Journal of Internet and Software Engineering Vol: 1, No 2, 2024, Page: 1-14

Penerapan dan Mitigasi Teknik Slowloris dalam Serangan *Distributed Denial-of-Service* (DDos) terhadap Website Ilegal dengan Kali Linux

Zata Ismah Sumayyah*, Silva Dimas Surya Permana, Muhammad Tsabit, Aep Setiawan

Teknologi Rekayasa Komputer, Sekolah Vokasi, IPB University

Abstrak: Keamanan teknologi informasi sangat penting untuk melindungi data yang dikirim atau disimpan di internet dari pihak yang tidak bertanggung jawab. *Hacker* dan *cracker* dapat mengakses internet dan melakukan penyusupan yang merugikan pemilik server dan jaringan komputer. Mereka menggunakan berbagai jenis serangan jaringan komputer dengan *tools* yang dibuat mandiri atau tersedia di pasar. Ancaman keamanan siber yang semakin kompleks, seperti serangan *Denial-of-Service* (DoS) dan *Distributed Denial-of-Service* (DDoS), bertujuan membuat layanan online tidak dapat diakses oleh pengguna yang sah dengan membanjiri sistem dengan lalu lintas berlebihan. Penelitian ini mengeksplorasi penerapan dan mitigasi teknik *Slowloris*, sebuah varian efektif dari serangan DDoS, terhadap *website* ilegal menggunakan Kali Linux. Eksperimen dilakukan di lingkungan pengujian terkontrol untuk melancarkan serangan *Slowloris* dan mengevaluasi teknik mitigasi. Hasil menunjukkan bahwa serangan *Slowloris* mengganggu kinerja server, namun dapat diidentifikasi melalui pola lalu lintas jaringan. Beberapa teknik mitigasi, seperti pengaturan batas koneksi server dan *firewall* aplikasi web, efektif mengurangi dampak serangan. Kesimpulan menyatakan bahwa pemahaman teknik serangan dan strategi mitigasi penting untuk meningkatkan keamanan jaringan.

Kata Kunci: *DDoS (Distributed Denial-of-Service), Kali Linux, Keamanan Jaringan, Mitigasi Serangan, Slowloris.*

DOI: https://doi.org/10.47134/pjise.v1i2.2694
*Correspondence: Zata Ismah Sumayyah
Email: sumayyahzata@apps.ipb.ac.id

Received: 01-02-2024
Accepted: 15-03-2024
Published: 31-04-2024

Abstract: *Information technology security is very important to protect data sent or stored on the internet from irresponsible parties. Hackers and crackers can access the internet and infiltrate servers and computer network owners. They use various types of computer network attacks with tools that are made independent or available in the market. Increasingly complex cybersecurity threats, such as Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, aim to make online services inaccessible to legitimate users by flooding systems with excessive traffic. This research explores the application and mitigation of the Slowloris technique, an effective variant of DDoS attacks, against illegal websites using Kali Linux. Experiments are conducted in a controlled testing environment to launch Slowloris attacks and evaluate mitigation techniques. Results show that Slowloris attacks disrupt server performance, but can be identified through network traffic patterns. Some mitigation techniques, such as setting server connection limits and web application firewalls, effectively reduce the impact of attacks. The conclusion states that understanding attack techniques and mitigation strategies is important to improve network security.*

Keywords: *Cybersecurity, DDoS (Distributed Denial-of-Service), Kali Linux, Attack Mitigation, Slowloris.*

Pendahuluan

Jaringan komputer adalah kumpulan komputer yang berkomunikasi satu sama lain dan berbagi data dan informasi melalui protokol komunikasi global. Internet juga dapat didefinisikan sebagai jaringan komputer dalam arti luas, yang melibatkan pemerintah, media, pendidikan, dan sektor keuangan (Prihantoro *et al.* 2021). Jaringan komputer menjadi sumber daya bersama yang digunakan oleh banyak aplikasi yang mewakili kepentingan berbeda,

Perkembangan jaringan komputer terjadi dengan sangat pesat, baik dalam bidang komersial, akademis instalasi dan di rumah-rumah masyarakat yang kini membutuhkan dan menggunakan akses internet. Oleh karena itu, internet tidak hanya diakses oleh pelajar, namun *hacker* dan *cracker* juga bisa mengakses internet (Sudewo *et al.* 2023). Keamanan informasi dan jaringan saat ini sangat penting untuk dilakukan, alasannya tidak lain dan tidak bukan karena pada era ini penyimpanan informasi tidak lagi menggunakan media konvensional seperti kertas, akan tetapi telah menggunakan teknologi komputer yang maju yang dipadukan dengan kecanggihan dari internet (Dwiyatno *et al.* 2019).

Hal ini dilakukan untuk memastikan bahwa setiap informasi yang dikirim atau disimpan melalui internet aman dari pihak yang tidak bertanggung jawab. Internet dapat diakses oleh semua orang, termasuk *hacker* dan *cracker*. Mereka melakukan penyusupan tanpa alasan yang jelas, dapat merugikan pemilik server dan jaringan. Mereka melakukan serangan jaringan komputer dengan berbagai alat yang dibuat sendiri atau dijual. Pengetahuan tentang penyusupan jaringan komputer berbeda dengan kecanggihan serangan dan alat jaringan (Jaya *et al.* 2020). Dalam beberapa tahun terakhir, jumlah serangan-serangan melalui internet telah meningkat. Pola dan target serangan sangat beragam dengan keluarnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Undang-Undang Telekomunikasi, pengelola sistem merasa lebih nyaman karena tindakan yang dilakukan oleh pelaku dapat mengakibatkan konsekuensi hukum. Teknologi komputer berbasis jaringan telah membuat aktivitas online seperti mengirim data atau hanya mengakses media online sangat mudah (Zulkifli *et al.* 2018).

