**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

ОТЧЕТ

по лабораторной работе № 7

Дисциплина «Администрирование сетевых подсистем»

*Тема «Расширенные настройки межсетевого экрана»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

# Цель работы

# Получить навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

# Задание

1. Настроить межсетевой экран виртуальной машины server для доступа к серверу по протоколу SSH не через 22-й порт, а через порт 2022.

2. Настроить Port Forwarding на виртуальной машине server.

3. Настроить маскарадинг на виртуальной машине server для организации доступа клиента к сети Интернет.

4. Написать скрипт для Vagrant, фиксирующий действия по расширенной настройке межсетевого экрана. Соответствующим образом внести изменения в Vagrantfile.

**Выполнение**

**1. Создание пользовательской службы firewalld**

1. На основе существующего файла описания службы ssh создала файл с собственным описанием и посмотрела содержимое файла службы (рис.1.1).

В файле /etc/firewalld/services/ssh-custom.xml определен пользовательский сервис SSH. Файл представляет собой конфигурацию для firewalld, позволяя настраивать правила файрвола для SSH-сервиса.

<?xml version="1.0" encoding="utf-8"?>: XML-заголовок, указывающий на версию XML и кодировку символов.

<service>: начало определения сервиса.

<short>SSH</short>: краткое описание сервиса, где указано, что это SSH.

<description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines...: здесь предоставлено более подробное описание сервиса SSH. Объясняется, что SSH - это протокол для входа и выполнения команд на удаленных машинах, обеспечивающий безопасные зашифрованные коммуникации. Также отмечается, что для использования этой опции необходим пакет openssh-server.

<port protocol="tcp" port="22"/>: здесь указывается, что сервис использует TCP-протокол и прослушивает порт 22.

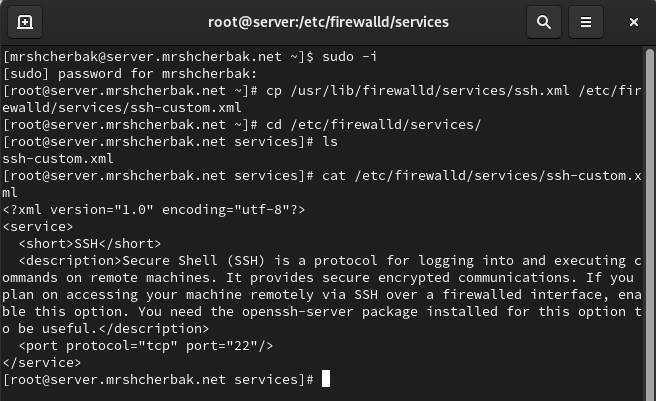


Рис.1.1. Создание файла ssh-custom.xml и просмотр его содержимого

2. Открыла файл описания службы на редактирование и заменила порт 22 на новый порт (2022), а также скорректировала описание службы для демонстрации, что это модифицированный файл службы (рис.1.2).

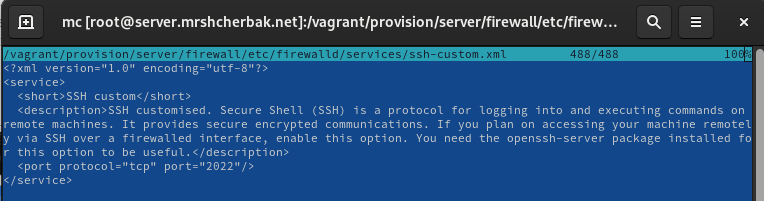


Рис.1.2. Редактирование файла ssh-custom.xml

3. Просмотрела список доступных FirewallD служб (рис.1.3). Новая служба ещё не отображается в списке.

