Лабораторная работа 11

Настройка безопасного удалённого доступа по протоколу SSH

Митрофанов Тимур Александрович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Задание

1. Настройте запрет удалённого доступа на сервер по SSH для пользователя root (см. раздел 11.4.1).
2. Настройте разрешение удалённого доступа к серверу по SSH только для пользователей группы vagrant и вашего пользователя (см. раздел 11.4.2).
3. Настройте удалённый доступ к серверу по SSH через порт 2022 (см. раздел 11.4.3).
4. Настройте удалённый доступ к серверу по SSH по ключу (см. раздел 11.4.4).
5. Организуйте SSH-туннель с клиента на сервер, перенаправив локальное соединение с TCP-порта 80 на порт 8080 (см. раздел 11.4.5).
6. Используя удалённое SSH-соединение, выполните с клиента несколько команд на сервере (см. раздел 11.4.6).
7. Используя удалённое SSH-соединение, запустите с клиента графическое приложение на сервере (см. раздел 11.4.7).
8. Напишите скрипт для Vagrant, фиксирующий действия по настройке SSH-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile (см. раздел 11.4.8).

3 Выполнение лабораторной работы

На сервере задайте пароль для пользователя root, если этого не было сделано ранее (рис. 3.1).

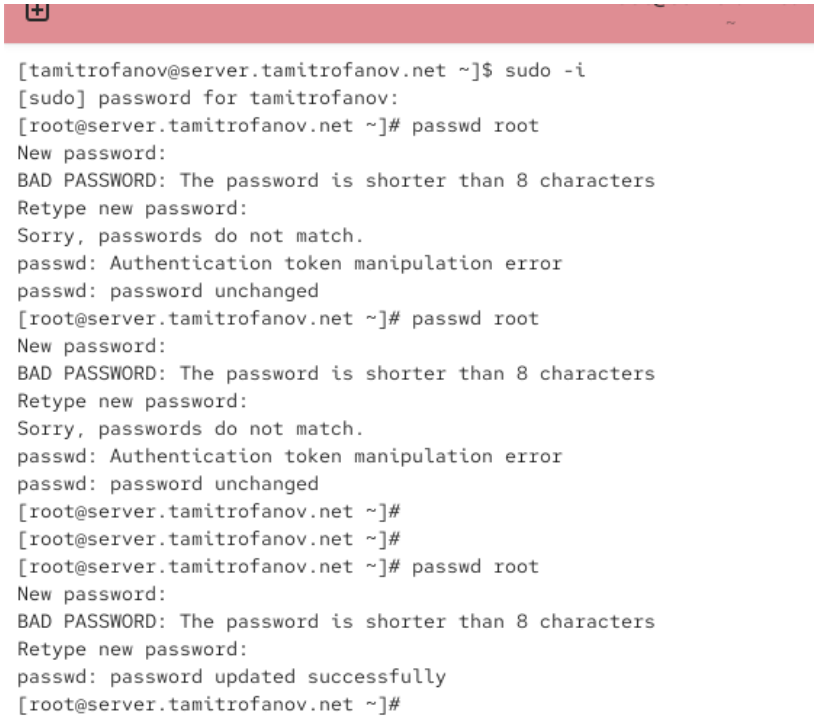

Рисунок 3.1: смена настройки

На сервере в дополнительном терминале запустите мониторинг системных событий (рис. 3.2).

