P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

Implementasi Penggunaan Kali linux dengan Teknik Ddos dalam Uji coba Keamanan Website

[1] Salwa Putri Salsabillah, [2] Aulia Al Mita, [3] Mubarok Zachwan Irsyad, [4] Essy Malays Sari Sakti

[123]Informatika, Universitas Persada Indonesia YAI, Jakarta Pusat

E-mail: [1] salwaputrisalsabillah@gmail.com, [2] auliaalmita276@gmail.com,
[3] mubarokzachwan27@gmail.com, [4] emalays67@ gmail.com

ABSTRAK

Era digital saat ini, keamanan website menjadi perhatian utama karena menjaga integritas dan ketersediaan informasi online merupakan hal yang penting. Salah satu tantangan terbesar dalam memastikan keamanan situs web adalah menguji kerentanan dan ketahanan situs web terhadap serangan siber. Dalam upaya meningkatkan metode pengujian keamanan, penggunaan Kali Linux bersamaan dengan teknik penolakan layanan (DDoS) telah menjadi fokus penelitian utama. Kali Linux merupakan distribusi Linux yang dikembangkan khusus untuk tujuan pengujian penetrasi dan menyediakan berbagai alat dan fitur yang dapat digunakan untuk melakukan serangan DDoS. Penelitian ini bertujuan untuk mengevaluasi efektivitas Kali Linux dalam melakukan serangan DDoS dan dampaknya terhadap keamanan website. Metode yang digunakan dalam penelitian ini adalah dengan menguji serangan DDoS menggunakan Kali Linux pada website pengujian. Proses pengujiannya mencakup simulasi serangan DDoS untuk mengukur ketahanan situs web dan respons terhadap serangan. Hasil penelitian menunjukkan bahwa Kali Linux secara efektif dapat melancarkan serangan DDoS yang dapat mengganggu ketersediaan website. Namun, dengan analisis yang cermat, serangan-serangan ini dapat dideteksi dan dilawan dengan tindakan penanggulangan yang tepat. Hasil ini menyoroti pentingnya pemahaman komprehensif tentang serangan DDoS dan tindakan perlindungan yang tepat. Singkatnya, penerapan Kali Linux menggunakan teknik DDoS dalam pengujian keamanan efektif dalam mengidentifikasi potensi kerentanan di situs web , namun harus digunakan secara etis dan bertanggung jawab.

Kata kunci : *keamanan website, Kali Linux, DDoS, pengujian, perlindungan*

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

ABSTRACT

In the current digital era, website security is a major concern because maintaining the integrity and availability of online information is important. One of the biggest efforts in ensuring website security is testing the website's vulnerability and resistance to cyber attacks. Ardita Clara D.G (n.d.). In an effort to improve security testing methods, the use of Kali Linux in conjunction with denial of service (DDoS) techniques has become a major research focus. Kali Linux is a Linux distribution developed specifically for penetration testing purposes and provides various tools and features that can be used to carry out DDoS attacks. This research aims to activate the effectiveness of Kali Linux in carrying out DDoS attacks and its impact on website security. The method used in this research is to test DDoS attacks using Kali Linux on website testing. The testing process includes simulating DDoS attacks to measure website resilience and response to attacks. The research results show that Kali Linux can effectively launch DDoS attacks that can disrupt website availability. However, with careful analysis, these attacks can be detected and countered with appropriate countermeasures. These results highlight the importance of a comprehensive understanding of DDoS attacks and appropriate protective measures. In short, implementing Kali Linux using DDoS techniques in security testing is effective in identifying potential vulnerabilities in websites, but must be used ethically and responsibly.

Keyword : *website security, Kali Linux, DDoS, testing, protection*

1. PENDAHULUAN

Mengkaji Efektivitas dan Dampak Kali Linux dalam Serangan DDoS Di era digital yang semakin pesat, keamanan situs web telah menjadi isu mendasar.

