|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| **Федеральное государственное бюджетное образовательное учреждение**  высшего образования  «МИРЭА – Российский технологический университет» |

Институт кибербезопасности и цифровых технологий

Практическая работа № 2.2

по дисциплине

«Управление информационной безопасностью»

**Выполнил:**

ББМО–01–22

Чадов В. Т.

**Проверил:**

Пимонов Р. В.

«Зачтено» «\_\_»\_\_\_\_\_\_\_\_\_2023 г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2023

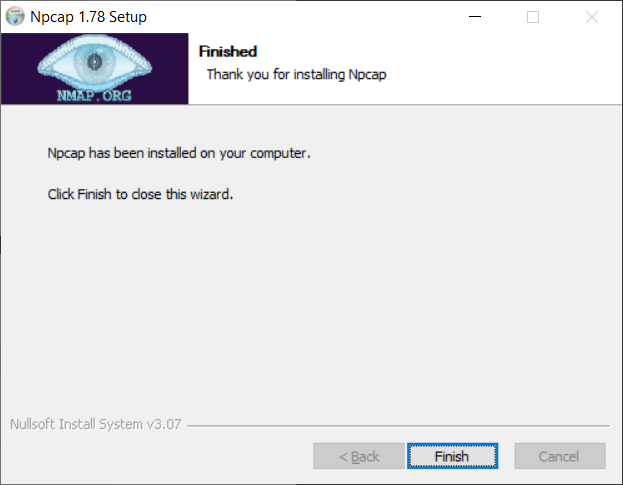
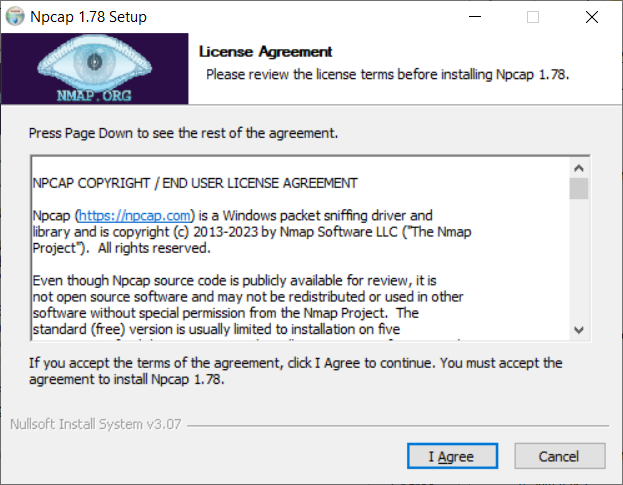
Содержание

**Установка и настройка параметров IDS Snort** 3

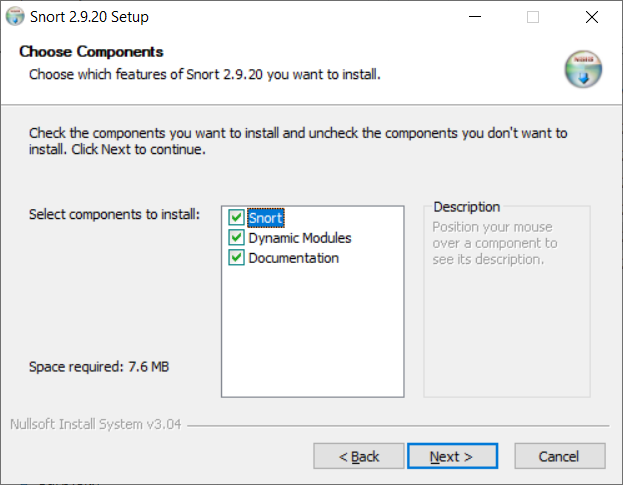
**Написание своего правила** 10

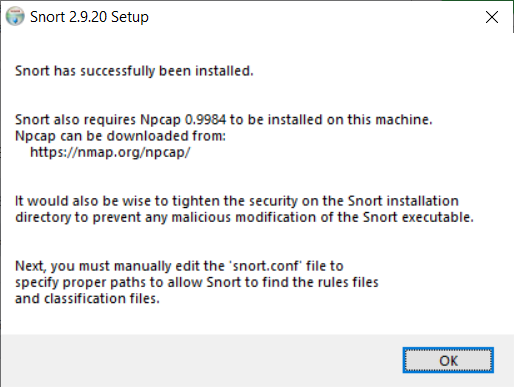
**Установка и настройка параметров IDS Snort**

Установим npcap.



