Лабораторная работа №11 (Настройка безопасного удалённого доступа по протоколу SS)

Шубина София Антоновна

31 октября 2025

Российский университет дружбы народов

Цель работы

Приобрести практические навыки 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

Выполнение лабораторной работы

Запрет удалённого доступа по SSH для пользователя root

На сервере зададим пароль для пользователя root, если этого не было сделано ранее, я обновила пароль:

```
[root@server.sashubina.net ~]# passwd root
New password:
Retype new password:
passwd: password updated successfully
[root@server.sashubina.net ~]#
```

Рис. 1: Установка пароля

На сервере в дополнительном терминале запустим мониторинг системных событий:

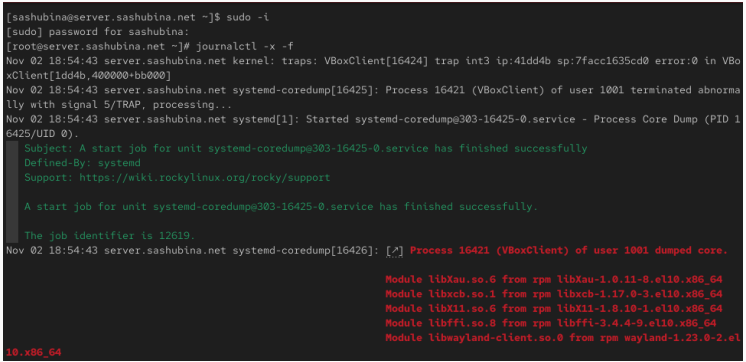

Рис. 2: Мониторинг системных событий

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя root: `ssh root@server.sashubina.net`

```
[sashubina@client.sashubina.net ~]$ ssh root@server.sashubina.net
ssh: connect to host server.sashubina.net port 22: Connection refused
[sashubina@client.sashubina.net ~]$
```

Рис. 3: Получение доступа к серверу посредством SSH-соединения

На сервере откроем файл /etc/ssh/sshd_config конфигурации sshd для редактирования и запретим вход на сервер пользователю root, установив: `PermitRootLogin no`

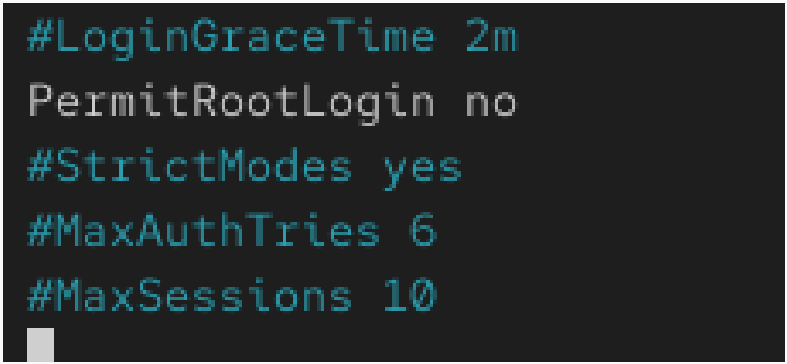

Рис. 4: Редактирование файла

После сохранения изменений в файле конфигурации перезапустим sshd: `systemctl restart sshd`

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

Рис. 5: Перезапуск sshd

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя root: `ssh root@server.sashubina.net`

```
[sashubina@client.sashubina.net ~]$ ssh root@server.sashubina.net
ssh: connect to host server.sashubina.net port 22: Connection refused
[sashubina@client.sashubina.net ~]$
```

Рис. 6: Получение доступа к серверу посредством SSH-соединения

Ограничение списка пользователей для удалённого доступа по SSH

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя sashubina: `ssh sashubina@server.sashubina.net`

```
[root@client.sashubina.net ~]# ssh sashubina@server.sashubina.net
kex_exchange_identification: read: Connection reset by peer
Connection reset by 192.168.1.20 port 22
```

Рис. 7: Получение доступа к серверу посредством SSH-соединения

На сервере откроем файл /etc/ssh/sshd_config конфигурации sshd на редактирование и добавим строку `AllowUsers vagrant`

