

Abstract

As one of the network threats, Denial of service always spread into one and many variations. The main differentiation between Denial of service and other threats is the vulnerability that Denial of service try to attack is the sistem in which the data are transferred, not the particular data. In this research, Denial of service will be tried to observe by done it on a simple Local Area Network consists of three computers use Windows operating system that supports both IPv4 and IPv6 protocols. IPv4 is the current network addressing model that many systems use nowadays and IPv6 is the other network addressing model that is predicted to replace IPv4 in the near future. Paramaters which are used in this research are relatively make sense for user consist of response time, transfer time, jitter, and throughput. The attack experiment and process of determining parameters above will be separated into both network addressing models, IPv4 and IPv6.

From the experiment, it could be known that the impacts on the services given by Denial of service is certainly negative but they are relatively not too big as the Local Area Network here only consist of a small number of computers. Then from the comparition analysis between these two addressing models, we can gain that IPv6 network is a little bit better for some particular services than IPv4 network, but in the other hand some services do not show any respectable differences for user between these two ones. So the results from this research should not be used particularly for a network development and to decide which addressing model might be used, as there area many aspects should be noticed in this case. But at least this experiment could be used as an useful reference.

Keyword : *Denial of service (DoS), Local Area Network, dual stack, Windows, IPv4, IPv6, response time, transfer time, throughput*