

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

**Практическая работа №5**

по дисциплине: «Управление информационной безопасностью»   
На тему:

«Настройка параметров системы обнаружения атак»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

Пимонов Р.В.

Москва, 2023

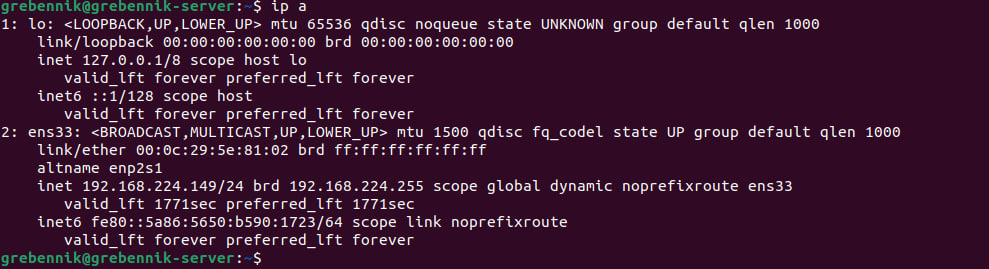
**Задание на практическую работу:**

1. Определить номер задания по формуле N = n mod m + 1.
2. . Создать правило для Snort, которое срабатывает при обнаружении всех входящих tcp-пакетов на Ваш ip-адрес с выводом соответствующего сообщения.

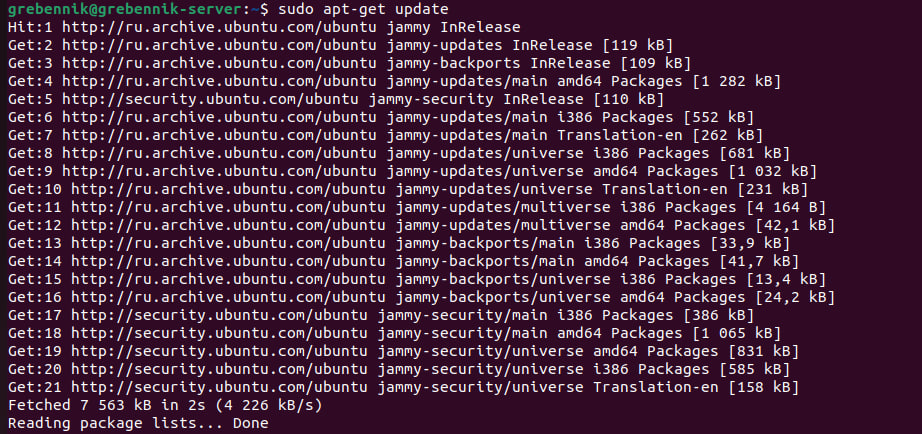
**Ход работы :**

**Подготовка SNORT**

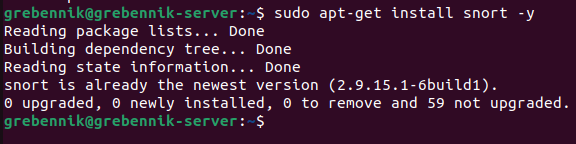
1. В начале узнаем ip адрес нашей виртуальной машины



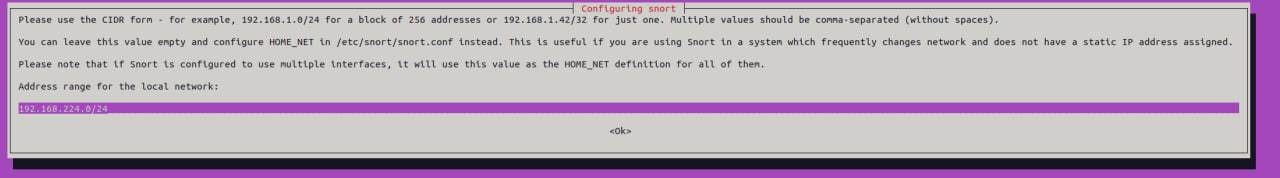
1. Обновим пакеты нашей ОС (Ubuntu), на которую собираемся устанавливать Snort.



