Министерство образования и науки Российской Федерации  
Государственное бюджетное образовательное учреждение высшего профессионального образования  
Российский государственный педагогический университет им. А. И. Герцена.

**Сети и телекоммуникации.**

**Лабораторная работа № 3.**

Выполнила

студентка 3 курса,   
института компьютерных наук   
и технологического образования

Волкова А. И.

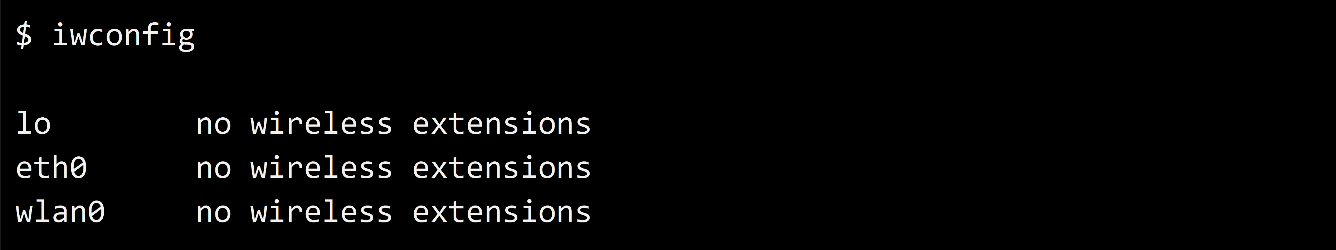
Санкт-Петербург

2017 г.

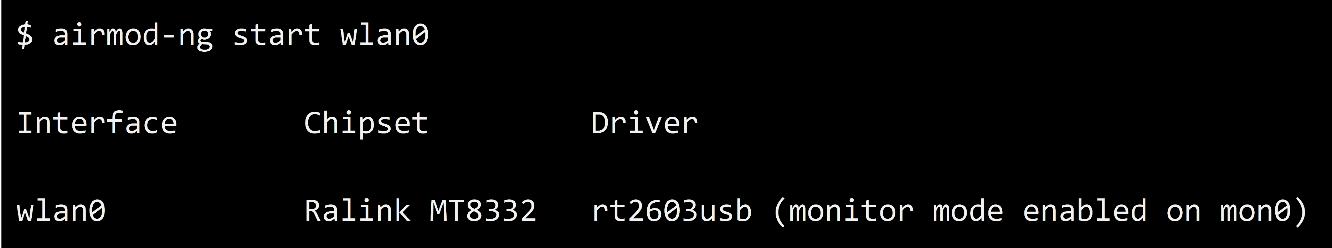
Ход работы

# WEP

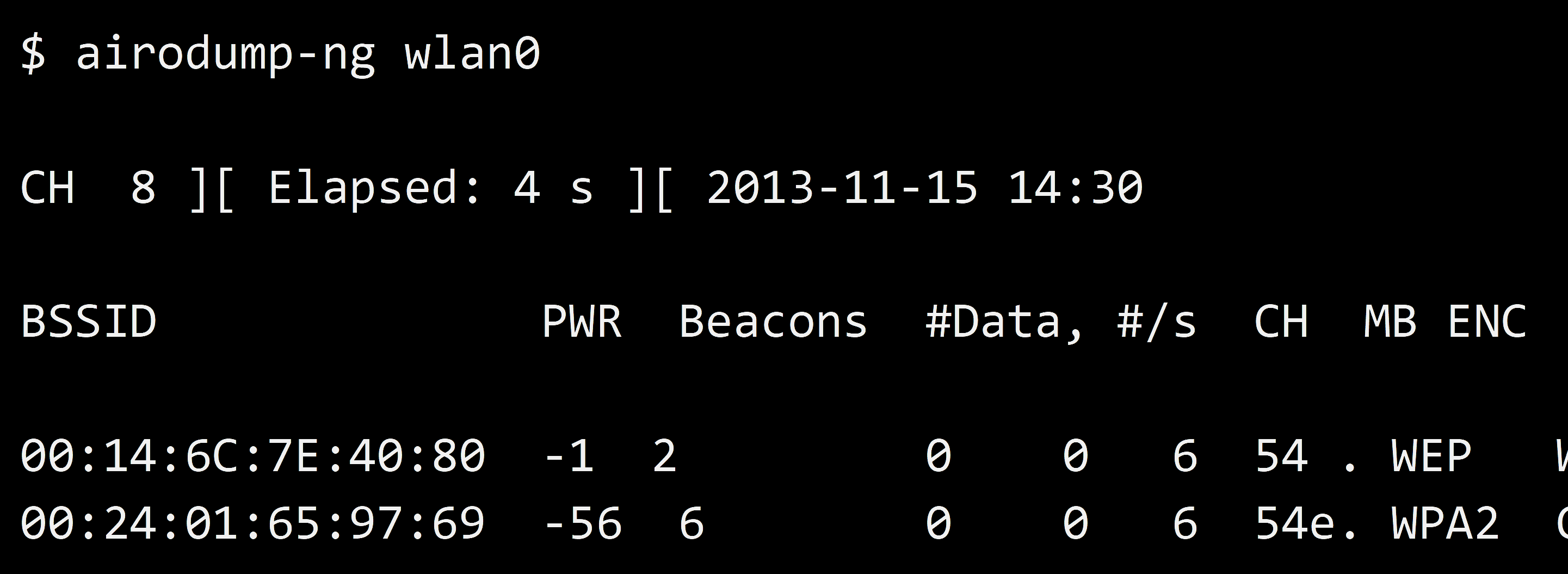
1. Узнаем имя беспроводного интерфейса с помощью iwconfig.



