ABSTRACT

Vulnerability Scanning is one of the initial stages used in the practice of penetration testing (or pentesting), vulnerability scanning can be said to be a vital process because it can determine how the penetration testing process will be carried out later. The conventional method requires scanning to be done as a whole, which takes a long time and uses a large amount of resources. In this paper, the author proposes a method that applies the Gradient Boosting which is one of a few types from Boosting Algorithm to perform a vulnerability scan based on the port response of the target host. There are only 5 (five) types of ports that being used as a parameters, which all ports have been determined and considered from several books references. And from a several books references itself, it is stated that three of these five ports have a percentage of 65% the most frequent and vulnerable to exploitation activities, these three ports include TCP 22, TCP 80, TCP 443, whereas the two other ports is only an addition to increase exploitation rate percentage which also determined and considered from a book reference, the other two ports is UDP 53, and UDP 80. From the results of tests carried out in 15 times of testing using the CV (or Cross Validation) method, the model built by applying the Gradient Boosting Algorithm gets the results of accuracy, precision, and recall respectively by 98.810%, 98.903%, and 98.812% and with average error rate around 0.00260.

Keywords: Vulnerability Scanning, Port Response, Machine Learning, Boosting, Gradient Boosting.