Отчёт по лабораторной работе №7

Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

Запускаем ВМ через рабочий каталог. На ВМ server входим под собственным пользователем и переходим в режим суперпользователя. На основе существующего файла описания службы ssh создаем файл с собственным описанием. Просматриваем содержимое файла (рис. 1).

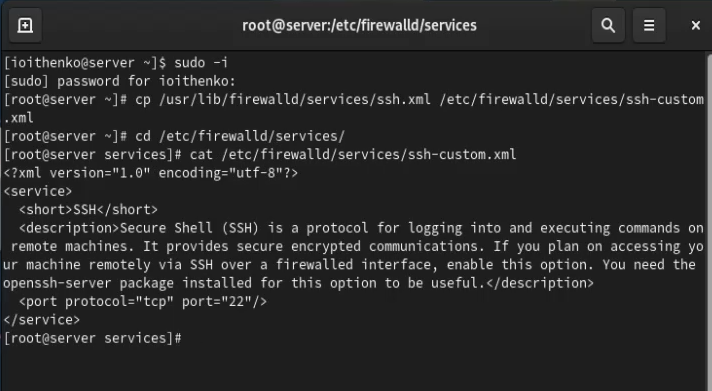


Рис. 1: Создание собственного файла описания службы и просмотр

Открываем файл на редактирование и меняем порт 22 на порт 2022, в описании службы указав, что порт был изменен (рис. 2)

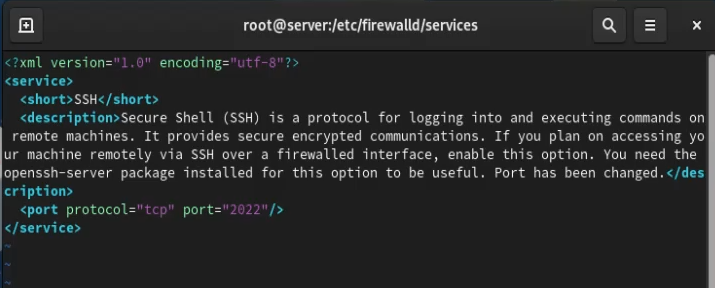


Рис. 2: Редактирование файла описания службы

Просматриваем список доступных служб (новой службы пока нет) (рис. 3).

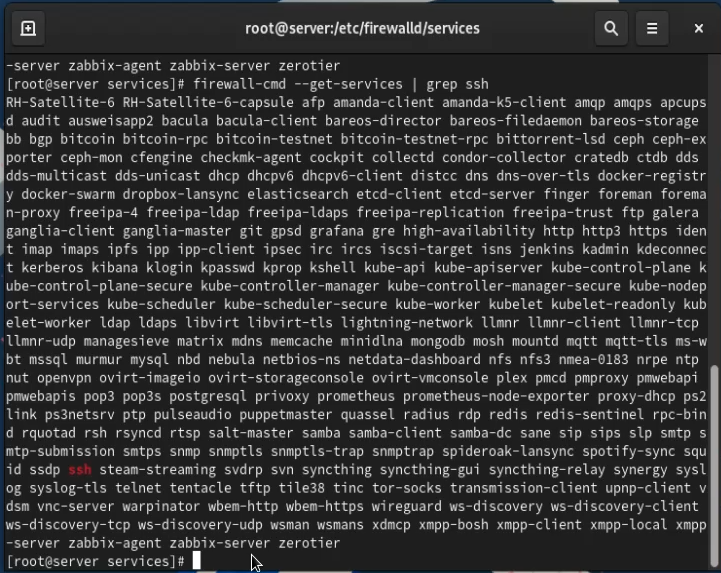


Рис. 3: Список доступных служб

Перезагружаем правила межсетевого экрана, снова просматриваем список доступных служб и видим новую (рис. 4).