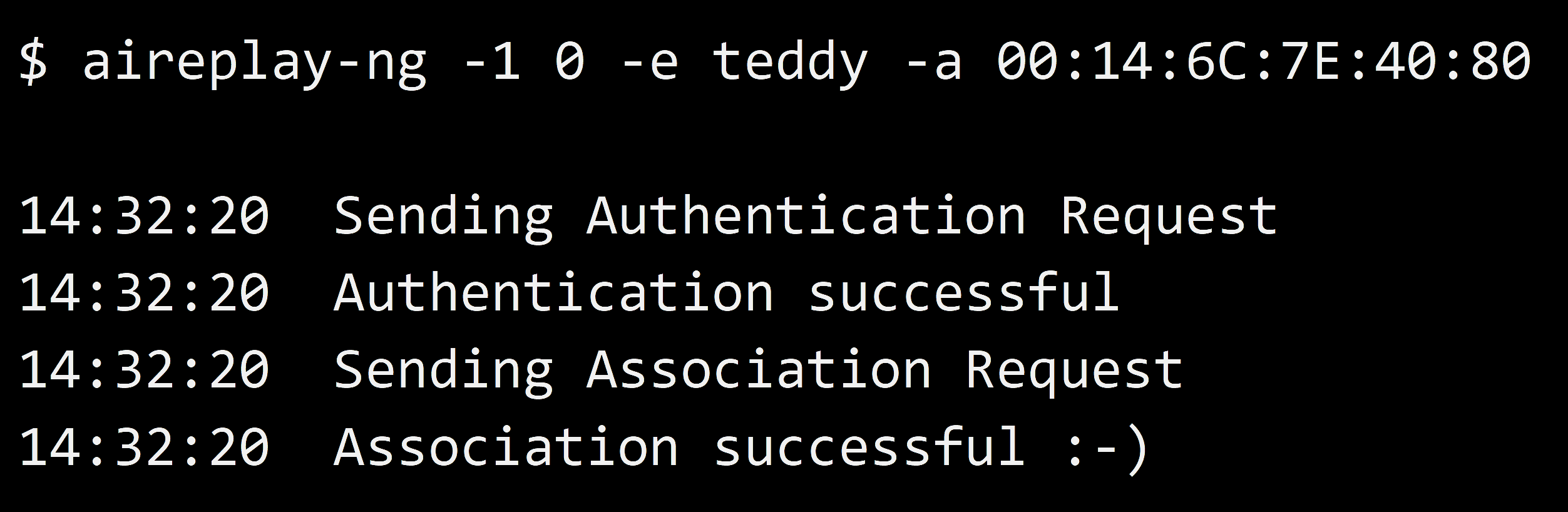
1. Запускаем интерфейс в режиме мониторинга



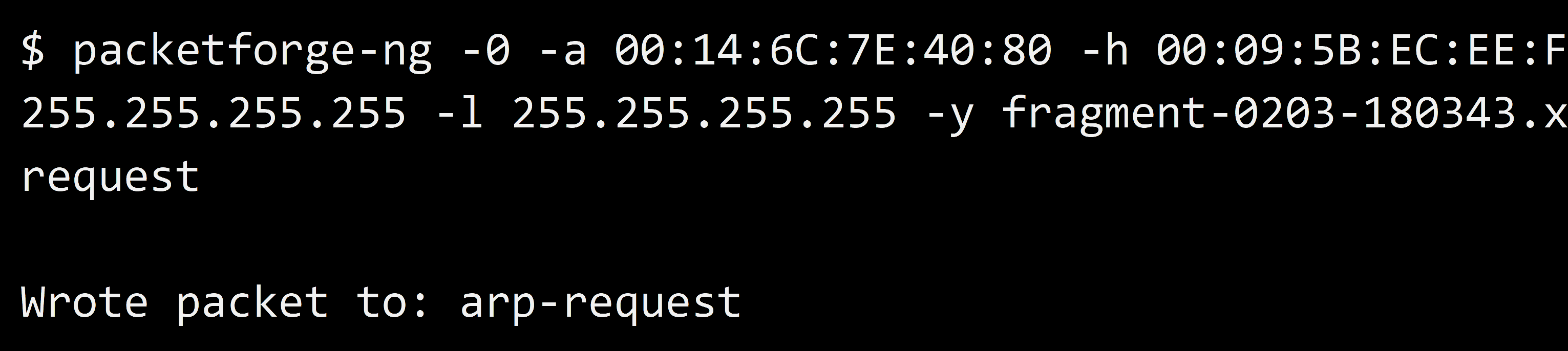
1. Выбираем сеть для атаки среди доступных.



