**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

ОТЧЕТ

по лабораторной работе № 11

Дисциплина «Администрирование сетевых подсистем»

*Тема «Настройка безопасного удалённого доступа по протоколу SSH»*

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

# Цель работы

Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

# Задание

1. Настроить запрет удалённого доступа на сервер по SSH для пользователя root.

2.Настроить разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя.

3. Настроить удалённый доступ к серверу по SSH через порт 2022.

4. Настроить удалённый доступ к серверу по SSH по ключу.

5.Организовать SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080.

6. Используя удалённое SSH-соединение, выполнить с клиента несколько команд на сервере.

7.Используя удалённое SSH-соединение, запустить с клиента графическое приложение на сервере.

8. Написать скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Внести изменения в Vagrantfile.

**Выполнение**

**1. Запрет удалённого доступа по SSH для пользователя root**

1. На сервере задала пароль для пользователя root (рис.1.1), а в дополнительном терминале запустила мониторинг системных событий.

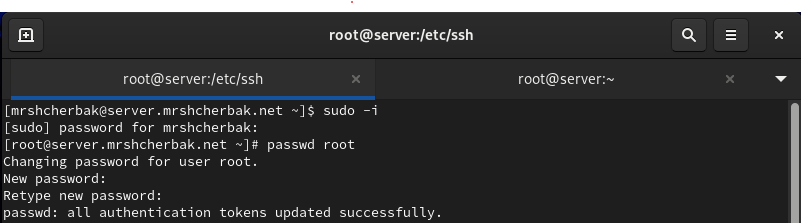


Рис.1.1. Создание пароля для пользователя root на сервере

2. С клиента попыталась получить доступ к серверу посредством SSH-соединения через пользователя root (рис.1.2). Доступ есть. Я зашла под рутом на сервер.

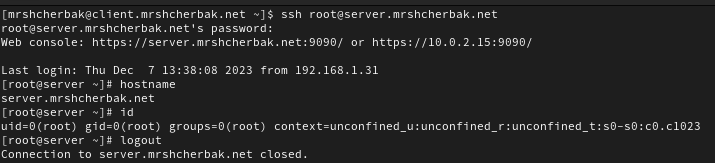


Рис.1.2. Получение доступа к серверу посредством SSH-соединения через пользователя root

3. На сервере открыла файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретила вход на сервер пользователю root (рис.1.3).

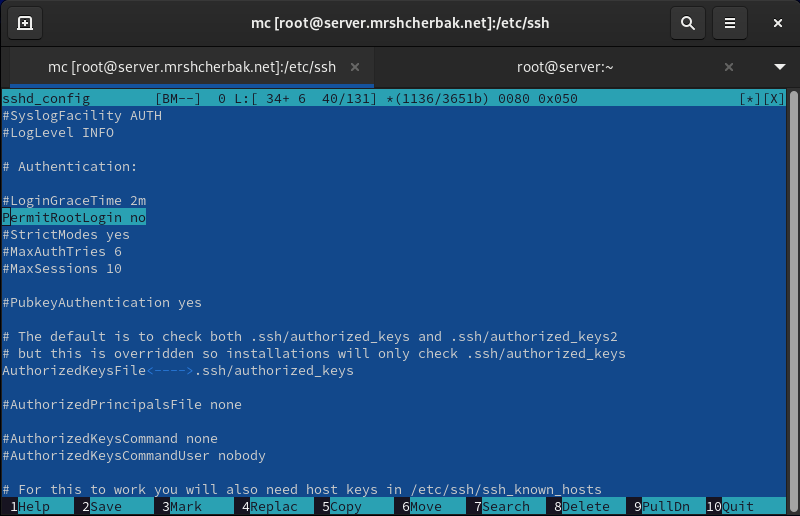


Рис.1.3. Запрет входа на сервер пользователю root

4. После сохранения изменений в файле конфигурации перезапустила sshd с помощью команды systemctl restart sshd.

5. Повторила попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя root (рис.1.4). Доступа нет.

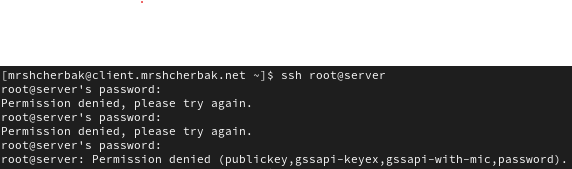


Рис.1.4. Отказ в доступе к серверу посредством SSH-соединения через пользователя root

**2. Ограничение списка пользователей для удалённого доступа по SSH**

1. С клиента попыталась получить доступ к серверу посредством SSH-соединения через пользователя mrshcherbak (рис.2.1). Доступ есть.

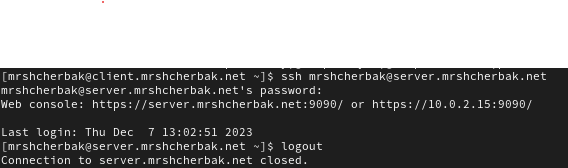


Рис.2.1. Получение доступа к серверу посредством SSH-соединения через пользователя mrshcherbak

2. На сервере открыла файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и добавила строку AllowUsers vagrant (рис.2.2).

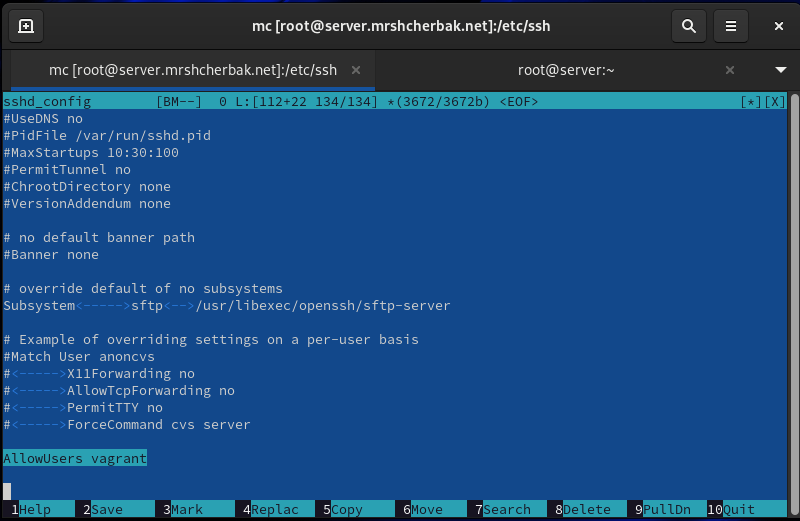


Рис.2.2. Редактирование файла /etc/ssh/sshd\_config

3. После сохранения изменений в файле конфигурации перезапустила sshd с помощью команды systemctl restart sshd.