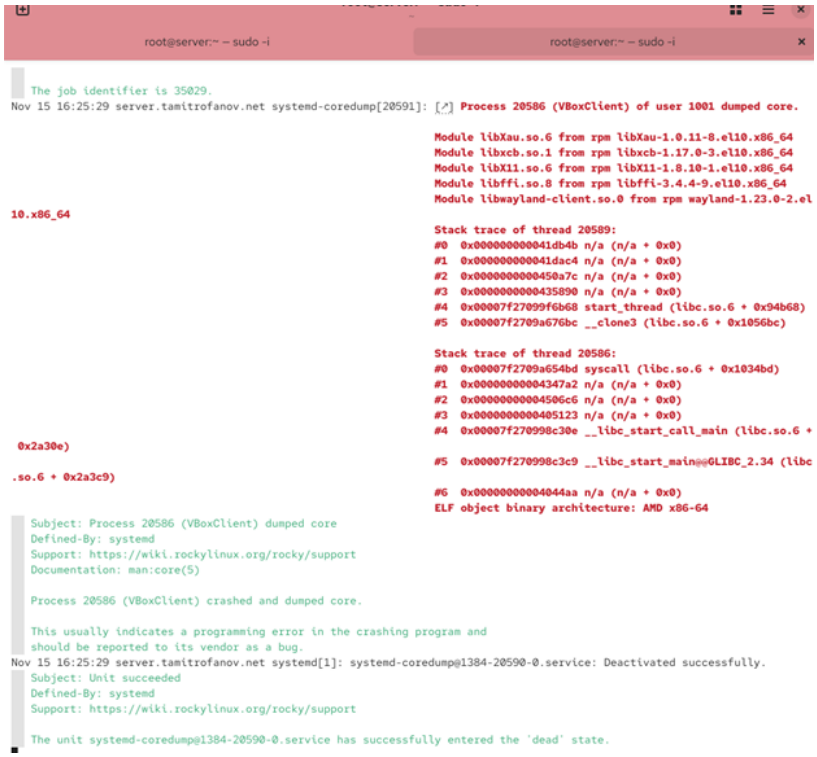

Рисунок 3.2: мониторинг

С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя root (рис. 3.3).

при поптке подключения создается отпечаток, но система запрещает войти под рутов в запись рут на сервере

Рисунок 3.3: попытка входа под рутом

На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd для редактирования и запретите вход на сервер пользователю root (рис. 3.4).

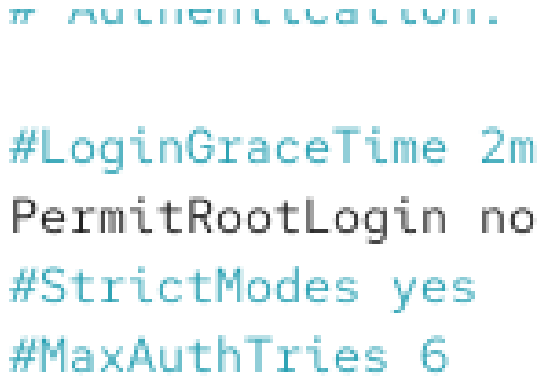

Рисунок 3.4: изменение файла

После сохранения изменений в файле конфигурации перезапустите sshd (рис. 3.5).

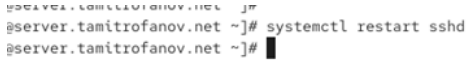

Рисунок 3.5: перезапуск службы

Повторите попытку получения доступа с клиента к серверу посредством SSHсоединения через пользователя root (рис. 3.6).

Рисунок 3.6: повторная попытка зайти под рутом и запрет сервера на это действие

П. С клиента попытайтесь получить доступ к серверу посредством SSHсоединения через пользователя user (вместо user укажите вашего пользователя) (рис. 3.7).

система нас пускает

Рисунок 3.7: подключение к пользователю на сервере

На сервере откройте файл /etc/ssh/sshd_config конфигурации sshd на редактирование и добавьте строку (рис. 3.8).

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
AllowUsers vagrant
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Рисунок 3.8: изменение конфига

После сохранения изменений в файле конфигурации перезапустите sshd Повторите попытку получения доступа с клиента к серверу посредством (рис. 3.9).

так как мы запретили иным польщователям кроме вгранта подключение нас перестаёт пускать

```
[tamitrofanov@server.tamitrofanov.net ~]$
[tamitrofanov@server.tamitrofanov.net ~]$
[tamitrofanov@server.tamitrofanov.net ~]$ ssh tamitrofnov@server.tamitrofanov.net
tamitrofnov@server.tamitrofanov.net's password:
Permission denied, please try again.
tamitrofnov@server.tamitrofanov.net's password:
Permission denied, please try again.
tamitrofnov@server.tamitrofanov.net's password:
tamitrofnov@server.tamitrofanov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[tamitrofanov@server.tamitrofanov.net ~]$
```

Рисунок 3.9: попытка подключения к серверу

В файле /etc/ssh/sshd_config конфигурации sshd внесите следующее изменение (рис. 3.10).

