**Лабораторная работа № 3.**

Анализ устойчивости алгоритмов шифрования wep и wpa-tkip

1.Постановка задачи:

Цель работы – анализ устойчивости ко взлому и уязвимостей протоколов шифрования WEP и WPA-TKIP, изучение признаков атак, направленных на взлом Wi-Fi сети, определение параметров сети, необходимых для обеспечения ее безопасности.

Результат выполненной работы:

1. Какой алгоритм лежит в основе шифрования WEP? Какой уровень защиты должно было обеспечить шифрование WEP? Обеспечивается ли этот уровень на данный момент?

Протокол WEP позволяет шифровать поток передаваемых данных на основе алгоритма RC4 с ключом размером 64 или 128 бит.

2. Какого размера могут быть ключи при использовании шифрования WEP? Из каких частей они состоят?

Ключи размером 64 или 128 бит

Данные ключи имеют так называемую статическую составляющую длиной от 40 до 104 бит и дополнительную динамическую составляющую размером 24 бита, называемую вектором инициализации (Initialization Vector)

3. В чем заключается основная уязвимость шифрования WEP?

• механизмы обмена ключами и проверки целостности данных

• малая разрядность ключа и вектора инициализации ( англ . Initialization vector )

• способ аутентификации

• алгоритм шифрования

4. Какое главное отличие шифрования WPA от WEP?

Поддержкой типа шифрования AES CCMP.

WEP или Wired Equivalent Privacy

Первой беспроводной сетью безопасности был WEP или Wired Equivalent Privacy протокол. Он начался с 64-битного шифрования (слабый) и в итоге прошел весь путь до 256-битного шифрования (сильный). Наиболее популярной реализацией в маршрутизаторах по-прежнему является 128-битное шифрование (промежуточное). Это было рассмотрено как возможное решение, пока исследователи безопасности не обнаружили несколько уязвимостей в нем, что позволило хакерам взломать ключ WEP в течение нескольких минут. Он использовал CRC или Cyclic Redundancy Check.

WPA или защищенный доступ Wi-Fi

Чтобы устранить недостатки WEP, WPA был разработан как новый стандарт безопасности для беспроводных протоколов. Для обеспечения целостности сообщений он использовал протокол целостности TKIP или Temporal Key Integrity. Это было отличным от WEP в некотором смысле, который использовал CRC или Cyclic Redundancy Check. Считалось, что TKIP намного сильнее, чем CRC. Его использование обеспечивало передачу каждого пакета данных с помощью уникального ключа шифрования. Комбинация клавиш увеличила сложность декодирования ключей и тем самым уменьшила количество вторжений из вне. Однако, как и WEP, WPA тоже имел недостаток. Таким образом, WPA был расширен в WPA 2.

5. Какой тип шифрования WPA в настоящее время уязвим для взлома?

WPA-PSK

6. Какое условие является обязательным при взломе WPA-PSK? Для чего оно необходимо?

Установить на беспроводной точке доступа WPA-PSK. Установите ключ, взятый из словаря, находящийся в начале списка

7. По какому методу осуществляется подбор WPA-PSK ключа?

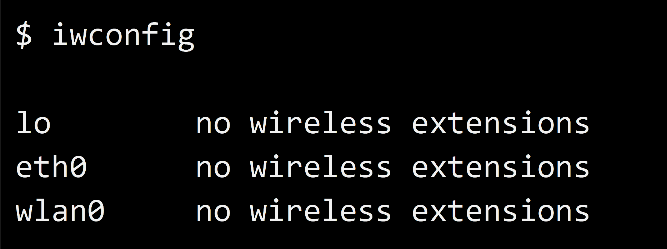
После захвата handshake- пакета можно перейти к процессу перебора ключей в программе airckrack. Скорость перебора зависит от характеристик компьютера, на современных компьютерах в среднем равна 300-600 вариантам в секунду. Также есть специальные программы, позволяющие использовать для процесса подбора ресурсы мощных видеоадаптеров, что позволяет на порядок увеличить скорость подбора .

8. От чего самым непосредственным образом зависит успешность подбора ключа?

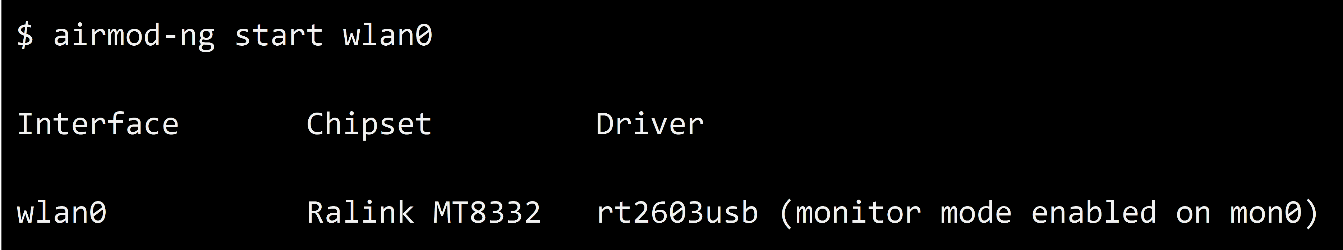
Может ли WPA-PSK обеспечить надежную защиту информации?

Подбор ключа WPA-PSK будет успешным только в том случае, если он будет присутствовать в словаре по которому ведется перебор .

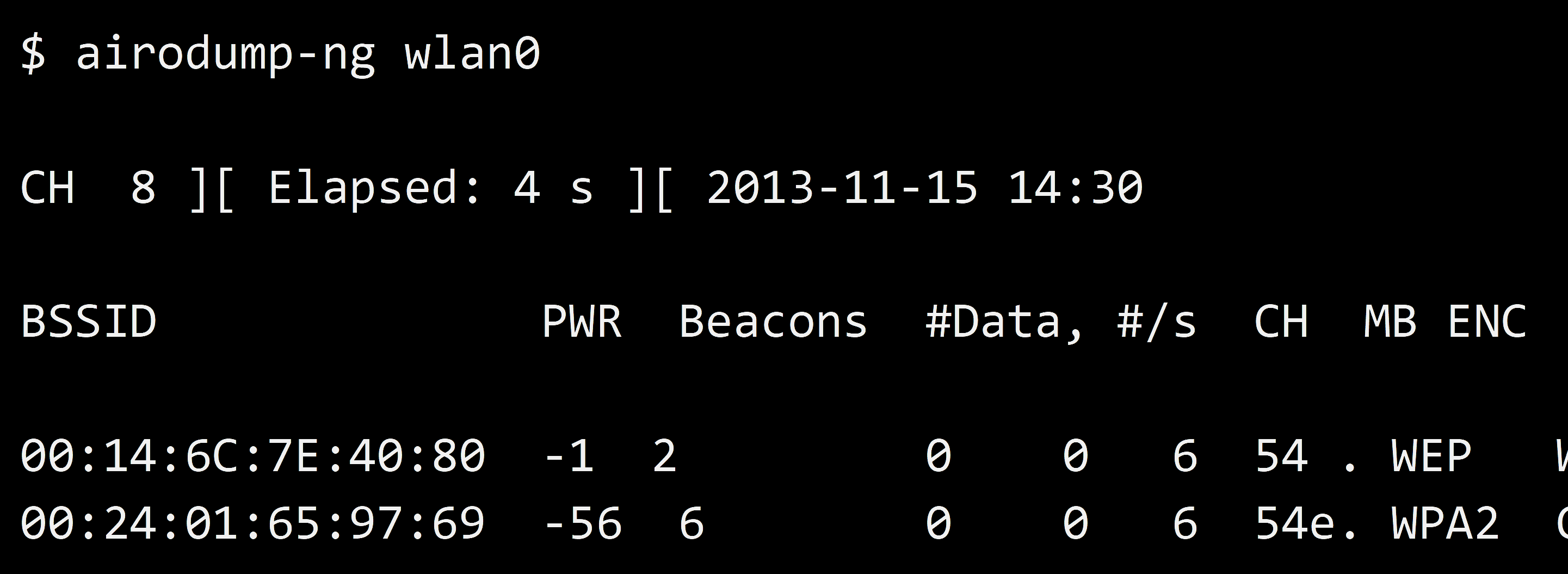
1. Узнаем имя беспроводного интерфейса с помощью iwconfig.



