ABSTRAK

IMPLEMENTASI DAN ANALISIS *ATTACK TREE* PADA *VULNERABLE MACHINE* METASPLOITABLE2 BERDASARKAN *TIME METRIC, COST METRIC,* DAN *FREQUENCY METRIC*

Oleh:

RHEZA DEWANTARA

1202184150

Eksploitasi merupakan salah satu cara terbaik untuk melindungi diri dari serangan siber yang sedang marak terjadi. Penelitian ini bertujuan untuk melakukan implementasi dan analisis dari *attack tree* terhadap *vulnerable machine* Metasploitable2 berdasarkan *time metric*, *cost metric*, dan *frequency metric* yang dilakukan untuk pemeringkatan, sehingga dapat mengetahui jalur tercepat untuk mengakses *privileged environment access* target. Metode yang digunakan pada penelitian ini adalah pengujian eksploitasi berdasarkan *walkthrough* dan melakukan penggambaran menggunakan *attack tree* dengan pendekatan SAND *gate*. Hasil akhir dari seluruh tahapan eksploitasi pada *vulnerable machine* Metasploitable2 adalah berhasil mengakses *privileged environment access* target. Seluruh langkah yang dilakukan pada *walkthrough* digambarkan dengan *activity diagram* dan alur data yang terjadi digambarkan dengan *data flow diagram*. Penggambaran *attack tree* mewakili seluruh tahapan eksploitasi berdasarkan *walkthrough* untuk dilakukan pemeringkatan berdasarkan *metrics*. Hasil pemeringkatan yang dilakukan berdasakan *time metric* menghasilkan *Attack tree* WT 1 sebagai waktu tempuh tercepat dengan *real time* sebesar 860,79 detik. Pemeringkatan berdasarkan *cost metric* menghasilkan *attack tree* WT 1 sebagai peringkat pertama karena jalur paling pendek dengan total 20 langkah. Netdiscover, Nmap, dan Msfconsole menjadi peringkat pertama pada pemeringkatan berdasarkan *frequency metric* karena ketiga *tools* tersebut digunakan pada semua *attack tree* berdasarkan lima *walkthrough* yang telah dipilih.

Kata kunci: Metasploitable2, *Attack Tree, Metrics*