Abstract

Advanced Persistent Threat is an attack that is carried out continuously with the aim of maintaining long-term access to the target network. Therefore, this research proposes a solution to the detection of Advanced Persistent Threat (APT) attacks in network traffic using machine learning methods. The proposed method includes the use of random forest algorithm, and recursive feature elimination to improve the accuracy of APT attack detection. The process includes retrieving datasets from SCVIC-APT-2021, preprocessing datasets, and developing detection system models. After the dataset preprocessing stage is carried out, the next dataset passes the feature selection stage to be trained using the random forest model. Evaluation of the final results was carried out using the confusion matrix to measure the performance of the model and obtained accuracy for the datasets of 99.99% and 99.88%.

Keywords: *advanced persistent threat, random forest, recursive feature elimination, malware, network traffic*, *APT attack detection*