|  |
| --- |
|  |
| 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»

**Отчёт по практической работе №2.2**

**по дисциплине «Управление информационной безопасностью»**

Группа:

ББМО-02-23

Выполнил:

Дурягин М.Р.

Москва, 2024

Содержание

[Введение 3](#_gjdgxs)

[Вопрос 1. Установка и настройка параметров IDS Snort 3](#_30j0zll)

[Вопрос 2. Разработка правил для IDS Snort 14](#_1fob9te)

[Заключение 16](#_2et92p0)

# Введение

**Цель работы:** Настройка параметров системы обнаружения атак.

**Задачи:**

**-** Установка и настройка параметров IDS Snort.  
- Разработка правил для IDS Snort.

# Вопрос 1. Установка и настройка параметров IDS Snort

Подготовительная часть для работы IDS Snort:

1. Установка npcap-1.78.exe.

Запускаем exe файл и устанавливаем npcap (рис. 1-2).

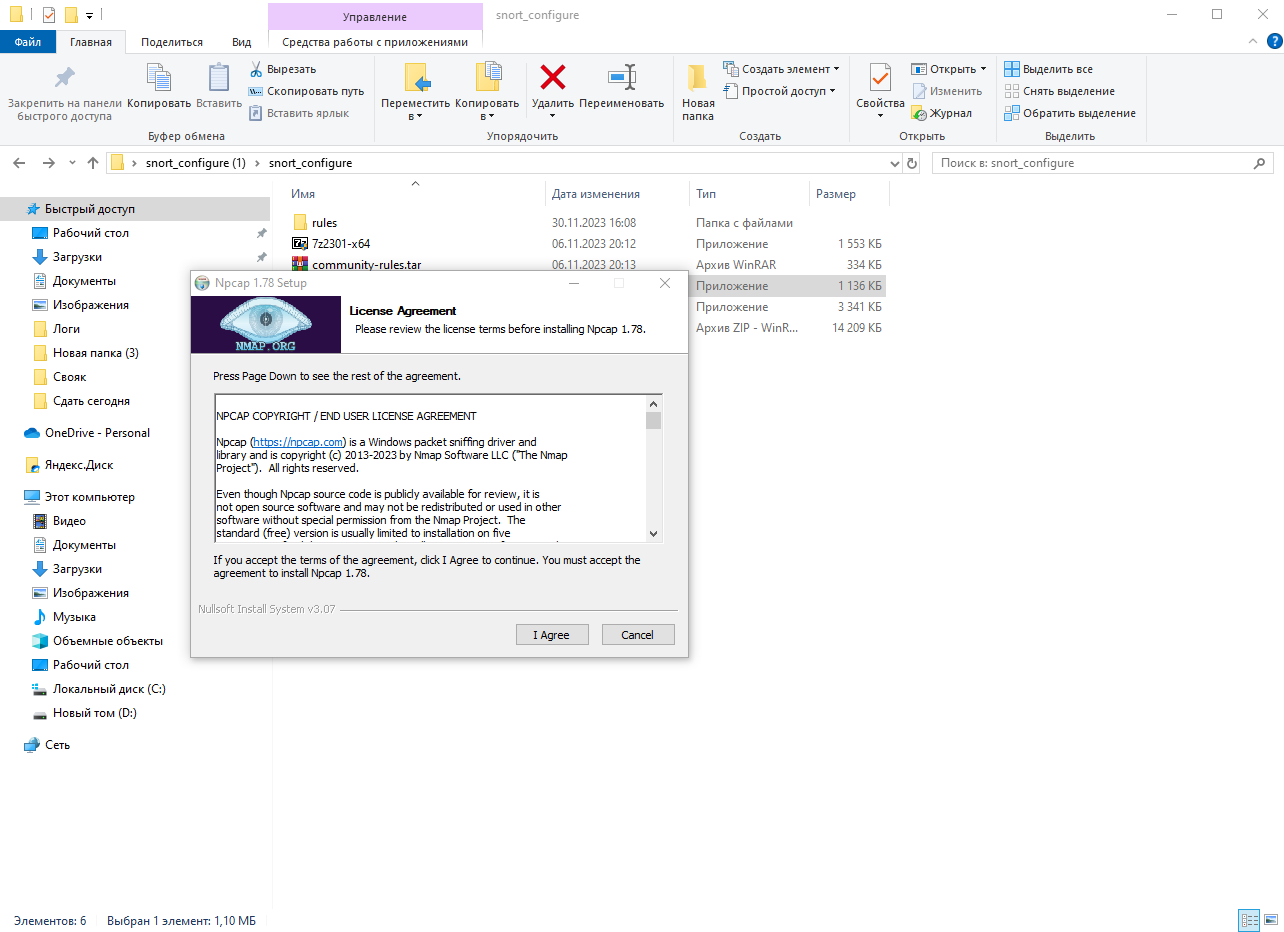


Рисунок 1 – Установка Npcap

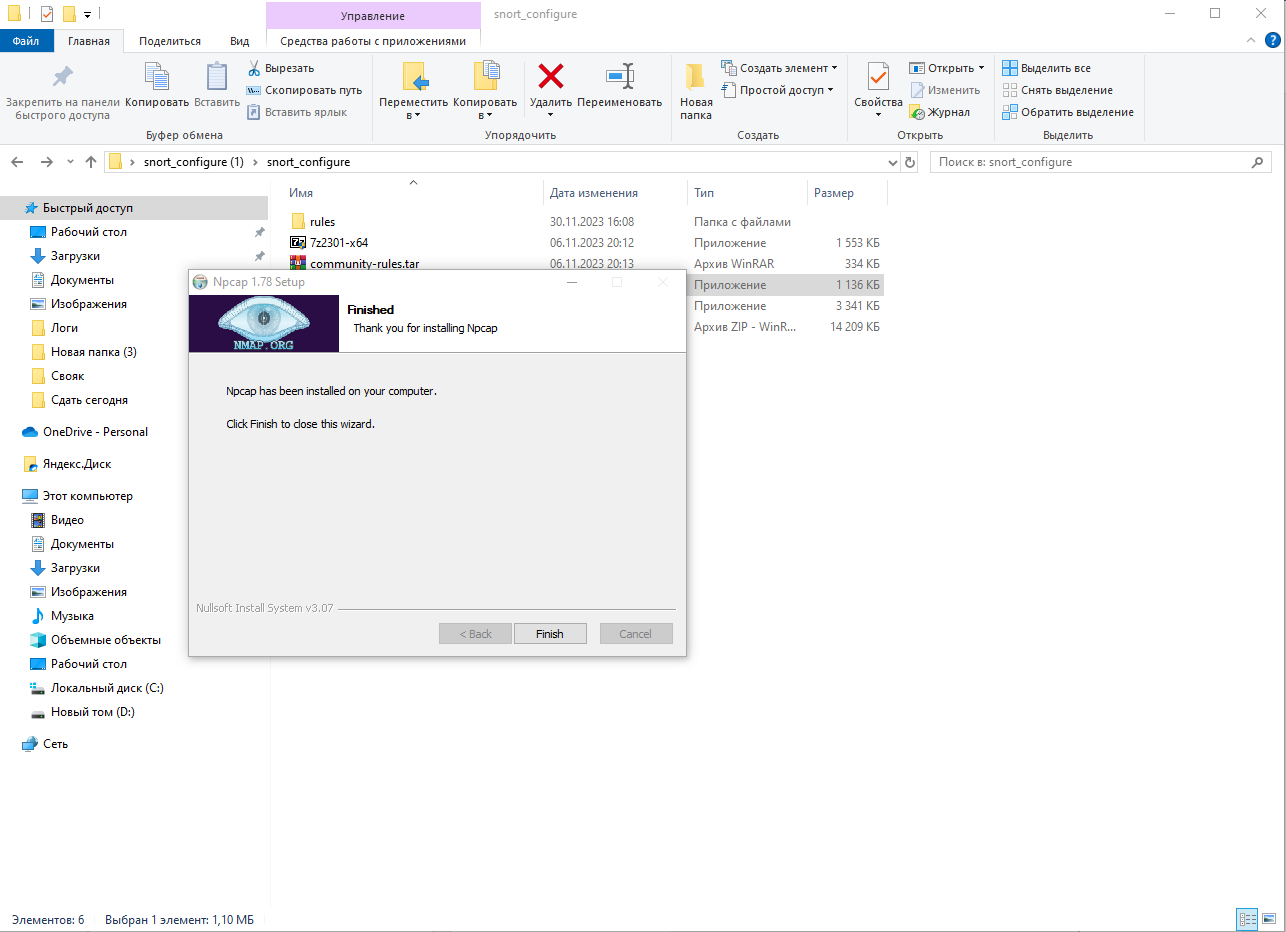


Рисунок 2 – Установка Npcap

2. Установка IDS Snort. Запускаем файл Snort\_2\_9\_20\_Installer.x64.exe и устанавливаем Snort (рис. 3).

