|  |
| --- |
|  |
| 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

по дисциплине: «Управление информационной безопасностью»

**Выполнил**:

Студент группы ББМО-02-22

Кузьмин Владимир Дмитриевич

**Проверил**:

Пимонов Роман Владимирович

Москва 2023

Содержание

[Задание на практическую работу 3](#_Toc152499693)

[Установка и настройка параметров IDS Snort 4](#_Toc152499694)

[Разработка правил для IDS Snort 14](#_Toc152499695)

[Заключение 16](#_Toc152499696)

# Задание на практическую работу

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

**Задачи**:

1. Установить и настроить параметры IDS Snort;

2. Создать правило для Snort, которое срабатывает при обнаружении DNS-трафика.

# Установка и настройка параметров IDS Snort

Установка Snort произведем с параметрами по умолчанию (рисунок 1).

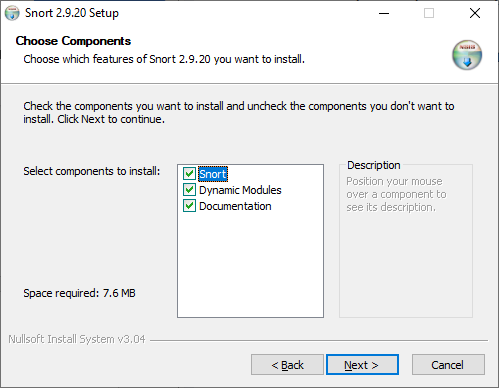


Рисунок 1 – Установка Snort

Приступим к редактированию конфигурационного файла Snort/etc/snort.conf. В строках 104-106 и 113-114 указываем абсолютные пути через корневую папку Snort к папкам с правилами (рисунок 2).

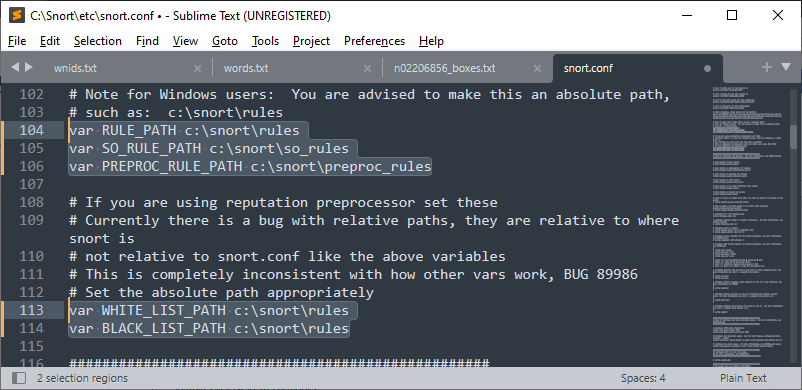


Рисунок 2 – Конфигурация правил

В строке 186 указываем параметр пути к папке для лог-файлов (рисунок 3).

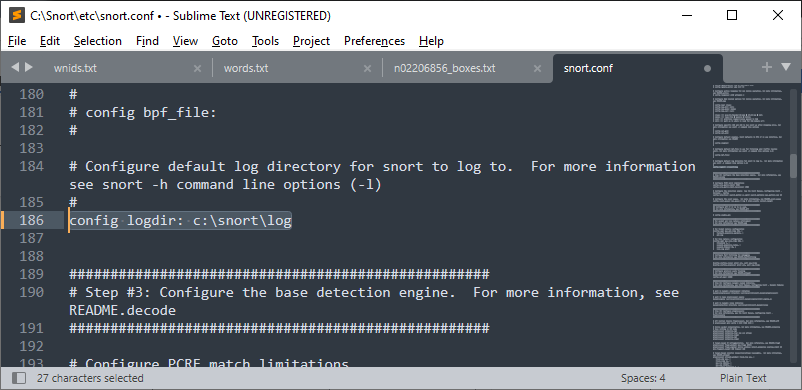


Рисунок 3 – Конфигурация логов

В строках 247, 250, 253 указываем пути через «c:\Snort\lib\», а также меняем движок предобработчика на sf\_engine.dll (рисунок 4).