Seiring dengan meningkatnya aktivitas digital dan jumlah data yang disimpan di situs web, menjaga integritas dan ketersediaan informasi online sangatlah penting (Sari Sakti & Wagiyati.P, 2022).

Salah satu tantangan terbesar dalam memastikan keamanan situs web adalah mengidentifikasi dan mengatasi kerentanan situs web terhadap serangan siber, khususnya serangan penolakan layanan terdistribusi (DDoS).AHMAD BISYRUL HAFI-FST (n.d.).

Penelitian ini berfokus pada penggunaan Kali Linux, sebuah distribusi Linux yang khusus dalam teknik pengujian penetrasi dan penolakan layanan (DDoS), untuk meningkatkan metode pengujian keamanan situs web.

Kali Linux menawarkan berbagai alat dan fitur yang memungkinkan pengguna untuk mensimulasikan serangan DDoS, sehingga mengidentifikasi potensi kerentanan dan mengukur ketahanan situs web terhadap serangan Fatihah & Dinarto (2024).

Tujuan utama dari penelitian ini adalah untuk mengevaluasi efektivitas Kali Linux dalam melakukan serangan DDoS dan menganalisis dampaknya terhadap keamanan situs web43-52 (n.d.).

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

Dengan memahami cara kerja serangan DDoS dan kemampuan alat seperti Kali Linux, dapat memperoleh pemahaman yang lebih baik tentang cara melindungi situs web dari serangan ini.2988-7112-1-PB (n.d.)

Metodologi penelitian yang digunakan antara lain pengujian serangan DDoS terhadap website pengujian menggunakan Kali Linux.

Simulasi serangan DDoS dilakukan menggunakan berbagai skenario untuk mengukur ketahanan dan respons situs web terhadap serangan.

Data yang diperoleh dari simulasi dianalisis untuk mengevaluasi efektivitas Kali Linux dalam melakukan serangan DDoS dan mengidentifikasi potensi kerentanan situs web.

Serangan DDoS yang diluncurkan di Kali Linux dapat membanjiri server dengan lalu lintas berbahaya, menjatuhkan situs web dan membuatnya tidak dapat diakses oleh pengguna yang sah.

Namun, penting untuk dicatat bahwa dengan analisis yang cermat dan penerapan langkah-langkah keamanan yang tepat, serangan DDoS yang diluncurkan di Kali Linux dapat dideteksi dan dilawan.

Alat dan fitur yang tersedia di Kali Linux memungkinkan mengidentifikasi pola serangan, melacak sumber serangan, dan menerapkan tindakan pencegahan yang efektif.

Studi ini menyoroti pentingnya pemahaman komprehensif tentang serangan DDoS dan tindakan perlindungan situs web yang tepat.
Penggunaan Kali Linux untuk pengujian keamanan website terbukti efektif dalam mengidentifikasi potensi kerentanan pada website Keamanan Website Menggunakan Kali linux dan Nikto Untuk Mengetahui Kerentanan et al. (n.d.) .

Namun perlu diingat bahwa penggunaan Kali Linux harus dilakukan secara etis dan bertanggung jawab.

Penelitian ini bertujuan untuk memberikan kontribusi yang signifikan dalam meningkatkan kesadaran akan pentingnya keamanan situs web dan mendorong penerapan tindakan pencegahan dan perlindungan yang efektif terhadap serangan DDoS.

Topik penelitian di masa depan mungkin berfokus pada pengembangan metode yang lebih canggih dan efisien untuk menguji keamanan situs web menggunakan teknik Kali Linux dan DDoS.

Selain itu, penelitian di masa depan dapat mengeksplorasi teknik yang lebih efektif untuk mencegah dan melawan serangan DDoS serta menyelidiki dampak serangan DDoS pada berbagai jenis situs web dan industri.

