РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 11

дисциплина: Администрирование сетевых подсистем

Студент:

Группа:

**МОСКВА**

2022 г.

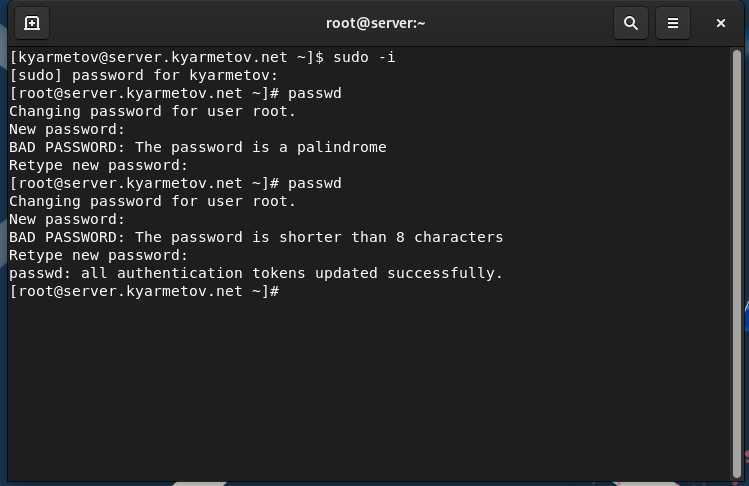
# Цель работы:

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

# Ход работы:

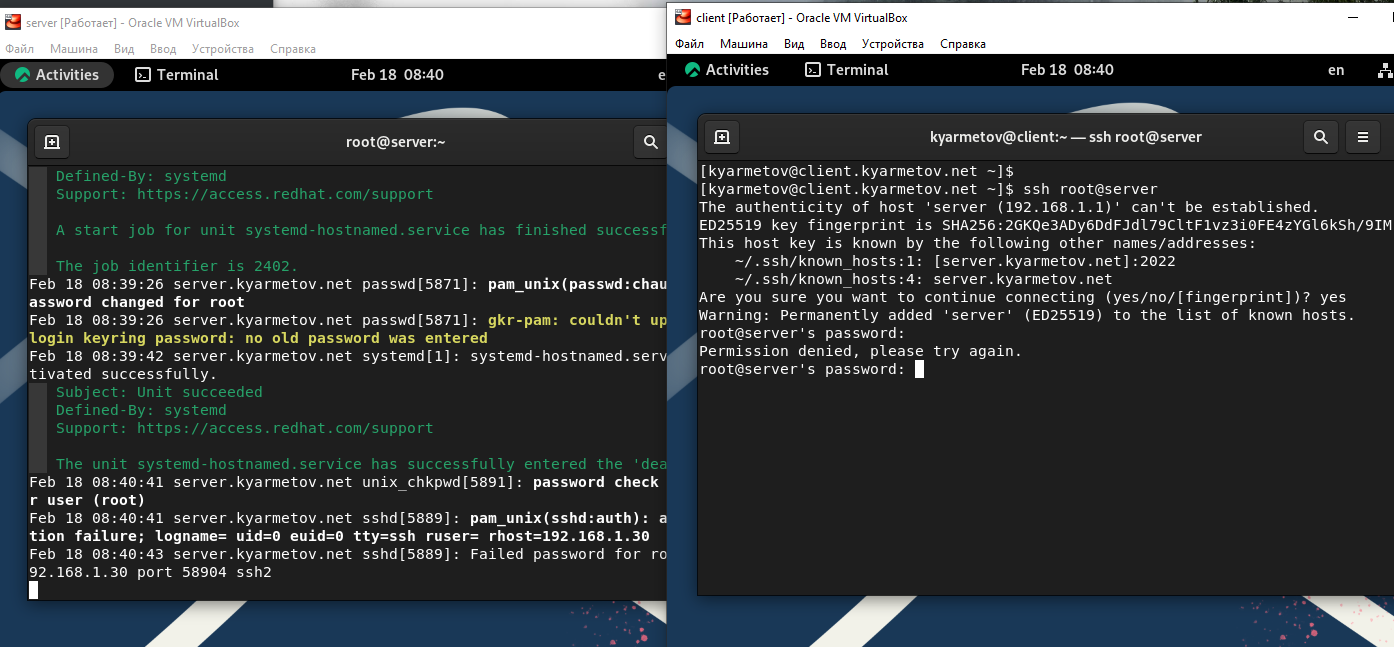
**11.4.1. Запрет удалённого доступа по SSH для пользователя root**

1. На сервере задайте пароль для пользователя root, если этого не было сделано ранее: sudo -i passwd root



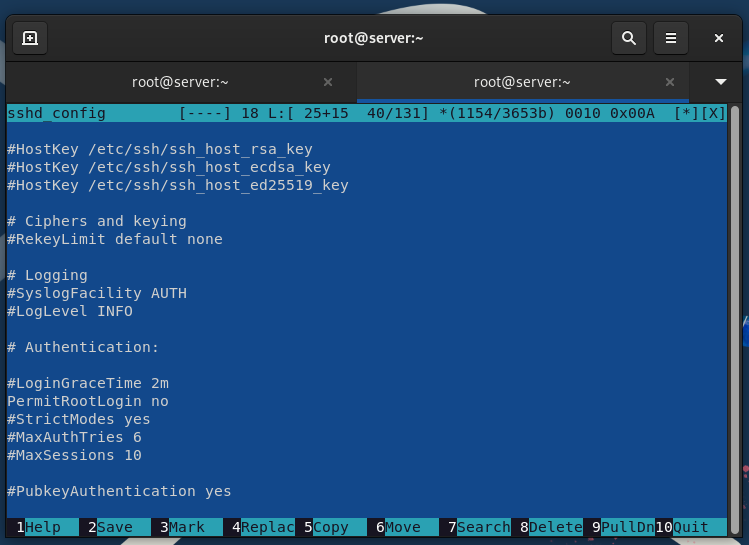
2. На сервере в дополнительном терминале запустите мониторинг системных событий: sudo -i journalctl -x -f

3. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя root: ssh root@server.user.net В отчёте поясните, что при этом происходит.



Клиент не подключается, оказалось, что нужно явно разрешить авторизацию суперпользователя

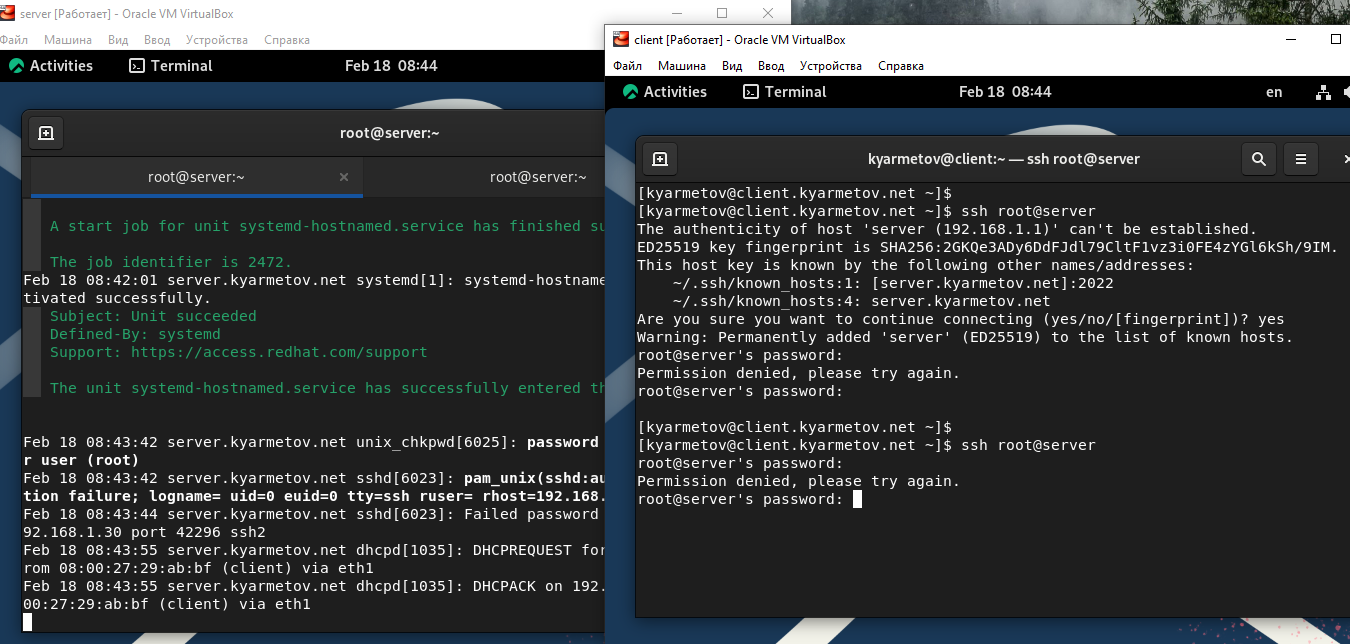
4. На сервере откройте файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root, установив: PermitRootLogin no



5. После сохранения изменений в файле конфигурации перезапустите sshd: systemctl restart sshd

