ABSTRACT

The Internet is a connection between various types of computers and also with networks in the world that have different operating systems and applications. Based on the survey results of the Indonesian Internet Service Providers Association (APJII), internet users in Indonesia reached 215.63 million people in the 2022-2023 period. The more internet users, the higher the cyberattacks that threaten computers. This research discusses attacks on dummy servers and strengthening the original server. The dummy server is made using a honeypot so that the system is able to record and monitor the activities carried out by the attacker so that it can provide information to an administrator. In this study will use two types of honeypots namely Kippo Graph and Dionaea to secure servers, these two honeypots have different capabilities. Where in the process of testing honeypots, kippo graphs are used to monitor Brute Force attacks, while Dionaea honeypots are used to monitor DoS and Sql attacks. Testing was carried out in twoscenarios, the first scenario attacked a mock server and the second scenario attacked the original server that had been strengthened by looking at the results in the first scenario. The results of the study in the first scenario showed that the honeypot system implemented in the study managed to record every activity carried out by the attacker where the information was recorded in real time and stored in the form of a log file, then in the second scenario the attacker could not enter the original server because the author had blocked the attacker's IP and closed all ports that could be entered by the attacker.

Keyword: *Brute Force, Daniel of Server, Honeypot, Honeypot Kippo Graph, Honeypot Dionaea, Medusa, SQL.*