BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang telah terbuka bebas, menjadikan *hacker* telah berevolusi dengan mampu menguasai teknik menurunkan kinerja perangkat jaringan dengan membanjiri lalu lintas jaringan [1]. Saat ini begitu banyak cara untuk melakukan serangan terhadap sistem jaringan. Cara-cara ini terus berkembang dari zaman dahulu sampai sekarang. Dahulu untuk melakukan serangan membutuhkan pengetahuan dan pemahaman teknis IT yang tinggi, akan tetapi saat ini sangat mudah untuk melakukan serangan bukan hanya orang yang mempunyai *skill* yang tinggi. Metode dan alat-alat yang digunakan semakin banyak dan mudah digunakan, bahkan untuk orang awam, maka dari itu semakin tinggi pula tingkat serangan yang terjadi terhadap sistem keamanan jaringan [2]. Salah satu jenis serangan yang paling sering dilakukan yaitu serangan *Distributed Denial Of Service (DDoS).*

Serangan *Denial Of Service (DoS)* dan *Distributed Denial Of Service (DDoS)* adalah serangan yang mungkin bisa sering kita jumpai diantara serangan serangan lainnya. *Denial Of Service (DoS)* dan *Distributed Denial Of Service (DDoS)* sendiri pada dasarnya adalah sama, namun *Distributed Denial Of Service (DDoS)* adalah serangan yang dapat dikatakan terstrukur. Dengan mekanisme yang pada dasarnya sama dengan *Denial Of Service (DoS)* namun memiliki dampak yang umumnya jauh lebih besar dibandingkan dengan *Denial Of Service (DoS)* [2].

Serangan *Distributed Denial Of Service (DDoS)* biasanya melibatkan penyerang mengirimkan pesan untuk mengekploitasi kerentanan tertentu yang mengarah kepada ketidakstabilan atau kelumpuhan sistem. Penyerang juga dapat melakukan serangan dengan mengirimkan sejumlah besar pesan normal dengan cepat ke *node* tunggal, tujuannya adalah untuk menghabiskan sumber daya sistem sehingga menyebabkan kegagalan sistem. Serangan *Distributed Denial Of Service (DDoS)* adalah serangan *Denial Of Service (DoS)* yang memanfaatkan beberapa sumber daya serangan yang terdistribusi. Biasanya, para *attacker* menggunakan sejumlah besar *bots* yang dikendalikan (komputer inang/*daemon*, juga disebut sebagai *zombie*) dan terdistribusi di beberapa lokasi untuk melancarkan sejumlah besar serangan *Distributed Denial Of Service (DDoS)* terhadap target tunggal atau beberapa target. Seiring dengan perkembangan pesat dari *botnet* (jaringan *bot*) dalam beberapa tahun terakhir, skala lalu lintas serangan yang disebabkan oleh serangan *Distributed Denial Of Service (DDoS)* telah meningkat, dengan targetnya tidak hanya *server* untuk keperluan bisnis, tetapi juga infrastruktur internet seperti *firewall, router* dan sistem DNS serta *bandwidth* jaringan [14].

Secara umum, paket data yang beredar di jaringan menggunakan protokol TCP/IP untuk transmisinya. Paket ini sendiri tidak berbahaya, tetapi jika ada terlalu bayak paket yang abnormal, maka perangkat jaringan atau *server* akan mengalami kelebihan beban/*overload*. Pada kondisi ini tentunya dapat dengan cepat menghabiskan sumber daya sistem. Kasus lain adalah jika paket serangan memanfaatkan celah keamanan pada protokol tertentu (misalnya *request* layanan

yang tidak lengkap atau penyalahgunaan formasi protokol). Tindakan ini juga dapat menyebabkan kegagalan perangkat jaringan atau *server*.

Ketika serangan *Distributed Denial Of Service (DDoS)* dilancarkan ke suatu *server*, maka akan terlihat perilaku *bot* yang secara signifikan mempengaruhi jaringan dan terjadi pada waktu yang hampir bersamaan [15]. Perilaku ini disebut dengan *network behavior*. Contoh yang sangat jelas dari *network behavior* ini adalah meningkatnya paket *service request* yang ditujukan pada sebuah layanan jaringan/*server* tertentu. Di bawah komandi penyerang, *bot* serentak melakukan *service requested* ke sebuah *server* dengan tujuan untuk merebut semua sumber daya *server* sehingga *server* tidak dapat melayani *service request* yang sah.

Sebuah serangan *Distributed Denial Of Service (DDoS)* adalah upaya jahat untuk membuat *server* atau sumber daya jaringan tidak tersedia bagi pengguna, biasanya dengan sementara mengganggu atau menangguhkan layanan dari sebuah host terhubung ke Internet [3].

Berdasarkan latar belakang yang telah di uraikan di atas, maka peneliti mencoba untuk melalukan penelitian dengan judul "**Analisis Pengaruh Variasi Serangan Distributed Denial of Service (DDoS) Pada Performa Router** ".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, peneliti dapat merumuskan permasalahan sebagai berikut :

1. Bagaimana melakukan variasi serangan *Distributed Denial of Service* dengan menggunakan metode TCP dan UDP ?

2. Bagaimana implementasi serangan *Distributed Denial of Service* yang dilakukan terhadap jaringan *client-server* ?
3. Bagaimana kinerja sumber daya *CPU Load* dan *traffic bandwidth* pada *router* ketika serangan *Distributed Denial of Service* terjadi ?

