ABSTRAK

Serangan Distributed Denial of Service (DDoS) merupakan salah satu ancaman serius terhadap layanan berbasis web yang dapat menyebabkan *downtime* sistem, kerugian finansial, dan kerusakan reputasi. Penelitian ini bertujuan untuk mengembangkan sistem monitoring dan mitigasi serangan DDoS secara real-time menggunakan metode Threshold-Based Detection dan Filtering. Sistem dirancang dengan pendekatan rekayasa perangkat lunak, menggunakan bahasa pemrograman Python, Redis untuk pencatatan trafik, serta observabilitas yang diintegrasikan melalui Slack dan SigNoz. Metode Threshold-Based Detection diterapkan dengan menghitung rata-rata pergerakan berbobot eksponensial (EWMA) dan deviasi standarnya (EWSTD) guna mendeteksi lonjakan trafik abnormal secara adaptif. Sementara itu, metode Filtering digunakan untuk memblokir lalu lintas yang mencurigakan menggunakan teknik rate-limiting dan behavior-based filtering. Sistem diuji melalui simulasi serangan DDoS menggunakan trafik HTTP dengan variasi intensitas. Efektivitas sistem dalam mendeteksi dan melakukan mitigasi serangan DDoS secara real-time dinilai tinggi yang mampu mencapai angka akurasi hingga 95% dengan rata-rata waktu deteksi dari jenis trafik HTTP Flood mencapai angka 0,8 detik waktu deteksi dengan waktu notifikasi mencapai 1,3 detik. Selain itu, jenis trafik SYN Flood Bursty Random yang menghasilkan waktu deteksi 0,9 detik dengan waktu notifikasi 1,1 detik. Serta Bursty Random yang mencapai waktu deteksi 1,2 detik dengan waktu notifikasi 1,5 detik, dengan demikian sistem mampu merespons serangan dengan cepat, mengurangi dampak sebelum mencapai ambang kritis, serta memberikan dukungan forensik dan analisis mendalam. Penelitian ini berkontribusi dalam pengembangan keamanan jaringan komputer, khususnya terkait pengembangan teknologi mitigasi serangan siber jaringan.

Kata Kunci: DDoS, Threshold-Based Detection, Filtering, Monitoring, Real-time, EWMA, EWSTD, Mitigasi.

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a serious threat to web-based services, potentially causing system downtime, financial losses, and reputational damage. This research aims to develop a real-time monitoring and mitigation system for DDoS attacks using Threshold-Based Detection and Filtering methods. The system is designed using a software engineering approach, implemented with Python, Redis for traffic logging, and integrated observability through Slack and SigNoz. The Threshold-Based Detection method is applied by calculating the Exponentially Weighted Moving Average (EWMA) and its standard deviation (EWSTD) to adaptively detect abnormal traffic spikes. Meanwhile, the Filtering method is employed to block suspicious traffic using rate-limiting and behavior-based filtering techniques. The system was tested through simulated DDoS attacks using HTTP traffic with varying intensity levels. The system demonstrated high effectiveness in detecting and mitigating DDoS attacks in real-time, achieving up to 95% accuracy. The average detection time for HTTP Flood traffic was 0.8 seconds with a notification time of 1.3 seconds. For SYN Flood Bursty Random traffic, the detection time was 0.9 seconds with a notification time of 1.1 seconds. For Bursty Random traffic, the detection time reached 1.2 seconds with a notification time of 1.5 seconds. These results indicate that the system can respond to attacks quickly, reduce impact before reaching a critical threshold, and provide forensic support and in-depth analysis. This research contributes to the advancement of computer network security, particularly in the development of cyberattack mitigation technologies.

Keywords: DDoS, Threshold-Based Detection, Filtering, Monitoring, Real-time, EWMA, EWSTD, Mitigation.