ABSTRACT

Docker is an open-source project that provides an open platform for developers and sysadmins to be able to build, package, and run applications anywhere as a lightweight container. This study uses Vulnerable Docker, a Virtual Machine containing vulnerable Docker created by NotSoSecure company, a company that focuses on computer security. This study aims to empirically test the vulnerability analysis in Vulnerable Docker using a vulnerability scanner concerning the CIS Control framework. The purpose of this research can be achieved by conducting experiments to collect the necessary data, analyzing the results of exploits that have been carried out on Vulnerable Docker, and finally making conclusions in the form of reports that are adapted to the CIS Control framework. The Vulnerability Scanner used in this study are AlienVault OSSIM and Docker Bench for Security. In this study, the highest risk was found at the application level, namely the risk caused by the WordPress User IDs and User Names Disclosure type vulnerability through AlienVault scanning. And at the system level caused by a vulnerability type Enable User Namespace Support. There are 6 controls in the CIS Control V8 that are used to reduce the risk that occurs in this study.

Keywords— ***docker, vulnerability, alienvault, cis control***