|  |
| --- |
|  |
| 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: Настройка параметров системы обнаружения атак

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

**Выполнил:**

Студент группы ББМО-01-22

ФИО: Загороднов Е.А.

**Проверил:**

Р.В. Пимонов

**Москва 2023**

Содержание

[ВВЕДЕНИЕ 3](#_Toc152438093)

[1. Установка и настройка параметров IDS Snort 3](#_Toc152438094)

[2. Разработка правил для IDS Snort 13](#_Toc152438095)

[Вывод 15](#_Toc152438096)

# ВВЕДЕНИЕ

Задача данного практической работы заключается в установке и настройке параметров IDS Snort, а также в создании эффективного правила для обнаружения сетевых атак. В ходе выполнения работы планируется осуществить установку необходимого программного обеспечения, провести настройку системы обнаружения вторжений Snort, и разработать качественное правило для обеспечения надежной защиты сети от потенциальных угроз. В конечном итоге, освоение данных навыков и практических нюансов в области IDS Snort позволит улучшить уровень безопасности информационной инфраструктуры.

# 1. Установка и настройка параметров IDS Snort

Для осуществления текущей практической работы необходимо провести установку указанного программного обеспечения. В данном контексте предлагается перейти по предоставленной ссылке и приступить к процессу установки. Подробности установки программного обеспечения наглядно продемонстрированы на рисунке 1.

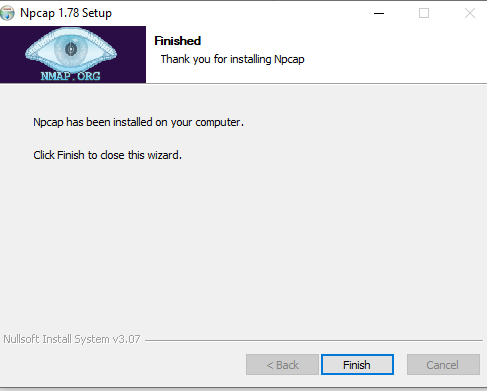


Рисунок 1 – Установка IDS Snort

Далее переходим в директорию **C:/Snort**,где в первую очередь необходимо

настроить файл конфигурации для его успешной работы. Для настройки этого файла необходимо перейти в директорию **C:/Snort/etc** и откроем файл **snort.con.** Процесс открытия файла показан на рисунке 2.

