# Лабораторная работа №11

## Настройка безопасного удалённого доступа по протоколу SSH

Беличева Дарья Михайловна

Российский университет дружбы народов, Москва, Россия

# 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.

# Задание

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. Соответствующим образом внести изменения в Vagrantfile.

# Выполнение лабораторной работы

# Запрет удалённого доступа по SSH для пользователя root

```
[dmbelicheva@server.dmbelicheva.net ~]$ sudo -i
[sudo] password for dmbelicheva:
[root@server.dmbelicheva.net ~]# journalctl -x -f
Dec 16 12:33:07 server.dmbelicheva.net systemd[1]: systemd-hostnamed.service: Deactivated successfully.
    Subject: Unit succeeded
    Defined-By: systemd
    Support: https://access.redhat.com/support

    The unit systemd-hostnamed.service has successfully entered the 'dead' state.
Dec 16 12:33:56 server.dmbelicheva.net systemd[5826]: Started Application launched by gnome-shell.
    Subject: A start job for unit UNIT has finished successfully
    Defined-By: systemd
    Support: https://access.redhat.com/support

    A start job for unit UNIT has finished successfully.

    The job identifier is 520.
Dec 16 12:33:56 server.dmbelicheva.net systemd[5826]: Started VTE child process 6881 launched by gnome-terminal-server process
    Subject: A start job for unit UNIT has finished successfully
    Defined-By: systemd
    Support: https://access.redhat.com/support

    A start job for unit UNIT has finished successfully.
```

**Рис. 1:** Мониторинг системных событий

# Запрет удалённого доступа по SSH для пользователя root

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

```
[root@client.dmbelicheva.net ~]# ssh root@server.dmbelicheva.net
The authenticity of host 'server.dmbelicheva.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:qAcEVloHrUBfplcMfDqV6X3jQFiMqxk1/IUBYBydgf4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.dmbelicheva.net' (ED25519) to the list of known hosts.
root@server.dmbelicheva.net's password:
Permission denied, please try again.
root@server.dmbelicheva.net's password:
Permission denied, please try again.
root@server.dmbelicheva.net's password:
root@server.dmbelicheva.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.dmbelicheva.net ~]# ssh root@server.dmbelicheva.net
```

**Рис. 2:** Получение доступа к серверу посредством SSH-соединения

# Запрет удалённого доступа по SSH для пользователя root

```
  GNU nano 5.6.1

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

**Рис. 3:** Редактирование файла

# Запрет удалённого доступа по SSH для пользователя root

```
[root@client.dmbelicheva.net ~]# ssh root@server.dmbelicheva.net
root@server.dmbelicheva.net's password:
Permission denied, please try again.
root@server.dmbelicheva.net's password:
Permission denied, please try again.
root@server.dmbelicheva.net's password:
root@server.dmbelicheva.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.dmbelicheva.net ~]# ^C
```

**Рис. 4:** Получение доступа к серверу посредством SSH-соединения

# Ограничение списка пользователей для удалённого доступа по SSH

```
[dmbelicheva@client.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net
The authenticity of host 'server.dmbelicheva.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:qAcEVloHrUBfplcMfDqV6X3jQFiMqxk1/IUBYBydgf4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.dmbelicheva.net' (ED25519) to the list of known hosts.
dmbelicheva@server.dmbelicheva.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec 16 12:21:52 2023
[dmbelicheva@server.dmbelicheva.net ~]$
```

**Рис. 5:** Получение доступа к серверу посредством SSH-соединения

# Ограничение списка пользователей для удалённого доступа по SSH

```
  GNU nano 5.6.1
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

#PubkeyAuthentication yes
```

Рис. 6: Редактирование файла

# Ограничение списка пользователей для удалённого доступа по SSH

