

Описание/документация к курсовой работе "Анализатор трафика"

Сазыкин Георгий Андреевич

April 2023

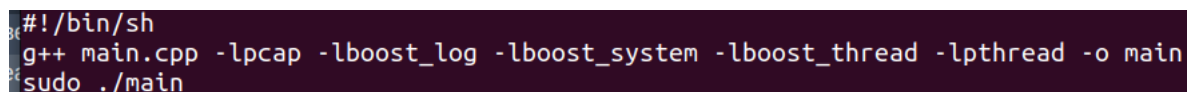
1 Введение

Реализация данного проекта была разбита на 2 части - получение данных о пакетах и сети с помощью библиотеки libpcap, а также получение информации об источнике с помощью библиотеки boost - для корректной работы программы на компьютере потребуется наличие данных библиотек. Результат работы программы - предоставление информации об источниках передаваемых пакетов и о самих пакетах; вывод в консоль разбит на сеансы - иначе, в каждый из сеансов функция sniffing запускается снова и снова; всего таких сеансов 10. Результат работы каждого сеанса - предоставление промежуточной информации; результат работы последнего сеанса - вывод итоговой информации об источниках и пакетах.

2 Реализация

- Сборка и запуск кода

Запускается проект с помощью скрипта sniffer.sh, который имеет следующую структуру:



```
#!/bin/sh
g++ main.cpp -lpcap -lboost_log -lboost_system -lboost_thread -lpthread -o main
sudo ./main
```

Рис. 1: shell скрипт

sudo необходим для получения доступа к сетевым интерфейсам, параметры выше необходимы для использования функций 2-х библиотек (заголовки которых есть в программе)

- Libpcap

С помощью методов libpcap можно получить информацию о сетевом интерфейсе, который будет прослушиваться (pcap_findalldevs), открывает устройство на прослушивание (pcap_open_live) и ведет захват пакетов (pcap_loop - в свою очередь, в эту функцию передается другая функция, которая ничего не возвращает - она служит для обработки информации о полученных пакетах посредством обновления map, в котором хранятся полученные данные; получение IP -адреса, получение JSON для их дальнейшей обработки).

- Boost

После получения IP адреса, с помощью методов библиотеки boost делается get-запрос, результат которого - JSON с полями country, org, isp, status и остальными. Его можно распарсить

и получить необходимые (в данном случае, программа получает поля country и isp - название организации)

- Хранение и обновление информации

Информация о серверах, с которых получена информация, хранится в словаре типа `map<pair<string, string>, pair<string, vector<int>>>` - в первую пару помещаются country и isp; в value значениях первым хранится IP адрес, во втором (векторе) хранится информация о переданных и полученных пакетах, а также о длине пакетов; далее, в каждом сеансе, шар выводится на экран в следующем формате:

```
Country: Russia
isp: Tinkoff Credit Systems Bank
IP: 91.194.226.43
Количество пакетов (IN): 1
Количество пакетов (OUT): 0
Суммарная длина пакетов (байт): 66
*****
Country: United Kingdom
isp: Telegram Messenger Amsterdam Network
IP: 149.154.167.41
Количество пакетов (IN): 92
Количество пакетов (OUT): 218
Суммарная длина пакетов (байт): 1021
*****
Country: United States
isp: Google LLC
IP: 108.177.14.194
Количество пакетов (IN): 6
Количество пакетов (OUT): 7
Суммарная длина пакетов (байт): 155
*****
```

Рис. 2: вывод в консоль

- логирование и вывод остальной информации

Поддерживается уровень логирования с уровнями info, warning и error; сообщения выводятся в консоль; после выводится результат работы сеанса.

3 Рекомендации

Время обработки пакетов может быть не моментальным, поэтому иногда программа может ждать пакеты и в это время ничего не выводить в консоль - это корректная работа программы =)