Abstract

Increasingly developed technology causes the Software Define Network (SDN) architecture to become increasingly popular. The more it is used, it is necessary to consider security concerns. In the OpenFlow SDN network there are security problems in the form of attacks that are exploited by hackers, one of which is Host Location Hijacking. This attack takes the form of deflecting packets to the attacker, the data from the victim is duplicated so that fake services appear and can cause service interruptions. Given this problem, a network forensic organization is required to perform log analysis to obtain evidence of the attack. However, log analysis is still done manually, so an automatic system analysis is required in order to carry out an investigation. The K-Means clustering method is used to automate log analysis in an attack. The results of this research produce a system that can display Host Location Hijacking attacks based on existing log data on the OpenFlow SDN network. The accuracy results obtained indicate that the cluster value that assesses the value, the higher the cluster value, the lower the value obtained, meaning that the more attacks are grouped, the fewer systems will attack.

Keywords: SDN OpenFlow, Host Site Hijacking, Forensics, K-Means Clustering.