Penggunaan Slowhttptest Untuk Menguji Kerentangan Jaringan Terhadap Flooding Attack

Adi Muslim[1] , Dwiky Rachmatullah[2] , Muhammad Refa Tsalits Ramdhani[3]
[1]Sistem Informasi, Universitas Pamulang
[2]Sistem Informasi, Universitas Pamulang
[3]Sistem Informasi, Universitas Pamulang

E-mail: dwikyrachmatullah77@gmail.com

ABSTRAK

Perkembangan teknologi informasi telah membawa banyak manfaat, namun juga meningkatkan ancaman keamanan siber, termasuk serangan flooding yang mengancam ketersediaan layanan jaringan. Flooding attack merupakan jenis serangan Denial of Service (DoS) yang bertujuan untuk membanjiri server dengan lalu lintas berlebihan, sehingga mengganggu atau menghentikan layanan bagi pengguna yang sah. Penelitian ini bertujuan untuk mengkaji penggunaan Slowhttptest sebagai alat untuk menguji kerentanan jaringan terhadap flooding attack. Metodologi penelitian melibatkan beberapa tahap, yaitu studi literatur, persiapan alat dan lingkungan uji, pelaksanaan pengujian, analisis data, dan penyusunan rekomendasi mitigasi. Slowhttptest digunakan untuk melakukan simulasi serangan dan mengukur respon jaringan terhadap serangan tersebut. Hasil pengujian menunjukkan bahwa Slowhttptest mampu mengidentifikasi kerentanan jaringan secara efektif. Data yang diperoleh dianalisis untuk menilai dampak serangan dan mengembangkan strategi mitigasi. Penelitian ini memberikan kontribusi akademis dalam bentuk pemahaman yang lebih mendalam tentang mekanisme serangan flooding dan alat uji kerentanannya. Secara praktis, penelitian ini memberikan panduan bagi administrator jaringan dalam mengidentifikasi dan mengatasi kerentanan terhadap flooding attack. Selain itu, penelitian ini juga mendorong pengembangan teknologi pengujian keamanan jaringan yang lebih baik.

Kata kunci: flooding attack, Denial of Service, Slowhttptest, kerentanan jaringan, keamanan siber

ABSTRACT

The development of information technology has brought many benefits, but has also increased cyber security threats, including flood attacks that threaten the availability of network services. A flood attack is a type of Denial of Service (DoS) attack that aims to flood a server with excessive traffic, thereby disrupting or stopping service for legitimate users. This research aims to examine the use of Slowhttptest as a tool to test network vulnerability to flood attacks. The research methodology involves several stages, namely literature review, preparation of test equipment and environment, test execution, data analysis, and preparation of mitigation proposals. Slowhttptest is used to simulate attacks and measure network response to these attacks. Test results show that Slowhttptest can effectively identify network vulnerabilities. The data obtained is analyzed to assess the impact of the attack and develop mitigation strategies. This research provides an academic contribution in the form of a deeper understanding of flood attack mechanisms and vulnerability testing tools. Practically, this research provides guidance for network administrators in identifying and overcoming vulnerabilities to flood attacks. In addition, this research also promotes the development of better network security testing technologies.

Keywords: *flood attack, Denial of Service, Slowhttptest, network vulnerability, cyber security.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa banyak kemudahan dalam berbagai aspek kehidupan, termasuk dalam dunia bisnis, pendidikan, dan pemerintahan. Namun, perkembangan ini juga diiringi dengan meningkatnya ancaman keamanan siber. Salah satu ancaman yang sering dihadapi oleh jaringan komputer adalah serangan flooding. Serangan ini bertujuan untuk membanjiri jaringan dengan lalu lintas yang berlebihan sehingga mengganggu ketersediaan layanan.

Flooding attack adalah jenis serangan Denial of Service (DoS) yang dilakukan dengan cara mengirimkan sejumlah besar permintaan ke server dengan tujuan untuk menghabiskan sumber daya server tersebut. Akibatnya, server tidak dapat merespon permintaan dari pengguna yang sah. Salah satu metode untuk menguji kerentanan jaringan terhadap serangan ini adalah dengan menggunakan Slowhttptest.

2. TINJAUAN PUSTAKA

Teknologi informasi dan komunikasi yang berkembang pesat tidak hanya memberikan banyak manfaat, tetapi juga menghadirkan tantangan berupa ancaman keamanan siber seperti flooding attack. Jenis serangan ini, yang termasuk dalam Denial of Service (DoS), bertujuan untuk membanjiri server dengan permintaan data yang sangat banyak, sehingga layanan untuk pengguna sah terganggu. Untuk menguji kerentanan jaringan terhadap ancaman tersebut, berbagai pendekatan telah dirancang, salah satunya dengan memanfaatkan perangkat lunak *Slowhttptest*.

