

# **Лабораторная работа №11**

**Настройка безопасного удалённого доступа по протоколу SSH**

Беличева Дарья Михайловна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
3.1	Запрет удалённого доступа по SSH для пользователя root . . . . .	6
3.2	Ограничение списка пользователей для удалённого доступа по SSH	8
3.3	Настройка дополнительных портов для удалённого доступа по SSH	10
3.4	Настройка удалённого доступа по SSH по ключу . . . . .	13
3.5	Организация туннелей SSH, перенаправление TCP-портов . . . . .	15
3.6	Запуск консольных приложений через SSH . . . . .	16
3.7	Запуск графических приложений через SSH (X11Forwarding) . . . . .	17
3.8	Внесение изменений в настройки внутреннего окружения виртуальной машины . . . . .	19
<b>4</b>	<b>Выводы</b>	<b>21</b>

## Список иллюстраций

3.1	Мониторинг системных событий . . . . .	6
3.2	Получение доступа к серверу посредством SSH-соединения . . . .	7
3.3	Редактирование файла . . . . .	7
3.4	Получение доступа к серверу посредством SSH-соединения . . . .	8
3.5	Получение доступа к серверу посредством SSH-соединения . . . .	8
3.6	Редактирование файла . . . . .	9
3.7	Получение доступа к серверу посредством SSH-соединения . . . .	9
3.8	Редактирование файла . . . . .	10
3.9	Получение доступа к серверу посредством SSH-соединения . . . .	10
3.10	Редактирование файла . . . . .	11
3.11	Расширенный статус работы sshd . . . . .	11
3.12	Мониторинг системных событий . . . . .	12
3.13	Настройка межсетевого экрана . . . . .	12
3.14	Расширенный статус работы sshd . . . . .	12
3.15	Получение доступа к серверу посредством SSH-соединения . . . .	13
3.16	Получение доступа к серверу посредством SSH-соединения через порт 2022 . . . . .	13
3.17	Редактирование файла . . . . .	14
3.18	Формирование ключа ssh . . . . .	14
3.19	Копирование открытого ssh ключа и получение доступа к серверу	15
3.20	Перенаправление на порт 8080 . . . . .	16
3.21	localhost:8080 . . . . .	16
3.22	Запуск консольных приложений через SSH . . . . .	17
3.23	Редактирование файла . . . . .	18
3.24	Запуск графических приложений через SSH . . . . .	18
3.25	Результат запуска графического приложения через SSH . . . . .	18
3.26	Редактирование файла . . . . .	19

# 1 Цель работы

Приобрести практические навыки по настройке удалённого доступа к серверу с помощью SSH.

## 2 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 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.

## 3 Выполнение лабораторной работы

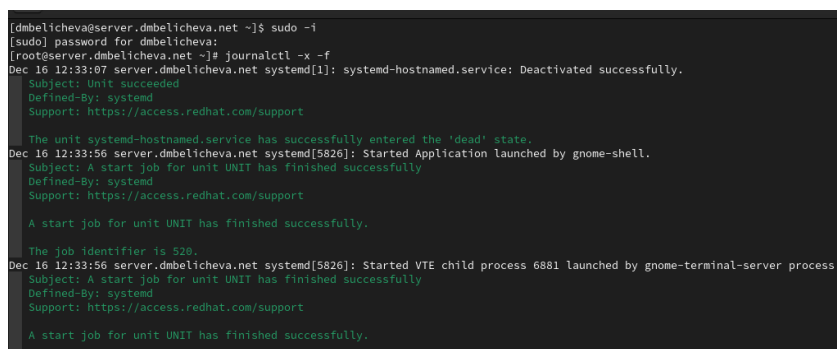
### 3.1 Запрет удалённого доступа по SSH для пользователя root

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

```
sudo -i  
passwd root
```

На сервере в дополнительном терминале запустим мониторинг системных событий:

```
sudo -i  
journalctl -x -f
```



```
[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 529.  
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. 3.1: Мониторинг системных событий

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/IUBYBydgr4.
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).
```

Рис. 3.2: Получение доступа к серверу посредством SSH-соединения

В доступе отказано.

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

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

# Authentication:

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

Рис. 3.3: Редактирование файла

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

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

```

[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. 3.4: Получение доступа к серверу посредством SSH-соединения

В доступе с клиента к серверу посредством SSH соединения через пользователя root отказано. Так и должно быть, ведь мызапретили вход на сервер пользователю root.

## 3.2 Ограничение списка пользователей для удалённого доступа по SSH

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

```

[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. 3.5: Получение доступа к серверу посредством SSH-соединения

Соединение через пользователя dmbelicheva произошло успешно.

