(2026), 4 (1): 1-7 **Scientica** 3021-8209

Jurnal Ilmiah Sain dan Teknologi

SIMULASI DAN ANALISIS DAMPAK SERANGAN *SLOWLORIS* PADA KINERJA WEB SERVER MENGGUNAKAN KALI LINUX

Randy Iqbal Putra Kesuma [*1], Saripudin [2], Ozin Ardianto [3], Yudi Prayoga [4], Antika Zahrotil Kamalia [5]

[1]Program Studi Teknik Informatika, Universitas Pelita Bangsa

Email: [1] kesumah.312210209@pelitabangsa.ac.id,

[2] saripudin.312210077@mhs.pelitabangsa.ac.id,

[3] ardianto312210201@mhs.pelitabangsa.ac.id, [4] pragoga.312210043@mhs.pelitabangsa.ac.id,

[5] antika.kamalia@pelitabangsa.ac.id

Abstract (English)

This research discusses the simulation and analysis of the impact of the Slowloris attack on web server performance using the Kali Linux operating system as the testing environment. Slowloris is a type of Denial of Service (DoS) attack that works by opening multiple connections to the server and sending incomplete HTTP requests slowly, exhausting the server's resources and preventing it from serving legitimate users. The experiment was conducted on a local XAMPP-based server under normal and attack conditions. The results show a significant increase in CPU usage from 20% to 52%, along with abnormal TCP connections such as Duplicate ACK and Retransmission. These findings confirm that the Slowloris attack can degrade web server performance and potentially cause service unavailability.

Article History

Submitted: 3 Januari 2026

Accepted: 6 Januari 2026

Published: 7 Januari 2026

Key Words

Slowloris, DoS, Kali Linux, Web Server, *Performance Analysis*

Abstrak (Indonesia)

Penelitian ini membahas simulasi dan analisis dampak serangan *Slowloris* terhadap kinerja web server menggunakan sistem operasi Kali Linux sebagai alat pengujian. Serangan *Slowloris* merupakan salah satu jenis *Denial of Service (DoS)* yang bekerja dengan cara membuka banyak koneksi ke server dan mengirimkan permintaan *HTTP* secara lambat, sehingga server kehabisan sumber daya untuk melayani pengguna lain. Pengujian dilakukan pada server lokal berbasis *XAMPP* dengan kondisi sebelum dan sesudah serangan. Hasil penelitian menunjukkan bahwa terjadi peningkatan signifikan pada penggunaan *CPU* dari 20% menjadi 52%, serta muncul banyak koneksi *TCP* tidak normal seperti Duplicate *ACK* dan *Retransmission*. Hal ini membuktikan bahwa serangan *Slowloris* dapat mengakibatkan penurunan performa web server dan berpotensi menyebabkan *service unavailability*.

Sejarah Artikel

Submitted: 3 Januari 2026

Accepted: 6 Januari 2026

Published: 7 Januari 2026

Kata Kunci

Slowloris, DoS, Kali Linux, Web Server, Analisis Kinerja

PENDAHULUAN

Serangan *Denial of Service (DoS)* merupakan salah satu ancaman utama dalam dunia keamanan siber yang bertujuan untuk melumpuhkan layanan, sistem, atau jaringan dengan membanjiri target menggunakan lalu lintas atau permintaan yang berlebihan, sehingga layanan menjadi tidak dapat diakses oleh pengguna sah. Dalam beberapa tahun terakhir, varian serangan *DoS* pada lapisan aplikasi, seperti *Slow HTTP DoS*, semakin sering digunakan oleh penyerang karena efektivitasnya dalam mengeksploitasi kelemahan manajemen koneksi pada server web, bahkan dengan sumber daya terbatas. Serangan ini menimbulkan kerugian signifikan, baik dari sisi finansial, reputasi, maupun kepercayaan. pengguna terhadap penyedia layanan digital.(Della Yunika Zebua et al. 2025). Keamanan jaringan komputer merupakan salah satu aspek fundamental dalam menjaga kontinuitas layanan digital di era modern. Ancaman keamanan siber, khususnya serangan *Distributed Denial of Service (DDoS)*, telah menjadi perhatian serius bagi organisasi dan institusi pendidikan di seluruh dunia. Serangan

DDoS tidak hanya mengganggu operasional normal suatu sistem, tetapi juga dapat menyebabkan kerugian finansial dan reputasi yang signifikan.(Dorthea Elvita Harefa et al. 2025). Perkembangan informasi teknologi saat ini telah berkembang dengan pesat. Penggunaan *website* dalam menyampaikan informasi sangatlah membantu dan bermanfaat bagi lembaga-lembaga atau perusahaan-perusahaan.

