Латыпов Шамиль, группа 323

Научный руководитель: Жуматий Сергей Анатольевич

15 декабря 2021 г.

Отчет по работе

(СЛАЙД 1 - Титульный слайд)

В чем заключается цель научной работы: (СЛАЙД 2) На данный момент есть потребность в изучении поведения сети – атаки, аномалии. Для этого есть различные инструменты по типу Snort/Suricata и другие, которые позволяют ловить весь трафик внутри сети, записывать логи и представлять их администратору в виде файлов со стеной текста. (СЛАЙД 3) Анализ этих данных становится сложной задачей, так как известные средства для обработки этих логов имеют недостатки. (СЛАЙД 4) Например, одна из самых популярных open-source систем ELK (аббревиатура берется из названия трех отдельных систем Elasticsearch, Kibana и Logstash, из которых эта система и состоит) помимо самих данных о трафике хранит в себе разбиение на поля и геометки, из-за чего кратно увеличивается требуемое место на хранение данных. Также ELK не имеет возможности настройки уровней доступа для пользователей. Есть и другой популярный инструмент Splunk, в которой эти проблемы отсутствует, но за эту систему надо платить лицензию для использования, при чем цена рассчитывается в зависимости от объема данных, проходящих через систему. Поэтому эти две архитектуры являются неудобными и дорогими соответственно. Цель моей научной работы – облегчение взаимодействия админов с внеплановыми вторжениями путём создания интерфейса для чтения и анализа записанных логов трафика. (СЛАЙД 5) Работа началась с изучения самой этой системы и как она работает. Были изучены классификации защитных систем IDS и IPS (как они в целом работают и в чем их сходства/отличия), устаревшая система Snort, которая очень похожа по функционалу на Suricata, а также был изучен принцип работы этой системы защиты.

(СЛАЙД 6). Начну с описания самой системы Suricata. Suricata — это система предотвращения сетевых вторжений и обнаружения нарушения безопасности. Есть две классификации - IDS (Intrusion Detection System) и IPS (Intrusion Prevention System). Основное отличие этих архитектур заключается в том, что IDS только находит нарушения в сети, а система IPS предотвращает её путем заданных пользователем способом (например, ограничивает трафик по IP). (Возможно где-то тут тоже можно поменять слайды). Также архитектура обнаружения атак имеет три вида - сигнатурные, основанные на правилах и основанные на аномалиях. Сигнатурные ищут анализируют трафик по шаблонам, то есть известным заранее потенциальным атакам. Основанные на правилах работают по принципу ФАКТ -> ДЕЙСТВИЕ, то есть точечные правила работы в сети, которые имеют очень тонкую настройку. Основанные на аномалиях системы ищут отличающееся от нормального поведения трафик в сети.

(СЛАЙД 7) Теперь расскажу о своем опыте взаимодействия с этой системе. По предоставленным мне файлов логов (как примеры для работы), была написана программа для чтения этих данных. Первая версия считывала все логи и записывала их в отдельный файл в сокращенном виде, последующее же улучшение программы уже позволило выводить конкретные данные по нужным параметрам. (СЛАЙД 8) Например, можно было задать параметр приоритета сетевой «атаки», и программа выводила все строки обращений с заданным приоритетом, который обозначила система Suricata. Это поможет в дальнейшем помочь в анализе всех «атак» в сети для выведения каких-то корреляций активностей, настроек шаблонов сканирования, и так далее.

Также, помимо написания своей программы для работы с логами, была попытка установки этой системы на личный ноутбук для тестовых прогонов некоторых функций. Были произведены базовый запуск системы и попытки по настройке флагов конфигурации. Этот этап, к сожалению, не принес каких-то полезных продвижений в работе в связи с ограниченностью работы архитектуры на новых версиях MacOS и малом количестве документаций для этой системы, но в ближайшее время появится возможность работать за компьютером под управлением системы Linux. Вся необходимая документация по установке и запуске систем была уже сохранена и изучена еще при первой установке, поэтому при старте работы на другом устройстве на это не будет потрачено много времени.

(СЛАЙД 9) Какие планы имеются на будущее: Во-первых – это модернизация программы. Она уже находится в совершенствовании и в нее планируется добавить больше параметров, настройки формата вывода и возможность выбора фильтров сразу по нескольким типам данных. Это поможет в дальнейшем продвинуться в анализе данных. Во-вторых – так как я в скором времени получу доступ к компьютеру под управлением Linux, было бы неплохо произвести установку Suricata. Таким образом получится лично повзаимодействовать с системой, что позволит осознать, как она выводит лог файлы и по каким параметрам её можно настраивать. Это даст полное понимание в значении всех выходных данных. Ну и дальнейшем уже появится задача по созданию полноценного интерфейса для взаимодействия администратора с этими данными и с системой Suricata.

(СЛАЙД 10 - «Спасибо за внимание») По этой работе могут возникать некоторые вопросы, отвечу сразу на некоторые из них.

* Для чего это нужно? Чтобы просто обезопасить свою систему от атак и вторжений. Для этого подобные системы анализируют весь входящий трафик, благодаря чему могут мониторить безопасность сети и обнаруживать вторжения. И моя цель помимо простого обнаружения еще и создать удобный для юзера/администратора интерфейс, чтобы подобные аномалии быстро предотвращать, так как сейчас такого легкого взаимодействия не присутствует.
* Какие есть аналоги? Snort, созданная еще в 1998 году. Её проблема заключается в том, что она не имеет какого-то графического интерфейса, поэтому с ней работать со стороны администратора может быть проблематично. Есть система Bro, или с другим названием Zeek. Она, возможно, даже лучше подходит для моей цели по предотвращению вторжений, так как эта архитектура имеет в себе механизм анализа трафика. Но также она имеет слишком сложную настройку и установку, из-за чего мне придется потратить лишнее время на эти пункты.