

1 Цель работы

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

2 Ход работы

2.1 Изучение

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

Кратко опишем назначение этих утилит.

1. **airmon-ng** Включает wifi адаптер в режим мониторинга. Это позволяет ему перехватывать не только пакеты предназначенные непосредственно ему, но и все доступные пакеты в сети.
2. **airodump-ng** Утилита, предназначенная для захвата сетевых пакетов протокола 802.11 для последующего их использования в последствии
3. **aireplay-ng** Утилита, которая генерирует и отправляет трафик. Может использоваться для принудительной деаутентификации пользователей.
4. **aircrack-ng** Непосредственно взламывает пароли WEP WPA используя перебор по словарю.

Запустить режим мониторинга на беспроводном интерфейсе

Запустить утилиту airodump, изучить формат вывода этой утилиты, форматы файлов, которые она может создавать.

2.2 Практическое задание

Запустить режим мониторинга на беспроводном интерфейсе.

Запустить сбор трафика для получения аутентификационных сообщений.

Если аутентификации не происходит, произвести деаутентификацию одного из клиентов.

Произвести взлом используя словарь паролей.

3 Вывод