Набор инструментов для аудита беспроводных сетей AirCrack

Абрамов Антон

1 июня 2015 г.

Содержание

1 Цель работы

Изучить возможности пакета AirCrack и принципы взлома WPA/WPA2 PSK и WEP.

2 Ход работы

Изучение

1. Изучить документацию по основным утилитам проекта - airmon-ng, airodump, aireplay, aircrack-ng.
2. Запустить режим мониторинга на беспроводном интерфейсе.
3. Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создать.

Практическое задание

Описание утилит:

- airmon-ng - Включение и отключение режима монитора беспроводных интерфейсов.
- airodump - Перехватывает кадры 802.11
- aireplay - Внедрение и повторение кадров беспроводной сети.
- aircrack-ng - 802.11 WEP и WPA/WPA2-PSK ключ программы взлома.

1. Запустить режим монитора на беспроводном интерфейсе.

   Выполним команду **airmon-ng start wlan0**.

   После этого появляется mon0, который будет осуществлять мониторинг сети, его мы и будем использовать.

   Вообще, такой сценарий может быть использован для включения режима монитора на беспроводных интерфейсах. Он также может быть использован, чтобы вернуться из режима мониторинга в управляемый режим. Ввод команды airmon-ng без параметров покажет статус интерфейсов.

   Использование:

   airmon-ng <start|stop> <interface> [channel] or airmon-ng <check|check kill>

   Где:

- <start|stop> - запустить/отключить интерфейс.
- <interface> - определяет интерфейс
- [channel] - Выбро канала
- <check|check kill> - "check покажет все процессы, мешающие Aircrack-ng. "check kill проверить и убить, мешающие процессы.

2. Запустить сбор трафика для получения аутентификационных сообщений. Запустив интерфейс в режим мониторинга посмотрим, какой трафик у нас идет в сети. Для этого используем Airodump-ng.

   airodump-ng -c 9 –bssid 00:14:6C:7E:40:80 -w psk ath0

   airodump-ng - используется для перехвата пакетов исходящих от 802.11 и особенно подходит для сбора WEP IVs для намерением использовать их с Aircrack-ng.

   Кроме того, Aircrack-ng записывает несколько файлов, содержащих информацию обо всех точках доступа и клиентах в зоне видимости.

3. Если аутентификации в сети не происходит в разный промежуток времени, произвести деаутентификацию одного из клиентов, до тех пор, пока не удасться собрать необходимых для взлома аутентификации сообщений.

   Используем **aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0**

   aireplay-ng используется для вброса кадров. Основная функция заключается в генерации трафика для последующего использования в Aircrack-ng для взлома WEP и WPA-PSK ключей. В настоящее время реализует несколько различных атак.

4. Произвести взлом используя словарь паролей.

Используем **aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap**

Цель этого шага является взлом WPA/WPA2 Pre-Shared Key. Чтобы сделать это, нужен словарь паролей. В принципе, Aircrack-ng принимает различные слова, чтобы проверить, являются ли они паролем.

2.1 Выводы

В ходе выполнения данной лабораторной работы были рассмотрен AirCrack с такими его утилитами, как: airmon-ng, airodump, aireplay и aircrack-ng.

Произведен мониторинг на беспроводном интерфейсе, отслеживающий аутентификации в сети, а также осуществлена деаутентификация одного из клиентов и перехвачен введенный им пароль. В итоге осуществлен взлом, использую словарь паролей.