

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-02-22

Выполнил:

Казаков М.В.

Проверил:

Пимонов Р.В.

Москва, 2023

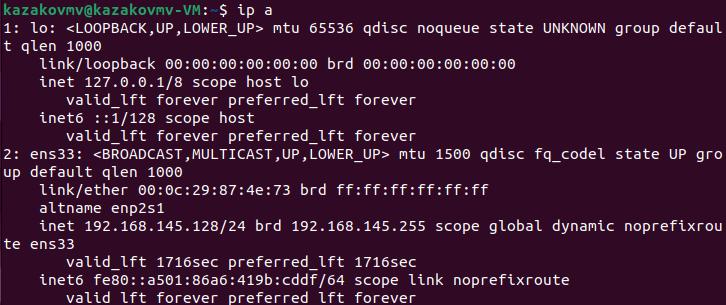
**Задание на практическую работу:**

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.

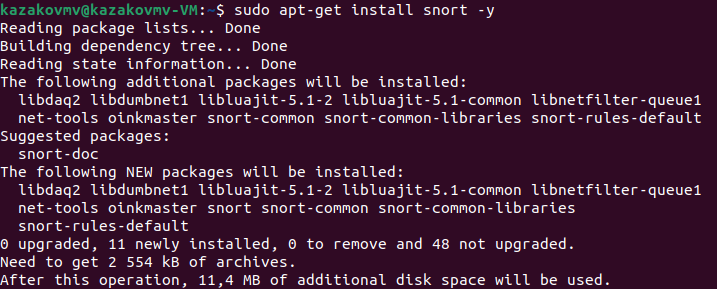
**Ход работы**

**Подготовка SNORT**

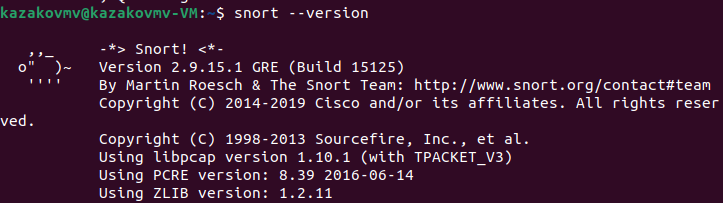
1. Необходимо знать IP-адрес виртуальной машины



1. Установка Snort через терминал, используя sudo apt-get install snort –y



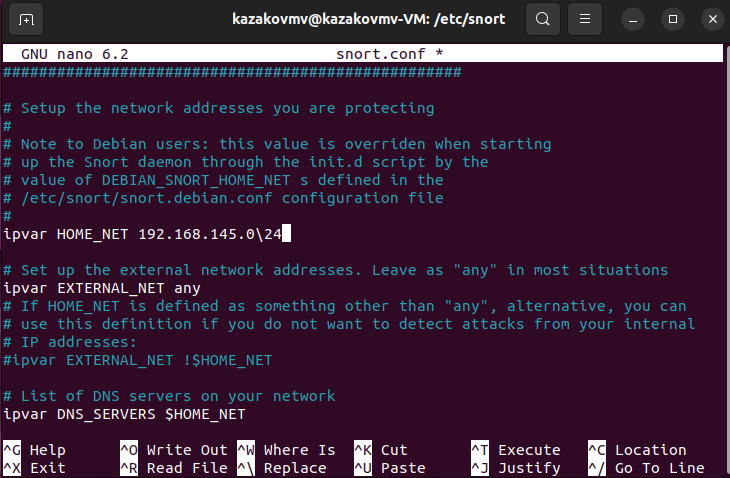
1. После установки Snort, появляется окно конфигурации, гле необходимо задать сеть. В текущем сетью является 192.168.145.0/24
2. Для проверки правильности установки Snort, можно сделать узнать версию snort командой snort --version.



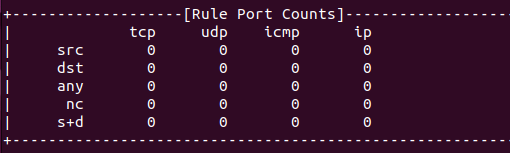
1. Далее необходимо установить режим, позволяющий сетевой карте захватывать все пакеты в сети.



1. Далее, переходим в каталог /etc/snort/, где дальше будет происходить работа с файлами конфигурации. Для начала необходимо указать локальную сеть в файле snort.conf



1. Далее, для более удобного отслеживания работы созданного правила, вынесем в комментарии все заводские правила. В результате чего, после запуска Snort, в терминале не будет записей о портах.



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.

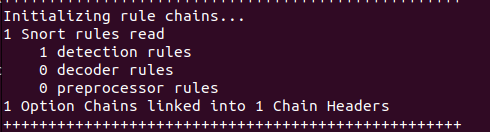
**any any**: Эти части указывают исходный IP-адрес и порт отправителя. "any" означает "любой", то есть правило применяется ко всем исходящим IP-адресам и портам.

->: 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. Для выполнения второго задания практической работы, необходимо отредактировать файл локальных правило, где будет указано правило из задания. Далее, запускаем Snort, где указано, что правило обнаружено и задействованно.



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