BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia teknologi dan informasi keamanan menjadi faktor penting yang berperan dalam menarik konsumen. Di era teknologi informasi seperti sekarang, menjaga kenyamanan dan keamanan informasi konsumen menjadi hal yang sangat penting agar dapat bersaing. Banyak ancaman yang dapat digunakan untuk mengganggu keamanan konsumen. Hal ini dapat saja terjadi bila pelayanan yang diberikan melalui internet sehingga dapat dikatakan kurang aman karena koneksi melewati jaringan. Beberapa ancaman yang mungkin diterima sebagai penyedia layanan salah satunya adalah serangan terhadap server.

Server administrator atau yang sering disingkat admin server merupakan orang yang bertanggung jawab atas server pada sebuah perusahaan. Selama ini seorang admin server selalu berada di dalam ruangan server untuk mengawasi server dari serangan. Sistem jaringan komputer yang beresiko tentu akan sangat berpengaruh dalam menjaga minat konsumen dalam menggunakan layanan server. Oleh karena itu, diperlukan *monitoring* untuk mengamankan jaringan agar dapat mengurangi dampak yang terjadi jika terjadi percobaan intrusi. Pentingnya penanganan yang cepat cepat terhadap server yang bermasalah menjadikan salah satu munculnya berbagai macam aplikasi *monitoring.*

Sistem *monitoring* adalah sistem yang dirancang agar dapat memberikan respon saat menjalankan program. Respon yang ditujukan agar dapat memberikan informasi keadaan sistem. Sistem *monitoring* terdiri dari mekanisme serta program dengan menjalankan sistem informasi pada komputer yang dirancang untuk mendata serta mampu untuk mengirimkan data sesuai dengan data yang diperoleh (Siswanto, A., & Faldana, 2014). Pada saat ini serangan luar yang diluncurkan oleh penyerang semakin banyak dan variatif. Contohnya adalah serangan *DDOS* (*Distributed Denial of Service*) ada beberapa jenis serangan *Distributed Denial of Service* yang sering terjadi seperti *UDP Flooding* dan *SYN Flooding*. Serangan *DDOS* mengakibatkan sistem yang diserang mengalami gangguan berupa *error*

request, *halt*, kegagalan sistem dan sebagainya.

Kasus-kasus yang terjadi belakangan ini menimpa salah satu perusahaan *IT* (*Information Technology*) terbesar yaitu Sony Playstation, yang menyebabkan pengguna tidak dapat mengakses karena terjadi kegagalan layanan (Wang, 2017), insiden juga terjadi saat pertengahan 2009 ketika domain.co.id mengalami *drop* selama 4 hari (Yuli, 2009). Dikarenakan server tempat menerima dan melayani permintaan dari pengguna dari *Web Browser* diserang dengan teknik penyerangan *Denial of Service* (*DOS*) yaitu penyerangan dengan satu penyerang dan *Distributed Denial of Service* (*DDOS*) yaitu penyerangan dengan lebih dari satu penyerang membanjiri dengan paket-paket kepada server. Sehingga server sibuk melayani permintaan paket yang sangat banyak dan membuat kinerja server menurun. Dan apabila permintaan paket yang lebih banyak lagi akan menyebabkan kerusakan pada perangkat keras atau server (S.S.Kolahi, 2015).

Cepatnya perkembangan teknologi informasi berbasis komputer dapat dikatakan telah memberikan perubahan yang signifikan dalam kegiatan manusia. Contoh mengenai perkembangan teknologi yaitu kecerdasan buatan (*artificial intelligence*). Dengan memanfaatkan kecerdasan buatan, komputer mampu untuk melakukan tugas seperti manusia sehingga sering disebut dengan *bot*. *JSON Web Token* (*JWT*) merupakan token berupa *string* yang *random* berguna dalam mengoperasikan sistem autentikasi serta untuk mengamankan dalam bertukar informasi (Salma, 2017). *JSON Web Token* menjaga keamanan data dengan cara melakukan *encode* pada klaim untuk diubah ke *JSON* serta mengubah *JSON Web Signature* ke *payload* (Bradley, 2015).