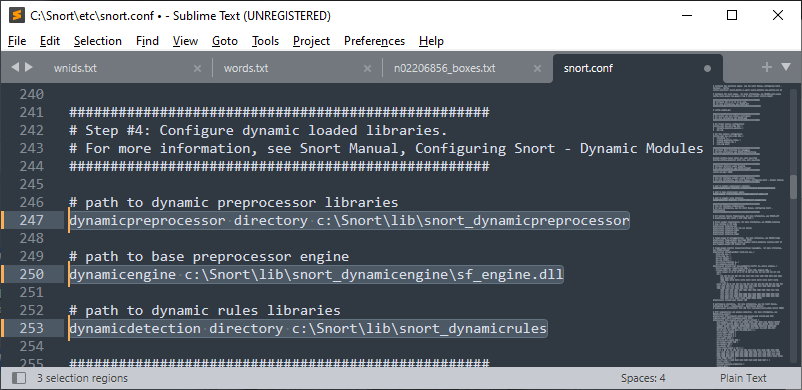


Рисунок 4 – Конфигурация динамической загрузки библиотек

Комментируем строки 265-269 (рисунок 5).

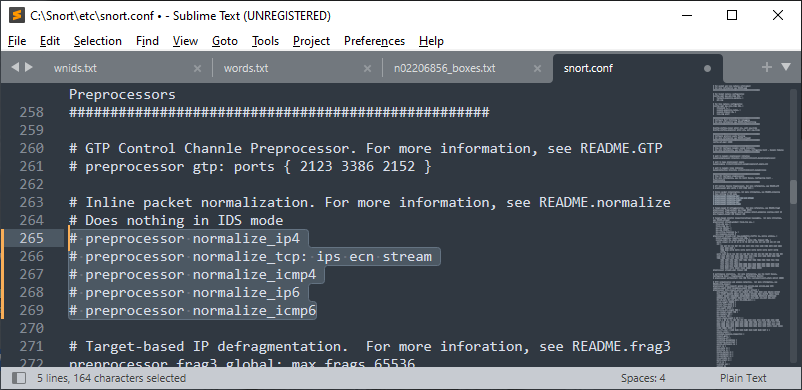


Рисунок 5 – Конфигурация пакетов нормализации

В строках 534-535 добавим к файлам абсолютный адрес расположения (рисунок 6).

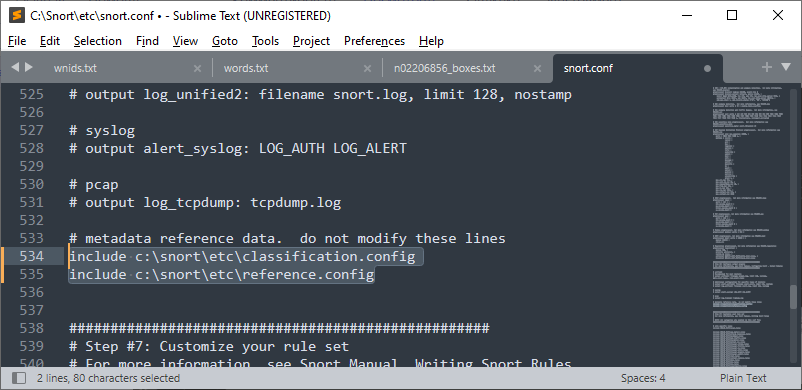


Рисунок 6 – Конфигурация справочных данных метаданных

Удалим строки 548-651, подключающие правила для Snort (рисунок 7).

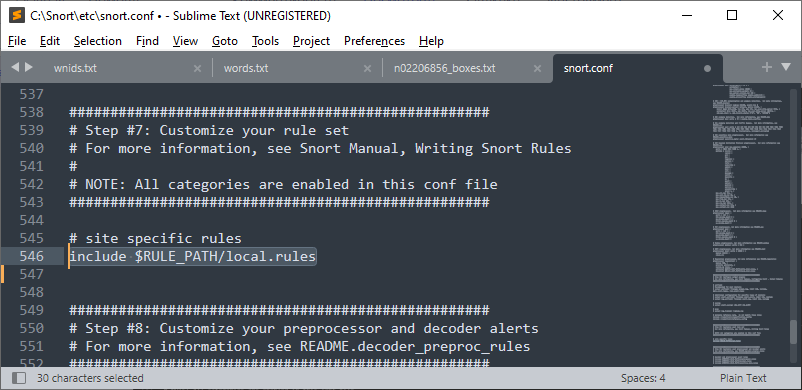


Рисунок 7 – Конфигурация подключения правил

Откроем консоль в папке c:\Snort\bin. Проверим версию Snort (рисунок 8).