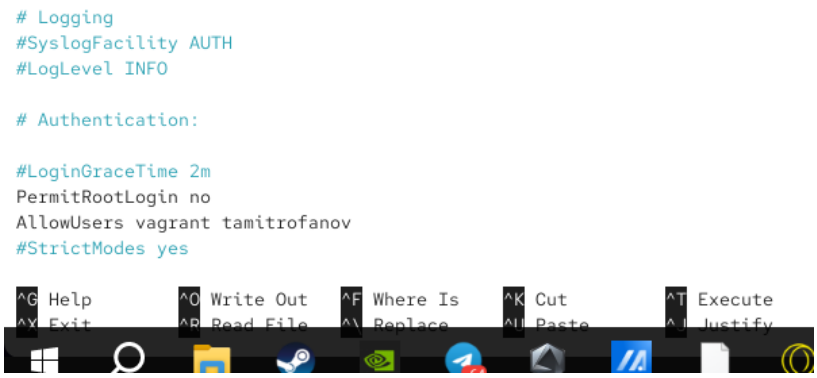

Рисунок 3.10: изменение файла

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 (рис. 3.11).

так как мы прописали разрешение нашему пользователю на подключение нас пускает

Рисунок 3.11: успешное подклбчение к серверу

На сервере в файле конфигурации sshd /etc/ssh/sshd_config найдите строку Port и ниже этой строки добавьте (рис. 3.12).

```
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22

Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
```

Рисунок 3.12: измениям кофиг

После сохранения изменений в файле конфигурации перезапустите sshd (рис. 3.13).

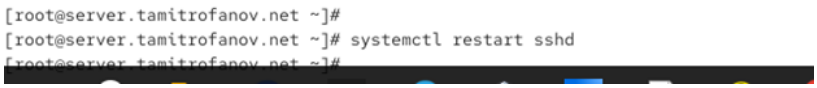

Рисунок 3.13: перезапуск служб

Посмотрите расширенный статус работы sshd (рис. 3.14).

проблема в том что нам надо шифрованое подключение на порту для безопасного подключения, но мы не указывали tcp на указанный порт

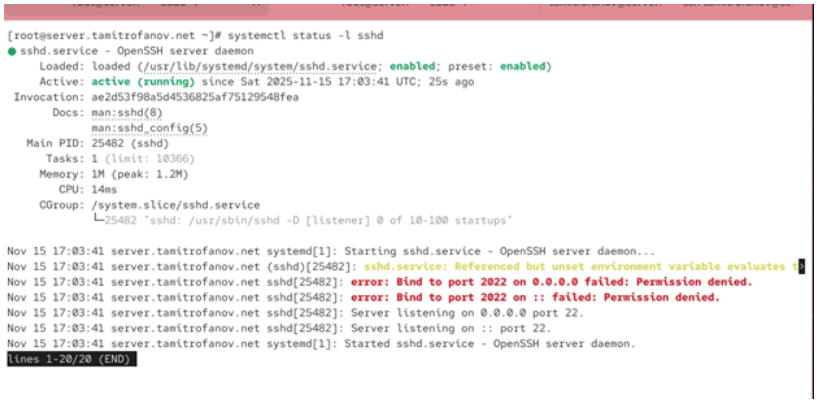

Рисунок 3.14: проверяяем наличие ошибки

Исправьте на сервере метки SELinux к порту 2022. В настройках межсетевого экрана откройте порт 2022 протокола TCP. Вновь перезапустите sshd и посмотрите

расширенный статус его работы. Статус должен показать, что процесс sshd теперь прослушивает два порта. (рис. 3.15).

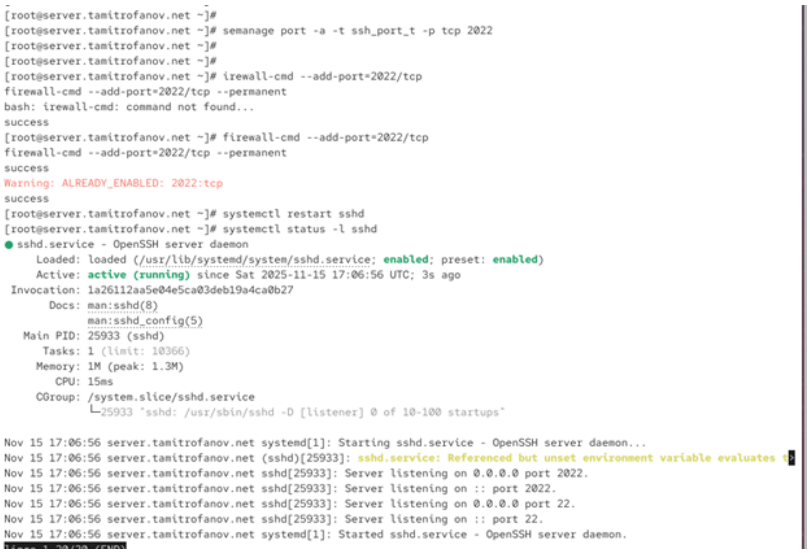

Рисунок 3.15: настрайка Postfix

С клиента попытайтесь получить доступ к серверу посредством SSH-соединения через пользователя user (вместо user укажите вашего пользователя). После открытия оболочки пользователя введите sudo -i для получения доступа root. Отлогиньтесь от root и вашего пользователя на сервере, введя дважды logout или используя дважды комбинацию клавиш Ctrl + d . (рис. 3.16).

