# ABSTRACT

## *SECURITY AUDITING ON VULNERABLE MACHINES USES SNORT INTRUISON DETECTION SYSTEM AND GREENBONE OPENVAS BASED ON THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY FRAMEWORK*

**By**

**KRISFIAN ADJI BRATA**

**NIM : 1202164373**

*This research is to analyze vulnerabilities and threats in determining the risk profile of vulnerable machines. The Vulnerable machine used in this research is Typhoon OS through a security auditing process. Security Auditing is needed to find out how much risk the OS is exposed to and develop a solution for the OS. The framework used in this research is the NIST cybersecurity framework, because the NIST cybersecurity framework is a defensive framework and is suitable for this research. The applications used to support this auditing process are OpenVAS and Snort. OpenVAS is used because it has a fairly complete vulnerability database and the scan results are easy to read. Snort is used because it has a fairly complete rules table compared to other IDS and for detection accuracy such as port scanning, Snort is superior to other IDS. For this reason, an analysis of existing vulnerabilities in the OS is carried out. By conducting a vulnerability analysis, it can be seen what attack models can be used to carry out attacks. Then an attack experiment using literature/walkthrough is also carried out. From the experiment, the relationship between vulnerability and threat will be searched, from the relationship between vulnerability and threat, a risk profile will be obtained. From the results of the risk profile, it can be seen how big the danger of each vulnerability that exists in the OS. Then after solving the problem, it can be seen that "CUPS < 2.0.3 Multiple Vulnerabilities" is a vulnerability with the greatest vulnerability of several existing vulnerabilities, namely with a score of 30 (50%) with Nmap as the most detected tool, which is 6 times out of six. Tried walkthrough. The results of the risk profile also show that vulnerable machines, especially Typhoons, have a high risk of cyber attacks.*

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