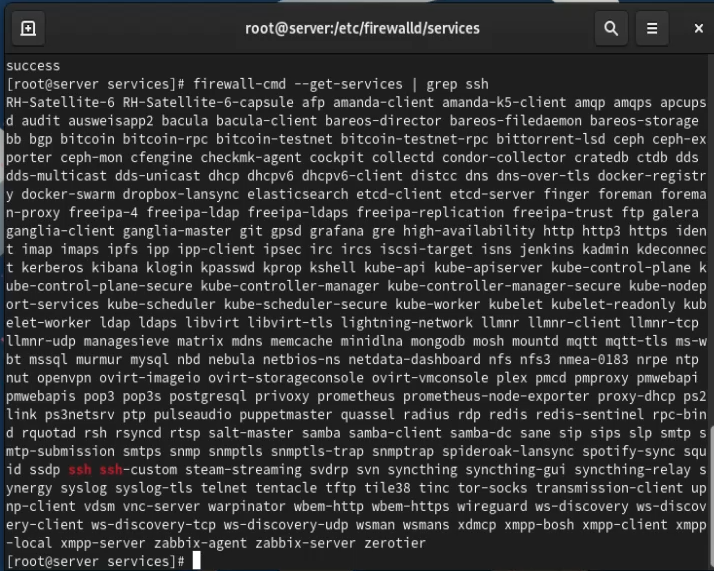


Рис. 4: Новая служба в списке доступных служб

Новая служба отображается в списке доступных, но пока не активирована. Добавляем новую службу в FirewallD и просматриваем список активных служб (служба появилась). Перегружаем правила межсетевого экрана с сохранением информации о состоянии (рис. 5)

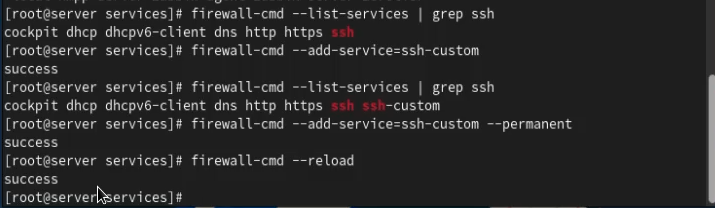


Рис. 5: Добавление новой службы и просмотр списка активных служб, сохранение информации о состоянии

Организовываем переадресацию с порта 2022 на порт 22 на сервере(рис. 6).



Рис. 6: Переадресация

На клиенте пробуем получить доступ по SSH через порт 2022. Доступ получен (рис. 7).

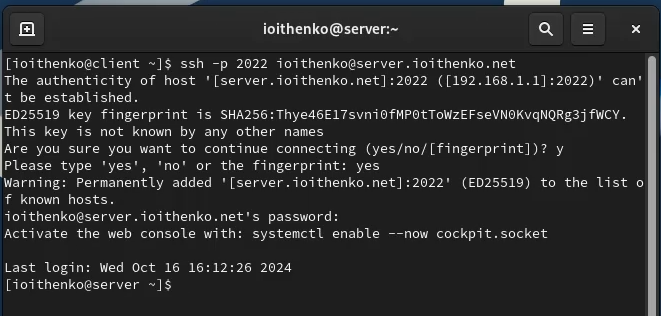


Рис. 7: Доступ по SSH к серверу через порт 2022 на клиенте

На сервере просматриваем, активирована ли в ядре системы возможность перенаправления IPv4-пакетов пакетов (рис. 8). Включаем перенаправление пакетов на сервере. Включаем маскарадинг на сервере (рис. 9). Убеждимся, что на клиенте доступен выход в интернет (доступен) (рис. 10).

