Лабораторная работа № 6

# Компрометация беспроводной сети

### Цель работы

### Изучить технологии защиты беспроводных Wi-Fi сетей, их преимущества, недостатки и уязвимости на примере компрометации технологии WPA2.

### Задачи

* ознакомится с назначением и возможностями следующих инструментов: airmon, airodump, crunch, aircrack;
* обнаружить целевую беспроводную сеть;
* перехватить WPA-хендшейк подключения клиента к целевой сети;
* сформировать список возможных паролей в соответствии с маской пароля;
* при помощи перехваченного хендшейка и сформированного списка паролей подобрать пароль целевой беспроводной сети;
* результаты выполнения работы оформить в виде отчета.

### Оборудование

1. Ноутбук с ОС Kali Linux или другой версией Debian-based Linux и сетевой картой, поддерживающей мониторинг беспроводных сетей. Возможно также использование загрузочного образа Kali Linux и Wi-Fi-адаптера, поддерживающего мониторинг беспроводных сетей. Кроме того, допускается использование виртуальной машины.
2. Маршрутизатор с поддержкой технологии Wi-Fi.
3. Устройство-клиент Wi-Fi сети.

### Содержание работы

1. **Подготовка**

В первую очередь необходимо запустить физическую или виртуальную машину с ОС Kali Linux. При необходимости подключите к ней адаптер беспроводной сети. Проверьте корректность функционирования машины.

1. **Обнаружение и прослушивание беспроводной сети**

Откройте терминал и выполните команду *airmon-ng* для вывода сведений об интерфейсах беспроводных сетей. Таким образом узнаем имя интерфейса.

Зная имя интерфейса, выполните в терминале команду *airmon-ng start [имя интерфейса]*. Благодаря этой команде Wi-Fi-адаптер будет переведён в режим мониторинга.

Теперь выполните команду: *airodump-ng [имя интерфейса]mon*. Это позволит получить сведения о Wi-Fi-сетях, развернутых поблизости, о том, какие методы шифрования в них используются, а также узнать SSID.

Далее воспользуйтесь командой: *airodump-ng -c [канал] –bssid [bssid] -w [директория и имя файла, в который будет записан хендшейк] [имя интерфейса в режиме монитора]*. В ней [канал] надо заменить на номер целевого канала, [bssid] — на целевой BSSID, [*имя интерфейса в режиме монитора*] — на интерфейс мониторинга *[имя интерфейса]mon*.

Утилита airodump будет мониторить сеть, ожидая момента, когда кто-нибудь к ней подключится. Это даст нам возможность получить handshake-файлы, которые будут сохранены в папке /root/Desktop.

После необходимо использовать следующую команду: aireplay-ng -0 2 -a [router bssid] -c [client bssid] [*имя интерфейса в режиме монитора*]. Здесь [router bssid] нужно заменить на BSSID Wi-Fi-сети, а [client bssid] — на идентификатор рабочей станции. Эта команда позволяет получить handshake-данные в том случае, если вам не хочется ждать момента чьего-либо подключения к сети. Фактически, эта команда атакует маршрутизатор, выполняя внедрение пакетов. Параметр -0 2 можно заменить другим числом, например, указать тут число 50, или большее число, и дождаться получения handshake-данных.

1. **Генерация списка паролей**

Для генерации списка паролей необходимо воспользоваться соответствующей утилитой. В данной лабораторной работе для этого предполагается использование утилиты *crunch*.

В первую очередь необходимо узнать у преподавателя маску пароля.

Для генерации списка паролей выполните следующую команду: *crunch [минимальная длина пароля] [максимальная длина пароля] -t [маска пароля] -o [путь к файлу (расширение txt)]*. При задании маски пароля следует использовать следующие обозначения: ^ — спецсимволы; @ — буквы в нижнем регистре; , — буквы в верхнем регистре; % — цифры.

**Важно!** Список паролей может занимать значительных объем дискового пространства.

1. **Подбор пароля**

Для подбора пароля по захваченному хендшейку и сформированному списку паролей выполните следующую команду: *aircrack-ng -a2 -b [router bssid] -w [путь до списка паролей] [путь до файла, содержащего хендшейк]*. Здесь -a2 означает WPA, -b - BSSID сети, а -w - путь к списку паролей.

После выполнения этой команды начнётся процесс перебора паролей.

**Важно!** Процесс перебора паролей может занимать значительное время.

1. **Дополнительные задания**

Дополнительно можете ознакомиться с утилитой hashcat и использованием радужных таблиц для перебора паролей. Выполните перебор паролей при помощи указанной утилиты и сравните время выполнения с утилитой aircrack.

### Требования к отчету

### Отчет должен содержать скриншоты по использованию каждой утилиты и описывать всю последовательность действий, указанную в разделе “Содержание работы” текущего документа.

Также к отчету необходимо приложить файл, содержащий хендшейк.

Оформление отчета выполняется в соответствии с требованиями преподавателя.

### Материалы для подготовки

<https://www.kaspersky.ru/resource-center/definitions/wep-vs-wpa>

<https://getwifi.ru/psecurity.html>

<https://habr.com/ru/post/224955/>

<https://habr.com/ru/company/ruvds/blog/534112/>

<https://habr.com/ru/company/pentestit/blog/337718/>

<https://habr.com/ru/company/alexhost/blog/536490/>