## ЛАБОРАТОРНАЯ РАБОТА № 3. АНАЛИЗ УСТОЙЧИВОСТИ АЛГОРИТМОВ ШИФРОВАНИЯ WEP И WPA-TKIP

Оформление отчета

* Напишите ответы на вопросы в соответствии с Вашим вариантом.
* Заполните таблицу.
* Напишите вывод по лабораторной работе.

Вопросы

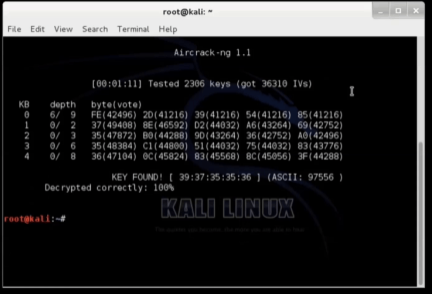
1. Какой алгоритм лежит в основе шифрования WEP? Какой уровень защиты должно было обеспечить шифрование WEP? Обеспечивается ли этот уровень на данный момент?
   * В основе WEP лежит поточный шифр RC4, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Для подсчета контрольных сумм используется CRC32. В настоящее время данная технология является устаревшей, так как её взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. Для безопасности в сетях Wi-Fi рекомендуется использовать WPA.
2. Какого размера могут быть ключи при использовании шифрования WEP? Из каких частей они состоят?
   * Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. Ключи имеют длину 40 и 104 бита для WEP-40 и WEP-104 соответственно. Используются два типа ключей: ключи по умолчанию и назначенные ключи. Назначенный ключ отвечает определенной паре отправитель-получатель. Может иметь любое, заранее оговоренное сторонами значение. Если же стороны предпочтут не использовать назначенный ключ, им выдается один из четырех ключей по умолчанию из специальной таблицы. Для каждого кадра данных создается сид (англ. Seed), представляющий собой ключ с присоединенным к нему вектором инициализации.
3. Какие пакеты необходимо перехватывать, чтобы иметь возможность определить ключ WEP?
   * В этом случае нам нужно отфильтровать только пакеты с вектором инициализации (IV-пакеты). Вектор инициализации (IV – Initialization Vector) длиной 24 бита, который добавляется к секретному ключу. WEP использует комбинацию секретного ключа и вектора инициализации в качестве ключа шифрования для алгоритма RC4.
4. В чем заключается основная уязвимость шифрования WEP?
   * Плохое проектирование WEP - основная проблема. Ключ фактически частями передает часть байт этого ключа. В алгоритме есть множество слабых мест: механизмы обмена ключами и проверки целостности данных, малая разрядность ключа и вектора инициализации (англ. Initialization vector), способ аутентификации, алгоритм шифрования.
5. Какое главное отличие шифрования WPA от WEP?
   * WPA был разработан как временная альтернатива WEP. Безопасная форма WPA использует шифрование TKIP, которое шифрует пароли для сетевой связи. Хотя это также более слабая форма безопасности, но она намного лучше, чем WEP. В отличие от WEP, WPA шифрует данные каждого клиента отдельно.
6. Какой тип шифрования WPA в настоящее время уязвим для взлома?
   * WPA-PSK. При применении режима PSK необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты, клиентские адаптеры). Если пароли совпадают с записями в базе, пользователь получит разрешение на доступ в сеть.
7. Какое условие является обязательным при взломе WPA-PSK? Для чего оно необходимо?
   * Нужно чтобы был подключен как минимум один клиент к точке доступа. Так как нам нужно перехватить “пакет-рукопожатия” для последующего перебора.
8. По какому методу осуществляется подбор WPA-PSK ключа?
   * По методу прямого перебора с использованием словарей.
9. От чего самым непосредственным образом зависит успешность подбора ключа?
   * Подбор ключа WPA-PSK будет успешным только в том случае, если он будет присутствовать в словаре по которому ведется перебор. Как правило словари содержат слова, несущие некоторую смысловую нагрузку. Правильно подобранный достаточно длинный пароль, не несущий смысловой нагрузки, содержащий символы разного регистра, цифры и специальные символы с очень большой вероятностью не будет содержаться в словарях, используемых при переборе. Прямой перебор всех возможных комбинаций в этом случае может занять десятки лет.
10. Может ли WPA-PSK обеспечить надежную защиту информации?
    * Только если правильно составить пароль.

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | WEP | | WPA-PSK | |
| Пароль | 97556 | qwert1234 | 97556 | qwert1234 |
| Время определения пароля, с | 71 | 94 | 153 | 179 |
| Количество пакетов, необходимых для определения пароля | 36310 | 45260 | 1225 | 2038 |

Примеры экранных форм

WEP



WPA-PSK



Вывод.

При использовании алгоритма WEP получить доступ к сети возможно за несколько минут, при наличии активного клиента, подключенного к данной точке доступа. Продолжительность ожидания зависит от активности в сети. Если к точке доступа никто не подключен, то время может затянуться. Расстояние до точки доступа не так важно, как активность в сети. К примеру: если клиентский компьютер загружает через взламывающую точку большой файл либо просматривает потоковое видео, то количество необходимых пакетов накопится довольно быстро (10-30 минут). Если же активного трафика нет, то необходимое число пакетов может перехватываться длительное время (целые дни).

Подбор ключа WPA-PSK будет успешным только в том случае, если он будет присутствовать в словаре по которому ведется перебор. Его можно легко найти на просторах интернета или создать свой. Но данный способ не оптимальный, т.к. если словарь на несколько тысяч комбинаций, перебор получается очень долгим и часто случается, что пароля, установленного на роутере, нет в нашем словаре. Такой способ удобен для перебора популярных комбинаций, таких как: 12345678, qwertyui и т.д. В случае сложных паролей данный способ может не иметь никакого успеха.

Анализ устойчивости беспроводных показал, что алгоритм обеспечения безопасности WEP , ровно так же, как и WPA-PSK, давно скомпрометирован и использование его для ограничения доступа просто нецелесообразно.