**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 6**

на тему «Метод «зомби» сканирования при помощи Nmap»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Решетникова Ирина Витальевна |
| (Фамилия, имя, отчество) |

**Цель:** научиться использовать метод “зомби” сканирования.

# **Ход работы:**

**Задание 1.** Настроить виртуальные машины для сканирования.

Для создания виртуальных машин с Windows XP я буду использовать технологию контейнеризации Docker, конфигурация Docker compose представлена на рисунке 1.

Для деплоя использовался проект dockurr/windows, с помощью которого можно создавать контейнеры Windows. Технология docker используется по той причине, что нативные виртуальные машины через Virtual Box и т.п потребляют очень много ОЗУ, ЦПУ.



Рисунок 1 – docker compose для лабораторной работы

**Задание 2.** Показать какие хосты и порты видно.

В нашем случае нет смысла проверять хосты и порты через терминал, так как данные действия явно были заданы в docker compose. Для зомби машины были открыты порты: 3390, 8006, IP – 192.168.1.11. Результат представлен на рисунке 2.

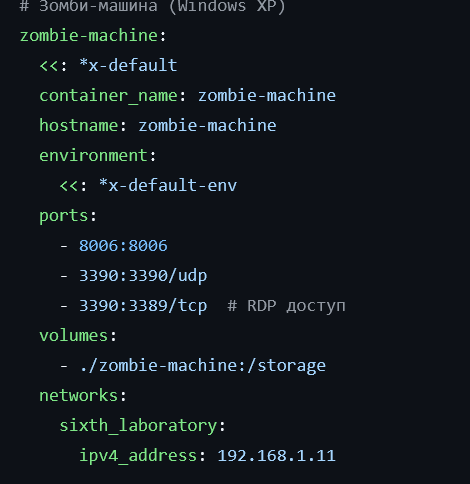


Рисунок 2 – параметры для зомби машины

Для машины target были заданы параметры, которые представлены ниже на рисунке 3. Здесь открыты порты: 3391, 8007, IP – 192.168.1.22.

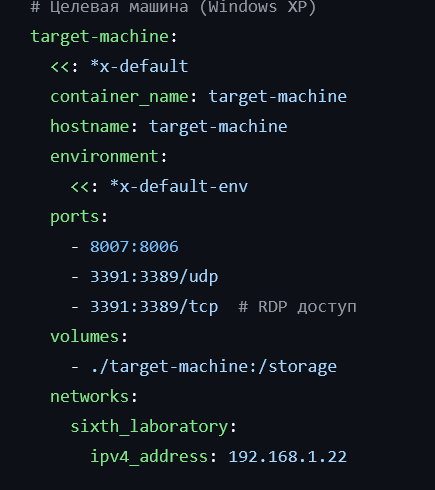


Рисунок 3 – параметры для target машины

**Задание 3.** Отправить RST пакеты на машину зомби.

Для выполнения задания использовалась команда, которая представлена ниже на рисунке 3. Рассмотрим более подробно ниже, что делает данная команда.

“sudo” - запуск с правами root (необходимо для работы с сырыми сокетами и управления сетевыми пакетами)

“-Pn”- "Treat all hosts as online" - пропуск проверки доступности хоста (не отправляет ICMP ping). Полезно, когда хост блокирует ping-запросы.

“-p 3390” - сканировать только порт 3390 (данный порт был открыт для всего tcp/udp трафика во внешний мир).

“—scanflags RST” **- ключевой параметр!** Устанавливает в TCP-заголовке только флаг RST (Reset).

“192.168.1.22”- целевой IP-адрес.

Что делает эта команда? Отправляет на порт 3390 целевого хоста TCP-пакет с **установленным только флагом RST.** Если порт **открыт**: большинство систем проигнорируют такой пакет (не ответят). Если порт **закрыт**: некоторые системы отправят RST в ответ (но поведение неоднозначно). Современные системы обычно **игнорируют** такие пакеты в обоих случаях.

Зачем это используется в контексте зомби-сканирования? Эта команда имитирует второй этап атаки при **закрытом порте** (Рисунок 3 из методички). Когда сканер отправляет зомби SYN-пакет с поддельным IP цели. Если порт на цели **закрыт**, цель отправляет зомби RST-пакет. Зомби **не изменяет свой IPID** при получении такого пакета.

