Использование Zizzania

Если вас интересует подробная справка, описание инструкция по установке и дополнительные примеры по использованию zizzania, то обратитесь к соответствующей статье в Энциклопедии инструментов для пентестинга.

Установка

```
$ sudo apt-get install scons libpcap-dev uthash-dev
$ make
$ make install
```

Предположим, нас интересует точка доступа с BSSID AA:BB:CC:DD:EE:FF, но к ней очень редко (раз в сутки, раз в неделю, раз в месяц) подключаются клиенты. Мы можем запустить zizzania на сетевом интерфейсе -i wlp2s0, ограничиваем прослушивание шестым каналом -c 6 (если мы указываем канал, то программа сама переводит сетевой интерфейс в режим наблюдения), указываем интересующую нас точку доступа -b AA:BB:CC:DD:EE:FF и файл, в который нужно записать перехваченные рукопожатия -w out.pcap:

```
sudo zizzania -i wlp2s0 -c 6 -b AA:BB:CC:DD:EE:FF -w out.pcap
```

Предположим, мы хотим прослушивать определённый канал и нас интересуют все точки доступа на нём. Тогда команда буде выглядеть примерно так (мы не указали ключ **-b** с BSSID какой-либо ТД):

```
sudo zizzania -i wlp2s0 -c 1 -2 -w zizza/out5
```

Откройте два окна терминала — даже если у вас одна беспроводная карта, этот пример всё равно у вас будет работать. Нам нужны две одновременно запущенные программы, но работать они будут на одном беспроводном интерфейсе.

airodump-ng мы запускаем на интерфейсе **wlp2s0**, после ключа **-f** можно указать время в миллисекундах через которое программа будет прыгать по каналам. Если указать 30000, то каналы будут сменяться раз в 30 секунд.

Если поставить слишком маленькое значение, то программы будут не успевать сделать атаку деатуентификация и захватить рукопожатие (особенно, если на канале много точек доступа). Если поставить слишком большое значение, то это приемлемо для стационарного размещения, если же вы передвигаетесь, то вам придётся передвигаться весьма медленно, чтобы программы успели отработать по всем каналам и точкам доступа в данном диапазоне доступности.

И ещё, я хочу, чтобы рукопожатия захватывала airodump-ng (я ей как-то больше доверяю), поэтому добавляю ключ **-w**. Обратите внимание, что в своём примере я сохраняю рукопожатия в файл с префиксом auto в каталоге hndshk (его я предварительно создал). Ещё я использую опцию **--berlin 1200**. Она нужна только для того, чтобы точки доступа не вылетали слишком быстро с экрана (на работу это никак не влияет):

```
sudo airodump-ng wlp2s0 -f 30000 -w hndshk/auto5 --berlin 1200
```

При запуске zizzania я указываю тоолько имя беспроводного интерфейса, на котором она будет работать (отправлять пакеты деаутентификации):

```
sudo zizzania -i wlp2s0
```

Для анализа файла с захваченными рукопожатиями я буду использовать Pyrit:

```
pyrit -r "hndshk/auto5-01.cap" analyze
```

Для анализа файла airdecap-ng decrypt:

```
airdecap-ng -b AA:BB:CC:DD:EE:FF -e SSID -p passphrase out.pcap
```