4. Повторила попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя mrshcherbak (рис.2.3). Доступа нет.

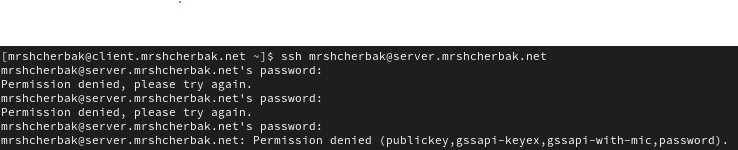


Рис.2.3. Отказ в доступе к серверу посредством SSH-соединения через пользователя mrshcherbak

5. В файле /etc/ssh/sshd\_config конфигурации sshd внесла следующее изменение:

AllowUsers vagrant mrshcherbak (рис.2.4).

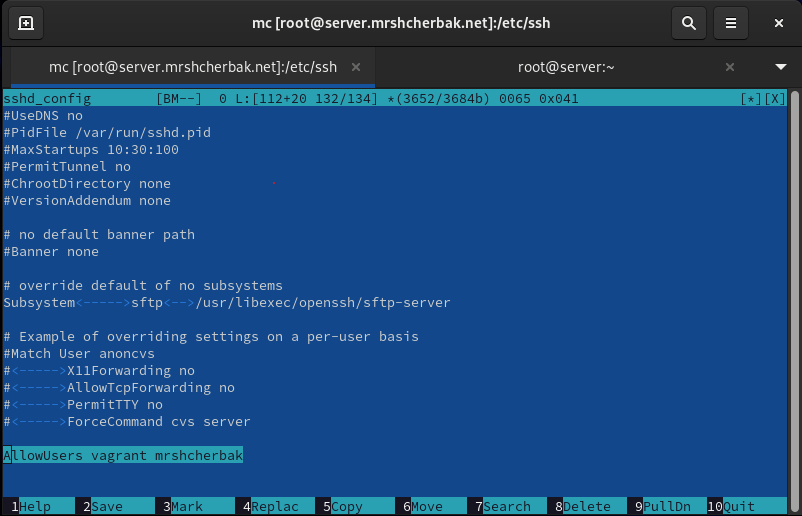


Рис.2.4. Редактирование файла /etc/ssh/sshd\_config

6. После сохранения изменений в файле конфигурации перезапустила sshd и вновь

попыталась получить доступ с клиента к серверу посредством SSH-соединения через пользователя mrshcherbak (рис.2.5). Доступ есть.

.

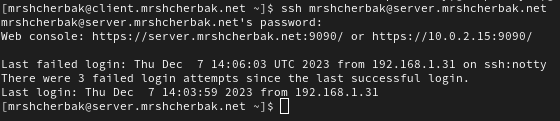


Рис.2.5. Получение доступа к серверу посредством SSH-соединения через пользователя mrshcherbak

**3. Настройка дополнительных портов для удалённого доступа по SSH**

1. На сервере в файле конфигурации sshd /etc/ssh/sshd\_config добавила запись (рис.3.1), которая сообщает процессу sshd о необходимости организации соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.

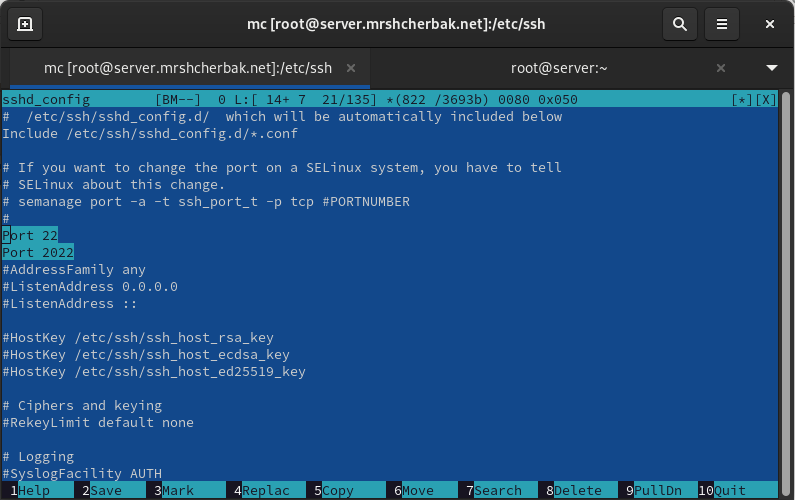


Рис.3.1. Редактирование файла /etc/ssh/sshd\_config

2. После сохранения изменений в файле конфигурации перезапустила sshd и посмотрела расширенный статус работы sshd (рис.3.2). Система сообщает об отказе в работе sshd через порт 2022. Дополнительно посмотрела сообщения в терминале с мониторингом системных событий (рис.3.3). SELinux запрещает подключение к порту 2022. Чтобы подключиться, необходимо изменить тип порта с помощью предложенной команды в сообщениях мониторинга.