Penyampaian informasi dengan *website* tidak membutuhkan waktu yang lama dan dapat dilakukan darimana saja. Tidak dibatasi oleh tempat,waktu dan biaya. Proses mendapatkan informasi dari *website* juge lebih *up to date.* Informasi yang ditampilkan dan disajikan dapat berubah seiring jalannya waktu sehingga informasi yang disajikan tidak ketinggalan zaman atau terlambat. Kemudahan ini yang membuat *website* sebagai sarana informasi yang digemari user saat ini(Arifin, Utami, and Pramono 2020).

Slowloris adalah jenis serangan DDoS pada lapisan aplikasi yang menggunakan permintaan HTTP parsial untuk membuka koneksi antara satu komputer dan server Web yang ditargetkan, kemudian menjaga koneksi tersebut tetap terbuka selama mungkin, sehingga membebani dan memperlambat kinerja target.(Zidane 2022) web adalah aplikasi berorientasi tugas yang digunakan pada web server, hal ini menjadi bagian penting karena web server dituntut harus menjaga integritas informasi yang disampaikan kepada pengguna web. serangan web atau cyber attack mendeteksi jumlah serangan naik 4 kali lipat jumlah serangan dari tahun sebelumnya yaitu 2019 dengan jumlah serangan hanya 98 juta.(Fachri 2023)

Keamanan siber atau yang sering disebut sebagai keamanan informasi digital, adalah disiplin ilmu yang berfokus pada perlindungan sistem komputer, jaringan, program, dan data dari serangan, kerusakan, atau akses yang tidak sah. Keamanan siber mencakup semua langkah-langkah teknis dan administratif yang diambil untuk melindungi informasi digital dari berbagai ancaman. Ancaman tersebut bisa berupa serangan siber, *malware*, *hacking*, dan banyak lagi. (Safitrah et al. 2024).

Linux adalah sebuah sistem operasi yang relatif aman dan populer digunakan dalam berbagai aplikasi. Dalam beberapa penelitian, Linux digunakan sebagai sistem operasi server utama, seperti dalam penelitian yang menggunakan Slowloris untuk melakukan seranganDoS (Rafid, Tambunan, and Neyman 2024) Serangan Denial of Service(DoS) telah menjadi salah satu ancaman utama bagi keamanan sistem dan layanan jaringan di seluruh dunia. (Haniyah et al. 2024) Serangan Distributed Denial of Service (DDoS) telah berkembang dari serangan volumetrik sederhana menjadi serangan yang lebih canggih dan sulit dideteksi. (Noor et al. 2025)

Salah satu varian serangan DDoS yang sangat efektif dan sulit dideteksi adalah serangan Slowloris. Berbeda dengan serangan DDoS tradisional yang mengonsumsi bandwidth besar, Slowloris menggunakan pendekatan "low and slow" dengan memanfaatkan keterbatasan kapasitas koneksi server web..(Harefa et al. 2025)

METODE PENELITIAN

Penelitian ini berfokus pada penerapan dan mitigasi serangan *Slowloris* terhadap server web menggunakan Kali Linux. Penelitian tersebut menggunakan pendekatan eksperimental, metode penelitian eksperimen termasuk dalam metode penelitian kuantitatif. Penelitian eksperimen merupakan satu-satunya tipe penelitian yang lebih akurat / teliti dibandingkan dengan penelitian lain, dalam menentukan relasi hubungan sebab akibat. Hal ini dikarenakan dalam penelitian eksperimen peneliti dapat melakukan pengawasan *(control)* terhadap variable bebas baik sebelum penelitian maupun selama penelitian. Melalui penelitian eksperimen ini peneliti mampu mengontrol kondisi kelompok eksperimen dan kelompok kontrol(Sumayyah et al. 2024). Metodologi penelitian merupakan suatu prosedur atau langkah sistematis yang dilakukan oleh peneliti dalam rangka implementasi, pengujian, dan evaluasi sistem keamanan jaringan. Metodologi penelitian ini memiliki gambaran rancangan penelitian yang meliputi

