1. Общая информация

Название проекта: wifi-warden

Профиль: Информационная безопасность

Тип проекта: Учебный исследовательский программный продукт

Назначение:

Анализ безопасности беспроводных Wi-Fi сетей и сетевых протоколов с использованием пассивных методов.

2. Назначение и область применения

Программный сервис предназначен для:

- оценки уровня безопасности Wi-Fi сетей;
- анализа параметров сетевых соединений;
- выявления потенциальных уязвимостей конфигурации сети.

Область применения:

- учебная деятельность;
- лабораторные работы;
- демонстрация принципов сетевой безопасности.

Проект не предназначен для проведения несанкционированных атак и используется только в разрешённых сетях.

3. Функциональные возможности

Сервис реализует следующие функции:

- обнаружение доступных Wi-Fi сетей;
- анализ типа шифрования Wi-Fi;
- проверка использования защищённых соединений HTTPS и TLS;

• определение сетевого шлюза;

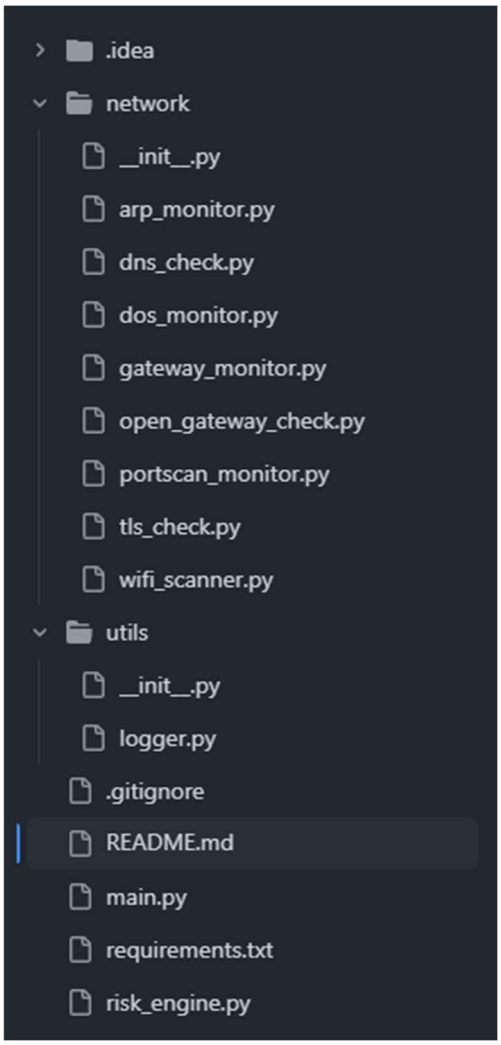
• анализ открытых сетевых портов;

• обнаружение признаков ARP spoofing;

• расчёт итоговой оценки уровня риска.

4. Архитектура системы

Проект построен по модульному принципу.



5. Описание модулей

5.1 main.py

Назначение: Точка входа в программу.

Функции:

• запуск всех модулей;

• организация логики работы;

• вывод информации пользователю.

5.2 wifi_scan.py

Назначение:

Сканирование доступных Wi-Fi сетей.

Основные функции:

• получение списка Wi-Fi сетей;

• определение уровня сигнала;

• анализ типа шифрования (WPA2/WPA3).

5.3 tls_check.py

Назначение:

Проверка защищённости соединений.

Функции:

• проверка наличия HTTPS;

• определение использования TLS;

• анализ корректности TLS-соединения.

5.4 port_scan.py

Назначение: Анализ сетевых портов и шлюзов.

Функции:

• определение сетевого шлюза;

• проверка доступных сетевых портов;

• выявление потенциально опасных открытых портов.

5.5 arp_monitor.py

Назначение: Обнаружение признаков ARP spoofing.

Функции:

• анализ ARP-трафика;

• выявление аномалий сопоставления IP–MAC;

• предупреждение пользователя о возможной атаке.

5.6 risk_assessment.py

Назначение: Оценка уровня сетевого риска.

Функции:

• анализ результатов всех модулей;

• формирование итогового рейтинга безопасности;

• вывод рекомендаций пользователю.

6. Используемые технологии

• Python 3

• Scapy

• socket

• ssl

• subprocess

• psutil

—

7. Требования к запуску

Операционная система

• Linux (Kali Linux)

• Windows

Права доступа

• Для некоторых функций требуется запуск с правами администратора/root.

—

8. Алгоритм работы системы

1. Запуск программы.
2. Сканирование Wi-Fi сетей.
3. Анализ сетевых параметров.
4. Проверка HTTPS и TLS.
5. Анализ шлюзов и портов.
6. Мониторинг ARP-трафика.
7. Расчёт уровня риска.
8. Вывод результатов пользователю.

—

9. Ограничения системы

• не выполняется расшифровка TLS-трафика;

• не используются активные методы атак;

• точность анализа зависит от конфигурации сети.

10. Безопасность и правовые аспекты

Проект разработан:

• в учебных целях;

• без нарушения законодательства;

• без вмешательства в работу сети.

Использование сервиса допускается только в сетях, на которые получено разрешение.

11. Возможности развития проекта

• добавление графического интерфейса;

• расширенный анализ DNS;

• автоматическая генерация отчётов;

• поддержка дополнительных протоколов.

12. Заключение

WiFi Security Analyzer демонстрирует практическое применение методов анализа сетевой безопасности и может использоваться как учебный инструмент для изучения Wi-Fi сетей и сетевых протоколов.

13. Источники

1. IEEE Std 802.11

2. RFC 826 — ARP

3. RFC 8446 — TLS 1.3

4. OWASP Network Security Testing Guide