**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**Факультет прикладной математики – процессов управления**

**отчет**

**по лабораторной работе**

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

**на тему «Разработка Сетевого Сканера»**

|  |  |  |
| --- | --- | --- |
| Студент гр. 22.Б15 |  | Добренкова Л.С. |
| Преподаватель |  | Киямов Ж.У. |

**Санкт-Петербург**

**2023 г.**

Содержание

[1. Цель работы 2](#__RefHeading___Toc836_2594690726)

[2. Задача 2](#__RefHeading___Toc838_2594690726)

[3. Теоретическая часть 2](#__RefHeading___Toc840_2594690726)

[4. Описание программы 3](#__RefHeading___Toc842_2594690726)

[5. Рекомендации пользователю 5](#__RefHeading___Toc844_2594690726)

[6. Рекомендации программисту 5](#__RefHeading___Toc846_2594690726)

[7. Контрольный пример 5](#__RefHeading___Toc848_2594690726)

[8. Заключение 7](#__RefHeading___Toc850_2594690726)

[9. Литература 7](#__RefHeading___Toc852_2594690726)

# **Цель работы**

Создать инструмент для сканирования и анализа сетевой активности.

# **Задача**

#### **Проектирование:**

* + Разработка алгоритма сбора данных о хостах.
  + Выбор структуры данных для хранения настроек и параметров.

#### **Работа с scapy:**

* + Изучение основ работы с scapy.
  + Интеграция scapy в проект.
  + Реализация механизма обработки ошибок.

#### **Работа со сторонним api для получения информации об ip:**

* + Исследование сервисов с данными.
  + Интеграция в проект.

#### **Форматированный вывод и графический интерфейс:**

* + Разработка метода форматирования для интуитивно понятного вывода.
  + Переформатирование в случае приминения фильтров.
  + Сбор статистики результатов сканирования.
  + Создать интуитивно понятный графический интерфейс.

# **Теоретическая часть**

#### **Сетевой сканер:**

Сетевой сканер – это инструмент, предназначенный для исследования и анализа сетевой активности, обеспечивая пользователю информацию о состоянии сетевых узлов, их открытых портах, используемых сервисах и других характеристиках.

#### **Scapy:**

Scapy - это мощный инструмент для работы с пакетами в сети на языке Python. Он позволяет создавать, отправлять, перехватывать и анализировать сетевые пакеты.

#### **Информация о хосте:**

На хосте могут быть открыты порты. К каждому порту привязана служба/сервис. В общем случае сервис может прослушивать любой порт, но для некоторых стандартных сервисов выделены специальные порты (1-1024).

Так же можно узнать местоположение хоста по ip адресу.

# **Описание программы**

Описание основных компонентов программы *«scanner.py»* представлено в таблице 4.1, *«main.py»* представлено в таблице 4.2.

*Таблица 4.1. Описание переменных программы «scanner.py»*

|  |  |  |
| --- | --- | --- |
| Имя | Параметры | Описание |
| format\_ip\_result | results: list – результаты сканирования | Форматирует результаты сканирования для вывода. |
| parse\_ints | ips: str - строка, содержащая диапозоны  expand: function - функция для раскрытия диапазонов | Парсит строку с диапазонами |
| expand\_port\_range | port\_range: str — диапазон портов | Раскрывает диапазон портов |
| expand\_ip\_range | ip\_range: str — диапазон ip адресов | Раскрывает диапазон ip |
| get\_ip\_info | ip: str — ip адрес | Собирает данные о геолокации хоста |
| get\_mac | ip: str — ip адрес | Собирает данные о mac адресе, если они доступны |
| get\_services | ip: str — ip адрес  ports: set — набор портов для сканирования | Получает открытые порты и соответствующие службы |

*Таблица 4.2. Описание переменных программы «main.py»*

|  |  |  |
| --- | --- | --- |
| Имя | Параметры | Описание |
| scan\_and\_insert | ips: set – набор ip адресов  ports: set – набор портов | Сканирует сеть и вставляет результат в текстовое поле |
| show\_popup | text: str – текст всплывающего окна | Отображает всплывающее окно с информацией |
| scan\_button\_clicked | - | Обработчик события нажатия кнопки "Scan". Запускает отдельный тред для сканирования |
| toggle\_filter | - | Включает или отключает фильтр по стране и обновляет результаты |
| save\_button\_clicked | - | Сохраняет вывод в указанный файл |

