

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil penelitian dan pengujian terhadap tiga skenario sistem keamanan, maka dapat disimpulkan seperti berikut:

- a. Rancangan kombinasi ModSecurity OWASP CRS dan DDoS Deflate berhasil meningkatkan keamanan *server web* terhadap serangan DDoS dengan pendekatan mitigasi berlapis pada lapisan aplikasi dan jaringan. ModSecurity berperan menyaring trafik HTTP berbahaya, sedangkan DDoS Deflate membatasi koneksi berlebih berbasis IP.
- b. Efektivitas sistem mitigasi terlihat dari hasil pengujian skenario 3, di mana jumlah HTTP request yang masuk berhasil ditekan secara signifikan, dari sekitar 5 juta menjadi hanya sekitar 800 ribu. Selain itu, lebih dari 5.5 juta koneksi berbahaya berhasil diblokir. Efisiensi *bandwidth* terhadap serangan HTTP Flood pun mencapai 87.76%, jauh lebih tinggi dibandingkan dengan penggunaan ModSecurity saja yang hanya menghasilkan efisiensi sebesar 1.37%.
- c. Dampak terhadap performa sumber daya server juga menunjukkan perbaikan signifikan. Penggunaan CPU saat terjadi serangan HTTP Flood dapat ditekan dari 97% pada skenario 1 menjadi hanya 8.38% dengan penerapan sistem mitigasi berlapis. Selain itu, waktu respons *server* menjadi lebih stabil dan terkendali, yang menunjukkan bahwa sistem tetap mampu memberikan layanan secara optimal meskipun berada dalam kondisi serangan.

5.2. Saran

Berdasarkan hasil penelitian dan analisis yang telah dilakukan pada Bab sebelumnya, terdapat beberapa saran yang dapat diberikan untuk implementasi praktis maupun pengembangan lebih lanjut di masa mendatang. Saran ini ditujukan bagi administrator sistem, peneliti, maupun pihak lain yang berkepentingan dalam bidang keamanan web server, khususnya dalam menghadapi ancaman serangan

Distributed Denial of Service (DDoS). Adapun saran yang dapat disampaikan adalah sebagai berikut:

- a. Penerapan sistem mitigasi berlapis seperti kombinasi antara ModSecurity OWASP CRS dan DDoS Deflate direkomendasikan untuk digunakan pada server web yang bersifat publik, khususnya yang rentan terhadap serangan DDoS. Kombinasi ini terbukti mampu memberikan perlindungan secara menyeluruh, baik pada lapisan aplikasi maupun jaringan.
- b. Penyesuaian konfigurasi keamanan perlu dilakukan secara cermat berdasarkan kapasitas sumber daya server dan pola lalu lintas jaringan yang dimiliki. Hal ini bertujuan agar mekanisme mitigasi tidak menyebabkan penurunan performa sistem secara signifikan akibat beban proses inspeksi atau pemblokiran yang berlebihan.
- c. Penelitian lanjutan diharapkan dapat menguji efektivitas kombinasi mitigasi ini terhadap jenis serangan lain seperti Slowloris, UDP Flood, atau serangan multi-vektor. Selain itu, pengembangan dapat diarahkan pada integrasi sistem dengan teknologi Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) modern, guna memperluas cakupan proteksi dan meningkatkan ketahanan sistem secara menyeluruh.