BAB I PENDAHULUAN

I.1 Latar Belakang

Kemajuan teknologi saat ini berkembang dengan pesat yang mengakibatkan informasi dapat mudah diakses dimana saja, kapan saja, dan oleh siapa saja tanpa ada batas ruang dan waktu. Salah satu media sebagai penyebar informasi yaitu aplikasi berbasis *web*site. Dengan begitu banyaknya jumlah media serta pengguna aplikasi berbasis *web*site, menyebabkan muncul berbagai celah keamanan. Dari celah keamanan tersebut, dimanfaatkan oleh orang-orang yang tidak bertanggung jawab untuk mengambil keuntungan pribadi dan merugikan suatu pihak. Untuk meminimalisir serta mencegah hal-hal yang akan berdampak merugikan terhadap pengguna ataupun *developer* aplikasi berbasis *web*, diperlukan solusi untuk mengatasinya. Salah satu solusinya yaitu dengan menggunakan *Web Application Firewall* (WAF).

WAF merupakan firewall yang menjadi solusi untuk mengatasi permasalahan kerentanan pada aplikasi berbasis *web*. WAF memiliki kemampuan untuk melakukan *filtering* paket, memblokir lalu lintas HTTP dan juga logging. Terdapat berbagai macam WAF salah satunya yaitu ModSecurity (Agung Muzaki et al., 2020). Pada penelitian ini, WAF digunakan sebagai *service* untuk melindung objek yang digunakan dalam studi kasus penelitian. WAF berperan untuk melindungi objek dari berbagai serangan serperti *SQL Injection*, *Brute Force*, dan lainnya. Untuk menguji kinerja WAF, maka perlu dilakukan pengujian yaitu eksploitasi. Pada proses pengujian eksploitasi, dibutuhkan standar untuk menjadi acuan kerangka kerja penyerangan pada objek.

Penelitian ini akan menggunakan daftar OWASP Top Ten sebagai acuan kerentanan kemanan yang akan dilakukan eksploitasi. Eksploitasi didasarkan pada hasil proses *vulnerability scanning* dan pengujian dilakukan dalam dua kondisi yaitu dengan kondisi perlindungan dan tidak dalam perlindungan WAF. Hasil dari pengujian eksploitasi diolah menjadi sebuah relasi tahapan eksploitasi yang digambarkan menjadi *activity diagram* dan *data flow diagram*. Kemudian, kedua data tersebut diolah menjadi sebuah kerangka penyerangan yang disebut dengan

attack tree, yang menjelaskan tahapan eksploitasi hingga mendapatkan *gain access root*. Selain itu, data hasil dari implementasi pengujian eksploitasi dilakukan analisis dan menghasilkan dua metrik yaitu metrik *time* dan metrik *probability*. Selanjutnya pada tahap analisis dilakukan perbandingan data hasil pengujian eksploitasi berdasarkan kedua metrik yang telah dibuat dari hasil proses pengujian WAF untuk mengetahui karakter dari setiap *attack tree*. Dengan begitu, *attack tree* dapat digunakan oleh penyerang untuk menentukan eksploitasi sistem dengan waktu tercepat serta kemungkinan penyerangan yang dapat terjadi.

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

Berdasarkan rumusan masalah di atas, sehingga tujuan dari penelitian Tugas Akhir adalah sebagai berikut:

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 pada penelitian Tugas Akhir ini adalah sebagai berikut:

1. Penelitian ini berdasarkan eksploitasi pada eksperimen dan simulasi .
2. Penyusunan data dan relasi eksploitasi dilakukan tanpa melakukan tahapan *post exploitation*.
3. Pembahasan karakter *attack tree* hanya berfokus pada metrik *time* dan *probability*.

I.5 Manfaat Penelitian

Adapun manfaat yang didapatkan 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 *probability*.
2. Secara praktis
    a. Dapat mengenali dan mengetahui eksploitasi yang berlangsung dalam waktu yang singkat serta dengan tingkat keberhasilan yang terjadi.
    b. Untuk tahapan lebih lanjut yaitu untuk aspek penguatan aplikasi berbasis *web* dapat dilakukan sesuai dengan suatu *attack tree* nya.