BAB I PENDAHULUAN

I.1 Latar Belakang

Keamanan informasi adalah bagian terpenting dari pengelolaan organisasi, aktivitas TI dapat terganggu ketika masalah timbul pada keamanan informasi terkait kerahasiaan, integritas, dan ketersediaan. Keamanan informasi merupakan upaya untuk melindungi sumber daya TI yang dimiliki. Tujuan dari keamanan informasi ini adalah untuk memastikan kelangsungan sistem dan mitigasi potensi risiko kerusakan pada sistem (Utomo, Ali & Affandi, 2012). Jika terdapat celah keamanan pada informasi maka, penyerang akan dengan mudah mengambil alih sistem dan data yang telah dibangun oleh organisasi.

Penyerang atau *hacker* merupakan seseorang atau sekumpulan orang yang melakukan kegiatan pembobolan sistem. Jika aktivitas berlangsung di jaringan komputer, seorang peretas dapat memperoleh akses ke jaringan dan mendapatkan akses ke semua pengguna sistem yang terhubung ke jaringan (Diskominfo, 2018). Seiring dengan perkembangan teknologi maka para penyerang memiliki banyak cara untuk melakukan penyusupan pada suatu sistem ataupun peretasan kelemahan pada web *server* untuk keuntungan pribadi maupun organisasi. Salah satu cara untuk mengetahui celah keamanan pada *vulnerable machine* dengan waktu dan biaya yang sedikit yaitu, dapat disusun menggunakan *attack tree.*

Attack tree adalah sebuah diagram atau model matematis berstruktur *tree* yang mewakili sistem yang ingin diambil alih oleh penyerang. Model *attack tree* ini menggambarkan pilihan atau tujuan yang dilakukan penyerang. *Attack tree* ini terdiri dari, simpul atas yang mewakili tujuan akhir penyerang dan simpul paling bawah menggambarkan operasi yang dilakukan penyerang untuk mengeksploitasi kerentanan dalam pertahanan sistem (Ingoldsby, 2021). *Attack tree* memiliki bagian yang dapat dilakukan perhitungan nilainya, bagian tersebut dinamakan *metric. Metrics* memiliki beberapa perhitungan *metrics* yaitu, waktu, biaya, frekuensi, probabilitas untuk berhasil menyerang, tingkat kemampuan yang dibutuhkan untuk melakukan penyerangan, peralatan khusus yang dibutuhkan serangan, dan kombinasi dari semua metrik (Kuipers, 2020). Hasil perhitungan

metrics tersebut dapat digunakan sebagai landasan untuk pemeringkatan *attack tree*.

Pada penelitian ini berfokus pada implementasi dan analisa *attack tree* pada *vulnerable machine* Toppo: 1 berdasarkan *time metric*, *cost metric*, dan *frequency metric*. Bagi pengelola *server*, *attack tree* dapat digunakan sebagai dasar penguatan keamanan sistem dengan menganalisa cara-cara di mana sistem itu diserang. Sedangkan bagi penyerang, *attack tree* hasil akhirnya dapat digunakan untuk mengetahui jalur tercepat dan dengan *cost* rendah berdasarkan analisa *metric*. Toppo: 1 merupakan sebuah *vulnerable machine operating system* (OS) yang sederhana. *Vulnerable machine* Toppo: 1 merupakan serangkaian Sistem Operasi (OS) yang dibuat untuk melatih, menambah wawasan, dan pengetahuan mengenai penetrasi. Toppo: 1 dikembangkan oleh Hadi Mene pada 12 Juli 2018 pada *website* Vulnhub.

I.2 Perumusan Masalah

Berdasarkan latar belakang di atas maka, rumusan masalah yang mendasari penelitian ini adalah:

1. Bagaimana menyusun alur eksploitasi berdasarkan *walkthrough* pada *vulnerable machine* Toppo: 1?
2. Bagaimana merancang *attack tree* dari lima *walkthrough* pada *vulnerable machine* Toppo: 1?
3. Bagaimana mendapatkan peringkat *attack tree* pada *vulnerable machine* Toppo: 1?

I.3 Tujuan Penelitian

Berdasarkan perumusan masalah di atas maka, penelitian ini bertujuan untuk:

1. Memahami implementasi *walkthrough* pada *vulnerable machine* dengan penggambaran *activity diagram* dan *data flow diagram*.
2. Menyusun *attack tree* berdasarkan pendekatan CubeSat *Security Attack Tree Analysis* dan SAND *gate* dari penggabungan lima *attack tree*.
3. Melakukan penyusunan peringkat *attack tree* berdasarkan perhitungan nilai *metrics*.

I.4 Batasan Penelitian

Berikut ini merupakan batasan penelitian ini sebagai berikut:

1. Penelitian berdasarkan simulasi eksperimen dilakukan dengan 5 buah *walkthrough* pada *vulnerable machine* untuk mengetahui *attack tree.*
2. Perhitungan *metrics* hanya sebatas pada *time, cost,* dan *frequency* untuk mengetahui pemeringkatan pada *attack tree.*
3. Tidak akan membahas tentang *vulnerability* yang terdapat pada sistem.
4. *Time metric* hanya mencakup waktu eksekusi dari eksploitasi yang dijalankan, tidak membahas terkait proses pemilihan *tools* dan alur eksploitasi.

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Secara keilmuan, penelitian ini bermanfaat untuk menambah wawasan, pengetahuan, dan pengalaman mengenai *walkthrough, attack tree,* dan pemeringkatan berdasarkan *attack tree.*
2. Secara praktis, penelitian ini bermanfaat untuk memberikan perhitungan-perhitungan berdasarkan *metrics* untuk menemukan pemeringkatan *attack tree*.

I.6 Sistematika Penelitian

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

BAB I **PENDAHULUAN**

Bab ini berisikan uraian mengenai latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penelitian.

BAB II **TINJAUAN PUSTAKA**

Bab ini berisi uraian teori–teori mengenai keamanan sistem informasi, eksploitasi, *threat*, Lubuntu, *vulnerable machine T*oppo: 1, eksperimen, *walkthrough, activity diagram, data*

flow diagram, pengukuran *walkthrough, attack tree*, dan penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan mengenai model konseptual yang menjelaskan rumusan solusi dari sebuah permasalahan. Serta, sistematika penelitian yang digunakan untuk menjelaskan tahapan-tahapan penyelesaian masalah.

BAB IV DESAIN EKSPERIMEN DAN SKENARIO *TESTING*

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

BAB V ANALISIS

Bab ini berisi analisis dari data hasil eksperimen pada Bab sebelumnya mengenai pengukuran *time walkthrough, activity diagram,* dan *data flow diagram*. Dari data tersebut kemudian akan dianalisis menggunakan pembuatan *attack tree* dan *metrics.* Kemudian, dilakukan pemeringkatan berdasarkan hasil analisis *attack tree* dan *metrics.*

BAB VI KESIMPULAN DAN SARAN

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