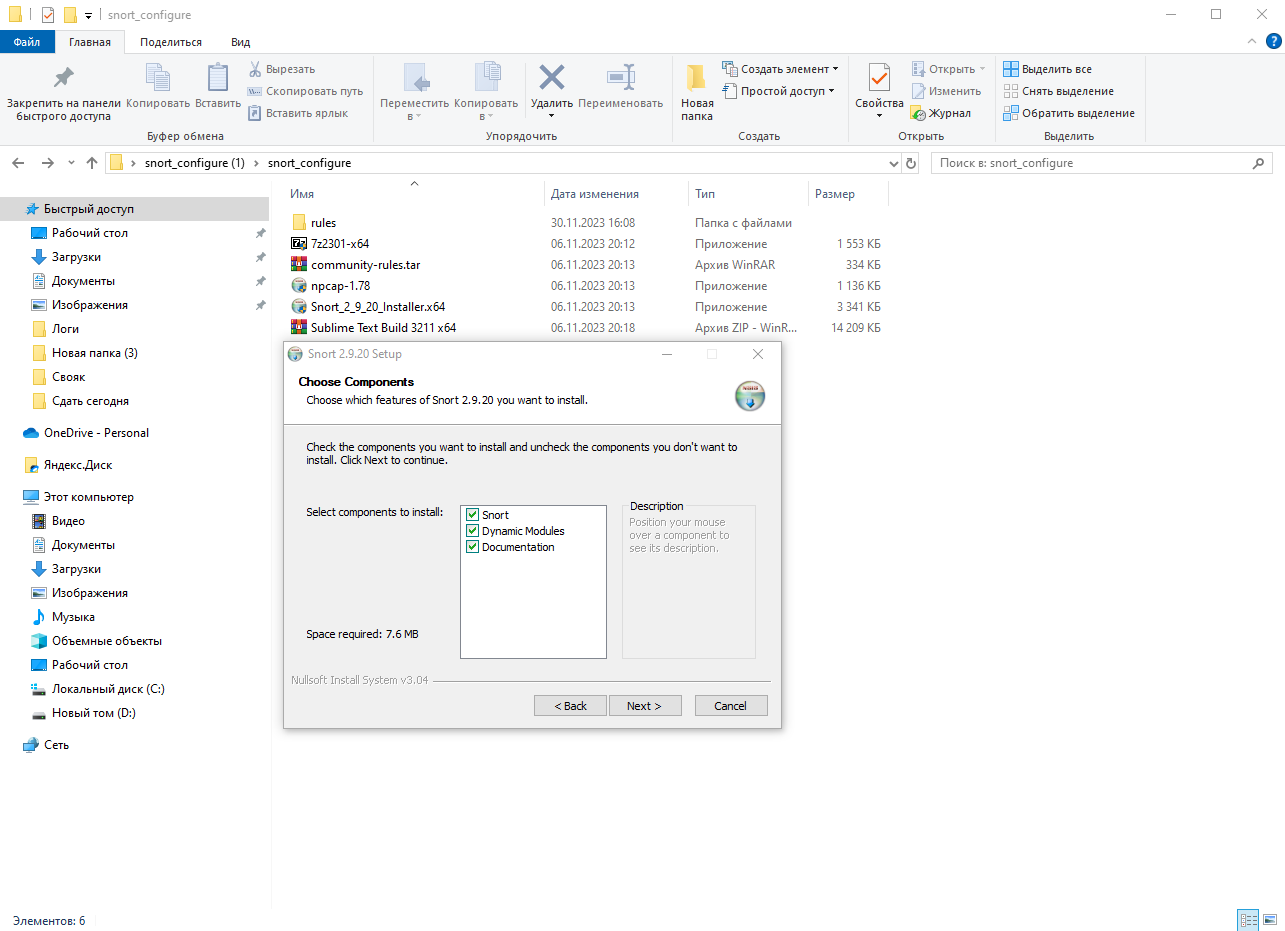


Рисунок 3 – Установка Snort

После установки в диске C:/ появится папка с файлами программы (рис. 4).