```
[dmbelicheva@server.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net
The authenticity of host 'server.dmbelicheva.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:qAcEVloHrUBfplcMfDqV6X3jQFiMqxk1/IUBYBydgf4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.dmbelicheva.net' (ED25519) to the list of known hosts.
dmbelicheva@server.dmbelicheva.net's password:
Permission denied, please try again.
dmbelicheva@server.dmbelicheva.net's password:
Permission denied, please try again.
dmbelicheva@server.dmbelicheva.net's password:
dmbelicheva@server.dmbelicheva.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[dmbelicheva@server.dmbelicheva.net ~]$
```

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

# Ограничение списка пользователей для удалённого доступа по SSH

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

Рис. 8: Редактирование файла

# Ограничение списка пользователей для удалённого доступа по SSH

```
[dmbelicheva@server.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net
dmbelicheva@server.dmbelicheva.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Dec 16 13:12:37 UTC 2023 from 192.168.1.1 on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Sat Dec 16 12:58:52 2023 from 192.168.1.30
[dmbelicheva@server.dmbelicheva.net ~]$
```

**Рис. 9:** Получение доступа к серверу посредством SSH-соединения

# Настройка дополнительных портов для удалённого доступа по SSH

```
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
Port 22
Port 2022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

**Рис. 10:** Редактирование файла

# Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.dmbelicheva.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Sat 2023-12-16 13:16:33 UTC; 13s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 7612 (sshd)
      Tasks: 1 (limit: 5724)
     Memory: 1.6M
        CPU: 33ms
     CGroup: /system.slice/sshd.service
             └─7612 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 16 13:16:33 server.dmbelicheva.net systemd[1]: Starting OpenSSH server daemon...
Dec 16 13:16:33 server.dmbelicheva.net sshd[7612]: main: sshd: ssh-rsa algorithm is disabled
Dec 16 13:16:33 server.dmbelicheva.net sshd[7612]: error: Bind to port 2022 on 0.0.0.0 failed: Permission denied.
Dec 16 13:16:33 server.dmbelicheva.net sshd[7612]: error: Bind to port 2022 on :: failed: Permission denied.
Dec 16 13:16:33 server.dmbelicheva.net sshd[7612]: Server listening on 0.0.0.0 port 22.
Dec 16 13:16:33 server.dmbelicheva.net sshd[7612]: Server listening on :: port 22.
Dec 16 13:16:33 server.dmbelicheva.net systemd[1]: Started OpenSSH server daemon.
[root@server.dmbelicheva.net ssh]#
```

**Рис. 11:** Расширенный статус работы sshd

# Настройка дополнительных портов для удалённого доступа по SSH

```
A start job for unit dbus-:1.1-org.fedoraproject.SetroubleshootPrivileged@2.service has finished successfully.

The job identifier is 3688.
Dec 16 13:16:41 server.dmbelicheva.net setroubleshoot[7613]: SELinux is preventing /usr/sbin/sshd from name_bind acce
ss on the tcp_socket port 2022. For complete SELinux messages run: sealert -l 8ed6ac2a-9568-4b46-8170-f5c769c980e1
Dec 16 13:16:41 server.dmbelicheva.net setroubleshoot[7613]: SELinux is preventing /usr/sbin/sshd from name_bind acce
ss on the tcp_socket port 2022.

                                                                  *****  Plugin bind_ports (92.2 confidence) suggests   **
**********************

                                                                  If you want to allow /usr/sbin/sshd to bind to network p
ort 2022

                                                                  Then you need to modify the port type.
                                                                  Do
                                                                  # semanage port -a -t PORT_TYPE -p tcp 2022
                                                                      where PORT_TYPE is one of the following: ssh_port_t,
```

Рис. 12: Мониторинг системных событий

# Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.dmbelicheva.net ssh]# semanage port -a -t ssh_port_t -p tcp 2022
[root@server.dmbelicheva.net ssh]# firewall-cmd --add-port=2022/tcp
success
[root@server.dmbelicheva.net ssh]# firewall-cmd --add-port=2022/tcp --permanent
success
```