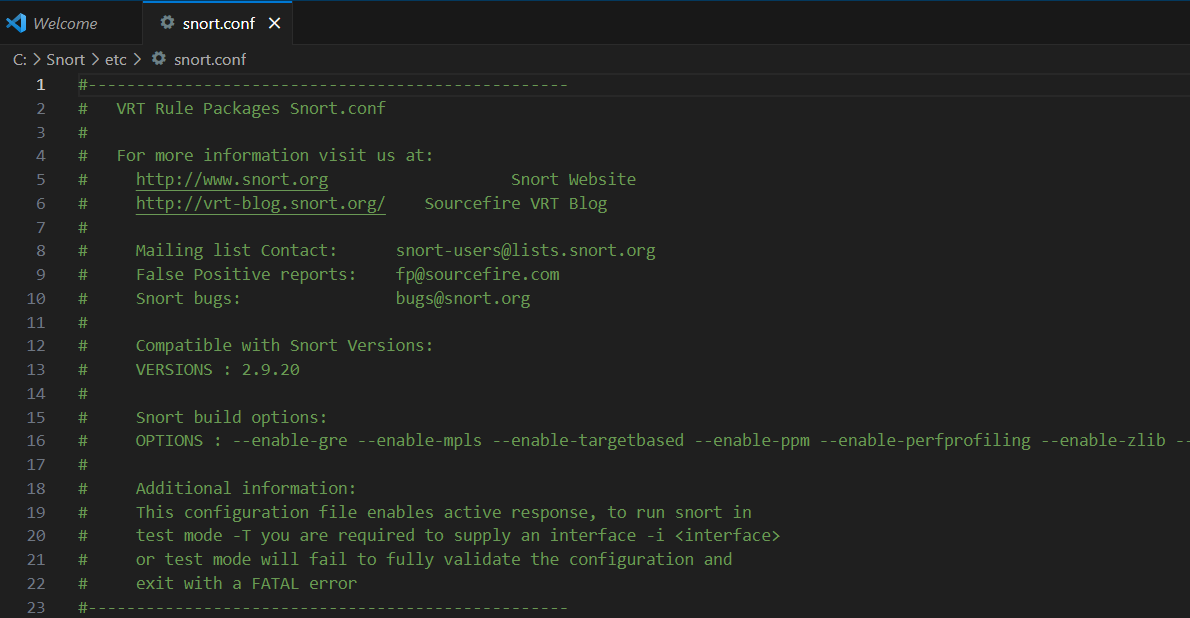
Установим snort.

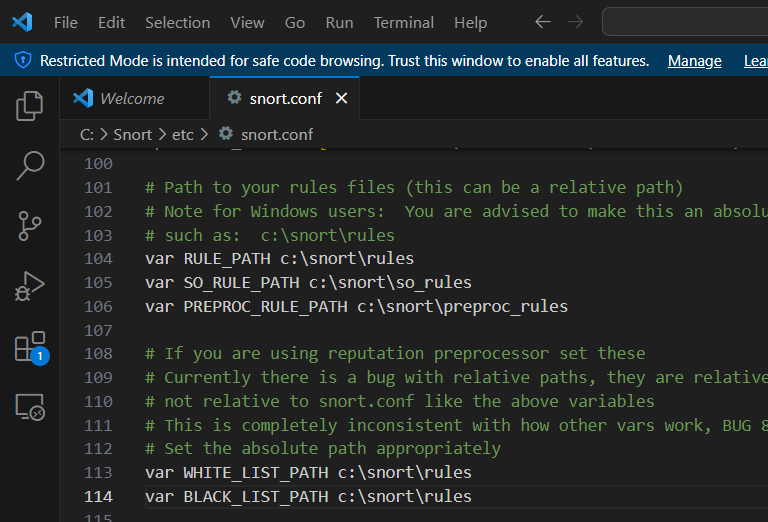


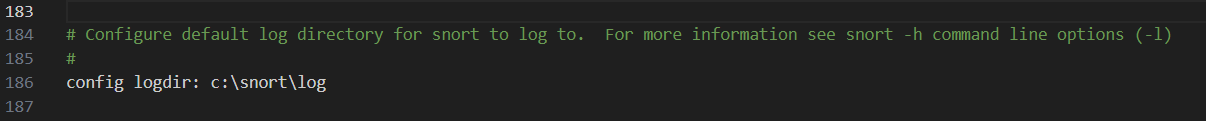


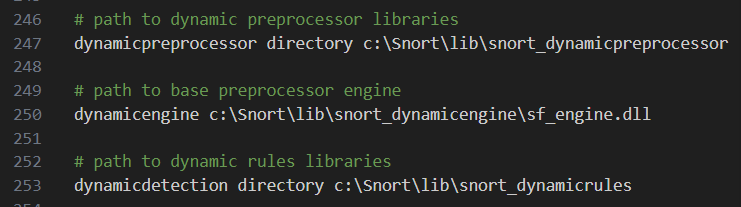


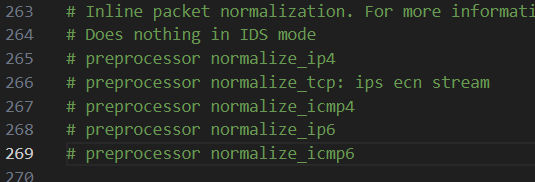
Сконфигурируем snort.conf.