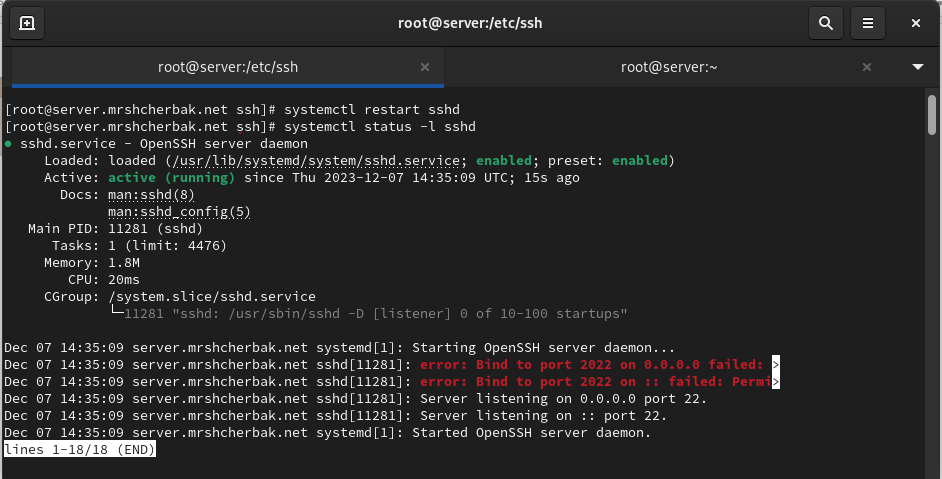


Рис.3.2. Просмотр расширенного статуса работы sshd

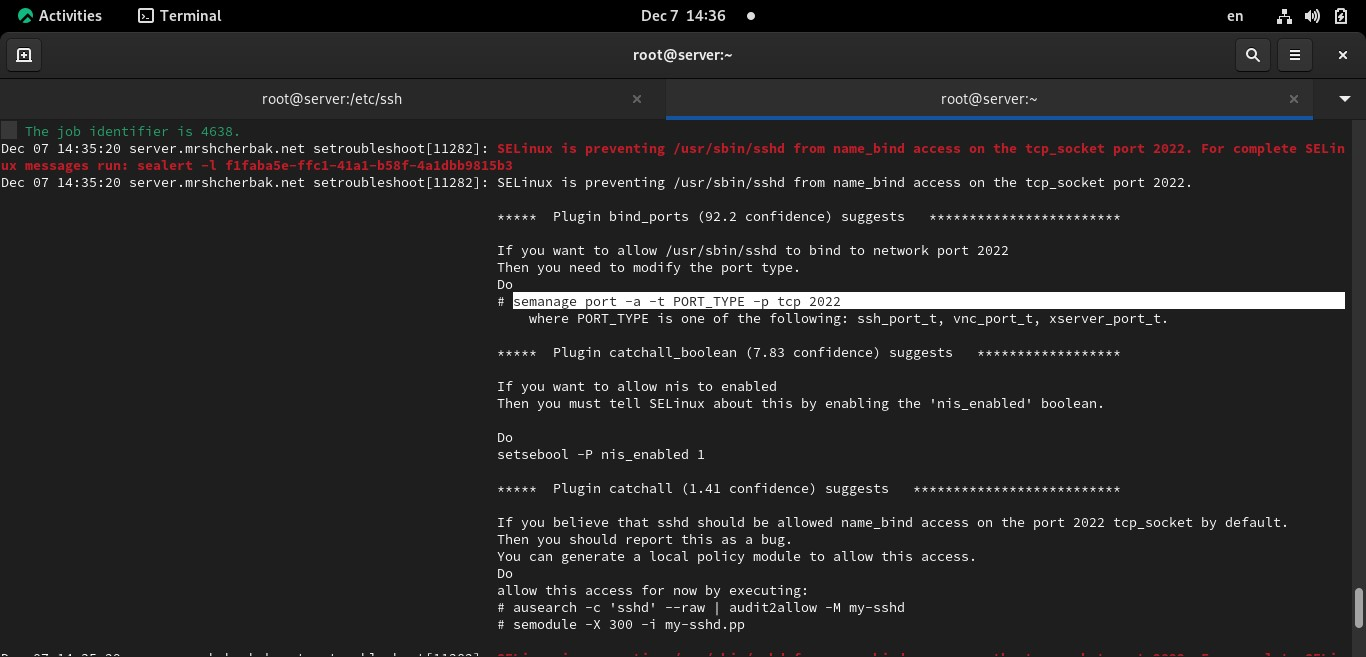


Рис.3.3. Мониторинг системных событий

3. Исправила на сервере метки SELinux к порту 2022 и в настройках межсетевого экрана открыла порт 2022 протокола TCP, после чего вновь перезапустила sshd и посмотрела расширенный статус его работы. Действия представлены на рис.3.4. Статус показывает, что процесс sshd теперь прослушивает два порта.

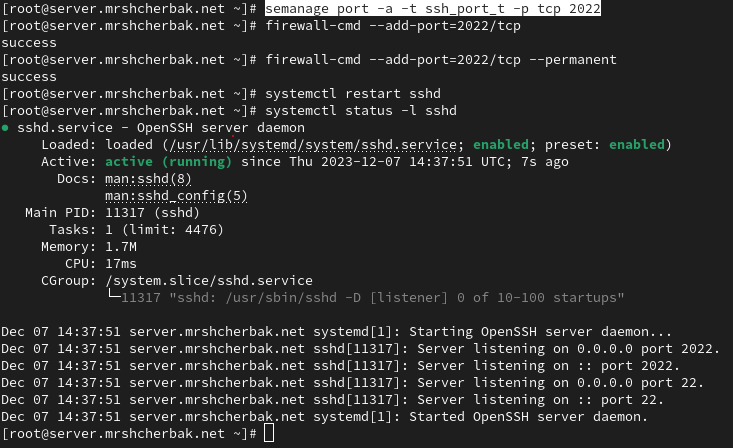


Рис.3.4. Выполнение команд

4. С клиента попыталась получить доступ к серверу посредством SSH-соединения через пользователя mrshcherbak. После открытия оболочки пользователя ввела sudo -i для получения доступа root. Повторила попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя mrshcherbak, указав порт 2022. После открытия оболочки пользователя ввела sudo -i для получения доступа

root. Действия представлены на рис.3.5.

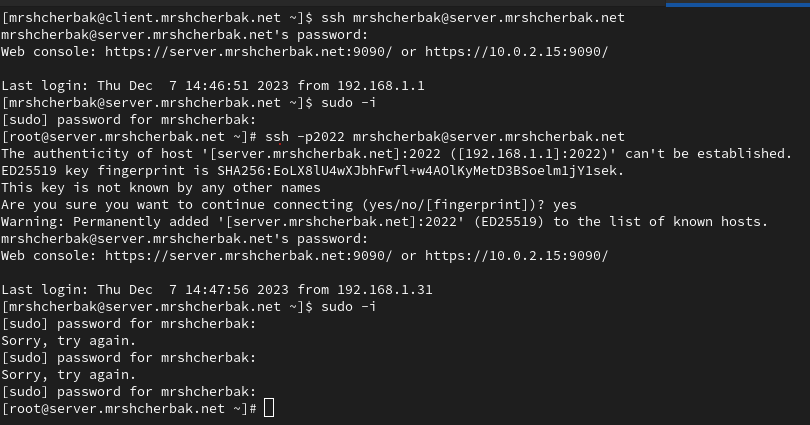


Рис.3.5. Выполнение команд

**4. Настройка удалённого доступа по SSH по ключу**

1. На сервере в конфигурационном файле /etc/ssh/sshd\_config задала параметр,

разрешающий аутентификацию по ключу (рис.4.1).