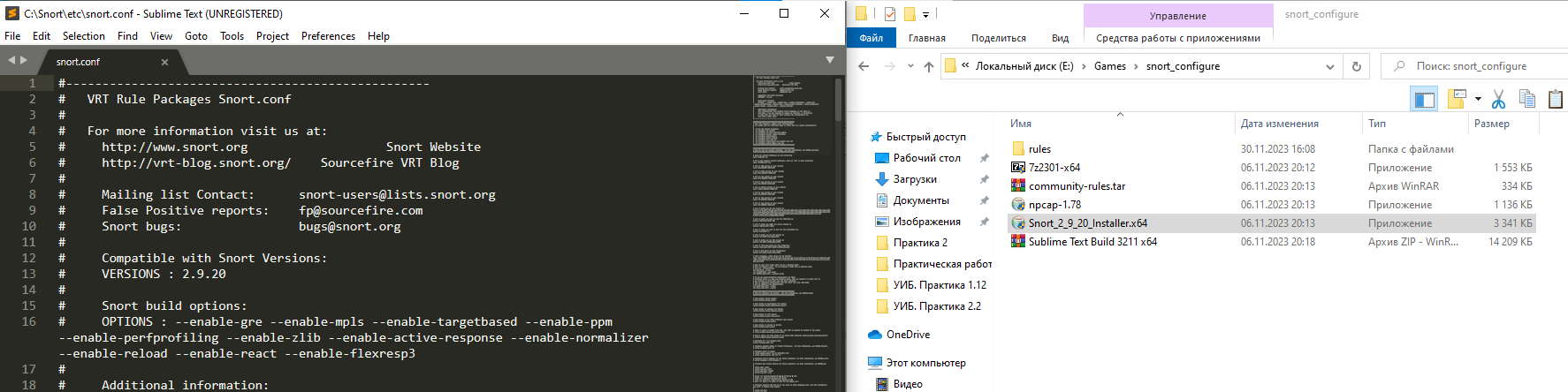


Рисунок 2 – Открытие файла Snort.con

Теперь переходим в файле snort.con к строкам 104-106 и вместо …\ прописываем c:\snort\. Процесс показан на рисунке 3

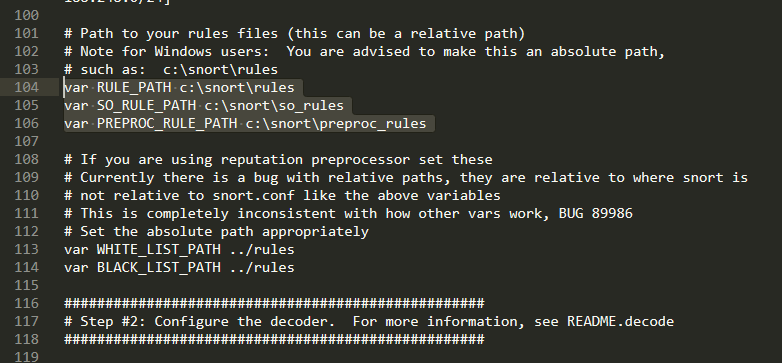


Рисунок 3 – Редактирование строк в файле snort.con

Далее переходим к строкам 113-114 и делаем те же действия, что и делали в строках 104-106. Процесс показан на рисунке 4.

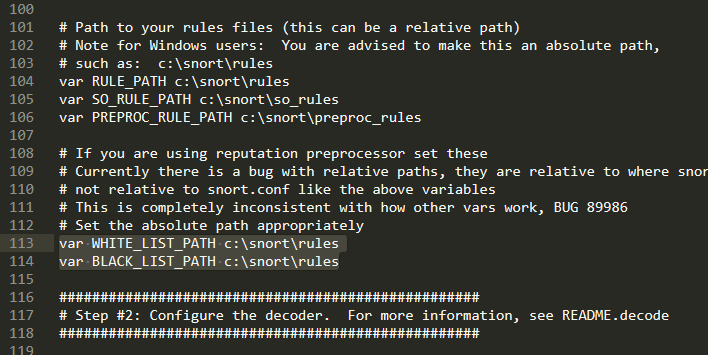


Рисунок 4 – Редактирование строк в файле snort.con

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. Процесс указания пути для папки Log-файлов показан на рисунке 5.

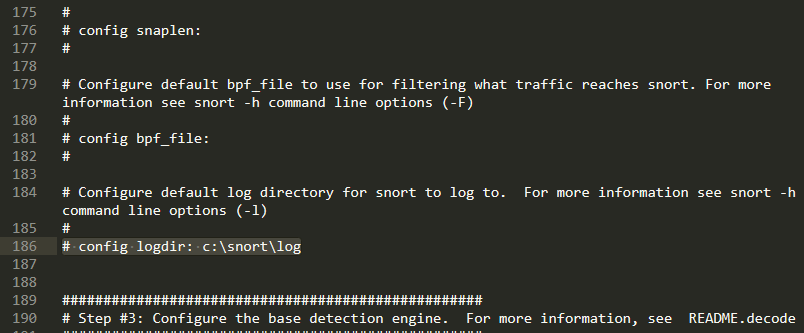


Рисунок 5 – Написание команды config logdir: c:\snort\log

Далее переходим к строкам 246-253 и прописываем нужны команды для изменения файла конфигурации. Процесс показан на рисунке 6.

