

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

----------------------------------------------------------------------------------------------------

Институт кибербезопасности и цифровых технологий

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

----------------------------------------------------------------------------------------------------

**Отчёт по практической работе № 2.2**

По дисциплине

«Управление информационной безопасностью»

Тема: «Обнаружение и предупреждение компьютерных атак»

Задание: «Настройка параметров системы обнаружения атак»

Студент Кузькин Павел Александрович

Группа ББМО-01-22

Работу проверил

Пимонов Р.В.

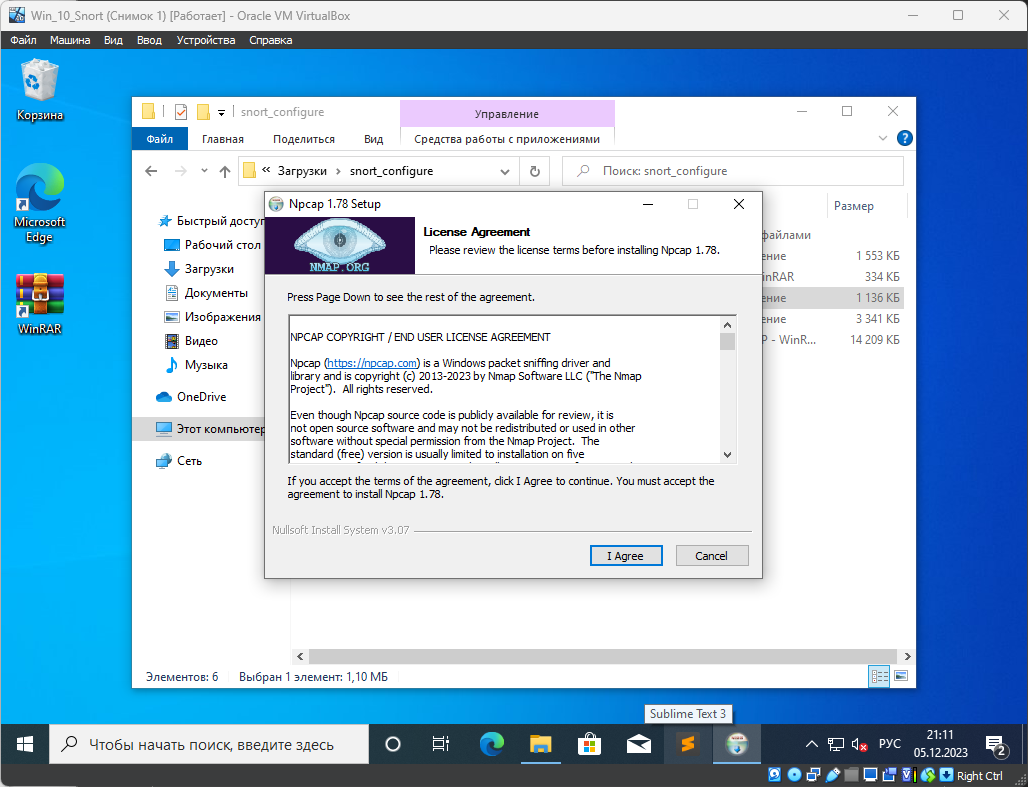
Москва, 2023

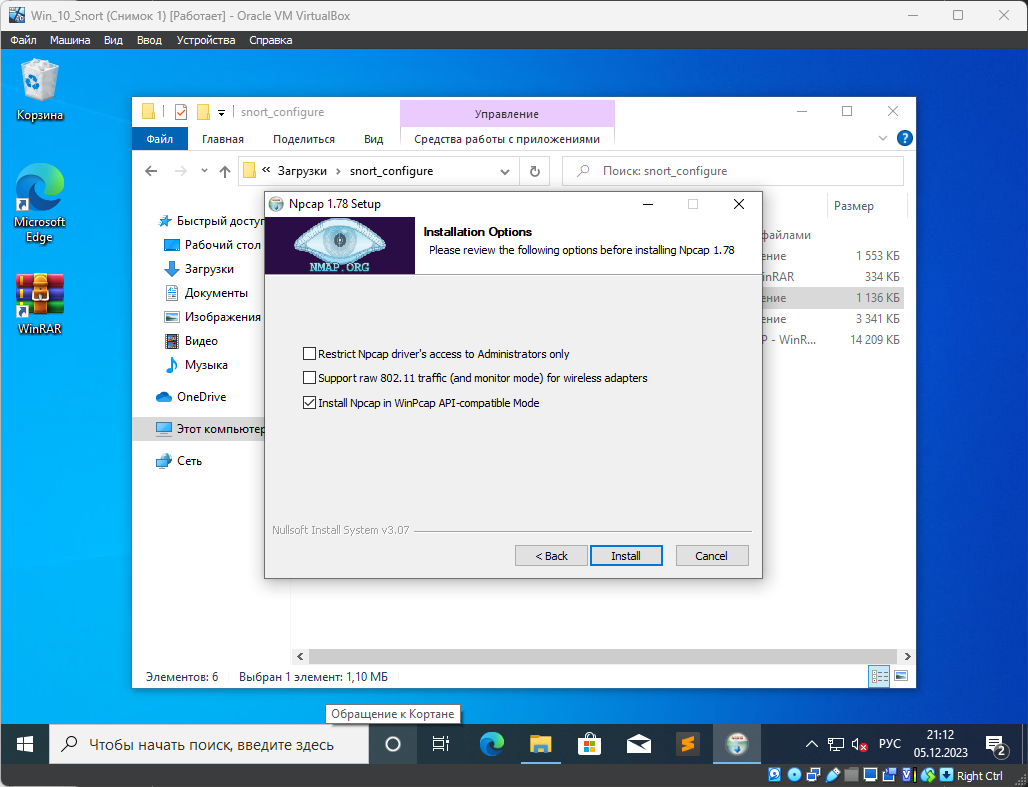
**Вопрос 1. Установка и настройка параметров IDS Snort**

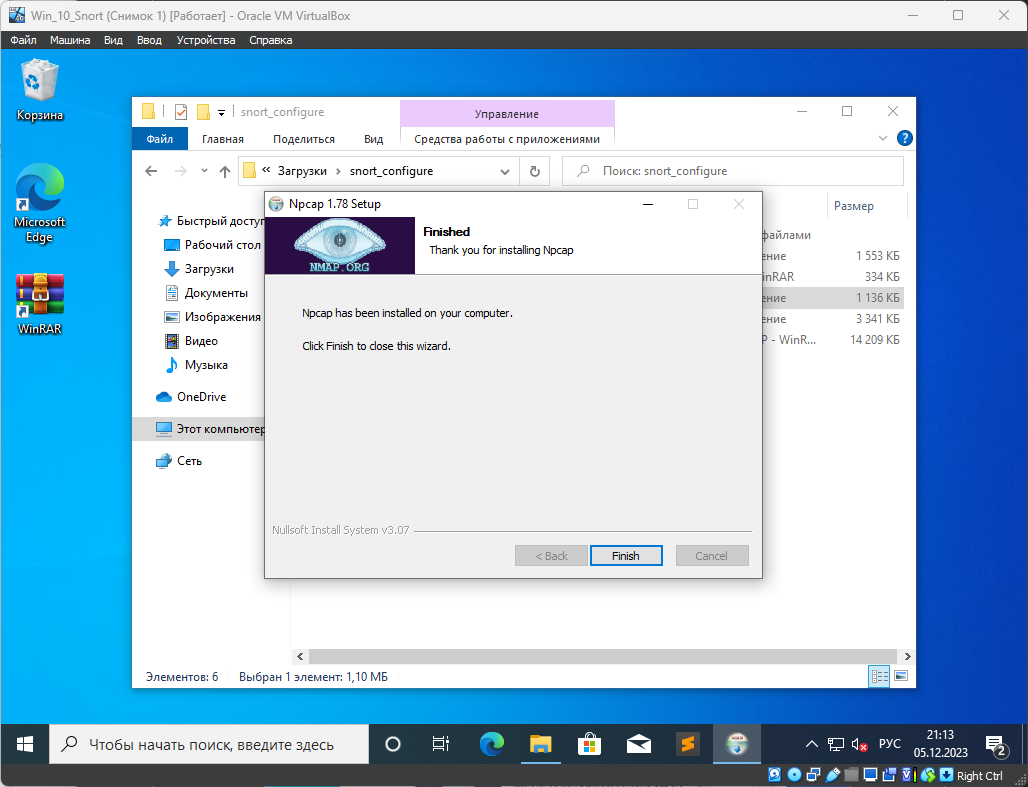
Перед выполнением задания скачаем архив с требующимся ПО по ссылке: <https://1drv.ms/u/s!AlN4iiJAxsjbgVMVo5Ha-52vbvT9?e=YbZNad>. Разархивируем его и посмотрим его содержимое:



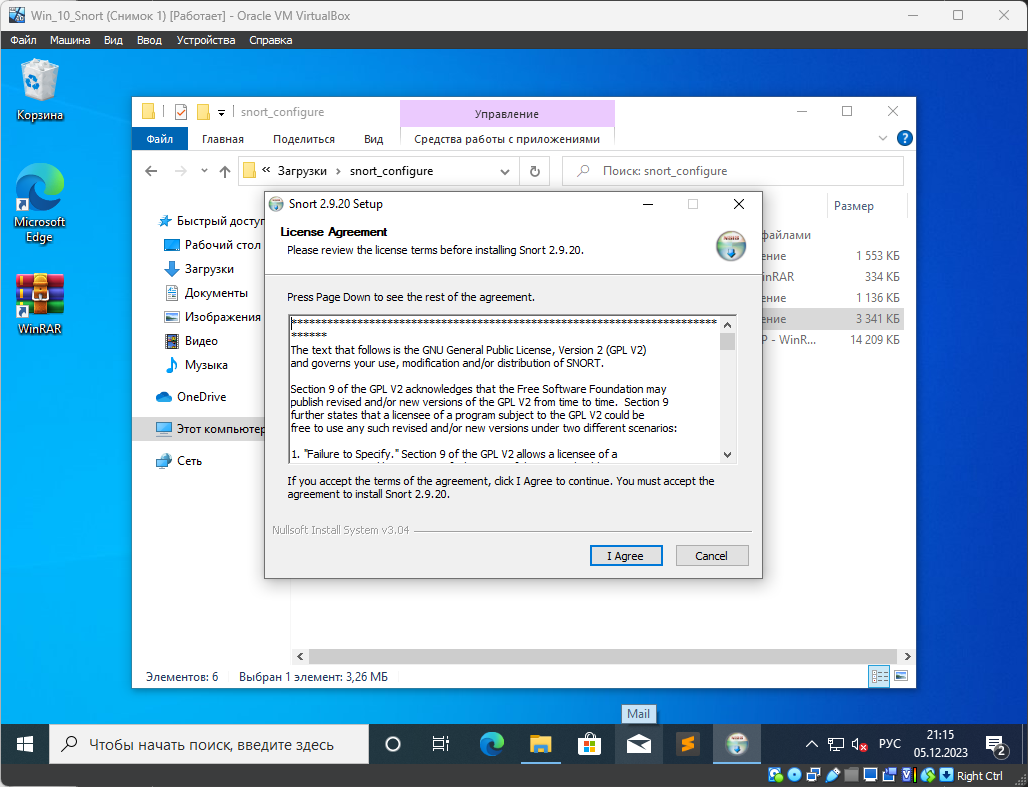
Выполним установку npcap:

