

ABSTRACT

The application of virtualization technology in providing computing infrastructure has increased considerably in line with the development of the IT industry. Implementation of virtualization and container technology is very influential on the efficiency of cloud computing infrastructure resource management. On the concept of virtualization, a system that can provide a virtualization technique that is capable of providing a system with performance close to or equal to the native is required. One of the factors that affect the performance of a virtualization technique is security. There are many types of attacks on computer systems, one of them is Denial of service, this type of attack is constantly evolving in various forms.

In this final project, a research will be conducted on container performance using Docker platform under DoS SYN flood attack. This study aims to analyze the performance of machines in terms of overall performance, and web services performance, which run on top of the container during normal state and under attack. The test results will be analyzed by comparing the performance native machine.

From the test results discovered that Denial of service attacks have the impact of performance degradation on overall performance and web services, both native machines and using Docker container virtualization techniques. In the relatively light attack, the results show that the request per second parameter resulted in a decrease in performance of 40,22% in Native and 37,65% in the Docker, whereas in the response time parameter of the web server, DoS attacks resulted in increased response time on the native server by 68,922%, while at the Docker by 62,303%.

Keywords ; Cloud security, Virtualization, Container.