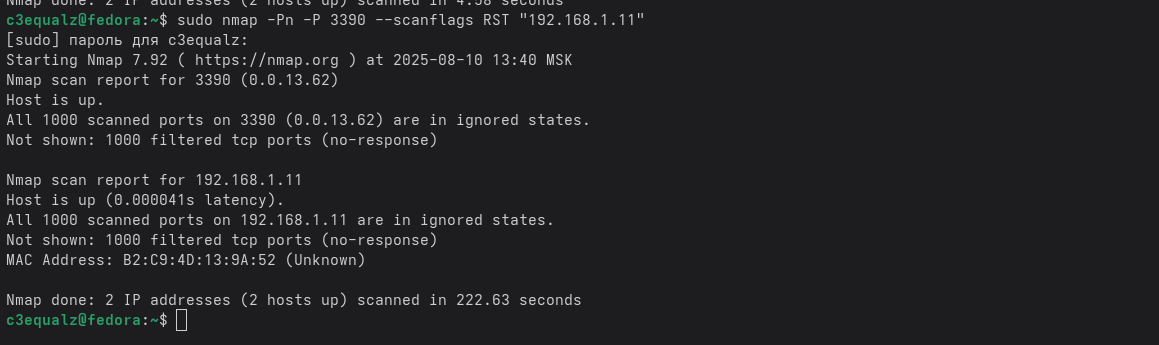


Рисунок 4 – результат отправки “RST” на хост.

Теперь рассмотрим какую информацию нам покажет Wireshark. Результат представлен на рисунке 5.