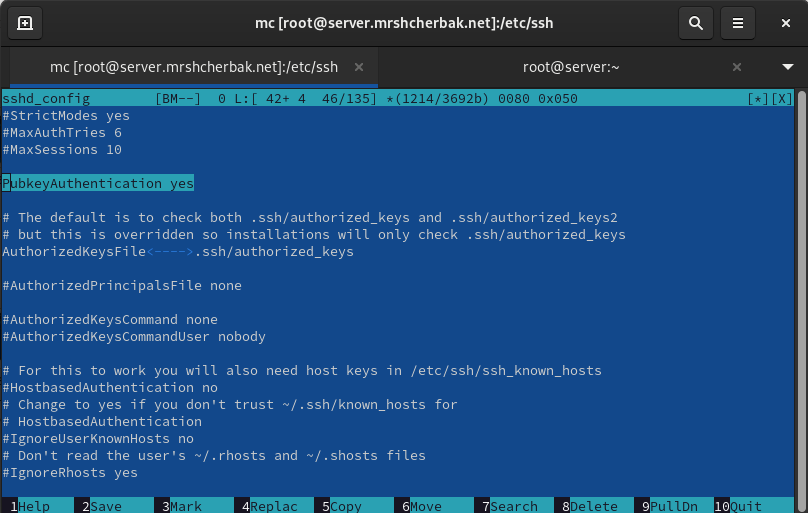


Рис.4.1. Редактирование файла /etc/ssh/sshd\_config

2. После сохранения изменений в файле конфигурации перезапустила sshd.

3. На клиенте сформировала SSH-ключ (рис.4.2).

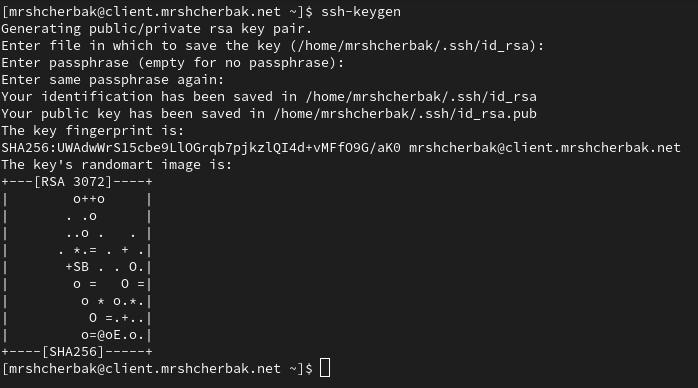


Рис.4.2. Выполнение команды ssh-keygen

4. Закрытый ключ теперь записан в файл ~/.ssh/id\_rsa, а открытый ключ ⎯ в файлe ~/.ssh/id\_rsa.pub.

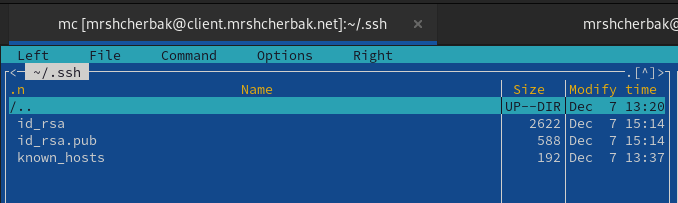


Рис.4.3. Содержимое ~/.ssh

5. Скопировала открытый ключ на сервер и попробовала получить доступ с клиента к серверу посредством SSH-соединения. Аутентификация пройдена без ввода пароля для учётной записи удалённого пользователя (рис.4.4).

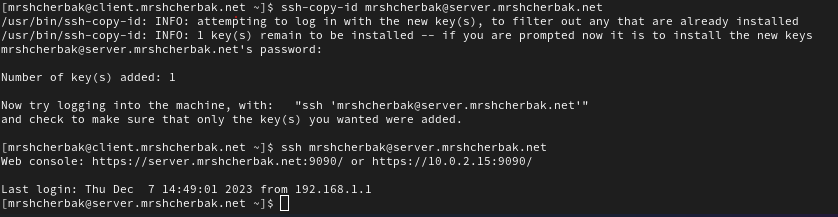


Рис.4.4. выполнение команд

**5. Организация туннелей SSH, перенаправление TCP-портов**

1. На клиенте посмотрела, запущены ли какие-то службы с протоколом TCP, а также перенаправила порт 80 на server.mrshcherbak.net на порт 8080 на локальной машине (рис.5.1). После на клиенте вновь посмотрела, запущены ли какие-то службы с протоколом TCP (рис.5.2).

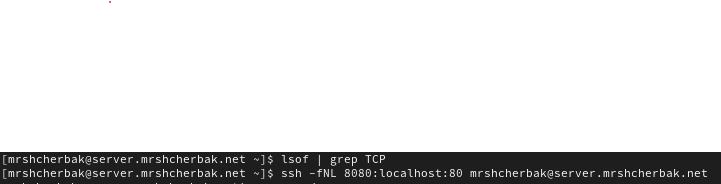


Рис.5.1. Перенаправление порта 80 на server.mrshcherbak.net на порт 8080 на локальной машине

Установлен SSH-туннель, и SSH слушает порт 8080. Произошло перенаправление порта.

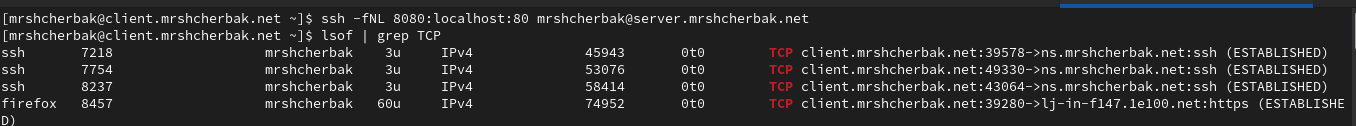


Рис.5.2. Выполнение команды

2. На клиенте запустила браузер и в адресной строке ввела localhost:8080. Отобразилась страница с приветствием (рис.5.3).

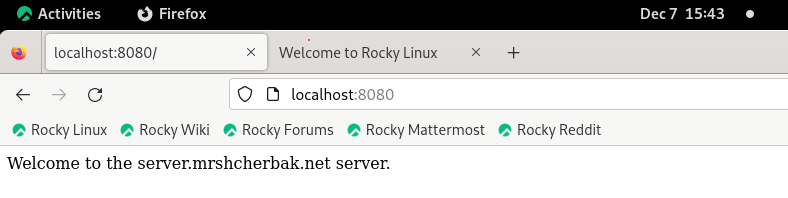


Рис.5.3. Отображение страницы по запросу localhost:8080

**6. Запуск консольных приложений через SSH**

1. На клиенте открыла терминал под пользователем mrshcherbak и посмотрела имя узла сервера, а также список файлов на сервере и почту (рис.6.1 – рис.6.2).

