Лаборатория Касперского

Обнаружение вторжений на основе интеллектуального анализа данных

Контекст / описание проблемы:

Целевые атаки становятся сложнее с технологической точки зрения. При этом выявление целевой атаки, в ходе которой атакующий использует новые неизвестные ранее инструменты (например, вредоносное программное обеспечение и уязвимости «нулевого дня») становится задачей нетривиальной. В процессе решения данной задачи предлагается разработать систему, которая на основе интеллектуального анализа данных в сетевом трафике, способна обнаружить активную целевую атаку в периметре корпоративной сети.

Задача:

Составить перечень признаков аномалий сетевого трафика и разработать алгоритм интеллектуального анализа данных (например, с использованием алгоритмов машинного обучения), архитектуру и концепт (proof-of-concept) системы выявления вторжений, которая будет проводить поиск в сетевом трафике (формат исходных данных - .pcap).

Требования к решению:

Презентация алгоритма, набора признаков сетевого трафика и программный модуль, выполняющий поиск атак в сетевом трафике (трафик задан в .pcap-формате)

Технические требования к решению:

Модуль необходимо предоставить в виде описания алгоритма и набора признаков, используемых данным алгоритмом. Кроме того, в процессе демонстрации данный модуль должен принимать на вход данные о трафике в формате .pcap и на выходе демонстрировать описание обнаруженных атак/аномалий.

Критерии оценки:

- Критерий: Предоставление набора признаков сетевого трафика и блок-схемы алгоритма (определяется проработанной блок-схемой)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Предоставление архитектуры системы (определяется полнотой представленной схемы)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Наличие списка OpenSource-решений и компонентов, использование которых возможно для решение данной задачи (с обоснованием их наличия)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Наличие отлаженного, работающего программного модуля (возможно наличие модуля в видео расширения к OpenSource-продукту)
  Шкала оценки: максимальный балл - 5, минимальный балл - 1.

Материалы для проработки:

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

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

Трафик: http://www.malware-traffic-analysis.net/2017/index.html