World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:06, 2018

Hierarchical Filtering Method of Threat Alerts Based on Correlation Analysis

Authors : Xudong He, Jian Wang, Jiqiang Liu, Lei Han, Yang Yu, Shaohua Lv

Abstract : Nowadays, the threats of the internet are enormous and increasing; however, the classification of huge alert messages generated in this environment is relatively monotonous. It affects the accuracy of the network situation assessment, and also brings inconvenience to the security managers to deal with the emergency. In order to deal with potential network threats effectively and provide more effective data to improve the network situation awareness. It is essential to build a hierarchical filtering method to prevent the threats. In this paper, it establishes a model for data monitoring, which can filter systematically from the original data to get the grade of threats and be stored for using again. Firstly, it filters the vulnerable resources, open ports of host devices and services. Then use the entropy theory to calculate the performance changes of the host devices at the time of the threat occurring and filter again. At last, sort the changes of the performance value at the time of threat occurring. Use the alerts and performance data collected in the real network environment to evaluate and analyze. The comparative experimental analysis shows that the threat filtering method can effectively filter the threat alerts effectively.

Keywords : correlation analysis, hierarchical filtering, multisource data, network security
Conference Title : ICICS 2018 : International Conference on Information and Communications Security
Conference Location : San Francisco, United States
Conference Dates : June 06-07, 2018