antara lain mulai dari persiapan lingkungan pengujian, konfigurasi sistem *Intrusion Detection System* berbasis *Wireshark*, simulasi serangan *DDoS SLOW HTTPS*, pengumpulan data packet capture dan analisis *traffic*, analisis efektivitas deteksi dan mitigasi(Ahmad Noor Alfinuha Shidiqqi Aldafian et al. 2025)

Dalam upaya untuk mengurangi dampak serangan DDoS, berbagai strategi pencegahan telah dikembangkan. Namun, seringkali diperlukan pengujian praktis untuk mengevaluasi efektivitas strategi pencegahan tersebut. Dalam penelitian ini, penggunaan sistem operasi Linux yang umum digunakan, seperti Kali Linux dan Linux Mint, dapat menjadi landasan yang tepat untuk melakukan uji coba pencegahan terhadap serangan DDoS. Kali Linux merupakan sebuah distribusi Linux yang terkenal sebagai alat untuk pengujian penetrasi dan keamanan. Kali Linux menyediakan beragam alat dan skrip yang dirancang khusus untuk mengevaluasi kerentanan sistem dan jaringan(Ruswandi et al. 2024)

Kali Linux digunakan sebagai sistem operasi utama dalam penelitian ini karena menyediakan lingkungan yang optimal untuk pengujian penetrasi dan keamanan siber. Sistem operasi ini dirancang khusus untuk kebutuhan profesional keamanan informasi, dengan koleksi alat yang sangat lengkap dan terintegrasi, seperti SlowHTTPTest, Wireshark, Nmap, Burp Suite, dan Metasploit Framework..(Sugiarto et al. 2025)

Wireshark, jaringan yang banyak digunakan Deteksi Penyusupan Jaringan Menggunakan Wireshark dan Machine alat analisis paket, dengan algoritme pembelajaran mesin yang canggih. Kemampuan Wireshark yang kuat untuk menangkap dan menganalisis data komunikasi jaringan menyediakan data yang kaya untuk mengidentifikasi kerentanan dan potensi gangguan. Dengan menggunakan model klasifikasi pembelajaran mesin seperti Random-Forest, K-NearestNeighbors, Naïve Bayes, Support vector machine, dan Gradient Boosting, model kami dirancang untuk meningkatkan kinerja dan efisiensi deteksi intrusi, memungkinkan peserta untuk secara proaktif mengidentifikasi dan memitigasi ancaman siber secara real-time.(Nmap and Metasploit 2025) Gunakan alat jaringan HPING3 untuk meluncurkan serangan DDoS. Sebuah aplikasi untuk jaringan bernama Hping3 memungkinkan pengiriman paket TCP/IP yang dipersonalisasi dan melihat balasan target. Alat ini sudah terpasang secara pre-installeddi Kali Linux. Hping3 dapat digunakan untuk berbagai keperluan seperti menguji aturan firewall, melakukan port scanning, dan menguji performa jaringan. Selain itu, hping3 juga dapat mengirim paket dengan kecepatan maksimal menggunakan opsi flood.(Nisa et al. 2024)

Serangan DDOS ini dapat memblokir atau bahkan menghentikan layanan sistem, sehingga pengguna yang sah tidak dapat menerima atau menerima layanan yang seharusnya. Bayangkan jika sebuah perusahaan perbankan tidak dapat memberikan pelayanan kepada nasabahnya, akibatnya bagi kelangsungan perusahaan sangat fatal. Atau penyedia internet yang tidak dapat menyediakan broadband kepada pelanggannya, tidak hanya mempengaruhi penyedia layanan tersebut,

HASIL

3.1. Penulisan Tabel

Pada tahap pengujian, dilakukan simulasi serangan Slowloris terhadap web server lokal yang dijalankan menggunakan *XAMPP* pada sistem operasi Windows. Serangan dilakukan melalui mesin virtual Kali Linux menggunakan skrip *Slowloris.py* dengan target alamat IP server 10.81.81.79. Sebelum serangan dijalankan, kondisi sistem diamati terlebih dahulu untuk memperoleh data dasar *(baseline)* seperti penggunaan *CPU*, memori, dan aktivitas jaringan. Hasil pengamatan awal menunjukkan bahwa penggunaan *CPU* berada di angka sekitar 20% dengan kecepatan prosesor rata-rata 2,89 GHz, dan aktivitas disk sebesar 33%. Lalu lintas jaringan yang tertangkap pada *Wireshark* juga menunjukkan kondisi normal tanpa adanya anomali paket *TCP* yang berulang.

