ABSTRAK

IMPLEMENTASI DAN ANALISA *ATTACK TREE* PADA *VULNERABLE MACHINE* TOPPO: 1 BERDASARKAN *TIME METRIC, COST METRIC,* DAN *FREQUENCY METRIC*

Oleh:

IRGI FAHREZI SALIM

NIM: 1202184270

Penelitian ini melakukan implementasi dan analisa *attack tree* pada *vulnerable machine* Toppo: 1 berdasarkan *time metric, cost metric,* dan *frequency metric*. Perhitungan *metrics* ini menggunakan tiga perhitungan *metrics* yaitu *time*, *cost,* dan *frequency.* Nilai *time, cost,* dan *frequency* didapatkan setelah melakukan eksploitasi dengan mencoba beberapa *walkthrough* hingga memperoleh *privileged environment access* dari *vulnerable machine* Toppo: 1. Skenario eksploitasi yang terdapat pada *walkthrough* memiliki beberapa tahapan yaitu, *information gathering, scanning, gaining access, exploit,* dan *privileged escalation*. Hasil akhir yang akan diperoleh setelah menyelesaikan tahapan-tahapan eksploitasi pada *vulnerable machine* Toppo: 1 adalah mendapatkan *privileged environment access* dengan cara mengakses *root* mesin target. *Walkthrough* tersebut dapat digambarkan dengan *activity diagram, activity diagram* ini dapat digunakan untuk menjelaskan tahapan-tahapan melakukan eksploitasi terhadap mesin terget. Analisa dan perumusan *attack tree* disusun dengan menggunakan pendekatan CubeSat *Security Attack Tree Analysis* dan SAND *gate*. *Attack tree* tersebut mewakili berbagai tahapan eksploitasi dan dapat dilakukan pemeringkatan berdasarkan *metrics. Metrics* tersebut dilakukan analisa untuk mendapatkan pemeringkatan *attack tree*. *Attack tree* 1 merupakan jalur tercepat secara relatif jika dibanding *attack tree* lainnya dengan nilai *real time* sebesar 167,868 detik. Data yang didapatkan berdasarkan *cost metric, attack tree* 1 memiliki nilai *cost* yang relatif rendah jika dibanding dengan *attack tree* lainnya dengan nilai *cost* 21. Data yang didapatkan berdasarkan *frequency metric, attack tools* Dirb dan Arp-scan memiliki persentase terbesar dalam penggunaannya pada lima *attack tree* sebesar 40% dan 30%. Kelanjutan dari penelitian ini dapat dilakukan dengan menambahkan faktor kerentanan dengan melakukan *vulnerability scanning* pada sistem.

Kata kunci: *Attack Tree, Time, Cost, Frequency,* Toppo: 1