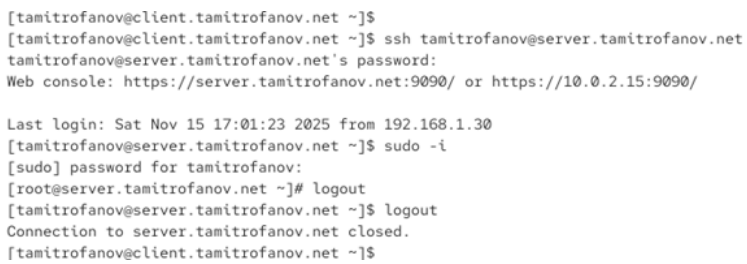

Рисунок 3.16: обычное подключение к серверу

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

Отлогиньтесь от root и вашего пользователя на сервере, введя дважды logout или используя дважды комбинацию клавиш Ctrl + d . (рис. 3.17).

```
[tamitrofanov@client.tamitrofanov.net ~]$
[tamitrofanov@client.tamitrofanov.net ~]$ ssh -p2022 tamitrofanov@server.tamitrofanov.net
tamitrofanov@server.tamitrofanov.net's password:
Web console: https://server.tamitrofanov.net:9090/ or https://10.0.2.15:9090/

Last login: Sat Nov 15 17:07:54 2025 from 192.168.1.30
[tamitrofanov@server.tamitrofanov.net ~]$ root
bash: root: command not found...
Install package 'root' to provide command 'root'? [N/y] ^C
[tamitrofanov@server.tamitrofanov.net ~]$ sudo -i
[sudo] password for tamitrofanov:
[root@server.tamitrofanov.net ~]# logout
[tamitrofanov@server.tamitrofanov.net ~]$ logout
Connection to server.tamitrofanov.net closed.
[tamitrofanov@client.tamitrofanov.net ~]$
```

Рисунок 3.17: поключение через новый порт

На сервере в конфигурационном файле /etc/ssh/sshd_config задайте параметр, разрешающий аутентификацию по ключу (рис. 3.18).

```
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized
# but this is overridden so installations will
AuthorizedKeysFile      .ssh/authorized_keys
```

Рисунок 3.18: меняем кофигурационный файл

После сохранения изменений в файле конфигурации перезапустите sshd (рис. 3.19).

```
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]# systemctl restart sshd
[root@server.tamitrofanov.net ~]#
[root@server.tamitrofanov.net ~]#
```

Рисунок 3.19: перезапуск служб

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. Скопируйте открытый ключ на сервер, введя на клиенте (вместо user укажите вашего пользователя) 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. Отлогиньтесь с сервера, используя комбинацию клавиш Ctrl + d .(рис. 3.20).

Рисунок 3.20: создание ключа и копирование ключа на сервер

На клиенте посмотрите, запущены ли какие-то службы с протоколом TCP (рис. 3.21).