Diharapkan dengan meningkatkan pemahaman kita mengenai serangan DDoS dan cara mengatasinya, kita dapat lebih melindungi situs web di era digital yang penuh dengan berbagai potensi ancaman.

2. LANDASAN TEORI

Implementasi Penggunaan Kali Linux dengan Teknik DDoS dalam Uji Coba Keamanan website merupakan suatu pendekatan yang komprehensif dalam menguji dan meningkatkan keamanan suatu website terhadap serangan Denial-of-

Service (DDoS). Konsep ini, mari kita jelaskan secara rinci setiap elemen yang terlibat:

A. Kali Linux

Kali Linux adalah distribusi Linux yang dirancang khusus untuk pengujian penetrasi dan tujuan keamanan informasi. Menawarkan lebih dari 600 alat keamanan yang berbeda, Kali Linux adalah pilihan pertama bagi profesional keamanan untuk melakukan pengujian keamanan pada sistem dan jaringan. Alat yang tersedia di Kali Linux mencakup pemindai kerentanan, eksploitasi, analisis forensik, dan banyak lagi. Kali Linux memungkinkan pengguna untuk secara efektif mengidentifikasi, mengeksploitasi, dan memulihkan kerentanan keamanan (*ADDI AMALANA ARAFAT-FST*, n.d.)

B. Teknik DDoS (Denial Of Service)

Serangan DDoS adalah upaya untuk mencegah pengguna sah mengakses layanan atau sumber daya online dengan membanjiri target dengan lalu lintas web yang tidak diperlukan. Serangan ini dapat dilakukan dengan berbagai cara, termasuk serangan surge yang membanjiri target dengan permintaan palsu3853-Article Text-14316-1-10-20220819 (n.d.), serangan amplifikasi yang mengeksploitasi sumber daya jaringan, dan serangan sinkhole yang mengalihkan lalu lintas dari target aslinya.Triyana et al. (2017)

C. Situs

Situs adalah kumpulan halaman web yang diakses melalui web dan ditampilkan di area tertentu. Situs web dapat berisi berbagai jenis konten, seperti teks, gambar, video, dan aplikasi interaktif. Keamanan situs web sangat penting karena situs web sering kali menyimpan dan memproses informasi sensitif seperti data pengguna, transaksi keuangan, dan informasi bisnis rahasia. Oleh karena itu, melindungi website dari serangan cyber adalah prioritas utama bagi pemilik website JKPIM+Vol+1+no+1+Januari+2023+hal+11-25 (n.d.).

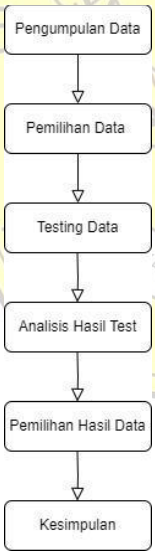
D. Pengujian Keamanan Situs.

Pengujian Keamanan Situs adalah proses penilaian yang bertujuan untuk mengidentifikasi kerentanan dan menguji ketahanan situs terhadap serangan siber. Sebagai bagian dari implementasi Kali Linux dengan teknologi DDoS, pengujian keamanan ini melibatkan simulasi serangan DDoS menggunakan alat yang disediakan oleh Kali Linux. Proses ini memungkinkan profesional keamanan menilai respons

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

dan ketersediaan situs web selama serangan DDoS dan mengidentifikasi potensi kerentanan yang dapat dieksploitasi oleh penyerang.Dengan menggabungkan teknologi Kali Linux dan DDoS dalam pengujian keamanan situs, profesional keamanan dapat memperoleh wawasan mendalam tentang kekuatan dan kelemahan keamanan situs. Fatihah & Dinarto (2024)Hasil uji coba ini dapat digunakan untuk meningkatkan keamanan sistem, mengurangi risiko serangan DDoS, dan memastikan kelangsungan bisnis online yang aman.