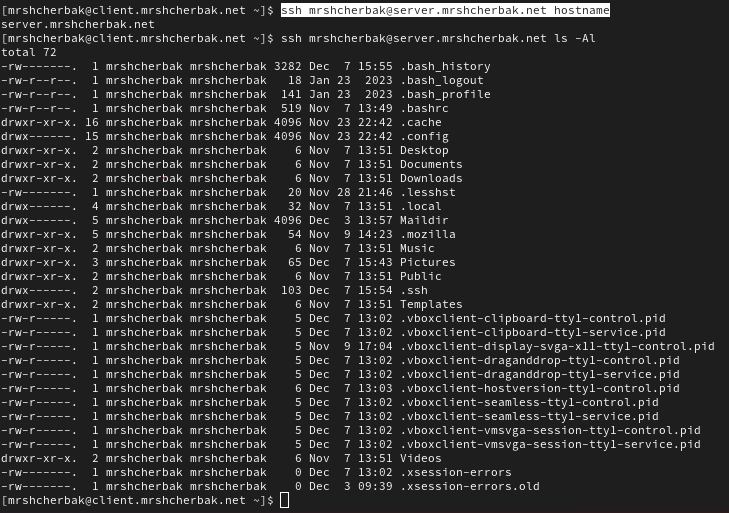


Рис.6.1. Просмотр имени узла сервера и списка файлов на сервере

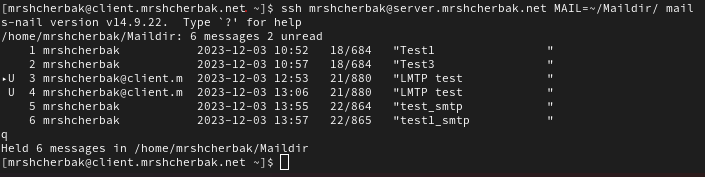


Рис.6.2. Просмотр почты на сервере с клиента

**7. Запуск графических приложений через SSH (X11Forwarding)**

1. На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешила отображать на локальном клиентском компьютере графические интерфейсы X11 (рис.7.1).

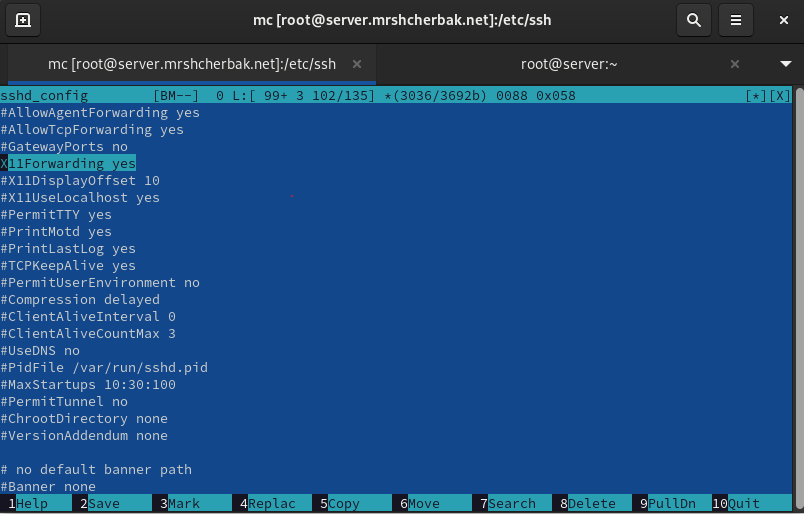


Рис.7.1. Редактирование файла /etc/ssh/sshd\_config

2. После сохранения изменения в конфигурационном файле перезапустила sshd.

3. Попробовала с клиента удалённо подключиться к серверу и запустить графическое приложение firefox (рис.7.2).

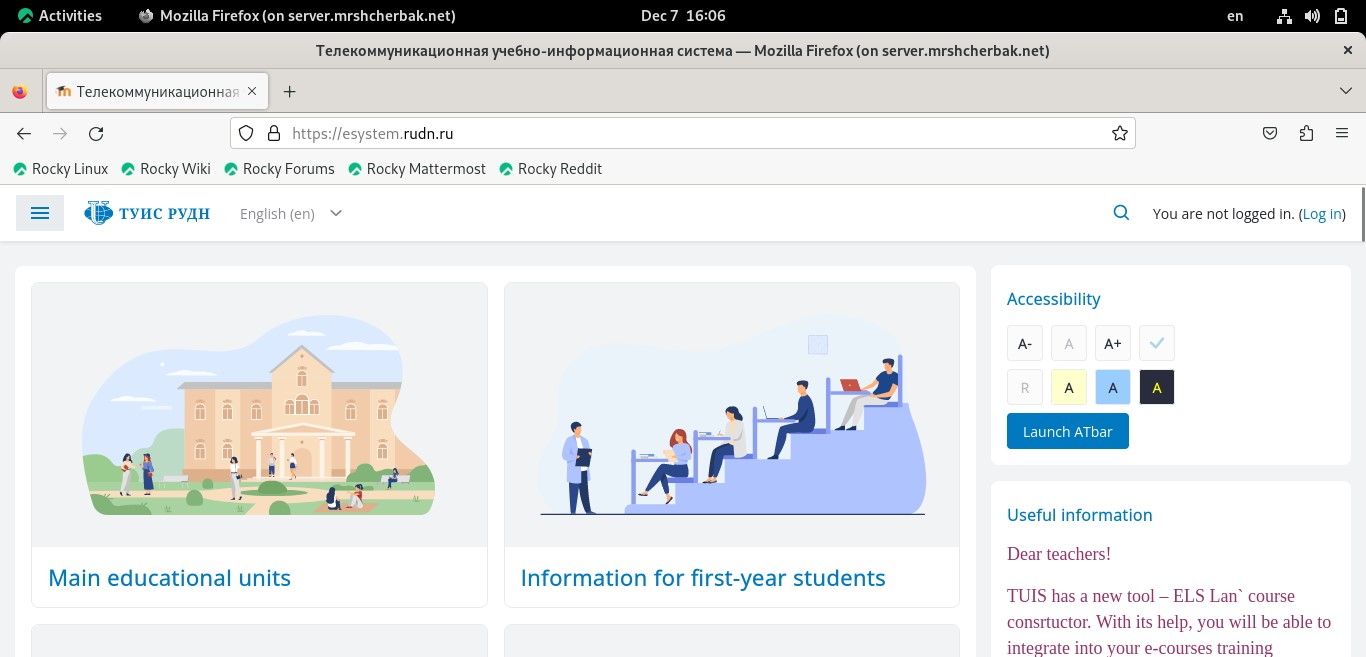


Рис.7.2. Страница сайта ТУИС на сервере в запущенном firefox

**8. 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 ssh, в который поместила в соответствующие подкаталоги конфигурационный файл sshd\_config, а в каталоге /vagrant/provision/server создала исполняемый файл ssh.sh и прописала в нём скрипт (рис.8.2). Действия представлены на рис.8.1.