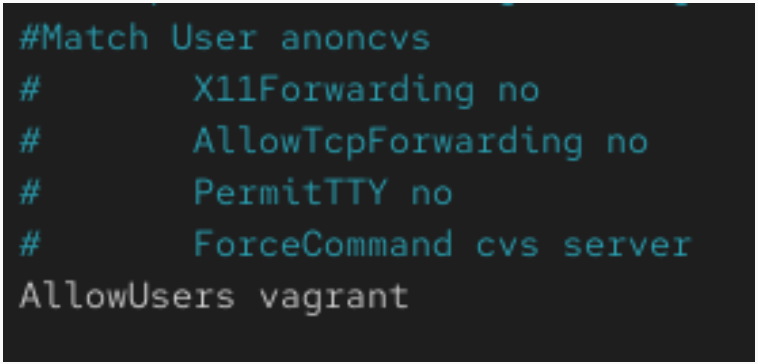

Рис. 8: Редактирование файла

После сохранения изменений в файле конфигурации перезапустим sshd: `systemctl restart sshd`

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

Рис. 9: Перезапуск sshd

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя sashubina: `ssh sashubina@server.sashubina.net`

```
[sashubina@server.sashubina.net ~]$ ssh sashubina@server.sashub
ina.net
ssh: connect to host server.sashubina.net port 22: No route to
host
[sashubina@server.sashubina.net ~]$
```

Рис. 10: Получение доступа к серверу посредством SSH-соединения

В файле /etc/ssh/sshd_config конфигурации sshd внесем следующее изменение: `AllowUsers vagrant sashubina`

```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server
AllowUsers vagrant sashubina
```

Рис. 11: Редактирование файла

После сохранения изменений в файле конфигурации перезапустим sshd и вновь попытаемся получить доступ с клиента к серверу посредством SSH-соединения через пользователя user.

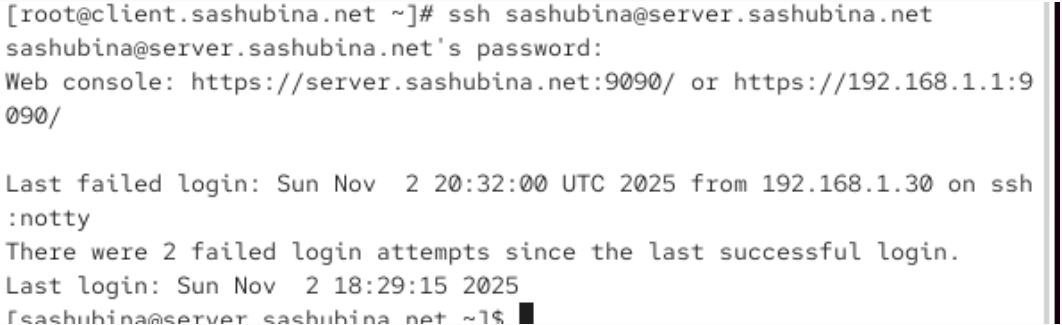

Рис. 12: Получение доступа к серверу посредством SSH-соединения

Настройка дополнительных портов для удалённого доступа по SSH

На сервере в файле конфигурации sshd /etc/ssh/sshd_config найдем строку Port и ниже этой строки добавим:

```
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
```

Рис. 13: Редактирование файла

После сохранения изменений в файле конфигурации перезапустим sshd: `systemctl restart sshd`

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

Рис. 14: Перезапуск

Посмотрим расширенный статус работы sshd: `systemctl status -l sshd`

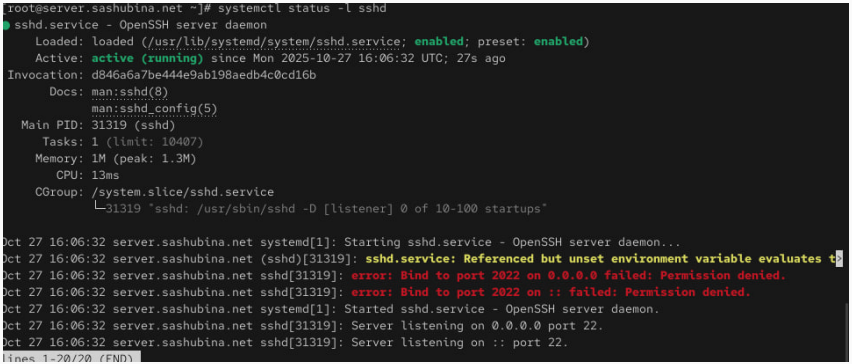

Рис. 15: Расширенный статус работы sshd

Система сообщает нам об отказе в работе sshd через порт 2022.Дополнительно посмотрим сообщения в терминале с мониторингом системных событий.