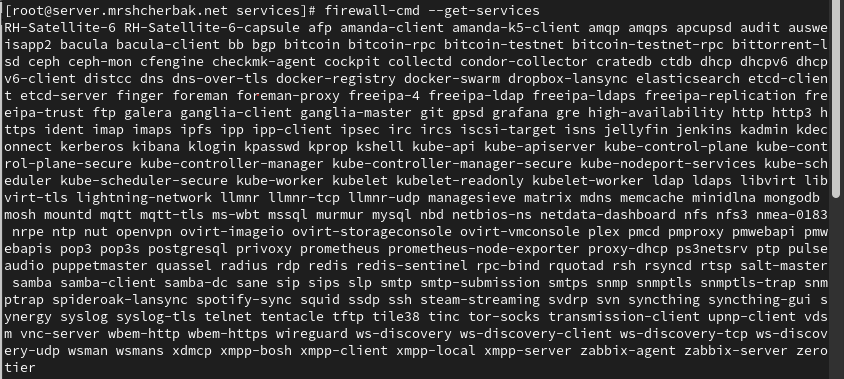


Рис.1.3. Просмотр списка доступных FirewallD служб

4. Перегрузила правила межсетевого экрана с сохранением информации о состоянии и вновь вывела на экран список служб, а также список активных служб (рис.1.4). Убедилась, что созданная служба отображается в списке доступных для FirewallD служб, но не активирована.

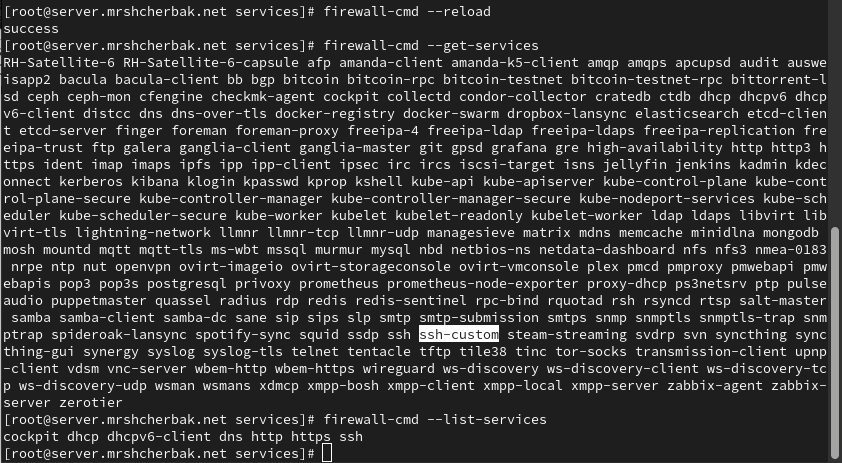


Рис.1.4. Выполнение команд

5. Добавила новую службу в FirewallD и вывела на экран список активных служб (рис.1.5).

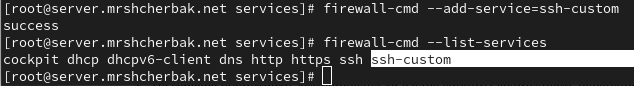


Рис.1.5. Служба активирована

**2. Перенаправление портов**

1. Организовала на сервере переадресацию с порта 2022 на порт 22 (рис.2.1).



Рис.2.1. Выполнение команды

2. На клиенте попробовала получить доступ по SSH к серверу через порт 2022 (рис.2.2).

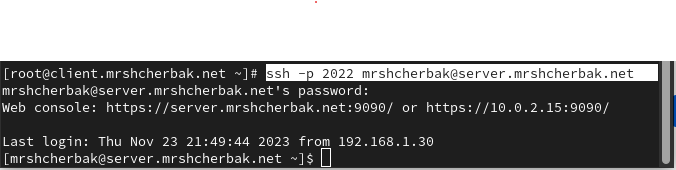


Рис.2.2. Выполнение команды

**3. Настройка Port Forwarding и Masquerading**

1. На сервере посмотрела, активирована ли в ядре системы возможность перенаправления IPv4-пакетов (рис.3.1).

