Sabri, N. Ismail, and A. Hazzim, "Slowloris DoS Attack Based Simulation," IOP Conf. Ser. Mater. Sci. Eng., vol. 1062, no. 1, 2021, doi: 10.1088/1757-899X/1062/1/012029.

[5] Riswandi, Kasim, and Muh. F. Raharjo, "Evaluasi Kinerja Web Server Apache menggunakan Protokol HTTP2," Journal of Engineering, Technology, and Applied Science, vol. 2, no. 1, pp. 19–31, 2020, doi: 10.36079/lamintang.jetas-0201.92.

[6] M. Hawarizmi Hafiz, M. Kurniawan Teguh, and M. Fathinuddin, "Sistem Deteksi Serangan Ddos Pada Software Defined Network Menggunakan Metode Entropy," Smart Comp: Jurnalnya Orang Pintar Komputer, vol. 11, no. 4, pp. 615–628, 2022, doi: 10.30591/smartcomp.v11i4.4246.

[7] A. Putra Dwi and M. Alghozy Bey Ridho Thorriq, "Analisis dan Implementasi Keamanan Jaringan File Transfer Protocol (FTP) Menggunakan Intrusion Prevention System (IPS) pada Mikrotik," Smart Comp: Jurnalnya Orang Pintar Komputer, vol. 11, no. 4, 2022, doi: 10.30591/smartcomp.v11i4.4263.

[8] N. ardi S. P. Pratama and Y. Servanda, "Analisis Serangan Forensik Terhadap Serangan Ddos Ping Of Death Menggunakan Tools NMAP dan HPING3," Jurnal Sains dan Teknologi (JSIT), vol. 4, no. 2, pp. 209–216, 2024, doi: 10.47233/jsit.v4i2.1842.

[9] A. Z. Nusri and R. Erwin Syah, "Analisis Trafik Jaringan Menggunakan Wireshark Untuk Meningkatkan Kinerja Jaringan Pada Smk 3 Soppeng," Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI), vol. 8, no. 1, pp. 114–122, 2025, doi: 10.57093/jisti.v8i1.281.

[10] N. R. Fitri, A. H. S. Budi, I. Kustiawan, and S. E. Suwono, "Low interaction honeypot as the defense mechanism against Slowloris attack on the web server," IOP Conf. Ser. Mater. Sci. Eng., vol. 850, no. 1, 2020, doi: 10.1088/1757-899X/850/1/012037.