МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «МЭИ»

**Факультет/институт** «Инженерно-экономический институт»

(название факультета/института)

**Кафедра** «Безопасности и информационных технологий»

(название кафедры)

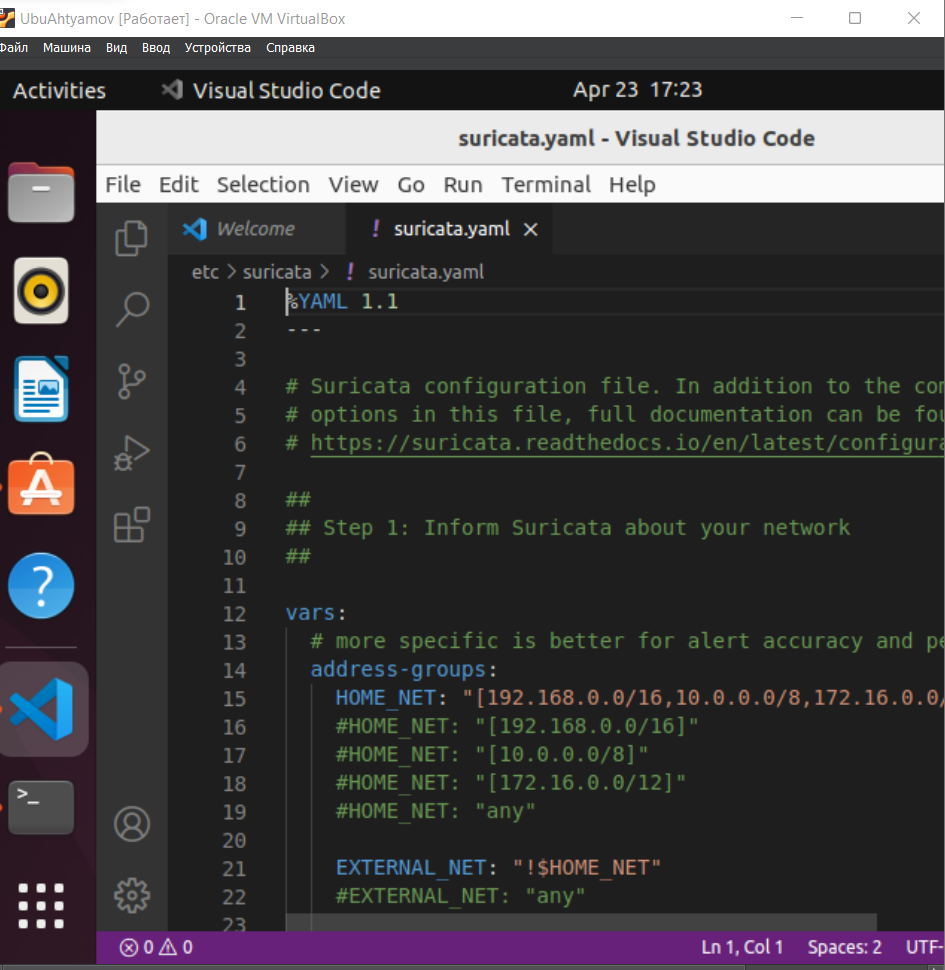
**Лабораторная работа № 4**

**Дисциплина:**Технологии защиты информационных систем от кибератак  
**Тема: Suricata и ELK**

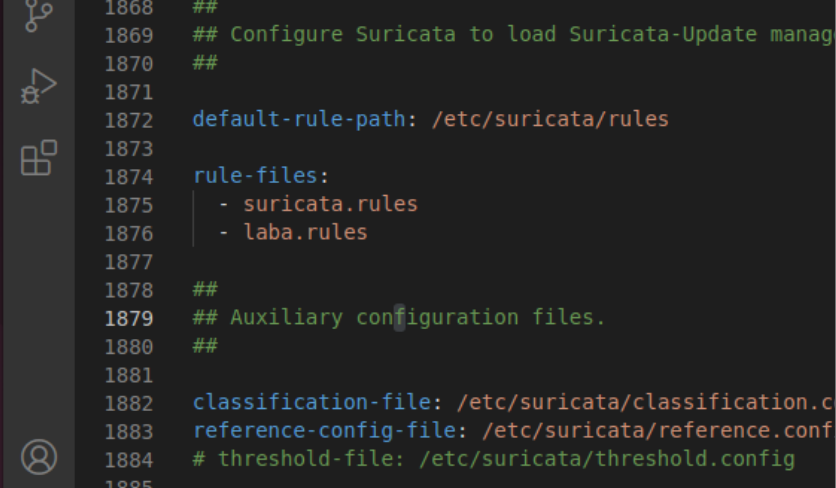
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Выполнил студент | | |  | | | курса | | | |
| очно-заочной формы обучения | | | | | | | |
| Группа №: | ИЭ-41-20 | | | | | | | |
| ФИО: | Ахтямов В.И. | | | | | | | |
| Проверил |  | | | | | | | |
| ФИО: | Дратвяк А.В. | | | | | | | |
| дата проверки: | « |  | | » |  | | 2023г. | |
| Оценка: |  | | | | | | | |