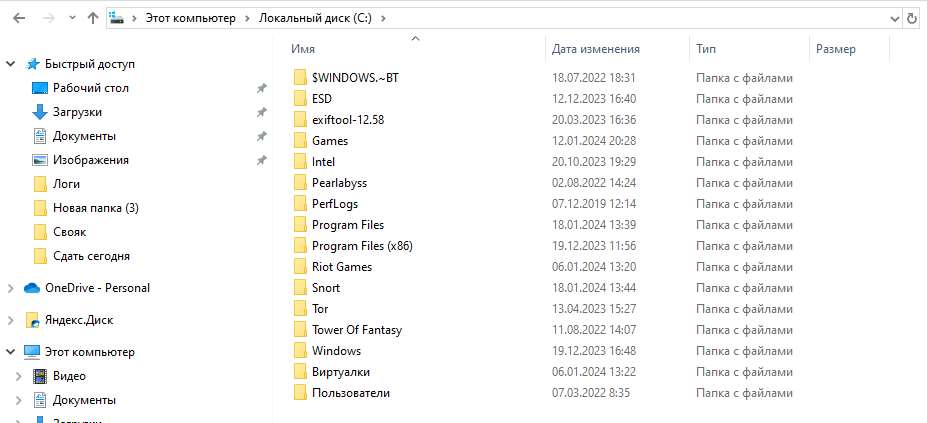


Рисунок 4 – директория Snort

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 (рис. 5).

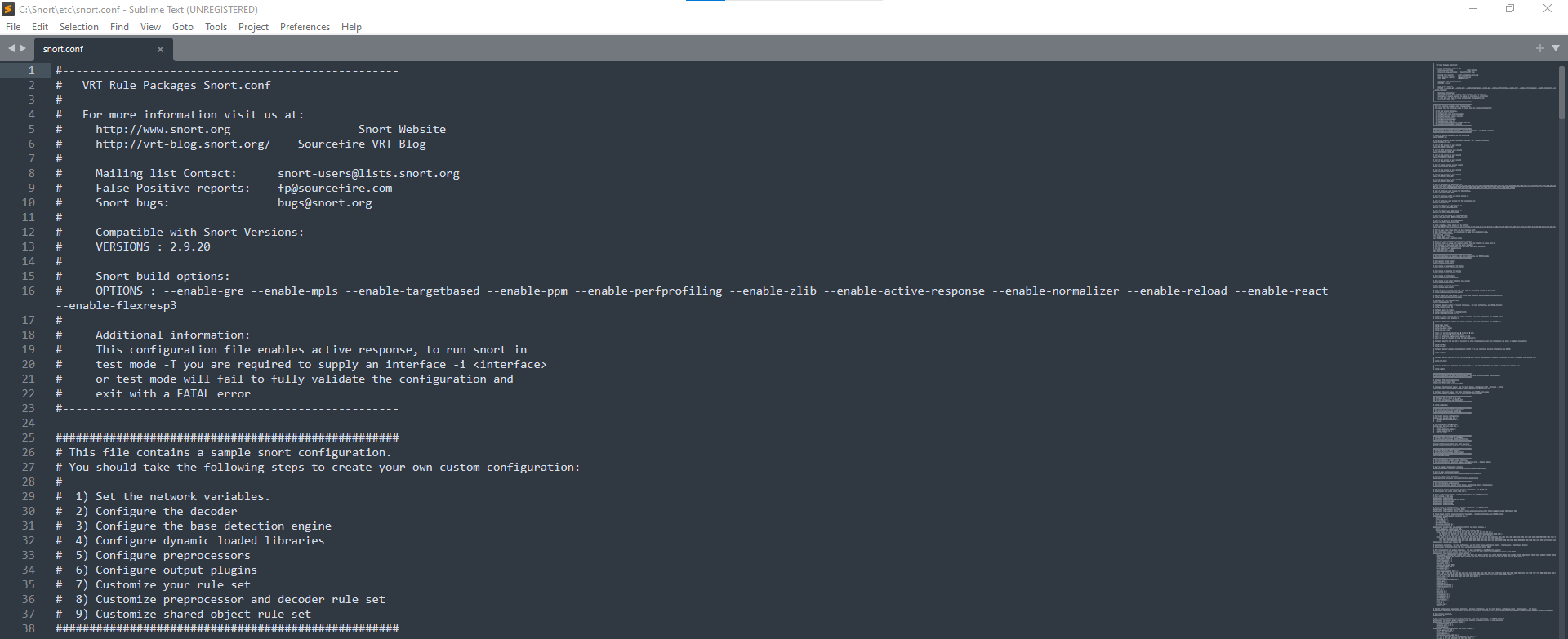


Рисунок 5 – Конфигурационный файл Snort (1)

Переходим к строкам 104-106 и вместо ..\ прописываем c:\snort\.