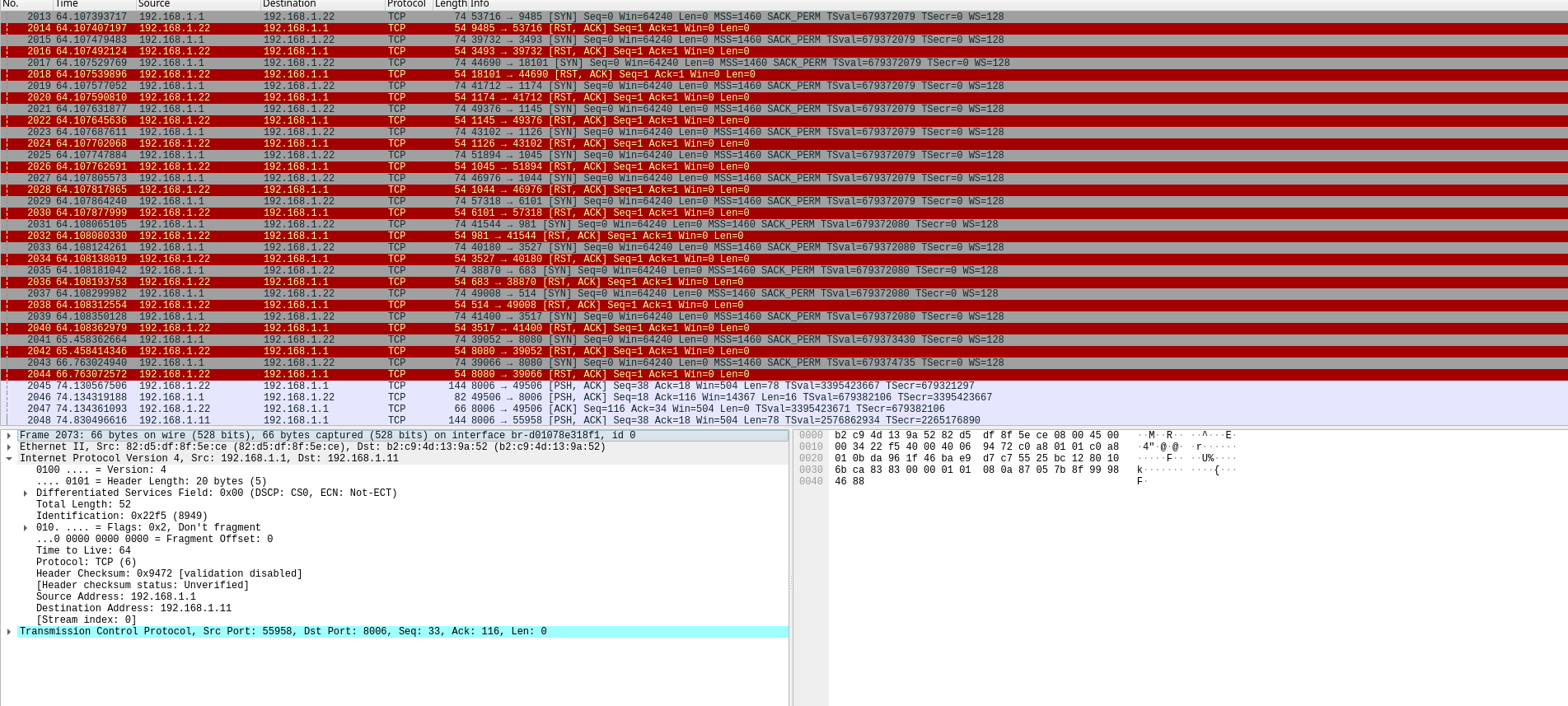


Рисунок 5 – Wireshark при отправке RST на зомби машину

**Задание 4.** Отправить SYNACK пакеты на зомби машину.

Попробуем теперь отправить SYNACK пакеты на зомби машину, для этого будем использовать команду, которая представлена на рисунке 6.

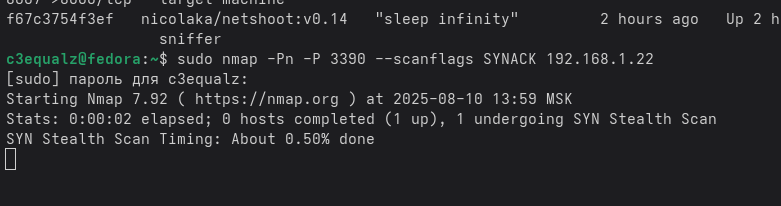


Рисунок 6 – результат отправки “SYNACK” на зомби машину

Теперь в Wireshark будет видно, что пакеты увеличиваются на 1. Интерфейс представлен на рисунке 7.

