BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Perkembangan jumlah pengguna akses *Internet* di era digital sangat pesat, tercatat di tahun 2017 ada 3,65 miliar pengguna *Internet* di dunia. Sementara untuk di tahun 2018 tercatat sudah ada pengguna *Internet* sebanyak 3,896 miliar pengguna *online* [1]. Indonesia tercatat memiliki sebanyak 143,26 juta pengguna *Internet* dari jumlah penduduk sebanyak 262 juta orang di tahun 2017. Jumlah ini mengalami kenaikan dari tahun 2016 yang memiliki 132,7 juta pengguna *Internet* [2]. Peningkatan jumlah pengguna tersebut membuat penggunaan *bandwidth* akan semakin meningkat. Penggunaan *bandwidth* yang lebar akan membuat akses informasi semakin cepat dan akurat bahkan hingga ke lembaga-lembaga penting.

Informasi yang sangat penting mengandung banyak hal yang mengharuskan akses yang dilakukan hanya diperbolehkan dari beberapa pihak saja. Semakin bebas akses layanan yang didapatkan maka tingkat kelemahan suatu jaringan juga akan memiliki banyak celah salah satunya percobaan serangan yang bisa dilakukan oleh *attacker*. Penyerang (*attacker*) dalam melakukan seranganya dapat berakibat terhadap beberapa hal yang merugikan suatu individu maupun kelompok. Pada skala dunia sendiri sampai tahun 2017 tercatat ada 4 jenis kerusakan yang dihasilkan dari beberapa aksi *cyber attack* seperti kehilangan informasi dengan 43%, gangguan bisnis sebesar 33%, hilangnya pendapatan sebesar 21%, dan kerusakan alat sebesar 3% [3]. Sementara di Indonesia sendiri pada survei di tahun 2017 sebanyak 83,98% pengguna *Internet* sadar akan maraknya penipuan di *Internet* dibanding dengan kesadaran 65,98% terhadap kasus pengambilan data di *Internet* [2]. Banyaknya kerugian yang didapat dan kurangnya kesadaran masyarakat akan keamanan tersebut, penyerang akan terus melakukan serangan yang beragam dan berkembang dalam setiap seranganya.

APJII mencatat sampai Agustus 2017 terdapat 8 jenis serangan populer yang pernah dialami pengguna diantaranya *Malware* dengan 98%, *Phising and Social Engineering* dengan 69%, *Web-Based Attack* dengan 67%, *Botnet* dengan 63%, *Malicious Code* dengan 58%, *Malicious Insider* dengan 53%, *Denial of Service*

43%, dan *Ransomware* dengan 27% [4]. Dari data jenis serangan tersebut, jenis serangan *Denial of Service* (DOS) merupakan serangan yang sudah sangat lama digunakan dalam dunia *cyber crime* dengan jumlah responden yang pernah mengalami sebanyak 43%. Serangan DDOS ini merupakan salah satu jenis serangan yang cara kerjanya serupa seperti serangan DOS biasa. Namun yang membedakan pada DDOS penyerang menggunakan serangan *zombie* yang akan menyerang secara bersama-sama dalam jumlah banyak pada satu waktu yang sama dengan cara mengalirkan data yang sangat besar untuk menurunkan kualitas jaringan atau bahkan melumpuhkannya [5]. Tentu serangan ini sangat berbahaya jika sampai terjadi pada suatu jaringan yang pastinya pengguna akan ikut merasakan dampaknya. Oleh karena itu dibutuhkan suatu sistem pengatur lalu lintas di suatu jaringan yang dapat memilah semua paket data, identitas, dan akses jalur yang digunakan untuk melakukan proses pengiriman paket data.

Squid Proxy Server memiliki banyak jenis penggunaan mulai dari mempercepat akses alamat *web* dengan melakukan *caching* dari *request* yang dilakukan berulang-ulang seperti *caching* DNS, *caching* pencarian di komputer, *caching* situs *web* untuk pengguna yang berada dalam satu jaringan yang sama, melakukan pemilahan data lalu lintas untuk meningkatkan keamanan, serta melakukan proses autentikasi pengguna dalam akses layanan [6]. Oleh karena itu, keberadaan *Squid* diharapkan dapat mengatasi serangan DDOS yang dilakukan penyerang demi mengamankan data yang diakses oleh pengguna.

