

ABSTRACT
ANALYSIS VULNERABILITY USING ALIENVAULT AND
QUALYS SOFTWARE IN THE VULNERABILITY OPERATING
SYSTEM BASED ON FRAMEWORK STRIDE

By
VRESELIANA AYUNINGTYAS
1202160234

The rapid development of information technology has made security very important. Besides easy access, there are also threats to vulnerabilities in information technology. The number of cyber attacks in 2019 shows the fifth rank with a total of 1,494,281, this data is supported by the statistics of cyber attacks released by the Honeynet Project BSSN. Therefore a vulnerability analysis software is needed. Vulnerability is a weakness in the system or design used when intruders execute commands, access unauthorized data and carry out denial of service attacks. The analysis was performed using one of the functions of AlienVault and Qualys software, namely Vulnerability Assessment. Vulnerability Scanning results are analyzed, then calculated with the formula $\text{risk} = \text{vulnerability} \times \text{threat}$. Threat is obtained from a sample walkthrough analysis, as a reference for exploitation that is often done. The results of the risk estimation with the number 73 have the highest risk of 75 as many as 5 risks, then the risk estimation is analyzed again using the STRIDE framework with the result that one functions does not accommodate the type of risk that exist, namely Spoofing.

Keywords: vulnerable machine, vulnerability, threats, framework STRIDE.