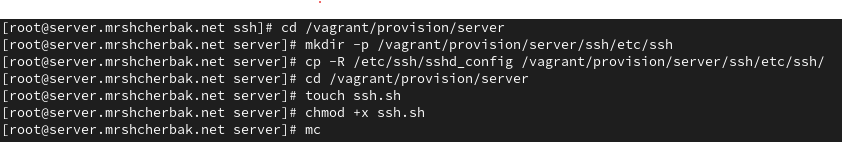


Рис.8.1. Выполнение команд

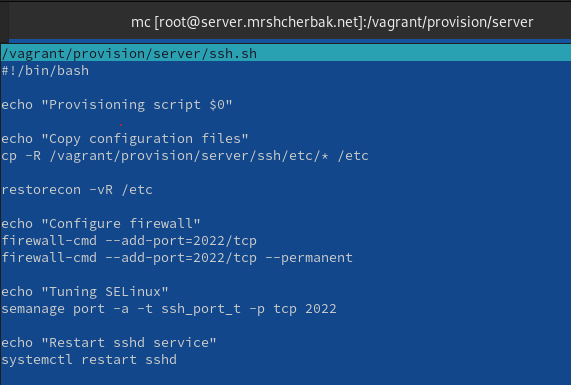


Рис.8.2. Содержимое файла ssh.sh

2. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавила в разделе конфигурации для сервера запись (рис.8.3).

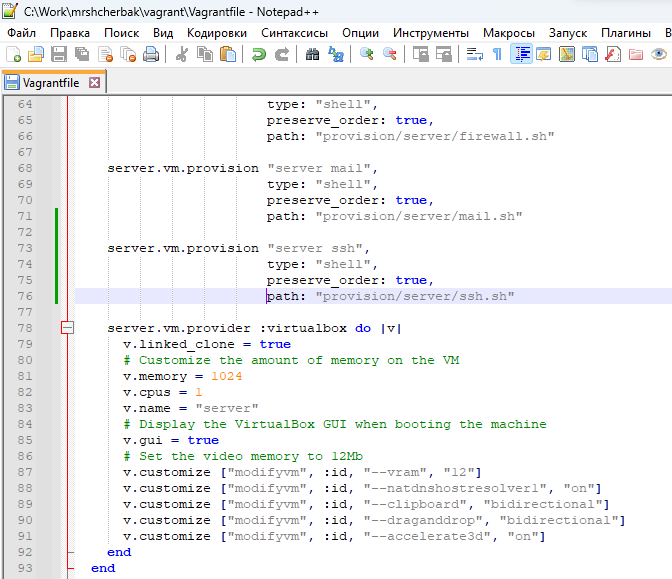


Рис.8.3. Редактирование файла Vagrantfile

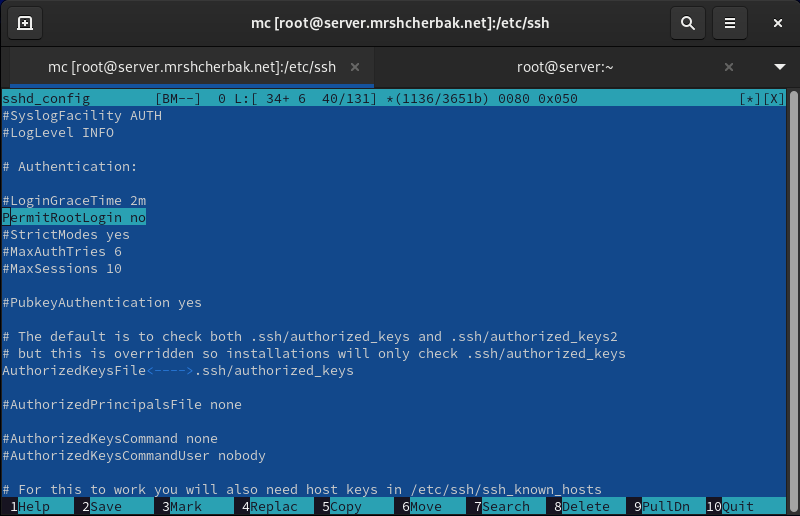
**Вывод:** таким образом, в ходе выполнения л/р №11, я приобрела практические навыки по настройке удалённого доступа к серверу с помощью SSH.

# Контрольные вопросы

1. Вы хотите запретить удалённый доступ по SSH на сервер пользователю root и разрешить доступ пользователю alice. Как это сделать?

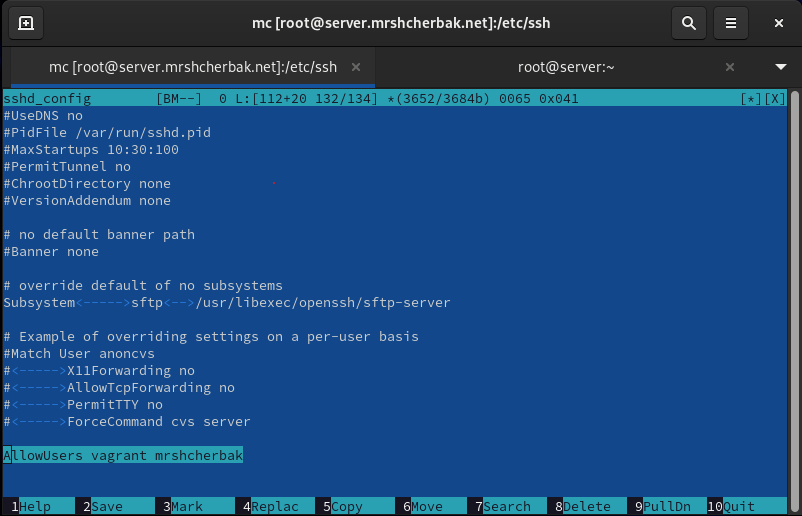
Чтобы запретить удалённый доступ по SSH пользователю root и разрешить доступ пользователю alice, нужно:

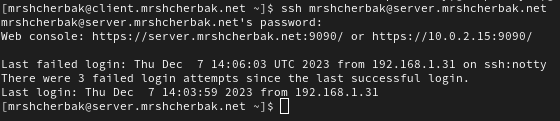
* отредактировать файл конфигурации SSH (/etc/ssh/sshd\_config) ⎯ найти строку PermitRootLogin и установить ее значение в no, после сохранения изменений в файле конфигурации перезапустить sshd: systemctl restart sshd.



