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

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

**Отчет**

по практической работе на тему: Настройка параметров системы обнаружения атак

**по дисциплине:**

«Управление информационной безопасностью»

**Выполнил:**

Студент группы ББМО-02-22

ФИО: Давыдов И.Д.

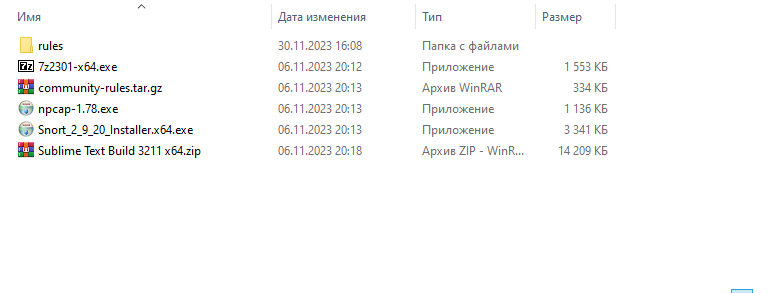
**Проверил:**

Р.В. Пимонов

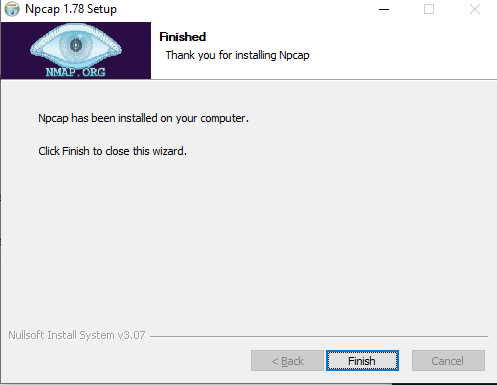
**Москва 2024**

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

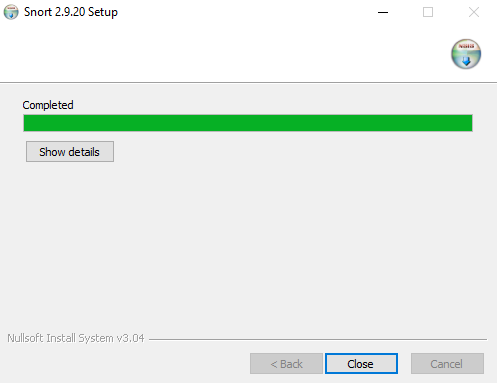
Перед выполнением задания скачаем архив с требующимся ПО по ссылке: <https://1drv.m/u/s!AlN4iiJAxsjbgVMVo5Ha-52vbvT9?e=YbZNad>. Разархивируем его и посмотрим его содержимое:



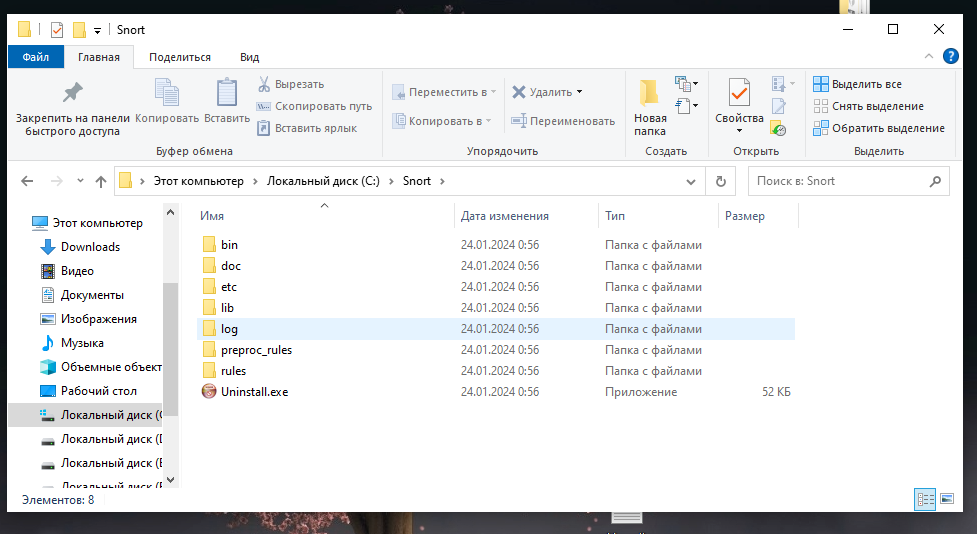
Выполним установку npcap:



Выполним установку IDS Snort:

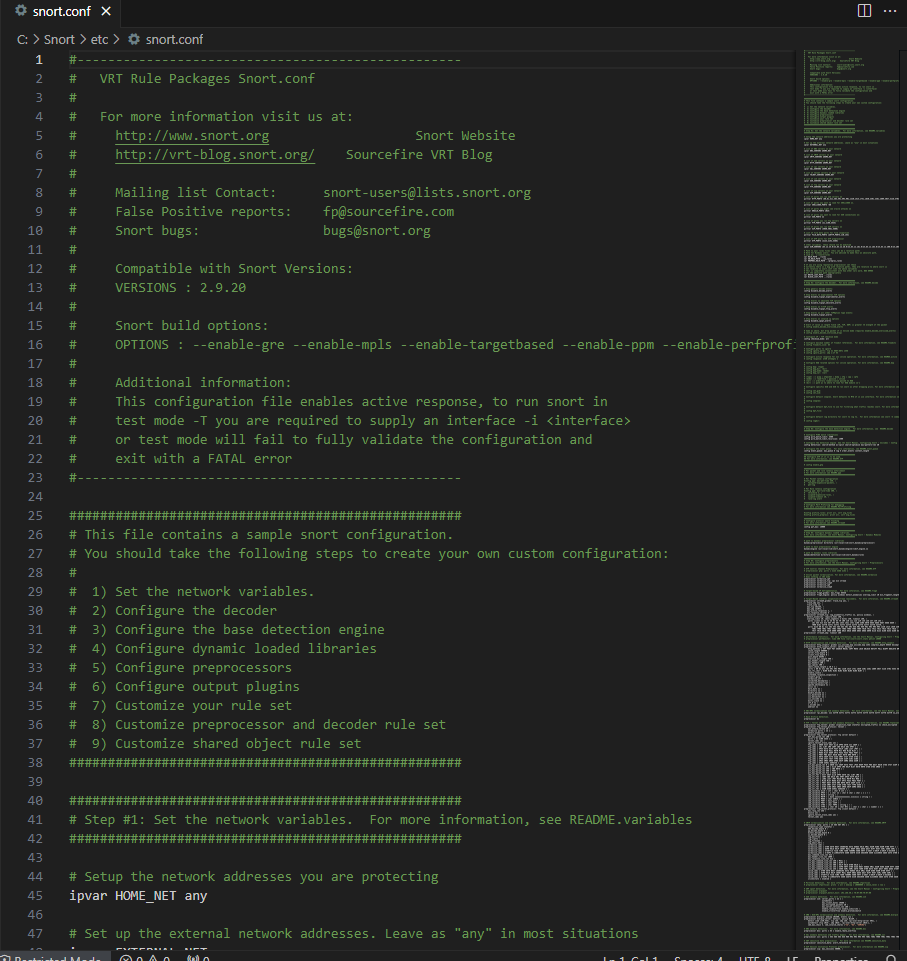


После установки в диске C:/ появится папка с файлами программы:

