BAB I. PENDAHULUAN

I.1 Latar Belakang

Peningkatan serangan siber semakin berkembang pesat. Perusahaan, organisasi, hingga individu memerlukan banyak sumber daya untuk melawan peretas dan menjamin keamanan sistem. Namun, kerentanan baru masih terus ditemukan. Maka eksploitasi merupakan cara terbaik untuk melindungi diri dari serangan siber (AWED, 2022). Eksploitasi dapat membantu untuk melakukan identifikasi kerentanan pada sistem sebelum peretas melakukan eksploitasi terhadap sistem, sehingga dapat melindungi berbagai sumber daya yang terdapat pada sistem. Metode yang dapat digunakan untuk melakukan eksplotasi dengan waktu dan biaya yang terjangkau adalah dengan menggunakan *vulnerable machine*, kemudian melakukan analisis berdasarkan hasil eksploitasi yang dilakukan dengan menggunakan *attack tree*.

Attack tree merupakan model keamanan yang digunakan untuk memberikan gambaran secara visual terhadap serangkaian langkah yang perlu dilakukan oleh penyerang dengan tujuan untuk mengambil alih suatu sistem atau jaringan komputer. Pada *attack tree* setiap langkah serangan yang dilakukan, digambarkan sebagai simpul atau *node* dengan menggunakan struktur pohon dan menghasilkan nilai yang bisa dihitung menggunakan *metrics*. *Metrics* merupakan sebuah nilai yang digunakan untuk menggambarkan karakteristik atau sifat dari simpul pada *attack tree* seperti waktu, biaya, frekuensi, probabilitas keberhasilan serangan, tingkat kesulitan dalam melakukan serangan, peralatan khusus yang dibutuhkan dalam serangan, hingga kombinasi dari semua metrik tersebut. Penggunaan *metrics* dapat membantu untuk mengevaluasi risiko eksploitasi sistem secara lebih rinci dan objektif (Kuipers, 2020). Hasil perhitungan *metrics* dapat digunakan sebagai dasar untuk memberikan peringkat pada *attack tree*. Dengan memberikan peringkat terhadap *attack tree*, dapat dilakukan identifikasi pada simpul-simpul yang paling rentan dan menentukan prioritas tindakan pencegahan untuk melindungi sistem dari serangan siber.

Penelitian ini berfokus pada implementasi dan analisis *attack tree* pada *vulnerable machine* Hackable 2 dengan menggunakan *time metric*, *cost metric*, dan *frequency*

metric. Pada penelitian ini, menggunakan sebuah *vulnerable machine* bernama Hackable 2 sebagai objek untuk melakukan eksploitasi terhadap kerentanan. *Vulnerable machine* Hackable 2 merupakan sebuah sistem operasi berbasis Linux yang dirancang khusus oleh Elias Sousa pada tanggal 15 Juni 2021 sebagai sarana latihan untuk mengembangkan keterampilan serta wawasan mengenai penetrasi pada sistem atau jaringan komputer.

I.2 Perumusan Masalah

Berdasarkan pada latar belakang yang telah diuraikan, dapat diambil beberapa permasalahan yang perlu dipecahkan pada penelitian ini. Permasalahan tersebut antara lain:

a. Bagaimana cara menyusun alur eksploitasi berdasarkan empat *walkthrough* yang telah dipilih pada *vulnerable machine* Hackable 2?
b. Bagaimana cara membuat *attack tree* dari empat *walkthrough* yang telah dipilih pada *vulnerable machine* Hackable 2?
c. Bagaimana cara membuat pemeringakatan pada *attack tree* yang dibuat untuk *vulnerable machine* Hackable 2?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mencapai hal-hal sebagai berikut.

a. Memahami praktik empat *walkthrough* pada *vulnerable machine* dengan penggambaran *activity diagram* dan *data flow diagram*.
b. Menyusun *attack tree* berdasarkan SAND *gate* dari empat *attack tree* yang digabungkan.
c. Melakukan pemeringkatan pada *attack tree* dengan menghitung nilai *metrics* (*time metric*, *cost metric*, dan *frequency metric*).

