ABSTRACT

ANALYSIS OF RISK ESTIMATION WITHIN DC-1, VULNIX, AND VULNOS USING ALIENVAULT AND QUALYS BASED ON MITRE ATT&CK MODEL

By

INAS MUTHIA

NIM : 1202164225

The use of framework and security tools is such a support for the cyber security department of an organization to identify vulnerabilities, risk probability, and decision. This research compares the vulnerability scan results of AlienVault and Qualys with the parameters of the vulnerabilities identification and time required to conduct a vulnerability scan. The research steps use the MITRE ATT&CK model. The testing scenario is executed by running the vulnerability scan toward the three vulnerability operating system, those are DC-1, Vulnix, and VulnOS using AlienVault and Qualys. The report generated from vulnerability scan contains the number of vulnerabilities on each severity level, vulnerabilities information and description, scan time, and time required to generate a vulnerability scan report. The result of the research shows that Qualys has more effective time than AlienVault to generate a vulnerability scan report. The highest risk score estimation owned by Drupal Core vulnerabilities that existed in DC-1. Vulnerabilities classification of DC-1, Vulnix, and VulnOS both from AlienVault and Qualys report have the same category of tactic and techniques mapped in MITRE ATT&CK matrices.

Keywords: Vulnerability operating system, AlienVault, Qualys, MITRE ATT&CK framework