* открыть файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и прописать строку AllowUsers vagrant alice, после сохранения изменений в файле конфигурации перезапустить sshd: systemctl restart sshd. Так, будет получен доступ к серверу посредством SSH-соединения через пользователя alice.

В данной л/р в разделах 1 и 2 я запрещала удалённый доступ по SSH на сервер пользователю root и разрешала доступ пользователю mrshcherbak.

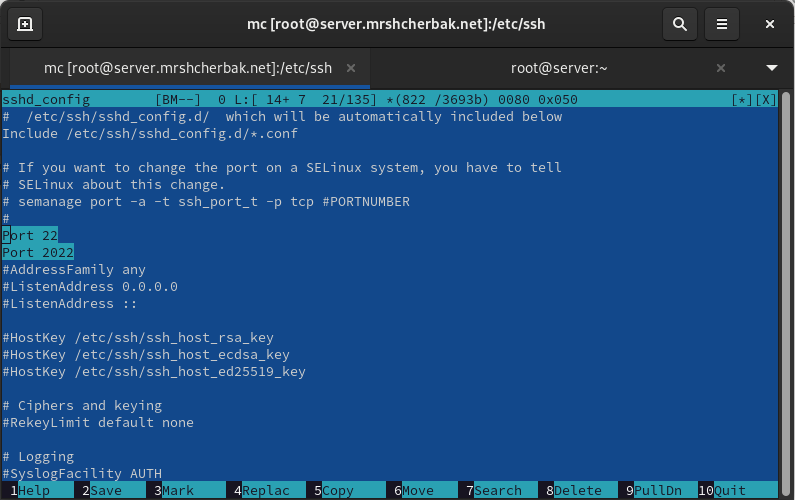




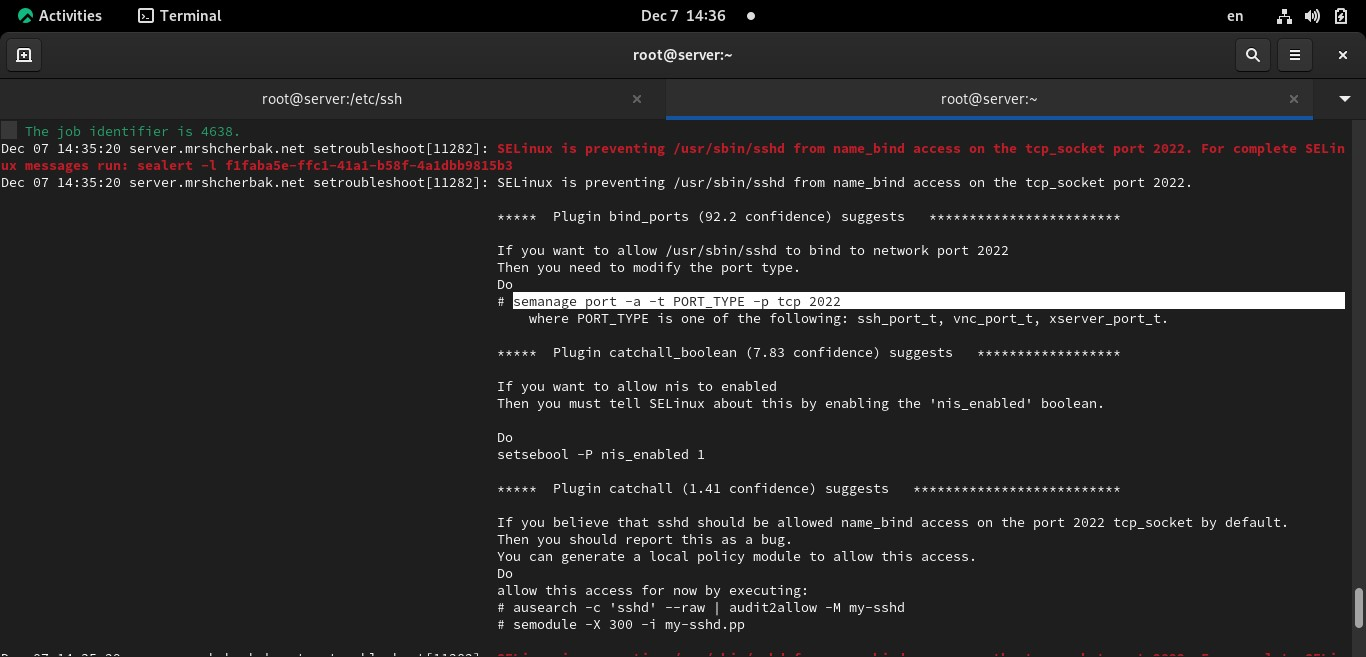
2. Как настроить удалённый доступ по SSH через несколько портов? Для чего это может потребоваться?

Для настройки удалённого доступа по SSH через несколько портов, необходимо отредактировать файл конфигурации SSH и добавить параметр Port, указав нужные порты, после чего, чтобы подключиться, необходимо изменить тип порта с помощью команды semanage в сообщениях мониторинга (более подробные действия описаны чуть ниже). Это может быть полезно для повышения безопасности, так как стандартный порт 22 может быть целью атак. Злоумышленник может использовать тот факт, что удалённый доступ по SSH обычно организуется через порт 22, а каждый узел Unix/Linux имеет учётную запись root. Основываясь на этой информации, злоумышленник может попытаться войти в систему как root, просто подбирая пароль. Возможные меры по усилению безопасности при организации удалённого доступа как раз включают в себя переадресацию стандартного для SSH порта 22 на нестандартный.

