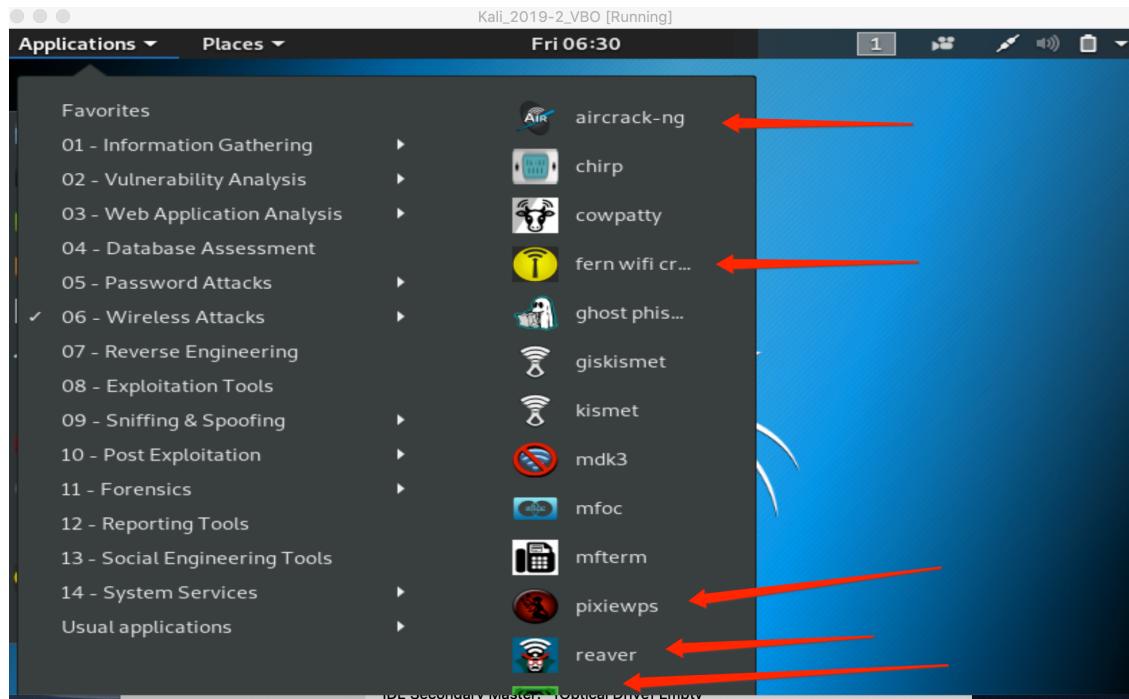


Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Изучить утилиты для работы с Wi-Fi.



Fern и wifite имеют простой интуитивный интерфейс с подсказками, а начиная исследования еще в 2010 на wps, потом перешли на wpa/wpa2 и здесь уже была развернута работа с AIRCRACK-NG, словарями, мощностями, потом появилась Alfa Awus 36, но не все режимы поддерживала.

Удобнее всего в работе оказалась связка wifite + alfa awus 51 atheros и результативностью и универсальностью. Было очень приятно работать, удавались самые разные атаки-исследования и даже по wordlist (удалось подключиться к wifi-принтеру).

Остальные утилиты более узко-специализированы, иногда срабатывал FERN - но там в основном работа со словарями. И были проблемы с хэндшейками.

Когда требовалась аккуратность в захвате хэндшейка всегда лучше всех работал стек AIRCRACK-NG.

```
wifite 2.2.5
automated wireless auditor
https://github.com/derv82/wifite2

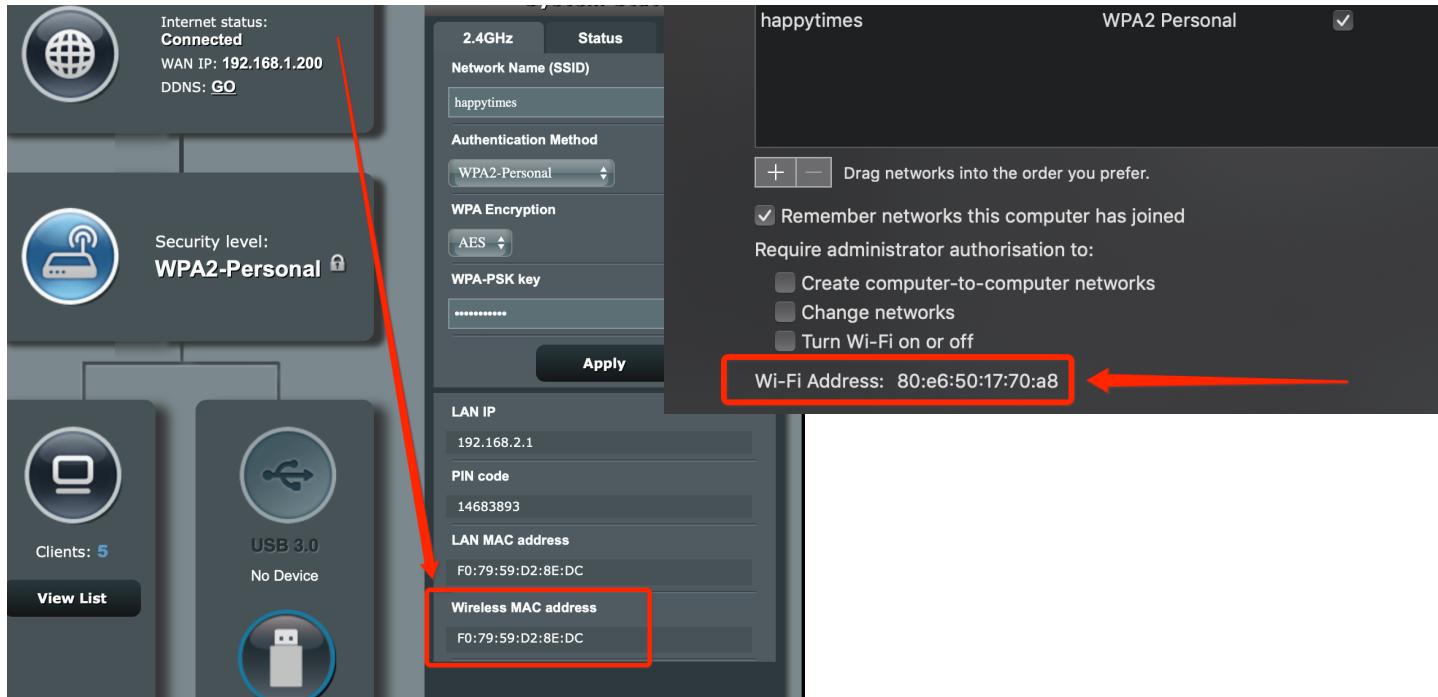
optional arguments:
  -h, --help            show this help message and exit

SETTINGS:
  -v, --verbose         Shows more options (-h -v). Prints commands and outputs. (deafult: quiet)
  -i [interface]        Wireless interface to use, e.g. wlan0mon (default: ask)
  -c [channel]          Wireless channel to scan (default: all 2Ghz channels)
  -mac, --random-mac   Randomize wireless card MAC address (default: off)
  -p [scan_time]        Pillage: Attack all targets after scan_time (seconds)
  --kill ff             Kill processes that conflict with Airmon/Airodump (default: off)
  --clients-only        Only show targets that have associated clients (default: off)
  --nodeauths           Passive mode: Never deauthenticates clients (default: deauth)
  --targets

WEP:
  --wep                Show only WEP-encrypted networks
  --require-fakeauth   Fails attacks if fake-auth fails (default: off)
  --keep-ivs            Retain .IVS files and reuse when cracking (default: off)
```

Задание 2: Снять дамп соединения утилитой Airodump-ng. Для этого создайте и подключитесь к своей тестовой незащищенной сети. Ввести логин и пароль на несколько сайтов. Найти сайт с незащищенным соединением (http), войти в аккаунт. Найти в дампе cookies от незащищенного сайта.

Фиксируем мак адрес точки доступа и вайфай-адаптера мака:



В режиме мониторинга atheros прекрасно ловит в бетонной коробке. Видно много всего и на первом месте нашу тестовую точку (скрытая) - видим на точке PSK.

```
root@kali: ~# airodump -ch 5 --bssid 80:e6:50:17:70:a8 -w /home/Downloads/test -v
[...]
BSSID          PWR  Beacons  #Data_#/s  CH  MB  ENC  CIPHER AUTH ESSID
80:79:59:D2:8E:DC -33   630    85  0   1  195  WPA2 CCMP  PSK happytimes
88:37:7A:91:FF:92 -54   1093   68  0   11  270  WPA2 CCMP  PSK happytimes
24:D3:F2:F6:09:B4 -62   630    68  0   1  138  WPA2 CCMP  PSK HappyNet127
30:5A:3A:E3:0B:8C -64   937    54  0   6  138  WPA2 CCMP  PSK happytimes2
F0:F9:59:D6:3A:3A -75   770    32  2   6  270  WPA2 CCMP  PSK SkyNet-122
D4:F9:A1:D3:8C:28 -80   675    918   0   6  138  WPA2 CCMP  PSK HUAWEI-7cb
74:9D:79:D3:EB:08 -80   514    0    0   2  138  WPA2 CCMP  PSK WiFi-EB06
64:70:02:4F:F5:5E -82   147    12   1   1  135  WPA2 CCMP  PSK SkyNet-122
C0:4A:00:84:B0:8C -84   601    281   9   9  138  WPA2 CCMP  PSK karakosbia

BSSID          STATION      PWR  Rate Lost  Frames Probe
(not associated) 14:6B:72:63:99:2B -76  0 . 1   0   26
(not associated) 90:22:FC:5A:54:70 -76  0 . 1   0   25
(not associated) 8A:DC:29:FD:66:93 -93  0 . 1   0   1
(not associated) 36:BF:9E:4A:36:81 -88  0 . 1   0   2
(not associated) EE:8C:3F:3D:53:7A -86  0 . 1   0   1
(not associated) F0:79:6A:AC:F0:88:87 -86  0 . 1   0   1
(not associated) F0:79:6A:AC:F0:88:87 -86  0 . 1   0   48
F0:79:59:D2:8E:DC F0:79:6A:AC:1C:AF -59  1e-24  0   7
E8:37:7A:91:FF:92 CC:B1:1A:2A:E2:DB -89  0 . 1   0   4
E8:37:7A:91:FF:92 64:1C:89:19:56:9A -56  0 . 1   0   8
30:5A:3A:E3:0B:8C 48:4B:AA:96:15:96 -76  11e- 1  0   576
F4:F2:6D:36:8C:3A AC:B5:7D:F1:9C:21 -59  5e- 1  0   2
D4:F9:A1:D3:8C:28 7C:93:5E:A6:83:BE -90  1e- 1  0   262
D4:F9:A1:D3:8C:28 98:DE:D8:1A:48:3F -1   1e- 0   0   262
C0:4A:00:84:B0:8C
```

Отключаем шифрование и захватим трафик идущий с нашего тестового компа, зайдем на сайт с авторизацией и без https.

```

File Edit View Terminal Tabs Help
terminal - root@kali:~home
CH 3 ][ Elapsed: 7 mins ][ 2019-08-18 10:37
BSSID          PWR Beacons #Data, /#s CH MB ENC CIPHER AUTH ESSID
F0:79:59:D2:8E:DC -33   973    166  0 11 195 0PNA happytimes
E8:37:7A:91:FF:92 -54   956    52   0 11 270 WPA2-CMP PSK LUBOM happytimes
24:D3:F2:F6:69:BC -61   630    0   0 1 130 WPA2-CMP PSK LUBOM happytimes
30:5A:EA:E3:98:0C -64   914    60   0 6 130 WPA2-CMP PSK happytimes2
F4:F2:6D:36:82:AA -54   674    674  0 6 270 WPA2-CMP PSK SkyNet-122
D4:F9:A1:D3:6C:28 -83   654    1145  0 5 130 WPA2-CMP PSK HUAWEI-7Cub
64:70:92:4F:F5:5E -81   268    27   0 1 130 WPA2-CMP PSK SkyNet-122
74:9D:79:D3:EB:08 -85   433    0   0 2 130 WPA2-CMP PSK SkyNet-122
C9:4A:60:84:8B:8C -85   654    149   0 9 130 WPA2-CMP PSK karakoboda
C8:D3:A3:4A:A2:6C -85   159    0   0 7 65 WPA2-CMP PSK DIR_136
00:1E:58:21:74:E4 -1    0    22   0 8 -1 WPA <length: 0>
BSSID          STATION PWR Rate Lost Frames Probe
(not associated) AA:27:84:4C:AE:15 -41  0 . 1 0 3
(not associated) 0A:2A:9E:E3:C9:E7 -38  0 . 1 0 6
(not associated) AE:8C:D9:88:C1:43 -39  0 . 1 0 5
(not associated) 3A:A0:4E:EC:26:FA -40  0 . 1 0 6
(not associated) E6:A6:28:AB:E6:BA -41  0 . 1 0 5
(not associated) EE:CC:61:F2:00:98 -47  0 . 1 0 1
(not associated) 7A:95:C3:00:00:98 -47  0 . 1 0 7 happytimes
(not associated) 3A:71:45:60:28:88 -51  0 . 1 0 5 happytimes
(not associated) C0:80:99:40:73:94 -54  0 . 1 0 4 happytimes
(not associated) B2:1A:7C:8A:AC:8E -54  0 . 1 0 1
(not associated) FE:89:39:8C:95:A5 -74  0 . 1 0 39
(not associated) 00:22:FC:5A:54:7E -92  0 . 1 0 4
(not associated) 84:9F:B5:0E:A7:9E

