**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 №4**

«Настройка межсетевого экрана»

**Выполнили:**

Нгуен Хоанг Хиеп, студент группы N33471

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

(подпись)

Чан Нгок Хуан, студент группы N33471

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

(подпись)

Чыонг Тан Зыонг, студент группы N33471

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

(подпись)

**Проверил:**

Есипов Дмитрий Андреевич, ассистент ФБИТ

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

(отметка о выполнении)

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

(подпись)

Санкт-Петербург

2022г.

Содержание

[Содержание 2](#_Toc119535050)

[Введение 3](#_Toc119535051)

[1 НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА 4](#_Toc119535052)

[1.1 Задание 4](#_Toc119535053)

[1.2 Ход работы 4](#_Toc119535054)

[1.2.1 Подготовка 4](#_Toc119535055)

[1.2.2 Задание 1 5](#_Toc119535056)

[1.2.3 Задание 2 6](#_Toc119535057)

[1.2.4 Задание 3 7](#_Toc119535058)

[1.2.5 Задание 4 8](#_Toc119535059)

[Заключение 11](#_Toc119535060)

[Список использованных источников 12](#_Toc119535061)

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, включающий: локальный сервер/межсетевой экран, клиент, удаленный сервер;
* настроить маршрутизацию проходящего трафика на локальном сервере;
* выполнить необходимые настройки межсетевого экрана на локальном сервере в соответствии с заданием;
* протестировать работу выполненных настроек;
* результаты выполнения работы оформить в виде отчета.

# НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА

## Задание

Вариант 1

Задание 1: Заблокировать весь исходящий трафик, кроме портов для SSH и веб-сервера.

Задание 2: Запретить прием и передачу всех пакетов, размер которых превышает 600 байт, а значение TTL при этом больше 10.

Задание 3: Настроить трансляцию адресов источников для всего транзитного трафика, проходящего через данный шлюз.

Задание 4: Реализовать блокирование атаки brutforce 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.

## Ход работы

### Подготовка

**ifconfig** означает «конфигурация интерфейса». Он используется для просмотра и изменения конфигурации сетевых интерфейсов в вашей системе [1].

Используем команду **ifconfig**, чтобы просмотреть конфигурацию интерфейса Kali (рисунок 1) и Ubuntu (рисунок 2).

Text

Description automatically generated

Рисунок 1 – IP-адрес стенда с настройками межсетевого экрана

Text

Description automatically generated

Рисунок 2 – IP-адрес стенда для проверки

**iptables** - это утилита командной строки, используемая для управления встроенным брандмауэром netfilter, доступным в ядре Linux, начиная с версии 2.4[2].

Проверяем настройки iptables до выполнения с помощью команды sudo iptables ‑L (рисунок 3).

A screenshot of a video game

Description automatically generated

Рисунок 3 – Проверка настройки iptables до выполнения

### Задание 1

Для блокировки трафика исходящих не от ssh и веб-сервера введём фильтр с помощью iptables (рисунок 4). Здесь мы запрещаем любой трафик, который не исходит из портов 22(ssh), 80(http), 443(https).

Используем следующую команду*: sudo iptables -A OUTPUT -p tcp -m multiport ! --dport 22,80,443 -j DROP*.

A screenshot of a computer

Description automatically generated

Рисунок 4 - Команда для настройки межсетевого экрана

Text

Description automatically generated

Рисунок 5 – Работа порта 22

Graphical user interface, text, application

Description automatically generated

Рисунок 6 – Работа порта 443

### Задание 2

Используем следующие команды:

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

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

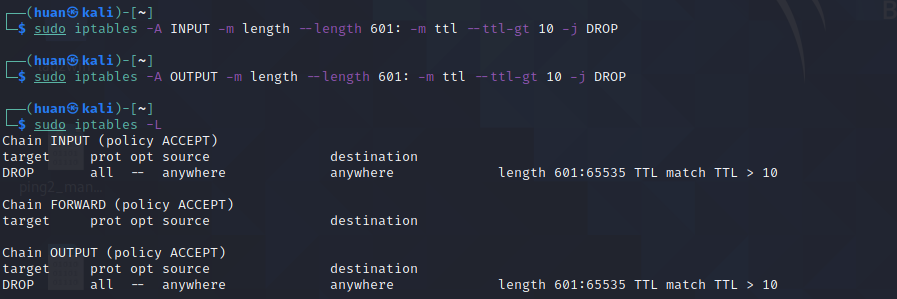


Рисунок 7 – Фильтр на размер и время жизни пакетов

Text

Description automatically generated

Рисунок 8 – Проверка работы правил

A picture containing text

Description automatically generated

Рисунок 9 – Проверка работы правил

### Задание 3

Нам необходимо было заменять IP всего транзитного трафика (который проходит через нашу машину). Для этого создадим правило, используя таблицу nat. Правила таблицы nat используются для трансляции сетевых адресов и номеров портов.

