|  |
| --- |
|  |
| 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 №6 на тему: Обнаружение и предупреждение компьютерных атак

**по дисциплине:** «Управление информационной безопасностью»

**Выполнил:**

Студент группы ББМО-01-22

ФИО: Карев Д.П.

**Проверил:**

Р.В. Пимонов

**Москва 2023**

# 1. Установка и настройка параметров IDS Snort

Для выполнения данной практической работы требуется установить данное ПО, поэтому мы переходи по ссылке и начинаем установку.

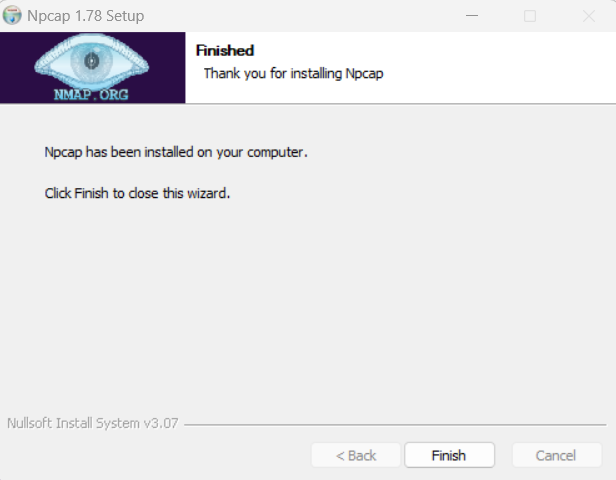


Рисунок 1 – Установка IDS Snort

Далее будет мы зайдем в конфигурационный файл и будем вносить некоторые правки для запуска ПО и установки правил.

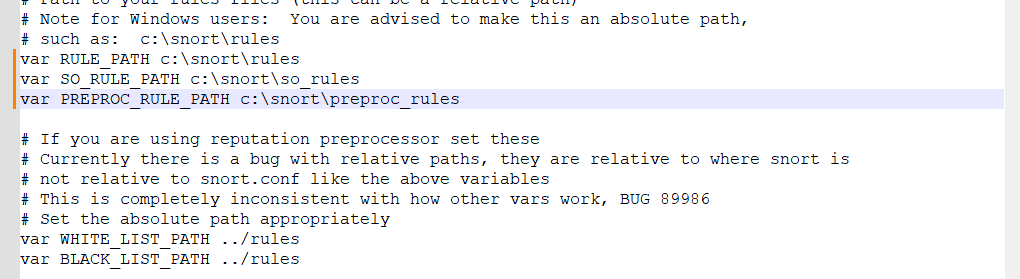


Рисунок 2 – Настройки файла

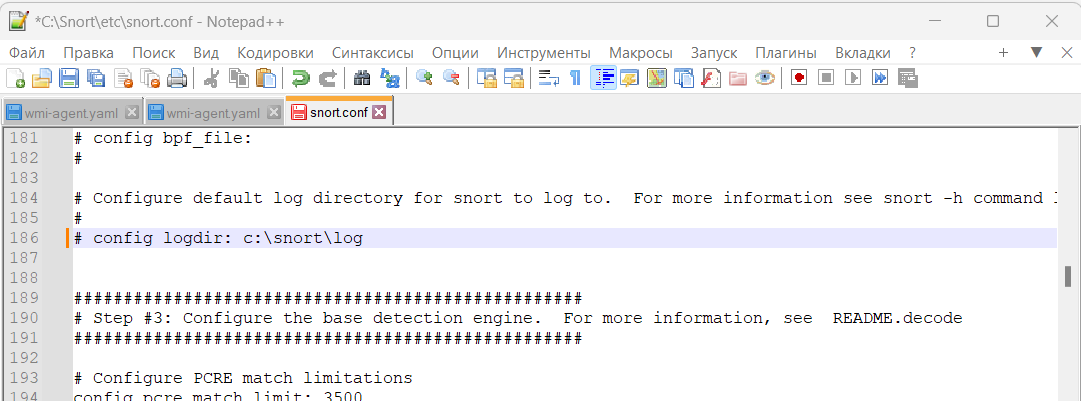


Рисунок 3 – Настройки файла

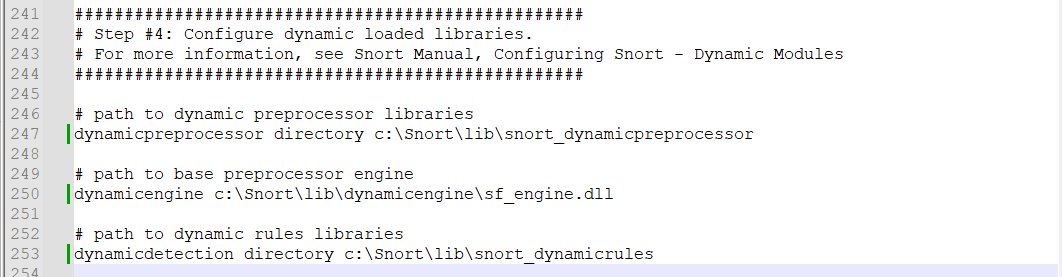


Рисунок 4 – Настройки файла

После того, как мы поменяли файл конфигурации у нас, должен успешно запуститься IDS Snort через командную строку.