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



```
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. 3.6: Редактирование файла

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

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

```
[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. 3.7: Получение доступа к серверу посредством SSH-соединения

В доступе отказано.

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

```
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

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

Рис. 3.8: 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.

```
[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. 3.9: Получение доступа к серверу посредством SSH-соединения

Теперь доступ успешно получен, поскольку мы разрешили пользователю dmbelicheva доступ к серверу посредством ssh.

### 3.3 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:

Port 22

Port 2022

```
# 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. 3.10: Редактирование файла

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.

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

Посмотрим расширенный статус работы sshd: systemctl status -l sshd

```
[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/ssh.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/ssh.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. 3.11: Расширенный статус работы sshd

Система должна сообщить вам об отказе в работе sshd через порт 2022. Дополнительно посмотрим сообщения в терминале с мониторингом системных событий.

```
A start job for unit dbus-1.1-org.fedoraproject.SetroubleshootPrivileged02.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 access 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 access 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 ports 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, ssh_port_t,
```

Рис. 3.12: Мониторинг системных событий

Видно, что отказ происходит из-за запрета SELinux на работу с этим портом.

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

В настройках межсетевого экрана откроем порт 2022 протокола TCP:

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

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

```
[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. 3.13: Настройка межсетевого экрана

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

```
[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/ssh.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/ssh.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. 3.14: Расширенный статус работы `sshd`

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

```
[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. 3.15: Получение доступа к серверу посредством SSH-соединения

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

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

```
[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. 3.16: Получение доступа к серверу посредством SSH-соединения через порт 2022

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

### 3.4 Настройка удалённого доступа по SSH по ключу

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

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

```
# Authentication:

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

PubkeyAuthentication yes
```

Рис. 3.17: Редактирование файла

После сохранения изменений в файле конфигурации перезапустим sshd.

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

Когда спросят, хотим ли мы использовать кодовую фразу, нажмем Enter, чтобы использовать установку без пароля. При запросе имени файла, в котором будет храниться закрытый ключ, примем предлагаемое по умолчанию имя файла (`~/.ssh/id_rsa`). Когда попросят ввести кодовую фразу, нажмем Enter дважды.

```
[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+7wt6aFXulsiXkKldHpcC4yo2oTjc 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. 3.18: Формирование ключа ssh

Закрытый ключ теперь будет записан в файл `~/.ssh/id_rsa`, а открытый ключ записывается в файл `~/.ssh/id_rsa.pub`.

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

При запросе введем пароль пользователя на удалённом сервере.

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

```
[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. 3.19: Копирование открытого ssh ключа и получение доступа к серверу

Теперь пройдем аутентификацию без ввода пароля для учётной записи удалённого пользователя.

## 3.5 Организация туннелей SSH, перенаправление

### TCP-портов

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

Перенаправим порт 80 на server.dmbelicheva.net на порт 8080 на локальной машине: `ssh -fNL 8080:localhost:80 dmbelicheva@server.dmbelicheva.net`

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

```

connection to server.dmbelicheva.net 60950
[dmbelicheva@client.dmbelicheva.net ~]$ ss -ltn | grep TCP
ssh      7688      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 ~]$ ss -ltn | grep TCP
ssh      7688      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 -fNL 8080:localhost:80 dmbelicheva@server.dmbelicheva.net hostname

```

Рис. 3.20: 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».

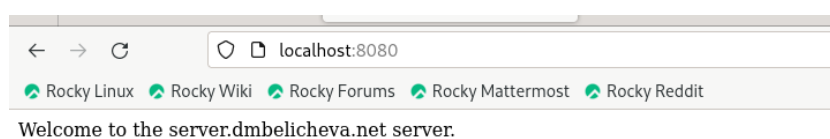


Рис. 3.21: localhost:8080

## 3.6 Запуск консольных приложений через SSH

На клиенте откройте терминал под пользователем dmbelicheva. Посмотрите с клиента имя узла сервера: `ssh dmbelicheva@server.dmbelicheva.net hostname`

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

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



```

(dmbelicheva)
[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-r--r--. 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--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-clipboard-tty1-control.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-clipboard-tty1-service.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-display-svg-x11-tty1-control.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-display-svg-x11-tty1-service.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-draganddrop-tty1-control.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-draganddrop-tty1-service.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:22 .vboxclient-hostversion-tty1-control.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-seamless-tty1-control.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:21 .vboxclient-seamless-tty1-service.pid
-rw-r--r--. 1 dmbelicheva dmbelicheva 6 Dec 16 12:22 .vboxclient-vmvga-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"
AC[dmbelicheva@client.dmbelicheva.net ~]$

