РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 11

**Настройка безопасного удалённого доступа по протоколу SSH**

*дисциплина: Администрирование* *Сетевых Подсистем*

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

**Цель работы:**

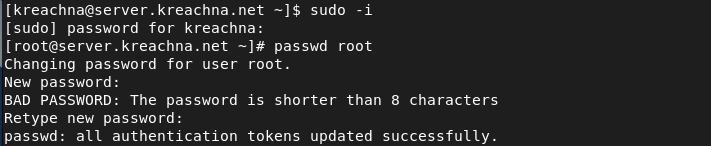
Приобретение практических навыков по настройке удалённого доступа к серверу с помощью SSH.

**Выполнение работы:**

1. **Запрет удалённого доступа по SSH для пользователя root**
2. На сервере задайте пароль для пользователя root, если этого не было сделано ранее:

sudo -i

passwd root



1. На сервере в дополнительном терминале запустите мониторинг системных событий:

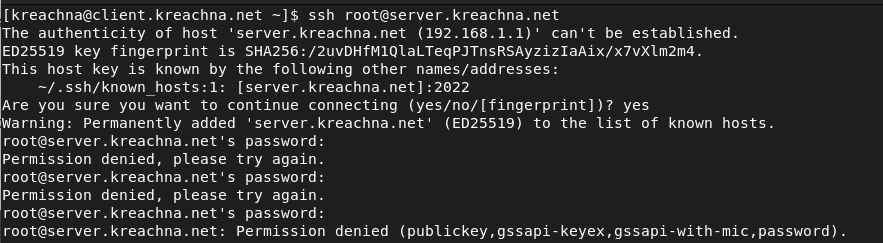
sudo -i

journalctl -x -f



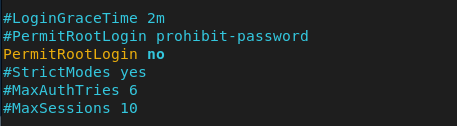
1. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя root:

ssh [root@server.kreachna.net](mailto:root@server.kreachna.net)



1. На сервере откройте файл /etc/ssh/sshd\_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root, установив:

PermitRootLogin no

****

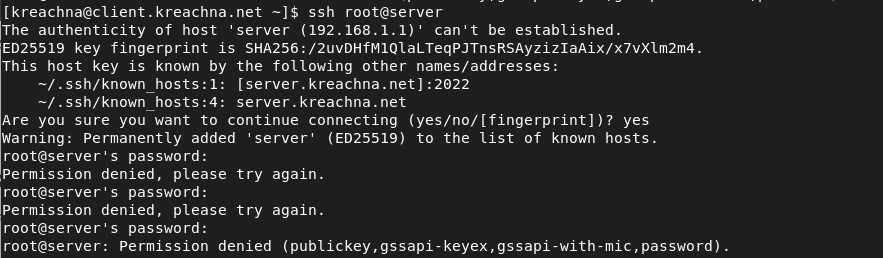
1. После сохранения изменений в файле конфигурации перезапустите sshd:

systemctl restart sshd



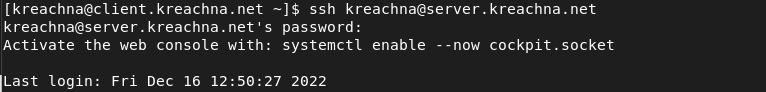
1. Повторите попытку получения доступа с клиента к серверу посредством SSH соединения через пользователя root:

ssh root@server



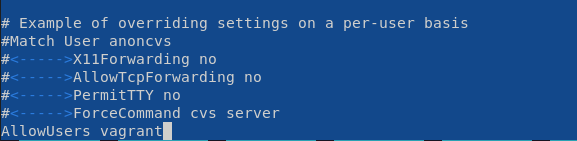
1. **Ограничение списка пользователей для удалённого доступа по SSH**
2. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя kreachna:

ssh [kreachna@server.kreachna.net](mailto:kreachna@server.kreachna.net)



