ABSTRAK

IMPLEMENTASI DAN ANALISIS *ATTACK TREE* PADA *VULNERABLE MACHINE* HACKABLE 2 BERDASARKAN *TIME METRIC, COST METRIC, DAN FREQUENCY METRIC*

Oleh:

M. ZAELANI SIDIQ

1202184149

Peningkatan serangan siber semakin berkembang pesat, kerentanan baru masih terus ditemukan. Maka eksploitasi merupakan cara terbaik untuk melindungi diri dari serangan siber. Penelitian ini bertujuan untuk melakukan analisis bagaimana implementasi attack tree terhadap *vulnerable machine* Hackable 2 berdasarkan *time metric*, *cost metric*, dan *frequency metric* yang menghasilkan nilai untuk dilakukan pemeringkatan, sehingga dapat mengetahui jalur tercepat untuk mengakses root target. Metode yang digunakan pada penelitian ini adalah pengujian eksploitasi berdasarkan *walkthrough* dan melakukan visualisasi menggunakan *attack tree* dengan pendekatan SAND *gate*. Hasil yang diperoleh dari seluruh tahapan eksploitasi pada *vulnerable machine* Hackable 2 adalah, berhasil mengakses root target. Seluruh tahapan yang dilakukan pada *walkthrough* dapat digambarkan dengan *activity diagram* dan alur data yang terjadi digambarkan dengan *data flow diagram*. Penggunaan *attack tree*, dapat mewakili seluruh tahapan eksploitasi berdasarkan *walkthrough* untuk dilakukan pemeringkatan berdasarkan *metrics*. Pemeringkatan berdasakan *time metric* menghasilkan *attack tree* wt 1 sebagai jalur tercepat dengan *real time* sebesar 718,52 detik. Seluruh *attack tree* memiliki nilai *cost metric* yang sama yaitu 29 langkah. Berdasarkan *frequency metric, tools* utama pada penelitian ini adalah Nmap dan Netcat yang digunakan pada seluruh *walkthrough*, dan tools yang paling efektif adalah Netdiscover, Nmap, Gobuster, dan Netcat.

Kata kunci: Attack Tree, Metrics, Hackable 2