Исследование безопасности беспроводных точек доступа

Касимов Дмитрий Ильдусович, студент ВятГУ. Киров

Введение

Простота использования сети, высокая мобильность пользователя, дешевизна установки - всё это о беспроводных точках доступа, которые используются практически повсеместно. Как и любая технология передачи данных, Wi-Fi сети несут некоторые угрозы. Злоумышленник может воспользоваться неосторожностью использования или некорректными настройками точки доступа, а это, в свою очередь, может привести к потере персональных данных, атаке на устройства сети, или даже удаленное подключение к устройствам, например. В целях повышения качества аудита безопасности беспроводных точек доступа - рассмотрим ситуацию с ракурса потенциального злоумышленника, так будет проще понять какие меры противодействия ему наиболее эффективны.

Методы исследования

Для исследования безопасности беспроводных точек доступа необходимо:

провести анализ методов получения несанкционированного подключения к беспроводной точке доступа Wi-Fi.

Провести анализ необходимого оборудования и ПО для успешной реализации атаки. Синтезировать полученные сведения.

Реализовать программное обеспечение для перехвата пакетов аутентификации пользователя.

Результаты исследований, их обсуждение

В качестве метода получения несанкциоинрованного подключения к точке доступа (цель) изначально был взят метод с перехватом «рукопожатия» между целью и её санкционированным пользователем. Каждый раз, когда этот пользователь подключается к точке доступа, его пароль зашифровывается (наиболее распространный алгоритм шифрования WPA2) и сравнивается с уже зашифрованным паролем точки доступа (хеш). Задача злоумышленника состоит в том, чтобы узнать этот хеш и расшифровать его. Успешным результатом выполнения будет пароль для подключения к точке доступа.

Таблица 1

Требования к чипу сетевого адаптера потенциального злоумышленника:

Требование	Описание
Режим монитора	Позволяет просматривать на уровне mac-адреса устройства в любой сети в зоне досягаемости
Режим инжектриования пакетов	Переподключить устройство в сети для перехвата хендшейка

Выводы

Метод с перехватом хендшейка требует относительно большую вычислительную мощность устройства, на котором будет осуществляться подбор хеша пароля. Это, несомненно, является недостатком. Однако к достоинству данного метода следует отнести простоту реализации данного способа атаки при наличии необходимого оборудования и ПО. Защититься от данного способа атаки достаточно просто - нужно лишь усложнить пароль (не использовать личные данные, увеличить количество символов, использовать специальные символы и т. п.). Хеш пароля точки доступа при этом перехватить всё же можно, однако вероятноть успеха расшифровки такого пароля обратно пропорциональна сложности искомой кодовой комбинации.

Библиографический список

1. Джеймс Куроуз, Кит Росс. Компьютерные сети. Нисходящий подход. - 2016. - Издание 6. Москва.

2. Фленов М. Е. Ф71 Linux глазами хакера. — 6-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2021. — 416 с.: ил