ABSTRACT

IMPLEMENTATION AND ANALYSIS OF ATTACK TREE ON VULNERABLE MACHINE METASPLOITABLE2 BASED ON TIME METRIC, COST METRIC, AND FREQUENCY METRIC

By:

RHEZA DEWANTARA

1202184150

Exploitation is one of the most effective ways to defend against the increasing prevalence of cyberattacks. This research aims to implement and analyze an attack tree on the vulnerable machine Metasploitable2 based on time metric, cost metric, and frequency metric for ranking purposes, thus identifying the fastest path to access the privileged environment access target. The method used in this research involves exploit testing based on walkthroughs and creating attack trees using a SAND gate approach. The final result of all exploitation stages on the vulnerable machine Metasploitable2 was successful in accessing the privileged environment access target. All steps taken in the walkthroughs are depicted using activity diagrams, and the data flow that occurs is illustrated using data flow diagrams. The creation of the attack tree represents all stages of exploitation based on walkthroughs for ranking based on metrics. The ranking based on the time metric resulted in Attack Tree WT 1 as the fastest route with a real-time of 860.79 seconds. Ranking based on the cost metric placed Attack Tree WT 1 in the first position because it had the shortest path with a total of 20 steps. Netdiscover, Nmap, and Msfconsole ranked first in the ranking based on the frequency metric because these three tools were used in all attack trees based on the selected five walkthroughs.

Keyword: Metasploitable2, Attack Tree, Metrics