ABSTRAK

Dalam dunia yang serba internet ini, serangan cyber menjadi hal yang sering ditemui, salah satu serangan yang sering ditemuai adalah *brute force attack*, adapun pada proyek akhir ini dikombinasikan dengan jaringan *Software Defined Networking* (SDN). Proyek akhir ini akan menerapkan deteksi serangan *brute force* pada SDN.

Untuk mengatasi ancaman serangan tersebut diperlukan adanya sistem pertahanan salah satunya *Honeypot Cowrie*. *Cowrie* sendiri merupakan suatu cara membuat sistem palsu yang berfungsi untuk menjebak penyerang. Perancangan SDN menggunakan *RYU Controller* dan terhubung ke *honeypot cowrie, client* dan penyerang melalui *switch openflow*, kemudian *honeypot cowrie* akan dihubungkan dengan *grafana* untuk menampilkan data dari serangan *brute force* yang dilakukan oleh penyerang menggunakan *nmap, hydra* dan *medusa* pada *kali linux*. Pada *honeypot cowrie* akan menyimpan sebuah data serangan terhadap *port ssh* kemudian data tersebut ditampilkan melalui *Mysql database* dan divisualisasikan menggunakan *grafana*.

Adapun data yang diperoleh yaitu; Jumlah penyerangan 4969 kali, jumlah penyerangan sukses sebesar 48 kali, periode penyerangan 90 hari terakhir. Juga diperoleh QoS pada saat terjadi serangan di pengujian 10 yaitu Throughput 100 kb/s turun sebesar 1 kb/s , Packet Loss 0.83 % naik sebesar 0.09 %, Delay 32.71 ms naik sebesar 2.91 ms dan Jitter 32.71 ms naik sebesar 2.91 ms.

Kata kunci: *software defined network, honeypot, cowrie, bruteforce*