ABSTRACT

VULNERABILITY MANAGEMENT ANALYSIS ON VULNERABLE DOCKER AND DOCKER IMAGES USING DOCKER SCAN *AND OPENSCAP BASED ON NIST CSF STANDARDS*

By

Fitria Nikmatul Hidayah

NIM : 1202184160

This study analyzes the Docker and Docker Images vulnerability management process using the NIST CSF standard. The vulnerability search uses two scanning tools , namely Docker scan and OpenSCAP. Vulnerabilities in docker and docker images version - 1, were overcome by creating a new system, namely version - 2 which upgrades the Docker software and Docker Images. The NIST (National Institute of Technologies) CSF (Cybersecurity Framework) standard is limited to the Identify, Protect, Detect, Respond, and Recover cores. The test scenario was run by scanning for vulnerabilities on two versions of the trial system. (displays the most number of scanning results) and (results from NIST). From the results of the analysis of the data that has been collected, the results obtained regarding the comparison of total anomalies and events, namely OpenSCAP is faster in generating vulnerability data with a percentage of 33.33% in version – 1 and 92.5% in version – 2, the comparison of total vulnerabilities with the results of version-1 has the percentage of total vulnerabilities is greater that is as much as 100% in version – 1 and 7.62% in version – 2, there are 6 vulnerabilities that reappear, there are 18 vulnerabilities that were not found again, how long does it take to recover, and remediation categories for vulnerabilities found includes critical and non-critical. Suggestions from this study are to use more detailed software vulnerability tools scanning, expand research on vulnerability management life cycles, and use all categories of the five core NIST CSF frameworks.

Keywords: Management, Docker, Vulnerability, NIST CSF