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

AllowUsers vagrant

****

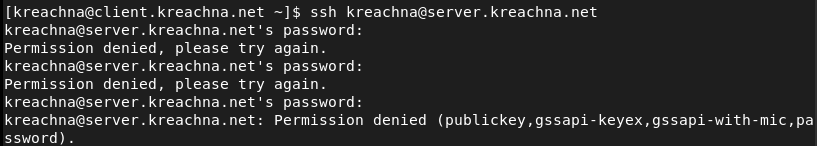
1. После сохранения изменений в файле конфигурации перезапустите sshd:

systemctl restart sshd



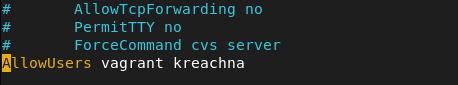
1. Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user:

ssh [kreachna@server.kreachna.net](mailto:kreachna@server.kreachna.net)

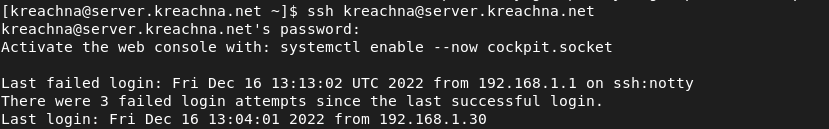


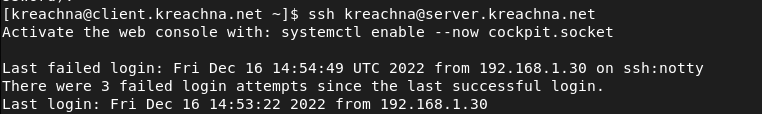
1. В файле /etc/ssh/sshd\_config конфигурации sshd внесите следующее изменение:

AllowUsers vagrant user

****

1. После сохранения изменений в файле конфигурации перезапустите sshd и вновь попытайтесь получить доступ с клиента к серверу посредством SSH-соединения через пользователя kreachna.

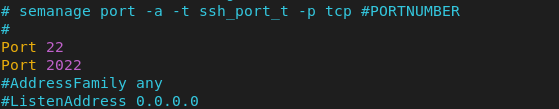




1. **Настройка дополнительных портов для удалённого доступа по SSH**
2. На сервере в файле конфигурации sshd /etc/ssh/sshd\_config найдите строку Port и ниже этой строки добавьте:

Port 22

Port 2022

****

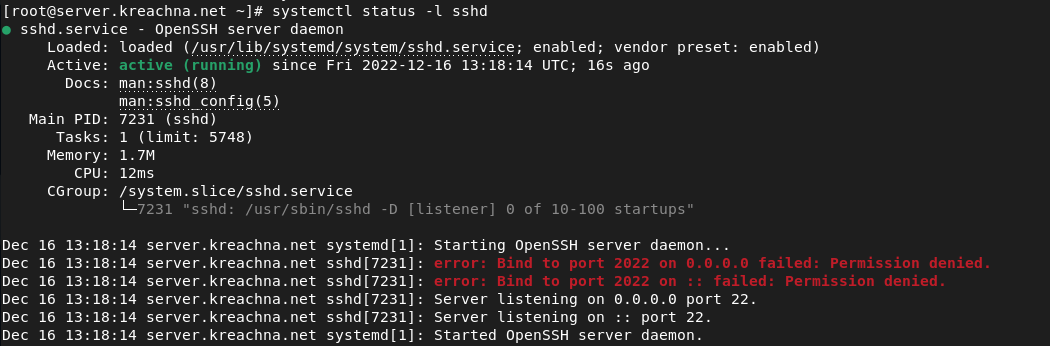
1. После сохранения изменений в файле конфигурации перезапустите sshd:

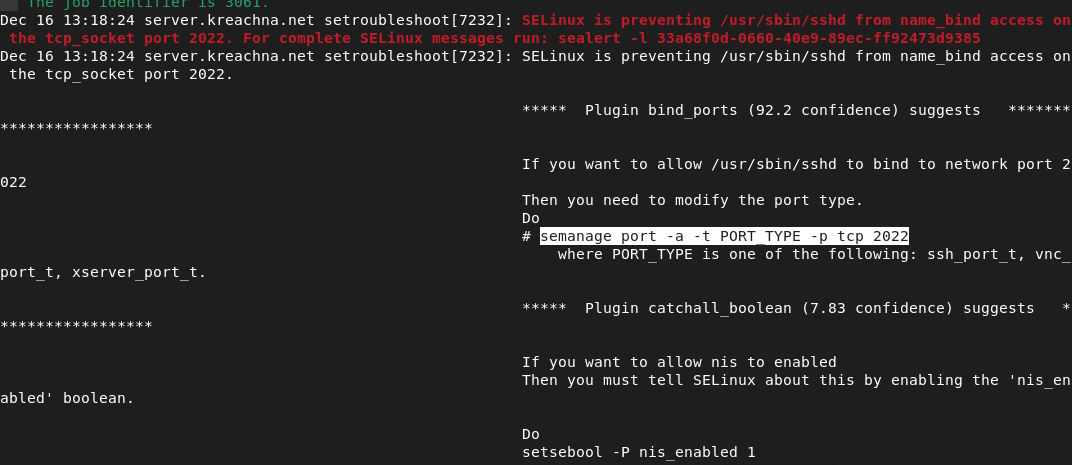
systemctl restart sshd



1. Посмотрите расширенный статус работы sshd:

systemctl status -l sshd



****

1. Исправьте на сервере метки SELinux к порту 2022:

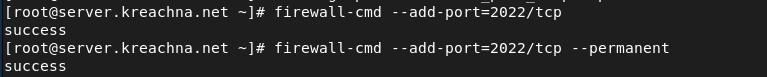
semanage port -a -t ssh\_port\_t -p tcp 2022



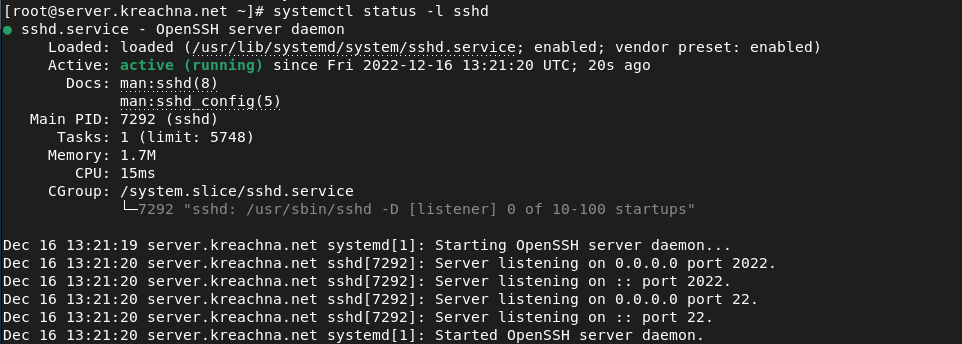
1. В настройках межсетевого экрана откройте порт 2022 протокола TCP:

firewall-cmd --add-port=2022/tcp

firewall-cmd --add-port=2022/tcp –permanent

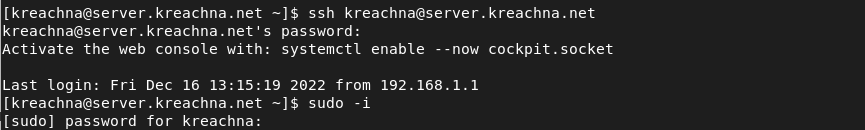


1. Вновь перезапустите sshd и посмотрите расширенный статус его работы. Статус должен показать, что процесс sshd теперь прослушивает два порта.



1. С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя kreachna:

ssh [kreachna@server.kreachna.net](mailto:kreachna@server.kreachna.net)



После открытия оболочки пользователя введите sudo -i для получения доступа root.

1. Повторите попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user, указав порт 2022:

ssh -p2022 [user@server.user.net](mailto:user@server.user.net)



После открытия оболочки пользователя введите sudo -i для получения доступа root.

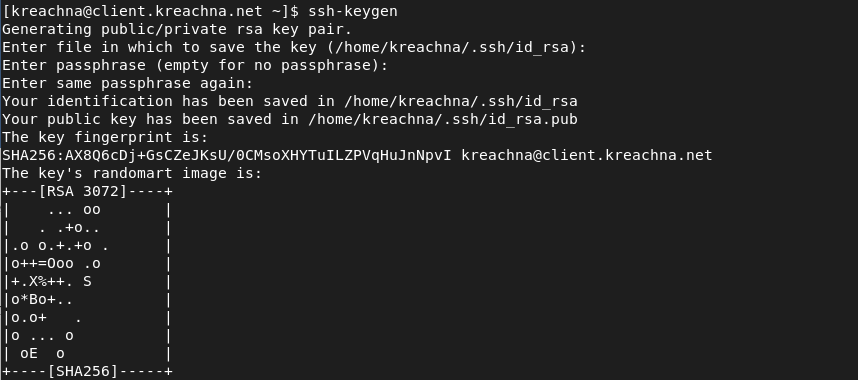
1. **Настройка удалённого доступа по SSH по ключу**
2. На сервере в конфигурационном файле /etc/ssh/sshd\_config задайте параметр, разрешающий аутентификацию по ключу:

PubkeyAuthentication yes

****

1. После сохранения изменений в файле конфигурации перезапустите sshd.
2. На клиенте сформируйте SSH-ключ, введя в терминале под пользователем kreachna:

ssh-keygen

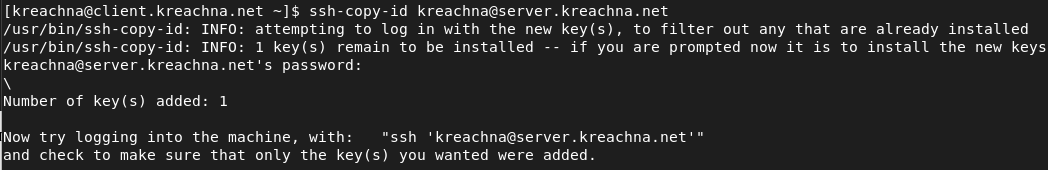


1. Закрытый ключ теперь будет записан в файл ~/.ssh/id\_rsa, а открытый ключ записывается в файл ~/.ssh/id\_rsa.pub.



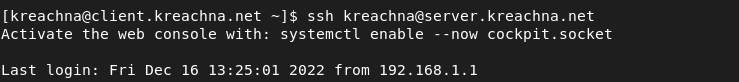
1. Скопируйте открытый ключ на сервер, введя на клиенте:

ssh-copy-id kreachna@server.kreachna.net



1. Попробуйте получить доступ с клиента к серверу посредством SSH-соединения:

ssh [kreachna@server.kreachna.net](mailto:kreachna@server.kreachna.net)



1. **Организация туннелей SSH, перенаправление TCP-портов**
2. На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP:

lsof | grep TCP



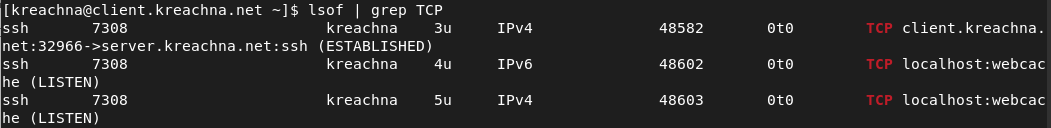
1. Перенаправьте порт 80 на server.user.net на порт 8080 на локальной машине:

ssh -fNL 8080:localhost:80 [kreachna@server.kreachna.net](mailto:kreachna@server.kreachna.net)



1. Вновь на клиенте посмотрите, запущены ли какие-то службы с протоколом TCP:

lsof | grep TCP



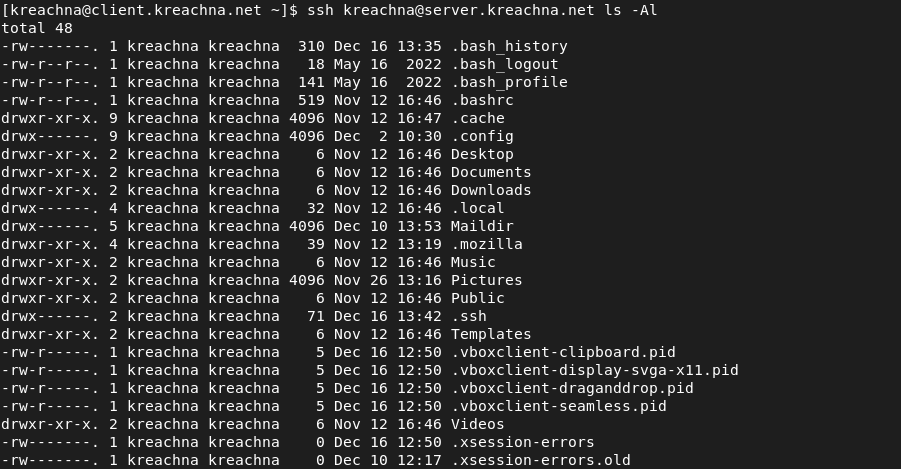
1. На клиенте запустите браузер и в адресной строке введите localhost:8080. Убедитесь, что отобразится страница с приветствием «Welcome to the server.kreachna.net server».
2. **Запуск консольных приложений через SSH**
3. На клиенте откройте терминал под пользователем user (вместо user используйте ваш логин).
4. Посмотрите с клиента имя узла сервера:

ssh kreachna@server.kreachna.net hostname



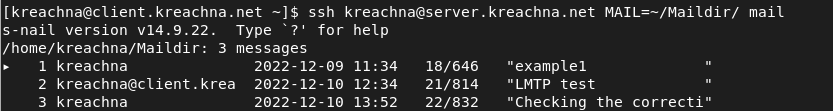
1. Посмотрите с клиента список файлов на сервере:

ssh kreachna@server.kreachna.net ls -Al



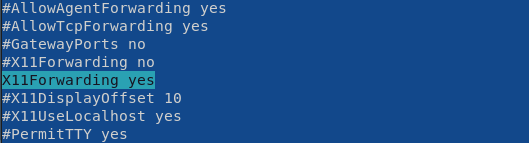
1. Посмотрите с клиента почту на сервере:

ssh kreachna@server.kreachna.net MAIL=~/Maildir/ mail



1. **Запуск графических приложений через SSH (X11Forwarding)**
2. На сервере в конфигурационном файле /etc/ssh/sshd\_config разрешите отображать на локальном клиентском компьютере графические интерфейсы X11:

X11Forwarding yes

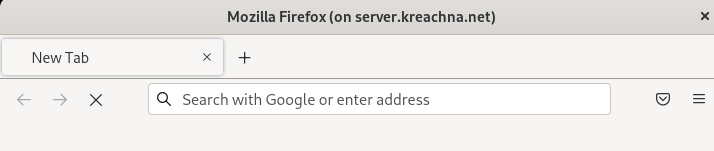


1. После сохранения изменения в конфигурационном файле перезапустите sshd.



1. Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox (вместо user используйте ваш логин):

ssh -YC kreachna@server.kreachna.net firefox



1. **Внесение изменений в настройки внутреннего окружения виртуальной машины**
2. 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:



1. В каталоге /vagrant/provision/server создайте исполняемый файл ssh.sh:

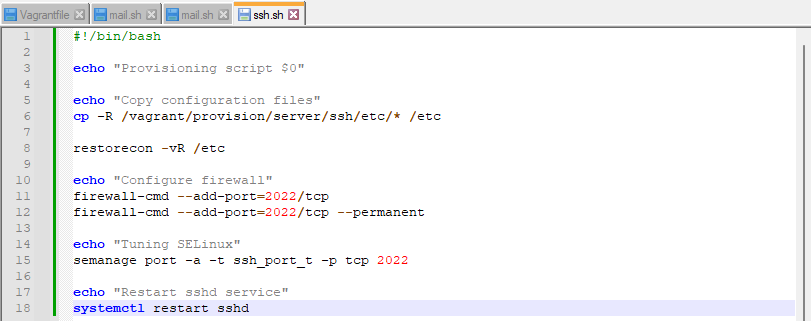
cd /vagrant/provision/server

touch ssh.sh

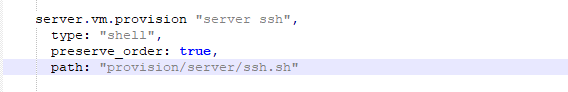
chmod +x ssh.sh



Открыв его на редактирование, пропишите в нём следующий скрипт:



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



**Ответ на контрольные вопросы:**

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

/etc/ssh/sshd\_config: PermitRootlogin no

/etc/ssh/sshd\_config: AllowUsers alice

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

Добавить новый порт в в файле конфигурации, исправить метки безопасности и открыть порт в настройках межсетевого экрана. Организация через разные порты дает гарантию возможности открыть сеансы ssh даже при ошибки конфигурации.

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

fN

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

ssh -fNL 5555:localhost:80 server2.example.com

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

semanage port -a -t ssh\_port\_t -p tcp 2022

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

firewall-cmd --add-port=2022/tcp

firewall-cmd --add-port=2022/tcp --permanent

**Вывод:**

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