ABSTRAK

Salah satu teknologi yang banyak digunakan oleh perusahaan untuk menjalankan aplikasi secara efektif dan aman adalah *container*. Melalui *container*, setiap aplikasi hanya perlu memiliki dependensi yang dibutuhkan oleh program tanpa adanya dependensi yang tidak diperlukan. *Container runtime* merupakan komponen inti dalam *container* untuk dapat menjembatani proses-proses yang ada di dalam *container* dan *host* server. Salah satu permasalahan yang muncul di balik maraknya penggunaan *container* adalah serangan siber seperti serangan *Denial of Service* (DOS) yang dapat mengakibatkan server menjadi lumpuh. Urgensi dalam menyiapkan *container runtime* yang tangguh terhadap serangan DOS semakin dibutuhkan. Penelitian ini bertujuan untuk memberikan analisis yang komprehensif mengenai kinerja antara *container runtime* runC yang umum digunakan, dengan *container runtime* yang memiliki arsitektur isolasi keamanan yang tinggi seperti gVisor dan Kata Containers. Kinerja runC, Kata Containers dan gVisor didasarkan pada *host* CPU, penggunaan memori *host*, *container* CPU, penggunaan memori *container*, *web throughput*, dan *web response time*. Hasil pengujian pada penelitian ini menunjukan bahwa runC memiliki hasil yang terbaik pada *host* CPU, *host* memori, *container* CPU, *web throughput*, dan *web response time*. Sementara, Kata Container memiliki hasil terbaik pada konsumsi *container* memori dan juga Kata Container menjadi *container runtime* setelah runC yang memiliki hasil terbaik pada setiap metriks.

Kata Kunci: *container runtime*, runc, gvisor, kata containers, *denial of services*.