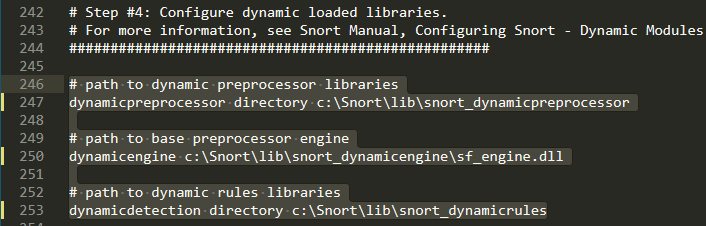


Рисунок 6 – Конфигурование файла

Далее переходим к строкам 259-265 и добавляем знаки комментария " # ". Процесс показан на рисунке 7.

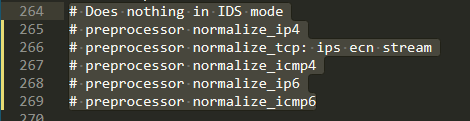


Рисунок 7 – Добавление знака комментария " # “

Также необходимо раcкомментировать строки 534-535, убрав знак #. Процесс показа на рисунке 8.

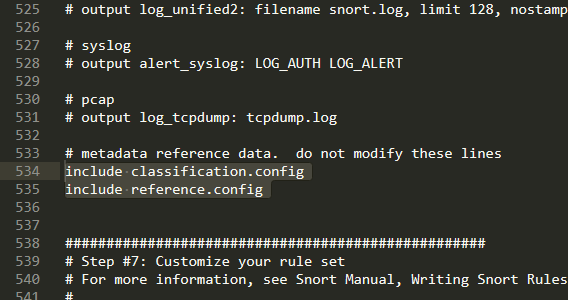


Рисунок 8 – Расскомментирование строк 534-535

Также отредактируем пункт, касающийся подключения правил для IDS Snort. Удалим строки 548-651. Процесс показан на рисунке на рисунках 9 и 10.

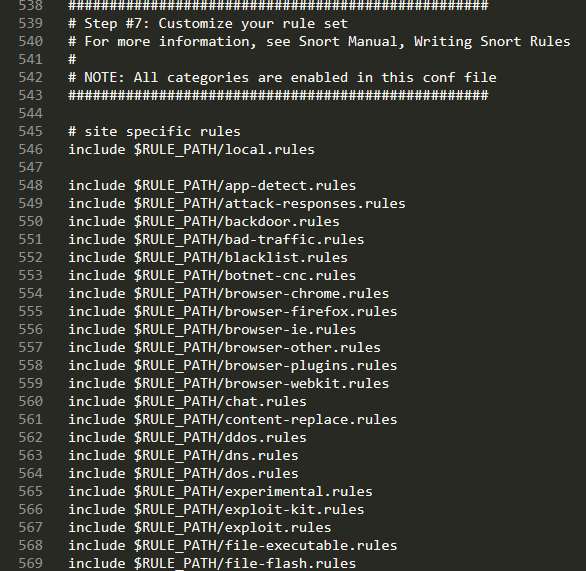


Рисунок 9 – Строки 548-569 до удаления

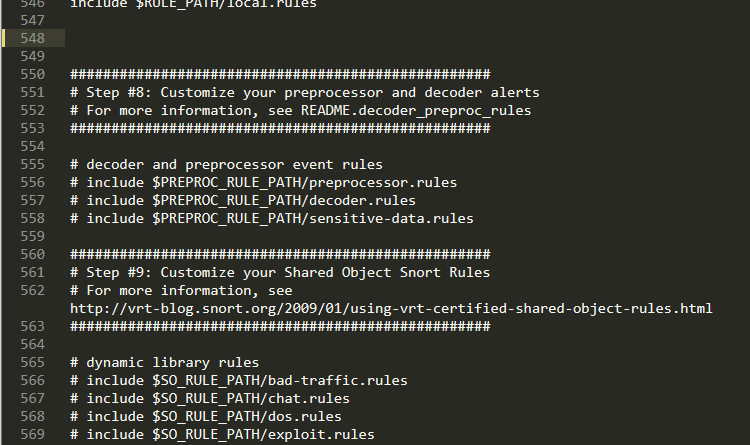


Рисунок 10 – Строки 548-569 после удаления

Конфигурирование файла закончено. Теперь необходимо проверить правильность написанной конфигурации. Для этого переходим в папку **C:/Snort/bin**. Запускаем командную строку через ввод команды **cmd**. У нас запускается командная строка и вводим команду **snort –V**, которая отображает текущую версию IDS Snort. Процесс показан на рисунке 11.

