ABSTRACT

With the development of technology, database server-based storage media is becoming increasingly used, especially for corporate or academic purposes. The use of this database server is very vulnerable to data security threats, so a vulnerability detector, namely the ELK Stack, is needed. Installation of security applications is important to reduce the risks posed by service providers so that the security of data owned by service providers can be maintained.

Using the ELK Stack can increase security because it can tell if there is log data that is vulnerable to attack or data theft. This ELK Stack is able to reduce threats by filtering the log data processed by Logstash based on data received by Elasticsearch when retrieving data from a server that has installed ELK Stack. By filtering the existing data, it will be categorized as vulnerable data and not then that information will be displayed on the Kibana main menu so that it can follow up on threats.

Tests were carried out on the ELK Stack as a Vulnerability Assessment Tool which resulted in the use of the ELK Stack application having a function to read logs. Subsequent testing of data that has been processed on the ELK Stack is carried out statistical tests using the 3 Sigma Rule method. The results obtained from statistical testing based on four times of testing obtained 100% results because all tests met the requirements, namely 99.7% of the data was in three sigma sections.

Keyword: ***Cloud, ELK Stack, Elasticsearch, Kibana, Logstash.***