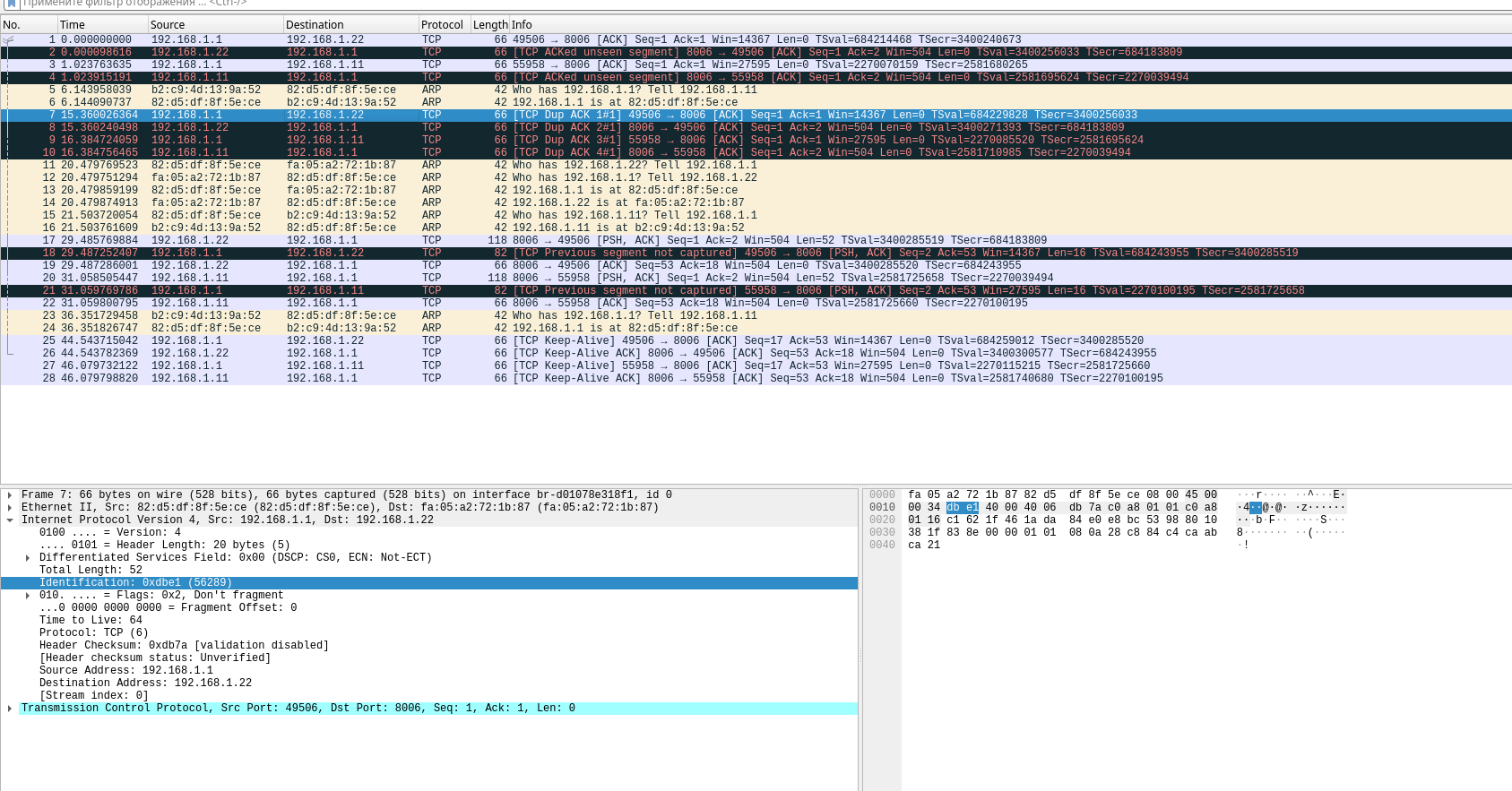


Рисунок 7 – интерфейс Wireshark

**Задание 5.** Выполнить сканирование портов с подменой IP.

Для выполнения задания используется команда, которая представлена на рисунке 8. Здесь мы получаем информацию об устройстве через другое устройство. В дальнейшем это может использоваться злоумышленниками для взлома.

