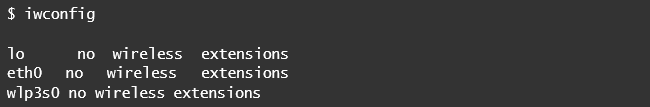
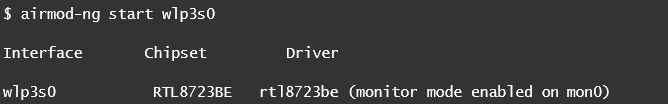
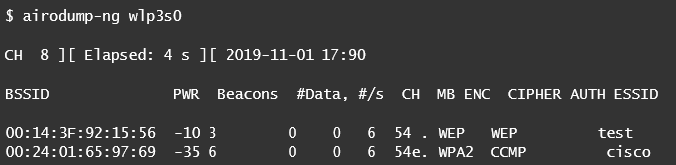
Лабораторная работа 3

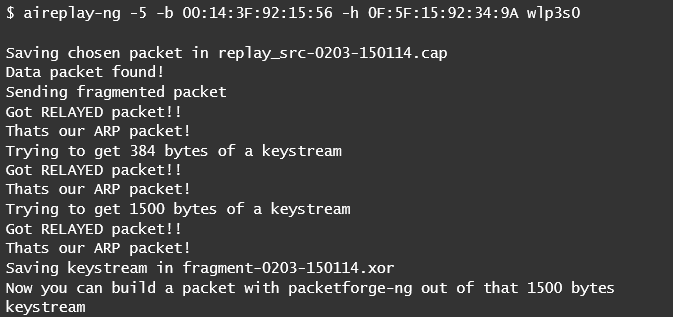
Анализ устойчивости алгоритмов шифрования WEB и WPA-TKIP

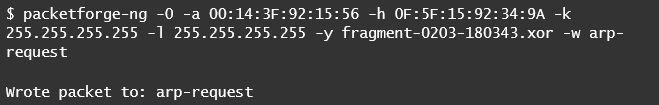
WEP



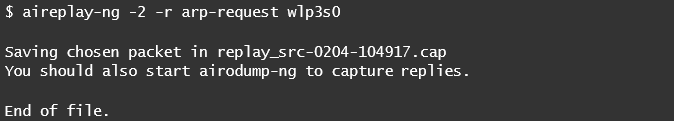


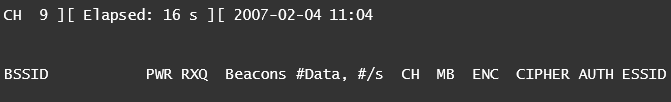


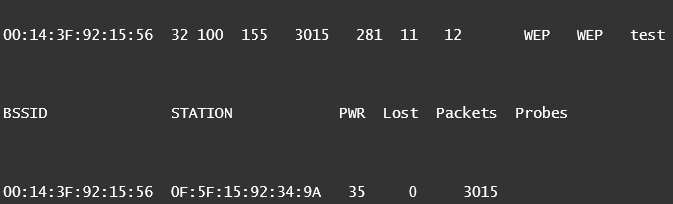






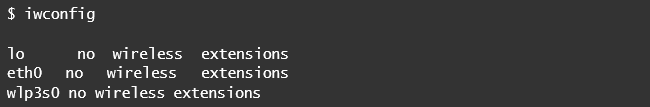


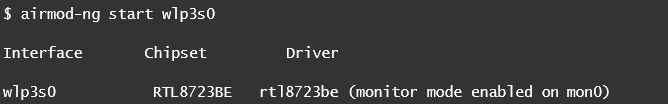


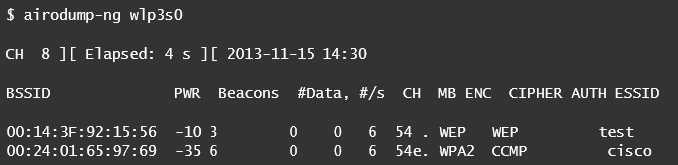


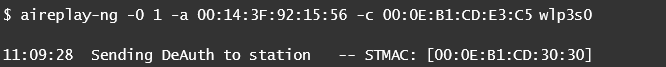


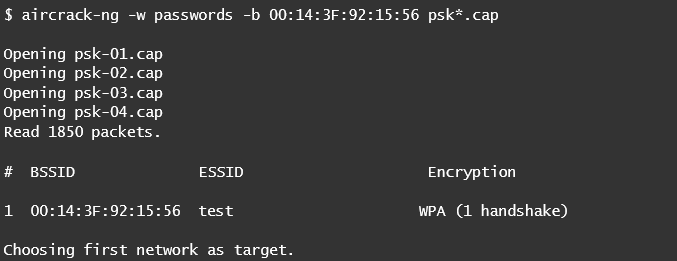
WPA-PSK

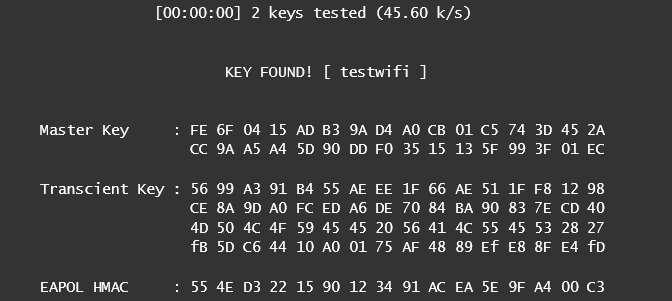












|  |  |  |
| --- | --- | --- |
| Параметры | WEP | WPA-PSK |
| Пароль | Qwert!1234!321 | Qwert!1234!321 |
| Время определения пароля(сек.) | 281 | 436 |
| Кол-во пакетов, необходимое для определения пароля | 3015 | 1850 |

1. Вопросы
2. Какой алгоритм лежит в основе шифрования WEP? Какой уровень защиты должно было обеспечить шифрование WEP? Обеспечивается ли этот уровень на данный момент?

*В основе алгоритма шифрования WEP лежит простой XOR, который не обеспечивает достаточный уровень защиты*

1. Какого размера могут быть ключи при использовании шифрования WEP? Из каких частей они состоят?

*Размер WEP ключей - 64 или 128 бит. Состоит из статической и динамической частей, но легко подбираются по анализу сетевого трафика.*

1. Какие пакеты необходимо перехватывать, чтобы иметь возможность определить ключ WEP?

*Чтобы определить ключ WEP нам нужно из радиоканала захватить векторы инициализации.*

1. В чем заключается основная уязвимость шифрования WEP?

*WEP частично передаёт ключ в простом для извлечения виде.*

1. Какое главное отличие шифрования WPA от WEP?

*В протоколе WPA для каждого подключения происходит независимое шифрование.*

1. Какой тип шифрования WPA в настоящее время уязвим для взлома?

*Уязвим WPA-PSK, протокол WPA2-PSK не подвержен этой уязвимости.*

1. Какое условие является обязательным при взломе WPA-PSK? Для чего оно необходимо?

*Для взлома необходимо чтобы был подключен как минимум один клиент к точке доступа, без этого невозможно перехватить вектор инициализации.*

1. По какому методу осуществляется подбор WPA-PSK ключа?

*При помощи словарей возможен перебор пароля.*

1. От чего самым непосредственным образом зависит успешность подбора ключа?

*На степень защищенности непосредственно влияет состав и количество символов.*

1. Может ли WPA-PSK обеспечить надежную защиту информации?

*Да, если пароль будет достаточно надежным.*