**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

1. **IDENTITAS PENGUSUL**

**NAMA : I Gusti Ngurah Agung Bayu Ditaprawira**

**NRP : 5109 100 068**

**DOSEN WALI : Ary Mazharuddin Shiddiqi, S.Kom, M.Comp.Sc**

1. **JUDUL TUGAS AKHIR**

Penerapan *Congestion Participation Rate* (CPR) untuk pendeteksian serangan *low - rate* DDoS

1. **LATAR BELAKANG**

Pada saat ini teknologi informasi sedang mengalami perkembangan yang sangat pesat. Kebutuhan akan penggunaan teknologi informasi semakin hari semakin besar. Salah satu bagian dari teknologi informasi yang saat ini kebutuhan dan penggunaannya semakin meluas adalah jaringan komputer. Saat ini semakin banyak layanan dan teknologi yang memanfaatkan jaringan komputer sebagai sarana untuk komunikasi, pertukaran data, dan juga layanan konten.

Dengan posisi yang begitu kritikal pada berbagai aspek kehidupan membuat jaringan komputer beserta perangkatnya menjadi sasaran tindak kejahatan. Salah satu tindak kejahatan tersebut adalah serangan *Distributed Denial of Service* (DDoS). DDoS merupakan salah satu jenis serangan ke komputer dari jaringan. Serangan DDoS menggunakan sejumlah *host* untuk membanjiri komputer korban dengan *request* informasi sehingga sistem dapat saja menjadi *crash* dan tidak dapat melayani sebagaimana mestinya [5].

Seiring berjalannya waktu, muncul variasi baru dari serangan DDoS yang diberi sebutan *low-rate* DDoS (LDDoS). Berbeda dengan DDoS pada umumnya, *low-rate* DDoS mengirimkan paket yang jumlahnya lebih sedikit[1]. Pengiriman paket yang tidak sporadis membuat sering kali serangan LDDoS tidak dengan mudah terdeteksi. Hal ini membuat kualitas dari layanan aplikasi yang berbasis TCP menjadi menurun namun tidak diketahui oleh pemilik dari komputer tempat layanan tersebut dijalankan.[2]

Karena sifat serangannya yang tidak sporadis dan terkadang memiliki interval waktu cukup lama dibandingkan DDoS biasa membuat munculnya kesulitan dalam melakukan pendeteksian terhadap serangan dari LDDoS. Untuk melakukan pendeteksian aliran serangan dari LDDoS ini diperlukan pendekatan khusus agar dapat membedakannya dari paket TCP biasa. *Congestion Participation Rate* (CPR) merupakan suatu pendekatan yang dapat dicoba digunakan untuk melakukan indetifikasi terhadap aliran serangan dari LDDoS[3].

1. **TUJUAN**

Tujuan pembuatan tugas akhir ini adalah membuat suatu sistem pendeteksian LDDoS dengan berdsarkan pada pendekatan CPR.

1. **HARAPAN**

Harapan pembuatan tugas akhir ini adalah aplikasi dapat membantu masyarakat dalam melakukan pendetksian LDDoS pada komputer.

1. **PERMASALAHAN**

Adapun yang menjadi permasalahan utama dalam tugas akhir ini.

1. Bagaimana cara melakukan pengecekan terhadap paket data yang masuk ke komputer korban ?
2. Bagaimana cara membedakan antara paket serangan LDDoS dengan paket TCP biasa ?
3. Bagaimana performa dari *Congestion Participation Rate* (CPR) dalam mendeteksi serangan LDDoS ?
4. **BATASAN MASALAH**

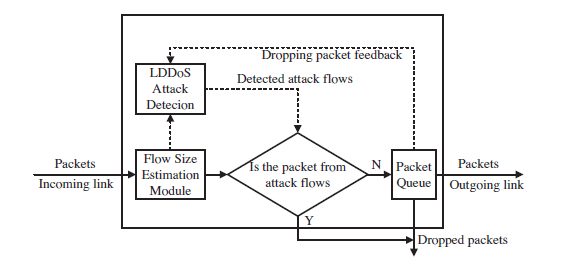
Dari permasalahan yang telah diuraikan di atas, terdapat beberapa batasan masalah terhadap tugas akhir ini, yaitu.

