BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi internet berjalan bersamaan dengan ancaman dan serangan-serangan terhadap layanan-layanan internet. Salah satu ancaman utama tersebut adalah *Denial of Service* (DoS). *Denial of Service* (DoS) merupakan program serangan untuk mencegah pengguna yang "sah" mengakses layanan dari sebuah *server*. Jenis serangan ini membuat sumber daya sistem menjadi saturasi sehingga terjadilah *crashing* (Papadie, 2017). Apabila sebuah serangan DoS diimplementasikan dengan cara terdistribusi dan dilakukan oleh lebih dari satu, maka serangan tersebut disebut dengan *Distributed Denial of Service* (DDoS). Serangan DDoS menggunakan komputer *"zombie"* sebagai *botnet* untuk membanjiri sebuah *server* dengan pesan-pesan sehingga terjadi *crash*. *Botnet* tersebut dikendalikan oleh server *Command and Control* (C&C) sebagai server pusat *botnet*. *Attacker* dapat mengirimkan perintah pada server *Command and Control* (C&C) kemudian perintah tersebut diteruskan pada mesin-mesin atau komputer yang sudah terinfeksi dengan *malware* untuk melakukan serangan *Distributed Denial of Service* terhadap *server* untuk waktu yang tak dapat ditentukan (Radware, 2013). Akibatnya pengguna tidak dapat mengakses layanan dari *server*. Metode serangan DDoS yang paling populer saat ini adalah dengan melibatkan *application level flooding*, terutama pada *web server*. Metode-metode tersebut diantaranya dapat berupa HTTP GET *Flood*, HTTP Post *Flood*, *Slowloris*, DNS, dll. (Bhosale, Nenova, & Iliev, 2017).

Slowloris merupakan salah satu serangan DDoS namun dapat berfungsi sebagai DDoS karena hanya dengan satu kali eksekusi oleh satu mesin dapat "membanjiri" *web server* dengan HTTP *Flooding*. *Slowloris* tidak dapat terdeteksi oleh *Intrusion Detection System* (IDS) dan *Intrusion Pervention System* (IPS) karena *Slowloris* tidak mengirimkan paket HTTP *request* yang rusak, sehingga terdeteksi oleh IDS atau IPS seperti pengguna "sebenarnya" (Choi & Guilley, 2004). *Slowloris*

mengirimkan paket-paket koneksi HTTP parsial agar koneksi tetap terbuka untuk waktu tertentu, sehingga paket-paket tersebut dapat melewati IPS (Shorey, Subbaiah, Goyal, & Sakxena, 2018). *Web server* berbasis *Apache* rentan terhadap serangan *Slowloris*, karena dalam proses penanganan *request* dengan sistem antrean (*queueing system*) dengan M/M/N sehingga probabilitas transisi ke kondisi "berlebih" atau saturasi lebih besar (Duravkin, Loktionova, & Carlsson, 2014). *Apache* merupakan salah satu *webserver* yang masih menjadi paling populer yang dipakai di dunia (Ling, 2015). Apabila *Slowloris* menyerang *web server*, pengguna tidak dapat mengakses layanan HTTP atau halaman *web* seakan-akan pengguna tidak memiliki jaringan internet untuk mengakses halaman *web* tersebut. Saat ini ada beberapa cara yang digunakan untuk menangkal serangan *Slowloris*, yaitu membatasi jumlah koneksi dari *host* tertentu, menambah jumlah *web server*, menentukan *timeout* yang berbeda-beda pada setiap koneksi sebagai fungsi jumlah koneksi dan *delayed binding* yang dilakukan oleh *load balancer* (Stallings, 2005). Selain itu, dapat menggunakan *Firewall* dan *operating system* mekanisme keamanan seperti *Dynamic* IP *Restriction*, *mod_evasive*, *mod_qos*, IPTables, dan Fail2Ban (Papadie, 2017).

Pada penelitian ini, mekanisme pertahanan *web server* terdiri dari *firewall* pada *router* MikroTik RouterBoard 951 2n dan *Low Interaction Honeypot*. *Low Interaction Honeypot* merupakan salah satu jenis *Honeypot* dimana bertindak seperti *server* asli dan mensimulasikan layanan-layanan tertentu tetapi tidak dapat diambil alih oleh *attacker* (Rahmatullah, Nasution, Azmi, & Server, 2016). Sebagian besar serangan *Slowloris* diarahkan menuju *honeypot*, sehingga serangan terminimalisir dan tidak perlu menambah jumlah *server*. *Web Server* diimplementasikan pada Raspberry Pi 2, *Low Interaction Honeypot* diimplementasikan pada Raspberry Pi 3 Model B+ dan *Slowloris* diimplementasikan pada komputer berbasis Ubuntu.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang penelitian yang telah dikemukakan di atas, maka didapat rumusan masalah sebagai berikut:

1. Bagaimana rancangan mekanisme pertahanan yang dapat meminimalisir serangan *Slowloris*?

2. Apakah dengan menambahkan *Low Interaction Honeypot* sebagai mekanisme pertahanan dapat membantu meminimalisir serangan *Slowloris* dan dampak yang ditimbulkan?

1.3 Batasan Masalah

Batasan masalah dalam perancangan dan simulasi mekanisme pertahanan yang terdiri dari *firewall* (*stateless firewall*) dan *low interaction honeypot* pada tugas akhir ini adalah:

1. Implementasi *stateless firewall* pada Mikrotik tipe RB 951 2n.
2. Implementasi *Low Interaction Honeypot* pada *Raspberry Pi* 3 *Model* B+.
3. Implementasi *web server* pada *Raspberry Pi* 2 dikarenakan PC yang akan digunakan sebelumnya terdapat kendala dalam *Netplan*-nya.
4. Implementasi serangan *Slowloris tool* pada PC berbasis Ubuntu 18.04.
5. Parameter yang diperhatikan adalah jumlah paket *client error,* jumlah dan besar trafik yang masuk ke *web server,* jumlah dan besar trafik yang masuk ke *honeypot*, jumlah dan besar trafik yang dibuang, TCP *connection rate*, HTTP *connection rate* serta TCP *errors rate*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah penelitian yang telah dikemukakan di atas, maka didapat tujuan penelitian sebagai berikut:

1. Merancang mekanisme pertahanan yang terdiri dari *firewall* dan *Low Interaction Honeypot*.
2. Meminimalisir serangan *Slowloris* terhadap *web server* dengan *Low Interaction Honeypot*.

1.5 Manfaat Penelitian

Manfaat penelitian ini diharapkan dengan menggunakan *Low Interaction Honeypot* akan meminimalisir serangan *Distributed Denial of Service* (DDoS): *Slowloris*. Sehingga, tidak perlu memperbanyak jumlah *web server* untuk mengatasi keterbatasan sumber daya. Sebagian besar serangan *Slowloris* akan di blokir oleh *firewall* dan langsung diarahkan menuju *honeypot*.

1.6 Sistematika Penulisan

Sitematika penulisan pada laporan tugas akhir ini dengan memberikan gambaran kandungan setiap bab secara rinci, urutan penulisannya, serta keterkaitan dengan bab sebelumnya dan bab selanjutnya. Sistematika penulisan laporan tugas akhir ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini menjelaskan latar belakang penelitian mengenai serangan *Distributed Denial of Service* (DDoS) dan *Slowloris* terhadap *web server*, rumusan masalah penelitian dalam bagaimana rancangan mekanisme pertahanan yang dapat menangkal serangan *Slowloris*, tujuan penelitian, manfaat penelitian, serta sistematika penulisan dalam melakukan penelitian tugas akhir.

BAB 2 KAJIAN PUSTAKA

Pada bab ini menjelaskan mengenai landasan teori mengenai *Distributed Denial of Service* (DDoS), *Slowloris*, penelitian terkait, komponen-komponen dalam mekanisme pertahanan, serta konsep mekanisme pertahanan untuk meminimalisir serangan *Distributed Denial of Service* (DDoS) hasil penelitian, baik dari buku maupun dari jurnal ilmiah yang terkait dengan penelitian tugas akhir ini.

BAB 3 METODE PENELITIAN

Pada bab ini menjelaskan metode penelitian kuantitatif berupa eksperimen, desain penelitian yang meliputi rancangan mekanisme pertahanan, instrumen penelitian, prosedur penelitian, serta analisis hasil akhir implementasi mekanisme pertahanan.

BAB 4 TEMUAN DAN PEMBAHASAN

Pada bab ini menjelaskan temuan penelitian berdasarkan hasil akhir penelitian dan menjawab pertanyaan penelitian yang telah dirumuskan sebelumnya.

BAB 5 SIMPULAN, IMPLIKASI DAN REKOMENDASI

Pada bab ini menjelaskan kesimpulan yang merupakan tafsiran terhadap hasil analisis temuan penelitian, serta rekomendasi untuk pengembangan selanjutnya

DAFTAR PUSTAKA

Bagian ini berisikan sumber referensi yang dijadikan sebagai acuan dalam penulisan tugas akhir.