ABSTRACT

Kubernetes is a popular container orchestration platform for simplifying and optimizing server performance. However, security issues can affect the use and performance of the Kubernetes platform. So this research will test servers on containers based on Kubernetes against Denial of Service attacks. Where DoS attacks by sending a lot of traffic continuously until it fills up the traffic and causes network resources to become unavailable. In order to analyze the effects arising from DoS attacks in the form of responsibility and server performance after the DoS attack. The tests will be carried out using three DoS attack scenarios, namely TCP flood, UDP flood, and smurf attack. The parameters analyzed were response time, throughput, CPU usage, and memory using the benchmark method. The results obtained are that server performance has decreased when attacked by DoS compared to normal conditions. For the UDP flood attack scenario, the performance decreases by 22.22%, the smurft attack decreases by 30.78%, and the attack that has the greatest effect is the TCP flood with a performance decrease of 86.72%.

Keywords: *Containers, Kubernetes, Denial of Service (DoS), benchmark*