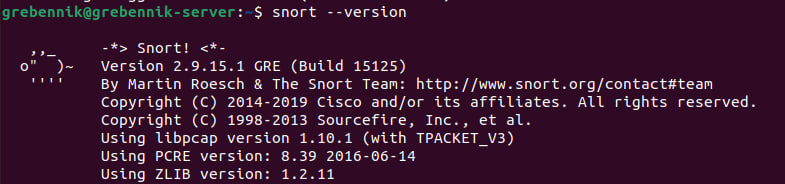
1. После завершения на нужно становить Snort через терминал, это действие выполняется командой: sudo apt-get install –y



1. Далее нас перенесет в программу конфигурации, где надм необходимо указать параметры нашей сети, которые мы узнали из пункта 1. Наша сеть 192.168.224.0/24



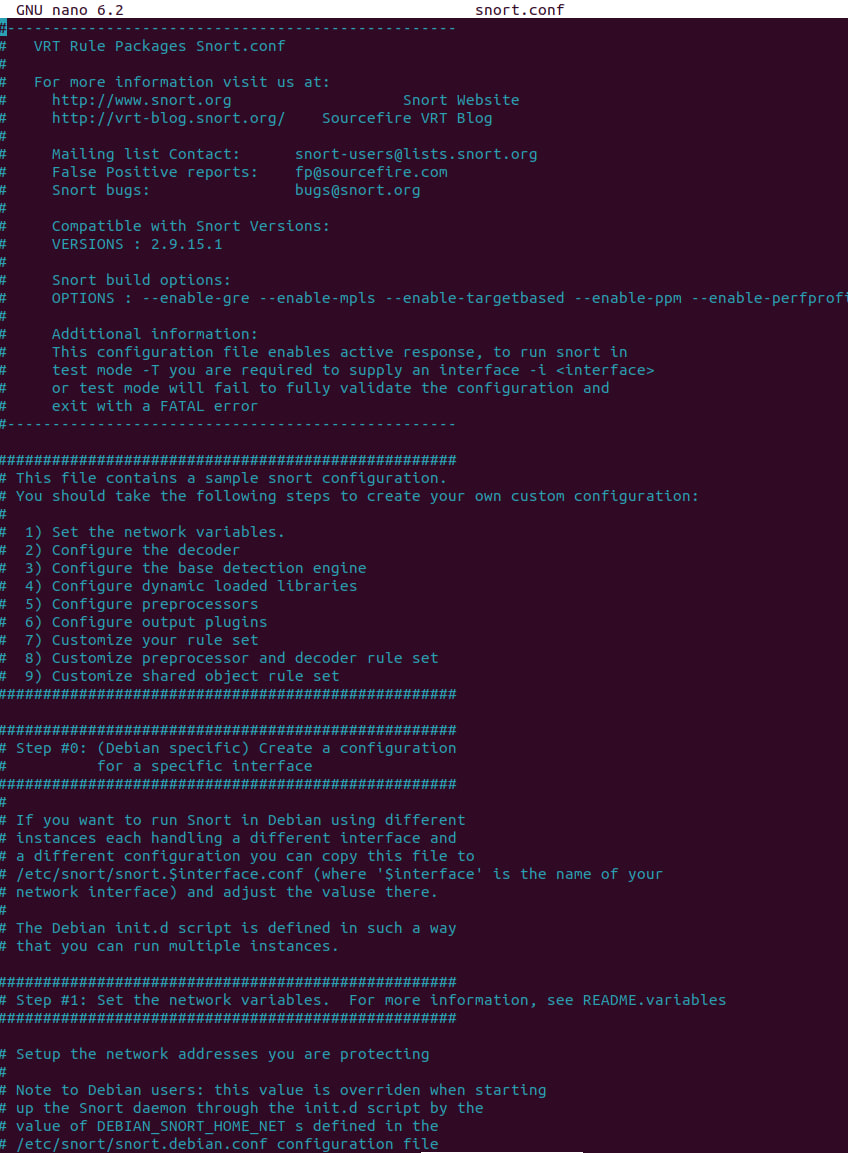
1. После этого установка Snort завершена, проверим версию командой snort –version

