ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY OWASP CRS DAN DDOS DEFLATE TERHADAP SERANGAN DDOS PADA WEB SERVER

HELMI HASYIM

ABSTRAK

Serangan Distributed Denial of Service (DDoS) merupakan ancaman serius yang dapat mengganggu ketersediaan layanan web server. Penelitian ini bertujuan untuk menganalisis efektivitas kombinasi ModSecurity OWASP Core Rule Set (CRS) dan DDoS Deflate dalam mendeteksi dan memitigasi serangan DDoS. Penelitian dilakukan dalam lingkungan laboratorium menggunakan tiga skenario: tanpa perlindungan, hanya dengan ModSecurity, dan kombinasi ModSecurity dengan DDoS Deflate. Metode pengujian menggunakan simulasi serangan HTTP Flood dan SYN Flood selama 10 menit, dengan pengamatan terhadap performa server melalui Prometheus, Grafana, dan tcpdump. Hasil menunjukkan bahwa skenario tanpa perlindungan menyebabkan lonjakan penggunaan CPU hingga 97% dan tingginya trafik masuk tanpa pemblokiran. Penggunaan ModSecurity saja menunjukkan perlindungan terbatas, terutama pada layer aplikasi, dengan blokir sebagian permintaan HTTP. Sementara itu, kombinasi ModSecurity dan DDoS Deflate mampu meningkatkan efisiensi mitigasi secara signifikan, dengan pemblokiran lebih dari 5 juta koneksi berbahaya dan efisiensi bandwidth HTTP Flood sebesar 87,76%. Kesimpulannya, pendekatan mitigasi berlapis terbukti lebih efektif dalam menjaga kestabilan performa server dan layak diterapkan sebagai strategi perlindungan web server dari serangan DDoS.

Kata Kunci : ModSecurity, DDoS Deflate, HTTP Flood, SYN Flood, Mitigasi.

ANALISIS EFEKTIVITAS KOMBINASI MODSECURITY OWASP CRS DAN DDOS DEFLATE TERHADAP SERANGAN DDOS PADA WEB SERVER

HELMI HASYIM

ABSTRACT

Distributed Denial of Service (DDoS) attacks pose a significant threat to the availability of web server services. This study aims to evaluate the effectiveness of combining ModSecurity OWASP Core Rule Set (CRS) and DDoS Deflate in detecting and mitigating DDoS attacks. The research was conducted in a controlled laboratory environment using three scenarios: without protection, with ModSecurity alone, and with a combination of ModSecurity and DDoS Deflate. The testing involved simulated HTTP Flood and SYN Flood attacks over a duration of 10 minutes, with performance metrics observed using Prometheus, Grafana, and tcpdump. The results indicate that in the unprotected scenario, server CPU usage spiked up to 97%, accompanied by a high volume of incoming traffic without any mitigation. The implementation of ModSecurity alone provided limited protection, primarily at the application layer, by partially blocking HTTP requests. In contrast, the combined use of ModSecurity and DDoS Deflate significantly improved mitigation effectiveness, successfully blocking over 5 million malicious connections and achieving a bandwidth efficiency of 87.76% against HTTP Flood attacks. In conclusion, the layered mitigation approach demonstrated a superior ability to maintain server performance stability and is highly recommended as a strategy for protecting web servers from DDoS attacks.

Keywords: ModSecurity, Deflate DDoS, HTTP Flood, SYN Flood, Mitigation.