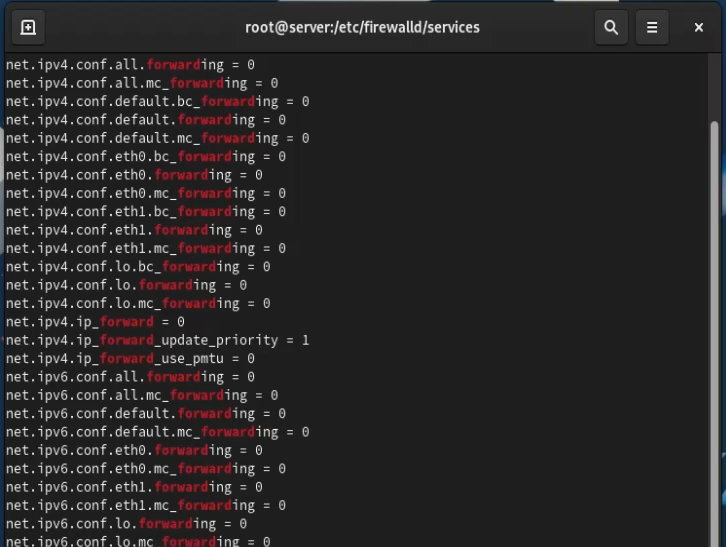


Рис. 8: Возможность перенаправления пакетов

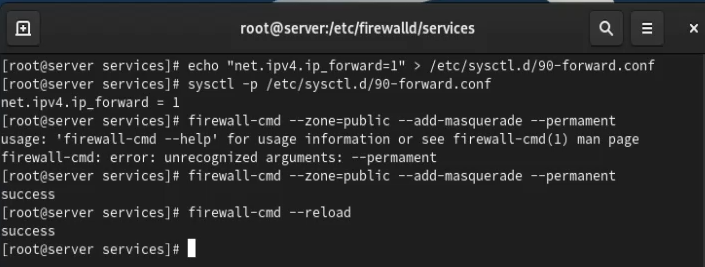


Рис. 9: Включение перенаправления пакетов и включение маскарадинга

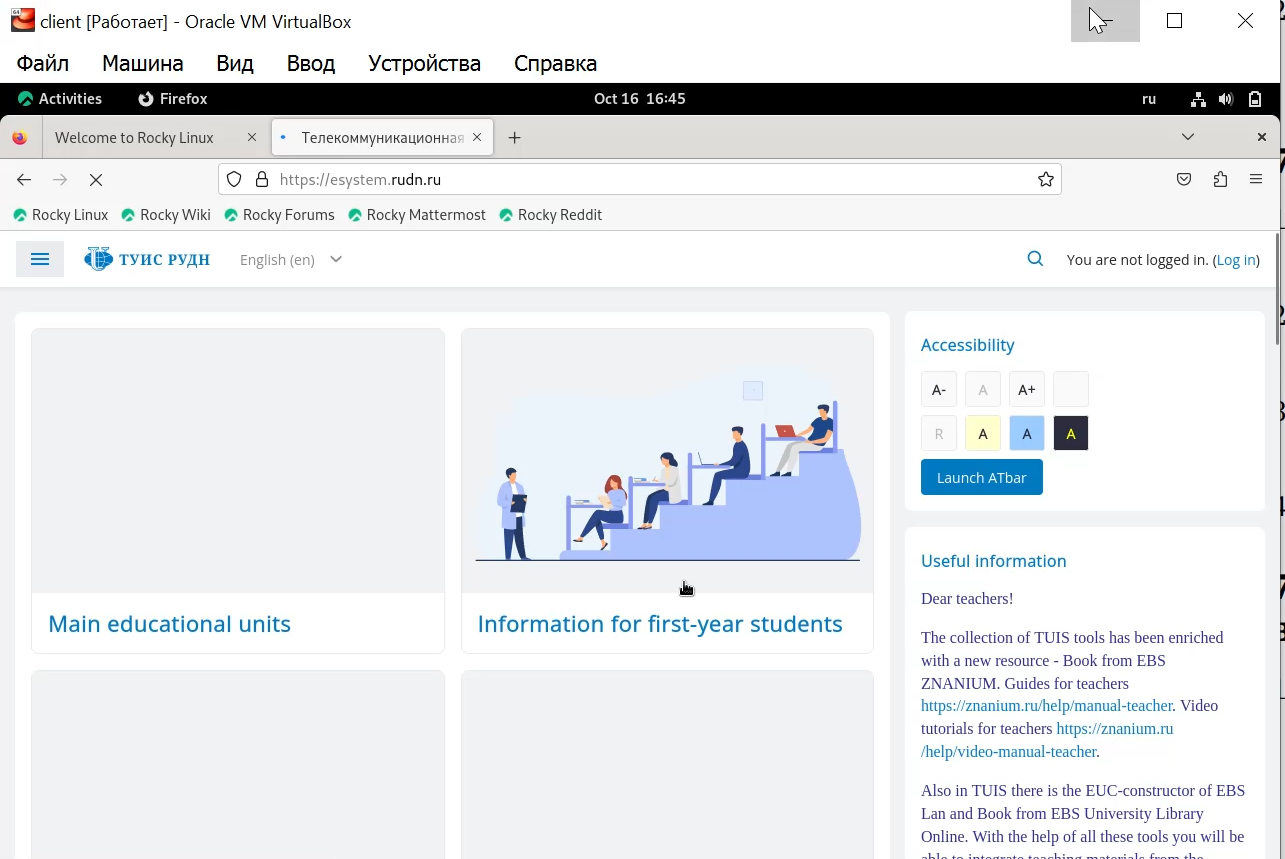


Рис. 10: Браузер клиента

На ВМ server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/ и копирую в соответствующие каталоги конфигурационные файлы (рис. 11).