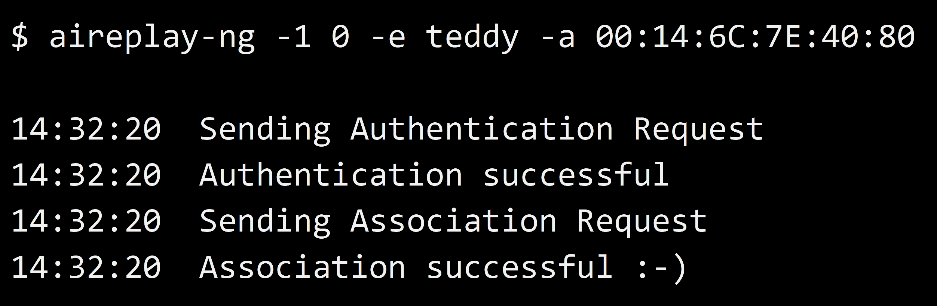
1. Запускаем интерфейс в режиме мониторинга



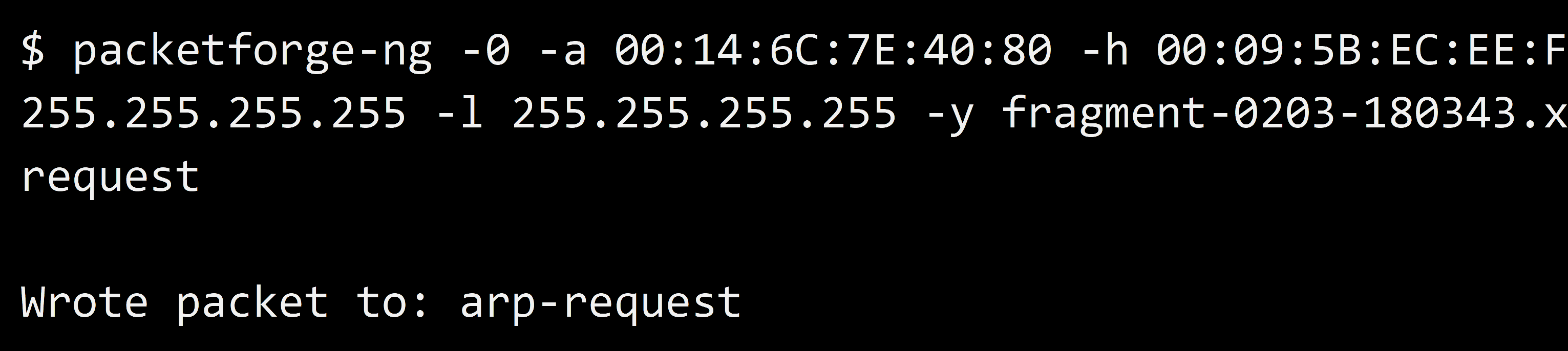
1. Выбираем сеть для атаки среди доступных.



1. Используем aircrack-ng, чтобы произвести авторизацию.