**Рис. 13:** Настройка межсетевого экрана

# Настройка дополнительных портов для удалённого доступа по SSH

```
[root@server.dmbelicheva.net ssh]# systemctl restart sshd
[root@server.dmbelicheva.net ssh]# systemctl status -l sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
     Active: active (running) since Sat 2023-12-16 13:20:07 UTC; 3s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 7671 (sshd)
      Tasks: 1 (limit: 5724)
     Memory: 1.6M
        CPU: 23ms
     CGroup: /system.slice/sshd.service
             └─7671 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 16 13:20:07 server.dmbelicheva.net systemd[1]: Starting OpenSSH server daemon...
Dec 16 13:20:07 server.dmbelicheva.net sshd[7671]: main: sshd: ssh-rsa algorithm is disabled
Dec 16 13:20:07 server.dmbelicheva.net sshd[7671]: Server listening on 0.0.0.0 port 2022.
Dec 16 13:20:07 server.dmbelicheva.net sshd[7671]: Server listening on :: port 2022.
Dec 16 13:20:07 server.dmbelicheva.net sshd[7671]: Server listening on 0.0.0.0 port 22.
Dec 16 13:20:07 server.dmbelicheva.net sshd[7671]: Server listening on :: port 22.
Dec 16 13:20:07 server.dmbelicheva.net systemd[1]: Started OpenSSH server daemon.
[root@server.dmbelicheva.net ssh]#
```

**Рис. 14:** Расширенный статус работы sshd

# Настройка дополнительных портов для удалённого доступа по SSH

```
[dmbelicheva@server.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net
dmbelicheva@server.dmbelicheva.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec 16 13:28:11 2023 from 192.168.1.1
[dmbelicheva@server.dmbelicheva.net ~]$ sudo -i
[sudo] password for dmbelicheva:
[root@server.dmbelicheva.net ~]#
```

**Рис. 15:** Получение доступа к серверу посредством SSH-соединения

# Настройка дополнительных портов для удалённого доступа по SSH

```
[dmbelicheva@server.dmbelicheva.net ~]$ ssh -p 2022 dmbelicheva@server.dmbelicheva.net
dmbelicheva@server.dmbelicheva.net's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Dec 16 13:31:40 2023 from 192.168.1.1
[dmbelicheva@server.dmbelicheva.net ~]$ sudo -i
[sudo] password for dmbelicheva:
[root@server.dmbelicheva.net ~]#
```

**Рис. 16:** Получение доступа к серверу посредством SSH-соединения через порт 2022

# Настройка удалённого доступа по SSH по ключу

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

```
# Authentication:

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

PubkeyAuthentication yes
```

**Рис. 17:** Редактирование файла

# Настройка удалённого доступа по SSH по ключу

```
[dmbelicheva@client.dmbelicheva.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dmbelicheva/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/dmbelicheva/.ssh/id_rsa
Your public key has been saved in /home/dmbelicheva/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:izh9dYdMFLDsKz+7wtGaFXulsiXkKldHpcC4yo2oTjc dmbelicheva@client.dmbelicheva.net
The key's randomart image is:
+---[RSA 3072]----+
|         o..o.   |
|        ..oo  .  |
|         .o..o   |
|        ..ooo..  |
|     o +S+o++o.  |
|    .o+.oo0o=.   |
|  ..E o.+B.B     |
| ... o..Boo      |
| ..    o .++     |
+----[SHA256]-----+
[dmbelicheva@client.dmbelicheva.net ~]$
```

Рис. 18: Формирование ключа ssh

# Настройка удалённого доступа по SSH по ключу

```
[dmbelicheva@client.dmbelicheva.net ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/dmbelicheva/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/dmbelicheva/.ssh/id_rsa
Your public key has been saved in /home/dmbelicheva/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:izh9dYdMFLDsKz+7wtGaFXulsiXkKldHpcC4yo2oTjc dmbelicheva@client.dmbelicheva.net
The key's randomart image is:
+---[RSA 3072]----+
|         o..o.   |
|        ..oo  .  |
|         .o..o   |
|        ..ooo..  |
|     o +S+o++o.  |
|    .o+.oo0o=.   |
|  ..E o.+B.B     |
| ... o..Boo      |
| ..    o .++     |
+----[SHA256]-----+
[dmbelicheva@client.dmbelicheva.net ~]$
```

