BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring berkembangnya teknologi dalam bidang informasi dan komunikasi yang begitu pesat dari zaman ke zaman, semakin tinggi pula permintaan servis internet diberbagai tempat baik itu menggunakan kabel atau nirkabel (*Wireless)* yang meliputi instansi pemerintahan, perusahaan-perusahaan, tempat hiburan dan termasuk juga sekolah serta kampus yang dinilai dapat membantu proses kelangsungan hidup manusia agar lebih efektif dan instan (Widodo, 2015).

Saat ini jaringan komputer sangat dibutuhkan dimana-mana terlihat dari banyak nya penyedia servis internet (*Internet Service Provider*) bermunculan dan saling menawarkan jasa mereka bagi instansi atau individu yang membutuhkan, karena di era globalisasi dan digitalisasi ini sudah menjadi syarat bahwa untuk kelangsungan bisnis, pendidikan, serta pemerintahan harus menerapkan jaringan komputer di kantor atau gedung tempat proses itu berlangsung baik antar wilayah, kota atau negara sekalipun (Lestariningati & Rozak, 2012).

Saat ini Internet menjadi salah satu pondasi untuk mendapatkan informasi, Situs atau *Web* merupakan salah satunya yang kini tengah berkembang sangat pesat dan merambat dari bidang bisnis, pendidikan, hiburan maupun pemerintahan pun memiliki situs pribadi untuk tujuan masing-masing baik untuk meraup keuntungan atau berbagi informasi, oleh karena itu bermunculan pula peretas atau *hacker* untuk meretas keamanan *Web* tersebut dengan motif tertentu apakah itu hobi semata atau mencari keuntungan pribadi atau kelompok yang saat ini populer dengan sebutan *Cyber Crime*.

Web server sendiri merupakan wadah untuk menopang sebuah *website* yang berisikan informasi, konten, maupun akun surel atau *email* pengguna, sekaligus sebagai penghubung antara *server* dan *client* dalam pengiriman dan perolehan informasi dan data serta mempercepat dan mengorganisasikan nya secara terpusat (Aziz & Tampati, 2015).

Web Application Firewall atau WAF adalah sebuah aplikasi yang bertujuan untuk mengamankan dan mencegah sebuah *web* dari upaya penyerangan dari peretas untuk mendapatkan data dan informasi dan eksploitasi dalam jumlah yang besar yang dapat mempengaruhi kestabilan sebuah *web* hingga memnyebabkan *web* tidak dapat diakses atau sering disebut *down* (Syaefuddin, 2018).

Brute Force atau dalam Bahasa Indonesia yaitu Serang Brutal merupakan sebuah serangan terhadap sistem kemaman pada sebuah perangkat komputer, *web server, database* dan lain sebagainya yang memiliki kunci dengan percobaan kumpulan sandi atau *password,* kode, dan kombinasi. Kata sandi yang dibongkar dengan menggunakan program yang dinamakan *password cracker*, adalah sebuah program yang mencoba membobol sebuah kata sandi yang telah terenkripsi dengan algoritma tertentu dari berbagai kemungkinan percobaan, walaupun sangat sederhana dan terbilang memakan waktu yang cukup lama tergantung seberapa rumit kata sandi itu sendiri namun belum ada sistem di masa kini yang aman terhadap serangan sederhana seperti ini (Pramaditya, 2016).

Berlandaskan rangkuman pada latar belakang diatas, dapat diketahui bahwa penting nya solusi serta cara bagaimana mengatasi dan melakukan tindakan pencegahan jika terjadi serangan *Brute Force* terhadap *website* dan *webserver*. Oleh

karena itu, saya sebagai penulis milih topik penelitian tugas akhir ini dengan judul "**Analisa dan Perancangan Keamanan *Web Server* Dengan Metode *Web Application Firewall* Menggunakan *ModEvasive* Terhadap Serangan *Brute Force*".**

1.2 Rumusan Masalah

Berikut merupakan 3 pokok permasalahan yang akan dikupas penulis dalam penilitian yang akan dilaksanakan:

1. Bagaimana tindakan pencegahan yang harus dilakukan sebelum *web server* terserang *Brute Force* menggunakan *Modevasive*?
2. Bagaimana cara dan tindakan yang harus dilakukan jika *web server* terkena serangan *Brute Force*?
3. Bagaimana peran *Web Application Firewall* dalam mengamankan *web server* terhadap serangan eksternal?

