Отчет по лабораторной работе №6 : Набор инструментов для аудита беспроводных сетей AirCrack

Бусаров Владислав

2015

Содержание

1 Цель работы

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

2 Ход работы

2.1 Изучить документацию по основным утилитам пакета – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng.

Aircrack-ng - набор программ, предназначенных для обнаружения беспроводных сетей, перехвата передаваемого через беспроводные сети трафика, аудита WEP и WPAWPA2-PSK ключей шифрования (проверка стойкости), в том числе пентеста (Penetration test) беспроводных сетей (подверженность атакам на оборудование и атакам на алгоритмы шифрования).

Программа работает с любыми беспроводными сетевыми адаптерами, драйвер которых поддерживает режим мониторинга (список можно найти на сайте программы). Программа работает в операционных системах Windows, UNIX, Linux и Mac OS X.

Версия для UNIX-подобных операционных систем имеет значительно бышую функциональность и поддерживает больше беспроводных адаптеров, чем Windows-версия. aircrack-ng был также портирован для платформ Zaurus и Maemo. Также программа была портирована для iPhone.

airmon-ng Выставления различных карт в режим мониторинга.

aireplay-ng Пакетный инжектор (Linux и Windows).

aircrack-ng Взламывает ключи WEP и WPA (Перебор по словарю).

2.2 Запустить режим мониторинга на беспроводном интерфейсе

airmon-ng start wlan0mon

```
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID Name
2221 NetworkManager
3392 wpa_supplicant
7009 dhclient


Interface Chipset Driver
```

```
wlan0mon Unknown  rtl8192cu - [phy0]
(monitor mode enabled on [phy0]wlan0mon)
```

2.3 Запустить утилиту airodump, изучить формат вывода этой утили-ты, форматы файлов, которые она может создавать

Запуск утилиты airodump:

airodump-ng wlan0mon

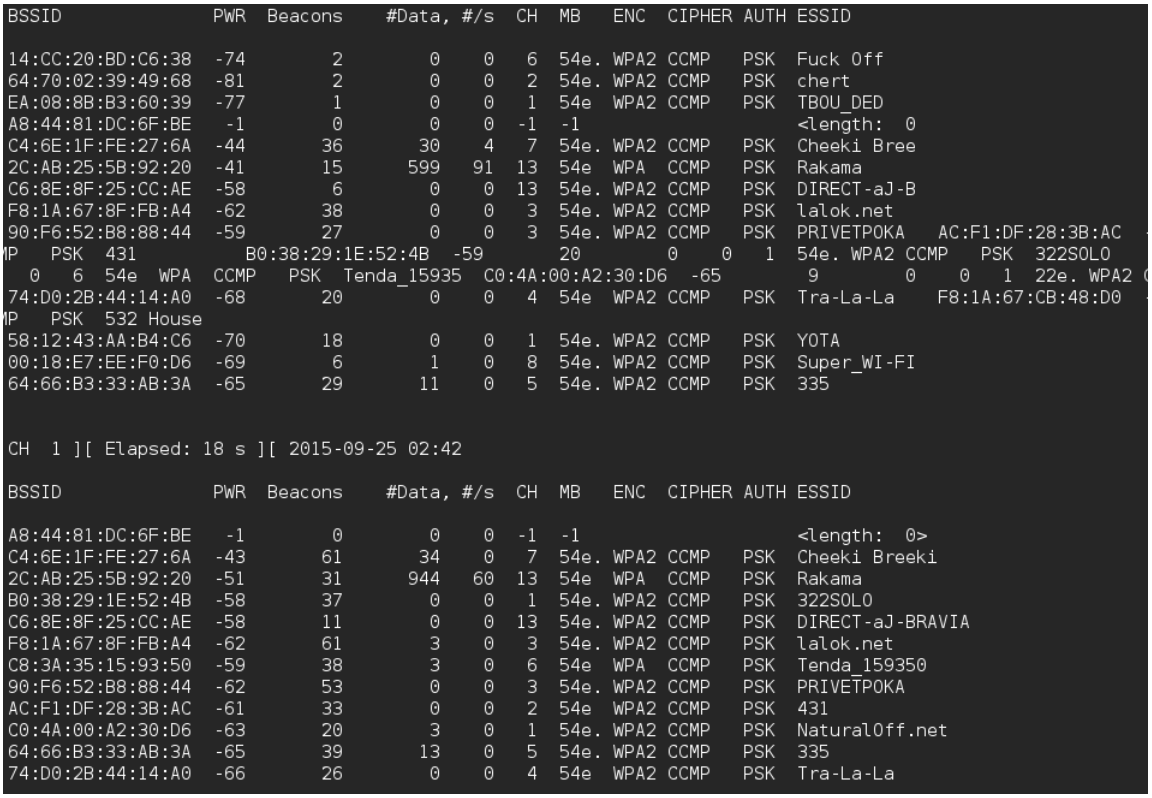

Рис. 1: Запуск airomon-ng

При указании ключа –write, утилита создает набор файлов с заданным префиксом. Два из которых связаны с информацией о доступных сетях и представлены в двух форматах: csv и xml. Еще два фала содержать информацию о перехваченных пакетах. Файл типа .cap содержит перехваченные пакеты, в то время как csv содержит лишь сокращенную информацию. Стоит отметить, что csv - это формат хранения простой таблицы.

cap - можно открыть в дальнейшем через wireshark, в нем отображаются все пакеты.