1. Pengecekan aliran data pada korban terbatas pada protokol TCP
2. Metode yang digunakan untuk melakukan pengecekan terhadap aliran serangan LDDoS adalah pendekatan *Congestion Participation Rate* (CPR)
3. Percobaan dilakukan dengan menggunaan dataset dan pembuatan topologi jaringan.
4. Fokus dari tugas akhir ini adalah untuk melakukan percobaan untuk mengetahui keberhasilan CPR dalam mendeteksi aliran LDDoS, sehingga tidak dilakukan percobaan dengan metode lain sebagai pembanding.
5. Pendeteksian yang dilakukan berdasarkan dari rekapitulasi aliran data.
6. **RINGKASAN ISI TUGAS AKHIR**

Pada tugas akhir ini akan dibuat sebuah aplikasi pendeteksian serangan LDDoS. Aplikasi ini melakukan pendeteksian berdasarkan pada input rekapitulasi aliran data pada suatu komputer. Paket data yang dianalisis adalah paket data dengan protol TCP. Dengan adanya aplikasi ini seseorang dapat melakukan analisis dan pendeteksian pada aliran data komputernya untuk mengetahui apakah ada serangan LDDoS atau tidak.

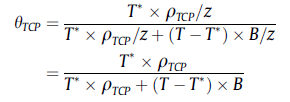
*Congestion Participation Rate* (CPR) merupakan suatu pendekatan dimana didasarkan pada sifat dari protokol TCP yang memiliki fungsi *Congestion Avoidance*. *Congestion Avoidance* merupakan fungsi standar bawaan pada protokol TCP [4]dimana paket data dengan protokol TCP akan melakukan pencegahan dengan perlambatan pengiriman paket data ketika terjadi *congestion* / kemacetan pada suatu jaringan. Berdasarkan hal tersebut, pendekatan *Congestion Participation Rate* (CPR) mengalisis kecendrungan tersebut dan kemudian membedakan paket LDDoS yang akan tetap melakukan pengiriman data walau terjadi kondisi *congestion*. Kondisi ini membuat dapat memperlihatkan bahwa paket LDDoS akan memiliki aliran data yang lebih besar daripada paket TCP biasa. Untuk mengetahui perbedaan CPR antara paket TCP biasa dan paket LDDoS dapat dilakukan dengan operasi pengurangan antara ambang batas atas dari aliran normal paket TCP dengan ambang batas rata - rata CPR dari aliran LDDoS.

Berdasarkan pada paper referensi [PAPER UTAMA], dibuatlah suatu skema alur pendeteksian paket LDDoS :



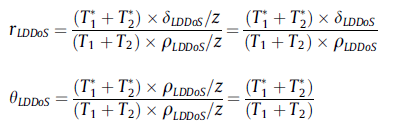
Gambar 1. skema pengecekan

Pada paper referensi, untuk mendapatkan agregat CPR dari aliran data paket TCP digunakan persamaan sebagai berikut :



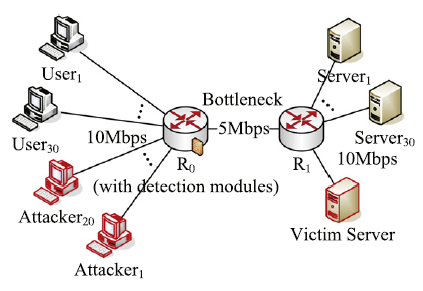
Gambar 2. persamaan agregat CPR paket TCP

Sedangkan untuk mengetahui batas bawah dari CPR dari aliran data LDDoS digunakan persamaan :



Gambar 3. persamaan batas bawah paket LDDoS

Rancangan topologi yang akan digunakan untuk mensimulasikan serangan LDDoS adalah dengan menggunakan skema topologi jaringan Dumbell [**17**]. Dimana pada topologi tersebut terdiri dari 2 router, dengan didalamnya terdapat komputer - komputer yang bertugas sebagai penyerang, komputer biasa, komputer *server*, dan komputer *server* yang akan menjadi target penyerangan. Berikut merupakan gambaran dari topologi yang akan dibangun untuk melakukan simulasi :