# **Рекомендации пользователю**

https://github.com/v131v/linux\_labs\_3\_sem/blob/main/lab4/README.md

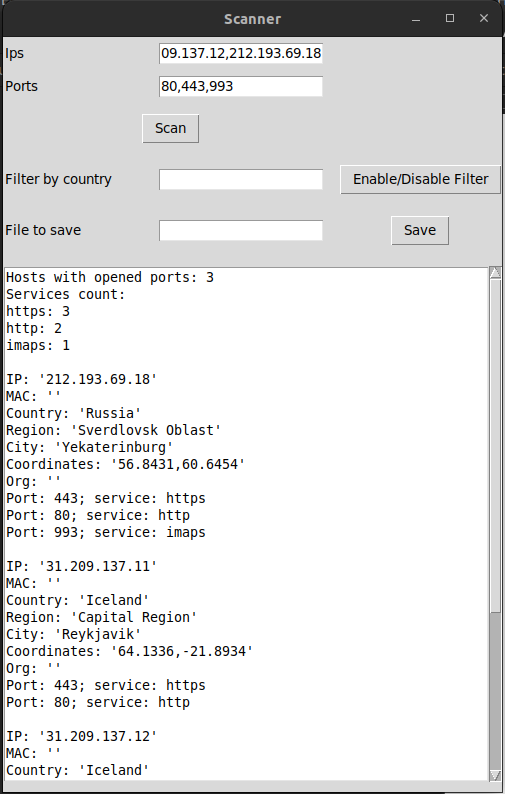
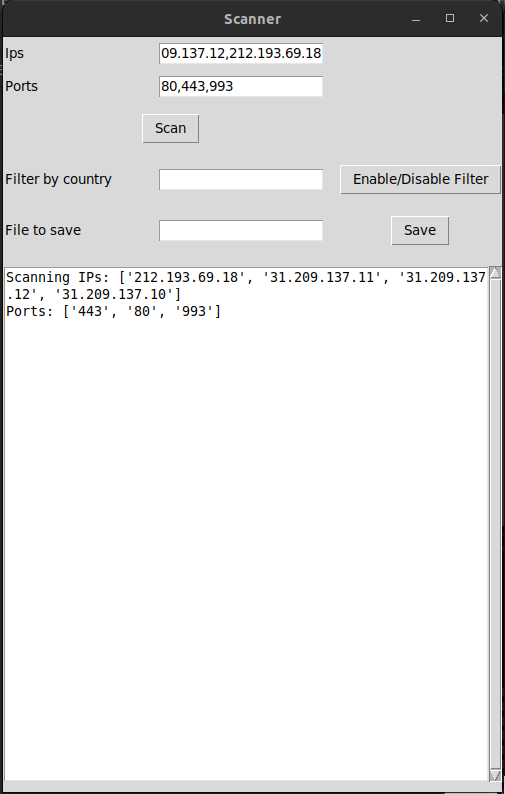
# **Рекомендации программисту**

* Python версии 3.12 или выше
* Подключение к сети
* Права администратора на сеть (sudo в linux)

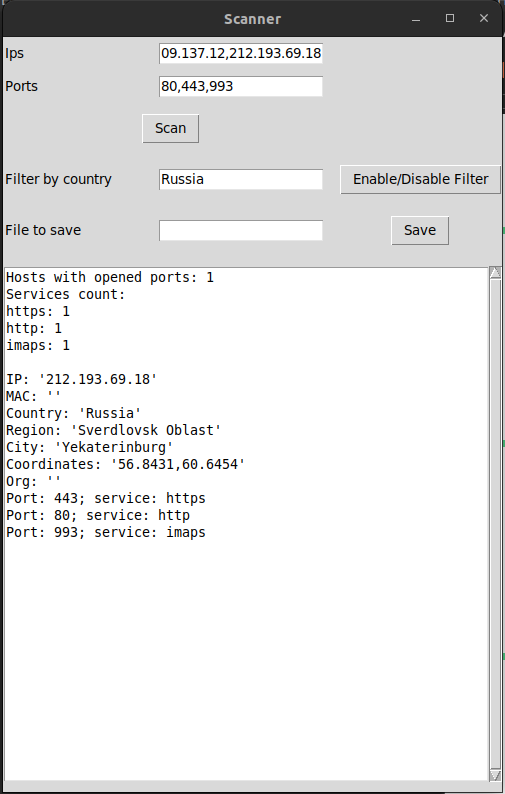
# **Контрольный пример**

В данном разделе представлены контрольный пример, демонстрирующий способность выполнять работу.

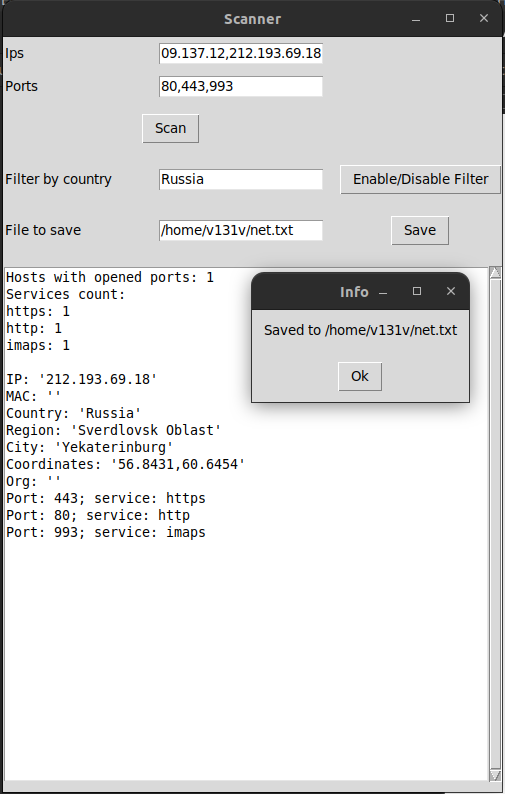
*Рисунок 7.1. «Scan»*

**

*Рисунок 7.2. «Filter»*

**

*Рисунок 7.3. «Save»*

**

# **Заключение**

В результате выполнения лабораторной работы был разработано полноценное приложение с интуитивно понятным интерфейсом для сканирования сети как по отдельным ip адресам и портам, так и по диапазонам.

Код доступен по ссылке:

[https://github.com/v131v/linux\_labs\_3\_sem/tree/main/lab](https://github.com/v131v/linux_labs_3_sem/tree/main/lab2)4

# **9. Литература**

* https://scapy.readthedocs.io/en/latest/introduction.html
* [https://ru.wikipedia.org/wiki/Список\_портов\_TCP\_и\_UDP](https://github.com/jtilly/inih/blob/master/INIReader.h)