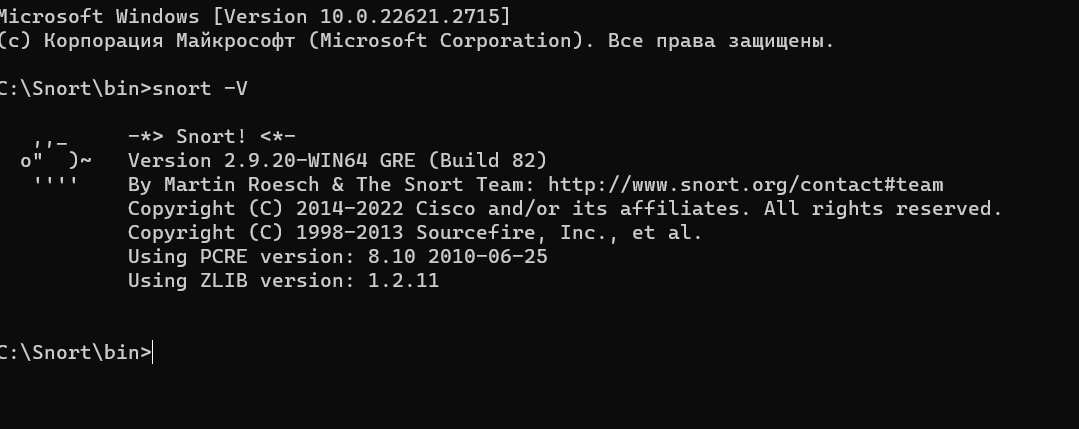


Рисунок 5 – Запуск Snort

Посмотрим какие интерфейсы подключены и воспользуемся сетевой картой.

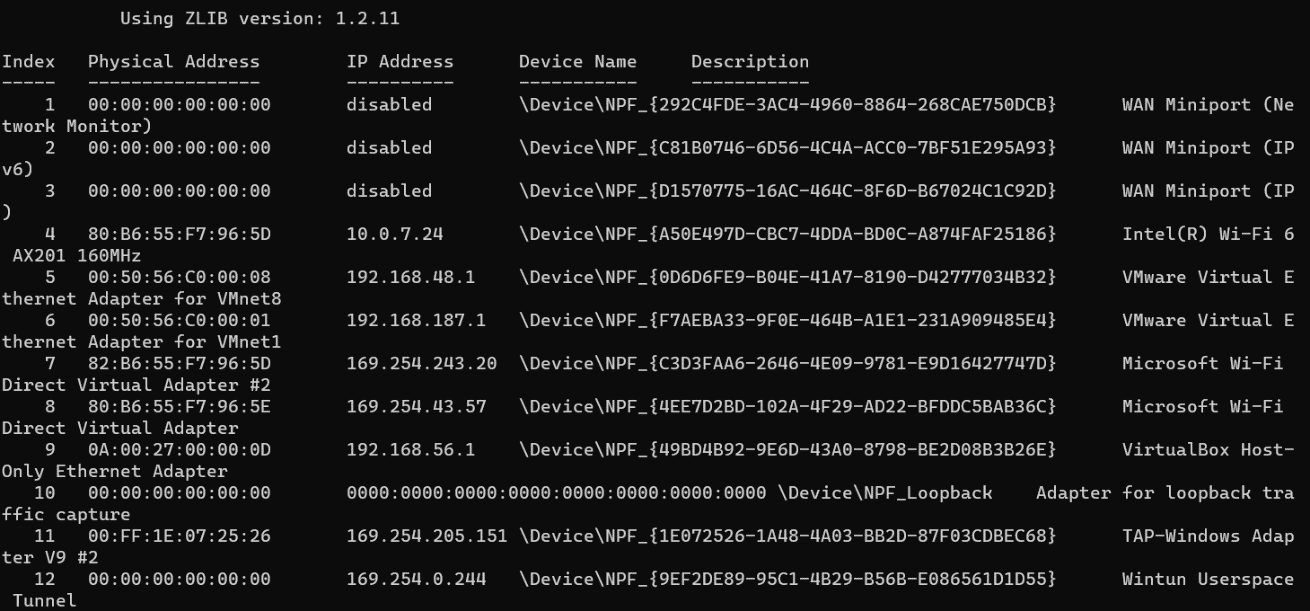


Рисунок 6 – Сетевые интерфейсы.

