Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет безопасности информационных технологий

Дисциплина:

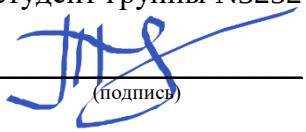
«Операционные системы»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №9

«Фильтр сетевых пакетов»

Выполнил:

Рядовой Т.С., студент группы N3252



(подпись)

Проверил:

Чебунин Константин Олегович

(отметка о выполнении)

(подпись)

Санкт-Петербург

2023 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель работы – познакомиться с работой сетевых пакетов, инструментом управления сетью iptables.

В обычном варианте:

- Написать фильтр сетевых пакетов на основе nfqueue и iptables;
- Протестировать скорость работы.

1 СЕТЕВЫЕ ПАКЕТЫ И IPTABLES

1.1 Задание

Настроить сетевой пакет и протестировать при разных режимах работы.

1.2 Написание фильтра

Напишем и скомпилируем программу на языке Python. Предварительно установим необходимые для работы библиотеки и зависимости (scapy и NetfilterQueue через pip). Строка «os.system("sudo iptables -A INPUT -j NFQUEUE --queue-num 0")» выполняет команду через системную оболочку, добавляя правило iptables для направления входящих пакетов в netfilterqueue с номером 0. В блоке try-except программа запускает бесконечный цикл NetfilterQueue, в котором она ожидает появления пакетов в очереди и вызывает функцию обратного вызова для их обработки. Прерывание выполнения программы осуществляется при нажатии комбинации клавиш Ctrl+C, после чего происходит корректное завершение работы, и очередь отключается. Тестирование происходит с помощью утилиты speedtest-cli для терминала от speedtest.

Листинг 1 – packet_filtet.py

```
from scapy.all import *
from netfilterqueue import NetfilterQueue
import os

os.system("sudo iptables -A INPUT -j NFQUEUE --queue-num 0")

def packet_callback(packet):
    ip_packet = IP(packet.get_payload())
    packet.accept()


nfqueue = NetfilterQueue()
nfqueue.bind(0, packet_callback)

try:
    print("---packet filtering started---")
    nfqueue.run()
except KeyboardInterrupt:  # ctrl + c
    print("---packet filtering stopped---")
    nfqueue.unbind()
```

Сначала протестируем входящий и исходящий трафик без работающего iptables. Для правдоподобности тестируем 3 раза. Итого: средняя входящая скорость составила 254 Мбит/с, а средняя исходящая 251 Мбит/с.

