Abstract

Internet has now become a necessity for most people. It is based on increasing number of information needed. To make it easier for people to get information, web servers built to provide a variety of information needed. Ease of getting Internet access raises the not responsible for the work to disrupt the web server. The easiest way to mess up the work web server is to use a ping flood. Ping flood is one way to perform Distributed Denial of Service (DDoS).

One of the method to detect DDOS attack is using K-means clustering on web server log. K-means clustering will group log traffic datas into two clusters, attack traffic and normal traffic.

To evaluate the accuracy of clustering process, labeling must be done at the initial log traffic to determine the attack and the normal traffic. After labeling, log traffic data is clustered by using K-means clustering. The result of clustering compared to the initial log traffic data. The accuracy is always above 90%.

The weakness of this method, K-means clustering, in this case, just separate into two clusters. So, if the inserted data just contain normal traffic data, then there will be error because the data is forced separate into two clusters, even there is no attack traffic data in the log.

Key words: K-Means Clustering, Distributed Denial of Service, Ping Flood.