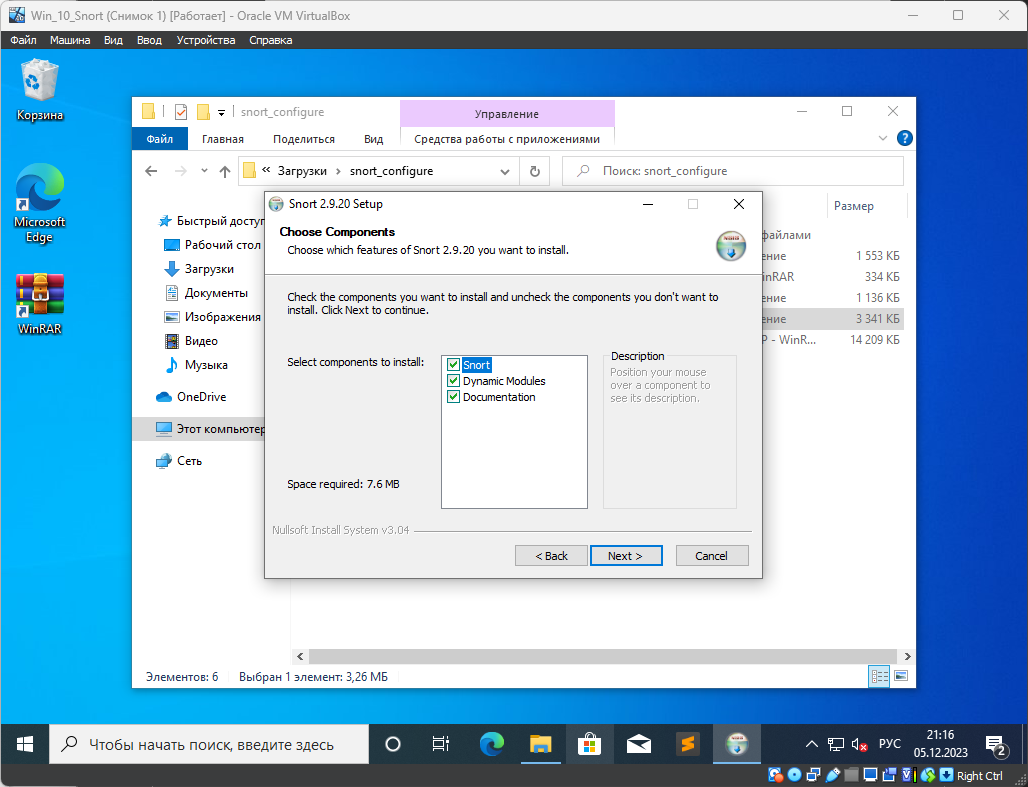


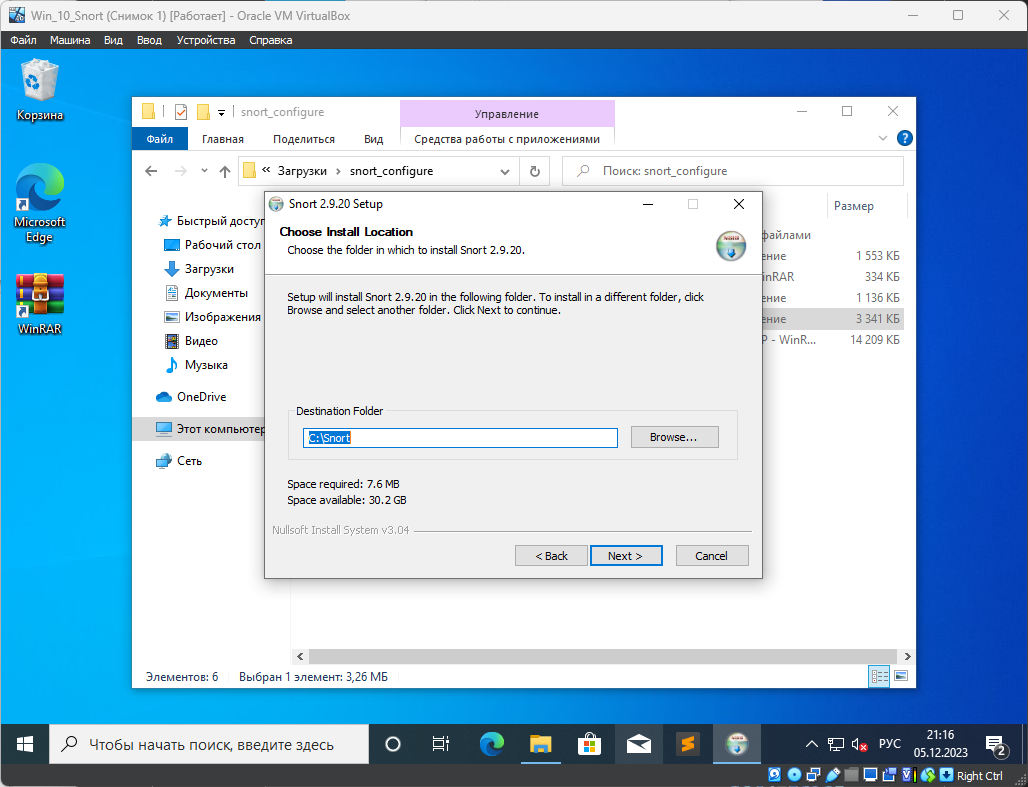


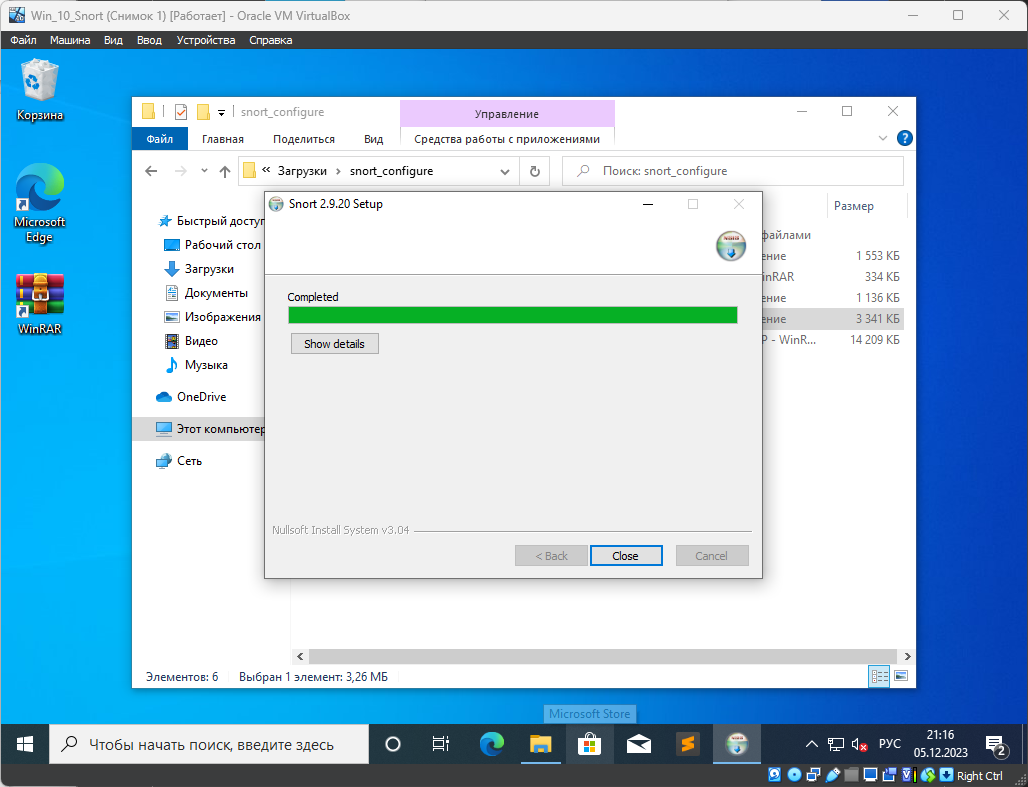


Выполним установку IDS Snort:

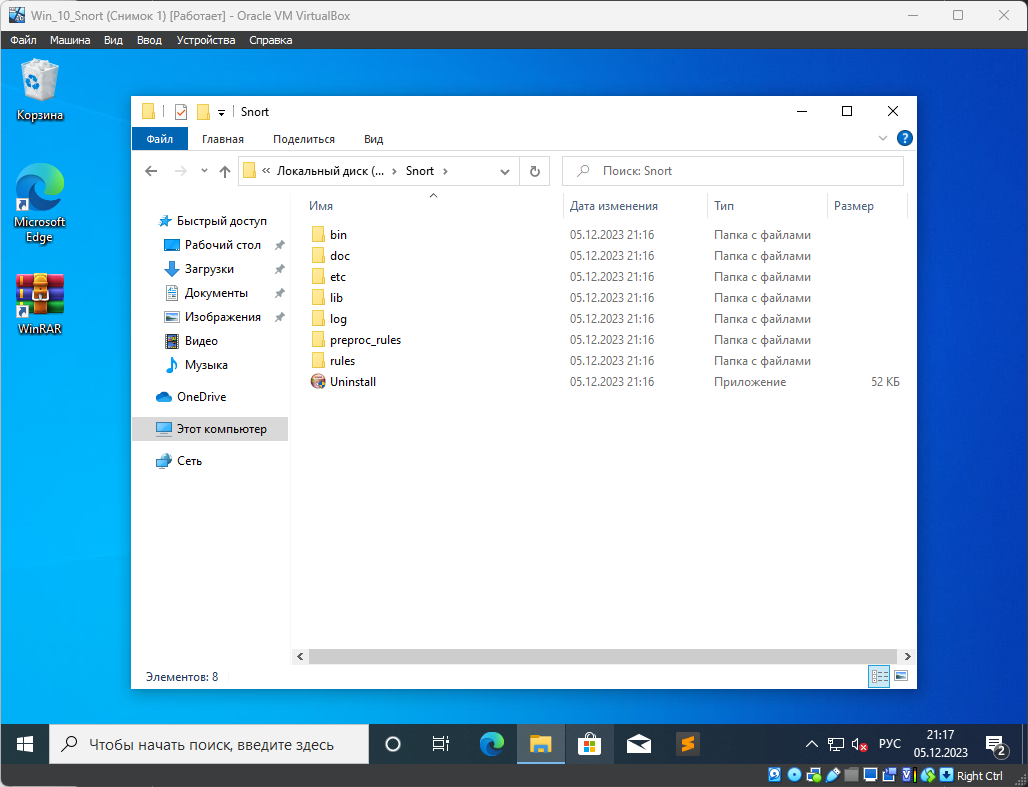






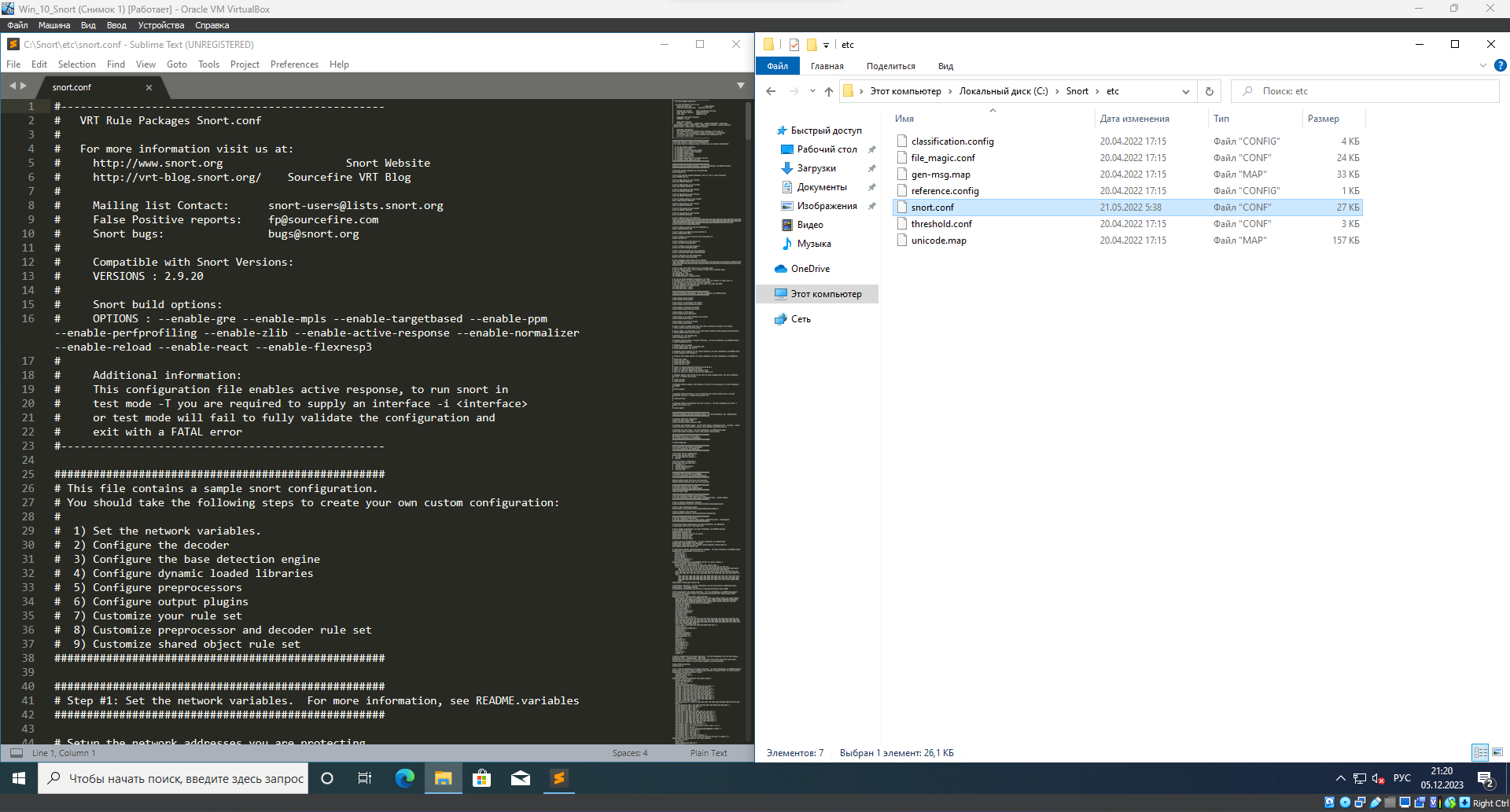


После установки в диске C:/ появится папка с файлами программы:

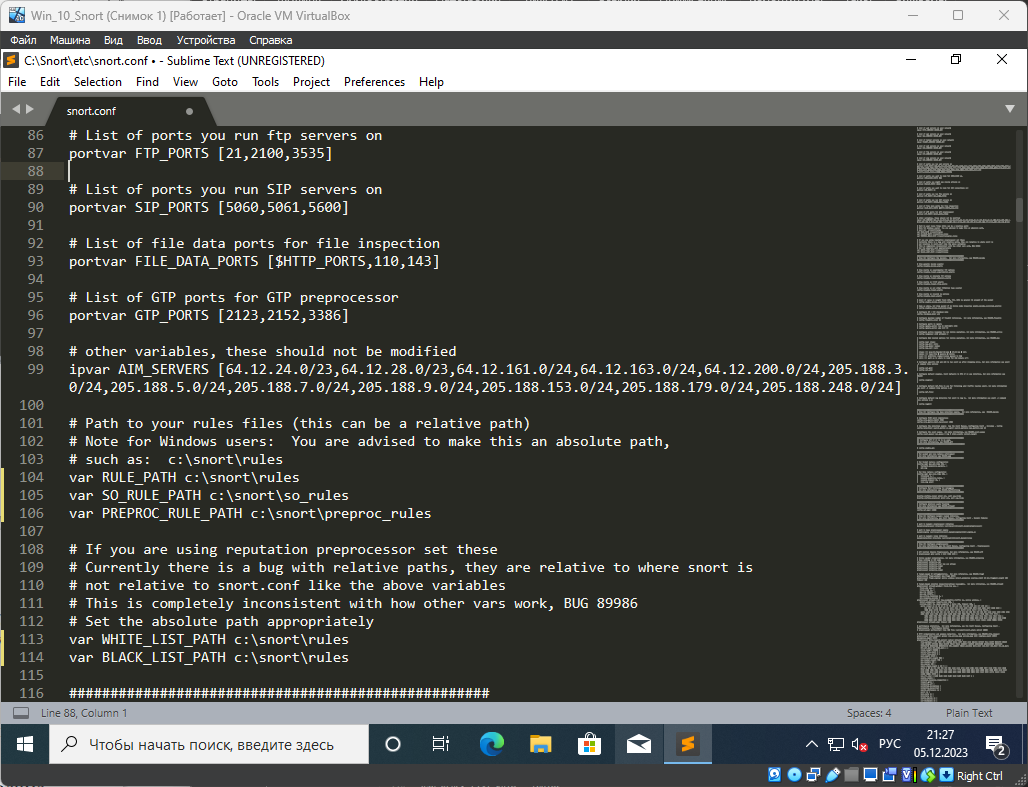


После перехода в директорию C:/Snort в первую очередь необходимо настроить файл конфигурации для его успешной работы.

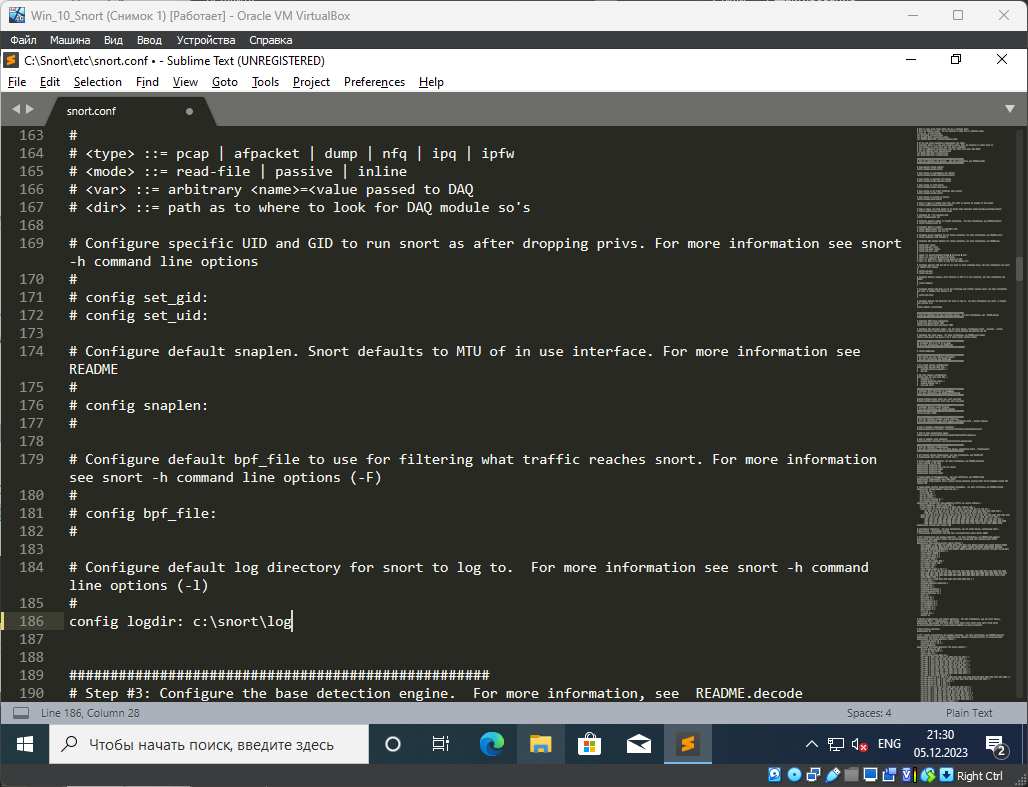
Для настройки этого файла необходимо перейти в директорию C:/Snort/etc и открыть файл snort.conf, сделать это можно, например в текстовом редакторе Sublime Text или VS Code. Дальнейшие операции по редактированию конфигурационных файлов будут производится с помощью Sublime Text. Откроем файл C:/Snort/etc/snort.conf:



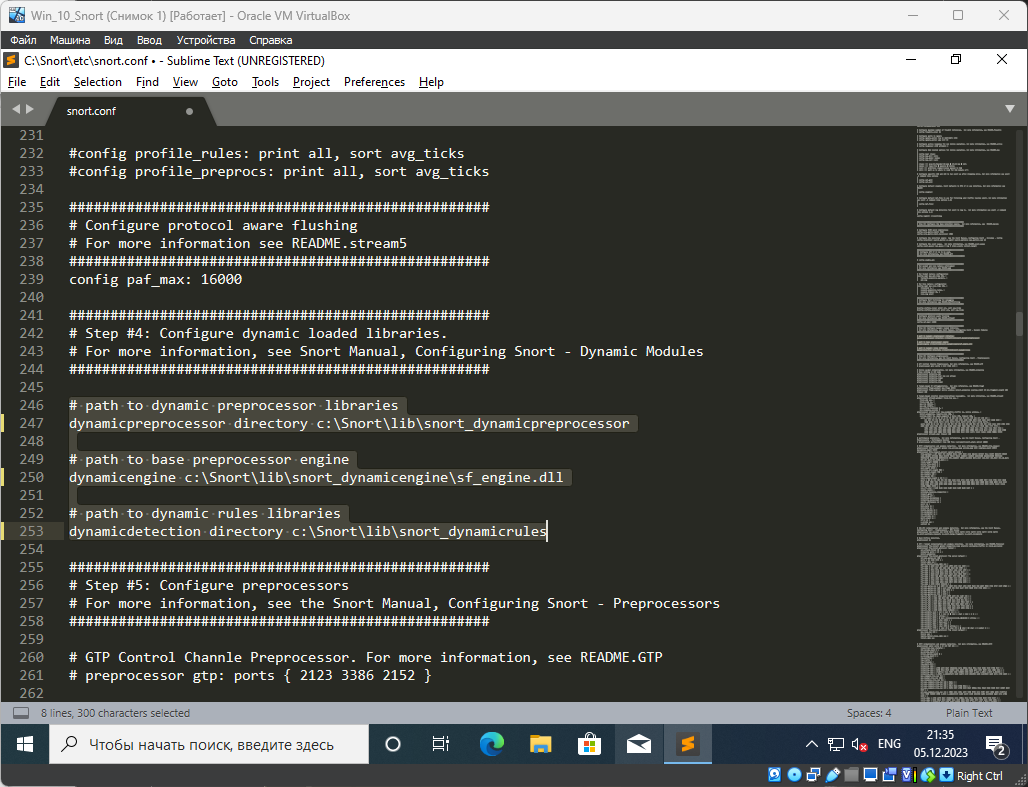
Зададим корректный пусть в строках 104-106, 113-114:



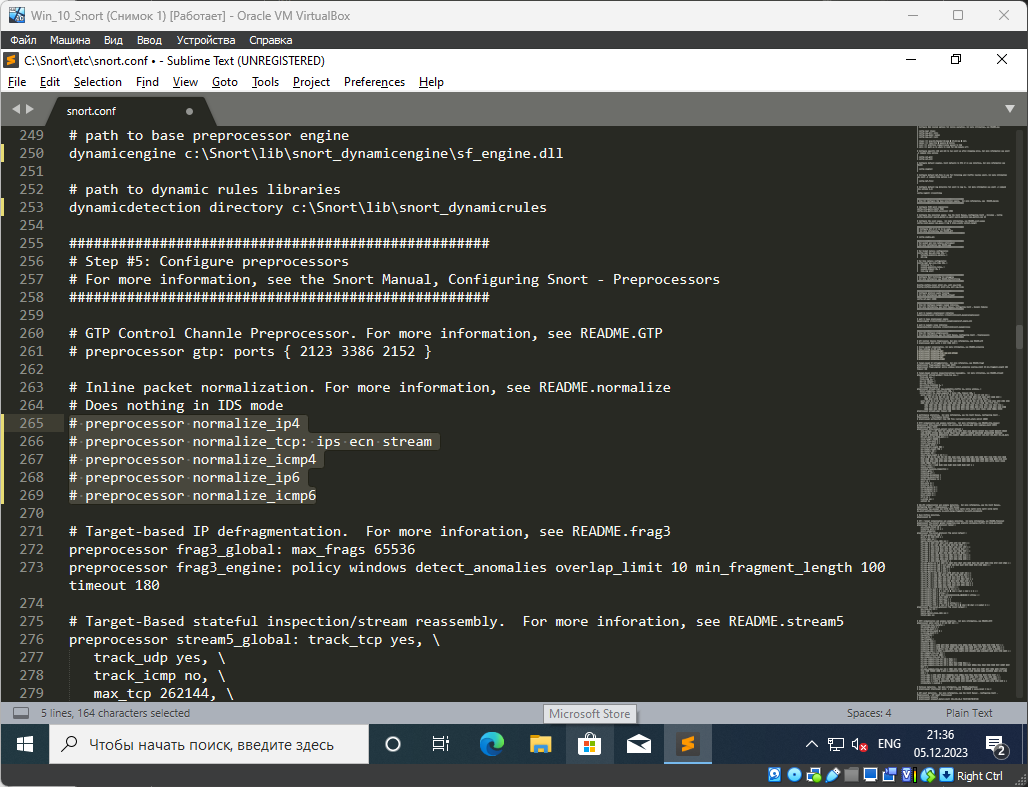
Теперь необходимо указать путь для папки Log-файлов, куда Snort будет записывать все логи, доступные для просмотра и изучения. Отредактируем 186 строку:



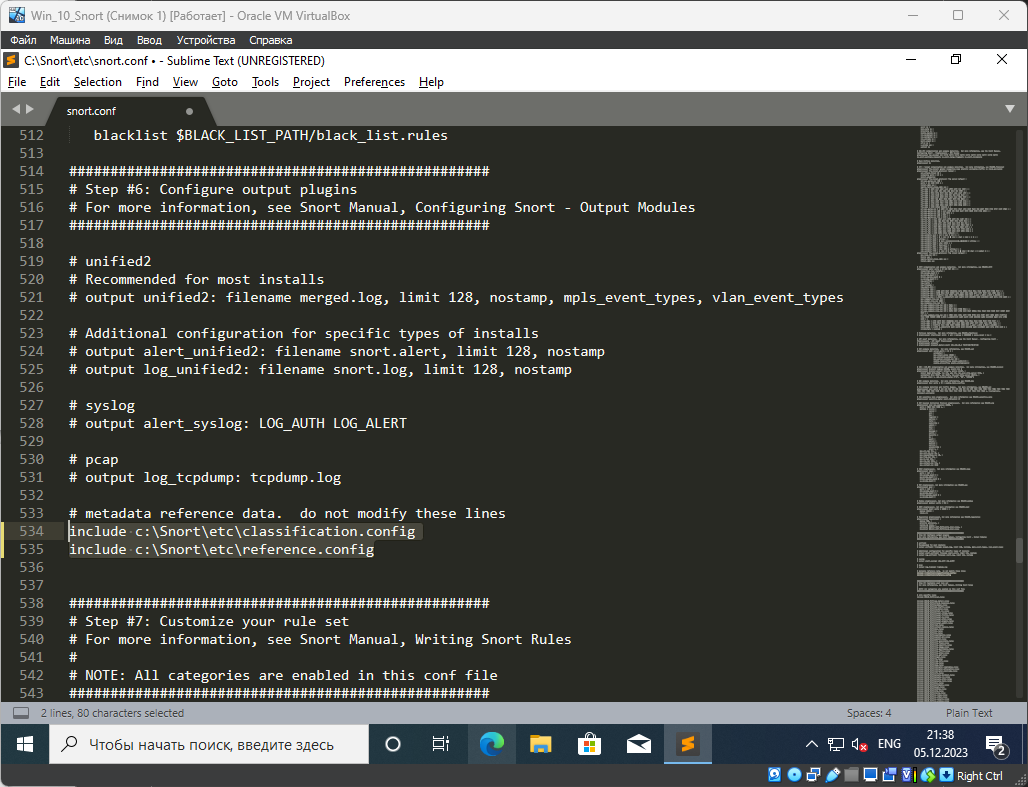
Далее отредактируем строки 247, 250, 253:



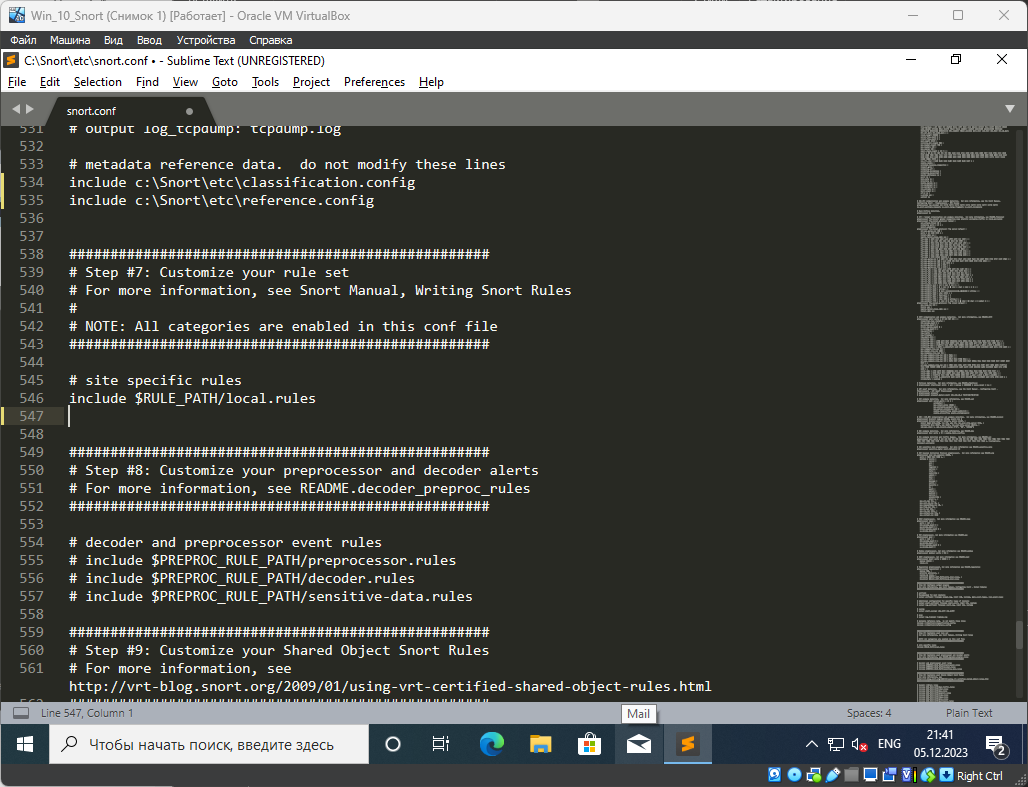
Закомментируем строки 265-269:



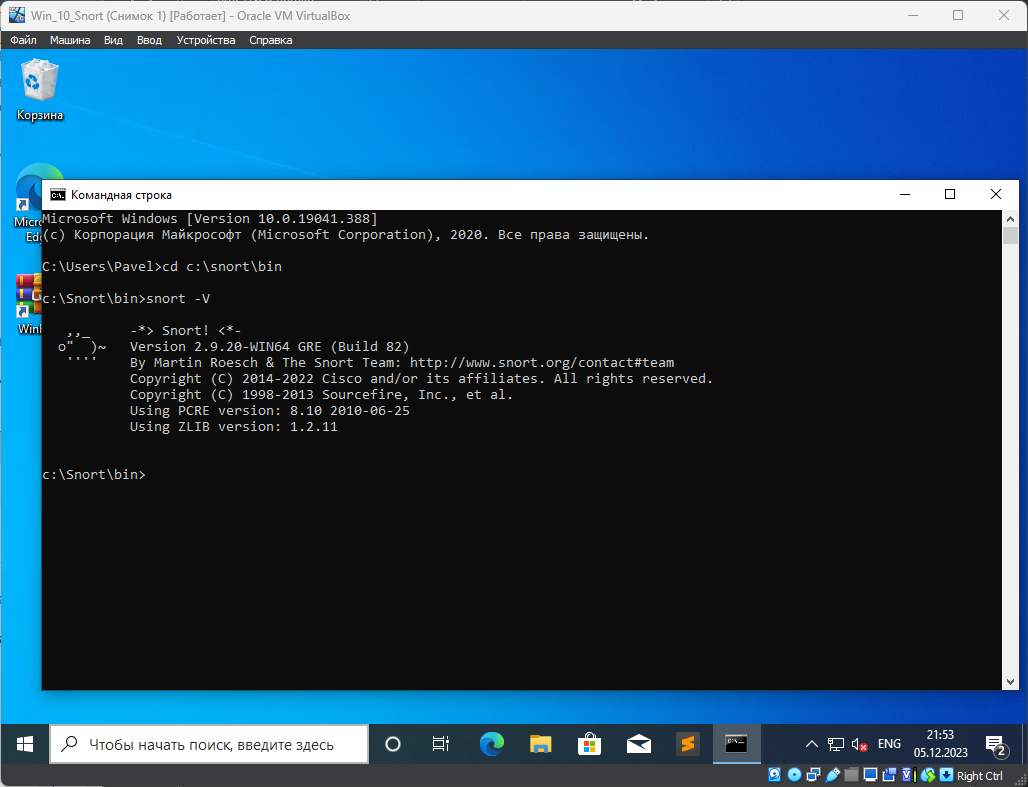
Отредактируем строки 534-535:



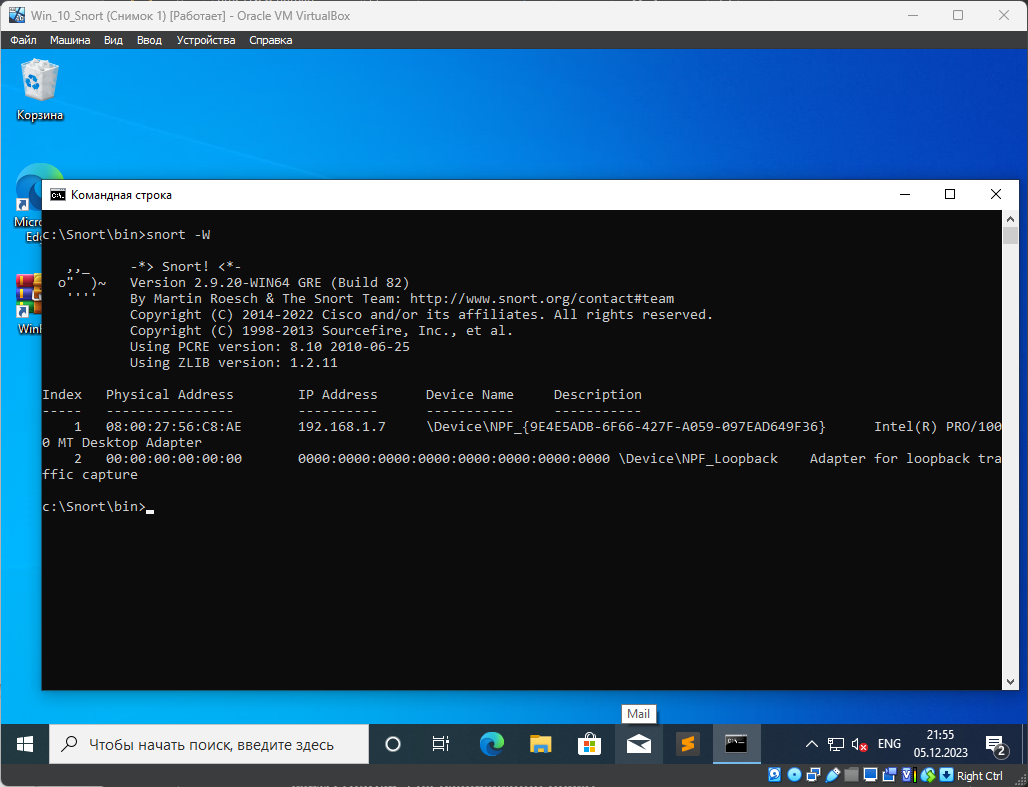
Также отредактируем пункт, касающийся подключения правил для IDS Snort. Удалим строки 548-651 и получим следующую картинку:



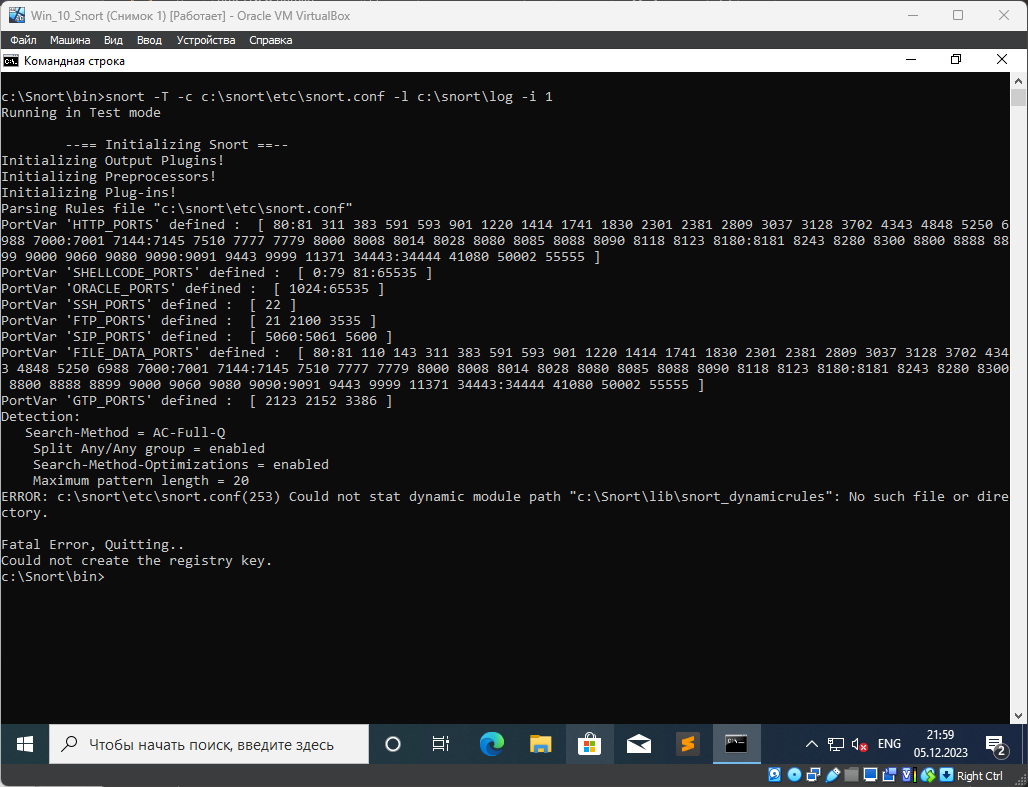
Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку C:/Snort/bin используя командную строку и выводим версию IDS Snort:



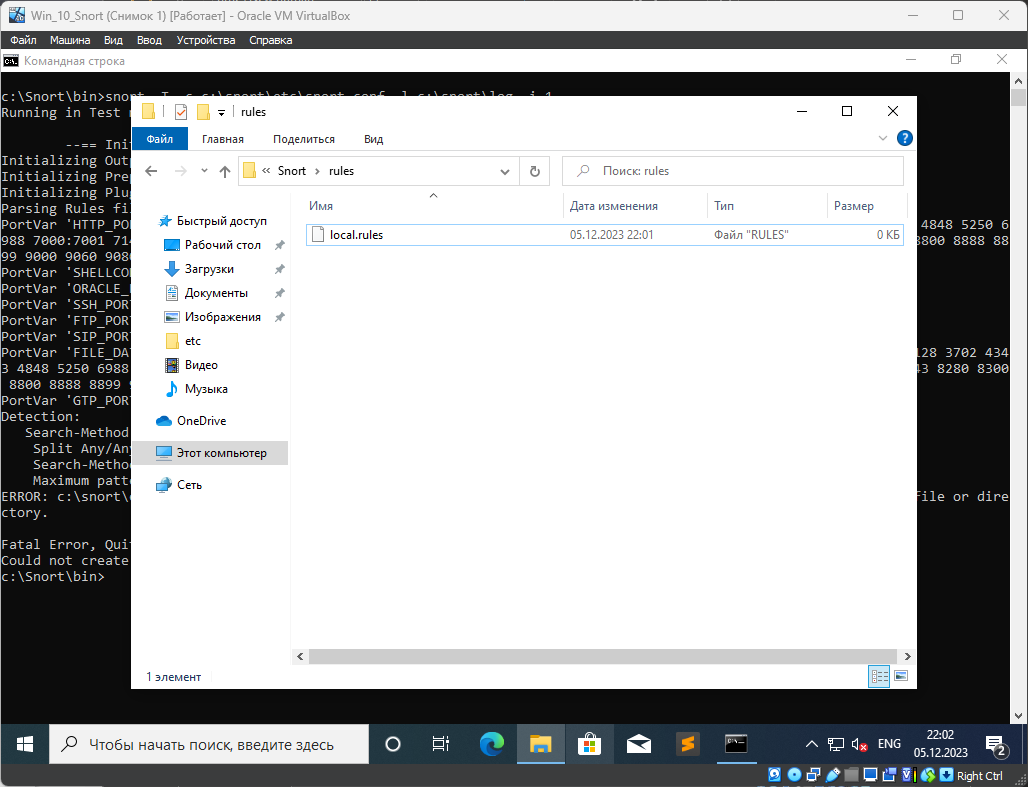
Просмотрим доступные интерфейсы. В данном случае наиболее подходящим для тестирования является интерфейс сетевой карты (номер 1 на изображении ниже):

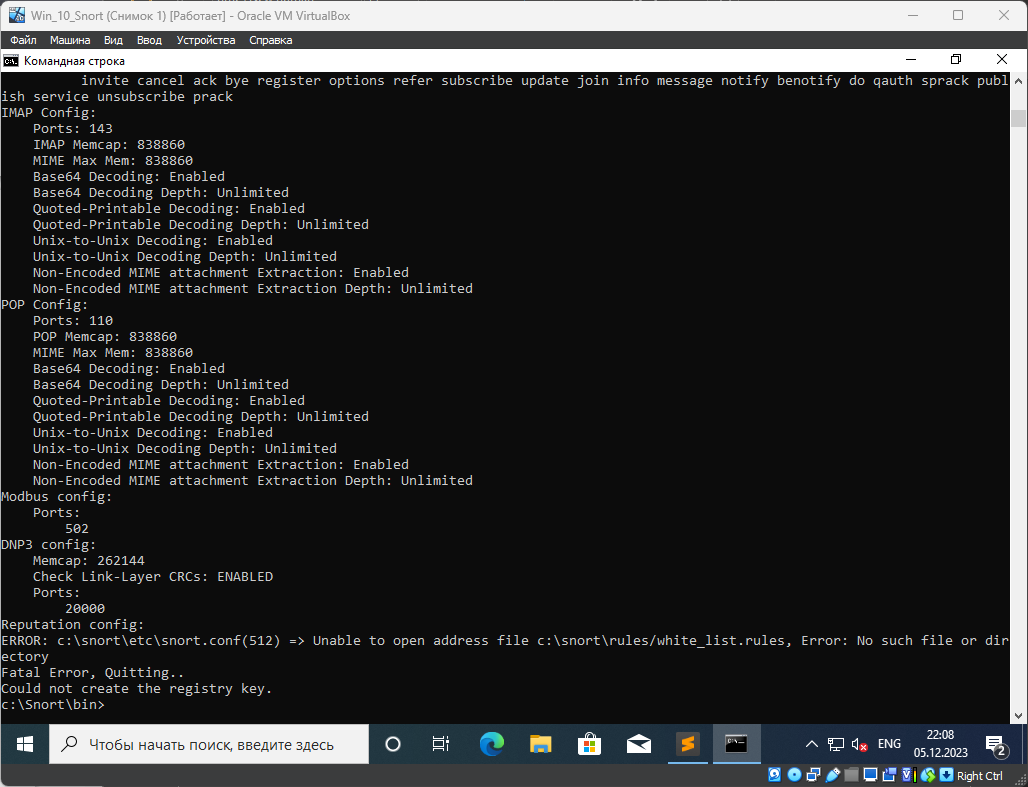


Тестируем конфигурацию Snort, вводим команду: snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 1, где ключ -T указывает, что нужно протестировать текущую конфигурацию Snort; ключ -с означает, что включён режим IDS (далее следует путь к конфигурационному файлу snort.conf); ключ -l включает режим записи на жесткий диск с указанием пути к файлу; ключ -i указывает на порядковый номер(index) интересующего нас интерфейса. Тестирование завершено ошибкой, которая указывает на отсутствие файла local.rules:

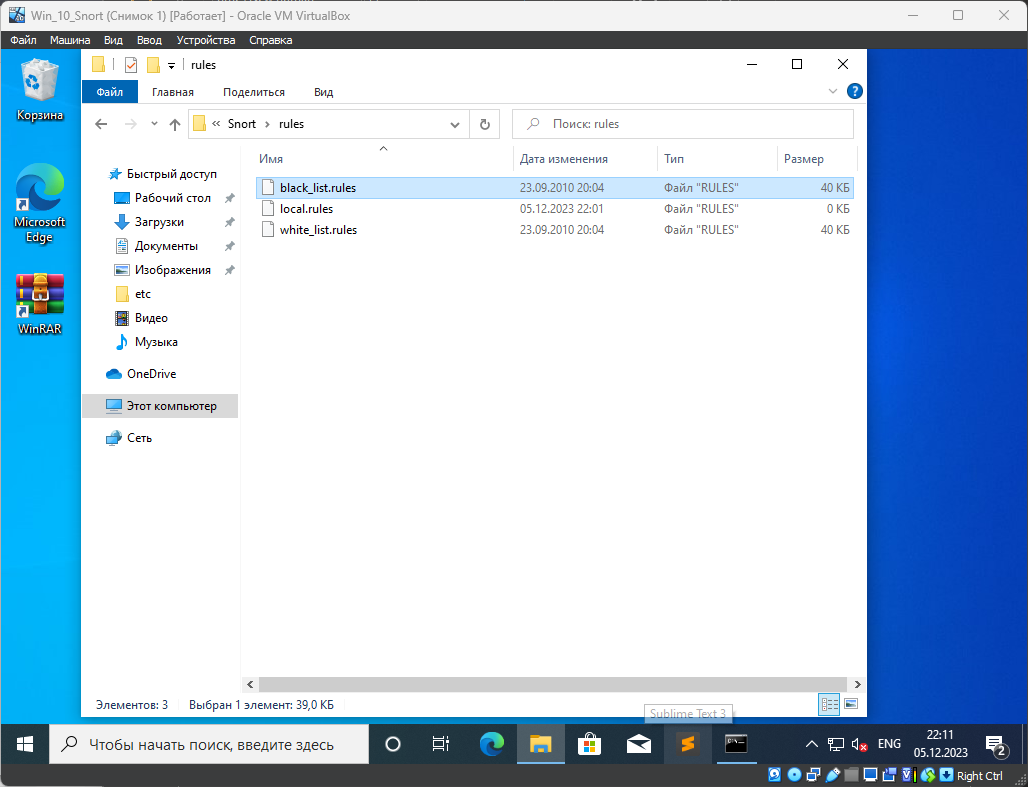


Исправим ошибку. Для этого добавим файл local.rules в папку C:\Snort\rules и снова запустим тестирование:

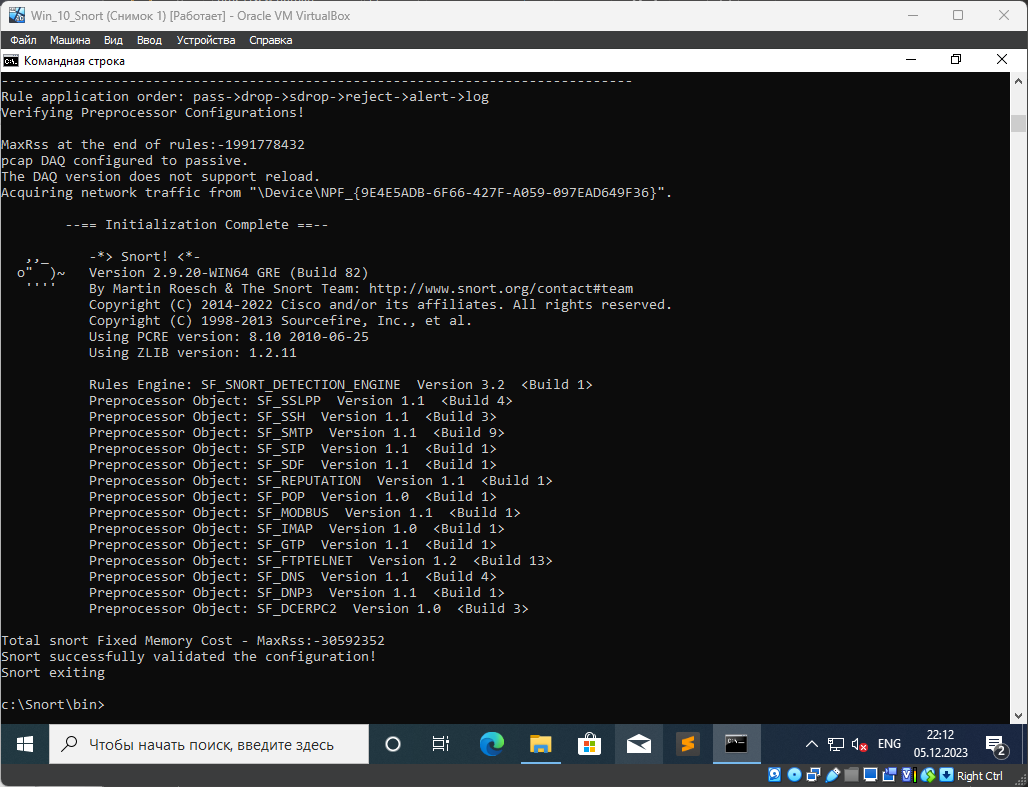




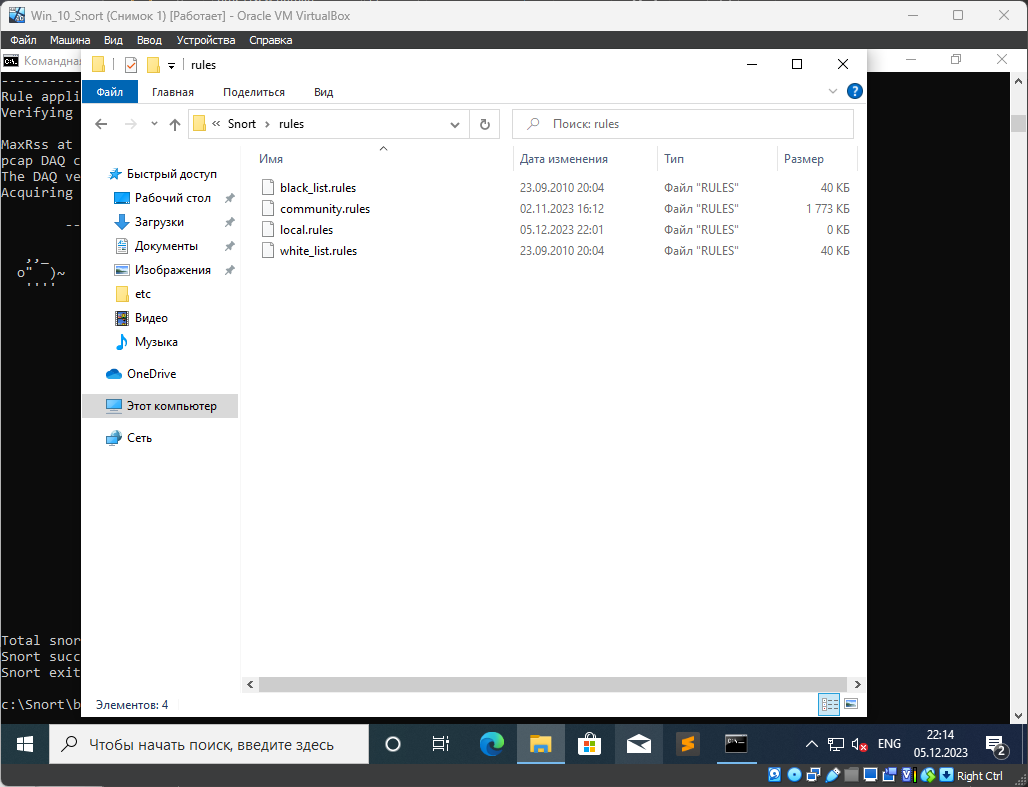
Увидим, что тестирование снова завершено ошибкой, которая указывает на отсутствие файла white\_list.rules. Исправим её. Сразу же добавим и файл black\_list.rules:



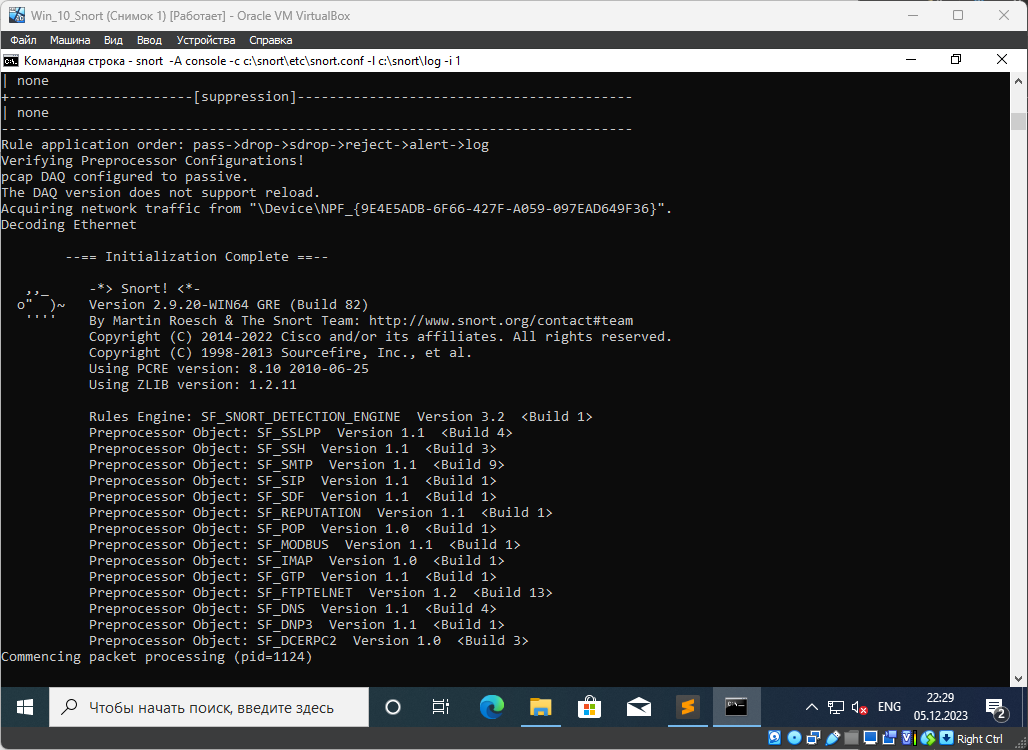
Снова запустим тест и убедимся, что ошибок нет:



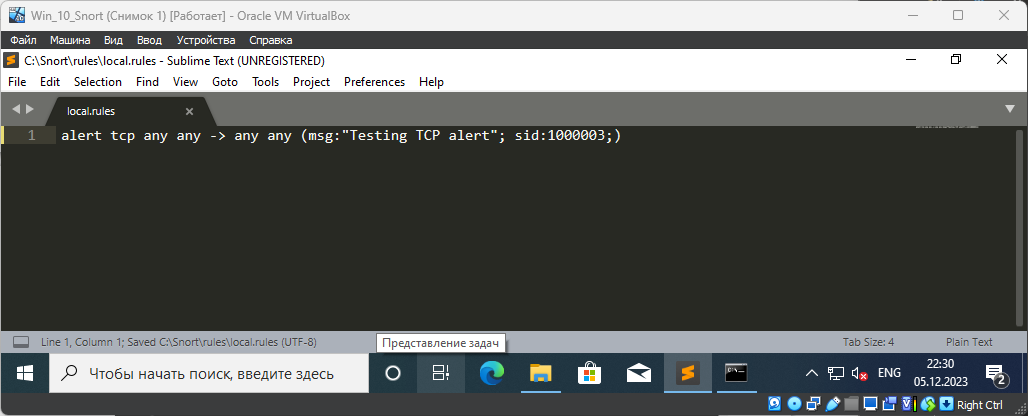
Теперь добавим ещё один файл с правилами community.rules:



Запускаем Snort в режиме IDS, введя данную команду в командной строке: snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 1. Новый ключ “-A” показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль. Snort проверил файл конфигурации и начал свою работу в режиме IDS:



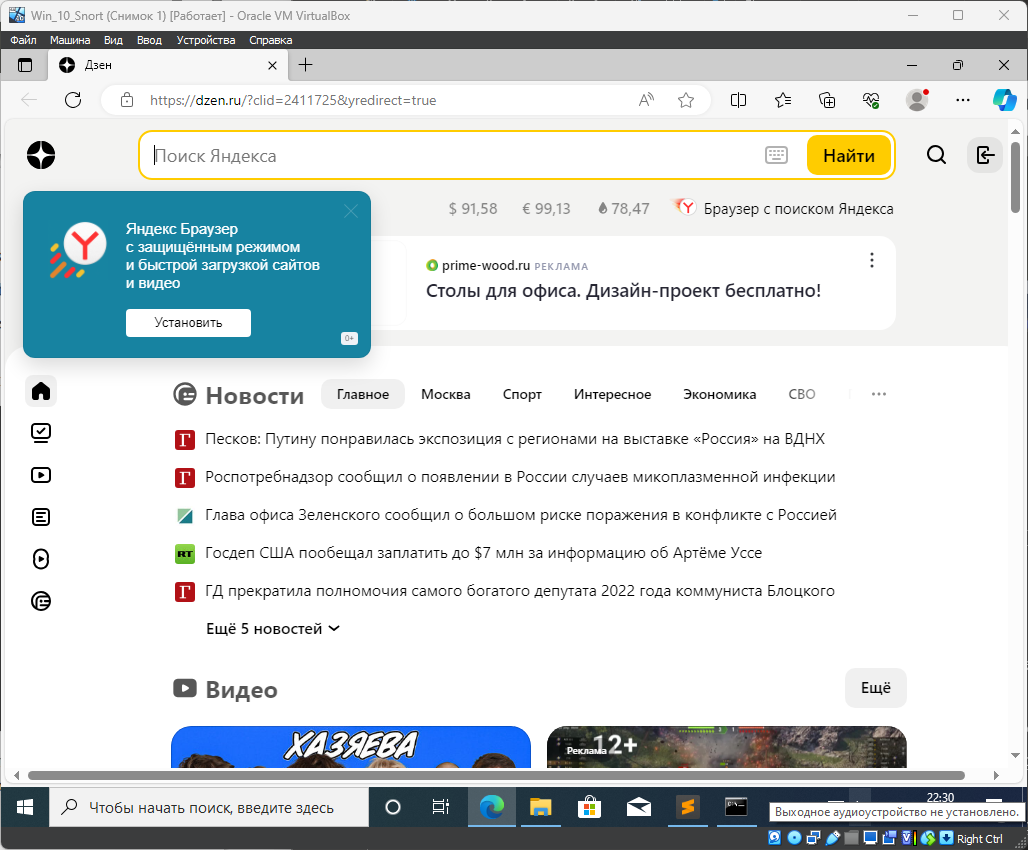
Теперь напишем правило (отредактируем файл local.rules), которое позволит генерировать предупреждение при обнаружении любых TCP пакетов от любого источника к любому назначению, с сообщением 'Testing TCP alert' и идентификатором сигнала 1000003:

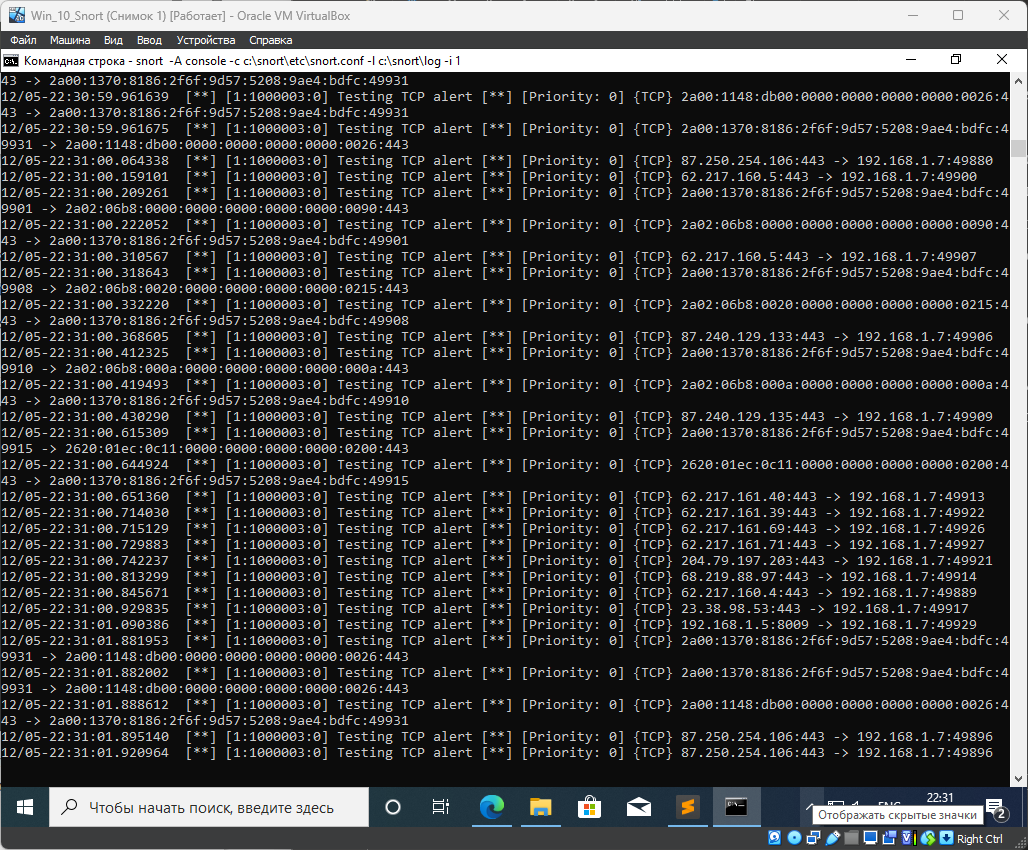


Поясним записи:

* аlert – это действие, которое предписывает системе генерировать предупреждение при срабатывании данного правила;
* tcp – это протокол, к которому применяется правило, в данном случае, это TCP (Transmission Control Protocol), один из основных протоколов передачи данных интернета;
* первая запись “any any” – эти части указывают исходный IP-адрес и порт отправителя ("any" означает "любой", то есть правило применяется ко всем исходящим IP-адресам и портам);
* – эта часть разделяет данные об исходе (source) и данных о назначении (destination);
* вторая запись “any any” – эти части указывают на IP-адрес и порт назначения;
* (msg:"Testing TCP alert"; sid:1000003;) – это дополнительная информация к правилу. Здесь msg указывает на сообщение или описание правила, в данном случае, это "Testing TCP alert". Идентификатор сигнала sid представляет собой уникальный числовой идентификатор этого правила в рамках системы IDS/IPS.

Снова запускаем Snort в режиме IDS, введя данную команду в командной строке: snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 1. Для проверки работы данного правила выйдем в сеть интернет и перейти по любому адресу, после этого в командной строке появится уведомление о срабатывании данного правила:



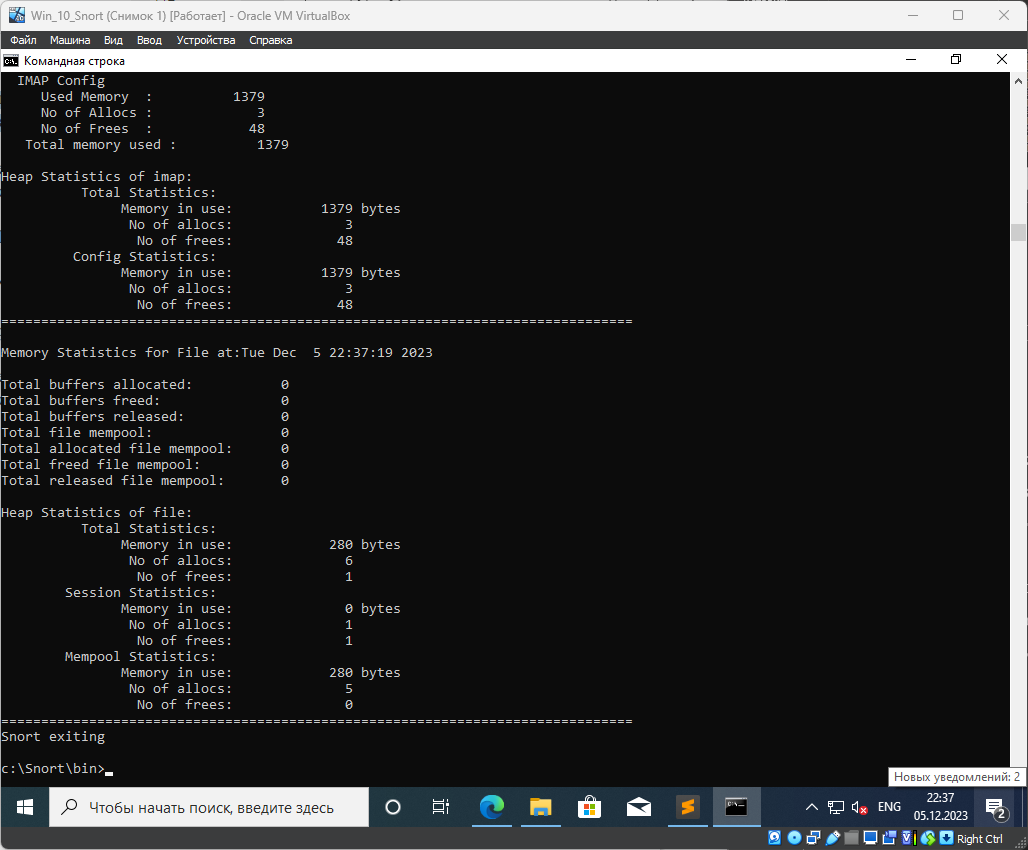


**Вопрос 2. Разработка правил для IDS Snort**

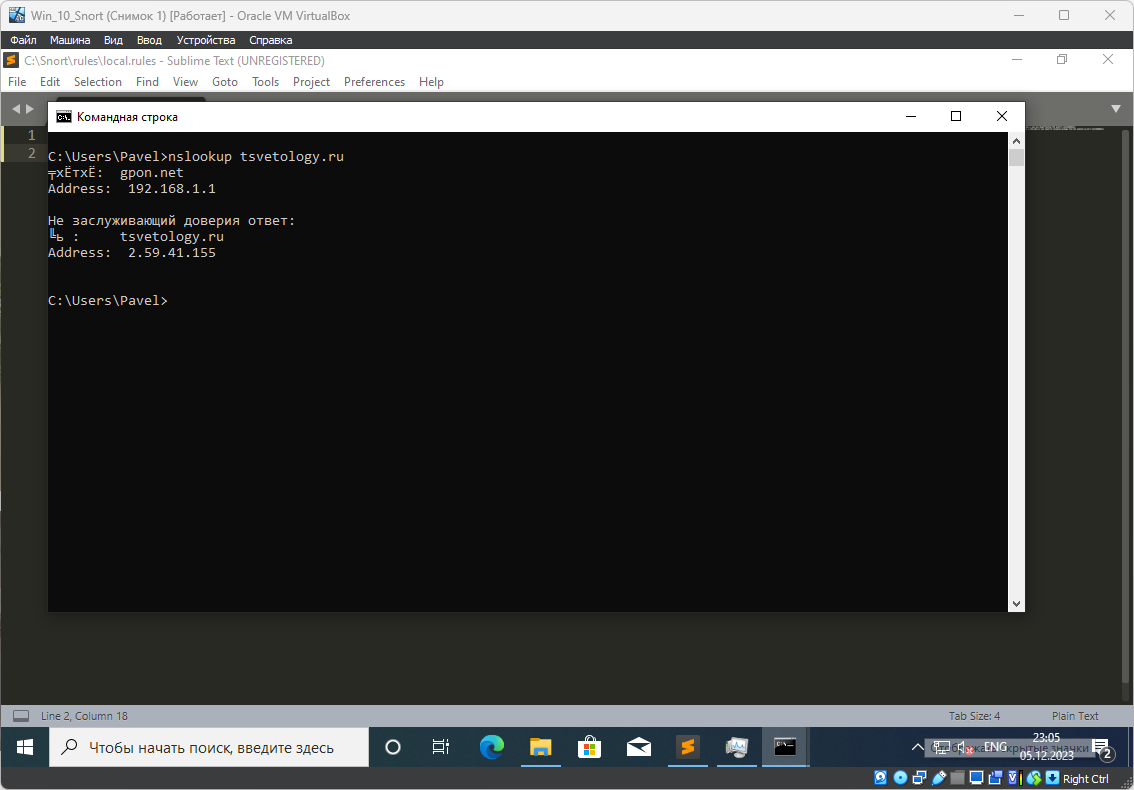
Номер строки с фамилией в файле равен 4, если поделить 4 на 10 (количество заданий), то остаток будет равен 4. Прибавляем к 4 единицу и получаем номер варианта = 5.

Таким образом, необходимо создать правило для Snort, которое срабатывает при обнаружении всех входящих tcp-пакетов с конкретного сайта с выводом соответствующего сообщения.

Прервём работу IDS Snort комбинацией клавиш “Сtrl+c”:



Предположим, мы хотим получать уведомления о входящих tcp-пакетах с сайта <https://tsvetology.ru>. Сперва узнаем какой ip-адреса резолвится (это можно сделать с помощью утилиты nslookup):



Теперь напишем правило (указан 443 порт, т.к. используется протокол https; 192.168.1.7 – это адрес, где установлен IDS Snort):



Снова запустим IDS Snort, перейдём на сайт <https://tsvetology.ru> и увидим оповещения:

