BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Serangan *Traffic Flooding* khususnya *Distributed Denial-of-service (DDoS)* menurut *F5 Labs Application Threat Intelligence* dalam situs resminya menyebutkan bahwa antara bulan Januari 2020 hingga bulan maret 2021 meningkat sebesar 55% dan menjadi lebih kompleks dengan 54% insiden diantaranya menggunakan berbagai macam teknik serangan, beberapa industri yang paling banyak mendapat serangan diantaranya adalah website industri teknologi, telekomunikasi, *finance*, *education*, *ISP/hosting*, *gaming*, *consultant*, *retail* dan lain sebagainya. *F5 Labs* menyebutkan juga dalam situsnya bahwa semakin banyaknya perangkat lunak penetration testing yang dapat diakses secara gratis dan dapat didownload langsung dari beberapa situs penyedia aplikasi penetration testing, sehingga saat ini tidak ada website industri yang sepenuhnya aman dari serangan *traffic flooding* khususnya *Distributed Denial-of-service (DDoS)*.

Ada berbagai macam cara untuk mencegah *serangan traffic flooding denial of service* diantara cara yang umum seperti menggunakan *firewall*, menggunakan *CDN* dan menggunakan layanan anti *Distributed Denial-of-service (DDoS)* dari pihak ketiga. Pada penelitian ini penulis memilih menggunakan *firewall* untuk mencegah dan mengatasi serangan *Distributed Denial-of-service (DDoS)*.

Penulis akan meneliti *Virtual Private Server* dimana nantinya akan dilakukan serangan *Traffic Flooding : Distributed Denial-of-service (DDoS)*, serangan akan dilakukan pada protokol *HTTP port* 80 menggunakan aplikasi *free license Low Orbit Ion Cannon* kemudian penulis akan membandingkan performa dan traffic *Virtual Private Server* dengan kondisi antara sebelum dan sesudah menggunakan *firewall*.

Dari latar belakang masalah tersebut maka peneliti mengajukan judul *Analisis Sistem Keamanan Jaringan Host Dan Server Menggunakan Metode Traffic Flooding*, dimana peneliti akan melakukan analisis perbandingan serangan *Traffic Flooding : Distributed Denial-of-service (DDoS)* pada server tanpa *firewall* dan server yang menggunakan *firewall*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka terdapat rumusan masalah :

1. Bagaimana pengaruh *Traffic Flooding* terhadap performa server sebelum dan sesudah menggunakan *firewall* ?
2. Apakah *Firewall* berpengaruh signifikan dalam menanggulangi serangan *Traffic Flooding* pada *server* ?

1.3 Batasan Masalah

Dalam perancangan dan pembuatan aplikasi ini memiliki cakupan yang cukup luas, untuk itu peneliti membuat beberapan batasan masalah, diantaranya sebagai berikut :

1. Penelitian ini menggunakan *Virtual Private Server* dengan sistem operasi ubuntu server 18.04.

2. Teknik serangan jaringan *Traffic Flooding* yang digunakan adalah *Distributed Denial-of-service (DDoS)*.
3. Penelitian ini membandingkan performa server sebelum dan sesudah menggunakan firewall dengan kondisi dilakukan serangan *Traffic Flooding : Distributed Denial-of-service (DDoS)*
4. Serangan ini menggunakan skenario yaitu serangan melalui protokol HTTP.
5. Perlakuan terhadap server berupa tanpa firewall dan menggunakan firewall.
6. Tahapan Pengembangan Penelitian menggunakan metode *SPDLC*, langkah dari tahapan *SPDLC* adalah, analisis, desain, implementasi, audit, dan evaluasi, pada penelitian ini hanya pada sampai pada tahap audit.
7. Penelitian ini berupa eksperimental dan tidak menggunakan objek penelitian berupa organisasi maupun instansi.

1.4 Maksud dan Tujuan

Maksud dari penelitian ini adalah menangkap, mencatat, dan menganalisis aktifitas jaringan dengan metode *traffic flooding*. Tujuan dari penelitian ini adalah untuk mengetahui apakah pengaruh *traffic flooding* terhadap *traffic* dan performa jaringan pada *server*.