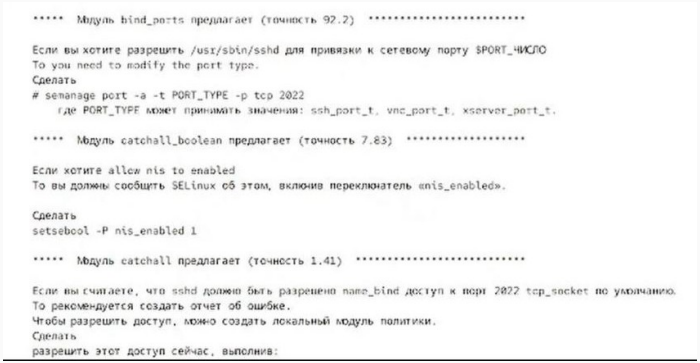

Рис. 16: Мониторинг системных событий

Исправим на сервере метки SELinux к порту 2022: `semanage port -a -t ssh_port_t -p tcp 2022`

```
[root@server.sashubina.net ~]# semanage port -a -t ssh_port_t -p tcp 2022
Port tcp/2022 already defined, modifying instead
[root@server.sashubina.net ~]#
```

Рис. 17: исправление меток

В настройках межсетевого экрана откроем порт 2022 протокола TCP:

```
[root@server.sashubina.net ~]# firewall-cmd --add-port=2022/tcp
Warning: ALREADY_ENABLED: '2022:tcp' already in 'public'
success
[root@server.sashubina.net ~]# firewall-cmd --add-port=2022/tcp --permanent
Warning: ALREADY_ENABLED: 2022:tcp
success
[root@server.sashubina.net ~]#
```

Рис. 18: Настройка межсетевого экрана

Вновь перезапустим sshd и посмотрим расширенный статус его работы. Статус должен показать, что процесс sshd теперь прослушивает два порта.

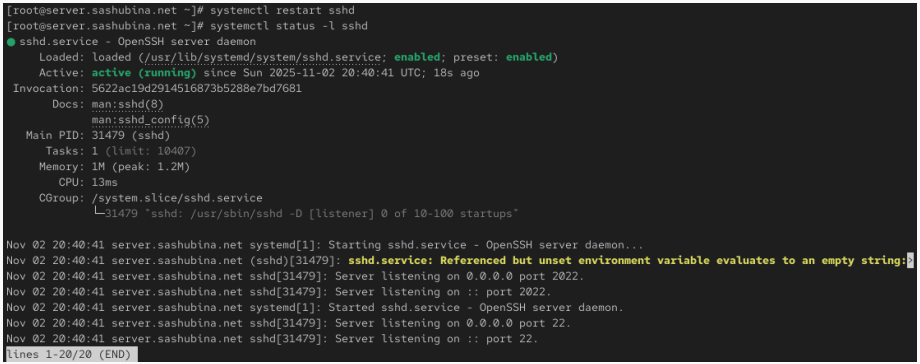

Рис. 19: Расширенный статус работы sshd

С клиента попытаемся получить доступ к серверу посредством SSH-соединения через пользователя sashubina: `ssh sashubina@server.sashubina.net`

```
[sashubina@server.sashubina.net ~]$ ssh sashubina@server.sashubina.net
Web console: https://server.sashubina.net:9090/ or https://192.168.1.1:9
090/

Last login: Sun Nov  2 20:33:38 2025 from 192.168.1.30
[sashubina@server.sashubina.net ~]$ ssh sashubina@server.sashubina.net
Web console: https://server.sashubina.net:9090/ or https://192.168.1.1:9
090/

Last login: Sun Nov  2 20:34:41 2025 from 192.168.1.20
[sashubina@server.sashubina.net ~]$
```

