ABSTRACT

IMPLEMENTATION AND ANALYSIS OF SECURITY AUDITING USING OPEN SOURCE SOFTWARE WITH MITRE ATT&CK FRAMEWORK

By

MUHAMMAD ATHALLARIQ RABBANI
1202164168

Security auditing is the process of gathering and evaluating evidence to determine whether the computer system used has been able to protect the assets belonging to the organization. In this research, security auditing is conducted based on the analysis of vulnerability and threat in order to see the relationship that occurs between vulnerability and threats that have been carried out on these IT assets. In this study the object used is vulnerable operating system (VulnOSv2) with the aim to determine vulnerability and threat. In this research 10 walkthroughs are used with the aim that comparative analysis can be performed on each walkthrough and see the efficiency of each tool used. Experiments were carried out using the MITRE ATT&CK framework which is used as a basis for developing threat models and methodologies. Open source software OpenVAS can be applied to see quantitative results based on exploitation *scanning* in the form of vulnerability. Whereas qualitatively by arranging attack tree models The MITRE ATT&CK Framework created can accommodate attack tree models, which is 80%.

Keywords: Security auditing, Vulnerability, Threat, Risk, Framework MITRE ATT&CK.