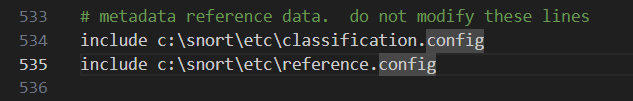


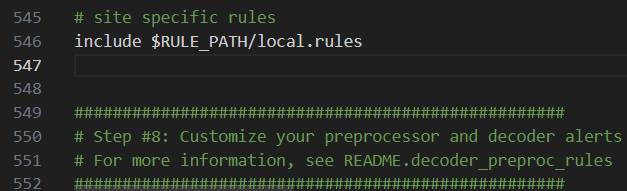




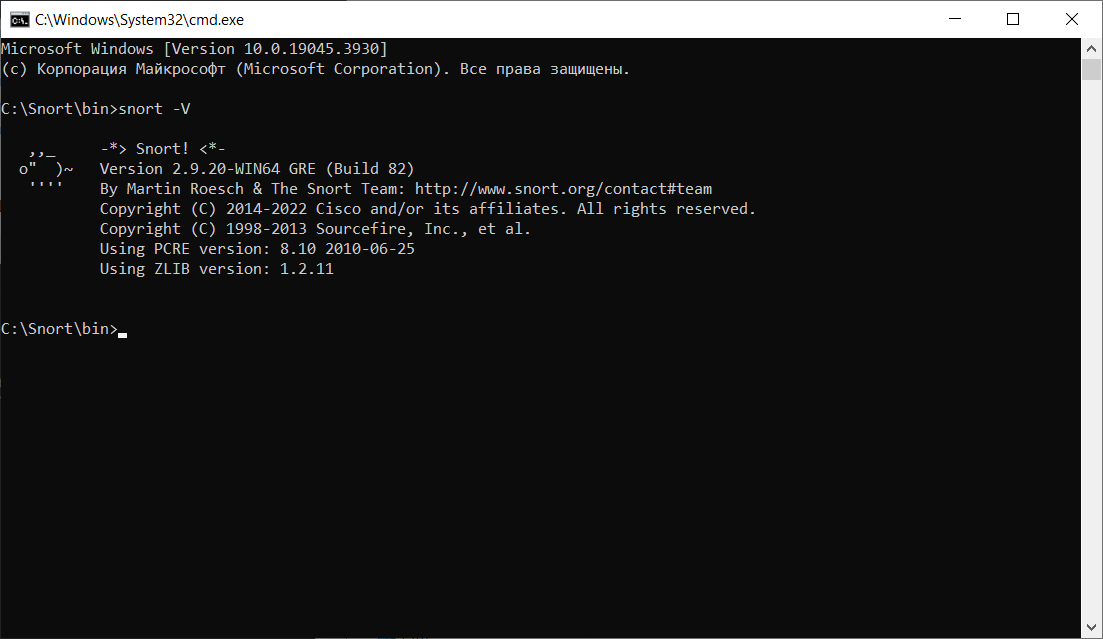




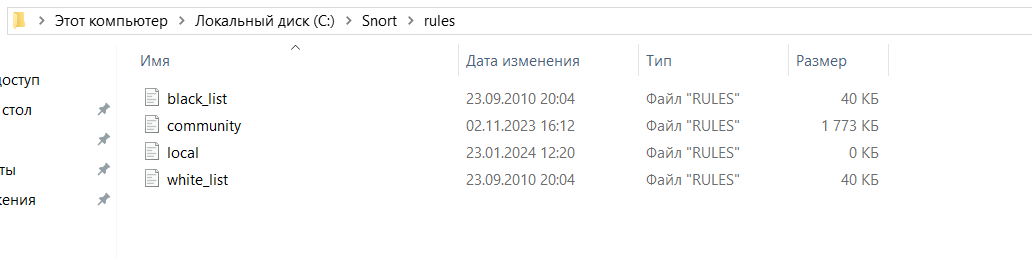




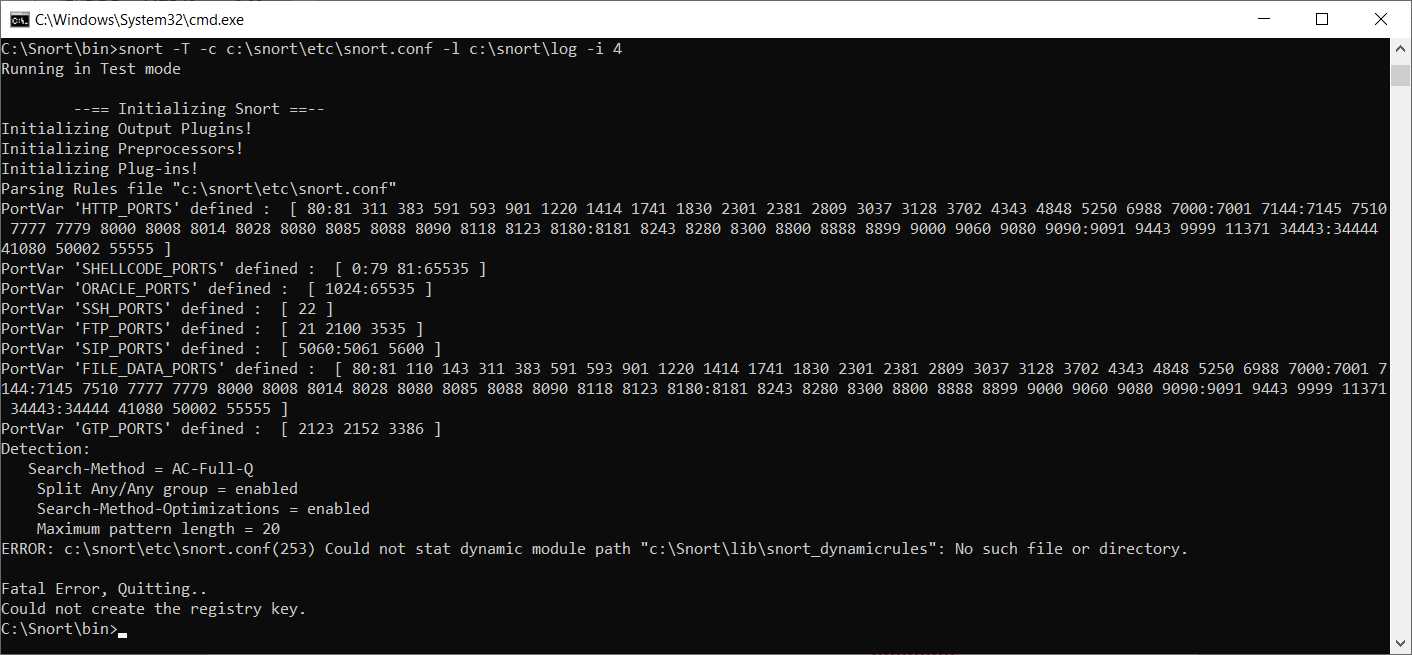
Протестируем snort.conf и запустим snort.