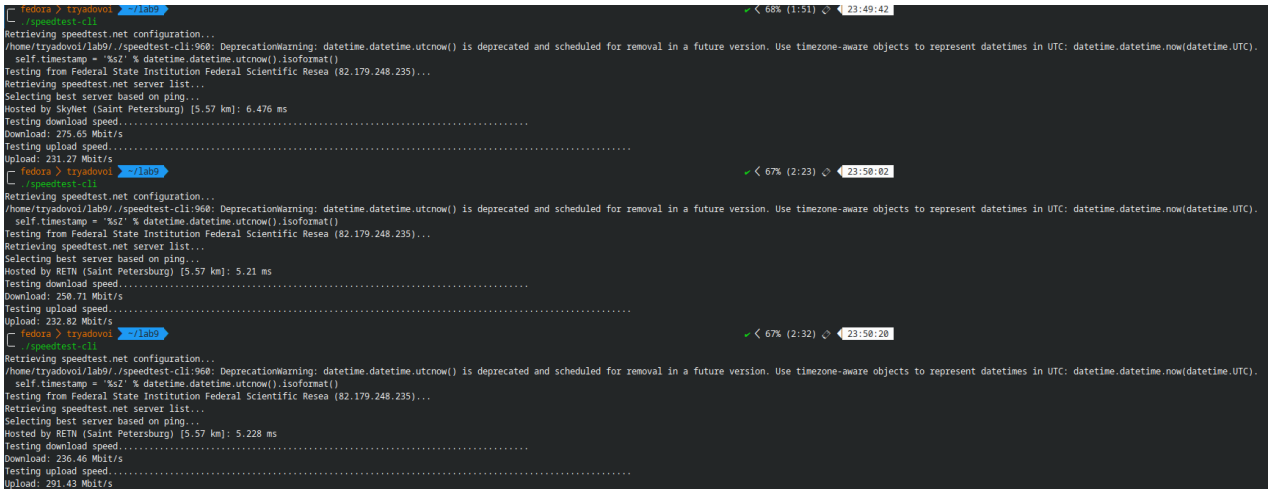


Рисунок 1 – Тесты без ограничений

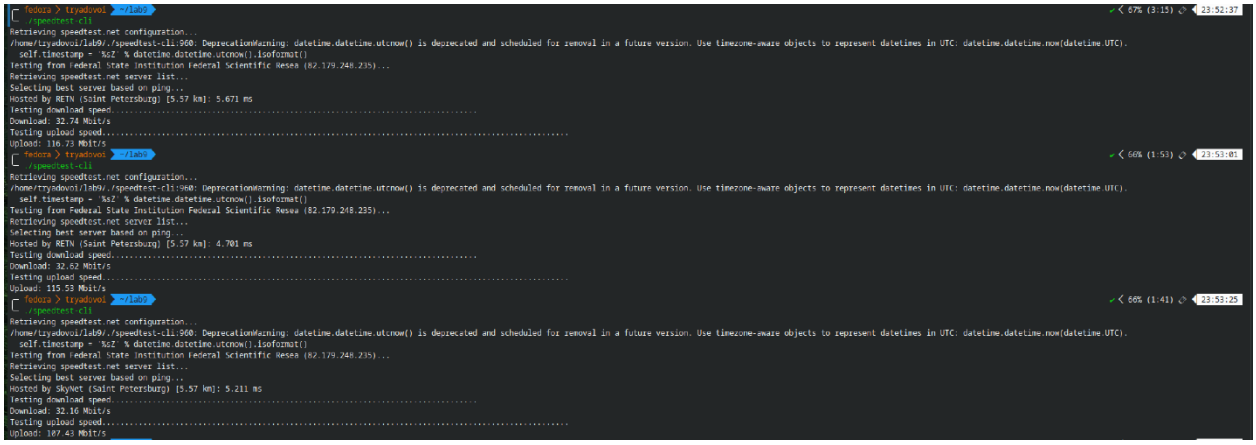


Рисунок 2 – Тесты с работающим iptables

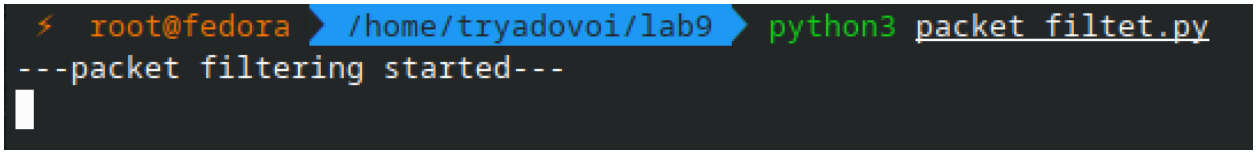


Рисунок 3 – Работа программы

Итоги второго тестирования (iptables on): средняя входящая скорость составила 32 Мбит/с, средняя исходящая 113 Мбит/с.

По результатам тестов видно значительное ограничение как входящего, так и исходящего трафика, причем у первого показатель больше. Так как строка настройки iptables с INPUT, те входящий трафик. Если мы хотим ограничить исходящий меняем INPUT на OUTPUT («os.system("sudo iptables -A OUTPUT -j NFQUEUE --queue-num 0")»).

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы мне удалось достигнуть поставленных целей:

Обычного варианта:

- Познакомиться с работой сетевых пакетов;
- Настроил iptables;
- Написал фильтр входящего трафика на python.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. https://habr.com/ru/articles/747616/
2. https://blog.finxter.com/fixed-modulenotfounderror-no-module-named-scapy/