005

Практическая работа

Информационно-аналитические технологии поиска угроз инорфмационной безопасности

Исследование информации о состоянии беспроводных сетей

Цель работы

1. Получить знания о методах исследования радиоэлектронной обстановки.
2. Составить представление о механизмах работы Wi-Fi сетей на канальном и сетевом уровне модели OSI.
3. Зекрепить практические навыки использования языка программирования R для обработки данных
4. Закрепить знания основных функций обработки данных экосистемы `tidyverse` языка R

Общая ситуация

Вы исследуете состояние радиоэлектронной обстановки с помощью журналов программных средств анализа беспроводных сетей – `tcpdump` и `airodump-ng`. Для этого с помощью сниффера (микрокомпьютера Raspberry Pi и специализированного Wi-Fi адаптера, переведенного в режим мониторинга) собирались данные. Сниффер беспроводного трафика был установлен стационарно (не перемещался). Какой анализ можно провести с помощью собранной информации?

Задание

Используя программный пакет dplyr языка программирования R провести анализ журналов и ответить на вопросы.

Данные

> **Ссылка на данные**
>
> https://storage.yandexcloud.net/dataset.ctfsec/P2_wifi_data.csv

Ход работы

Для выполнения предложенного задания Вам необходимо последовательно проделать следующие шаги:

Подготовка данных

1. Импортируйте данные.

> **Что за формат данных**
>
> Данные были собраны с помощью анализатора беспроводного трафика **airodump-ng**

> **Обратите внимание!**
>
> Формат CSV лога **airodump-ng** меняется внутри файла (имеет разное число столбцов). По сути, это два разных датасета:
>
> - датасет 1 – анонсы беспроводных точек доступа;
> - датасет 2 – запросы на подключение клиентов к известным им точкам доступа.
>
> Для решения проблемы можно использовать параметр `skip` в функции `readr::read_csv()`

2. Привести датасеты в вид “аккуратных данных”, преобразовать типы столбцов в соответствии с типом данных
3. Просмотрите общую структуру данных с помощью функции `glimpse()`

Анализ

Точки доступа

1. Определить небезопасные точки доступа (без шифрования – OPN)
2. Определить производителя для каждого обнаруженного устройства

> **Для этого можно воспользоваться:**
>
> - базой данных производителей из состава Wireshark;
> - онлайн сервисами OUI lookup.

3. Выявить устройства, использующие последнюю версию протокола шифрования WPA3, и названия точек доступа, реализованных на этих устройствах
4. Отсортировать точки доступа по интервалу времени, в течение которого они находились на связи, по убыванию.

> **Обратите внимание!**
>
> Не забудьте склеить сессии! Сессии считаются независимыми если интервал времени между ними превышает **45 минут**.

5. Обнаружить топ-10 самых быстрых точек доступа.
6. Отсортировать точки доступа по частоте отправки запросов (beacons) в единицу времени по их убыванию.

Данные клиентов

1. Определить производителя для каждого обнаруженного устройства

> **Для этого можно воспользоваться:**
>
> - базой данных производителей из состава Wireshark;
> - онлайн сервисами OUI lookup.

2. Обнаружить устройства, которые НЕ рандомизируют свой MAC адрес
3. Кластеризовать запросы от устройств к точкам доступа по их именам. Определить время появления устройства в зоне радиовидимости и время выхода его из нее.
4. Оценить стабильность уровня сигнала внури кластера во времени. Выявить наиболее стабильный кластер.

> **Обратите внимание!**
>
> Для оценки стабильности оценить математическое ожидание и среднеквадратичное отклонение для каждого найденного кластера.

> **Tip**
>
> Дополнительные материалы можно найти в Telegram https://t.me/datadrivencybersec

Отчет

Для оформления отчета используйте следующие материалы:

1. https://i2z1.ddslab.ru/posts/lab_recommendations/
2. https://i2z1.quarto.pub/checklab/criteria.html
3. https://github.com/i2z1/Report_template

Сайт курса

https://i2z1.ddslab.ru/IAMCTH