МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

Мегафакультет трансляционных информационных технологий

Факультет информационных технологий и программирования

**Лабораторная работа №02**

**По дисциплине «Информационная безопасность»**

**Сетевая безопасность.**

Выполнил студент

группы № М34081

Зайцев Артем Павлович

Проверил:

Едрец Илья Григорьевич

*САНКТ-ПЕТЕРБУРГ*

*2023*

**1)** **Запуск Nmap**

Проверим свой ip

Изображение выглядит как текст

Автоматически созданное описание

Пропингуем его

Изображение выглядит как текст

Автоматически созданное описание

Пробуем nmap -O

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

Установим ssh-server

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

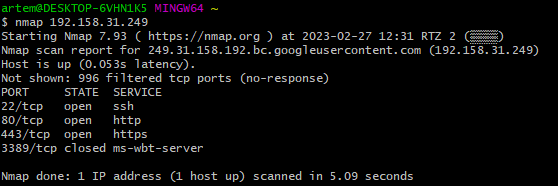
Автоматически созданное описание

Запустим как службу

Изображение выглядит как текст

Автоматически созданное описание

Появился новый порт 22/tcp



Определяем ОС

Изображение выглядит как текст

Автоматически созданное описание

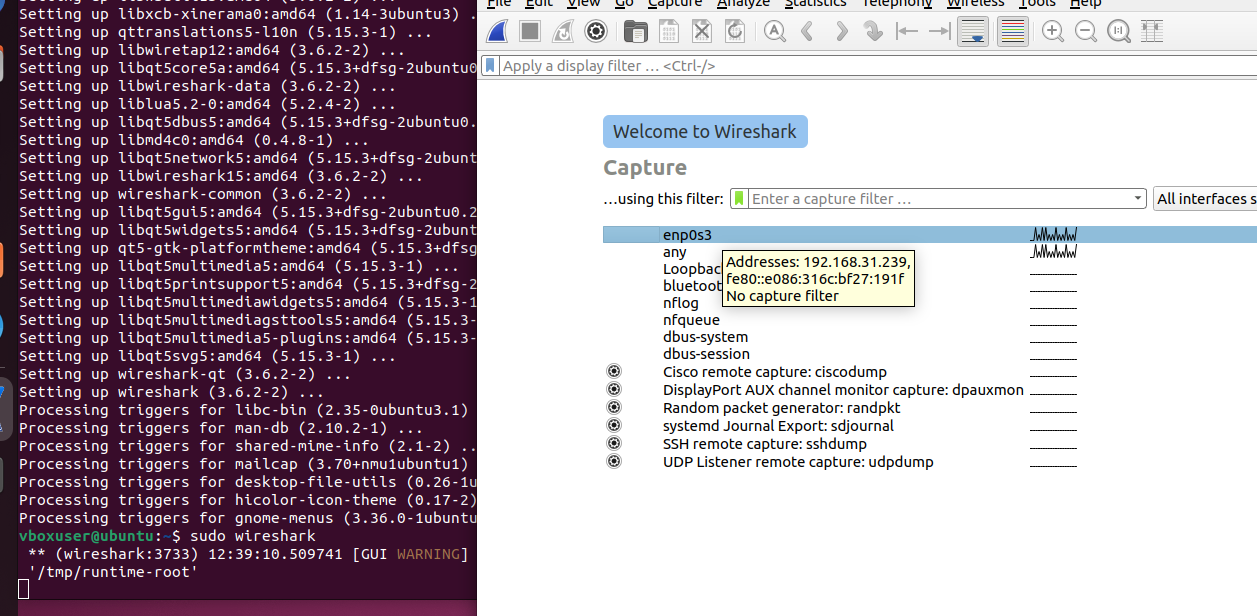
**2) Анализируем отправленные пакеты используя Wireshark**

Установим wireshark

Изображение выглядит как текст

Автоматически созданное описание

Запустим утилиту и выбираем сетевой интерфейс



Запустим enp и утилиту nmap:

Изображение выглядит как стол

Автоматически созданное описание

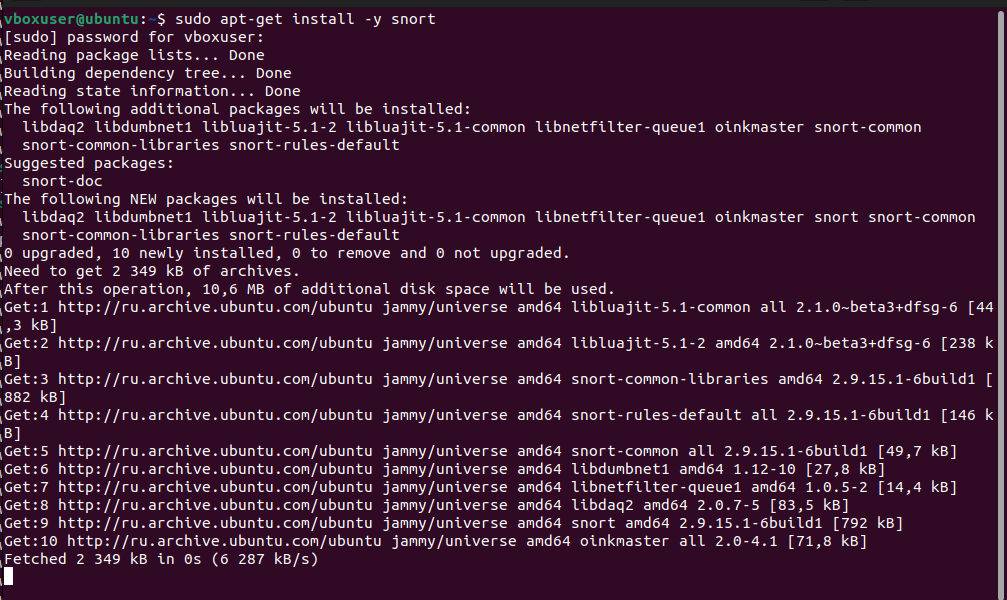
**3) Разбираемся в том какие именно пакеты были использованы для определения версии ОС**

