ABSTRACT

IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM (IPS) TO COPE DISTRIBUTED DENIAL OF SERVICES (DDOS) ON THE WEBSITE

The Internet is a primary need for the daily life of both communities and the government use a lot of internet service. According to data from the agency marketing We Are Social and Platform of 274,9 million, as much as the 61.8% use the internet. The Website is a collection of web pages which consists of domain or a subdomain and a variety of other important information available in the website, which is very easy for us in finding important information. However, the ease of access in the search for information, there is the threat of cyber attacks that lurk especially attacks on the website such as Denial Distributed of Services (DDoS). According to data from Kaspersky Lab in the second quarter of 2019 the total number of DDoS attacks increased by 18%, compared with the same period in 2018. Such attacks can be detrimental to a relevant agencies to incur losses of up to $74,00 - $120,000/h. Therefore, we need a system that can ward off cyber attacks including DDoS attacks. This research applies Intrusion Prevention System (IPS), i.e., tools Splunk to cope with DDoS attacks using using tools Slowloris to attack the website. The results of this study indicate when the tools Splunk to detect the presence of an attack Slowloris and packet of slowloris automatically in the block and is categorized as alerts.

Keywoards : DDoS, Slowloris, Splunk.