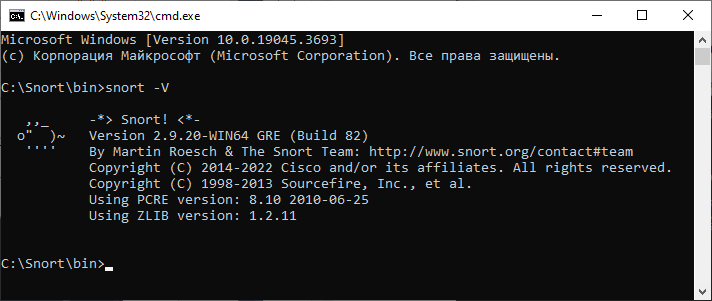


Рисунок 8 – Версия Snort

Посмотрим доступные интерфейсы (рисунок 9).

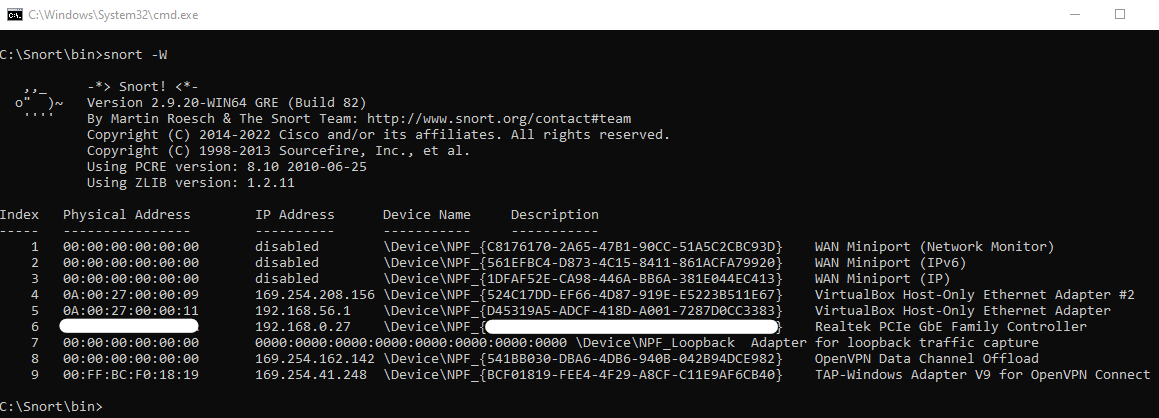


Рисунок 9 – Список доступных интерфейсов

Протестируем конфигурацию, выполнив команду snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 6, где:

* 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.

Получаем ошибку об отсутствии папки c:\snort\lib\snort\_dynamicrules (рисунок 10).

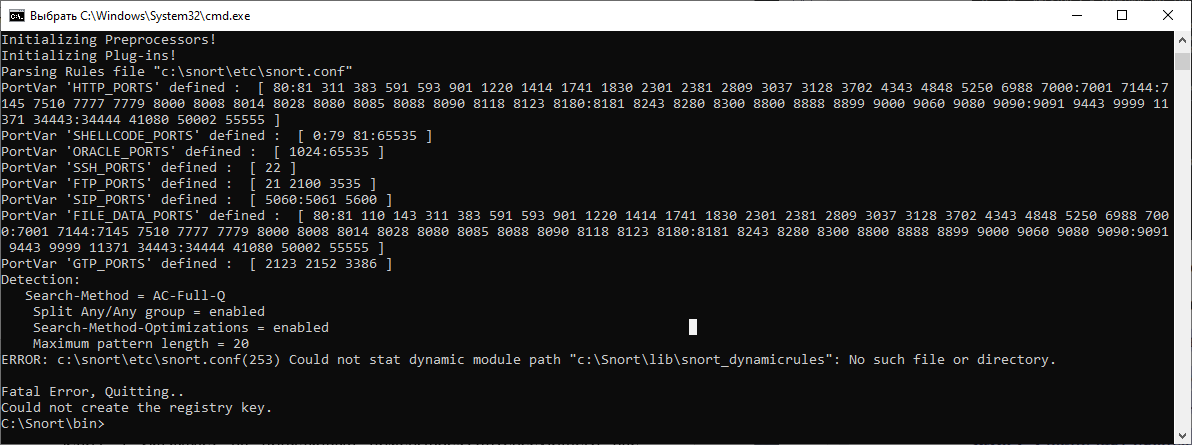


Рисунок 10 – Ошибка 1

Создадим необходимую папку. Повторим процедуру тестирования. Получаем ошибку об отсутствии файла local.rules (рисунок 11).