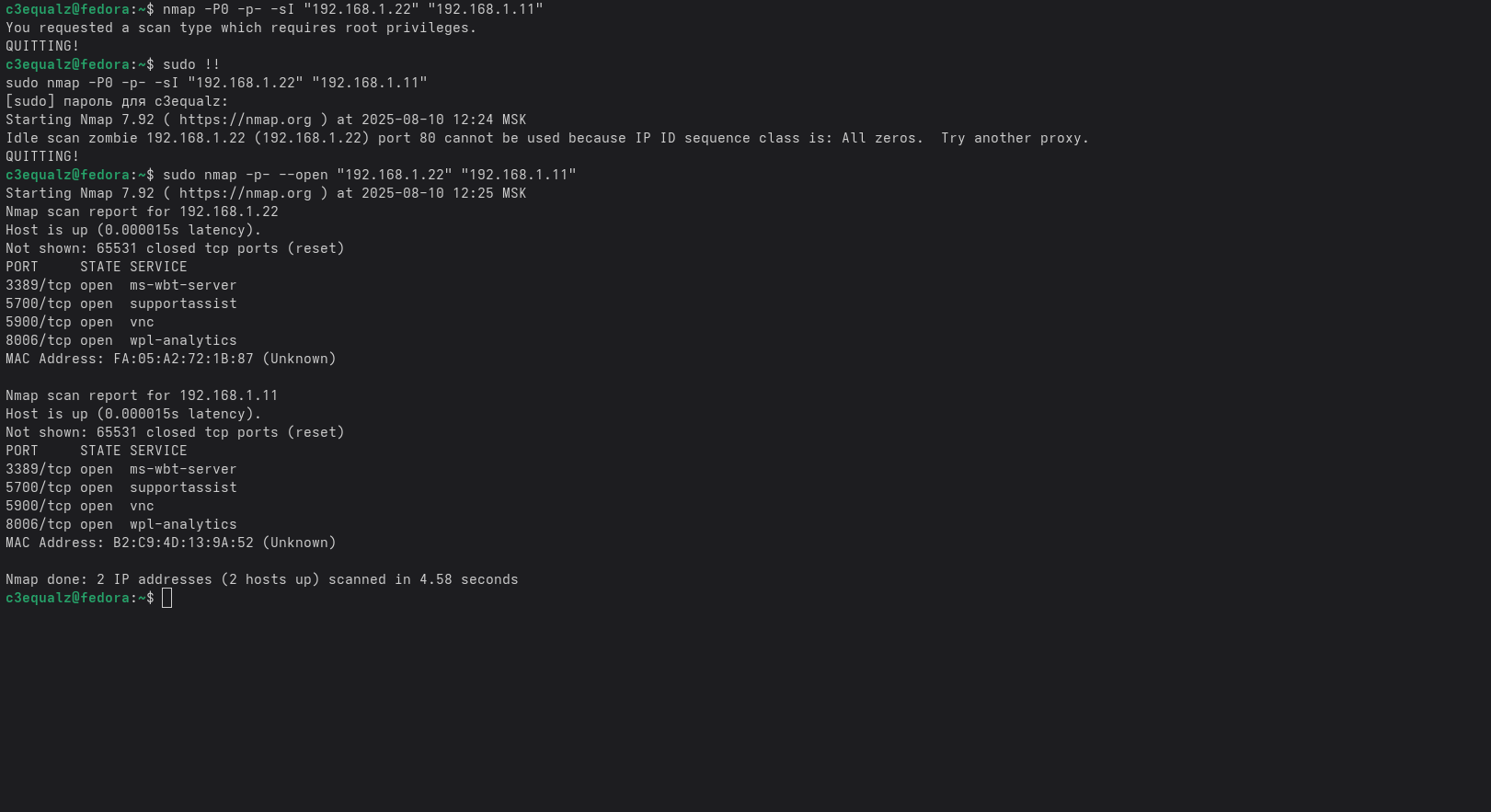
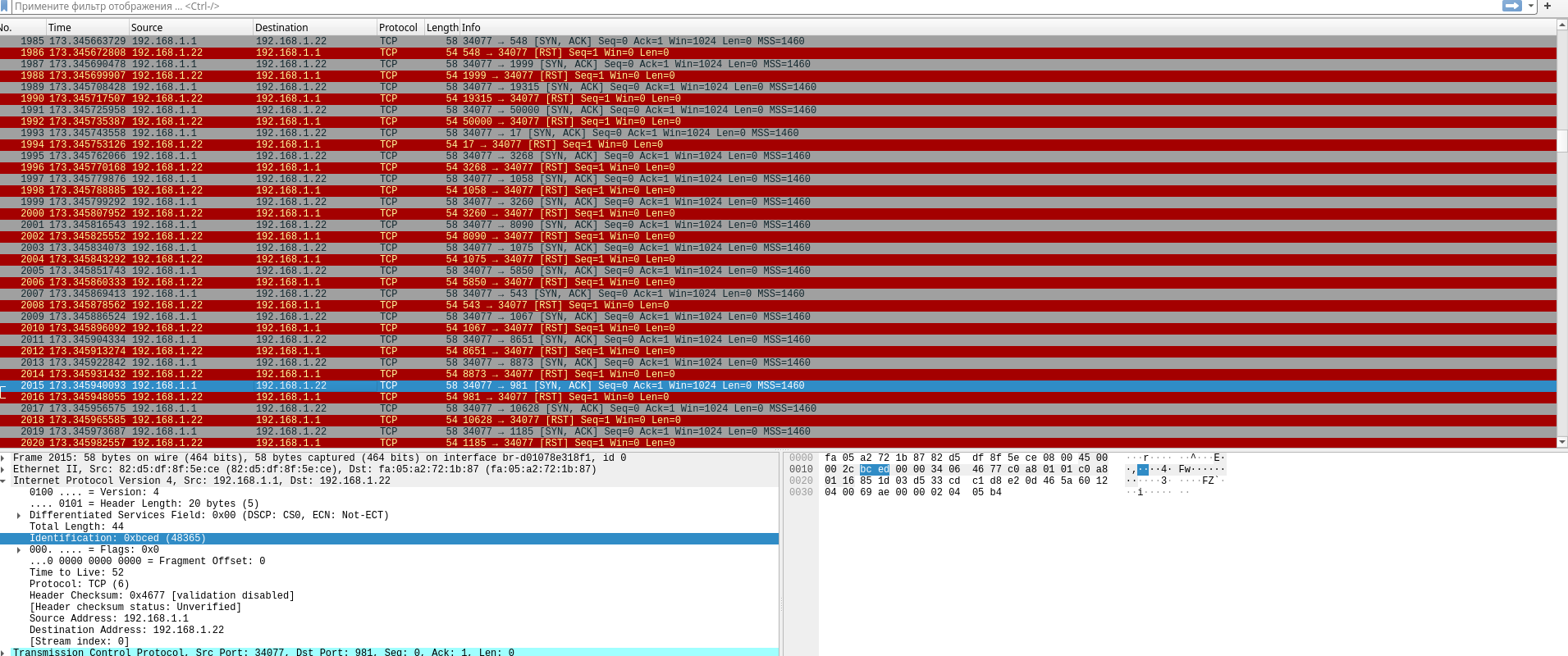


Рисунок 8 – результат проведенного сканирования

**Задание 6**. Включить брандмауэр и проверить поведение.

При включении брандмаэра и отправки RST пакетов происходит то, что представлено на рисунке 9. В результате выходит так, что все данные блокируются и информация не проходит.



**Вывод**: В результате выполнения данной лабораторной работы был изучен метод “Зомби”.