ABSTRACT

Servers are the heart of several platforms now such as websites, games, DHCP, mail, cloud, databases, and many more that can meet user needs. Therefore, security is very crucial to reduce the percentage of attacks or data leaks, especially on the database server. Prevention of this attack uses the vulnerability assessment method using the ELK Stack which will be applied to the database server. By using statistical tests and three sigma on the results of the ELK Stack graph to test the vulnerability assessment in this Final Project research.

The ELK Stack works independently by breaking it into sections. Starting from Elasticsearch, Logstash, and Kibana which have their respective functions. Has a workflow starting from the logs that Elasticsearch will search for, also Logstash which then sorts the log search results which will later display graphical results from Elasticsearch and Logstash on Kibana. So that the graphical results on Kibana can be tested statistically whether the ELK Stack can be used for vulnerability assessment tools.

Tests in the implementation of the ELK Stack on vulnerability assessment tools use statistical testing methods by looking for standard deviation values and three sigma values. As the results of this test get an average standard deviation value of 1,266.9 from 5 dataset features. From the results of this test, the implementation on the ELK Stack for vulnerability assessment tools is only able to read logs but cannot scan the logs.

Keywords: Dataset, DDoS, ELK Stack, Security, Server, Vulnerability Assessment.