```

```

File Edit View Terminal Tabs Help
terminal - root@kali:~home
CH 12 ][ Elapsed: 42 s ][ 2019-08-18 10:45
BSSID          PWR RXQ Beacons #Data, /#s CH MB ENC CIPHER AUTH ESSID
F0:79:59:D2:8E:DC -36   0 435 47 0 11 195 OPN <length: 10>
E8:37:7A:91:FF:92 -54  100 432 29 0 11 270 WPA2-CMP PSK LUBOM
BSSID          STATION PWR Rate Lost Frames Probe
(not associated) 52:80:FE:7A:A3:66 -40  0 . 1 0 1
(not associated) A6:7A:AD:64:9E:75 -41  0 . 1 2 4
(not associated) 00:22:FC:5A:54:F7 -78  0 . 1 0 2
root@kali:/home# ls
root@kali:/home# wifidz-01.cap wifidz-01.kismet.csv wifidz-01.netxml wifidz-01.log.csv
root@kali:/home# 

```

Можно открыть файл в ваершарке, но мы знаем, что искать и поэтому просто найдем в файле наши данные:

```

danlee — -bash — 80x24
~ — -bash
lees-MBP:~ danlee$ strings /Users/danlee/Desktop/wifidz-01.cap | grep dz
dztest@mailto:ru
dztestpass
lees-MBP:~ danlee$ 

```

Задание 3: Найти хендшейк в предложенных дампах. Назвать ESSID, BSSID и канал атакованной сети, имя файла с EAPOL-пакетами

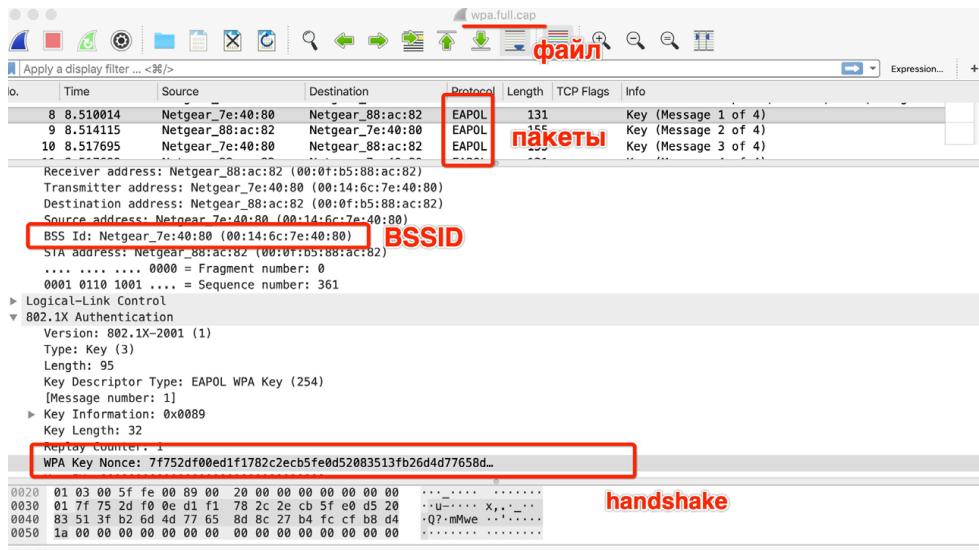
No.	Time	Source	Destination	Protocol	Length	TCP Flags	Info
434...	170.443958		Tp-LinkT_d5:c9:1e (d4:6e:0e:d5:c9:1e) (RA)	EAPOL	133		Acknowledgement, Key (Message 1 o)
434...	170.445490	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.447027	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.448563	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.450098	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.462376		SamsungE_d9:79:77 (08:ee:8b:d9:79:77) (RA)	802.11	10		Acknowledgement, Key (Message 1 o)
434...	170.463925	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.465460	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.473138	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.474675	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.477748	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.479796	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.482867	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.485427	Tp-LinkT_d5:c9:1e	Alfa_97:1d:20	EAPOL	133		Key (Message 1 o)
434...	170.488501		AsustekC_ea:47:e5 (38:2c:4a:ea:47:e5) (RA)	802.11	10		Acknowledgement, I

ESSID/BSSID
пакеты
802.11

0000 88 0a 3a 01 00 c0 ca 97 1d 20 d4 6e 0e d5 c9 1e ...:.....n...
0010 d4 6e 0e d5 c9 1e 00 00 00 aa 03 00 00 00 ..n.....
0020 88 8e 01 03 00 5f 02 00 8a 00 10 00 00 00 00?..^oU.|...
0030 00 00 01 97 3f d0 8b 5e c1 6f 55 a8 7c f5 fc ec ..?..^oU.|...

Смотрим файл номер 1:

Второй файл, отметим и хэндшейк (вероятно, мост между двумя точками поднимали):



Третий файл из двух частей, где много пакетов с деаутентификацией и как итог пойманные хэндшейки:

