ABSTRAK

Penelitian ini merupakan sebuah analisis dampak dari suatu *flooding attack*. *Flooding* merupakan bentuk serangan dari DoS *attack*. DoS adalah serangan yang sering terjadi dijaringan internet maupun jaringan lokal. Terdapat berbagai dampak negatif yang ditimbulkan oleh DoS *attack*, yaitu menghabiskan *bandwidth*, memutuskan koneksi antar *server*, *client* dari *server* tidak dapat menggunakan *service* yang tersedia dan juga dapat merusak sistem korbannya. Oleh karena itu akan diperlukan sebuah mekanisme pertahanan yang dapat mengurangi dampak serangan ini.

Pada penelitian ini dibuat 2 buah pengujian simulasi dengan beberapa skenario. Pengujian simulasi menggunakan aplikasi Riverbed Modeler Academic Edition dengan lama simulasi 30 menit. Terdapat 3 skenario simulasi, yaitu skenario 1 yaitu Normal *Network*, skenario 2 yaitu *Network with* DoS *Attack* dan skenario 3 yaitu *Defense Against* DoS *Attack*.

Hasil analisa didapatkan dengan membandingkan parameter-parameter yang telah ditentukan. Dari pengujian tersebut menghasilkan TCP *Delay* untuk skenario Normal *Network* adalah 200*sec, Network with DoS Attack* adalah 200-240*sec* dan *Defense Against* DoS *Attack* adalah 250-300*sec*. CPU *Utilization* untuk skenario Normal *Network* adalah 0,5%, *Network with DoS Attack* adalah 2-2,2% dan *Defense Against* DoS *Attack* adalah 2,5-3%. DB *Query Respons Time* untuk skenario Normal *Network* adalah 300*sec, Network with DoS Attack* adalah 800-900*sec* dan *Defense Against* DoS *Attack* adalah 900-1000*sec*. FTP *Download Respons Time* untuk skenario Normal *Network* adalah 500*sec, Network with DoS Attack* adalah 650-700sec dan *Defense Against* DoS *Attack* adalah 300-480*sec*. FTP *Upload Respons Time* untuk skenario Normal *Network* adalah 600-630*sec, Network with DoS Attack* adalah 700-750*sec* dan *Defense Against* DoS *Attack* adalah 180-290*sec*.

Kata Kunci : *DoS Attack, Flooding Data*, Keamanan Jaringan

ABSTRACT

This research is an analysis of the impact of a flooding data. Flooding is a form of DoS attack. DoS is attack that often occurs in the internet network and the local network. There are various bad impact of DoS attack, like draining bandwidth, disconnected the connection between server, client of the server can't use the avaliable services and also break the system. Therefore, it would be need a defense system that can reduce the impact of DoS attack.

In this research have two simulation testing with several scenarios. Simulation testing using Riverbed Modeler Academic Edition application with 30 minutes of simulation time. There is 3 scenario, scenario 1 the Normal Network, scenario 2 the Network with DoS Attack and scenario 3 the Defense Against DoS Attack.

In this research, i will explain the results of a simulation DoS Attack to know the impact of DoS attack. Result of these test are TCP Delay for scenario Normal Network is 200sec, Network with DoS Attack is 200-240sec and Defense Against DoS Attack is 250-300sec. CPU Utilization for scenario Normal Network is 0,5%, Network with DoS Attack is 2-2,2% and Defense Against DoS Attack is 2,5-3%. DB Query Respons Time for scenario Normal Network is 300sec, Network with DoS Attack is 800-900sec and Defense Against DoS Attack is 900-1000sec. FTP Download Respons Time for scenario Normal Network is 500sec, Network with DoS Attack is 650-700sec dan Defense Against DoS Attack is 300-480sec. FTP Upload Respons Time for scenario Normal Network is 600-630sec, Network with DoS Attack is 700-750sec and Defense Against DoS Attack is 180-290sec.

Key Word : DoS Attack, Flooding Data, Network Security