# *SECURITY AUDITING IMPLEMENTATION AND ANALYSIS USING OPEN SOURCE VULNERABILITY SCANNER SOFTWARE ON ANSIBLE CONTROLLER SERVER*

***By***

**HARRY WAHYU RAMADHAN**

**NIM : 1202160358**

*There are several statistics relating to information systems that can be accessed here. The data are generally conservative given that many companies do not want to be found out as having suffered a "security breach" because this information could cause "negative publicity". The company chose to remain silent and try to solve its own security problems without publication. 1996, U.S. Federal Computer Incident Response Capability (FedCIRC) reports that more than 2500 incidents of "incidents" on a computer system or computer network were caused by a failure of the security system or an attempt to break into the security system (Yuli Praptomo PHS, 2006). Therefore, this study was conducted which aims to compare the security audit of open source software on a possible server controller. The software used to support the audit process of this research is Greenbone and OpenSCAP. Greenbone is used because it has a fairly complete vulnerability database and easy-to-read scan results. OpenSCAP is used because it has a complete and integrated rule profile using satellite. The research being carried out is scanning the possible server controllers to find vulnerabilities in possible server controllers. From this group, it was found that the most vulnerable was Ansible Engine, which has 11 vulnerabilities with vulnerabilities reaching 55%. After that, a vulnerability analysis was found so that it was found that the suitable method used for this vulnerability was mitigation with a value of 60%. It is recommended to mitigate before running a server controller that possible vulnerabilities are found.*

*Keywords: Security Auditing, Server, Ansible, Greenbone, OpenSCAP, CVSSv3, vulnerability*