Рис. 20: Получение доступа к серверу посредством SSH-соединения

После открытия оболочки пользователя введем `sudo -i` для получения доступа root.Отлогинемся от root и нашего пользователя на сервере,введя дважды logout

```
[sashubina@server.sashubina.net ~]$ sudo -i
[sudo] password for sashubina:
Sorry, try again.
[sudo] password for sashubina:
[root@server.sashubina.net ~]#
logout
[sashubina@server.sashubina.net ~]$
logout
Connection to server.sashubina.net closed.
[sashubina@server.sashubina.net ~]$
```

Рис. 21: logout

Повторим попытку получения доступа с клиента к серверу посредством SSH-соединения через пользователя user, указав порт 2022: `ssh sashubina@server.sashubina.net`

```
[sashubina@server.sashubina.net ~]$ ssh -p2022 sashubina@server.sashubin
a.net
Web console: https://server.sashubina.net:9090/ or https://192.168.1.1:9
090/

Last login: Sun Nov  2 20:45:04 2025 from 192.168.1.20
[sashubina@server.sashubina.net ~]$
```

Рис. 22: Получение доступа к серверу посредством SSH-соединения через порт 2022

После открытия оболочки пользователя введем `sudo -i` для получения доступа root.Отлогинемся от root и нашего пользователя на сервере,введя дважды logout

```
[sashubina@server.sashubina.net ~]$ sudo -i
[sudo] password for sashubina:
[root@server.sashubina.net ~]#
logout
[sashubina@server.sashubina.net ~]$
logout
Connection to server.sashubina.net closed.
[sashubina@server.sashubina.net ~]$
```

Рис. 23: logout

Настройка удалённого доступа по SSH по ключу

На сервере в конфигурационном файле /etc/ssh/sshd_config зададим параметр, разрешающий аутентификацию по ключу: `PubkeyAuthentication yes`

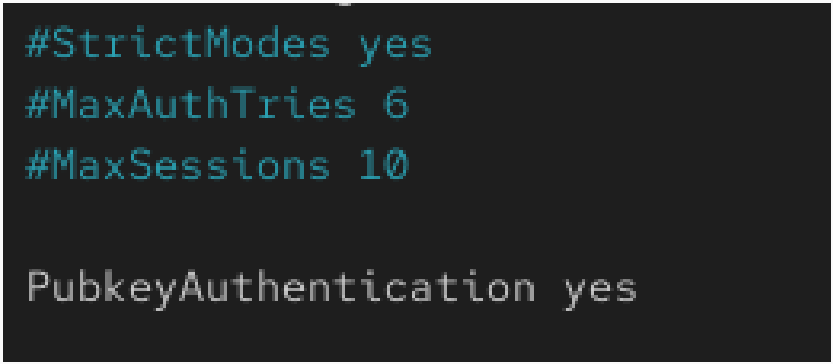

Рис. 24: Редактирование файла

После сохранения изменений в файле конфигурации перезапустим sshd.

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

Рис. 25: Перезапуск

На клиенте сформируем SSH-ключ, введя в терминале под пользователем sashubina: `ssh-keygen`

```
[sashubina@server.sashubina.net ~]$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/sashubina/.ssh/id_ed25519):
/home/sashubina/.ssh/id_ed25519 already exists.
Overwrite (y/n)? y
Enter passphrase for "/home/sashubina/.ssh/id_ed25519" (empty for no pas
sphrase):
Enter same passphrase again:
Your identification has been saved in /home/sashubina/.ssh/id_ed25519
Your public key has been saved in /home/sashubina/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:ryHx6gyF8XXUWeuloLU/wfadbkprmJ3oVNsaHhy4B7U sashubina@server.sash
ubina.net
The key's randomart image is:
+--[ED25519 256]--+
|                 .  |
|            . o . |
|           . =.. .|
|          . oo=.o |
|     . . S oo.E*  |
|      + + o  =o+oo|
|     . + o .o=B+oo|
|      o o o.+++*o |
|     .o+ . ...=o. |
+----[SHA256]-----+
[sashubina@server.sashubina.net ~]$
```