1.5 Manfaat Penelitian

1.5.1 Bagi Penulis

1. Menambah pengetahuan tentang jenis serangan terhadap sebuah *server*.

2. Mengetahui pengaruh serangan jaringan terhadap sebuah *server*.
3. Sebagai syarat kelulusan dan mendapat gelar sarjana

1.5.2 Bagi Administrator Jaringan

1. Dapat menjadi bahan pertimbangan tindakan terhadap serangan *denial of service* pada *server*.

1.5.3 Bagi Pembaca

1. Media pengetahuan tentang sebuah serangan jaringan yakni metode *traffic flooding*.

1.6 Metode Penelitian

Metode pengumpulan data yang digunakan peneliti untuk melakukan analisis data dan menjadikannya informasi yang akan digunakan untuk mengetahui permasalahan yang dihadapi.

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan peneliti untuk melakukan analisis data dan menjadikannya informasi yang akan digunakan untuk mengetahui permasalahan yang dihadapi.

1. Studi Pustaka

Metode yang digunakan untuk pengumpulan data yang diperoleh dari buku-buku, literatur, laporan dan berbagai karya ilmiah lainnya yang dijadikan sebagai acuan serta penunjang konsep teori yang berkaitan dengan topik skripsi dalam penelitian ini.

2. Metode Eksperimen

Peneliti melakukan beberapa eksperimen untuk menguji *server* dengan menyerang server menggunakan teknik *Distributed Denial-of-service (DDoS)* kemudian mencatat dan membandingkan hasilnya.

1.6.2 Metode Pengembangan

Metodologi Pengembangan yang digunakan adalah metode *SPDLC* "*Security Policy Development Life Cycle*", yaitu sebuah metode yang bergantung pada proses pembangunan sebelumnya. Tahapan yang terdapat dalam *SPDLC* adalah Identifikasi, Analisis, Desain, Implementasi, Audit, dan Evaluasi. Penjelasan masing-masing tahapan sebagai berikut :

a. Analisis

Pada Tahap awal ini dilakukan untuk menemukan berbagai macam masalah keamanan yang dihadapi oleh jaringan pada saat ini dan bagaimana sistem yang sedang berjalan. Dari data yang didapatkan pada tahap identifikasi, dilakukan proses analisis kebutuhan *user*.

b. Desain

Tahap desain ini akan membuat suatu gambar rancangan topologi sistem keamanan yang akan dibangun, alur sistem autentikasi serta menjelaskan kebutuhan sistem baik *software* maupun *hardware*.

c. Implementasi

Pada fase implementasi yaitu mengimplementasikan semua yang telah dirancang sesuai analisis dan desain yang dilakukan pada fase sebelumnya.

d. Enforcement (Audit)

Pada tahap ini sistem yang disimulasikan akan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sudah sesuai dengan tujuan awal. Tahap ini dilakukan dengan 4 macam skenario testing.

e. Enhancement (Evaluasi)

Pada tahap ini dilakukan evaluasi hasil dari testing yang telah dilakukan, sejauh mana tingkat efektivitas dari teknologi keamanan yang dibangun, dan membandingkan dengan tujuan awal serta kondisi ideal yang diharapkan. Hasil dari analisa akan dijadikan sebagai masukan untuk perbaikan sistem juga sebagai saran untuk usaha perbaikan di masa yang akan datang.

1.7 Sistematika Penulisan

Secara umum sistematika penulisan yang digunakan dalam skripsi ini memuat uraian-uraian dalam setiap bab, yaitu :

BAB I : Pendahuluan

Bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II : Landasan Teori

Bab ini berisi tentang tinjauan pustaka yang memaparkan ringkasan referensi yang berupa karya ilmiah. Kemudian dasar teori yang berisi penjelasan mengenai dasar-dasar teori sebagai penunjang dalam penelitian ini.

BAB III : Metode Penelitian

Bab ini membahas langkah – langkah yang dilaksanakan dalam proses penelitian, yaitu proses identifikasi dan pengumpulan data, analisis kebutuhan *software* dan *hardware*, desain, implementasi, Audit, Evaluasi serta pengujian pada *QoS*.

BAB IV : Implementasi dan Pembahasan

Bab ini berisikan implementasi jaringan, pengujian jaringan, serta pembahasan dari hasil penelitian.

BAB V: Penutup

Bab ini berisikan kesimpulan yang merupakan pendapat terakhir berdasarkan uraian-uraian pada bab selanjutnya, serta saran yang berguna untuk melakukan pengembangan lebih lanjut pada sistem ini.