Berdasarkan analisis data sistem *monitoring traffic* ID-SIRTII (*Indonesia Security Incident Response Team On Internet Infrastructure*), tercatat bahwa insiden serangan siber di Indonesia mencapai satu juta dan terus meningkat akibat kelemahan sistem dan aplikasi (Chotimah 2019). Keamanan siber di Asia Tenggara masih jauh dari sempurna dan berdampak signifikan terhadap perkembangan ekonomi digital di ASEAN. Pada tahun 2025, ekonomi digital ASEAN diperkirakan mencapai 102 miliar dolar AS (E-Trade for All, 2018), dengan keuntungan sebesar 20 miliar dolar AS pada tahun 2018 (ASEAN-UP, 2019). Serangan siber di Asia Tenggara dapat menyebabkan disrupsi terhadap perekonomian digital. Oleh karena itu, negara-negara ASEAN tidak bisa mengabaikan ancaman ini (Ramadhan 2020).

Di balik kemajuan ini, terdapat ancaman keamanan siber yang semakin kompleks dan berbahaya. DDoS, yang melakukan serangan dalam jumlah besar dan terus meningkat hingga *terabyte*, adalah salah satu serangan yang paling berbahaya dan menantang. Serangan DDoS memiliki tujuan utama menurunkan kinerja server secara signifikan karena

server menjadi kewalahan untuk menerima banyak permintaan palsu, menyebabkan kemacetan total. DDoS menyebabkan kerusakan yang sangat besar dan menembus lapisan aplikasi dan jaringan-jaringan komputer, mengancam web server (Suharti *et al.* 2022).

Keamanan data pengguna adalah elemen penting yang harus diperhatikan dan dapat digunakan sebagai ukuran kualitas situs web. Beberapa faktor kualitas mempengaruhi kualitas konten *website*; contohnya, kualitas informasi dapat menggambarkan kualitas konten. Menurut Endang Supriyati, tiga faktor mempengaruhi kualitas website: kualitas sistem, kualitas layanan, dan kualitas informasi (Andria 2020). Meskipun serangan DDoS ini merupakan serangan yang relatif sederhana, namun dampak dan tindakan penanggulangannya tidak boleh dianggap remeh.

Di beberapa wilayah, serangan yang ditujukan hanya untuk memperlambat server mungkin merupakan hal yang normal dan tidak berdampak nyata pada organisasi atau bisnis Anda. Namun, hal ini berbeda dengan area yang fokus pada layanan pelanggan dan kepuasan dalam menggunakan server yang ada. Tentu saja serangan seperti DDoS bisa sangat mematikan bagi bisnis/organisasi. Serangan DDoS memiliki banyak varian, semuanya dengan tujuan yang sama yaitu menyebabkan penolakan layanan karena server/host yang diserang tidak lagi memiliki sumber daya untuk menerima permintaan (Server *et al.* 2023).

Serangan *Distributed Denial-of-Service* (DDoS) adalah serangan yang membanjiri jaringan dengan paket atau permintaan yang merusak server dan sistem. Sistem jaringan yang semakin berkembang memiliki lebih banyak pengguna. Akibatnya, sangat sulit untuk membedakan antara pengguna legal dan peretas. Selain itu, ada peningkatan dalam teknologi yang digunakan untuk melakukan serangan DDos. Beberapa jenis serangan DDoS adalah *ICMP flood*, *SYN flood*, dan *IP packet flood*, antara lain. Mengidentifikasi serangan DDoS menjadi lebih sulit karena ada berbagai jenis strategi (Zidane 2022).

Serangan *Distribute Denial of Service* (DDoS) *Slowloris* adalah salah satu jenis serangan yang paling sering terjadi yang berfokus pada mengganggu ketersediaan layanan. Serangan seperti itu dapat datang dalam berbagai bentuk, seperti serangan fisik terhadap sistem IT, melebihi kapasitas koneksi jaringan, atau menggunakan kelemahan aplikasi. Sebagian besar serangan *Cyber* ditujukan untuk mengganggu keamanan dengan membajak data dan informasi penting (Gera dan Battula 2018).

Serangan yang akan dilakukan dalam penelitian ini akan dilakukan melalui *Virtual Machine* (VM). *Virtual Machine* (VM) adalah perangkat lunak untuk implementasi komputer dan menjalankan program seperti *host* pada komputer, dan VM menggunakan sumber daya fisik dari komputer *host*. Alasan menggunakan VM adalah agar menjadi lebih mudah untuk menerapkan serangan DDOS yang membutuhkan banyak *host* (Santoso *et al.* 2022). Program yang paling penting dalam sistem komputer adalah sistem operasi. Bisa dianggap sebagai program kontrol yang bertanggung jawab untuk menjalankan program-program lain yang ada dalam komputer. membuat sistem operasi (OS) mesin lebih mudah bagi *programmer* untuk bekerja dengan perangkat keras (Abhilash dan V 2015).

Penggunaan Kali Linux sebagai platform untuk melaksanakan dan menganalisis serangan *Slowloris* menambah dimensi penting pada riset ini. Kali Linux menyediakan berbagai alat keamanan dan penestingan yang terintegrasi yang dapat digunakan untuk

memfasilitasi simulasi serangan ini dalam lingkungan yang terkontrol. Hal ini memungkinkan para peneliti untuk tidak hanya memahami dan mendemonstrasikan cara kerja serangan *Slowloris*, tetapi juga menguji dan mengembangkan strategi mitigasi yang efektif.

Penelitian ini berfokus pada penerapan dan mitigasi teknik *Slowloris* dalam serangan DDoS terhadap *website* ilegal menggunakan Kali Linux. Tujuan dari penelitian ini adalah untuk memahami bagaimana serangan *Slowloris* dapat dilancarkan dan diidentifikasi, serta untuk mengevaluasi berbagai teknik mitigasi yang dapat digunakan untuk melindungi server dari serangan semacam itu. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang berarti bagi upaya meningkatkan keamanan jaringan dan melindungi sistem dari ancaman serangan DDoS.