Рис. 26: Формирование ключа ssh

Скопируем открытый ключ на сервер, введя на клиенте: `ssh-copy-id sashubina@server.sashubina.net`

```
[sashubina@server.sashubina.net ~]$ ssh-copy-id sashubina@server.sashubi
na.net
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/sas
hubina/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to
 filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you ar
e prompted now it is to install the new keys
sashubina@server.sashubina.net's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'sashubina@server.sashubina
.net'"
and check to make sure that only the key(s) you wanted were added.

[sashubina@server.sashubina.net ~]$
```

Рис. 27: Копирование ключа

Попробуем получить доступ с клиента к серверу посредством SSH-соединения: `ssh sashubina@server.sashubina.net`

```
[sashubina@server.sashubina.net ~]$ ssh sashubina@server.sashubina.net
Web console: https://server.sashubina.net:9090/ or https://192.168.1.1:9
090/

Last login: Sun Nov  2 20:47:13 2025 from 192.168.1.20
[sashubina@server.sashubina.net ~]$
```

Рис. 28: получение доступа к серверу

Теперь мы прошли аутентификацию без ввода пароля для учётной записи удалённого пользователя. Отлогинимся от сервера

```
[sashubina@server.sashubina.net ~]$
logout
Connection to server.sashubina.net closed.
[sashubina@server.sashubina.net ~]$
logout
Connection to server.sashubina.net closed.
[root@client.sashubina.net ~]#
```

Рис. 29: logout

Организация туннелей SSH, перенаправление TCP-портов

На клиенте посмотрим, запущены ли какие-то службы с протоколом TCP: `lsof | grep TCP`

```
[root@client.sashubina.net ~]# lsof | grep TCP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
systemd       1                            root   80u     IPv6               8111       0t0       TCP *:websm (LISTEN)
cupsd      1230                            root    7u     IPv6              10062       0t0       TCP localhost:ipp (LISTEN)
cupsd      1230                            root    8u     IPv4              10063       0t0       TCP localhost:ipp (LISTEN)
sshd       1235                            root    7u     IPv4              10784       0t0       TCP *:ssh (LISTEN)
sshd       1235                            root    8u     IPv6              10787       0t0       TCP *:ssh (LISTEN)
master     1366                            root   13u     IPv4              11142       0t0       TCP localhost:smtp (LISTEN)
firefox   12493                         sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12521 firefox         sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12522 WaylandPr       sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12523 pool-spaw       sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12524 gmain           sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12526 dconf\x20       sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12527 gdbus           sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12528 gdbus.dis       sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12530 IPC\x20I/       sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12536 Timer           sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
firefox   12493 12537 Netlink         sashubina   60u     IPv4             251175       0t0       TCP client.sashubina.net:49134->93.243.107.34.bc.googleuser
content.com:https (ESTABLISHED)
```

Рис. 30: просмотр какие службы запущены

Перенаправим порт 80 на server.sashubina.net на порт 8082, тк портт 8080 занят `ssh -fNL 8082:localhost:80 sashubina@server.sashubina.net`

```
[root@client.sashubina.net ~]# ssh -fNL 0.0.0.0:8082:server.sashubina.net:80 sashubina@server.sashubina.net
sashubina@server.sashubina.net's password:
```

Рис. 31: перенаправим порт 80 на 8082

Вновь на клиенте посмотрим, запущены ли какие-то службы с протоколом TCP: Я использовала именно эту команду, а не `lsof | grep TCP`, потому что там не были отображены изменения `lsof -i:8082`

```
[root@client.sashubina.net ~]# lsof -i:8082
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
ssh     35462 root    4u  IPv4 438316      0t0  TCP *:us-cli (LISTEN)
```

Рис. 32: Перенаправление на порт 8082

На клиенте запустим браузер и в адресной строке введем localhost:8082. Убедимся, что отобразится страница с приветствием «Welcome to the server.sashubina.net server».

