

Аудит безопасности Wi-Fi сетей

С.А. Жулев, И.С. Позняк

Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия

Обоснование. Существующие Wi-Fi сети широко распространены и являются неотъемлемой частью современной информационной инфраструктуры. Однако с увеличением числа беспроводных сетей возрастает их уязвимость перед атаками и нарушениями безопасности. PMKID (Pairwise Master Key Identifier) атака является одним из распространенных методов взлома Wi-Fi сетей, и ее изучение и анализ являются важными для обеспечения безопасности данных и конфиденциальности пользователей, то есть попав в сеть злоумышленник может перехватить информацию, проходящую через роутер.

Цель — проведение аудита безопасности Wi-Fi сетей с использованием атаки PMKID. Мы стремимся изучить эффективность этой атаки и определить, насколько уязвимы различные типы Wi-Fi сетей перед такими атаками. Дополнительно мы планируем исследовать возможности защиты от PMKID атаки и предложить рекомендации по улучшению безопасности Wi-Fi сетей.

Методы.

1. Анализ существующей литературы. Мы провели обзор предыдущих исследований, связанных с PMKID атаками и аудитом безопасности Wi-Fi сетей, чтобы получить полное представление о текущем состоянии исследований в этой области.

2. Разработка экспериментальной среды. Мы создали специальную экспериментальную среду, включающую адаптер беспроводной сети и необходимое программное обеспечение.

3. Использование утилит. Для реализации атаки PMKID мы использовали утилиты hcxdumpool, pscapngtool и Hashcat. Hcxdumpool позволяет собирать PMKID из захваченных пакетов, pscapngtool использовался для конвертации захваченных данных в формат, совместимый с Hashcat. Hashcat — это мощный инструмент для восстановления паролей, который мы использовали для подбора паролей на основе PMKID.

4. Проведение атак PMKID. Мы выполнили серию атак PMKID на выбранные Wi-Fi сети, используя разработанную экспериментальную среду и утилиты.

5. Оценка уязвимости и анализ защитных механизмов. Мы оценили уязвимость каждой тестируемой Wi-Fi сети и проанализировали эффективность различных защитных механизмов против PMKID атак на основе полученных результатов.

Результаты. В результате нашего исследования мы получили:

- 1) оценку уязвимости различных типов Wi-Fi сетей перед атаками PMKID;
- 2) описание эффективности PMKID атаки в контексте аудита безопасности Wi-Fi сетей;
- 3) анализ эффективности защитных механизмов против PMKID-атак и их пригодности для обеспечения безопасности Wi-Fi сетей.

Выводы. На основе полученных результатов и проведенного анализа мы делаем выводы о необходимости улучшения безопасности Wi-Fi сетей, особенно в отношении защиты от PMKID-атак. Мы предлагаем рекомендации для организаций и пользователей по улучшению безопасности Wi-Fi сетей и защите от атак, связанных с PMKID. Также материалы исследования в дальнейшем можно использовать для проведения лабораторных работ по специальности информационная безопасность.

Ключевые слова: анализ; Wi-Fi; PMKID; сети; атаки.

Список литературы

1. [hackware.ru](https://hackware.ru/?p=18103) [Электронный ресурс]. Аудит безопасности Wi-Fi с Hashcat и hcxdumpool. Доступ по: <https://hackware.ru/?p=18103>

Сведения об авторах:

Сергей Алексеевич Жулев — студент, группа ИБТС-13, факультет кибербезопасности и управления (факультет №1); Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: serg12345290@gmail.com

Ирина Сергеевна Позняк — научный руководитель, доцент кафедры «Информационная безопасность»; Поволжский государственный университет телекоммуникаций и информатики, Самара, Россия. E-mail: i.pozdnyak@psuti.ru