Kaspersky Lab

Intrusion detection based on intelligent data analysis

Background / Problem statement:

Targeted attacks are becoming increasingly sophisticated in terms of the technologies used. It becomes a non-trivial task to detect a targeted attack in which the attacker uses unknown tools, such as new malware or 0-day vulnerabilities. In this task, you have to develop a system that will use intelligent analysis of data communicated in network traffic to detect an ongoing targeted attack within a corporate network.

Task:

Compile a list of indicators of network traffic anomalies, and develop an algorithm of intelligent data analysis (e.g. using machine learning algorithms), develop architecture and a proof-of-concept of an intrusion detection system that will perform a search of network traffic (source data to be provided in .PCAP format).

Solution requirements

Presentation of the algorithm, list of network traffic anomaly indicators and software module that searches for attacks within network traffic (traffic to be provided in .PCAP format).

Technical requirements for the solution

The module must be provided in the form of an algorithm description and a list of indicators that the algorithm uses. During the demonstration, the model must accept input data about network traffic in the .PCAP format, and provide a description of the detected attacks/anomalies as output.

Evaluation criteria

- Criterion: List of network traffic anomaly indicators and algorithm flowchart (depending on how well developed the diagram is)
  Evaluation: maximum 5 - minimum 1.
- Criterion: System architecture (depending on the completeness of the provided chart)
  Evaluation: maximum 5 - minimum 1.
- Criterion: List of open-source solutions and components that can be used to solve the task (with proof of their existence)
  Evaluation: maximum 5 - minimum 1.
- Criterion: Debugged and operational software module (can be delivered in the form of an extension to an open-source product)
  Evaluation: maximum 5 - minimum 1.

Study materials

https://people.csail.mit.edu/kalyan/AI2_Paper.pdf

https://www.elastic.co/blog/introducing-machine-learning-for-the-elastic-stack

You may take traffic here: http://www.malware-traffic-analysis.net/2017/index.html