Часть 1

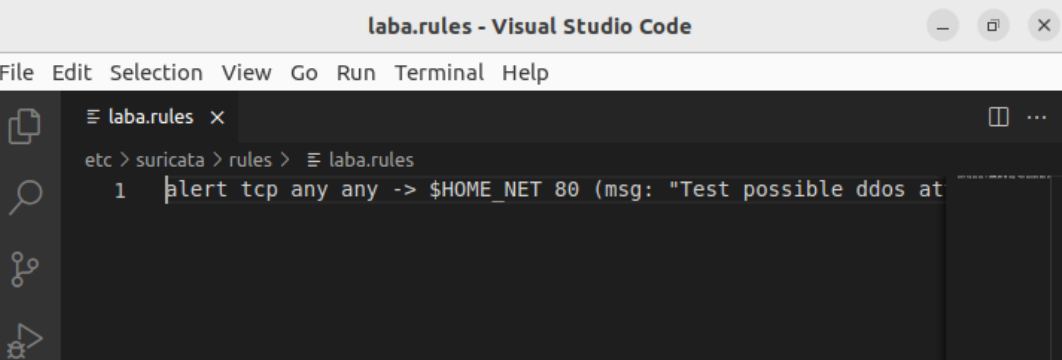
Редактируем suricata. yaml



8. Добавляем наш будущий файлик с нашими правилами



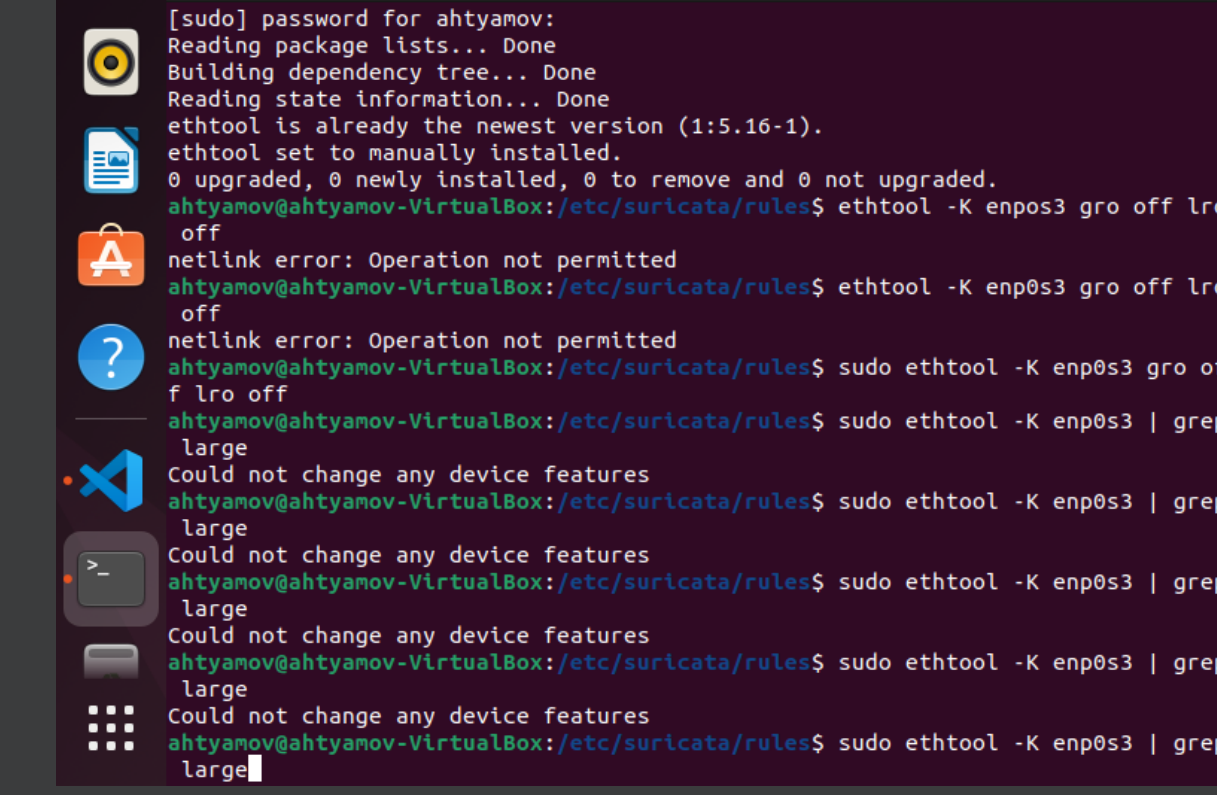
9. Создаем наши правила



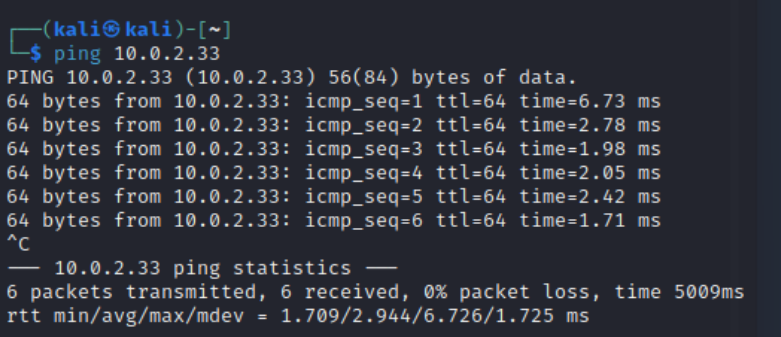
10. Настраиваем сетевой интерфейс

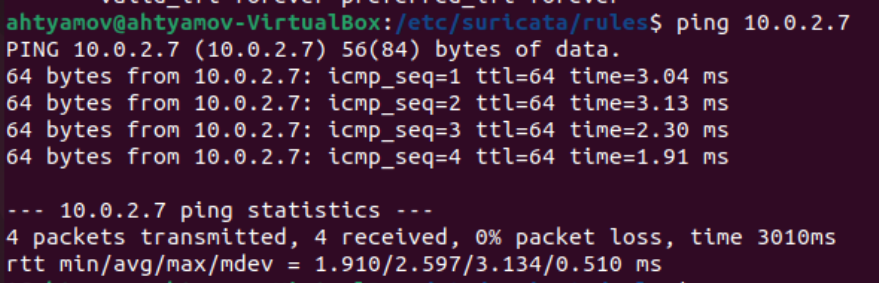
sudo apt install ethtool

ethtool -K enp0s3 gro off lro off



Проверяем пинги в обе стороны