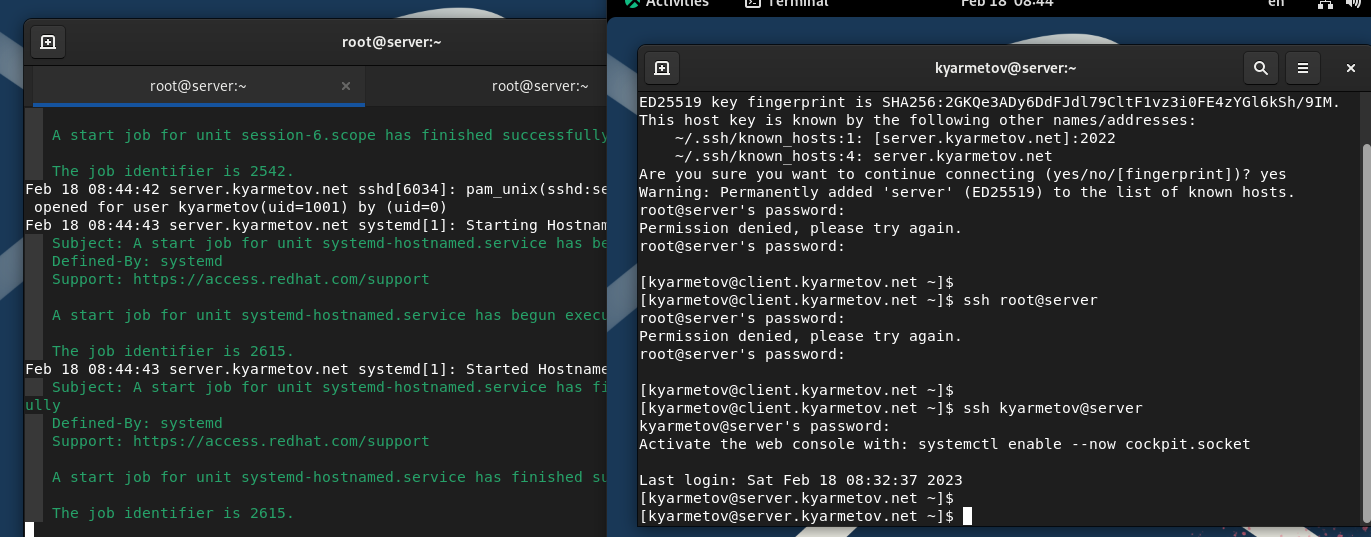
6. Повторите попытку получения доступа с клиента к серверу посредством SSHсоединения через пользователя root: ssh root@server В отчёте поясните, что при этом происходит.

Сервер отвергает подключение от имени суперпользователя.

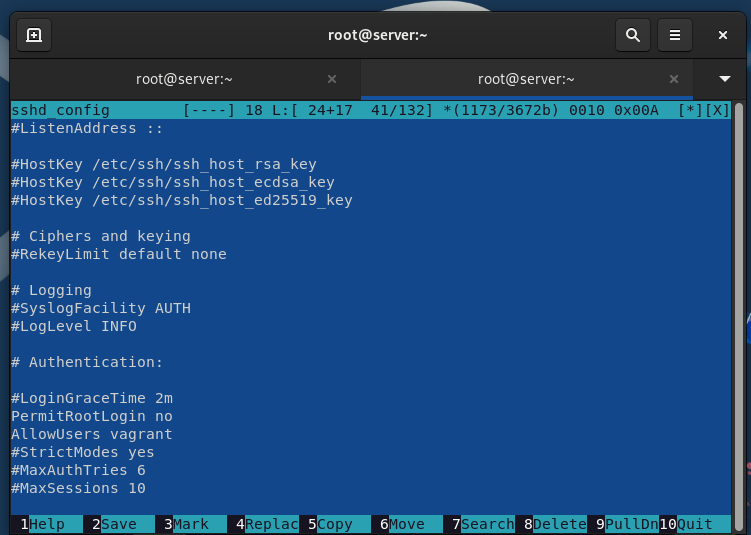


**11.4.2. Ограничение списка пользователей для удалённого доступа по SSH**

1. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user (вместо user укажите вашего пользователя): ssh user@server.user.net В отчёте поясните, что при этом происходит.

