ABSTRACT

As the development of computer network technology is rapidly increasing, the more types of attacks has been emerged such as DOS attack, OS fingerprinting, scanning, smurf attack, and the others. Therefore, people needed a system that can detect attacks in real-time response.

Intrusion Detection System (IDS) is an application that monitors computer network from attackers actions that connected in a Local Area Network (LAN). This application is used as the initial stage of protection against the source within a system or network, thus simplifying network management by network administrators and network utilization can be maximized. In this thesis used the product of the Intrusion Detection System (IDS) itself, namely Snort 2.9.0.5 on Linux operating system.

Attack detection based on IDS using k-means clustering algorithm is a system that detects attacks based on the Snort log data by grouping or cluster to the log data into 3 types of attacks. The system uses the k-means clustering algorithm where the number of clusters to be formed initially determined as many as three clusters of malicious attacks, middle, and not dangerous. This system detects the type of attacks using clustering process training data and new data obtained from the snort log data in realtime. K-means method is used because k-means method able to cluster data with large size and fast.

Based on theories and experiments have been conducted with more than 100 training data, the results provide the conclusion that the results of clustering with k-means has produced accuracy values that vary depending on the outcome of random initial cluster centroid. Comparison of experiments has conducted 7:6 to the clusters that have more decision. After cluster the attacks that enter the system into three categories, then the system will take action in the form of banned IP source and also shut the port is attacked.

Keywords: IDS, Snort, cluster, k-means.