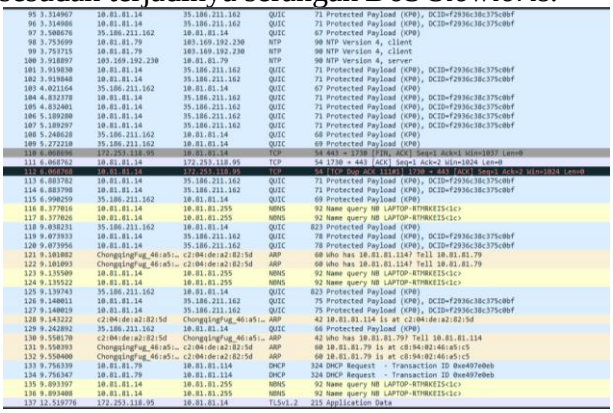
Setelah serangan Slowloris dijalankan, terjadi peningkatan signifikan pada kinerja sistem. Penggunaan *CPU* naik menjadi sekitar 52% dengan kecepatan prosesor meningkat hingga 3,37 GHz. Jumlah proses dan thread juga mengalami kenaikan akibat banyaknya koneksi palsu yang dikirim ke server. Berdasarkan hasil *capture Wireshark*, ditemukan banyak paket *TCP Duplicate ACK*, *Retransmission*, dan koneksi *SYN* yang menandakan adanya aktivitas serangan. Pola lalu lintas ini membebani server karena harus mempertahankan koneksi parsial tanpa menerima permintaan lengkap dari klien penyerang. Dengan demikian, hasil simulasi membuktikan bahwa serangan *Slowloris* dapat secara nyata menurunkan performa web server dengan meningkatkan beban *CPU* dan sumber daya sistem.

Parameter	Sebelum Serangan (Normal)	Sesudah Serangan (Slowloris)	Perubahan (Selisih)	Keterangan
CPU Utilization (%)	20%	52%	↑ 32 %	Kenaikan signifikan menunjukkan beban CPU meningkat akibat banyak koneksi/tuntutan
CPU Speed (GHz)	2.89 GHz	3.37 GHz	↑ 0.48 GHz	Frekuensi naik (boost) saat beban meningkat
Processes (jumlah)	248	258	↑ 10	Bertambahnya proses aktif pada saat serangan
Threads (jumlah)	3665	3814	↑ 149	Bertambah karena proses menangani koneksi
Handles (jumlah)	110472	115217	↑ 4745	Jumlah handle meningkat sejalan dengan thread/proses
Memory Used (GB)	13.6 / 15.3 GB (89%)	6.9 / 15.3 GB (45%)	↓ 6.7 GB (↓44%)	Perubahan nilai mungkin dikarenakan snapshot berbeda atau caching; mohon verifikasi sumber
Disk Activity (SSD %)	33%	2%	↓ 31 %	Disk activity menurun — beban lebih ke network/CPU daripada I/O disk
Wireshark: Paket TCP (contoh)	Normal: sedikit ACK/SYN	Banyak: Duplicate ACK, Retransmission, SYN/ACK floods	–	Capture menunjukkan banyak paket TCP duplicate dan retransmission selama serangan
Wireshark: Alamat Sumber/Tujuan	Traffic normal ke server publik	Sumber: 10.81.81.14 → Dest: 10.81.81.79 banyak koneksi	–	IP lokal terlihat mengirim banyak segmen yang menyebabkan server sibuk

