

## **ABSTRACT**

### **IMPLEMENTATION AND ANALYSIS OF ATTACK TREE ON VULNERABLE MACHINE HACKABLE 2 BASED ON TIME METRIC, COST METRIC, DAN FREQUENCY METRIC**

**By:**

**M. ZAELANI SIDIQ**

**1202184149**

The increase in cyber-attacks is growing rapidly, new vulnerabilities are still being discovered. So, exploitation is the best way to keep protected from cyber-attacks. This research aims to conduct an analysis of how the implementation of an attack tree on the vulnerable machine Hackable 2, based on time metric, cost metric, and frequency metric, results in values for ranking. This allows us to determine the quickest path to gaining root access to the target. The method used in this research involves exploitation testing based on a walkthrough and visualization using an attack tree with the SAND gate approach. The results obtained from all stages of exploitation on the vulnerable machine Hackable 2 reveal successful access to the root target. All steps taken in the walkthrough can be depicted using an activity diagram, and the data flow during these steps is illustrated with a data flow diagram. The use of an attack tree can represent all stages of exploitation based on the walkthrough for ranking based on metrics. Ranking based on the time metric yields attack tree wt 1 as the quickest path, with a real-time value of 718.52 seconds. All attack trees have the same cost metric value, which is 29 steps. Based on the frequency metric, the primary tools used in this research are Nmap and Netcat, which were used throughout the walkthrough. The most effective tools are Netdiscover, Nmap, Gobuster, and Netcat.

**Keyword:** Attack Tree, Metrics, Hackable 2