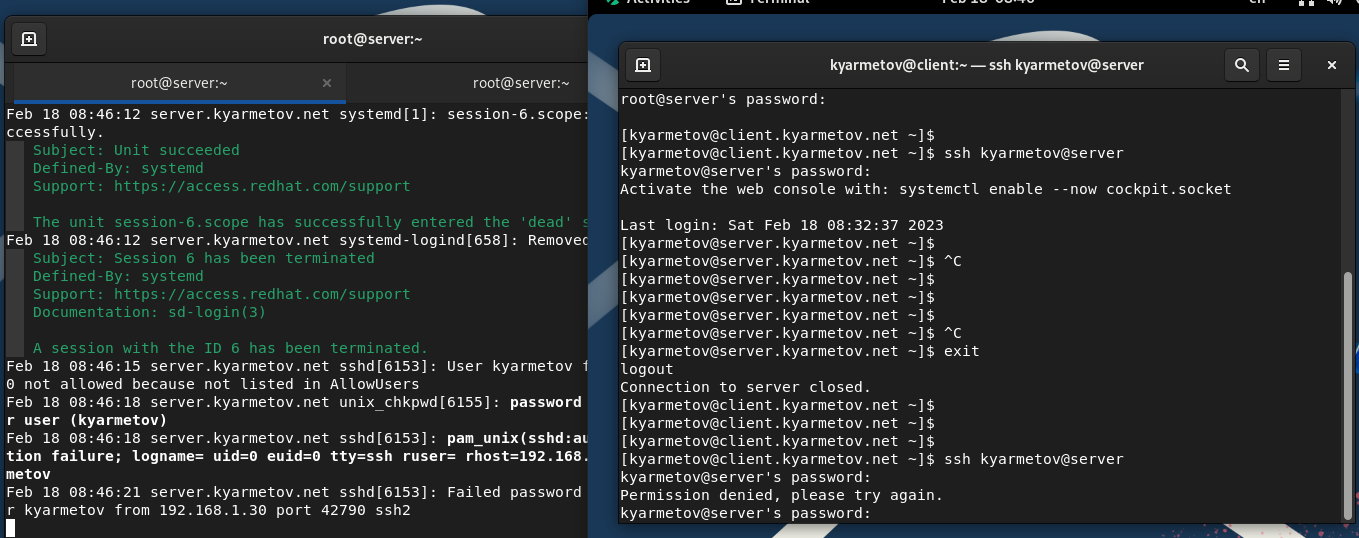


2. На сервере откройте файл /etc/ssh/sshd\_config конфигурации sshd на редактирование и добавьте строку AllowUsers vagrant

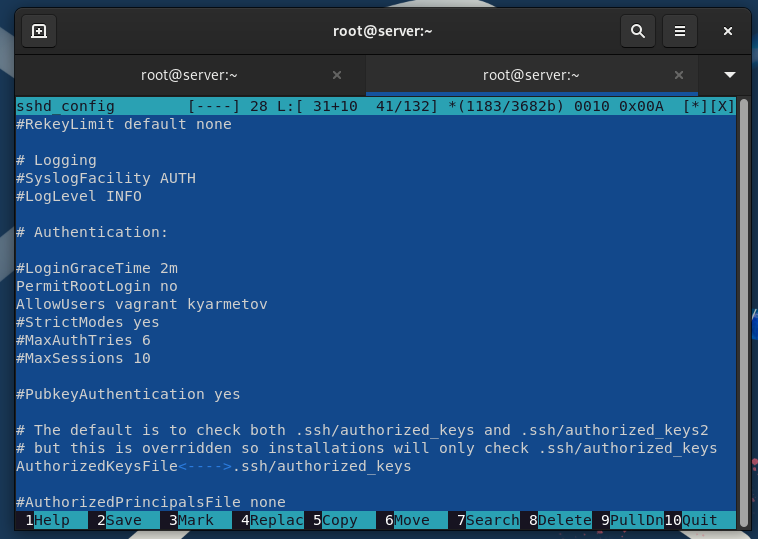


3. После сохранения изменений в файле конфигурации перезапустите sshd: systemctl restart sshd

