1. Тема Магистерской диссертации – Универсальный анализатор трафика. Система предотвращения/обнаружения вторжений (IPS/IDS).
2. Руководитель – Казаков Федор Александрович
3. Цель:

Создание технологий обнаружения и предупреждения компьютерных атак на объекты критической информационной инфраструктуры (далее — КИИ) на ранних стадиях их подготовки.

Задачи:

- Сопоставление технологий идентификации устройств в трафике и выявление сетевых атак в условиях априорной информации

- Экспериментальная проверка программных реализаций алгоритмов идентификации устройств в трафике и выявление сетевых атак

- Исследование в области создания интеллектуальных технологий анализа трафика, способных заменить человека-оператора при решении задач по картированию сегмента сети Интернет и защите ресурсов в сети.

1. Типичная бизнес-сеть имеет несколько точек доступа к другим сетям, как общедоступным, так и частным. Задача состоит в том, чтобы поддерживать безопасность этих сетей, оставляя их открытыми для своих клиентов. В настоящее время атаки настолько сложны, что они могут быть направленны на системы безопасности, которые работают в сети защищенной шифрованием или фаерволами. К сожалению, одних этих технологий недостаточно для противодействия сегодняшним атакам.
2. Существует два типа IDS:

- IDS на основе хоста: защищает конечную систему или сетевые ресурсы.

- Сетевой IDS: отслеживает сетевой трафик на предмет атак. Сетевой IDS развернут в сети рядом с брандмауэром, в DMZ или даже внутри доверенной внутренней сети.

Snort - вызывает модуль анализа, который применяет набор правил к трафику при его прохождении. Эти правила называются «базовыми политиками. Также можно написать свои собственные правила, для этой IDS, а также загрузить правила, разработанные опытными пользователями Snort

Suricata, вероятно, является основной альтернативой Snort. У Suricata есть ключевое преимущество перед Snort, он собирает данные на прикладном уровне, ждет, пока все данные в пакетах не будут собраны, прежде чем переместит информацию на анализ

Несовершенство IDS и ошибки в их ПО позволяют находить условия, при которых они не способны обнаружить атаку в сетевом трафике. Среди достаточно давно известных техник обхода стадии разбора стримов можно перечислить и такие:

• Нестандартная фрагментация пакетов на уровнях IP, TCP или, например, DCERPC, с которой IDS порой не способна справиться.

• Пакеты с пограничными или некорректными значениями TTL или MTU также могут обрабатываться IDS некорректно.

• Неоднозначность восприятия накладывающихся TCP-фрагментов (номеров TCP SYN) может трактоваться IDS иначе, чем на сервере или клиенте, которому этот TCP-трафик предназначался.

• Подставной пакет TCP FIN, например с неверной контрольной суммой (т. н. TCP un-sync), может быть воспринят как конец сессии вместо игнорирования.

• Разное время таймаута TCP-сессии между IDS и клиентом также может послужить инструментом для сокрытия атак.

1. Проект OPNids, предоставляет разработчику ПО с открытым исходным кодом и аналитикой центра операционной безопасности (SOC). Это первый случай, когда аналитика может интегрировать механизм машинного обучения DragonFly Machine Learning Engine (MLE) с механизмом обнаружения вторжений Suricata, для сетевой проверки сложных угроз
2. В основе OPNids лежит механизм машинного обучения DragonFly (MLE), который использует модель анализа потоковых данных для получения сетевых данных с линейной скоростью из Suricata

Dragonfly MLE предоставляет мощную среду для развертывания алгоритмов обнаружения аномалий, поиска угроз и прогнозов машинного обучения в инфраструктуре сетевой безопасности. MLE может обрабатывать сотни тысяч событий в секунду, используя многопоточный механизм потоковых приложений с поддержкой сценариев для обнаружения сетевых угроз, реализованный в C.

Сценарии включают в себя следующие возможности:

- Lua (LuaJIT - это компилятор Just-In-Time (JIT) для языка программирования Lua (язык сценариев))

- JSON

- Redis (Хранилище структуры данных в памяти, с открытым исходным кодом, используется как для баз данных, так и для реализации кэшей. Он поддерживает структуры данных, такие как строки, хэши, списки, наборы, отсортированные наборы с запросами диапазона, растровые изображения. Redis имеет встроенную репликацию, сценарии Lua)

- Redis-ML - это модуль для Redis, который включает в себя возможность оценивать ранее обученные модели, включая:

- Линейная регрессия

- Логистическая регрессия

- Дерево принятия решений (Random forest)

1. Основная задача, выяснить механизм работы машинного обучения по обнаружению вторжения. Убедится, что машинное обучение позволяет IDS, уменьшить время обнаружения вторжения и повысит качество определения класса атаки.