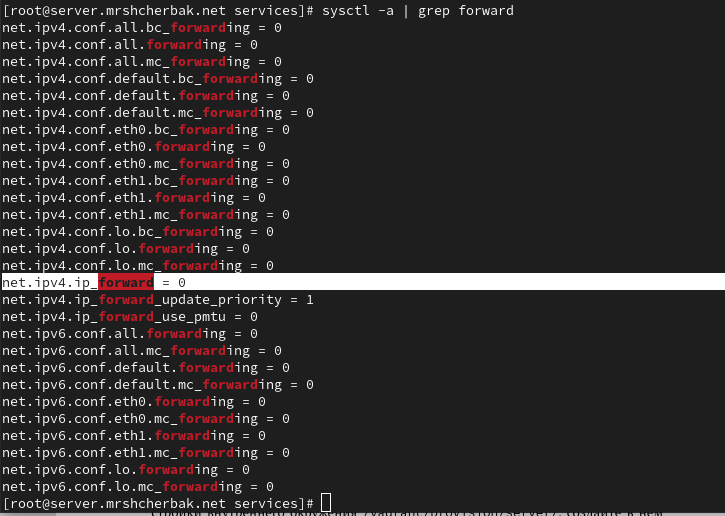


Рис.3.1. Возможность перенаправления IPv4-пакетов в ядре системы не активирована

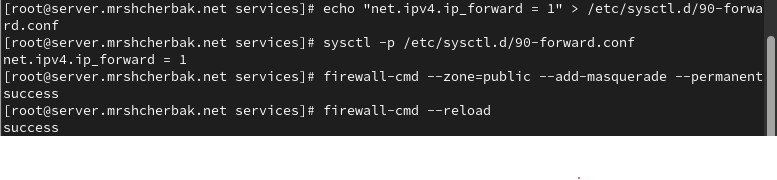
2. Включила перенаправление IPv4-пакетов и маскарадинг на сервере (рис.3.2).  


Рис.3.2. Выполнение команд

3. На клиенте проверила доступность выхода в Интернет (рис.3.3).

