# ABSTRAK

Kubernetes adalah *platform* orkestrasi kontainer populer untuk menyederhanakan dan mengoptimalkan kinerja *server*. Namun masalah keamanan dapat mempengaruhi penggunaan dan kinerja dari *platform* Kubernetes. Maka penelitian ini akan menguji server pada kontainer *berplatform* Kubernetes terhadap serangan *Denial of Service*. Dimana DoS menyerang dengan cara mengirimkan trafik yang sangat banyak secara terus menerus hingga memenuhi trafik dan menyebabkan sumber daya jaringan tidak tersedia lagi. Guna menganalisa efek yang ditimbulkan dari serangan DoS berupa *responsibility* dan kinerja server tersebut setelah adanya penyerangan DoS. Pengujian yang akan dilakukan menggunakan tiga skenario penyerangan DoS yaitu TCP *flood*, UDP *flood*, dan *smurf attack*. Parameter yang dianalisis yaitu *response time*, *throughput*, CPU *usage*, dan *memory* dengan menggunakan metode *benchmark*. Hasil yang diperoleh yaitu performansi server mengalami penurunan ketika diserang DoS dibanding ketika keadaan normal. Untuk *scenario* penyerangan UDP *flood* performansi menurun sebesar 22,22%, *smurft attack* menurun sebesar 30,78%, dan penyerangan yang mempunyai efek paling besar yaitu TCP *flood* dengan penurunan performansi sebesar 86,72%.



**Kata Kunci:** Kontainer, Kubernetes, *Denial of Service* (DoS), *benchmark*.