```

Рис. 3.22: Запуск консольных приложений через SSH

## 3.7 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 yes
#PermitTTY yes
#PrintMotd yes
```

Рис. 3.23: Редактирование файла

После сохранения изменения в конфигурационном файле перезапустим sshd. Попробуем с клиента удалённо подключиться к серверу и запустить графическое приложение, например firefox: `ssh -YC user@server.dmbelicheva.net firefox`

```
AC[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) [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. 3.24: Запуск графических приложений через SSH

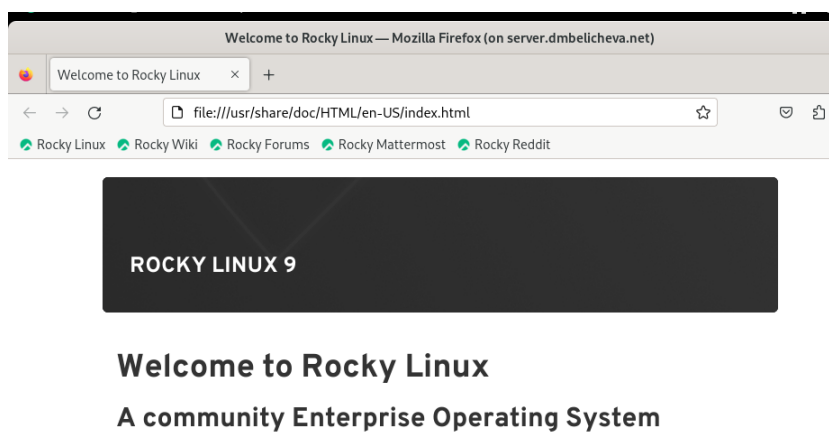


Рис. 3.25: Результат запуска графического приложения через SSH

## 3.8 Внесение изменений в настройки внутреннего окружения виртуальной машины

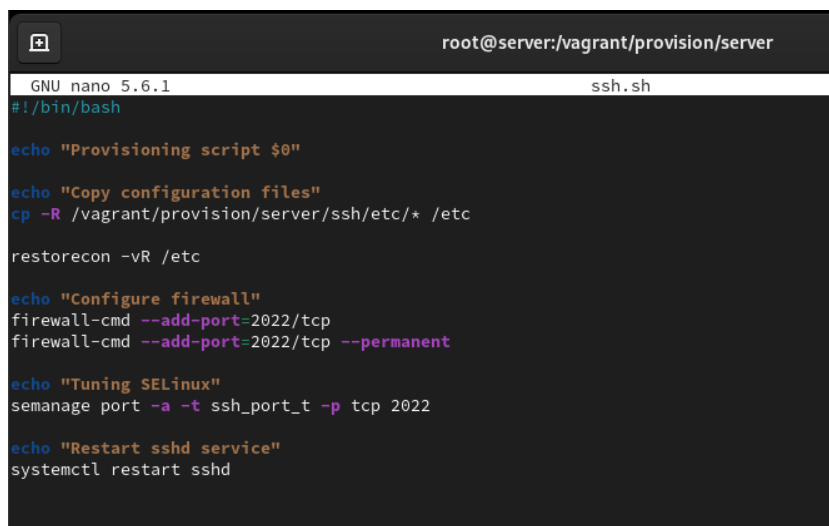
На виртуальной машине `server` перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `ssh`, в который поместим в соответствующие подкаталоги конфигурационный файл `sshd_config`:

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

В каталоге `/vagrant/provision/server` создадим исполняемый файл `ssh.sh`:

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

Открыв его на редактирование, пропишем в нём следующий скрипт:

A screenshot of a terminal window with a dark background. The title bar at the top shows a window icon, a close button, and the text 'root@server:/vagrant/provision/server'. The terminal content shows the GNU nano 5.6.1 editor editing the file 'ssh.sh'. The first line is the shebang '#!/bin/bash'. The script contains several echo statements for logging and several system commands: 'cp -R /vagrant/provision/server/ssh/etc/\* /etc', 'restorecon -vR /etc', 'firewall-cmd --add-port=2022/tcp' and 'firewall-cmd --add-port=2022/tcp --permanent', 'semanage port -a -t ssh\_port\_t -p tcp 2022', and 'systemctl restart sshd'.

```
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. 3.26: 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"
```

## 4 Выводы

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