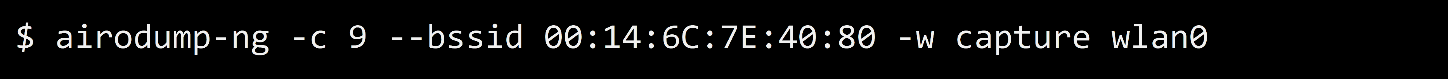
1. Используем aircrack-ng, чтобы произвести авторизацию.



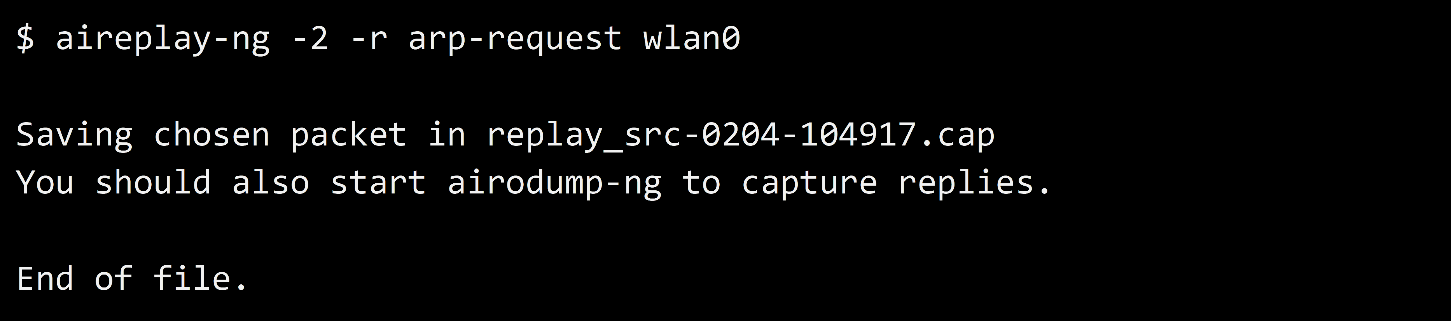
1. Получаем PRGA в новой консоли.
2. Получили. xor файл. Генерируем пакет для инъекции.



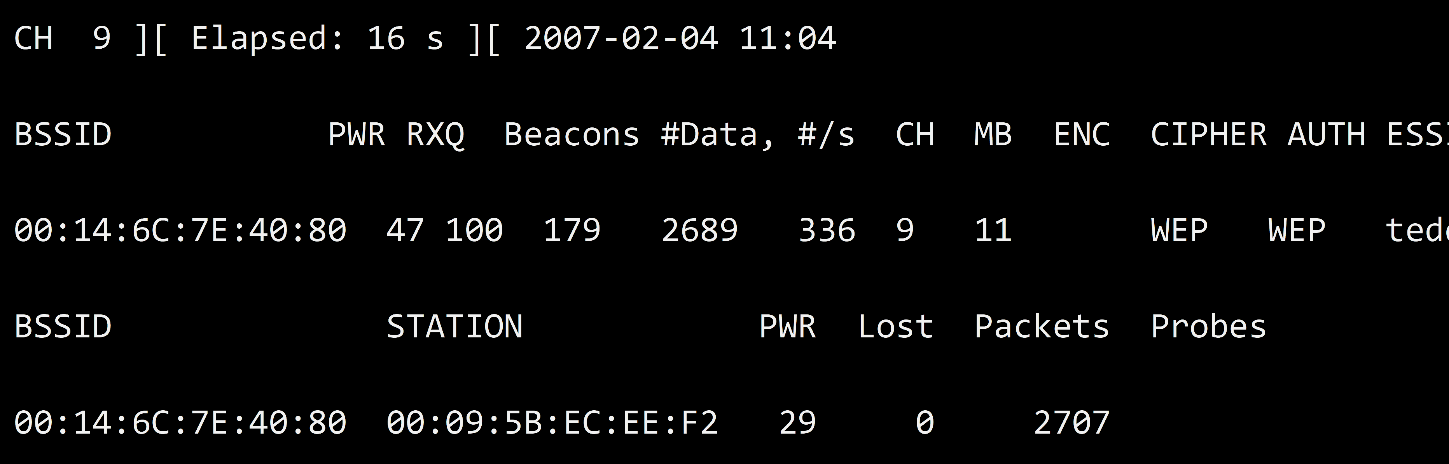
1. В новой консоли:



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



1. Вывод в третьей консоли:

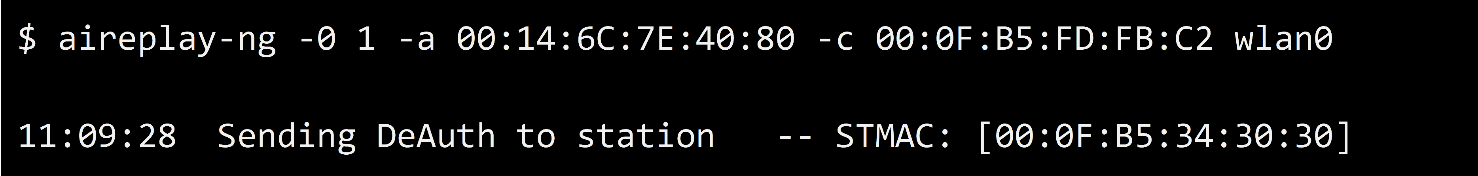


1. Запускаем aircrack-ng для получения WEP ключа

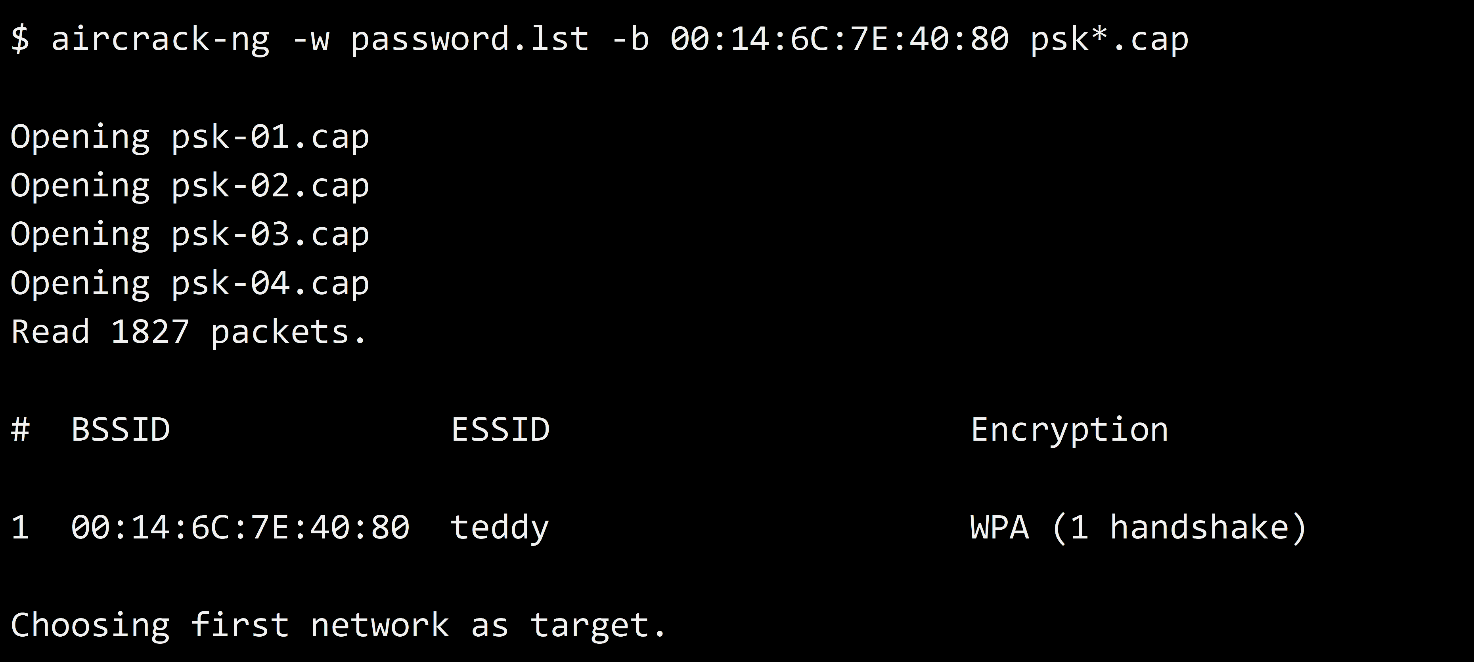


# WPA-PSK

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.