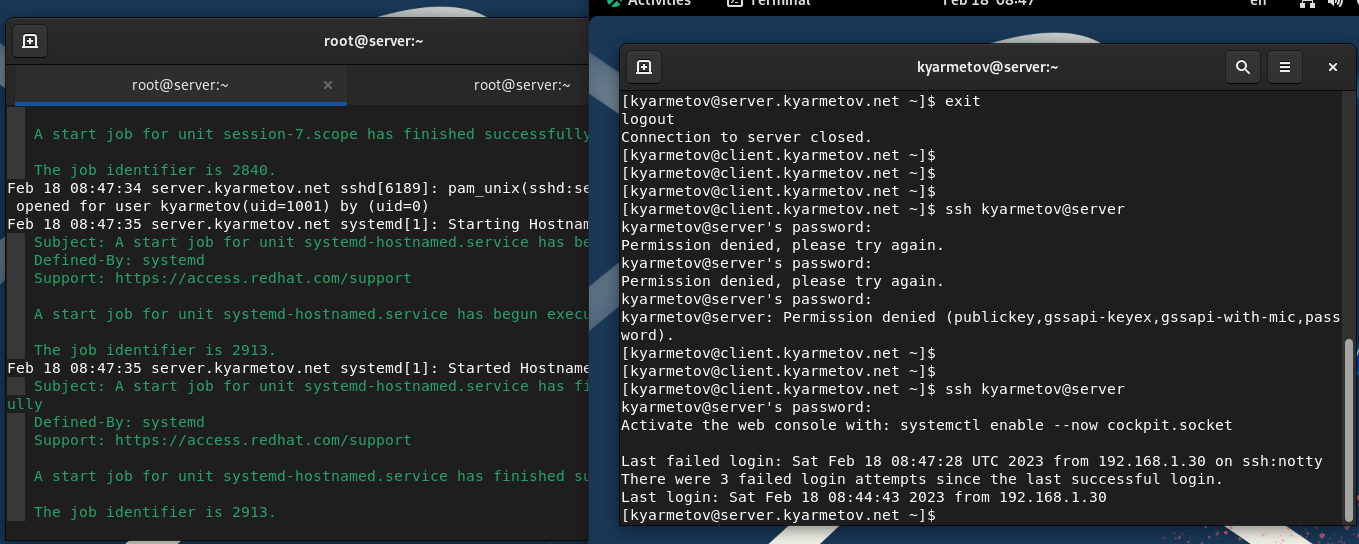
4. Повторите попытку получения доступа с клиента к серверу посредством SSHсоединения через пользователя user: ssh user@server.user.net В отчёте поясните, что при этом происходит.



5. В файле /etc/ssh/sshd\_config конфигурации sshd внесите следующее изменение: AllowUsers vagrant user

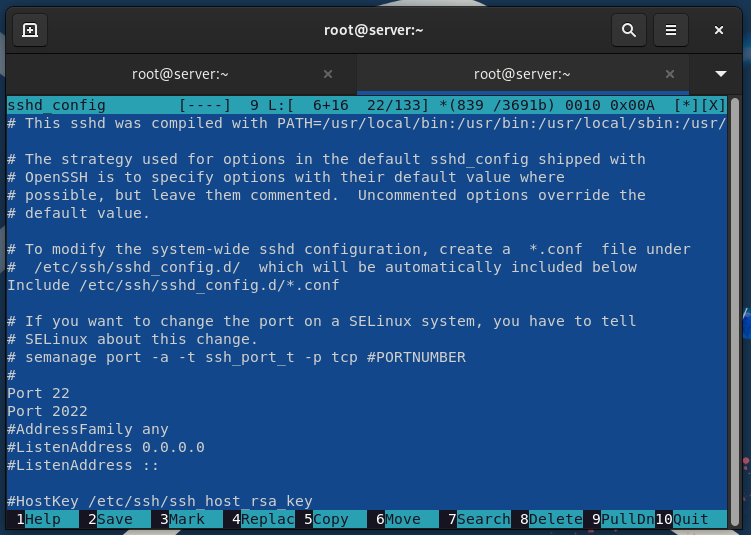


6. После сохранения изменений в файле конфигурации перезапустите sshd и вновь попытайтесь получить доступ с клиента к серверу посредством SSH-соединения через пользователя user. В отчёте поясните, что при этом происходит.



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

1. На сервере в файле конфигурации sshd /etc/ssh/sshd\_config найдите строку Port и ниже этой строки добавьте: Port 22 Port 2022 Эта запись 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.



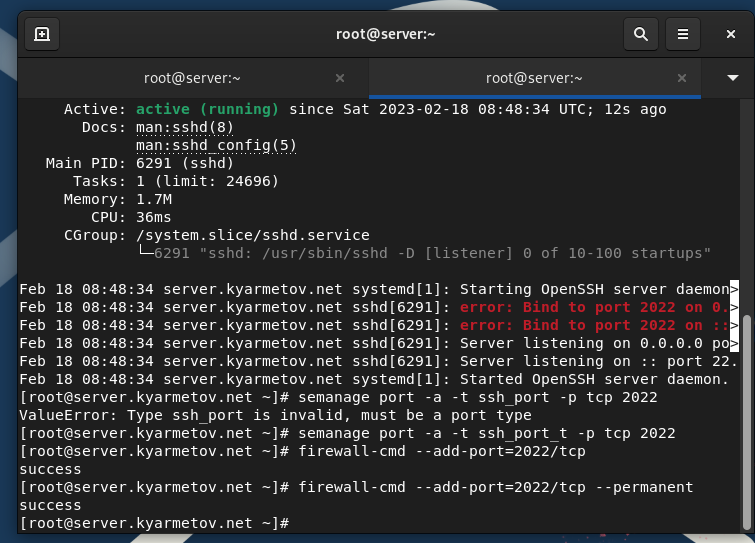
2. После сохранения изменений в файле конфигурации перезапустите sshd: systemctl restart sshd

3. Посмотрите расширенный статус работы sshd: systemctl status -l sshd Система должна сообщить вам об отказе в работе sshd через порт 2022.Дополнительно посмотрите сообщения в терминале с мониторингом системных событий. В отчёте поясните суть системных сообщений.