1.3 Batasan Masalah

Agar topik pembahasan penelitian ini dapat dipahami dengan mudah oleh penulis maka batasan masalah akan berfokus pada hal-hal berikut:

1. Penelitian akan dilakukan seputar dengan masalah kemanan *web server*
2. *Web Application Firewall* yang digunakan adalah *ModEvasive*
3. Metode serangan yang akan digunakan dalam pengujian penelitian ini adalah serangan *Brute Force*

1.4 Tujuan Proyek

Tujuan tugas akhir berupa penelitian dengan topik "Analisa dan Perancangan Keamanan *Web Server* Dengan Metode *Web Application Firewall* Menggunakan *ModEvasive* Terhadap Serangan *Brute Force*" tersebut memilki tujuan yaitu:

1. Memberikan proteksi kemananan terhadap *web server* menggunakan WAF sebagai tindakan pencegahan dan pendeteksi agar terhindar dari serangan dan dapat bertahan dari serangan *Brute Force*.
2. Sebagai sarana ilmu pengatahuan terhadap kemanan jaringan terkhusus *web server* dan bagaimana peran WAF dalam mengamankannya.
3. Sebagai syarat kelulusan bagi penulis untuk menuju Strata 1 (S-1) di Universitas Internasional Batam.
4. Betujuan agar dapat menambah pengalaman dan wawasan penulis maupun pembaca seputar masalah keamanan *web server* serta *Web Application Firewall* yang diyakini merupakan topik yang cukup penting terkait pertumbuhan teknlogi *website* di masa yang akan datang.

1.5 Manfaat Proyek

Adapun fungsi dan manfaat dari tugas akhir Analisa dan Perancangan Keamanan *Web Server* Dengan Metode *Web Application Firewall* menggunakan *ModEvasive* terhadap serangan *Brute Force* bagi pengguna, Peneliti dan Akademisi yaitu:

1. Bagi Pengguna
    a. Memberikan edukasi dan informasi terkait permasalahan kemanan *web server* serta bahaya dari salah satu jenis serangan yang umum yakni *Brute Force.*
    b. Memberikan opsi refrensi WAF untuk perlindungan terhadap *web server* yaitu *ModEvasive* kepada pengguna baik itu instansi pendidikan, pemerintah, pelaku usaha maupun *website* pribadi.
2. Bagi Peneliti
    a. Menambah pengalaman dan pengetahuan penulis terhadap keamanan *web server* dari bahaya serangan *Brute Force*.
    b. Menambah wawasan dan keterampilan penulis dalam menaggulangi permasalah terhadap *web server* dengan menggunakan metode WAF.
3. Bagi Akademisi
    a. Memberikan contoh dan gambaran bagaimana menerapkan WAF terhadap *web server* untuk mencegah *website* terkena serangan *Brute Force*.

1.6 Sistematika Pembahasan

Berikut merupakan sistematika pembahasan dalam penelitian yang dibuat secara singkat:

BAB I PENDAHULUAN

Pada bab ini terkandung uraian dari awal permulaan penilitian seperti latar belakang, rumusan, dan batasan masalah serta tujuan, dan manfaat

proyek lalu diakhiri dengan sistematika pembahasan yang memaparkan kesuluruhan isi bab secara jelas, singkat dan padat.

BAB II TINJAUAN PUSTAKA

Bab ini memuat beberapa hal seperti teori yang berperan sebagai pondasi untuk memperkuat penelitian yang berlandaskan dari penelitian sebelumnya yang berkaitan pada penelitian yang akan penulis laksanakan.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisi metode dan desain perancangan yang diikuti oleh analisis dari berbagai pemasalahan dan teknik dalam mengumpulkan data serta alur penelitian dari berbagai tahapan selama penelitian berlangsung.

BAB IV IMPLEMENTASI

Bab ini merupakan bab dimana penulis akan memaparkan tahap-tahapan dalam mengimplementasikan *Web Application Firewall* pada *web server* serta definisi-definisi tentang cara kerja terhadap serangan *Brute Force*.

BAB V PENUTUP

Pada bab ini dapat diketahui bahwa penulis telah berada di penghujung penelitian, maka bab ini akan mengulas kesimpulan-kesimpulan yang diperoleh selama penelitian berlangsung dan diakhiri dengan saran yang berlandaskan pengalaman penulis selama melakukan penelitian yang ditujukan kepada generasi selanjutnya yang mungkin akan mengembangkan topik serupa di masa yang akan dating.