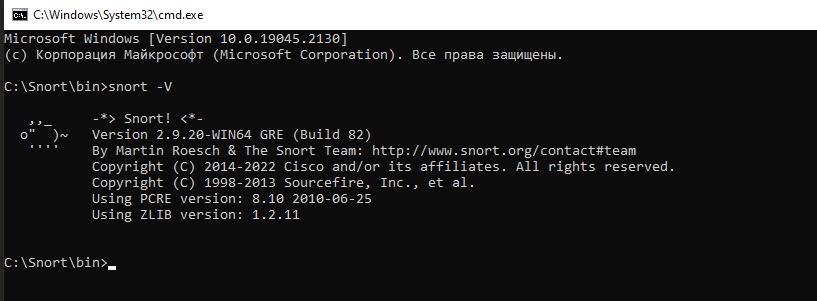


Рисунок 11 – Запуск Snort

Далее командой **snort –W** просмотри доступные интерфейсы, в данном случае наиболее подходящим для тестирования является интерфейс сетевой карты. Процесс ввода команды показан на рисунке 12.

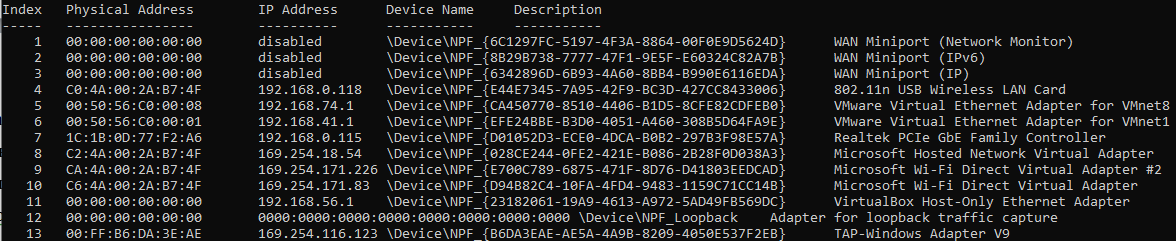


Рисунок 12 – Доступные сетевые интерфейсы

Тестируем конфигурацию Snort, вводим команду: **snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2.** Процесс ввода показан на рисунке 13. Видим, что Тестирование завершено ошибкой, которая указывает на отсутствие файла **local.rules**.

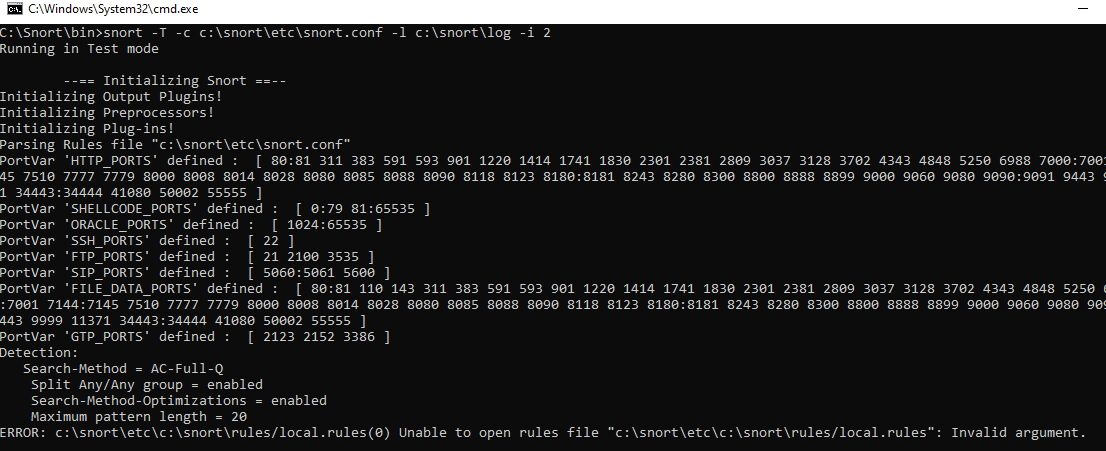


Рисунок 13 – Тестирование конфигурации Snort

Для исправления ошибка добавим файл **local.rules** в папку C:/Snort/rules. Процесс добавления файла показан на рисунке 14.

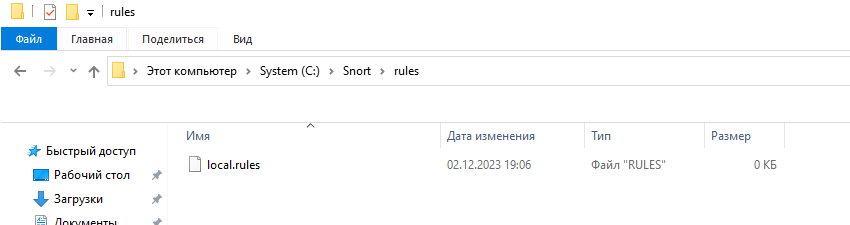


Рисунок 14 – Добавление файла local.rules в директорию

Снова тестируем конфигурацию Snort, вводим команду: **snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**. Процесс тестирования показан на рисунке 15. Тестирование снова завершено с ошибкой. Ошибка заключается в том, что отсутствует файл white\_list.rules.

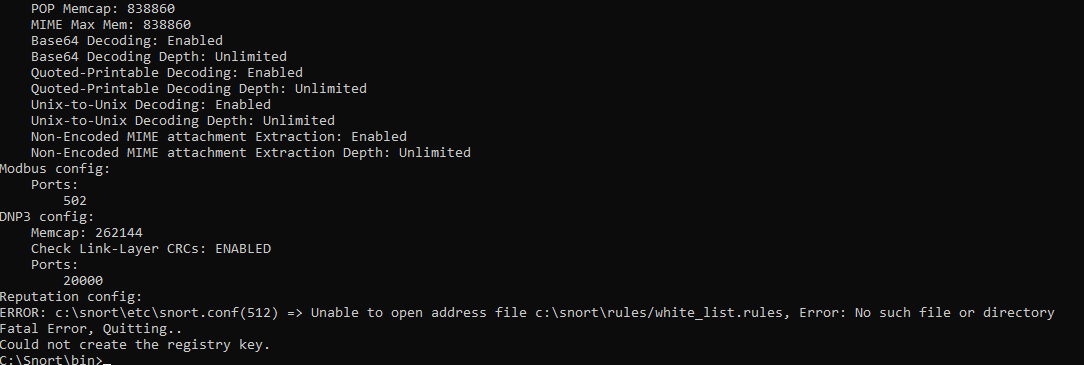


Рисунок 15 – Тестирование конфигурации Snort

Добавим файлы **white\_list.rules** и **black\_list.rules** в папку с файлом local.rules. Процесс добавления файлов показан на рисунке 16.

