ABSTRACT

In computer terms, Honeypot is a method of security mechanism to detect, block, or in some way be able to counter unauthorized actions on a computer. Honeypot is included in the intrusion prevention system (IPS) category which is widely used on computers to secure the computer. Honeypots can help in learning how attackers carry out attacks because in Honeypots you can find out what the attackers did to carry out attacks. Of all the capabilities of the Honeypot, Honeypot has one drawback where the User Interface is less friendly to humans, there is no explanation of the total number of incoming logs, and there is no time and date for the log to be received.

Therefore, in this final project, I want to try to use Elasticsearch and Kibana applications to make the results of the Honeypot recording more user-friendly. By using Elasticsearch as the database engine and Kibana as an application to display the results from the Elasticsearch. Then it can make the data from the Honeypot easier to read and can be stored by the user, so as to make it easier to use the Honeypot. Testing is carried out by carrying out cyber attacks on honeypots, comparing log results from these attacks, and analyzing server resources that are used when an attack occurs.

Test results can be concluded that Elasticsearch is able to receive all Log data from Honeypot. Where the results of the comparison of Log data in the honeypot are exactly the same as those in Kibana. And from the server resource analysis, it was found that the use of Elasticsearch to help monitor logs was a burden on the server because Elasticsearch uses a lot of server resources. Elasticsearch uses up to 86% of server resources. Where only 17% resource usage if Honeypot runs without Elasticsearch

Keywords: *Honeypot, Elasticsearch, Kibana, Docker.*