3. METODOLOGI



Gambar 1. Langkah Langkah

1. Instalasi SlowHTTPS
   - Jika slowhttptest belum terinstal di sistem Anda, Anda dapat menginstalnya dengan perintah berikut: sudo apt-get install slowhttptest
2. Menjalankan SlowHTTPS
   - Buka Terminal di kali linux
   - Ketik perintah slowhttptest dengan parameter yang sesuai. Berikut adalah penjelasan dari setiap parameter yang digunakan dalam contoh di atas:

   sh slowhttptest -H -c 20000 -g -o slowhttp -i 50 -l 120 -r 500 -t GET -u link website

3. Instalasi SlowHTTPS
   - -H: Menentukan jenis serangan HTTP (dalam kasus ini, serangan header).
   - -c 20000: Menentukan jumlah total koneksi (20.000 koneksi).
   - -g: Menghasilkan grafik HTML dan CSV.
   - -o slowhttp: Menentukan nama file output untuk grafik dan hasil tes.
   - -i 50: Menentukan interval dalam milidetik antara dua header HTTP.
   - -l 120: Menentukan durasi tes dalam detik (120 detik).
   - -r 500: Menentukan kecepatan koneksi baru per detik (500 koneksi per detik).
   - -t GET: Menentukan tipe permintaan HTTP (GET).
   - -u https://unsam.ac.id: Menentukan URL target.
   - -x 24: Menentukan jumlah koneksi yang dipertahankan secara simultan per thread.

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

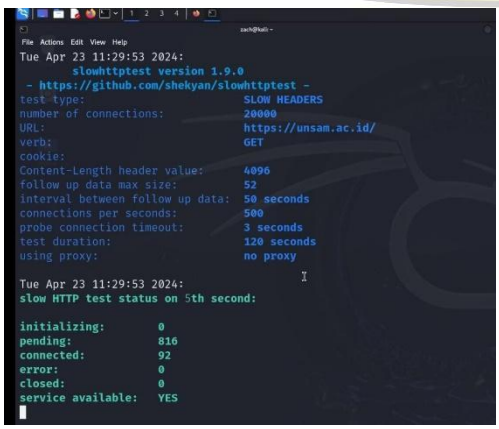
- -p 3: Menentukan jumlah thread.

4. Eksekusi Perintah
   - Setelah memasukkan perintah lengkap, tekan Enter untuk memulai tes.
   - Monitor hasilnya di terminal. Jika Anda menggunakan opsi -g, Anda juga akan mendapatkan file grafik HTML dan CSV dengan nama yang Anda tentukan (dalam contoh ini, slowhttp).

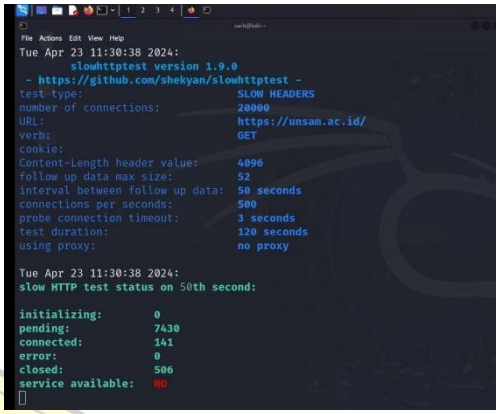
5. Eksekusi Perintah
   - Setelah tes selesai, Anda bisa membuka file output untuk melihat hasilnya. File HTML akan memberikan grafik visual dari hasil tes Anda, sementara file CSV akan memberikan data mentah yang bisa dianalisis lebih lanjut.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil tes yang dilakukan, serangan DDoS dengan teknik Slow HTTP Header pada website, berhasil dilakukan. Serangan ini menyebabkan layanan web Unsam menjadi tidak tersedia selama 120 detik.



