Безопасность, взлом и защита Wi-Fi-сетей

Важным элементом сегодня является Wi-Fi. Именно его люди ищут в качестве точка доступа, подключается в кафе, на вокзале, у друзей, у себя, у родителей. Но при такой широкой популярности Wi-Fi является и одной их главный угроз утечки данных.

Wi-Fi (Wireless Fidelity) – это технологии, обеспечивающая беспроводную передачу данных по радиоканалам, которая используется для подключения устройств к сети Интернет и локальным сетям без использования проводов.

Wi-Fi широко применяется в повседневной жизни для обеспечения беспроводного доступа к сети на мобильных устройствах, ноутбуках, настольных компьютерах и других устройствах.

Практика атак на Wi-Fi должна проводиться исключительно в этических и легальных рамках. Для этого существуют специализированные онлайн-платформы и виртуальные лаборатории, которые предоставляют безопасную среду для обучения и практики. Вот некоторые из них:

1. Hack The Box (HTB)

Hack The Box – это популярная платформа для практики в области кибербезопасности, которая также ключает задачи, связанные с атаками на Wi-Fi. HTB предоставляет виртуальные машины и реальные сценарии для взлома, включая задачи по проникновению в беспроводные сети.

Преимущества:

- Реальные сценарии и уязвимости

- Сообщество для обмена знаниями

- Регулярное обновление новых задач и машин

Недостатки:

- Некоторые задачи могут быть слишком сложными для начинающих

2. WiFi Pineapple University

WiFi Pineapple University – это обучающая платформа, связанная с использованием устройства WiFi Pineapple от Hack5. Она предлагает различные учебные материалы и сценарии для обучения атакам на беспроводные сети.

Преимущества:

- Фокус на практических атаках и реальных сценариях.

- Интерактивные учебные материалы

- Подходит как для начинающих, так и для опытных пользователей.

Недостатки:

- Требуется наличие устройства WiFi Pineapple.

3. VulnHub

VulnHub – предоставляет виртуальные машины, которые можно использовать для практики атак на различные цели, включая беспроводные сети. Платформа предлагает множество различных сценариев и задач, связанных с кибербезопасностью.

Преимущества:

- Множество различных виртуальных машин и сценариев

- Бесплатный доступ ко всем ресурсам

- Сообщество для обмена знаниями и опытом

Недостатки:

- Требуется локальная настройка и запуск виртуальных машин.

4. Wireless Village (DefCon)

Wireless Village – это ежегодное мероприятие на конференции DefCon, посвященное беспроводной безопасности. Оно включает в себя различные соревнование и задачи, связанные с атаками на Wi-Fi-сети.

Преимущества:

- Фокус на беспроводной безопасности

- Возможность участвовать в реальных соревнованиях.

- Сообщество для обмена знаниями и опытом

Недостатки:

- Мероприятие проводится раз в год.

5. Aircrack-ng Online Labs

Aircrack-ng – это набор инструментов для тестирования безопасности Wi-Fi-сетей. Существуют онлайн-курсы и лаборатории, которые обучают использованию Aircrack-ng для атак на Wi-Fi-сетей.

Преимущества:

- Обучение работе с популярным набором инструментов

- Практические задания и сценарии

- Подходит для различных уровней подготовки

Недостатки:

- Может требоваться установка и настройка инструментов на локальной машине

6. SANS Wireless Security Training

SANS предлагает курсы и тренинги по беспроводной безопасности, которые включают в себя практические занятия и лаборатории для обучения атакам на Wi-Fi-сети.

Преимущества:

- Высокое качество обучения и материалов

- Сертификация по окончании курсов

- Практические задания и сценарии

Недостатки:

- Высокая стоимость курсов

7. WiGLE.net

WiGLE.net предоставляет информацию о беспроводных сетях по всему миру и может быть использован для анализа и исследования Wi-Fi-сетей. Хотя это не платформа для обучения атакам, она предоставляет полезные данные для исследования беспроводных сетей.

Преимущества:

- Доступ к базе данных беспроводных сетей

- Возможность исследования реальных сетей

- Сообщество для обмена знаниями

Недостатки:

- Не предоставляет учебных материалов и задач для практики.

Эти онлайн-сервисы и платформы предоставляют безопасную среду для обучения и практики атак на Wi-Fi-сети, помогая пользователям улучшить свои навыки и знания в области беспроводной безопасности.

5.1. Основы беспроводных сетей

5.1.1. Основные принципы

Для начала разберем, что такое Wi-Fi и каковы основные принципы работы Wi-Fi:

* Радиоволны и частоты: Wi-Fi работает на радиочастотах в диапазонах 2,4 ГГц и 5 ГГц. Эти частоты были выбраны из-за их способности проникать через стены и другие преграды, обеспечивая устойчивое и широкое покрытие сети.
* Модуляция сигнала: для передачи данных по радиоканалу Wi-Fi использует различные методы модуляции сигнала, такие как DSSS (Direct Sequence Spread Spectrum) and OFDM (Orthogonal Frequency Division Multiplexing), которые позволяют передавать большие объемы данных с минимальными помехами и потерями.
* Протоколы и стандарты: Wi-Fi работает по стандартам, определенным организацией IEEE (Institute of Electrical and Electronics Engineers). Наиболее распространенными стандартами являются IEEE 802.11 a/b/g/n/ac/ax, каждый из которых имеет свои характеристики, скорость передачи данных и частотные диапазоны.

5.1.2. Стандарты Wi-Fi

Рассмотрим стандарты Wi-Fi, которые определают спецификации для беспроводных локальных сетей (WLAN) и устанавливают, как устройства должны взаимодействовать в беспроводной сети. Ниже приведены основные стандарты Wi-Fi и их ключевые характеристики:

1. IEEE 802.11b:

* Скорость передачи данных: до 11 Мбит/с
* Частота: 2,4 ГГц
* Технология: DSSS
* Принят в 1999 году и был одним из первых широко распространенных стандартов Wi-Fi.

1. IEEE 802.11a:

Скорость передачи данных: до 54 Мбит/с

Частота: 5 ГГц

Технология: OFDM

Обеспечивает высокую скорость передачи данных, но имеет меньшую дальность действия по сравнению с 802.11b из-за более высокой частоты.

1. IEEE 802.11g:

Скорость передачи данных: до 54 Мбит/с

Частота: 2,4 ГГц

Технология: OFDM

Обратная совместимость с 802.11b, улучшенная производительность и дальность действия

1. IEEE 802.11n:

Скорость передачи данных: до 600 Мбит/с

Частота: 2,4 ГГц и 5 ГГц

Технология: MIMO (Multiple Input Multiple Output), использование нескольких антенн для улучшения производительности и покрытия

1. IEEE 802.11ас:

Скорость передачи данных: до 7 Мбит/с

Частота: 5 ГГц

Технология: MIMO широкие каналы (до 160 МГц), улучшенная производительность и скокрость