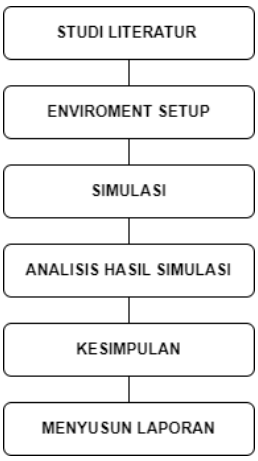
Metode

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.

Fraenkel dan Wallen menyatakan bahwa keunikan penelitian eksperimen adalah satu-satunya tipe penelitian yang memberi kesempatan kepada peneliti untuk secara langsung dapat mempengaruhi *variable* penelitian dan satu-satunya pula tipe penelitian yang dapat menguji hipotesis tentang relasi hubungan sebab akibat (Akbar *et al.* 2023).

Metode penelitian yang digunakan dalam Penerapan dan Mitigasi Teknik *Slowloris* Dalam Serangan *Distributed Denial-of-Service* (DDos) terhadap *Website* Ilegal Dengan Kali Linux ini adalah studi kepustakaan (*library study*) dan penelitian eksperimental (*experimental research*).

Adapun tahapan proses penelitian secara sistematis dapat dilihat pada Gambar 1 berikut.



Gambar 1. Tahap Penelitian

Berdasarkan tahapan penelitian yang ada pada **Gambar 1**, dapat diuraikan sebagai berikut:

A. Studi Literatur

Studi literatur adalah jenis penelitian yang menggunakan kumpulan informasi dan data dari berbagai sumber, seperti dokumen, buku, artikel, majalah, berita, dan sebagainya. Studi literatur mencakup pengumpulan bahan referensi yang relevan dengan tujuan penelitian, penggunaan teknik pengumpulan data kepustakaan, dan integrasi dan presentasi data (Idhartono 2020).

Tahap pertama dalam penelitian ini adalah studi literatur, pada tahap ini kami melakukan studi literatur sebagai melakukan kajian literatur yang mendalam mengenai serangan DDoS, khususnya teknik *Slowloris*, dan penggunaan Kali Linux sebagai *platform* untuk simulasi serangan dan penelitian keamanan siber. Ini termasuk penelitian sebelumnya, buku, jurnal, dan sumber online yang relevan.

B. Enviroment SetUp

Pada dasarnya tahap *environment setup* adalah untuk memastikan bahwa environment test yang akan dijalankan baik *hardware* maupun *software*, berjalan sesuai dengan rencana. Fase ini juga dapat dilakukan bersamaan dengan *fase test case development*. Fase ini merupakan fase independen atau tidak terikat dengan fase yang lain (Gusti *et al.* 2021).

Dalam penelitian ini, membangun infrastruktur simulasi yang memadai adalah langkah penting untuk menyimulasikan serangan Slowloris terhadap server web. Infrastruktur ini harus memungkinkan peneliti untuk melakukan serangan dalam lingkungan yang terkendali dan memonitor dampaknya secara detail.

1. Perangkat Keras

Sediakan beberapa mesin fisik atau virtual yang akan digunakan sebagai server target dan mesin penyerang. Minimal satu mesin untuk server target dan satu mesin untuk penyerang. Spesifikasi minimum untuk mesin: CPU 2-core, RAM 4GB, dan penyimpanan 20GB.

2. Perangkat Lunak

Instalasi sistem operasi yang relevan pada setiap mesin. Server target akan menjalankan distribusi Linux yang umum digunakan seperti Ubuntu Server atau CentOS. Instalasi Kali Linux pada mesin penyerang untuk digunakan dalam simulasi serangan.

3. Serta menyiapkan web illegal yang akan menjadi pengujian untuk melakukan penyerangan *teknik slowloris*.

C. Pengujian (Simulasi Serangan)

Simulasi adalah sebagai suatu model sistem dimana komponennya di presentasikan oleh prosesor prosesor aritmatika dan logika yang di jalankan komputer untuk memperkirakan sifat sifat dinanamis sistem tersebut (Hery *et al.* 2020).

Pelaksanaan simulasi serangan merupakan tahap penting dalam penelitian ini untuk memahami dampak serangan *Slowloris* terhadap server web dan mengevaluasi efektivitas strategi mitigasi. Proses ini dimulai dengan memastikan bahwa semua

komponen infrastruktur simulasi telah diatur dan berfungsi dengan baik. Mesin penyerang yang menjalankan Kali Linux dan mesin target yang menjalankan server web (baik Apache maupun Nginx) harus berada dalam kondisi siap untuk menjalani pengujian.serangan Slowloris akan dilaksanakan dengan menggunakan alat yang telah diinstal pada Kali Linux. Hasil dari simulasi serangan ini akan digunakan untuk mengembangkan dan menguji strategi mitigasi. Strategi-strategi ini akan diuji dalam kondisi yang sama untuk menilai efektivitasnya dalam mengurangi dampak serangan Slowloris.

D. Analisis Hasil Simulasi

Seringkali, analisis dilakukan untuk sampai pada kesimpulan tentang bagaimana kegiatan tersebut dilakukan. Analisis, menurut Kamus Besar Bahasa Indonesia, adalah proses penyelidikan dan penguraian suatu masalah untuk mengetahui keadaan sebenarnya dan proses pemecahan masalah yang dimulai dengan dugaan dan kebenarannya (Magdalena *et al.* 2020).

Menganalisis data yang dikumpulkan untuk menilai dampak serangan *Slowloris* pada kinerja server. Membandingkan kinerja server selama serangan dengan kondisi normal untuk mengidentifikasi penurunan kinerja yang signifikan.