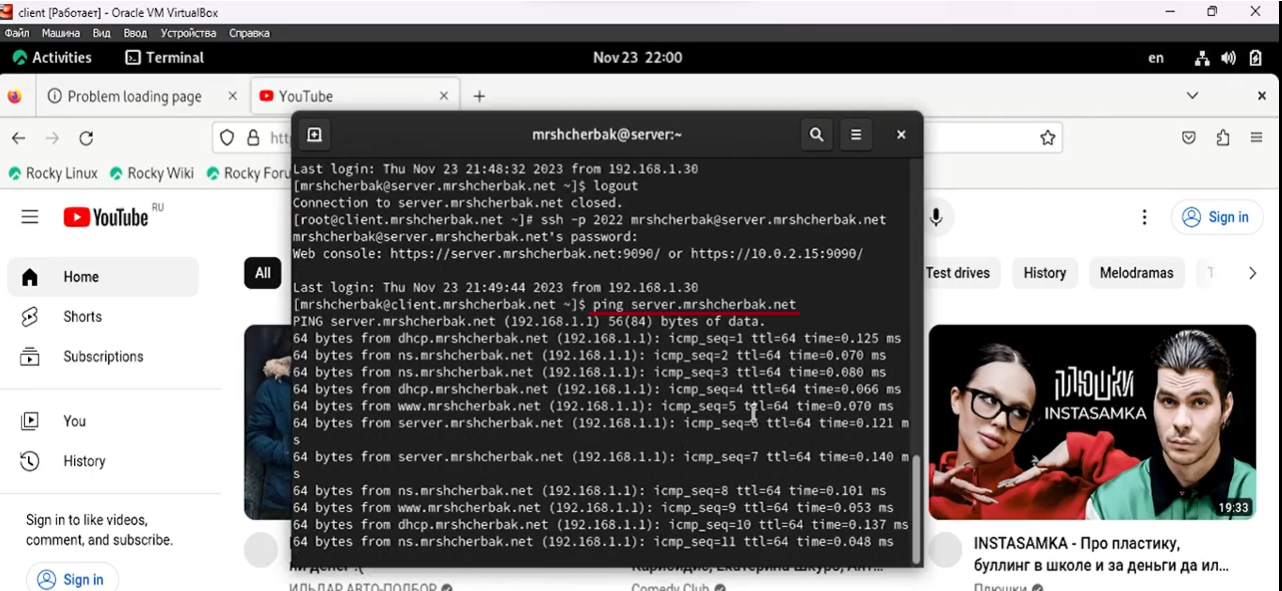


Рис.3.3. Выход в Интернет есть

**4. Внесение изменений в настройки внутреннего окружения виртуальной машины**

1. На виртуальной машине server перешла в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создала в нём каталог firewall, в который поместила в соответствующие подкаталоги конфигурационные файлы FirewallD. В каталоге /vagrant/provision/server создала файл firewall.sh. Действия представлены на рис.4.1.

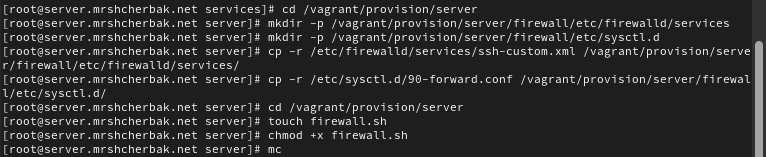


Рис.4.1. Выполнение команд

2. Открыв файл firewall.sh на редактирование, прописала в нём скрипт (рис.4.2).

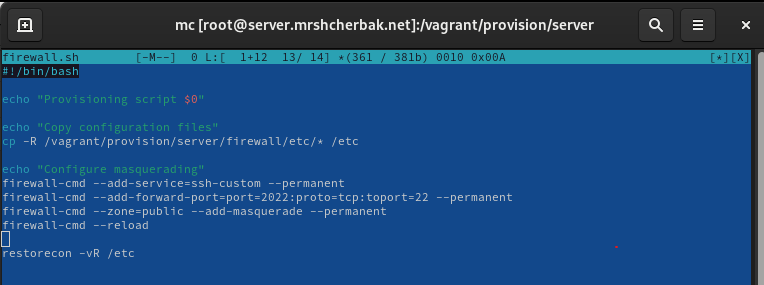


Рис.4.2. Редактирование файла firewall.sh

3. Для отработки созданного скрипта во время загрузки виртуальной машины server

в конфигурационном файле Vagrantfile добавила в разделе конфигурации для сервера запись (рис.4.3).