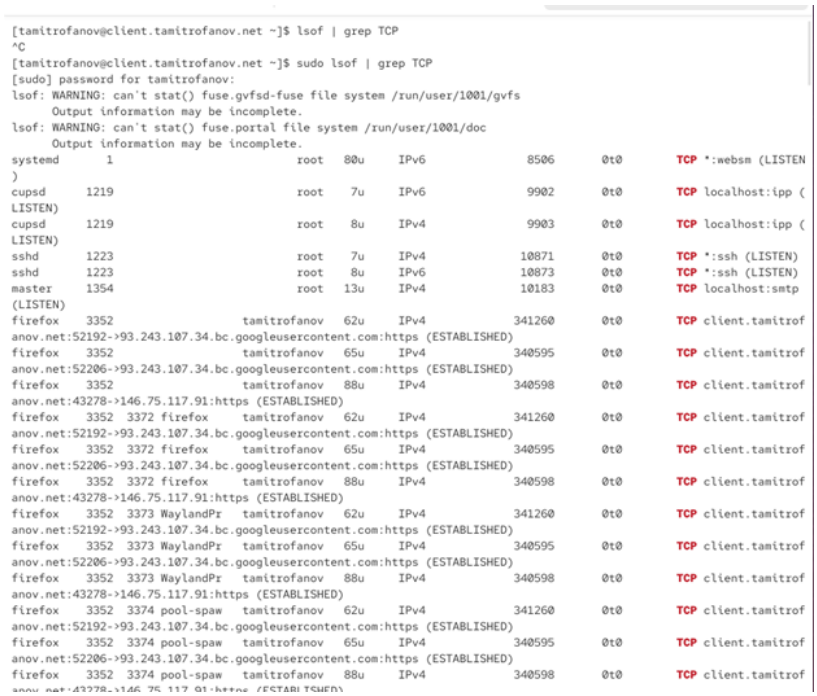

Рисунок 3.21: проверием запущенные службы

Перенаправьте порт 80 на server.user.net на порт 8080 на локальной машине (вместо user используйте ваш логин) (рис. 3.22).

Рисунок 3.22: перенаправление

Вновь на клиенте посмотрите, запущены ли какие-то службы с протоколом TCP (рис. 3.23).

Теперь у нас всёё ыремя шифрованный пртокол на порту 80

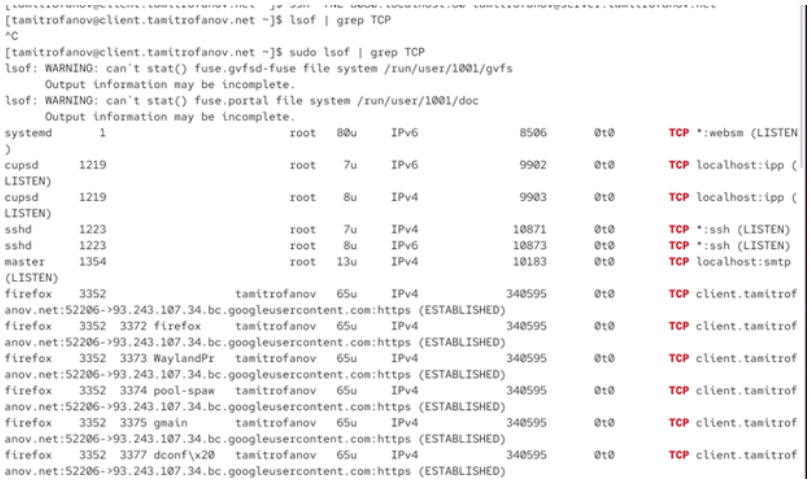

Рисунок 3.23: проверием запущенные службы

На клиенте запустите браузер и в адресной строке введите localhost:8080. Убедитесь, что отобразится страница с приветствием «Welcome to the server.user.net server». (рис. 3.24).

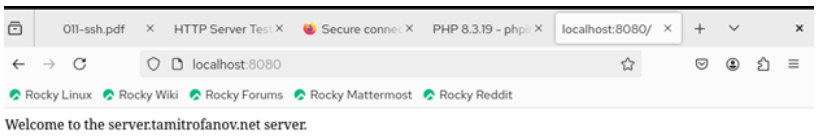

Рисунок 3.24: проверка работы перенаправления

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
4. Посмотрите с клиента почту на сервере: ssh user@server.user.net MAIL=~/Maildir/ mail (рис. 3.25).