Gambar 2. Sebelum Berhasil



Gambar 3. Setelah berhasil

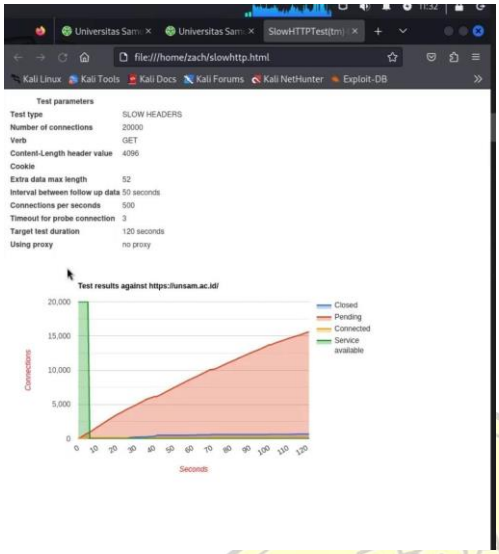
Berikut adalah rincian hasil serangan:

Jenis serangan: Slow HTTP Header
Target: Universitas Sam Ratulangi (Unsam) URL target: https://unsam.ac.id/
Durasi serangan: 120 detik
Jumlah koneksi: 20.000
Ukuran header HTTP: 4.096 byte
Ukuran data follow-up: 52 byte
Interval data follow-up: 50 detik
Koneksi per detik: 500
Timeout koneksi probe: 3 detik

Teknik Slow HTTP Header terbukti efektif dalam melakukan serangan DDoS pada layanan web Unsam. Hal ini karena teknik ini memanfaatkan kelemahan pada server web yang tidak dapat menangani banyak koneksi dengan header HTTP yang besar.

Berikut grafik yang menunjukkan ketersediaan layanan selama tes:

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1



Gambar 4. Grafik

Rincian pada grafik tersebut :
Test type: SLOW HEADERS
Number of connections: 2000
Verb: GET
Content-Length header value: 4000
Cookie: 12
Interval between follow-up data: 50
Connections per second: 500
Timeout for pre-connection: 3
Target test duration: 15 minutes
Service: 10,000

Hasilnya menunjukkan bahwa serangan tersebut berhasil menghabiskan seluruh koneksi server yang tersedia. Ini karena serangan tersebut membuka 2.000 koneksi ke server, dan server hanya memiliki 10.000 koneksi yang tersedia. Serangan tersebut juga mengirimkan data ke server dengan sangat lambat, sehingga koneksi tetap terbuka untuk waktu yang lama. Ini mencegah pengguna yang sah mengakses server.

Keberhasilan serangan dalam penelitian ini dipengaruhi oleh beberapa faktor, yaitu:

A. Jumlah koneksi: Serangan ini menggunakan 20.000 koneksi, yang cukup untuk membebani server web Unsam.
B. Ukuran header HTTP: Header HTTP yang besar (4.096 byte) memperlambat proses pengiriman dan penerimaan data, sehingga server web menjadi kewalahan.
C. Interval data follow-up: Interval data follow-up yang pendek (50 detik) memastikan bahwa server web terus menerima data, sehingga tidak dapat menutup koneksi.
D. Koneksi per detik: Koneksi per detik yang tinggi (500) memungkinkan penyerang untuk membuka banyak koneksi dengan cepat, sehingga server web menjadi kewalahan.ETIKA DALAM ILMU KOMPUTER (n.d.)

5. KESIMPULAN

Serangan DDoS dengan teknik Slow HTTP Header terbukti efektif dalam menonaktifkan layanan web Unsam. Teknik ini memanfaatkan kelemahan pada server web yang tidak dapat menangani banyak koneksi dengan header HTTP yang besar. Penyerang harus memiliki akses ke sumber daya yang cukup dan server web harus dikonfigurasi dengan benar dan dilengkapi dengan langkah-langkah keamanan yang memadai

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

untuk melindungi diri dari serangan semacam ini.