E. Kesimpulan

Penarikan kesimpulan atau verifikasi adalah salah satu metode analisis data kualitatif adalah penarikan kesimpulan; hasilnya adalah dasar untuk tindakan (Engko dan Usmany 2020). Penarikan kesimpulan dan verifikasi dalam penelitian ini akan menjelaskan efektivitas berbagai teknik mitigasi terhadap serangan *Slowloris* yang dilancarkan pada *website* ilegal menggunakan Kali Linux. Setelah menjalankan simulasi serangan dan mengamati dampaknya terhadap kinerja server, penelitian ini akan mengevaluasi berbagai strategi mitigasi, seperti pengaturan batas koneksi server, penggunaan *firewall*, dan penerapan perangkat lunak khusus

F. Menyusun Laporan

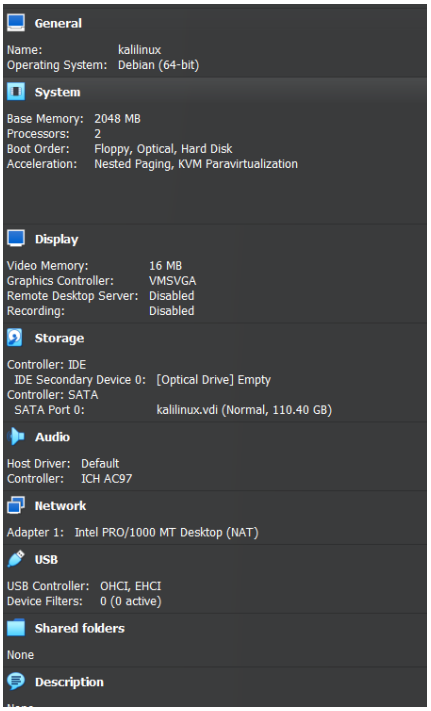
Menyusun laporan adalah langkah terakhir dalam proses penelitian, yang merupakan gambaran menyeluruh dari proses penelitian secara keseluruhan. Dalam proses ini, peneliti menggabungkan hasil penelitian dengan temuan literatur, serta rencana penelitian sebagai hasil dari uji coba dan evaluasi. Proses persiapan laporan melibatkan analisis menyeluruh data yang dikumpulkan, memilih struktur informasi yang logis, dan menulis laporan dengan cara yang jelas dan ringkas (Mayasari 2021).

Hasil dan Pembahasan

A. Membangun Infrastruktur Simulasi

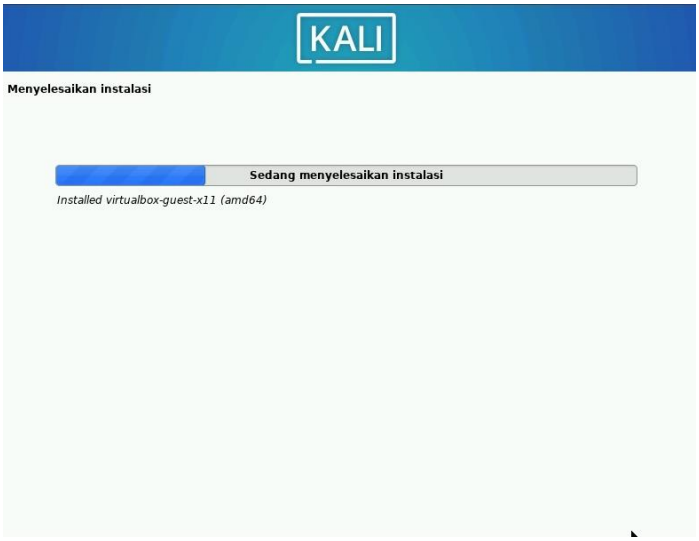
Dalam penelitian ini, digunakan perangkat komputer dengan sistem operasi Kali Linux 64-bit. Tahap awal penelitian melibatkan pembuatan mesin virtual baru untuk menginstal sistem operasi Kali Linux. Kali Linux digunakan sebagai platform utama untuk melancarkan serangan *Slowloris*. Kali Linux, sebagai distribusi Linux yang dirancang

khusus untuk pengujian penetrasi dan keamanan siber, menyediakan berbagai alat dan utilitas yang diperlukan untuk mengimplementasikan serangan tersebut.



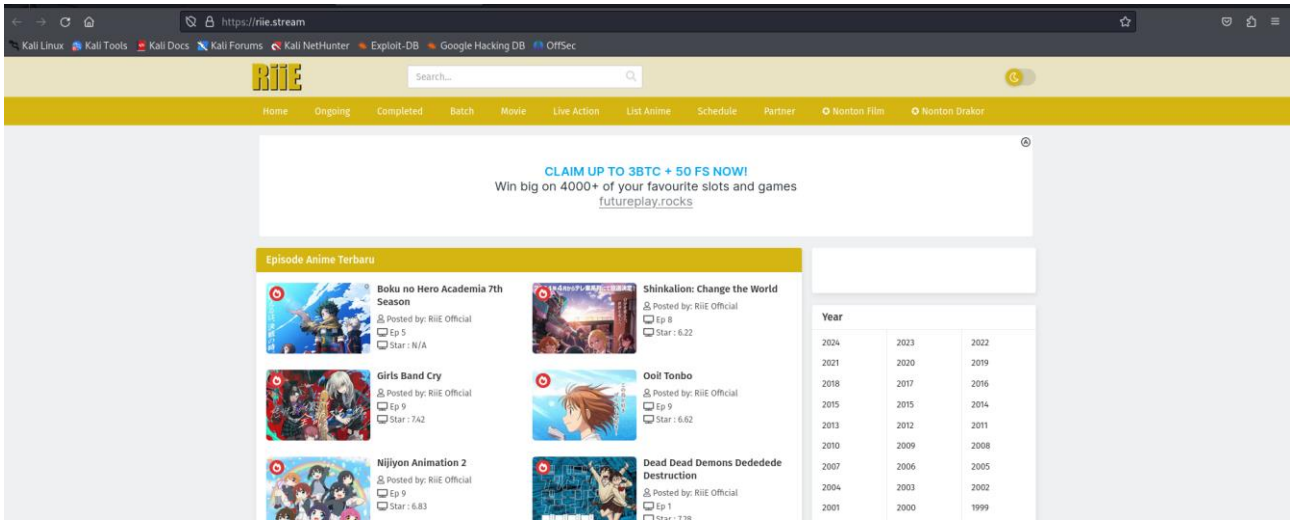
Gambar 2. Virtual Mesin Kali Linux

Setelah itu, tahap selanjutnya adalah melakukan instalasi Kali Linux pada mesin virtual tersebut.



