BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan, walaupun terkadang ada beberapa instansi yang menempatkan masalah keamanan ini pada urutan yang ke terakhir setelah *quality of service* (QoS) dan lain sebagainya. Akan tetapi ketika jaringan mendapat serangan dan terjadi kerusakan atau menggangu kinerja sistem, Investasi yang dikeluarkan cukup besar untuk melakukan perbaikan sistem. Untuk itu sudah selayaknya investasi dibidang keamanan jaringan lebih diperhatikan, untuk mencegah kerusakan dari ancaman serangan yang saat ini semakin beragam serta semakin canggih. Terlebih lagi ketika jaringan lokal sudah terhubung ke internet maka ancaman serangan terhadap keamanan jaringan akan semakin meningkat, berbagai macam teknik serangan terus dikembangkan. *Distribute Denial Of Service* tidak menutup kemungkinan juga serangan hacker yang digunakan untuk melumpuhkan suatu layanan atau jaringan yang berada di lokal maupun di internet, dengan alasan untuk merusak, persaingan yang tidak sehat, politik, atau hanya sekedar keisengan para hacker. semuanya merupakan ancaman serangan yang tidak bisa diabaikan. Untuk itu perlu disiapkan teknik yang dapat setidaknya meminimalisir ancaman serangan *Denial of Service* (DoS) yang dapat memasuki sistem jaringan, Sehingga kerusakan dan gangguan dapat diperkecil.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah seperti yang diuraikan di atas, dapat dikemukakan beberapa rumusan masalah sebagai berikut.

1. Bagaimana analisis dan dampak serangan *Denial of Service* (DoS) terhadap perangkat jaringan dan pelanggan internet Media ICT ?
2. Bagaimana membangun sistem keamanan jaringan agar terhindar dari serangan *Denial of Service* (DoS) yang berdampak pada perangkat jaringan dan pelanggan Media ICT ?

1.3 Batasan Masalah

Untuk mendapatkan hasil penelitian seperti yang diharapkan dan penelitian dapat terarahkan, maka permasalahan dalam penelitian ini akan dibatasi sebagai berikut:

1. Membangun sistem keamanan jaringan dilakukan menggunakan perangkat CISCO *Adaptive Security Appliance* (ASA) 5505.
2. Aplikasi yang digunakan hanya menggunakan *Cisco Adaptive security Manager* (ASDM) untuk :
   a. Memantau *traffic* .
   b. Memantau Serangan DoS *attack alert*.
   c. Memantau grafik *connection*.
   d. Memantau *usage* CPU pada Cisco ASA 5505.
3. Serangan DoS Menggunakan *software Low Orbit Ion Cannon v.2.0.0.4*.

4. Menggunakan *Denial of Service attack* jenis TCP *Flood* dan SYN *Attack*.
5. Hanya melakukan konfigurasi TCP *intercept* pada Cisco ASA 5505 dengan menggunakan putty.
6. Melakukan tahap uji coba sebanyak 4 kali.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Berdasarkan uraian latar belakang masalah dan rumusan masalah diatas, maka maksud dari penelitian ini ialah untuk mengidentifikasi masalah dan meminimalisir serangan *Denial of Service* (DoS) pada Media ICT *internet service provider*.

1.4.2 Tujuan Penelitian

Adapun tujuan penelitian ini sebagai berikut:

1. Menganalisis dan mencegah terjadinya serangan *Denial of Service* (DoS) pada jaringan Media ICT.
2. Melakukan identifikasi karakteristik paket yang mengandung serangan *Denial of Service* (DoS).

1.5 Metode Penelitian

Metode Penelitian dalam pembuatan tugas akhir ini sebagai berikut.

1.5.1 Metode Pengumpulan Data

Pengumpulan data dilakukan dengan 2 cara yaitu:

a. Wawancara

Pada tahap ini dilakukan pengumpulan data yang mendukung dengan mengadakan percakapan langsung dengan *Administrator* Jaringan di Media ICT.

b. Observasi

Metode ini digunakan untuk mengamati secara langsung bagaimana alur topologi dan *traffic* jaringan pada Media ICT agar data-data lebih akurat.

1.5.2 Metode Analisis

Pada tahap ini dilakukan analisis sebagai berikut.

1. Metode analisis PIECES (*Performance, Information, Economy, Control, Eficiency and Service*) untuk memperoleh pokok-pokok permasalahan yang lebih spesifik.
2. Analisis Kebutuhan Sistem
   a. Analisis Kebutuhan Fungsional
   b. Analisis Kebutuhan Non Fungsional

1.5.3 Metode Perancangan

Setelah menganalisis dari data-data yang sudah diperoleh dan mengetahui kelemahan lalu perancangan system yang baru sudah dibuat. Maka selanjutnya dengan metode perancangan untuk di terapkan. Metode perancangan yang digunakan adalah metode dari Cisco yaitu "*The* PPDIOO *Network Lifecycle*"

(Teare, 2008). Dan berikut ini adalah singkatan dari PPDIOO (*Prepare, Plan, Design, Implement, Operate* dan *Optimize*) dan berikut penjelasannya :

1. ***Prepare*** **(Persiapan)**

   Dalam tahap awal penulis mengumpulkan data, mengidentifikasi permasalahan, menganalisis sistem lama agar mengetahui kelemahannya dan mempersiapkan sistem baru yang sesuai dengan kebutuhan.

2. ***Plan*** **(Perencanaan)**

   Pada tahap ini dibuat perecanaan jaringan berdasar tujuan dan sistem baru yang akan dibuat. Perencanaan ini harus sesuai dan sejalan dengan batasan masalah yang ada, agar perencanaan yang dibuat sesuai.

3. ***Design*** **(Perancangan)**

   Tahap perancangan yang dimaksud adalah infrastruktur jaringan yang akan dibuat dan jaringan yang akan dibuat bisa berjalan dengan baik sesuai kebutuhan.

4. ***Implement*** **(Implementasi)**

   Pada fase ini dilakukan konfigurasi sesuai dari analisis dan design yang sudah dibuat. Memperbaiki sistem lama dengan yang baru yaitu dengan menambahkan *CISCO Adaptive Security Appliance* (ASA) 5505 dan menerapkan metode *TCP intercept* dan *TCP Packet Handling*.

5. ***Operate*** **(Pengoperasian)**

   Fase operasional adalah dimana kita menguji coba sistem baru yang sudah dibuat.

6. ***Optimize*** **(Optimalisasi)**

   pada fase terakhir ini identifikasi dan persiapan menyelesaikan masalah baru yang akan muncul jika terjadi kesalahan dari sistem yang baru.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I : PENDAHULUAN

Bab ini membahas mengenai latar belakang masalah yang diteliti, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Bab ini membahas mengenai tinjauan pustaka, dasar-dasar teori yang berhubungan dengan penelitian dan perancangan sistem yang dibuat oleh penulis.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini membahas mengenai tata cara metode analisa dan perancangan sistem yang digunakan untuk mengolah sumber data yang dibutuhkan sistem, antara lain: Topologi jaringan, Perangkat jaringan yang digunakan, identifikasi paket SYN DoS, konfigurasi dan analisis kinerja jaringan yang dilakukan dalam penelitian.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Bab ini memuat mengenai tahapan perancangan sistem keamanan jaringan dengan Cisco ASA.

BAB V : PENUTUP

Bab ini berisikan kesimpulan dari semua hasil tahapan yang telah dilalui selama penelitian serta saran-saran untuk penelitian selanjutnya.