ABSTRACT

SECURITY AUDITING IN VULNERABLE MACHINE USING OPEN SOURCE IDS AND VULNERABILITY SCANNER BASED ON NIST CYBERSECURITY FRAMEWORK

By

HERI SULTAN FRANSISCUS SITINJAK

NIM : 1202164304

This research is to determine the risk profile of a vulnerable machine. The vulnerable machine used in this study is Typhoon OS through a security audit process. Security audits are needed to find out the importance of the OS required by the attack and compile a solution for the OS. The framework used in this study is the NIST cybersecurity framework, because the NIST cybersecurity framework is a defensive framework and is suitable for this research. Applications used to support the research audit process are OpenVAS and Suricata. OpenVAS is used because it has a complete database with easy-to-read scans. Suricata was purchased because it has fairly complete table rules for other IDS and the application size is smaller than other IDS applications. To do the analysis in the OS. By doing a repair analysis, we can find out what attack models can be used to carry out attacks. After modeling the attack, an assault attempt was carried out using literature / walkthrough. From the experiment we will look for the relationship between vulnerability and threat. Then, from the relationship between vulnerability and threats, a risk profile will be obtained. From the results of the risk profile, it can be seen the great danger from every consideration in the OS. The vulnerability of the "GNU Bash Environment Handling Variable Shell Remote Command Exulability Vulnerabilities" had the greatest risk of cyber attacks of 85.71%, and also showed Typhoon OS 25.40% more risky than with other OS. From the results of the risk profile also shows that vulnerable machines have a high risk of cyber attacks.

***Keyword** : security auditing, vulnerable machines, framework, risk profile, attack model*