Gambar 3. Proses Instalasi Kali Linux

Setelah itu, penelitian ini melanjutkan dengan menyiapkan *website* ilegal yang akan menjadi target pengujian untuk serangan teknik *Slowloris*.



Gambar 4. Tampilan *Website* Riie.Stream

Website ilegal yang digunakan dalam pengujian ini adalah situs *streaming* ilegal bernama riie.stream. Ilegal dalam arti luas menurut Kamus Besar Bahasa Indonesia (KBBI) yaitu tidak sah, tanpa hak, tanpa izin, tidak menurut hukum. Sedangkan pengertian ilegal konten adalah sebuah informasi yang diunggah di internet tetapi dianggap melanggar hukum dan dapat merugikan beberapa pihak yang terlibat (Handariyanti *et al.* 2023).

Memilih *website* ilegal sebagai sasaran pengujian dalam penelitian ini didasarkan pada beberapa pertimbangan penting. Pertama, dari segi etika dan legalitas, menyerang *website* yang sah dapat menimbulkan konsekuensi hukum dan moral yang serius, termasuk pelanggaran hukum dan kerugian bagi pihak yang tidak bersalah. *Website* ilegal, seperti situs *streaming* yang melanggar hak cipta, sudah berada dalam domain yang tidak sah, sehingga risiko etika dan legalitas dapat diminimalisir. Kedua, relevansi penelitian menjadi alasan kuat, karena fokus penelitian ini adalah pada efektivitas teknik Slowloris dalam serangan *Distributed Denial-of-Service* (DDoS). Menggunakan *website* ilegal memberikan konteks yang lebih nyata dan relevan untuk menguji dan mengevaluasi teknik serangan dan mitigasi dalam situasi yang mungkin sering terjadi. Ketiga, aspek keamanan juga menjadi pertimbangan, karena menguji serangan DDoS pada jaringan atau server yang sah dapat menyebabkan gangguan layanan yang tidak diinginkan. Dengan memilih *website* ilegal sebagai target, penelitian dapat menghindari dampak negatif terhadap layanan legal dan pengguna yang sah. Terakhir, penggunaan *website* ilegal memungkinkan penelitian untuk mengevaluasi teknik mitigasi dalam skenario dunia nyata yang lebih relevan dengan ancaman aktual, sehingga memberikan hasil yang lebih akurat dan aplikatif.

B. Melakukan Simulasi Serangan

Pada bagian ini, akan dibahas secara mendetail mengenai proses simulasi penyerangan menggunakan teknik *Slowloris* terhadap *website* ilegal yang telah dipilih sebagai target. Kami menggunakan *repository Slowloris* yang tersedia di GitHub, dan kami memulai dengan mengkloning *repository* dengan perintah **git clone**, seperti yang ditunjukkan pada **Gambar 5.**

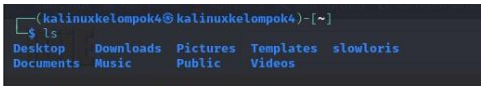
Gambar 5. Proses *Cloning Repository*

menunjukkan perintah yang dijalankan pada terminal Linux untuk mengkloning *repository Slowloris* dari GitHub menggunakan perintah **git clone**. Berikut penjelasan perintah pada gambar 5.

G. **git clone**: Perintah ini digunakan untuk mengkloning (menyalin) *repository* dari server GitHub ke mesin lokal.
H. **https://github.com/gkbrk/slowloris**: URL ini adalah lokasi *repository Slowloris* di GitHub.

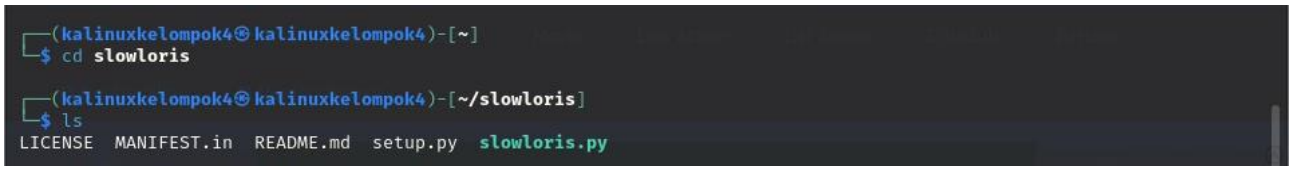
Status dan Statik menunjukkan **100% (152/152), 25.90 KiB | 1.13 MiB/s, done**, menunjukkan bahwa seluruh objek (152 objek) telah diterima, dengan total data yang diunduh sebesar 25.90 KiB pada kecepatan 1.13 MiB/s dan Resolving deltas, menunjukkan 100% (80/80). Keseluruhan proses pada tampilan **Gambar** 5, memastikan bahwa *repository* Slowloris dari GitHub berhasil dikloning ke sistem lokal, memungkinkan pengguna untuk mengakses dan menggunakan kode sumber dari proyek *Slowloris*.

Pada **Gambar 6** menunjukkan perintah **ls** yang digunakan untuk menampilkan daftar isi direktori *home*, menunjukkan bahwa direktori *slowloris* telah dikloning.



