МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ

ОТЧЕТ

по лабораторной работе
по дисциплине «Системное программирование в Linux»
на тему «Разработка Сетевого Сканера»

Студент гр. 22.Б15-пу _____ Осовский Н.С

Преподаватель _____ Киямов Ж.У.

Санкт-Петербург
2023 г.

Оглавление

1. Цель работы

Создать инструмент для сканирования и анализа сетевой активности

2. Задача

Реализовать функционал для сканирования портов на заданном диапазоне IP-адресов.

По результатам сканирования определять активные сервисы и службы на каждом обнаруженном узле.

Предоставить детализированную информацию об обнаруженных хостах, включая IP-адрес, MAC-адрес, страну, провайдера и др.

Разработать графический интерфейс для удобного взаимодействия с приложением.

Предоставить интуитивно понятный и информативный вывод результатов.

3. Теоретическая часть

- IP (интернет-протокол) - это основной протокол сети Интернет, используемый для маршрутизации пакетов данных между узлами сети. Каждый узел в IP-сети идентифицируется уникальным IP-адресом, который состоит из 32 бит или 128 бит (IPv6). IP-адрес используется для маршрутизации пакетов данных по сети.

- Порт в компьютерных сетях представляет собой числовой адрес, который используется для идентификации конкретного процесса или службы в сети. TCP и UDP используют порты для организации коммуникации между устройствами.

- Сетевой сканер - это инструмент, который может использоваться для анализа сети, обнаружения устройств, открытых портов и служб, а также для выполнения различных видов анализа безопасности сети.

- Scapy - это мощная библиотека Python, которая позволяет программистам создавать, отправлять, перехватывать и анализировать сетевые пакеты. Метод sr1 в библиотеке Scapy используется для отправки сетевых запросов (например, ICMP, ARP, DNS) и получения одиночного ответа. Это удобный инструмент для отправки кастомизированных сетевых пакетов и анализа ответов.

- ARP - это протокол канального уровня, используемый для отображения IP-адресов в физические MAC-адреса в локальных сетях. ARP запрос используется для определения MAC-адреса устройства по его IP-адресу в локальной сети.

- Библиотека Requests в Python - это простой в использовании инструмент для выполнения HTTP-запросов. Она предоставляет удобный интерфейс для отправки запросов на серверы, обработки ответов и управления сеансами.

4. Описание программы

Данная программа представляет инструмент для сканирования портов на заданном диапазоне IP-адресов, анализа обнаруженных сервисов на каждом узле сети и предоставления детализированной информации об обнаруженных хостах. Она также включает функции для определения доступности сервера, извлечения MAC-адреса устройства и получения информации о хосте с использованием внешнего API.

4.1. Описание функций

В программе используются 8 функций

Таблица 5.1. Описание функций

Имя функции	Описание функции
port_scan	- Описание: Эта функция предназначена для сканирования указанных IP-адресов и портов с использованием пакетов TCP. Результаты сканирования возвращаются в виде словаря, содержащего информацию о статусе каждого сканируемого порта (открыт, закрыт, отфильтрован). - Параметры: - `target` - список IP-адресов, которые необходимо отсканировать. - `ports` - (необязательный) список портов, которые следует отсканировать. По умолчанию используются порты из словаря `services`. - Возвращаемое значение: словарь, содержащий результаты сканирования для каждого IP-адреса и порта.
is_server_available	- Описание: Эта функция используется для определения доступности сервера по заданному IP-адресу путем отправки пакета ICMP. - Параметры:

	- `ip` - IP-адрес сервера. - Возвращаемое значение: логическое значение, указывающее, доступен ли сервер.
detect_services	- Описание: Эта функция предназначена для анализа результатов сканирования портов и определения служб, работающих на открытых портах. - Параметры: - `port_results` - результаты сканирования портов. - Возвращаемое значение: словарь, содержащий информацию о службах, обнаруженных на открытых портах.
get_mac_address	- Описание: Эта функция используется для получения MAC-адреса устройства по его IP-адресу с помощью протокола ARP. - Параметры: - `ip_address` - IP-адрес устройства. - Возвращаемое значение: MAC-адрес устройства.
get_host_information	- Описание: Эта функция получает информацию о хосте (IP-адрес, провайдер услуг, страна, регион, город и MAC-адрес) с использованием запроса к внешнему API. - Параметры: - `ip_address` - IP-адрес хоста. - Возвращаемое значение: словарь, содержащий информацию о хосте.
get_info	- Описание: Эта функция создает отчет о доступности серверов, информации о хостах и обнаруженных службах, сохраняя его в файл при необходимости. - Параметры: - `ips` - список IP-адресов для сканирования. - `ports` - список сканируемых портов. - `is_save` - (необязательный) логическое значение, указывающее, нужно ли сохранить результат в файл (по умолчанию True). - `filename` - (необязательный) имя файла для сохранения результата (по умолчанию "info.log"). - Возвращаемое значение: строка, содержащая сгенерированный отчет.
interface_get_ips	- Описание: Эта функция используется для извлечения списка IP-адресов из входной строки, которая может включать диапазоны адресов. Например, 192.168.0.*[10-20],192.168.1.1. - Параметры: - `in_ips` - строка, содержащая IP-адреса или диапазоны адресов.

