BAB I

PENDAHULUAN

1.1 Latar Belakang

Jaringan komputer terus mengalami kemajuan dan perkembangan yang pesat. Salah satu teknologi jaringan komputer yang berkembang cukup pesat adalah *internet*. Perkembangan ini pun memicu berbagai pihak untuk terhubung dengan internet. Bahkan sekarang ini hampir semua orang di dunia terhubung dengan internet. Menurut data dari internet World Stats pertumbuhan internet dari tahun 2000 ke 2014 pertumbuhannya mencapai 741% di seluruh dunia [1]. Di Indonesia sendiri, selama tahun 2014 menunjukkan pengguna internet naik menjadi 88,1 juta pengguna atau dengan kata lain penetrasi sebesar 34,9% [2]. Hal ini memerlukan pengelolaan jaringan yang baik agar dapat menjamin ketersediaan jaringan yang selalu tinggi.

Perkembangan internet juga memicu juga memicu perkembangan bidang keamanan jaringan. Dalam laporan keamanan Akamai Technologies pada kuartal pertama 2013 hingga akhir kuartal kedua 2013, tercatat jumlah serangan *cyber* terbesar berasal dari Indonesia, meningkat hingga dua kali lipat dari periode sebelumnya. Berdasarkan laporan keamanan tersebut, Indonesia menempati posisi teratas dengan prosentase 38%, naik 17% dari priode sebelumnya, disusul China dengan prosentase 33%. [3]

Salah satu metode serangan yang cukup dikenal adalah *ICMP flood Attack*. Menurut Bogdanoski, dkk.,(2011), ICMP (*Internet Control Message Protocol*)

adalah bagian dari rangkaian TCP / IP yang dirancang untuk menangani kesalahan dan kontrol pesan. Salah satu contoh yang paling dikenal dalam praktek adalah utilitas *ping*. ICMP digunakan untuk memeriksa *remote host* untuk tanggap, menampilkan waktu pulang-pergi, atau mendeteksi kegagalan komunikasi antara *host*. Dalam hal serangan *ICMP flood*, serangan itu menguasai komputer target dengan mengirimkan sejumlah besar "*ICMP Echo Requests*" ke komputer target. Korban menerima paket ini akan menjawab "*ICMP Echo Reply*" kembali ke alamat sumber. Akibatnya, akan mengkonsumsi bandwidth yang baik masuk dan keluar, dan dalam kasus yang ekstrim dapat menonaktifkan konektivitas jaringan. [4]. Dengan serangan *ICMP flood* ini membuat suatu jaringan mengalami tidak adanya *availability* atau ketersediaan, yang merupakan salah satu aspek dari keamanan jaringan.

Biswas, Anupama (2008), melakukan pengujian mengenai penggunaan *resource* dari *host* target selama proses serangan *ICMP flood*. Dari hasil pengujian tersebut dapat dilihat terjadinya peningkatan penggunaan *CPU (Central Processing Unit)* sebesar 2.19 % dan penggunaan memori sebesar 4.22 % dalam waktu 150 detik. [5]

STMIK Amikom Yogyakarta merupakan perguruan tinggi swasta yang berada di kabupaten Sleman, Daerah Istimewa Yogyakarta telah menerapkan infrastruktur jaringan yang cukup besar. Sebagai institusi perguruan tinggi dibidang teknologi informasi terdapat beberapa *server* yang digunakan untuk melayani berbagai aktivitas akademik. Tidak adanya pembatasan dan terbukanya protokol ICMP tentunya dapat dimanfaatkan untuk melakukan serangan ke *server*.

Mengingat ICMP merupakan salah satu dari tiga aplikasi yang memiliki trafik terbesar pada interval bulan desember 2015 sampai bulan juli 2016 di STMIK Amikom Yogyakarta dengan total trafik mencapai 2,84 *Gigabyte*.

Berdasarkan permasalah diatas dibutuhkan sebuah infrastruktur yang mampu menangani pengiriman paket data yang berlebih seperti *ICMP flood* sehingga menghidari terjadinya tabrakan data ataupun penurunan performa jaringan. Maka dari itu akan dilakukan penelitian yang berjudul "Perancangan Sistem Deteksi dan Mitigasi *ICMP Flood* Berbasis *Software Defined Network* dan *sFlow-RT* di STMIK Amikom Yogyakarta".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana merancang sistem deteksi dan mitigasi *ICMP Flood* berbasis *Software Defined Network* dan *sFlow-RT* di STMIK Amikom Yogyakarta

1.3 Batasan Masalah

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

Beberapa batasan masalah yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Arsitektur jaringan yang digunakan adalah *Software Defined Network* dengan protokol *OpenFlow*.
2. Kolektor *sFlow* yang digunakan adalah *sFlow-RT*.
3. Jenis perangkat yang digunakan adalah prototipe yang telah diuji

performanya.