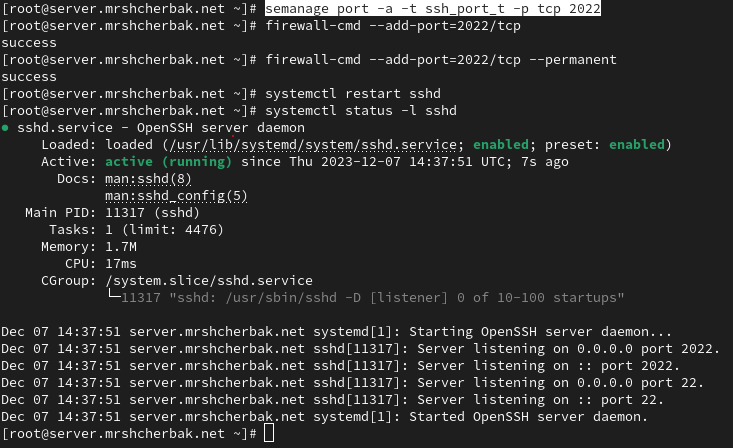
В данной л/р я на сервере в файле конфигурации sshd /etc/ssh/sshd\_config добавляла запись, которая сообщает процессу sshd о необходимости организации соединения через два разных порта, что даёт гарантию возможности открыть сеансы SSH, даже если была сделана ошибка в конфигурации.



После сохранения изменений в файле конфигурации перезапускала sshd и, чтобы подключиться, изменяла тип порта с помощью предложенной команды в сообщениях мониторинга.



Исправляла на сервере метки SELinux к порту 2022 и в настройках межсетевого экрана открывала порт 2022 протокола TCP, после чего перезапускала sshd. Статус показывал, что процесс sshd теперь прослушивает два порта.



3. Какие параметры используются для создания туннеля SSH, когда команда ssh устанавливает фоновое соединение и не ожидает какой-либо конкретной команды?

Чтобы создать туннель SSH в фоновом режиме без выполнения конкретной команды, можно использовать опции -fN. Пример:

ssh -fN -L локальный\_порт:удаленный\_хост:удаленный\_порт → пользователь@удаленный\_хост

Где:

-f указывает на фоновый режим.

-N говорит SSH не выполнять удаленную команду.

-L определяет локальный порт проброса.

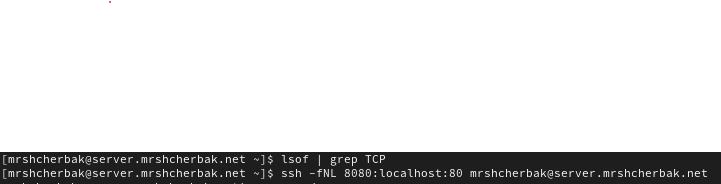
локальный\_порт - порт на вашей локальной машине.

удаленный\_хост - удаленный хост, к которому вы подключаетесь.

удаленный\_порт - порт на удаленном хосте.

Это создаст SSH-туннель, проброшенный через указанный удаленный хост и порт, и установит его в фоновом режиме.

В л/р я перенаправляла порт 80 на server.mrshcherbak.net на порт 8080 на локальной машине.

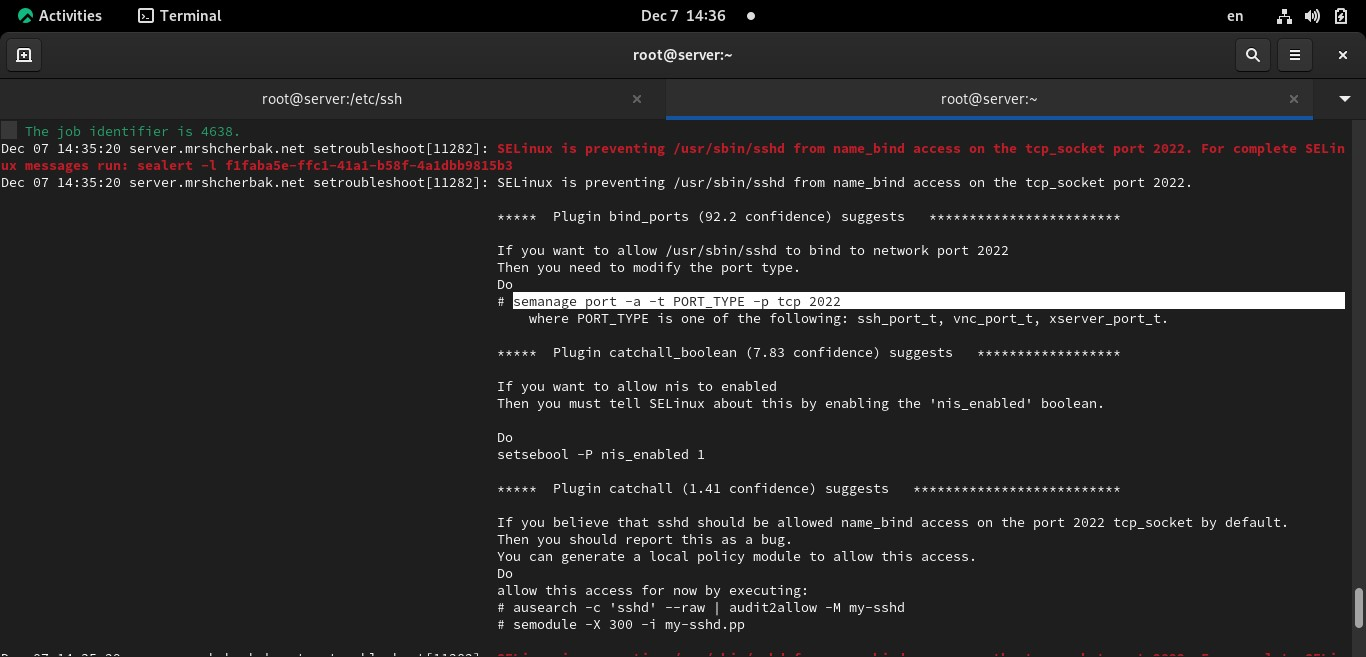


4. Как настроить локальную переадресацию с локального порта 5555 на порт 80 сервера server2.example.com?

ssh -L 5555:server2.example.com:80 user@your\_server.

5. Как настроить SELinux, чтобы позволить SSH связываться с портом 2022?

Чтобы SELinux позволял SSH связываться с портом 2022, необходимо выполнить команду: semanage port -a -t ssh\_port\_t -p tcp 2022.



6. Как настроить межсетевой экран на сервере, чтобы разрешить входящие подключения по SSH через порт 2022?

Открыла порт 2022 на уровне межсетевого экрана. Важно добавить --permanent, чтобы изменения сохранялись после перезагрузки системы. Далее перезапуск sshd и просмотр его статуса, чтобы проверить, правильно ли применены изменения.