Запустим nmap -o

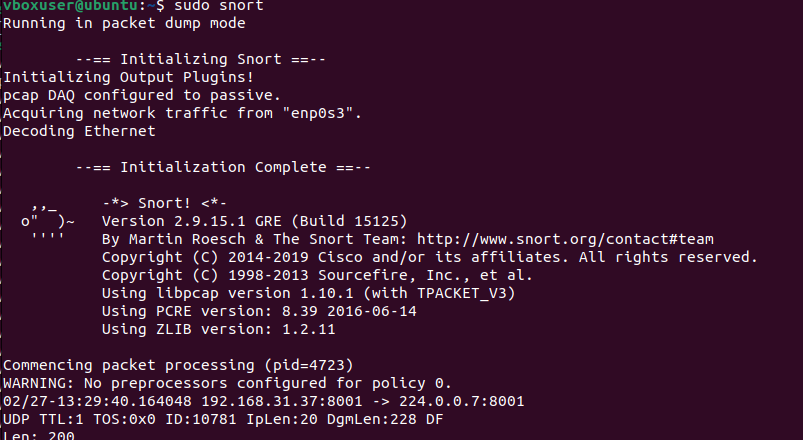
Изображение выглядит как стол

Автоматически созданное описание

**4) Устанавливаем систему обнаружения атак Snort**



Sudo snort

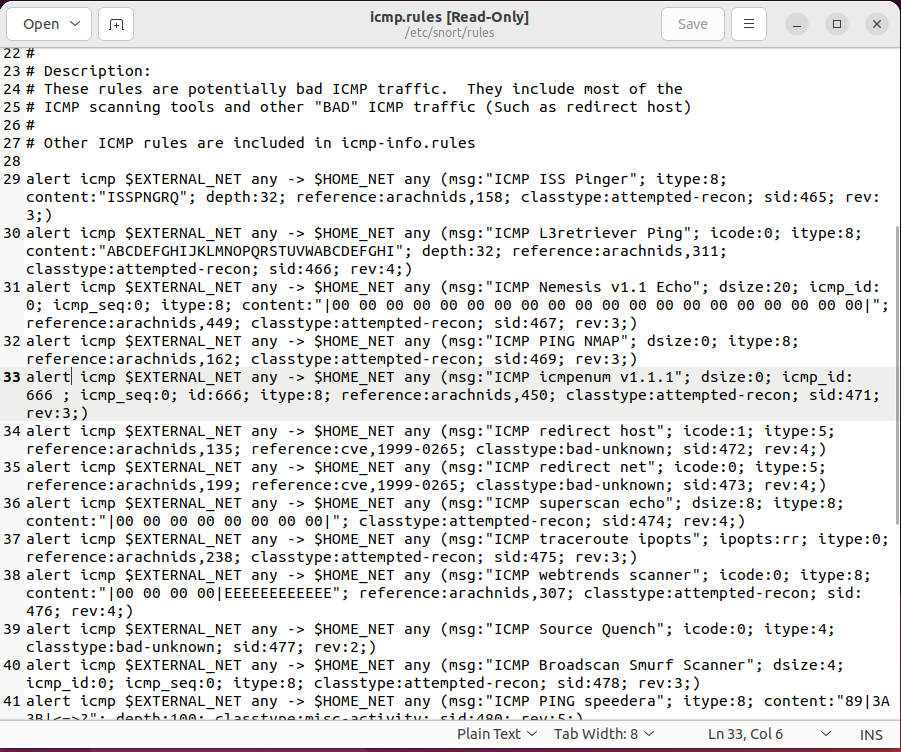


Посмотрим правила

Изображение выглядит как текст

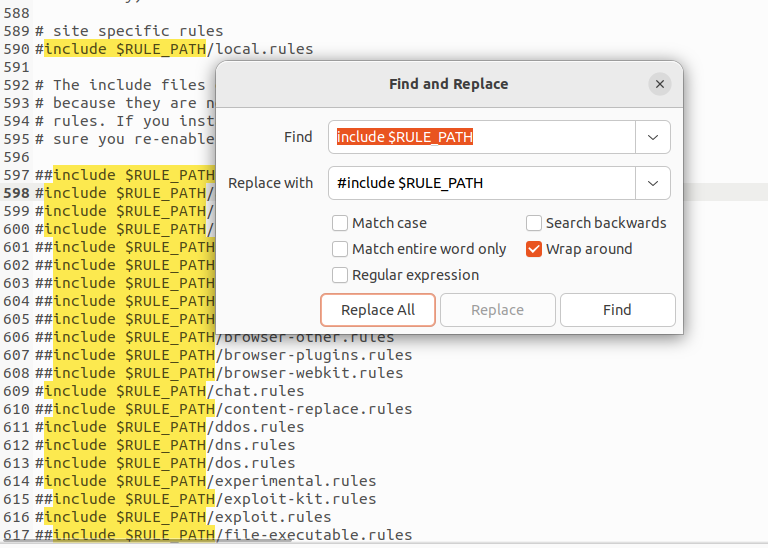
Автоматически созданное описание

Gedit /etc/snort/rules/icmp.rules

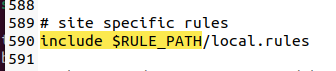


Напишем свое правило

Sudo gedit /etc/snort/snort.conf

Закоментим все подключенные правила 

Оставим

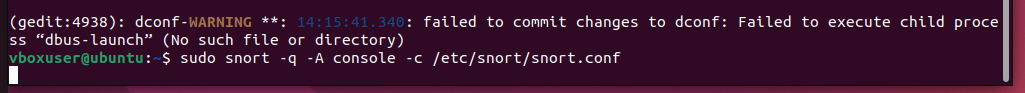


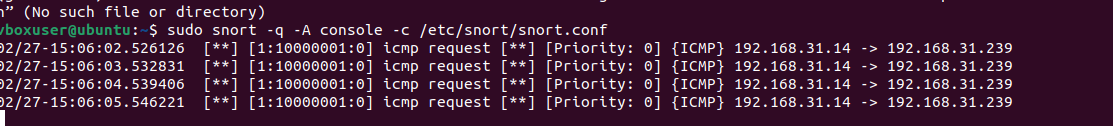
Написали свое правило

Изображение выглядит как текст

Автоматически созданное описание

Запустим snort с выводом в консоль





Добавим rev:1 для отслеживания nmap

Изображение выглядит как текст

Автоматически созданное описание

Проверка