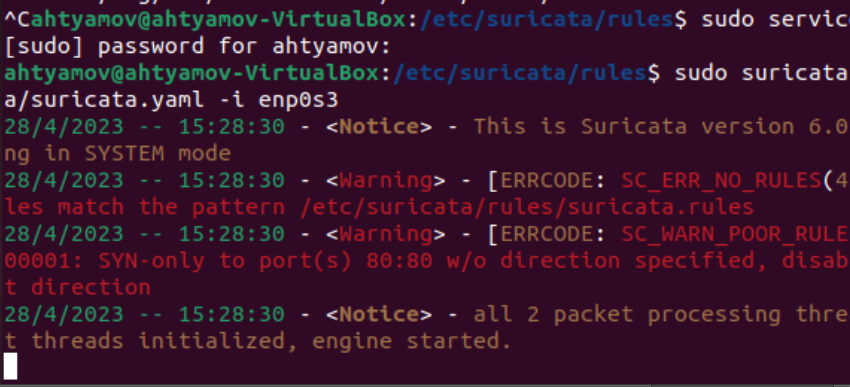




Запускаем Suricata

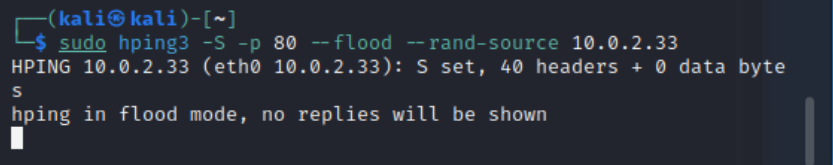
sudo service suricata restart

sudo suricata -c /etc/suricata/suricata.yaml -i enp0s3



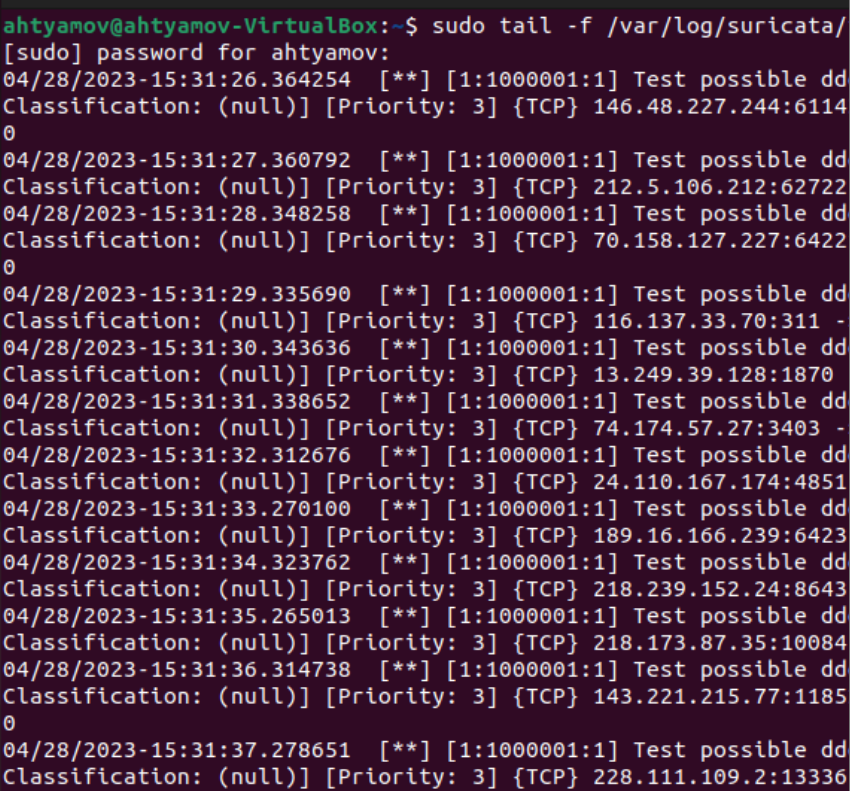
sudo apt install hping3

sudo hping3 -S -p 80 --flood --rand-source 10.0.2.15



Посмотри наши логи Suricata

sudo tail -f /var/log/suricata/fast.log



Эластик скачался при помощи freeopenVPN

Но кибана нет, пришлось скачивать через более навороченный vpn на телефоне и передавать архив на комп

Далее скинул на флешку, но опять проблема не дает перенести файл с флешки хоть куда-то в систему – говорит не хватает места – решение нашел в этой статье

https://askubuntu.com/questions/540142/not-enough-space-when-trying-to-transfer-files-from-one-hdd-to-another