ABSTRACT

The emergence of science and technology led to more losses in the field of technology itself. Just like a network, the more complex the network is designed, the more complex the problems that will arise from an irresponsible attack. Attacks that cannot be predicted when they occur, sometimes make the server owner careless about attacks that occur when the network is not monitored for a long time.

Based on the problems, the author makes a monitoring system for attack activities carried out by irresponsible parties by applying traps to trick the party. This implementation is applied to a Raspberry Pi by implementing Honeypot in it. All attacker activities that occur will be recorded by Cowrie and stored in a database. The information that has been obtained is then visualized to Grafana and automatically notified to the server owner.

The results of this implementation, can catch all activities of the attacker without any significant errors in network traffic when the server owner uses the server simultaneously. Attacks that can be logged include bruteforce and port scanning as well as normal login activity on the server. The attack records are categorized into two conditions, if the attack is successful in entering the username and password combination it will be symbolized by the number 1 and vice versa if failed will be symbolized 0, which will help visualize the activities that occur.

Keywords: *Cowrie, Server, Grafana, Raspberry Pi, Telegram*