Berbagai penelitian telah membahas metode deteksi serangan, seperti penggunaan model *deep learning*, penerapan logika fuzzy untuk identifikasi serangan, dan strategi mitigasi berbasis firewall. Studi-studi ini menekankan perlunya alat uji yang mampu mendeteksi serangan secara akurat, serta perlunya kerja sama antara komunitas akademik dan profesional TI dalam menghadapi ancaman keamanan yang terus berkembang. Penelitian sebelumnya membuktikan bahwa *Slowhttptest* efektif dalam mensimulasikan serangan dan mengevaluasi respons jaringan, sehingga menjadi alat yang berguna bagi pengelola jaringan dalam mengidentifikasi dan memperbaiki kerentanan sistem mereka.

3. METODE

Metode penelitian ini menggunakan pendekatan eksperimental dengan langkah-langkah sebagai berikut:

1. Studi Literatur: Mengumpulkan dan mempelajari literatur terkait flooding attack dan alat pengujian seperti Slowhttptest.
2. Persiapan Alat dan Lingkungan: Mengkonfigurasi jaringan dan memasang Slowhttptest untuk simulasi serangan.
3. Pengujian: Melakukan serangan simulasi menggunakan Slowhttptest dan mencatat hasil pengujian.
4. Analisis Data: Menganalisis data yang diperoleh untuk menilai kerentanan jaringan dan efektivitas Slowhttptest

3.1 Rumusan Masalah

Berdasarkan latar belakang di atas, terdapat beberapa rumusan masalah yang perlu dijawab dalam penelitian ini, yaitu:

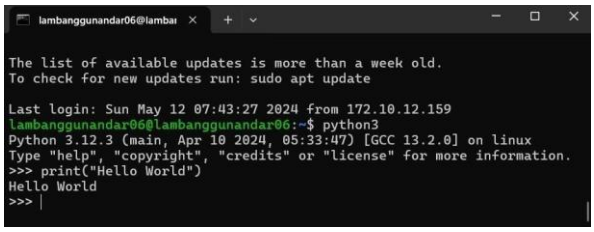
1. Bagaimana cara kerja Slowhttptest dalam menguji kerentanan jaringan terhadap flooding attack?
2. Seberapa efektif Slowhttptest dalam mengidentifikasi kelemahan jaringan?

4. HASIL DAN PEMBAHASAN

Penelitian ini bertujuan untuk mengirimkan jumlah paket data yang berbeda-beda ke server target menggunakan Slowhttptest. serangan Distributed Denial of Service (DDoS) pada server web Apache2, serta untuk menguji respons server terhadap serangan tersebut. Dalam rangka mencapai tujuan tersebut, serangkaian langkah-langkah telah diimplementasikan. Langkah pertama melibatkan konfigurasi pada dua sistem operasi yang digunakan, konfigurasi spesifikasi OS disusun menggunakan VirtualBox. Dengan menggunakan konfigurasi ini, system operasi windows dan Ubuntu pada virtual box dapat dijalankan secara efisien, memungkinkan untuk pengujian penelitian ini dengan aman dan efektif

Gambar 1. Web Server Apache2 pada Windows

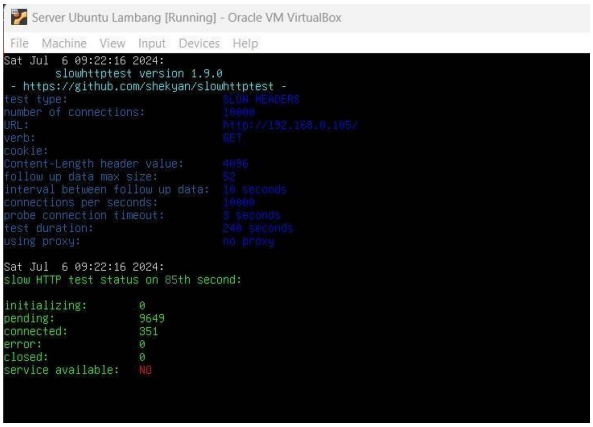
Dari konfigurasi yang telah dilakukan, peneliti memperoleh alamat IP untuk kedua OS tersebut, yaitu 192.168.0.113 untuk Ubuntu dan 192.168.100.105 untuk Windows. Setelah konfigurasi awal selesai, peneliti melakukan pengecekan terhadap konektivitas SSH dari Windows ke Ubuntu. Dengan menggunakan perintah SSH, peneliti memeriksa apakah koneksi antara kedua sistem operasi berfungsi dengan baik . Langkah ini penting untuk memastikan bahwa pengaturan jaringan dan layanan SSH telah dikonfigurasi dengan benar, sehingga memungkinkan akses yang aman dan terenkripsi antara kedua OS. Dengan berhasilnya pengecekan konektivitas SSH, peneliti dapat melanjutkan ke tahap berikutnya dalam penelitian, termasuk pengujian dan implementasi serangan DDoS terhadap web server Apache2 yang berjalan pada OS Ubuntu.