Теперь мы можем запустить наше ПО (при условии выполнения всех пунктов установки)

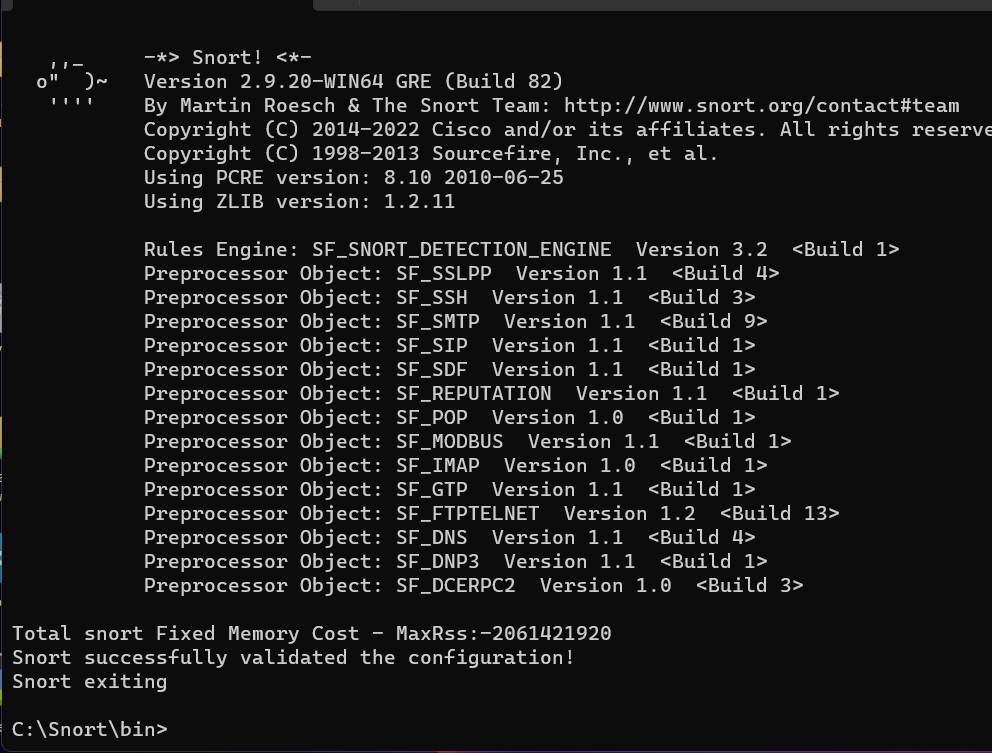


Рисунок 6 – Список действий с высоким приоритетом

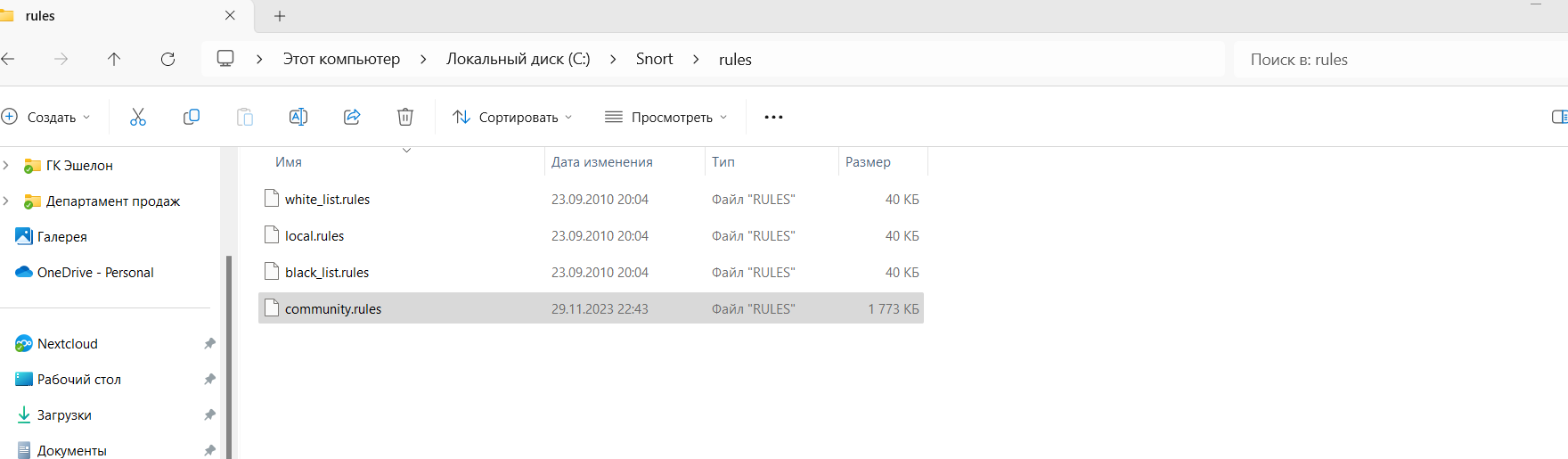
Далее добавим правила с официального сайта Snort и добавим правило в папку Rules.