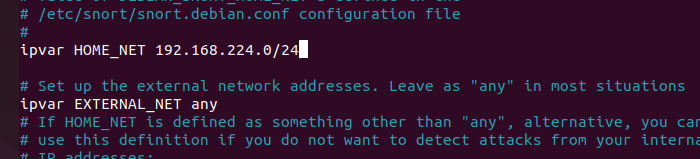


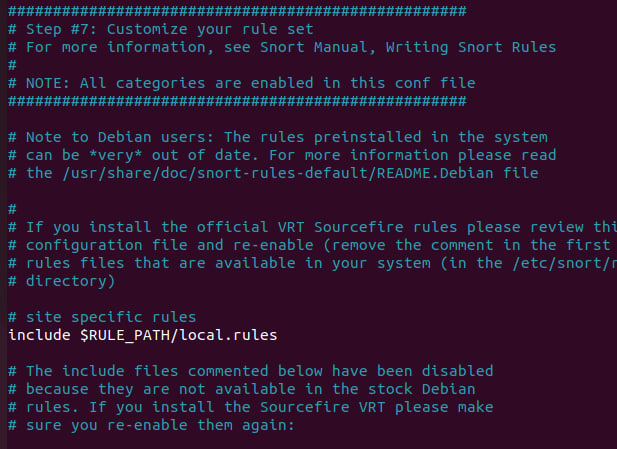
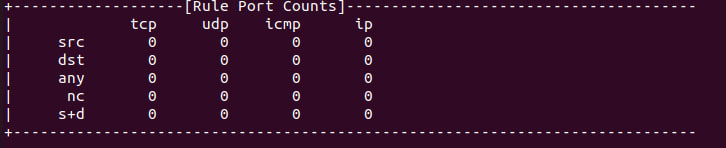
1. Далее необходимо установить беспорядочный режим, что бы сетевая карта захватывала все пакеты, которые проходят по сети. Для этого нужно ввести команду sudo ip link set ens33 promisc on C:\Users\gesha\Downloads\Telegram Desktop\image_2024-01-21_06-49-22.png
2. После необходимо перейти по пути /etc/snort/ что бы добраться до конфигурационных файлов Snort.

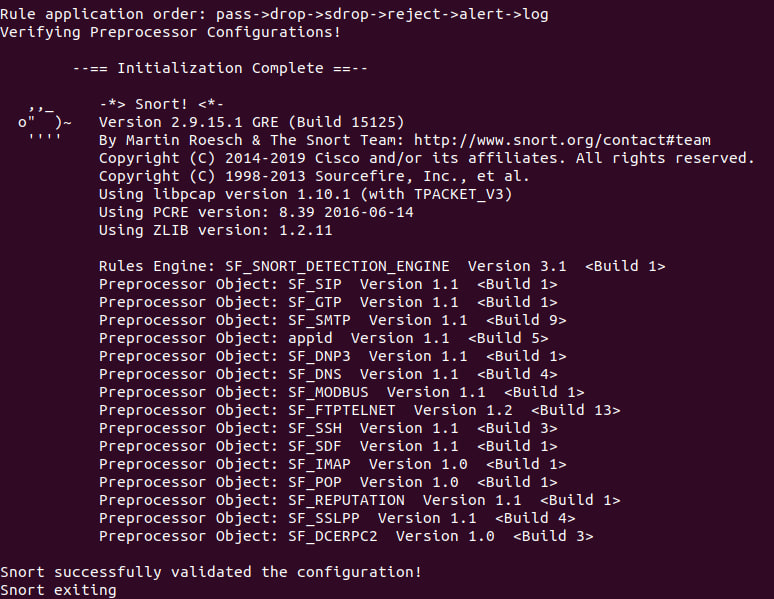


1. Дальше действия будут выполняться в конфигурационном файле snort.conf. При открытии файла мы увидим 9 разделов настройки первоочередно мы должны указать адрес нашей подсети





1. Далее необходимо перейти в файл с локальными правилами, для выполнения задания, чтобы узнать его местоположение достаточно открыть раздел 7(customize your rule set) и там мы обнаружим, что файл в котором будет находиться наше будущее правило располагается в папке rules по пути /etc/snort/rules/local.rules/ 
2. Закомментируем остальные правила для добства детектирования работы нашего правила. После при запуске Snort мы должны увидеть, что нет записей в правилах по каким-либо портам. Запустить Snort можно с помощью команды sudo snort –T –c/etc/snort/snort.conf



1. Далее необходимо перейти в режим конфигурации файла local.rules и выполнить вторую часть практической работы, а именно: Создать правило для Snort, которое срабатывает при обнаружении всех входящих tcp-пакетов на Ваш ip-адрес с выводом соответствующего сообщения.