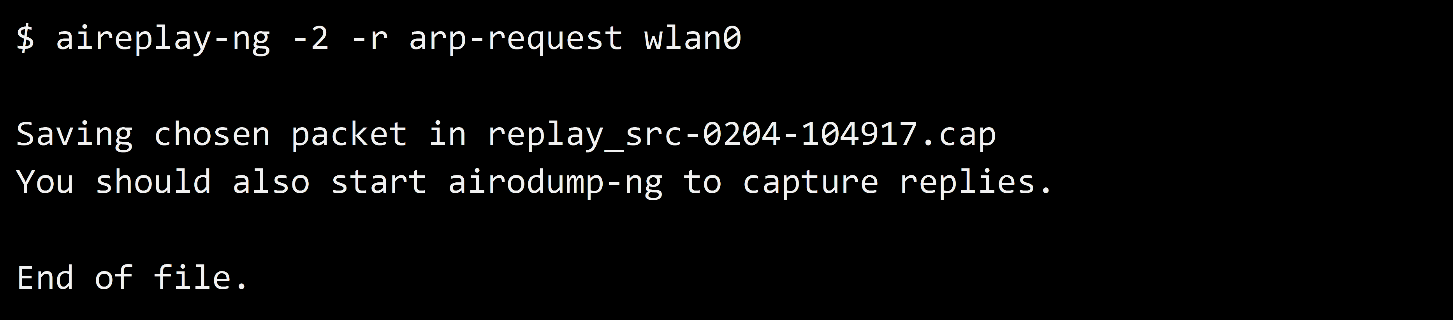
1. Получаем PRGA в новой консоли.
2. Получили .xor файл. Генерируем пакет для инъекции.



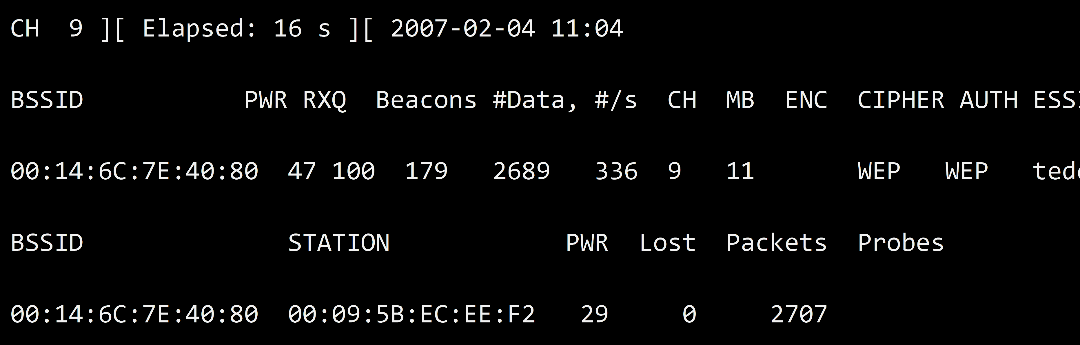
1. В новой консоли:



1. В консоли, где сгенерировали пакет – начинаем инъекцию:



1. Вывод в третьей консоли:

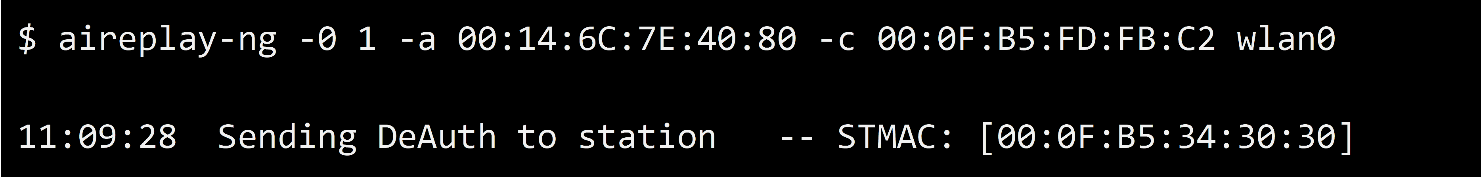


1. Запускаем aircrack-ng для получения WEP ключа

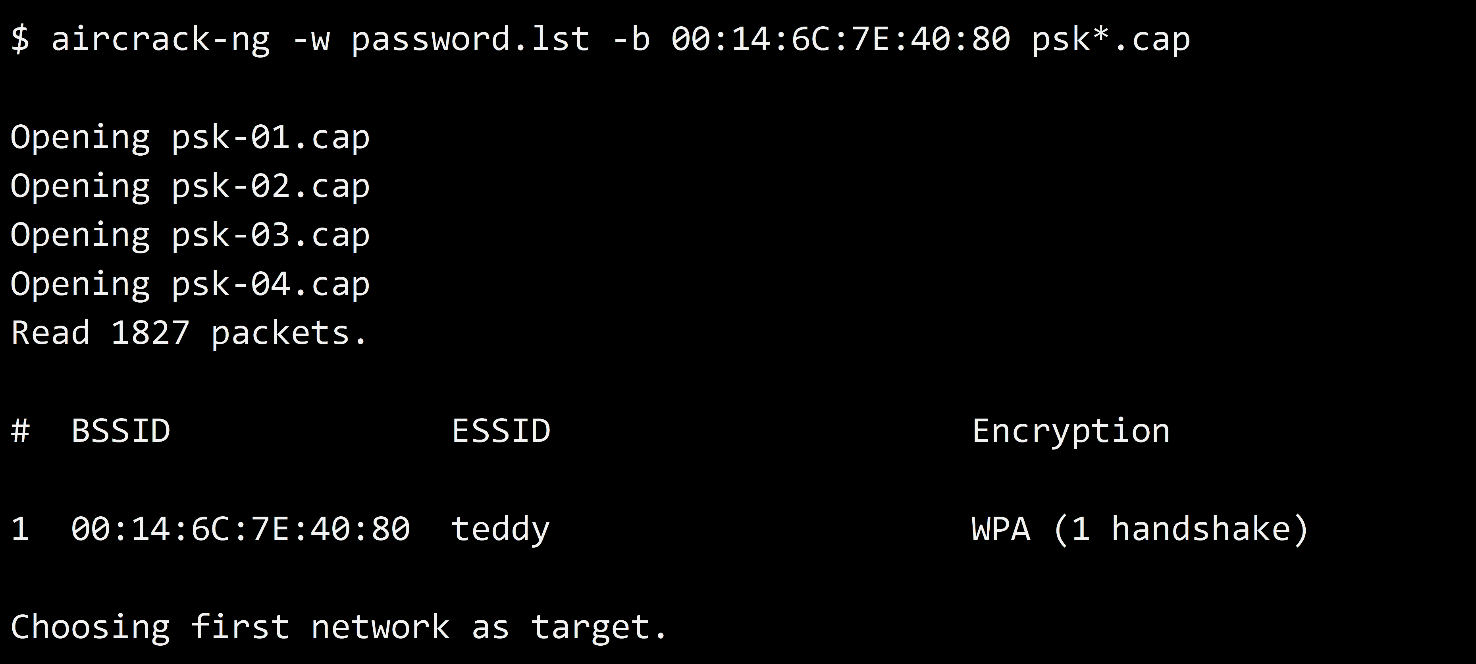


WPA-PSK

1. Повторяем пункты 1-3 прошлого эксперимента.
2. Используем aireplay-ng для деаутентификации клиентов.



1. Запускаем aircrack-ng для взлома ключа пре-авторизации.



1. Результат.



|  |  |  |
| --- | --- | --- |
|  | **WEP** | **WPA-PSK** |
| Пароль | 1234qwert | 1234qwert |
| Время определения пароля, с | 425c | 535c |
| Количество пакетов, необходимое для определения пароля. | 2807 | 1927 |

* В основе алгоритма шифрования WEP лежит простой XOR, который не обеспечивает должный уровень защиты на сегодняшний день.
* Размер WEP ключей - 64 или 128 бит. Состоит из статической и динамической частей.
* Чтобы определить ключ WEP нам нужно перехватить векторы инициализации (динамическая часть).
* Плохое проектирование WEP - основная проблема. Ключ фактически частями передает часть байт этого ключа.
* WPA шифрует данные каждого клиента отдельно.
* Уязвим WPA-PSK.
* Нужно чтобы был подключен как минимум один клиент к точке доступа. Так как нам нужно перехватить “пакет-рукопожатия” для последующего перебора.
* Прямой перебор пароля используя словари.
* Количество символов в пароле, их вариативность.
* Да, если грамотно подобрать пароль.