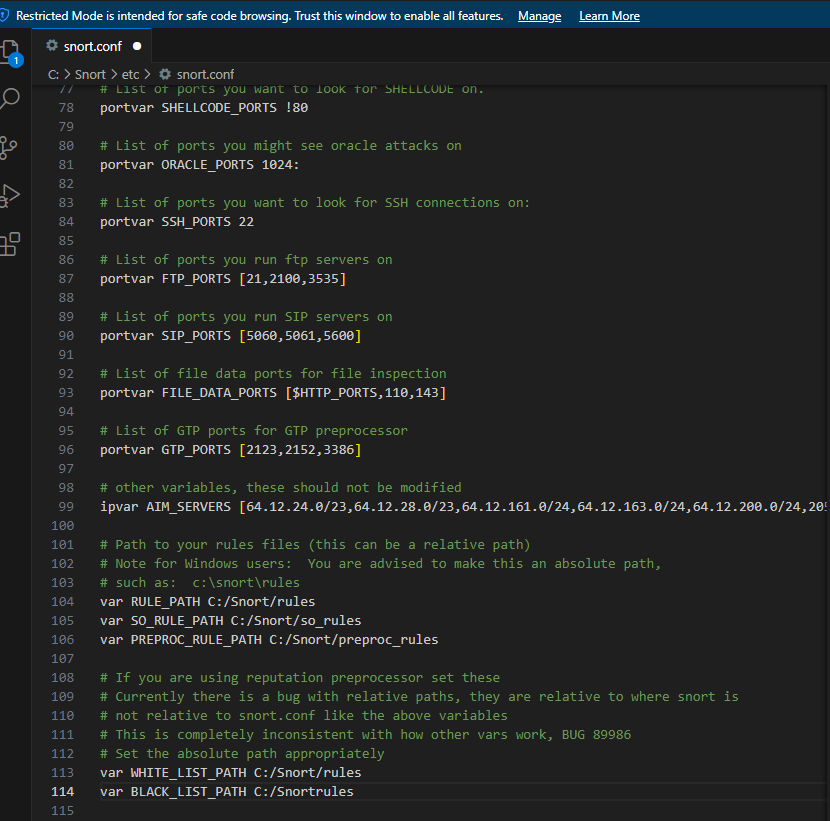


После перехода в директорию C:/Snort в первую очередь необходимо настроить файл конфигурации для его успешной работы.

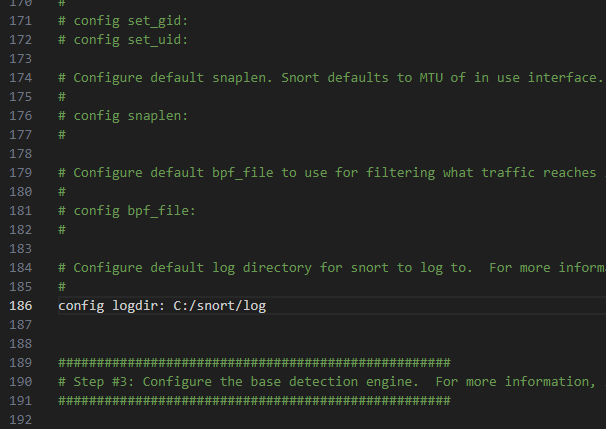
Для настройки этого файла необходимо перейти в директорию C:/Snort/etc и открыть файл snort.conf, сделать это можно, например в текстовом редакторе Sublime Text или VS Code. Дальнейшие операции по редактированию конфигурационных файлов будут производится с помощью VS code. Откроем файл C:/Snort/etc/snort.conf:



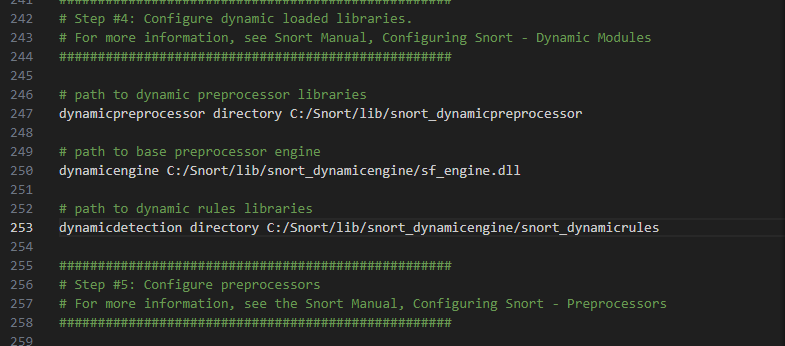
Зададим корректный пусть в строках 104-106, 113-114:



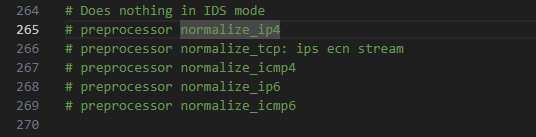
Теперь необходимо указать путь для папки Log-файлов, куда Snort будет записывать все логи, доступные для просмотра и изучения. Отредактируем 186 строку:



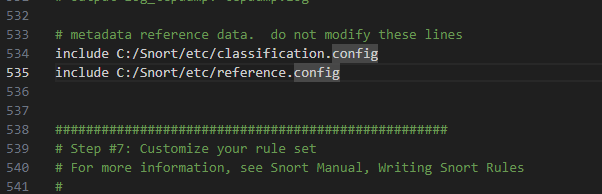
Далее отредактируем строки 247, 250, 253:



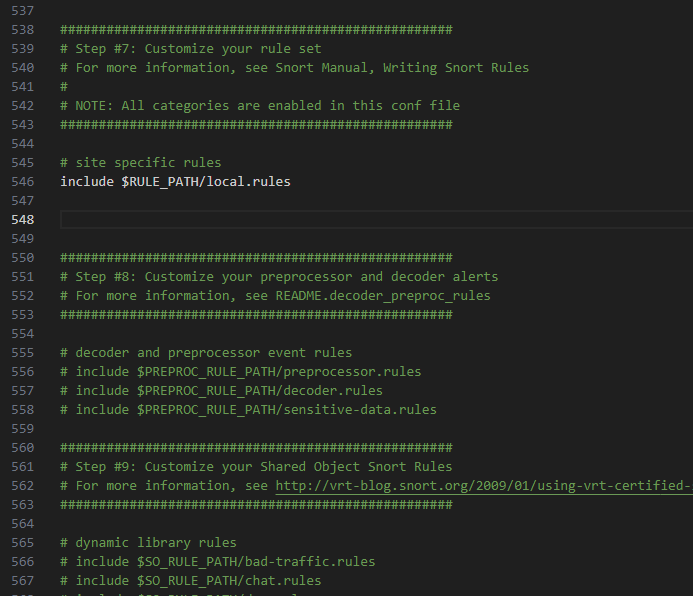
Закомментируем строки 265-269:



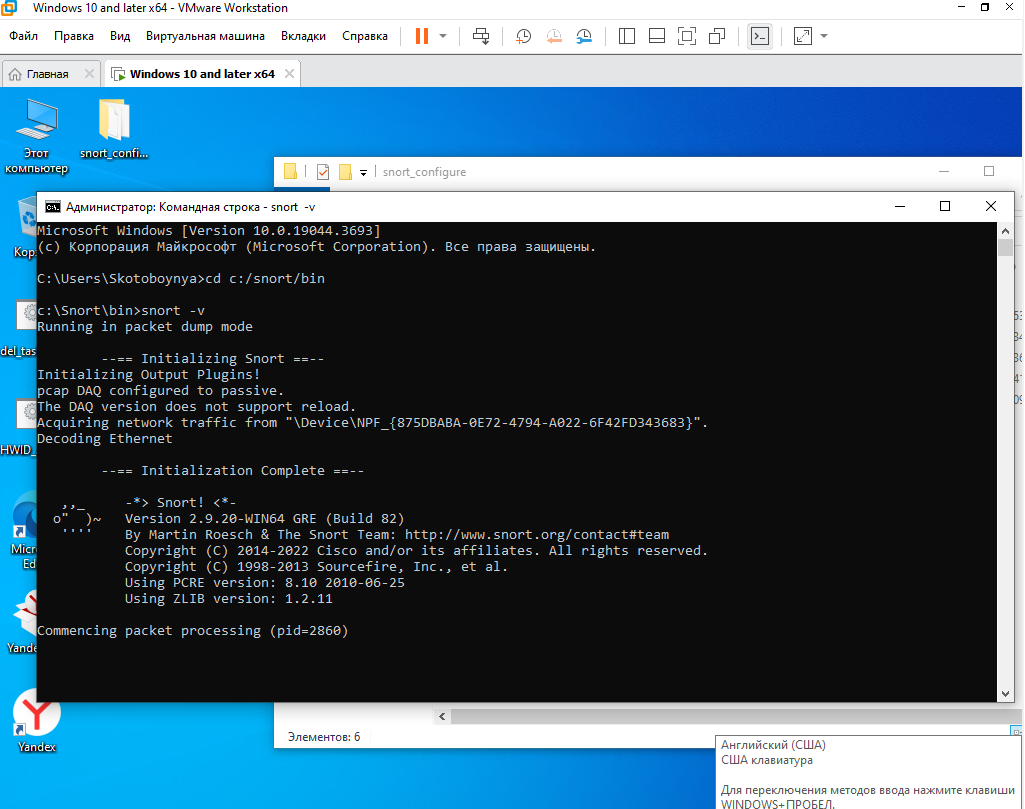
Отредактируем строки 534-535:



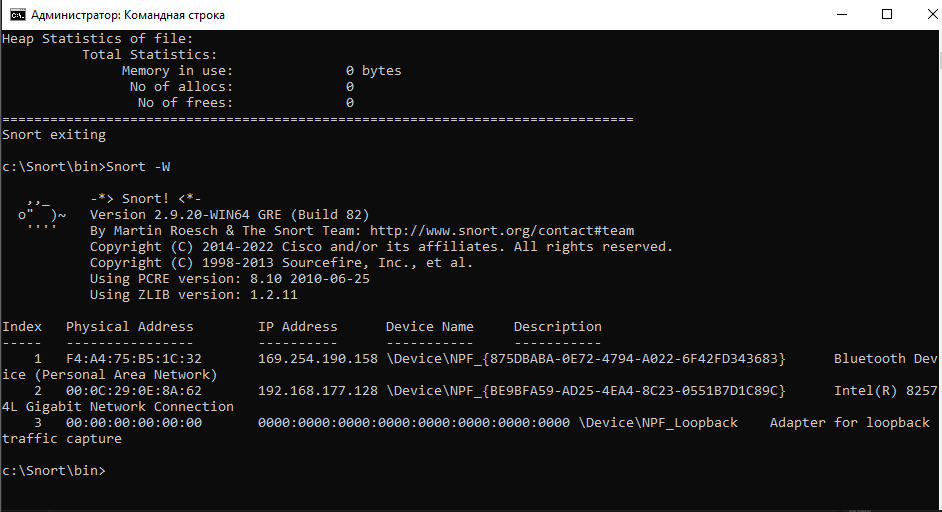
Также отредактируем пункт, касающийся подключения правил для IDS Snort. Удалим строки 548-651 и получим следующую картинку:



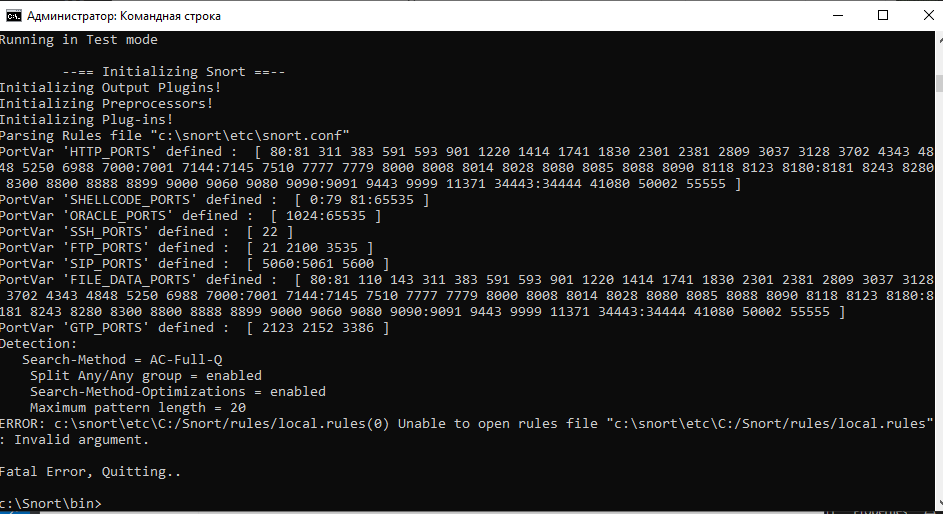
Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку C:/Snort/bin используя командную строку и выводим версию IDS Snort:



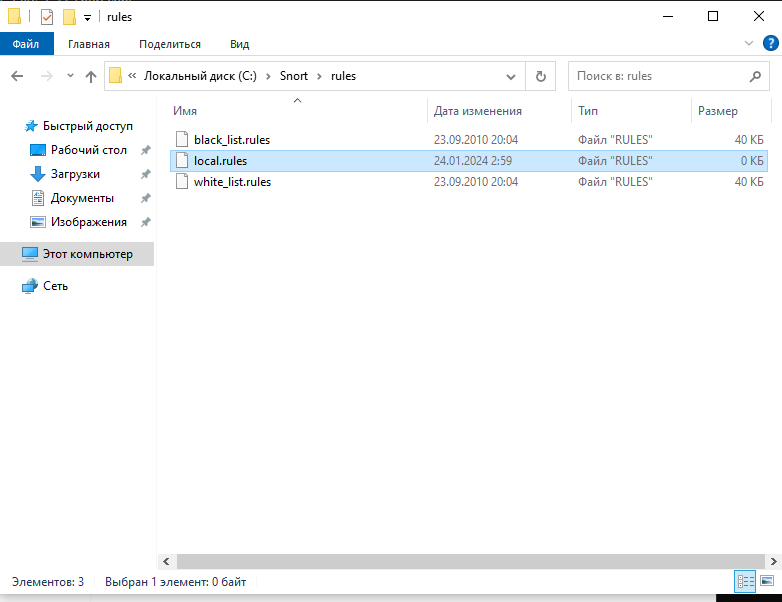
Просмотрим доступные интерфейсы. В данном случае наиболее подходящим для тестирования является интерфейс сетевой карты (номер 2 на изображении ниже):



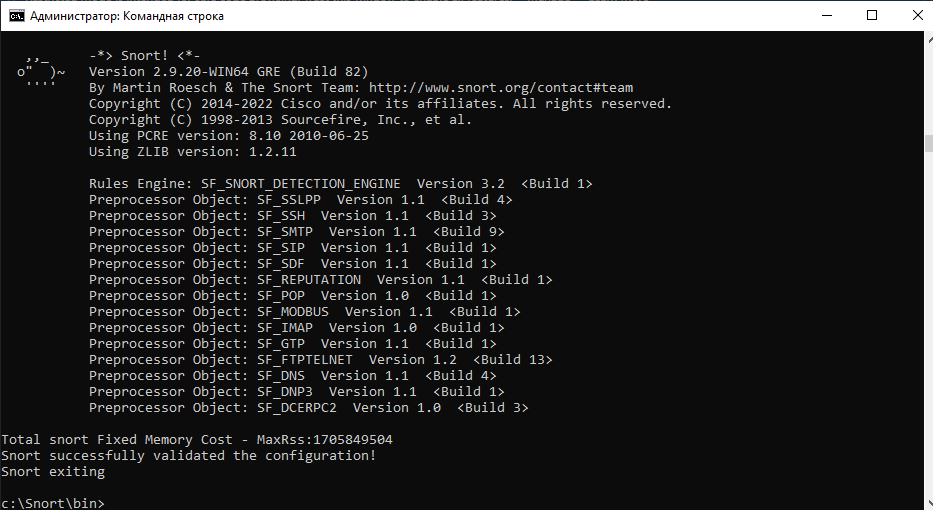
Тестируем конфигурацию Snort, вводим команду: snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2, где ключ -T указывает, что нужно протестировать текущую конфигурацию Snort; ключ -с означает, что включён режим IDS (далее следует путь к конфигурационному файлу snort.conf); ключ -l включает режим 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:



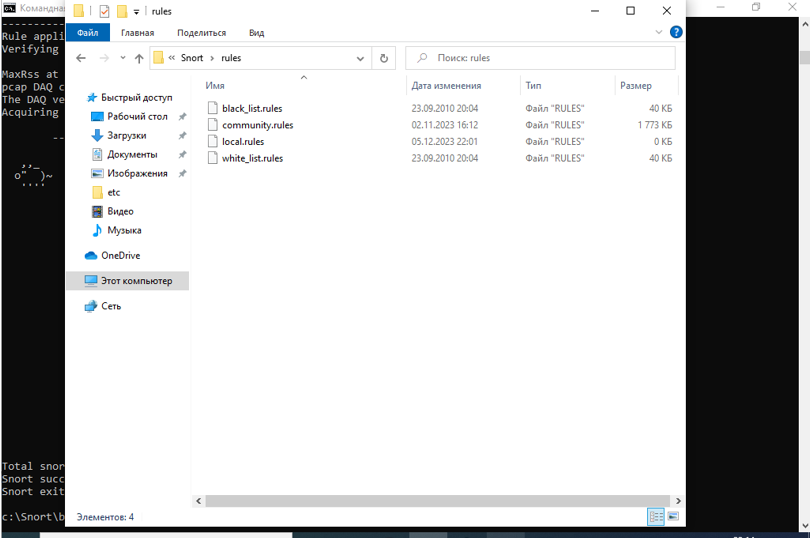
Исправим ошибку. Для этого добавим файл local.rules в папку C:\Snort\rules. Сразу же добавим и файлы black\_list.rules, white\_list.rules и снова запустим тестирование:



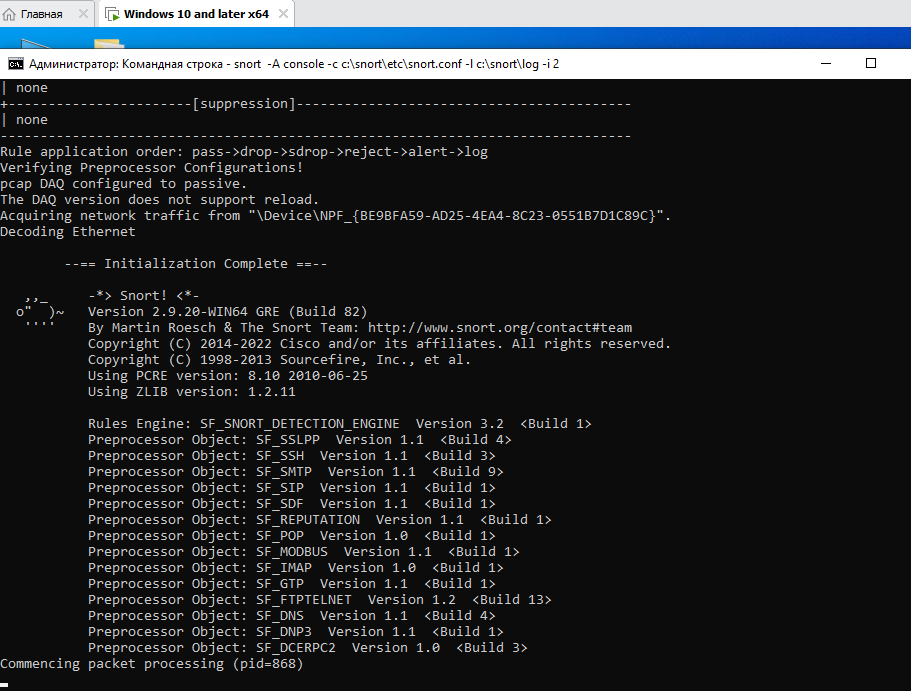
Снова запустим тест и убедимся, что ошибок нет:



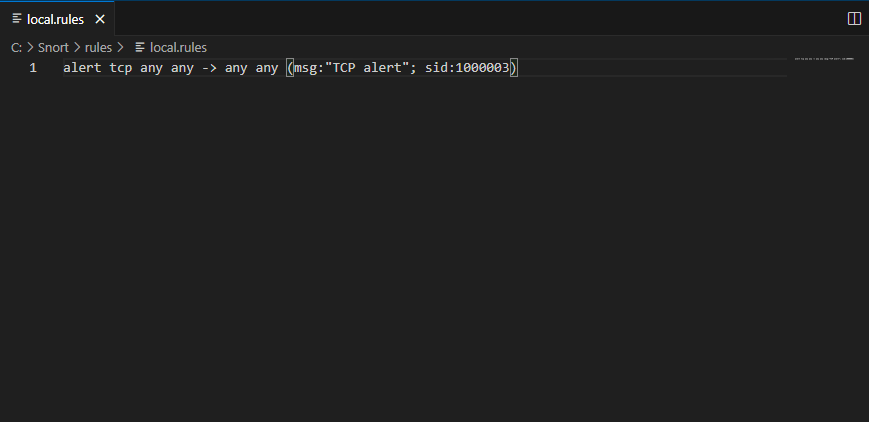
Теперь добавим ещё один файл с правилами community.rules:



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 2. Новый ключ “-A” показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль. Snort проверил файл конфигурации и начал свою работу в режиме IDS:



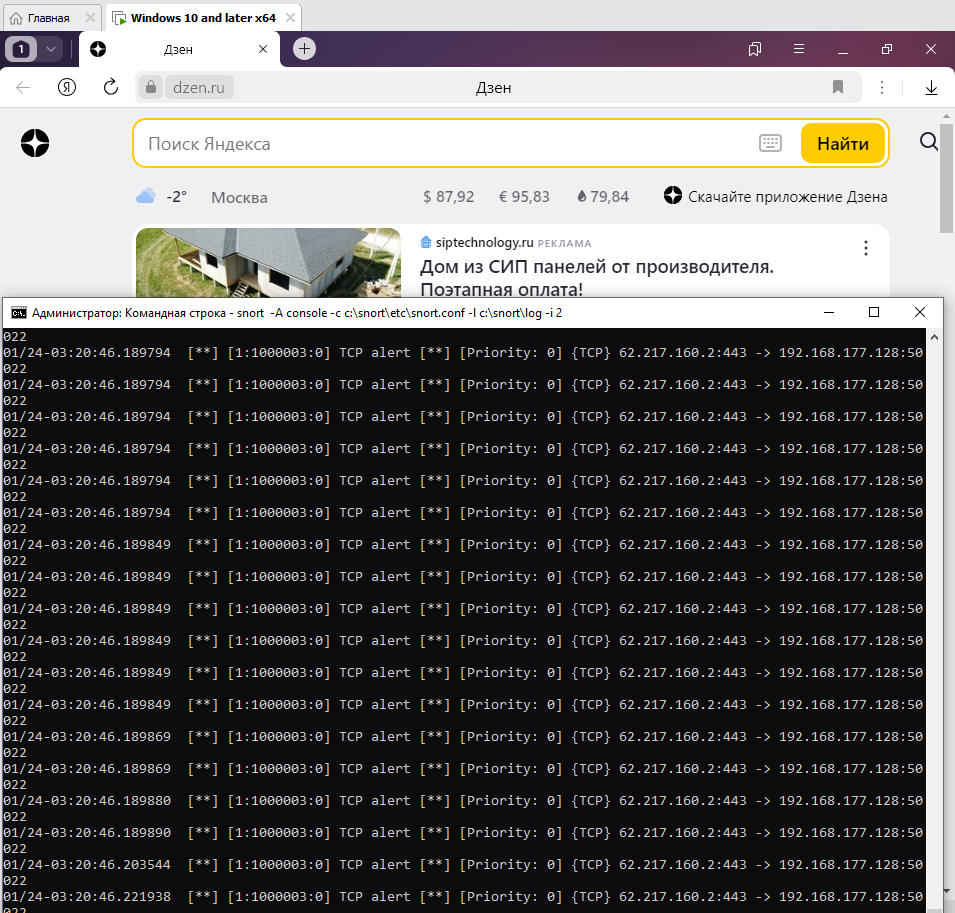
Теперь напишем правило (отредактируем файл local.rules), которое позволит генерировать предупреждение при обнаружении любых TCP пакетов от любого источника к любому назначению, с сообщением 'Testing TCP alert' и идентификатором сигнала 1000003:



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.

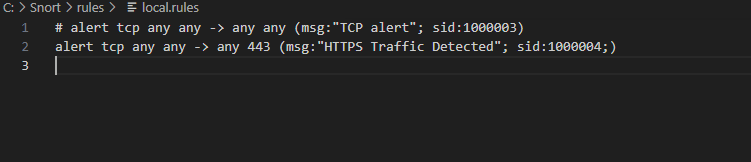
Снова запускаем Snort в режиме IDS, введя данную команду в командной строке: snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 2. Для проверки работы данного правила выйдем в сеть интернет и перейти по любому адресу, после этого в командной строке появится уведомление о срабатывании данного правила:



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

Номер строки с фамилией в файле равен 36, если поделить 36 на 10 (количество заданий), то остаток будет равен 6. Прибавляем к 6 единицу и получаем номер варианта = 7.

Таким образом, необходимо создать правило для Snort, которое срабатывает при обнаружении HTTPS-трафика.



* alert - указывает, что правило выполняется при обнаружении события.
* tcp any any -> any 443 - указывает, что правило применяется к TCP-пакетам на любых адресах и портах отправителя и получателя, где получатель имеет порт 443 (стандартный порт HTTPS).
* msg:"HTTPS Traffic Detected" - задает сообщение, которое будет выведено при срабатывании правила.

- определяет содержимое пакета, на которое будет откликаться правило. В данном случае, это строка "https".

* sid:1000001 - уникальный идентификатор сигнатуры. Можете использовать любой уникальный номер.

Запустим snort и убедимся, что все работает

