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

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Вычислительные сети и контроль безопасности в компьютерных сетях»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

«Настройка межсетевого экрана»

**Выполнили:**

Молитвин Илья Алексеевич, студент группы N3345

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Бучаев Абдулхамид Яхьяевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Содержание**

[1 НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА 4](#_30j0zll)

[1.1 Настройка лабораторного стенда 4](#_1fob9te)

[1.2 Блокировка исходящего трафика 4](#_f54bn5mjd81a)

[1.3 Ограничение приема и передачи пакетов 5](#_smb7yqdqwetq)

[1.4 Трансляция адресов источников 6](#_pvdpf0cbrfu1)

[1.5 Блокировка атаки bruteforce на SSH 7](#_utaebpf7oelp)

[1.6 Конфигурация межсетевого экрана 8](#_893bv31mkni5)

**Введение**

Цель работы – изучить на примере netfilter/iptables основные принципы работы

межсетевых экранов. Освоить базовую настройку правил iptables.

Для достижения поставленной цели необходимо решить следующие задачи:

− настроить лабораторный стенд;

− настроить маршрутизацию проходящего трафика на локальном сервере;

− выполнить необходимые настройки межсетевого экрана на локальном

сервере в соответствии с заданием:

1. заблокировать весь исходящий трафик, кроме портов для SSH и веб-сервера

2. запретить прием и передачу всех пакетов, размер которых превышает 600

байт, а значение TTL при этом больше 10.

3. настроить трансляцию адресов источников для всего транзитного трафика,

проходящего через данный шлюз

4. реализовать блокирование атаки bruteforce на сервис SSH локального сервера.

Если за последние 10 минут с одного адреса было 5 и более новых SSH

соединений, адрес блокируется. Блокировка должна работать только в рамках

сервиса SSH и не влиять на другие сервисы.

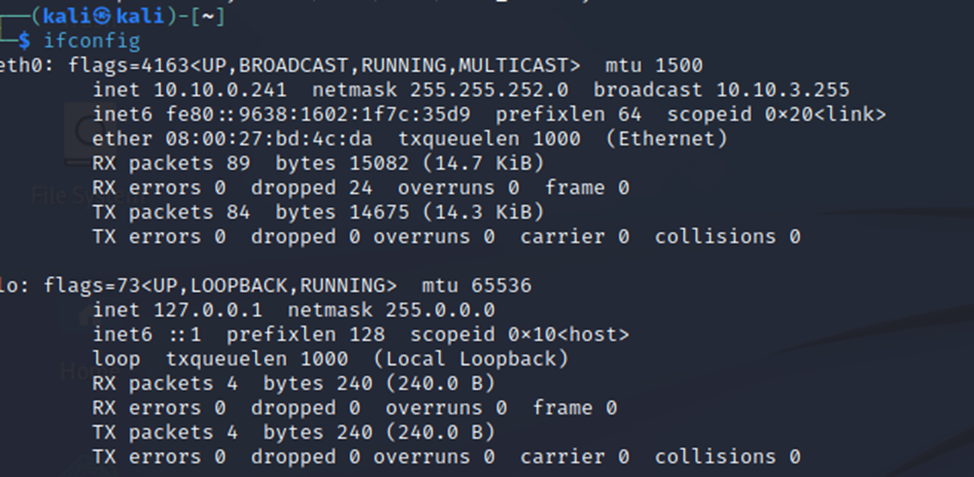
− протестировать работу выполненных настроек.

# НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА

## **Настройка лабораторного стенда**

Настроить лабораторный стенд, включающий: Локальный сервер / Межсетевой

экран, клиент, удаленный сервер.



1. *IP второй машины*

## **Блокировка исходящего трафика**

Блокировка исходящего трафика, кроме портов для SSH и веб-сервера. Для этого используем команду:

iptables -A OUTPUT -p tcp -m multiport ! --dport 22,80,443 -j DROP.

-A OUTPUT добавляет новое правило в цепочку OUTPUT (для пакетов,

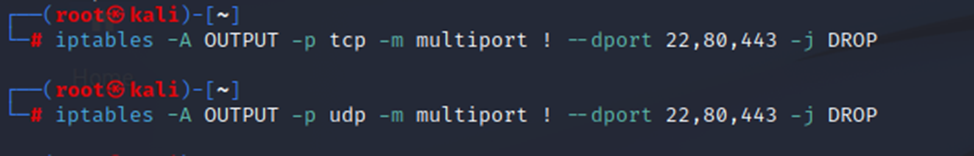
отправленных с этого сервера);

-p tcp указывает на протокол (в данном случае TCP);

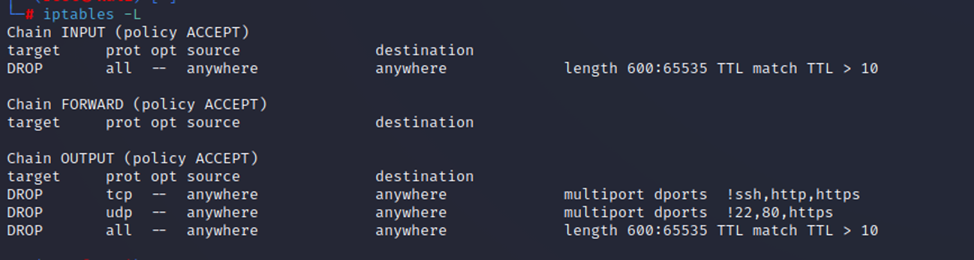
-m multiport позволяет указывать в тексте правила несколько портов;

! --dport 22,80,443 указывает на все порты кроме 22(SSH), 80(HTTP), 443(HTTPS);

-j DROP указывает, что все пакеты, соответствующие этому правилу, должны быть отброшены.



1. *Блокировка исходящего трафика*



1. *Блокировка исходящего трафика*

## **Ограничение приема и передачи пакетов**

Запретить прием и передачу всех пакетов, размер которых превышает 600 байт, а

значение TTL при этом больше 10. Для этого используем команды:

iptables -A INPUT -m length --length 600: -m ttl --ttl-gt 10 -j DROP

iptables -A OUTPUT -m length --length 600: -m ttl --ttl-gt 10 -j DROP

-A INPUT добавляет новое правило в цепочку OUTPUT (для пакетов, отправленных

с этого сервера);

-A OUTPUT добавляет новое правило в цепочку OUTPUT (для пакетов,

отправленных с этого сервера);

-m length –length 600: условие, которое проверяет длину пакета и применяет правило к пакетам определенной длины (в данном случае, от 600 байт и выше);

-m ttl –ttl-gt 10 условие, которое проверяет значение TTL (Time to Live) в заголовке

IP-пакета и применяет правило к пакетам с TTL больше 10;

-j DROP указывает, что все пакеты, соответствующие этому правилу, должны быть

отброшены.



1. *Ограничение на пакеты*



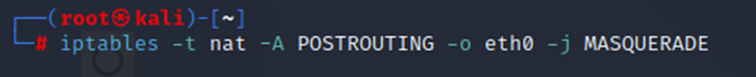
1. *Ограничение на пакеты*

## **Трансляция адресов источников**

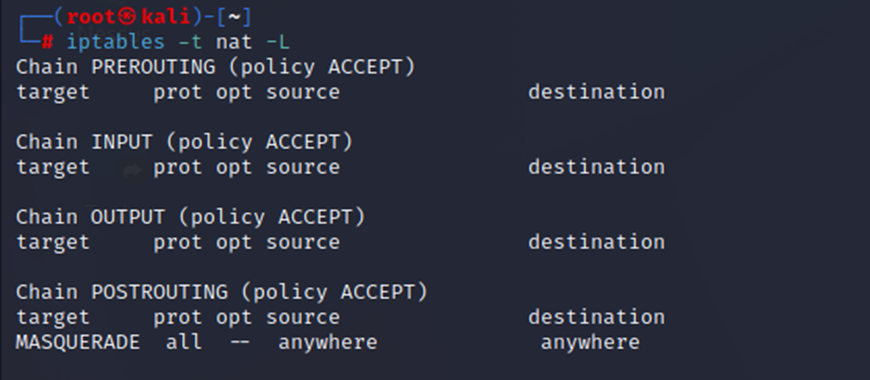
Настроить трансляцию адресов источников для всего транзитного трафика,

проходящего через данный шлюз. Для этого используем команду:

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE



1. *Трансляция адресов*



1. *Трансляция адресов*

## **Блокировка атаки bruteforce на SSH**

Реализовать блокирование атаки bruteforce на сервис SSH локального сервера. Если за последние 10 минут с одного адреса было 5 и более новых SSH соединений, адрес блокируется. Блокировка должна работать только в рамках сервиса SSH и не влиять на другие сервисы.

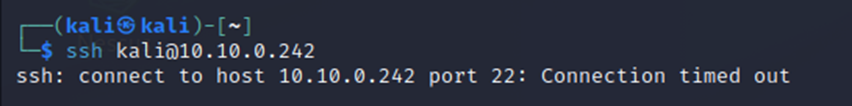
**

1. *Блокировка атаки brutforce*

**

1. *Блокировка атаки brutforce*

На рисунке 8 можно увидеть, что при попытке в пятый раз подключиться по SSH возникла ошибка, то есть за период в 10 минут невозможно более чем 4 подключения с одного адреса.

**

1. *Проверка настройки iptables*

## **Конфигурация межсетевого экрана**

На рисунке 9 приведена итоговая конфигурация межсетевого экрана с применением настроек, необходимых по заданию.



1. *Конфигурация межсетевого экрана*

**Заключение**

В ходе выполнения лабораторной работы были решены следующие задачи:

− настроен лабораторный стенд;

− настроена маршрутизация проходящего трафика на локальном сервере;

− выполнены необходимые настройки межсетевого экрана на локальном

сервере в соответствии с заданием;

− протестирована работа выполненных настроек.

Таким образом, все поставленные задачи решены, цель достигнута.

**СПИСОК ИСПОЛЬЗУЕМЫХ МАТЕРИАЛОВ**

1. [**https://www.opennet.ru/docs/RUS/iptables/**](https://www.opennet.ru/docs/RUS/iptables/)
2. **https://stuffphilwrites.com/2014/09/iptables-processing-flowchart/**
3. **https://habr.com/ru/articles/747616/**