2.4 Запустить сбор трафика для получения аутентификационных сообщений

airodump-ng wlan0mon -w new1 –bssid C4:6E:1F:FE:27:6A Так же можно указать канал используя ключ: –channel

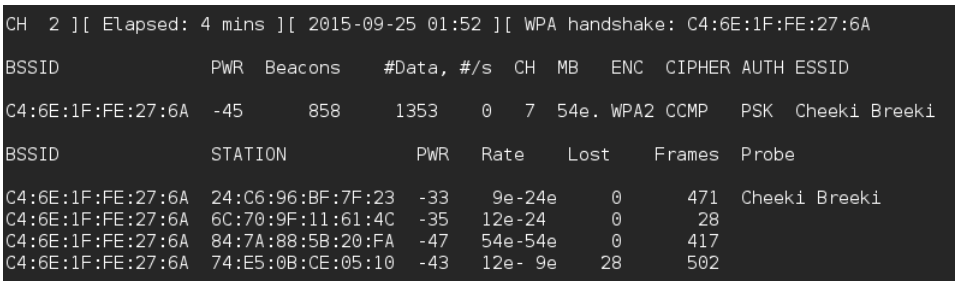

Рис. 2: Запуск airodump-ng

2.5 Произвести деаутентификацию одного из клиентов, до тех пор, пока не удастся собрать необходимых для взлома аутенти-фикационных сообщений

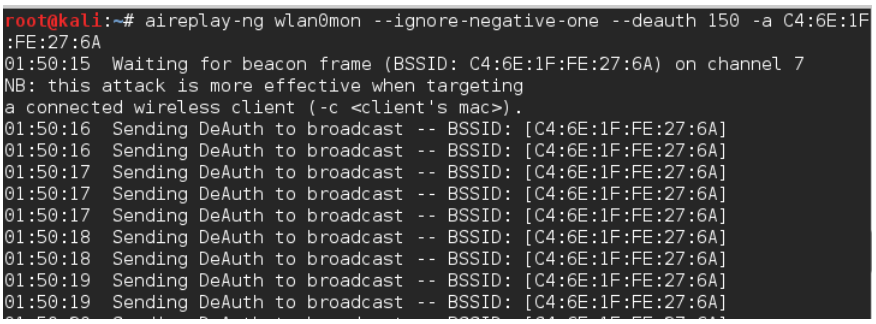

Рис. 3: DeAuth Broadcast

В результате перехватываем пакет handshake:

2.6 Произвести взлом используя словарь паролей

Так как используемый пароль слишком сложный, в некоторую часть словаря был вставлен искомый пароль. Команда: aircrack-ng -w /tmp/words.lst -b C4:6E:1F:FE:27:6A /tmp/wpa2*.cap words.lst - файл с предполагаемыми паролями. Это может быть какой-либо сборник слов или же обычный

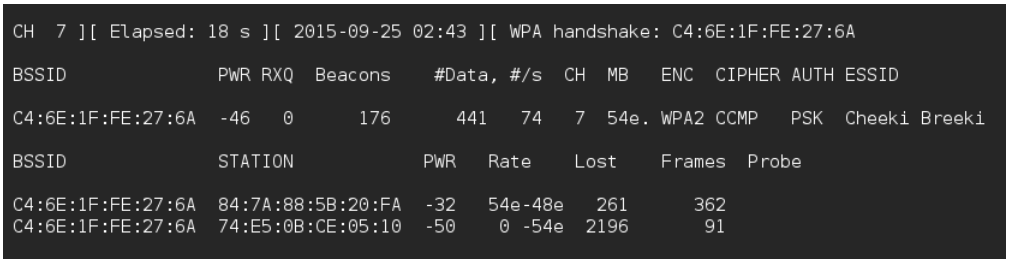

Рис. 4: airodump-ng Handshake

словарь. wpa2.cap - файл airodump-ng который мы записали когда получили Handshake.

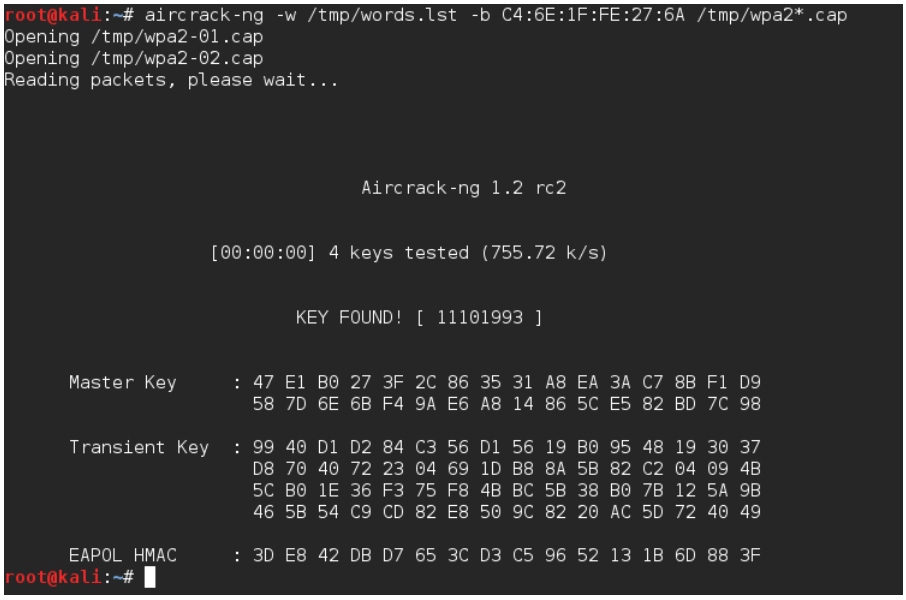

Рис. 5: Работа Aircrack-ng

3 Выводы

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

Произведен мониоринг на беспроводном инерфейсе, ослеживающий аутентификации в сети, а также осуществлена деаутентификация одного из клиентов и перехвачен введенный им пароль. В итоге осуществден взлом, посредсвом словаря паролей.