Berdasarkan latar belakang ini, serangan DDOS yang diluncurkan menuju ke suatu perangkat berdasarkan akses lalu lintas jaringan diharapakan dapat diatasi dengan sistem *proxy server* menggunakan *Squid* pada sistem operasi *Linux Debian*.

1.2 RUMUSAN MASALAH

Rumusan masalah pada penelitian ini yaitu:

a. Seberapa besar akibat yang ditimbulkan oleh serangan DDOS terhadap jaringan dan pengguna?
b. Bagaimana sistem keamanan *proxy server* dan *firewall* dapat mengatasi serangan DDOS dari penyerang yang terjadi tanpa menghambat akses pengguna pada suatu jaringan?

1.3 TUJUAN

Tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut:

1. Mengetahui konsep dan bentuk serangan DDOS yang dilakukan attacker dari aplikasi LOIC.
2. Mengenali konsep pengamanan jaringan berdasarkan aturan yang dibuat dengan proxy dan firewall untuk memblokir serangan DDOS yang berlangsung.

1.4 BATASAN MASALAH

Batasan masalah pada penelitian ini yaitu:

a. Jaringan dijalankan secara *virtual* menggunakan aplikasi *Oracle VM VirtualBox 6.0*.
b. Simulasi Jaringan yang dilakukan menggunakan sistem operasi *Linux Debian Stretch 8.11.0*.
c. Paket aplikasi *proxy server* yang digunakan *Squid* dengan versi 3.2 dan *iptables* dengan versi 1.4.21 sebagai paket aplikasi *firewall*.
d. Konfigurasi protokol *routing* pada *Debian Server* dilakukan menggunakan *Quagga 1.2.4* dengan protokol OSPF.
e. Jenis serangan yang dilakukan *attacker* adalah *Distributed Denial of Service* (DDOS) menggunakan aplikasi *LOIC* dengan versi 1.0.4.0.
f. Pengalamatan IP menggunakan *IPversion4* yang dihubungkan wired secara *virtual*.
g. Pengujian terhadap parameter *delay*, *packet loss* dan *throughput* dilakukan untuk menguji perbandingan dampak serangan DDOS terhadap akses pengguna saat sebelum dan sesudah sistem keamanan diterapkan.
h. Pengujian keamanan jaringan dilakukan terhadap segi *availability* sistem keamanan dalam mengatasi serangan DDOS.

1.5 MANFAAT

Penelitian ini diharapkan dapat memberikan manfaat kepada beberapa objek pengguna jaringan dalam memanfaatkan sistem keamanan jaringan berbasis *proxy server* dalam mengatasi serangan DDOS, seperti pengembangan sistem keamanan jaringan, peningkatan keamanan lalu lintas data pada link yang di akses *client*,

penghematan penggunaan sumber daya pada perangkat *server*, penentuan dalam pembuatan kebijakan pada peningkatan sistem keamanan jaringan, dan sebagai bahan pengembangan pada pengkajian materi sistem keamanan jaringan pada komunitas terkait.

1.6 SISTEMATIKA PENULISAN

Penulisan penelitian dengan judul ini memiliki beberapa topik pembahasan yang sistematis terdiri dari 5 bab. Bab I berisi latar belakang, perumusan masalah, batasan masalah, tujuan pembahasan serta metode penelitian yang menjelaskan ide dari pengkajian permasalahan yang muncul maupun perkembangan dari penelitian sebelumnya. Lalu pada bab II berisi mengenai pondasi dasar pembangunan teori yang dibutuhkan guna mendukung implementasi sistem dari sistem *proxy server* pada suatu lalu lintas jaringan. Pada bab III menjelaskan mengenai alur penelitian serta konfigurasi mengenai metode yang digunakan saat melakukan percobaan skenario penelitian. Pada bab IV berisi pembahasan mengenai hasil data yang diperoleh beserta bagaiman konsep akses dan pemblokiran yang dilakukan oleh sistem keamanan *proxy server* dan *firewall* yang diterapkan berdasarkan hasil percobaan skenario sebelum dan setelah diterapkan sistem keamanan tersebut. Dan pada bab V berisi kesimpulan dari hasil implementasi dan saran yang diberikan penulis untuk pengembangan pada penelitian serupa selanjutnya.