Рисунок 8 – Правила.

Приступим к написанию правила для нашего правила для: *создать правило для Snort, которое срабатывает при обнаружении.*

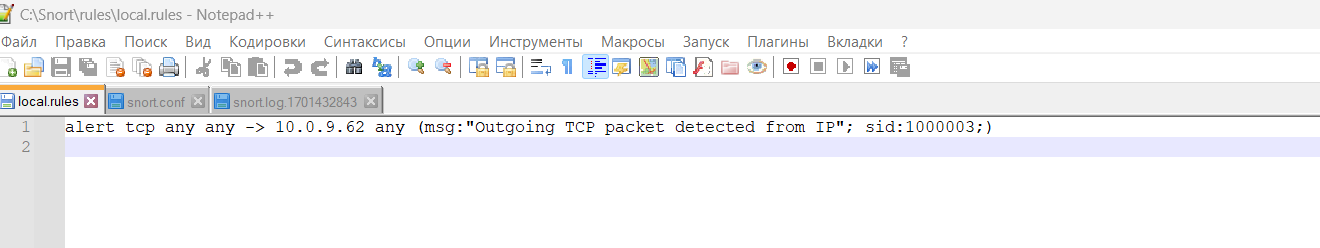
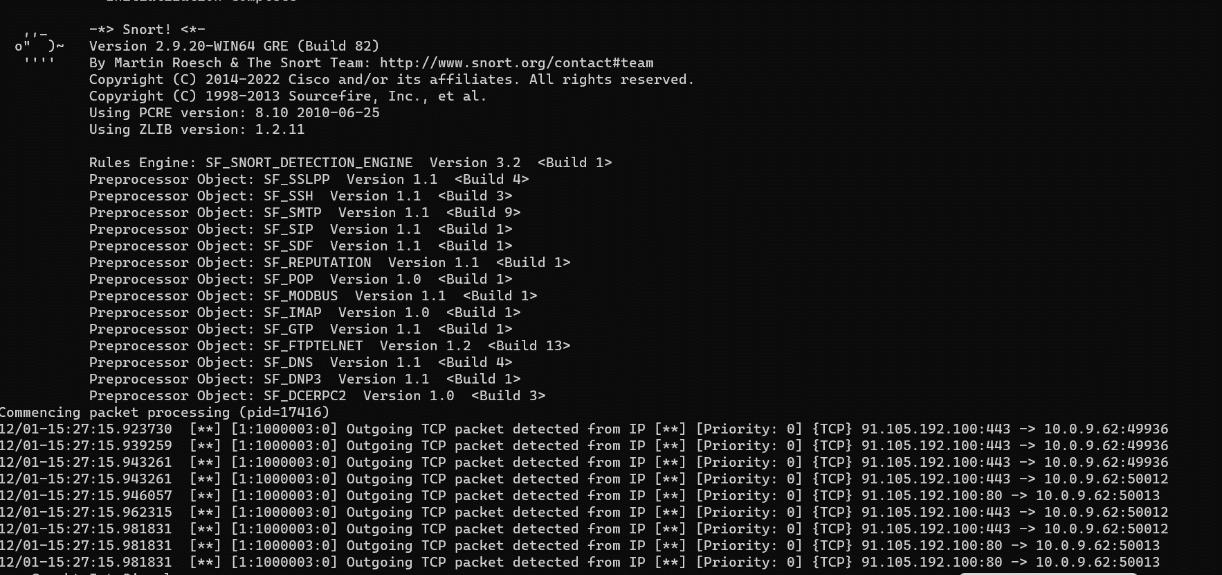


Рисунок – 9 Написание правила

Проверим наше правило в действии.





Рисунки 10-11 – Проверка правила

**Вывод**

По итогам практической работы мы ознакомились с ПО IDS Snort и смогли написать правила для обнаружения какой либо активности.