

**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.....	4
1 Сетевые пакеты и iptables.....	5
1.1 Задание.....	5
1.2 Написание фильтра.....	5
Заключение.....	7
Список использованных источников	8

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.

```

[~] /home/tryadovoi/lab9
[~] /speedtest-cli
Retrieving speedtest.net configuration...
/home/tryadovoi/lab9/.speedtest-cli:960: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
self.timestamp = "%sZ" % datetime.datetime.utcnow().isoformat()
Testing from Federal State Institution Federal Scientific Resea (82.179.248.235)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by SkyNet (Saint Petersburg) [5.57 km]: 6.476 ms
Testing download speed.....
Download: 275.65 Mbit/s
Testing upload speed.....
Upload: 231.27 Mbit/s
[~] /home/tryadovoi/lab9
[~] /speedtest-cli
Retrieving speedtest.net configuration...
/home/tryadovoi/lab9/.speedtest-cli:960: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
self.timestamp = "%sZ" % datetime.datetime.utcnow().isoformat()
Testing from Federal State Institution Federal Scientific Resea (82.179.248.235)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by RETN (Saint Petersburg) [5.57 km]: 5.21 ms
Testing download speed.....
Download: 250.71 Mbit/s
Testing upload speed.....
Upload: 232.82 Mbit/s
[~] /home/tryadovoi/lab9
[~] /speedtest-cli
Retrieving speedtest.net configuration...
/home/tryadovoi/lab9/.speedtest-cli:960: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
self.timestamp = "%sZ" % datetime.datetime.utcnow().isoformat()
Testing from Federal State Institution Federal Scientific Resea (82.179.248.235)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by RETN (Saint Petersburg) [5.57 km]: 5.228 ms
Testing download speed.....
Download: 236.46 Mbit/s
Testing upload speed.....
Upload: 291.43 Mbit/s

```

Рисунок 1 – Тесты без ограничений

```

[~] /home/tryadovoi/lab9
[~] /speedtest-cli
Retrieving speedtest.net configuration...
/home/tryadovoi/lab9/.speedtest-cli:960: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
self.timestamp = "%sZ" % datetime.datetime.utcnow().isoformat()
Testing from Federal State Institution Federal Scientific Resea (82.179.248.235)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by RETN (Saint Petersburg) [5.57 km]: 5.671 ms
Testing download speed.....
Download: 32.74 Mbit/s
Testing upload speed.....
Upload: 116.73 Mbit/s
[~] /home/tryadovoi/lab9
[~] /speedtest-cli
Retrieving speedtest.net configuration...
/home/tryadovoi/lab9/.speedtest-cli:960: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
self.timestamp = "%sZ" % datetime.datetime.utcnow().isoformat()
Testing from Federal State Institution Federal Scientific Resea (82.179.248.235)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by RETN (Saint Petersburg) [5.57 km]: 4.701 ms
Testing download speed.....
Download: 30.53 Mbit/s
Testing upload speed.....
Upload: 115.55 Mbit/s
[~] /home/tryadovoi/lab9
[~] /speedtest-cli
Retrieving speedtest.net configuration...
/home/tryadovoi/lab9/.speedtest-cli:960: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
self.timestamp = "%sZ" % datetime.datetime.utcnow().isoformat()
Testing from Federal State Institution Federal Scientific Resea (82.179.248.235)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by SkyNet (Saint Petersburg) [5.57 km]: 5.211 ms
Testing download speed.....
Download: 32.16 Mbit/s
Testing upload speed.....
Upload: 107.43 Mbit/s

```

Рисунок 2 – Тесты с работающим iptables

```

root@fedora /home/tryadovoi/lab9 python3 packet_filtet.py
---packet filtering started---
```

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/>