4. Perangkat *software-base switch OpenFlow* yang digunakan adalah TP-LINK TL-1043WND Ver. 1.11 dengan jumlah 1 buah.
5. Pengujian sistem meliputi pengujian *latency* dan jumlah paket ICMP.
6. *Software* kontroler yang digunakan adalah *opendaylight* dengan seri *hydrogen* versi 4.0.
7. Menggunakan aplikasi siege untuk mengirimkan paket melalui beberapa *host*.
8. Menggunakan *host* sebagai *fake router* untuk membagi dua jaringan pada jaringan *openflow*.
9. Menggunakan sistem operasi *linux Ubuntu desktop* 14.01 LTS pada *host*.
10. Penelitian ini hanya membahas masalah *ICMP flood* atau *ping flood*, selebihnya tidak dibahas.
11. Penelitian dilakukan di STMIK Amikom Yogyakarta.
12. Metode pengembangan sistem menggunakan metode PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*). Penelitian ini hanya sampai membahas pada tahap *Operate*, tahap *Optimize* tidak dibahas.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Adapun maksud dari penelitian ini antara lain :

1. Sebagai prasyarat untuk kelulusan program studi Strata 1 Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Amikom Yogyakarta.

1.4.2 Tujuan

Adapun tujuan dari penelitian ini antara lain :

1. Untuk merancang infrastruktur yang mampu mendeteksi serangan *ICMP flood* berbasis *software defined network* dan *sFlow-RT.*
2. Untuk merancang infrastruktur yang mampu mengontrol atau mengurangi *ICMP flood attack* berbasis *software defined network* dan *sFlow-RT.*

1.5 Metode Penelitian

Langkah-langkah dalam melakukan penelitian yang berjudul "Penanganan *ICMP Flood Attack* Berbasis *Software Defined Network* dan *sFlow-RT* di STMIK Amikom Yogyakarta" ini sebagai berikut antara lain :

1.5.1 Metode Pengumpulan Data

1.5.1.1 Metode Observasi

Metode yang digunakan untuk melakukan pengamatan secara langsung terhadap objek penelitian, menggali dan merumuskan masalah yang ada. Metode ini dilakukan untuk mengumpulkan dokumen yang merupakan sumber informasi yang sangat penting yang dapat membantu dalam analisa dan untuk langkah selanjutnya dalam melakukan penelitian.

1.5.1.2 Metode Wawancara

Pengumpulan data dan informasi dengan cara melakukan wawancara secara langsung dengan penanggung jawab jaringan STMIK Amikom Yogyakarta untuk mendapatkan informasi mengenai infrastruktur yang sedang berjalan.

1.5.1.3 Metode Kepustakaan

Studi pustaka dilakukan untuk mempelajari dan mendapatkan pengetahuan dari buku, jurnal, internet atau literatur yang diperlukan sebagai dasar teori dalam perancangan sistem.

1.5.1.4 Metode Studi Sejenis

Metode pengumpulan data dengan mempelajari penelitian-penelitian sebelumnya yang memiliki karakteristik sama, baik dari segi teknologi maupun objek penelitian.

1.5.2 Metode Pengembangan Sistem

Metode pengembangan sistem menggunakan metode *PPDIOO life cycle* yang terdiri dari *Prepare, Plan, Design, Implement, Operate, Optimize*. Adapun rincian dari masing-masing proses tersebut antara lain :

1. *Prepare*

   Tahap yang pertama adalah *prepare* atau persiapan. Dimulai dari persiapan mengenai gambaran sistem yang ada,trafik data, penangan paket data, serta identifikasi masalah dan solusi yang ditawarkan.

2. *Plan*

   Pada tahap ini mengidentifikasi kebutuhan dari sistem yang akan dibangun seperti kebutuhan perangkat keras dan kebutuhan perangkat lunak.

3. *Design*

   Dalam tahapan membahas tentang detil logis perancangan arsitektur topologi yang sesuai dengan mekanisme sistem. Pada tahap ini akan

dibuat perancangan menggunakan *flowchart* untuk menggambarkan mekanisme kerja serta topologi jaringan sistem deteksi dan mitigasi berbasis *software defined network* dan *sFlow-RT*.

4. *Implementation*

   Tahap selanjutnya adalah tahap implementasi, pada tahap ini menerapkan semua yang telah direncanakan. Dalam tahap ini mencakup instalasi serta konfigurasi terhadap rancangan topologi, dan konfigurasi yang dilakukan pada masing-masing perangkat.

5. *Operate*

   Pada tahap ini dilakukan pengecekan atau pengopersian tiap-tiap fungsi yang sudah dibuat. Pengoperasian dilakukan dengan memonitoring tiap fungsi yang dibuat. Mulai dari kontroler, *swirch OpenFlow* dan *sFlow-RT* sampai pengujian penanganan paket *ICMP*.

1.6 Sistematika Penulisan

Dalam penyusunan laporan penelitian ini akan disajikan dalam bentuk bab, antara lain sebagai berikut :

BAB I. PENDAHULUAN

Bab ini akan membahas latar belakang, perumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode peneltian dan sistematika penulisan.

BAB II. LANDASAN TEORI

Pada bab ini akan membahas dan menjelaskan mengenai dasar teoritis yang menjadi landasan dan mendukung pelaksanaan penulisan laporan penelitian.

BAB III. ANALISIS DAN PERANCANGAN

Dalam bab ini akan membahas mengenai dasar metode yang digunakan dalam melakukan penelitian ini.

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas inplementasi dan pengujian dari perancangan sistem deteksi dan mitigasi *temp flood* berbasis *software defined network* dan *sFlow-RT*.

BAB V. PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilaksanakan dan saran-saran dari masalah yang terkait untuk mengembangkan sistem yang lebih baik lagi.