Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и технологий

Высшая школа программной инженерии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №8

**Курс по сетям Dell EMC**

Выполнил

студент гр. 3530904/80103 Королев Д.О.

Проверил: Шакуро П.Е.

«26» апреля 2022 г.

Санкт-Петербург

2022

**Оглавление**

[1. Задание 3](#_Toc104597568)

[**1.1 Задача:** 3](#_Toc104597569)

[**1.2 Шаги:** 3](#_Toc104597570)

[2. Выполнение работы 3](#_Toc104597571)

[**2.1 Посмотреть правила firewall по умолчанию** 3](#_Toc104597572)

[**2.2 Разрешить доступ со всех адресов, но оставить только 22 порт для SSH** 4](#_Toc104597573)

[**2.3 Запретить доступ со всех ip-адресов кроме своего (аккуратно!)** 5](#_Toc104597574)

[**2.4 Установить FTP сервер (например proftpd), настроить его работу в пассивном режиме, открыть в фаерволле порты, необходимые для его работы** 6](#_Toc104597575)

1. Задание

* 1. **1.1 Задача:**

Изучить настройку Firewall в ОС Linux

* 1. **1.2 Шаги:**

1. Посмотреть правила firewall по умолчанию
2. Разрешить доступ со всех адресов, но оставить только 22 порт для SSH
3. Запретить доступ со всех ip-адресов кроме своего (аккуратно!)
4. Установить FTP сервер (например proftpd), настроить его работу в пассивном режиме, открыть в фаерволле порты, необходимые для его работы

2. Выполнение работы

* 1. **2.1 Посмотреть правила firewall по умолчанию**

1. Для просмотра правил firewall по умолчанию выполним команду ***sudo iptables -L***

Изображение выглядит как текст

Автоматически созданное описание

В iptables существуют следующие правила (цепочки)

**1.Input.**

Правило применяется, когда необходимо контролировать входящий трафик. В зависимости от примененного действия доступ пользователю будет открыт или закрыт.

**2.Forward.**

Правило применяется в случаях, когда необходимо проверить входящий трафик, проходящее через данный компьютер. Применяется в маршрутизаторах, постоянно пересылающих сообщения к адресату, или в компьютерах, раздающих wifi.

**3.Output.**

Правило применяется к исходящим сообщениям. Под это правило попадают при попытке проверить пинг к одному из заданных сайтов или открыть его в браузере.

В iptables существуют следующие действия над пакетами:

**Accept** – разрешение определенного соединения;

**Drop** – игнорирование запросов (firewall продолжает свое функционирование, будто никакого запроса не происходило, а запрашивающие ресурсы не узнают об игнорировании);

**Reject** – блокировка входящего трафика и отправка ответных сообщений с обозначением ошибки (в таком случае запрашивающие ресурсы будут уведомлены о блокировке трафика).

**LOG** - осуществление записи о пакете в файл логов.

**QUEUE** - отправка пакета пользовательскому приложению.

По умолчанию для всех правил установлены действия ACCEPT.

* 1. **2.2 Разрешить доступ со всех адресов, но оставить только 22 порт для SSH**

1. Очистим загруженные правила, выполнив ***sudo iptables -F.***
2. Разрешим подключение по SSH, выполнив ***sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT.***

Где A (append) - добавление одного или нескольких правил в конец указанной цепочки;

p (protocol) - сетевой протокол применяемого правила;

m (match) - имя модуля;

dport - номер порта;

j - цель правила (определение действия).

1. Изменим цепочки по умолчанию. Для цепочки OUTPUT оставим значение ACCEPT, для INPUT и FORWARD укажем DROP.

***sudo iptables -P INPUT DROP***

***sudo iptables -P OUTPUT ACCEPT***

***sudo iptables -P FORWARD DROP***

1. Сохраним внесенные изменения, выполнив ***sudo*** ***iptables-save.***
2. После выполнения этих операций правила firewall имеют следующий вид.

***Изображение выглядит как текст

Автоматически созданное описание***

1. Подключимся по SSH к виртуальной машине.

Изображение выглядит как текст

Автоматически созданное описание

* 1. **2.3 Запретить доступ со всех ip-адресов кроме своего (аккуратно!)**

1. Изменим созданное в пункте 2.2 правило, запретив доступ со всех ip-адресов кроме своего. Для этого выполним ***sudo iptables -R INPUT -p tcp -m tcp --dport 22 -j -s 10.176.108.181 ACCEPT.***

Где R (replace) - замена правила в указанной цепочке;

s (source) - адрес источника. Адресом может быть сетевое имя, имя хоста, диапазон IP-адресов (с маской через слэш) или одиночный IP-адрес.

1. Сохраним внесенные изменения, выполнив ***sudo*** ***iptables-save.***
2. После чего правила firewall имеют следующий вид.

***Изображение выглядит как текст

Автоматически созданное описание***

1. Подключимся по SSH к виртуальной машине.

Изображение выглядит как текст

Автоматически созданное описание

* 1. **2.4 Установить FTP сервер (например proftpd), настроить его работу в пассивном режиме, открыть в фаерволле порты, необходимые для его работы**

1. Для установки ProFTPd выполним ***sudo apt-get install proftpd***.
2. Для открытия необходимых портов выполним ***iptables -A INPUT -p tcp --match multiport --dports 20,21,60000:65535 -j ACCEPT.***
3. Сохраним внесенные изменения, выполнив ***sudo*** ***iptables-save.***
4. В конфигурационном файле ***/etc/proftpd/proftpd.conf*** снимем комментарий для опции PassivePorts и зададимм ей следующее значение:

***PassivePorts 60000 65535***

где 60000 - 65535 — диапазон динамических портов для пассивного режима.

1. Разрешаем автозапуск FTP-серверу и перезапускаем его:

***systemctl enable proftpd***

***systemctl restart proftpd***

1. На хост машине скачиваем бесплатный FTP клиент FileZilla по ссылке <https://filezilla.ru/> и устанавливаем его.
2. Подключаемся к FTP серверу, используя FileZilla. В качестве логина и пароля используем учетную запись пользователя Ubuntu.

Изображение выглядит как текст

Автоматически созданное описание

В результате было осуществлено подключение к FTP серверу с применением клиента FileZilla.

Изображение выглядит как текст

Автоматически созданное описание