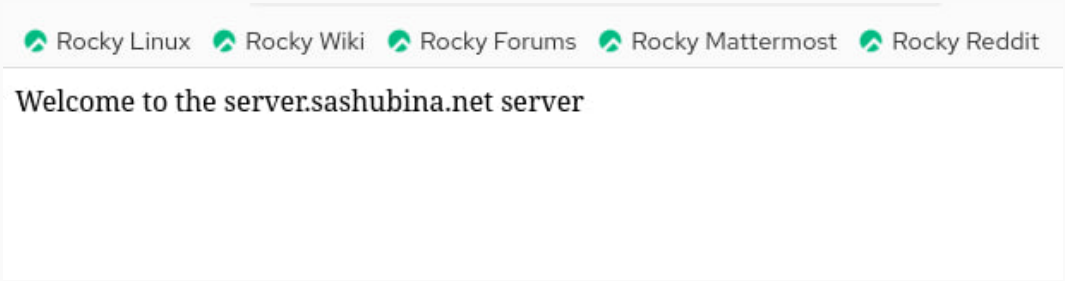

Рис. 33: localhost:8082

Запуск консольных приложений через SSH

На клиенте откроем терминал под пользователем sashubina. Посмотрим с клиента имя узла сервера: `ssh sashubina@server.sashubina.net hostname`

```
[sashubina@client.sashubina.net ~]$ ssh sashubina@server.sashubina.net h
ostname
sashubina@server.sashubina.net's password:
server.sashubina.net
[sashubina@client.sashubina.net ~]$
```

Рис. 34: hostname

Посмотрим с клиента список файлов на сервере: `ssh sashubina@server.sashubina.net ls -Al`

```
[sashubina@client.sashubina.net ~]$ ssh sashubina@server.sashubina.net ls -Al
sashubina@server.sashubina.net's password:
total 56
-rw-------.  1 sashubina sashubina 3873 Nov  2 20:56 .bash_history
-rw-r--r--.  1 sashubina sashubina   18 Oct 29  2024 .bash_logout
-rw-r--r--.  1 sashubina sashubina  144 Oct 29  2024 .bash_profile
-rw-r--r--.  1 sashubina sashubina  549 Sep 19 13:19 .bashrc
drwx------. 11 sashubina sashubina 4096 Sep 20 14:32 .cache
drwx------. 10 sashubina sashubina 4096 Sep 20 15:36 .config
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Desktop
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Documents
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Downloads
drwx------.  4 sashubina sashubina   32 Sep 19 18:03 .local
drwx------.  5 sashubina sashubina 4096 Oct 20 22:01 Maildir
drwxr-xr-x.  5 sashubina sashubina   54 Sep 19 18:04 .mozilla
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Music
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Pictures
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Public
drwx------.  2 sashubina sashubina   88 Nov  2 20:53 .ssh
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Templates
-rw-r-----.  1 sashubina sashubina    6 Nov  2 18:29 .vboxclient-clipboard-tty2-control.pid
-rw-r-----.  1 sashubina sashubina    7 Nov  2 21:56 .vboxclient-clipboard-tty2-service.pid
-rw-r-----.  1 sashubina sashubina    6 Nov  2 18:29 .vboxclient-draganddrop-tty2-control.pid
-rw-r-----.  1 sashubina sashubina    6 Nov  2 18:29 .vboxclient-hostversion-tty2-control.pid
-rw-r-----.  1 sashubina sashubina    6 Nov  2 18:29 .vboxclient-seamless-tty2-control.pid
-rw-r-----.  1 sashubina sashubina    6 Nov  2 18:29 .vboxclient-vmsvga-session-tty2-control.pid
-rw-r-----.  1 sashubina sashubina    6 Nov  2 18:29 .vboxclient-vmsvga-session-tty2-service.pid
drwxr-xr-x.  2 sashubina sashubina    6 Sep 19 18:03 Videos
[sashubina@client.sashubina.net ~]$
```

Рис. 35: список файлов на сервере

Посмотрите с клиента почту на сервере: ssh sashubina@server.sashubina.net MAIL=~/Maildir/ mail

```
[sashubina@client.sashubina.net ~]$ ssh sashubina@server.sashubina.net M
AIL=~/Maildir/ mail
sashubina@server.sashubina.net's password:
s-nail version v14.9.24.  Type `?' for help
/home/sashubina/Maildir: 4 messages 3 unread
    1 Sofia                  2025-10-12 15:23   18/630   "1
      "
▸U  2 Sofia                  2025-10-12 17:16   18/630   "3
      "
 U  3 Super User             2025-10-20 16:58   18/605   "LMTP test
      "
 U  4 Super User             2025-10-20 22:01   18/605   "LMTP test
      "
```

Рис. 36: просмотр с клианта почту на сервере

Запуск графических приложений через SSH (X11Forwarding)

На сервере в конфигурационном файле /etc/ssh/sshd_config разрешим отображать на локальном клиентском компьютере графические интерфейсы X11: `X11Forwarding yes`

```
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
X11UseLocalhost no
```

Рис. 37: Редактирование файла

После сохранения изменения в конфигурационном файле перезапустим sshd.