Berdasarkan permasalahan yang dijelaskan, maka diperlukan sebuah *bot* untuk *monitoring* yang akan memudahkan seorang admin server dalam mengawasi keaktifan jaringan dan keamanan pada server. Sehingga dengan adanya *bot* maka seorang admin server akan selalu mendapatkan notifikasi pada suatu aktifitas, apabila *server* terjadi mendapatkan gangguan maupun lancar. serta membantu seorang admin server untuk melakukan *monitoring* terhadap server dan melihat keamanan pada server yang diserang. Dalam perancangan *bot* untuk *monitoring* pada server menggunakan metode *JSON Web Token.* Adapun judul yang diusulkan

untuk skripsi ini adalah "**Perancangan *Bot* Untuk *Monitoring Server* Dari Serangan *Distributed Denial Of Service* Menggunakan *JSON Web Token***".

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang di atas, dapat disimpulkan bahwa terdapat rumusan masalah :

1. Bagaimana cara *bot* mendeteksi serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding* dalam *monitoring* server?
2. Bagaimana penerapan metode *JSON Web Token* agar bisa dioperasikan oleh *bot* admin server?

1.3 Tujuan Penelitian

Tujuan penelitian berdasarkan pemaparan latar belakang serta rumusan masalah adalah sebagai berikut, yaitu :

1. Bagaimana cara memonitoring server agar dapat mendeteksi serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding*?
2. Mempermudah pekerjaan admin server dalam mengatasi serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding*.

1.4 Manfaat Penelitian

Berdasarkan pemaparan latar belakang, rumusan masalah dan tujuan penelitian, dapat disimpulkan bahwa penelitian ini memiliki manfaat, yaitu:

1. Memahami konsep *monitoring* pada server.
2. Mampu menerapkan *bot* untuk *monitoring* server dari serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding*.

1.5 Ruang Lingkup

Mengingat luasnya pembahasan masalah pada penelitian, maka penelitian ini akan dibatasi ruang lingkupnya sehingga pembahasan dapat lebih terfokus. Pembatasan ruang lingkup permasalahan dalam penelitian ini meliputi:

1. *Bot* merupakan program yang berjalan di sisi server untuk melindungi server dari serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding*.
2. *Bot* juga berfungsi sebagai pemberi informasi kepada admin server apabila terjadi serangan *UDP Flooding* dan *SYN Flooding* terhadap server.

3. *Monitoring* pada server.
4. *Bot* hanya bisa mendeteksi jenis serangan *UDP Flooding* dan *SYN Flooding*.
5. Informasi yang diberikan kepada *admin* dari *bot* hanya *port ICMP*, *SSH*, *HTTP*, *HTTPS*, dan *FTP*.
6. Memberitahukan *IP* yang telah melakukan penyerangan terhadap server melalui *bot.*
7. Sistem Operasi yang digunakan oleh server berbasis Linux (UBUNTU).

1.6 Luaran Yang Diharapkan

Luaran yang diharapkan pada penelitian ini adalah untuk meningkatkan keamanan server dengan merancang *Bot* yang mampu untuk melakukan *monitoring* server dari serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding*.

1.7 Sistematika Penelitian

Penulis akan menampilkan gambaran sistematika penulisan laporan pada penelitian ini yang menjadi beberapa bagian, yaitu :

BAB 1 PENDAHULUAN

Bab yang membahas mengenai latar belakang, rumusan masalah, tujuan manfaat, ruang lingkup dan luaran yang diharapkan dari penelitian.

BAB 2 LANDASAN TEORI

Bab yang membahas berbagai teori yang berhubungan dengan Perancangan *Bot* Untuk *Monitoring Server* Dari Serangan *DDOS* Dengan Menggunakan *JSON WEB TOKEN*.

BAB 3 METODOLOGI PENELITIAN

Bab yang membahas metode dan kerangka berfikir yang dilakukan dalam penelitian.

BAB 4 HASIL PEMBAHASAN

Bab yang membahas uraian tentang hasil tes Perancangan *Bot* Untuk *Monitoring Server* Dari Serangan *Distributed Denial Of Service* Dengan Menggunakan *JSON WEB TOKEN*.

BAB 5 PENUTUP

Bab yang membahas mengenai kesimpulan atas hasil yang diperoleh serta saran terhadap kekurangan dari penelitian.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN