# ABSTRACT

## ATTACK TREE IMPLEMENTATION AND ANALYSIS ON SUNSET: 1 VULNERABLE MACHINE BASED ON CUBESAT SECURITY ATTACK TREE ANALYSIS AND SAND GATE APPROACH

**By:**

**Wahyu Limutu**

**1202184109**

This study implements and analyzes the attack tree on Sunset: 1 vulnerable machine using the CubeSat Security Attack Tree Analysis and SAND gate approaches. Attack tree analysis also uses the calculation of three components, namely time metric, cost metric, and frequency metric. Time, cost, and frequency values are obtained from exploitation by trying five walkthroughs from the Sunset vulnerable machine: 1. The exploitation scenario for the five walkthroughs generally has the same stages. These stages are information gathering, scanning, enumeration, exploitation, and privilege escalation, with the ultimate goal of environment access privileges. The exploitation process can be described as an activity diagram and an attack tree. Activity diagrams are used as a basis for cost metric calculations by calculating the number of steps.The attack tree represents various stages of exploitation and is ranked based on metrics, namely time, cost, and frequency. These *metrics* are the basis for obtaining an attack tree ranking. The data is based on time *metrics*; attack tree 1 is the fastest path compared to other attack trees, with a real-time value of 64.895 seconds. Data obtained based on cost metric, attack trees 1, 3, and 4 have a relatively low-cost value compared to other attack trees with a cost value of 15. Data obtained based on frequency metric, attack *tools* John The Ripper and Netdiscover have the most significant percentage in its use in the attack tree is 40% and 30%, respectively. The continuation of this research can be done by adding a vulnerability factor by scanning the security holes in the system.

Keywords: Sunset: 1, *Attack Tree, Metrics, Time, Cost, Frequency*