ABSTRACT

Web server is a device that provides services based on packet data to the client via the HyperText Transfer Protocol (HTTP) protocol. This protocol provides information sharing services through the World Wide Web (WWW) where the client will request information from the website and the web server will provide the requested information. Based on measurement data released by McAfee Labs, during 2016 36% of attacks on the network invade Web Server. One of the attacks is a Denial of Service (DOS) and Distributed Denial of Service (DDOS) which aims to make Server remain compromised and can even damage the Hardware from the Web Server. Because of the many ways offered to keep the Server stable, one of them is Host Intrusion Prevention System (HIPS).

This Final Project measures the performance of HIPS by implementing it in a virtual network that also features Snort Defense client on the web server side. The use of Snort is because it is able to detect and drop data packets that are indicated as DOS and DDOS with tool attack TCP SYN Flood. This implementation consists of several components, the Server using the Ubuntu Linux operating system, the attacker uses the Linux operating system Kali and the client accessing information on the web server using the Ubuntu Linux operating system.

From the results of some tests, the average number of attack packets sent to the Server with 4 Attackers for 1 minute reached 2,454,930. Successful attacks and dropped did reach 97.8% or 2,402,626, and about 2.19% or 52.304 packets were missed.

Keyword : Web Server, HIPS, DOS, DDOS, Snort dan TCP SYN Flood