BAB I PENDAHULUAN

I.1 Latar Belakang

Data-data komputer merupakan data yang berharga karena mengandung informasi penting. Oleh sebab itu dibutuhkan keamanan informasi untuk melindungi data-data tersebut. Keamanan informasi merupakan proses memproteksi informasi dan sistem informasi dari pengaksesan, pemakaian, publikasi, perubahan, atau perusakan secara ilegal (Garfinkel, Schwartz, & Pafford, 2003). Salah satu fungsi nyata dari keamanan informasi adalah untuk mengantisipasi penipuan atau menyadari penipuan pada sebuah sistem yang memiliki basis informasi, yang informasinya tidak memiliki arti fisik. Jika terdapat celah keamanan informasi, maka dengan mudah penyerang akan memanfaatkannya untuk masuk ke dalam sistem

Penyerang mengidentifikasi dan mengeksploitasi kerentanan dalam sistem komputer atau jaringan, biasanya untuk mendapatkan akses tidak sah ke data pribadi atau organisasi (Lab, 2022). Dengan semakin majunya teknologi, penyerang bisa memakai banyak jalur untuk memanfaatkan celah keamanan sistem komputer atau jaringan dengan tujuan mendapat keuntungan untuk dirinya sendiri. Pilihan terbaik yang bisa dipakai oleh penyerang untuk melalui jalur tercepat dalam peretasan adalah dengan memakai *attack tree*.

Attack tree menurut (Moore, Ellison, & Linger, 2001) adalah struktur data bercabang dan hierarkis yang mewakili serangkaian pendekatan potensial untuk mencapai suatu peristiwa di mana keamanan sistem ditembus atau disusupi dengan cara tertentu. *Attack tree* memiliki bagian yang akan dihitung nilainya, bagian itu disebut *metrics* (Kuipers, 2020). Perhitungan *metrics* diantaranya yaitu waktu, biaya, frekuensi, kemungkinan untuk berhasil menyerang, tingkat kemampuan yang dibutuhkan untuk melakukan penyerangan, peralatan khusus untuk melakukan penyerangan, dan kombinasi dari semua *metrics* (Kuipers, 2020). Hasil perhitungan dari *metrics* akan dijadikan landasan untuk perangkingan *attack tree*.

Penelitian ini bertujuan untuk mengetahui perumusan *attack tree* dengan menggunakan pendekatan CubeSat *Security Attack Tree Analysis* dan *Sequential* AND *gate* (SAND *gate*), serta mengetahui *attack tree* tercepat berdasarkan analisa *metrics.* Bagi penyerang, *attack tree* tercepat bisa digunakan untuk melakukan eksploitasi pada sistem dengan alokasi waktu sesedikit mungkin. Bagi pengelola *server, attack tree* bisa digunakan sebagai dasar penguatan keamanan sistem dengan menganalisis cara-cara di mana sistem dapat diserang. Perumusan *attack tree* ini menggunakan *Vulnerable Machine* (VM) Sunset: 1. Sunset: 1: adalah sebuah *vulnerable machine* sederhana yang dirilis oleh whitecr0wz pada 29 Juli 2019 di situs web vulnhub.com dengan tujuan memperkaya pengalaman dalam segmen eksperimen dan *penetration testing*.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini:

1. Bagaimana merumuskan alur eksploitasi berdasarkan 5 *walkthrough* pada *vulnerable machine* Sunset: 1?
2. Bagaimana penyusunan *attack tree* dari 5 *walkthrough* pada *vulnerable machine* Sunset: 1?
3. Bagaimana mendapatkan perangkingan *attack tree* pada *vulnerable machine* Sunset: 1?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah di atas, maka tujuan dari penulisan Tugas Akhir ini adalah:

1. Mengetahui implementasi *walkthrough* pada *vulnerable machine* dengan penggambaran *activity diagram* dan *data flow diagram.*
2. Merumuskan *attack tree* dengan menggunakan pendekatan CubeSat *Security Attack Tree Analysis* dan SAND-*gate* dari penggabungan 5 *attack tree.*
3. Menyusun rangking *attack tree* berdasarkan perhitungan nilai *metrics.*

I.4 Batasan Penelitian

Batasan pada penelitian ini yaitu:

1. Penelitian berdasarkan simulasi eksperimen dilakukan berdasarkan 5 buah *walkthrough* dari *vulnerable machine* untuk mengetahui *attack tree*.
2. Perhitungan *metrics* hanya sebatas *time*, *cost*, dan *frequency* untuk mengetahui rangking *attack tree*.
3. *Time metric* hanya menghitung waktu eksekusi dari tahapan eksploitasi, dan tidak membahas bagaimana proses pemilihan *tools* dan alur eksploitasi.
4. Tidak membahas tentang *vulnerability* yang ada pada sistem.

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Secara keilmuan bisa menambah wawasan mengenai *walkthrough*, *attack tree*, dan kategorisasi *attack tree*.
2. Secara praktis dapat memberikan perhitungan berdasarkan *metric-metric* yang terbatas untuk menemukan rangking *attack tree.*

I.6 Sistematika Penelitian

Sistematika penulisan pada penelitian ini terdiri dari tujuh Bab, yang tersusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi penjelasan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini berisi literatur-literatur yang sesuai dengan permasalahan yang diteliti pada penelitian ini. Mencantumkan teori, metode, alat-alat yang dipakai dalam melakukan eksperimen, serta menunjukkan penelitian terdahulu yang berkaitan dengan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan mengenai konseptual model untuk merumuskan solusi dari permasalahan yang ada. Selain itu, ada juga sistematika penelitian yang digunakan untuk menjelaskan langkah-langkah penyelesaian masalah.

BAB IV PERANCANGAN DAN SKENARIO PENGUJIAN

Bab ini berisi penjelasan rancangan sistem dan penggunaan *open source tools* terhadap skenario eksperimen. Serta keluaran berupa *activity diagram*, *data flow diagram*, dan pengukuran *time* berdasarkan *walkthrough*.

BAB V ANALISIS

Bab ini berisi analisis dari data hasil pengukuran *walkthrough* yang telah dilakukan pada Bab sebelumnya mengenai *activity diagram, data flow diagram* dan pengukuran *time walkthrough*. Dari data tersebut kemudian akan dianalisis menggunakan *attack tree* dan *metrics* serta dilakukan perangkingan.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi penjelasan kesimpulan dari penelitian yang telah dilakukan, rancangan sistem dan skenario pengujian, perancangan dan analisis usulan, serta memberikan saran untuk penelitian selanjutnya.