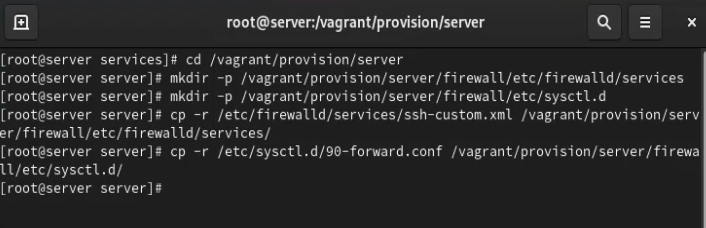


Рис. 11: Внесение изменений в настройки внутреннего окружения

Создаю скрипт firewall.sh (рис. 12).

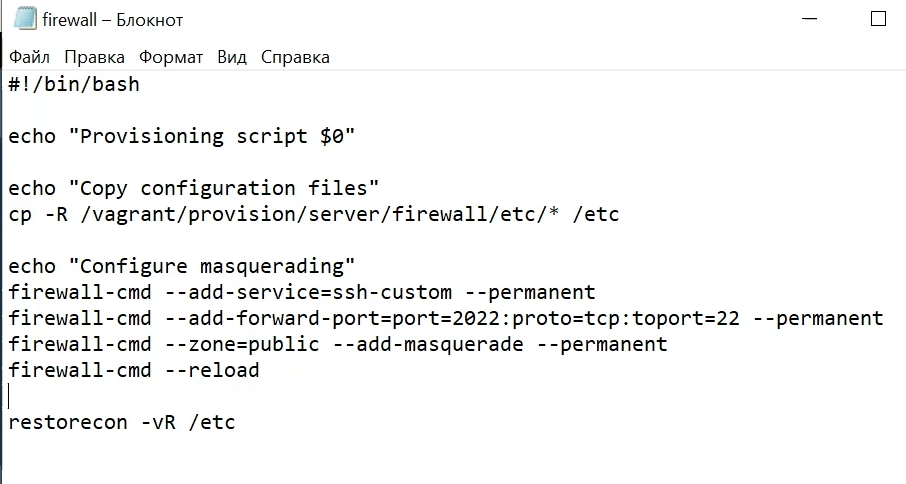


Рис. 12: Создание скрипта firewall.sh

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавляем в разделе конфигурации для сервера следующую запись (рис. 13):