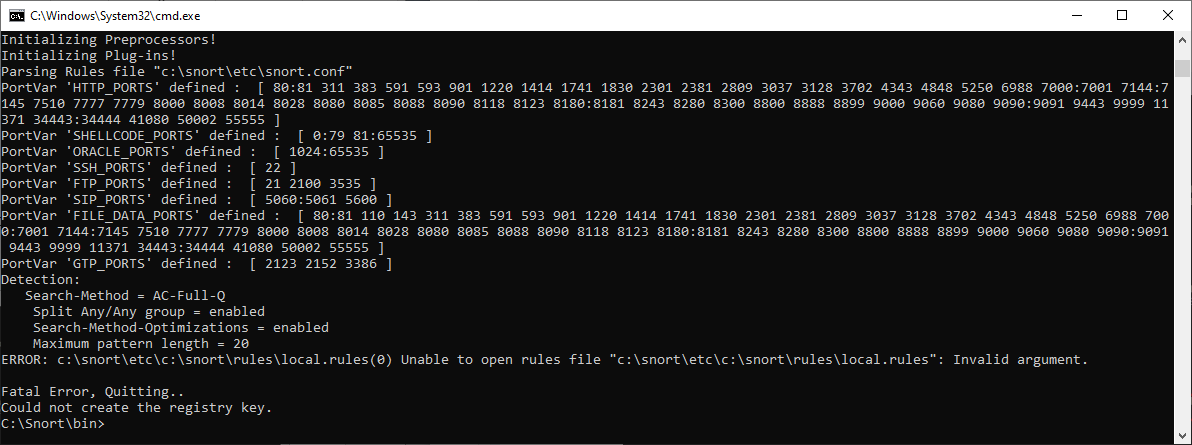


Рисунок 11 – Ошибка 2

Создадим необходимый файл. Повторим процедуру тестирования. Получаем ошибку об отсутствии файла white\_list.rules (рисунок 12).

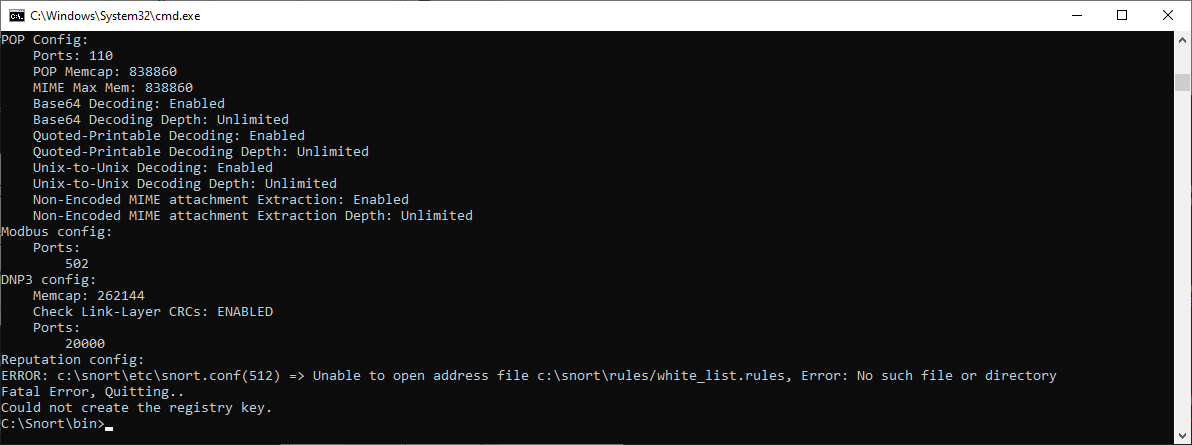


Рисунок 12 – Ошибка 3

Добавим необходимые файлы white\_list.rules, а также black\_list.rules, которые содержат правила, которые можно найти и скачать на официальном сайте Snort. Повторим процедуру тестирования. Получаем сообщение об успешном прохождении тестирования (рисунок 13).

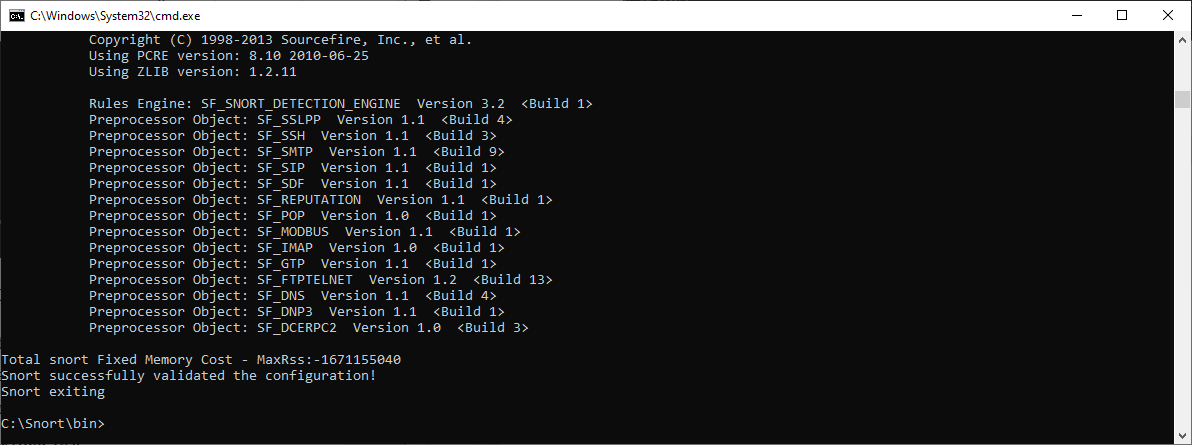


Рисунок 13 – Успешный тест

Добавим файл с правилами community.rules, который можно найти на официальном сайте Snort. А также укажем путь к нему в конфигурационном файле snort.conf (рисунок 14).

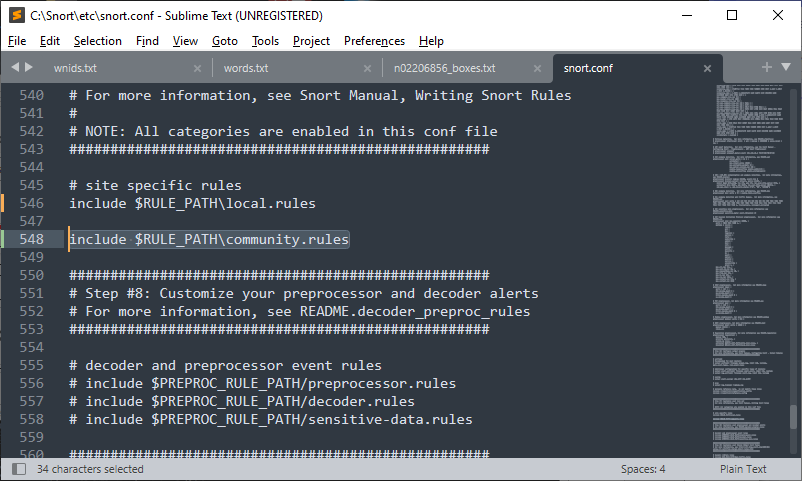


Рисунок 14 – Подключение файла community.rules

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 6 (рисунок 15). Ключ -A показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль.

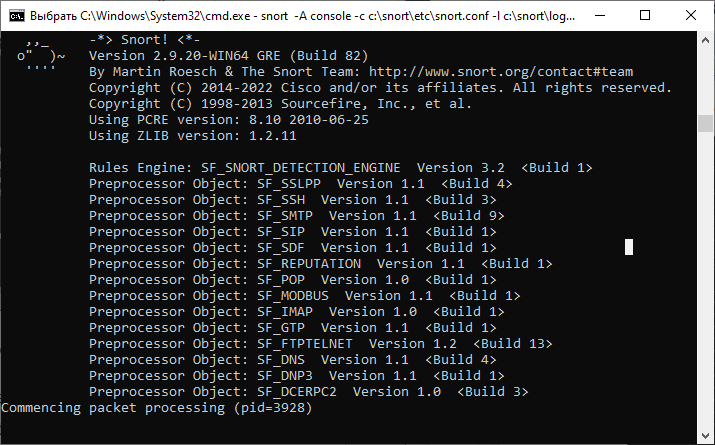


Рисунок 15 – Запуск Snort

Добавим локальное правило в файл local.rules, чтобы проверить работоспособность Snort (рисунок 16).