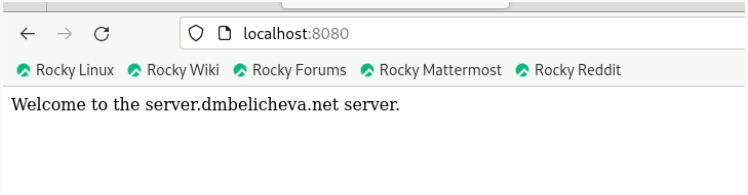
**Рис. 19:** Копирование открытого ssh ключа и получение доступа к серверу

# Организация туннелей SSH, перенаправление TCP-портов

```
[dmbelicheva@client.dmbelicheva.net ~]$ lsof | grep TCP
ssh       7088                    dmbelicheva    3u     IPv4              40984       0t0        TCP client.dmbelicheva
.net:37520->dhcp.dmbelicheva.net:ssh (ESTABLISHED)
[dmbelicheva@client.dmbelicheva.net ~]$ ssh -fNL 8080:localhost:80 dmbelicheva@server.dmbelicheva.net
[dmbelicheva@client.dmbelicheva.net ~]$ lsof | grep TCP
ssh       7088                    dmbelicheva    3u     IPv4              40984       0t0        TCP client.dmbelicheva
.net:37520->ns.dmbelicheva.net:ssh (ESTABLISHED)
ssh       7691                    dmbelicheva    3u     IPv4              58582       0t0        TCP client.dmbelicheva
.net:37930->ns.dmbelicheva.net:ssh (ESTABLISHED)
ssh       7691                    dmbelicheva    4u     IPv6              58606       0t0        TCP localhost:webcache
 (LISTEN)
ssh       7691                    dmbelicheva    5u     IPv4              58607       0t0        TCP localhost:webcache
 (LISTEN)
[dmbelicheva@client.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net hostname
```

**Рис. 20:** Перенаправление на порт 8080

На клиенте запустим браузер и в адресной строке введем localhost:8080. Убедимся, что отобразится страница с приветствием «Welcome to the server.dmbelicheva.net server».



# Запуск консольных приложений через SSH

```
[dmbelicheva@client.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net hostname
server.dmbelicheva.net
[dmbelicheva@client.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net ls -Al
total 76
-rw-------.  1 dmbelicheva dmbelicheva  301 Dec 16 13:33 .bash_history
-rw-r--r--.  1 dmbelicheva dmbelicheva   18 Jan 23  2023 .bash_logout
-rw-r--r--.  1 dmbelicheva dmbelicheva  141 Jan 23  2023 .bash_profile
-rw-r--r--.  1 dmbelicheva dmbelicheva  546 Nov  6 11:06 .bashrc
drwxr-xr-x. 15 dmbelicheva dmbelicheva 4096 Nov 13 17:24 .cache
drwx------. 12 dmbelicheva dmbelicheva 4096 Nov 24 17:05 .config
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Desktop
drwxr-xr-x.  3 dmbelicheva dmbelicheva   18 Dec  2 19:06 Documents
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Downloads
drwx------.  4 dmbelicheva dmbelicheva   32 Nov  6 10:54 .local
drwx------.  5 dmbelicheva dmbelicheva 4096 Dec 11 10:30 Maildir
drwxr-xr-x.  5 dmbelicheva dmbelicheva   54 Nov 13 17:24 .mozilla
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Music
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Pictures
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Public
drwx------.  2 dmbelicheva dmbelicheva   71 Dec 16 13:39 .ssh
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Templates
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-clipboard-tty1-control.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-clipboard-tty1-service.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-display-svga-x11-tty1-control.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-display-svga-x11-tty1-service.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-draganddrop-tty1-control.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-draganddrop-tty1-service.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:22 .vboxclient-hostversion-tty1-control.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-seamless-tty1-control.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:21 .vboxclient-seamless-tty1-service.pid
-rw-r-----.  1 dmbelicheva dmbelicheva    6 Dec 16 12:22 .vboxclient-vmsvga-session-tty1-control.pid
drwxr-xr-x.  2 dmbelicheva dmbelicheva    6 Nov  6 10:54 Videos
-rw-------.  1 dmbelicheva dmbelicheva  318 Dec 16 12:21 .xsession-errors
-rw-------.  1 dmbelicheva dmbelicheva  318 Dec 11 09:24 .xsession-errors.old
[dmbelicheva@client.dmbelicheva.net ~]$ ssh dmbelicheva@server.dmbelicheva.net MAIL=~/Maildir/ mail
s-nail version v14.9.22.  Type `?' for help
/home/dmbelicheva/Maildir: 7 messages
▸   1 dmbelicheva@dmbelich  2023-12-08 19:57   14/485   "test1                 "
    2 Belicheva Daria       2023-12-08 18:11   18/679   "test                  "
    3 Belicheva Daria       2023-12-09 12:50   18/671   "test2                 "
    4 Belicheva Daria       2023-12-09 12:55   22/844   "test3                 "
    5 Belicheva Daria       2023-12-09 13:24   22/850   "test                  "
    6 Belicheva Daria       2023-12-11 10:29   22/843   "test                  "
    7 root                  2023-12-11 10:30   21/842   "test1                 "
```