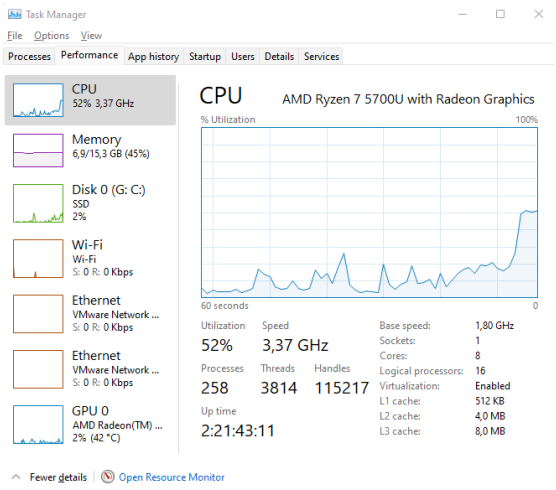
3.1 Gambar Tabel Peforma Cpu

3.2. Penggunaan Gambar

Gambar digunakan dalam penelitian ini sebagai bukti visual untuk memperjelas hasil pengujian sebelum dan sesudah terjadinya serangan *DoS Slowloris.*



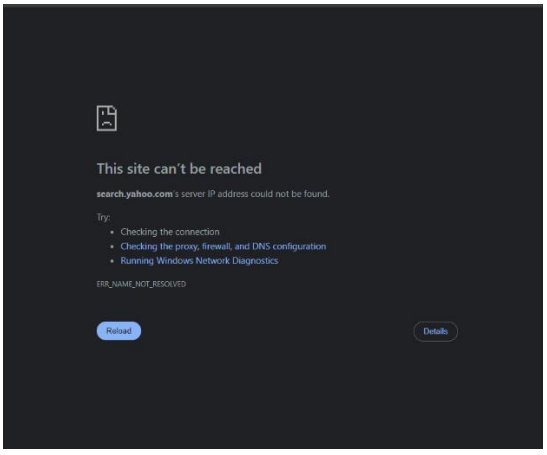
Gambar 3.1 *Before Wireshark DOS Slowloris*



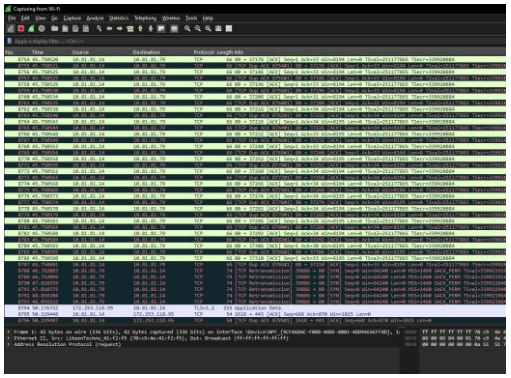
Gambar 3.2 (*Before CPU DOS Slowloris)*

Menunjukkan kondisi server ketika sistem masih berjalan normal tanpa adanya gangguan. Pada kondisi ini, tampilan *Task Manager* memperlihatkan penggunaan *CPU* yang stabil di sekitar 20%, dengan kecepatan prosesor sekitar 2,89 *GHz.* Aktivitas *disk* juga terlihat rendah, serta koneksi jaringan pada *Wireshark* menunjukkan lalu lintas data yang normal tanpa adanya anomali. Hal ini menandakan bahwa server dalam kondisi optimal dan mampu menangani permintaan pengguna dengan baik sebelum dilakukan serangan.

Setelah dilakukan simulasi serangan menggunakan *tools Slowloris* di Kali Linux, hasil pengujian visual ditampilkan pada



Gambar 3.3 *After Website DOS Slowloris*



Gambar 3.4 *(After Wireshark DOS Slowloris)*

Pada gambar 3.3 menunjukkan peningkatan signifikan pada penggunaan *CPU* hingga mencapai sekitar 52%, serta peningkatan kecepatan prosesor menjadi 3,37 *GHz* akibat beban koneksi palsu yang dikirim secara terus-menerus oleh penyerang. Sedangkan Gambar 3.4 hasil tangkapan *Wireshark* memperlihatkan banyak paket *TCP* yang berulang seperti *Duplicate ACK, Retransmission,* dan koneksi *half-open,* yang merupakan indikasi jelas dari serangan *Slowloris.* Dengan demikian, keempat gambar ini memperkuat analisis bahwa serangan Slowloris mampu membebani sumber daya server hingga menurunkan performa layanan web secara signifikan.

