ABSTRACT

Security systems on computer networks at this time there are still many ways to carry out attacks on the intended target such as DoS (Denial of Service) and DDoS (Distribute-Denial of Service) attacks. DoS and DDoS attacks are one of the methods of attack that can result in losses to targets that experience this attack such as damage to some files that are on the computer or laptop, computer or laptop running slowly. So we need to know all types of defense from DoS and DDoS attacks using several methods such as HIPS Snort and firewall which will become the main wall before packets that are considered insecure enter computer networks that we need to secure data or files on the target computer or laptop from the attack will later be analyzed and compared between several defense methods that I will make so as to conclude which method is the most efficient way to carry out defense from DoS and DDoS attacks.

HIPS (Host Intrusion Prevention System) is one of my suggestions to be a defense against DoS and DDoS attacks because this method can detect abnormal activities, IPS (Intrusion Prevention System) will do further prevention with the aim of keeping the network safe and there is no disruption in computer networks. Snort and firewall can also help to detect and prevent various attacks such as DoS and DDoS that enter on a computer network.

With the method used in the form of HIPS Snort and Firewall as a defense from DoS and DDoS attacks. It can be concluded that HIPS Snort is better than Firewall, because HIPS Snort can get packet drops with a proportion that ends in 100%, while on the simple side of a firewall it cannot display the proportion of packet drops.

Keywords: HIPS, snort, DoS, DDoS, attack, defense.