# Запуск графических приложений через SSH (X11Forwarding)

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

**Рис. 23:** Редактирование файла

# Запуск графических приложений через SSH (X11Forwarding)

```
^C[dmbelicheva@client.dmbelicheva.net ~]$ ssh -YC dmbelicheva@server.dmbelicheva.net firefox
/usr/bin/xauth:  file /home/dmbelicheva/.Xauthority does not exist
Crash Annotation GraphicsCriticalError: |[0][GFX1-]: glxtest: ManageChildProcess failed
 (t=4.72477) [GFX1-]: glxtest: ManageChildProcess failed

Crash Annotation GraphicsCriticalError: |[0][GFX1-]: glxtest: ManageChildProcess failed
 (t=4.72477) |[1][GFX1-]: glxtest: X error, error_code=1, request_code=154, minor_code=1 (t=4.72659) [GFX1-]: glxtest:
 X error, error_code=1, request_code=154, minor_code=1
```

**Рис. 24:** Запуск графических приложений через SSH

# Запуск графических приложений через SSH (X11Forwarding)

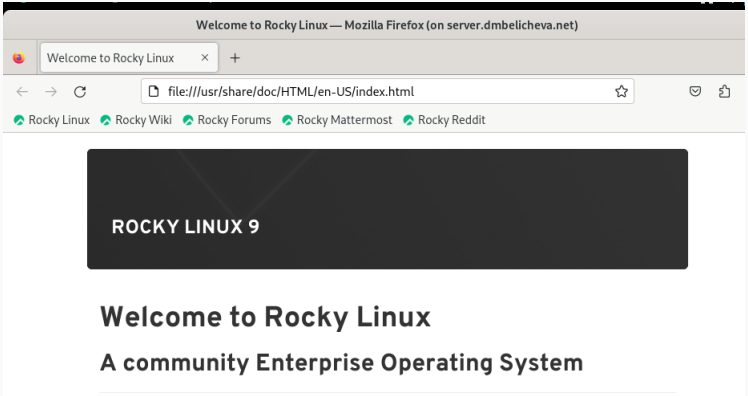



**Рис. 25:** Результат запуска графического приложения через SSH

# Внесение изменений в настройки внутреннего окружения виртуальной машины

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/ssh/etc/ssh
cp -R /etc/ssh/sshd_config /vagrant/provision/server/ssh/etc/ssh/
```

# Внесение изменений в настройки внутреннего окружения виртуальной машины

```
cd /vagrant/provision/server
touch ssh.sh
chmod +x ssh.sh
```

# Внесение изменений в настройки внутреннего окружения виртуальной машины

root@server:/vagrant/provision/server

GNU nano 5.6.1 ssh.sh

```
#!/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
```

**Рис. 26:** Редактирование файла

# Внесение изменений в настройки внутреннего окружения виртуальной машины

```
server.vm.provision "server ssh",
  type: "shell",
  preserve_order: true,
  path: "provision/server/ssh.sh"
```

# Выводы

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