# BAB I. PENDAHULUAN

## I.1 Latar Belakang

Perkembangan teknologi telah mengakibatkan peningkatan serangan siber. Perusahaan-perusahaan memerlukan banyak sumber daya agar dapat melawan peretas dan menjamin keamanan sistem, namun kedapatan adanya kerentanan baru masih terus ditemukan. Oleh karena itu, pengujian eksploitasi merupakan cara terbaik untuk melindungi diri dari serangan siber (AWED, 2022). Dengan pengujian eksploitasi, perusahaan ataupun organisasi dapat mengidentifikasi kerentanan pada sistem sebelum peretas mengeksploitasi, sehingga banyak sumber daya dapat diamankan. Cara yang dapat dilakukan untuk melakukan pengujian eksploitasi dengan waktu dan biaya yang terjangkau adalah dengan menggunakan *vulnerable machine*, kemudian menganalisisnya menggunakan *attack tree*.

*Attack tree* memberikan gambaran visual tentang bagaimana penyerang dapat mengeksploitasi kerentanan dalam sistem menjadi lebih mudah dipahami. *Attack tree* memiliki bagian yang dapat dihitung nilainya, yaitu *metrics*. *Metrics* merupakan nilai numerik yang menggambarkan karakteristik atau sifat dari simpul *attack tree* seperti waktu, biaya, frekuensi, probabilitas keberhasilan serangan, tingkat kesulitan dalam melakukan serangan, peralatan khusus yang dibutuhkan dalam serangan, dan kombinasi dari semua metrik tersebut. Dengan menggunakan *metrics*, ahli keamanan siber dapat mengevaluasi risiko keamanan sistem secara lebih rinci dan objektif (Kuipers, 2020). *Metrics* yang dihitung dapat digunakan sebagai dasar untuk melakukan pemeringkat pada *attack tree* sehingga dapat mengidentifikasi pada simpul yang paling rentan dan menentukan prioritas tindakan pencegahan untuk melindungi sistem.

Penelitian ini berfokus pada implementasi dan analisis *attack tree* pada *vulnerable machine* Metasploitable2 dengan menggunakan *time metric*, *cost metric*, dan *frequency metric*. *Attack tree* dapat digunakan sebagai dasar untuk memperkuat keamanan sistem dengan menganalisis cara-cara serangan terhadap sistem tersebut, serta dapat menjadi panduan untuk mengetahui jalur tercepat dan biaya rendah dalam melakukan serangan berdasarkan pemilihan *metrics*.

## I.2 Perumusan Masalah

Dari latar belakang yang telah diuraikan, terdapat beberapa permasalahan yang perlu dipecahkan dalam penelitian ini. Permasalahan tersebut antara lain:

a. Bagaimana cara menyusun alur eksploitasi berdasarkan lima *walkthrough* yang telah dipilih pada *vulnerable machine* Metasploitable2?
b. Bagaimana cara membuat *attack tree* dari lima *walkthrough* yang telah dipilih pada *vulnerable machine* Metasploitable2?
c. Bagaimana cara membuat pemeringakatan pada *attack tree* yang dibuat untuk *vulnerable machine* Metasploitable2?

## I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mencapai hal-hal sebagai berikut.

a. Memahami praktik lima *walkthrough* pada *vulnerable machine* dengan penggambaran *activity diagram* dan *data flow diagram*.
b. Menyusun *attack tree* berdasarkan SAND *gate* dari lima *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 di perhatikan, yaitu:

a. Penelitian dilakukan berdasarkan simulasi eksperimen dengan menggunakan lima *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*.
c. Penelitian tidak membahas kerentanan atau *vulnerability* yang terdapat pada sistem.
d. *Time metric* menyajikan informasi seputar waktu eksekusi dari eksploitasi yang dijalankan, namun tidak membahas proses pemilihan *tools* dan alur eksploitasi secara detail.

## 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** **METODOLOGI PENELITIAN**

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* Metasploitable2, 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 kerangka kerja yang jelas dan terstruktur, sistematika penelitian untuk menjelaskan semua tahap dalam penelitian dan memberikan gambarannya, metode pengumpulan data

yang didapatkan dari hasil eksperimen (*activity diagram, data flow diagram, metrics, dan attack tree)*, metode pengolahan data dari hasil data yang telah didapatkan, dan metode evaluasi untuk melakukan perbandingan *attack tree* berdasarkan *metrics* dengan tujuan mendapatkan jalur tercepat.

**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 keamanan 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 *attack tree*.