Тоже самое делаем в строках 113-114 (рис. 6).

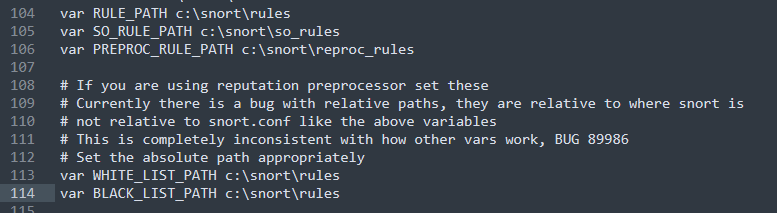


Рисунок 6 – Конфигурационный файл Snort (2)

Теперь необходимо указать путь для папки Log-файлов, куда Snort будет записывать все логи, доступные для просмотра и изучения. Редактируем пути к лог-файлам.

В папке C:/snort уже есть папка log, для этого предназначенная, поэтому прописываем путь C:\snort\log.

На строчке 186 прописываем в config logdir: c:\snort\log. Также необходимо удалить символ " # ", который выбрасывает строки из исполняемого файла, превращая их в комментарий. Результат (рис. 7):

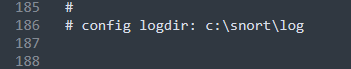


Рисунок 7 – Конфигурационный файл Snort (3)

Строки 246-253 необходимо прописать так, как показано на изображении ниже (рис. 8):

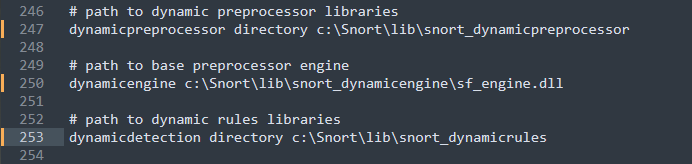


Рисунок 8 – Конфигурационный файл Snort (4)

Продолжаем редактирование. Теперь комментируем, добавляя знаки комментария " # " к строкам 259-265. В отредактированном варианте это выглядит так (рис. 9):

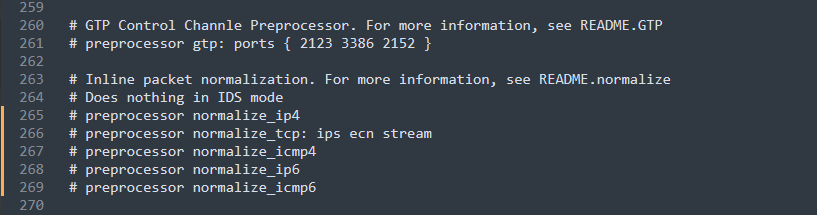


Рисунок 9 – Конфигурационный файл Snort (5)

Также необходимо раcкомментировать строки 534-535, убрав знак # (рис. 10).



Рисунок 10 – Конфигурационный файл Snort (6)

Также отредактируем пункт, касающийся подключения правил для IDS Snort. Удалим строки 548-651 (рис. 11).

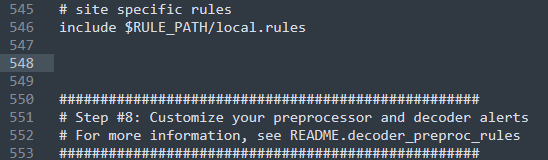


Рисунок 11 – Конфигурационный файл Snort (7)

Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку C:/Snort/bin.

Открываем эту папку в командной строке Windows (сделать это можно нажав на панель, отображающую текущую директорию, ввести в ней cmd и нажать Enter, командная строка откроется сразу в данной папке).

Введем команду snort –V, отображающую текущую версию IDS Snort (рис. 12).

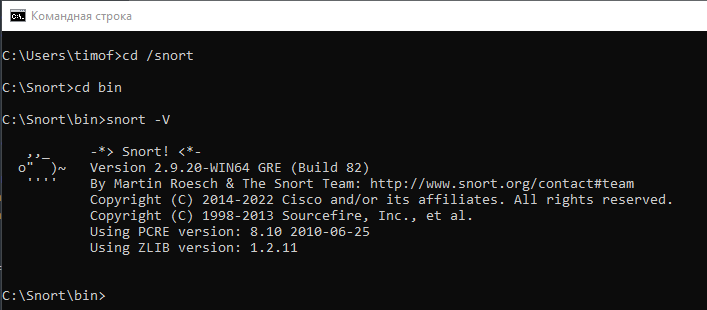


Рисунок 12 – Версия Snort

Просмотрим командой snort –W доступные интерфейсы, в данном случае наиболее подходящим для тестирования является интерфейс сетевой карты (номер 5 на изображении ниже) (рис. 13).