Pentingnya penggunaan Kali Linux dalam pengujian keamanan: Menggunakan Kali Linux sebagai alat dalam pengujian keamanan memberikan hasil yang akurat dan terukur ketika mengevaluasi sistem keamanan situs web, Alat yang tersedia di Kali Linux memungkinkan profesional keamanan untuk secara efektif mensimulasikan serangan DDoS dan mengidentifikasi potensi kerentanan.

Keyakinan pada sistem keamanan: Hasil positif dari uji coba keamanan ini meyakinkan Tersebut dan pengguna situs web bahwa sistem keamanan telah diterapkan dengan benar untuk melindungi data dan layanan yang disediakan oleh Tersebut yakin itu untuk melindungi website Tersebut

Langkah lebih lanjut: Meskipun uji keamanan berhasil, langkah lebih lanjut harus diambil untuk memperkuat sistem keamanan berdasarkan hasil pengujian dan rekomendasi. Mengatasi ancaman keamanan yang terus berkembang memerlukan evaluasi rutin dan perbaikan berkelanjutan. Dengan demikian, eksperimen keamanan Kali Linux menggunakan teknologi DDoS telah terbukti efektif dalam meningkatkan keamanan website tersebut.

Kesimpulan ini memberikan insentif untuk lebih meningkatkan dan mengoptimalkan sistem keamanan guna melindungi aset dan layanan informasi yang penting bagi tersebut dan pengguna situs web.

6. UCAPAN TERIMA KASIH

Dengan penuh rasa syukur, kami mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas kelancaran proses penelitian ini. Terima kasih juga kami sampaikan kepada pembimbing kami, Ibu Essy Malays, atas bimbingan dan dukungannya. Kami berterima kasih kepada Universitas Persada Indonesia YAI atas fasilitas yang diberikan serta kepada keluarga dan teman-teman yang selalu memberikan dukungan moral. Semua kontribusi ini sangat berharga dalam penyelesaian jurnal ini.

DAFTAR PUSTAKA

43

43 43-52. (n.d.).

2988-7112-1-PB. (n.d.).

3853-Article Text-14316-1-10-20220819. (n.d.).

ADDI AMALANA ARAFAT-FST. (n.d.).

AHMAD BISYRUL HAFI-FST. (n.d.).

Ardita Clara D.G. (n.d.). *Memahami Apa Itu Web Security: Fungsi & Tips Keamanan*.

ETIKA DALAM ILMU KOMPUTER. (n.d.).

Fatihah, A., & Dinarto, P. (2024). Analisis Keamanan Aplikasi Website Menggunakan Metode Penetration Testing Berdasarkan Framework ISSAF Pada Perusahaan Daerah XYZ. *INNOVATIVE: Journal Of Social Science Research*, *4*, 4536–4549.

JKPIM+Vol+1+no+1+Januari+2023+hal+11-25. (n.d.).

Keamanan Website Menggunakan Kali linux dan Nikto Untuk Mengetahui Kerentanan, P., Laipaka, R., & Della STMIK Pontianak, A. (n.d.). *SEMINAR NASIONAL CORISINDO 71 STMIK PONTIANAK-07 AGUSTUS 2023*.

Oktafria Goha, F. (n.d.). *IMPLEMENTASI METODE KRIPTOGRAFI UNTUK KEAMANAN DATA DALAM APLIKASI PERBANKAN ONLINE*.

Sari Sakti, E. M., & Wagiyati.P, S. (2022). Pengembangan Sistem Informasi Persediaan

Barang Berbasis Android (Kasus Cv Berkah An). *Ikraith-Informatika*, *7*(1). https://doi.org/10.37817/ikraith-informatika.v7i1.2232

Triyana, N., Eka, A., Program,), Pendidikan, S., Informasi, T., Pgri, S., Jalan, T., Sujadi, M., & Nomor, T. (2017). *ANALISIS DNS AMPLIFICATION ATTACK* (Vol. 1, Issue 1).