Gambar 4. topologi untuk simulasi serangan

1. **METODOLOGI**

Metodologi yang akan dilakukan dalam Tugas Akhir ini memiliki beberapa tahapan, di antaranya sebagai berikut:

1. **Studi Literatur**

Tahap ini merupakan tahap pengumpulan informasi yang diperlukan untuk pengerjaan tugas akhir sekaligus mempelajarinya. Mulai dari pengumpulan literatur, diskusi, serta pemahaman topik tugas akhir di antaranya tentang :

1. Sifat dari serangan LDDoS
2. *congestion participation rate* (CPR)
3. Penggunaan *tools* untuk mensimulasikan serangan DDoS
4. penggunaan *tools* untuk rekapitulasi aliran paket data
5. **Perancangan Sistem**

Pada tahap ini dilakukan analisa awal dan pendefinisian kebutuhan sistem untuk mengetahui masalah yang sedang dihadapi. Dari proses tersebut selanjutnya dirumuskan rancangan sistem yang dapat memberi permecahan masalah tersebut.

1. **Implementasi**

Pada tahap implementasi ini akan dilakukan proses pembuatan aplikasi pendeteksian LDDoS dengan berdasarkan pada pendekatan CPR. Selain itu dilakukan persiapan pembuatan topologi dan konfigurasi *tools - tools* pendukung untuk simulasi

1. **Pengujian dan Evaluasi**

Pengujian aplikasi ini dapat dilakukan antara lain sebagai berikut:

1. aplikasi dapat membaca rekapitulasi aliran data yang didapatkan dari hasil simulasi serangan.
2. aplikasi dapat membedakan antara paket TCP biasanya dan paket serangan LDDoS.
3. aplikasi dapat mendeteksi aliran - aliran paket serangna LDDoS.
4. **Penyusunan Buku Tugas Akhir**

Tahap terakhir merupakan penyusunan laporan yang memuat dokumentasi mengenai pembuatan serta hasil dari ujicoba dari perangkat lunak yang telah dibuat. Secara garis besar, Buku Tugas Akhir yang nantinya akan dibuat terdiri dari beberapa bagian antara lain

1. Pendahuluan
   1. Latar Belakang
   2. Permasalahan
   3. Batasan Tugas Akhir
   4. Tujuan
   5. Metodologi
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Uji Coba dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka
7. **JADWAL KEGIATAN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Kegiatan** | **Bulan** | | | | | | | | | | | | | | | | | |
| **Oktober** | | | | **November** | | | | **Desember** | | | | | **Januari** | | | | |
| 1. | Studi Literatur |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 2. | Perancangan Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 3. | Implementasi & Pembuatan Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 4. | Uji Coba dan Evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 5. | Penyusunan Buku Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |

1. **DAFTAR PUSTAKA**

[1] Y. Xiang, K. Li, W, Zhou Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics. 2011

[2] A. Kuzmanovic, E.W. Knightly, Low-rate TCP-targeted denial of service attacks – (the shrew vs. the mice and elephants), in: ACM SIGCOMM, Karlsruhe, Germany, 2003, pp. 75–86.

[3] C. Zhang, Z. Cai, W. Chen, X. Luo, J. Yin: flow level detection and filtering of low-rate DDoS, 2012

[4] Congestion Avoidance

http://tools.ietf.org/html/rfc5681

[5] DDoS

http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

**LEMBAR PENGESAHAN**

Surabaya, 17 Oktober 2012

Mengetahui/Menyetujui,

**Ary Mazharuddin Shiddiqi, S,Kom, M.Komp.Sc**

NIP. 19810620 200501 1003

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Dosen Pembimbing I | Dosen Pembimbing II | |  |  | |  | **Rully Soelaiman, S.Kom.,M.Kom.**  NIP. 19700213 199402 1001 | | |
|  |