4. Исправьте на сервере метки SELinux к порту 2022: semanage port -a -t ssh\_port\_t -p tcp 2022

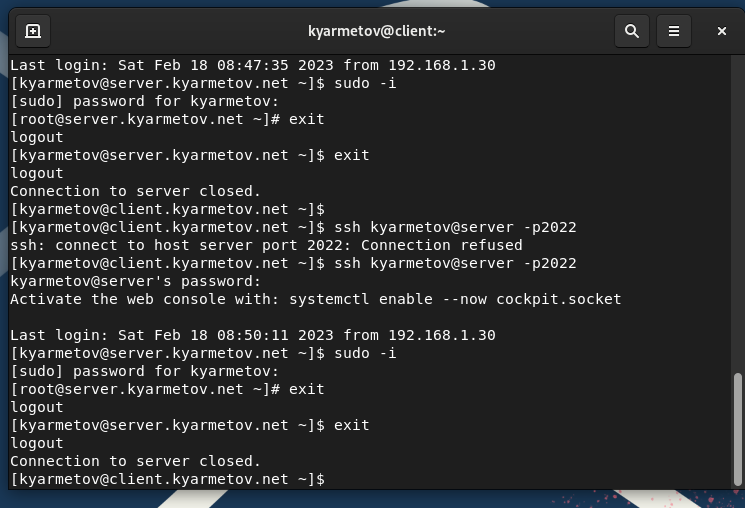
5. В настройках межсетевого экрана откройте порт 2022 протокола TCP: firewall-cmd --add-port=2022/tcp firewall-cmd --add-port=2022/tcp --permanent

6. Вновь перезапустите sshd и посмотрите расширенный статус его работы. Статус должен показать, что процесс sshd теперь прослушивает два порта. \



7. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user (вместо user укажите вашего пользователя): ssh user@server.user.net После открытия оболочки пользователя введите sudo -i для получения доступа root.

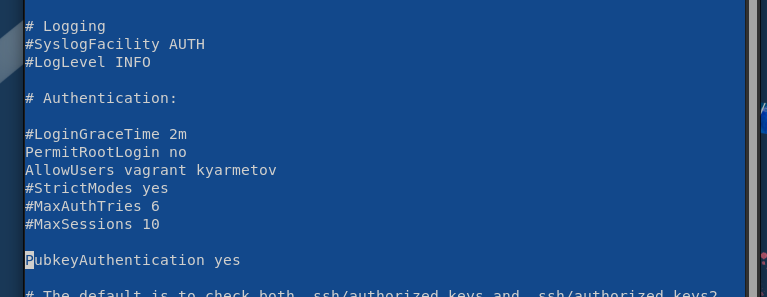
8. Повторите попытку получения доступа с клиента к серверу посредством SSHсоединения через пользователя user, указав порт 2022: ssh -p2022 user@server.user.net После открытия оболочки пользователя введите sudo -i для получения доступа root.



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

В этом упражнении вы создаёте пару из открытого и закрытого ключей для входа на сервер.

1. На сервере в конфигурационном файле /etc/ssh/sshd\_config задайте параметр, разрешающий аутентификацию по ключу: PubkeyAuthentication yes



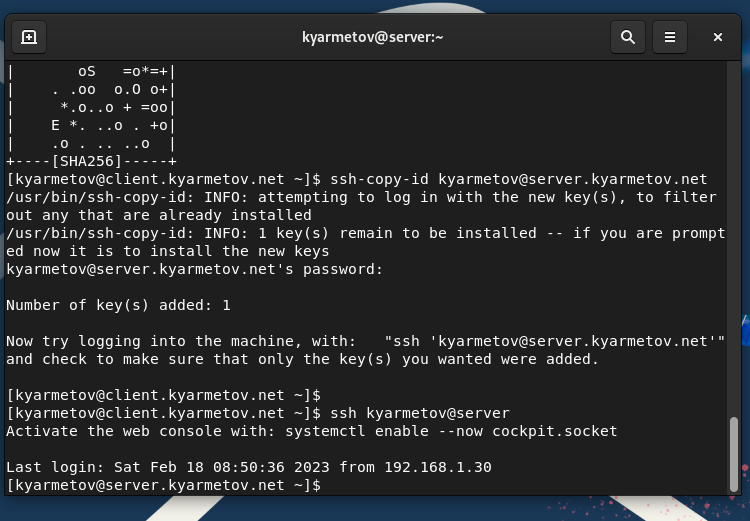
2. После сохранения изменений в файле конфигурации перезапустите sshd.

