УДК 004.056

ПОДХОД К ВЫЯВЛЕНИЮ АНОМАЛИЙ В ЛОКАЛЬНОЙ СЕТИ НА ОСНОВЕ АНАЛИЗА ЗАГОЛОВКОВ TCP ПАКЕТОВ.

Автор – Щетинин Даниил Сергеевич (Университет ИТМО)

Научный руководитель - к.т.н. Попов Илья Юрьевич

Введение. Злоумышленники придумывают все более изощренные сценарии атак. Наиболее сложными с точки зрения реализации и выявления являются целевые или APT (Advanced Persistent Threat) атаки. Реализация подобных сценариев, часто сопровождающихся эксплуатацией «0-day» уязвимостей, требует от злоумышленников тщательной подготовки, высоко уровня знаний, владения различными техниками взлома и разведки, а также терпения, т.к. атака может растягиваться на длительный период времени. Злоумышленники действуют максимально осторожно, что позволяет им избегать детектирования стандартными системами обнаружения вторжений, которые для принятия решений используют сигнатурный анализ. Указанная проблема стала причиной роста числа исследований, которые связывают обнаружение аномалий в сетевом трафике с обнаружением целевых атак. Одним из перспективных направлений исследований, связанных с классификацией сетевого трафика является применение технологий машинного обучения (МО). В качестве основной проблемы решений, основанных на МО, выделяют высокий процент ложноположительных срабатываний, что сильно ограничивает возможность их практического применения.

Цель работы. Целью данной работы является сравнение различных методов к обнаружению аномальной активности сетевом трафике и разработка собственного подхода, учитывающего необходимость минимизации процента ложноположительных срабатываний.

Основной результат. Работа включает сравнение различных алгоритмов машинного обучения в аспекте обнаружения аномальной активности в сетевом трафике. Выделяются основные актуальные проблемы применения подходов, основанных на МО. Предлагается решение, которое сочетает в себе простоту сигнатурного анализа заголовков TCP пакетов и возможности подходов, основанных на машинном обучении, за счет их совместного использования для достижения поставленной цели. Проведена апробация предлагаемого подхода, результаты которой доказывают его применимость для решения задачи выявления аномальной сетевой активности в ряде конкретных случаев. Выдвинута новая гипотеза, определено направление дальнейших исследований.

Автор _____ Щетинин Д.С

Научный руководитель _____ Попов И.Ю