Пишем правило трансляции адреса источника для пакетов из сети 192.168.177.0: пакеты отправляются через интерфейс eth0 с заменой ip-адреса источника на ip-адрес интерфейса eth0 (рисунок 10).

Используем следующую команду: *sudo iptables -t nat -A POSTROUTING -s 192.168.177.0/24 -o eth0 -j MASQUERADE*

Text

Description automatically generated

Рисунок 10 – Настройка трансляции транзитого трафика

### Задание 4

Эти 2 правила устанавливают частоту в 5 новых попыток подключения в 10 минуту[3]:

*sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH*

*sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 600 --hitcount 6 --rttl --name SSH -j DROP*

Последнее правило – ACCEPT для SSH на порту 22:

*sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT*

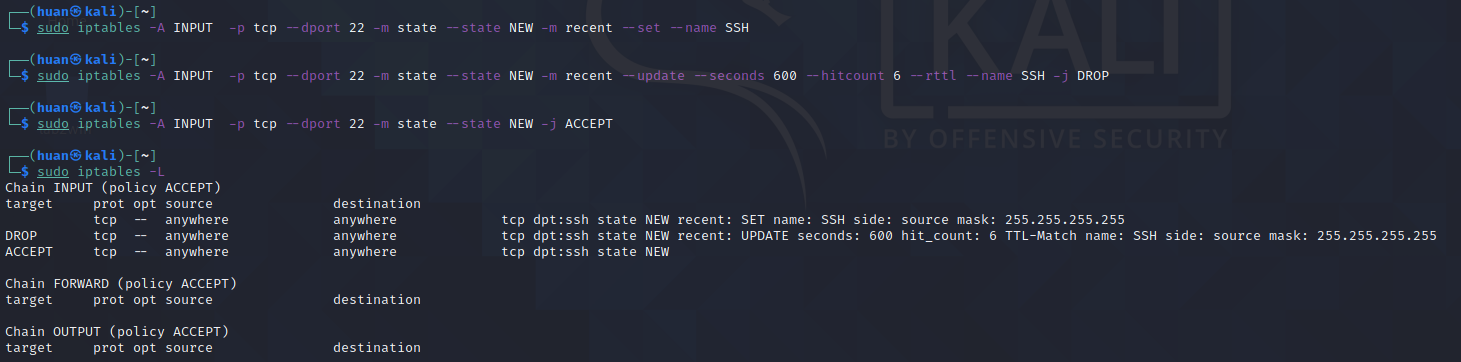


Рисунок 11 – Настройка iptables после выполнения команд

Text

Description automatically generated

Рисунок 12 – Попытка подключения к машине номер один и два

Text

Description automatically generated

Рисунок 13 – Попытка подключения к машине номер три и четыре

Text

Description automatically generated

Рисунок 14 – Попытка подключения к машине номер пять и шесть

Как мы видели на рисунках 12, 13, 14, на шестой раз попытка соединения будет разорвана.

Заключение

В ходе выполнения лабораторной работы были решены следуюшие задачи:

− настроен лабораторный стенд, включающий: локальный сервер, межсетевой экран, клиент, удаленный сервер;

− настроена маршрутизация проходящего трафика на локальном сервере;

− выполнены необходимые настройки межсетевого экрана на локальном сервере в соответствии с заданием;

− протестирована работа выполненных настроек;

− оформлены результаты выполнения работы оформить в виде отчета.

Таким образом, все поставленные задачи решены. Цель работы достигнута.

Список использованных источников

1. Linux ifconfig command. – Текст : электронный. – 2021. – URL : <https://www.computerhope.com/unix/uifconfi.htm> (дата обращения: 13.11.2022).
2. Руководство по iptables (Iptables Tutorial 1.1.19) – Текст : электронный. – URL : <https://www.opennet.ru/docs/RUS/iptables/#STARTINGSNAT> (дата обращения: 13.11.2022).
3. 8 способов предотвратить атаки брутфорс на SSH на Linux (CentOS / RHEL) – Текст : электронный. – URL : <https://bom.so/2Q0KOf> (дата обращения: 13.11.2022).