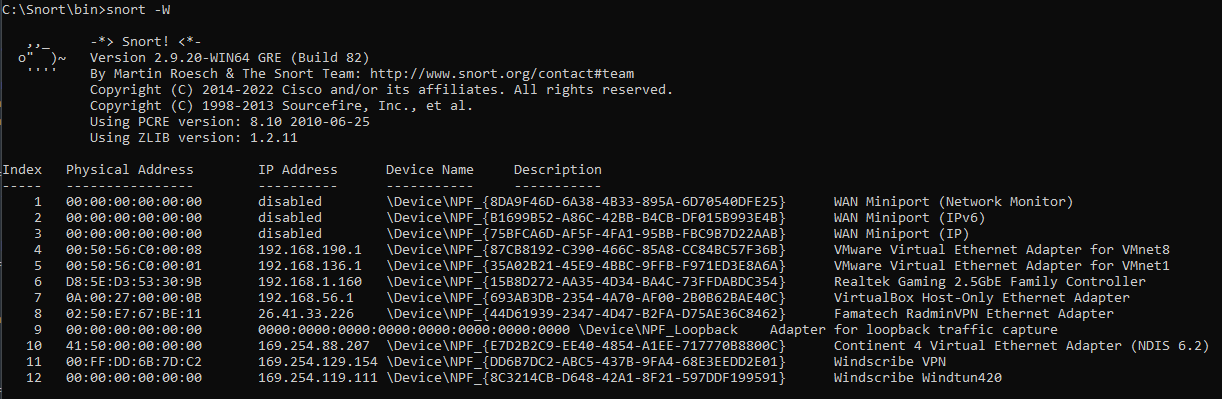


Рисунок 13 – Доступные интерфейсы

Тестируем конфигурацию Snort, вводим команду:

snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 5

ключ -T указывает, что нужно протестировать текущую конфигурацию Snort;

ключ -с означает, что включен 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 айла local.rules. Исправим ее.

Добавим файл local.rules в папку C:/Snort/rules (рис. 14):

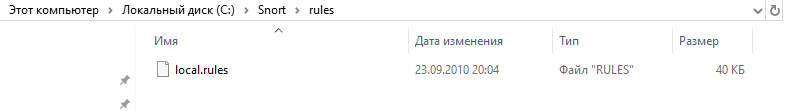


Рисунок 14 – Добавление файла

Снова тестируем конфигурацию Snort, вводим команду:

snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 5

Тестирование завершено ошибкой, которая указывает на отсутствие файла white\_list.rules. Исправим ее. Сразу же добавим и файл black\_list.rules. Эти файлы нет необходимости создавать вручную, их достаточно скопировать из папки для занятия rules. Если эти два файла также открыть в тестовом редакторе, то можно увидеть уже написанные правила, которые можно найти и скачать на официальном сайте Snort (рис. 15-16).

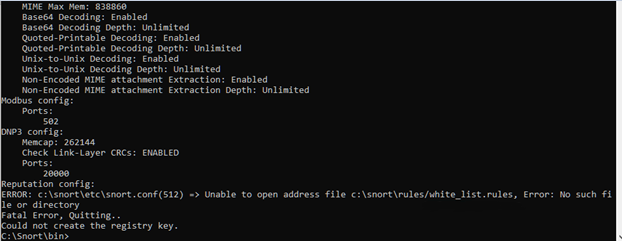


Рисунок 15 – Ошибка white\_list.rules

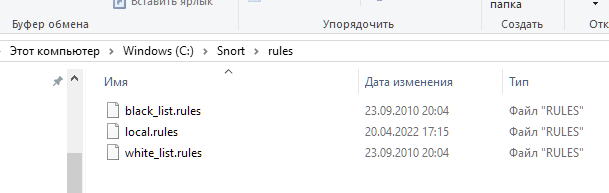


Рисунок 16 – добавление white\_list.rules и black\_list.rules

После исправления всех ошибок и повторном вводе команды

snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2

в командной строке появится сообщение об успешном окончании тестирования конфигурационного файла (рис. 17).