3. На клиенте сформируйте SSH-ключ, введя в терминале под пользователем user (вместо user используйте ваш логин): ssh-keygen Когда вас спросят, хотите ли вы использовать кодовую фразу, нажмите Enter , чтобы использовать установку без пароля. При запросе имени файла, в котором будет храниться закрытый ключ, примите предлагаемое по умолчанию имя файла (~/.ssh/id\_rsa). Когда вас попросят ввести кодовую фразу, нажмите Enter дважды.

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

5. Скопируйте открытый ключ на сервер, введя на клиенте (вместо user укажите вашего пользователя): ssh-copy-id user@server.user.net При запросе введите пароль пользователя на удалённом сервере.

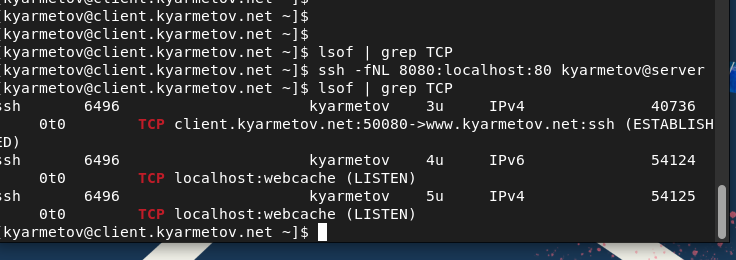
6. Попробуйте получить доступ с клиента к серверу посредством SSH-соединения (вместо user используйте ваш логин): ssh user@server.user.net Теперь вы должны пройти аутентификацию без ввода пароля для учётной записи удалённого пользователя.



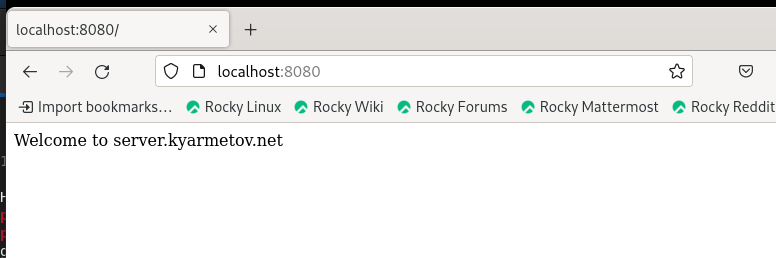
**11.4.5. Организация туннелей SSH, перенаправление TCP-портов**

1. На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP: lsof | grep TCP

1. Перенаправьте порт 80 на server.user.net на порт 8080 на локальной машине (вместо user используйте ваш логин): ssh -fNL 8080:localhost:80 [user@server.user.net](mailto:user@server.user.net)
2. Вновь на клиенте посмотрите, запущены ли какие-то службы с протоколом TCP: lsof | grep TCP В отчёте прокомментируйте полученную при выводе на экран информацию.



1. На клиенте запустите браузер и в адресной строке введите localhost:8080. Убедитесь, что отобразится страница с приветствием «Welcome to the server.user.net server».

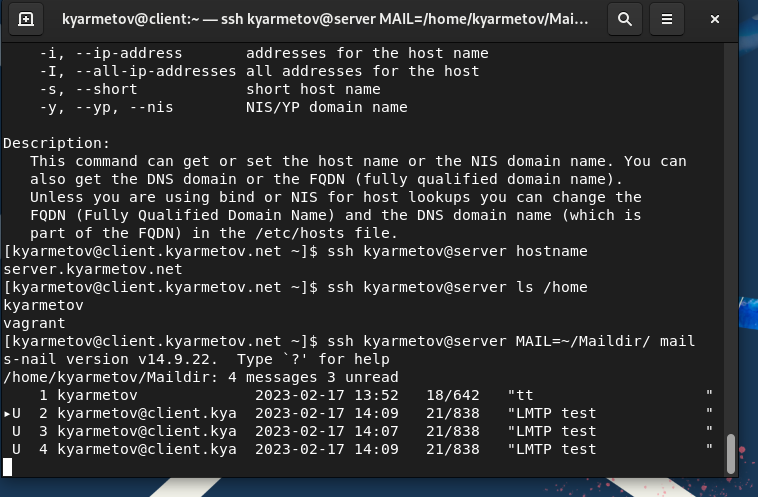


**11.4.6. Запуск консольных приложений через SSH**

1. На клиенте откройте терминал под пользователем user (вместо user используйте ваш логин).

