ABSTRACT

Docker as container virtualization has a superior position compared to other container virtualization technologies. Having a container in Docker provides many conveniences, but there are many things that must be considered, one of which is about security issues / vulnerabilities that exist in Docker. Prevention in improving system security can be done by conducting vulnerability tests to assist in the process of knowing system weaknesses before an attack occurs. Efforts to detect a vulnerability that exists in Docker can use vulnerability scanners, namely VAS and Docker Scan. At the time of testing, of course there must be a clear stage, therefore the standard used in this study is NIST 800-115, this standard is carried out for testing simulations with stages starting from the planning, discovery, attack and reporting stages. Therefore, vulnerability analysis in Docker is carried out based on vulnerabilities and threats. The results of the analysis can be used to carry out several steps that will later get the results of exploits and total attack threats that will be used in risk analysts. The highest risk analysis result using OpenVas is 116 on WordPress User IDs and User Names Disclosure and the highest risk analysis result using Docker Scan is 88.5 on Information Exposure Improper Input Validation and Improper Input Validation

Keywords — ***docker, nist,OpenVAS,vulnerabilities***