	- Возвращаемое значение: список IP-адресов.
interface_get_ports	- Описание: Эта функция используется для извлечения списка портов из входной строки, разделенной запятыми. - Параметры: - `in_ports` - строка, содержащая порты, разделенные запятыми (например, "80, 443"). - Возвращаемое значение: список портов.

5. Контрольный пример

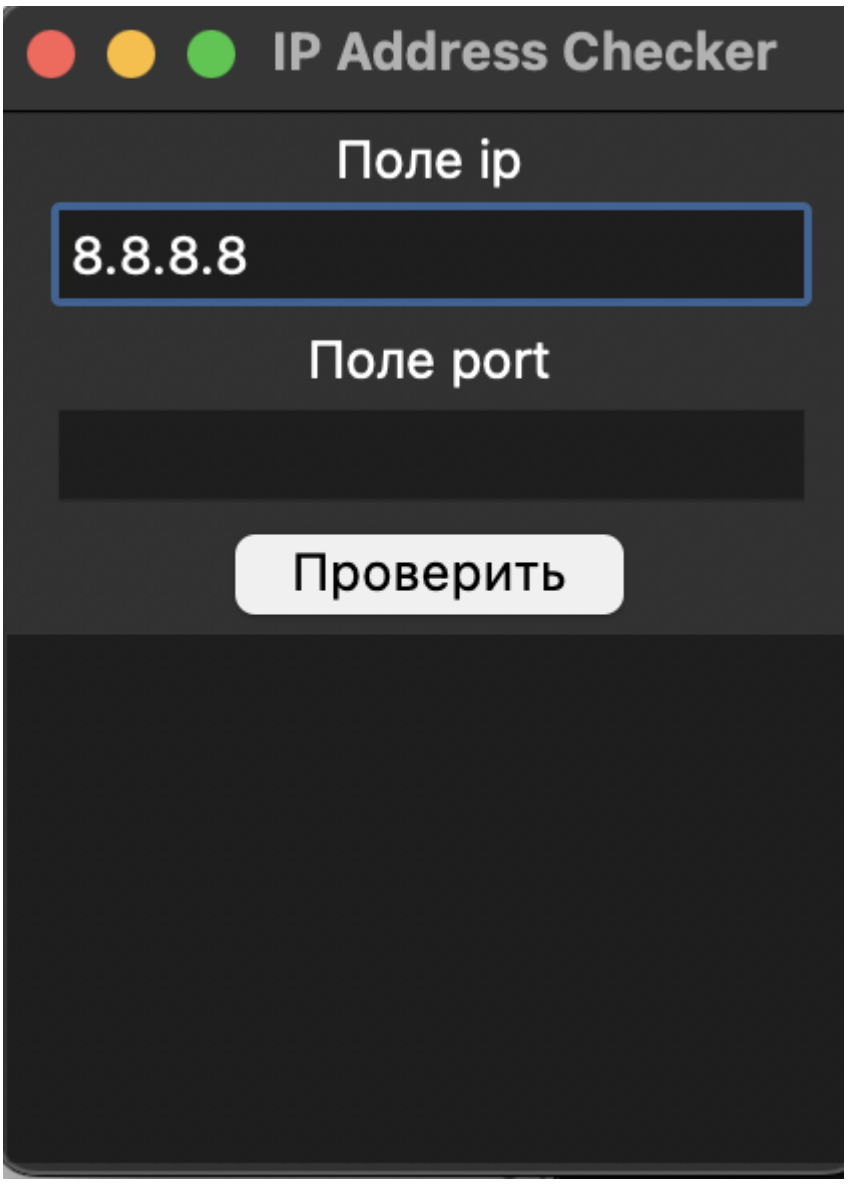

Рис 5.1 Пример работы программы

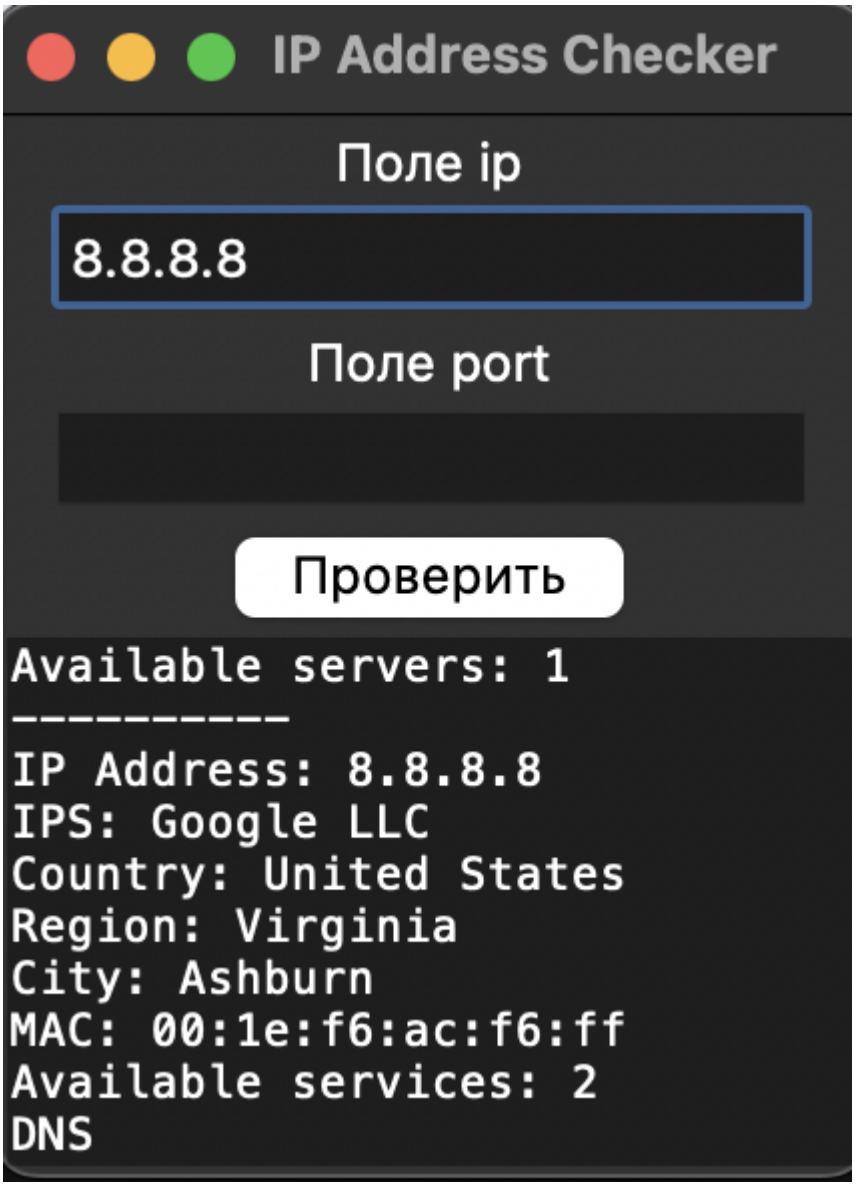

Рис 5.1 Пример вывода

Получили вывод:

Available servers: 1

IP Address: 8.8.8.8

IPS: Google LLC

Country: United States

Region: Virginia

City: Ashburn

MAC: 00:1e:f6:ac:f6:ff

Available services: 2

DNS

HTTPS (HTTP over SSL)

---

6. Рекомендации пользователя

Изучите понятия ip адреса и порта.

7. Рекомендации программиста

Для запуска необходим Python 3.11 и выше. Необходимо установить следующие библиотеки:

scapy, requests.

8. Вывод

В ходе выполнения этих задач были изучены средства Python для взаимодействия с сетью (Scapy), работа с внешними API (запросы через библиотеку requests). Полученный результат представляет собой функциональное и информативное приложение для работы с сетью, позволяющее выполнять сканирование и анализ узлов сети.

Приложение

https://github.com/naelxd/linuxspbu

Дополнительные материалы

https://scapy.readthedocs.io/en/latest/usage.html