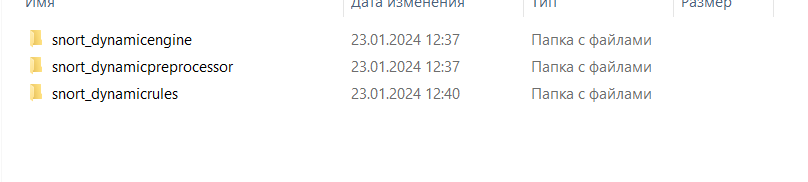


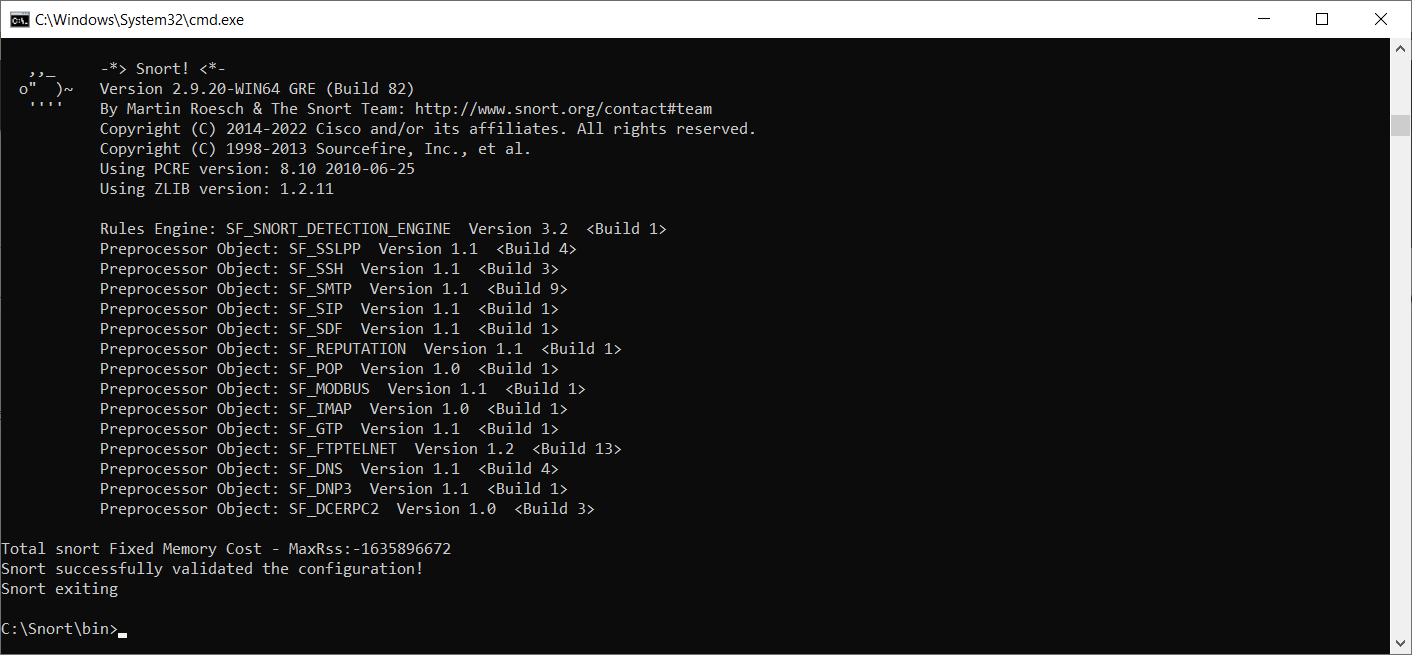
Добавим сразу все файлы с правилами.



