BAB I PENDAHULUAN

I.1 Latar Belakang

Kebutuhan dan penggunaan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui internet pula komunikasi menjadi bagian terbesar dan pesat pertumbuhannya serta menembus berbagai batas negara. Akan tetapi dampak negatif pun tidak bisa dihindari. Salah satunya adalah dapat menyebabkan kemungkinan munculnya kejahatan yang disebut dengan *cybercrime*. Keamanan siber menjadi perhatian belakangan ini sehingga ada perlunya sedikit dari ribuan kemungkinan penyerangan siber dapat dianalisa dan dikaji lebih lanjut untuk menangkal dan membuat pertahanan pada perangkat komputer, salah satunya dengan penerapan *Web Aplication Firewall* (WAF).

WAF merupakan sebuah *firewall* untuk aplikasi *web* yang berfungsi untuk filterisasi lalu lintas jaringan (Tekerek & Bay, 2019). Filterisasi paket data dari lalu lintas jaringan yang ditemukan, dapat dilakukan blokir paket-paket data yang di curigai lalu dilakukan pencatatan aktifitas tersebut sehingga terlihat data untuk dianalisis lebih lanjut. Salah satu contoh dari WAF adalah ModSecurity. Untuk mendapatkan keamanan yang lebih lanjut, dilakukan analisis terhadap pengujian eksploitasi serangan yang menggunakan perlindungan dari WAF maupun non WAF agar terlihat hasil perbandingan dari pengujian tersebut.

Pada penelitian ini menggunakan WAF untuk melakukan perlindungan terhadap objek yang dipakai dalam studi kasus penelitian. Dasar kinerja dari WAF yaitu dapat melindungi objek dari serangan seperti *Brute Force*, *SQL Injection*, *XSS,* dan serangan-serangan lainnya. Pengujian pada penelitian kali ini dilakukan berdasarkan eksploitasi dan menggunakan standar dari OWASP TOP TEN yang menjadi acuan kerangka penyerangan pada objek. Hasil dari eksploitasi lantas diolah menjadi sebuah kerangka penyerangan yang disebut dengan *Attack tree*. *Attack tree* merupakan metodologi yang dapat menjelaskan keamanan sebuah sistem dengan berisikan berbagai kemungkinan dari serangan eksploitasi penyerang untuk dilakukan analisis lebih lanjut sebagai pencegahan keamanan sistem.

Pada tugas akhir ini, dilakukan implementasi dari peran kinerja WAF terhadap pengujian eksploitasi untuk diolah dan dianalisis yang menjadi hasil akhir berupa catatan pengukuran dan kumpulan data informasi yang diolah menjadi metrik metrik dan diagram penyerangan eksploitasi. Metode serangan eksploitasi yang dipakai dalam pengujian diambil berdasarkan hasil *vulnerability scanning* dan pengujian dilakukan dengan dua kondisi yaitu pada saat *web* aplikasi dalam perlindungan WAF maupun tidak. Pada analisis, dilakukan perbandingan hasil data pengujian berdasarkan metrik metrik yang diukur pada proses pengujian WAF. Hasil analisis yang didapat bertujuan untuk mengetahui karakter eksploitasi berdasarkan metrik tertentu menggunakan *attack tree*.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana mencari relasi tahapan eksploitasi pada aset IT berbasis *web*?
b. Bagaimana menyusun relasi tersebut dalam bentuk *attack tree*?
c. Bagaimana mendapatkan karakter dari beberapa *attack tree*?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Menganalisa dan menyusun relasi eksploitasi berdasarkan data eksperimen pada aplikasi berbasis *web*.
b. Menganalisa dan menyusun *attack tree* berdasarkan data dan relasi dari *activity diagram* dan *data flow diagram*.
c. Menganalisa karakter eksplotasi berdasarkan dua metrik *attack tree* pada eksploitasi tersebut.

I.4 Batasan Penelitian

Adapun batasan penelitian pada penelitian ini adalah sebagai berikut:

a. Penelitian ini berdasarkan eksploitasi pada eksperimen dan simulasi.
b. Penyusunan data dan relasi eksploitasi dilakukan tanpa melakukan tahapan *post exploitation*.
c. Pembahasan karakter *attack tree* hanya berfokus pada metrik *time* dan *cost.*

I.5 Manfaat Penelitian

Adapun manfaat yang didaptkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut:

1. Secara teoritis
    a. Dapat menambah pengetahuan terkait dengan penyusunan *attack tree* berdasarkan eksploitasi pada aplikasi berbasis *web.*
    b. Dapat mengenali karakter *attack tree* berdasarkan metrik *time* dan *cost*.
2. Secara praktis
    a. Dapat mengenali dan mengetahui eksploitasi yang berlangsung dalam waktu yang singkat serta dengan langkah pada proses eksploitasi.
    b. Untuk tahapan lebih lanjut yaitu untuk aspek penguatan aplikasi berbasis *web* dapat dilakukan sesuai dengan suatu *attack tree*.