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

Рис. 38: Перезапуск sshd

Для начала необходимо загрузить xorg на сервер и клиент, только после этого у меня получилось запустить firefox

```
 xorg-x11-xauth      x86_64     1:1.1.2-8.el10        appstream      34 k
Installing dependencies:
 libXmu              x86_64     1.1.4-8.el10          appstream      76 k
 libXt               x86_64     1.3.0-5.el10          appstream     180 k

Transaction Summary
================================================================================
Install  3 Packages

Total download size: 291 k
Installed size: 678 k
Downloading Packages:
(1/3): xorg-x11-xauth-1.1.2-8.el10.x86_  11 kB/s |  34 kB     00:03
(2/3): libXmu-1.1.4-8.el10.x86_64.rpm    24 kB/s |  76 kB     00:03
(3/3): libXt-1.3.0-5.el10.x86_64.rpm     57 kB/s | 180 kB     00:03
--------------------------------------------------------------------------------
Total                                    44 kB/s | 291 kB     00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : libXt-1.3.0-5.el10.x86_64                              1/3
  Installing       : libXmu-1.1.4-8.el10.x86_64                             2/3
  Installing       : xorg-x11-xauth-1:1.1.2-8.el10.x86_64                   3/3
  Running scriptlet: xorg-x11-xauth-1:1.1.2-8.el10.x86_64                   3/3

Installed:
  libXmu-1.1.4-8.el10.x86_64              libXt-1.3.0-5.el10.x86_64
  xorg-x11-xauth-1:1.1.2-8.el10.x86_64
```

Рис. 39: установка

Попробуем с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox: `ssh -YC sashubina@server.sashubina.net firefox`

```
[sashubina@client.sashubina.net ~]$ ssh -YC sashubina@server.sashubina.n
et firefox
sashubina@server.sashubina.net's password:
[sashubina@client.sashubina.net ~]$
```

Рис. 40: Запуск графических приложений через SSH

Результат запуска графического приложения через SSH

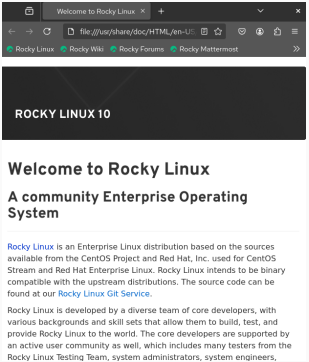

Рис. 41: Результат запуска графического приложения через SSH

Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог ssh, в который поместим в соответствующие подкаталоги конфигурационный файл sshd_config:

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

Рис. 42: Создание файла

Открыв его на редактирование, пропишем в нём следующий скрипт:

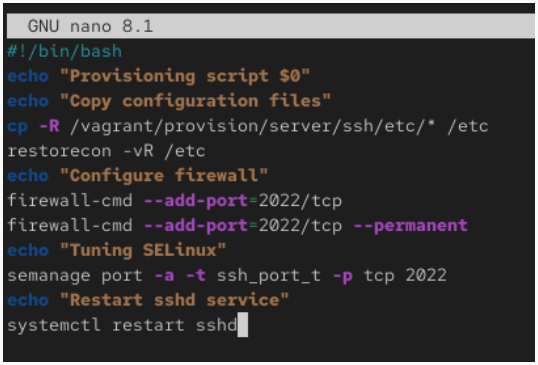

Рис. 43: Редактирование файла

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"
```

Рис. 44: Редактирование файла

Выводы

В процессе выполнения данной лабораторной работы я приобрела практические навыки по настройке удалённого доступа к серверу с помощью SSH.