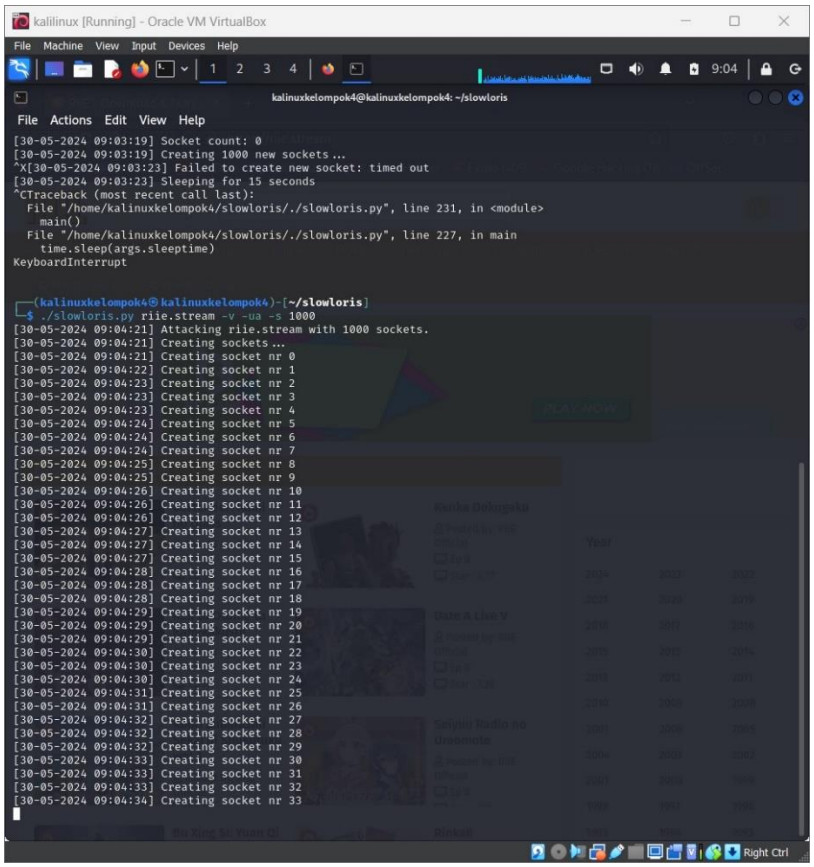
Gambar 6. Menampilkan Isi Direktori

Perintah selanjutnya pada Gambar 7, Perintah **cd slowloris** digunakan untuk berpindah ke direktori *slowloris* yang berisi file dan skrip yang diperlukan untuk serangan *slowloris*. Lalu perintah selanjutnya berfungsi untuk menampilkan daftar file dalam direktori *slowloris*, termasuk **slowloris.py**.



Gambar 7. Menampilkan Isi Direktori *Slowloris*

Selanjutnya melakukan tahapan yang paling penting, yaitu menjalankan serangan *Slowloris*. Bisa dilihat pada **Gambar 8** menunjukkan serangan *Slowloris* yang dilakukan terhadap *website* ilegal riie.stream.



Gambar 8. Menampilkan Proses Penyerangan

Perintah yang dijalankan ./slowloris.py riie.stream -v -ua -s 1000, berikut penjelasan fungsi dari perintah tersebut.

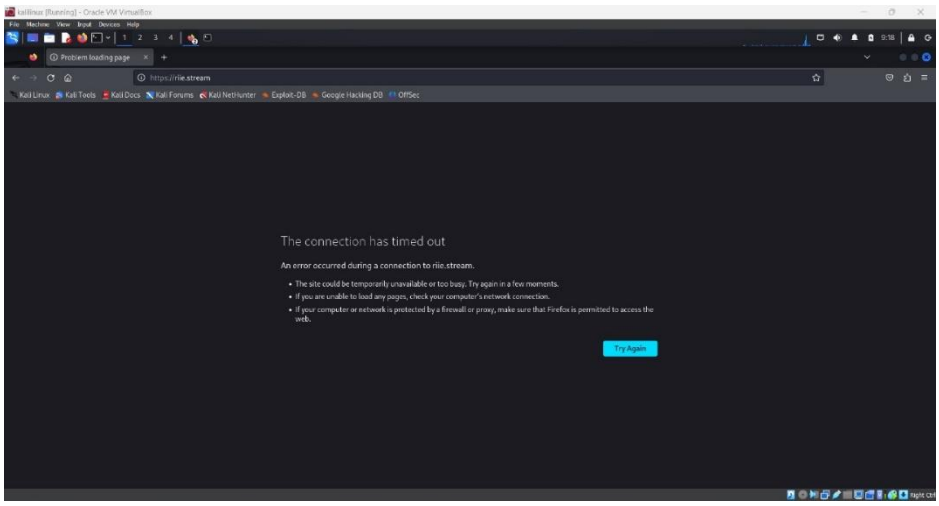
- **./slowloris.py**: Menjalankan skrip Python slowloris.py.
- riie.stream: Nama domain dari *website* target serangan.
- **-v**: Mode verbose untuk menampilkan output lebih detail selama serangan.
- **-ua**: Menambahkan *header User-Agent* acak dalam permintaan HTTP untuk menyimulasikan berbagai jenis klien.
- **-s 1000**: Menentukan jumlah soket yang akan dibuka oleh Slowloris untuk melakukan serangan, dalam hal ini 1000 soket.

Output serangan yang dihasilkan adalah **Attacking riie.stream with 1000 sockets** menandakan mulainya serangan terhadap alamat domain target dengan 1000 soket., **Creating sockets** berguna untuk membuka soket untuk mengirim permintaan HTTP parsial dan *output* serangan terakhir adalah **Creating socket nr X** menunjukkan pembukaan soket satu per satu, di mana X adalah nomor soket yang sedang dibuka. Hingga gambar terakhir, ada 33 soket yang telah berhasil dibuka. Proses ini menunjukkan bahwa skrip *Slowloris* mencoba membuka banyak koneksi (soket) ke server riie.stream dengan tujuan menghabiskan sumber daya server tersebut dan membuatnya tidak responsif. Dengan menggunakan 1000 soket, serangan ini bertujuan untuk membebani server dan menyebabkan gangguan layanan yang signifikan, menguji efektivitas teknik *Slowloris* dalam melakukan serangan DDoS.

