ABSTRACT

ANALYSIS OF VULNERABILITIES USING ALIENVAULT AND QUALYS IN *VULNERABILITY OPERATING SYSTEM* ON CYBER KILL *FRAMEWORK*

By

BOBBY ABDULLAH

NIM : 1202164334

Many parties are not responsible for data robbery, data manipulation, by exploiting vulnerabilities in a system. The results of research made by the Federal Bureau of Investigation (FBI) and the Internet Crime Complaint Center (IC3) in 2019 brought losses due to global cyber crime activities to reach 3.5 billion USD. This study compares the results of vulnerability scanning between two open source software tools (AlienVault and Qualys) with the test parameters for indicating vulnerability. This research uses the CYBER KILL framework. Simulations were carried out using the vulnerability operating systems (VulnOS2, Vulnix, and DC-1) on VirtualBox as research objects for scanning and AlienVault and Qualys as scanning managers. The test scenario being run is to perform vulnerability scanning for three vulnerability operating systems using AlienVault and Qualys. Reports generated from the AlienVault and Qualys vulnerability scans containing the number of vulnerabilities, as well as information and descriptions of the vulnerabilities. From the results of risk calculation using the formula Risk = Vulnerability x Threat, the results show that the vulnerability of Drupal Core Multiple Security Vulnerabilities (SA-CORE-2016-001) has the highest score with a total risk score: 433.5, then an analysis of the exploitation of threats to vulnerability based on Cyber Kill Chain framework and the results show that the exploitation of threats to vulnerabilities is Drupal Core type.

Keywords: (*AlienVault, Qualys, Vulnerability, Open Source, Tools, Framework, Cyber Kill, Cyber*)