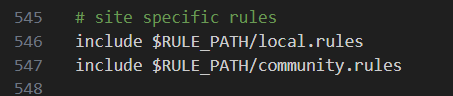
Получили ошибку о отсутствии snort\_dynamicrules

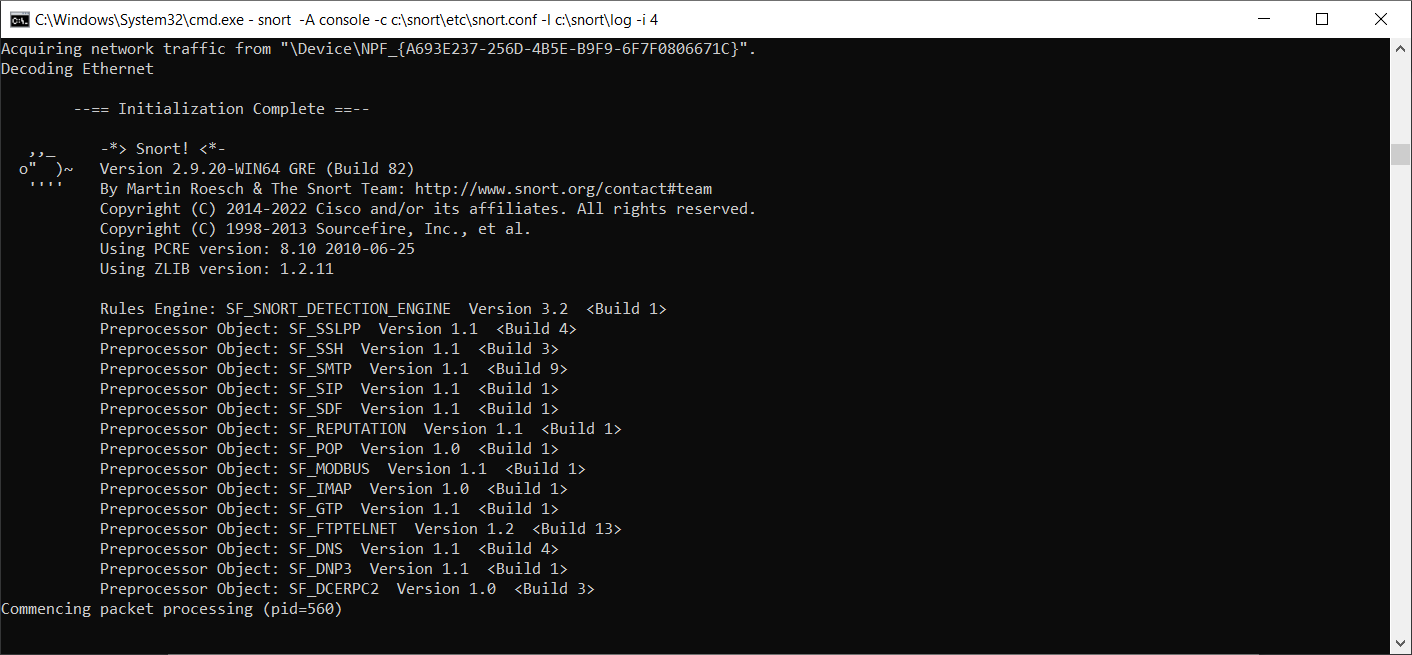




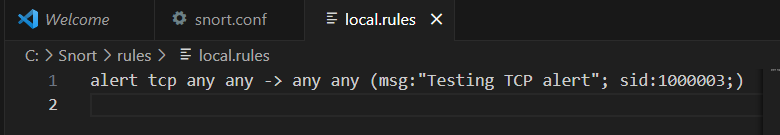


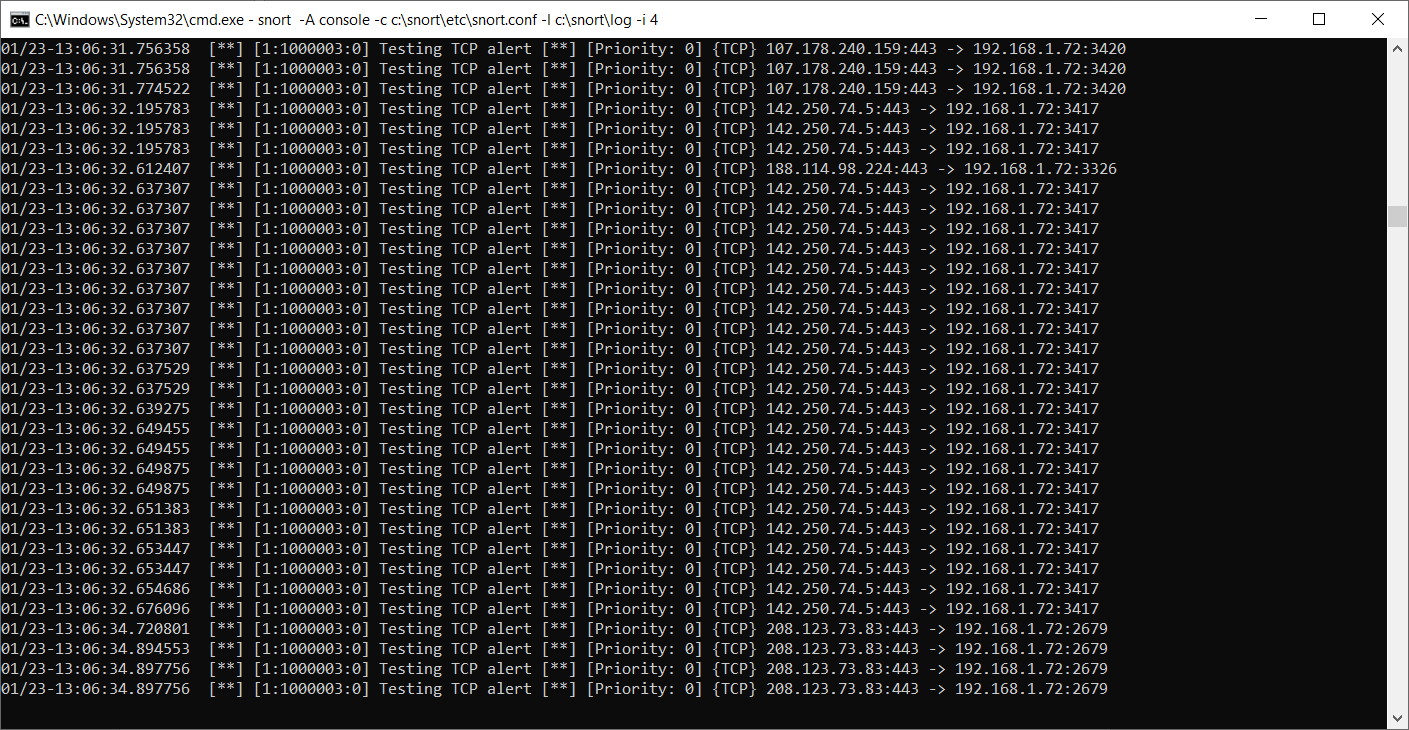
Добавим путь для community.rules





Напишем правило для теста которое будет реагировать на любое tcp соединение с sid 1000003





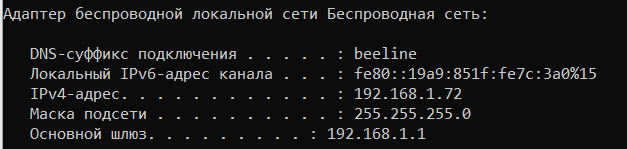
**Написание своего правила**

Выполним задание по варианту, напишем правило.

N = n mod m + 1 = 9 mod 10 + 1 = 10

10. Создать правило для Snort, которое срабатывает при обнаружении всех исходящих ip-пакетов с Вашим ip-адресом с выводом соответствующего сообщения.

Мой ip



Добавим собственный ip (основной шлюз) и поменяем сообщение, вместо tcp поставим ip чтобы поймать все пакеты