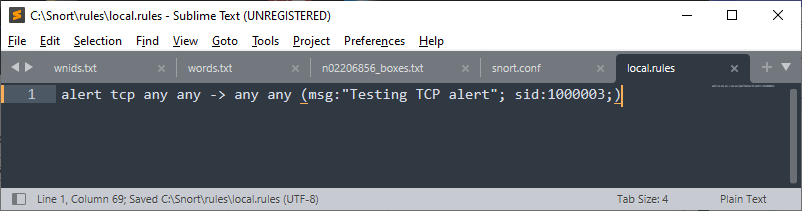


Рисунок 16 – Тестовое правило

Запускаем Snort и открываем любой ресурс через браузер. Наблюдаем алерты (рисунок 17).

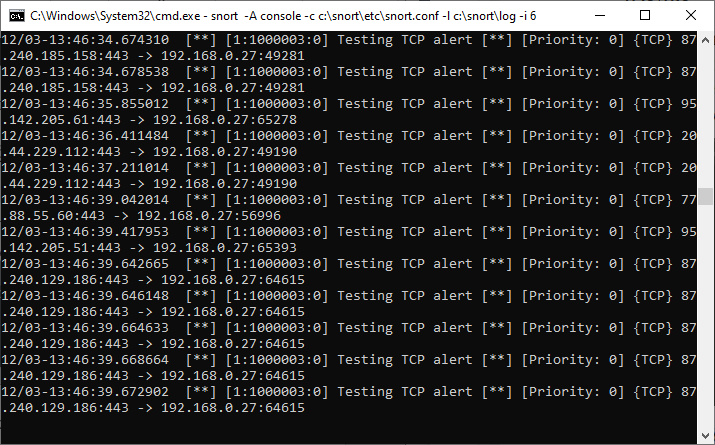


Рисунок 17 – Тестовые алерты

# Разработка правил для IDS Snort

Для того, чтобы создать правило Snort, которое будет срабатывать при обнаружении DNS-трафика, откроем файл local.rules и добавим в него строку, представленную на рисунке 18.

DNS (Domain Name System) использует несколько портов для своей работы. Основной порт, который обычно используется для DNS-запросов и ответов, это порт 53. Этот порт был выделен для использования DNS ввиду его функциональной важности в интернет-коммуникации.

Однако стоит отметить, что в некоторых случаях DNS может использовать и другие порты, если настроен соответствующим образом. Например, для отладки или при использовании нестандартных конфигураций.

DNS использует UDP (User Datagram Protocol) в качестве транспортного протокола для отправки и получения DNS-запросов и ответов. Однако, если настроены безопасные DNS-серверы, такие как DNSCrypt или DNS over TLS, DNS может использовать TCP (Transmission Control Protocol) для обеспечения дополнительной безопасности и конфиденциальности данных.

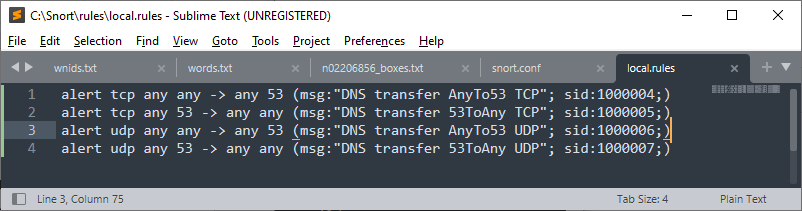


Рисунок 18 – DNS правила

Теперь протестируем правило. Для этого запускаем Snort (рисунок 19).

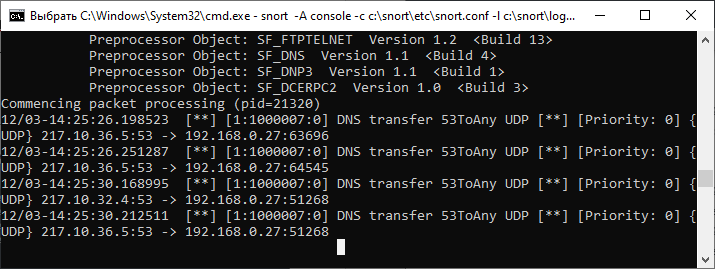


Рисунок 19 – DNS проверка

# Заключение

В ходе выполнения практической работы были выполнены необходимые задачи, а именно:

1. Установить и настроить параметры IDS Snort;

2. Создать правило для Snort, которое срабатывает при обнаружении DNS-трафика.

Соответственно, цель работы – настройка параметров системы обнаружения атак, была достигнута.