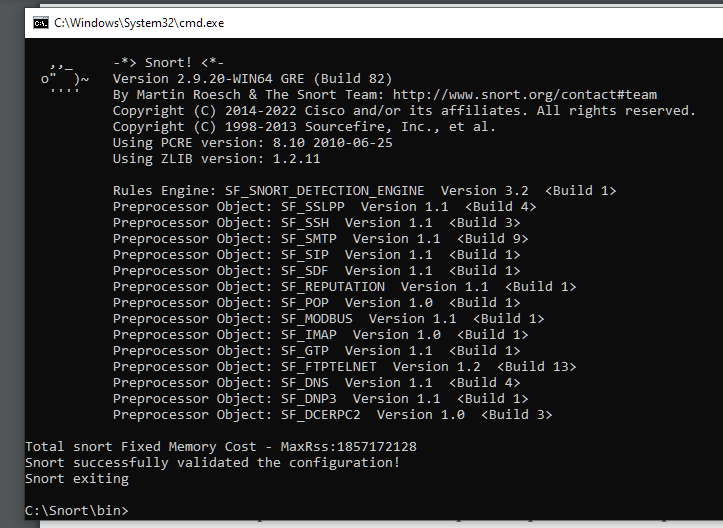


Рисунок 17 – Работа Snort без ошибок

Теперь добавим еще один файл с правилами, который можно скачать с официального сайта snort.org. Этот файл называется community.rules. При скачивании он изначально содержится в архиве с расширением tar.gz (рис. 18).

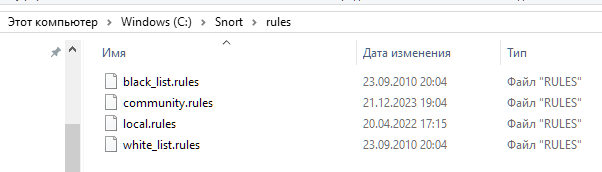


Рисунок 18 – добавление community\_rules

Открываем файл конфигурации и добавляем в него строку, которая добавляет еще один файл правил в конфигурацию IDS Snort (рис. 19).

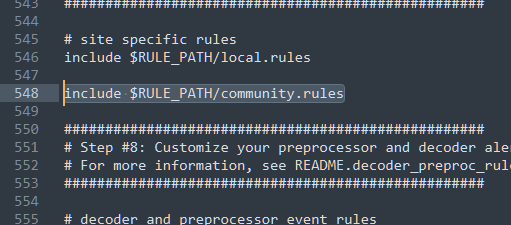


Рисунок 19 – Правим конфиг

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 5

Ключ -A показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль.

Snort проверил файл конфигурации и начал свою работу в режиме IDS (рис. 20):

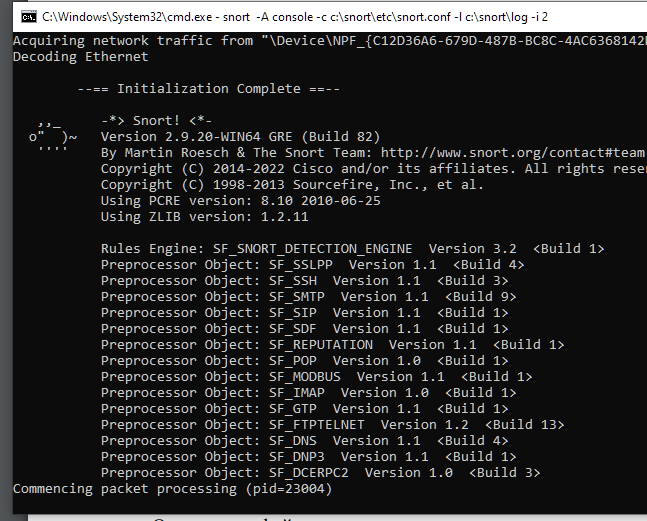


Рисунок 20 – Режим IDS

Теперь самостоятельно попробуем написать правило для IDS Snort. Открываем файл в текстовом редакторе и вводим строку, как показано на рисунке ниже.

Описание введенной строки по частям:

alert: 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.

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).

any any: Эти части указывают на IP-адрес и порт назначения. Аналогично "any" означает "любой", применение правила ко всем IP-адресам и портам назначения.