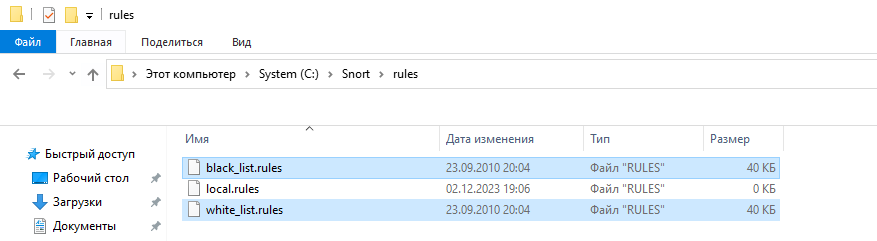


Рисунок 16 – Добавление файлов в директорию

После добавления данных файлов снова запускаем тестирование с помощью команды **snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**. Процесс показан на рисунке 17. Видим, что тестирование завершено успешно.

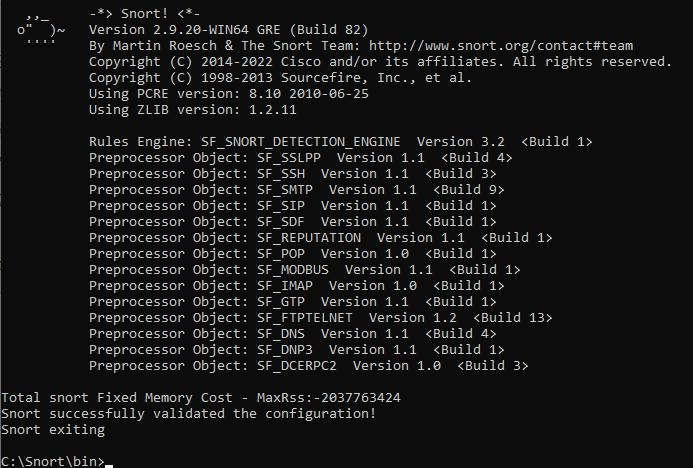


Рисунок 17 – Успешное завершение тестирования

Теперь добавим еще один файл с правилами, который можно скачать софициального сайта snort.org. Этот файл называется **community.rules.** Процесс добавление файла в папку rules показан на рисунке 18.

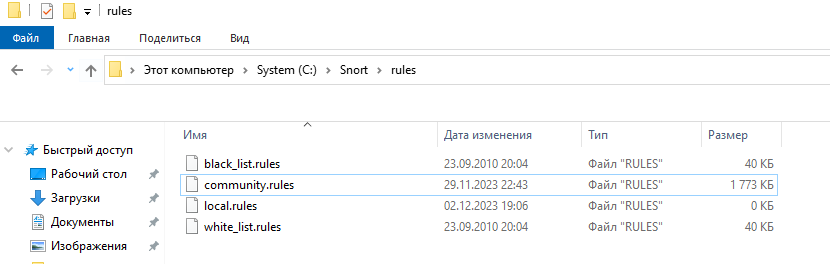


Рисунок 18 – Добавление файла community.rules

Открываем файл конфигурациии добавляем в него строку, которая добавляет еще один файл правил в конфигурацию IDS Snort. Процесс показан на рисунке 19.

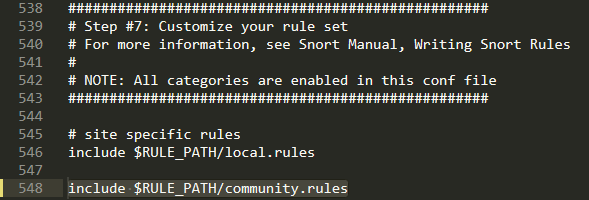


Рисунок 19 – Добавление строки 548

Далее 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** . Процесс запуска в режиме IDS показан на рисунке 20.

