**Санкт-Петербургский государственный УНИВЕРСИТЕТ**

**Факультет прикладной математики и процессов управления**

**отчет**

**по лабораторной работе №5**

**по дисциплине «системное программирование в Linux»**

**на тему «Сетевой сканер»**

|  |  |  |
| --- | --- | --- |
| Студент гр. 22Б16 |  | Шувалов Ф.В. |
| Преподаватель |  | Киямов Ж.У. |

**Санкт-Петербург**

**2023 г.**

**Оглавление**

[1. Цель 4](#_Toc152349454)

[2. Задача 4](#_Toc152349455)

[3. Теория 4](#_Toc152349456)

[4. Решение 4](#_Toc152349457)

[5. Рекомендации программиста 5](#_Toc152349459)

[6. Рекомендации пользователю 5](#_Toc152349460)

[7. Пример 5](#_Toc152349461)

[8. Вывод 6](#_Toc152349467)

[9. Список литературы 7](#_Toc152349468)

# Цель

Разработать системный инструмент, который будет использоваться для сканирования сетей

# Задачи

1. **Основные Функции:**
   1. **Сканирование Портов**: Реализовать функционал для сканирования портов на заданном диапазоне IP-адресов.
   2. **Определение Сервисов:** По результатам сканирования определять активные сервисы и службы на каждом обнаруженном узле.
   3. **Отображение Информации о Хостах:** Предоставить детализированную информацию об обнаруженных хостах, включая IP-адрес, страну, провайдера и др.
2. **Типы Сканирования:**
   1. **Полное Сканирование:** Сканирование всех возможных портов на всех обнаруженных узлах.
   2. **Сканирование Определенных Портов:** Пользователь может выбрать определенные порты для сканирования.
   3. **Сканирование Определенных IP-адресов:** Возможность указать конкретные IP-адреса для сканирования.
3. **Графический Интерфейс:**
   1. Разработать графический интерфейс для удобного взаимодействия с приложением.
   2. Предоставить интуитивно понятный и информативный вывод результатов.
4. **Сохранение Результатов:** Предусмотреть возможность сохранения результатов сканирования в файл для последующего анализа.
5. **Ожидаемый Вывод:**
   1. Исходный код проекта в репозитории.
   2. Собранное и готовое к использованию приложение.
   3. ●Документация по использованию и установке.

# Теория

Сетевая безопасность является критически важным аспектом в обеспечении надежности информационных систем. Одним из методов обеспечения безопасности сети является регулярное сканирование портов на удаленных узлах. Порт-сканнеры позволяют выявлять открытые порты, что является ключевым аспектом для предотвращения возможных атак и обеспечения целостности сетевой инфраструктуры.

Порт-сканирование представляет собой процесс определения состояния портов на удаленных узлах сети. В зависимости от результата сканирования можно определить, какие порты открыты, закрыты или фильтруются. Открытые порты могут быть потенциальной уязвимостью, а знание их состояния является важным шагом в обеспечении безопасности.

# Решение

*Таблица 4.1 Классы*

|  |  |
| --- | --- |
| Классы | Назначение |
| MainWindow | Интерфейс программы |
| Host Info | Словарь для информации о IP адресе |

*Таблица 4.2 Таблица Функций*

|  |  |
| --- | --- |
| Имя | Описание |
| main | Основная функция, запускается при вызове программы из консоли |
| Scan\_port | Функция для непосредственного сканирования порта |
| Scan\_host | Функция для непосредственного сканирования IP |
| Setup\_ui | Функция для настройки интерфейса |
| Scan\_ip | Функция для считывания введенной информации и сканирования IP |
| Scan\_ports | Функция для считывания введенной информации и для сканирования портов |
| Save\_results | Функция, сохраняет результаты |
| Display\_results | Функция, которая выводит результаты на экран |

# Рекомендации программисту

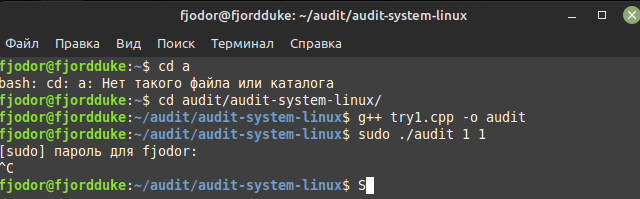
Для запуска программы необходима 64-битная операционная система Linux и python версии не ниже 3.10. Для корректной работы программы требуются библиотеки, указанные в README.md файла github .

# Рекомендации пользователю

Выполните действия, указанные на github (<https://github.com/zer0rbt/Linux/course2/scanner>). Для запуска Вам нужно иметь права superuser’a - иначе не гарантируется корректная работа программы. При наличии ошибок проверьте консоль. При невозможности устранения ошибок самостоятельно рекомендуется переустановить программу и написать разработчику.

# Контрольный Пример

Запустив программу, пользователь увидит окно. В нем можно ввести IP адрес и диапазон портов для сканирования. Для начала сканирования и сохранения результатов следует нажать на соответствующие кнопки.



*Рисунок 7.1 Основное окно программы*

# Вывод

Разработанный порт-сканнер представляет собой эффективный инструмент для администраторов сети и специалистов по безопасности для обнаружения потенциальных уязвимостей в сетевой инфраструктуре. Программа обладает простым, но мощным интерфейсом, что делает ее доступной широкому кругу пользователей.

# Список литературы

<https://github.com/zer0rbt/Linux/course2/scanner>