I.4 Batasan Penelitian

Penelitian ini memiliki beberapa batasan yang perlu diperhatikan, yaitu:

a. Penelitian dilakukan berdasarkan simulasi eksperimen dengan menggunakan empat *walkthrough* yang telah dipilih pada *vulnerable machine* yang telah dipilih untuk mengetahui *attack tree*.

b. Perhitungan *metrics* yang dilakukan hanya mencakup *time, cost*, dan *frequency* untuk menentukan pemeringkatan *attack tree*. *Time metric* menyajikan informasi seputar waktu eksekusi dari eksploitasi yang dijalankan, namun tidak membahas proses pemilihan *tools* dan alur eksploitasi secara detail.
c. Penelitian tidak membahas kerentanan atau *vulnerability* yang terdapat pada sistem.

I.5 Manfaat Penelitian

Penelitian ini memiliki manfaat sebagai berikut:

a. Secara akademik, penelitian ini dapat menambah wawasan, pengetahuan, dan pengalaman tentang praktik *walkthrough*, *attack tree*, dan pemeringkatan berdasarkan *attack tree*.
b. Secara praktis, penelitian ini dapat memberikan perhitungan *metrics* yang berguna dalam menentukan pemeringkatan pada *attack tree*. Dengan demikian, hasil penelitian ini dapat membantu ahli keamanan siber dalam melakukan evaluasi risiko dan memperkuat keamanan sistem.

I.6 Sistematika Penelitian

Struktur penulisan pada penelitian ini terdiri dari enam bab yang disusun sebagai berikut:

BAB I **PENDAHULUAN**

Bab ini berisi penjelasan mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, serta struktur penulisan yang digunakan dalam penelitian ini.

BAB II **TINJAUAN PUSTAKA**

Bab ini berisikan tentang beberapa teori-teori mulai dari keamanan sistem informasi, keamanan informasi, keamanan sistem informasi, *threat* / ancaman, eksploitasi, sistem operasi, Kali Linux, *vulnerable machine* Hackable 2, keamanan sistem operasi, eksperimen, *walkthrough*, *activity*

diagram, data flow diagram, attack tree, attack trees with SAND *gate, metrics, time metric, cost metric, frequency metric,* dan penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini membahas model konseptual yang mendeskripsikan solusi dari permasalahan penelitian berupa lingkungan eksperimen, elemen penelitian, dan dasar ilmu yang digunakan pada penelitian. Lalu, sistematika penelitian yang berisi mengenai tahapan penelitian dari tahap awal hingga akhir menggunakan *attack tree* dan *metrics.* Pada Bab ini juga berisi metode pengumpulan data menggunakan *activity diagram, data flow diagram, metrics,* dan *attack tree* metode pengolahan data menggunakan *attack tree* dan *metrics*, serta metode evaluasi dengan melakukan pemeringkatan *attack tree* berdasarkan *metrics.*

BAB IV DESAIN EKSPERIMEN DAN SKENARIO TESTING

Bab ini menjelaskan tentang perancangan dan penggunaan *tools open-source* untuk mengimplementasikan skenario eksperimen. Bab ini juga membahas *output* atau hasil dari percobaan tersebut, seperti skenario pengujian, *activity* diagram, *data flow* diagram, serta pengukuran waktu berdasarkan *walkthrough*. Dengan demikian, bab ini dapat memberikan gambaran tentang metode yang digunakan dalam penelitian untuk mencapai hasil yang diinginkan.

BAB V ANALISIS

Bab ini berisi analisis dari hasil eksperimen pada bab sebelumnya yang mencakup pengukuran waktu *walkthrough, activity* diagram, dan *data flow* diagram. Data tersebut kemudian dianalisis menggunakan metode pembuatan *attack tree* beserta *metrics*. Selanjutnya, dilakukan pemeringkatan berdasarkan hasil analisis dari *attack tree* dan *metrics* untuk menentukan tingkat

kerentanan dan risiko eksploitasi sistem. Bab ini memberikan gambaran tentang proses analisis dan evaluasi data dalam penelitian serta hasil kesimpulan yang dapat diambil dari analisis tersebut.

BAB VI KESIMPULAN DAN SARAN

Bab ini menyajikan kesimpulan dari penelitian yang telah dilakukan, termasuk perancangan dan skenario pengujian, analisis data, serta saran untuk penelitian selanjutnya. Bab ini memberikan gambaran tentang hasil penelitian secara keseluruhan, dengan mempertimbangkan tujuan penelitian dalam konteks eksploitasi sistem. Selain itu, bab ini juga memberikan rekomendasi atas temuan dan hasil penelitian, serta memberikan arahan untuk penelitian masa depan di bidang keamanan siber.