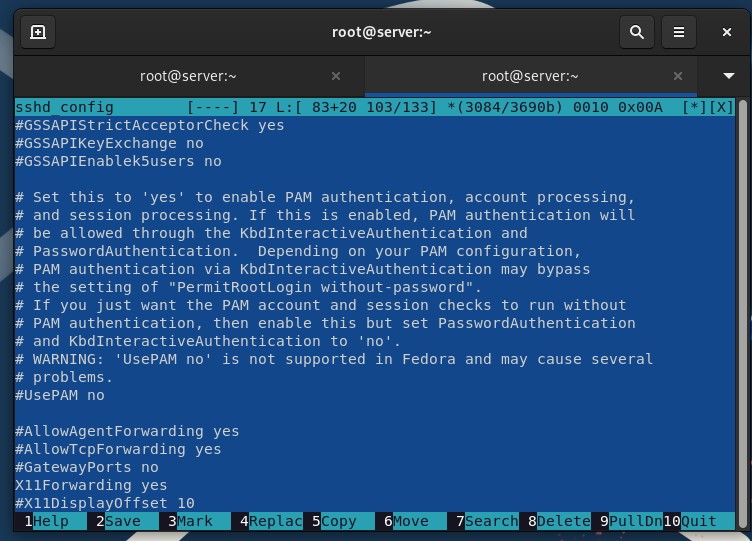
2. Посмотрите с клиента имя узла сервера: ssh user@server.user.net hostname

3. Посмотрите с клиента список файлов на сервере: ssh user@server.user.net ls –Al



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

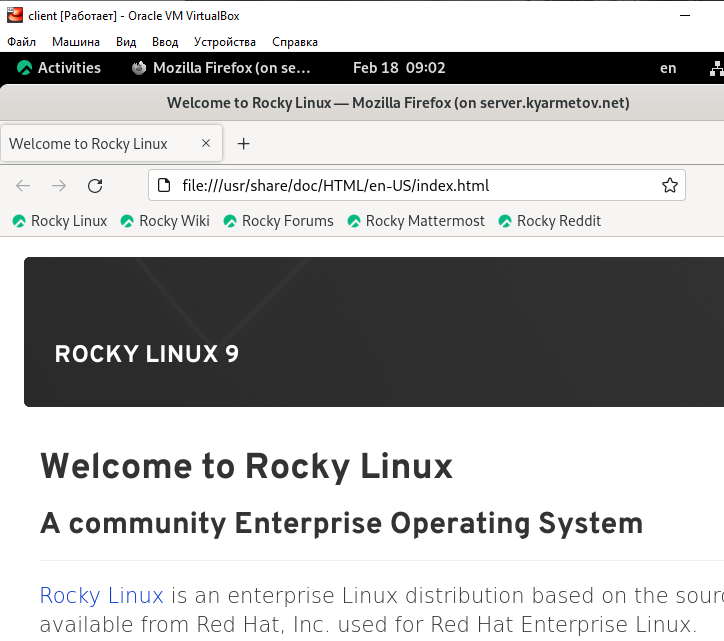
1. На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешите отображать на локальном клиентском компьютере графические интерфейсы X11: X11Forwarding yes



2. После сохранения изменения в конфигурационном файле перезапустите sshd.

3. Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox (вместо user используйте ваш логин): ssh -YC user@server.user.net

firefox



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

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог ssh, в который поместите в соответствующие подкаталоги конфигурационный файл sshd\_config: cd /vagrant/provision/server mkdir -p /vagrant/provision/server/ssh/etc/ssh cp -R /etc/ssh/sshd\_config /vagrant/provision/server/ssh/etc/ssh/

2. В каталоге /vagrant/provision/server создайте исполняемый файл ssh.sh: cd /vagrant/provision/server touch ssh.sh chmod +x ssh.sh Открыв его на редактирование, пропишите в нём следующий скрипт: #!/bin/bash echo "Provisioning script $0" echo "Copy configuration files" cp -R /vagrant/provision/server/ssh/etc/\* /etc restorecon -vR /etc echo "Configure firewall" firewall-cmd --add-port=2022/tcp firewall-cmd --add-port=2022/tcp --permanent echo "Tuning SELinux" semanage port -a -t ssh\_port\_t -p tcp 2022 echo "Restart sshd service" systemctl restart sshd

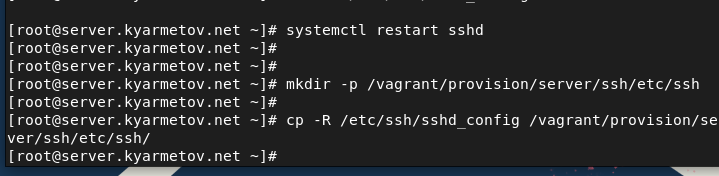
3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:

server.vm.provision "server ssh",

type: "shell",

preserve\_order: true,

path: "provision/server/ssh.sh"



# 

# Вывод:

Приобретены практические навыки по работе с ssh и перенаправлением портов.