ABSTRACT

In this internet world, cyber attacks are common, one of the most common attacks is brute force attack, while in this final project it is combined with a Software Defined Networking (SDN) network. This final project will implement brute force attack detection on SDN.

To overcome the threat of attack, it is necessary to have a defense system, one of which is Honeypot Cowrie. Cowrie itself is a way to create a fake system that serves to trap attackers. The SDN design uses RYU Controller and connects to the cowrie honeypot, client and attacker via an openflow switch, then the cowrie honeypot will be connected to grafana to display data from brute force attacks carried out by attackers using nmap, hydra and medusa on kali linux. In honeypot cowrie will save an attack data on the ssh port then the data is displayed through the Mysql database and visualized using grafana.

The data obtained are; The number of attacks 4969 times, the number of successful attacks is 48 times, the attack period is last 90 days. Also obtained QoS during an attack in test 10, namely Throughput 100 kb/s decreased by 1 kb/s, Packet Loss 0.83% increased by 0.09%, Delay 32.71 ms increased by 2.91 ms and Jitter 32.71 ms increased by 2.91 ms.

Keywords : *software defined network, honeypot, cowrie, bruteforce*