Setelah itu, menunggu metode *Slowloris* bekerja dengan mengirimkan sejumlah besar permintaan HTTP ke server web riie.stream. Hal ini akan menyebabkan server menjadi kewalahan dan tidak dapat merespons permintaan lainnya. Akibatnya, *website* riie.stream menjadi tidak dapat diakses karena semua koneksi HTTP penuh oleh permintaan yang dikirimkan secara terus-menerus.

C. Analisis Hasil Simulasi

Melakukan analisis dan hasil simulasi pada **Gambar 9**, kami melakukan serangan Slowloris terhadap *website* riie.stream menggunakan Kali Linux. Serangan ini mengirimkan sejumlah besar permintaan HTTP parsial secara terus-menerus untuk menjaga koneksi tetap terbuka dan memakan sumber daya server. Hal ini ditunjukkan dengan pesan "*The connection has timed out*" yang muncul pada layar. Pesan tersebut mengindikasikan bahwa perangkat tidak dapat terhubung ke server *website* yang ingin diakses dan menunjukkan bahwa setelah beberapa saat, server riie.stream menjadi kewalahan dan tidak mampu merespons permintaan lain.



Gambar 9. Menampilkan *Website Down*

Hal ini menyebabkan situs tersebut tidak dapat diakses oleh pengguna lain. Indikator keberhasilan serangan ini terlihat dari peningkatan signifikan dalam waktu respons *server* dan akhirnya ketidakmampuan server untuk memproses permintaan baru. Pengamatan ini menegaskan efektivitas teknik *Slowloris* dalam menyebabkan *Distributed Denial-of-Service* (DDoS) pada target, khususnya pada server web yang tidak memiliki perlindungan yang memadai terhadap jenis serangan ini. Hasil simulasi ini juga memberikan wawasan penting tentang perlunya implementasi mitigasi dan keamanan yang lebih kuat pada server web untuk mencegah serangan serupa di masa depan.

D. Implementasi Mitigasi dalam Serangan Slowloris

Untuk mengatasi *website* yang telah terkena serangan DDos slowloris. Berikut adalah beberapa strategi yang dapat diterapkan:

1. Melakukan analisis serangan DDos dengan memantau trafik jaringan dan **pemeriksaaan log server**, dengan cara mencari aktivitas mencurigakan seperti

peningkatan tiba-tiba dalam koneksi ke server dan pola permintaan yang aneh dari alamat ip yang sama.

2. Apabila *website* dibuat dengan **menggunakan Nginx** bisa mengubah pengaturan seperti **client_body_timeout**, **client_header_timeout**, dan **keepalive_timeout** untuk memutus koneksi yang tidak aktif lebih cepat. Berikut contoh *source code* yang digunakan:

```
http {
    ...
    client_body_timeout 10s;       # Batas waktu untuk menerima
body dari klien
    client_header_timeout 10s;     # Batas waktu untuk menerima
header dari klien
    keepalive_timeout 10s;          # Batas waktu koneksi keep-
alive
    send_timeout 10s;              # Batas waktu untuk mengirim
respon ke klien
    ...
}
```

Keterangan:

- *client_body_timeout*: Mengatur batas waktu untuk menerima *body* dari klien. Dengan memperpendek *timeout*, server dapat lebih cepat mengenali koneksi yang tidak aktif dan memutusnya.
- *client_header_timeout*: Mengatur batas waktu untuk menerima *header* dari klien. Hal ini juga membantu dalam mengenali koneksi yang tidak aktif lebih cepat.
- *keepalive_timeout*: Mengatur batas waktu untuk koneksi *keep-alive*. Dengan memperpendek *timeout*, server akan lebih cepat memutus koneksi yang tidak aktif.
- *send_timeout*: Mengatur batas waktu untuk mengirim respons ke klien. Ini membantu dalam menghindari koneksi yang terlalu lama menunggu respons.

3. Jika **menggunakan apache**, bisa menggunakan modul 'mod_reqtimeout' untuk menetapkan batas waktu permintaan. Berikut *source code* yang digunakan:

```
<IfModule mod_reqtimeout.c>
    RequestReadTimeout header=10-20,minrate=500
    RequestReadTimeout body=10,minrate=500
</IfModule>
```

Keterangan:

- *RequestReadTimeout*: Menetapkan batas waktu untuk membaca permintaan dari klien. Dengan menyesuaikan *timeout* ini, server dapat memutus koneksi yang tidak aktif lebih cepat, membantu melindungi dari serangan DDoS seperti *Slowloris*.

4. Penerapan *Firewall*, melakukan konfigurasi *firewall* untuk memblokir lalu lintas yang mencurigakan. *Firewall* dapat dikonfigurasi untuk membatasi jumlah koneksi rendah dan lambat dari alamat IP yang sama.

Dengan mengimplementasikan penyesuaian ini, server akan lebih dapat menghadapi serangan DDoS *Slowloris* dengan memutus koneksi yang tidak aktif lebih cepat, mengurangi dampak serangan tersebut terhadap ketersediaan dan kinerja *website*.

Simpulan

Penelitian ini berhasil menerapkan teknik *Slowloris* untuk melancarkan serangan *Distributed Denial-of-Service* (DDoS) terhadap *website* ilegal menggunakan Kali Linux. Hasil simulasi menunjukkan bahwa serangan *Slowloris* efektif dalam menghabiskan sumber daya server dan menyebabkan penurunan kinerja yang signifikan. Evaluasi berbagai teknik mitigasi, termasuk pengaturan batas koneksi server, penggunaan *firewall*, dan perangkat lunak khusus, menunjukkan bahwa mitigasi tersebut dapat secara efektif mengurangi dampak serangan dan mengembalikan kinerja normal server. Kesimpulannya, teknik mitigasi yang tepat dapat meningkatkan keamanan *website* dari ancaman serangan *Slowloris*, sehingga memberikan panduan praktis untuk melindungi infrastruktur digital dari serangan DDoS di masa depan.

Daftar Pustaka

Abhilash P, V Asv. 2015. Comparison Of Windows And Linux Operating Systems In Advanced Features. *Journal Of Engineering Research And Applications Www.Ijera.Com*. 5(2):81–83. Www.Ijera.Com.