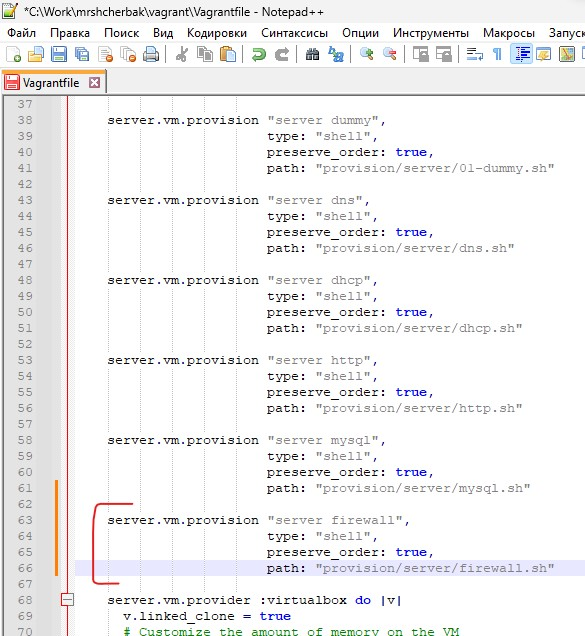


Рис.4.3. Содержимое файла Vagrantfile

# Вывод: таким образом, в ходе выполнения л/р №7 я получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

# Контрольные вопросы

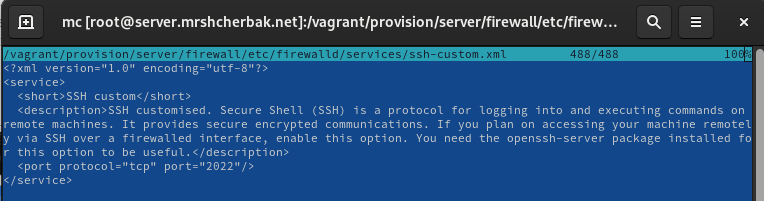
1. Где хранятся пользовательские файлы firewalld?

Пользовательские файлы firewalld обычно хранятся в директории /etc/firewalld/. В данной л/р, например, в файле /etc/firewalld/services/ssh-custom.xml определен пользовательский сервис SSH. Firewalld хранит все настройки, связанные со службами, в XML-файлах в каталоге /usr/lib/firewalld/services. Если требуется переопределить настройки имеющейся службы или подключить собственную службу, то необходимо файл с описанием службы разместить в каталоге /etc/firewalld/services.

2. Какую строку надо включить в пользовательский файл службы, чтобы указать порт TCP 2022?

Для указания порта TCP 2022 в пользовательском файле службы, нужно добавить строку в секцию <port> следующим образом:

<port protocol="tcp" port="2022"/>: здесь указывается, что сервис использует TCP-протокол и прослушивает порт 2022.

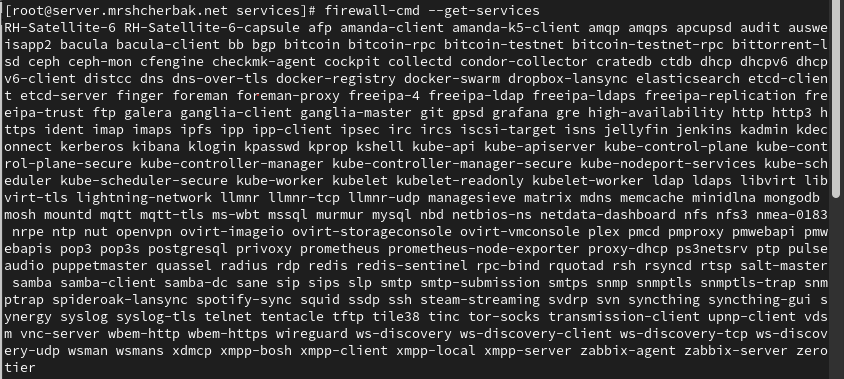


3. Какая команда позволяет вам перечислить все службы, доступные в настоящее время на вашем сервере?

Для перечисления всех служб, доступных на сервере, используем команду:

firewall-cmd --get-services

Так, в данной л/р я просматривала список доступных FirewallD служб.



4. В чем разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading)?

Разница между NAT и маскарадингом в том, что NAT переводит один IP-адрес в другой, а маскарадинг скрывает внутренние IP-адреса за единственным внешним IP-адресом. NAT может использовать уникальные или общие внешние адреса, в то время как маскарадинг всегда использует общий внешний адрес для группы устройств в локальной сети.

5. Какая команда разрешает входящий трафик на порт 4404 и перенаправляет его в службу ssh по IP-адресу 10.0.0.10?

Команда для разрешения входящего трафика на порт 4404 и перенаправления его на службу SSH по IP-адресу 10.0.0.10 может выглядеть так:

firewall-cmd --add-forward-port=port=4404:proto=tcp:toport=22:toaddr=10.0.0.10

6. Какая команда используется для включения маcкарадинга IP-пакетов для всех пакетов, выходящих в зону public?

Для включения маскарадинга IP-пакетов для всех пакетов, выходящих в зону public, используем команду:

firewall-cmd --zone=public --add-masquerade –permanent