Gambar 2. Akses SSH dari Ubuntu di Windows

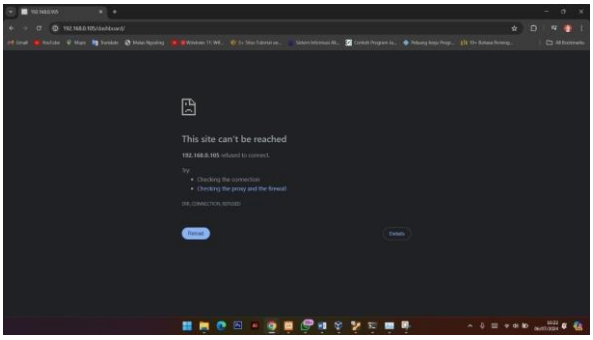
4.1 Simulasi serangan dengan slowhttptest.

Langkah pertama dalam penelitian adalah melakukan simulasi serangan menggunakan tool slowhttptest. Perintah “slowhttptest -c 1000 -H -g -o slowhttp -i 10 -r 500 -t GET -u http://192.168.0.105 -x 24 -p 3” digunakan untuk memberikan serangan lambat (slow HTTP) terhadap server web. Simulasi ini memungkinkan peneliti untuk melihat kerentanan server apache dari serangan jenis ini.



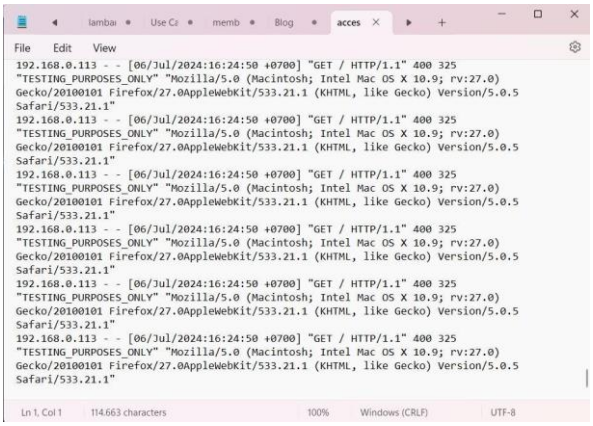
Gambar 3. Melakukan Penyerangan DDoS di Ubuntu ke Windows

4.2 Akses Web Server dan Cek Log Aktivitas untuk Mendeteksi Serangan



Gambar 4. Mengecek Pada Web Server Windows

Setelah melakukan simulasi serangan, peneliti mengakses kembali web server Apache2 dan menemukan bahwa akses menjadi sangat lambat dan sering mengalami lag. Hal ini menunjukkan bahwa serangan slow HTTP berhasil mempengaruhi kinerja server, menyebabkan penurunan kecepatan akses dan responsibilitas. Kondisi ini menegaskan dampak nyata dari serangan DDoS terhadap server web, yang berpotensi mengganggu layanan dan pengalaman pengguna.



Gambar 5. Log Aktivitas Pada Server Windows

Setelah simulasi serangan dilakukan, peneliti memeriksa log aktivitas server web Apache2 untuk melihat apakah ada tanda-tanda serangan yang terdeteksi. Dengan memeriksa file access.log di direktori /var/log/apache2/, peneliti dapat mengidentifikasi alamat IP penyerang yaitu 192.168.0.113 dan aktivitas lain yang mencurigakan.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa Slowhttptest efektif dalam mengidentifikasi kerentanan jaringan terhadap serangan flooding, khususnya jenis serangan Denial of Service (DoS). Melalui simulasi serangan menggunakan Slowhttptest, penelitian ini mampu menunjukkan dampak nyata dari serangan ini pada kinerja server, yang ditandai dengan penurunan kecepatan akses dan responsibilitas server. Hasil analisis data menunjukkan bahwa Slowhttptest dapat menjadi alat yang efektif untuk menguji kerentanan jaringan dan membantu administrator jaringan dalam mengidentifikasi serta mengatasi kelemahan yang ada.

Penelitian ini memberikan kontribusi akademis dengan memberikan pemahaman lebih mendalam tentang mekanisme serangan flooding dan pengujian kerentanannya. Secara praktis, penelitian ini memberikan panduan bagi administrator jaringan untuk mengidentifikasi dan mengatasi kerentanan terhadap serangan flooding, serta mendorong pengembangan teknologi pengujian keamanan jaringan yang lebih baik.

DAFTAR PUSTAKA

[1]. M. Gyanchandani, J. L. Rana, and R. N. Yadav, “Taxonomy of Anomaly Based Intrusion Detection System: A Review,” In: International Journal of Scientific and Research Publications, v.2, n.12, 2012.