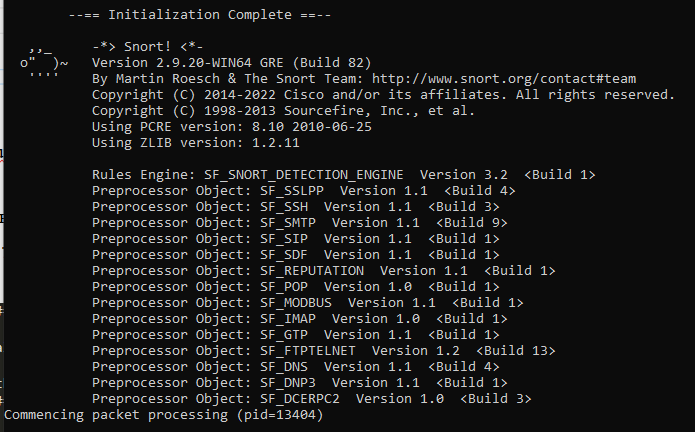


Рисунок 20 – Запуска в режиме IDS

# 2. Разработка правил для IDS Snort

Для начала определим номер выполняемого задания по формуле:

**N = n mod m + 1,**

где N – номер задания;

m – количество заданий;

n – номер строки с Фамилией в файле:

Расчитав формулу со своими значениями, получалось значение **9**. Следовательно приступаем к заданию 9: **Создать правило для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.**

Приступим к написанию правила для нашего правила для: **Создать правило для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.** Переходим в файл local.rules и пишем правило: **alert udp any any -> any 53 (msg:"** **DNS query with the keyword 'hack'"; content:"|68 61 63 6B|"; nocase; dns; sid:1000001;)**. Процесс добавления правила показан на рисунке 21.

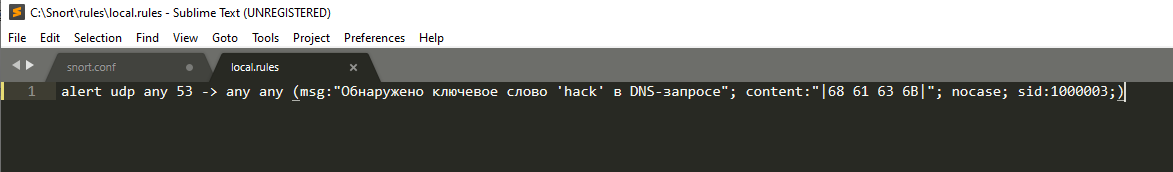
****

Рисунок 21 – Добавление правила для выполнения задания

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**. Процесс запуска Snort в режиме IDS показан на рисунке 22. Успешный запуск с правилом, которое мы добавили раннее показа на рисунке 23.

****

Рисунок 22 – Запуск Snort в режиме IDS

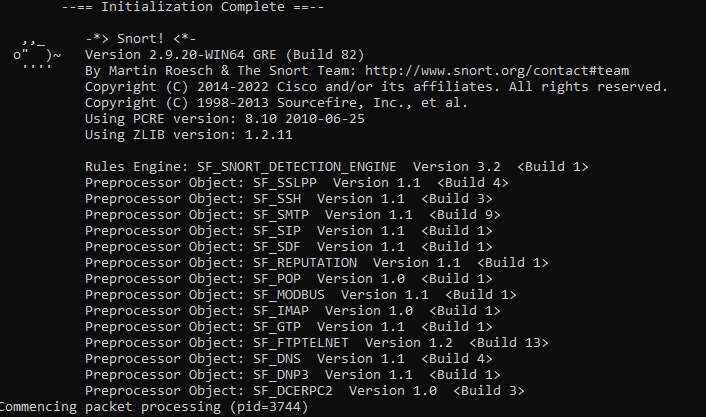


Рисунок 23 – Успешный запуск с правилом для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.

# Вывод

В результате выполнения практической работы с Snort были приобретены ценные навыки по установке и настройке системы обнаружения вторжений. Создание собственных правил, например, для обнаружения конкретных строк в сетевом трафике, дает возможность персонализировать защиту и адаптировать ее к конкретным потребностям. Опыт работы с Snort подчеркнул важность баланса между точностью обнаружения и предотвращением ложных срабатываний, что является критическим аспектом при обеспечении безопасности в сетевой среде. Этот опыт предоставил понимание того, как эффективно использовать инструменты обнаружения вторжений для повышения уровня защиты в информационных системах.