Далее следуя методичке можно увидеть пример написания такого же правила, только срабатывающего на все входящие пакеты на наш ip-адрес, чтобы понять как это выполнить обратимся к методичке, где описано правило:

**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.

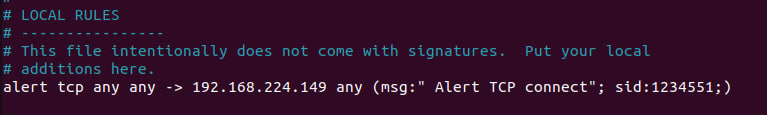
**any any**: Эти части указывают исходный IP-адрес и порт отправителя. "any" означает "любой", то есть правило применяется ко всем исходящим IP-адресам и портам.

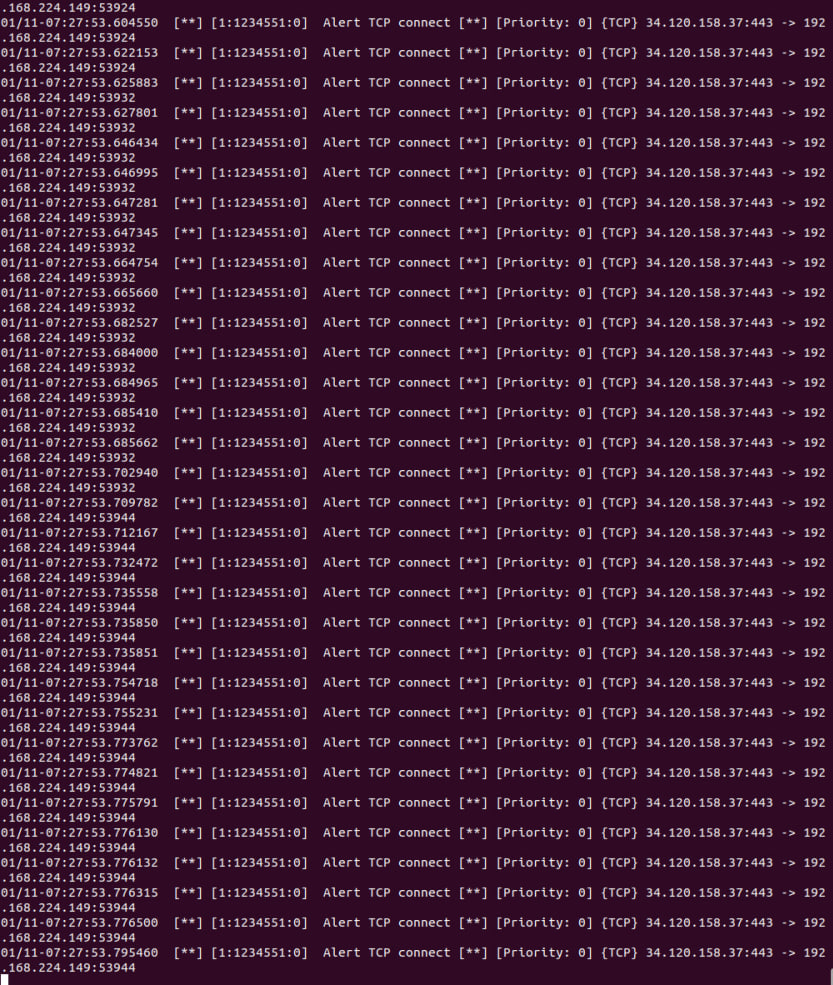
->: Эта часть разделяет данные об исходе (source) и данных о назначении (destination).

**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.

1. Перейдя в режим конфигурации файла local.rules напишим наше правило



1. Далее опять запустим Snort командой из пункта 10 и увидим срабатывания нашего правила 

**Вывод:** Ознакомившись с методическими материалами и документацией было написано правило срабатывния на все tcp входящие tcp пакеты на наш адрес.