Akbar R, Siroj Ra, Win Afgani M. 2023. Experimental Reseacrch Dalam Metodologi Pendidikan. *Jurnal Ilmiah Wahana Pendidikan, Januari*. 2023(2):465–474. Doi:10.5281/Zenodo.7579001.

Andria. 2020. Audit Keamanan Website Menggunakan Uniscan Di Kali Linux. *Seminar Nasional Inovasi Teknologi* ., Siap Terbit. Www.Andriakode.Rf.Gd.

Chotimah Hc. 2019. Tata Kelola Keamanan Siber Dan Diplomasi Siber Indonesia Di Bawah Kelembagaan Badan Siber Dan Sandi Negara Cyber Security Governance And Indonesian Cyber Diplomacy By National Cyber And Encryption Agency. *Riwayat Artikel Diterima*. 10(2). Doi:10.22212/Jp.V10i1.1447.

Dwiyatno S, Purnama Sari A, Irawan A, Serang Raya Jl Raya Serang Cilegon Drangong Taktakan Kota Serang Banten U. 2019. Pendeteksi Serangan Ddos (Distributed Denial Of Service) Menggunakan Honeypot Di Pt. Torini Jaya Abadi. *Jurnal Forma*. 2(2).

Engko C, Usmany P. 2020. Jak Dampak Pandemi Covid-19 Terhadap Proses Pembelajaran Online. *Jurnal Akuntansi •*. 6(1):23–38.

Gera J, Battula Bp. 2018. Detection Of Spoofed And Non-Spoofed Ddos Attacks And Discriminating Them From Flash Crowds. *Eurasip J Inf Secur*. 2018(1). Doi:10.1186/S13635-018-0079-6.

Gusti I, Putu N, Dicky Diastama D, Made Sukarsa I, Kadek N, Wirdiani A. 2021. Pengembangan Test Script Untuk Load Testing Web Dengan Metode Software Testing Life Cycle. *Jitter- Jurnal Ilmiah Teknologi Dan Komputer*. 2(1).

Handariyanti K, Kumalarani Mahakerty D, Tri Tanti A, Fitriyah S, Angeline D. 2023. Analisis Faktor Penggunaan Layanan Situs Ilegal Streaming Oleh Mahasiswa Its Dan Hubungannya Dengan Uu Ite. *Jurnal Sosial Dan Teknologi (Sostech)* . 3(10).

Hery La, Stit Q, Nusantara P, Ntb L. 2020. Pemanfaatan Media Dalam Metode Simulasi Pada Pembelajaran Pai. *Pensa : Jurnal Pendidikan Dan Ilmu Sosial*. 2(2):195–211. Https://Ejournal.Stitpn.Ac.Id/Index.Php/Pensa.

Idhartono Ar. 2020. Studi Literatur : Analisis Pembelajaran Daring Anak Berkebutuhan Khusus Di Masa Pandemi. *Jurnal Studi Guru Dan Pembelajaran*. 3(3):529–533. Doi:10.30605/Jsgp.3.3.2020.541.

Jaya B, Yuhandri Y, Sumijan S. 2020. Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial Of Service (Dos). *Jurnal Sistim Informasi Dan Teknologi*. 2(4):115–123. Doi:10.37034/Jsisfotek.V2i4.32.

Magdalena I, Sundari T, Nurkamilah S, Ayu Amalia D, Muhammadiyah Tangerang U. 2020. Analisis Bahan Ajar. Volume Ke-2. Https://Ejournal.Stitpn.Ac.Id/Index.Php/Nusantara.

Mayasari. 2021. Laporan Dan Evaluasi Penelitian. *Alacrity : Journal Of Education*. 1(2):30–38.

Prihantoro C, Hidayah Ak, Fernandez S. 2021. Analisis Manajemen Bandwidth Menggunakan Metode Queue Tree Pada Jaringan Internet Universitas Muhammadiyah Bengkulu. *Just Ti (Jurnal Sains Terapan Teknologi Informasi)*. 13(2):81. Doi:10.46964/Justti.V13i2.750.

Ramadhan I. 2020. Strategi Keamanan Cyber Security Di Kawasan Asia Tenggara. *Jurnal Asia Pacific Studies*. 3(2):181–192. Doi:10.33541/Japs.V3i1.1081.

Santoso D, Noertjahyana A, Andjarwirawan J. 2022. Implementasi Dan Analisa Snort Dan Suricata Sebagai Ids Dan Ips Untuk Mencegah Serangan Dos Dan Ddos. *Jurnal Infra*. 10(1).

Server W, Indrajid F, Andika Kf, Surya Gk, Putra A, Karisma Bramanda K, Arna G, Saskara J, Made I, Listartha E. 2023. Analisis Hasil Dos Syn Flood Attack Pada. *Jurnal Simika*. 12.

Sudewo K, Wikrama M, Firdaus R, Zal L, Mendrofa M, Arna G, Saskara J, Made I, Listartha E. 2023. Ddos Attack Using Goldeneye, Davoset, And Pyloris Tools. *Jurnal Coreit*. 9(2). Http://Testphp.Vulnweb.Com/Index.Php.

Suharti S, Yudhana A, Riadi I. 2022. Forensik Jaringan Ddos Menggunakan Metode Addie Dan Hids Pada Sistem Operasi Proprietary. *Matrik : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*. 21(3):567–582. Doi:10.30812/Matrik.V21i3.1732.

Zidane M. 2022. Klasifikasi Serangan Distributed Denial-Of-Service (Ddos) Menggunakan Metode Data Mining Naïve Bayes. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*. 6(1):172–180. Http://J-Ptiik.Ub.Ac.Id.

Zulkifli Ma, Riadi I, Prayudi Y. 2018. Live Forensics Method For Analysis Denial Of Service (Dos) Attack On Routerboard. *Int J Comput Appl*. 180(35):975–8887. Doi:Http://Doi.Org/10.5120/Ijca2018916879.