1.3 Batasan Masalah

Beberapa batasan masalah yang di gunakan dalam penelitian ini adalah sebagai berikut :

1. Peneliti melakukan variasi serangan dengan mengubah jumlah serangan dari masing-masing level penyerangan.
2. Pengukuran di lakukan berdasarkan parameter yang telah di tentukan yaitu penggunaan sumber daya *CPU* pada *router* mikrotik.
3. *Software* yang digunakan dalam melakukan serangan *Distributed Denial of Service* adalah *Low Orbit Ion Canon (LOIC).*
4. Pengujian dilakukan pada sistem operasi *windows 7* dan *web server* yang digunakan adalah *Apache2.*
5. Pengujian dilakukan dengan menggunakan jaringan *client-server.*

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud

Maksud penelitian dengan judul "Analisis Pengaruh Variasi Serangan *Distributed Denial of Service (DDoS)* Pada Performa *Router*" adalah untuk memenuhi persyaratan dalam mencapai gelar sarjana pada program studi S1 Informatika di Universitas Amikom Yogyakarta.

1.4.2 Tujuan

Tujuan dari penelitian ini adalah :

1. Merancang *Distributed Denial of Service* untuk melakukan serangan terhadap *router*.
2. Mengetahui kinerja *router* pada saat serangan sedang berlangsung.

1.5 Manfaat Penelitian

1. Bagi Peneliti

   Manfaat dari penelitian ini ialah pembelajaran bagi peneliti untuk menganalisa serangan *Distributed Denial of Service* sehingga peneliti dapat melakukan pencegahan sebelum terjadinya serangan *Distributed Denial of Service*.

2. Bagi Universitas Amikom Yogyakarta

   Menambah referensi ilmiah dalam bentuk skripsi bagi mahasiswa yang sedang dan akan menyusun skripsi di Perpustakaan Amikom Yogyakarta

3. Bagi Peneliti Selanjutnya

   Penelitian ini diharapkan dapat digunakan sebagai bahan bagi penelitian selanjutnya yang berkaitan dengan *Distributed Denial of Service* dan juga dapat di harapkan bisa membuat program yang dapat mendeteksi ketika terjadi serangan *Distributed Denial of Service*.

1.6 Metode Penelitian

Pada pembuatan skripsi ini, peneliti menggunakan beberapa metode penelitian. Adapun metode-metode penelitian yang digunakan adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

1. Studi Literatur

   Mengumpulkan bahan atau materi dari journal atau buku yang relevan yang di jadikan referensi dan melakukan studi konfigurasi terhadap topologi jaringan, snort dan semua *software* yang dibutuhkan dalam melakukan penelitian serta melakukan studi konsep serangan *Distributed Denial of Service*.

1.6.2 Tahapan Pengembangan Jaringan

Penelitian ini menggunakan metodologi NDLC *(Network Development Life Cycle)*. Berikut adalah penjelasan dari masing-masing tahapan metodologi NDLC :

1. *Analysis*

   Pada tahap ini peneliti melakukan analisa kebutuhan, analisa permasalahan yang muncul dan analisa topologi jaringan yang sudah ada saat ini.

2. *Design*

   Dari data-data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun.

Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

3. *Simulation Prototype*

Pada tahap ini peneliti melakukan bentuk simulasi dengan bantuan *tools* khusus dibidang *network*. Hal ini dimaksudkan untuk melihat kinerja awal dari jaringan yang akan dibangun.

4. *Implementation*

Pada tahap ini peneliti akan menerapkan semua yang telah dirancang dan didesain sebelumnya. Yaitu dengan melakukan serangan *Distributed Denial of Services* terhadap jaringan yang telah dibangun.

5. *Monitoring*

Pada tahap ini peneliti melakukan *monitoring* terhadap *router* untuk mengetahui penggunaan sumber daya *CPU* pada saat terjadinya serangan *Distributed Denial of Services*.

6. *Management*

Pada tahap ini peneliti melakukan manajemen atau pengaturan. salah satu yang menjadi perhatian khusus adalah masalah kebijakan *(policy)*. Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini peneliti menerangkan tentang latar belakang penelitian, perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang dasar-dasar teori yang di gunakan dalam penyusunan skripsi ini dan pendukung pelaksanaan penelitian.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi analisis sistem yang akan dibangun, topologi jaringan dan konfigurasi *software LOIC*.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi pembahasan tentang implementasi dari analisis dan perancangan yang di susun pada Bab 3 dan pengujian apakah hasil yang di dapatkan sesuai dengan yang diharapkan.

BAB V PENUTUP

Bab ini berisi kesimpulan dari keseluruhan uraian bab-bab sebelumnya dan saransaran yang diajukan untuk pengembangan penelitian selanjutnya.

DAFTAR PUSTAKA

Berisi sumber bacaaan yang digunakan peneliti sebagai bahan penelitan.