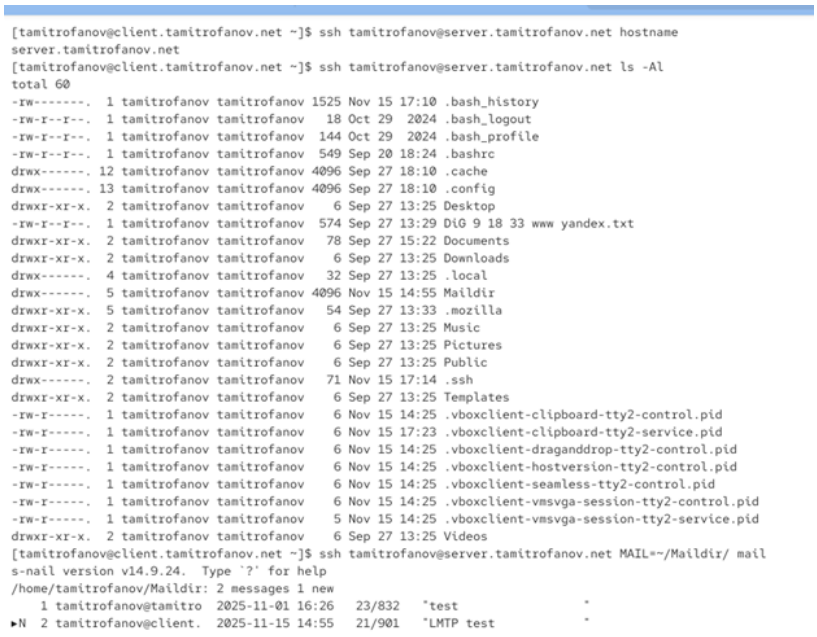

Рисунок 3.25: проверка домтупа к серверу без пароля

На сервере в конфигурационном файле /etc/ssh/sshd_config разрешите отображать на локальном клиентском компьютере графические интерфейсы X11(рис. 3.26).

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
```

Рисунок 3.26: изменения конф файла

Попробуйте с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox (вместо user используйте ваш логин) (рис. 3.27).

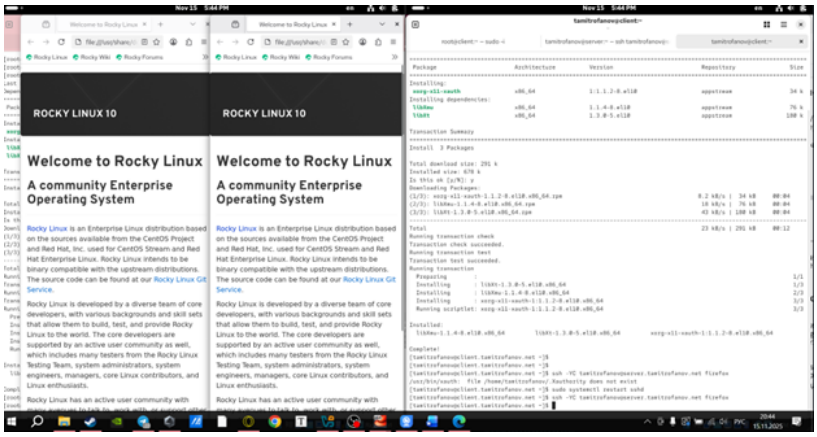

Рисунок 3.27: ткрываем удалённо браузер на сервере

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 В каталоге /vagrant/provision/server создайте исполняемый файл ssh.sh (рис. 3.28).

```
[root@server.tamitrofanov.net ~]# cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/ssh/etc/ssh
cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
[root@server.tamitrofanov.net server]# cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
[root@server.tamitrofanov.net server]#
```

Рисунок 3.28: сохранение файлов и их создание

ДОткрыв его на редактирование, пропишите в нём следующий скрипт (рис. 3.29).

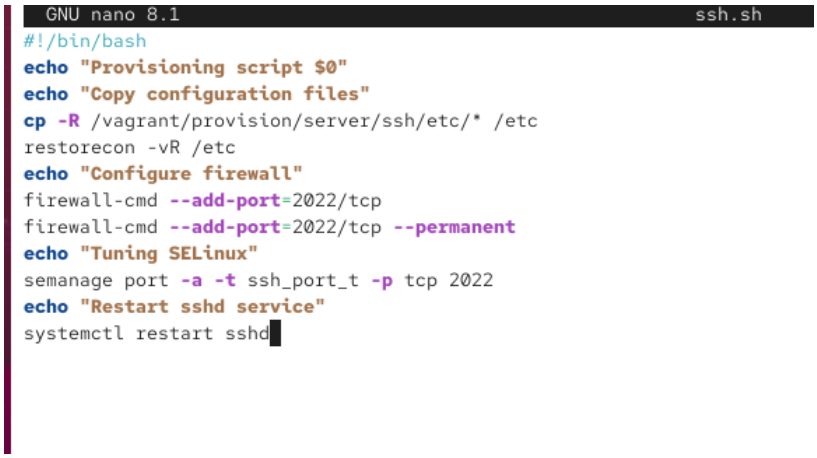

Рисунок 3.29: новый скрипт

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера (рис. 3.30).

Рисунок 3.30: дополнение скрипта на основной системе

4 Выводы

Сегодня я приобрёл практические навыки по настройке удалённого доступа к серверу с помощью SSH.

Список литературы