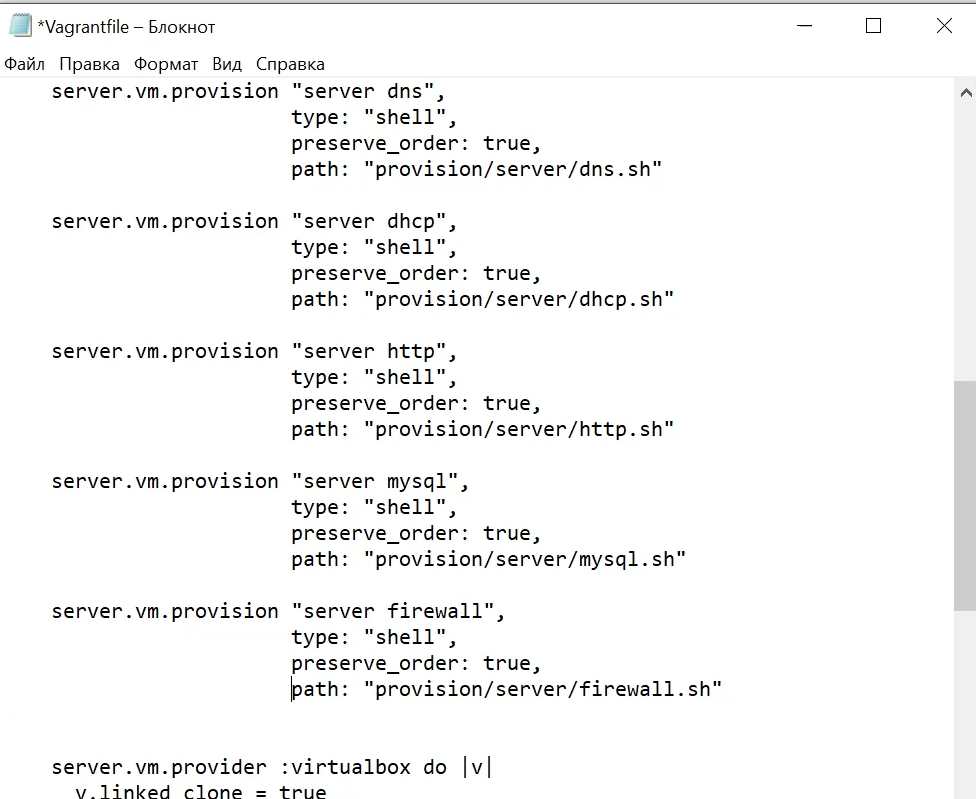


Рис. 13: Vagrantfile

# 3 Выводы

В ходе лабораторной работы я получила навыки настройки межсетевого экрана в Linux в части переадресации портов и настройки Masquerading.

# 4 Ответы на контрольные вопросы

1. Где хранятся пользовательские файлы firewalld?

* В firewalld пользовательские файлы хранятся в директории /etc/firewalld/.

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

* Для указания порта TCP 2022 в пользовательском файле службы, вы можете добавить строку в секцию port следующим образом:

<port protocol="tcp" port="2022"/>

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

* firewall-cmd --get-services

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

* Разница между трансляцией сетевых адресов (NAT) и маскарадингом (masquerading) заключается в том, что в случае NAT исходный IP-адрес пакета заменяется на IP-адрес маршрутизатора, а в случае маскарадинга используется маршрутизатора.

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

firewall-cmd --zone=public --add-port=4404/tcp --permanent  
firewall-cmd --zone=public --add-forward-port=port=4404  
 ↪:proto=tcp:toport=22:toaddr=10.0.0.10 --permanent  
firewall-cmd --reload

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

* firewall-cmd --zone=public --add-masquerade --permanent
* firewall-cmd --reload