[2]. A. S. Raut, and K. R. Singh, “Anomaly Based Intrusion Detection-A Review,” Int. J. on Network Security, vol. 5, 2014.

[3]. F. Palmieri, and U. Fiore, “Network anomaly detection through nonlinear analysis,” Computers & Security, 29(7), pp. 737 755, 2010.

[4]. Ahanger, T. A. (2017). An effective approach of detecting DDoS using artificial neural networks. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 707–711.

[5]. Alghazzawi, D., Bamasag, O., Ullah, H., & Asghar, M. Z. (2021). Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Applied Sciences, 11(24), 11634.

[6]. P. A. Nugraha, M. A. Irwansyah, and H. Priyanto, “Rancang Bangun Web Server Berbasis Linux Dengan Metode Load Balancing (Studi Kasus : Laboratorium Teknik Informatika),” vol. 3, no. 1, pp. 1–5, 2016.

[7]. N. Sugianti, Y. Galuh, S. Fatia, and K. F. H. Holle, “Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno,” Jiska, vol. 4, no. 3, pp. 18–26, 2020, [Online]. Available: http://ejournal.uin-suka.ac.id/saintek/JISKA/article/view/1658.

[8]. L. P. Ayuningtias, M. Irfan, and J. Jumadi, “Analisa Perbandingan Logic Fuzzy Metode Tsukamoto, Sugeno, Dan Mamdani (Studi Kasus : Prediksi Jumlah Pendaftar Mahasiswa Baru Fakultas Sains Dan Teknologi Universitas Islam Negeri Sunan Gunung Djati Bandung),” J. Tek. Inform., vol. 10, no. 1, 2017, doi: 10.15408/jti.v10i1.5610.

[9]. I. P. D. A. N. Port, S. D. A. N. Wireshark, D. N. Apriliani, M. A. Sasmita, and T. Windari, “Kata Kunci :,” vol. 1, pp. 6–16, 2017.

[10]. R. A. Purnomo, D. Syauqy, and M. H. Hanafi, “Implementasi Metode Fuzzy Sugeno Pada Embedded System Untuk Mendeteksi Kondisi Kebakaran Dalam Ruangan,” J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya, vol. 2, no. 4, pp. 1428–1435, 2018.

[11]. J. Warmansyah and D. Hilpiah, “Penerapan metode fuzzy sugeno untuk prediksi persediaan bahan baku,” vol. 9, no. 2, pp. 12–20, 2019.

[12]. M. Hilmi Hafid, “Investigasi Log Jaringan Untuk Deteksi Serangan Distributed Denial Of Service (Ddos) Dengan Menggunakan Metode General Regression Neural Network Skripsi Oleh : Muhammad Hilmi Hafid,” 2019.

[13]. S. Dwiyatno, A. P. Sari, A. Irawan, and Safig, “Pendeteksi Serangan Ddos (Distributed Denial Of Service) Menggunakan

Honeypot Di PT. Torini Jaya Abadi," Simika, vol. 2, no. 2, pp. 64–80, 2019.

[14]. As' ad, Ihwana. "Analisis Forensik Terhadap Serangan DDoS Ping of Death Pada Server." *Cyber Security dan Forensik Digital (CSFD)* 5.1 (2022): 23-31.

[15]. Ridho, M. Alfine, and Molavi Arman. "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan." *Jurnal Sisfokom (Sistem Informasi Dan Komputer)* 9.3 (2020): 373-379.

[16]. Firdaus, Diash, Fahira Fahira, and Resa Rianti. "DETEKSI ANOMALI DAN SERANGAN LOW RATE DDOS DALAM LALU LINTAS JARINGAN MENGGUNAKAN NAIVE BAYES." *Naratif: Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika* 5.2 (2023): 140-148.

[17]. Hansen, Jerry, and Tata Sutabri. "Mendesain Cyber Security Untuk Mencegah Serangan DDoS Pada Website Menggunakan Metode Captcha." *Digital Transformation Technology* 3.1 (2023): 289298.

[18]. Bahri, Syaiful. "Mengamankan Perangkat Jaringan Dari Serangan DDoS Menggunakan Fitur Firewall-RAW di Router MikroTik." *KAKIFIKOM (Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer)* (2024): 1-6.

[19]. Ulfa, Husnul. *SISTEM PENGAMANAN JARINGAN SDN DARI SERANGAN DDOS BERBASIS MULTI CONTROLLER DAN LOAD BALANCER*. Diss. Universitas Pendidikan Indonesia, 2024.

[20]. Rahmadaniar, Ihda, et al. "Implementasi Firewall Menggunakan Iptables untuk Melindungi Server dari Serangan DDoS." *Journal of Internet and Software Engineering* 1.3 (2024): 10-10.