(msg:"Testing TCP alert"; sid:1000003;): Это дополнительная информация к правилу. msg указывает на сообщение или описание правила, в данном случае, это "Testing TCP alert". sid (идентификатор сигнала) представляет собой уникальный числовой идентификатор этого правила в рамках системы IDS/IPS.

Введенное правило в файле local.rules означает следующее: «Генерировать предупреждение при обнаружении любых TCP пакетов от любого источника к любому назначению, с сообщением 'Testing TCP alert' и идентификатором сигнала 1000003» (рис. 21).

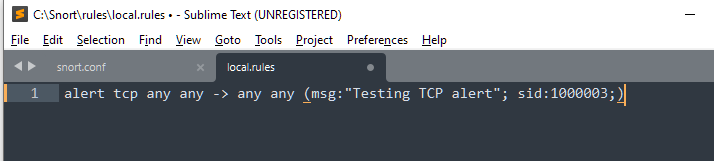


Рисунок 21 – Тестовое правило

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 достаточно выйти в сеть интернет и перейти по любому адресу, после этого в командной строке появится уведомление о срабатывании данного правила (рис. 22).

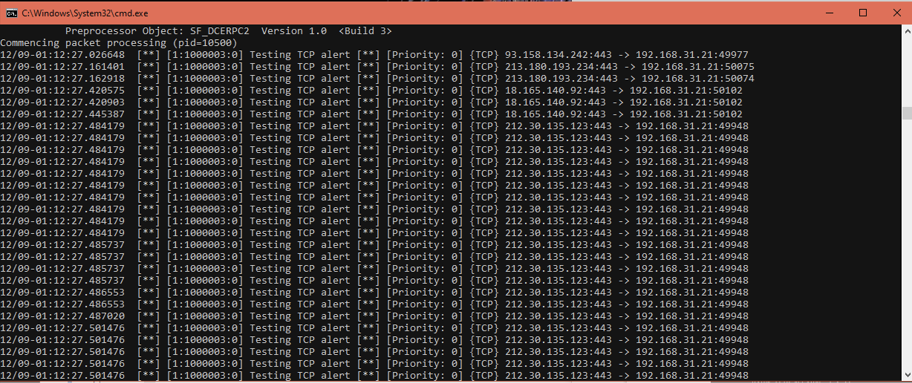


Рисунок 22 – Проверка правила

# Вопрос 2. Разработка правил для IDS Snort

**Вариант 2. (по списку 21 )**

Задание 2. Создать правило для Snort, которое срабатывает при обнаружении всех исходящих tcp-пакетов с Вашего ip-адреса с выводом соответствующего сообщения.

Для того чтобы создать правило Snort, которое будет срабатывать при обнаружении всех исходящих tcp-пакетов, откроем файл local.rules и добавим в него строки, представленные на рисунке 23.

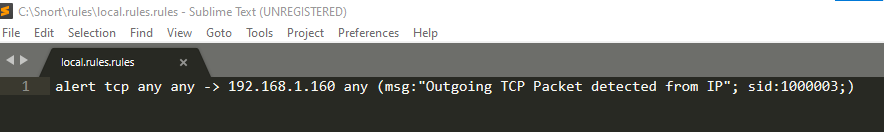


Рисунок 23 – Создали правило

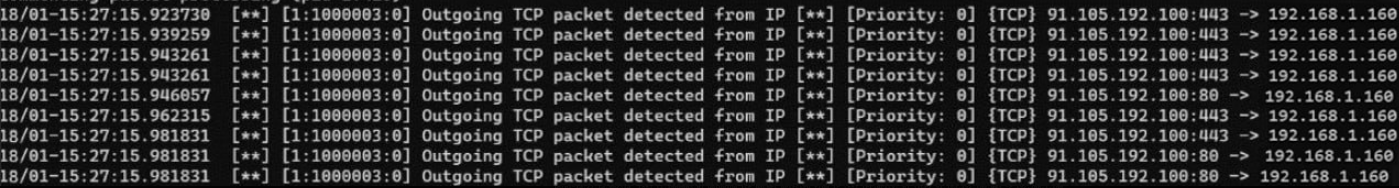
На рисунке проверим работу правила (рис. 24).

Рисунок 24 – Проверяем работоспособность правила

# Заключение

Системы обнаружения вторжений, такие как Snort, используются для мониторинга сетевого трафика с целью обнаружения атаки, осуществляемой злоумышленником, прежде чем она сможет причинить вред или повлиять на сеть.В данной практической работе мы установили и настроили параметры IDS Snort. Разработали правило для IDS Snort по своему варианту.