PEMBAHASAN

Hasil pengujian menunjukkan bahwa serangan *DoS Slowloris* mampu memengaruhi performa server secara signifikan. Setelah serangan dijalankan, terjadi peningkatan penggunaan *CPU* dan aktivitas jaringan yang cukup tinggi dibandingkan kondisi normal. Hal ini disebabkan karena metode *Slowloris* memanfaatkan kelemahan pada cara server menangani

koneksi *HTTP* yang terbuka, dengan terus mengirim permintaan sebagian *(partial request)* sehingga server harus mempertahankan banyak koneksi palsu dalam waktu lama.

Dampak dari kondisi tersebut adalah penurunan kemampuan server dalam merespons permintaan pengguna yang sah. Server menjadi lambat bahkan berpotensi tidak dapat diakses jika serangan dilakukan dalam waktu lama. Dengan demikian, penelitian ini membuktikan bahwa serangan *Slowloris* merupakan ancaman serius bagi server web yang tidak memiliki mekanisme perlindungan seperti *mod_evasive* atau *firewall* yang baik.

Denial of Service attack (DoS) merupakan bentuk ancaman penyerangan yang bertujuan untuk mengeksploitasi sebuah komputer ataupun server didalam jaringan internet dengan cara menghabiskan sumber dan melumpuhkan sistem yang dijadikan sasaran, sehingga sistem tersebut tidak dapat menyediakan berbagai servis yang diminta oleh pengguna. Dapat disimpulkan juga bahwa DoS memberhentikan suatu server atau sistem yang menyebabkan server atau sistem itu tidak berguna.(Ginting 2023).

Serangan DDoS (Distributed Denial of Service) pada jaringan skala besar dapat dikategorikan menjadi beberapa jenis, termasuk serangan pada layer aplikasi dan serangan volumetrik. Serangan DDoS layer aplikasi melibatkan penggunaan program atau alat yang dirancang untuk melancarkan serangan dengan tujuan membuat layanan atau sumber daya jaringan tidak tersedia bagi pengguna yang sah. Ini dicapai dengan membanjiri server target dengan trafik berlebihan yang mengakibatkan server tidak dapat menangani permintaan yang sah. Di sisi lain, serangan volumetrik DDoS bertujuan untuk membanjiri target dengan sejumlah besar data, sehingga target kewalahan dan tidak dapat melayani permintaan yang sah. (Rahman and Odja 2024) Dampak dari serangan DDoS ini dapat bermacam-macam salah satunya adalah tidak dapatnya mengakses sumber daya yang disediakan oleh web server, tentu hal tersebut menjadi sangat merugikan terutama bagi website pengelola media informasi.(Hasani and A 2024)

KESIMPULAN DAN SARAN

Berdasarkan hasil simulasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa serangan *Slowloris* memiliki dampak signifikan terhadap kinerja web server. Serangan ini menyebabkan peningkatan penggunaan *CPU*, bertambahnya jumlah proses dan thread, serta munculnya anomali paket *TCP* seperti *Duplicate ACK* dan *Retransmission.* Kondisi tersebut membebani sumber daya server dan dapat mengakibatkan penurunan kecepatan respon hingga server *downtime.* Dengan demikian, penelitian ini berhasil menunjukkan bahwa *Slowloris* termasuk jenis serangan *DoS* yang efektif dalam mengganggu stabilitas layanan web.

Untuk meminimalkan risiko serangan *Slowloris*, administrator server disarankan untuk menerapkan konfigurasi keamanan tambahan seperti penggunaan modul *mod_evasive* atau *mod_reqtimeout* pada *Apache*, serta pengaturan firewall untuk membatasi koneksi yang mencurigakan. Selain itu, pemantauan performa server secara berkala dan analisis lalu lintas jaringan menggunakan tools seperti Wireshark juga penting dilakukan agar potensi serangan dapat terdeteksi lebih dini. Penelitian selanjutnya dapat memperluas analisis dengan membandingkan efektivitas berbagai teknik mitigasi terhadap serangan *DoS* lainnya, sehingga hasilnya dapat menjadi acuan dalam meningkatkan keamanan server web secara menyeluruh.

DAFTAR PUSTAKA

Ahmad Noor Alfinuha Shidiqqi Aldafian, Muhlis Tahir, Moch Ersa Noer Firmansyah, and Siti Nur Khofifah. 2025. “Implementasi Implementasi IDS Wireshark Untuk Deteksi Serangan DDoS SLOW HTTPS Di Kali Linux.” *Jurnal RESTIKOM : Riset Teknik Informatika dan Komputer* 7(2): 148–61.

Arifin, M. Zainal, Ema Utami, and Eko Pramono. 2020. “Perancangan Sistem Deteksi Dini Bencana Banjir Menggunakan Teknik Pengiriman DTMF Berbasis Modul RF 433 Mhz

Dan Arduino." *Jurnal Teknologi Informasi dan Komunikasi (TIKomSiN)* 8(2).
Dorthea Elvita Harefa et al. 2025. "Analisis Dampak Serangan Ddos Tipe Slowloris Pada Infrastruktur Jaringan Lokal." *Jurnal Sistem Informasi dan Teknologi Informasi* 7(2): 743–52.
Fachri, Fahmi. 2023. "OPTIMASI KEAMANAN WEB SERVER TERHADAP SERANGAN BRUTE-FORCE MENGGUNAKAN PENETRATION TESTING OPTIMIZING WEB SERVER SECURITY FOR BRUTE-FORCE ATTACKS USING." 10(1): 51–58.
Ginting, Erwin. 2023. "UNES Journal of Information System." 8(1): 9–19.
Haniyah, Wanda et al. 2024. "Simulasi Serangan Denial of Service (DoS) Menggunakan Hping3 Melalui Kali Linux." (2): 1–8.
Harefa, Dorthea Elvita et al. 2025. "Analisis Dampak Serangan Ddos Tipe Slowloris Pada Infrastruktur Jaringan Lokal." 7(2): 743–52.
Hasani, Fikri Rizqillah, and R Yadi Rakhman A. 2024. "Pencegahan Serangan DDOS Syn Flood Terhadap Web Server."
Nisa, Afifah Rodhiyatun et al. 2024. "Analisis Log Server Untuk Mendeteksi Serang DDoS Pada Keamaan Jaringan Di Website." (3): 1–17.
Nmap, Penggunaan, and D A N Metasploit. 2025. "KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI." 9(1): 1188–96.
Noor, Ahmad et al. 2025. "Implementasi IDS Wireshark Untuk Deteksi Serangan DDoS SLOW HTTPS Di Kali Linux." 7(2): 148–61.
Rafid, Muhammad, Habibi Tambunan, and Shelvie Nidya Neyman. 2024. "Implementasi Firewall Pada Linux Untuk Pencegahan Dari Serangan DoS." (4): 1–10.
Rahman, Rakhmadi, and Ghina R S Odja. 2024. "Technology Sciences Insights Journal." d.
Ruswandi, Keinanjung et al. 2024. "Strategi Pencegahan Efektif Terhadap Serangan DDoS Slowloris Menggunakan Kali Linux Dan Linux Mint." (4): 1–11.
Safitrah, Tiara, Antonio Banggas Gregory Sinaga, Muhammad Alghifari, and Shelvie Nidya Neyman. 2024. "Pengaruh Serangan Slow HTTP DoS Terhadap Layanan Web: Studi Eksperimental Dengan Slowhttptest." *Journal of Technology and System Information* 1(4): 11.
Sugiarto, Bambang et al. 2025. "PENGUJIAN KEAMANAN WEB TERHADAP SERANGAN." 15(2).
Sumayyah, Zata Ismah, Silva Dimas Surya Permana, Muhammad Tsabit, and Aep Setiawan. 2024. "Penerapan Dan Mitigasi Teknik Slowloris Dalam Serangan Distributed Denial-of-Service (DDos) Terhadap Website Ilegal Dengan Kali Linux." *Journal of Internet and Software Engineering* 1(2): 14.
Della Yunika Zebua et al. 2025. "Simulasi Serangan DOS Menggunakan SLOWHTTPTEST." *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)* 4(2): 409–19.
Zidane, Muamar. 2022. "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) Menggunakan Metode Data Mining Naïve Bayes." 6(1): 172–80.