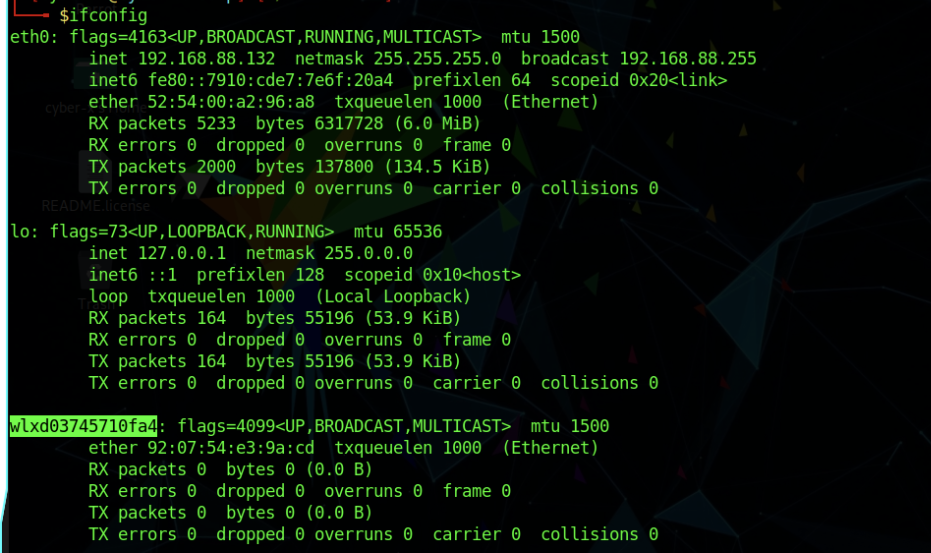
34.6. Практика. Модуль 34. Атаки на беспроводные сети

## **Задание 34.6.2**

[Course | SkillFactory](https://apps.skillfactory.ru/learning/course/course-v1:SKILLFACTORY+hack_pentest+2020/block-v1:SKILLFACTORY+hack_pentest+2020+type@sequential+block@514b59381839458d928c15566c08204d/block-v1:SKILLFACTORY+hack_pentest+2020+type@vertical+block@275c41bb31b744afa386ec7382f44562)

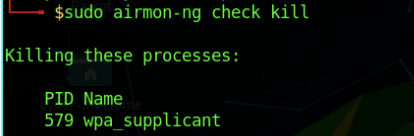
## Решение

Выясню какие сетевые устройства имеются. Первый способ, это команда “ifconfig”, а вторая “ip a”. Необходимо выяснить название Wi-Fi карты:

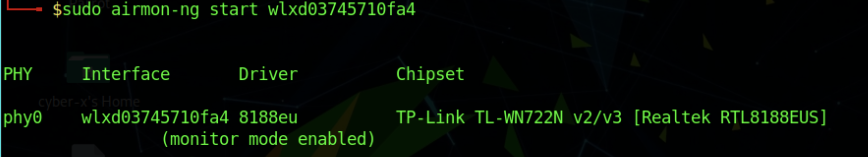


Итак, wi-fi карта - “wlxd03745710fa4”.

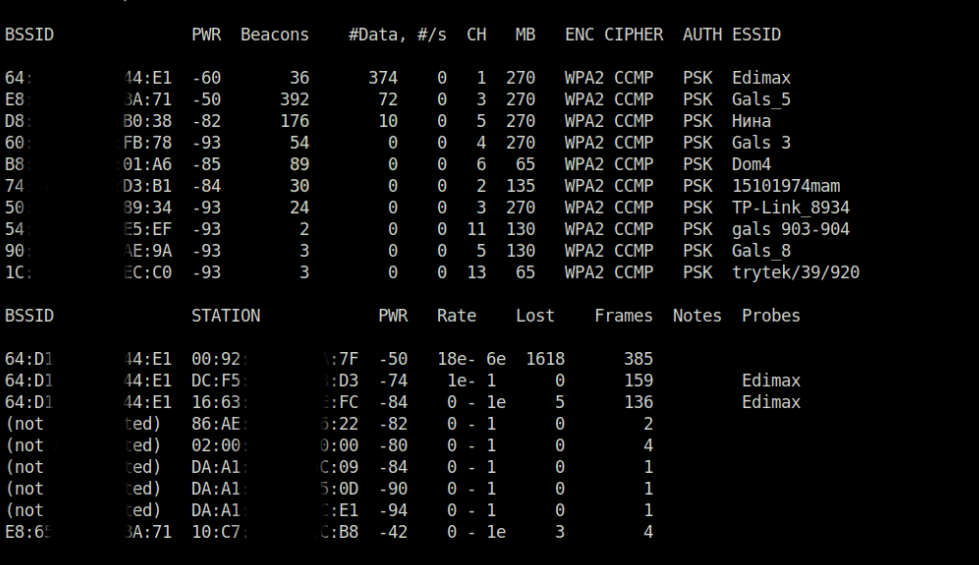
Убираем лишние процессы, которые могут аффектить нашу атаку, используя команду sudo airmon-ng check kill



Переведу Wi-Fi карту в режим монитора командой sudo airmon-ng start wlxd03745710fa4



Запускаю сканирование сетей.



MAC адрес устройства находится в столбце “BSSID”. В столбце “CH” указывается канал, в “ENC” указывается технология защиты WPA или WPA2, что и понадобится для атаки. Для атаки на выбранную Wi-Fi сеть вводим команду:

sudo airodump-ng --bssid 64:00:00:00:44:E1 --channel 1 -w ~/Documents/wifihand wlxd03745710fa4

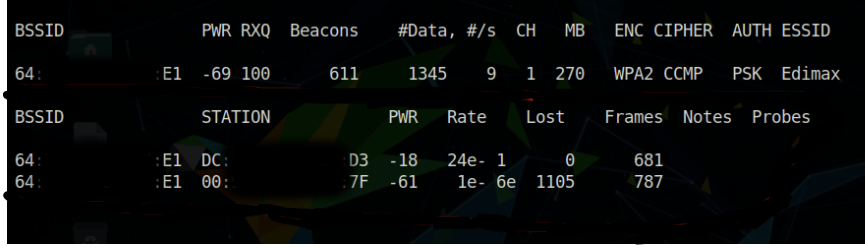
–bssid указываем MAC

–channel канал

-w указываем путь, куда будет записан хендшейк

wlxd03745710fa4 название Wi-Fi адаптера

Выбираю устройство, которое уже подключено и заставляю его переподключиться. Что ускорит процесс получения хендшейка. Узнать какие устройства подключены можно из списка, который выводится.

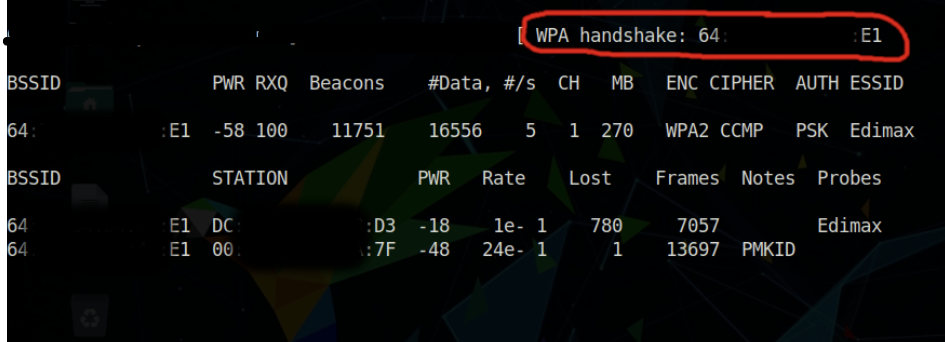


К сети подключено два устройства, для того чтобы заставить одно из них переподключиться, копируем MAC адреса из “BSSID” и “STATION”. А затем открываем новую вкладку терминала и выполняем команду:

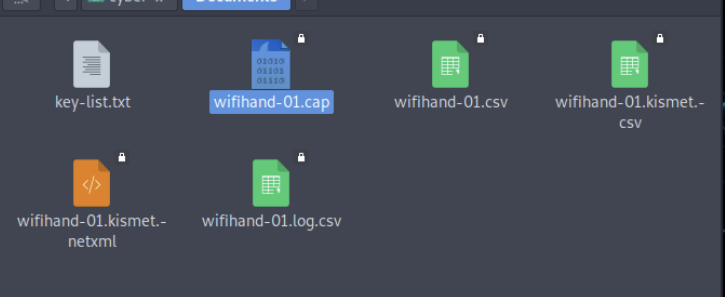
sudo aireplay-ng –deauth 20 -a 64:00:00:00:44:E1 -с 00:00:00:00:00:7F wlxd03745710fa4



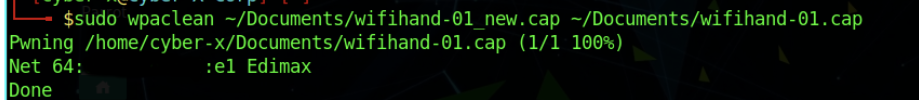
Нас интересует надпись “handshake”, которая появится при удачном переподключении устройства:



Теперь смотрим файлы в папке, которую указывали. Нам нужен всего один, в котором храниться тот самый хендшейк, данный файл будет иметь расширение “.cap”:



Почистим файл от лишнего.



Теперь расшифруем Handshake, используя словари паролей для брутфорса. В Kali Linux уже присутствует один словарь и расположен он по адресу: /usr/share/wordlists/rockyou.txt.gz.

Выполню команду “aircrack-ng -w” затем указываю путь к словарю, пишу атрибут -b и вписываю MAC адрес точки доступа, и указываю путь до очищенного хендшейка:

sudo aircrack-ng -w ~/Documents/key-list.txt -b 64:00:00:00:00:e1 ~/Documents/wifihand-01\_new.cap

В результате, получу пароль от точки доступа. Пароль будет в строке “KEY FOUND!”:

